kaspersky

# Kaspersky Embedded Systems Security 4.0 for Windows

© 2025 AO Kaspersky Lab

# 目次


Kaspersky Embedded Systems Security for Windows
- 新機能
- 製品の購入
- システム要件
- サポート対象の Kaspersky Security Center のバージョン
- 機能要件および制限事項
  - 本製品のインストールと削除
  - システム変更監視
  - ファイアウォール
  - 古いバージョンの Windows における制限
  - Kaspersky Security Center との連携
  - その他の制限事項
- 他のアプリケーションとの互換性情報

本製品のインストールと削除
- インストールの計画
  - 管理ツールの選択
  - インストール方法の選択
- ウィザードを使用した製品のインストールとアンインストール
  - セットアップウィザードを使用したインストール
    - Kaspersky Embedded Systems Security のインストール
    - Kaspersky Embedded Systems Security コンソールのインストール
    - アプリケーションコンソールを別のデバイスにインストールした後の詳細設定
      - COM アプリケーションへの匿名リモートアクセスの許可
      - Kaspersky Embedded Systems Security リモート管理プロセスに対するネットワーク接続の許可
    - Kaspersky Embedded Systems Security インストール後に実行する処理
      - 定義データベースと製品機能のアップデートタスクの開始と設定
      - 簡易スキャン
  - コンポーネントセットの変更と Kaspersky Embedded Systems Security の修復
  - セットアップウィザードを使用したアンインストール
    - Kaspersky Embedded Systems Security のアンインストール
    - Kaspersky Embedded Systems Security コンソールのアンインストール
- コマンドラインによる製品のインストールとアンインストール
  - コマンドラインからの Kaspersky Embedded Systems Security のインストールとアンインストール
  - Windows インストーラーサービスでの Kaspersky Embedded Systems Security ソフトウェアコンポーネントの指定時に使用するコンポーネントコード
    - Kaspersky Embedded Systems Security ソフトウェアコンポーネント
    - 「管理ツール」ソフトウェアコンポーネント
  - インストールと復元の設定、および Windows インストーラーのコマンドラインオプション
  - Kaspersky Embedded Systems Security のインストールで使用するコマンド事例
  - Kaspersky Embedded Systems Security インストール後に実行する処理
  - コンポーネントの追加および削除：サンプルコマンド
  - Kaspersky Embedded Systems Security のアンインストール：サンプルコマンド
  - リターンコード

Kaspersky Security Center を使用した製品のインストールとアンインストール
Kaspersky Security Center を使用したインストールに関する全般的な情報
Kaspersky Embedded Systems Security をインストールまたはアンインストールする権限
Kaspersky Security Center を使用した Kaspersky Embedded Systems Security のインストール
Kaspersky Embedded Systems Security インストール後に実行する処理
Kaspersky Security Center を使用したアプリケーションコンソールのインストール
Kaspersky Security Center を使用した Kaspersky Embedded Systems Security のアンインストール
Kaspersky Security Center を使用した製品コンポーネントのセットの変更
Active Directory のグループポリシーを使用した本製品のインストールとアンインストール
Active Directory のグループポリシーを使用した Kaspersky Embedded Systems Security のインストール
Kaspersky Embedded Systems Security インストール後に実行する処理
Active Directory のグループポリシーを使用した Kaspersky Embedded Systems Security のアンインストール
Kaspersky Embedded Systems Security のインストールログとアンインストールログ
Kaspersky Embedded Systems Security インストール後のシステム変更
Kaspersky Embedded Systems Security プロセス
Kaspersky Embedded Systems Security の機能のテスト：テスト用ウイルス EICAR の使用
テスト用ウイルス EICAR について
ファイルのリアルタイム保護機能とオンデマンドスキャン機能のテスト
旧バージョンの Kaspersky Embedded Systems Security のバージョン 4.0 へのアップグレード
Kaspersky Embedded Systems Security のアップデート
Kaspersky Embedded Systems Security の管理ツールのアップデート
ポリシーおよびタスクの移行
アップデート中の製品バージョンの設定の移行
Kaspersky Embedded Systems Security バージョン 3.4 および 4.0 のコンポーネントとタスクの対応
製品のインターフェイス
管理プラグインの使用
Kaspersky Security Center を使用した Kaspersky Embedded Systems Security の管理
アプリケーション設定の管理
操作方法
アプリケーションのプロパティウィンドウでの全般的な製品設定の表示と編集
ポリシーでの全般的な製品設定の表示と編集
Kaspersky Security Center での全般的なアプリケーション設定
Kaspersky Security Center でのインターフェイスおよびスキャンの設定
Kaspersky Security Center でのセキュリティ設定
Kaspersky Security Center を使用した接続の設定
ローカルタスクのスケジュールによる開始の設定
Kaspersky Security Center でのバックアップ設定
ポリシーの作成と編集
ポリシーの作成
ポリシーの設定
セキュリティレベルインジケーター
Kaspersky Security Center を使用したタスクの作成と編集
Kaspersky Security Center でのタスクの作成について
Kaspersky Security Center を使用したタスクの作成
個々のコンピューターのローカルタスク設定と全般的な製品設定への移動

Kaspersky Security Center でのグループタスクの設定
本製品のアクティベーションタスク
アップデートタスク
アプリケーションの整合性チェック
タスクスケジュールの管理
タスクのスケジュールを設定する
スケジュールに従ったタスクの有効化と無効化
Kaspersky Security Center のレポート
Kaspersky Embedded Systems Security コンソールの使用
アプリケーションコンソールの起動
Kaspersky Embedded Systems Security コンソールのインターフェイス
Kaspersky Embedded Systems Security コンソールのウィンドウ
通知領域のシステムトレイアイコン
アプリケーションコンソールを使用した全般設定
Kaspersky Embedded Systems Security タスクの管理
Kaspersky Embedded Systems Security タスクのカテゴリ
手動でのタスクの開始、一時停止、再開、停止
タスクスケジュールの管理
タスクスケジュールの設定
スケジュールに従ったタスクの有効化と無効化
タスクを開始するユーザーアカウントの使用
タスク実行用のアカウントについて
タスクを実行するユーザーアカウントの指定
設定のインポートとエクスポート
設定のインポートとエクスポートについて
設定のエクスポート
設定のインポート
保護ステータスと Kaspersky Embedded Systems Security の情報の表示
Web コンソールおよび Cloud コンソールからの Web プラグインの操作
Web コンソールおよび Cloud コンソールを使用した Kaspersky Embedded Systems Security の管理
Web プラグインの制限事項
アプリケーション設定の管理
Web プラグインでの全般的なアプリケーション設定
Web プラグインでのインターフェイスおよびスキャンの設定
Web プラグインでのセキュリティと信頼性の設定
Web プラグインでの接続設定
Web プラグインでローカルタスクのスケジュールによる開始の設定
Web プラグインでのバックアップ設定
ポリシーの作成と編集
Kaspersky Security Center を使用したタスクの作成と編集
Web プラグインでのタスク作成について
Web プラグインでのタスクの作成
Web プラグインでのグループタスクの設定
Web プラグインでの本製品のアクティベーションタスクの設定
Web プラグインでのアップデートタスクの設定

タスクスケジュールの管理
タスクのスケジュールを設定する
スケジュールに従ったタスクの有効化と無効化
Kaspersky Security Center のレポート
製品のライセンス
使用許諾契約書について
ライセンスの概要
ライセンス証明書について
ライセンス情報について
ライセンス情報ファイルについて
アクティベーションコードの概要
ライセンス種別による製品機能の比較
ライセンス情報ファイルによる製品のアクティベーション
アクティベーションコードによる製品のアクティベーション
現在のライセンスに関する情報の表示
ライセンスの更新
ライセンスの削除
データの提供について
欧州連合の規則（GDPR）の順守
Kaspersky Embedded Systems Security の起動と終了
本製品の起動と停止
プロテクションとコントロールの一時停止と再開
コンパクト診断インターフェイス
コンパクト診断インターフェイスについて
コンパクト診断インターフェイスを使用した Kaspersky Embedded Systems Security ステータスの確認
セキュリティイベント統計の確認
現在のアプリケーション動作の確認
アプリケーショントレースとメモリダンプの記録の設定
Kaspersky Embedded Systems Security のセルフディフェンス機構
セルフディフェンスの有効化と無効化
AM-PPL 技術のサポート
オペレーティングシステムのサービスの保護
Kaspersky Embedded Systems Security を管理するためのユーザー権限の設定
Kaspersky Security サービスを管理するためのユーザーアクセス権限
Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス
セキュアデスクトップの通知
信頼ゾーン
信頼するオブジェクトの作成
検知可能なオブジェクトの選択
信頼するアプリケーションのリストの編集
ローカルの信頼ゾーンの作成
信頼ゾーンでのエクスポート / インポート
信頼するシステム証明書ストアの使用
ファイルのリアルタイム保護
タスクの保護範囲とセキュリティ設定について
定義済みの保護範囲
定義済みのセキュリティレベルについて

ファイルのリアルタイム保護コンポーネントで既定でスキャンされるファイルの拡張子
ファイルのリアルタイム保護コンポーネントの設定
ファイルのリアルタイム保護コンポーネントの保護範囲の設定
手動でのセキュリティの設定
コンテナーのスキャン
KSN の使用
Kaspersky Security Network の使用の有効化
Kaspersky Security Network の使用統計情報
Kaspersky Private Security Network
KSN プロキシ設定
脆弱性攻撃ブロック
脆弱性攻撃ブロックモード
脆弱性攻撃ブロックの有効化と無効化
メモリ保護の有効化と無効化
保護対象プロセスのリストの作成
修復エンジン
ふるまい検知
ローカルフォルダーの暗号化保護の有効化と無効化
外部からの暗号化に対する共有フォルダーの保護
外部からの暗号化に対する共有フォルダーの保護の有効化または無効化
保護範囲の作成
外部データ暗号化用の信頼できるコンピューターの追加
信頼できないコンピューターのブロック期間の設定
外部からの暗号化に対する共有フォルダーの保護の除外リストのエクスポートおよびインポート
ネットワーク脅威対策
AMSI スキャナー
AMSI スキャナーの有効化と無効化
AMSI スキャナーの設定
アプリケーション起動コントロール
アプリケーション起動コントロールルールについて
ソフトウェア配布コントロールについて
アプリケーション起動コントロールルールの自動生成の設定
アプリケーション起動コントロールの有効化と設定
ソフトウェア配布コントロールの設定
アプリケーション起動コントロールルールとの影響関係
アプリケーション起動コントロールルールの追加
アプリケーション起動コントロールルールの適用条件の追加
アプリケーション起動コントロールルールの範囲から除外する項目の追加
「既定で許可」モードを有効にする
Kaspersky Security Center のブロック対象のアプリケーションのイベントの抽出を含む TXT ファイルの生成
アプリケーション起動コントロールルールの自動生成グループタスクの設定
アプリケーション起動コントロールルールの自動生成グループタスクを使用したルールの作成
デバイスコントロール
デバイスアクセスルール
種別ごとのデバイスアクセス制御
Wi-Fi 接続の制御
プリンターのコントロール

入力デバイスコントロール（HID）
リムーバブルドライブの使用状況の監視
Bluetooth デバイスへのアクセスの管理
デバイスに対するユーザーアクセス権の区別
外部デバイスの監査
信頼するデバイスの追加
信頼するデバイスのリストのエクスポート / インポート
ファイアウォール
ファイアウォールのルールについて
ファイアウォールの設定
ファイアウォールの全般的な設定
ファイアウォールルールの作成と設定
ファイアウォールのルールの有効化と無効化
有害 USB 攻撃ブロック
システム変更監視
システム変更監視ルールについて
リアルタイムシステム変更監視
オンデマンドのシステム変更チェック
システム変更監視ルールのエクスポートとインポート
システム変更監視レポートの表示
Windows イベントログ監視
カスタムルールの追加
事前定義済みのルールの設定
オンデマンドスキャン
オンデマンドスキャンタスクについて
タスクのスキャン範囲とセキュリティ設定について
定義済みのスキャン範囲
オンラインストレージのファイルのスキャン
定義済みのセキュリティレベルについて
リムーバブルドライブスキャン
オンデマンドスキャンタスクの既定の設定
オンデマンドスキャンの管理
操作方法
オンデマンドスキャンタスクウィザード
オンデマンドスキャンタスクの設定ウィンドウ
オンデマンドスキャンタスクの作成
オンデマンドスキャンタスクのバックグラウンドでの実行
簡易スキャンの実行の登録
オンデマンドスキャンタスクでのスキャン範囲の設定
オンデマンドスキャンタスクの設定
リムーバブルドライブスキャンの設定
オンデマンドスキャンタスクの定義済みセキュリティレベルの選択
手動でのセキュリティの設定
オンデマンドスキャンタスクの統計情報
Kaspersky Embedded Systems Security データベースおよびソフトウェアモジュールのアップデート
定義データベースと製品機能のアップデート
アップデートタスクについて

Kaspersky Embedded Systems Security の定義データベースとモジュールのアップデートスキーム
アップデートタスクの設定
本製品の SMU アップデート
Kaspersky Embedded Systems Security 定義データベースのロールバック
アップデートタスクの統計情報
オブジェクトのバックアップコピーの作成
オブジェクトのバックアップコピーの作成：バックアップ
バックアップ内のオブジェクトの表示
「バックアップ」内のファイルの並べ替え
「バックアップ」内のファイルのフィルタリング
バックアップからのファイルの復元
バックアップからのファイルの削除
感染の可能性があるオブジェクトを分析するためのカスペルスキーへの送信
バックアップの設定
バックアップの統計情報
ネットワークリソースへのアクセスのブロック：ブロック対象ネットワークセッション
ブロック対象のネットワークセッションのリスト
ブロック対象のネットワークセッションのリストの管理
イベントの登録：Kaspersky Embedded Systems Security のログ
Kaspersky Embedded Systems Security のイベントを登録する方法
ログ設定の指定
ログ内のイベントの並べ替え
ログ内のイベントのフィルタリング
ログからのイベントの削除
ログからの情報のエクスポート
システム監査ログ
実行ログ
タスク実行ログでの Kaspersky Embedded Systems Security のタスクに関する統計と情報の表示
イベントビューアでの Kaspersky Embedded Systems Security のイベントログの表示
SIEM 連携について
SIEM 連携設定
管理者およびユーザーへの通知方法
管理者およびユーザーへの通知の設定
メール通知の設定
管理サーバーとのインタラクションの設定
Managed Detection and Response
MDR 連携設定
テクニカルサポートへのお問い合わせ
テクニカルサポートの利用方法
カスペルスキーカンパニーアカウントからのテクニカルサポート
テクニカルサポートの担当者への詳細な診断情報の提供
アプリケーションの動作のトレース
メモリダンプの記録
Kaspersky Embedded Systems Security に関する情報源
用語解説
Kaspersky Security Network（KSN）
OLE オブジェクト

SIEM
アーカイブ
アップデート
イベントの重要性
隔離
感染したオブジェクト
感染の可能性があるファイル
管理サーバー
駆除
現在のライセンス
誤検知
スタートアップオブジェクト
脆弱性
セキュリティレベル
タスク
タスクの設定
定義データベース
バックアップ
ヒューリスティックアナライザー
ファイル名マスク
保護ステータス
ポリシー
ライセンスの有効期間
ローカルタスク
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
補足資料
簡易スキャンのファイルの拡張子
アプリケーションコンポーネントルールのユーザーアカウント

# Kaspersky Embedded Systems Security for Windows

Kaspersky Embedded Systems Security for Windows（以降「Kaspersky Embedded Systems Security」とも表記）は、Microsoft® Windows® のコンピューターおよびその他の組み込みシステム（以降、「保護対象デバイス」とも表記）をウイルスやその他のコンピューターの脅威から保護します。Kaspersky Embedded Systems Security の対象ユーザーは、企業ネットワークをアンチウイルスによって保護することを責務とする企業のネットワーク管理者およびスペシャリストです。

本製品は、自動制御システムを伴う技術プロセスでの使用を想定していません。そのようなシステムでデバイスを保護するには、Kaspersky Industrial CyberSecurity for Nodes の使用を推奨します。

Kaspersky Embedded Systems Security は、Windows の様々な組み込みシステムにインストールできます。それには、次のデバイス種別も含まれます：

- ATM（現金自動預払機）
- POS（販売時点情報管理システム）

Kaspersky Embedded Systems Security は次の方法で管理できます：

- Kaspersky Embedded Systems Security と同じ保護対象デバイスまたは異なるデバイスにインストールされたアプリケーションコンソールを使用する方法
- コマンドラインでコマンドを使用する方法
- Kaspersky Security Center 管理コンソールを使用する方法

Kaspersky Security Center アプリケーションを使用して、Kaspersky Embedded Systems Security を実行している複数の保護対象デバイスを一元管理することもできます。

「システム監視」アプリケーション用の Kaspersky Embedded Systems Security のパフォーマンスカウンターに加えて、SNMP カウンターおよび SNMP トラップを確認することができます。

## Kaspersky Embedded Systems Security のコンポーネントと機能

本製品には、次のコンポーネントが含まれています：

- **ファイルのリアルタイム保護**：Kaspersky Embedded Systems Security はオブジェクトがアクセスされたタイミングでスキャンを行います。Kaspersky Embedded Systems Security は次のオブジェクトをスキャンします：
  - ファイル
  - 代替のファイルシステムストリーム（NTFS ストリーム）
  - ローカルハードディスクおよびリムーバブルドライブのマスターブートレコードとブートセクター

- **オンデマンドスキャン**：Kaspersky Embedded Systems Security は、指定した領域で、ウイルスやその他のコンピューターセキュリティの脅威のスキャンを1回実行します。保護対象デバイスで、ファイルやメモリ、自動実行オブジェクトをスキャンします。

- **アプリケーション起動コントロール**：このコンポーネントは、ユーザーによるアプリケーションの起動試行を監視し、保護対象デバイスでのアプリケーションの起動を規制します。

- **デバイスコントロール**：外部デバイスとの登録と使用を制御し、USB 接続フラッシュドライブやその他の種別の外部デバイスとファイルを交換している際に発生する可能性のあるコンピューターセキュリティの脅威からデバイスを保護します。

- **ファイアウォール**：コンポーネントは、モードに応じて、Windows ファイアウォールによるトラフィックのフィルタリングを監視したり、保護されたコンピューターのネットワーク動作に関するイベントをコンポーネントのログに記録することだけを行ったり、ファイアウォールの設定に従ってネットワークトラフィックをフィルタリングしたりします。

- **ファイル変更監視**：Kaspersky Embedded Systems Security では、タスク設定で指定された監視範囲内のファイルの変更が検出されます。これらの変更は、保護対象デバイスでのセキュリティ侵害を示している場合があります。

- **Windows イベントログ監視**：このコンポーネントは、Windows イベントログの検査の結果に基づいて、保護された環境の整合性を監視します。

この製品で実装されている機能は次の通りです：

- **定義データベースと製品機能のアップデート**：Kaspersky Embedded Systems Security は、カスペルスキーの FTP または HTTP アップデートサーバー、Kaspersky Security Center 管理サーバー、またはその他のアップデート元から定義データベースやモジュールのアップデートをダウンロードします。

- **隔離**：Kaspersky Embedded Systems Security は、感染の可能性があるオブジェクトを、元の場所から*隔離*フォルダーに移動することで隔離します。セキュリティ上の理由から、隔離フォルダーのオブジェクトは暗号化されて保存されます。

- **バックアップ**：Kaspersky Embedded Systems Security では、*感染*分類されたオブジェクトの暗号化されたコピーが、駆除または削除の前にバックアップに保存されます。

- **管理者およびユーザーへの通知**：保護対象デバイスにアクセスする管理者とユーザーに、Kaspersky Embedded Systems Security の動作中のイベント、およびデバイスのアンチウイルス保護ステータスについて通知するよう設定できます。

- **設定のインポートとエクスポート**：Kaspersky Embedded Systems Security の設定を XML 設定ファイルにエクスポートしたり、設定ファイルから Kaspersky Embedded Systems Security に設定をインポートしたりすることができます。設定ファイルには、すべてのアプリケーション設定または個別のコンポーネント設定のみを保存できます。

- **テンプレートの適用**：保護対象デバイスのファイルリソースのツリー内またはリスト内のフォルダーのセキュリティ設定を手動で設定し、その設定値をテンプレートとして保存できます。その後、そのテンプレートを使用して、Kaspersky Embedded Systems Security の保護やスキャンタスクで、他のフォルダーのセキュリティを設定できます。

- **Kaspersky Embedded Systems Security の各種機能に対するアクセス権限の管理**：アプリケーションに登録されているユーザーやグループユーザーに対して Kaspersky Embedded Systems Security サービスおよび Windows サービスを管理する権限を設定できます。

- **Windows イベントログへのイベントの書き込み**：Kaspersky Embedded Systems Security はソフトウェアコンポーネントの設定や、タスクの現在の状態、タスクの実行中に発生したイベント、Kaspersky Embedded Systems Security 管理に関連付けられたイベントなどの情報や、Kaspersky Embedded Systems Security におけるエラーの診断に必要な情報を記録します。

- **信頼ゾーン**：Kaspersky Embedded Systems Security がオンデマンドおよびコンピューターのリアルタイム保護タスクで適用する、保護またはスキャン範囲から除外する対象のリストを生成できます。

- **脆弱性攻撃ブロック**：外部の保護エージェントを使用して、プロセスメモリを脆弱性攻撃による注入から保護できます。

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

# 新機能

Kaspersky Embedded Systems Security 4.0 の新機能と改良点は次の通りです：

- アプリケーションコンソールのユーザーインターフェイスと、Kaspersky Security Center を使用して製品を管理するプラグインが大幅に更新されました。

- Windows 11 24H2 のサポート。

- アプリケーションコンソールが製品をインストールしたコンピューターに接続する際に使用するポートを変更することができるようになりました。

- *信頼ゾーン*の改善点：

  - 信頼するプロセスをより細かく設定できるようになりました。

  - 信頼する証明書ストアを使用することができるようになりました。

- 本製品を管理するユーザーおよびグループの権限を新しく設定できるようになりました。

- 新しい*アンチルートキット*コンポーネントが追加されました。既定では、*ファイルのリアルタイム保護*が有効になっているとコンポーネントも有効になっています。このコンポーネントは、製品のインストール中、*Kaspersky Embedded Systems Security の製品コンポーネントの変更*タスク、または製品のインストールパッケージのプロパティで無効にすることができます。

- *脆弱性攻撃ブロック*の設定で、保護されたプロセスを自動的に識別することができるようになりました。

- 新しく*修復エンジン*コンポーネントが追加されました。

- ネットワーク脅威対策コンポーネントは、ネットワークトラフィックを監視し、ポートスキャンや高強度のネットワーク要求を検出することができるようになりました。

- アプリケーションが Windows ファイアウォールに対応しました。アプリケーションをインストールするために Windows ファイアウォールを削除する必要がなくなりました。

- *ふるまい検知*コンポーネントは、ローカルフォルダーだけでなく共有フォルダーも監視するようになりました。

- *アプリケーション起動コントロール* コンポーネントの改善点：
  - コンポーネント設定構成を大幅に変更しました。
  - アプリケーション起動コントロールルールの適用条件と除外の指定に、ドライブ種別、KL カテゴリ、KSN グループを使用できるようになりました。
- *デバイスコントロール*コンポーネントの改善点：
  - 既定では、*デバイスコントロール*コンポーネントはすべてのデバイスの接続を許可するよう設定されています。
  - 以前独立したコンポーネントであった *Wi-Fi コントロール*はデバイスコントロールの一部となりました。
  - 接続バスに応じて接続機器を制御するオプションが追加されました。
  - 製品の以前のバージョンからバージョン 4.0 にアップグレードする際に、リムーバブルドライブへのアクセスに関する設定の移行が追加されました。
- *ファイアウォール管理*コンポーネントは、*ファイアウォール*コンポーネントに変更され、Windows ファイアウォールとの連携に加え、ファイアウォールとしての機能も追加されました。
- *ファイル変更監視*および*レジストリアクセス管理*コンポーネントは、新しく*システム変更監視* コンポーネントに統合されました。この改良により、ファイルシステムと Windows レジストリの変更を効率的に追跡できるようになり、データの不正変更に対する保護が強化されました。
- 本製品では、個々のコンポーネントのスケジュール設定はサポートされません。コンポーネントが有効になっている場合、本製品の実行中はコンポーネントも実行され続けます。
- Kaspersky Security Center Windows 15.1 がサポートされるようになりました。
- 次のグループタスクが追加されました：
  - *管理サーバーの接続の保護*
  - *Kaspersky Embedded Systems Security のコンポーネントセットの変更*
  - *ベースラインシステム変更監視*（*ベースラインファイル変更監視*から変更されました）
  - *アップデート*（*アップデートのコピー*、*定義データベースのアップデート*、*ソフトウェアモジュールのアップデート*から変更されました）
  - *アップデートのロールバック*（*定義データベースのロールバック*から変更されました）
  - *ライセンスの削除*
- 本製品は、設定を保存する前に、管理コンポーネントの設定を確認します。アプリケーション起動コントロール、デバイスコントロール、システム変更監視のコンポーネントのチェックが追加されました。管理コンポーネントの現在の設定によってコンピューターの負荷が増加したり、システム障害が発生したりする可能性がある場合に、本製品で警告が表示されるようになりました。たとえば、アプリケーション起動コントロールで、許可されたアプリケーションを除くすべてのアプリケーションをブロックするモードを選択し、許可ルールを追加していないと、このような設定ではシステム障害が発生する可能性があるため、本製品で警告が表示されます。

- アプリケーション起動コントロールの許可ルールを自動的に作成し、これらのルールをファイルにエクスポートするオプションが追加されました。これを行うには、*アプリケーション起動コントロールルールの自動生成*タスクを実行し、実行中のアプリケーションに基づく許可ルールの自動作成と許可ルールのエクスポートを有効にします。生成されたファイルを使用して、デバイスにインストールされているソフトウェアをインベントリできます。

- 新しいコンポーネント、*有害 USB 攻撃ブロック*が追加されました。有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。オペレーティングシステムがキーボードとして識別する USB デバイスがコンピューターに接続されると、本製品は、キーボードを認証するためにこのキーボードで入力するようにユーザーに要求します。

- *セキュリティレベルインジケーター*が追加されました。セキュリティレベルインジケーターは、ポリシーのプロパティウィンドウの上部に表示され、セキュリティ設定が Kaspersky Lab の推奨事項に準拠している度合いを示します。セキュリティレベルインジケーターを使用すると、ポリシーをすばやく設定し、必要な保護機能を有効にすることができます。

# 製品の購入

配布キットには、次のことを実行できる開始アプリケーションが含まれます：

- Kaspersky Embedded Systems Security のセットアップウィザードの起動。
- Kaspersky Embedded Systems Security コンソールのセットアップウィザードの起動。
- Kaspersky Virus Removal Tool の起動。
- このバージョンの Kaspersky Embedded Systems Security に関する情報の確認。
- Kaspersky Embedded Systems Security 4.0 のヘルプを開くこと。
- カスペルスキーの Web サイトの Kaspersky Embedded Systems Security のページを確認してください。
- カスペルスキーの Web サイトへのアクセス。
- テクニカルサポートサイトへのアクセス。

配布キットファイルは、使用目的によって異なるフォルダーに保存されています（下表を参照）。

Kaspersky Embedded Systems Security 配布キットファイル

| ファイル | 目的 |
|---|---|
| autorun.inf | リムーバブルドライブからインストールする場合の Kaspersky Embedded Systems Security セットアップウィザードの自動実行ファイル。 |
| setupui.exe | アプリケーションのようこそ画面の起動ファイル。 |
| ess_win.kud | Kaspersky Security Center を経由したアプリケーションのインストールパッケージのリモートインストールの説明が含まれる Kaspersky Unicode Definition フォーマット内のファイル。 |
| \console\esstools.msi | Windows インストーラーのインストールパッケージ。保護対象デバイスに Kaspersky Embedded Systems Security コンソールをインストールします。 |
| \console\setup_esstool.exe | 一連の管理ツールコンポーネント（Kaspersky Embedded Systems Security コンソールを含む）をインストールするウィザードのスタートアップファイル。インストールパッケージファイル esstools.msi は、ウィザードで指定されたインストール設定を使用して起動されます。 |
| \console\license.txt | Kaspersky Embedded Systems Security 管理コンソールの使用許諾契約およびプライバシーポリシーのテキストファイル。 |
| \exec\bases.cab | 製品のリリース時点で最新の定義データベースのアーカイブファイル。 |

| ファイル | 目的 |
| --- | --- |
| \exec\cleaner_v2.cab<br>\exec\cleanerapi_v2.cab | 競合するソフトウェアをアンインストールするためのファイル。 |
| \exec\ess.cab | 製品のグラフィカルインターフェイス用ファイル。 |
| \exec\ess_win.kud | Kaspersky Security Center を経由したアプリケーションのインストールパッケージのリモートインストールの説明が含まれる Kaspersky Unicode Definition フォーマット内のファイル。 |
| \exec\ess_win.msi | Windows インストーラーのインストールパッケージ：保護対象デバイスに Kaspersky Embedded Systems Security をインストールします。 |
| \exec\incompatible.txt | カスペルスキーは、Kaspersky Embedded Systems Security とファイルにリストされたアプリケーションとの互換性を保証しません。 |
| \exec\installer.ini | 配信キットの内部設定を含むファイル。 |
| \exec\klcfginst.msi | Kaspersky Security Center を介して使用できる Kaspersky Embedded Systems Security 管理プラグインのインストーラー。この管理プラグインを Kaspersky Embedded Systems Security の管理に使用する場合は、Kaspersky Security Center 管理コンソールがインストールされている保護対象の各デバイスに管理プラグインをインストールします。 |
| \exec\ksn_en.txt | KSN 声明の本文で記載したファイル。 |
| \exec\license.txt | Kaspersky Embedded Systems Security 使用許諾契約およびプライバシーポリシーのテキストファイル。 |
| \exec\package.kcat | 配布キットファイルの署名が含まれるファイル。 |
| \exec\setup_ess.exe | 保護対象デバイスに Kaspersky Embedded Systems Security をインストールするためのウィザードを起動するファイル。ウィザードで指定されたインストール設定を使用してインストーラーパッケージファイル ess_win.msi を起動します。 |
| \kvrt\KVRT.exe | Kaspersky Virus Removal Tool のインストーラー。 |
| \product_long_term\cleaner_v2.cab<br>\product_long_term\cleanerapi_v2.cab | 競合するソフトウェアをアンインストールするためのファイル。 |
| \product_long_term\ess.cab | 製品のグラフィカルインターフェイス用ファイル。 |
| \product_long_term\ess_win.kud | Kaspersky Security Center を経由したアプリケーションのインストールパッケージのリモートインストールの説明が含まれる Kaspersky Unicode Definition フォーマット内のファイル。 |
| \product_long_term\ess_win.msi | Windows インストーラーのインストールパッケージ。保護対象デバイスに Kaspersky Embedded Systems Security を **Default Deny テクノロジーによるコンピューターの保護**の設定でインストールします。 |
| \product_long_term\incompatible.txt | カスペルスキーは、Kaspersky Embedded Systems Security とファイルにリストされたアプリケーションとの互換性を保証しません。 |
| \product_long_term\installer.ini | 配信キットの内部設定を含むファイル。 |
| \product_long_term\klcfginst.exe | Kaspersky Security Center を介して使用できる Kaspersky Embedded Systems Security 管理プラグインのインストーラー。この管理プラグインを Kaspersky Embedded Systems Security の管理に使用する場合は、Kaspersky Security Center 管理コンソールがインストールされている保護対象の各デバイスに管理プラグインをインストールします。 |
| \product_long_term\ksn_en.txt | KSN 声明の本文をロシア語で記載したファイル。 |
| \product_long_term\license.txt | Kaspersky Embedded Systems Security 使用許諾契約およびプライバシーポリシーのテキストファイル。 |
| \product_long_term\package.kcat | 配布キットファイルの署名が含まれるファイル。 |
| \product_long_term\setup_ess.exe | 保護対象デバイスに Kaspersky Embedded Systems Security をインストールするためのウィザードを起動するファイル。ウィザードで指定されたインストール設定を使用してインストーラーパッケージファイル ess_win.msi を起動します。 |
| \setup\images | アプリケーションのようこそ画面の起動ファイルが含まれるフォルダー。 |
| \setup\setup.hta | アプリケーションのようこそ画面の起動ファイル。 |
| \setup\SETUP_STRINGS.JS | アプリケーション文字列リソースを含むファイル。 |

配布キットファイルはインストール CD から実行できます。配布パッケージファイルを事前にローカルドライブにコピーした場合は、配布キットファイルの構造が保持されていることを確認してください。

# システム要件

## 保護対象デバイスのソフトウェア要件

Microsoft Windows XP の保護対象デバイスに本製品を正しくインストールし動作させるには、Windows インストーラー 3.1 が必要です。

Kaspersky Embedded Systems Security を組み込みオペレーティングシステムの保護対象デバイスにインストールし、使用するには、フィルターマネージャーコンポーネント（Filter Manager）が必要です。

Kaspersky Embedded Systems Security を正しく動作させるには、Microsoft Windows で SHA-2 をサポートする必要があります。詳細については、テクニカルサポートサイトのナレッジベースを参照してください。

Kaspersky Embedded Systems Security は、次の 32 ビット または 64 ビットの Microsoft Windows オペレーティングシステムのデバイスへインストール可能です：

ワークステーション：

- Windows XP Professional SP2 以降 32 ビット / 64 ビット
- Windows Vista SP2 32 ビット / 64 ビット
- Windows 7 SP1 以降 Home / Pro / Enterprise / Ultimate 32 ビット / 64 ビット
- Windows 8 Pro / Enterprise 32 ビット / 64 ビット
- Windows 8.1 Pro / Enterprise 32 ビット / 64 ビット
- Windows 10 TH1 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 TH2 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 RS1 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 RS2 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 RS3 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 RS4 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 RS5 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 RS6 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 19H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット

- Windows 10 20H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 20H2 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 21H1 Home / Pro / Pro for Workstations / Education / Enterprise 32 ビット / 64 ビット
- Windows 10 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 ビット
- Windows 10 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 ビット
- Windows 11 21H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 ビット
- Windows 11 22H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 ビット
- Windows 11 23H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 ビット
- Windows 11 24H2 Home / Pro / Pro for Workstations / Education / Enterprise 64 ビット

サーバーオペレーティングシステム：

- Windows Server 2003 SP1 以降 Standard / Enterprise 32 ビット / 64 ビット
- Windows Server 2003 R2 SP2 Standard / Enterprise 64 ビット
- Windows Server 2008 SP2 Standard / Enterprise 32 ビット / 64 ビット
- Windows Server 2008 R2 SP2 以降 Foundation / Standard / Enterprise 64 ビット

組み込みシステム：

- Windows XP Embedded SP3 POS Ready 32 ビット
- Windows 7 Embedded POS Ready Standard 32 ビット/ 64 ビット
- Windows 7 Embedded SP1 Standard 32 ビット/ 64 ビット
- Windows 8.0 Embedded Standard 32 ビット / 64 ビット
- Windows 8.1 Embedded Industry / Pro 32 ビット / 64 ビット
- Windows 10 バージョン 1507 IoT Enterprise（32 ビット、64 ビット）
- Windows 10 バージョン 1607 IoT Enterprise（32 ビット、64 ビット）
- Windows 10 バージョン 1803 IoT Enterprise（32 ビット、64 ビット）
- Windows 10 バージョン 1809 IoT Enterprise（32 ビット、64 ビット）
- Windows 10 バージョン 1909 IoT Enterprise（32 ビット、64 ビット）
- Windows 10 バージョン 21H2 IoT Enterprise（32 ビット、64 ビット）
- Windows 10 バージョン 22H2 IoT Enterprise（32 ビット、64 ビット）
- Windows 11 バージョン 21H2 IoT Enterprise 64 ビット

- Windows 11 バージョン 22H2 IoT Enterprise 64 ビット
- Windows 11 バージョン 23H2 IoT Enterprise 64 ビット
- Windows 11 バージョン 24H2 IoT Enterprise 64 ビット

# 保護対象デバイスのハードウェア要件

保護対象デバイスのハードウェア要件

| OS の種類 | OS 名 | 最小要件 | 推奨要件 |
| --- | --- | --- | --- |
| ワークステーション | Windows XP x86 / x64 | • プロセッサ：1.4 GHz シングルコアプロセッサ Pentium III (x32)、Pentium IV (x64)<br>• メモリ：<br>  • アプリケーション起動コントロールのみのインストール：256 MB<br>  • すべてのアプリケーションコンポーネントのインストール：512 MB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：50 MB<br>  • すべてのアプリケーションコンポーネントのインストール：2 GB | • プロセッサ：クアッドコア 2.4 GHz<br>• RAM：2 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：2 GB<br>  • すべてのアプリケーションコンポーネントのインストール：4 GB |
| | Windows 7 / 8 / 10 x86 | • プロセッサ：1.4 GHz シングルコアプロセッサ Pentium III (x32)、Pentium IV (x64)<br>• メモリ：<br>  • アプリケーション起動コントロールのみのインストール：256 MB<br>  • すべてのアプリケーションコンポーネントのインストール：1 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：50 MB<br>  • すべてのアプリケーションコンポーネントのインストール：2 GB | • プロセッサ：クアッドコア 2.4 GHz<br>• RAM：2 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：2 GB<br>  • すべてのアプリケーションコンポーネントのインストール：4 GB |
| | Windows 7 / 8 / 10 / 11 x64 | • プロセッサ：1.4 GHz シングルコアプロセッサ Pentium IV (x64)<br>• メモリ：<br>  • アプリケーション起動コントロールのみのインストール：1 GB<br>  • すべてのアプリケーションコンポーネントのインストール：2 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：50 MB<br>  • すべてのアプリケーションコンポーネントのインストール：2 GB | • プロセッサ：クアッドコア 2.4 GHz<br>• メモリ：<br>  • アプリケーション起動コントロールのみのインストール：2 GB<br>  • すべてのアプリケーションコンポーネントのインストール：4 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：2 GB<br>  • すべてのアプリケーションコンポーネントのインストール：4 GB |
| 組み込みシステム | Windows XP Embedded | • プロセッサ：1.4 GHz シングルコアプロセッサ Pentium III (x32)、Pentium IV (x64)<br>• メモリ：<br>  • アプリケーション起動コントロールのみのインストール：256 MB<br>  • すべてのアプリケーションコンポーネントのインストール：512 MB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：50 MB<br>  • すべてのアプリケーションコンポーネントのインストール：2 GB | • プロセッサ：クアッドコア 2.4 GHz<br>• RAM：2 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：2 GB<br>  • すべてのアプリケーションコンポーネントのインストール：4 GB |
| | Windows 7 / 8 | • プロセッサ：1.4 GHz シングルコアプロセッサ | • プロセッサ：クアッドコア 2.4 GHz |

| OS の種類 | OS 名 | 最小要件 | 推奨要件 |
| --- | --- | --- | --- |
| | Embedded<br>Windows 10 / 11 IoT | Pentium IV (x64)<br>• メモリ：1 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：50 MB<br>  • すべてのアプリケーションコンポーネントのインストール：2 GB | • RAM：2 GB<br>• 空きディスク容量：<br>  • アプリケーション起動コントロールのみのインストール：2 GB<br>  • すべてのアプリケーションコンポーネントのインストール：4 GB |

# サポート対象の Kaspersky Security Center のバージョン

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

- Kaspersky Security Center Windows バージョン 10.5、11。Microsoft Windows XP SP2 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にインストールされた Kaspersky Embedded Systems Security の管理は、Kaspersky Security Center 管理コンソールと、Kaspersky Security Center Web コンソールによってサポートされます。
- Kaspersky Security Center Windows バージョン 14.2、15.1。Kaspersky Embedded Systems Security の管理は、Kaspersky Security Center 管理コンソールと、Kaspersky Security Center Web コンソールによってサポートされます。
- Kaspersky Security Center Linux バージョン 15.0、15.1、15.2、15.3、15.4、16.0。Kaspersky Embedded Systems Security の管理は、Kaspersky Security Center Web コンソールによってサポートされます。

Kaspersky Security Center 経由で Kaspersky Embedded Systems Security を管理するには、 Kaspersky Security Center ネットワークエージェントが必要です。

Kaspersky Security Center ネットワークエージェントは、Kaspersky Embedded Systems Security 配布キットには含まれていません。製品のダウンロードページの［**Kaspersky Security Center**］セクションからダウンロードできます。

# 機能要件および制限事項

このセクションでは、Kaspersky Embedded Systems Security コンポーネントの追加の機能要件および既存の制限事項について説明します。

# 本製品のインストールと削除

- Kaspersky Embedded Systems Security を正しく動作させるには、Microsoft Windows で SHA-2 をサポートする必要があります。

- Kaspersky Embedded Systems Security のインストールフォルダーへの指定されたパスに 150 文字以上の文字が含まれている場合、本製品のインストール時に画面に警告が表示されることがあります。この警告はインストールプロセスには影響しません。Kaspersky Embedded Systems Security をインストールして実行できます。

- SNMP プロトコルサポートコンポーネントをインストールする場合、SNMP サービスが実行されている状況では、必ず SNMP サービスを再起動してください。

- Kaspersky Embedded Systems Security を組み込みオペレーティングシステム上で動作するデバイスにインストールして実行する場合は、フィルターマネージャーコンポーネントを忘れずにインストールしてください。

- Microsoft Active Directory® グループポリシーを介して Kaspersky Embedded Systems Security 管理ツールをインストールすることはできません。

- インストールされているアプリケーションコンポーネントのリストからアンチウイルス保護ノードを除外した場合、インストールが完了すると、このノードは使用可能なコンポーネントのリストから消えます。インストールパッケージにはコンポーネントの完全なリストが含まれているため、アンチウイルス保護ノードのコンポーネントをインストールするには、インストールパッケージからインストールウィザードを開始します。

- Kaspersky Embedded Systems Security 管理コンソールがインストールされている場合、インストールウィザードでコンピューターを再起動するように指示されることがあります。この場合、再起動は必須ではありません。管理コンソールをインストールしたユーザーのセッションを終了し、システムに再度ログインするだけで十分です。

- 本製品を Windows XP または Windows Vista のデバイスにインストールする場合は、DigiCert Assured ID Root CA ルート証明書をインストールして、ドライバーの署名検証を有効にする必要がある可能性があります。必要に応じて、この証明書は、本製品のインストールパッケージから、オペレーティングシステムの信頼するルート証明書ストアに自動的にインストールされます。

- 本製品を Windows XP または Windows Vista のデバイスにインストールする場合は、DigiCert High Assurance EV Root CA. が存在するかどうかを確認する必要があります。

  このルート証明書がインストールされていない場合、本製品が正しく機能しない可能性があります。できるだけ早く証明書をインストールすることを推奨します。

- インストールフォルダーへのパスが、定義データベースのフォルダー、バックアップフォルダー、隔離からのオブジェクトの復元用フォルダー、一時ファイルフォルダーの少なくとも 1 つのフォルダーへのパスと同じである場合、本製品のインストールはエラーで終了します。

- Kaspersky Security Center Cloud コンソールを使用して Kaspersky Embedded Systems Security を管理する場合、ローカルで本製品をアップデートすることはできません。ローカルで本製品をアップデートする場合、Kaspersky Security Center Cloud コンソールのデータ処理契約に同意することはできません。

# システム変更監視

既定では、システム変更監視コンポーネントは、システムフォルダーの変更やファイルシステムの状態監視ファイルの変更を監視しません。オペレーティングシステムによって絶えず行われる定期的なファイル変更に関する情報でタスクレポートが煩雑にならないようにするためです。こうしたフォルダーを監視範囲に含めることはできません。

監視範囲から除外されるフォルダーおよびファイルは、次の通りです：

- ファイル ID が 0 ～ 33 の NTFS の状態監視ファイル
- %SystemRoot%\Prefetch\
- %SystemRoot%\ServiceProfiles\LocalService\AppData\Local\
- %SystemRoot%\System32\LogFiles\Scm\
- %SystemRoot%\Microsoft.NET\Framework\v4.0.30319\
- %SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\
- %SystemRoot%\Microsoft.NET\
- %SystemRoot%\System32\config\
- %SystemRoot%\Temp\
- %SystemRoot%\ServiceProfiles\LocalService\
- %SystemRoot%\System32\winevt\Logs\
- %SystemRoot%\System32\wbem\repository\
- %SystemRoot%\System32\wbem\Logs\
- %ProgramData%\Microsoft\Windows\WER\ReportQueue\
- %SystemRoot%\SoftwareDistribution\DataStore\
- %SystemRoot%\SoftwareDistribution\DataStore\Logs\
- %ProgramData%\Microsoft\\Windows\AppRepository\
- %ProgramData%\Microsoft\Search\\Data\Applications\Windows\
- %SystemRoot%\Logs\SystemRestore\
- %SystemRoot%\System32\Tasks\Microsoft\\Windows\TaskScheduler\

最上位のフォルダーは除外されます。

このコンポーネントは、ReFS/NTFSファイルシステムをバイパスするファイルの変更（BIOS、LiveCD などによって行われたファイルの変更）を監視しません。

# ファイアウォール

- 複数のアドレスを指定する必要があります。そうしないと、IPv6 を使用できません。
- 設定済みのファイアウォールのルールによって、保護対象デバイスと管理サーバー間のやり取りの基本的なシナリオがサポートされます。Kaspersky Security Center の機能を十分に活用するには、ポートルールを設定する必要があります。ポート番号、プロトコル、機能に関する情報は、Kaspersky Security Center のナレッジベースを参照してください。
- 本製品をインストールしファイアウォールのルールを設定した後、ファイアウォールコンポーネントの実行時に Windows ファイアウォールのルールおよびルールグループの変更が監視されます。ステータスを更新し、必要な Windows ファイアウォールのルールを追加するには、ファイアウォールコンポーネントを再起動します。
- ファイアウォールコンポーネントを起動すると、拒否ルールと送信トラフィックを制御するルールが Windows ファイアウォールの設定から自動的に削除されます。
- 本製品のパスと、アプリケーションのファイアウォールのルールの名前には、文字「`*`」と「`?`」は使用できません。
- Windows オペレーティングシステムのファイアウォールの設定（［**設定**］→［**更新とセキュリティ**］→［**Windows セキュリティ**］→［**ファイアウォールとネットワーク保護**］）の Kaspersky Embedded Systems Security ファイアウォールを有効にするボタンでは、ファイアウォールが有効になるだけで、［*ブロック*］モードに切り替わることはありません（ファイアウォールを有効にする前に、［*Windows ファイアウォールの状態を確認する*］ファイアウォールモードを有効にした場合を除く）。Kaspersky Embedded Systems Security ファイアウォールを有効にするボタンは、ファイアウォールモードが［*ブロック*］に変更された後に限り、表示されなくなります。

# 古いバージョンの Windows における制限

- Windows XP SP2 バージョンでは、リモートデバイスをブロックしたり、ブロック対象のネットワークセッションのリストを設定したりすることはできません。このバージョンの Windows では、［**悪意のある活動を示すセッションのネットワーク共有リソースへのアクセスをブロックする**］は無効です。
- Kaspersky Embedded Systems Security のインストール：
  - Windows XP SP2 Professional（32 ビット、64 ビット）、Windows Server 2003、Windows Server 2003 R2 を実行しているコンピューターでは、製品の配布キットを使用するか、標準のインストールパッケージ「Kaspersky Security Center 10.5 Network Agent for Windows XP」の実行ファイル setup.exe を Kaspersky Security Center の製品のインストールパッケージフォルダーに配置する必要があります。
  - Windows XP SP3 Professional（32 ビット）および Windows XP Embedded SP3（32 ビット）を実行しているコンピューターでは、製品の配布キットを使用するか、Kaspersky Security Center バージョン 14 で作成された製品のインストールパッケージまたは標準のインストールパッケージ「Kaspersky Security Center 14 Network Agent for Windows XP」の実行ファイル setup.exe を Kaspersky Security Center の製品のインストールパッケージフォルダーに配置する必要があります。

**Kaspersky Security Center の標準のインストールパッケージからファイル setup.exe を抽出する方法**

1. Kaspersky Security Center 管理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. 作業領域内で、［**その他の操作**］をクリックして、ドロップダウンリストから［**カスペルスキー製品の現在のバージョンの表示**］を選択します。
3. リストから必要な製品を選択します。たとえば、Kaspersky Security Center 10.5 Network Agent for Windows XP などを選択します。
4. ［**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。
   作成されたインストールパッケージは、［**インストールパッケージ**］リストに表示されます。
5. 作成されたインストールパッケージのプロパティを開きます。
6. ［**全般**］セクションで、インストールパッケージフォルダーへのパスをコピーします。
7. インストールパッケージフォルダーを開きます。
8. ファイル setup.exe をコピーします。

- Kaspersky Security Center 経由で Kaspersky Embedded Systems Security を管理するには：
  - Windows XP SP2 Professional（32 ビット、64 ビット）、Windows Server 2003、または Windows Server 2003 R2 を実行しているコンピューターでは、 Kaspersky Security Center ネットワークエージェント（klnagent）のバージョン 10.5.1781 を使用する必要があります。
  - Windows XP SP3 Professional（32 ビット）および Windows XP Embedded SP3（32 ビット）を実行しているコンピューターでは、 Kaspersky Security Center ネットワークエージェント（klnagent）のバージョン 14.0.0.20023 を使用する必要があります。
- Windows XP コンピューターでは、MQTT プロトコルを使用してテレメトリをデータダイオードに送信することはできません。

# Kaspersky Security Center との連携

- アップデートパッケージを受信すると、管理サーバーはデータベースのアップデートを確認してから、アップデートをネットワーク上の保護対象デバイスに送信します。Kaspersky Security Center 管理サーバーは、製品機能のアップデートを確認しません。
- ネットワークリストを使用して Kaspersky Security Center に動的に変更されたデータを送信するコンポーネントを使用する場合、Kaspersky Security Center 管理サーバーとの対話の設定で必要なチェックボックスがオンになっていることを確認してください（隔離、バックアップ）。
- ネットワークエージェント 10.5 は、インストール済みコンポーネントに関する情報を Kaspersky Security Center 管理サーバーに送信しません。このため、Kaspersky Security Center 管理コンソールおよび Kaspersky Security Center Web コンソールでは、ネットワークエージェント 10.5 を搭載したデバイスの設定に、インストール済みの Kaspersky Embedded Systems Security コンポーネントとその設定が表示されません。

- デバイスに Kaspersky Security Center ネットワークエージェント 10.5 がインストールされている場合、Kaspersky Security Center Web コンソールを使用してバックアップ内のファイルをダウンロードすることはできません。

- Kaspersky Security Center ネットワークエージェントのリソース低消費モードを有効にして（`SKIP_KLNAG_FLAG_TEST_VM_PERF=0`。これが既定です）Kaspersky Embedded Systems Security がインストールされてから、ネットワークエージェントがインストールされた場合、Windows ファイアウォールでネットワークエージェントについての除外が作成されないため、Windows ファイアウォールはネットワークエージェントをブロックします。

- Kaspersky Security Center ネットワークエージェントのリソース低消費モードを有効にして（`SKIP_KLNAG_FLAG_TEST_VM_PERF=0`。これが既定です）Kaspersky Embedded Systems Security がインストールされている場合、ネットワークリストの変更は、約 10 分遅れて Kaspersky Security Center 管理コンソールに反映されます。

# その他の制限事項

## オンデマンドスキャンとファイルのリアルタイム保護

- MTP 接続のデバイスのスキャンは使用できません。

- アーカイブのスキャンを実行する場合、SFX アーカイブをスキャン対象から外すことはできません。Kaspersky Embedded Systems Security の保護設定でアーカイブのスキャンを有効にすると、アーカイブ内および SFX アーカイブ内のオブジェクトが自動的にスキャンされます。通常のアーカイブをスキャンせずに、SFX アーカイブのみをスキャンすることは可能です。

- ［**起動プロセスの詳細な分析（分析中はプロセスの起動がブロックされます）**］がオンで、［**KSN の使用**］が有効になっている場合、「通知」モードが選択されていても、URL Web アドレスを引数として受け取る起動済みプロセスはすべてブロックされます。プロセスのブロックを回避するには、次のいずれかのオプションを選択します：

  - ［**KSN の使用**］サービスを無効にする。

  - ［**起動プロセスの詳細な分析（分析中はプロセスの起動がブロックされます）**］をオフにする。

  推奨オプション：［**起動プロセスの詳細な分析（分析中はプロセスの起動がブロックされます）**］をオフにする。

## ライセンス管理

- ライセンスが SUBST コマンドを使用して作成された場合、またはライセンス情報ファイルへのパスがネットワークパスである場合、セットアップウィザードの実行中にライセンスを使用して本製品をアクティベートすることはできません。

- Kaspersky Security Center プロキシサーバーを使用してクライアントデバイスで製品をアクティベートする場合は、Kaspersky Security Center ネットワークエージェントをインストールする時に、このデバイスで VDI 最適化を無効にします。

## アップデート

- 既定では、Kaspersky Embedded Systems Security の重要なモジュールのアップデートがインストールされると、アプリケーションアイコンは非表示になります。
- KLRAMDISK は、Windows XP または Windows Server® 2003 オペレーティングシステムで稼働している保護対象デバイスではサポートされません。
- Kaspersky Embedded Systems Security のパッチのインストールが失敗した場合、パッチはロールバックされ、オペレーティングシステムを再起動するよう要求されます。

## インターフェイス

- アプリケーションコンソールで、隔離、バックアップ、システム監査ログ、実行ログのフィルタリングは大文字と小文字が区別されます。
- アプリケーションコンソールで保護範囲またはスキャン範囲を設定する場合、1つのパスに対して使用できるマスクは1つのみで、マスクを指定できる場所はパスの末尾のみです。正しいマスクの例は次の通りです：「`C:\Temp\Temp*`」、「`C:\Temp\Temp???.doc`」、「`C:\Temp\Temp*.doc`」。この制限事項は信頼ゾーンの設定には影響しません。
- アプリケーションコンソールの［**テレメトリ収集サーバー**］セクションでは、タスクの実行がスケジュールされている時間が表示されません。その［**開始時刻**］列は空になります。

## セキュリティ

- オペレーティングシステムのユーザーアカウント制御機能が有効になっている場合、タスクトレイ通知領域にある本製品のアイコンをダブルクリックしてアプリケーションコンソールを開けるようにするには、ユーザーアカウントを ESS Administrators グループに追加する必要があります。この手順を行わない場合は、コンパクト診断インターフェイスまたは Microsoft 管理コンソールスナップインを開くことを許可されたユーザーとしてログインする必要があります。
- ユーザーアカウント制御が有効になっている場合、Microsoft Windows の［プログラムと機能］ウィンドウから本製品をアンインストールすることはできません。

## 脆弱性攻撃ブロック

- 現在の環境設定に apphelp.dll ライブラリが読み込まれていない場合、脆弱性攻撃ブロックは使用できません。
- 脆弱性攻撃ブロックコンポーネントは、Microsoft Windows 10 オペレーティングシステムの保護対象デバイス上の Microsoft の EMET ユーティリティと互換性がありません。EMET ユーティリティがインストールされた保護対象デバイスに脆弱性攻撃ブロックコンポーネントがインストールされている場合、 Kaspersky Embedded Systems Security は EMET をブロックします。
- 脆弱性攻撃ブロックコンポーネントは、SQL Server® 2012 データベースエンジンと互換性がありません。MS SQL Server 2012 がインストールされているコンピューターに Kaspersky Embedded Systems Security をインストールする場合は、データベースサーバーの sqlos.dll ライブラリを脆弱性攻撃ブロックタスクの除外リストに追加する必要があります。

### Detection and Response

- 脅威応答プロセスの途中で共有フォルダーのアクセスエラーが発生した場合、そのようなエラーは脅威応答履歴（Kaspersky Security Center Web コンソール→アプリケーションがインストールされているホストのプロパティ→［**Detection and Response**］→［**応答履歴**］セクション）に反映されません。

- [KESS + KEA + 組み込みエージェント] の構成はサポートされません。このような構成は、本製品と組織内で導入されている Detection and Response ソリューションとの連携を阻害します。さらに、同じコンピューター上で Kaspersky Endpoint Agent と組み込みエージェントを使用すると、テレメトリの重複を招く可能性があり、コンピューターとネットワークの負荷を増大させることになります。

  インストーラーでは Kaspersky Endpoint Agent を Kaspersky Embedded Systems Security と組み込みエージェントがインストールされているコンピューターに導入することが許可されています。Kaspersky Endpoint Agent と組み込みエージェントは、*コンポーネントの変更*タスクの結果として 1 台のコンピューターにインストールすることも可能です。動作は Kaspersky Embedded Systems Security と Kaspersky Endpoint Agent のバージョンにより異なります。

### イベントの設定

Kaspersky Security Center ポリシーの［**イベントの設定**］セクションで設定できる*管理領域でのファイル操作をコントロールできません*のイベントの設定は、次のイベントにも適用されます：

- *信頼するユーザーによる管理領域でのファイル操作を許可しました*
- *管理領域でのファイル操作を禁止しました*
- *統計のみ：管理領域でのファイル操作を禁止しました*
- *管理領域でのファイル操作をコントロールできません*

### コンパクト診断インターフェイス

Windows XP コンピューターでは、コンパクト診断インターフェイスを使用するには、ターミナルサービスが動作している必要があります。

# 他のアプリケーションとの互換性情報

*すべての機能*の設定の Kaspersky Embedded Systems Security は、サードパーティのエンドポイント保護システム（Endpoint Protection Platform、EPP）の一部であるアプリケーションとは互換性がありません。Kaspersky Embedded Systems Security は、他のアプリケーションや一部のカスペルスキー製品と互換性がない場合もあります。互換性を判断するために、Kaspersky Embedded Systems Security は、カスペルスキーが用意したソフトウェアのリストを参照します。このリストは incompatible.txt ファイルに含まれています。このファイルは配信キットに含まれています。

incompatible.txt リスト内のソフトウェアが検出されると、インストーラーは Kaspersky Embedded Systems Security のインストールを中止します。サードパーティ製のウイルス対策製品を削除する必要があります。インストーラーはリストにある一部のアプリケーションを自動的に削除する場合があります。

コンピューターに Windows ファイアウォールがインストールされている場合は、インストーラーによって無効になり、Kaspersky Embedded Systems Security のインストールが続行されます。

リスクを承知の上で、incompatible.txt リストにあるソフトウェアと一緒に Kaspersky Embedded Systems Security をインストールする必要がある場合は、インストールされているサードパーティ製のウイルス対策製品のチェックをスキップできます。このためには、インストーラーに `SKIPINCOMPATIBLESW= 1` パラメータを渡す必要があります。

例：

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p  SKIPINCOMPATIBLESW= 1
```

# 本製品のインストールと削除

このセクションでは、Kaspersky Embedded Systems Security のインストール方法と削除方法を説明します。

# インストールの計画

のセクションでは、Kaspersky Embedded Systems Security 管理ツールの説明と、ウィザード、コマンドライン、Kaspersky Security Center、および Active Directory グループポリシーを介した Kaspersky Embedded Systems Security のインストールおよびアンインストールでの留意点を記載しています。

Kaspersky Industrial CyberSecurity for Nodes または Kaspersky Endpoint Security for Windows を削除した後で Kaspersky Embedded Systems Security をインストールする場合は、コンピューターを再起動する必要があります。

Kaspersky Embedded Systems Security のインストールを開始する前に、インストールの主要な段階について計画しましょう。

1. Kaspersky Embedded Systems Security の管理と設定に使用する管理ツールを決定します。
2. インストールに必要な製品コンポーネントを選択します。
3. インストール方法を選択します。

# 管理ツールの選択

Kaspersky Embedded Systems Security の設定およびアプリケーションの管理に使用する管理ツールを決定します。Kaspersky Embedded Systems Security の管理には、アプリケーションコンソール、コマンドラインユーティリティ、Kaspersky Security Center 管理コンソールが使用できます。

## Kaspersky Embedded Systems Security コンソール

Kaspersky Embedded Systems Security コンソールは、Microsoft 管理コンソールに追加される独立したスナップインです。Kaspersky Embedded Systems Security は、企業ネットワーク上の保護対象デバイスやその他のデバイスにインストールされたアプリケーションコンソール経由で管理できます。

複数の Kaspersky Embedded Systems Security スナップインを、作成者モードで開かれた 1 つの Microsoft 管理コンソールに追加できます。これにより、Microsoft 管理コンソールを使用して、Kaspersky Embedded Systems Security がインストールされている複数のデバイスに対する保護を管理できます。

アプリケーションコンソールは、「管理ツール」製品コンポーネントセットに含まれます。

## コマンドラインユーティリティ

保護対象デバイスのコマンドラインを使用して Kaspersky Embedded Systems Security を管理できます。

コマンドラインユーティリティは、Kaspersky Embedded Systems Security のソフトウェアコンポーネントグループに含まれます。

### Kaspersky Security Center

Kaspersky Security Center を使用してアンチウイルスによるデバイスの保護を一元管理している場合、Kaspersky Security Center 管理コンソールを使用して Kaspersky Embedded Systems Security を管理できます。

次のコンポーネントがインストールされます：

- **Kaspersky Security Center ネットワークエージェントとの連携モジュール**：Kaspersky Embedded Systems Security のソフトウェアコンポーネントグループに含まれます。Kaspersky Embedded Systems Security とネットワークエージェントとの通信を可能にします。Kaspersky Security Center ネットワークエージェントとの連携モジュールは保護対象デバイスにインストールします。

- **Kaspersky Security Center ネットワークエージェント**：各保護対象デバイスにインストールします。このコンポーネントでは、保護対象デバイスにインストールされている Kaspersky Embedded Systems Security と Kaspersky Security Center 管理コンソールのやり取りがサポートされます。ネットワークエージェントのインストールファイルは、Kaspersky Security Center の配布キットフォルダーに含まれます。

- **Kaspersky Embedded Systems Security 管理プラグイン**：管理コンソールを使用して、Kaspersky Security Center 管理サーバーがインストールされている保護対象デバイスに Kaspersky Embedded Systems Security 管理プラグインをインストールすることもできます。これにより、Kaspersky Security Center によるアプリケーションの管理インターフェイスを利用できるようになります。管理プラグインのインストールファイル \exec\klcfginst.exe は、Kaspersky Embedded Systems Security の配布キットに含まれます。

## インストール方法の選択

Kaspersky Embedded Systems Security でインストールするソフトウェアコンポーネントを指定したら、製品のインストール方法を選択する必要があります。

ネットワークアーキテクチャと次の条件に従って、インストール方法を選択します：

- Kaspersky Embedded Systems Security の特別なインストール設定が必要か、それとも推奨のインストール設定を使用するか。

- すべての保護対象デバイスに対して同じインストール設定を使用するか、各保護対象デバイスによって異なるインストール設定を使用するか。

Kaspersky Embedded Systems Security は、セットアップウィザードを使用してインタラクティブに、またはサイレントモードでユーザーの介在なしでインストールできます。また、コマンドラインからインストール設定を指定してインストールパッケージファイルを実行し、起動することもできます。Active Directory のグループポリシーまたは Kaspersky Security Center のリモートインストールタスクを使用すると、Kaspersky Embedded Systems Security を一元的にリモートでインストールできます。

Kaspersky Embedded Systems Security をある 1 つの保護対象デバイスにインストールして設定し、その設定を設定情報ファイルに保存しておくと、Kaspersky Embedded Systems Security を他の保護対象デバイスにインストールする際にその設定情報ファイルを使用できます。Active Directory のグループポリシーを使用して製品をインストールされた場合は使用できません。

## セットアップウィザードの起動

セットアップウィザードでは次のインストールを実行できます：

- 保護対象デバイスへの Kaspersky Embedded Systems Security コンポーネントのインストール：開始アプリケーションのリンクをクリックします。開始アプリケーションは、setupui.exe を開くか、配布キットのファイル \exec\setup_ess.exe を直接使用して起動できます。

- 保護対象デバイスまたは LAN 上の他のデバイス上への Kaspersky Embedded Systems Security コンソールのインストール：開始アプリケーションのリンクをクリックします。開始アプリケーションは、setupui.exe を開くか、配布キットのファイル \console\setup_esstools.exe を直接使用して起動できます。

## コマンドラインで必要なインストール設定を指定して、インストールパッケージファイルを実行します

コマンドラインオプションを設定せずにインストールパッケージファイルを開始した場合、Kaspersky Embedded Systems Security は既定の設定でインストールされます。Kaspersky Embedded Systems Security のオプションを使用してインストールの設定を変更できます。

アプリケーションコンソールは、保護対象デバイスまたは管理者のワークステーションにインストールできます。

Kaspersky Embedded Systems Security とアプリケーションコンソールのインストール用のサンプルコマンドを使用することもできます。

## Kaspersky Security Center による一括インストール

お使いのネットワークで Kaspersky Security Center を使用してアンチウイルスによるネットワークデバイスの保護を管理している場合、リモートインストールタスクを使用して複数のデバイスに Kaspersky Embedded Systems Security をインストールできます。

Kaspersky Security Center を使用して Kaspersky Embedded Systems Security をインストールする場合、インストール先となる保護対象デバイスは、Kaspersky Security Center と同じドメインに存在していても異なるドメインに存在していてもかまいません。また、属するドメインがなくてもかまいません。

## Active Directory のグループポリシーによる一括インストール

Active Directory のグループポリシーを使用して、保護対象デバイスに Kaspersky Embedded Systems Security をインストールできます。アプリケーションコンソールは、保護対象デバイスおよび管理者のワークステーションにインストールできます。

Active Directory のグループポリシーを使用して Kaspersky Embedded Systems Security をインストールする場合、推奨されているインストール設定でしかインストールできません。

Active Directory グループポリシーを使用して Kaspersky Embedded Systems Security をインストールする保護対象デバイスは、同じドメインおよび同じ組織単位に存在している必要があります。保護対象デバイスの起動時、Microsoft Windows にログインする前にインストールが実行されます。

# ウィザードを使用した製品のインストールとアンインストール

このセクションでは、セットアップウィザードを使用した Kaspersky Embedded Systems Security とアプリケーションコンソールのインストールとアンインストール、および Kaspersky Embedded Systems Security の追加の設定とインストール時に実行される処理について説明します。

## セットアップウィザードを使用したインストール

このセクションでは、Kaspersky Embedded Systems Security とアプリケーションコンソールのインストールの情報について説明します。

*Kaspersky Embedded Systems Security をインストールして使用するには：*

1. Kaspersky Embedded Systems Security を保護対象デバイスにインストールします。
2. アプリケーションコンソールは、Kaspersky Embedded Systems Security を管理する時に操作するデバイスにインストールしてください。
3. アプリケーションコンソールがネットワーク上の（保護対象デバイス以外の）いずれかのデバイスにインストールされている場合、アプリケーションコンソールのユーザーが Kaspersky Embedded Systems Security をリモート管理できるようにするには、追加設定を実行してください。
4. Kaspersky Embedded Systems Security のインストール後に処理を実行します。

### Kaspersky Embedded Systems Security のインストール

Kaspersky Embedded Systems Security のインストール前に、次の操作を行います：

1. 保護対象デバイスに他のウイルス対策製品がインストールされていないことを確認します。Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition を削除する必要があります。Kaspersky Embedded Systems Security のインストールでは、Kaspersky Security 10 for Windows Server を削除する必要はありません。
2. セットアップウィザードの起動に使用するアカウントが、保護対象デバイスの管理グループに属していることを確認します。

上記の確認が完了したら、インストールの手順に進んでください。セットアップウィザードの説明に続いて、Kaspersky Embedded Systems Security のインストール設定を指定します。Kaspersky Embedded Systems Security のインストールプロセスは、セットアップウィザードのどの段階でも中断できます。それには、［セットアップウィザード］ウィンドウで［**キャンセル**］をクリックします。

インストール（アンインストール）の設定については詳細情報があります。

*セットアップウィザードを使用して Kaspersky Embedded Systems Security をインストールするには：*

1. 保護対象デバイスでファイル setup.exe を実行します。
2. 表示されたウィンドウで、［**インストール"**］セクションの［**Default Deny テクノロジーによるコンピューターの保護"**］または［**アンチウイルスベースでのコンピューターの保護"**］をクリックします。

「**アンチウイルスベースでのコンピューターの保護"**」の設定が選択されている場合、ファイアウォールコンポーネントとパフォーマンスカウンターコンポーネントを除くすべての Kaspersky Embedded Systems Security コンポーネントが既定で含まれています。

コンピューターを保護するためにシグネチャ分析と定義データベースを使用しないアプリケーションのバージョンに Kaspersky Embedded Systems Security の［**アンチウイルスベースでのコンピューターの保護"**］の設定をインストールすると、次のコンポーネントを追加することによってアプリケーションコンポーネントのセットが自動的に拡張されます：

- ファイルのリアルタイム保護
- オンデマンドスキャン。
- ネットワーク脅威対策。

アップデートを有効にするコンポーネントは、［**Default Deny テクノロジーによるコンピューターの保護"**］の設定には含まれていません。

［**Default Deny テクノロジーによるコンピューターの保護"**］の設定が選択されている場合、既定で含まれるコンポーネントは、次の通りです：

- Core
- 脆弱性攻撃ブロック
- アプリケーション起動コントロール
- システムトレイアイコン

コンピューターを保護するためにシグネチャ分析と定義データベースを使用するアプリケーションのバージョンに Kaspersky Embedded Systems Security の「**Default Deny テクノロジーによるコンピューターの保護"**」の設定をインストールすると、次のコンポーネントを削除することによってアプリケーションコンポーネントのセットが自動的に削減されます：

- ファイルのリアルタイム保護
- オンデマンドスキャン。
- アップデートを有効にするコンポーネント

この設定は、リソースが限られているデバイスの保護に推奨されます。この場合、本製品を長期間アクティベートすることができ、アプリケーション起動コントロールによりコンピューターが保護されます。

3. Kaspersky Embedded Systems Security のセットアップウィザードの開始ウィンドウで［**次へ >**］をクリックします。

［**使用許諾契約書**］ウィンドウが表示されます。

4. 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。

5. 使用許諾契約書とプライバシーポリシーの条項に同意する場合、［**内容をすべて読み、理解したので、使用許諾契約書の諸条件に同意します**］および［**プライバシーポリシーをすべて確認し、理解した上で同意します。データは、プライバシーポリシーに従って、処理および送信されること（第三国への送信を含む）を理解しました**］のチェックボックスをオンにします。

使用許諾契約書とプライバシーポリシーに同意しない場合は、インストールは中止されます。

6. ［**次へ >**］をクリックします。

［**カスタムインストール**］ウィンドウが表示されます。

7. インストールするコンポーネントを選択します。

Kaspersky Embedded Systems Security の SNMP プロトコルサポートは、Microsoft Windows SNMP サービスが保護対象デバイスにインストールされている場合にのみ、インストールするコンポーネントのリストに表示されます。

8. すべての変更をキャンセルするには、［**カスタムインストール**］ウィンドウで［**リセット**］をクリックします。［**次へ >**］をクリックします。

9. ［**インストール先フォルダー**］ウィンドウで、次のいずれかの手順を実行します：

- 必要に応じて、Kaspersky Embedded Systems Security のファイルのコピー先のフォルダーを指定します。
- 必要に応じて、［**ディスク**］をクリックして、ローカルディスクの使用可能な容量の情報を確認します。

［**次へ >**］をクリックします。

10. ［**設定**］ウィンドウで、保護範囲からオブジェクトとフォルダーを除外し、ファイルのリアルタイム保護を設定できます。

11. ［**設定ファイルからのインポートの設定**］ウィンドウで、本製品の以前のバージョンで作成された既存の設定情報ファイルから Kaspersky Security for Windows Server の設定をインポートする場合は、設定情報ファイルへのパスを指定します。

12. ［**アプリケーションのアクティベーション**］ウィンドウで、次のいずれかを行います：

- 製品をアクティベートする場合は、アクティベーションに使用する Kaspersky Embedded Systems Security のライセンス情報ファイルを指定します。
- 製品を後でアクティベートする場合は、［**次へ >**］をクリックします。
- ライセンス情報ファイルがあらかじめ配布キットの \product フォルダーに保存されている場合は、このファイルの名前が［**ライセンス**］フィールドに表示されます。
- 別のフォルダーに保存されている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、そのライセンス情報ファイルを指定します。

インストールウィザードでは、アクティベーションコードを使用して本製品をアクティベートすることはできません。アクティベーションコードを使用して本製品をアクティベートする場合は、本製品のインストール後にコードを指定できます。

ライセンス情報ファイルが追加されると、ライセンス情報がウィンドウに表示されます。ライセンスの有効期限日までの日数を計算して表示します。ライセンスの有効期間は、ライセンスが追加された時間から実行され、ライセンス情報ファイルの有効期限日まで有効です。

［**次へ >**］をクリックして、ライセンス情報ファイルを本製品に追加します。

13. 必要に応じて、［**リモートアクセス設定**］セクションで、アプリケーションコンソールが製品をインストールしたコンピューターにリモート接続する際に使用する TCP ポートを変更します。

    Windows 資格情報による接続の既定のポート番号は 13032 で、手動で作成されたユーザーの資格情報による接続の既定のポート番号は 13031 です。指定可能なポートの番号の範囲：1 ～ 65535。

    手動で作成したユーザーアカウントの資格情報による接続を防ぐには、［**手動で作成したユーザーの資格情報を使用**］をオフにしてください。

14. ［**インストールの準備ができました**］ウィンドウで、必要に応じて［**本製品のインストールのプロセスを保護する**］を無効にします。インストールの保護機能には、悪意のあるアプリケーションによる配布パッケージの置き換えの防止、Kaspersky Embedded Systems Security のインストールフォルダーへのアクセスのブロック、製品のレジストリキーが保存されているシステムレジストリセクションへのアクセスのブロックが含まれます。ただし、製品をインストールできない場合は、インストールプロセスの保護を無効にする必要があります（たとえば、Windows Remote Desktop でリモートインストールを実行するとき）。

15. 必要に応じて、コマンドラインインターフェイスを便利に使用できるように、%PATH% システム変数にファイル kavshell.exe のパスを追加します。

16. ［**インストール**］をクリックします。

17. インストールが完了すると［**インストールの完了**］ウィンドウが表示されます。

18. ［**完了**］をクリックします。

セットアップウィザードが閉じます。アクティベーションコードを入力している場合、インストールが完了すると Kaspersky Embedded Systems Security が使用できるようになります。

## Kaspersky Embedded Systems Security コンソールのインストール

セットアップウィザードの指示に従い、アプリケーションコンソールのインストール設定を編集します。インストールプロセスは、セットアップウィザードのどの段階でも中断できます。それには、［セットアップウィザード］ウィンドウで［**キャンセル**］をクリックします。

*アプリケーションコンソールをインストールするには：*

1. セットアップウィザードの起動に使用するアカウントが、デバイスの管理グループに属していることを確認します。

2. 保護対象デバイスでファイル setup.exe を実行します。

   プログラムの開始ウィンドウが表示されます。

3. ［**Kaspersky Embedded Systems Security for Windows コンソールのインストール"**］リンクをクリックします。

   セットアップウィザードの開始ウィンドウが表示されます。［**次へ >**］をクリックします。

4. 使用許諾契約書とプライバシーポリシーの条項に同意する場合、［**内容をすべて読み、理解したので、使用許諾契約書の諸条件に同意します**］および［**プライバシーポリシーをすべて確認し、理解した上で同意します。データは、プライバシーポリシーに従って、処理および送信されること（第三国への送信を含む）を理解しました**］のチェックボックスをオンにします。［**次へ >**］をクリックします。

5. ［**インストール先フォルダー**］ウィンドウで、インストールするファイルの保存先フォルダーを指定します。

6. ［**次へ >**］をクリックします。

7. ［**インストールの準備ができました**］ウィンドウの［**インストール**］をクリックします。
   選択したコンポーネントのインストールが開始します。

8. ［**終了**］をクリックします。

セットアップウィザードが閉じます。アプリケーションコンソールが、保護対象デバイスにインストールされます。

管理ツールがネットワーク上の、ネットワーク上の保護対象デバイス以外のデバイスにインストールされた場合、詳細設定を編集してください。

## アプリケーションコンソールを別のデバイスにインストールした後の詳細設定

アプリケーションコンソールを、ネットワーク上の、保護対象デバイス以外のデバイスにインストールした場合、次の操作を実行してリモートで Kaspersky Embedded Systems Security を管理できるようにします：

- アプリケーション設定でリモート接続する権限を持つユーザーアカウントを使用します。既定では、Administrators グループと ESS Administrators グループのすべてのユーザーにこの権限が与えられます。

- リモートデバイスの Windows ファイアウォールの設定で、Windows システムユーザーアカウントによる接続用に TCP 13032 ポートを開き、アプリケーション設定で手動で作成されたユーザーアカウントによる接続用に TCP 13031 ポートを開きます。また、Kaspersky Embedded Systems Security リモート管理プロセスの実行ファイル avp.exe のネットワーク接続も許可します。この設定は、コマンドラインで本製品をインストールする際に、`ADDWFEXCLUSION=1` のオプションを使用して管理できます。

Kaspersky Embedded Systems Security をリモートで実行する必要がある場合は、さらに次の操作を行います：

本製品をリモートで起動するユーザーアカウントは、Administrators グループに属している必要があります。

- リモートデバイスの Windows ファイアウォールの設定で、**ファイルとプリンターの共有（SMB 受信）**のルール（ポート TCP 445）を有効にします。デバイスへの接続を容易にするために、ポート TCP 135 を開くことも推奨します。

- Windows Vista 以降を実行しているリモートデバイスが、ドメインに属していないか、ローカルユーザーアカウントによって管理される場合、**リモートのユーザーアカウント制御（UAC）を無効にします。**

  1. コンピューター上のレジストリエディタを開きます。
  2. レジストリエディタで、[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]キーを開きます。
  3. [LocalAccountTokenFilterPolicy]値を開きます。

     このキーに LocalAccountTokenFilterPolicy の値がない場合は、この名前で DWORD（32 ビット）値を作成します（詳細については、Microsoft のテクニカルサポートサイトを参照してください）。
  4. 1 に設定して［**OK**］をクリックします。

     リモートの UAC を無効にしても、ローカルの UAC には影響しません。

- アプリケーションコンソールがインストールされているデバイスまたは保護対象デバイスが Windows 8.1 以前のバージョンの Windows を実行している場合、**Windows 10 以降を実行しているデバイス上の SMB 1.0/CIFS ファイルへの共有アクセスのサポートを有効にします。**

  - 「Windows の機能」アプリケーションで、次の操作を行います：

    1. ［**スタート**］→［**コントロールパネル**］→［**プログラムと機能**］→［**Windows の機能の有効化または無効化**］の順に選択します。
    2. ［**Windows の機能**］ウィンドウで、［**SMB 1.0/CIFS ファイル共有のサポート**］をオンにします。
    3. ［**OK**］をクリックします。

- Windows PowerShell で、次の操作を行います：

  1. Windows PowerShell を管理者として実行します。
  2. 次のコマンドを実行します：

     ```
     Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
     ```

その他のソフトウェアまたはハードウェアのファイアウォールを設定する時にも、同じ手順を適用してください。

*保護対象デバイスとアプリケーションコンソールがインストールされているデバイス間の接続を設定中にアプリケーションコンソールが開かれた場合：*

1. アプリケーションコンソールを閉じます。
2. Kaspersky Embedded Systems Security リモート管理プロセス（avp.exe）が終了するまで待機します。
3. アプリケーションコンソールを再起動します。
   新しい接続設定が適用されます。

## COM アプリケーションへの匿名リモートアクセスの許可

インストールされている Windows オペレーティングシステムによって、設定名が異なる場合があります。

*COM アプリケーションへ匿名リモートアクセスを許可するには：*

1. Kaspersky Embedded Systems Security コンソールがインストールされたリモートデバイスで、**コンポーネントサービス**コンソールを開きます。これを行うには：
   a. ［**スタート**］→［**ファイル名を指定して実行**］の順に選択します。
   b. `dcomcnfg` コマンドを実行します。
   c. **コンポーネントサービス**コンソールが開きます。
2. 保護対象デバイスの**コンポーネントサービス**コンソールで［**コンピューター**］を展開します。
3. ［**マイコンピューター**］のコンテキストメニューを開きます。
4. ［**プロパティ**］を選択します。
5. ［**プロパティ**］ウィンドウの［**COM セキュリティ**］タブで、［**アクセス許可**］設定グループの［**制限の編集**］をクリックします。
6. ［**リモートアクセスを許可する**］ウィンドウで、ANONYMOUS LOGON ユーザーに対して［**リモートアクセスを許可する**］になっていることを確認します。
7. ［**OK**］をクリックします。

## Kaspersky Embedded Systems Security リモート管理プロセスに対するネットワーク接続の許可

インストールされている Windows オペレーティングシステムによって、設定名が異なる場合があります。

*Windows ファイアウォールで TCP ポート 135 を開き、Kaspersky Embedded Systems Security リモート管理プロセスに対してネットワーク接続を許可するには：*

1. リモートデバイスで Kaspersky Embedded Systems Security コンソールを閉じます。
2. 次のいずれかを行います：
   - Microsoft Windows XP SP2 以降の場合：
     a. ［**スタート**］→［**Windows ファイアウォール**］の順に選択します。
     b. ［**Windows ファイアウォール**］ウィンドウ（または［Windows ファイアウォールの設定］）の［**除外**］タブで、［**ポートの追加**］をクリックします。
     c. ［**名前**］にポート名「RPC (TCP/135)」を指定するか、他の名前（「Kaspersky Embedded Systems Security DCOM」など）を入力し、［**ポート番号**］にポート番号（135）を指定します。
     d. ［**TCP**］プロトコルを選択します。
     e. ［**OK**］をクリックします。
     f. ［**除外リスト**］タブで、［**追加**］をクリックします。
   - Microsoft Windows 7 以降の場合：
     a. ［**スタート**］→［**コントロール パネル**］→［**Windows ファイアウォール**］の順に選択します。
     b. ［**Windows ファイアウォール**］ウィンドウで、［**Windows ファイアウォールを介したプログラムまたは機能を許可する**］を選択します。
     c. ［**Windows ファイアウォール経由の通信をプログラムに許可します**］ウィンドウで、［**別のプログラムの許可**］をクリックします。
3. ［**アプリケーションを追加**］ウィンドウでファイル kavfsrcn.exe を指定します。このファイルは、Microsoft 管理コンソールを使用して Kaspersky Embedded Systems Security コンソールをインストールする時に指定したインストール先フォルダー内にあります。
4. ［**OK**］をクリックします。
5. ［**Windows ファイアウォール**］（［**Windows ファイアウォールの設定**］）ウィンドウで、［**OK**］をクリックします。

# Kaspersky Embedded Systems Security インストール後に実行する処理

製品をアクティベート済みである場合、インストールが完了すると保護タスクとスキャンタスクがすぐに開始されます。Kaspersky Embedded Systems Security のインストール中に［**製品インストール後にファイルのリアルタイム保護を有効にする（推奨）**］チェックボックスをオンにしていた場合、デバイスのファイルのシステムオブジェクトにアクセスした際にそれらのオブジェクトをスキャンします。スクリプト監視コンポーネントがカスタムインストールの一部としてインストールされた場合、Kaspersky Embedded Systems Security は、すべてのスクリプトのソースコードをその起動時にスキャンします。毎週金曜日の午後 8 時に*簡易スキャンタスク*が実行されます。

Kaspersky Embedded Systems Security のインストール後に、次の手順を実行してください：

- 定義データベースのアップデートタスクを開始します。インストール後、製品の配布キットに含まれる定義データベースを使用してオブジェクトがスキャンされます。

  定義データベースは最新のものでない可能性があるため、すぐにアップデートしてください。

  その後定義データベースは、タスクで設定されている既定のスケジュールに従って 1 時間ごとにアップデートされます。

- Kaspersky Embedded Systems Security をインストールする前にファイルのリアルタイム保護機能のあるアンチウイルス製品がデバイスにインストールされていなかった場合、簡易スキャンをデバイスで実行します。

- Kaspersky Embedded Systems Security イベントに関する管理者への通知を設定します。

## 定義データベースと製品機能のアップデートタスクの開始と設定

*インストール後に定義データベースをアップデートするには：*

1. 定義データベースと製品機能のアップデートタスクで、アップデート元への接続を設定します。
2. 定義データベースと製品機能のアップデートタスクを開始します。

LAN でプロキシサーバー設定を自動的に検知するための、Web Proxy Auto-Discovery Protocol（WPAD）がネットワークで設定されていないことがあります。その場合、プロキシサーバーにアクセスする時に認証が必要になる場合があります。

*プロキシサーバーにアクセスするためにオプションのプロキシサーバー設定と認証設定を行うには：*

1. ［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューを開きます。
2. ［**アプリケーションのプロパティ**］を選択します。
3. 表示されたウィンドウで、**ネットワークの設定**タブを選択します。
4. ［**プロキシサーバー設定**］セクションで［**設定**］をクリックして、表示されたウィンドウで、［**指定したプロキシサーバーを使用する**］をオンにします。

5. ［**アドレス**］フィールドにプロキシサーバーのアドレスを入力して、［**ポート**］フィールドにプロキシサーバーのポート番号を入力します。

6. ［**プロキシサーバーの認証設定**］セクションで、ドロップダウンリストから必要な認証方法を選択します：

   - **NTLM 認証**：プロキシサーバーによって組み込みの Microsoft Windows NTLM 認証がサポートされている場合に選択します。指定されたアカウントを使用して、プロキシサーバーにアクセスします。既定では、タスクはシステムユーザーアカウント（SYSTEM）で開始されます。

   - **ユーザー名とパスワードを指定して NTLM 認証を使用する**：プロキシサーバーによって組み込みの Microsoft Windows NTLM 認証がサポートされている場合に選択します。指定されたアカウントを使用してプロキシサーバーにアクセスします。ユーザー名とパスワードを入力するか、リストからユーザーを選択します。

   - **ユーザー名とパスワード**：基本認証を選択する場合に選択します。ユーザー名とパスワードを入力するか、リストからユーザーを選択します。

7. ［**OK**］をクリックします。

*定義データベースと製品機能のアップデートタスクを実行するには：*

1. アプリケーションコンソールツリーで、［**アップデート**］フォルダーを展開します。

2. ［**定義データベースのアップデート**］サブフォルダーのコンテキストメニューで、［**起動**］を選択します。

   定義データベースと製品機能のアップデートタスクが開始されます。

   タスクが正常に完了すると、インストールされた定義データベースの最新のアップデートの公開日が［**Kaspersky Embedded Systems Security**］フォルダーの結果ペインで確認できます。

## 簡易スキャン

Kaspersky Embedded Systems Security の定義データベースのアップデートが完了したら、*簡易スキャンタスク*を使用して保護対象デバイスをスキャンしてマルウェアの有無を確認します。

*簡易スキャンタスクを実行するには：*

1. アプリケーションコンソールツリーで、［**オンデマンドスキャン**］フォルダーを展開します。

2. ［**簡易スキャン**］サブフォルダーのコンテキストメニューで、［**起動**］を選択します。

タスクが開始し、［**実行中**］というタスクステータスが結果ペインに表示されます。

*タスクの実行ログを確認するには：*

［**簡易スキャン**］フォルダーの結果ペインで、［**タスクログを開く**］をクリックします。

# コンポーネントセットの変更と Kaspersky Embedded Systems Security の修復

Kaspersky Embedded Systems Security コンポーネントは追加と削除ができます。ファイルのリアルタイム保護を削除する場合は、事前にファイルのリアルタイム保護タスクを停止する必要があります。それ以外の状況では、ファイルのリアルタイム保護タスクや Kaspersky Security サービスを停止する必要はありません。

アプリケーション管理がパスワードで保護されている場合、セットアップウィザードでコンポーネントセットを削除または変更しようとすると、パスワードの入力を要求されます。

*Kaspersky Embedded Systems Security のコンポーネントセットを変更するには：*

1. Windows の［**コントロールパネル**］で、［**アプリと機能**］を選択します。［**変更または削除**］ウィンドウが表示されます。
2. ［**Kaspersky Embedded Systems Security**］を右クリックし、［**編集**］を選択します。
   セットアップウィザードの［**アプリケーションの変更、修復、削除**］ウィンドウが表示されます。
3. ［**変更**］を選択します。
   ［**カスタムインストール**］ウィンドウが表示されます。［**すべての機能**］を選択し、［**次へ(N) >**］をクリックします。
4. ［**カスタムインストール**］ウィンドウの、選択可能なコンポーネントのリストで Kaspersky Embedded Systems Security に追加するコンポーネントまたは削除するコンポーネントを選択します。それには、次の操作を実行します：
   - コンポーネントのセットを変更するには、選択したコンポーネント名の隣にあるボタンをクリックします。コンテキストメニューで、次のように選択します：
     - **ローカルハードディスクにインストール**：1つのコンポーネントをインストールする場合
     - **ローカルハードディスクにすべてインストール**：コンポーネントのグループをインストールする場合
   - 以前インストールしたコンポーネントを削除するには、選択したコンポーネント名の隣にあるボタンをクリックします。コンテキストメニューから［**インストールしない**］を選択します。

   ［**次へ(N) >**］をクリックします。
5. ［**インストールの準備ができました**］ウィンドウで、［**インストール**］をクリックして、アプリケーションコンポーネントの選択を確定します。
6. インストールの完了後に表示されるウィンドウで、［**終了**］をクリックします。

指定の設定に基づいて、Kaspersky Embedded Systems Security のコンポーネントのセットが変更されます。

Kaspersky Embedded Systems Security の実行中に問題が発生した場合（タスクのクラッシュや、タスクが開始しないなどの Kaspersky Embedded Systems Security のクラッシュ）、Kaspersky Embedded Systems Security の修復を行うことができます。Kaspersky Embedded Systems Security の現在の設定の保存中に、修復を実行できます。または、Kaspersky Embedded Systems Security のすべての設定を既定値にリセットするオプションを選択できます。

*アプリケーションまたはタスクのクラッシュ後に Kaspersky Embedded Systems Security を修復するには：*

1. Windows の［**コントロールパネル**］で、［**アプリと機能**］を選択します。［**変更または削除**］ウィンドウが表示されます。
2. ［**Kaspersky Embedded Systems Security**］を右クリックし、［**編集**］を選択します。
3. セットアップウィザードの［**アプリケーションの変更、修復、削除**］ウィンドウが表示されます。
4. ［**修復**］を選択します。

   ［**Kaspersky Embedded Systems Security の修復**］ウィンドウが表示されます。［**次へ(N) >**］をクリックします。
5. 復元操作が完了するまで待ち、表示されるウィンドウで［**終了**］をクリックします。

指定した設定を使用して、Kaspersky Embedded Systems Security が修復されます。

# セットアップウィザードを使用したアンインストール

このセクションでは、セットアップ / アンインストールウィザードを使用した保護対象デバイスからの Kaspersky Embedded Systems Security およびアプリケーションコンソールの削除方法について説明します。

## Kaspersky Embedded Systems Security のアンインストール

Kaspersky Embedded Systems Security をアンインストールしても、ダンプファイルとトレースファイルは削除されません。ダンプファイルとトレースファイルの書き込みの設定で指定したフォルダーから、ダンプファイルとトレースファイルを手動で削除できます。

インストールされている Windows オペレーティングシステムによって、設定名が異なる場合があります。

セットアップおよびアンインストールウィザードを使用して、保護対象デバイスから Kaspersky Embedded Systems Security をアンインストールできます。

保護対象デバイスからの Kaspersky Embedded Systems Security のアンインストール後、再起動が必要になる場合があります。再起動は延期することもできます。

本製品のアンインストール、復元およびインストールは Windows のコントロールパネルでは実行できません。

Kaspersky Embedded Systems Security は、ユーザーがセットアップウィザードでコンポーネントを削除または変更しようとすると、ユーザーのアカウント認証情報を要求します。適切な権限を持つユーザーの認証情報を入力してください。削除を実行するユーザーアカウントに Windows のパスワードが設定されていない場合、削除を開始する前に**［重要な操作の確認用のパスワードを要求する］**を無効にしていることを確認してください。

*Kaspersky Embedded Systems Security をアンインストールするには：*

1. Windows の［**コントロールパネル**］で、［**アプリと機能**］を選択します。［**変更または削除**］ウィンドウが表示されます。
2. ［**Kaspersky Embedded Systems Security**］を右クリックし、［**編集**］を選択します。
3. セットアップウィザードの［**アプリケーションの変更、修復、削除**］ウィンドウが表示されます。
4. ［**削除**］を選択します。
   ［**データの保存**］ウィンドウが表示されます。
5. 必要に応じて、［**データの保存**］ウィンドウで、次の操作を実行します：
   ［**データの保存**］で、保持するオブジェクトまたは設定を指定します。既定では、このチェックボックスはオフです。
   - ［**ライセンスを保存する**］チェックボックスをオンにします。
   - ［**バックアップファイル**］チェックボックスをオンにします。
   - ［**以前の設定を使用する**］チェックボックスをオンにします。

   ［**データのエクスポート**］で、エクスポートするオブジェクトを指定します。既定では、このチェックボックスはオフです。
   - 隔離されたオブジェクトをエクスポートする場合は、［**隔離されたオブジェクトをエクスポートする**］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。
   - Kaspersky Embedded Systems Security のバックアップからオブジェクトをエクスポートする場合は、［**バックアップされたオブジェクトをエクスポートする**］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。
   - ［**保存する**］をクリックし、オブジェクトのエクスポート先のフォルダーを選択します。既定では、オブジェクトは %ProgramData%\Kaspersky Lab\KESS.4.0\QB のフォルダーにエクスポートされます。

     ［**次へ**］をクリックします。
6. ［**アンインストールの準備ができました**］ウィンドウで、［**削除**］をクリックして削除を確定します。
7. アンインストールの完了後に表示されるウィンドウで、［**終了**］をクリックします。

Kaspersky Embedded Systems Security が保護対象デバイスからアンインストールされます。

## Kaspersky Embedded Systems Security コンソールのアンインストール

インストールされている Windows オペレーティングシステムによって、設定名が異なる場合があります。

セットアップおよびアンインストールウィザードを使用して、保護対象デバイスからアプリケーションコンソールをアンインストールできます。

アプリケーションコンソールのアンインストール後、保護対象デバイスを再起動する必要はありません。

*アプリケーションコンソールをアンインストールするには：*

1. Windows の［**コントロールパネル**］で、［**アプリと機能**］を選択します。［**変更または削除**］ウィンドウが表示されます。

2. ［**Kaspersky Embedded Systems Security コンソール**］を右クリックし、［**編集**］を選択します。
   ウィザードの［**アプリケーションの変更、修復、削除**］ウィンドウが表示されます。

3. ［**削除**］を選択します。
   ［**アンインストールの準備ができました**］ウィンドウが表示されます。［**アンインストール**］をクリックします。

4. アンインストールの完了後に表示されるウィンドウで、［**OK**］をクリックします。

アンインストールが完了し、セットアップウィザードが終了します。

# コマンドラインによる製品のインストールとアンインストール

このセクションでは、コマンドラインを使用して Kaspersky Embedded Systems Security をインストールおよびアンインストールする方法について説明します。コマンドラインから Kaspersky Embedded Systems Security をインストールおよびアンインストールするためのコマンドの例や、コマンドラインから Kaspersky Embedded Systems Security のコンポーネントを追加または削除するためのコマンドの例も記載されています。

## コマンドラインからの Kaspersky Embedded Systems Security のインストールとアンインストール

Kaspersky Embedded Systems Security をアンインストールしても、ダンプファイルとトレースファイルは削除されません。ダンプファイルとトレースファイルの書き込みの設定で指定したフォルダーから、ダンプファイルとトレースファイルを手動で削除できます。

コマンドラインオプションを使用して、インストール設定を指定した後で、コマンドラインからインストールパッケージファイル \exec\ess_win.msi を実行することにより、Kaspersky Embedded Systems Security をインストールまたはアンインストールし、そのコンポーネントを追加または削除できます。

「管理ツール」セットは、保護対象デバイスまたはネットワークにある別のデバイスにインストールして、ローカルまたはリモートでアプリケーションコンソールを使用できます。それには、インストールパッケージ \console\esstools.msi を使用します。

インストールは、製品がインストールされている保護対象デバイスの管理グループに登録されているアカウントを使用して実行します。

ファイル \exec\ess_win.msi が、追加のコマンドラインオプションがない状態で保護対象デバイスで実行されている場合、Kaspersky Embedded Systems Security は、既定のインストール設定でインストールされます。

ADDLOCAL コマンドラインオプションを使用して、選択したコンポーネントやコンポーネントセットのコードをリストすることで、インストールする一連のコンポーネントを割り当てることができます。

# Windows インストーラーサービスでの Kaspersky Embedded Systems Security ソフトウェアコンポーネントの指定時に使用するコンポーネントコード

ファイル \product_long_term\ess_win.msi は、Kaspersky Embedded Systems Security の **Default Deny テクノロジーによるコンピューターの保護**の設定をインストールするように設計されており、ファイル \exec\ess_win.msi は、**アンチウイルスベースでのコンピューターの保護**の設定をインストールするように設計されています。

「**アンチウイルスベースでのコンピューターの保護"**」の設定が選択されている場合、ファイアウォールコンポーネントとパフォーマンスカウンターコンポーネントを除くすべての Kaspersky Embedded Systems Security コンポーネントが既定で含まれています。

コンピューターを保護するためにシグネチャ分析と定義データベースを使用しないアプリケーションのバージョンに Kaspersky Embedded Systems Security の［**アンチウイルスベースでのコンピューターの保護"**］の設定をインストールすると、次のコンポーネントを追加することによってアプリケーションコンポーネントのセットが自動的に拡張されます：

- ファイルのリアルタイム保護
- オンデマンドスキャン
- ネットワーク脅威対策

アップデートを有効にするコンポーネントは、［**Default Deny テクノロジーによるコンピューターの保護"**］の設定には含まれていません。

［**Default Deny テクノロジーによるコンピューターの保護"**］の設定が選択されている場合、既定で含まれるコンポーネントは、次の通りです：

- Core
- 脆弱性攻撃ブロック
- アプリケーション起動コントロール
- システムトレイアイコン

コンピューターを保護するためにシグネチャ分析と定義データベースを使用するアプリケーションのバージョンに Kaspersky Embedded Systems Security の「**Default Deny テクノロジーによるコンピューターの保護"**」の設定をインストールすると、次のコンポーネントを削除することによってアプリケーションコンポーネントのセットが自動的に削減されます：

- ファイルのリアルタイム保護
- オンデマンドスキャン
- アップデートを有効にするコンポーネント

この設定は、リソースが限られているデバイスの保護に推奨されます。この場合、本製品を長期間アクティベートすることができ、アプリケーション起動コントロールによりコンピューターが保護されます。

ファイル \console\esstools.msi により、管理ツールに含まれるすべての製品コンポーネントがインストールされます。

次のセクションでは、Windows インストーラーサービスでの Kaspersky Embedded Systems Security ソフトウェアコンポーネントの指定時に使用するコンポーネントコードをリストにまとめています。これらのコードを使用して、コマンドラインから Kaspersky Embedded Systems Security をインストールする際に、インストールするコンポーネントのリストを指定することができます。

## Kaspersky Embedded Systems Security ソフトウェアコンポーネント

次の表には、Kaspersky Embedded Systems Security のソフトウェアコンポーネントのコードと説明が記載されています。

Kaspersky Embedded Systems Security ソフトウェアコンポーネントの説明

| コンポーネント | コード | コンポーネントの機能 |
|---|---|---|
| ファイルのリアルタイム保護 | `FileThreatProtection` | 保護対象デバイスにあるファイルにアクセスした際に、それらのファイルに対してウイルススキャンを実行します。 |
| AMSI スキャナー | `AMSI` | この機能は Microsoft 社の AMSI（Antimalware Scan Interface）をサポートすることを目的とした機能です。AMSI（Antimalware Scan Interface）により、AMSI 機能をそなえたサードパーティ製品は、オブジェクト（たとえば、PowerShell スクリプトなど）のより詳細なスキャンを実行するために Kaspersky Embedded Systems Security へオブジェクトを送信し、スキャン結果を取得できます。 |
| ふるまい検知 | `BehaviorDetection` | このコンポーネントは、ブロック対象コンピューターのリストに、悪意のある動作を示しているリモートデバイスの名前を入力します。 |
| 脆弱性攻撃ブロック | `ExploitPrevention` | このコンポーネントは、デバイスのメモリにあるプロセスが使用するメモリを保護する設定の管理を可能にします。 |
| 修復エンジン | `RemediationEngine` | このコンポーネントにより、マルウェアがオペレーティングシステム内で行った処理を、Kaspersky Embedded Systems Security がロールバックできるようになります。 |
| ファイアウォール | `Firewall` | このコンポーネントを使用すると、Windows ファイアウォールを、Kaspersky Embedded Systems Security のグラフィカルユーザーインターフェイスから管理することが可能になります。 |
| ネットワーク脅威対策 | `NetworkThreatProtection` | このコンポーネントは、受信ネットワークトラフィックにおいて、典型的なネットワーク攻撃の活動があるかどうかをスキャンします。使用中のコンピューターを標的としてネットワーク攻撃が試行されたことが検知された場合、Kaspersky Embedded Systems Security は攻撃側コンピューターからのネットワーク活動をブロックします。 |
| アプリケーション起動コントロール | `ApplicationControl` | このコンポーネントは、ユーザーによるアプリケーションの起動の試行を監視し、指定されたアプリケーション起動コントロールルールに基づいて起動を許可または拒否します。 |
| デバイスコントロール | `DeviceControl` | このコンポーネントは、保護対象デバイスへの外部デバイスの接続の試行を追跡し、指定したデバイスコントロールルールに従って、それらのデバイスの使用を許可または拒否します。 |
| Kaspersky Security Center ネットワークエージェントとの連携モジュール | `AdminKitConnector` | このコンポーネントにより、Kaspersky Embedded Systems Security と Kaspersky Security Center ネットワークエージェント間の接続が可能になります。<br>Kaspersky Security Center を使用して製品を管理する場合、保護対象デバイスにこのコンポーネントをインストールできます。 |
| Windows イベントログ監視 | `LogInspector` | このコンポーネントは、Windows イベントログの検査の結果に基づいて、保護された環境の整合性を監視します。 |
| システム変更監視 | `SystemIntegrityMonitor` | このコンポーネントには、ファイル変更監視のすべての機能が含まれており、さらにレジストリの変更や外部デバイスの接続を監視することもできます。 |

| コンポーネント | コード | コンポーネントの機能 |
| --- | --- | --- |
| 有害 USB 攻撃ブロック | `BadUSBAttackPrevention` | このコンポーネントは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。 |
| Managed Detection and Response | `MDR` | このコンポーネントは、Kaspersky Managed Detection and Response ソリューションとのやり取りをサポートします。 |

## 「管理ツール」ソフトウェアコンポーネント

「管理ツール」ソフトウェアコンポーネントのコードとその説明を次の表に示します。

「管理ツール」ソフトウェアコンポーネントの説明

| コンポーネント | コード | コンポーネントの機能 |
| --- | --- | --- |
| Kaspersky Embedded Systems Security スナップイン | MmcSnapin | Kaspersky Embedded Systems Security コンソールから本製品を管理するために Microsoft 管理コンソールスナップインをインストールします。<br>MmcSnapin は自動的にインストールされるため、セットアップコマンドパラメータで指定する必要はありません。 |

# インストールと復元の設定、および Windows インストーラーのコマンドラインオプション

このセクションでは、Kaspersky Embedded Systems Security のインストールと復元の設定について説明します。このセクションには、インストール設定を変更するためのキーと可能なキー値も記載されています。これらのキーは、コマンドラインから Kaspersky Embedded Systems Security をインストールする時に Windows インストーラーサービスのコマンド `msiexec` で使用する標準のキーと一緒に使用できます。

## インストール設定と Windows インストーラーのコマンドラインオプション

- 使用許諾契約書の条件に同意。

  `EULA=<` **値** `>` コマンドラインオプションで取り得る値は、次の通りです：

  - `0` - 使用許諾契約書の条件を拒否する（既定値）。
  - `1` - 使用許諾契約書の条件に同意する。

- プライバシーポリシーの条項に同意。

  `PRIVACYPOLICY=<` **値** `>` コマンドラインオプションで取り得る値は、次の通りです：

  - `0` - プライバシーポリシーの条項を拒否する（既定値）。
  - `1` - プライバシーポリシーの条項に同意する。

- アップグレード中に以前のバージョンの設定を保持した状態で、Kaspersky Embedded Systems Security をインストール。

RESTOREDEFSETTINGS=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

- 0 – アップデート中に以前のバージョンのすべてのデータが新しいバージョンに移行されます（既定値）。
- 1 – アクティベーションデータと秘密鍵を含むファイルのみが、アップデート中に新しいバージョンに移行されます（[ドライブ]:\ProgramData\Kaspersky Lab\<製品>\<バージョン>\Data\product.dat）。設定、定義データベース、レポート、隔離、バックアップオブジェクトなど、以前のバージョンのその他のデータはすべて削除されます。

- アップグレード中に以前のレポートを保持した状態で、Kaspersky Embedded Systems Security をインストール。

  KEEP_REPORTS=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

  - 0 – レポート（[ドライブ]:\ProgramData\Kaspersky Lab\<製品>\<バージョン>\Reports）を除く、以前のバージョンのすべてのデータは、アップグレード中に新しいバージョンに移行されます。レポートは削除されます。
  - 1 - 設定、定義データベース、レポート、隔離、バックアップオブジェクトなど、以前のバージョンのすべてのデータがアップデート中に新しいバージョンに移行されます（既定値）。

- インストールの時に Kaspersky Embedded Systems Security のファイルが保存されるフォルダー。別のフォルダーも指定できます。

  INSTALLDIR=< フォルダーの完全パス > コマンドラインオプションの既定値は、次の通りです：

  - 32 ビット版の Microsoft Windows：
    - Kaspersky Embedded Systems Security: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0
    - Kaspersky Embedded Systems Security コンソール: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools.4.0.0
  - 64 ビット版の Microsoft Windows：%ProgramFiles(x86)%。これ以降のパスは、32 ビット版の Microsoft Windows のパスと同様です。

- ファイルのリアルタイム保護タスクを、Kaspersky Embedded Systems Security の起動後すぐに開始するかどうかの設定。

  RUNRTP=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

  - 1 - 開始する（既定値）。
  - 0 - 開始しない。

- ライセンス情報ファイルのパス（LICENSEKEYPATH）。既定では、配布キットのフォルダー \product にある、拡張子が .key のファイルをインストーラーが探そうとします。フォルダー \exec に複数のライセンス情報ファイルが含まれている場合、Windows インストーラーは有効期限が最も遠い日付であるライセンス情報ファイルを選択します。ライセンス情報ファイルは、フォルダー \exec または LICENSEKEYPATH パラメータで指定できる別のパスに事前に保存できます。

  LICENSEKEYPATH が取り得る値は次の通りです。

  - ライセンス情報ファイルへの完全パス（ファイル名を含む）。
  - ライセンス情報ファイルが保存されるフォルダーへのパス。

Kaspersky Embedded Systems Security のインストール後、アプリケーションコンソールなどの管理ツールを使用してライセンスを追加できます。製品のインストール時にライセンスを追加しない場合、Kaspersky Embedded Systems Security は機能しません。

- 設定情報ファイルのパス。Kaspersky Embedded Systems Security は、製品に作成された指定の設定情報ファイルから各設定をインポートします。タスクの起動に使用するアカウントのパスワードやプロキシサーバーに接続するためのパスワードなどのパスワードは、設定情報ファイルからインポートされません。設定のインポートが完了すると、すべてのパスワードを手動で入力する必要があります。設定情報ファイルを指定しない場合、セットアップの完了後、既定の設定が使用されます。

  `CONFIGPATH=<` **設定情報ファイル名** `>` の既定値は指定されていません。

- *オペレーティングシステムの起動時にスキャンモード*（SCANSTARTUP_BLOCKING）。SCANSTARTUP_BLOCKING キーを使用せずに Kaspersky Embedded Systems Security がインストールされた場合、［オペレーティングシステムの起動時にスキャン］の**スキャン範囲**パラメータは次のように設定されます。

  - 感染などの問題があるオブジェクトの処理：**通知する**。
  - 感染の可能性があるオブジェクトの処理：**通知する**。

  SCANSTARTUP_BLOCKING キーを使用して Kaspersky Embedded Systems Security がインストールされた場合、［オペレーティングシステムの起動時にスキャン］の**スキャン範囲**パラメータは次のように設定されます。

  - 感染などの問題があるオブジェクトの処理：**推奨処理を実行する**。
  - 感染の可能性があるオブジェクトの処理：**推奨処理を実行する**。

  *オペレーティングシステムの起動時にスキャンタスク*は、自動的に作成されます。既定では、［**通知する**］モードが適用されます。この場合、 Kaspersky Embedded Systems Security をデバイスに導入した後、スキャン中にシステムサービスに問題が検知されなければ、*オペレーティングシステムの起動時にスキャンタスク*を有効にできます。本製品が重要なシステムサービスを感染したオブジェクトまたは感染している可能性のあるオブジェクトとして検知した場合、［**通知する**］モードを使用すると、その理由を突き止めて問題を解決する時間が与えられます。本製品で［**推奨処理を実行する**］モードが適用されている場合、［**駆除する。駆除できない場合は削除する**］の処理が実行されます。駆除またはシステムファイルの削除により、オペレーティングシステムの起動に重大な問題が発生する可能性があります。

- 非互換ソフトウェアのチェックの無効化。この設定を使用して、保護対象デバイスへの本製品のバックグラウンドインストール中に、互換性のないソフトウェアのチェックを有効または無効にします。この設定の値にかかわらず、Kaspersky Embedded Systems Security のインストール中に、保護対象デバイスに他のバージョンの本製品がインストールされていることを常に警告します。

  `SKIPINCOMPATIBLESW=<` **値** `>` コマンドラインオプションで取り得る値は、次の通りです：

  - `0` - 非互換ソフトウェアのチェックを実行する（既定値）。
  - `1` - 非互換ソフトウェアのチェックを実行しない。

- オペレーティングシステムの更新プログラム KB5007186 のチェックを無効にします。

  更新プログラム KB5007186 をインストールしても、本製品は引き続き正常に動作し、システムのセキュリティは侵害されませんが、本製品のマイナーアップデートはできなくなります。本製品をインストールする前に、インストーラーによって、インストールされているオペレーティングシステムの更新プログラムがチェックされます。更新プログラム KB5007186 が検出されると、インストーラーはインストールを中止します。コマンドラインで `SKIPKB5007186CHECK` キーを使用して、オペレーティングシステムの更新プログラム KB5007186 のチェックを有効または無効にすることができます。

SKIPKB5007186CHECK=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

- 0 - インストーラーは、オペレーティングシステムの更新プログラム KB5007186 がインストールされているかどうかをチェックします。
- 1 - インストーラーは、オペレーティングシステムの更新プログラム KB5007186 がインストールされているかどうかをチェックしません。

既定では、キーは設定されてません（0 と同じ）。

- オペレーティングシステムのサービスの保護機能の設定。

  この機能が有効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することはできません。PROTECTOSSERVICES=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

  - 1：オペレーティングシステムのサービスの保護は有効です（既定値）。
  - 0：オペレーティングシステムのサービスの保護は無効です。

- 本製品がインストールされているコンピューターへのアプリケーションコンソールのリモート接続に使用するポートを設定するには：

  Windows の資格情報で接続するためのポートを設定するには、パラメータ UIPORT=< ポート番号 > を使用できます。指定可能なポートの番号の範囲：1 ～ 65535。番号が指定された範囲外の場合、既定のポート番号が使用されます。既定値は 13032 です。

  必要に応じて、パラメータ ENABLEUIKLPORT=< 値 > を使用して、手動で作成したユーザーの資格情報を使用して接続するためのポートを閉じることができます：

  - 1：ポートを開きます（既定の設定）。
  - 0：ポートを閉じます。

  このポートの既定値は 13031 です。パラメータ UIKLPORT=< 値 > を指定することで、ポート番号を変更することができます。指定可能なポートの番号の範囲は 1 ～ 65535 です。

- 別のコンピューターにインストールされたアプリケーションコンソールを使用して、Kaspersky Embedded Systems Security をリモートから管理するネットワーク接続を有効にするための設定。

  ADDWFEXCLUSION=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

  - 1。この値を指定すると、アプリケーションコンソールからアプリケーションがインストールされているコンピュータへのリモート接続用に構成された TCP ポート（パラメータ UIPORT=< 値 >、UIKLPORT=< 値 >）が Windows ファイアウォールで開かれ、 Kaspersky Embedded Systems Security のリモート管理プロセスの実行ファイル avp.exe へのネットワーク接続が許可されます。

    別のデバイスに本製品をインストールする場合の追加設定についてもご確認ください。

  - 0。この値が指定された場合は、何も行われません。

## 復元設定と Windows インストーラーのコマンドラインオプション

- 隔離されたオブジェクトの復元。

RESTOREQTN=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

- 0 - 隔離されたコンテンツを削除する（既定値）。
- 1 - 隔離されたコンテンツをパラメータ RESTOREPATH で指定したフォルダーの \QB サブフォルダーに復元する。

- バックアップのコンテンツの復元。

  RESTOREBCK=< 値 > コマンドラインオプションで取り得る値は、次の通りです：

  - 0 - バックアップのコンテンツを削除する（既定値）。
  - 1 - バックアップコンテンツをパラメータ RESTOREPATH で指定したフォルダーの \QB サブフォルダーに復元する。

- 現在のパスワードの入力による、復元を実行してよいかの確認（パスワードによる保護が有効の場合）。

  UNLOCK_PASSWORD=< 指定されたパスワード > の既定値は指定されていません。

- 復元されたオブジェクトのフォルダー。復元したオブジェクトは、指定されたフォルダーに保存されます。

  RESTOREPATH=< フォルダーの完全パス > コマンドラインオプションの既定値は、%ALLUSERSPROFILE%\Program Data\Kaspersky Lab\KESS.4.0.0\QB\Restored です。

# Kaspersky Embedded Systems Security のインストールで使用するコマンド事例

このセクションでは、Kaspersky Embedded Systems Security のインストールに使用するコマンドの例を紹介します。

保護対象デバイスで、配布キットのファイル ess_win.msi を実行します。

Windows インストーラーの標準的なコマンドとコマンドラインオプションの使用についての詳細な情報については、Microsoft から提供されるガイドを参照してください。

## ファイル setup_ess.exe からの Kaspersky Embedded Systems Security のインストールの例

*推奨されているインストール設定に基づき、ユーザーの操作を必要とせず Kaspersky Embedded Systems Security をインストールするには：*

```
\exec\setup_ess.exe EULA=1 PRIVACYPOLICY=1
```

*デバイスコントロールなどのコンポーネントをインストールするには：*

```
\exec\setup_ess.exe /p ADDLOCAL=DevCtrl /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

アプリケーションのインストール後にシステムクラッシュを引き起こすネットワークデバイスおよび SCSI デバイスが搭載されたコンピューターに Kaspersky Embedded Systems Security をインストールする場合、このコマンドで次の追加オプションを使用できます：

```
/p SKIP_NETWORK_UPPERFILTERS=<1|0>
```

ネットワークアダプターの監視を有効（1）または無効（0）にします。

```
/p SKIP_SCSIADAPTER_UPPERFILTERS=<1|0>
```

SCSI アダプターの監視を有効（1）または無効（0）にします。

*ライセンス情報ファイルを使用して Kaspersky Embedded Systems Security をインストールしてアクティベートするには：*

```
setup_ess.exe /s EULA=1 PRIVACYPOLICY=1 /p LICENSEKEYPATH=C:\0000000A.key
```

*Windows のユーザー資格情報で本製品がインストールされているコンピューターへのアプリケーションコンソールのリモート接続に使用するポートを変更するには：*

```
setup_ess.exe /pUIPORT=<ポート番号>
```

指定可能なポートの番号の範囲：1 ～ 65535。既定値は 13032 です。

## インストールで使用するコマンドのリスト：msi ファイルを実行

*推奨されているインストール設定に基づき、ユーザーの操作を必要とせず Kaspersky Embedded Systems Security をインストールするには：*

```
msiexec /i ess_win.msi /qn EULA=1 PRIVACYPOLICY=1
```

*推奨されているインストール設定に基づき、インストールインターフェイスを表示して Kaspersky Embedded Systems Security をインストールするには：*

```
msiexec /i ess_win.msi /qf EULA=1 PRIVACYPOLICY=1
```

*Kaspersky Embedded Systems Security を推奨インストール設定でインストールし、トレースファイルの数が指定された最大数に達した時にトレースファイルのローテーションを有効にするには：*

```
msiexec /i ess_win.msi TRACE_FOLDER=C:\Traces TRACE_MAX_ROLL_COUNT=50 /qn EULA=1
PRIVACYPOLICY=1
```

TRACE_FOLDER パラメータは必須です。

TRACE_MAX_ROLL_COUNT パラメータには次のルールが適用されます：

- このパラメータを指定すると、トレースファイルの数がパラメータで指定した最大数に達した時に、トレースファイルのローテーションが有効になります。使用可能なパラメータ値の範囲：1 ～ 999。
- トレースファイルの最大数を 0 に指定すると、トレースファイルのローテーションが無効になります。
- パラメータ値が指定されているが、無効であるか、使用可能な値の範囲（1 ～ 999）を超えている場合、トレースファイルのローテーションは、既定のトレースファイルの最大数が 5 に設定されて有効になります。
- パラメータが指定されていない場合：
  - トレースファイルのローテーションがデバイス上で設定済みである場合、その設定は変更されません。入力されたパラメータは無視されます。
  - デバイスでトレースファイルのローテーションが設定されていない場合、ローテーションオプションはトレースファイルの既定の最大数が 5 に設定されて有効になります。

*ライセンス情報ファイル C:\0000000A.key を使用して Kaspersky Embedded Systems Security をインストールしてアクティベートするには：*

```
msiexec /i ess_win.msi     LICENSEKEYPATH=C:\0000000A.key /qn EULA=1 PRIVACYPOLICY=1
```

*実行中のプロセスとローカルドライブのブートセクターを事前にスキャンし、Kaspersky Embedded Systems Security のインストールを実行するには：*

```
msiexec /i ess_win.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

*Kaspersky Embedded Systems Security をインストールフォルダー C:\KESS にインストールするには：*

```
msiexec /i ess_win.msi INSTALLDIR=C:\KESS/qn EULA=1 PRIVACYPOLICY=1
```

*Kaspersky Embedded Systems Security をインストールし、Kaspersky Embedded Systems Security の msi ファイルが保存されているフォルダーに ess.log という名前のインストールログファイルを保存するには：*

```
msiexec /i ess_win.msi/l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

*Kaspersky Embedded Systems Security コンソールをインストールするには：*

```
msiexec /i esstools.msi /qn EULA=1
```

*Kaspersky Embedded Systems Security をインストールしてライセンス情報ファイル C:\0000000A.key を使用してアクティベートし、設定情報ファイル C:\settings.xml の設定に応じて Kaspersky Embedded Systems Security を設定するには、次のコマンドを実行します：*

```
msiexec /i ess_win.msi LICENSEKEYPATH=C:\0000000A.key CONFIGPATH=C:\settings.xml /qn
EULA=1 PRIVACYPOLICY=1
```

*Kaspersky Embedded Systems Security がパスワードによって保護されている場合、製品のパッチをインストールするには：*

```
msiexec /p "<msp ファイル名とそのパス>" UNLOCK_PASSWORD=<パスワード>
```

# Kaspersky Embedded Systems Security インストール後に実行する処理

製品をアクティベート済みである場合、インストールが完了すると保護タスクとスキャンタスクがすぐに開始されます。Kaspersky Embedded Systems Security のインストール中に［**製品インストール後にファイルのリアルタイム保護を有効にする（推奨）**］チェックボックスをオンにしていた場合、デバイスのファイルのシステムオブジェクトにアクセスした際にそれらのオブジェクトをスキャンします。スクリプト監視コンポーネントがカスタムインストールの一部としてインストールされた場合、Kaspersky Embedded Systems Security は、すべてのスクリプトのソースコードをその起動時にスキャンします。毎週金曜日の午後 8 時に*簡易スキャン*タスクが実行されます。

Kaspersky Embedded Systems Security のインストール後に、次の手順を実行してください：

- Kaspersky Embedded Systems Security 定義データベースのアップデートタスクを開始します。インストール後、製品の配布キットに含まれる定義データベースを使用してオブジェクトがスキャンされます。Kaspersky Embedded Systems Security の定義データベースをすぐにアップデートすることを推奨します。それには、定義データベースのアップデートタスクを実行する必要があります。その後定義データベースは、既定のスケジュールに従って 1 時間ごとにアップデートされます。

例として、定義データベースのアップデートタスクは、次のコマンドを使用して開始できます：

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser
/PROXYPWD:123456
```

この場合、Kaspersky Embedded Systems Security の定義データベースのアップデートは、カスペルスキーのアップデートサーバーからダウンロードされます。アップデート元への接続は、プロキシサーバーを経由し（プロキシサーバーアドレス：proxy.company.com、ポート：8080）、ビルトイン Windows NTLM 認証を使用して、アカウント下のサーバー（ユーザー名：inetuser、パスワード：123456）にアクセスして確立します。

- Kaspersky Embedded Systems Security をインストールする前にファイルのリアルタイム保護機能のあるアンチウイルス製品がデバイスにインストールされていなかった場合、簡易スキャンをデバイスで実行します。

*コマンドラインを使用して簡易スキャンタスクを開始するには：*

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

このコマンドでは、現在のフォルダーに含まれるファイル scancritical.log に実行ログを保存します。

- Kaspersky Embedded Systems Security イベントに関する管理者への通知を設定します。

# コンポーネントの追加および削除：サンプルコマンド

*オンデマンドスキャンをインストールするには、次のコマンドを実行します：*

```
msiexec /i ess_win.msi ADDLOCAL=Oas,Ods /qn
```

または

```
\exec\setup_ess.exe /s /p ADDLOCAL=Oas,Ods
```

リストへのコンポーネントの追加後、既存のコンポーネントが再インストールされ、指定したコンポーネントがインストールされます。

*インストールされたコンポーネントを削除するには、次のコマンドを実行します：*

```
msiexec /i ess_win.msi REMOVE=Firewall,PerfMonCounters EULA=1 PRIVACYPOLICY=1 /qn
```

*新しいコンポーネントをインストールするには、次のコマンドを実行します。*

```
msiexec /i ess_win.msi
ADDLOCAL=AKIntegration,AVProtection,AntiExploit,AppCtrl,DevCtrl,Fim,Ksn,LogInspector,Oas
EULA=1 PRIVACYPOLICY=1 /qn
```

インストールまたは削除するコンポーネントをリストへ追加した後、そのコンポーネントがインストールまたは削除されます。

# Kaspersky Embedded Systems Security のアンインストール：サンプルコマンド

*保護対象デバイスから Kaspersky Embedded Systems Security をサイレントモードでアンインストールするには、次のコマンドを実行します：*

```
msiexec /x ess_win.msi KLLOGIN=<user name> KLPASSWD=<password> /qn
```

または

```
msiexec /x {70579418-34B7-49A8-A1EB-CF309F4D032B} KLLOGIN=<user name> KLPASSWD=<password> /qn
```

または

```
setup_ess.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
```

`<user name>` は、アンインストールするために必要な権限を持つユーザーの名称とログインアカウントです。

削除を実行するユーザーアカウントに Windows のパスワードが設定されていない場合、 削除を開始する前に**［重要な操作の確認用のパスワードを要求する］**を無効にしていることを確認してください。

*Kaspersky Embedded Systems Security コンソールをサイレントモードでアンインストールするには、次のコマンドを実行します：*

```
msiexec /x esstools.msi /qn
```

または

```
msiexec /x {D66EC1A9-A456-46FF-8B49-308A23FEBF88} /qn
```

# リターンコード

本製品のインストーラーによって、この記事で説明されているリターンコードが返される場合があります。

コマンドラインのリターンコードのリストを次の表に示します。

リターンコード

| コード | 説明 |
|---|---|
| 27100 | 認証エージェントがテストモードでインストールされたドライブがこのコンピューターで検出されました。 |
| 27101 | 認証エージェントがテストモードでインストールされたドライブがこのコンピューターで検出されました。 |
| 27102 | 暗号化されたディスクが見つかりませんでした。 |
| 27200 | メモリから製品をアンロードできませんでした。 |
| 27201 | AVP.exe プロセスの起動中にエラーが発生しました。コンピューターが感染している可能性があります。 |
| 27204 | パッケージのキャッシュに失敗しました。 |
| 27205 | ライセンス情報の統合に失敗しました。 |
| 27206 | ライセンス情報の削除に失敗しました。 |
| 27207 | 互換性のないソフトウェアの削除に失敗しました。 |
| 27208 | 互換性のないソフトウェアのチェックに失敗しました。 |

| コード | 説明 |
| --- | --- |
| 27209 | キャビネットからのファイルの展開に失敗しました。 |
| 27210 | セルフディフェンスの設定に失敗しました。 |
| 27211 | セルフディフェンスを有効にできませんでした。 |
| 27212 | オペレーティングシステムのバージョン情報を取得できませんでした。 |
| 27213 | スタートアップフォルダーの取得に失敗しました。 |
| 27214 | インストールフォルダーの検証に失敗しました。 |
| 27215 | サービスを設定できませんでした。 |
| 27216 | klcp のアップグレードの設定に失敗しました。 |
| 27217 | klcp のアップグレードに失敗しました。 |
| 27218 | kl1 ドライブパラメータの設定に失敗しました。 |
| 27219 | klelam ドライバーのパラメータの設定に失敗しました。 |
| 27220 | klwfp ドライバーのパラメータの設定に失敗しました。 |
| 27221 | ドライバー互換モードの設定に失敗しました。 |
| 27222 | レジストリキーの削除に失敗しました。 |
| 27223 | オペレーションシステムの再起動に失敗しました。 |
| 27224 | ドライバーをインストールできませんでした。 |
| 27225 | ドライバーの設定を移行できませんでした。 |
| 27226 | ドライバーを停止できませんでした。 |
| 27227 | ドライバーの開始をブロックできませんでした。 |
| 27228 | ファイルの署名の検証に失敗しました。 |
| 27230 | kldl ドライバーの設定を準備できませんでした。 |
| 27231 | kldl ドライバーの設定を構成できませんでした。 |
| 27300 | ドライバーのインストールエラー。 |
| 27301 | ドライバーの削除エラー。 |
| 27302 | ネットワークコンポーネントのインストールエラー。 |
| 27303 | ドライバーの登録情報が不一致または不完全です。オペレーティングシステムを再起動してもう一度お試しください。 |
| 27305 | ドライバーの無効化中にエラーが発生しました。 |
| 27310 | デジタル署名済みのカタログファイルをインストールできませんでした 。 |
| 27311 | デジタル署名済みのカタログファイルをアンインストールできませんでした 。 |
| 27312 | 証明書をインストールできませんでした。 |
| 27313 | 証明書を削除できませんでした。 |
| 27320 | サービスを設定できませんでした。 |
| 27321 | サービスの保護を解除できませんでした。 |
| 27350 | パッチ <パッチ名> は製品の言語版 <アプリケーション名> に対応していません。 |
| 27352 | ディスク全体の暗号化のパッチを削除できません。 |
| 27353 | パッチ <パッチ 1> をインストールするにはパッチ <パッチ 2> が必要です。 |
| 27354 | 製品を変更または修正する前に、コンピューターを再起動してパッチを適用する必要があります。 |
| 27355 | ディスク全体の暗号化の管理のロックに失敗しました。ディスク全体の暗号化の管理のロックに失敗しました。暗号化を完了してからインストールするか、ディスク全体の暗号化のアップデートをインストールしてください。 |
| 27356 | パッチをインストールできません。 |
| 27357 | インストールパッケージに取り消されたパッチが含まれています。インストールを中止します。 |

| コード | 説明 |
| --- | --- |
| 27360 | パッチを登録できません。 |
| 27361 | パッチインストールのパラメータの設定に失敗しました。 |
| 27363 | 暗号化ライブラリを含むパッチは、インストールされている暗号化ライブラリと互換性がありません。 |
| 27370 | .NET 8.0 のアップデートの解凍エラー。 |
| 27371 | .NET 8.0 の解凍エラー。 |
| 27372 | 以前のバージョンの製品の登録情報は削除されました。インストールを再開してください。 |
| 27373 | 以前のバージョンの製品の登録情報を削除できませんでした。 |
| 27374 | 本製品をアップグレード中です。しばらくたってからもう一度お試しください。 |
| 27375 | アンインストールのパスワードまたはユーザー名が指定されていないか、無効です。 |
| 27376 | Kaspersky Endpoint Agent をアンインストールできませんでした。手動でアプリケーションを削除するか、設定でパスワード保護を無効にしてください。その後、本製品のインストールを再度実行してください。 |
| 27377 | Kaspersky Security for Windows Server をアンインストールできませんでした。手動でアプリケーションを削除するか、設定でパスワード保護を無効にしてください。その後、本製品のインストールを再度実行してください。 |
| 27378 | ディスク容量が不足しています。 |
| 27379 | 互換性のないコンポーネントが選択されたため、本製品のインストールが失敗しました。インストールするコンポーネントを変更してインストールを再度開始してください。 |
| 27380 | 無効な設定ファイルが選択されました。 |
| 27381 | 無効なライセンスが選択されました。 |
| 27382 | 製品の管理グループを作成できませんでした。 |
| 27383 | 無効なフォルダーが選択されています。インストールフォルダー名には、160 文字を超える名前または特殊文字を指定できません。 |
| 27384 | インストール先に無効なフォルダーまたはディスクが選択されています。ローカルハードディスクにインストールする必要があります。 |
| 27385 | 無効なフォルダーが選択されています。ドライブのルートフォルダーへはインストールできません。 |
| 27386 | 無効なフォルダーが選択されています。Windows フォルダーまたはそのサブフォルダーにはインストールできません。 |
| 27387 | 無効なフォルダーが選択されています。Temp フォルダーが含まれているフォルダーへはインストールできません。 |
| 27388 | 無効なフォルダーが選択されています。Program Files フォルダーへ直接インストールすることはできません。 |
| 27389 | 無効なフォルダーが選択されています。仮想ディスクにはインストールできません。 |
| 27390 | インストール先に無効なフォルダーまたはディスクが選択されています。以前のバージョンがインストールされているフォルダーへはインストールできません。 |
| 27391 | 選択されたフォルダーに既にファイルが存在します。他のデータを含むフォルダーにアプリケーションをインストールできません。セルフディフェンス機能が有効になると、このデータを利用できなくなるためです。 |
| 27392 | 再解析ポイントを含むフォルダーへはインストールできません。別のインストールフォルダーを選択してください。 |
| 27393 | 本製品は、名前にセミコロン(;)が含まれているフォルダーにインストールできません。別のインストールフォルダーを選択してください。 |
| 27394 | 無効なフォルダーが選択されています。ルートフォルダーを指定することはできません。 |
| 27395 | 無効なフォルダーが選択されています。「Windows」フォルダーまたはそのサブフォルダーを指定することはできません。 |
| 27396 | 無効なフォルダーが選択されています。「Program Files」フォルダーを直接指定することはできません。 |
| 27397 | 無効なフォルダーが選択されています。「Temp」サブフォルダーを含むフォルダーを指定することはできません。 |
| 27400 | ファイルアップデートの初期化エラー。 |
| 27450 | CAB ファイルをインストールできません。 |
| 27451 | 削除エラー。 |
| 27452 | ファイルの削除エラー。 |
| 27453 | ファイルの移動エラー 。 |
| 27454 | レジストリファイルの作成に失敗しました。 |

| コード | 説明 |
| --- | --- |
| 27455 | オペレーティングシステムのバージョン情報を取得できませんでした。 |
| 27456 | レジストリ値のロールバックをスケジュールできませんでした。 |
| 27457 | よく知られているセキュリティ識別子 (SID)を取得できませんでした。 |
| 27460 | セキュリティ記述子の作成エラー。 |
| 27461 | セキュリティ記述子の復元エラー。 |
| 27462 | Windows ファイアウォール向けのルールを作成できませんでした。 |
| 27463 | Windows ファイアウォール向けのルールを削除できませんでした。 |

# Kaspersky Security Center を使用した製品のインストールとアンインストール

このセクションには、 Kaspersky Security Center を使用した Kaspersky Embedded Systems Security のインストールに関する情報、Kaspersky Security Center を使用した Kaspersky Embedded Systems Security のインストールおよびアンインストール手順の説明、および Kaspersky Embedded Systems Security のインストール後に実行する処理の説明が含まれています。

## Kaspersky Security Center を使用したインストールに関する全般的な情報

リモートインストールタスクを使用することで、Kaspersky Security Center を介して Kaspersky Embedded Systems Security をインストールできます。

リモートインストールタスクが完了すると、Kaspersky Embedded Systems Security は同じ設定で複数の保護対象デバイスにインストールされます。

すべての保護対象デバイスを 1 つの管理グループに統合し、このグループの保護対象デバイスに対して Kaspersky Embedded Systems Security をインストールするためのグループタスクを作成できます。

同じ管理グループに含まれていない一部の保護対象デバイスに対して、Kaspersky Embedded Systems Security をリモートでインストールするタスクを作成できます。このタスクを作成する際、Kaspersky Embedded Systems Security をインストールする個別の保護対象デバイスのリストを生成する必要があります。

リモートインストールタスクの詳細な情報については、*Kaspersky Security Center* のヘルプを参照してください。

# Kaspersky Embedded Systems Security をインストールまたはアンインストールする権限

リモートインストール（削除）タスクで指定されたアカウントは、あらゆる場合において各保護対象デバイスの管理グループに含まれている必要があります。ただし、以下で説明する場合を除きます：

- Kaspersky Embedded Systems Security のインストール先となる保護対象デバイスに Kaspersky Security Center ネットワークエージェントが既にインストールされている場合（保護対象デバイスのドメインや、保護対象デバイスがドメインに属しているかは問わない）。

  ネットワークエージェントが保護対象デバイスにインストールされていない場合、リモートインストールタスクを使用して、Kaspersky Embedded Systems Security と一緒にネットワークエージェントをインストールできます。ネットワークエージェントをインストールする前に、タスクで指定するアカウントが各保護対象デバイスの管理グループに含まれていることを確認してください。

- Kaspersky Embedded Systems Security のインストール先となるすべての保護対象デバイスが管理サーバーと同じドメインにあり、**ドメイン管理者**のアカウントで管理サーバーが登録されている場合（このアカウントが、そのドメイン内の保護対象デバイスに対してローカルの管理者権限を持っている場合）。

既定では、**強制インストール**の方法を使用する場合、リモートインストールタスクは管理サーバーが実行されるアカウントから実行されます。

強制インストール（アンインストール）モードでグループタスクまたは特定の保護対象デバイスに対するタスクを使用する場合、アカウントは保護対象デバイスに対して次の権限を持っている必要があります：

- リモートアプリケーションを実行する権限
- **Admin$** 共有に対する権限
- **サービスとしてログオンする**権限

# Kaspersky Security Center を使用した Kaspersky Embedded Systems Security のインストール

インストールパッケージの生成およびリモートインストールタスクの作成の詳細な情報については Kaspersky Security Center のヘルプを参照してください。

今後、Kaspersky Security Center を介して Kaspersky Embedded Systems Security を管理する場合、次の条件を満たす必要があります：

- Kaspersky Security Center 管理サーバーがインストールされている保護対象デバイスに、管理プラグインもインストールされていること（Kaspersky Embedded Systems Security 配布キットのファイル \exec\klcfginst.exe）。

- Kaspersky Security Center ネットワークエージェントが保護対象デバイスにインストールされていること。Kaspersky Security Center ネットワークエージェントが保護対象デバイスにインストールされていない場合、リモートインストールタスクを使用して Kaspersky Embedded Systems Security と一緒にネットワークエージェントをインストールできます。

後で Kaspersky Security Center のポリシーとグループタスクを使用して保護設定を管理するために、複数のデバイスを 1 つの管理グループにまとめることもできます。

*リモートインストールタスクを使用して Kaspersky Embedded Systems Security を Kaspersky Security Center 経由でインストールするには：*

1. Kaspersky Security Center の管理コンソールを開きます。

2. Kaspersky Security Center 管理コンソールで、［**詳細**］フォルダーを展開します。

3. ［**リモートインストール**］サブフォルダーを展開します。

4. ［**インストールパッケージ**］サブフォルダーの結果ペインで、［**インストールパッケージの作成**］をクリックします。

5. ［**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。

6. 新しいインストールパッケージ名を入力します。

7. インストールパッケージファイルとして、Kaspersky Embedded Systems Security 配布キットからファイル ess_win.kud を指定します。

   コンピューターの保護にシグネチャ分析と定義データベースを使用しない製品設定で［**アンチウイルスベースでのコンピューターの保護"**］の設定を使用して本製品をインストールする場合、またはその逆の場合は、まずファイル ess_win.kud で本製品をインストールするための権限を持つアカウントのログイン ID とパスワードを指定する必要があります。これを行うには、テキストエディターでファイル ess_win.kud を開き、`Params` 行に `/pKLLOGIN=<login>` と `/pKLPASSWD=<password>.` のパラメータを追加します。

   ［**使用許諾契約書とプライバシーポリシー**］ウィンドウが表示されます。

8. 使用許諾契約書とプライバシーポリシーの条項に同意する場合、［**この使用許諾契約書の内容をすべて確認し、理解した上で条項に同意します**］および［**データは、プライバシーポリシーに従って処理および送信されること（第三国への送信を含む）を理解しました。プライバシーポリシーの内容をすべて確認し、理解した上で同意します**］のチェックボックスをオンにします。

   インストールを続行するには、使用許諾契約書とプライバシーポリシーに同意する必要があります。

9. インストールする Kaspersky Embedded Systems Security コンポーネントのセットと、インストールパッケージの既定のインストール設定を変更するには：

   a. Kaspersky Security Center 管理コンソールで、［**リモートインストール**］フォルダーを展開します。

   b. ［**インストールパッケージ**］サブフォルダーの結果ペインで、作成した Kaspersky Embedded Systems Security インストールパッケージのコンテキストメニューを開いて［**プロパティ**］をクリックします。

c. インストールパッケージのプロパティウィンドウで、［**設定**］セクションを開きます。

d. インストールの種別を選択します。

e. ［**設定**］をクリックして、産業用システムの除外リストを指定します。

f. ［**コンポーネントの選択**］セクションで、インストールする Kaspersky Embedded Systems Security コンポーネントの名前の隣にあるチェックボックスをオンにします。

g. ［**ファイルのリアルタイム保護モード**］セクションで、［**製品インストール後にファイルのリアルタイム保護を有効にする（推奨）**］をオンにしてセキュリティレベルを指定します。

h. 必要に応じて、アプリケーションコンソールが製品をインストールしたコンピューターにリモート接続する際に使用する TCP ポートを変更します。

Windows 資格情報による接続の既定のポート番号は 13032 で、手動で作成されたユーザーの資格情報による接続の既定のポート番号は 13031 です。指定可能なポートの番号の範囲：1 ～ 65535。

手動で作成したユーザーアカウントの資格情報による接続を防ぐには、［**手動で作成したユーザーの資格情報を使用**］をオフにしてください。

i. インストールフォルダーを既定ではないものに指定する場合、［**設定**］をクリックして、フォルダーの名前とパスを［**アプリケーションのインストールパスを設定する**］セクションに指定します。

j. 適用可能な場合は設定情報ファイルを指定します。

k. 変更内容を保存します。

10. ［**インストールパッケージ**］フォルダーで、選択した保護対象デバイス（管理グループ）に Kaspersky Embedded Systems Security をリモートでインストールするタスクを作成します。タスクの設定を編集します。

リモートインストールタスクの作成と設定の詳細は、*Kaspersky Security Center* のヘルプを参照してください。

11. Kaspersky Embedded Systems Security リモートインストールタスクを実行します。

タスクで指定した保護対象デバイスに Kaspersky Embedded Systems Security がインストールされます。

# Kaspersky Embedded Systems Security インストール後に実行する処理

Kaspersky Embedded Systems Security をインストールしたら、デバイスにある Kaspersky Embedded Systems Security の定義データベースをアップデートしてください。また、Kaspersky Embedded Systems Security のインストール前に、リアルタイム保護機能が有効になっているアンチウイルス製品がデバイスにインストールされていなかった場合は、デバイスの簡易スキャンを実行してください。

Kaspersky Embedded Systems Security がインストールされた保護対象デバイスが、Kaspersky Security Center で同じ管理グループにまとめられている場合、次の方法を使用してこれらのタスクを実行できます：

1. Kaspersky Embedded Systems Security がインストールされた保護対象デバイスのグループに対して、定義データベースのアップデートタスクを作成します。Kaspersky Security Center 管理サーバーをアップデート元として設定します。

2. *簡易スキャン*のステータスを持つオンデマンドスキャンのグループタスクを作成します。*簡易スキャン*タスクの結果ではなく、このタスクの結果に基づいて、グループの各保護対象デバイスのセキュリティレベルが Kaspersky Security Center によって診断されます。

3. 保護対象デバイスのグループに対して新しいポリシーを作成します。ポリシーのプロパティの［**本製品の設定**］セクションで、［**ローカルシステムタスクの実行**］サブセクションの設定から、オンデマンドスキャンのシステムタスクのスケジュールによる開始と、管理グループの保護対象デバイスでの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。

Kaspersky Embedded Systems Security イベントに関する管理者への通知を設定することもできます。

# Kaspersky Security Center を使用したアプリケーションコンソールのインストール

インストールパッケージおよびリモートインストールタスクの作成の詳細な情報については Kaspersky Security Center のヘルプを参照してください。

*リモートインストールタスクを使用してアプリケーションコンソールをインストールするには：*

1. Kaspersky Security Center 管理コンソールで、［**詳細**］フォルダーを展開します。

2. ［**リモートインストール**］サブフォルダーを展開します。

3. インストールパッケージを作成します：

   a. ［**インストールパッケージ**］サブフォルダーの結果ペインで、［**インストールパッケージの作成**］をクリックします。

   b. ［**新規パッケージウィザード**］ウィンドウで、［**指定した実行ファイルのインストールパッケージを作成する**］をパッケージの種別として選択します。

   c. 新しいインストールパッケージ名を入力します。

   d. Kaspersky Embedded Systems Security 配布キットのフォルダーからファイル \client\setup_esstool.exe を選択し、［**すべてのフォルダーをインストールパッケージへコピー**］をオンにします。

   e. ［**実行ファイルの起動設定（オプション）**］フィールドに、パラメータ値 EULA=1 および PRIVACYPOLICY=1 を指定します。そうしないと、コンポーネントをインストールできません。

   ```
   /s /p "EULA=1 PRIVACYPOLICY=1"
   ```

f. 必要に応じて、［**実行ファイルの起動設定（オプション）**］フィールドで、ADDLOCAL コマンドラインオプションを使用して、インストールするコンポーネントのセットを変更し、INSTALLDIR コマンドラインオプションを使用して、既定以外のインストール先フォルダーを指定できます。例として、フォルダー C:\KasperskyConsole にスタンドアロンインストールを実行するには、次のコマンドラインオプションを使用します：

```
/s /p "INSTALLDIR=C:\KasperskyConsole EULA=1 PRIVACYPOLICY=1"
```

4. ［**インストールパッケージ**］サブフォルダーで、選択した保護対象デバイス（管理グループ）にアプリケーションコンソールをリモートでインストールするタスクを作成します。

5. タスクの設定を編集します。

リモートインストールタスクの作成と設定の詳細は、Kaspersky Security Center のヘルプを参照してください。

6. リモートインストールタスクを実行します。

タスクで指定した保護対象デバイスにアプリケーションコンソールがインストールされます。

# Kaspersky Security Center を使用した Kaspersky Embedded Systems Security のアンインストール

Kaspersky Embedded Systems Security をアンインストールしても、ダンプファイルとトレースファイルは削除されません。ダンプファイルとトレースファイルの書き込みの設定で指定したフォルダーから、ダンプファイルとトレースファイルを手動で削除できます。

ネットワークデバイスでの Kaspersky Embedded Systems Security 管理がパスワードで保護されている場合、1つ以上のアプリケーションをアンインストールするタスクを作成する際にはパスワードを入力します。パスワードによる保護が Kaspersky Security Center ポリシーにより集中管理されていない場合、Kaspersky Embedded Systems Security は、デバイスのうち入力したパスワードが設定値に適合したデバイスから正常にアンインストールされます。Kaspersky Embedded Systems Security は、その他の保護対象デバイスからはアンインストールされません。

*Kaspersky Embedded Systems Security をアンインストールするには：*

1. Kaspersky Security Center の管理コンソールで、アプリケーションを削除するタスクを作成し、開始します。

2. タスクで、アンインストール方法を選択し（インストール方法の選択と同様。前のセクションを参照）、管理サーバーがアンインストールを実行する保護対象デバイスにアクセスするために使用するアカウントを指定します。Kaspersky Embedded Systems Security のアンインストールで使用できるのは、既定のアンインストール設定のみです。

# Kaspersky Security Center を使用した製品コンポーネントのセットの変更

［*コンポーネントの変更*］タスクを使用すると、インストール後でも Kaspersky Embedded Systems Security のコンポーネントセットを変更できます。

**Kaspersky Security Center 管理コンソールで本製品コンポーネントのセットを変更する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**タスク**］フォルダーを選択します。

   タスクのリストが表示されます。

2. ［**新規タスク**］をクリックします。

タスクウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：タスク種別の選択

［**Kaspersky Embedded Systems Security for Windows (4.0)**］→［**コンポーネントの変更**］の順に選択します。

## ステップ 2：製品コンポーネントの変更のタスク設定

ユーザーのコンピューターで使用できる製品コンポーネントを選択します。タスクの詳細設定を指定します（下の表を参照ください）。

## ステップ 3：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。次の設定方法があります：

- 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
- *未割り当てデバイス*など、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
- デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。

## ステップ 4：タスク開始スケジュールの設定

たとえば、手動で、またはコンピューターを使用していないときに、タスクを開始するスケジュールを設定します。

### ステップ 5：タスク名の定義

［*アプリケーションコントロールコンポーネントの追加*］などのタスク名を入力します。

### ステップ 6：タスク作成の完了

ウィザードの操作を完了します。必要に応じて、［**ウィザードの終了後にタスクを実行**］をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

**Web コンソールで本製品コンポーネントのセットを変更する方法**

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**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。ウィザードの指示に従います。

### ステップ 1：タスクの基本設定の指定

タスクの全般設定を指定します：

1. ［**アプリケーション**］から［**Kaspersky Embedded Systems Security 4.0.0**］を選択します。
2. ［**タスク種別**］から［**Kaspersky Embedded Systems Security コンポーネントの変更**］を選択します。
3. ［**タスク名**］に「*アプリケーションコントロールコンポーネントの追加*」などの簡潔な名前を付けます。
4. ［**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。

### ステップ 2：タスクを割り当てるデバイスの選択

タスクを実行するコンピューターを選択します。たとえば、別の管理グループを選択するか、選択を作成します。

### ステップ 3：タスク作成の完了

1. ［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにしてウィザードを終了します。
2. タスクのプロパティで、［**アプリケーション設定**］セクションを選択します。
3. ユーザーのコンピューターで使用できる製品コンポーネントを選択します。タスクの詳細設定を指定します（下の表を参照ください）。

その結果、ユーザーのコンピューター上の Kaspersky Embedded Systems Security コンポーネントのセットはサイレントモードで変更されます。

タスクの詳細設定

| パラメータ | 説明 |
| --- | --- |
| **信頼ゾーン** | コンポーネントの変更タスクでは、信頼するオブジェクトと信頼するアプリケーションを信頼ゾーンに追加することのみが可能です。 |
| **製品コンポーネントの構成の変更に対してパスワードを使用する** | Kaspersky Embedded Systems Security へのアクセスを制限するために、管理者がパスワードによる保護を有効にしているケースが多くあります。つまり、製品コンポーネントの選択を変更するには、［**本製品の削除 / 変更 / 修復**］権限を持つユーザーの資格情報を入力する必要があります。例としては、KLAdmin アカウントを使用することができます。 |

# Active Directory のグループポリシーを使用した本製品のインストールとアンインストール

このセクションでは、Active Directory グループポリシーを使用してKaspersky Embedded Systems Security をインストールおよびアンインストールする方法と、グループポリシーを使用して Kaspersky Embedded Systems Security をインストールした後に実行する必要がある処理について説明します。

# Active Directory のグループポリシーを使用した Kaspersky Embedded Systems Security のインストール

Active Directory のグループポリシーを使用して複数の保護対象デバイスに Kaspersky Embedded Systems Security をインストールできます。同じ方法でアプリケーションコンソールもインストールできます。

Kaspersky Embedded Systems Security またはアプリケーションコンソールのインストール先となるすべての保護対象デバイスが、同じドメインおよび同じ組織単位内に存在している必要があります。

Active Directory のグループポリシーを使用して Kaspersky Embedded Systems Security をインストールするすべての保護対象デバイスのオペレーティングシステムが、同じビット数（32 ビットまたは 64 ビット）である必要があります。

ドメイン管理者権限で実行する必要があります。

Kaspersky Embedded Systems Security をインストールするには、インストールパッケージ ess_win.msi を使用します。アプリケーションコンソールをインストールするには、インストールパッケージ esstools.msi を使用します。

Active Directory のグループポリシーの使用についての詳細な情報は、Microsoft が提供するガイドを参照してください。

*Kaspersky Embedded Systems Security（またはアプリケーションコンソール）をインストールするには：*

1. ess_win.msi をドメインコントローラーの共有フォルダーに保存します。
2. ドメインコントローラー上の同じパブリックフォルダーにライセンス情報ファイルを保存します。

3. ドメインコントローラー上の同じ共有フォルダーに、以下の行を含むファイル install_props.json を作成します。これは、使用許諾契約書およびプライバシーポリシーの条項に同意したことを意味します。

```
{
"EULA": "1",
"PRIVACYPOLICY": "1"
}
```

4. ドメインコントローラーで、保護対象デバイスが所属するグループに対して新しいポリシーを作成します。

5. **グループポリシーオブジェクトのエディター**を使用して、［**コンピューターの構成**］フォルダーで新しいインストールパッケージを作成します。Kaspersky Embedded Systems Security（またはアプリケーションコンソール）の MSI ファイルのパスを UNC（ユニバーサルネーミング規約）形式で指定します。

6. Windows インストーラーで、選択したグループの［**コンピューターの構成**］フォルダーと［**ユーザーの構成**］フォルダーの両方で、［**常にシステム特権でインストールする**］を選択します。

7. `gpupdate / force` コマンドで変更を適用します。

グループの保護対象デバイスを再起動すると、Kaspersky Embedded Systems Security がインストールされます。

# Kaspersky Embedded Systems Security インストール後に実行する処理

保護対象デバイスへの Kaspersky Embedded Systems Security のインストールが完了したら、すぐに定義データベースをアップデートし、簡易スキャンを実行することを推奨します。これらの処理は、アプリケーションコンソールから実行できます。

Kaspersky Embedded Systems Security イベントに関する管理者への通知を設定することもできます。

# Active Directory のグループポリシーを使用した Kaspersky Embedded Systems Security のアンインストール

Kaspersky Embedded Systems Security をアンインストールしても、ダンプファイルとトレースファイルは削除されません。ダンプファイルとトレースファイルの書き込みの設定で指定したフォルダーから、ダンプファイルとトレースファイルを手動で削除できます。

Active Directory のグループポリシーを使用してグループ内の保護対象デバイスに Kaspersky Embedded Systems Security（またはアプリケーションコンソール）をインストールした場合、このポリシーを使用して Kaspersky Embedded Systems Security（またはアプリケーションコンソール）をアンインストールできます。

この方法で本製品をアンインストールする場合、使用できるのは既定のアンインストール設定だけです。

Active Directory のグループポリシーの使用についての詳細な情報は、Microsoft が提供するガイドを参照してください。

アプリケーション管理がパスワードによって保護されている場合、Active Directory グループポリシーを使用して Kaspersky Embedded Systems Security をアンインストールすることはできません。

*Kaspersky Embedded Systems Security（またはアプリケーションコンソール）をアンインストールするには：*

1. Kaspersky Embedded Systems Security またはアプリケーションコンソールをアンインストールする保護対象デバイスのドメインコントローラーで、組織単位を選択します。
2. Kaspersky Embedded Systems Security のインストール用に作成したポリシーを選択し、**グループポリシーオブジェクトエディター**の［**ソフトウェアインストール**］フォルダー（［**コンピューターの構成**］>［**ソフトウェアの設定**］>［**ソフトウェアインストール**］）で Kaspersky Embedded Systems Security（またはアプリケーションコンソール）のインストールパッケージのコンテキストメニューを開き、［**すべてのタスク**］>［**削除**］を選択します。
3. アンインストール方法として［**直ちに、ソフトウェアをユーザーとコンピューターからアンインストールする**］を選択します。
4. `gpupdate /force` コマンドで変更を適用します。

   保護対象デバイスを再起動すると、Microsoft Windows へのログイン前に Kaspersky Embedded Systems Security が保護対象デバイスから削除されます。

# Kaspersky Embedded Systems Security のインストールログとアンインストールログ

インストール（アンインストール）ウィザードを使用して Kaspersky Embedded Systems Security をインストール（アンインストール）した場合、Windows インストーラーサービスによってインストール（アンインストール）のログが作成されます。kl-install-<uid>.log（<uid> は 8 文字からなる一意のログ識別子）という名前のログファイルが、ファイル setup_ess.exe またはファイル setup_esstool.exe を起動したアカウントのユーザーのフォルダー %temp% に保存されます。

Kaspersky Embedded Systems Security がコマンドラインからインストールまたはアンインストールされた場合、既定ではインストールのログファイルは作成されません。

*Kaspersky Embedded Systems Security のインストールの際にドライブ C:\ にログファイルを作成するには、次のコマンドを実行します。*

```
msiexec /i ess_win.msi /l*v C:\<log_name>.log /qn EULA=1 PRIVACYPOLICY=1
```

# Kaspersky Embedded Systems Security インストール後のシステム変更

Kaspersky Embedded Systems Security と「管理ツール」のセット（アプリケーションコンソールを含む）が一緒にインストールされると、Windows インストーラーサービスにより、次の変更が保護対象デバイスに加えられます：

- 保護対象デバイスおよびアプリケーションコンソールがインストールされている保護対象デバイスに Kaspersky Embedded Systems Security のフォルダーが作成されます。
- Kaspersky Embedded Systems Security サービスが登録されます。
- Kaspersky Embedded Systems Security ユーザーグループが作成されます。
- Kaspersky Embedded Systems Security のキーがシステムレジストリに登録されます。
- Windows タスクスケジューラに表示される Kaspersky Embedded Systems Security OS アップグレード検出システムタスクが作成されます。

以下に、これらの変更点を示します。

## 保護対象デバイス上の Kaspersky Embedded Systems Security フォルダー

Kaspersky Embedded Systems Security がインストールされる場合、次のフォルダーが保護対象デバイスに作成されます：

- Kaspersky Embedded Systems Security の実行ファイルが配置される Kaspersky Embedded Systems Security の既定のインストールフォルダー。既定では、次のインストールフォルダーが使用されます：

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0

- SNMP プロトコルを使用して Kaspersky Embedded Systems Security により公開されるカウンターとフックの説明を含む、管理情報ベース（MIB）ファイル：

  %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0\mibs

- Kaspersky Embedded Systems Security サービスファイル：
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Data
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Settings
  - %ProgramData%\Kaspersky Lab\KESS.4.0\Dskm
- アップデート元の設定を含むファイル：

  %ProgramData%\Kaspersky Lab\KESS.4.0\Data

- アップデートタスクを使用してダウンロードされた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（フォルダーは、初めてアップデートタスクを使用してアップデートがダウンロードされた時に作成されます）。

  %ProgramData%\Kaspersky Lab\KESS.4.0\Update distribution

- 実行ログとシステム監査ログ：
  %ProgramData%\Kaspersky Lab\KESS.4.0\Reports
- 現在使用されている定義データベースのセット：
  %ProgramData%\Kaspersky Lab\KESS.4.0\Bases
- 定義データベースのバックアップコピー。定義データベースがアップデートされるたびに上書きされます：
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB
- アップデートタスクの実行時に作成される一時的なファイル：
  %ProgramData%\Kaspersky Lab\KESS.4.0\Data\temp\temporaryFolder
- 隔離されたオブジェクト（既定のフォルダー）：
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB
- バックアップされたオブジェクト（既定のフォルダー）：
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB
- バックアップおよび隔離から復元されたオブジェクト（復元されたオブジェクトの既定のフォルダー）：
  %ProgramData%\Kaspersky Lab\KESS.4.0\QB\Restored

## アプリケーションコンソールのインストール時に作成されるフォルダー

「管理ツール」を含むアプリケーションコンソールの既定のインストールフォルダーは、オペレーティングシステムのビットセットによって異なります。既定では、次のインストールフォルダーが使用されます：

%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools.4.0.0.

## Kaspersky Embedded Systems Security グループ

ESS Administrators は、保護対象デバイス上のグループで、グループのユーザーには、Kaspersky Security 管理サービスと Kaspersky Embedded Systems Security の全機能にアクセスできる権限があります。

## システムレジストリキー

Kaspersky Embedded Systems Security がインストールされる場合、次のシステムレジストリキーが作成されます：

- Kaspersky Embedded Systems Security の設定：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AVP.ESS.4.0]
- Kaspersky Embedded Systems Security イベントログ設定（Kaspersky Event Log）：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Embedded Systems Security]
- トレースファイルの設定：
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.0\Trace]

- アプリケーションのタスクと機能の設定:
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KESS.4.0\environment]

### Kaspersky Embedded Systems Security OS アップグレード検出システムタスク

Windows インストーラーサービスは、本製品のインストール中に Kaspersky Embedded Systems Security OS Upgrade Detectタスクを作成します。タスクは作成直後に開始され、その後は OS が起動するたびに開始されます。このタスクは、本製品が使用するドライバーのバージョンをチェックします。オペレーティングシステムのバージョンがアップデートされた場合、オペレーティングシステムの対応するバージョンのドライバーがアップデートされます。

タスクはアプリケーションに影響を与えないため、削除できます。オペレーティングシステムのアップグレードシナリオを念頭に置いておくことを推奨します。

# Kaspersky Embedded Systems Security プロセス

Kaspersky Embedded Systems Security が下表に記載されたプロセスを開始します。

Kaspersky Embedded Systems Security プロセス

| ファイル名 | 目的 |
| --- | --- |
| avp.exe | Kaspersky Embedded Systems Security ワークフロー |
| avpsus.exe | このプロセスにより、重要な承認された製品機能のアップデートをインストールおよびロールバックできます。 |

# Kaspersky Embedded Systems Security の機能のテスト：テスト用ウイルス EICAR の使用

このセクションでは、テスト用ウイルス EICAR について、またこのテスト用ウイルスを使用して Kaspersky Embedded Systems Security のファイルのリアルタイム保護機能およびオンデマンドスキャン機能をテストする方法について説明します。

## テスト用ウイルス EICAR について

EICAR はアンチウイルス製品の動作テストを目的としたテスト用ウイルスです。European Institute for Computer Antivirus Research（EICAR）により開発されました。

このテスト用ウイルスは本物のマルウェアではなく、お使いのデバイスに損害を与える可能性のある実行コードは含まれていません。ただし、ほとんどの製造元のアンチウイルス製品によって脅威として検知されるように作成されています。

このテスト用ウイルスを含むファイルは eicar.com と呼ばれます。EICAR の Web サイトからダウンロードできます。

デバイスのハードディスクにファイルを保存する前に、そのドライブのファイルのリアルタイム保護が無効になっていることを確認してください。

ファイル eicar.com には、1行のテキストが含まれています。このファイルをスキャンする際、Kaspersky Embedded Systems Security がこの文字列の中でテスト用の脅威を検知し、このファイルに対し「**感染**」のステータスを割り当て、ファイルを削除します。ファイルで検知された脅威に関する情報は、アプリケーションコンソールおよびタスク実行ログに表示されます。

ファイル eicar.com を使用して、Kaspersky Embedded Systems Security が感染したオブジェクトをどのようにして駆除するか、また Kaspersky Embedded Systems Security がどうやって感染の可能性があるオブジェクトを検知するかを確認できます。それには、テキストエディターを使用してファイルを開き、ファイル内のテキスト行の先頭に下の表にリストされた接頭辞の1つを追加して、新しい名前（たとえば eicar_cure.com）でファイルを保存します。

接頭辞を追加したファイル eicar.com が Kaspersky Embedded Systems Security によって問題なく処理されることを確認するには、［**オブジェクトの保護**］セキュリティ設定セクションで、Kaspersky Embedded Systems Security のコンピューターのリアルタイム保護タスクと既定のオンデマンドスキャンタスクに対して［**すべてのオブジェクト**］の値を設定します。

EICAR ファイルの接頭辞

| 接頭辞 | スキャンおよび Kaspersky Embedded Systems Security 処理後のファイルステータス |
|---|---|
| **接頭辞なし** | **Kaspersky Embedded Systems Security によって「感染」のステータスが割り当てられ、オブジェクトが削除されます。** |
| SUSP- | Kaspersky Embedded Systems Security によって「**感染の可能性あり**」のステータスがヒューリスティックアナライザーにより検知されたオブジェクトに割り当てられます。さらに、感染の可能性があるオブジェクトは駆除されないため、そのオブジェクトは削除されます。 |
| WARN- | Kaspersky Embedded Systems Security によって「**感染の可能性あり**」のステータスがオブジェクト（オブジェクトのコードが既知の脅威のコードと部分的に一致）に割り当てられます。さらに、感染の可能性があるオブジェクトは駆除されないため、そのオブジェクトは削除されます。 |
| CURE- | Kaspersky Embedded Systems Security によって「**感染**」のステータスが割り当てられ、オブジェクトが駆除されます。駆除に成功した場合、ファイル全体のテキストが「CURE」という単語に置き換わります。 |

# ファイルのリアルタイム保護機能とオンデマンドスキャン機能のテスト

Kaspersky Embedded Systems Security のインストール後、Kaspersky Embedded Systems Security による悪意あるコードが含まれるオブジェクト検知を確認できます。これを行うには、EICAR テストウイルスを使用します。

*ファイルのリアルタイム保護機能を確認するには：*

1. EICAR の Web サイトからファイル eicar.com をダウンロードします。ネットワークにある任意のデバイスのローカルドライブの共有フォルダーに保存します。

   パブリックフォルダーに保存する前に、このフォルダーのファイルのリアルタイム保護が無効になっていることを確認してください。

2. ネットワークユーザー通知の動作を確認する場合は、保護対象デバイスとファイル eicar.com を保存したデバイスの両方で、Microsoft Windows Messenger サービスが有効になっていることを確認してください。

3. 保護対象デバイスでアプリケーションコンソールを開きます。

4. 次のいずれかの方法を使用して、保存したファイル eicar.com を保護対象デバイスのローカルドライブにコピーします：

   - ターミナルサービスのウィンドウを通して通知のテストを行う場合、リモートデスクトップ接続ユーティリティを使用して保護対象デバイスに接続してから、ファイル eicar.com を保護対象デバイスにコピーします。

   - Microsoft Windows Messenger サービスを使用して通知をテストするには、ファイル eicar.comを保存したデバイスのネットワークの場所を使用してファイルをコピーします。

次に条件を満たすと、ファイルのリアルタイム保護が正常に機能していることになります：

- ファイル eicar.com が、保護対象デバイスから削除されている。

- アプリケーションコンソールで、実行ログが「緊急」のステータスになります。ログには、ファイル eicar.com 内の脅威に関する情報を含む新しい行があります。

- 次の Microsoft Windows Messenger Service メッセージが、ファイルのコピー元のデバイスに表示されます：Kaspersky Embedded Systems Security によって、コンピューター <デバイスのネットワーク名> の <デバイス上のファイルへのパス>\eicar.com へのアクセスが <イベント発生時> にブロックされました。理由：脅威の検知。検知した脅威：EICAR-Test-File。ユーザー名：<ユーザー名>。コンピューター名：<ファイルのコピー元であるデバイスのネットワーク名>。

  ファイル eicar.com のコピー元であるデバイスで、Microsoft Windows Messenger サービスが実行されていることを確認してください。

*オンデマンドスキャン機能を確認するには：*

1. EICAR の Web サイトからファイル eicar.com をダウンロードします。ネットワークにある任意のデバイスのローカルドライブの共有フォルダーに保存します。

   パブリックフォルダーに保存する前に、このフォルダーのファイルのリアルタイム保護が無効になっていることを確認してください。

2. アプリケーションコンソールを開き、アプリケーションコンソールツリーで［**オンデマンドスキャン**］フォルダーを展開します。

3. ［**簡易スキャン**］サブフォルダーを選択します。

4. ［**すべてのネットワークドライブ**］をオンデマンドスキャンタスクの範囲に追加します。

5. 簡易スキャンタスクを実行します。

次の条件を満たすと、オンデマンドスキャンが正常に機能していることになります：

- ファイル eicar.com が、デバイスのハードディスクから削除されている。
- アプリケーションコンソールで、実行ログが「緊急」のステータスになります。オンデマンドスキャンタスクの実行ログには、ファイル eicar.com 内の脅威に関する情報を含む新しい行があります。

# 旧バージョンの Kaspersky Embedded Systems Security のバージョン 4.0 へのアップグレード

旧バージョンの Kaspersky Embedded Systems Security をバージョン 4.0 にアップグレードする場合は、次の推奨事項に従ってください：

- 事前に計画を立ててアップグレードをスケジュールします。週末など、サーバーの動作中の負荷が一番低い時刻を選択してください。
- アップグレード後に、アプリケーションコンポーネントを1つずつオンにします。例えば、ファイルのリアルタイム保護を単独で有効にしてから、その他の保護機能をオンにして、その他のコントロールコ機能をオンにするなどの方法をとります。各ステップで本製品をテストすることを推奨します。
- アップグレードを段階的に実行します。まず1台のコンピューターをアップグレードし、次に複数のコンピューターをアップグレードし、その後で組織内のすべてのコンピューターをアップグレードします。

## アップグレード手順のステップ

次の順序で Kaspersky Embedded Systems Security をバージョン 4.0 にアップグレードします：

1. **Kaspersky Security Center をアップグレードする**

   ユーザーのコンピューター上にあるネットワークエージェントと Kaspersky Security Center Web コンソールを含むすべての Kaspersky Security Center コンポーネントをバージョン 14.2 以降にアップグレードします。

2. **Kaspersky Embedded Systems Security Web プラグインをアップグレードする**

   Kaspersky Security Center Web コンソールで、Kaspersky Embedded Systems Security Web プラグインをバージョン 4.0 にアップグレードします。

3. **Kaspersky Embedded Systems Security のタスクとポリシーを移行する**

   ポリシーとタスクを移行したら、移行ウィザードで移行できない設定、および本製品の以前のバージョンに存在しなかった設定を指定する必要があります。移行ウィザードによってすべての設定が正しく移行されたかどうかを確認することも推奨します。

4. **Kaspersky Embedded Systems Security 4.0 をインストールする**

   Kaspersky Embedded Systems Security のバージョン 4.0 は、DCOM プロトコルの代わりに HTTPS プロトコルを使用します。そのため、Kaspersky Embedded Systems Security の新しいバージョンをインストールする前に、アプリケーションが更新されるデバイス上で、KESSサービスのリモート起動を有効にするようデバイスを設定する必要があります。この設定を行わない場合、リモートサービスの起動は利用できません。

   Kaspersky Embedded Systems Security 4.0 は、旧バージョンの製品を削除した後でインストールすることも、旧バージョンの製品に上書きインストールすることもできます。

   旧バージョンの製品に上書きインストールすると、一部のコンポーネントの新しい名前と内容を考慮して、同じ一連の製品コンポーネントがインストールされます。

リモートでインストールする場合、インストーラーによって、インストールパッケージのプロパティで選択したコンポーネントがインストールされます。

5. **必要に応じて、Kaspersky Embedded Systems Security 4.0 をアクティベートする**

   Kaspersky Embedded Systems Security 4.0 を旧バージョンの製品に上書きインストールすると、現在のライセンスが自動的に製品に適用されて、新しいアプリケーションコンポーネントとタスクが完全に使用可能になります。ライセンス期間は変更されません。

6. **製品が動作していることを確認する**

   Kaspersky Embedded Systems Security をアップグレードしたら、製品が想定通りに動作していることを確認してください。製品でエラーがレポートされていないことを確認し、管理サーバーに最後に接続された時刻、最終アップデートの時刻およびコンピューター保護のステータスも確認してください。

除外リスト、信頼するアプリケーション、デバイスコントロールルール、アプリケーション起動コントロールルールの移行に注意してください。

# Kaspersky Embedded Systems Security のアップデート

Kaspersky Embedded Systems Security バージョン 4.0 へのアップグレードは、本製品のバージョン 2.3、3.1 以降でサポートされています。本製品のそれ以前のバージョンからアップデートするには、インストールされているバージョンを削除し、バージョン 4.0 をインストールします。

アップデートは、インストールされている本製品のバージョンに新しいバージョンを上書きインストールすることで実行されます。コンピューターを再起動する必要はありません。

既定では、既存の本製品のインストールフォルダーへのパスに基づいて、新しい製品バージョンの名前でインストールフォルダーが新規作成されます。新しいインストールフォルダーのパスは、手動で指定できます。

Kaspersky Embedded Systems Security をバージョン 4.0 にアップグレードすると、以前にインストールされていた本製品のバージョンが自動的に削除されます。

Kaspersky Embedded Systems Security のパスワード保護されたインストールをアップデートする場合は、次のいずれかの方法でインストーラーにパスワードを渡します。

- インストールウィザードのインターフェイスまたは対話型 CLI モードでローカルにインストールする場合は、要求された時にパスワードを指定します。
- 非対話型 CLI モードでローカルにインストールする場合は、`UNLOCK_PASSWORD` キーにパスワードを指定します。
- Active Directory グループポリシーを使用してインストールする場合は、設定情報ファイル install_props.json で `UNLOCK_PASSWORD` キーの値を使用します。

パスワードで保護されている本製品を Kaspersky Security Center を介してリモートからアップグレードする場合は、まず Kaspersky Security Center ポリシーを使用してパスワードによる保護を無効にする必要があります。

本製品をアップデートすると、現在のライセンスが Kaspersky Embedded Systems Security バージョン 4.0 に自動的に適用され、新しい本製品のコンポーネントとタスクを完全に使用できるようになります。ライセンス期間は変更されません。

有効期限が切れたライセンスで本製品をアップデートした場合、新しいバージョンはインストール後に機能制限モードで実行されます（たとえば、定義データベースがアップデートできません）。

# Kaspersky Embedded Systems Security の管理ツールのアップデート

Kaspersky Security Center を使用して本製品を管理するための管理プラグインを、バージョン 2.3、3.1、3.2、3.3、3.4、またはそれ以降からバージョン 4.0 にアップデートできます。それ以前のバージョンの管理プラグインおよびアプリケーションコンソールをアップデートするには、インストールされているバージョンを削除してからバージョン 4.0 をインストールする必要があります。

アップデート中に、新しいバージョンの管理プラグインが以前にインストールされたバージョンに上書きインストールされます。コンピューターの再起動は不要です。

管理プラグインの設定の移行について詳しくは、この記事を参照してください。

# ポリシーおよびタスクの移行

次の方法で、本製品の以前のバージョンのポリシーとタスクの設定をバージョン 4.0 に移行できます：

- ポリシーとタスクの一括変換ウィザード（Kaspersky Security Center 管理コンソールでのみ使用可能）を使用する。
- Kaspersky Embedded Systems Security 4.0 のポリシーとタスクの移行ウィザード（Kaspersky Security Center Web コンソールでのみ使用可能）を使用する。

最初に単一のコンピューターで Kaspersky Embedded Systems Security のポリシーとタスクを移行し、次にコンピューターのグループで移行してから組織のすべてのコンピューターでの移行を完了させてください。

**ポリシーとタスクの一括変換ウィザードを使用してポリシーとタスクの設定を移行する方法**

1. Kaspersky Security Center 管理コンソールで、管理サーバーを選択して右クリックしてコンテキストメニューを開きます。
2. ［**すべてのタスク**］→［**ポリシーとタスクの一括変換ウィザード**］の順に選択します。

これにより、ポリシーとタスクの一括変換ウィザードが起動します。ウィザードの指示に従います。

## ステップ 1：ポリシーとタスクを変換するアプリケーションの選択

Kaspersky Embedded Systems Security 4.0 を選択します。次の手順に進みます。

### ステップ 2：ポリシーの変換

アップグレードされる製品バージョンで、Kaspersky Embedded Systems Security 4.0 向けに作成するポリシーを選択します。次の手順に進みます。

### ステップ 3：タスクの変換

アップグレードされる製品バージョンで、Kaspersky Embedded Systems Security 4.0 向けに作成するタスクを選択します。

グループ以外のタスク（個別のデバイスに割り当てられているタスク）は現在のステップでは表示されません。

*お使いの本製品のバージョンのグループ以外のタスクを Kaspersky Embedded Systems Security 4.0 に変換するには：*

1. ［**次へ**］をクリックします。
   ［**追加のスケジュールとタスクの移行**］ウィンドウが表示されます。
2. ［**グループ以外のタスクのスケジュールを移行する**］チェックボックスをオンにします。
3. Kaspersky Security Center Administration Server への接続設定を指定します。
4. ［**OK**］をクリックします。

### ステップ 4：ウィザードの完了

ウィザードの操作を完了します。ウィザードは以下の処理を実行します：

- Kaspersky Embedded Systems Security 4.0 向けの新しいポリシーが作成されます。
  新しいポリシーには、選択した Kaspersky Embedded Systems Security のポリシーの設定と、Kaspersky Embedded Systems Security 4.0 で導入された新しい設定が含まれます。新しいポリシーの名前は、変換前の Kaspersky Embedded Systems Security のポリシーの名前と同じですが、「(変換済み)」が追加されます。新しいポリシーのステータスは*非アクティブポリシー*になっています。
- Kaspersky Embedded Systems Security 4.0 向けの新しいタスクが作成されます。
  新しいタスクには、選択した Kaspersky Embedded Systems Security のタスクの設定と、Kaspersky Embedded Systems Security 4.0 で導入された新しい設定が含まれます。新しいタスクの名前は、変換前の Kaspersky Embedded Systems Security のタスクの名前と同じですが、「(変換)」が追加されます。
- 変換対象として選択されたポリシーとタスクは変更されません。

**移行ウィザードを使用してポリシーとタスクの設定を移行する方法**

Web コンソールのメインウィンドウで、［**操作**］→［**KESS 4.0.0 への移行**］の順に選択します。

ポリシーとタスクの移行ウィザードが開始されます。ウィザードの指示に従います。

### ステップ 1：ポリシーの移行

Kaspersky Embedded Systems Security 4.0 向けに作成する Kaspersky Embedded Systems Security のポリシーを選択します。次の手順に進みます。

### ステップ 2：タスクの移行

タスクのリストで、 Kaspersky Embedded Systems Security 4.0 向けに作成する Kaspersky Embedded Systems Security のタスクを選択します。次の手順に進みます。

### ステップ 3：ウィザードの完了

ウィザードの操作を完了します。ウィザードは以下の処理を実行します：

- Kaspersky Embedded Systems Security 4.0 向けの新しいポリシーが作成されます。

  新しいポリシーには、移行した Kaspersky Embedded Systems Security のポリシーの設定と、Kaspersky Embedded Systems Security 4.0 で導入された新しい設定が含まれます。新しいポリシーの名前は、統合前の Kaspersky Embedded Systems Security のポリシーの名前と同じですが、「KESS からコピー済み」という語句が追加されます。新しいポリシーのステータスは*非アクティブポリシー*になっています。

- Kaspersky Embedded Systems Security 4.0 向けの新しいタスクが作成されます。

  新しいタスクには、移行した Kaspersky Embedded Systems Security のタスクの設定と、Kaspersky Embedded Systems Security 4.0 で導入された新しい設定が含まれます。新しいタスクの名前は、統合前の Kaspersky Embedded Systems Security のタスクの名前と同じですが、「KESS からコピー済み」という語句が追加されます。

# アップデート中の製品バージョンの設定の移行

次は、本製品とその管理プラグインをバージョン 4.0 にアップグレードしても変更されずに移行されます：

- 既定値にリセットされるものと「設定とコンポーネントの移行の制限」に記載されているものを除く、コンポーネントとタスクの設定
- 実行ログとシステム監査ログ、および Windows イベントログの項目
- タスクの通知設定
- タスクが開始されるユーザーアカウント
- アプリケーション管理用のユーザーアクセス権限
- プロキシサーバーの接続用パスワード
- 属性の状態

次の設定は、本製品とそのプラグインをバージョン 4.0 にアップグレードした後でリセットされるか、本製品の新しいバージョンの既定値に設定されます：

- 定義データベースのステータスを含むすべてのカウンター
- ソフトウェアモジュールおよび定義データベースのインストール済みアップデートに関するデータ
- タスクのステータス
- Kaspersky Security サービスを管理するための権限
- レジストリを使用して設定された製品とコンポーネントの設定
- 重要な修正プログラムのインストール中に変更されたアプリケーションとタスクの設定
- イベントの設定
- Kaspersky Security Center 管理サーバーへのデータ転送の設定（既定では、すべてのデータの転送が有効になります）
- トレースとダンプの設定
- ［**通知**］タブにある、製品のローカルタスクの設定

アップデートする本製品のバージョンに存在しなかった設定には既定値が適用されます。

## 設定とコンポーネントの移行の制限

- アップグレードされるバージョンの隔離の内容は、バージョン 4.0 のバックアップに移動されます。同時に、バックアップの最大サイズは 400 MB に増加され、空き容量のしきい値は 100 MB に増加されます。
- Kaspersky Embedded Systems Security 3.4 の［**隔離フォルダー**］、［**バックアップフォルダー**］、［**オブジェクトの復元用フォルダー**］の設定は、Kaspersky Embedded Systems Security 4.0 以降には存在しないため、移行されません。古いバージョンに存在し、新しいバージョンには存在しないその他の設定も、同様に移行されません。
- クライアントコンピューターのブロックされたネットワークセッションのリストは移行されません。同時に、ブロックされたネットワークファイルリソースへのアクセスのブロックを自動的に解除するための設定は、本製品のアップグレード後も変更されません。
- パスワードによる保護の設定は移行されません。Kaspersky Embedded Systems Security 4.0 では、パスワードによる保護が大幅に変更されました。必要に応じて、パスワードによる保護をオンにしてパスワードを設定してください。
- 信頼ゾーン：
  - Kaspersky Embedded Systems Security 4.0 では、信頼ゾーンオブジェクトの選択方法が変更されました。個々のファイルや、ファイルまたはフォルダーのパスとして定義された除外リストを移行できます。定義済みの範囲（ハードディスクなど）またはスクリプト URL として定義された除外リストは移行されません。移行後にこれらの除外リストを手動で追加する必要があります。
  - サーバー上での本製品の設定に役立つ、設定済みの信頼するオブジェクトとアプリケーションが、信頼ゾーンに追加されました。

- アプリケーションコントロールとデバイスコントロールのコンポーネントが大幅に改良されました。アップグレードされるバージョンのコンポーネントの設定は、Kaspersky Embedded Systems Security 4.0 の新しい設定の構造を考慮して移行されます。

- アップグレードされる製品バージョンのファイル変更監視およびレジストリアクセス管理のコンポーネントの設定は、システム変更監視コンポーネントの設定に移行されます。

- ファイアウォール管理コンポーネントは、ファイアウォールコンポーネントに変更され、Windows ファイアウォールとの連携に加え、ファイアウォールとしての機能も追加されました。移行が完了したら、最初からコンポーネントのモードを設定する必要があります。

- KSN を使用するには、KSN 声明を再度確認して同意する必要があります。

- 本製品のバージョン 4.0 以降では、個々のコンポーネントのスケジュール設定はサポートされません。コンポーネントが有効になっている場合、本製品の実行中はコンポーネントも実行され続けます。

- タスクを移行する場合、タスクのスケジュールされた開始時刻は、移行が実行されるコンピューターの OS で設定されているタイムゾーンの数値と一致する時間数だけオフセットされます。たとえば、本製品の以前のバージョンでのタスクの開始時刻が 7:00 で、オペレーティングシステムに設定されているタイムゾーンが UTC +3:00 であるとします。その場合、タスクが移行されると、開始時刻は 10:00 に変更されます。

- 感染の可能性があるオブジェクトの処理を設定するセクションが、ファイルのリアルタイム保護コンポーネントとオンデマンドスキャンタスクの設定から削除されました。これらの設定は新しい製品バージョンには移行されません。

- 本製品の 3.4 以前のバージョンを 4.0 以降のバージョンにアップグレードした後でバックアップオブジェクトを移行した場合、Kaspersky Security Center Web コンソールまたは管理コンソールを使用して、分析のためにカスペルスキーにこれらのオブジェクトを送信することはできません。

- オンデマンドスキャンタスクを移行する場合、定義済みのスキャン範囲の既定のセキュリティレベルは、*通知*から*カスタム*に変わります。

# Kaspersky Embedded Systems Security バージョン 3.4 および 4.0 のコンポーネントとタスクの対応

Kaspersky Embedded Systems Security 3.4 をバージョン 4.0 にアップグレードする場合、製品がローカルにインストールされている場合にのみ、コンポーネントとタスクのセットが移行されます。

Kaspersky Embedded Systems Security バージョン 3.4 および 4.0 のコンポーネントの対応

| Kaspersky Embedded Systems Security 3.4 のコンポーネント | Kaspersky Embedded Systems Security 4.0 のコンポーネント |
|---|---|
| 信頼ゾーン | 信頼ゾーン |
| ファイルのリアルタイム保護 | ファイルのリアルタイム保護 |
| KSN の使用 | KSN の使用 |
| 脆弱性攻撃ブロック | 脆弱性攻撃ブロック |
| AMSI スキャナー | AMSI 保護 |
| アプリケーション起動コントロール | アプリケーション起動コントロール |
| デバイスコントロール | デバイスコントロール |

| Kaspersky Embedded Systems Security 3.4 のコンポーネント | Kaspersky Embedded Systems Security 4.0 のコンポーネント |
| --- | --- |
| ファイアウォール管理 | ファイアウォール<br>Windows ファイアウォールが Kaspersky Embedded Systems Security 3.4 のファイアウォールとして機能し、本製品によって Windows ファイアウォールが管理されます。Kaspersky Embedded Systems Security 4.0 では、ファイアウォール機能は個別のコンポーネントが実行されています。 |
| ネットワーク脅威対策 | ネットワーク脅威対策 |
| ファイル変更監視 | システム変更監視<br>ファイル変更監視とレジストリアクセス監視のコンポーネントの機能は、システム変更監視コンポーネントに統合されました。 |
| Windows イベントログ監視 | Windows イベントログ監視 |
| レジストリアクセス監視 | システム変更監視<br>ファイル変更監視とレジストリアクセス監視のコンポーネントの機能は、システム変更監視コンポーネントに統合されました。 |
| *（なし）* | ふるまい検知 |
| *（なし）* | 修復エンジン |
| **Kaspersky Embedded Systems Security 3.4 のタスク** | **Kaspersky Embedded Systems Security 4.0 のタスク** |
| 製品のアクティベーション | 製品のアクティベーション |
| アップデートのコピー | アップデート<br>アップデートのコピータスクの機能は、アップデートタスクに統合されました。 |
| ベースラインファイル変更監視 | ベースラインシステム変更監視 |
| 定義データベースのアップデート | アップデート<br>定義データベースのアップデートタスクの機能は、アップデートタスクに統合されました。 |
| ソフトウェアモジュールのアップデート | アップデート<br>ソフトウェアモジュールのアップデートタスクの機能は、アップデートタスクに統合されました。 |
| 定義データベースのロールバック | アップデートのロールバック |
| オンデマンドスキャン | オンデマンドスキャン |
| アプリケーションの整合性チェック | アプリケーション整合性コントロール |
| アプリケーション起動コントロールルールの自動生成 | アプリケーション起動コントロールルールの自動生成 |
| デバイスコントロールルールの自動生成 | デバイスコントロールルールの自動生成 |
| *（なし）* | 管理サーバーの接続の保護 |
| *（なし）* | Kaspersky Embedded Systems Security コンポーネントの変更 |
| *（なし）* | システム変更ステータスのリセット |

# 製品のインターフェイス

Kaspersky Embedded Systems Security は、以下のインターフェイスを使用してコントロールできます：

- アプリケーションコンソール
- Kaspersky Security Center 管理コンソール
- Kaspersky Security Center Web コンソール

## Kaspersky Security Center 管理コンソール

Kaspersky Security Center を使用すると、Kaspersky Embedded Systems Security に対する次の操作をリモートで行うことができます：インストールとアンインストール、起動と停止、アプリケーションの設定、使用可能なアプリケーションコンポーネントのセットの変更、ライセンスの追加、タスクの開始と停止。

本製品は、Kaspersky Embedded Systems Security 管理プラグインを使用して Kaspersky Security Center 経由で管理できます。Kaspersky Security Center 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。

## Kaspersky Security Center Web コンソール

*Kaspersky Security Center Web コンソール*（以降「Web コンソール」とも表記）は、組織のネットワークのセキュリティシステムを管理および維持するための主要なタスクを一元的に実行することを目的とした Web アプリケーションです。Kaspersky Security Center Web コンソールは、ユーザーインターフェイスを提供する Kaspersky Security Center コンポーネントです。Kaspersky Security Center Web コンソールについて詳しくは、*Kaspersky Security Center* ヘルプを参照してください。

Web コンソールでは次の処理を使用できます：

- 組織のセキュリティシステムのステータスの監視
- ネットワーク内のデバイスへのカスペルスキー製品のインストール
- インストール済み製品の管理
- セキュリティシステムのステータスに関するレポートの表示

# 管理プラグインの使用

このセクションでは、Kaspersky Embedded Systems Security 管理プラグインについての情報を提供するとともに、保護対象デバイスまたは保護対象デバイスのグループにインストールされているアプリケーションコンソールを管理する方法について説明します。

# Kaspersky Security Center を使用した Kaspersky Embedded Systems Security の管理

Kaspersky Embedded Systems Security がインストールされ、管理グループに追加された複数の保護対象デバイスを、Kaspersky Embedded Systems Security 管理プラグインを使用して一元管理できます。Kaspersky Security Center では、管理グループに含まれる各保護対象デバイスの設定を個別に指定することもできます。

*管理グループ*は、Kaspersky Security Center で手動で作成されます。グループには、Kaspersky Embedded Systems Security がインストールされている複数のデバイスが含まれます。それらのデバイスに対して、同一の管理や保護を設定できます。管理グループの使用の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

保護対象デバイスにインストールされている Kaspersky Embedded Systems Security の動作が Kaspersky Security Center のアクティブポリシーによって制御されている場合、単一の保護対象デバイスに対するアプリケーション設定は編集できません。

Kaspersky Security Center で Kaspersky Embedded Systems Security 管理プラグインを起動するには、追加の操作は必要ありません。管理者の保護対象デバイスにインストールされた管理プラグインは、すべての種別の Kaspersky Security Center 管理コンソールと同時に開始されます。

Kaspersky Security Center から Kaspersky Embedded Systems Security を管理するには、次の方法を実行します：

- **Kaspersky Security Center のポリシーを使用する**：Kaspersky Security Center のポリシーでは、デバイスグループに対して同一の保護をリモートで設定できます。アクティブポリシーで指定されるタスク設定は、アプリケーションコンソールでローカルで指定されるタスク設定や Kaspersky Security Center の保護対象デバイスのプロパティウィンドウでリモートで指定されるタスク設定よりも優先度が高いです。

  ポリシーを使用して、全般的なアプリケーション設定、コンピューターのリアルタイム保護タスクの設定、デバイス上の活動を管理するタスク、ネットワークストレージの保護タスクおよびスケジュールに従ってローカルシステムタスクを開始するための設定を指定できます。

- **Kaspersky Security Center のグループタスクを使用する**：Kaspersky Security Center のグループタスクでは、デバイスグループに対して、有効期限があるタスクの共通設定をリモートで編集できるようになります。

  グループタスクを使用して、製品をアクティベートしたり、オンデマンドスキャンタスクの設定、アップデートタスクの設定、アプリケーション起動コントロールルールの自動生成タスクの設定を編集したりできます。

- **特定のデバイスのタスクを使用する**：特定のデバイスのタスクを使用すると、どの管理グループにも属していない保護対象デバイスに対して、共通のタスク設定（実行可能な期間に制限あり）をリモートで編集できます。

- **単一のデバイスのプロパティウィンドウを使用する**：**保護対象デバイスのプロパティ**ウィンドウで、管理グループに含まれる個別の保護対象デバイスに対して、タスクをリモートで設定できます。選択した保護対象デバイスが、Kaspersky Security Center のアクティブポリシーによって制御されていない場合、アプリケーションの全般的な設定とすべての Kaspersky Embedded Systems Security タスクの設定の両方を編集できます。

# アプリケーション設定の管理

このセクションでは、Kaspersky Security Center 管理コンソールを使用した Kaspersky Embedded Systems Security の全般的な設定について説明します。

## 操作方法

必要なタスクの設定を選択したインターフェイスから操作する方法について説明します。

### アプリケーションのプロパティウィンドウでの全般的な製品設定の表示と編集

*単一の保護対象デバイスで Kaspersky Embedded Systems Security のプロパティウィンドウを開くには：*

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**デバイス**］タブを選択します。
4. 次のいずれかの方法で、**プロパティ：<保護対象デバイス名>**ウィンドウを開きます：
   - 保護対象デバイスの名前をダブルクリックする。
   - 保護対象デバイス名のコンテキストメニューを開き、［**プロパティ**］を選択する。

   保護対象デバイスのプロパティウィンドウが表示されます。
5. ［**アプリケーション**］セクションで、**Kaspersky Embedded Systems Security** を選択します。
6. ［**プロパティ**］をクリックします。
   **Kaspersky Embedded Systems Security** の［**設定**］ウィンドウが開きます。
7. ［**アプリケーション設定**］に移動します。
8. 設定のサブセクションで、［**設定**］をクリックします。

## ポリシーでの全般的な製品設定の表示と編集

*ポリシーから Kaspersky Embedded Systems Security のアプリケーションの設定を開くには：*

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**ポリシー**］タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. 表示される**プロパティ：<ポリシー名>**ウィンドウで、［**アプリケーション設定**］へ移動します。
6. 設定のサブセクションで、［**設定**］をクリックします。

# Kaspersky Security Center での全般的なアプリケーション設定

Kaspersky Security Center から、保護対象デバイスグループまたは 1 台の保護対象デバイスに対して Kaspersky Embedded Systems Security の全般的な設定を行えます。

## Kaspersky Security Center でのインターフェイスおよびスキャンの設定

*スケーラビリティ設定およびアプリケーションインターフェイスを設定するには：*

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。
2. アプリケーション設定を編集する管理グループを選択します。
3. 選択した管理グループの詳細ペインで、次のいずれかを実行します：
   - 保護対象デバイスグループに対してアプリケーションを設定するには、［**ポリシー**］タブを選択して、設定する**プロパティ：<ポリシー名>**ウィンドウを開きます。
   - 個々の保護対象デバイスのタスクまたは本製品の設定を指定するには、［**デバイス**］タブを選択し、ローカルタスク設定またはアプリケーション設定に移動します。
4. ［**アプリケーション設定**］セクションで、［**インターフェイスの設定**］サブセクションの［**設定**］をクリックします。

5. ［**インターフェイスの設定**］ウィンドウの［**全般**］タブで、次の設定を行います：

   - ［**ユーザーインターフェイス**］セクションで、各アプリケーション起動後のタスクバーにシステムトレイアイコンが表示されるかどうかを設定します。

     - **ユーザーインターフェイスを表示する**：クライアントコンピューターでは、Windows トレイにアイコンが表示されます。アイコンのコンテキストメニューから Kaspersky Embedded Systems Security の操作を実行できます。製品アイコンの上の通知も表示されます。Windows システムトレイのアイコンのコンテキストメニューを使用すると、コンパクト診断インターフェイスを開くことができます。コンパクト診断インターフェイスのリンクをクリックすると、アプリケーションコンソールが開きます。

     - **ユーザーインターフェイスを表示しない**：クライアントコンピューター上で、Kaspersky Embedded Systems Security の動作に関するメニューなどが表示されません。Windows の通知領域のアイコンと通知も表示されません。

   - ［**状態**］セクションでは、Kaspersky Embedded Systems Security システムトレイアイコンに表示する警告を指定できます。

6. ［**OK**］をクリックします。

アプリケーションの設定内容が保存されます。

## Kaspersky Security Center でのセキュリティ設定

*手動でセキュリティを設定するには：*

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。

2. アプリケーション設定を編集する管理グループを選択します。

3. 選択した管理グループの詳細ペインで、次のいずれかを実行します：

   - 保護対象デバイスグループに対してアプリケーションを設定するには、［**ポリシー**］タブを選択して、設定する**プロパティ：<ポリシー名>**ウィンドウを開きます。

   - 個々の保護対象デバイスのタスクまたは本製品の設定を指定するには、［**デバイス**］タブを選択し、ローカルタスク設定またはアプリケーション設定に移動します。

4. ［**アプリケーション設定**］セクションで、［**セキュリティと信頼性**］サブセクションの［**設定**］をクリックします。

5. ［**セキュリティ設定**］ウィンドウの［**セキュリティ**］タブで、次の設定を行います：

   - ［**全般**］セクションでは、［**コンピューターの開始時に本製品を開始する（推奨）**］を有効（既定）のままにしておくことを推奨します。

   - ［**セルフディフェンス**］セクションで、［**アプリケーションプロセスを外部の脅威から保護する**］機能を有効または無効にします。

   - ［**UPS 電源への切り替え時の処理**］セクションで、UPS 電源への切り替え後における、Kaspersky Embedded Systems Security による保護対象デバイスの負荷に対する制限を指定できます：

     - **スケジュール設定済みのスキャンタスクを開始しない**

- スキャンタスクの実行を中止する

- ［**設定が適用された際のコンピューターの状態**］セクションで、ポリシーの適用時またはタスクの実行時にエラーが発生した場合における、本製品がインストールされているクライアントコンピューターの状態の表示を設定します。

- ［**互換性設定**］セクションで、［**リモート管理ソフトウェアとの互換性**］を設定します：

  Kaspersky Embedded Systems Security をリモート管理ツール（RAT）と一緒に使用すると問題が発生する場合は、互換性モードを有効にすることができます。この問題は、RAT と製品のセキュアデスクトップ機能に互換性がないことに関連して生じる可能性があります。この機能の目的は、コンピューターのセキュリティレベルを低下させる可能性のある処理を確認することです。この機能により、アプリケーションで他のプロセスから分離された確認ダイアログを表示することができます。この機能では昇格した権限を使用してリクエストの安全を確保します。こうすることで、マルウェアではなくユーザーだけが処理を確認できるようになります。

  このチェックボックスをオンにすると、RAT 互換性モードが有効になります。この機能を使用しない場合、アプリケーションは確認ダイアログを表示します。これは、コンピューターのセキュリティレベルを低下させる可能性があります。Kaspersky Embedded Systems Security と RAT で問題が発生していない場合、互換性モードを有効にすることは推奨しません。

  このチェックボックスをオフにすると、RAT 互換性モードは無効になります。既定では、このチェックボックスはオフです。

  例：ブラウザーを RemoteApp モードで使用している場合、信頼されていない証明書を使用する Web サイトにアクセスしたときに確認ウィンドウが表示されないことがあります。これは、RemoteApp が本製品のセキュアデスクトップ機能をサポートしていないためです。これにより、ブラウザーが応答しなくなることがあります。RemoteApp モードでブラウザーを正しく動作させるには、互換性モードを有効にする必要があります。

  他のサードパーティ製ソフトウェアを使用しているときにセキュアデスクトップ機能に問題が発生した場合にも、互換性モードを有効にしてみることができます。

6. ［**スキャンの設定**］タブで、次の設定を行います：

   - **スキャンタスクの CPU 使用率を制限する**：オンデマンドスキャンタスクでの保護対象デバイスの CPU の使用が、［**上限**］フィールドで指定した値に制限されます。このオプションを有効にすることで、Kaspersky Embedded Systems Security のパフォーマンスに悪影響を与える可能性があります。

   - 他のアプリケーションにシステムリソースを優先的に割り当てるKaspersky Embedded Systems Security がコンピューターをスキャンする際にコンピューターのリソースを消費するため、CPU やハードディスクサブシステムの負荷が増加する可能性があります。これにより、他のアプリケーションの動作が遅くなることがあります。パフォーマンスを最適化するために、Kaspersky Embedded Systems Security には、他のアプリケーションにリソースを振り分けるモードが用意されています。このモードでは、CPU の負荷が高い場合に、オペレーティングシステムが Kaspersky Embedded Systems Security のスキャンタスクスレッドの優先度を下げることができます。これにより、オペレーティングシステムのリソースを他のアプリケーションに再分配することが可能になり、スキャンタスクの CPU 時間が減ります。その結果、Kaspersky Embedded Systems Security のスキャンに時間がかかるようになります。既定では、製品は他のアプリケーションにリソースを割り当てるように設定されています。

7. ［**OK**］をクリックします。

スケーラビリティと信頼性の設定内容が保存されます。

# Kaspersky Security Center を使用した接続の設定

接続設定は、Kaspersky Embedded Systems Security がアップデートサーバーおよびアクティベーションサーバーに接続するのに使用します。また、アプリケーションを KSN サービスと連携する際にも使用します。

*接続設定を行うには、次の手順を実行します：*

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。
2. アプリケーション設定を編集する管理グループを選択します。
3. 選択した管理グループの詳細ペインで、次のいずれかを実行します：
   - 保護対象デバイスグループに対してアプリケーションを設定するには、［**ポリシー**］タブを選択して、設定する**プロパティ：<ポリシー名>**ウィンドウを開きます。
   - 個々の保護対象デバイスのタスクまたは本製品の設定を指定するには、［**デバイス**］タブを選択し、ローカルタスク設定またはアプリケーション設定に移動します。
4. ［**アプリケーション設定**］セクションで、［**接続設定**］サブセクションの［**設定**］をクリックします。
   ［**接続設定**］ウィンドウが表示されます。
5. ［**接続設定**］ウィンドウで、次の設定を行います：
   - ［**プロキシサーバー**］セクションで、［**設定**］をクリックして、プロキシサーバー設定を指定します：
     - **プロキシサーバーを使用しない**
     - **プロキシサーバー設定を自動的に検出する**
     - **指定したプロキシサーバーを使用する**
     - **プロキシサーバーの IP アドレスまたはシンボリック名、およびポート番号**
     - **ローカルアドレスにはプロキシサーバーを使用しない**
     - ［**プロキシサーバーの認証設定**］セクションで、認証を設定します。ドロップダウンリストより認証設定を選択します：
       - **認証を使用しない** – 認証は行われません。
       - **NTLM 認証** – Microsoft が開発した NTLM ネットワーク認証プロトコルを使用して認証が行われます。既定では、このモードが選択されます。
     - 必要に応じて、ユーザー名とパスワードを入力します。
     - ［**ライセンス**］セクションで、［**アプリケーションのアクティベーション時に Kaspersky Security Center をプロキシサーバーとして使用する**］をオンまたはオフにします。

- ［**監視対象のポート**］セクションで、監視対象のネットワークポートを指定します。

  - **すべてのネットワークポートを監視する**：このネットワークポート監視モードでは、保護機能はコンピューターで開いているすべてのネットワークポート経由で送信されるデータストリームを監視します。

  - **選択されたネットワークポートのみを監視する**：このネットワークポートの監視モードでは、コンピューターの選択したポートおよび選択したアプリケーションのネットワークの動作を監視します。メールの送信とネットワークトラフィックで通常使用されるネットワークポートのリストは、カスペルスキーの専門家の推奨に従って構成されます。

  ［**設定**］をクリックし、次の設定を行います：

  - **カスペルスキー推奨のリストに登録されているアプリケーションのすべてのポートを監視する**：Kaspersky Embedded Systems Security によってポートが監視されるアプリケーションの事前定義済みのリストを使用します。このリストには例えば、Google Chrome、Adobe Reader、Java やその他のアプリケーションが含まれます。

  - **選択したアプリケーションのすべてのポートを監視する**：Kaspersky Embedded Systems Security によってポートが監視されるアプリケーションのリストを使用します。

6. ［**OK**］をクリックします。

接続設定の内容が保存されます。

## ローカルタスクのスケジュールによる開始の設定

ポリシーを使用して、ローカルシステムのオンデマンドスキャンタスクとアップデートタスクの開始を許可またはブロックできます。これは、管理グループ内の各保護対象デバイスでローカルに設定されたスケジュールに従って実行されます。

- 特定の種類のローカルシステムタスクの開始スケジュールがポリシーによって禁止される場合、これらのタスクは保護対象デバイス上でスケジュールどおりに実行されません。ローカルシステムタスクは手動で開始できます。

- 特定の種類のローカルシステムタスクの開始スケジュールがポリシーによって許可されている場合、これらのタスクは、このタスクに対してローカルに設定されたスケジュールパラメータに従って実行されます。

既定では、ローカルシステムタスクの開始はポリシーによって禁止されています。

アップデートまたはオンデマンドスキャンが Kaspersky Security Center グループタスクによって管理されている場合、ローカルシステムタスクの開始を許可しないことをお勧めします。

グループアップデートまたはオンデマンドスキャンタスクを使用しない場合は、ポリシーでローカルシステムタスクの開始を許可します。Kaspersky Embedded Systems Security は既定のスケジュールに従って定義データベースおよびモジュールのアップデートを実行し、すべてのローカルシステムのオンデマンドスキャンタスクを開始します。

ポリシーを使用して、次のローカルのシステムタスクに対するスケジュールによる開始を許可またはブロックできます：

- オンデマンドスキャンタスク：*簡易スキャン*、*オペレーティングシステムの起動時にスキャン*、*アプリケーション整合性チェック*、*ベースラインシステム変更監視*。
- アップデートタスク：*定義データベースと製品機能のアップデート*、*製品アップデート*。

保護対象デバイスが管理グループから除外される場合、ローカルのシステムタスクのスケジュールは自動的に有効になります。

*ポリシーで本製品のローカルタスクの起動スケジュール管理を許可またはブロックするには、次の手順を実行します：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開して、関連するグループを展開し、結果ペインで［**ポリシー**］タブを選択します。
2. ［**ポリシー**］タブで、保護対象デバイスのグループでの Kaspersky Embedded Systems Security のローカルシステムタスクのスケジュールを設定するポリシー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。
3. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］セクションを選択します。
4. ［**ローカルシステムタスクの実行**］サブセクションの［**設定**］をクリックします。
5. ［**ローカルタスクの使用を許可する**］チェックボックスをオンにします。
6. ［**スケジュール管理を許可する**］を使用して、本製品のローカルタスクの起動スケジュール管理を許可またはブロックします。

# Kaspersky Security Center でのバックアップ設定

Kaspersky Security Center でバックアップの全般的な設定を行うには：

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。
2. アプリケーション設定を編集する管理グループを選択します。
3. 選択した管理グループの詳細ペインで、次のいずれかを実行します：
   - 保護対象デバイスグループに対してアプリケーションを設定するには、［**ポリシー**］タブを選択して、設定する**プロパティ：<ポリシー名>**ウィンドウを開きます。
   - 個々の保護対象デバイスのタスクまたは本製品の設定を指定するには、［**デバイス**］タブを選択し、ローカルタスク設定またはアプリケーション設定に移動します。
4. ［**詳細設定**］に移動します。
5. ［**設定**］サブセクションの［**保管領域**］をクリックします。
6. 以下の表に、設定方法を示します。

保管領域の設定

| パラメータ | 説明 |
| --- | --- |
| ［**レポート**］タブで、次のレポート設定を指定します： | |
| **保存期間** | このチェックボックスをオンにすると、レポートの最長保管期間は指定した期間に制限されます。既定の最長レポート保管期間は 30 日です。この期間を経過すると、Kaspersky Embedded Systems Security は最も古いデータをレポートファイルから自動的に削除します。 |
| **レポートファイルのサイズを制限する** | このチェックボックスをオンにすると、最大レポートファイルサイズは指定した値に制限されます。既定では、最大ファイルサイズは 1024 MB です。最大レポートファイルサイズを超過しないように、最大レポートファイルサイズに到達すると、Kaspersky Embedded Systems Security は最も古いデータをレポートファイルから自動的に削除します。 |
| ［**バックアップ**］タブで、次のバックアップ設定を指定します： | |
| **保存期間** | 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。既定の最長ファイル保管期間は 30 日です。最大保管期間を経過すると、最も古いファイルがバックアップから削除されます。 |
| **バックアップのサイズを制限する** | 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、最大サイズは 400 MB です。保管領域の最大サイズを超過しないように、保管領域の最大サイズに到達すると、Kaspersky Embedded Systems 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。 |
| **空き容量のしきい値** | このチェックボックスにより、［バックアップ］の空き容量の下限を監視する機能を有効または無効に設定できます（既定値：100 MB）。空き容量が指定したしきい値を下回った場合、Kaspersky Embedded Systems Security により、［*バックアップの空き容量がしきい値より少なくなりました*］イベントが記録されて、この種別のイベントに関する通知の設定に従って通知が発行されます。<br>このチェックボックスをオンにすると、Kaspersky Embedded Systems Security により、［バックアップ］の空き容量が監視されます。<br>［**空き容量のしきい値**］は、［**バックアップのサイズを制限する**］をオンにした場合にアクティブになります。 |

# ポリシーの作成と編集

このセクションでは、Kaspersky Security Center のポリシーによる複数の保護対象デバイスの Kaspersky Embedded Systems Security の管理について説明します。

Kaspersky Security Center のグローバルポリシーは、Kaspersky Embedded Systems Security がインストールされている複数のデバイスでの保護を管理するために作成できます。

ポリシーは、1 つの管理グループに所属するすべての保護対象デバイスに対して、Kaspersky Embedded Systems Security の設定、機能、および指定したタスクを適用するものです。

1 つの管理グループに対して複数のポリシーを作成して適用できます。管理コンソールでは、グループに対して現在アクティブなポリシーのステータスは、「*アクティブ*」として示されます。

ポリシー適用に関する情報は、Kaspersky Embedded Systems Security システム監査ログに記録されます。この情報は、アプリケーションコンソールの［**Windows イベントログ監視**］フォルダーで参照できます。

Kaspersky Security Center では、保護対象デバイスにポリシーを適用する方法として、*設定の編集の禁止*があります。ポリシーが適用された後、Kaspersky Embedded Systems Security は、ポリシーのプロパティで［**編集がブロックされています**］に が指定された設定の値を使用します。この場合、Kaspersky Embedded Systems Security はポリシーが適用される前の設定値を使用しません。ポリシーのプロパティで［**編集が許可されています**］に が指定されたアクティブポリシーの設定値は適用されません。

ポリシーが有効の場合、ポリシーで アイコンが付いている設定の値がアプリケーションコンソールに表示されますが、編集はできません。その他の設定の値は、アプリケーションコンソールで編集できます。

アクティブなポリシーで設定されて アイコンが付いている設定は、個別の保護対象デバイスに対する Kaspersky Security Center の**保護対象デバイスのプロパティ**ウィンドウを使用した変更がブロックされます。

指定され、アクティブなポリシーを使用して保護対象デバイスに送信された設定は、アクティブなポリシーが無効になるとローカルタスク設定に保存されます。

ポリシーが現在実行中のコンピューターのリアルタイム保護タスクまたはネットワーク接続ストレージの保護タスクの設定を定義している場合、ポリシーによって定義されている設定は、ポリシーが適用された直後に変更されます。タスクが実行中でない場合は、タスクの開始時に設定が適用されます。

# ポリシーの作成

ポリシーを作成する前に、管理プラグイン klcfginst.exe をインストールする必要があります。

*本製品がインストールされ実行されている保護対象デバイスのグループのポリシーを作成するには、次の手順を実行します：*

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開し、ポリシーを作成する保護対象デバイスが含まれる管理グループを選択します。
2. 選択した管理グループの結果ペインで［**ポリシー**］タブを選択し、［**ポリシーの作成**］をクリックして、新規ポリシーウィザードを開始します。

   ［**新規ポリシーウィザード**］ウィンドウが開きます。
3. ［**グループポリシー作成対象のアプリケーションを選択**］ウィンドウで、Kaspersky Embedded Systems Security を選択します。
4. ［**次へ**］をクリックします。
5. ［**名前**］にグループポリシー名を入力します。

   次の記号をポリシー名に含めることはできません：`" * < : > ? \ |` 。
6. 本製品の以前のバージョンで使用されたポリシー設定を適用するには：
   a. ［**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**］チェックボックスをオンにします。
   b. ［**参照**］をクリックします。
   c. 適用するポリシーを選択します。
   d. ［**次へ**］をクリックします。

7. ［**処理の選択**］ウィンドウの［**ファイルのリアルタイム保護の設定**］で、［**ファイルのリアルタイム保護を有効にする**］をオンにしてセキュリティレベルを指定します。

タスク実行方法が選択されていない場合は、新規ポリシーウィザードの次の段階に進むことができません。

8. コンピューターのリアルタイム保護を設定します。

9. 信頼するオブジェクトとアプリケーションを設定します。

10. ［**アプリケーションのグループポリシーを作成**］ウィンドウで、次のいずれかのポリシーステータスを選択します：

- **アクティブポリシー** - ポリシーの作成後、すぐに適用する場合。アクティブポリシーが既にグループに存在する場合、既存のポリシーは無効となり、新しいポリシーが適用されます。
- **非アクティブポリシー** - 作成するポリシーをすぐには適用しない場合。この場合、ポリシーは後で有効にできます。
- **モバイルユーザーポリシー**は、コンピューターが組織ネットワーク外に出た場合に有効になります。
- ［**ポリシーの作成後すぐにプロパティを開く**］をオンにすると、**新規ポリシーウィザード**が自動的に閉じ、［**次へ**］をクリックした後で新しく作成されたポリシーを設定します。

11. ［**完了**］をクリックします。

**作成したポリシー**が、選択した管理グループの［**ポリシー**］タブのポリシーのリストに表示されます。ポリシーのプロパティウィンドウで、Kaspersky Embedded Systems Security のその他の設定、タスク、機能を設定できます。

新しいポリシーの作成後、本製品のブロックを防止するための一連の許可ルールが作成され、本製品の動作が中断されなくなります。タスク設定で既定のルールを表示できます。詳細と制限事項は、下を参照してください。

既定では、新しいポリシーを作成すると、受信ネットワークトラフィックの一連のルールが作成されます：

- Kaspersky Security Center ネットワークエージェントを使用して Windows デスクトップを共有するプロセスに対する 2 つの許可ルール。フォルダー %Program Files% とフォルダー %Program Files (x86)% にあります。ステータス：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。
- ローカルポート 15000 の 2 つの許可ルール。状態：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。

既定では、新しいポリシーを作成すると、送信ネットワークトラフィックの一連のルールが作成されます：

- Kaspersky Embedded Systems Security サービスの 2 つの許可ルール。フォルダー %Program Files% およびフォルダー %Program Files (x86)% にあります。ステータス：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。
- Kaspersky Embedded Systems Security のワーカー プロセスに対する 2 つの許可ルール。フォルダー %Program Files% と フォルダー %Program Files (x86)% にあります。ステータス：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。
- ローカルポート 13000 の 2 つの許可ルール。状態：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。

# ポリシーの設定

*ポリシー設定を行うには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. 関連するポリシーを設定する管理グループを展開して、詳細ペインで［**ポリシー**］タブを開きます。
3. 設定するポリシー名をクリックします。

   次のいずれかの方法で、**ポリシーのプロパティ** 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で［**プロパティ**］を選択する。
   - 選択されたポリシーをダブルクリックする。
4. ［**全般**］タブの［**ポリシーのステータス**］セクションで、ポリシーを有効または無効にします。それには、次のいずれかのオプションを選択します：
   - **アクティブポリシー** - 選択した管理グループ内のすべての保護対象デバイスにポリシーを適用する場合に選択します。
   - **モバイルユーザーポリシー** - このポリシーは、コンピューターが組織ネットワーク外に出た場合に有効になります。
   - **非アクティブポリシー** - 選択した管理グループ内のすべての保護対象デバイスで後からポリシーを有効にする場合に選択します。
5. ポリシーの他のセクションで、本製品を設定します。

   Kaspersky Security Center のポリシーを使用して、管理グループ内のすべての保護対象デバイスに対するタスクの実行を有効または無効にできます。

個別のソフトウェアコンポーネントに対して、すべてのネットワークの保護対象デバイスにポリシー設定を適用するかどうかを指定できます。

6. ［**OK**］をクリックします。

設定の内容がポリシーに適用されます。

## セキュリティレベルインジケーター

セキュリティレベルインジケーターは、ポリシーのプロパティウィンドウの上部に表示されます。このインジケーターの値は以下のいずれかです：

- **保護レベル：高**：以下のカテゴリに属するすべてのコンポーネントが有効になっていて でマークされている場合は、インジケーターがこの値で緑色になります：
  - **緊急**：このカテゴリには以下のコンポーネントが含まれます：
    - ファイルのリアルタイム保護
    - ふるまい検知
    - 脆弱性攻撃ブロック
    - 修復エンジン
    - セキュアデスクトップの通知を有効にする
  - **重要**：このカテゴリにはKSN の使用コンポーネントが含まれます。
- **保護レベル：中**：1つの「重要」コンポーネントが無効になっていて でマークされている場合は、インジケーターがこの値で黄色になります。
- **保護レベル：低**：1つまたは複数の「緊急」コンポーネントが無効になっていて でマークされている場合は、インジケーターがこの値で赤色になります。

インジケーターに［**保護レベル：中**］または［**保護レベル：低**］の値が表示されている場合、インジケーターの右側にあるリンクをクリックすると、［**推奨される保護機能**］ウィンドウが開きます。このウィンドウでは、推奨される保護機能を有効にしたり、無効にならないようにしたりできます。

# Kaspersky Security Center を使用したタスクの作成と編集

このセクションでは、Kaspersky Embedded Systems Security タスク、そのタスクの作成方法と設定方法、およびそのタスクの開始方法と停止方法に関する情報について説明します。

# Kaspersky Security Center でのタスクの作成について

管理グループと特定の保護対象デバイスに対してグループタスクを作成できます。Kaspersky Security Center を介して次の種別のタスクを作成できます。

- *アクティベーションの完了*
- *管理サーバーの接続の保護*
- *Kaspersky Embedded Systems Security コンポーネントの変更*
- *ベースラインシステム変更監視*
- *アップデート*
- *アップデートのロールバック*
- *オンデマンドスキャン*
- *アプリケーション整合性チェック*
- *ライセンスの削除*
- *アプリケーション起動コントロールルールの自動生成*
- *デバイスコントロールルールの自動生成*

次の方法で、ローカルタスクおよびグループタスクを作成できます：

- 個別の保護対象デバイスの場合、［**タスク**］セクションから作成します。
- 管理グループの場合、選択された保護対象デバイスのグループのフォルダーの詳細ペインの［**タスク**］タブから作成します。
- 一連の保護対象デバイスの場合、［**デバイスの抽出**］フォルダーの詳細ペインから作成します。

ポリシーを使用し、同じ管理グループのすべての保護対象デバイス上で、*アップデート*と*オンデマンドスキャン*のローカルシステムタスクのスケジュールを無効にできます。

Kaspersky Security Center のタスクの一般的な情報については、*Kaspersky Security Center* のヘルプを参照してください。

# Kaspersky Security Center を使用したタスクの作成

*Kaspersky Security Center の管理コンソールで新しいタスクを作成するには：*

1. 次のいずれかの方法でタスクウィザードを開始します：

   - ローカルタスクを作成するには：

     a. アプリケーションコンソールツリーで［**管理対象デバイス**］フォルダーを展開し、保護対象サーバーが所属するグループを選択します。

     b. 結果ペインの［**デバイス**］タブで、保護対象デバイス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。

     c. 表示されたウィンドウで、［**タスク**］セクションの［**追加**］をクリックします。

   - グループタスクを作成するには：

     a. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。

     b. タスクを作成する管理グループを選択します。

     c. 結果ペインで［**タスク**］タブを開き、［**新規タスク**］を選択します。

   タスクウィザードのウィンドウが開きます。

2. ［**タスク種別の選択**］ウィンドウの［**Kaspersky Embedded Systems Security**］ヘッダーで、作成するタスクの種別を選択します。

3. タスクの種別に応じて、設定が異なります：

   - オンデマンドスキャンタスクを作成します。

   - アップデートタスクを作成するには、要件に基づいてタスク設定を行います：

     a. ［**アップデート元**］ブロックで、アプリケーションのアップデート元として、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を指定できます。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。

     手動でカスタマイズしたサーバーが使用できない場合、カスペルスキーのアップデートサーバーの使用を指定できます。

     b. ディスクサブシステムの負荷を軽減する機能を設定します：

     c. 重要なソフトウェアモジュールのアップデートが必要な場合、および重要なアップデートのインストール完了後に Kaspersky Embedded Systems Security が実行する操作を指定できます。また、Kaspersky Embedded Systems Security が適用可能なスケジュールされたアップデートに関する情報を受信するかどうかを指定できます。

     d. コピーする一連のアップデートを指定して、コピーしたアップデートの保存先として使用するフォルダーのパスを指定します。

- ［アクティベーションの完了］タスクを作成するには：

  a. ［**アクティベーション設定**］ウィンドウでは、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情報ファイルまたはアクティベーションコードを指定します。

  b. ライセンスを更新するタスクを作成するには［**予備のライセンスとして使用する**］をオンにします。

- ［アプリケーション起動コントロールルールの自動生成］タスクを作成します。

- ［デバイスコントロールルールの自動生成］タスクを作成します。

4. タスクのスケジュールを設定します。

5. ［**OK**］をクリックします。

6. タスクが複数の保護対象デバイス用に作成されている場合は、このタスクを実行する保護対象デバイスのネットワーク（またはグループ）を選択します。

7. ［**タスクを実行するアカウントの選択**］ウィンドウで、タスクの実行で使用するアカウントを指定します。

8. ［**タスク名の定義**］ウィンドウで、タスク名を入力します（100 文字以内にする必要があり、**" * < > ? \ | :** の記号は使用できません）。
   タスクの種別をタスクの名前に追加してください（「共有フォルダーのオンデマンドスキャン」など）。

9. ［**タスク作成の終了**］ウィンドウで、次のいずれかの手順を実行します：

   a. 作成された後すぐにタスクを開始する場合は［**ウィザードの終了後にタスクを実行**］を選択します。

   b. ［**終了**］をクリックします。

［**タスク**］のリストに作成したタスクが表示されます。

# 個々のコンピューターのローカルタスク設定と全般的な製品設定への移動

アプリケーションが Kaspersky Security Center ポリシーに従っており、このポリシーでアプリケーション設定の変更が禁止されている場合、個別のコンピューター向けにこれらの設定を編集することはできません。

*個々のコンピュータのローカルタスク設定に移動するには、次の手順を実行します：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

2. 保護対象デバイスが所属するグループを選択します。

3. 結果ペインで、［**デバイス**］タブを選択します。

4. 次のいずれかの方法で、**プロパティ：<保護対象デバイス名>**ウィンドウを開きます：

   - 保護対象デバイスの名前をダブルクリックする。
   - 保護対象デバイスの名前のコンテキスト メニューで、［**プロパティ**］を選択します。

   保護対象デバイスのプロパティウィンドウが表示されます。

5. ［**タスク**］セクションに進みます。

6. タスクリストで、設定するローカルタスクを次のいずれかの方法で選択します。

   - タスク名をダブルクリックします。
   - リスト内のタスクを選択し、［**プロパティ**］をクリックします。
   - タスク名の上でコンテキストメニューを開き、［**プロパティ**］を選択します。

   ［**プロパティ：<タスク名>**］ウィンドウが開きます。

*個々のコンピュータの全般的なアプリケーション設定に移動するには、次の手順を実行します：*

1. Kaspersky Security Center 管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開し、保護対象デバイスが所属するグループを選択します。

2. 結果ペインで、［**デバイス**］タブを選択します。

3. 次のいずれかの方法で、**プロパティ：<保護対象デバイス名>**ウィンドウを開きます：

   - 保護対象デバイスの名前をダブルクリックする。
   - 保護対象デバイスの名前のコンテキスト メニューで、［**プロパティ**］を選択します。

   保護対象デバイス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**］セクションに進みます。

5. 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 Embedded Systems Security を次のいずれかの方法で選択します：

   - Kaspersky Embedded Systems Security の名前をダブルクリックします。
   - リストから Kaspersky Embedded Systems Security を選択し、［**プロパティ**］をクリックします。
   - Kaspersky Embedded Systems Security の名前のコンテキストメニューで、［**プロパティ**］を選択します。

   **Kaspersky Embedded Systems Security** の［**設定**］ウィンドウが開きます。

# Kaspersky Security Center でのグループタスクの設定

*複数の保護対象デバイスに対してグループタスクを設定するには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開し、製品のタスクを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで［**タスク**］タブを開きます。
3. 以前作成したグループタスクのリストで、設定するタスクを選択します。
4. 次のいずれかの方法で、**プロパティ：<タスク名>**ウィンドウを開きます：
   - 作成済みのタスクのリストで、タスク名をダブルクリックする。
   - 作成済みのタスクのリストでタスク名を選択し、詳細ペインの［**タスクの設定**］をクリックする。
   - 作成済みのタスクのリストからタスク名の上でコンテキストメニューを開き、［**プロパティ**］を選択する。
5. ［**通知**］セクションで、タスクイベントの通知設定を行います。このセクションでの設定の詳細情報については、*Kaspersky Security Center のヘルプ*を参照してください。
6. 設定したタスクの種別に従って、次のいずれかを実行します：
   - *オンデマンドスキャンのタスクを設定するには：*
     - ［**スキャン範囲**］セクションで、スキャン範囲を設定します。
     - ［**設定**］セクションで、タスクの優先度とソフトウェアのその他のコンポーネントとの連携を設定します。
   - *アップデートのタスクを設定するには：*
     - ［**設定**］セクションに移動し、［**定義データベースとモジュールのアップデート設定**］を指定します。
     - 実行する操作を指定します：ソフトウェアモジュールの重要なアップデートのコピーおよびインストール、またはその確認のみ。
   - *アクティベーションの完了のタスクを設定するには：*
     - ［**設定**］セクションでは、製品のアクティベーションに使用するライセンス情報ファイルを指定します。
     - ライセンスの更新に使用するアクティベーションコードまたはライセンス情報ファイルを追加する場合は、［**予備のライセンスとして使用する**］をオンにします。
   - *デバイスコントロールルールの自動生成*タスクを設定するには、［**設定**］セクションで、デバイスコントロールルールのリストを作成するために使用する設定を指定します。
7. ［**スケジュール**］セクションでタスクスケジュールを設定します。

8. ［**アカウント**］セクションで、タスクの実行で使用する権限を持つアカウントを指定します。このセクションでの設定の詳細情報については、*Kaspersky Security Center* のヘルプを参照してください。

9. 必要に応じて、［**タスク範囲からの除外**］セクションで、タスクの範囲から除外するオブジェクトを指定します。このセクションでの設定の詳細情報については、*Kaspersky Security Center* のヘルプを参照してください。

10. **タスクのプロパティ**ウィンドウで、［OK］をクリックします。

新たに設定したタスクの内容が保存されます。

グループタスクの構成可能な設定を以下に示します。

- アプリケーション起動コントロールルールの自動生成

  *アプリケーション起動コントロールルールの自動生成*タスクの設定時に、［**ルール**］タブで、許可ルールの作成方法を選択できます：

  - **実行中のアプリケーションに基づいて許可ルールを作成する**
  - **アプリケーション向けの許可ルールを作成する**

  ［**設定**］タブで、アプリケーション起動コントロールの許可ルールを作成する際に、以下の処理を実行するよう指定できます：

  - **デジタル証明書を使用する**
  - **デジタル証明書の発行先とサムプリントを使用する**
  - **証明書がない場合に次を使用する**
  - **SHA256 ハッシュを使用する**
  - **次のユーザーまたはユーザーグループに対するルールを生成**

  Kaspersky Embedded Systems Security がタスク完了時に作成する許可ルールリストで、設定情報ファイルの設定ができます。

  スケジュールでタスクを開始する設定を指定できます。

- デバイスコントロールルールの自動生成

  - 処理モードを［過去に接続されたすべての外部デバイスについてシステムデータを考慮する］と［現在接続している外部デバイスだけを考慮する］から選択します。
  - Kaspersky Embedded Systems Security がタスク完了時に作成する許可ルールリストで、設定情報ファイルを設定します。
  - スケジュールでタスクを開始する設定を指定できます。

- アクティベーションの完了

  - 製品のアクティベーションやライセンスの更新には、ライセンス情報ファイルまたはアクティベーションコードを追加します。
  - スケジュールでタスクを開始する設定を指定できます。

- 定義データベースと製品機能のアップデート

  - ［**アップデート元**］設定ブロックで、アプリケーションのアップデート元として、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を指定できます。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。

    手動でカスタマイズしたサーバーが使用できない場合、カスペルスキーのアップデートサーバーの使用を指定できます。

  - ディスクサブシステムの負荷を軽減する機能を設定できます：

    - **ディスク I/O の負荷の低減**

    - **最適化に使用するメモリ（MB）**

  - 重要なソフトウェアモジュールのアップデートが必要な場合、および重要なアップデートのインストール完了後に Kaspersky Embedded Systems Security が実行する操作を指定できます。また、Kaspersky Embedded Systems Security が適用可能なスケジュールされたアップデートに関する情報を受信するかどうかを指定できます。

  - コピーする一連のアップデートを指定して、コピーしたアップデートの保存先として使用するフォルダーのパスを指定できます。

  - スケジュールでタスクを開始する設定を指定できます。

- オンデマンドスキャン

  - オンデマンドスキャンタスクのスキャン範囲を指定し、セキュリティレベルを設定できます。

  - ［**ヒューリスティックアナライザー**］設定ブロックでは、オンデマンドスキャンタスクでのヒューリスティックアナライザーの使用を有効または無効にし、スライダーを使用して分析レベルを設定できます。

  - ［**他のコンポーネントとの連携**］ブロックでは、次の設定を行うことができます。

    - スキャンタスクをバックグラウンドモードで開始します。

    - タスクを簡易スキャンとします。

    - 複数のスキャンタスクの同時起動を無効にします。

  - スケジュールでタスクを開始する設定を指定できます。

- アプリケーション整合性チェック

  - スケジュールでタスクを開始する設定を指定できます。

- ベースラインシステム変更監視

  - 監視モードと、ファイル、レジストリ、デバイスに対して実行する処理を指定するルールを設定できます。

  - スケジュールでタスクを開始する設定を指定できます。

## 本製品のアクティベーションタスク

*アクティベーションの完了のタスクを設定するには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開し、製品のタスクを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで［**タスク**］タブを開きます。
3. 以前作成したグループタスクのリストで、設定するタスクを選択します。
4. 次のいずれかの方法で、**プロパティ：<タスク名>**ウィンドウを開きます：
   - 作成済みのタスクのリストで、タスク名をダブルクリックする。
   - 作成済みのタスクのリストからタスク名の上でコンテキストメニューを開き、［**プロパティ**］を選択する。

   ［**通知**］セクションで、タスクイベントの通知設定を行います。このセクションでの設定の詳細情報については、*Kaspersky Security Center* のヘルプを参照してください。
5. ［**アクティベーション設定**］セクションでは、製品のアクティベーションに使用するライセンス情報ファイルを指定します。更新用のライセンスを追加する場合は、［**予備のライセンスとして使用する**］をオンにします。
6. ［**スケジュール**］セクションで、タスクのスケジュールを設定します。
7. 必要に応じて、［**タスク範囲からの除外**］セクションで、タスクの範囲から除外するオブジェクトを指定します。

   これらのセクションでの設定の詳細情報については、*Kaspersky Security Center* のヘルプを参照してください。
8. **タスクのプロパティ**ウィンドウで、［OK］をクリックします。

   新たに設定したタスクの内容が保存されます。

## アップデートタスク

*アップデートのタスクを設定するには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開し、製品のタスクを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで［**タスク**］タブを開きます。
3. 以前作成したグループタスクのリストで、設定するタスクを選択します。

4. 次のいずれかの方法で、**プロパティ：<タスク名>**ウィンドウを開きます：

   - 作成済みのタスクのリストで、タスク名をダブルクリックする。
   - 作成済みのタスクのリストからタスク名の上でコンテキストメニューを開き、［**プロパティ**］を選択する。

5. ［**通知**］セクションで、タスクイベントの通知設定を行います。このセクションでの設定の詳細情報については、*Kaspersky Security Center* のヘルプを参照してください。

6. ［**設定**］セクションで、次の操作を行います：

   a. ［**定義データベースとモジュールのアップデート設定**］セクションの［**設定**］を使用してアップデート元を選択します：

      - Kaspersky Security Center 管理サーバー
      - カスペルスキーのアップデートサーバー
      - カスタム HTTP サーバーか FTP サーバー、またはネットワークフォルダー

      > SMB 共有フォルダーをアップデート元として使用するには、タスクを開始するユーザーアカウントを指定する必要があります。

      手動でカスタマイズしたサーバーが使用できない場合、カスペルスキーのアップデートサーバーの使用を指定できます。

   b. ディスクサブシステムの負荷を軽減する機能を設定します：

      - **ディスク I/O の負荷の低減**：このチェックボックスでは、メモリの仮想ドライブへのアップデートファイルを保管することによりディスクサブシステムを最適化するプロセス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。
      - **最適化に使用するメモリ（MB）**

   c. 製品機能の重要なアップデートが適用可能な場合、または定期的なアップデートに関する情報がある場合に、Kaspersky Embedded Systems Security が実行する処理を指定します。

   d. アップデートのコピー設定を指定します。

7. ［**スケジュール**］セクションで、タスクのスケジュールを設定します（アップデートのロールバックを除くすべてのタスク種別に対して、スケジュールを設定できます）。

8. ［**アカウント**］セクションで、タスクの実行で使用する権限を持つアカウントを指定します。

   > これらのセクションでの設定の詳細情報については、*Kaspersky Security Center* のヘルプを参照してください。

9. タスクのプロパティウィンドウで、［**OK**］をクリックします。

*アップデートのロールバック*タスクについては、Kaspersky Security Center の［**通知**］セクションと［**タスク範囲からの除外**］セクションによってコントロールされる標準タスク設定のみを設定できます。これらのセクションでの設定の詳細情報については、*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整合性チェック

*アプリケーション整合性チェックのグループタスクを設定するには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開し、アプリケーション整合性コントロールのタスクを設定する管理グループを選択します。
2. 選択した管理グループの詳細ペインで［**タスク**］タブを開きます。
3. 以前作成したグループタスクのリストで、設定するアプリケーション整合性コントロールのタスクを選択します。
4. 次のいずれかの方法で、**プロパティ：<タスク名>**ウィンドウを開きます：
   - 作成済みのタスクのリストで、タスク名をダブルクリックする。
   - 作成済みのタスクのリストからタスク名の上でコンテキストメニューを開き、［**プロパティ**］を選択する。
5. ［**通知**］セクションで、タスクイベントの通知設定を行います。このセクションでの設定の詳細情報については、*Kaspersky Security Center のヘルプ*を参照してください。
6. ［**デバイス**］セクションで、アプリケーションの整合性チェックタスクを設定するデバイスを選択します。
7. ［**スケジュール**］セクションで、タスクのスケジュールを設定します。
8. ［**アカウント**］セクションで、タスクの実行で使用する権限を持つアカウントを指定します。
9. 必要に応じて、［**タスク範囲からの除外**］セクションで、タスクの範囲から除外するオブジェクトを指定します。

   これらのセクションでの設定の詳細情報については、*Kaspersky Security Center のヘルプ*を参照してください。

10. **タスクのプロパティ**ウィンドウで、［OK］をクリックします。

# タスクスケジュールの管理

Kaspersky Embedded Systems Security のタスクにスケジュールを設定できます。

## タスクのスケジュールを設定する

アプリケーションコンソールでは、ローカルのシステムタスクとカスタムタスクの開始スケジュールを設定することができます。アプリケーションコンソールを使用してグループタスクのスケジュールを設定することはできません。

*管理プラグインを使用してグループタスクのスケジュールを設定するには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. 保護対象デバイスが所属するグループを選択します。
3. 結果ペインで、［**タスク**］タブを選択します。
4. 次のいずれかの方法で、**プロパティ：<タスク名>**ウィンドウを開きます：
   - タスクの名前をダブルクリックする。
   - 対象のタスクのコンテキストメニューを開き、［**プロパティ**］を選択する。
5. ［**スケジュール**］セクションを選択します。
6. ［**実行予定**］ドロップダウンリストで、起動パラメータを選択します：

   オンデマンドスキャンタスクとアップデートタスクのスケジュール設定に使用するフィールドは、これらのタスクのスケジュールの設定が Kaspersky Security Center ポリシーによってブロックされた場合、使用できません。

   - **N 時間ごと**：タスクを数時間ごとに定期的に実行する場合に選択します。［**開始までの間隔（時間）**］フィールドに時間数を入力します。
   - **N 日ごと**：タスクを数日ごとに定期的に実行する場合に選択します。［**開始までの間隔（日）**］フィールドに日数を入力します。
   - **N 分ごと**：タスクを数分ごとに定期的に実行する場合に選択します。［**開始までの間隔（分）**］フィールドに分数を入力します。
   - **毎週**：タスクを特定の曜日に実行する場合に選択します。実行する時刻も指定します。
   - **毎月**：タスクを月の特定の日に実行する場合に選択します。実行する時刻も指定します。
   - **1回**：指定した日時にタスクを1回実行する場合に選択します。
   - **手動**：タスクを手動で実行する場合に選択します。
   - **アプリケーション開始時**：Kaspersky Embedded Systems Security が起動するたびにタスクを実行する場合に選択します。
   - **新しいアップデートがリポジトリにダウンロードされ次第**：リポジトリにアップデートがダウンロードされるたびにタスクを実行する場合に選択します。
   - **ウイルスアウトブレイク検知次第**：ウイルス攻撃が検知された場合にタスクを実行する場合に選択します。
   - **他のタスクが完了次第**：他のタスクの完了時にタスクを実行する場合に選択します。

   a. ［**開始時刻**］フィールドにタスクを最初に開始する時刻を指定します。

   b. ［**開始時間**］フィールドにスケジュールの開始日を指定します。

タスクの開始時間、日付、および頻度のスケジュールを設定した後、次回タスクが開始される予定の日時が表示されます。

［**スケジュール**］に移動し、［**タスク設定**］ウィンドウを開きます。ウィンドウの上部にある［**次回の開始**］フィールドに開始予定時刻が表示されます。ウィンドウを開くたびに、この開始予定時刻が更新されて表示されます。

Kaspersky Security Center ポリシーの設定でローカルシステムタスクのスケジュール設定が禁止されている場合、［**次回の開始**］フィールドには［**ポリシーによりブロック**］と表示されます。

7. ［**未実行のタスクを実行する**］をオンにして、スキップしたタスクの開始を有効にします。
8. ［**タスクの開始を自動的かつランダムに遅延させる**］がオンの場合、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。
9. ［**詳細**］をクリックして、要件に従って以下のスケジュール設定を指定します：
   - **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。
   - **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がオンの場合、タスクの完了後にデバイス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**このチェックボックスがオンの場合、指定された時間より長く実行された場合にタスクが停止されます。
10. ［**OK**］をクリックします。
11. ［**適用**］をクリックして、タスクの開始設定を保存します。

Kaspersky Security Center を使用して 1 つのタスクの設定を指定する場合、「Kaspersky Security Center のアプリケーションの設定ウィンドウでのローカルタスクの設定」セクションを参照してください。

## スケジュールに従ったタスクの有効化と無効化

スケジュール設定を行う前、または行った後で、スケジュールに従ったタスクを有効または無効にできます。

*タスクの開始スケジュールを有効または無効にするには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. 保護対象デバイスが所属するグループを選択します。
3. 結果ペインで、［**タスク**］タブを選択します。

4. 次のいずれかの方法で、**プロパティ：<タスク名>**ウィンドウを開きます：

   - タスクの名前をダブルクリックする。
   - 対象のタスクのコンテキストメニューを開き、［プロパティ］を選択する。

5. ［**スケジュール**］セクションを選択します。
6. スケジュールに従ったタスクの開始を有効にする場合は、［**実行予定**］ドロップダウンリストから、スケジュールに従ったタスクを実行するための設定を選択します。
7. スケジュールに従ったタスクの開始を無効にする場合は、ドロップダウンリストから［**手動**］を選択します。

   タスクの開始スケジュール設定は削除されませんが、スケジュールを設定したタスクの開始を有効または無効にした結果が次回以降適用されます。

8. ［OK］をクリックします。

タスク開始スケジュールの設定が保存されます。

# Kaspersky Security Center のレポート

Kaspersky Security Center のレポートには、管理対象デバイスのステータスに関する情報が含まれます。レポートは管理サーバーに保存される情報に基づきます。

Kaspersky Security Center 11 より、Kaspersky Embedded Systems Security で次の種別のレポートが利用できるようになりました：

- 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
- 禁止されたアプリケーションに関するレポート
- テストモードで禁止されたアプリケーションに関するレポート

Kaspersky Security Center のレポートやその設定方法の詳細は、*Kaspersky Security Center のオンラインヘルプ*をご参照ください。

## Kaspersky Embedded Systems Security のコンポーネントステータスに関するレポート

すべてのネットワークデバイスの保護ステータスを監視して、各デバイスで設定されているコンポーネントの構造化された概要を取得できます。

レポートには、コンポーネントごとに以下のステータスのいずれかが表示されます：*実行中*、*一時停止済み*、*停止済み*、*ライセンスに含まれていません*。

［*未インストール*］ステータスは、アプリケーション自体ではなくコンポーネントを参照します。アプリケーションが Kaspersky Security Center にインストールされていない場合は、N/A（利用不可）のステータスを割り当てます。

コンポーネントの選択を作成し、フィルターを使用して、指定されたコンポーネントのセットおよびその状態のネットワークデバイスを表示します。

選択の作成および利用の詳細については、『*Kaspersky Security Center ヘルプ*』を参照してください。

*アプリケーションの設定でコンポーネントステータスを確認するには：*

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開し、アプリケーションを設定する管理グループを選択します。
2. ［**デバイス**］タブを選択して［**アプリケーションの設定**］ウィンドウを開きます。
3. ［**コンポーネント**］セクションを選択します。
4. ステータステーブルを確認します。

*Kaspersky Security Center の標準レポートを確認するには：*

1. 管理コンソールツリーで［**管理サーバー <管理サーバー名>**］フォルダーを選択します。
2. ［**レポート**］タブを選択します。
3. ［**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**］リストの項目をダブルクリックします。
   レポートが生成されます。
4. 以下のレポートの詳細を確認します：
   - 図表。
   - コンポーネント、各コンポーネントがインストールされているネットワークデバイスの合計数、およびそれらが属するグループの概要のテーブル。
   - コンポーネントステータス、バージョン、デバイス、およびグループを指定する詳細なテーブル。

## 処理を実行モードおよび統計情報モードでのブロックされたアプリケーションのレポート

アプリケーション起動コントロールタスクの実行結果に基づいて、次の 2 種類のレポートを生成できます：禁止したアプリケーションのレポート（処理を実行モードでタスクを開始した場合）、テストモードで禁止したアプリケーションのレポート（通知モードでタスクを開始した場合）。これらのレポートは、ネットワークの保護対象デバイス上にあるブロックされたアプリケーションの情報を表示します。すべての管理グループに対して各レポートが生成され、保護対象デバイス上にインストールされたすべてのカスペルスキー製品からのデータを蓄積します。

*通知モードで禁止されたアプリケーションに関するレポートを表示するには：*

1. アプリケーション起動コントロールタスクを処理を通知モードで開始します。
2. 管理コンソールツリーで［**管理サーバー <管理サーバー名>**］フォルダーを選択します。
3. ［**レポート**］タブを選択します。
4. ［**テストモードで禁止されたアプリケーションに関するレポート**］の項目をダブルクリックします。
   レポートが生成されます。
5. 以下のレポートの詳細を確認します：
   - ブロックされた起動が最も多いアプリケーションの上位 10 個を表示する図表。
   - ブロックされたアプリケーションについて、実行ファイルの名前、理由、ブロックの時刻、ブロックされたデバイスの数を示す概要のテーブル。
   - デバイス、ファイルパス、およびブロックの条件に関するデータを示す詳細なテーブル。

*処理を実行モードで禁止されたアプリケーションに関するレポートを表示するには：*

1. アプリケーション起動コントロールタスクを処理を実行モードで開始します。
2. 管理コンソールツリーで［**管理サーバー <管理サーバー名>**］フォルダーを選択します。
3. ［**レポート**］タブを選択します。
4. ［**禁止されたアプリケーションに関するレポート**］リストの項目をダブルクリックします。
   レポートが生成されます。

このレポートは、テストモードで禁止されたアプリケーションに関するレポートと同じブロックに関するデータで構成されます。

# Kaspersky Embedded Systems Security コンソールの使用

このセクションでは、Kaspersky Embedded Systems Security コンソールについての情報を提供するとともに、保護対象デバイスまたは別のデバイスにインストールされているアプリケーションコンソールを使用してアプリケーションを管理する方法について説明します。

## アプリケーションコンソールの起動

*アプリケーションコンソールを起動するには：*

1. 次のいずれかの方法でコンパクト診断インターフェイスを開きます：

   - 保護対象デバイスのアプリケーションのインストールフォルダーにあるファイル avpui.exe を実行します。既定では、ファイルは C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0 にあります。
   - タスクバーの通知エリアの製品アイコンをクリックします。

2. 表示されたコンパクト診断インターフェイスウィンドウで、［**Kaspersky Embedded Systems Security コンソール**］をクリックします。

   保護対象デバイスへの接続が既に設定されている場合は、アプリケーションコンソールが開きます。

   アプリケーションコンソールを初めて起動する場合は、［**保護対象デバイスの選択**］ウィンドウが表示されて、そのウィンドウで**アプリケーションコンソールと保護対象コンピューターの接続を設定する**必要があります。

   a. Kaspersky Embedded Systems Security とアプリケーションコンソールが同じコンピューターにインストールされている場合は、［**ローカルコンピューター（アプリケーションコンソールが実行されているコンピューター）**］を選択します。

   b. Kaspersky Embedded Systems Security とアプリケーションコンソールが異なるコンピューターにインストールされている場合は、次の手順を実行します：

      1. ［**別のデバイス**］を選択します。
      2. ［**参照**］をクリックして、本製品がインストールされているコンピューターの名前を指定します。
      3. 本製品がインストールされているコンピューターに接続するためのポートを入力します。

   c. ［**次のユーザーとして接続**］をオンまたはオフにして、本製品がインストールされているコンピューターにアプリケーションコンソールを接続する際のユーザーアカウント権限の使用を有効または無効にします。

d. ユーザーとしての接続を有効にする場合は、ユーザーの名前とパスワードを入力します。指定されたユーザーは、本製品がインストールされているコンピューターの ESS Administrators グループのメンバーである必要があります。

ユーザー名は大文字と小文字が区別されます。

e. ［**接続**］をクリックします。

# Kaspersky Embedded Systems Security コンソールのインターフェイス

このセクションでは、本製品のインターフェイスの主な項目について説明します。

## Kaspersky Embedded Systems Security コンソールのウィンドウ

異なる保護対象デバイスにインストールされた Kaspersky Embedded Systems Security への接続が確立されると、フォルダーの名前に、本製品がインストールされた保護対象デバイスの名前、接続が確立されたユーザーアカウントの名前が追加されます：**Kaspersky Embedded Systems Security <保護対象デバイス名> アカウント：<アカウント名>**。Kaspersky Embedded Systems Security コンソールと同じ保護対象デバイスにインストールされた Kaspersky Embedded Systems Security に接続した場合、フォルダー名は［Kaspersky Embedded Systems Security］です。

### コンソールツリー

アプリケーションコンソールツリーには、［**Kaspersky Embedded Systems Security**］フォルダーと製品の機能コンポーネントのサブフォルダーが表示されます。

［**Kaspersky Embedded Systems Security**］フォルダーには、次のサブフォルダーが含まれます：

- **コンピューターのリアルタイム保護**：次のタスクを設定できます：
  - **ファイルのリアルタイム保護**
  - **Kaspersky Security Network**
  - **脆弱性攻撃ブロック**
  - **ネットワーク脅威対策**
  - **ふるまい検知**
  - **修復エンジン**
  - **AMSI 保護**

- **コンピューターコントロール**：保護対象デバイスおよび接続されたデバイス上で実行されているアプリケーションの管理。
  - **アプリケーション起動コントロール**
  - **デバイスコントロール**
  - **ファイアウォール**
- **ルールの自動生成**：アプリケーション起動コントロールタスクおよびデバイスコントロールタスクでのグループおよびシステムルールの自動生成を設定します。
  - **アプリケーション起動コントロールルールの自動生成**
  - **デバイスコントロールルールの自動生成**
  - ルール生成グループタスク **<タスク名>**（存在する場合）

    グループタスクは Kaspersky Security Center を使用して作成されます。Kaspersky Embedded Systems Security コンソールからグループタスクを管理することはできません。
- **システム監査**：システム変更監視と Windows イベントログ分析を設定します。
  - **Windows イベントログ監視**
  - **システム変更監視**
- **オンデマンドスキャン**：オンデマンドスキャンタスクを管理します。各タスクに対して別々のフォルダーがあります：
  - **簡易スキャン**
  - **アプリケーションの整合性チェック**
  - **リムーバブルドライブスキャン**
  - **完全スキャン**
  - カスタムタスク **<タスク名>**（存在する場合）

  フォルダーには、アプリケーションがインストールされ、カスタムタスク、およびグループオンデマンドタスクが作成され、Kaspersky Security Center を使用して保護対象デバイスに送信された時に作成されたシステムタスクが表示されます。
- **アップデート**：Kaspersky Embedded Systems Security の定義データベースと製品機能のアップデートを管理し、前回のアップデートをロールバックすることができます：
  - **定義データベースと製品機能のアップデート**
  - **前回のアップデートのロールバック**
  - **製品アップデート**

  フォルダーには、すべてのカスタムタスクと、Kaspersky Security Center を使用して作成され、保護対象デバイスに送信されたグループアップデートタスクが表示されます。

- **保管領域**：バックアップ設定とブロック対象のネットワークセッションのリストを管理します。
  - **バックアップ**
  - **ブロック対象のネットワークセッション**
- **ログと通知**：ローカルタスクのログと Kaspersky Embedded Systems Security のシステム監査ログを管理します。
  - **システム監査**
  - **アプリケーション起動コントロール**
  - **デバイスコントロール**
  - **アプリケーション整合性コントロール**
  - **Windows イベントログ監視**
  - **システム変更監視**
  - **ネットワーク脅威対策**
  - **オンデマンドスキャン**
  - **ファイアウォール**
  - **脆弱性攻撃ブロック**
  - **ふるまい検知**
  - **AMSI スキャナー**
  - **アップデート**
  - **ファイルのリアルタイム保護**
  - **バックアップ**
- **ライセンス**：Kaspersky Embedded Systems Security のライセンスを追加または削除し、ライセンスの詳細を表示します。

## 詳細ペイン

詳細ペインに、選択したフォルダーの情報が表示されます。［**Kaspersky Embedded Systems Security**］フォルダーを選択した場合、詳細ペインには現在のデバイスの保護ステータスに関する情報と、Kaspersky Embedded Systems Security の機能コンポーネントの保護ステータス、およびライセンス情報ファイルのステータスに関する情報が表示されます。

## ［Kaspersky Embedded Systems Security］フォルダーのコンテキストメニュー

［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューの項目を使用して実行可能な操作は次の通りです：

- **保護機能を一時停止する**
- **信頼ゾーンの設定**：信頼ゾーンの設定を表示および編集します。
- **リムーバブルドライブスキャン**：USB ポートを介して保護対象デバイスに接続されているリムーバブルドライブのスキャンを設定します。
- **アプリケーション管理用のユーザーアクセス権限**：Kaspersky Embedded Systems Security の各種機能にアクセスするための権限を確認および設定します。
- **Kaspersky Security サービス管理用のユーザーアクセス権限**：Kaspersky Security サービスを管理するユーザー権限を確認および設定します。
- **保管領域**
- **設定のエクスポート**：アプリケーション設定を XML 形式で設定情報ファイルに保存します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。
- **設定のインポート**：XML 形式の設定情報ファイルからアプリケーション設定をインポートします。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。
- **更新**：Kaspersky Embedded Systems Security コンソールのウィンドウの内容を更新します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。
- **アプリケーションのプロパティ**：Kaspersky Embedded Systems Security または選択したタスクを表示および設定します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。

  そのために、［Kaspersky Embedded Systems Security］フォルダーの詳細ペインにある［**アプリケーションのプロパティ**］を使用することもできます。

- **ヘルプ**：Kaspersky Embedded Systems Security ヘルプの情報を表示します。この操作は、アプリケーションタスクのコンテキストメニューで実行することもできます。

## Kaspersky Embedded Systems Security タスクのツールバーとコンテキストメニュー

Kaspersky Embedded Systems Security コンソールツリー内の各タスクのコンテキストメニューの項目を使用して、アプリケーションタスクを管理できます。

コンテキストメニューの項目を使用して次の操作を実行できます：

- **再開 / 一時停止**：タスクの実行を再開または一時停止します。この操作を実行するために、ツールバーのボタンを使用できます。この操作は、リアルタイム保護タスクおよびオンデマンドスキャンタスクで使用できます。
- **タスクの作成**：新しいカスタムタスクを作成します。
- **タスクの削除**：カスタムタスクを削除します。

- **設定のエクスポート / 設定のインポート**：タスク設定をエクスポートまたはインポートします。
- **プロパティ**：タスク設定ウィンドウを開きます。
- **ヘルプ**：対応するオンラインヘルプのトピックを開きます。

# 通知領域のシステムトレイアイコン

Kaspersky Embedded Systems Security をインストールするとすぐに、Microsoft Windows タスクバーの通知領域に製品アイコンが表示されます。

タスクバーの通知領域の製品アイコンが非表示になっている場合、管理者は、ポリシーで製品のインターフェイスの表示をオフにしています。

このアイコンは、次の目的で表示されます：

- 製品の動作を表示する
- 製品のコンテキストメニューおよびメインウィンドウへのショートカットを提供する

製品の動作に関する情報をユーザーが確認できるように、製品ステータスに応じて次のアイコンが表示されます：

- アイコンは、製品の非常に重要な保護機能が有効であることを示しています。本製品のアップデート後に再起動が必要な場合など、ユーザーが操作を実行する必要がある場合は警告アイコン（）が表示されます。
- アイコンは、製品の非常に重要な保護機能が無効になっているか、不具合があることを示しています。例えば、ライセンスの有効期間が終了していたり、アプリケーションエラーの結果として保護機能の不具合となることがあります。コンピューターの保護の問題についての説明とともに警告アイコン（）が表示されます。

システムトレイアイコンを右クリックすると、コンテキストメニューが開きます。

コンテキストメニューには、製品ウィンドウを表示するいくつかのコマンドが表示されます（以下の表を参照）。

システムトレイアイコン内のコンテキストメニューのコマンド

| コマンド | 説明 |
|---|---|
| **アプリケーションコンソールを開く** | Kaspersky Embedded Systems Security コンソールを開きます（インストールされている場合）。 |
| **コンパクト診断インターフェイスを開く** | ［コンパクト診断インターフェイス］を開きます。 |
| **製品情報** | Kaspersky Embedded Systems Security に関する情報を含む［**製品情報**］ウィンドウを開きます。<br>登録済みの Kaspersky Embedded Systems Security ユーザーの場合、［**製品情報**］ウィンドウには、インストールされている緊急アップデートに関する情報が表示されます。 |
| **非表示にする** | ツールバー通知領域のシステムトレイアイコンを非表示にします。 |

非表示のシステムトレイアイコンは、いつでも表示できます。

*システムトレイアイコンを再び表示するには、*

Microsoft Windows の［**スタート**］メニューから、［**すべてのプログラム**］→［**Kaspersky Embedded Systems Security**］の順に選択します。アイコンが Microsoft Windows タスクバーの通知領域に表示されます。

インストールされているオペレーティングシステムによって、設定名が異なる場合があります。

# アプリケーションコンソールを使用した全般設定

Kaspersky Embedded Systems Security の全般設定とトラブルシューティングの設定では、本製品の全般的な動作の条件を設定します。これらの設定では、Kaspersky Embedded Systems Security で使用される処理対象プロセスの数を制御したり、異常終了後に Kaspersky Embedded Systems Security のタスクを復元できるようにしたり、ログを維持したり、異常終了時に Kaspersky Embedded Systems Security のダンプファイルを作成できるようにしたり、その他の全般的な設定を行ったりすることができます。

Kaspersky Security Center アクティブポリシーによってこれらの設定への変更がブロックされている場合、Kaspersky Embedded Systems Security コンソールではアプリケーションの設定を実行できません。

*Kaspersky Embedded Systems Security の全般設定を指定するには：*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、次のいずれかを行います：
   - フォルダーの結果ペインで、［**アプリケーションのプロパティ**］をクリックします。
   - フォルダーのコンテキストメニューで［**アプリケーションのプロパティ**］を選択します。

   ［**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。
2. ［**インターフェイス**］タブでは、Kaspersky Embedded Systems Security システムトレイアイコンに表示する警告を指定します。
3. ［**セキュリティ設定**］タブで、次の設定を行います：
   - ［**全般**］セクションで、［**コンピューターの開始時に本製品を開始する（推奨）**］を設定します。
   - ［**セルフディフェンス**］で、製品モジュールとオペレーティングシステムのサービスの保護を設定します。
   - ［**UPS 電源への切り替え時の処理**］セクションで、UPS 電源への切り替え後における、Kaspersky Embedded Systems Security による保護対象デバイスの負荷に対する制限を指定できます：
     - **スケジュール設定済みのスキャンタスクを開始しない**
     - **スキャンタスクの実行を中止する**

- ［**互換性設定**］セクションで、［**リモート管理ソフトウェアとの互換性**］を設定します：

  Kaspersky Embedded Systems Security をリモート管理ツール（RAT）と一緒に使用すると問題が発生する場合は、互換性モードを有効にすることができます。この問題は、RAT と製品のセキュアデスクトップ機能に互換性がないことに関連して生じる可能性があります。この機能の目的は、コンピューターのセキュリティレベルを低下させる可能性のある処理を確認することです。この機能により、アプリケーションで他のプロセスから分離された確認ダイアログを表示することができます。この機能では昇格した権限を使用してリクエストの安全を確保します。こうすることで、マルウェアではなくユーザーだけが処理を確認できるようになります。

  このチェックボックスをオンにすると、RAT 互換性モードが有効になります。この機能を使用しない場合、アプリケーションは確認ダイアログを表示します。これは、コンピューターのセキュリティレベルを低下させる可能性があります。Kaspersky Embedded Systems Security と RAT で問題が発生していない場合、互換性モードを有効にすることは推奨しません。

  このチェックボックスをオフにすると、RAT 互換性モードは無効になります。既定では、このチェックボックスはオフです。

  例：ブラウザーを RemoteApp モードで使用している場合、信頼されていない証明書を使用する Web サイトにアクセスしたときに確認ウィンドウが表示されないことがあります。これは、RemoteApp が本製品のセキュアデスクトップ機能をサポートしていないためです。これにより、ブラウザーが応答しなくなることがあります。RemoteApp モードでブラウザーを正しく動作させるには、互換性モードを有効にする必要があります。

  他のサードパーティ製ソフトウェアを使用しているときにセキュアデスクトップ機能に問題が発生した場合にも、互換性モードを有効にしてみることができます。

- ［**スキャンの設定**］セクションで、**スキャンタスクの CPU 使用率の制限**を設定し、他のアプリケーションにシステムリソースを優先的に割り当てることを許可します。

  オンデマンドスキャンタスクでの保護対象デバイスの CPU の使用が、［**上限**］フィールドで指定した値に制限されます。

  > ただし、他のコンポーネントによって、より多くの CPU 時間が使用される場合があります。

  この機能を有効にすることで、Kaspersky Embedded Systems Security のパフォーマンスに悪影響を与える可能性があります。

  既定では、この機能は無効になっています。

4. ［**ネットワークの設定**］タブで、次の設定を行います：

   - ［**プロキシサーバー**］セクションで、プロキシサーバー設定（プロキシサーバーでの認証に必要な認証種別と詳細）を指定します。

   - 必要に応じて、［**リモート接続用ポート**］で、アプリケーションコンソールが製品をインストールしたコンピューターに接続する際に使用するポートを変更します。

     Windows 資格情報による接続の既定のポート番号は 13032 で、手動で作成されたユーザーの資格情報による接続の既定のポート番号は 13031 です。指定可能なポートの番号の範囲：1 ～ 65535。

     > 本製品が再起動されるまで、以前に保存されたポート番号が使用されます。

5. ［**誤作動診断**］タブで、［**設定**］をクリックして、本製品の**トレース**と**メモリダンプを設定**します。

1. ［**アプリケーションダンプの設定**］タブを選択します。
2. ［**ダンプファイルの作成**］をオンまたはオフにして、誤動作が発生した場合のメモリダンプを有効または無効にします。

   既定では、メモリダンプファイルは %ProgramData%\Kaspersky Lab\KESS.4.0\Traces のフォルダーに保存されます。別のパスを指定することもできます。

［**トレースファイル用フォルダー**］フィールドには、Kaspersky Embedded Systems Security が既定でトレースファイルを保存するローカルフォルダーへの完全パスが含まれます。別のパスを指定することもできます。

1. ［**詳細レベル**］ドロップダウンリストから、デバッグ情報の詳細レベルを選択します：

   - **緊急**：トレースファイルには、深刻なエラーに関するメッセージのみが保存されます。
   - **診断**：トレースファイルには、すべてのエラーと警告に関するメッセージが保存されます。
   - **重要**：トレースファイルには、すべてのエラー、警告、および追加情報に関するメッセージが保存されます。
   - **通常**：トレースファイルには、すべてのエラー、警告、および本製品の通常の処理に関する情報に関するメッセージが保存されます（既定）。
   - **詳細**：トレースファイルには、本製品の処理に関するすべての情報が保存されます。

   発生した問題を解決するために必要な詳細レベルは、テクニカルサポートが判断します。

   既定の詳細レベルは、［**通常**］に設定されています。

2. **トレースファイルの最大サイズ（MB）**を指定します。

   使用可能な値：1～4095 MB。既定では、トレースファイルの最大サイズは 100 MB に設定されています。

3. ファイルの最大数に達した時に古いトレースファイルを削除するには、［**古いトレースファイルを削除する**］をオンにします。

4. **トレースログあたりの最大ファイル数**を指定します。

   使用可能な値：1～999。既定では、ファイルの最大数は 5 に設定されています。このフィールドは、［**古いトレースファイルを削除する**］をオンにした場合に使用できます。

Kaspersky Embedded Systems Security では、暗号化されていない形式でトレースファイルとダンプファイルに情報を書き込みます。ファイルが保存されるフォルダーは、オペレーティングシステムの設定と Kaspersky Embedded Systems Security の設定によって管理されます。アクセス権限を設定して、必要なユーザーのみにログやトレースファイル、ダンプファイルへのアクセスを許可することができます。

6. ［**OK**］をクリックします。

Kaspersky Embedded Systems Security 設定が保存されます。

# Kaspersky Embedded Systems Security タスクの管理

このセクションでは、Kaspersky Embedded Systems Security のタスクの作成、設定、開始および停止について説明します。

# Kaspersky Embedded Systems Security タスクのカテゴリ

Kaspersky Embedded Systems Security のコンピューターのリアルタイム保護、コンピューターコントロール、ルールの自動生成、システム監査、オンデマンドスキャン、産業用ネットワーク保護、保管領域の管理、およびアップデートの各機能は、タスクとして実装されます。

これらのタスクは、Kaspersky Embedded Systems Security コンソールツリーのタスクコンテキストメニューと、結果ペインを使用して管理できます。結果ペインで、タスクのステータス情報を表示できます。タスク管理操作は、システム監査ログに記録されます。

Kaspersky Embedded Systems Security のタスクには、*ローカル*と*グループ*の 2 つの種別があります。

## ローカルタスク

ローカルタスクは、作成された保護対象デバイスでのみ実行されます。開始方法に応じて、次の種別のローカルタスクがあります：

- **ローカルのシステムタスク**：これらは Kaspersky Embedded Systems Security のインストール時に自動的に作成されます。*アップデートのロールバック*タスクを除くすべてのローカルシステムタスクの設定を変更できます。ローカルシステムタスクは、名前を変更したり削除したりできません。ローカルのシステムオンデマンドスキャンタスクとカスタムオンデマンドスキャンタスクは同時に実行できます。

- **ローカルのカスタムタスク**：アプリケーションコンソールでは、オンデマンドスキャンタスク、アップデートタスク、ベースラインシステム変更監視タスクを作成できます。Kaspersky Security Center では、オンデマンドスキャンタスク、アップデートタスクなどを作成できます。カスタムタスクの名前変更、設定、削除が可能です。いくつかのカスタムタスクを同時に実行することもできます。

## グループタスク

Kaspersky Security Centerからグループタスクと保護対象デバイスのセットのタスクを管理できます。すべてのグループタスクはカスタムタスクです。グループタスクは、アプリケーションコンソールにも表示されます。アプリケーションコンソールでは、グループタスクのステータスの表示のみができます。アプリケーションコンソールを使用して、グループタスクを管理または構成することはできません。

# 手動でのタスクの開始、一時停止、再開、停止

タスクを手動で開始、一時停止、再開、または停止できます。これらのオプションは、すべての Kaspersky Embedded Systems Security タスクで使用できるわけではありません。

*タスクの開始、一時停止、再開、停止を行うには：*

1. アプリケーションコンソールで、タスクのコンテキストメニューを開きます。
2. ［**起動**］または［**一時停止**］のコマンドを選択します。

操作が実行され、システム監査ログに記録されます。

# タスクスケジュールの管理

Kaspersky Embedded Systems Security のタスクにスケジュールを設定できます。

## タスクスケジュールの設定

アプリケーションコンソールでは、ローカルのシステムおよびカスタムタスクを開始するスケジュールを設定できます。ただし、グループタスクの開始のスケジュールを設定することはできません。

*タスクのスケジュールを設定するには：*

1. コンソールツリーで、スケジュールを設定するタスクを選択します。
2. 結果ペインで、［**実行方法**］または［**プロパティ**］をクリックします。
3. ［**実行方法**］セクションで、［**スケジュールで指定**］を選択します。
4. スケジュールを設定するには、次の手順に従います。
   a. ［**頻度**］ドロップダウンリストから、次のいずれかを選択します：
      - **分ごと**：タスクを数分ごとに定期的に実行する場合に選択します。［**実行間隔 <数値> 分ごと**］フィールドに分数を入力します。
      - **時間ごと**：タスクを数時間ごとに定期的に実行する場合に選択します。［**実行間隔 <数値> 時間**］フィールドに時間数を入力します。
      - **日ごと**：タスクを数日ごとに定期的に実行する場合に選択します。［**実行間隔 <数値> 日ごと**］フィールドに日数を入力します。
      - **指定した時刻**：指定した日時にタスクを1回実行する場合に選択します。
      - **毎月**：タスクを毎月実行する場合に選択します。タスクを実行する日と時刻を指定します（既定では、タスクは毎月1日に実行されます）。
      - ［**本製品の起動後**］：Kaspersky Embedded Systems Security が起動するたびにタスクを実行します。
   b. 最初のステップでオンにしたオプションに応じて、タスクの最初の開始の期間または日時を指定します。

c. 本製品を起動してからタスクを実行するまでの遅らせる時間を指定することもできます。

d. タスクを実行するためのログインとパスワードを指定します。

5. ［**OK**］をクリックします。

タスクのスケジュール設定が保存されます。

## スケジュールに従ったタスクの有効化と無効化

スケジュール設定を行う前、または行った後で、スケジュールに従ったタスクを有効または無効にできます。

*スケジュールに従ったタスクの開始を有効または無効にするには：*

1. アプリケーションコンソールツリーで必要なタスクを選択します。
2. 結果ペインで、［**実行方法**］をクリックします。
   ［**スケジュールと実行方法**］ウィンドウが表示されます。
3. 表示されたウィンドウの［**実行方法**］セクションで、次のいずれかの処理を実行します：
   - スケジュール設定されたタスクの開始を無効にする場合は、［**手動**］をオンにします。
   - スケジュール設定されたタスクの開始を有効にする場合は、［**スケジュールで指定**］をオンにします。
4. ［**OK**］をクリックします。

タスクのスケジュール設定が保存されます。

# タスクを開始するユーザーアカウントの使用

システムアカウントを使用してタスクを開始することも、別のアカウントを指定することもできます。

## タスク実行用のアカウントについて

アカウントを指定して、次の Kaspersky Embedded Systems Security タスクを実行することができます：

- アプリケーション起動コントロールルールの自動生成
- デバイスコントロールルールの自動生成
- Windows イベントログ監視
- アプリケーション整合性チェック
- 定義データベースと製品機能のアップデート
- アップデート

既定では、これらのタスクはシステムアカウントの権限で実行されます。

次の場合は、適切なアクセス権限を持つ異なるアカウントを指定してください：

- **アップデート**タスク：アップデート元としてネットワーク内の別のデバイス上の共有フォルダーを指定した場合
- **アップデート**タスク：Windows NTLM 認証が組み込まれたプロキシサーバーを使用してアップデート元にアクセスする場合
- **アプリケーション起動コントロールルールの自動生成** タスク：システムアカウントがアクセスできない設定情報ファイルに生成されたルールがエクスポートされた場合（例：保護対象デバイスの共有フォルダーなど）

リストされたタスクは、システムアカウントの権限で開始できます。ネットワーク上の別のデバイスが保護対象デバイスと同じドメインに登録されている場合、Kaspersky Embedded Systems Security は、これらのタスクを実行し、このデバイスの共有フォルダーにアクセスします。この場合、システムアカウントには、これらのフォルダーへのアクセス権限が必要です。Kaspersky Embedded Systems Security が **<ドメイン名 \ デバイス名>** アカウントの権限を使用してデバイスにアクセスします。

## タスクを実行するユーザーアカウントの指定

アプリケーションコンソールでアカウントを指定するオプションは、すべてのタスクで使用できるわけではありません。

*タスクを実行するアカウントを指定するには：*

1. アプリケーションコンソールツリーで、特定のアカウントの権限で開始するタスクを選択します。
2. 結果ペインで、［**実行方法**］をクリックします。
   ［**スケジュールと実行方法**］ウィンドウが表示されます。
3. 表示されたウィンドウの［**ユーザー**］セクションで、次の操作を行います：
   a. ［**他のユーザーでタスクを実行する**］を選択します。
   b. 使用するアカウントのユーザー名とパスワードを入力します。

   選択したユーザーは、保護対象デバイスまたはそのデバイスと同じドメイン内に登録されている必要があります。
4. ［**OK**］をクリックします。

変更された設定が保存されます。

# 設定のインポートとエクスポート

このセクションでは、Kaspersky Embedded Systems Security の設定をエクスポートする方法について説明します。また、特定の製品コンポーネントの設定を XML 設定情報ファイルにエクスポートする方法、それらの設定を製品設定にインポートする方法についても説明します。

## 設定のインポートとエクスポートについて

Kaspersky Embedded Systems Security の設定を XML 設定ファイルにエクスポートしたり、設定ファイルから Kaspersky Embedded Systems Security に設定をインポートしたりすることができます。設定ファイルには、すべてのアプリケーション設定または個別のコンポーネント設定のみを保存できます。

Kaspersky Embedded Systems Security のすべての設定をファイルにエクスポートする場合、アプリケーションの全般設定と、次の Kaspersky Security コンポーネントと機能の設定が保存されます：

- ファイルのリアルタイム保護
- 脆弱性攻撃ブロック
- ネットワーク脅威対策
- ふるまい検知
- 修復エンジン
- AMSI スキャナー
- アプリケーション起動コントロール
- デバイスコントロール
- ファイアウォール
- アプリケーション起動コントロールルールの自動生成
- デバイスコントロールルールの自動生成
- Windows イベントログ監視
- システム変更監視
- 簡易スキャン
- アプリケーション整合性チェック
- リムーバブルドライブスキャン
- 完全スキャン
- 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

- 前回のアップデートのロールバック
- アップデート

これらに加えて、Kaspersky Embedded Systems Security の全般設定とユーザーアカウントの権限をファイルに保存できます。

グループタスクの設定はエクスポートできません。

Kaspersky Embedded Systems Security は、タスクを実行したりプロキシサーバーに接続したりするユーザーアカウントの設定など、製品が使用するすべてのパスワードをエクスポートします。エクスポートしたパスワードは、暗号化された形式で設定情報ファイルに保存されます。再インストールまたはアップデートされていない場合、この保護対象デバイスにインストールされた Kaspersky Embedded Systems Security を使用することでのみ、パスワードをインポートできます。

別の保護対象デバイスにインストールされた Kaspersky Embedded Systems Security を使用して以前保存されたパスワードはインポートできません。保護対象デバイスに設定がインポートされた後で、すべてのパスワードを手動で入力する必要があります。

Kaspersky Security Center のポリシーがエクスポート時にアクティブである場合、そのポリシーによって使用される設定値がエクスポートされます。

Kaspersky Embedded Systems Security の個々のコンポーネントのパラメータを含む設定情報ファイルから（たとえば、インストールされた Kaspersky Embedded Systems Security で作成された、コンポーネントの一部を含むファイルから）、設定をインポートできます。設定をインポートすると、設定情報ファイルに含まれていた Kaspersky Embedded Systems Security の設定のみが変更されます。その他の設定は同じです。

ブロックされた Kaspersky Security Center のアクティブポリシーの設定は、設定のインポート時には変更されません。

## 設定のエクスポート

*設定情報ファイルに設定をエクスポートするには：*

1. Kaspersky Embedded Systems Security のすべての設定をエクスポートするには、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューで、［**設定のエクスポート**］コマンドを選択します。

   個々のコンポーネントの設定をエクスポートするには、結果ペインの［**設定のエクスポート**］をクリックします。

   Kaspersky Security Network の設定はエクスポートできません。Kaspersky Security Network は手動で設定する必要があります。

2. 表示されたウィンドウで、設定のリストをエクスポートする XML 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。

   パスを指定する際にシステム環境変数を使用できますが、ユーザー環境変数は使用できません。

   Kaspersky Security Center のポリシーがエクスポート時にアクティブである場合、そのポリシーによって使用される設定がエクスポートされます。

3. ファイルを保存します。

4. ［**設定のエクスポートが完了しました**］ウィンドウの［**OK**］をクリックします。

   Kaspersky Embedded Systems Security は、設定のリストを XML ファイルにエクスポートします。

*信頼するアプリケーションのリストをエクスポートするには：*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューを開きます。

2. ［**信頼ゾーンの設定**］を選択します。

3. ［**信頼ゾーンの設定**］ウィンドウが表示されます。

4. ［**信頼するアプリケーション**］セクションに移動し、［**設定**］をクリックします。

   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. エクスポート対象の信頼するアプリケーションを選択します。

   信頼するアプリケーションが何も選択されていない場合、すべての信頼するアプリケーションがエクスポートされます。

6. 矢印をクリックし、ドロップダウンリストから［**エクスポート**］を選択します。

7. 表示されたウィンドウで、信頼するアプリケーションのリストをエクスポートする XML 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。

8. ファイルを保存します。

   Kaspersky Embedded Systems Security は、信頼するアプリケーションのリストを XML ファイルにエクスポートします。

## 設定のインポート

*保存された設定情報ファイルから設定をインポートするには：*

1. Kaspersky Embedded Systems Security のすべての設定をインポートするには、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューで、［**設定のインポート**］コマンドを選択します。

   個々のコンポーネントの設定をインポートするには、結果ペインの［**設定のインポート**］をクリックします。

   Kaspersky Embedded Systems Security の設定またはその機能コンポーネントの全般設定を保護対象デバイス上にインポートした後は、以前の設定に戻すことはできません。

   Kaspersky Security Network の設定をインポートできません。Kaspersky Security Network は手動で設定する必要があります。

2. 表示されたウィンドウで、設定をインポートする XML 設定情報ファイルを選択し、［**開く**］をクリックします。

3. ［**設定のインポートが完了しました**］ウィンドウの［**OK**］をクリックします。

4. アプリケーションコンソールのツールバーで、［**アップデート**］をクリックします。

   アプリケーションコンソールウィンドウに、インポートされた設定が表示されます。

Kaspersky Embedded Systems Security が再インストールまたは更新されたのとは別の保護対象デバイスまたは同じ保護対象デバイスで作成されたファイルからパスワード（タスクの実行またはプロキシサーバーへの接続に使用されるアカウントの認証情報）がインポートされることはありません。インポートが完了したら、パスワードを手動で入力する必要があります。

*信頼するアプリケーションのリストをインポートするには：*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューを開きます。

2. ［**信頼ゾーンの設定**］を選択します。

3. ［**信頼ゾーンの設定**］ウィンドウが表示されます。

4. ［**信頼するアプリケーション**］セクションに移動し、［**設定**］をクリックします。

5. 矢印をクリックし、ドロップダウンリストから［**インポート**］を選択します。

6. 表示されたウィンドウで、信頼するアプリケーションのリストをインポートする XML ファイルを選択します。

7. ファイルを開きます。

   コンピューターに信頼するアプリケーションのリストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

8. リストは［**信頼するアプリケーション**］タブに表示されます。［**OK**］をクリックします。

# 保護ステータスと Kaspersky Embedded Systems Security の情報の表示

*Kaspersky Embedded Systems Security のデバイス保護ステータスに関する情報を表示するには：*

Kaspersky Embedded Systems Security コンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択します。

既定では、Kaspersky Embedded Systems Security コンソールの詳細ペインの情報は自動的に更新されます：

- ローカル接続の場合は 10 秒ごと
- リモート接続の場合は 15 秒ごと

情報を手動で更新できます。

*［**Kaspersky Embedded Systems Security**］フォルダーの情報を手動で更新するには：*

［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューで［**更新**］コマンドを選択します。

Kaspersky Embedded Systems Security コンソールの詳細ペインに、以下の製品情報が表示されます：

- Kaspersky Security Network の使用のステータス。
- デバイスの保護のステータス。
- 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情報。
- 実際の診断データ。
- 保護対象デバイスコントロールタスクに関するデータ。
- ライセンスの情報。
- Kaspersky Security Center との連携のステータス：アプリケーションの接続先になっている Kaspersky Security Center がインストールされているサーバーの詳細、アクティブなポリシーによって制御されるアプリケーションタスクの情報が表示されます。

保護ステータスを表示するために、色分けが使用されます。

- *緑色*：タスクは設定に従い実行されています。保護は有効です。
- *黄色*：タスクが開始されなかったか、一時停止または停止されました。セキュリティの脅威が発生する可能性があります。タスクを設定し、開始してください。
- *赤色*：エラーが発生した状態でタスクが終了したか、タスクの実行中に深刻な脅威が検知されました。タスクを開始するか、検知されたセキュリティの脅威を除去するための措置を取ってください。

このブロックの詳細にはリンクになっているものもあり（タスク名、検知された脅威の数など）、クリックすると、関連するタスクのフォルダーに移動したりタスク実行ログが開いたりします。

［**KSN の使用**］セクションには、「*実行中*」、「*停止済み*」、「*一度も実行されていません*」など、現在のタスクのステータスが表示されます。インジケーターでは、次の値が使用されます：

- パネルの色が緑色 - **KSN の使用**タスクが実行中であり、ステータスのファイル要求を KSN に送信中であることを示します。
- パネルの色が黄色 - 声明の 1 つが同意されたがタスクが実行中でないか、タスクは実行されているがファイル要求は KSN に送信されていないことを示します。
- パネルの色が赤色 - タスクは失敗しました。

## コンピューター保護

［**コンピューター保護**］セクション（下の表を参照）には、デバイスの最新の保護の状態に関する情報が表示されます。

デバイスの保護ステータスに関する情報

| セクション | 情報 |
| --- | --- |
| **デバイス保護ステータスのインジケーター** | セクションの名前が表示されたパネルの色は、セクションで実行中のタスクのステータスを反映します。インジケーターでは、次の値が使用されます：<br>• パネルの色が緑色 - この色は既定で表示されます。ファイルのリアルタイム保護コンポーネントがインストールされ、タスクが実行中であることを示します。<br>• パネルの色が黄色 - ファイルのリアルタイム保護コンポーネントがインストールされておらず、*簡易スキャン*タスクが長期間実行されていないことを示します。<br>• パネルの色が赤色 - ファイルのリアルタイム保護タスクは実行されていません。 |
| **ファイルのリアルタイム保護** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。 |
| **簡易スキャン** | **前回のスキャン実行日** - ウイルスおよびその他のコンピューターセキュリティ脅威に対する前回の簡易スキャンの日時。<br>*一度も実行されていません* - *簡易スキャン*タスクが過去 30 日以上実行されていない場合に発生するイベント（既定値）。このイベントが生成されるしきい値は変更可能です。 |
| **ネットワーク脅威対策** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。 |
| **脆弱性攻撃ブロック** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。<br>**操作モード** - 脆弱性攻撃ブロックタスクで使用可能な 2 つのモードのうちの 1 つ（［**ブロックする**］または［**通知する**］）。 |
| **ふるまい検知** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。<br>**操作モード** - ふるまい検知タスクで使用可能な 3 つのモードのうちの 1 つ（［**削除する**］、［**ブロックする**］、または［**通知する**］）。 |

## アップデート

［**アップデート**］セクション（下の表を参照）には、最新の定義データベースとソフトウェアモジュールの状態に関する情報が表示されます。

Kaspersky Embedded Systems Security の定義データベースとモジュールのステータスに関する情報

| セクション | 情報 |
| --- | --- |
| **定義データベースと製品機能のステータスインジケーター** | セクションの名前が表示されたパネルの色は、定義データベースと製品機能のステータスを反映します。インジケーターでは、次の値が使用されます：<br>• パネルの色が緑色 - この色は既定で表示されます。定義データベースが最新で、前回の定義データベースと製品機能のアップデートタスクが正常に完了したことを示します。<br>• パネルの色が黄色 - 定義データベースがアップデートされていないか、前回の定義データベースと製品機能のアップデートタスクが失敗したことを示します。<br>• パネルの色が赤色 - ［*定義データベースが長期間アップデートされていません*］イベントまたは［*定義データベースは最新です*］イベントが発生しました。 |
| **定義データベースのアップデート** | **データベースの状態** - 定義データベースのアップデートステータスの評価。<br>オプションとして、次の値が使用されます：<br>• **定義データベースは最新です** - 定義データベースが 7 日以内（既定）にアップデートされています。<br>• **定義データベースがアップデートされていません** - 定義データベースが 7 ～ 14 日前（既定）にアップデートされています。<br>• **定義データベースが長期間アップデートされていません** - 定義データベースが 14 日以内（既定）にアップデートされていません。<br>［*定義データベースがアップデートされていません*］イベントと［*定義データベースが長期間アップデートされていません*］イベントが生成されるしきい値は変更可能です。<br>**定義データベースの公開日時** - 最新の定義データベースのアップデートが公開された日時。日時は UTC 形式で指定されます。<br>**前回完了した定義データベースのアップデートタスクの状態** - 最新の定義データベースのアップデートの日時。日時は、保護対象デバイスのローカル時刻に基づいて指定されます。このフィールドの値は、［*失敗*］イベントが発生すると赤色になります。 |

## コントロール

［**コントロール**］セクション（下の表を参照）には、アプリケーション起動コントロール、デバイスコントロール、およびファイアウォールタスクに関する情報が表示されます。

保護対象デバイスコントロールのステータスに関する情報

| セクション | 情報 |
| --- | --- |
| **保護対象デバイスコントロールのステータスインジケーター** | セクションの名前が表示されたパネルの色は、セクションで実行中のタスクのステータスを反映します。インジケーターでは、次の値が使用されます：<br>• パネルの色が緑色 - 既定で表示されます。すべてのアプリケーション起動コントロールコンポーネントがインストールされ、タスクがアクティブモードで実行中であり、脆弱性攻撃ブロック機能がインストールされてアクティブであることを示します。<br>• 次のいずれかの条件に1つでも当てはまる場合、パネルは黄色で表示されます：脆弱性攻撃ブロックが実行されていないこと、アプリケーション起動コントロールが通知モードで実行されていること、脆弱性攻撃ブロックがアクティブモードで実行されており、アプリケーション起動コントロールが実行されていないか失敗したこと。<br>• パネルの色が赤色 - アプリケーション起動コントロールタスクが実行されていないか失敗しており、脆弱性攻撃ブロックが実行されていないか［**通知する**］モードで実行されている。 |
| **アプリケーション起動コントロール** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。<br>**操作モード** - アプリケーション起動コントロールタスクで使用可能な 2 つのモードのうちの1つ（［**$EntAppControl_OperatingMode_Active**］または［**$EntAppControl_OperatingMode_StatisticsOnly**］）。 |
| **デバイスコントロール** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。<br>**操作モード** - デバイスコントロールタスクで使用可能な 2 つのモードのうちの1つ（［**ルールに準拠**］または［**通知する**］）。 |
| **ファイアウォール** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。 |

## 診断

［**診断**］セクション（下の表を参照）には、ファイル変更監視および Windows イベントログ監視タスクに関する情報が表示されます。

システム監査ステータスに関する情報

| セクション | 情報 |
| --- | --- |
| **診断ステータスのインジケーター** | セクションの名前が表示されたパネルの色は、セクションで実行中のタスクのステータスを反映します。インジケーターでは、次の値が使用されます：<br>• 緑色 - 既定で表示されます。システム監査コンポーネントの1つまたは両方がインストールされ、タスクが実行中であることを示します。<br>• 黄色 - 両方のコンポーネントがインストールされていますが、システム監査タスクの1つが実行されておらず、［*実行されていません*］イベントが発生したことを示します。<br>• 赤色 - タスクの1つが失敗したことを示します。 |
| **システム変更監視** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。 |
| **Windows イベントログ監視** | **ステータス** - 現在のコンポーネントのステータス（「*実行中*」や「*無効*」など）。 |

Kaspersky Embedded Systems Security のライセンスに関する情報は、［**Kaspersky Embedded Systems Security**］フォルダーの詳細ペインの左下隅にある行に表示されます。

Kaspersky Embedded Systems Security のプロパティを設定するには、［アプリケーションのプロパティ］をクリックします。

別の保護対象デバイスを接続するには、［リモートコンピューターに接続］をクリックします。

# Web コンソールおよび Cloud コンソールからの Web プラグインの操作

このセクションでは、Web コンソールに対応した Kaspersky Embedded Systems Security 管理プラグインについての情報を提供するとともに、保護対象デバイスまたは保護対象デバイスのグループにインストールされているアプリケーションコンソールを管理する方法について説明します。

# Web コンソールおよび Cloud コンソールを使用した Kaspersky Embedded Systems Security の管理

Kaspersky Embedded Systems Security がインストールされ、同一の管理グループに含まれた複数の保護対象デバイスを、Kaspersky Embedded Systems Security Web プラグインを使用することで一元管理できます。Kaspersky Security Center Web コンソールおよび Cloud コンソールでは、管理グループの各保護対象デバイスの操作設定を個別に設定することもできます。

*管理グループ*は、Kaspersky Security Center Web コンソールで手動で作成されます。グループには、Kaspersky Embedded Systems Security がインストールされている複数のデバイスが含まれます。それらのデバイスに対して、同一の管理や保護を設定できます。管理グループの使用の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

保護対象デバイスにインストールされている Kaspersky Embedded Systems Security の動作が Kaspersky Security Center のアクティブポリシーによって制御されている場合、単一の保護対象デバイスに対するアプリケーション設定は編集できません。

Kaspersky Security Center Web コンソールから Kaspersky Embedded Systems Security を管理するには、次の方法を実行します：

- **Kaspersky Security Center のポリシーを使用する**：Kaspersky Security Center のポリシーでは、デバイスグループに対して同一の保護をリモートで設定できます。アクティブポリシーで指定されるタスク設定は、アプリケーションコンソールでローカルで指定されるタスク設定や Kaspersky Security Center Web コンソールの保護対象デバイスのプロパティウィンドウでリモートで指定されるタスク設定よりも優先度が高いです。ポリシーを使用して、全般的なアプリケーション設定、コンピューターのリアルタイム保護タスクの設定、デバイス上の活動を管理するタスク、ネットワークストレージの保護タスクおよびスケジュールに従ってローカルシステムタスクを開始するための設定を指定できます。

- **Kaspersky Security Center のグループタスクを使用する**：Kaspersky Security Center のグループタスクでは、デバイスグループに対して、有効期限があるタスクの共通設定をリモートで編集できるようになります。グループタスクを使用して、製品をアクティベートしたり、オンデマンドスキャンタスクの設定、アップデートタスクの設定、アプリケーション起動コントロールルールの自動生成タスクの設定を編集したりできます。

- **特定のデバイスのタスクを使用する**：特定のデバイスのタスクを使用すると、どの管理グループにも属していない保護対象デバイスに対して、共通のタスク設定（実行可能な期間に制限あり）をリモートで編集できます。

- **単一のデバイスのプロパティウィンドウを使用する**：デバイスのプロパティウィンドウで、管理グループに含まれる個別の保護対象デバイスに対して、タスクをリモートで設定できます。選択した保護対象デバイスが、Kaspersky Security Center のアクティブポリシーによって制御されていない場合、アプリケーションの全般的な設定とすべての Kaspersky Embedded Systems Security タスクの設定の両方を編集できます。

Kaspersky Security Center Web コンソールおよび Cloud コンソールを使用すると、アプリケーションや高度な機能を設定し、ログや通知も利用できます。個別の保護対象デバイスだけでなく、保護対象デバイスのグループに対してもこれらの設定ができます。

# Web プラグインの制限事項

Kaspersky Embedded Systems Security Web プラグインは、Kaspersky Embedded Systems Security 管理プラグインと比較して、次の制限があります：

- アプリケーション起動コントロールタスクのルールは、デジタル証明書または Kaspersky Security Center イベントを使用して作成することはできません。

- デバイスコントロールタスクのルールを、接続されたデバイスまたはシステムデータに基づいて生成することはできません。

# アプリケーション設定の管理

このセクションでは、Kaspersky Security Center 管理コンソールを使用した Kaspersky Embedded Systems Security の全般的な設定について説明します。

# Web プラグインでの全般的なアプリケーション設定

保護対象デバイスグループまたは 1 台の保護対象デバイスに対して、Web プラグインで Kaspersky Embedded Systems Security の全般的な設定を編集できます。

## Web プラグインでのインターフェイスおよびスキャンの設定

*製品インターフェイスを設定するには：*

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

2. 設定するポリシー名をクリックします。

3. 表示される**<ポリシー名>**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. ［**本製品の設定**］セクションを選択します。

5. ［**インターフェイスの設定**］サブセクションの［**設定**］をクリックします。

6. 以下の表に、設定方法を示します。

ユーザー操作の設定とスキャンの設定

| パラメータ | 説明 |
| --- | --- |
| **ユーザーインターフェイス** | **ユーザーインターフェイスを表示しない**：クライアントコンピューター上で、Kaspersky Embedded Systems Security の動作に関するメニューなどが表示されません。Windows の通知領域のアイコンと通知も表示されません。<br>**ユーザーインターフェイスを表示する**：クライアントコンピューターでは、Windows トレイにアイコンが表示されます。アイコンのコンテキストメニューから Kaspersky Embedded Systems Security の操作を実行できます。製品アイコンの上の通知も表示されます。Windows システムトレイのアイコンのコンテキストメニューを使用すると、コンパクト診断インターフェイスを開くことができます。コンパクト診断インターフェイスのリンクをクリックすると、アプリケーションコンソールが開きます。 |
| **通知領域に製品のステータスを表示する** | Microsoft Windows の通知領域に通知を表示するイベントカテゴリの横にあるチェックボックスをオンにします。 |

# Web プラグインでのセキュリティと信頼性の設定

*手動でセキュリティ設定を行うには、次の手順を実行します：*

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

2. 設定するポリシー名をクリックします。

3. 表示される**<ポリシー名>**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. ［**本製品の設定**］セクションを選択します。

5. ［**セキュリティと信頼性**］サブセクションの［**設定**］をクリックします。

6. 以下の表に、設定方法を示します。

セキュリティと信頼性の設定

| パラメータ | 説明 |
| --- | --- |
| **コンピューターの開始時に本製品を開始する（推奨）** | チェックボックスをオンにすると、オペレーティングシステムの読み込み後に Kaspersky Embedded Systems Security が起動し、セッション中にコンピューターを保護します。<br><br>チェックボックスをオフにすると、オペレーティングシステムの読み込み後、ユーザーが手動で起動するまでは Kaspersky Embedded Systems Security が起動しません。コンピューター保護が無効になるため、ユーザーデータが脅威にさらされる可能性があります。 |
| **アプリケーションプロセスを外部の脅威から保護する** | このチェックボックスをオンにすると、Kaspersky Embedded Systems Security によってハードディスクのアプリケーションファイル、メモリプロセス、システムレジストリエントリの改竄や削除が防止されます。 |
| **オペレーティングシステムのサービスを保護する** | オペレーティングシステムのサービスの保護が有効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することはできません。<br>オペレーティングシステムのサービスの保護が無効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することができます。 |

| パラメータ | 説明 |
| --- | --- |
| **バッテリー使用中はスケジュールタスクを延期する** | このチェックボックスをオンにすると、省エネモードが有効になります。Kaspersky Embedded Systems Security がスケジュールされているタスクを延期します。必要に応じて、スキャンタスクとアップデートタスクを手動で実行できます。<br>省エネモードが有効のときは、コンピューターがバッテリーの電力で動作している場合、以下のタスクがスケジュールされていても実行されません。<br>• *定義データベースと製品機能のアップデート*<br>• *完全スキャン*<br>• *簡易スキャン*<br>• *オブジェクトスキャン*<br>• *アプリケーション整合性チェック*<br>• *IOC スキャン* |
| **設定が適用された際のコンピューターの状態** | Kaspersky Embedded Systems Security がインストールされたクライアントコンピューターについて、ポリシーの適用またはタスクの実行時にエラーが発生した場合に、Web コンソールで表示されるステータスの設定です。*OK*、*警告*および*緊急*のステータスが利用可能です。 |
| **リモート管理ソフトウェアとの互換性** | Kaspersky Embedded Systems Security をリモート管理ツール（RAT）と一緒に使用すると問題が発生する場合は、互換性モードを有効にすることができます。この問題は、RAT と製品のセキュアデスクトップ機能に互換性がないことに関連して生じる可能性があります。この機能の目的は、コンピューターのセキュリティレベルを低下させる可能性のある処理を確認することです。この機能により、アプリケーションで他のプロセスから分離された確認ダイアログを表示することができます。この機能では昇格した権限を使用してリクエストの安全を確保します。こうすることで、マルウェアではなくユーザーだけが処理を確認できるようになります。<br>このチェックボックスをオンにすると、RAT 互換性モードが有効になります。この機能を使用しない場合、アプリケーションは確認ダイアログを表示します。これは、コンピューターのセキュリティレベルを低下させる可能性があります。Kaspersky Embedded Systems Security と RAT で問題が発生していない場合、互換性モードを有効にすることは推奨しません。<br>このチェックボックスをオフにすると、RAT 互換性モードは無効になります。既定では、このチェックボックスはオフです。<br>例：ブラウザーを RemoteApp モードで使用している場合、信頼されていない証明書を使用する Web サイトにアクセスしたときに確認ウィンドウが表示されないことがあります。これは、RemoteApp が本製品のセキュアデスクトップ機能をサポートしていないためです。これにより、ブラウザーが応答しなくなることがあります。RemoteApp モードでブラウザーを正しく動作させるには、互換性モードを有効にする必要があります。<br>他のサードパーティ製ソフトウェアを使用しているときにセキュアデスクトップ機能に問題が発生した場合にも、互換性モードを有効にしてみることができます。 |
| **スキャンタスクの CPU 使用率を制限する** | オンデマンドスキャンタスクでの保護対象デバイスの CPU の使用が、［**上限**］フィールドで指定した値に制限されます。<br>ただし、他のコンポーネントによって、より多くの CPU 時間が使用される場合があります。<br>この機能を有効にすることで、Kaspersky Embedded Systems Security のパフォーマンスに悪影響を与える可能性があります。<br>既定では、この機能は無効になっています。 |
| **他のアプリケーションにシステムリソースを優先的に割り当てる** | Kaspersky Embedded Systems Security がコンピューターをスキャンする際にコンピューターのリソースを消費するため、CPU やハードディスクサブシステムの負荷が増加する可能性があります。これにより、他のアプリケーションの動作が遅くなることがあります。パフォーマンスを最適化するために、Kaspersky Embedded Systems Security には、他のアプリケーションにリソースを振り分けるモードが用意されています。このモードでは、CPU の負荷が高い場合に、オペレーティングシステムが Kaspersky Embedded Systems Security のスキャンタスクスレッドの優先度を下げることができます。これにより、オペレーティングシステムのリソースを他のアプリケーションに再分配することが可能になり、スキャンタスクの CPU 時間が減ります。その結果、Kaspersky Embedded Systems Security のスキャンに時間がかかるようになります。既定では、製品は他のアプリケーションにリソースを割り当てるように設定されています。 |

# Web プラグインでの接続設定

接続設定は、Kaspersky Embedded Systems Security がアップデートサーバーおよびアクティベーションサーバーに接続するのに使用します。また、アプリケーションを KSN サービスと連携する際にも使用します。

*接続設定を行うには、次の手順を実行します：*

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. 設定するポリシー名をクリックします。
3. 表示される**<ポリシー名>**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. ［**本製品の設定**］セクションを選択します。
5. ［**接続設定**］サブセクションの［**設定**］をクリックします。
6. 以下の表に、設定方法を示します。

接続設定

| パラメータ | 説明 |
| --- | --- |
| **従量制接続時に本製品によるデータ通信量を抑制する** | このチェックボックスをオンにすると、インターネット接続が制限されているときに本製品のネットワークトラフィックを制限します。高速モバイルインターネット接続は制限するネットワークとして、Wi-Fi 接続は無制限のネットワークとして判断されます。<br>ネットワークにかかる費用の対策は、Windows 8 以降を実行中のコンピューターで動作します。 |
| **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、Kaspersky Embedded Systems Security はプロキシサーバーを使用せずに KSN サービスに直接接続します。 |
| **プロキシサーバー設定を自動的に検出する** | このオプションをオンにすると、Kaspersky Embedded Systems Security によってプロキシサーバー設定が自動的に定義されます。 |
| **指定したプロキシサーバーを使用する** | このオプションをオンにすると、Kaspersky Embedded Systems Security は手動で指定されたプロキシサーバー設定を使用して KSN に接続します。 |
| **ローカルアドレスにはプロキシサーバーを使用しない** | このチェックボックスにより、Kaspersky Embedded Systems Security がインストールされている保護対象デバイスと同じネットワークにある保護対象デバイスに接続する際のプロキシサーバーの使用を有効または無効にします。<br>このチェックボックスをオンにすると、Kaspersky Embedded Systems Security がインストールされている保護対象デバイスをホストするネットワークから直接デバイスにアクセスします。プロキシサーバーは使用されません。<br>チェックボックスがオフの場合、ローカルデバイスに接続するためにプロキシサーバーが使用されます。<br>既定では、このチェックボックスはオンです。 |
| **プロキシサーバーの認証設定** | 認証設定を指定します。 |
| **認証を使用しない** | 認証を行いません。 |
| **NTLM 認証** | Microsoft が開発した NTLM ネットワーク認証プロトコルを使用して認証が行われます。既定では、このモードが選択されます。 |
| **ユーザー名とパスワードを指定して NTLM 認証を使用する** | 名前とパスワードを使用して、Microsoft が開発した NTLM ネットワーク認証プロトコルを通して認証が行われます。 |
| **ユーザー名とパスワード** | ユーザー名とパスワードを使用して認証が行われます。 |
| **すべてのネットワークポートを監視する** | このネットワークポート監視モードでは、保護機能はコンピューターで開いているすべてのネットワークポート経由で送信されるデータストリームを監視します。 |

| パラメータ | 説明 |
| --- | --- |
| **選択されたネットワークポートのみを監視する** | このネットワークポートの監視モードでは、コンピューターの選択したポートおよび選択したアプリケーションのネットワークの動作を監視します。メールの送信とネットワークトラフィックで通常使用されるネットワークポートのリストは、カスペルスキーの専門家の推奨に従って構成されます。 |
| **アプリケーションのアクティベーション時に Kaspersky Security Center をプロキシサーバーとして使用する** | Kaspersky Security Center がアプリケーションのアクティベーション用のプロキシサーバーとして使用されるかどうかを指定します。 |

# Web プラグインでローカルタスクのスケジュールによる開始の設定

ポリシーを使用して、ローカルシステムのオンデマンドスキャンタスクとアップデートタスクの開始を許可またはブロックできます。これは、管理グループ内の各保護対象デバイスでローカルに設定されたスケジュールに従って実行されます。

- 特定の種類のローカルシステムタスクの開始スケジュールがポリシーによって禁止される場合、これらのタスクは保護対象デバイス上でスケジュールどおりに実行されません。ローカルシステムタスクは手動で開始できます。
- 特定の種類のローカルシステムタスクの開始スケジュールがポリシーによって許可されている場合、これらのタスクは、このタスクに対してローカルに設定されたスケジュールパラメータに従って実行されます。

既定では、ローカルシステムタスクの開始はポリシーによって禁止されています。

アップデートまたはオンデマンドスキャンが Kaspersky Security Center グループタスクによって管理されている場合、ローカルシステムタスクの開始を許可しないことをお勧めします。

グループアップデートまたはオンデマンドスキャンタスクを使用しない場合は、ポリシーでローカルシステムタスクの開始を許可します。Kaspersky Embedded Systems Security は既定のスケジュールに従って定義データベースおよびモジュールのアップデートを実行し、すべてのローカルシステムのオンデマンドスキャンタスクを開始します。

ポリシーを使用して、次のローカルのシステムタスクに対するスケジュールによる開始を許可またはブロックできます：

- オンデマンドスキャンタスク：*簡易スキャン*、*オペレーティングシステムの起動時にスキャン*、*アプリケーション整合性チェック*、*ベースラインシステム変更監視*。
- アップデートタスク：定義データベースと製品機能のアップデート、 製品アップデート。

保護対象デバイスが管理グループから除外される場合、ローカルのシステムタスクのスケジュールは自動的に有効になります。

*Kaspersky Embedded Systems Security のローカルのシステムタスクのスケジュールによる開始をポリシーで許可またはブロックするには：*

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. 設定するポリシー名をクリックします。
3. 表示される**<ポリシー名>**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. ［**本製品の設定**］セクションを選択します。

5. ［**ローカルシステムタスクの実行**］サブセクションの［**設定**］をクリックします。

6. 以下の表に、設定方法を示します。

ローカルタスクを起動するための設定

| パラメータ | 説明 |
| --- | --- |
| **ローカルタスクの使用を許可する** | 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 Embedded Systems Security ローカルインターフェイスに表示されます。その他のポリシー制限がない場合、ユーザーはタスクの設定と実行ができます。ただし、ユーザーはタスク実行スケジュールを設定することはできません。ユーザーはタスクを手動でのみ実行できます。<br>チェックボックスをオフにすると、ローカルタスクの使用を停止します。このモードでは、スケジュールにのっとったローカルタスクの実行は行われません。Kaspersky Embedded Systems Security のローカルインターフェイスでタスクの開始や設定ができなくなります。また、コマンドラインの使用時にもタスクの開始や設定ができなくなります。 |
| **スケジュール管理を許可する** | このチェックボックスは、［**ローカルタスクの使用を許可する**］をオンにした場合に使用できます。<br>このチェックボックスをオンにすると、アプリケーションコンソールのローカルタスクプロパティでスケジュール管理が使用可能になります。<br>既定では、このチェックボックスはオフです。 |
| **グループタスクの表示を許可する** | このチェックボックスをオンにすると、グループタスクが Kaspersky Embedded Systems Security ローカルインターフェイスに表示されます。アプリケーションコンソールでタスクのリストを表示できます。<br>このチェックボックスをオフにすると、空白のタスクリストを表示します。 |
| **グループタスクの管理を許可する** | このチェックボックスをオンにすると、Kaspersky Security Center 内で指定されたグループタスクを開始および停止できます。ユーザーはアプリケーションコンソールまたは簡略化した製品インターフェイスでタスクを開始および停止できます。<br>このチェックボックスをオフにすると、Kaspersky Embedded Systems Security がスケジュールされたタスクを自動的に開始するか、管理者が Kaspersky Security Center で手動でタスクを開始します。 |

# Web プラグインでのバックアップ設定

Kaspersky Security Center でバックアップの全般的な設定を行うには：

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

2. 設定するポリシー名をクリックします。

3. 表示される**<ポリシー名>**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. ［**詳細設定**］セクションを選択します。

5. ［**保管領域**］サブセクションの［**設定**］をクリックします。

6. 以下の表に、設定方法を示します。

保管領域の設定

| パラメータ | 説明 |
| --- | --- |
| ［**レポート**］タブで、次のレポート設定を指定します： | |
| **保存期間** | このチェックボックスをオンにすると、レポートの最長保管期間は指定した期間に制限されます。既定の最長レポート保管期間は 30 日です。この期間を経過すると、Kaspersky Embedded Systems Security は最も古いデータをレポートファイルから自動的に削除します。 |
| **レポートファイルのサイズを制限する** | このチェックボックスをオンにすると、最大レポートファイルサイズは指定した値に制限されます。既定では、最大ファイルサイズは 1024 MB です。最大レポートファイルサイズを超過しないように、最大レポートファイルサイズに到達すると、Kaspersky Embedded Systems Security は最も古いデータをレポートファイルから自動的に削除します。 |
| ［**バックアップ**］タブで、次のバックアップ設定を指定します： | |

| パラメータ | 説明 |
| --- | --- |
| **保存期間** | 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。既定の最長ファイル保管期間は 30 日です。最大保管期間を経過すると、最も古いファイルがバックアップから削除されます。 |
| **バックアップのサイズを制限する** | 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、最大サイズは 400 MB です。保管領域の最大サイズを超過しないように、保管領域の最大サイズに到達すると、Kaspersky Embedded Systems 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。 |
| **空き容量のしきい値** | このチェックボックスにより、［バックアップ］の空き容量の下限を監視する機能を有効または無効に設定できます（既定値：100 MB）。空き容量が指定したしきい値を下回った場合、Kaspersky Embedded Systems Security により、［バックアップの空き容量がしきい値より少なくなりました］イベントが記録されて、この種別のイベントに関する通知の設定に従って通知が発行されます。<br>このチェックボックスをオンにすると、Kaspersky Embedded Systems Security により、［バックアップ］の空き容量が監視されます。<br>［**空き容量のしきい値**］は、［**バックアップのサイズを制限する**］をオンにした場合にアクティブになります。<br>既定では、このチェックボックスはオンです。 |

# ポリシーの作成と編集

このセクションでは、Kaspersky Security Center のポリシーによる複数の保護対象デバイスの Kaspersky Embedded Systems Security の管理について説明します。

Kaspersky Security Center のグローバルポリシーは、Kaspersky Embedded Systems Security がインストールされている複数のデバイスでの保護を管理するために作成できます。

ポリシーは、1つの管理グループに所属するすべての保護対象デバイスに対して、Kaspersky Embedded Systems Security の設定、機能、および指定したタスクを適用するものです。

1つの管理グループに対して複数のポリシーを作成して適用できます。Web コンソールでは、グループに対して現在アクティブなポリシーのステータスは、「アクティブ」として示されます。

ポリシー適用に関する情報は、Kaspersky Embedded Systems Security システム監査ログに記録されます。この情報は、アプリケーションコンソールの［**ログと通知**］フォルダーで参照できます。

Kaspersky Security Center では、保護対象デバイスにポリシーを適用する方法として、*設定の変更の禁止*があります。ポリシーが適用された後、Kaspersky Embedded Systems Security は保護対象デバイスのポリシーのプロパティでアイコンが選択された設定を使用します。この場合、ポリシーが適用される前に有効だった設定の代わりに選択された設定が使用されます。ポリシーのプロパティで アイコンが選択されたアクティブポリシーの設定は適用されません。

ポリシーが有効の場合、ポリシーで アイコンが付いている設定の値がアプリケーションコンソールに表示されますが、編集はできません。その他の設定（ポリシーで アイコンが付いている設定）の値は、アプリケーションコンソールで編集できます。

アクティブなポリシーで設定されて アイコンが付いている設定は、個別の保護対象デバイスに対する Kaspersky Security Center の**保護対象デバイスのプロパティ**ウィンドウを使用した変更がブロックされます。

指定され、アクティブなポリシーを使用して保護対象デバイスに送信された設定は、アクティブなポリシーが無効になるとローカルタスク設定に保存されます。

現在実行中のコンピューターのリアルタイム保護まタスクまたはネットワークストレージの保護タスクの設定がポリシーで定義されている場合、ポリシーで定義された設定は、ポリシーが適用された直後に変更されます。タスクが実行中でない場合は、タスクの開始時に設定が適用されます。

## Kaspersky Security Center 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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. ［**追加**］をクリックします。
3. ［**新規ポリシー**］ウィンドウが表示されます。
4. ［**アプリケーションの選択**］セクションで、Kaspersky Embedded Systems Securityを選択します。
5. 保護対象デバイスでの Kaspersky Embedded Systems Security のモードを指定します。
6. 必要に応じて、すべての製品コンポーネントまたは一部の製品コンポーネントによるスキャンから除外するファイルまたはフォルダー、およびオブジェクトの名前（ウイルス百科事典に基づく）を指定します。
7. ［**全般**］タブで次の操作を実行できます：
   - ポリシー名の変更

     次の記号をポリシー名に含めることはできません：`" * < : > ? \ |` 。
   - ポリシーのステータスの選択：
     - **アクティブ**次の同期の実行後、このポリシーがクライアントコンピューター上でアクティブなポリシーとして使用されます。
     - **非アクティブ**バックアップ用のポリシーです。必要に応じて、非アクティブなポリシーのステータスをアクティブに変更できます。
     - **モバイルユーザー**このポリシーは、コンピューターが組織ネットワーク外に出た場合に有効になります。
   - 設定の継承設定：
     - **親ポリシーから設定を継承する**このスイッチをオンにすると、上位のポリシーからポリシーの設定値が継承されます。親ポリシーで🔒が指定されている設定は子ポリシーで変更できません。
     - **設定を子ポリシーへ強制的に継承させる**このオプションがオンの場合、ポリシー設定の値が子ポリシーに反映されます。子ポリシー設定では、［**親ポリシーから設定を継承する**］が自動的にオンになります。🔓のマークが付いた設定を除き、子ポリシーの設定は親ポリシーから継承されます。親ポリシーで🔒ステータスが設定された子ポリシーは編集できません。
8. ［**アプリケーション設定**］タブで、必要に応じて、ポリシーの設定を編集します。
9. ［**保存**］をクリックします。

**作成したポリシー**が、選択した管理グループの［**ポリシーとプロファイル**］タブのポリシーのリストに表示されます。ポリシーのプロパティウィンドウで、Kaspersky Embedded Systems Security のその他の設定、タスク、機能を設定できます。

新しいポリシーの作成後、本製品のブロックを防止するための一連の許可ルールが作成され、本製品の動作が中断されなくなります。タスク設定で既定のルールを表示できます。詳細と制限事項は、下を参照してください。

既定では、新しいポリシーを作成すると、受信ネットワークトラフィックの一連のルールが作成されます：

- Kaspersky Security Center ネットワークエージェントを使用して Windows デスクトップを共有するプロセスに対する 2 つの許可ルール。フォルダー %Program Files% とフォルダー %Program Files (x86)% にあります。ステータス：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。

- ローカルポート 15000 の 2 つの許可ルール。状態：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。

既定では、新しいポリシーを作成すると、送信ネットワークトラフィックの一連のルールが作成されます：

- Kaspersky Embedded Systems Security サービスの 2 つの許可ルール。フォルダー %Program Files% およびフォルダー %Program Files (x86)% にあります。ステータス：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。

- Kaspersky Embedded Systems Security のワーカー プロセスに対する 2 つの許可ルール。フォルダー %Program Files% と フォルダー %Program Files (x86)% にあります。ステータス：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。

- ローカルポート 13000 の 2 つの許可ルール。状態：有効。許可された外部アドレス：すべて。プロトコル：TCP および UPD、プロトコルごとに 1 つのルール。

# Kaspersky Security Center を使用したタスクの作成と編集

このセクションでは、Kaspersky Embedded Systems Security タスク、そのタスクの作成方法と設定方法、およびそのタスクの開始方法と停止方法に関する情報について説明します。

# Web プラグインでのタスク作成について

次の方法で、ローカルタスクおよびグループタスクを作成できます：

- 1 台の保護対象デバイスの場合、［**<保護対象デバイス名>**］ウィンドウの［**タスク**］セクションから作成します。
- 管理グループの場合、選択された保護対象デバイスのグループのフォルダーの詳細ペインの［**タスク**］タブから作成します。
- 一連の保護対象デバイスの場合、［**デバイスの抽出**］フォルダーの詳細ペインから作成します。

ポリシーを使用し、同じ管理グループのすべての保護対象デバイス上で、*アップデートとオンデマンドスキャンのローカルシステムタスクのスケジュールを無効にできます。*

Kaspersky Security Center のタスクの一般的な情報については、*Kaspersky Security Center のヘルプ*を参照してください。

# Web プラグインでのタスクの作成

*Kaspersky Security Center Web コンソールで新しいタスクを作成するには：*

1. 次のいずれかの方法でタスクウィザードを開始します：
   - ローカルタスクを作成するには：
     a. 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。
     b. 保護対象デバイスの名前をクリックします。
     c. 表示される**<デバイス名>**ウィンドウで、［**タスク**］タブを選択します。
     d. ［**追加**］をクリックします。
   - グループタスクを作成するには：
     a. 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。
     b. ［**追加**］をクリックします。

   タスクウィザードのウィンドウが開きます。
2. ［**アプリケーション**］ドロップダウンリストで、［**Kaspersky Embedded Systems Security**］を選択します。
3. ［**タスク種別**］ドロップダウンリストで、作成するタスク種別を選択します。

4. 選択したタスクの種別によって、次のいずれかの操作を実行します：

- オンデマンドスキャンタスクを作成します。
- アップデートタスクを作成するには、要件に基づいてタスク設定を行います：

  a. ［**アップデート元**］ブロックで、アプリケーションのアップデート元として、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を指定できます。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。

  手動でカスタマイズしたサーバーが使用できない場合、カスペルスキーのアップデートサーバーの使用を指定できます。

  b. ディスクサブシステムの負荷を軽減する機能を設定します：

  c. 重要なソフトウェアモジュールのアップデートが必要な場合、および重要なアップデートのインストール完了後に Kaspersky Embedded Systems Security が実行する操作を指定できます。また、Kaspersky Embedded Systems Security が適用可能なスケジュールされたアップデートに関する情報を受信するかどうかを指定できます。

  d. コピーする一連のアップデートを指定して、コピーしたアップデートの保存先として使用するフォルダーのパスを指定します。

- ［アクティベーションの完了］タスクを作成するには：

  a. ［**ライセンスを選択**］ウィンドウでは、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情報ファイルまたはアクティベーションコードを指定します。

  b. ライセンスを更新するタスクを作成するには［**予備のライセンスとして使用する**］をオンにします。

- アプリケーション起動コントロールルールの自動生成タスクを作成して設定を編集します。
- デバイスコントロールルールの自動生成タスクを作成して設定を編集します。

5. ［**次へ**］をクリックします。

6. タスクが複数の保護対象デバイス用に作成されている場合は、このタスクを実行する保護対象デバイスのネットワーク（またはグループ）を選択します。

7. ［**次へ**］をクリックします。

8. タスク設定を行う場合は、［**タスク作成の終了**］ウィンドウで、［**タスクの作成が完了したらタスクの詳細を表示する**］をオンにします。

9. ［**終了**］をクリックします。

［**タスク**］のリストに作成したタスクが表示されます。

# Web プラグインでのグループタスクの設定

*複数の保護対象デバイスに対してグループ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、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. Kaspersky Security Center タスクのリストで、タスク名をクリックします。
   ［**<タスク名>**］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. 設定したタスクの種別に従って、次のいずれかを実行します：
   - *オンデマンドスキャンのタスクを設定するには：*
     a. ［**スキャン範囲**］セクションで、スキャン範囲を設定します。
     b. ［**オプション**］セクションで、ヒューリスティック分析のレベルとその他の製品コンポーネントとの連携を設定します。
   - *アップデートタスクを設定するには、要件に基づいてタスク設定を調整します：*
     a. ［**アップデート元**］セクションで、アップデート元を設定します。
     b. ［**アップデート設定**］セクションで、ディスクサブシステムの最適化設定を管理し、製品機能の重要なアップデートが適用可能な場合、または定期的なアップデートに関する情報がある場合に Kaspersky Embedded Systems Security で実行する処理を指定し、アップデートのコピー設定を指定します。
   - *アクティベーションの完了*タスクを設定する場合は、製品のアクティベーションに使用する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適用します。ライセンスの更新に使用するアクティベーションコードまたはライセンス情報ファイルを追加する場合は、［**予備のライセンスとして使用する**］をオンにします。
   - デバイスコントロールの許可ルールの自動生成を設定する場合は、許可ルールのリストを作成するために使用される設定を指定します。
5. ［**スケジュール**］セクションで、タスクのスケジュールを設定します（*アップデートのロールバック*を除くすべてのタスク種別に対して、スケジュールを設定できます）。
6. ［**アカウント**］セクションの［**設定**］タブで、タスクの実行で使用する権限を持つアカウントを指定します。このセクションでの設定の詳細情報については、*Kaspersky Security Center* のヘルプを参照してください。
7. ［**保存**］をクリックします。

新たに設定したタスクの内容が保存されます。

# Web プラグインでの本製品のアクティベーションタスクの設定

*アクティベーションの完了の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、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. Kaspersky Security Center タスクのリストで、タスク名をクリックします。
   ［**<タスク名>**］ウィンドウが表示されます。
3. ［**アプリケーション設定**］セクションでは、製品のアクティベーションに使用するライセンス情報ファイルを指定します。更新用のライセンスを追加する場合は、［**予備のライセンスとして使用する**］をオンにします。
4. ［**スケジュール**］セクションでタスクスケジュールを設定します。
5. ［**<タスク名>**］ウィンドウで、［**保存**］をクリックします。

# Web プラグインでのアップデートタスクの設定

*アップデートの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、［**デバイス**］→［**タスク**］の順に選択します。
2. Kaspersky Security Center タスクのリストで、タスク名をクリックします。
   ［<タスク名>］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、アップデート元を設定します：
   a. アプリケーションのアップデート元として、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を指定します。カスタム HTTP サーバーおよび FTP サーバーまたはネットワークフォルダーを手動で追加しアップデート元として設定することで、カスタマイズしたアップデート元のリストを作成することもできます。
      手動でカスタマイズしたサーバーが使用できない場合、カスペルスキーのアップデートサーバーの使用を指定できます。
   b. ディスクサブシステムの負荷を軽減する機能を設定します：
      - **ディスク I/O の負荷の低減**
      - **最適化に使用するメモリ（MB）**
   c. 製品機能の重要なアップデートが適用可能な場合、または定期的なアップデートに関する情報がある場合に、Kaspersky Embedded Systems Security が実行する処理を指定します。
   d. アップデートのコピー設定を指定します。

5. ［**スケジュール**］セクションで、タスクのスケジュールを設定します（*アップデートのロールバック*を除くすべてのタスク種別に対して、スケジュールを設定できます）。

6. ［**<タスク名>**］ウィンドウで、［**OK**］をクリックします。

# タスクスケジュールの管理

Kaspersky Embedded Systems Security のタスクにスケジュールを設定できます。

## タスクのスケジュールを設定する

Web コンソールで、ローカルのシステムタスクとカスタムタスクの開始スケジュールを設定することができます。

*Web コンソールを使用してグループタスクのスケジュールを設定するには：*

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

2. Kaspersky Security Center タスクのリストで、タスク名をクリックします。
   ［**<タスク名>**］ウィンドウが表示されます。

3. ［**スケジュール**］セクションに移動して、必要に応じてスケジュールを設定します。

   オンデマンドスキャンタスクとアップデートタスクのスケジュール設定に使用するフィールドは、これらのタスクのスケジュールの設定が Kaspersky Security Center ポリシーによってブロックされた場合、使用できません。

   a. ［**タスク開始**］ドロップダウンリストから、次のいずれかを選択します：

   - **N 時間ごと**：タスクを数時間ごとに定期的に実行する場合に選択します。［**間隔**］フィールドに時間数を入力します。
   - **N 日ごと**：タスクを数日ごとに定期的に実行する場合に選択します。［**間隔**］フィールドに日数を入力します。
   - **N 分ごと**：タスクを数分ごとに定期的に実行する場合に選択します。［**間隔**］フィールドに分数を入力します。
   - **曜日ごと**：タスクを特定の曜日に実行する場合に選択します。実行する時刻も指定します。

     Kaspersky Security Center 15.1 では、数週間間隔でタスクを実行できます（［**間隔**］のパラメータ）。Kaspersky Embedded Systems Security は、複数週間隔でのタスクの実行をサポートしていません。Kaspersky Embedded Systems Security のタスクを数週間間隔で実行するようにスケジュール設定している場合、指定された日時に毎週そのタスクが実行されます。

   - **毎月**：タスクを月の特定の日に実行する場合に選択します。実行する時刻も指定します。
   - **1 回**：指定した日時にタスクを 1 回実行する場合に選択します。

- **手動**：タスクを手動で実行する場合に選択します。
- **アプリケーション開始時**：Kaspersky Embedded Systems Security が起動するたびにタスクを実行する場合に選択します。
- **新しいアップデートがリポジトリにダウンロードされ次第**：リポジトリにアップデートがダウンロードされるたびにタスクを実行する場合に選択します。
- **ウイルスアウトブレイク検知次第**：ウイルス攻撃が検知された場合にタスクを実行する場合に選択します。
- **他のタスクが完了次第**：他のタスクの完了時にタスクを実行する場合に選択します。

b. ［**開始時刻**］フィールドと［**日付**］フィールドに、タスクを最初に開始する時刻を指定します。

4. ［**追加設定**］ブロック：
   - ［**未実行のタスクを実行する**］をオンにして、スキップしたタスクの開始を有効にします。
   - ［**タスクの開始を自動的かつランダムに遅延させる**］がオンの場合、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。
   - **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。
   - **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がオンの場合、タスクの完了後にデバイス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**このチェックボックスがオンの場合、指定された時間より長く実行された場合にタスクが停止されます。
5. ［**保存**］をクリックして、タスクの開始設定を保存します。

## スケジュールに従ったタスクの有効化と無効化

スケジュール設定を行った後で、スケジュールに従ったタスクを無効にできます。

*タスクの開始スケジュールを無効にするには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］→［**タスク**］の順に選択します。
2. Kaspersky Security Center タスクのリストで、タスク名をクリックします。
   ［**<タスク名>**］ウィンドウが表示されます。
3. ［**アプリケーション設定**］に移動します。
4. ［**スケジュール**］セクションを選択します。
5. スケジュールに従ったタスクの開始を有効にする場合は、［**実行予定**］ドロップダウンリストから、スケジュールに従ったタスクを実行するための設定を選択します。

6. スケジュールに従ったタスクの開始を無効にする場合は、ドロップダウンリストから［**手動**］を選択します。

7. ［**保存**］をクリックします。

# Kaspersky Security Center のレポート

Kaspersky Security Center のレポートには、管理対象デバイスのステータスに関する情報が含まれます。レポートは管理サーバーに保存される情報に基づきます。

Kaspersky Security Center 11 より、Kaspersky Embedded Systems Security で次の種別のレポートが利用できるようになりました：

- 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
- 禁止されたアプリケーションに関するレポート
- テストモードで禁止されたアプリケーションに関するレポート

Kaspersky Security Center のレポートやその設定方法の詳細は、*Kaspersky Security Center のオンラインヘルプ*をご参照ください。

## Kaspersky Embedded Systems Security のコンポーネントステータスに関するレポート

すべてのネットワークデバイスの保護ステータスを監視して、各デバイスで設定されているコンポーネントの構造化された概要を取得できます。

レポートには、コンポーネントごとに以下のステータスのいずれかが表示されます：*実行中*、*一時停止済み*、*停止済み*、*ライセンスに含まれていません*。

［*未インストール*］ステータスは、アプリケーション自体ではなくコンポーネントを参照します。アプリケーションがインストールされていない場合は、Kaspersky Security Center Web コンソールは N/A（利用不可）のステータスを割り当てます。

コンポーネントの選択を作成し、フィルターを使用して、指定されたコンポーネントのセットおよびその状態のネットワークデバイスを表示します。

選択の作成および利用の詳細については、『*Kaspersky Security Center ヘルプ*』を参照してください。

*Kaspersky Security Center Web コンソールでコンポーネントステータスを確認するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］→［**管理対象デバイス**］の順に選択します。
2. デバイス名をクリックして、［**アプリケーション**］セクションに移動します。
3. Kaspersky Embedded Systems Security のアプリケーション名をクリックします。

4. 表示されたウィンドウの［**全般**］タブで、［**コンポーネント**］セクションに移動します。

5. ステータステーブルを確認します。

*Kaspersky Security Center Web コンソールで標準レポートを確認するには：*

1. ［**監視とレポート**］→［**レポート**］を選択します。

2. ［**製品コンポーネントのステータスに関するレポート**］のリスト項目を選択し、クリックします。
   レポートが生成されます。

3. 以下のレポートの詳細を確認します：

   - 図表。
   - コンポーネント、各コンポーネントがインストールされているネットワークデバイスの合計数、およびそれらが属するグループの概要のテーブル。
   - コンポーネントステータス、バージョン、デバイス、およびグループを指定する詳細なテーブル。

## 処理を実行モードおよび統計情報モードでのブロックされたアプリケーションのレポート

アプリケーション起動コントロールタスクの実行結果に基づいて、次の 2 種類のレポートを生成できます：禁止したアプリケーションのレポート（処理を実行モードでタスクを開始した場合）、テストモードで禁止したアプリケーションのレポート（通知モードでタスクを開始した場合）。これらのレポートは、ネットワークの保護対象デバイス上にあるブロックされたアプリケーションの情報を表示します。すべての管理グループに対して各レポートが生成され、保護対象デバイス上にインストールされたすべてのカスペルスキー製品からのデータを蓄積します。

*通知モードで禁止されたアプリケーションに関するレポートを表示するには：*

1. アプリケーション起動コントロールタスクを処理を通知モードで開始します。

2. ［**監視とレポート**］→［**レポート**］の順に選択します。

3. ［**テストモードで禁止されたアプリケーションに関するレポート**］のリスト項目を選択し、クリックします。
   レポートが生成されます。

4. 以下のレポートの詳細を確認します：

   - ブロックされた起動が最も多いアプリケーションの上位 10 個を表示する図表。
   - ブロックされたアプリケーションについて、実行ファイルの名前、理由、ブロックの時刻、ブロックされたデバイスの数を示す概要のテーブル。
   - デバイス、ファイルパス、およびブロックの条件に関するデータを示す詳細なテーブル。

*処理を実行モードで禁止されたアプリケーションに関するレポートを表示するには：*

1. アプリケーション起動コントロールタスクを処理を実行モードで開始します。

2. ［**監視とレポート**］→［**レポート**］の順に選択します。

3. ［**禁止されたアプリケーションに関するレポート**］のリスト項目を選択し、クリックします。

   レポートが生成されます。

このレポートは、テストモードで禁止されたアプリケーションに関するレポートと同じブロックに関するデータで構成されます。

# 製品のライセンス

このセクションでは、本製品のライセンスに関する主要な概念について説明します。

## 使用許諾契約書について

*使用許諾契約書*は、ユーザーと AO Kaspersky Lab との間で締結される拘束力のある契約であり、製品の使用条件を規定しています。

製品の使用を開始する前に、使用許諾契約書の条件をよくお読みください。

データの処理と送信について説明している使用許諾契約書とプライバシーポリシーの条項は、次の方法で読むことができます：

- Kaspersky Embedded Systems Security のインストール中。
- Kaspersky Embedded Systems Security コンソールのインストール中。
- 配布キットに含まれるファイル license.txt ドキュメントを読む。
- カスペルスキーの Web サイト（https://www.kaspersky.co.jp/business/eula）。

製品のインストール時に使用許諾契約書への同意が確認されると、使用許諾契約書の条件に承諾したものとみなされます。使用許諾契約書の条件に同意しない場合は、製品のインストールを終了するか、製品の使用を中止する必要があります。

## ライセンスの概要

*ライセンス*は、使用許諾契約書に基づいて提供される、製品を使用する期限付きの権利です。

有効なライセンスにより、使用許諾契約書の条件に従って本製品を使用できるようになり、必要に応じてテクニカルサポートを受けることができます。

サービスの範囲と製品の使用期間は、製品のアクティベーションに使用されるライセンスの種別によって異なります。

製品のアクティベーションは、次の 2 つの方法で実行できます：

- 製品版ライセンスでの使用が許可される、ライセンス情報ファイルを使用
- 製品版ライセンスを購入するためのアクティベーションコードを使用

製品版ライセンスの有効期限が終了した場合、引き続き使用できるのは次のアプリケーションコンポーネントとタスクのみとなり、定義データベースはアップデートされません：

- ファイルのリアルタイム保護
- システム変更監視
- オンデマンドスキャンタスク

Kaspersky Embedded Systems Security のすべての機能を継続して使用するには、製品版ライセンスを更新する必要があります。最大の保護を確保するために、ライセンスの有効期限前に有効期間を延長することを推奨します。

ライセンス情報ファイルが削除されても、本製品は引き続き実行されます。システム変更監視コンポーネントは引き続き使用可能ですが、その他のコンポーネント、タスク、および Kaspersky Embedded Systems Security の定義データベースのアップデートは使用できなくなります。カスペルスキーがライセンスを拒否リストに追加した場合も同様です。

# ライセンス証明書について

*ライセンス証明書*は、ライセンス情報ファイルやアクティベーションコードと一緒に提供されるドキュメントです。

ライセンス証明書には、提供されるライセンスに関する次の情報が含まれます：

- ライセンスの識別子または注文番号
- ライセンスを付与されたユーザーに関する情報
- 提供されるライセンスでアクティベートできる本製品に関する情報
- ライセンス単位の数の制限（例：ライセンスを使用してアプリケーションを使用できるデバイスの数）
- ライセンスの有効期間の開始日
- ライセンス有効期限またはライセンス期間
- ライセンス種別

# ライセンス情報について

*ライセンス情報*は、使用許諾契約書の条件に従って本製品をアクティベートして利用するのに使用する数値列です。ライセンス情報はカスペルスキーが生成します。

ライセンス情報ファイルを使用して、本製品にライセンスを追加できます。本製品にライセンスを追加すると、ライセンスは製品インターフェイスに一意の英数字文字列として表示されます。

使用許諾契約書に違反すると、カスペルスキーによってライセンスが拒否リストに追加される場合があります。ライセンスがブロックされた場合、本製品を動作させるためには、別のライセンスを追加する必要があります。

ライセンスには、現在と予備の 2 種類があります。

*現在のライセンス*は、製品が機能するために現在使われているライセンスです。製品版のライセンスを現在のライセンスとして追加できます。1つの製品に対して現在のライセンスを 2 つ以上使用することはできません。

*予備のライセンス*は、製品を使用する権限を確認する、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した場合、自動的に予備のライセンスがアクティブになります。予備のライセンスは、現在のライセンスがある場合のみ追加できます。

# ライセンス情報ファイルについて

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

Kaspersky Embedded Systems Security の購入後に指定したメールアドレスで、ライセンス情報ファイルを受け取ります。

ライセンス情報ファイルで製品をアクティベートする際に、カスペルスキーのアクティベーションサーバーに接続する必要はありません。

誤って削除してしまったライセンス情報ファイルは復元できます。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には：

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

# アクティベーションコードの概要

*アクティベーションコード*は、20 文字の英数字で構成された一意な文字の並びです。Kaspersky Embedded Systems Security をアクティベートするライセンスを追加するには、アクティベーションコードを入力する必要があります。Kaspersky Embedded Systems Security の購入後に指定したメールアドレスで、アクティベーションコードを受け取ります。

アクティベーションコードを使用して製品をアクティベートするには、カスペルスキーのアクティベーションサーバーへのインターネット接続が必要です。

本製品のインストール後にアクティベーションコードを紛失した場合は、復元できます。アクティベーションコードは、カスペルスキーカンパニーアカウントへの登録時などに必要となる場合があります。アクティベーションコードを回復するには、ライセンスを購入したカスペルスキーのパートナーにお問い合わせください。

# ライセンス種別による製品機能の比較

Kaspersky Embedded Systems Security で利用できる機能の組み合わせはライセンス種別により異なります（下の表を参照）。

Kaspersky Embedded Systems Security の機能の比較表

| 機能 | Kaspersky Embedded Systems Security | Kaspersky Embedded Systems Security Compliance Edition |
|---|---|---|
| ファイルのリアルタイム保護 | ✓ | ✓ |
| オンデマンドスキャン | ✓ | ✓ |
| アプリケーション起動コントロール | ✓ | ✓ |
| デバイスコントロール | ✓ | ✓ |
| ファイアウォール | ✓ | ✓ |
| ファイル変更監視 | – | ✓ |
| Windows イベントログ監視 | – | ✓ |

# ライセンス情報ファイルによる製品のアクティベーション

ライセンス情報ファイルを適用して Kaspersky Embedded Systems Security をアクティベートできます。

*ライセンス情報ファイルを適用して Kaspersky Embedded Systems Security をアクティベートするには：*

1. アプリケーションコンソールツリーで、［**ライセンス**］フォルダーを展開します。
2. ［**ライセンス**］フォルダーの結果ペインで、［**ライセンスの追加**］をクリックします。
3. 表示されたウィンドウの［**参照**］をクリックします。
4. 拡張子が .key のライセンス情報ファイルを選択します。

   予備のライセンスとして追加することもできます。ライセンスを予備のライセンスとして追加するには、［**予備のライセンスとして使用する**］をオンにします。

5. ［OK］をクリックします。

選択したライセンス情報ファイルが適用されます。この場合、次のようになります：

- 本製品をアクティベートするために現在のライセンスが既に追加されている場合、別のライセンスを現在のライセンスとして追加すると、新しいライセンスが以前に追加されたライセンスと置き換わります。以前に追加されたライセンスは削除されます。
- 本製品をアクティベートするために予備のライセンスが既に追加されている場合、別のライセンスを予備のライセンスとして追加すると、新しいライセンスが以前に追加されたライセンスと置き換わります。以前に追加された予備のライセンスは削除されます。
- 本製品をアクティベートするために現在のライセンスと予備のライセンスが既に追加されている場合、新しいライセンスを現在のライセンスとして追加すると、新しいライセンスが以前に追加された現在のライセンスと置き換わります。この場合、予備のライセンスは削除されません。

追加されるライセンスに関する情報は［**ライセンス**］フォルダーにあります。

# アクティベーションコードによる製品のアクティベーション

アクティベーションコードを使用して製品をアクティベートするには、保護対象デバイスがインターネットに接続している必要があります。

アクティベーションコードを使用して、Kaspersky Embedded Systems Security をアクティベートすることができます。

この方法で製品をアクティベートする場合、入力したコードを確認するために、アクティベーションサーバーにデータが送信されます：

- アクティベーションコードの確認が正常に完了すると、製品がアクティベートされます。
- アクティベーションコードが正常に確認できない場合、対応する通知が表示されます。この場合、Kaspersky Embedded Systems Security のライセンスを購入したソフトウェアの販売元にお問い合わせください。
- アクティベーションコードによるアクティベーションが既定の回数を超えると、対応する通知が表示されます。製品のアクティベーションが中断され、カスペルスキーのテクニカルサポートへの連絡が促されます。

Kaspersky Embedded Systems Security のアクティベーションは、アプリケーションコンソールを使用してアクティベーションコードで行うか、管理プラグインまたは Web プラグインからアクティベーションの完了ループタスクを作成することで行うことができます。

*アプリケーションコンソールを使用してアクティベーションコードで Kaspersky Embedded Systems Security をアクティベートするには：*

1. アプリケーションコンソールツリーで、［**ライセンス**］フォルダーを展開します。
2. ［**ライセンス**］フォルダーの結果ペインで、［**アクティベーションコードの追加**］をクリックします。
3. 表示されたウィンドウで、［**アクティベーションコード**］にアクティベーションコードを入力します。
   - アクティベーションコードを予備のライセンスとして使用する場合は、［**予備のライセンスとして使用する**］を選択にします。
   - ライセンスに関する情報を表示するには、［ **ライセンス情報を表示する**］をクリックします。［**ライセンス情報**］ブロックに情報が表示されます。
4. ［OK］をクリックします。

   適用されたアクティベーションコードの情報がアクティベーションサーバーに送信されます。

# 現在のライセンスに関する情報の表示

## ライセンスステータスの表示

現在のライセンスの情報は、アプリケーションコンソールにある［**Kaspersky Embedded Systems Security**］フォルダーの詳細ペインに表示されます。ライセンスステータスには次の値が使用されます：

- **ライセンスの状態を確認しています。**： – Kaspersky Embedded Systems Security は、追加されたライセンス情報ファイルをチェックして、現在のステータスに関する応答を待ちます。
- **有効期限：%s。** – Kaspersky Embedded Systems Security は指定された日付までアクティベートされています。次の場合にステータスが黄色で表示されます：
  - ライセンスの有効期間の残り日数が 30 日で、予備のライセンスが追加されていない。
  - 追加されたライセンスが拒否リストに含まれていて、ブロックされる予定である。
- **アクティベートされていません。** – ライセンスが追加されていないため、Kaspersky Embedded Systems Security はアクティベートされていません。ステータスは赤色で表示されます。
- **ライセンスの有効期間が終了しています。** – ライセンスの有効期間が終了したため、Kaspersky Embedded Systems Security はアクティベートされていません。ステータスは赤色で表示されます。
- **使用許諾契約書に違反しています。** – 使用許諾契約書の条件に違反しているため、Kaspersky Embedded Systems Security はアクティベートされていません。ステータスは赤色で表示されます。
- **ライセンスが拒否リストに登録されています。** – ライセンスが第三者によって不正にアクティベートするために使用されたなどの理由から、追加されたライセンス情報ファイルがブロックされ、カスペルスキーによって拒否リストに登録されています。ステータスは赤色で表示されます。

## 現在のライセンスに関する情報の表示

*現在のライセンスに関する情報を表示するには：*

アプリケーションコンソールツリーで、［**ライセンス**］フォルダーを展開します。

現在のライセンスの全般的な情報が、［**ライセンス**］フォルダーの詳細ペインに表示されます（次の図を参照）。

［ライセンス］フォルダーで表示されるライセンスの全般的な情報

| フィールド | 説明 |
| --- | --- |
| **アクティベーションコードまたはライセンスのステータス** | アクティベーションコードのステータス、またはライセンス情報ファイルのステータス：*現在のライセンス*または*予備のライセンス*。 |
| **有効期限** | 現在のライセンスの有効期限の日時。 |
| **種別** | ライセンス種別：*製品版*。 |

| フィールド | 説明 |
| --- | --- |
| **アクティベーションステータス** | アクティベーションステータス情報には次の値が使用されます：<br>• **適用済み** - ライセンスを使用して製品をアクティベートした場合。<br>• **アクティベーションの完了** - アクティベーションコードを適用して製品をアクティベートしたが、アクティベーションのプロセスがまだ完了していない場合。製品のアクティベートが完了し、フォルダーの詳細ペインの内容が更新されると、ステータスは［**適用済み**］に変更されます。<br>• **アクティベーションエラー** – 製品がアクティベーションできなかった場合。アクティベーションエラーの原因は、タスク実行ログで確認できます。 |
| **ライセンス** | 製品をアクティベートするために使用したライセンスの番号。 |

*ライセンスの詳細情報を確認するには：*

［**ライセンス**］フォルダーの詳細ペインで、表示するライセンス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。

［プロパティ <ライセンス番号>］ウィンドウの詳細なライセンス情報

| フィールド | 説明 |
| --- | --- |
| **キー** | 製品をアクティベートするために使用したライセンスの番号。 |
| **アプリケーション** | 追加されたライセンスでアクティベートされた製品の名前。 |
| **種別** | ライセンスの種別（製品版または試用版）。 |
| **ライセンスの有効期間** | 製品のアクティベーション日から始まる、ライセンスが有効な日数。 |
| **アクティベーション日** | 本製品にライセンスが追加された日付。 |
| **有効期限** | 現在のライセンスの有効期限の日付。無制限の定額制サービスで製品をアクティベートした場合、値は*無制限*と表示されます。ライセンスの有効期限が特定できない場合、値は*不明*と設定されます。 |
| **有効期間終了までの日数** | 現在のライセンスの有効期限までの残り日数。 |
| **テクニカルサポート利用可能** | カスペルスキーまたはそのパートナーがライセンス条件に従ってお客様にテクニカルサポートを提供するかどうかに関する情報。 |
| **サポート情報** | カスペルスキーまたはテクニカルサポートを提供するパートナーの連絡先の詳細。テクニカルサポートが提供されていない場合は空欄となる場合があります。 |
| **所有者情報** | ライセンスのお客様の情報：お客様の名前およびライセンスを取得している組織の名前。 |
| **ライセンス情報** | 現在のライセンスの番号と種別。 |
| **機能** | ライセンスを使用して利用できる製品機能。 |

# ライセンスの更新

既定では、 Kaspersky Embedded Systems Security は、ライセンスの有効期間が残り 30 日になると通知します。

予備のライセンスを使用して、有効期限前にライセンスを更新できます。これにより、現在のライセンスの有効期間終了後から、本製品を新しいライセンスでアクティベートするまでの期間、デバイスを保護された状態に保つことができます。

*ライセンスを更新するには：*

1. 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新たに取得します。
2. アプリケーションコンソールツリーで、［**ライセンス**］フォルダーを選択します。

3. ［**ライセンス**］フォルダーの結果ペインで、次のいずれかの処理を実行します：

- ライセンス情報ファイルを使用して更新する場合：

  a. ［**ライセンスの追加**］リンクをクリックします。

  b. 表示されたウィンドウの［**参照**］をクリックします。

  c. 拡張子が .key の新しいライセンス情報ファイルを選択します。

  d. ［**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します。

- アクティベーションコードを使用して更新する場合：

  a. ［**アクティベーションコードの追加**］リンクをクリックします。

  b. 表示されるウィンドウで、購入済みのアクティベーションコードを入力します。

  c. ［**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します。

  > アクティベーションコードを適用するには、インターネット接続が必要です。

4. ［**OK**］をクリックします。

予備のライセンスは、現在のライセンスの有効期限が切れると自動的に適用されます。

# ライセンスの削除

> 追加されたライセンスを削除した場合、ライセンス情報ファイルを再度適用しないと削除したライセンスを復元できません。

*以前に追加したライセンスを削除するには：*

1. アプリケーションコンソールツリーで、［**ライセンス**］フォルダーを選択します。
2. ［**ライセンス**］フォルダーの結果ペインにある追加されているライセンスに関する情報の表で、削除するライセンスを選択します。
3. 選択したライセンスの情報が表示されている行のコンテキストメニューで［**削除**］を選択します。
4. 確認ウィンドウで［**はい**］をクリックしてライセンスを削除することを確認します。

選択したライセンスが削除されます。

# データの提供について

Kaspersky Embedded Systems Security の使用許諾契約書の「データ処理の条件」という項には、このガイドに記載されているデータの送信および処理に関する諸条件、責任、手順が明記されています。使用許諾契約書に同意する前に、その条項ならびに使用許諾契約書にリンクされているすべての文書を慎重に確認してください。

お客様からカスペルスキーに送信されるデータは、プライバシーポリシー（www.kaspersky.co.jp/Products-and-Services-Privacy-Policy）に従って保護され、処理されます。

使用許諾契約書とプライバシーポリシーの内容は、配布キットの一部として、Kaspersky Embedded Systems Security のインストール中に確認できます。インストール後は、［**スタート**］メニュー（［**すべてのプログラム**］→［**Kaspersky Embedded Systems Security**］→［**使用許諾契約書とプライバシーポリシー**］）から確認できます。

Kaspersky Embedded Systems Security のアンインストール中に、Kaspersky Embedded Systems Security によって保護対象デバイスに保存されたすべてのデータが削除されます。

使用許諾契約書の条項に同意することにより、お客様は次の情報をカスペルスキーに自動的に送信することに同意するものとします：

- アップデートを受信する仕組みをサポートするための情報 - インストールされている製品とアクティベーションに関する情報：インストールされている製品の識別子と完全なバージョン（ビルド番号、種別、ライセンス識別子、インストール識別子、アップデートタスク識別子など）。
- アプリケーションエラーが発生した時にナレッジベースの記事を参照する機能を使用するための情報（リダイレクターサービス） - 製品とリンク種別に関する情報：製品の名前、ロケール、完全バージョン番号、リダイレクトリンクの種別、エラー識別子。
- データ処理についての承認を管理するための情報 - データ転送に関する条項を定めた使用許諾契約書やその他のドキュメントの承認状態に関する情報：使用許諾契約書やその他のドキュメントの識別子またはバージョン（データの処理に関する条項を承認または拒否した部分）、属性、ユーザー動作での表示（条件承認の確認）、データの処理に関する条項の承認に関するステータス変更の日時。

## ローカルでのデータ取り扱い方法

このガイドで説明している製品の主要な機能の実行中に、Kaspersky Embedded Systems Security は、一連のデータをローカルで処理し、保護対象デバイスに保存します。

レポートに含まれるデータの Kaspersky Embedded Systems Security によるローカル処理と保存に関する情報は、次の表の通りです。

レポートに含まれるデータの処理と保存

| 機能の領域 | イベントの登録 |
| --- | --- |
| 使用の種別 | Kaspersky Embedded Systems Security によりデータがローカルに保存され、管理サーバーに送信されます。管理サーバーのデータベースには、管理対象の保護されたデバイスで発生する製品のイベントに関する情報が格納されます。 |
| 保管領域 | • %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<製品のバージョン>\Reports<br>• %SystemRoot%\System32\Winevt\Logs\Kaspersky Security.evtx<br>• 管理サーバーのデータベース |

| | |
|---|---|
| セキュリティ対策 | アクセスコントロールリスト。 |
| 保管期間 | データは、Kaspersky Embedded Systems Security をアンインストールするまで Kaspersky Embedded Systems Security によって保存されます。<br>Kaspersky Embedded Systems Security のアンインストール中に、Kaspersky Embedded Systems Security によって保護対象デバイスに保存されたすべてのデータが削除されます。 |
| 目的 | 主要な機能の提供。 |

Kaspersky Embedded Systems Security は、Kaspersky Embedded Systems Security のアンインストール中に発生するイベントを含む、Windows イベントログのイベントを削除しません。

イベント登録機能を提供するため、Kaspersky Embedded Systems Security はローカルで次のデータを処理します：

- 処理されたファイルの名前、チェックサム（MD5、SHA-256）属性、およびスキャンされたメディア上の処理されたファイルへの完全パス。
- Kaspersky Embedded Systems Security がスキャンしたファイルに対して行われた操作。
- 保護対象デバイス上のスキャンされたファイルに対して行われたユーザーの操作。
- 保護対象のネットワークやデバイスで操作を実行しているユーザーのアカウントに関する情報。
- デバイスコントロールルールに追加されたデバイスのデバイスインスタンスのパス値。
- システムで実行されているプロセスとスクリプトに関する情報：チェックサム（MD5、SHA-256）と実行ファイルへの完全パス、デジタル証明書に関する情報。
- Windows ファイアウォールの設定。
- Windows イベントログのエントリ。
- 保護対象デバイス上のスキャンされたファイルに対して操作を行ったユーザーアカウントの名前。
- 開始される実行ファイルのインスタンスと、これらのファイルの種別、名前、チェックサム、属性。
- ネットワーク活動に関する情報：
  - ブロックされた外部デバイスの IP アドレス。
  - 処理された IP アドレス。
- Windows USN ジャーナルのステータスに関する情報。

次の表では、Kaspersky Embedded Systems Security によって処理されるサービスデータに関する情報について説明しています。サービスデータには、プログラムのパラメータ、隔離ファイルとバックアップファイル、プログラムのサービスデータベースの情報、ライセンスデータが含まれます。

ユーザーが指定したパラメータに関するデータの、Kaspersky Embedded Systems Security によるローカル処理と保存に関する情報は、次の表の通りです。

ユーザーが指定したパラメータに関するデータの処理と保存

| | |
|---|---|
| 機能の領域 | Kaspersky Embedded Systems Security のすべての機能 |
| 使用の種別 | Kaspersky Embedded Systems Security によりデータがローカルに保存され、管理サーバーに送信されます。データは管理サーバーのデータベースに保存されます。<br>本製品がローカルで処理したデータが、カスペルスキーのシステムやその他のサードパーティのシステムに自動的に送信されることはありません。 |
| 保管領域 | • %ALLUSERSPROFILE%\Kaspersky Lab\Kaspersky Security for Windows Server\<製品のバージョン>\<br>• 管理サーバーのデータベース |
| セキュリティ対策 | アクセスコントロールリスト。 |
| 処理期間 | データは、Kaspersky Embedded Systems Security をアンインストールするまで Kaspersky Embedded Systems Security によって保存されます。<br>Kaspersky Embedded Systems Security のアンインストール中に、Kaspersky Embedded Systems Security によって保護対象デバイスに保存されたすべてのデータが削除されます。<br>設定情報ファイルにエクスポートされたパラメータに関するデータは削除されません。<br>セットアップウィザードで［**隔離されたオブジェクトをエクスポートする**］および［**バックアップされたオブジェクトをエクスポートする**］がオンになっている場合、隔離オブジェクトとバックアップオブジェクトは削除されません。 |
| 目的 | 主要な機能の提供。 |

特定の目的のため、Kaspersky Embedded Systems Security により次のデータがローカルで処理されます：

- 隔離またはバックアップに配置されたオブジェクト。
- タスクを実行するユーザーアカウント（ユーザー名とパスワード）に関する情報。
- Kaspersky Embedded Systems Security のパスワード。
- ブロックされたログオンセッションの IP アドレスと識別子。
- Windows ファイアウォールの設定と Windows ファイアウォールルールの設定。
- チェックサム（MD5、SHA-256）およびアプリケーション起動コントロールタスクのルールに追加された実行ファイルへのパス。
- デバイスコントロールルールに追加されたデバイスのデバイスインスタンスのパス値。
- Kaspersky Embedded Systems Security タスクの範囲に含まれるファイルとフォルダーに関する情報。
- 保護範囲に含まれる、または保護範囲から除外される IP アドレス。
- Windows イベントログのイベントに関する情報。
- iSwift または iChecker テクノロジーを使用した検知に関する情報。
- 除外設定で指定されたチェックサム（MD5、SHA-256）、完全パス、およびマスク。
- 信頼ゾーンに追加されたプロセスに関する情報。
- 追加されたライセンスに関する情報。
- デジタル証明書に関する情報。
- スキャン中にアーカイブやその他の複合オブジェクトから展開されたファイル。

Kaspersky Embedded Systems Security は、製品イベントの記録や診断データの受信などの製品の基本機能の一部として、データを処理し保存します。ローカルで処理されたデータは、設定して適用された製品設定に従って保護されます。

Kaspersky Embedded Systems Security では、ローカルで処理されたデータに対して保護レベルを設定できます。処理するデータへのアクセスに関するユーザー権限の変更、そのようなデータの保存期間の変更、データの記録を伴う機能全体または一部の無効化、データが記録されているドライブのフォルダーのパスと属性の変更などができます。

本製品がローカルで処理したデータが、カスペルスキーのシステムやその他のサードパーティのシステムに自動的に送信されることはありません。

既定では、本製品が動作中にローカルで処理したすべてのデータは、保護対象デバイスから Kaspersky Embedded Systems Security をアンインストールすると削除されます。

診断情報を含むファイル（トレースファイルとダンプファイル）、Windows イベントログ内のアプリケーションイベント、およびエクスポートされた Kaspersky Embedded Systems Security の設定を含むファイルは例外です。これらのファイルは手動で削除することを推奨します。

本製品の診断データを含むファイルの取り扱いについて詳しくは、本ガイドの該当するセクションを参照してください。

標準のオペレーティングシステムツールを使用して、 Kaspersky Embedded Systems Security アプリケーションイベントを含む Windows イベントログファイルを削除できます。

## 本製品の補助コンポーネントによるローカルでのデータ取り扱い方法

Kaspersky Embedded Systems Security のインストールパッケージには、本製品の補助コンポーネントが含まれています。これらの補助コンポーネントは、Kaspersky Embedded Systems Security がインストールされていないデバイスにもインストールできます。補助コンポーネントとして次のコンポーネントが挙げられます：

- アプリケーションコンソール：Kaspersky Embedded Systems Security の管理ツールセットに含まれ、Microsoft 管理コンソールのスナップインとして動作するコンポーネントです。
- 管理プラグイン：Kaspersky Security Center と本製品との完全な連携を提供するコンポーネントです。

このガイドで説明されている本製品の主要な機能の実行時、本製品の補助コンポーネントはそれぞれがインストールされている保護対象デバイスのローカルでデータを処理し、保存します。これは、補助コンポーネントが Kaspersky Embedded Systems Security 本体とは別のデバイスにインストールされている場合にも当てはまります。

それぞれの補助コンポーネントは次のデータをローカルで処理し、保存します：

- アプリケーションコンソール：Kaspersky Embedded Systems Security がインストールされており、アプリケーションコンソールが最後にリモート接続した保護対象デバイスの名前（IP アドレスまたはドメイン名）、Microsoft 管理コンソールのスナップインで設定された表示パラメータ、アプリケーションコンソールが最後に選択したオブジェクトが含まれるフォルダーに関するデータ（[**参照**] をクリックしてシステムダイアログを開きオブジェクトを選択した場合）。アプリケーションコンソールのトレースファイルには次の情報が含まれます：Kaspersky Embedded Systems Security がインストールされており、リモート接続が確立された保護対象デバイスの名前、リモート接続の確立に使用されたユーザーアカウント名。
- 管理プラグインは、Kaspersky Embedded Systems Security が処理したデータを処理し、一時的に保存します。該当するデータとして、たとえば、本製品のタスクとコンポーネントで指定した設定、Kaspersky Security Center のポリシーの設定、ネットワークリストで送信されたデータなどが含まれます。

ダンプファイルとトレースファイルに書き込まれたデータの、Kaspersky Embedded Systems Security によるローカル処理と保存に関する情報は、次の表の通りです。

Kaspersky Embedded Systems Security は、ダンプファイルとトレースファイルに書き込まれた次のデータをローカルで処理し、保存します：

- Kaspersky Embedded Systems Security によって保護対象デバイス上で実行された処理に関する情報。
- Kaspersky Embedded Systems Security によって処理されたオブジェクトに関する情報。
- Kaspersky Embedded Systems Security によって処理された保護対象デバイスの動作に関する情報。
- Kaspersky Embedded Systems Security の実行中に発生したエラーに関する情報。

補助コンポーネントがローカルで処理したデータが、カスペルスキーのシステムやその他のサードパーティのシステムに自動的に送信されることはありません。

既定では、本製品の補助コンポーネントが動作中にローカルで処理したすべてのデータは、該当する補助コンポーネントをアンインストールすると削除されます。

例外は、補助アプリケーションコンポーネントのトレースファイルです。これらのファイルは手動で削除することを推奨します。

## トレースファイルとダンプファイルのデータ

Kaspersky Embedded Systems Security の動作中にテクニカルサポートが対応できるようにするため、Kaspersky Embedded Systems Security は設定に応じて、トレースファイルにデバッグ情報を書き込むことができます。

Kaspersky Embedded Systems Security のダンプファイルは、アプリケーションのクラッシュ時にオペレーティングシステムによって生成されます。次のクラッシュが起こると、そのダンプファイルに上書きされます。

トレースファイルとダンプファイルには、ユーザーの個人データや組織の機密データを含めることができます。

組織のポリシーによってデータの送信が禁止されているデバイスでは、Kaspersky Embedded Systems Security を使用しないでください。

既定では、デバッグ情報は記録されません。

トレースファイルとダンプファイルは、それらが生成されたコンピューターから自動的に送信されることはありません。トレースファイルの内容は、標準のテキストファイルビューアーを使用して表示できます。トレースファイルとダンプファイルは無期限に保持され、Kaspersky Embedded Systems Security をアンインストールしても削除されません。

デバッグ情報はテクニカルサポートに役立ちます。

トレースファイルとダンプファイルへのアクセスを制限するための特別なメカニズムは提供していません。管理者は、このデータが保護されたフォルダーに書き込まれるように設定できます。

トレースファイルとダンプファイルのフォルダーへのパスは、既定では設定されていません。トレースファイルとダンプファイルのフォルダーを使用するには、管理者がフォルダーを指定する必要があります。

トレースファイルとダンプファイルのデータには、次のものを含めることができます：

- Kaspersky Embedded Systems Security によって保護対象デバイス上で実行された処理に関する情報。
- Kaspersky Endpoint Agent によって処理されるオブジェクトに関する情報。
- Kaspersky Endpoint Agent の操作中に発生するエラー。

# 欧州連合の規則（GDPR）の順守

Kaspersky Embedded Systems Security は次の方法でデータをカスペルスキーに送信することがあります：

- Kaspersky Security Network を使用する
- 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
- 製品機能と定義データベースをアップデートする
- アプリケーションコンソールでリンクを使用する

データの分類およびどこからデータを受け取ったかにかかわらず、カスペルスキーは高い水準のデータセキュリティ対策を遵守し、お客様のデータを保護するためにさまざまな法的、組織的および技術的な手法を取り入れてデータのセキュリティおよび機密性を保証し、適用法によりお客様の権利を確保します。プライバシーポリシーの本文は製品の配信キットに含まれており、カスペルスキーの Web サイトでも参照いただけます。

Kaspersky Embedded Systems Security を使用する前に、使用許諾契約書および Kaspersky Security Network に関する声明の転送されるデータの説明（Kaspersky Security Network に関する声明に記載）をよく読み、ご確認ください。説明されている方法で Kaspersky Embedded Systems Security から転送される特定のデータが、お客様の地域の法律または基準により個人データと分類される場合は、これらのデータは合法的に処理され、このようなデータの転送および収拾についてはお客様の同意のもと行われるものであることをお客様自身が保証する必要があります。

使用許諾契約書および Kaspersky Security Network に関する声明に同意した後の製品使用状況に関する情報の取得、処理、保存、破棄の詳細な方法については、使用許諾契約書を読み、カスペルスキーの Web サイトをご参照ください。ファイル license.txt および ksn_<言語 ID>.txt には、使用許諾契約書および Kaspersky Security Network に関する声明の本文が記載されています。これらは本製品の配信キットに含まれています。

カスペルスキーにデータを送信したくない場合は、データの提供を無効にすることができます。

## Kaspersky Security Network の使用

Kaspersky Security Network を使用することで、お客様は自動的に Kaspersky Security Network に関する声明で説明されるデータを提供することに合意したものとします。カスペルスキーへのこのようなデータの提供に同意しない場合は、Kaspersky Private Security Network (KPSN) を使用するか、KSN の使用を無効にしてください。

## アクティベーションコードによる製品のアクティベーション

アクティベーションコードを使用することで、お客様は使用許諾契約書に記載されているデータを自動的に提供することに同意するものとします。カスペルスキーへのデータの提供に同意しない場合は、ライセンス情報ファイルを使用して Kaspersky Embedded Systems Security をアクティベートしてください。

## 製品機能と定義データベースをアップデートする

カスペルスキーのサーバーを使用することで、お客様は使用許諾契約書に記載されているデータを自動的に提供することに同意するものとします。カスペルスキーは、この情報を Kaspersky Embedded Systems Security が合法的に使用されていることを検証するために使用します。このような情報をカスペルスキーに提供したくない場合、Kaspersky Security Center を使用してデータベースをアップデートしてください。

## アプリケーションコンソールでリンクを使用する

アプリケーションコンソールのリンクを使用することで、お客様は使用許諾契約書に記載されているデータを自動的に提供することに同意するものとします。特定のリンクがどのようなデータを提供するかについては、アプリケーションコンソールのどこにあるリンクか、またどのような問題を解決しようとしているかによって異なります。この情報をカスペルスキーに提供することに同意しない場合は、製品インターフェイスの表示を無効にしてください。

# Kaspersky Embedded Systems Security の起動と終了

このセクションでは、Kaspersky Embedded Systems Security の起動と終了、Kaspersky Embedded Systems Security コンソールの起動、および Kaspersky Security Center 管理コンソールに対応した管理プラグインの起動について説明します。

## 本製品の起動と停止

Kaspersky Embedded Systems Security をユーザーのコンピューターにインストールすると、製品が自動的に起動されます。既定では、Kaspersky Embedded Systems Security はオペレーティングシステムが起動してから起動します。オペレーティングシステムの設定でアプリケーションの自動起動を構成することはできません。

オペレーティングシステムの起動後 Kaspersky Embedded Systems Security の定義データベースをダウンロードするには、コンピューターの性能によって最大 2 分かかることがあります。その間、コンピューターの保護レベルが低下します。既に起動したオペレーティングシステム上で Kaspersky Embedded Systems Security を起動したときの定義データベースのダウンロードでは、コンピューターの保護レベルは低下しません。

**Kaspersky Security Center 管理コンソールで本製品の自動起動を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**アプリケーション設定**］→［**セキュリティと信頼性**］の順に選択し、［**設定**］をクリックします。
4. ［**セキュリティ**］タブで、［**コンピューターの開始時に本製品を開始する（推奨）**］をオンまたはオフにして、本製品の自動起動を有効または無効にします。
5. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで本製品の自動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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**アプリケーション設定**］→［**セキュリティと信頼性**］に移動します。

5. ［**設定**］をクリックします。
［**セキュリティと信頼性**］ウィンドウが表示されます。
6. ［**コンピューターの開始時に本製品を開始する（推奨）**］を使用して製品の自動起動を有効または無効にします。
7. 変更内容を保存します。

*アプリケーションコンソールで本製品の自動起動を設定する方法*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択します。
2. フォルダーのコンテキストメニューで［**アプリケーションのプロパティ**］を選択します。
3. ウィンドウが表示されるので、そのウィンドウで［**セキュリティ設定**］タブを選択します。
4. ［**コンピューターの開始時に本製品を開始する（推奨）**］を使用して製品の自動起動を有効または無効にします。
5. 変更内容を保存します。

保護対象デバイスの管理者グループのメンバーは、Kaspersky Embedded Systems Security を開始および停止することができます。

**Kaspersky Security Center 管理コンソールで本製品を起動または停止する方法**

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、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。
2. 作業領域で、［**デバイス**］タブを選択します。
3. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
4. コンピューター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。
5. コンピューターにインストールされているカスペルスキー製品のリストで、［**Kaspersky Embedded Systems Security for Windows (4.0.0)**］を選択します。
6. 次のいずれかを行います：
   - 本製品を起動するには、カスペルスキー製品リストの右側にある ボタンをクリックします。
   - 本製品を停止するには、カスペルスキー製品リストの右側にある ボタンをクリックします。

### Kaspersky Security Center Web コンソールで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。
2. 本製品を起動または停止するコンピューターを選択します。
   コンピューターのプロパティウィンドウが開きます。
3. ［**アプリケーション**］タブを選択します。
4. **Kaspersky Embedded Systems Security for Windows (4.0.0)** のチェックボックスを選択します。
5. ［**開始**］または［**停止**］をクリックします。

### *アプリケーションコンソールで本製品を起動または停止する方法*

1. アプリケーションコンソールツリーの［**Kaspersky Embedded Systems Security**］フォルダーの作業領域内で、［**リモートコンピューターに接続**］をクリックします。
2. 本製品の再起動のメッセージで、［**はい**］をクリックします。
3. ［**保護対象デバイスの選択**］ウィンドウの［**サービスの管理**］の横で、次のいずれかを行います：
   - 製品を停止する場合は、［**停止**］をクリックします。
   - 製品を起動する場合は、［**開始**］をクリックします。

本製品が停止または起動されます。

［**保護対象デバイスの選択**］ウィンドウは、本製品がインストールされているコンピューターとの接続が失われた場合や、KESS サービスに障害が発生した場合にも表示されます。［**開始**］をクリックして KESS サービスを復元できます。

### *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*

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。
2. cd コマンドを使用して、ファイル klpsm.exe および kavshell.exe があるフォルダーに移動します。
   例：`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0`

3. コマンドラインから本製品を起動するには、次のいずれかのコマンドを実行します：

   - `klpsm.exe start_avp_service`

   - `KAVSHELL start [/login:<現在のユーザーアカウントの名前>] [/PWD:</login のパスワードまたは /login が指定されていない場合は KLAdmin パスワード>]`

4. コマンドラインから本製品を停止するには、次のいずれかのコマンドを実行します：

   - `klpsm.exe stop_avp_service`

   - `KAVSHELL stop [/login:<現在のユーザーアカウントの名前>] [/PWD:</login のパスワードまたは /login が指定されていない場合は KLAdmin パスワード>]`

# プロテクションとコントロールの一時停止と再開

プロテクションとコントロールを一時停止すると、Kaspersky Embedded Systems Security の保護および管理コンポーネントが一時的にすべて無効になります。

製品のステータスは、タスクバーの通知領域の製品アイコンによって示されます。

- アイコンは、コンピュータープロテクションとコントロールが一時停止されていることを表します。
- アイコンは、コンピュータープロテクションとコントロールが有効になっていることを表します。

プロテクションとコントロールを一時停止または再開しても、スキャンまたはアップデートタスクには影響ありません。

プロテクションとコントロールを一時停止または再開するときにネットワーク接続が既に確立されている場合、ネットワーク接続の中断に関する通知が表示されます。

*プロテクションとコントロールを一時停止するには：*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューを開きます。
2. ［**保護機能を一時停止する**］を選択します。
3. 次のいずれかのオプションを選択します：

   - **指定した時間だけ一時停止する**：プロテクションとコントロールは、下部のドロップダウンリストで指定した時間が経過すると再開されます。
   - **再起動まで一時停止する**：プロテクションとコントロールは、製品を終了して再開したとき、またはオペレーティングシステムを再起動したときに再開されます。このオプションを使用するには、自動起動を有効にする必要があります。
   - **一時停止**：プロテクションとコントロールは、再び有効にしたときに再開されます。

Kaspersky Embedded Systems Security はポリシーでロック（）が設定されていないすべての保護機能および管理コンポーネントの動作を一時的に停止します。

*プロテクションとコントロールを再開するには：*

1. タスクバーの通知領域にある製品アイコンの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から［**保護機能を再開する**］を選択します。

プロテクションとコントロールは、選択したプロテクションとコントロールの一時停止オプションに関係なく、いつでも再開できます。

# コンパクト診断インターフェイス

このセクションでは、コンパクト診断インターフェイスの使用について説明します。

## コンパクト診断インターフェイスについて

コンパクト診断インターフェイス（「CDI」とも表記）は、アプリケーションコンソールが保護対象デバイスにインストールされていない場合、アプリケーションコンソールとは独立して、システムトレイアイコンとともにインストールおよびアンインストールされます。コンパクト診断インターフェイスは、システムトレイアイコンから起動します。また、保護対象デバイスのアプリケーションフォルダーから avpui.exe を実行することでも起動できます。

コンパクト診断インターフェイスでは、次のことを実行できます：

- ［**製品情報**］ウィンドウが開き、インストールされているアップデートおよび使用できるパッチのリストが表示されます。
- 全般的なアプリケーションステータスに関する情報を確認する。
- 発生したセキュリティインシデントを確認する。
- 保護対象デバイスで現在のアプリケーションの動作を確認する。
- ダンプファイルおよびトレースファイルの書き込みを開始または停止する。
- アプリケーションコンソールを開きます。

Kaspersky Embedded Systems Security の機能へのアクセスがパスワードで保護されている場合でも、コンパクト診断インターフェイスは使用可能です。パスワードは必要ありません。

コンパクト診断インターフェイスは、Kaspersky Security Center を使用して設定できません。

## コンパクト診断インターフェイスを使用した Kaspersky Embedded Systems Security ステータスの確認

*コンパクト診断インターフェイスを使用して本製品のステータスを表示するには：*

1. 次のいずれかの方法でコンパクト診断インターフェイスを開きます：
   - 保護対象デバイスのアプリケーションのインストールフォルダーにあるファイル avpui.exe を実行します。既定では、ファイルは C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0 にあります。
   - タスクバーの通知エリアの製品アイコンをクリックします。

2. ［**保護の状態**］セクションで、ライセンスの現在のステータス、コンピューターのリアルタイム保護タスク、およびアップデートタスクを確認します。保護ステータスをユーザーに通知するために、異なる色で表示されます（次の表を参照）。

コンパクト診断インターフェイスウィンドウの色表示

| セクション | ステータス |
| --- | --- |
| **リアルタイム保護の状態** | 次のいずれかの場合、パネルは*緑色*で表示されます（当てはまる条件の数は問いません）：<br>• 推奨構成：<br>  • ファイルのリアルタイム保護タスクが既定の設定で開始されている。<br>  • アプリケーション起動コントロールタスクが、既定の設定で**ブロックする**モードで開始されている。<br>• 許容できる構成：<br>  • ファイルのリアルタイム保護タスクがユーザーにより設定されている。<br>  • アプリケーション起動コントロールタスクの設定が変更されている。 |
| | 次のいずれかの条件に1つでも当てはまる場合、パネルは*黄色*で表示されます：<br>• ファイルのリアルタイム保護タスクが一時停止されている（ユーザーまたはスケジュールにより）。<br>• アプリケーション起動コントロールタスクが**通知**モードで開始されている。<br>• 脆弱性攻撃ブロックとアプリケーション起動コントロールが**通知**モードで開始されている。 |
| | 次の条件の両方に当てはまる場合、パネルは*赤色*で表示されます：<br>• ファイルのリアルタイム保護がインストールされていないか、タスクが停止または一時停止されている。<br>• アプリケーション起動コントロールがインストールされていないか、タスクが**通知**モードで開始されている。 |
| **ライセンス** | 現在のライセンスが有効な場合、パネルは*緑色*で表示されます。 |
| | パネルが*黄色*で表示される場合は、次のいずれかのイベントが発生したことを示します：<br>• *ライセンスのステータスの確認。*<br>• *ライセンスの有効期間の残り日数が30日で、予備のライセンスまたはアクティベーションコードが追加されていない。*<br>• *追加されたライセンスが拒否リストに含まれていて、ブロックされる予定である。* |
| | パネルが*赤色*で表示される場合は、次のいずれかのイベントが発生したことを示します：<br>• *アクティベートされていません。*<br>• *ライセンスの有効期間が終了しています。*<br>• *使用許諾契約書に違反しています。*<br>• *ライセンスが拒否リストに登録されています。* |
| **アップデート** | 定義データベースが最新の場合、パネルは*緑色*で表示されます。 |
| | 定義データベースがアップデートされていない場合、パネルは*黄色*で表示されます。 |
| | 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、パネルは*赤色*で表示されます。 |

# セキュリティイベント統計の確認

［**使用統計**］セクションには、すべてのセキュリティイベントが表示されます。保護タスクごとに統計情報がそれぞれのブロックに表示され、インシデント数と最後にインシデントが発生した日時が示されます。インシデントが記録されると、ブロックの色は赤に変わります。

*統計情報を表示するには：*

1. 次のいずれかの方法でコンパクト診断インターフェイスを開きます：

   - 保護対象デバイスのアプリケーションのインストールフォルダーにあるファイル avpui.exe を実行します。既定では、ファイルは C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0 にあります。

   - タスクバーの通知エリアの製品アイコンをクリックします。

2. ［**使用統計**］に移動します。

3. 保護タスクのセキュリティインシデントを確認します。

# 現在のアプリケーション動作の確認

*保護対象デバイス上で現在のアプリケーション動作を確認するには：*

1. 次のいずれかの方法でコンパクト診断インターフェイスを開きます：

   - 保護対象デバイスのアプリケーションのインストールフォルダーにあるファイル avpui.exe を実行します。既定では、ファイルは C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0 にあります。

   - タスクバーの通知エリアの製品アイコンをクリックします。

2. ［**現在のアプリケーションの動作**］に移動します。

アプリケーション動作ステータスを示すために、異なる色で表示されます：

- ［**タスク**］セクション：

  - *緑色*：黄色や赤色となる条件がありません。

  - *黄色*：重要領域の簡易スキャンが長期間実行されていません。

  - *赤色*：次のいずれかの条件のうち、少なくとも 1 つの条件を満たしています：

    - タスクが開始されず、開始スケジュールがタスクに対して設定されていない。

    - アプリケーション起動エラーが重要なイベントとして記録されている。

- ［**Kaspersky Security Network**］セクション：

  - *緑色*：**KSN の使用**タスクが開始されています。

  - *黄色*：KSN 声明に同意しているが、タスクが開始されていない。

# アプリケーショントレースとメモリダンプの記録の設定

*アプリケーショントレースとメモリダンプの記録を設定するには：*

1. 次のいずれかの方法でコンパクト診断インターフェイスを開きます：

   - 保護対象デバイスのアプリケーションのインストールフォルダーにあるファイル avpui.exe を実行します。既定では、ファイルは C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0 にあります。

   - タスクバーの通知エリアの製品アイコンをクリックします。

2. ［**誤作動診断**］に移動します。

3. ［**デバッグ情報をトレースファイルに書き込む**］を使用してアプリケーションの操作の追跡を有効または無効にします。

4. 必要に応じて、［**参照**］をクリックして、トレースファイルを保存するフォルダーを指定します。

   フォルダーは事前に作成し、SYSTEM アカウントで書き込み可能にする必要があります。ネットワークフォルダー、ドライブ、環境変数は指定できません。

5. ［**詳細レベル**］ドロップダウンリストから、デバッグ情報の詳細レベルを選択します。

   - **緊急**：トレースファイルには、深刻なエラーに関するメッセージのみが保存されます。

   - **診断**：トレースファイルには、すべてのエラーと警告に関するメッセージが保存されます。

   - **重要**：トレースファイルには、すべてのエラー、警告、および追加情報に関するメッセージが保存されます。

   - **通常**：トレースファイルには、すべてのエラー、警告、および本製品の通常の処理に関する情報に関するメッセージが保存されます（既定）。

   - **詳細**：トレースファイルには、本製品の処理に関するすべての情報が保存されます。

   発生した問題を解決するために必要な詳細レベルは、テクニカルサポートが判断します。

   既定の詳細レベルは、［**通常**］に設定されています。

6. **トレースファイルの最大サイズ（MB）**を指定します。

   使用可能な値：1～4095 MB。既定では、トレースファイルの最大サイズは 100 MB に設定されています。

7. ファイルの最大数に達した時に古いトレースファイルを削除するには、［**古いトレースファイルを削除する**］をオンにします。

8. **トレースファイルの最大数**を指定します。

   使用可能な値：1～999。既定では、ファイルの最大数は 5 に設定されています。このフィールドは、［**古いトレースファイルを削除する**］をオンにした場合に使用できます。

9. 必要に応じて、メモリダンプを設定します：

   a. ［**誤動作のダンプファイルを次のフォルダーに作成する**］をオンまたはオフにして、誤動作が発生した場合のメモリダンプを有効または無効にします。

   b. 必要に応じて、［**参照**］をクリックして、メモリダンプファイルを保存するフォルダーを指定します。既定では、メモリダンプファイルは %ProgramData%\Kaspersky Lab\KESS.4.0\Traces のフォルダーに保存されます。

      フォルダーは事前に作成し、SYSTEM アカウントで書き込み可能にする必要があります。ネットワークフォルダー、ドライブ、環境変数は指定できません。

10. ［**適用**］をクリックします。

# Kaspersky Embedded Systems Security のセルフディフェンス機構

セルフディフェンスは、他のアプリケーションが Kaspersky Embedded Systems Security の動作を妨げる可能性のある処理を実行することを防ぎます。本製品はセルフディフェンス機構を備えており、本製品のフォルダー、メモリプロセス、システムレジストリエントリを改変や削除から保護します。Kaspersky Embedded Systems Security は、悪意のある活動からアプリケーションプロセスを保護する Microsoft の Antimalware Protected Process Light（AM-PPL）技術をサポートします。さらに、本製品では、製品機能と製品のサービスへのユーザーアクセス権限を個別に管理できます。

## セルフディフェンスの有効化と無効化

Kaspersky Embedded Systems Security によってハードディスクのアプリケーションファイル、メモリプロセス、システムレジストリエントリの改竄や削除が防止されます。

次の製品コンポーネントへのアクセスをブロックします：

- Kaspersky Embedded Systems Security のインストールフォルダーにあるファイルおよび本製品のファイル
- 本製品に属する項目を含むレジストリキー
- 本製品が実行するプロセス

既定では、Kaspersky Embedded Systems Security のセルフディフェンス機構は有効です。

**Kaspersky Security Center 管理コンソールでセルフディフェンスを有効または無効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］をクリックします。
4. ［**セキュリティと信頼性**］ブロックの［**設定**］をクリックします。
5. ウィンドウが表示されるので、そのウィンドウで［**セキュリティ**］タブを選択します。
6. ［**セルフディフェンス**］ブロックで、［**アプリケーションプロセスを外部の脅威から保護する**］チェックボックスを使用して、セルフディフェンスを有効または無効にします。
7. コンピューターにポリシーを適用するには、南京錠（）を閉じます。
8. ［**OK**］をクリックして、変更内容を保存します。

*アプリケーションコンソールでセルフディフェンスを有効または無効にする方法*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、結果ペインで［**アプリケーションのプロパティ**］をクリックします。
2. ウィンドウが表示されるので、そのウィンドウで［**セキュリティ設定**］タブを選択します。
3. ［**セルフディフェンス**］ブロックで、［**アプリケーションプロセスを外部の脅威から保護する**］チェックボックスを使用して、セルフディフェンスを有効または無効にします。
4. ［**OK**］をクリックして、変更内容を保存します。

**Kaspersky Security Center Web コンソールでセルフディフェンス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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**アプリケーション設定**］セクションを選択します。
5. ［**セキュリティと信頼性**］ブロックの［**設定**］をクリックします。
   ［**セキュリティと信頼性**］ウィンドウが表示されます。
6. ［**セルフディフェンス**］ブロックで、［**アプリケーションプロセスを外部の脅威から保護する**］チェックボックスを使用して、セルフディフェンスを有効または無効にします。
7. コンピューターにポリシーを適用するには、南京錠（）を閉じます。
8. ［**OK**］をクリックして、変更内容を保存します。

# AM-PPL 技術のサポート

Kaspersky Embedded Systems Security は Microsoft の Antimalware Protected Process Light 技術（以降、「AM-PPL」）をサポートします。AM-PPL は、Kaspersky Embedded Systems Security のプロセスを悪意のある処理（アプリケーションの終了など）から保護します。AM-PPL が実行を許可するのは信頼するプロセスのみです。Kaspersky Embedded Systems Security のプロセスは Windows のセキュリティ要件に従って署名されているため、信頼するプロセスとして扱われます。AM-PPL 技術について詳しくは、Microsoft の Web サイトの情報を参照してください。既定では、AM-PPL 技術が有効です。

また、Kaspersky Embedded Systems Security には製品のプロセスを保護するための機構が組み込まれています。AM-PPL のサポートにより、プロセスのセキュリティ機能をオペレーティングシステムに委任できます。したがって、本製品の動作速度を向上し、コンピューターリソースの消費量を削減できます。

本製品は、Kaspersky Embedded Systems Security（AVP）サービスと Kaspersky Seamless Update Service（AVPSUS）サービスを登録します。AM-PPL 技術は AVP サービスのみを保護します。

AM-PPL 技術は常に有効にしてください。AM-PPL は、オペレーティングシステムの防御の重要なコンポーネントです。AM-PPL の無効化は、本製品のトラブルシューティングの目的で、個別のテスト環境で行う場合にのみ許可されます。

AM-PPL 技術は Windows 10 バージョン 1703（RS2）以降および Windows Server 2019 で利用できます。

*AM-PPL 技術を有効または無効にするには：*

1. 製品のセルフディフェンス機構を無効にします。

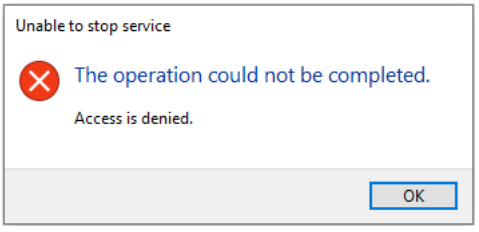
   セルフディフェンス機構は、AM-PPL の状態の変更を含めて、コンピューターメモリ内で本製品のプロセスが変更されたり削除されたりしないようにします。

2. 管理者としてコマンドラインインタープリタ（cmd）を実行します。
3. Kaspersky Embedded Systems Security の実行ファイルがあるフォルダーに移動します。
4. コマンドラインに以下のように入力します：

   - `klpsm.exe enable` – AM-PPL 技術のサポートを有効にします。
   - `klpsm.exe disable` – AM-PPL 技術のサポートを無効にします。

5. Kaspersky Embedded Systems Security を再起動します。
6. 製品のセルフディフェンス機構を再び有効にします。

その結果、ユーザーが AVP サービスを停止しようとすると、システムウィンドウにエラーメッセージが表示されます。ユーザーは、Kaspersky Embedded Systems Security インターフェイスからのみアプリケーションサービスを管理できます。




アプリケーションサービスアクセスエラー

# オペレーティングシステムのサービスの保護

*オペレーティングシステムのサービスを保護する*機能を使用して、オペレーティングシステムのサービスに対するサードパーティ製アプリケーションの処理を許可または禁止できます。

### Kaspersky Security Center 管理コンソールでオペレーティングシステムのサービスの保護を有効または無効にする方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］をクリックします。
4. ［**セキュリティと信頼性**］ブロックの［**設定**］をクリックします。
5. ウィンドウが表示されるので、そのウィンドウで［**セキュリティ**］タブを選択します。
6. ［**オペレーティングシステムのサービスを保護する**］を使用してオペレーティングシステムのサービスの保護を有効または無効にします。

   オペレーティングシステムのサービスの保護が有効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することはできません。

   オペレーティングシステムのサービスの保護が無効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することができます。

   機能を有効または無効にした後で、変更を適用するにはコンピューターを再起動する必要があります。
7. コンピューターにポリシーを適用するには、南京錠（）を閉じます。
8. ［OK］をクリックして、変更内容を保存します。

*アプリケーションコンソールでオペレーティングシステムのサービスの保護を有効または無効にする方法*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、結果ペインで［**アプリケーションのプロパティ**］をクリックします。
2. ウィンドウが表示されるので、そのウィンドウで［**セキュリティ設定**］タブを選択します。
3. ［**オペレーティングシステムのサービスを保護する**］を使用してオペレーティングシステムのサービスの保護を有効または無効にします。

   オペレーティングシステムのサービスの保護が有効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することはできません。

   オペレーティングシステムのサービスの保護が無効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することができます。

   機能を有効または無効にした後で、変更を適用するにはコンピューターを再起動する必要があります。
4. ［OK］をクリックして、変更内容を保存します。

**Kaspersky Security Center Web コンソールでオペレーティングシステムのサービスの保護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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**アプリケーション設定**］セクションを選択します。
5. ［**セキュリティと信頼性**］ブロックの［**設定**］をクリックします。
   ［**セキュリティと信頼性**］ウィンドウが表示されます。
6. ［**オペレーティングシステムのサービスを保護する**］を使用してオペレーティングシステムのサービスの保護を有効または無効にします。
   オペレーティングシステムのサービスの保護が有効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することはできません。
   オペレーティングシステムのサービスの保護が無効になっている場合、サードパーティ製アプリケーションはオペレーティングシステムのプロセスに対して処理を実行することができます。
   機能を有効または無効にした後で、変更を適用するにはコンピューターを再起動する必要があります。
7. コンピューターにポリシーを適用するには、南京錠（）を閉じます。
8. ［OK］をクリックして、変更内容を保存します。

# Kaspersky Embedded Systems Security を管理するためのユーザー権限の設定

既定では、保護対象デバイスの Administrators グループのメンバー、Kaspersky Embedded Systems Security のインストール時に保護対象デバイスに作成された ESS Administrators グループのメンバー、および SYSTEM グループは、Kaspersky Embedded Systems Security の全機能にアクセスできます。

Kaspersky Embedded Systems Security ユーザーのリストに登録されていないユーザーは、アプリケーションコンソールを開くことができません。

個々のユーザーまたはユーザーグループに対して、Kaspersky Embedded Systems Security の特定の機能へのアクセスを許可またはブロックできます。

Kaspersky Embedded Systems Security の各種機能に対するアクセス権限

| ユーザー権限 | 説明 |
| --- | --- |
| タスクの管理 | Kaspersky Embedded Systems Security タスクを開始、停止、一時停止、または再開できます。 |
| タスクの作成および削除 | オンデマンドスキャンタスクを作成および削除できます。 |
| 設定の編集 | 以下の操作を実行できます：<br>• 設定情報ファイルからの Kaspersky Embedded Systems Security の設定のインポート。<br>• 製品設定の編集。 |

| ユーザー権限 | 説明 |
| --- | --- |
| 設定の読み取り | 以下の操作を実行できます：<br>• Kaspersky Embedded Systems Security 全般的な設定とタスクの設定の表示。<br>• Kaspersky Embedded Systems Security 設定の設定情報ファイルへのエクスポート。<br>• 実行ログ、システム監査ログ、および通知に関する設定の表示。 |
| 保管領域の管理 | 以下の操作を実行できます：<br>• オブジェクトの隔離への移動<br>• 隔離およびバックアップからのオブジェクトの削除<br>• 隔離およびバックアップからのオブジェクトの復元 |
| ログの管理 | タスク実行ログとシステム監査ログを削除できます。 |
| ログの読み取り | タスク実行ログとシステム監査ログのアンチウイルスイベントを表示できます。 |
| 統計情報の取得 | 各 Kaspersky Embedded Systems Security タスクの統計情報を表示できます。 |
| 製品ライセンスの管理 | Kaspersky Embedded Systems Security のアクティベーションを実行できます。 |
| 本製品のアンインストール | Kaspersky Embedded Systems Security をアンインストールできます。 |
| 読み取り権限 | Kaspersky Embedded Systems Security ユーザーとユーザーごとのアクセス権限のリストを表示できます。 |
| 編集権限 | 以下の操作を実行できます：<br>• アプリケーション管理のアクセス権を持つユーザーリストの編集。<br>• Kaspersky Embedded Systems Security の各種機能に対するユーザーアクセス権限を編集します。 |
| アプリケーションへのリモート接続 | アプリケーションコンソールを使用して本製品にリモート接続できます。<br>リモートアクセスの場合、ユーザーは［**設定の読み取り**］機能へのアクセス権も持っている必要があります。 |
| 本製品の終了 | アプリケーションコンソールを使用して本製品を終了できます。 |
| Kaspersky Security Center ポリシーを無効にする | Kaspersky Security Center ポリシーを無効化できます。 |
| 設定のエクスポート | Kaspersky Embedded Systems Security の設定をエクスポートできます。 |

### Kaspersky Security Center 管理コンソールで Kaspersky Embedded Systems Security を管理するためのユーザー権限を設定する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**詳細設定**］を選択します。
4. ［**アプリケーション管理用のユーザーアクセス権限**］セクションで、［**設定**］をクリックします。
5. 表示されたウィンドウで、［**手動で作成したユーザーの資格情報を使用して、製品操作を確定することを許可する**］を選択して KLAdmin ユーザーアカウントのパスワードを設定します。ユーザーアカウントは、ユーザーアカウントのリストに自動的に追加されます。
6. 必要に応じて、アプリケーション管理へのアクセスを許可するユーザーアカウントを追加します。これを行うには、ユーザーアカウントのテーブルで［**追加**］をクリックします。

   これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。

7. ユーザーを追加するために使用する方法を選択します：

   - **Active Directory からユーザーまたはグループを選択する**：Active Directory ドメイン内の個々のユーザーまたはグループに、Kaspersky Embedded Systems Security へのアクセス権を付与できます。たとえば、Everyone グループに対して「本製品の終了」操作がブロックされている場合でも、［**本製品の終了**］権限を個別のユーザーに対して付与できます。

   - **ユーザーまたはユーザーグループを手動で追加する**：Active Directory 内に存在しないユーザーアカウントを作成し、そのユーザーアカウントに個別の権限を割り当てることができます。つまり、KLAdmin の代わりに *サービスユーザーアカウント*を作成して使用できます。これにより、KLAdmin パスワードを他のユーザーと共有したり、新しい Active Directory ユーザーアカウントを作成したりする必要がなくなります。任意のユーザー名とパスワードを指定できます。たとえば、サービスユーザーアカウントに［**ログの読み取り**］権限を付与することができます。これにより、［すべて］グループに対してレポートの表示が禁止された場合は、サービスユーザーアカウントまたは KLAdmin ユーザーアカウントを使用してレポートを開くことができます。

     ユーザーまたはユーザーグループを手動で追加するには、パスワードによる保護を有効にする必要があります。

8. 本製品を管理するためにアクセスを許可するユーザーまたはユーザーグループを選択します。

9. ［**権限**］リストで、製品機能へのユーザーのアクセス権限を設定します。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

***アプリケーションコンソールで Kaspersky Embedded Systems Security を管理するためのユーザー権限を設定する方法***

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**アプリケーション管理用のユーザーアクセス権限**］を選択します。

2. 表示されたウィンドウで、［**手動で作成したユーザーの資格情報を使用して、製品操作を確定することを許可する**］を選択して KLAdmin ユーザーアカウントのパスワードを設定します。ユーザーアカウントは、ユーザーアカウントのリストに自動的に追加されます。

3. 必要に応じて、アプリケーション管理へのアクセスを許可するユーザーアカウントを追加します。これを行うには、ユーザーアカウントのテーブルで［**追加**］をクリックします。

   これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。

4. ユーザーを追加するために使用する方法を選択します：

   - **Active Directory からユーザーまたはグループを選択する**：Active Directory ドメイン内の個々のユーザーまたはグループに、Kaspersky Embedded Systems Security へのアクセス権を付与できます。たとえば、Everyone グループに対して「本製品の終了」操作がブロックされている場合でも、［**本製品の終了**］権限を個別のユーザーに対して付与できます。

   - **ユーザーまたはユーザーグループを手動で追加する**：Active Directory 内に存在しないユーザーアカウントを作成し、そのユーザーアカウントに個別の権限を割り当てることができます。つまり、KLAdmin の代わりに *サービスユーザーアカウント*を作成して使用できます。これにより、KLAdmin パスワードを他のユーザーと共有したり、新しい Active Directory ユーザーアカウントを作成したりする必要がなくなります。任意のユーザー名とパスワードを指定できます。たとえば、サービスユーザーアカウントに［**ログの読み取り**］権限を付与することができます。これにより、［すべて］グループに対してレポートの表示が禁止された場合は、サービスユーザーアカウントまたは KLAdmin ユーザーアカウントを使用してレポートを開くことができます。

     ユーザーまたはユーザーグループを手動で追加するには、パスワードによる保護を有効にする必要があります。

5. 本製品を管理するためにアクセスを許可するユーザーまたはユーザーグループを選択します。

6. ［**権限**］リストで、製品機能へのユーザーのアクセス権限を設定します。

7. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで Kaspersky Embedded Systems Security を管理するためのユーザーアクセス権を設定する方法**

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

2. Kaspersky Embedded Systems 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. ［**詳細設定**］→［**アプリケーション管理用のユーザーアクセス権限**］に移動し、［**設定**］をクリックします。

5. 表示されたウィンドウで、［**手動で作成したユーザーの資格情報を使用して、製品操作を確定することを許可する**］を選択して KLAdmin ユーザーアカウントのパスワードを設定します。ユーザーアカウントは、ユーザーアカウントのリストに自動的に追加されます。

6. 必要に応じて、アプリケーション管理へのアクセスを許可するユーザーアカウントを追加します。これを行うには、ユーザーアカウントのテーブルで［**追加**］をクリックします。

   これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。

7. ユーザーを追加するために使用する方法を選択します：

   - **Active Directory からユーザーまたはグループを選択する**：Active Directory ドメイン内の個々のユーザーまたはグループに、Kaspersky Embedded Systems Security へのアクセス権を付与できます。たとえば、Everyone グループに対して「本製品の終了」操作がブロックされている場合でも、［**本製品の終了**］権限を個別のユーザーに対して付与できます。

   - **ユーザーまたはユーザーグループを手動で追加する**：Active Directory 内に存在しないユーザーアカウントを作成し、そのユーザーアカウントに個別の権限を割り当てることができます。つまり、KLAdmin の代わりに *サービスユーザーアカウント*を作成して使用できます。これにより、KLAdmin パスワードを他のユーザーと共有したり、新しい Active Directory ユーザーアカウントを作成したりする必要がなくなります。任意のユーザー名とパスワードを指定できます。たとえば、サービスユーザーアカウントに［**ログの読み取り**］権限を付与することができます。これにより、［すべて］グループに対してレポートの表示が禁止された場合は、サービスユーザーアカウントまたは KLAdmin ユーザーアカウントを使用してレポートを開くことができます。

     ユーザーまたはユーザーグループを手動で追加するには、パスワードによる保護を有効にする必要があります。

8. 本製品を管理するためにアクセスを許可するユーザーまたはユーザーグループを選択します。

9. ［**権限**］リストで、製品機能へのユーザーのアクセス権限を設定します。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

# Kaspersky Security サービスを管理するためのユーザーアクセス権限

インストール中に、Kaspersky Embedded Systems Security は製品のサービス（Kaspersky Security サービス）を Windows に登録します。したがって、本製品には、オペレーティングシステムの起動時に開始される機能コンポーネントが含まれます。製品のサービスを使用して第三者によって保護対象デバイスの製品機能やセキュリティ設定にアクセスされるリスクを低下させるために、Kaspersky Security サービスを管理する権限を制限することができます。

既定では、Kaspersky Security サービスを管理するためのアクセス権限は、保護対象デバイスの管理者グループのユーザーに付与されます。読み取り権限は SERVICE グループと INTERACTIVE グループに付与され、読み取り権限と実行権限は SYSTEM グループに付与されます。

SYSTEM ユーザーアカウントを削除したり、このアカウントの権限を編集したりすることはできません。SYSTEM アカウントの権限を編集する場合、変更を保存する時に、最大限の権限が回復されます。

編集権限を必要とする機能へのアクセス権を持つユーザーは、保護対象デバイスに登録されているその他のユーザー、またはドメインに含まれているユーザーに対して、Kaspersky Security サービスを管理するためのアクセス権を付与できます。

Kaspersky Security サービスの管理のため、Kaspersky Embedded Systems Security のユーザーまたはユーザーのグループに対し、次のいずれかの設定済み Kaspersky Embedded Systems Security アクセス権限レベルを選択できます：

- **フルコントロール**：Kaspersky Security サービスの全般設定とユーザー権限を表示および編集でき、さらに Kaspersky Security サービスの開始と停止ができます。
- **読み取り**：Kaspersky Security サービスの全般的な設定とユーザー権限を表示できます。
- **編集**：Kaspersky Security サービスの全般的な設定とユーザー権限を表示、変更できます。
- **実行**：Kaspersky Security サービスの開始と停止ができます。

特定の Kaspersky Embedded Systems Security 機能へのアクセスを許可または拒否するように、高度なアクセス権限を指定することもできます（以下の表を参照）。

Kaspersky Security サービスの各機能に対するアクセス権限

| 機能 | 説明 |
| --- | --- |
| サービス設定の読み込み | Kaspersky Security サービスの全般的な設定とユーザー権限を表示できます。 |
| Service Control Manager からのサービスステータスの要求 | Microsoft Windows のサービスコントロールマネージャーから Kaspersky Security サービスの実行ステータスを要求できます。 |
| サービスステータスの要求 | Kaspersky Security サービスからサービス実行ステータスを要求できます。 |
| 依存するサービスのリストの読み込み | Kaspersky Security サービスが依存するサービス、および Kaspersky Security サービスに依存するサービスのリストを表示できます。 |
| サービス設定の変更 | Kaspersky Security サービスの全般的な設定とユーザー権限を表示、変更できます。 |
| サービスの開始 | Kaspersky Security サービスを開始できます。 |
| サービスの停止 | Kaspersky Security サービスを停止できます。 |
| サービスの一時停止/再開 | Kaspersky Security サービスの一時停止と再開ができます。 |
| 読み取り権限 | Kaspersky Security サービスのユーザーのリストと、各ユーザーのアクセス権限を表示できます。 |
| 編集権限 | 以下の操作を実行できます：<br>• Kaspersky Security サービスユーザーの追加と削除。<br>• Kaspersky Security サービスに対するユーザーのアクセス権限を編集します。 |
| サービスの削除 | Microsoft Windows のサービスコントロールマネージャーで Kaspersky Security サービスを登録解除できます。 |
| サービスへのユーザー定義要求 | Kaspersky Security サービスへユーザー要求を作成して送信できます。 |

Kaspersky Security サービスを管理できるユーザーとユーザーグループのリストを編集したり、それらのユーザーとユーザーグループのアクセス権限を編集したりできます。

### Kaspersky Security Center 管理コンソールで Kaspersky Security サービスを管理するためのユーザー権限を設定する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**詳細設定**］を選択します。
4. ［**Kaspersky Security サービス管理用のユーザーアクセス権限**］セクションで、［**設定**］をクリックします。

   これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。

5. Kaspersky Security サービスのユーザー権限を設定する Active Directory ユーザーまたはグループを追加します。

6. 本製品を管理するためにアクセスを許可するユーザーまたはユーザーグループを選択します。

7. 権限のリストで、Kaspersky Security サービスを管理するためのユーザー権限を設定します。

8. 必要に応じて、ユーザーに対して特別な権限を設定します：

   a. ［**詳細**］をクリックします。

   b. 表示されたウィンドウで、ユーザーアカウントを選択します。

   c. ダブルクリックしてユーザーアカウントのプロパティを開きます。

   d. 表示されたウィンドウで、［**追加の権限を表示する**］をクリックします。

   e. 表示されたウィンドウで、そのユーザーに対して特別な権限を設定します。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

***アプリケーションコンソールで Kaspersky Security サービスを管理するためのユーザー権限を設定する方法***

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**Kaspersky Security サービス管理用のユーザーアクセス権限**］を選択します。

2. 表示されたウィンドウで、［**権限**］ブロックの［**追加**］をクリックします。
   これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。

3. Kaspersky Security サービスのユーザー権限を設定する Active Directory ユーザーまたはグループを追加します。

4. 本製品を管理するためにアクセスを許可するユーザーまたはユーザーグループを選択します。

5. 権限のリストで、Kaspersky Security サービスを管理するためのユーザー権限を設定します。

6. 必要に応じて、ユーザーに対して特別な権限を設定します：

   a. ［**詳細**］をクリックします。

   b. 表示されたウィンドウで、ユーザーアカウントを選択します。

   c. ダブルクリックしてユーザーアカウントのプロパティを開きます。

   d. 表示されたウィンドウで、［**追加の権限を表示する**］をクリックします。

   e. 表示されたウィンドウで、そのユーザーに対して特別な権限を設定します。

7. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで Kaspersky Security サービスを管理するためのユーザー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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**詳細設定**］→［**Kaspersky Security サービス管理用のユーザーアクセス権限**］に移動し、［**設定**］をクリックします。

   ［**Kaspersky Security サービス管理用のユーザーアクセス権限**］ウィンドウが表示されます。
5. Kaspersky Security サービスのユーザー権限を設定する Active Directory ユーザーまたはグループを追加します。
6. 本製品を管理するためにアクセスを許可するユーザーまたはユーザーグループを選択します。

   Web コンソールでは、製品のサービスを管理するための特別な権限を設定することはできません。
7. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

# Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス

ユーザー権限を設定すると、ユーザー権限の設定でアプリケーション管理や登録されたサービスへのアクセスを制限できます。Kaspersky Embedded Systems Security 設定でパスワードによる保護を設定して、重要な操作をさらに保護することもできます。

パスワードによって保護されている操作をユーザーが試行した場合、Kaspersky Embedded Systems Security はユーザー名とパスワードの組み合わせまたは一時パスワードの入力を求めます。パスワードによる保護では次のアカウントがサポートされます：

- **KLAdmin**：Kaspersky Embedded Systems Security に制限なくアクセスできる管理者アカウント。KLAdmin アカウントには、パスワードによって保護されるすべての操作を実行する権限が付与されています。KLAdmin アカウントに対する権限を取り消すことはできません。パスワードによる保護を有効にすると、Kaspersky Embedded Systems Security では KLAdmin アカウントのパスワードの指定が要求されます。
- **手動で追加されたアカウント**：Active Directory ドメイン外のアカウント。管理者パスワードを共有しない場合は、KLAdmin の代わりにこのサービスアカウントを使用できます。任意のユーザー名とパスワードを設定して、個々の権限を設定できます。

- **Everyone グループ**：Windows で定義済みのグループで、組織ネットワーク内のすべてのユーザーが含まれています。Everyone グループに含まれるユーザーは、グループに対して付与されている権限に応じて本製品にアクセスできます。

- **個別のユーザーまたはグループ**：ユーザーアカウントに対して個別に権限を設定できます。たとえば、Everyone グループに対してはブロックされている操作を、個別のユーザーやグループに対して許可することができます。

Kaspersky Embedded Systems Security インターフェイスでは、指定したパスワードは画面にそのまま表示されません。パスワードを入力するとチェックサムが計算され、パスワードが保存されます。

パスワードの強度はチェックされません。また、パスワードの入力を何度も失敗してもブロックされません。

パスワードの作成には、次の条件があります：

- パスワードにアカウント名やコンピューター名を含めることはできません。
- パスワードの文字数は、8文字以上です。
- パスワードには、次の文字種のうち 3 つ以上を組み合わせてください：
  - アルファベット大文字（A-Z）
  - アルファベット小文字（a-z）
  - 数字（0～9）
  - 感嘆符（!）、ドル（$）、ハッシュ（#）、パーセント（%）

**Kaspersky Security Center 管理コンソールでパスワードを使用して Kaspersky Embedded Systems Security の機能へのアクセスを保護する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**詳細設定**］を選択します。
4. ［**アプリケーション管理用のユーザーアクセス権限**］セクションで、［**設定**］をクリックします。
5. 表示されたウィンドウで、［**手動で作成したユーザーの資格情報を使用して、製品操作を確定することを許可する**］をオンにします。
6. 必要に応じて、［**重要な操作の確認用のパスワードを要求する**］をオフにします。

   この機能を有効にすると、本製品を削除、変更、または復元するとき、および**デバイスの保護レベルを低下させる可能性のあるコマンドラインの操作**を実行するときにユーザー名とパスワードが要求されます。

本製品は、次のコマンドを実行するときに資格情報を要求します。

- KAVSHELL APPCONTROL
- KAVSHELL APPCONTROL /CONFIG
- KAVSHELL APPCONTROL /GENERATE /import
- KAVSHELL DEVCONTROL
- KAVSHELL EXITPOLICY
- KAVSHELL IMPORT
- KAVSHELL ISOLATION /DISABLE
- KAVSHELL LICENSE /DEL
- KAVSHELL PASSWORD
- KAVSHELL PREVENTION /DISABLE
- KAVSHELL QUARANTINE /ADD
- KAVSHELL QUARANTINE /DELETE
- KAVSHELL REMOTEACCESS
- KAVSHELL RESETMDRMACHINEID
- KAVSHELL SERVERBINDINGDISABLE
- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

この機能が無効になっていて、また現在のユーザーが 必要な権利を持っている場合、Kaspersky Embedded Systems Security は資格情報を要求しません。このオプションは既定では有効になっています。

現在のユーザーに Windows パスワードが設定されていない場合は、必要な権限を持ち、パスワードが設定されているユーザーの資格情報を入力する必要があります。

7. KLAdmin ユーザーアカウントのパスワードを指定します。

8. 必要に応じて、アプリケーション管理へのアクセスを許可するユーザーアカウントを追加します：

   a. ［**追加**］をクリックします。
   これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。

   b. 表示されたウィンドウで、ユーザーを追加する方法（［**ユーザーまたはユーザーグループを手動で追加する**］）を選択します。

   c. ユーザー名とパスワードを指定します。

   d. ［**権限**］リストで、製品機能へのユーザーのアクセス権限を設定します。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

***アプリケーションコンソールでパスワードを使用して Kaspersky Embedded Systems Security の機能へのアクセスを保護する方法***

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**アプリケーション管理用のユーザーアクセス権限**］を選択します。

2. 表示されたウィンドウで、［**手動で作成したユーザーの資格情報を使用して、製品操作を確定することを許可する**］をオンにします。

3. 必要に応じて、［**重要な操作の確認用のパスワードを要求する**］をオフにします。
   この機能を有効にすると、本製品を削除、変更、または復元するとき、および**デバイスの保護レベルを低下させる可能性のあるコマンドラインの操作**を実行するときにユーザー名とパスワードが要求されます。

   本製品は、次のコマンドを実行するときに資格情報を要求します。

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`

- KAVSHELL QUARANTINE /DELETE
- KAVSHELL REMOTEACCESS
- KAVSHELL RESETMDRMACHINEID
- KAVSHELL SERVERBINDINGDISABLE
- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

この機能が無効になっていて、また現在のユーザーが 必要な権利を持っている場合、Kaspersky Embedded Systems Security は資格情報を要求しません。このオプションは既定では有効になっています。

現在のユーザーに Windows パスワードが設定されていない場合は、必要な権限を持ち、パスワードが設定されているユーザーの資格情報を入力する必要があります。

4. KLAdmin ユーザーアカウントのパスワードを指定します。
5. 必要に応じて、アプリケーション管理へのアクセスを許可するユーザーアカウントを追加します：
   a. ［**追加**］をクリックします。
      これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。
   b. 表示されたウィンドウで、ユーザーを追加する方法（［**ユーザーまたはユーザーグループを手動で追加する**］）を選択します。
   c. ユーザー名とパスワードを指定します。
   d. ［**権限**］リストで、製品機能へのユーザーのアクセス権限を設定します。
6. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでパスワードを使用して Kaspersky Embedded Systems Security の機能へのアクセスを保護する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**詳細設定**］→［**アプリケーション管理用のユーザーアクセス権限**］に移動し、［**設定**］をクリックします。
5. 表示されたウィンドウで、［**手動で作成したユーザーの資格情報を使用して、製品操作を確定することを許可する**］をオンにします。
6. 必要に応じて、［**重要な操作の確認用のパスワードを要求する**］をオフにします。
   この機能を有効にすると、本製品を削除、変更、または復元するとき、および**デバイスの保護レベルを低下させる可能性のあるコマンドラインの操作**を実行するときにユーザー名とパスワードが要求されます。

   本製品は、次のコマンドを実行するときに資格情報を要求します。

   - `KAVSHELL APPCONTROL`
   - `KAVSHELL APPCONTROL /CONFIG`
   - `KAVSHELL APPCONTROL /GENERATE /import`
   - `KAVSHELL DEVCONTROL`
   - `KAVSHELL EXITPOLICY`
   - `KAVSHELL IMPORT`
   - `KAVSHELL ISOLATION /DISABLE`
   - `KAVSHELL LICENSE /DEL`
   - `KAVSHELL PASSWORD`
   - `KAVSHELL PREVENTION /DISABLE`
   - `KAVSHELL QUARANTINE /ADD`
   - `KAVSHELL QUARANTINE /DELETE`
   - `KAVSHELL REMOTEACCESS`
   - `KAVSHELL RESETMDRMACHINEID`
   - `KAVSHELL SERVERBINDINGDISABLE`

- KAVSHELL SIGMA /DISABLE
- KAVSHELL SIGMA /ADD
- KAVSHELL SIGMA /REMOVE>
- KAVSHELL STOP
- KAVSHELL TASK /STOP
- KAVSHELL TELEMETRYFILTERS /IMPORT

この機能が無効になっていて、また現在のユーザーが 必要な権利を持っている場合、Kaspersky Embedded Systems Security は資格情報を要求しません。このオプションは既定では有効になっています。

現在のユーザーに Windows パスワードが設定されていない場合は、必要な権限を持ち、パスワードが設定されているユーザーの資格情報を入力する必要があります。

7. KLAdmin ユーザーアカウントのパスワードを指定します。
8. 必要に応じて、アプリケーション管理へのアクセスを許可するユーザーアカウントを追加します：
   a. ［**追加**］をクリックします。
      これにより、ユーザーのアクセス権限を設定するためのフォームが開きます。
   b. 表示されたウィンドウで、ユーザーを追加する方法（［**ユーザーまたはユーザーグループを手動で追加する**］）を選択します。
   c. ユーザー名とパスワードを指定します。
   d. ［**権限**］リストで、製品機能へのユーザーのアクセス権限を設定します。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

このパスワードは復元できません。パスワードを紛失すると、アプリケーションをまったくコントロールできなくなります。また、保護対象デバイスから本製品を削除できなくなります。

パスワードはいつでもリセットできます。リセットするには［**手動で作成したユーザーの資格情報を使用して、製品操作を確定することを許可する**］をオフにして、変更内容を保存します。パスワードによる保護が無効になり、古いパスワードのチェックサムが削除されます。新しいパスワードを使用して、パスワード作成プロセスを繰り返します。

# セキュアデスクトップの通知

Kaspersky Embedded Systems Security はセキュアデスクトップ（Secure Desktop）の機能をサポートしています。この機能の目的は、コンピューターのセキュリティレベルを低下させる可能性のある処理を確認することです。この機能により、アプリケーションで他のプロセスから分離された確認ダイアログを表示することができます。この機能では昇格した権限を使用してリクエストの安全を確保します。こうすることで、マルウェアではなくユーザーだけが処理を確認できるようになります。

Kaspersky Embedded Systems Security は、次の操作を確認するセキュアデスクトップの通知を表示します：

- トレースの有効化または無効化
- アプリケーション設定のエクスポートまたはインポート
- 保護の一時停止
- アプリケーションの終了
- 現在のライセンスの削除
- Kaspersky Embedded Systems Security のアンインストール
- デバイスコントロールの無効化
- ファイルのリアルタイム保護の無効化
- Kaspersky Security Center のポリシーの無効化
- レポートの表示
- バックアップからのファイルの復元
- Kaspersky Embedded Systems Security の設定の変更
- アプリケーションタスクの管理（起動以外）

**Kaspersky Security Center 管理コンソールでセキュアデスクトップの通知を有効または無効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**アプリケーション設定**］をクリックします。
4. ［**セキュリティと信頼性**］ブロックの［**設定**］をクリックします。
5. ウィンドウが表示されるので、そのウィンドウで［**セキュリティ**］タブを選択します。

6. ［**セルフディフェンス**］ブロックで、［**セキュアデスクトップの通知を有効にする**］をオンまたはオフにして、セキュアデスクトップの通知を有効または無効にします。

   セルフディフェンス機構が無効になっている場合、［**セキュアデスクトップの通知を有効にする**］は使用できません。

7. コンピューターにポリシーを適用するには、南京錠（）を閉じます。

8. ［**OK**］をクリックして、変更内容を保存します。

*管理コンソールでセキュアデスクトップの通知を有効または無効にする方法*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、結果ペインで［**アプリケーションのプロパティ**］をクリックします。

2. ウィンドウが表示されるので、そのウィンドウで［**セキュリティ設定**］タブを選択します。

3. ［**セルフディフェンス**］ブロックで、［**セキュアデスクトップの通知を有効にする**］をオンまたはオフにして、セキュアデスクトップの通知を有効または無効にします。

   セルフディフェンス機構が無効になっている場合、［**セキュアデスクトップの通知を有効にする**］は使用できません。

4. ［**OK**］をクリックして、変更内容を保存します。

**Kaspersky Security Center Web コンソールでセキュアデスクトップの通知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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**アプリケーション設定**］セクションを選択します。

5. ［**セキュリティと信頼性**］ブロックの［**設定**］をクリックします。
   ［**セキュリティと信頼性**］ウィンドウが表示されます。

6. ［**セルフディフェンス**］ブロックで、［**セキュアデスクトップの通知を有効にする**］をオンまたはオフにして、セキュアデスクトップの通知を有効または無効にします。

   セルフディフェンス機構が無効になっている場合、［**セキュアデスクトップの通知を有効にする**］は使用できません。

7. コンピューターにポリシーを適用するには、南京錠（🔒）を閉じます。

8. ［**OK**］をクリックして、変更内容を保存します。

# 信頼ゾーン

*信頼ゾーン*は Kaspersky Embedded Systems 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 Embedded Systems 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。管理者が、ユーザーが特定のコンピューターに対してローカルの信頼するゾーンを作成するよう許可することも可能です。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。

EDR テレメトリを信頼ゾーンに追加することも可能です。これにより、アプリケーションが Kaspersky Anti Targeted Attack Platform (EDR) ソリューション向けにテレメトリサーバーに送信するデータを最適化できます。

設定済みの信頼するオブジェクトとアプリケーションが信頼ゾーンに追加されました。設定済みの信頼するオブジェクトとアプリケーションにより、 信頼ゾーンを手動で作成することなく、Kaspersky Embedded Systems Security を迅速に設定できます。

# 信頼するオブジェクトの作成

*信頼するオブジェクト*とは、Kaspersky Embedded Systems 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。

信頼するオブジェクトは、次のアプリケーションコンポーネントとタスクで使用できます：

- **ファイルのリアルタイム保護**
- **オンデマンドスキャン**
- **ふるまい検知**
- **AMSI 保護**
- **ネットワーク脅威対策**

スキャンタスクの開始時にこのオブジェクトを含むドライブやフォルダーがスキャン範囲に含まれている場合、オブジェクトはスキャンされません。ただし、ある特定のオブジェクトについてオブジェクトスキャンタスクが開始された場合、信頼するオブジェクトは適用されません。

Kaspersky Embedded Systems Security は、5000 を超えるオブジェクトを含む除外リストをサポートしていません。

### Kaspersky Security Center の管理コンソールで信頼するオブジェクトを作成する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**詳細設定**］→［**信頼ゾーン**］の順に選択し、［**設定**］をクリックします。
4. ［**信頼するオブジェクト**］タブを選択します。
5. 組織内のすべてのコンピューターの除外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除外リストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。
6. ローカルの除外リストをユーザーが作成できるようにするには、［**ローカルの除外リストの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するオブジェクトのリストがアプリケーションコンソールで非表示になります。
7. ［**追加**］をクリックして、処理を選択します：
   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも 1 つの信頼するオブジェクトをカテゴリに追加します。
   - **新しい除外**：Kaspersky Embedded Systems Security は新しい信頼するオブジェクトをリストのルートに追加します。
   - **選択したカテゴリに新しい除外を追加**：新しい信頼するオブジェクトを特定のカテゴリに追加するには、カテゴリを選択します。
   - **リストから除外を選択**：Kaspersky Embedded Systems Security を素早く設定するために、設定済みの信頼するオブジェクトのリストから除外項目を追加できます。
8. ファイルまたはフォルダーをスキャンから除外するには、［**ファイルまたはフォルダー**］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選択**］をクリックしてウィンドウを開き、そのウィンドウで［**参照**］をクリックしてファイルまたはフォルダーを選択します。

手動でパスを入力することもできます。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

- 「*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:**.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

- 2 つの連続した「*」（アスタリスク）文字。ファイル名またはフォルダー名内の、「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder***.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:***.txt」というマスクの指定は無効です。

- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

  ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「?:\Users*\Folder\」と入力できます。

9. 定義済みの範囲をスキャンから除外するには、［**定義済みの範囲**］チェックボックスをオンにします。［**定義済みの範囲の選択**］をクリックして、ウィンドウを開き、そのウィンドウで、保護対象デバイスの標準の範囲を 1 つ選択します。

10. 特定のオブジェクトをスキャンから除外するには、［**検知するオブジェクトの種別**］をオンにします。［**オブジェクト名の入力**］をクリックして、［**追加**］をクリックし、表示されたウィンドウで、「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（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。

11. 個々のファイルをスキャンから除外するには、［**オブジェクトハッシュ**］をオンにします。［**オブジェクトハッシュの入力**］をクリックしてウィンドウを開き、そのウィンドウでファイルハッシュを入力します。

    ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

12. ［**ルールの使用範囲**］ブロックで、スキャンの例外を適用するコンポーネントを選択します。

13. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

14. 変更を保存して、除外項目をリストに追加します。いつでもオブジェクトの横のチェックボックスを使用して信頼するオブジェクトを無効にできます。

*Kaspersky Security Center Web コンソールで信頼するオブジェクトを作成する方法*

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）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**詳細設定**］→［**信頼ゾーン**］に移動し、［**設定**］をクリックします。
5. ［**信頼するオブジェクト**］タブを選択します。
6. 組織内のすべてのコンピューターの除外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除外リストが結合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの除外リストは子ポリシー内では読み取り専用で表示されます。親ポリシーの除外リストは、変更または削除できません。
7. ローカルの除外リストをユーザーが作成できるようにするには、［**ローカルの除外リストの使用を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された全体的な除外リストに加えて自分のローカルの除外リストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の除外リストの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するオブジェクトのリストがアプリケーションコンソールで非表示になります。
8. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも 1 つの信頼するオブジェクトをカテゴリに追加します。
   - **新しい除外**：Kaspersky Embedded Systems Security は新しい信頼するオブジェクトをリストのルートに追加します。
   - **リストから除外を選択**：Kaspersky Embedded Systems Security を素早く設定するために、設定済みの信頼するオブジェクトのリストから除外項目を追加できます。
9. ファイルまたはフォルダーをスキャンから除外する場合は、［**ファイルまたはフォルダー**］を選択して、同じ名前のフィールドにある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へのパスを指定する

Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

- 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

- 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。

- 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

  ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「`?:\Users\*\Folder\`」と入力できます。

10. 定義済みの範囲をスキャンから除外するには、［**定義済みの範囲**］をオンにします。ドロップダウンリストで、保護対象デバイスの標準の範囲を 1 つ選択します。

11. 特定のオブジェクトをスキャンから除外する場合は、［**検知するオブジェクトの種別**］をオンにして、「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（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。

12. 個々のファイルをスキャンから除外するには、［**オブジェクトハッシュ**］をオンにして、ファイルまたはイベントのリストからハッシュを追加します。

    ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

13. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

14. ［**保護機能**］ブロックで、スキャンの例外を適用するコンポーネントを選択します。

15. 新しい信頼するオブジェクトがリストに追加されます。いつでも［**ステータス**］列のチェックボックスを使用して信頼するオブジェクトを無効にできます。

16. 変更内容を保存します。

### アプリケーションコンソール信頼するオブジェクトを作成する方法

1. アプリケーションコンソールツリーで、［Kaspersky Embedded Systems Security］フォルダーを選択して、フォルダーのコンテキストメニューから［**信頼ゾーン**］を選択します。

   ［**信頼ゾーンの設定**］ウィンドウが表示されます。

2. ［**除外リスト**］セクションで、［**信頼するオブジェクト**］ブロックの横にある［**設定**］をクリックします。

3. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも1つの信頼するオブジェクトをカテゴリに追加します。
   - **新しい除外**：Kaspersky Embedded Systems Security は新しい信頼するオブジェクトをリストのルートに追加します。
   - **選択したカテゴリに新しい除外を追加**：新しい信頼するオブジェクトを特定のカテゴリに追加するには、カテゴリを選択します。
   - **リストから除外を選択**：Kaspersky Embedded Systems Security を素早く設定するために、設定済みの信頼するオブジェクトのリストから除外項目を追加できます。

4. ファイルまたはフォルダーをスキャンから除外するには、［**ファイルまたはフォルダー**］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選択**］をクリックしてウィンドウを開き、そのウィンドウで［**参照**］をクリックしてファイルまたはフォルダーを選択します。

   手動でパスを入力することもできます。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

   - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
   - 2つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。
   - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が3文字のすべてのファイルのパスを含みます。

     ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「`?:\Users\*\Folder\`」と入力できます。

5. 定義済みの範囲をスキャンから除外するには、［**定義済みの範囲**］チェックボックスをオンにします。［**定義済みの範囲の選択**］をクリックして、ウィンドウを開き、そのウィンドウで、保護対象デバイスの標準の範囲を1つ選択します。

6. 特定のオブジェクトをスキャンから除外するには、［**検知するオブジェクトの種別**］をオンにします。［**オブジェクト名の入力**］をクリックして、［**追加**］をクリックし、表示されたウィンドウで、「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（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。

7. 個々のファイルをスキャンから除外するには、［**オブジェクトハッシュ**］をオンにします。［**オブジェクトハッシュの入力**］をクリックしてウィンドウを開き、そのウィンドウでファイルハッシュを入力します。

   ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

8. ［**ルールの使用範囲**］ブロックで、スキャンの例外を適用するコンポーネントを選択します。

9. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

10. 変更を保存して、除外項目をリストに追加します。いつでもオブジェクトの横のチェックボックスを使用して信頼するオブジェクトを無効にできます。

パスマスクの例：
任意のフォルダーにあるファイルへのパス：

- 「`*.exe`」というマスクには、拡張子が「exe」のファイルへのすべてのパスが含まれます。
- 「`example*`」というマスクには、名前が「EXAMPLE」のファイルへのすべてのパスが含まれます。

特定のフォルダーにあるファイルへのパス：

- 「`C:\dir\*.*`」というマスクには、「C:\dir\」フォルダーにあるすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「`C:\dir\*`」というマスクには、「C:\dir\」フォルダーとそのサブフォルダーにあるすべてのファイルへのパスが含まれます。
- 「`C:\dir\`」というマスクには、「C:\dir\」フォルダーとそのサブフォルダーにあるすべてのファイルへのパスが含まれます。
- 「`C:\dir\*.exe`」というマスクには、「C:\dir\」フォルダーに存在し拡張子が「EXE」のすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「`C:\dir\test`」というマスクには、「C:\dir\」フォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれますが、「C:\dir\」のサブフォルダーにあるファイルへのパスは含まれません。
- 「`C:\dir\*\test`」というマスクには、「C:\dir\」フォルダーとそのサブフォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれます。
- 「`C:\dir1\*\dir3\`」というマスクには、「C:\dir1\」からサブフォルダー「dir3」までの間1レベルのすべてのファイルのパスが含まれます。
- 「`C:\dir1\**\dirN\`」というマスクには、「C:\dir1\」からサブフォルダー「dir3」までのすべてのレベルにあるファイルすべてのパスが含まれます。

特定の名前のすべてのフォルダーにあるファイルへのパス：

- 「`dir\*.*`」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「`dir\*`」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「`dir\`」というマスクには、名前が「dir」のフォルダーにあるすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「`dir\*.exe`」というマスクには、名前が「dir」のフォルダーに存在し拡張子が「EXE」のすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。
- 「`dir\test`」というマスクには、名前が「dir」のフォルダーに存在し名前が「test」のすべてのファイルへのパスが含まれますが、そのサブフォルダーにあるファイルへのパスは含まれません。

# 検知可能なオブジェクトの選択

*検知可能なオブジェクトを選択するには：*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、次のいずれかを行います：

   - フォルダーの結果ペインで、［**信頼ゾーンの設定**］をクリックします。
   - フォルダーのコンテキストメニューで［**信頼ゾーン**］を選択します。

   ［**信頼ゾーンの設定**］ウィンドウが表示されます。

2. ［**検知するオブジェクトの種別**］セクションで、［**設定**］をクリックします。

3. 表示されたウィンドウで、チェックボックスを使用して Kaspersky Embedded Systems Security が検知するオブジェクトの種類を選択します：

   - **ウイルス、ワーム**

     **サブカテゴリ**：ウイルスやワーム（Viruses_and_Worms）

     **危険度**：高

     古典的なウイルスやワームは、ユーザーが許可していない処理を実行します。このようなウイルスやワームは、自己複製が可能な自身のコピーを作成することができます。

     **古典的ウイルス**

     古典的ウイルスがコンピューターに侵入すると、ファイルに感染して活動を開始し、悪意のある処理を実行し、それ自体のコピーを他のファイルに追加します。

     古典的ウイルスは、コンピューターのローカルリソースでしか増殖しないため、自力で他のコンピューターに侵入できません。このウイルスが別のコンピューターに感染するのは、ウイルス自身のコピーを共有フォルダーに保管されているファイルまたは挿入された CD に追加したときや、ユーザーが感染したファイルを添付したメールを転送したときです。

     古典的ウイルスのコードはコンピューター、オペレーティングシステム、アプリケーションの各種領域に侵入する可能性があります。環境により、ウイルスは、*ファイルウイルス*、*ブートウイルス*、*スクリプトウイルス*、および*マクロウイルス*に分けられます。

     ウイルスはさまざまな技法を駆使してファイルを感染させます。*上書き*ウイルスは、そのコードを、感染したファイルのコードに上書きして、そのファイルの内容を消去します。感染したファイルは機能しなくなり、復元できません。*寄生*ウイルスは、ファイルを変更しますが、ファイルが完全にまたは部分的に機能する状態を維持します。*コンパニオンウイルス*は、ファイルを変更しませんが、代わりに複製を作成します。感染したファイルが開かれると、ウイルスの複製（実際にはこれがウイルス）が起動します。他にも、次のような種別のウイルスが見つかっています：*リンクウイルス*、*OBJ ウイルス*、*LIB ウイルス*、*ソースコードウイルス*など多数。

     **ワーム**

古典的ウイルスのコードと同様に、ワームのコードは、コンピューターに侵入してから活動を開始し、悪意のある処理を実行します。ワームは、コンピューターから別のコンピューターに「這うように移動」し、ユーザーの許可なく多数のデータチャネルを経由してコピーを拡散させることから、この名が付けられました。

さまざまなワームの種類を区別する主な特徴は、その拡散方法です。次のテーブルに、拡散方法によって分類される各種ワームの概要を示します：

ワームの拡散方法

| 種別 | Name | 説明 |
|---|---|---|
| **メールワーム** | メールワーム | これらのワームはメールを介して広がります。<br>感染したメールには、ワームのコピーを含んだ添付ファイル、あるいは感染した Web サイトまたは感染させる目的で作成された Web サイトにアップロードされるファイルへのリンクが含まれています。添付ファイルを開くと、ワームが起動します。リンクをクリックし、ファイルをダウンロードして開くと、ワームも悪意のある処理を実行し始めます。その後、ワームは他のメールアドレスを検索して、これらのアドレスに感染メールを送信しながら、自身のコピーを拡散し続けます。 |
| **IM ワーム** | IM クライアントワーム | インスタントメッセージ（IM）クライアント経由で拡散します。<br>通常、このようなワームは、ユーザーの連絡先リストを使用して、ワームのコピーに感染した Web サイト上のファイルへのリンクを含んだメールを送信します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。 |
| **IRC ワーム** | インターネットチャットワーム | このワームはインターネットリレーチャット（インターネット上の別のユーザーとリアルタイムで通信できるサービスシステム）を介して拡散します。<br>この種のワームは、インターネットチャットで自身のコピーを含むファイルまたはそのファイルへのリンクを公開します。ユーザーがファイルをダウンロードして開くと、ワームが起動します。 |
| **インターネットワーム（Net-Worm）** | ネットワークワーム | これらのワームは、コンピューターネットワークを介して広がります。<br>通常のネットワークワームは、他の種類のワームと異なり、ユーザーが参加していなくても拡散します。このワームはプライベートネットワークに、脆弱性のあるプログラムがインストールされたコンピューターがないか探します。この操作を行うために、このワームはワームコードまたはその一部を含む特別に形成されたネットワークパケット（エクスプロイト）を送信します。ネットワーク上に「脆弱な」コンピューターが存在すると、そのコンピューターはこのようなネットワークパケットを受信します。ワームが完全にコンピューターに侵入すると、ワームが起動します。 |
| **P2P ワーム** | ファイル共有ネットワークワーム | peer-to-peer のファイル共有ネットワーク経由で拡散します。<br>P2P ネットワークに潜入するために、ワームはそれ自身をファイル共有フォルダーにコピーします。このフォルダーは通常、ユーザーのコンピューター上にあります。P2P ネットワークでは、ネットワーク上の感染したファイルをユーザーが他のファイルと同様に「見つけ」、このファイルをダウンロードして開くように、このファイルに関する情報が表示されます。<br>さらに巧妙なワームは特定の P2P ネットワークのネットワークプロトコルを装って検索クエリに肯定応答を返し、自身のコピーをダウンロードさせます。 |
| **ワーム** | 他の種類のワーム | 他の種類のワームには、以下のものがあります：<br>• 自身のコピーをネットワークリソースを介して拡散するワーム。このようなワームは、オペレーティングシステムの機能を使って使用可能なネットワークフォルダーを検索し、インターネット上のコンピューターへ接続し、このコンピューターのディスクドライブへのフルアクセス権を取得しようと試みます。他の種類のワームは上記種類のワームとは異なり、自力で起動するのではなく、ユーザーがワームのコピーを含むファイルを開いたときに起動します。<br>• 上記のどの拡散方法も使用しないワーム（携帯電話を通じて拡散するワームなど）。 |

- **トロイの木馬**

**サブカテゴリ**：トロイの木馬

**危険度**：高

ワームやウイルスとは異なり、トロイの木馬は自己複製しません。たとえば、ユーザーが感染している Web サイトにアクセスすると、トロイの木馬はメールやブラウザーからコンピューターに侵入します。トロイの木馬は、ユーザーの関与によって起動します。起動直後に、悪意のある処理を実行し始めます。

トロイの木馬は多種多様で、感染コンピューター上でのふるまいも多岐にわたります。トロイの木馬の主な機能は、情報のブロック、改変、破壊、およびコンピューターまたはネットワークの無効化です。また、トロイの木馬はファイルの送受信、ファイルの実行、画面上へのメッセージの表示、Web サイトの要求、プログラムのダウンロードとインストール、コンピューターの再起動を行うこともできます。

多くの場合、ハッカーはトロイの木馬の「セット」を使用します。

次のテーブルでは、トロイの木馬における動作の種類について説明します。

感染コンピューターにおけるトロイの木馬の動作種類

| 種別 | Name | 説明 |
|---|---|---|
| **Trojan-ArcBomb** | トロイの木馬 - 「圧縮爆弾」 | このアーカイブは、解凍するとコンピューターの動作に影響を与える程度のサイズにまで膨張します。<br>ユーザーがこのようなアーカイブを解凍しようとすると、コンピューターは処理速度が低下したりフリーズしたりすることがあります。また、ハードディスクが「空の」データで満杯になることがあります。「圧縮爆弾」は、特にファイルサーバーやメールサーバーにとって危険です。サーバーが自動システムを使用して受信情報を処理すると、「圧縮爆弾」によってサーバーが停止することがあります。 |
| **バックドア** | リモート管理用のトロイの木馬 | このプログラムは、トロイの木馬の中でも最も危険なものと考えられます。機能面で、コンピューターにインストールされるリモート管理アプリケーションに似ています。<br>これらのプログラムは、ユーザーに気付かれずにコンピューターにインストールされるので、侵入者はコンピューターを遠隔管理できます。 |
| **トロイの木馬** | トロイの木馬 | トロイの木馬には、次のような悪意のあるアプリケーションがあります：<br>• **古典的なトロイの木馬**：これらのプログラムはトロイの木馬の主な機能（情報のブロック、改変または破壊、およびコンピューターまたはネットワークの無効化）のみを実行し、テーブルに示す他の種類のトロイの木馬とは異なり、高度な機能を持っていません。<br>• **多目的なトロイの木馬**：これらのプログラムは、数種類のトロイの木馬に特徴的な先進機能を備えています。 |
| **Trojan-Ransom** | トロイの木馬型ランサムウェア | このプログラムは、ユーザーの情報を「人質」にとって改変したり、ブロックしたりします。また、ユーザーが情報を使用する能力を喪失するように、コンピューターの動作に影響を与えます。侵入者は、コンピューターのパフォーマンスと保存されていたデータを復元するアプリケーションを送るという約束と引き替えに、ユーザーから身代金を要求します。 |
| **Trojan-Clicker** | トロイの木馬クリッカー | このプログラムは、ブラウザーにコマンドを送信するか、オペレーティングシステムファイルで指定されている Web アドレスを変更することによって、ユーザーのコンピューターから Web サイトにアクセスします。<br>侵入者はこのようなプログラムを使用することによって、ネットワーク攻撃を行って Web サイトのアクセス数を増やし、バナー広告の表示回数を増やします。 |
| **Trojan-Downloader** | トロイの木馬ダウンローダー | これは侵入者の Web サイトにアクセスして、そこから他の悪意のあるアプリケーションをダウンロードし、ユーザーのコンピューターにインストールします。このプログラムには、悪意のあるアプリケーションをダウンロードまたは受信するためにアクセスした Web サイトのファイル名が含まれていることがあります。 |
| **Trojan-Dropper** | トロイの木馬ドロッパー | このプログラムは他のトロイの木馬を内包しており、この内包されたプログラムがハードディスクにインストールされ、実行されます。<br>侵入者は、トロイの木馬ドロッパー型プログラムを次のような目的で使用することがあります：<br>• ユーザーに気付かれずに悪意のあるプログラムをインストールする：トロイの木馬ドロッパー型プログラムは、メッセージを表示しないか、たとえば、アーカイブ中にエラーが発生したことやオペレーティングシステムが互換性のないバージョンであることを示すといった偽のメッセージを表示します。<br>• 既知の悪意のある別のアプリケーションが検知されないようにする：すべてのアンチウイルスのソフトウェアがトロイの木馬ドロッパー型アプリケーション内の悪意のあるアプリケーションを検知できるわけではありません。 |

| 種別 | Name | 説明 |
| --- | --- | --- |
| **Trojan-Notifier** | トロイの木馬型ノーティファイア | このプログラムは、感染したコンピューターにアクセスできることを侵入者に教えるため、コンピューターの次のような情報を侵入者に送信します：IP アドレス、開いているポートの番号、メールアドレスなど。このプログラムはこれらの情報をメール、FTP、侵入者の Web サイトへのアクセス、あるいはこれら以外の方法で侵入者に送ります。<br>トロイの木馬型ノーティファイアプログラムは、多くの場合、複数のトロイの木馬からなるセットとして使用されます。また、このプログラムはトロイの木馬がユーザーのコンピューターにインストールされたことを侵入者に知らせます。 |
| **Trojan-Proxy** | トロイの木馬型プロキシ | これらのトロイの木馬により、侵入者は、ユーザーのコンピューターを使って匿名で Web サイトにアクセスします。このトロイの木馬はスパムの送信によく利用されます。 |
| **Trojan-PSW** | パスワード窃盗ソフトウェア | パスワード窃盗ソフトウェアは、ソフトウェア登録データなどのユーザーアカウントを盗むトロイの木馬の一種です。このトロイの木馬はシステムファイルおよびレジストリ内の機密データを見つけ、そのデータを「攻撃者」にメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって送信します。<br>これらのトロイの木馬のうち、いくつかがこのテーブルに示す種類に分類されます。これらは、銀行のアカウント情報（Trojan-Banker）、メッセンジャークライアントのユーザーのデータ（Trojan-IM）、およびオンラインゲームのユーザーの情報（Trojan-GameThief）を盗むトロイの木馬です。 |
| **Trojan-Spy** | スパイウェア型トロイの木馬 | このトロイの木馬はコンピューター上で動作しながら、ユーザーが行う処理に関する情報を収集して、ユーザーの行動を秘密裏に監視します。このトロイの木馬は、ユーザーがキーボードで入力するデータの傍受、スクリーンショットの撮影、あるいはアクティブなアプリケーションのリストの収集などを行うことがあります。このプログラムが情報を入手すると、その情報をメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。 |
| **Trojan-DDoS** | トロイの木馬ネットワークアタッカー | このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、または DoS 攻撃）。ハッカーは、1 台のサーバーを多数のコンピューターから同時に攻撃できるように、このプログラムを利用して多数のコンピューターを感染させることがあります。<br>DoS プログラムは 1 台のコンピューターから、ユーザーに気付かれることなく攻撃を実行します。DDoS（分散 DoS）プログラムは、感染したコンピューターのユーザーに気付かれずに、複数のコンピューターから分散して攻撃を行います。 |
| **Trojan-IM** | メッセンジャークライアントのユーザーから情報を盗むトロイの木馬 | このトロイの木馬は、メッセンジャークライアントのユーザーのアカウント番号とパスワードを盗みます。このプログラムは、データをメールや FTP で送信する、あるいは侵入者の Web サイトにアクセスするなどによって侵入者に転送します。 |
| **ルートキット** | ルートキット | ルートキットは、他の悪意のあるアプリケーションやその活動を隠蔽します。そのため、このアプリケーションはオペレーティングシステムに長期間潜入します。また、ルートキットはファイル、感染しているコンピューターのメモリ内のプロセス、または悪意のあるアプリケーションを実行するレジストリキーを隠蔽することもできます。さらにルートキットは、ユーザーのコンピューターにインストールされているアプリケーションとネットワーク上の他のコンピューターにインストールされているアプリケーションの間で行われるデータ交換を隠蔽できます。 |
| **Trojan-SMS** | SMS メッセージ形式のトロイの木馬 | このトロイの木馬は携帯電話を感染させ、高額の通話料が発生する電話番号に SMS メッセージを送信します。 |
| **Trojan-GameThief** | オンラインゲームのユーザーから情報を盗むトロイの木馬 | このトロイの木馬は、オンラインゲームのユーザーのアカウント情報を盗み、このデータを侵入者にメールや FTP で送信するか、侵入者の Web サイトにアクセスするなどによって送信します。 |
| **Trojan-Banker** | 銀行のアカウント情報を盗むトロイの木馬 | このトロイの木馬は、銀行のアカウント情報や電子マネーシステムのデータを盗み、このデータをメールや FTP を使用して侵入者に送信するか、侵入者の Web サイトにアクセスするなどして送信します。 |
| **Trojan-Mailfinder** | メールアドレスを収集するトロイの木馬 | このトロイの木馬は、コンピューターに保存されているメールアドレスを収集し、侵入者にメールや FTP で送信するか、侵入者の Web サイトにアクセスするなどによって送信します。侵入者が収集したアドレスにスパムを送信することがあります。 |

- **悪意のあるツール**

**サブカテゴリ**：悪意のあるツール

**危険度**：中

悪意のあるツールは、他の種類のマルウェアとは異なり、起動した直後に処理を実行しません。このプログラムはユーザーのコンピューターに安全に侵入し、そこで起動することができます。侵入者は、多くの場合、悪意のあるツールの機能を悪用して、ウイルス、ワーム、トロイの木馬を作成したり、リモートサーバーに対してネットワーク攻撃を仕掛けたりします。

悪意のあるツールのさまざまな機能を、次のテーブルに示す種類別に分類しています：

悪意のあるツールの機能

| 種別 | Name | 説明 |
|---|---|---|
| **コンストラクター** | コンストラクター | このツールを使用して、新しいウイルス、ワームおよびトロイの木馬を作成します。一部のコンストラクターは標準的なウィンドウベースのインターフェイスを備えています。このインターフェイスでは、悪意のあるアプリケーションの種類を選択して、デバッガを無効にする手段やその他の機能を作成できます。 |
| **Dos** | ネットワーク攻撃 | このプログラムは、ユーザーのコンピューターから大量の要求をリモートサーバーに送ります。サーバーは、要求を処理するためのリソースが不足するので、機能を停止します（サービス妨害攻撃、または DoS 攻撃）。 |
| **エクスプロイト** | エクスプロイト | *エクスプロイト*は、処理されるアプリケーションの脆弱性を利用する一連のデータまたはプログラムコードで、コンピューター上で悪意のある処理を実行します。たとえば、エクスプロイトは、ファイルの書き込みまたは読み取り、あるいは「感染している」Web サイトの要求を行うことができます。<br>それぞれのエクスプロイトは、さまざまなアプリケーションまたはネットワークサービスの脆弱性を利用します。ネットワークパケットに偽装したエクスプロイトは、ネットワーク経由で多数のコンピューターに送信され、脆弱なネットワークサービスを備えるコンピューターを探します。DOC ファイルのエクスプロイトは、テキストエディターの脆弱性を利用します。このエクスプロイトは、ユーザーが感染したファイルを開いたときに、ハッカーが事前にプログラミングした処理を開始することがあります。メールに組み込まれたエクスプロイトは、メールクライアントの脆弱性を探します。このエクスプロイトは、ユーザーがメールクライアントの感染メールを開くとすぐに悪意のある処理を実行します。<br>エクスプロイトを使用してネットワーク上に拡散するのがネットワームです。ヌーカー型エクスプロイトは、コンピューターを無効にするネットワークパケットです。 |
| **FileCryptor** | エンクリプター | このプログラムは、他の悪意のあるアプリケーションを暗号化してアンチウイルス製品から隠蔽します。 |
| **Flooder** | ネットワークを「汚染する」ためのプログラム | このプログラムは大量のメールをネットワークチャネル上に送信します。この種のツールには、インターネットリレーチャットなどを汚染するプログラムがあります。<br>Flooder 型ツールには、メール、IM クライアントおよびモバイル通信システムで使用されるチャネルを「汚染する」プログラムは含まれません。これらのプログラムは、テーブルに示す別種（Email-Flooder、IM-Flooder および SMS-Flooder）として区別されます。 |
| **HackTool** | ハッキングツール | このプログラムは、たとえば、ユーザーの許可なしに新しいシステムアカウントを追加したり、システムログを消去してオペレーティングシステムにおける存在の痕跡を隠蔽したりすることによって、このプログラムがインストールされたコンピューターをハッキングすることや別のコンピューターを攻撃することを可能にします。この種のツールには、パスワードの傍受などの悪意のある機能を特徴とする一部のスニファーが含まれます。スニファーは、ネットワークトラフィックの監視を可能にするプログラムです。 |
| **Hoax** | デマウイルス | このプログラムはウイルスメッセージに似たメッセージでユーザーに注意を喚起します。具体的には、感染していないファイルで「ウイルスを検知した」というメッセージや、実際にはディスクのフォーマットが発生しなかったのに、ディスクがフォーマットされたというメッセージを表示します。 |
| **スプーファ** | スプーフィングツール | このツールは、メッセージ要求やネットワーク要求を送信者の偽装アドレスで送信します。たとえば、侵入者はスプーファ型のツールを使用して、ツール本体をメールの実際の送信者として渡します。 |
| **VirTool** | 悪意のあるアプリケーションを改変するツール | このツールを使用すると、他のマルウェアを改変して、アンチウイルス製品から隠蔽することができます。 |
| **Email-Flooder** | メールアドレスを「汚染する」プログラム | このプログラムはさまざまなメールアドレスに大量のメールを送信して、これらのメールアドレスを「汚染」します。大量の受信メールによって、ユーザーは必要なメールを受信ボックスで表示できなくなります。 |

| 種別 | Name | 説明 |
| --- | --- | --- |
| IM-Flooder | メッセンジャークライアントのトラフィックを「汚染する」プログラム | IM クライアントのユーザーをメッセージであふれさせます。大量のメールが送られてくるため、ユーザーは必要な受信メールを表示できなくなります。 |
| SMS-Flooder | トラフィックを SMS メッセージで「汚染する」プログラム | このプログラムは携帯電話に大量の SMS メッセージを送信します。 |

- **アドウェア**

  **サブカテゴリ**：広告ソフトウェア（アドウェア）

  **危険度**：中

  アドウェアはユーザーに対して広告情報を表示します。アドウェアは、他のプログラムのインターフェイスにバナー広告を表示して、検索クエリを広告 Web サイトにリダイレクトします。このようなプログラムには、ユーザーに関するマーケティング情報を収集し、それを開発者に送信するものがあります。この情報には、ユーザーが表示した Web サイトの名前や、ユーザーの検索の内容などが含まれます。スパイウェア型のトロイの木馬とは異なり、アドウェアは、このような情報をユーザーの同意を得てから開発者に送ります。

- **オートダイヤラー**

  **サブカテゴリ**：オートダイヤラー（ダイヤラー）

  **危険度**：中

  オートダイヤラーはモデムを使用して密かに電話接続を確立できます。

- **ユーザーに損害を与える目的で悪用される可能性がある正規のソフトウェア**

  **サブカテゴリ**：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合法的なソフトウェア。

  **危険度**：中

  これらのアプリケーションのほとんどが有用なものであるため、多くのユーザーが実行しています。これらのアプリケーションには、IRC クライアント、オートダイヤラー、ファイルダウンロードプログラム、コンピューターシステム動作モニター、およびパスワードユーティリティや、FTP、HTTP、および Telnet 用のインターネットサーバーなどがあります。

  ただし、侵入者がこれらのプログラムにアクセスした場合やユーザーのコンピューターにこれらのプログラムを仕掛けた場合、アプリケーションの機能の一部がセキュリティを侵害するために利用されることがあります。

これらのアプリケーションは機能によって異なります。次のテーブルに、これらのアプリケーションの種類を示します：

| 種別 | Name | 説明 |
|---|---|---|
| **Client-IRC** | インターネットチャットクライアント | これらのプログラムは、ユーザーがインターネットリレーチャットで人々と会話するためにインストールします。侵入者は、マルウェアを拡散させるためにこのプログラムを使用します。 |
| **ダウンローダー** | ダウンロード用プログラム | これらのプログラムは、Web サイトからファイルをひそかにダウンロードできます。 |
| **モニター** | 監視用プログラム | このプログラムは、インストールされているコンピューター上のアクティビティを監視します（どのアプリケーションがアクティブであるか、他のコンピューターにインストールされているアプリケーションとどのようにデータをやり取りしているかを監視する）。 |
| **PSWTool** | パスワード不正取得ツール | このツールは、忘失したパスワードを表示して復元します。侵入者は、これと同じ目的でこのツールをユーザーのコンピューターにひそかに埋め込みます。 |
| **RemoteAdmin** | リモート管理プログラム | このプログラムはシステム管理者の中で広く使用されています。このプログラムを使用すると、リモートコンピューターのインターフェイスにアクセスして、そのコンピューターの監視および管理を行うことができます。侵入者も、リモートコンピューターを監視および管理することを目的として、このプログラムをユーザーのコンピューターにひそかに埋め込みます。<br>合法的なリモート管理プログラムは、リモート管理用のバックドア型トロイの木馬と異なります。トロイの木馬は単独でオペレーティングシステムに侵入して、自身をインストールすることができますが、合法的なプログラムでは、このような動作は不可能です。 |
| **Server-FTP** | FTP サーバー | このプログラムは FTP サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、FTP 経由でコンピューターへのリモートアクセスを開きます。 |
| **Server-Proxy** | プロキシサーバー | このプログラムはプロキシサーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。 |
| **Server-Telnet** | Telnet サーバー | このプログラムは Telnet サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、Telnet 経由でコンピューターへのリモートアクセスを開きます。 |
| **Server-Web** | Web サーバー | このプログラムは Web サーバーとして機能します。侵入者は、このプログラムをユーザーのコンピューターに埋め込み、HTTP 経由でコンピューターへのリモートアクセスを開きます。 |
| **RiskTool** | ローカルコンピューターで動作するツール | このプログラムは、ユーザーのコンピューターで動作中に、ユーザーに追加オプションを提供します。このツールを使用すると、ユーザーはアクティブなアプリケーションのファイルやウィンドウを非表示にしたり、アクティブなプロセスを終了したりできます。 |
| **NetTool** | ネットワークツール | このプログラムは、ネットワーク上の他のコンピューターで動作しているときに、ユーザーに追加のオプションを提供します。このようなツールは、コンピューターを再起動して、開いているポートを検知し、コンピューターにインストールされているアプリケーションを起動することできます。 |
| **Client-P2P** | P2P ネットワーククライアント | このプログラムはピアツーピアネットワークで動作できます。また、侵入者がマルウェア拡散のためにこのプログラムを使用する場合があります。 |
| **Client-SMTP** | SMTP クライアント | このプログラムは、ユーザーが知らないうちにメールを送信します。侵入者は、このプログラムをユーザーのコンピューターに埋め込んで、そのユーザーの名前でスパムを送信します。 |
| **WebToolbar** | Web ツールバー | このツールは、検索エンジンを使用するためのツールバーを他のアプリケーションのインターフェイスに追加します。 |
| **FraudTool** | 擬似プログラム | このプログラムは、そのプログラム自体を他のプログラムとして渡します。たとえば、マルウェアが検知されたというメッセージを表示する擬似アンチウイルスプログラムがあります。しかし、実際には、何も検知または駆除しません。 |

- **悪意のあるコードを保護するために圧縮されている可能性があるオブジェクト**

**サブカテゴリ**：損害を与える可能性がある圧縮ファイル

**危険度**：中

ファイルは、マルウェア（ウイルス、ワーム、トロイの木馬）の圧縮に使用される特殊なパッカーを使用して圧縮されます。Kaspersky Embedded Systems Security は、SFX（自己解凍形式）アーカイブ内に解凍モジュールがないかスキャンします。

マルウェアをアンチウイルスによる検知から隠すために、ハッカーは特殊なパッカーを使用してマルウェアを圧縮します。カスペルスキーのエキスパートは、ハッカーの間で最も使用されているパッカーを特定しています。

- **多重圧縮オブジェクト**

  **サブカテゴリ**：多重圧縮ファイル

  **危険度**：中

  ファイルは1つ以上のパッカーを使用して3回以上圧縮されます。

  マルウェアをアンチウイルスによる検知から隠すために、ハッカーがファイルを複数回圧縮することがあります。Kaspersky Embedded Systems Security は圧縮されたファイルをスキャンします。

4. 変更内容を保存します。

# 信頼するアプリケーションのリストの編集

*信頼するアプリケーションのリスト*は、ファイルおよびネットワークの動作（悪意のある動作を含む）やシステムレジストリへのアクセスが Kaspersky Embedded Systems Security によって監視されないアプリケーションのリストです。既定では、Kaspersky Embedded Systems Security はすべてのアプリケーションプロセスによってオープン、実行、保存されるオブジェクトを監視し、すべてのアプリケーションとこのようなアプリケーションが生成するネットワークトラフィックの処理を管理します。アプリケーションが信頼するアプリケーションのリストに追加されると、Kaspersky Embedded Systems Security はアプリケーションのアクティビティの監視を停止します。

信頼するオブジェクトと信頼するアプリケーションの違いは、信頼するオブジェクトの場合、Kaspersky Embedded Systems Security はファイルをスキャンしないのに対し、信頼するアプリケーションの場合は、開始されたプロセスを制御しないことです。信頼するアプリケーションが信頼するオブジェクトに含まれていないフォルダーに悪意のあるファイルを作成した場合、Kaspersky Embedded Systems Security はそのファイルを検知して脅威を排除します。フォルダーが除外リストに追加されている場合、Kaspersky Embedded Systems Security はこのファイルをスキップします。

たとえば、Microsoft Windows 標準のメモ帳アプリケーションで使用するオブジェクトが安全であり信頼できると考える場合は、Microsoft Windows メモ帳を信頼するアプリケーションのリストに追加し、このアプリケーションが使用するオブジェクトが監視されないようにすることができます。これにより、サーバーアプリケーションで特に重要となるコンピューターのパフォーマンスを高めることができます。

また、特定の処理が Kaspersky Embedded Systems Security によって疑わしい処理に分類されたとしても、多数のアプリケーションの機能を考慮すると安全な場合があります。たとえば、キーボードで入力したテキストの取得は、自動キーボードレイアウト切り替えプログラム（Punto Switcher など）では通常の処理です。このようなアプリケーションの特性を考慮して、アプリケーション処理を監視対象から除外するために、このようなアプリケーションを信頼するアプリケーションのリストに追加してください。

信頼するアプリケーションは、Kaspersky Embedded Systems Security と他のアプリケーションとの間の互換性の問題（たとえば、Kaspersky Embedded Systems Security と他のアンチウイルス製品によるサードパーティ製コンピューターのネットワークトラフィックの二重スキャンなど）を回避するのに役立ちます。

ただし、信頼するアプリケーションの実行ファイルとプロセスのウイルスおよびその他のマルウェアスキャンは実行されます。アプリケーションを Kaspersky Embedded Systems Security のスキャンから完全に除外するには、信頼するオブジェクトを設定します。

Kaspersky Embedded Systems Security は、5000 を超えるオブジェクトを含む信頼するアプリケーションのリストをサポートしていません。

**Kaspersky Security Center 管理コンソールで信頼リストにアプリケーションを追加する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**詳細設定**］を選択します。
4. ［**信頼ゾーン**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウで、**信頼するアプリケーション**タブを選択します。

   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。
6. このチェックボックスにより、保護対象デバイスにインストールされたバックアップツールによってファイルの読み取り操作が実行される場合に、その操作のスキャンをスキップする場合は［**ファイルのバックアップ処理を確認しない**］をオンにします。
7. 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。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの信頼するアプリケーションは子ポリシー内では読み取り専用で表示されます。親ポリシーの信頼するアプリケーションは、変更することも削除することもできません。
8. 信頼するアプリケーションのローカルのリストをユーザーが作成できるようにするには、［**ローカルの信頼するアプリケーションの編集を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された信頼するアプリケーションの全体的なリストに加えて自分のローカルの信頼するアプリケーションのリストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の信頼するアプリケーションの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するアプリケーションのリストがアプリケーションコンソールで非表示になります。
9. 信頼するプロセスのファイル操作のスキャンをスキップするには、［**指定したプロセスでのファイルの処理をチェックしない**］をオンにします。
10. ［**追加**］をクリックして、処理を選択します：

    - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも 1 つカテゴリに追加します。
    - **新しい除外**：Kaspersky Embedded Systems Security は新しい信頼するアプリケーションをリストのルートに追加します。

- **選択したカテゴリに新しい除外を追加**：新しい信頼するアプリケーションを特定のカテゴリに追加するには、カテゴリを選択します。
- **リストから除外を選択**：Kaspersky Embedded Systems Security を素早く設定するために、設定済みの信頼するアプリケーションのリストからアプリケーションを追加できます。

11. 表示されたウィンドウで、［**信頼対象と判断するためにディスク上でフルプロセスパスを使用する**］をオンにして、ファイルへのパスを入力し、プロセスが信頼対象かどうかを判断します。

    Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

    > Kaspersky Security Center コンソールで信頼するアプリケーションのリストを作成する際、環境変数 `%userprofile%` は Kaspersky Embedded Systems Security ではサポートされません。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「*」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

12. 信頼するアプリケーションの詳細設定を指定します（下の表を参照ください）。
13. ［**OK**］をクリックします。

    新しい信頼するアプリケーションがリストに追加されます。いつでもオブジェクトの横のチェックボックスを使用して信頼ゾーンからアプリケーションを除外できます。

14. 変更内容を保存します。

### *Kaspersky Security Center Web コンソールで信頼リストにアプリケーションを追加する方法*

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. Kaspersky Embedded Systems 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。

4. ［**アプリケーション設定**］タブを選択します。
5. ［**詳細設定**］→［**信頼ゾーン**］に移動し、［**設定**］をクリックします。
6. 表示されたウィンドウで、**信頼するアプリケーション**タブを選択します。
7. このチェックボックスにより、保護対象デバイスにインストールされたバックアップツールによってファイルの読み取り操作が実行される場合に、その操作のスキャンをスキップする場合は［**ファイルのバックアップ処理を確認しない**］をオンにします。
8. 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。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシーの信頼するアプリケーションは子ポリシー内では読み取り専用で表示されます。親ポリシーの信頼するアプリケーションは、変更することも削除することもできません。

9. 信頼するアプリケーションのローカルのリストをユーザーが作成できるようにするには、［**ローカルの信頼するアプリケーションの編集を許可する**］を選択します。こうすることで、ユーザーはポリシー内で作成された信頼するアプリケーションの全体的なリストに加えて自分のローカルの信頼するアプリケーションのリストを作成することができます。管理者は Kaspersky Security Center を使用してコンピューターのプロパティ内のリストの項目を表示、追加、変数または削除することができます。

   チェックボックスがオフの場合、ユーザーはポリシー内の信頼するアプリケーションの全体的なリストのみにアクセスできます。また、このチェックボックスがオフの場合、すべての信頼するアプリケーションのリストがアプリケーションコンソールで非表示になります。

10. 信頼するプロセスのファイル操作のスキャンをスキップするには、［**指定したプロセスでのファイルの処理をチェックしない**］をオンにします。

11. ［**追加**］をクリックして、処理を選択します：

    - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも 1 つカテゴリに追加します。
    - **新しい除外**：Kaspersky Embedded Systems Security は新しい信頼するアプリケーションをリストのルートに追加します。
    - **選択したカテゴリに新しい除外を追加**：新しい信頼するアプリケーションを特定のカテゴリに追加するには、カテゴリを選択します。
    - **リストから除外を選択**：Kaspersky Embedded Systems Security を素早く設定するために、設定済みの信頼するアプリケーションのリストからアプリケーションを追加できます。

12. 表示されたウィンドウで、［**信頼対象と判断するためにディスク上でフルプロセスパスを使用する**］をオンにして、ファイルへのパスを入力し、プロセスが信頼対象かどうかを判断します。

    Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

    > Kaspersky Security Center コンソールで信頼するアプリケーションのリストを作成する際、環境変数 `%userprofile%` は Kaspersky Embedded Systems Security ではサポートされません。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「*」を使用できます。新しい環境変数を追加したら本製品を再起動する必要があります。

13. 信頼するアプリケーションの詳細設定を指定します（下の表を参照ください）。

14. ［**OK**］をクリックします。

    新しい信頼するアプリケーションがリストに追加されます。いつでも［**処理**］列のチェックボックスを使用して信頼ゾーンからアプリケーションを除外できます。

15. 変更内容を保存します。

**アプリケーションコンソールで信頼リストにアプリケーションを追加する方法**

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**信頼ゾーン**］を選択します。

   ［**信頼ゾーンの設定**］ウィンドウが表示されます。

2. ［**除外リスト**］セクションで、［**信頼するアプリケーション**］ブロックの横にある［**設定**］をクリックします。

3. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも1つカテゴリに追加します。
   - **新しい除外**：Kaspersky Embedded Systems Security は新しい信頼するアプリケーションをリストのルートに追加します。
   - **選択したカテゴリに新しい除外を追加**：新しい信頼するアプリケーションを特定のカテゴリに追加するには、カテゴリを選択します。
   - **リストから除外を選択**：Kaspersky Embedded Systems Security を素早く設定するために、設定済みの信頼するアプリケーションのリストからアプリケーションを追加できます。

4. リストからファイルを選択するか、信頼するアプリケーションの実行ファイルのパスを入力します。

   Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

   > Kaspersky Embedded Systems Security は環境変数をサポートしています。同時に、Kaspersky Embedded Systems Security は、本製品のローカルインターフェイスでパスを変換します。たとえば、ファイルパス「`%userprofile%\Documents\File.exe`」、「`C:\Users\Fred123\Documents\File.exe`」がユーザー「Fred123」の本製品のローカルインターフェイスに追加されたとします。結果、Kaspersky Embedded Systems Security は信頼するアプリケーション「`File.exe`」を別のユーザーに対して無視します。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「`*`」を使用できます。

   > 新しい環境変数を追加したら本製品を再起動する必要があります。

5. 信頼するアプリケーションの詳細設定を指定します（下の表を参照ください）。

6. ［**OK**］をクリックします。

   新しい信頼するアプリケーションがリストに追加されます。いつでもオブジェクト名の横のチェックボックスを使用して信頼ゾーンからアプリケーションを除外できます。

7. 変更内容を保存します。

信頼するアプリケーションの設定

| パラメータ | 説明 |
| --- | --- |
| **信頼対象と判断するためにディスク上でフルプロセスパスを使用する** | ファイルの完全パスを使用してプロセスを信頼するかどうかが判定されます。 |
| **信頼対象と判断するためにプロセスファイルハッシュを使用する** | 選択したファイルのハッシュを使用してプロセスの信頼ステータスが決定されます。チェックボックスがオフの場合、プロセスの信頼ステータスを判定する基準として、ファイルのハッシュは使用されません。 |

| パラメータ | 説明 |
| --- | --- |
| **アプリケーションインターフェイスの操作を許可する** | Kaspersky Embedded Systems Security は、リモートコンピューターからのアプリケーションサービスを管理しようとする試行をすべてブロックします。このチェックボックスをオンにすると、リモートアクセスアプリケーションで Kaspersky Embedded Systems Security インターフェイスを経由して Kaspersky Embedded Systems Security 設定を管理できます。 |
| **子アプリケーションの動作を監視しない** | Kaspersky Embedded Systems Security はファイルまたはこのアプリケーションによって開始されたアプリケーションのネットワークの動作を監視しません。例外は再帰的に適用できます。そのため、子アプリケーションのチェーン全体の動作は監視されません。 |
| **親プロセス（アプリケーション）の制限を継承しない** | 親プロセスで設定された制限は子プロセスには適用されません。親プロセスは、アプリケーション権限およびアプリケーションネットワークルールが設定されたアプリケーションによって開始されます。 |
| **プロセスメモリをスキャンしない** | プロセスメモリはスキャンされません。 |

# ローカルの信頼ゾーンの作成

ユーザーが特定のコンピューター用に自分のローカル信頼ゾーンを作成できるようになりました。これにより、ユーザーはポリシー内の信頼ゾーンの全体的なリストに加えて自分のローカルの除外リストと信頼するアプリケーションのリストを作成することができます。管理者はローカルの除外リストまたはローカルの信頼するアプリケーションの使用をポリシー設定で許可またはブロックできます。これを行うには、ポリシーの［**信頼ゾーン**］セクションの［**信頼するオブジェクト**］タブと［**信頼するアプリケーション**］タブにある［**ローカルの除外リストの使用を許可する**］と［**ローカルの信頼するアプリケーションの編集を許可する**］を使用します。

ローカルの信頼ゾーンの作成を管理者が許可している場合、ユーザーはアプリケーションコンソールで自分の信頼するオブジェクトとアプリケーションを追加できます。また、ユーザーはポリシーで設定された信頼するゾーンに含まれるオブジェクトを変更または削除する権限がありません。管理者は、個別のコンピューターに除外リストを追加する必要がある場合、Kaspersky Security Center のコンソールでリスト項目の表示、追加、変更、削除も行なうことができます。

信頼ゾーンの設定がコンソールで管理者によってブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するオブジェクトとアプリケーションが禁止されている場合は、信頼するオブジェクトとアプリケーションのリストがアプリケーションコンソールで非表示になります。

### Kaspersky Security Center 管理コンソールでローカルの信頼ゾーンにオブジェクトを追加する方法

1. コンソールツリーの［**管理対象デバイス**］フォルダーで、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。
2. 作業領域で、［**デバイス**］タブを選択します。
3. ダブルクリックして、コンピューターのプロパティウィンドウを開きます。
4. コンピューター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。
5. コンピューターにインストールされているカスペルスキー製品のリストから［**Kaspersky Embedded Systems 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を開きます。
6. 本製品の設定ウィンドウで、［**詳細設定**］→［**信頼ゾーン**］の順に選択し、［**設定**］をクリックします。

7. ［**信頼するオブジェクト**］タブで、ローカルの信頼するオブジェクトのリストを作成します。

   ローカルの信頼するオブジェクトのリストを作成するルールは、一般的な除外リストの場合と同じです。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

8. ［**信頼するアプリケーション**］タブで、ローカルの信頼するアプリケーションのリストを作成します。ローカルの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表示されます。

   ローカルの信頼するアプリケーションのリストにアプリケーションを追加するルールは、一般的なリストに追加するルールと同じです。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。

9. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでローカルの信頼ゾーンにオブジェクトを追加する方法**

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。
2. ブロックされている操作の実行を許可するユーザーのコンピューターの名前をクリックします。
3. ［**アプリケーション**］タブを選択します。
4. ［**Kaspersky Embedded Systems Security**］をクリックします。

   ローカルアプリケーション設定が表示されます。
5. ［**アプリケーション設定**］タブを選択します。
6. 本製品の設定ウィンドウで、［**詳細設定**］→［**信頼ゾーン**］の順に選択し、［**設定**］をクリックします。

   ［**除外リストと検知したオブジェクトの種別**］ウィンドウが表示されます。
7. ［**信頼するオブジェクト**］タブで、ローカルの信頼するオブジェクトのリストを作成します。

   ローカルの除外リストを作成するルールは、一般的な除外リストを作成するルールと同じです。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。
8. ［**信頼するアプリケーション**］タブで、ローカルの信頼するアプリケーションのリストを作成します。

   ローカルの信頼するアプリケーションのリストにアプリケーションを追加するルールは、一般的なリストに追加するルールと同じです。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「*」および「?」をサポートします。
9. 変更内容を保存します。

***アプリケーションコンソールでローカルの信頼するオブジェクトを作成する方法***

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**信頼ゾーン**］を選択します。

   ［**信頼ゾーンの設定**］ウィンドウが表示されます。

2. ［**信頼するオブジェクトとアプリケーション**］セクションで、［**ローカルの信頼するオブジェクト**］ブロックの横にある［**設定**］をクリックします。

   信頼するオブジェクトの設定が Kaspersky Security Center 管理コンソールで管理者によってブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するオブジェクトが禁止されている場合（［**ローカルの除外リストの使用を許可する**］がオフ）は、信頼するオブジェクトのリストがアプリケーションコンソールで非表示になります。

3. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するオブジェクトを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、少なくとも 1 つの信頼するオブジェクトをカテゴリに追加します。
   - **新しい除外**：Kaspersky Embedded Systems Security は新しい信頼するオブジェクトをリストのルートに追加します。
   - **選択したカテゴリに新しい除外を追加**：新しい信頼するオブジェクトを特定のカテゴリに追加するには、カテゴリを選択します。
   - **リストから除外を選択**：Kaspersky Embedded Systems Security を素早く設定するために、設定済みの信頼するオブジェクトのリストから除外項目を追加できます。

4. ［**新しい除外**］を選択すると、［**信頼するオブジェクト**］ウィンドウが表示されます。

5. ファイルまたはフォルダーをスキャンから除外するには、［**ファイルまたはフォルダー**］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選択**］をクリックしてウィンドウを開き、そのウィンドウで［**参照**］をクリックしてファイルまたはフォルダーを選択します。

   手動でパスを入力することもできます。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

   - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
   - 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。
   - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

     ファイルパスの最初、途中、または最後のどこでもマスクを使用できます。たとえば、すべてのユーザーの特定のフォルダーを除外リストに含める場合は、マスク「`?:\Users\*\Folder\`」と入力できます。

6. 定義済みの範囲をスキャンから除外するには、［**定義済みの範囲**］チェックボックスをオンにします。［**定義済みの範囲の選択**］をクリックして、ウィンドウを開き、そのウィンドウで、保護対象デバイスの標準の範囲を 1 つ選択します。

7. 特定のオブジェクトをスキャンから除外するには、［**検知するオブジェクトの種別**］をオンにします。［**オブジェクト名の入力**］をクリックして、［**追加**］をクリックし、表示されたウィンドウで、「ウイルス百科事典」の分類に従ってオブジェクト名を入力します（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。

8. 個々のファイルをスキャンから除外するには、［**オブジェクトハッシュ**］をオンにします。［**オブジェクトハッシュの入力**］をクリックしてウィンドウを開き、そのウィンドウでファイルハッシュを入力します。

   ファイルが変更されている場合はファイルのハッシュも変更されます。この場合、除外リストには更新されたファイルは追加されません。

9. ［**ルールの使用範囲**］ブロックで、スキャンの例外を適用するコンポーネントを選択します。

10. 必要に応じて、［**コメント**］に、作成する信頼するオブジェクトの簡単なコメントを入力します。

11. 変更を保存して、除外項目をリストに追加します。いつでもオブジェクトの横のチェックボックスを使用して信頼するオブジェクトを無効にできます。

### *アプリケーションコンソールでローカルの信頼するアプリケーションにアプリケーションを追加する方法*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**信頼ゾーン**］を選択します。

   ［**信頼ゾーンの設定**］ウィンドウが表示されます。

2. ［**除外リスト**］セクションで、［**ローカルの信頼するアプリケーション**］ブロックの横にある［**設定**］をクリックします。

   信頼するアプリケーションの設定がKaspersky Security Center管理コンソールで管理者によってブロックされている場合（「鍵が閉じた」シンボル）とローカルの信頼するアプリケーションが禁止されている場合（［**ローカルの信頼するアプリケーションの編集を許可する**］がオフ）は、すべての信頼するアプリケーションのリストがアプリケーションコンソールで非表示になります。

3. ［**追加**］をクリックして、処理を選択します：

   - **カテゴリ**：信頼するアプリケーションを個別のカテゴリに分類できます。新しいカテゴリを作成するには、カテゴリの名前を入力し、信頼するアプリケーションを少なくとも1つカテゴリに追加します。
   - **新しい除外**：Kaspersky Embedded Systems Securityは新しい信頼するアプリケーションをリストのルートに追加します。
   - **選択したカテゴリに新しい除外を追加**：新しい信頼するアプリケーションを特定のカテゴリに追加するには、カテゴリを選択します。
   - **リストから除外を選択**：Kaspersky Embedded Systems Securityを素早く設定するために、設定済みの信頼するアプリケーションのリストからアプリケーションを追加できます。

4. ［**新しい除外**］を選択すると、［**信頼するオブジェクト**］ウィンドウが表示されます。

5. ［**信頼対象と判断するためにディスク上でフルプロセスパスを使用する**］をオンにして、信頼するアプリケーションの実行ファイルのパスを入力します。

   Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。

   > Kaspersky Embedded Systems Security は環境変数をサポートしています。同時に、Kaspersky Embedded Systems Security は、本製品のローカルインターフェイスでパスを変換します。たとえば、ファイルパス「`%userprofile%\Documents\File.exe`」、「`C:\Users\Fred123\Documents\File.exe`」がユーザー「Fred123」の本製品のローカルインターフェイスに追加されたとします。結果、Kaspersky Embedded Systems Security は信頼するアプリケーション「`File.exe`」を別のユーザーに対して無視します。すべてのユーザーアカウントに入力を適用するには、「`C:\Users\*\Documents\File.exe`」のように文字「`*`」を使用できます。

   > 新しい環境変数を追加したら本製品を再起動する必要があります。

6. 信頼するアプリケーションのプロパティウィンドウで、詳細設定を指定します。

7. 変更を保存して、除外項目をリストに追加します。

# 信頼ゾーンでのエクスポート / インポート

*信頼ゾーン*は Kaspersky Embedded Systems 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。信頼ゾーンは、*信頼するオブジェクト*と*信頼するアプリケーション*の 2 つのリストから構成されます。これにより、例えば同じ種別の多数の除外リスト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、除外リストおよび信頼するアプリケーションのリスト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。

本製品は、*除外リスト*および信頼するアプリケーションのリストのインポートおよびエクスポートに XML 形式のファイルを使用します：

> Kaspersky Embedded Systems Security は、5000 を超えるオブジェクトを含む除外リストおよび信頼するアプリケーションのリストをサポートしていません。

### Kaspersky Security Center 管理コンソールで信頼ゾーンをエクスポートおよびインポートする方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**詳細設定**］→［**信頼ゾーン**］の順に選択し、［**設定**］をクリックします。

4. ルールのリストをエクスポートするには：

   a. ［**信頼するオブジェクト**］タブを選択します。

   b. エクスポートする除外リストを選択します。

      除外リストが何も選択されていない場合、すべての除外リストがエクスポートされます。

   c. フォルダーアイコンをクリックして、ドロップダウンリストから［**エクスポート**］を選択します。

      表示されたウィンドウで、除外リストをエクスポートする XML 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. 信頼するアプリケーションのリストをエクスポートするには：

   a. ［**信頼するアプリケーション**］タブを選択します。

      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。

   b. エクスポート対象の信頼するアプリケーションを選択します。

      信頼するアプリケーションが何も選択されていない場合、すべての信頼するアプリケーションがエクスポートされます。

   c. フォルダーアイコンをクリックして、ドロップダウンリストから［**エクスポート**］を選択します。

   d. 表示されたウィンドウで、信頼するアプリケーションのリストをエクスポートする XML 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。

   e. ファイルを保存します。

      Kaspersky Embedded Systems Security は、リストを XML ファイルにエクスポートします。

6. 除外リストをインポートするには：

   a. ［**信頼するオブジェクト**］タブを選択します。

      除外リストを含むウィンドウが開きます。

   b. フォルダーアイコンをクリックして、ドロップダウンリストから［**インポート**］を選択します。

   c. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。

   d. ファイルを開きます。

      コンピューターに除外リストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

7. 信頼するアプリケーションのリストをインポートするには：

   a. ［**信頼するアプリケーション**］タブを選択します。

      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。

   b. ［**インポート**］をクリックします。

   c. 表示されたウィンドウで、信頼するアプリケーションのリストをインポートする XML ファイルを選択します。

d. ファイルを開きます。

コンピューターに信頼するアプリケーションのリストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

8. 変更内容を保存します。

### Kaspersky Security Center Web コンソールで信頼ゾーン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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**詳細設定**］→［**信頼ゾーン**］に移動し、［**設定**］をクリックします。
5. ルールのリストをエクスポートするには：

a. ［**信頼するオブジェクトとアプリケーション**］タブで、エクスポートする除外リストを選択します。

b. 3 つの点をクリックして［**エクスポート**］を選択します。

c. 選択した除外リストのみをエクスポートするか、または除外リストの全体をエクスポートするかを確認します。

Kaspersky Embedded Systems Security は、リストを XML ファイルにエクスポートします。

6. 信頼するアプリケーションのリストをエクスポートするには：

a. ［**信頼するオブジェクトとアプリケーション**］タブで、エクスポートするアプリケーションを選択します。

b. 3 つの点をクリックして［**エクスポート**］を選択します。

c. 選択したアプリケーションのみをエクスポートするか、またはリストの全体をエクスポートするかを確認します。

Kaspersky Embedded Systems Security は、リストを XML ファイルにエクスポートします。

7. 除外リストをインポートするには：

a. ［**信頼するオブジェクトとアプリケーション**］タブで、バージョン 3.4 以前の本製品で作成された XML ファイルから除外リストをインポートする場合は、［**以前のバージョンからインポートする**］をクリックします。

バージョン 4.0 以降で作成された XML ファイルからルールをインポートする場合は、［**インポート**］をクリックします。

b. コンピューターに除外リストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

c. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。

d. ［**インポート**］をクリックします。

8. 信頼するアプリケーションのリストをインポートするには：

a. ［**信頼するオブジェクトとアプリケーション**］タブで、バージョン 3.4 以前の本製品で作成された XML ファイルから信頼するアプリケーションのリストをインポートする場合は、［**以前のバージョンからインポートする**］をクリックします。

バージョン 4.0 以降で作成された XML ファイルから信頼するアプリケーションのリストをインポートする場合は、［**インポート**］をクリックします。

b. コンピューターに信頼するアプリケーションのリストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

c. 表示されたウィンドウで、信頼するアプリケーションのリストをインポートする XML ファイルを選択します。

d. ［**インポート**］をクリックします。

9. 変更内容を保存します。

***アプリケーションコンソールで信頼ゾーンをエクスポートまたはインポートする方法***

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**信頼ゾーン**］を選択します。

［**信頼ゾーンの設定**］ウィンドウが表示されます。

2. 除外リストと信頼するアプリケーションのリストをエクスポートするには：

a. ［**除外リスト**］セクションで、［**信頼するオブジェクト**］ブロックまたは［**信頼するアプリケーション**］ブロックの横にある［**設定**］をクリックします。

b. エクスポート対象の除外リストまたは信頼するアプリケーションを選択します。

c. フォルダーアイコンをクリックして［**エクスポート**］を選択します。

d. 表示されたウィンドウで、除外リストまたは信頼するアプリケーションのリストをエクスポートする XML 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。

e. ファイルを保存します。

Kaspersky Embedded Systems Security は、リストを XML ファイルにエクスポートします。

3. 除外リストと信頼するアプリケーションのリストをインポートするには：

a. ［**除外リスト**］セクションで、［**信頼するオブジェクト**］ブロックまたは［**信頼するアプリケーション**］ブロックの横にある［**設定**］をクリックします。

b. インポート対象の除外リストまたは信頼するアプリケーションを選択します。

c. フォルダーアイコンをクリックして［**エクスポート**］を選択します。

d. 表示されたウィンドウで、除外リストまたは信頼するアプリケーションのリストをインポートする XML ファイルを選択します。

e. ファイルを開きます。

コンピューターに除外リストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

4. 変更内容を保存します。

# 信頼するシステム証明書ストアの使用

システム証明書ストアを使用することで、信頼されるデジタル署名で署名されたアプリケーションをスキャンから除外できます。Kaspersky Embedded Systems Security はこのようなアプリケーションを*信頼済みグループ*に割り当てます。

信頼するシステム証明書ストアの使用を開始するには：

**Kaspersky Security Center 管理コンソールで信頼するシステム証明書ストアの使用を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**詳細設定**］→［**信頼ゾーン**］の順に選択し、［**設定**］をクリックします。
4. ［**信頼するシステム証明書ストア**］タブを選択します。
5. ［**信頼するシステム証明書ストアを使用**］をオンにして、ドロップダウンリストで、Kaspersky Embedded Systems Security で信頼できると判断するシステムストアを選択します。
6. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで信頼するシステム証明書ストアの使用を設定する方法**

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**詳細設定**］→［**信頼ゾーン**］に移動し、［**設定**］をクリックします。
5. ［**信頼するシステム証明書ストア**］タブを選択します。

6. ［**信頼するシステム証明書ストアを使用**］をオンにして、ドロップダウンリストで、Kaspersky Embedded Systems Security で信頼できると判断するシステムストアを選択します。

7. 変更内容を保存します。

***アプリケーションコンソールで信頼するシステム証明書ストアの使用を設定する方法***

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーを選択して、フォルダーのコンテキストメニューから［**信頼ゾーン**］を選択します。

   ［**信頼ゾーンの設定**］ウィンドウが表示されます。

2. ［**信頼するシステム証明書ストア**］で、［**信頼するシステム証明書ストアを使用**］をオンにして、ドロップダウンリストで、Kaspersky Embedded Systems Security で信頼できると判断するシステムストアを選択します。

3. 変更内容を保存します。

# ファイルのリアルタイム保護

次の保護対象デバイスのオブジェクトにアクセスされた時に、Kaspersky Embedded Systems Security のファイルのリアルタイム保護コンポーネントによってそのオブジェクトがスキャンされます：

- ファイル
- NTFS 代替データストリーム。
- ローカルハードディスクおよび外部デバイスのマスターブートレコードとブートセクター。
- Windows Server 2016 と Windows Server 2019 のコンテナファイル。

何らかのアプリケーションが保護対象デバイスに対してファイルの書き込みを行った場合、または保護対象デバイスからファイルの読み取りを行った場合に、Kaspersky Embedded Systems Security によってそのファイルがインターセプトされ、脅威がスキャンされます。脅威が検知された場合は、ファイルの駆除を試行する処理、隔離に移動する処理、または削除する処理のうち、既定の処理または指定した処理が実行されます。駆除または削除の前には、ソースファイルの暗号化されたコピーがバックアップに保存されます。

Kaspersky Embedded Systems Security は、Windows Server 2016 と Windows Server 2019 のコンテナで実行されるファイル操作をインターセプトします。

コンテナは、アプリケーションがオペレーティングシステムと直接やり取りすることなく実行できる分離された環境です。コンテナがコンポーネントの保護範囲内にある場合、Kaspersky Embedded Systems Security は、ユーザーがアクセスしているコンテナファイルをスキャンしてコンピューターの脅威を検知します。脅威が検知されると、コンテナの駆除が試行されます。駆除が成功すると、コンテナは動作を続けます。駆除に失敗した場合は、コンテナがオフになります。

Kaspersky Embedded Systems Security は、Windows Subsystem for Linux® で実行するプロセスでも悪意のあるソフトウェアを検知します。そのようなプロセスに対して、ファイルのリアルタイム保護コンポーネントは現在の設定で定義されている処理を適用します。

# タスクの保護範囲とセキュリティ設定について

既定では、ファイルのリアルタイム保護コンポーネントはデバイスのファイルシステムのすべてのオブジェクトを保護します。ファイルシステムのオブジェクトをすべて保護対象とするセキュリティ要件がない場合、またはタスク範囲から一部のオブジェクトを除外する場合は、保護範囲を制限できます。

アプリケーションコンソールでは、保護範囲は、Kaspersky Embedded Systems Security が監視できるデバイスのファイルリソースのリストとして表示されます。

## セキュリティ設定

タスクのセキュリティ設定は、保護範囲に含まれるすべてのフォルダーや項目の共通の設定として、あるいはデバイスのファイルリソースリストのフォルダーや項目ごとに異なる設定として、設定することができます。

選択した親フォルダーに対するセキュリティ設定は、すべてのサブフォルダーに自動的に適用されます。親フォルダーのセキュリティ設定は、個別に設定されたサブフォルダーに適用されません。

選択した保護範囲の設定は、次のいずれかの方法で行います：

- 3 つの定義済みセキュリティレベルのいずれかを選択する。
- ファイルリソースリストで選択したフォルダーや項目に対してセキュリティ設定を手動で行う（セキュリティレベルが［**カスタム**］に変更されます）。

# 定義済みの保護範囲

ファイルリソースリストには、Microsoft Windows のセキュリティの設定に従って読み取りアクセス権のあるフォルダーが表示されます。

Kaspersky Embedded Systems Security は次の定義済み保護範囲をカバーします：

- **ローカルハードディスク**：Kaspersky Embedded Systems Security はデバイスのハードディスク上のファイルを保護します。
- **リムーバブルドライブ**：CD やリムーバブルドライブなどの外部デバイスのファイルが保護されます。すべてのリムーバブルドライブ、個々のディスク、フォルダー、ファイルを保護範囲に含めたり保護範囲から除外したりすることができます。
- **ネットワーク**：デバイス上で実行されているアプリケーションによってネットワークフォルダーに書き込まれたファイルとネットワークフォルダーから読み取られたファイルが保護されます。他の保護対象デバイスのアプリケーションによってそのようなファイルにアクセスされた場合には、ファイルは保護されません。

既定では、範囲リストで、あらかじめ定義された保護範囲を設定、表示できます。保護範囲設定時に、あらかじめ定義された範囲をリストに追加することもできます。

接続されているネットワークドライブも、保護対象デバイスのファイルリソースのリストには表示されません。ネットワークドライブ上のオブジェクトを保護範囲に含めるには、そのネットワークドライブに対応するフォルダーへのパスを UNC（Universal Naming Convention）フォーマットで指定します。

# 定義済みのセキュリティレベルについて

保護対象デバイスのファイルリソースツリーまたはファイルリソースリストで選択したフォルダーに対して、次のいずれかの定義済みセキュリティレベルを適用できます：［**最大のパフォーマンス**］、［**推奨**］、［**最大の保護**］および［**通知する**］。これらのレベルにはそれぞれ、独自の定義済みセキュリティ設定が含まれます（以下の表を参照）。

### 最大のパフォーマンス

［**最大のパフォーマンス**］のセキュリティレベルは、保護対象デバイスとワークステーションでの Kaspersky Embedded Systems Security の使用に加えて、ファイアウォールや既存のポリシーなど、保護対象デバイスの追加のセキュリティ対策がネットワークに備えられている場合に使用してください。

## 推奨

［**推奨**］セキュリティレベルは、デバイスの保護とパフォーマンスへの影響が、最適な組み合わせで設定されています。カスペルスキーでは、このレベルがほとんどの企業ネットワークのデバイスの保護に十分なものとして推奨しています。既定では、［**推奨**］セキュリティレベルが選択されています。

## 最大の保護

組織のネットワークのデバイスセキュリティ要件が引き上げられた場合、［**最大の保護**］セキュリティレベルを推奨します。

## 通知する

企業ネットワーク内に感染したコンピューターが多数存在する可能性があり、それらをブロックすると組織の業務に大きな支障をきたす可能性がある場合は、［**通知する**］セキュリティレベルを推奨します。

設定済みセキュリティレベルと対応する設定値

| オプション | セキュリティレベル | | | |
|---|---|---|---|---|
| **最大のパフォーマンス** | **推奨** | **最大の保護** | **通知する** | |
| **オブジェクトの保護** | 定義データベース指定の拡張子リストによってオブジェクトをスキャン | ファイル形式によってオブジェクトをスキャン | ファイル形式によってオブジェクトをスキャン | ファイル形式によってオブジェクトをスキャン |
| **作成または変更されたファイルのみをスキャン** | 有効 | 有効 | 無効 | 有効 |
| **複合ファイルのスキャン** | 無効 | Microsoft Office 形式のファイルをスキャン | Microsoft Office 形式のファイルをスキャン | Microsoft Office 形式のファイルをスキャン |
| **感染などの問題があるオブジェクトの処理** | アクセスをブロックして駆除。駆除できない場合は削除 | アクセスをブロックし、カスペルスキーが推奨するアクションを実行 | アクセスをブロックして駆除。駆除できない場合は削除 | 通知 |
| **選択したオブジェクト種別に操作を適用する** | 無効 | 無効 | 無効 | 無効 |
| **埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する** | 無効 | 無効 | 有効 | 無効 |
| システムに重大な影響があるオブジェクトは、オペレーティングシステムおよび Kaspersky Embedded Systems Security の動作に必要なファイルです。これらのファイルは削除できません。このようなオブジェクトに関連付けられたプロセスは終了できません。 | | | | |
| **次のサイズを超える複合ファイルをバックグラウンドで解凍する（MB）** | | | | |
| **スキャン時間が次を超えたら停止する（秒）** | 60 秒 | 60 秒 | 60 秒 | 60 秒 |
| **スキャンする複合オブジェクトの最大サイズ（MB）** | 8 MB | 8 MB | オフ | 8 MB |
| **iSwift を使用する** | 有効 | 有効 | 有効 | 有効 |
| **iChecker を使用する** | 有効 | 有効 | 有効 | 有効 |

# ファイルのリアルタイム保護コンポーネントで既定でスキャンされるファイルの拡張子

Kaspersky Embedded Systems Security で、既定でスキャンされるファイルの拡張子は、次の通りです：

- *386*
- *acm*
- *ade*、*adp*
- *asp*
- *asx*
- *ax*
- *bas*
- *bat*
- *bin*
- *chm*
- *cla*、*clas**
- *cmd*
- *com*
- *cpl*
- *crt*
- *dll*
- *dpl*
- *drv*
- *dvb*
- *dwg*
- *efi*
- *emf*
- *eml*

- *exe*
- *fon*
- *fpm*
- *hlp*
- *hta*
- *htm、html**
- *htt*
- *ico*
- *inf*
- *ini*
- *ins*
- *isp*
- *jpg、jpe*
- *js、jse*
- *lnk*
- *mbx*
- *msc*
- *msg*
- *msi*
- *msp*
- *mst*
- *nws*
- *ocx*
- *oft*
- *otm*
- *pcd*
- *pdf*
- *php*

- *pht*
- *phtm**
- *pif*
- *plg*
- *png*
- *pot*
- *prf*
- *prg*
- *reg*
- *rsc*
- *rtf*
- *scf*
- *scr*
- *sct*
- *shb*
- *shs*
- *sht*
- *shtm**
- *swf*
- *sys*
- *the*
- *them**
- *tsp*
- *url*
- *vb*
- *vbe*
- *vbs*
- *vxd*

- *wma*
- *wmf*
- *wmv*
- *wsc*
- *wsf*
- *wsh*
- *do?*
- *md?*
- *mp?*
- *ov?*
- *pp?*
- *vs?*
- *xl?*

# ファイルのリアルタイム保護コンポーネントの設定

既定では、ファイルのリアルタイム保護コンポーネントでは、次の表の設定が使用されます。これらの設定の値を変更できます。

ファイルのリアルタイム保護コンポーネントの既定の設定

| パラメータ | 既定値 | 説明 |
| --- | --- | --- |
| 保護範囲 | 仮想ドライブを除く保護対象デバイス全体。 | このオプションを使用して、保護範囲を変更します。 |
| セキュリティ設定 | 保護範囲全体の共通の設定で、［**推奨**］セキュリティレベルに対応します。 | 保護対象デバイスのファイルリソースリストまたはツリーで選択したフォルダーに対して、次の操作を実行できます：<br>• 別の定義済みセキュリティレベルを選択する<br>• 手動でセキュリティ設定を変更する<br>後で異なるフォルダーに使用するためのテンプレートとして、選択したフォルダーのセキュリティ設定グループを保存できます。 |
| **オブジェクトの保護モード** | **スマートモード** | このオプションを使用して、保護モードを選択できます。つまり、Kaspersky Embedded Systems Security がオブジェクトをスキャンするアクセス試行の種別を定義できます。 |
| **ヒューリスティックアナライザー** | ［**中**］セキュリティレベルが適用されます。 | ヒューリスティックアナライザーを有効または無効にできます。また、分析レベルを設定できます。 |
| **悪意のある活動を示すセッションのネットワーク共有リソースへのアクセスをブロックする** | 適用されません。 | このオプションを使用して、現在のセッションをブロックし、［ブロック対象コンピューターの保管領域］セクションで悪意のある活動が検知されたホスト IP またはホスト LUID を追加します。 |
| **アクティブな脅威の検知時に簡易スキャンを起動する** | 適用されます。 | アクティブな感染を検知すると、簡易スキャンタスクが作成され、起動します。 |

| パラメータ | 既定値 | 説明 |
| --- | --- | --- |
| **駆除できない場合はコンテナーを停止する** | 適用されます。 | 本製品に、検知したオブジェクトに対する読み取りおよび書き込み権限がない可能性があります。この場合、検知したオブジェクトを駆除することも削除することもできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。 |
| **Windows コンテナー内で実行されたファイル操作をスキャンしない** | 適用されます。 | このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナをリアルタイムで継続的にスキャンします。 |

### Kaspersky Security Center 管理コンソールでファイルのウイルススキャンを有効にする方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ファイルのリアルタイム保護の設定**］セクションで、［**設定**］をクリックします。
5. ［**ファイルのリアルタイム保護**］チェックボックスをオンにします。
6. ［**オブジェクトの保護モード**］ブロックの［**全般**］タブで、ファイルのリアルタイム保護の操作モードを選択します：
   - **スマートモード**：スキャンするオブジェクトが自動的に選択されます。開いているオブジェクトがスキャンされ、オブジェクトが変更された場合は保存された後にもう一度スキャンされます。オブジェクトがプロセスによって複数回アクセスされて変更された場合、プロセスによってオブジェクトが最後に保存された後でのみオブジェクトが再スキャンされます。
   - **アクセス時と変更時**：オブジェクトが開いている時にスキャンされ、オブジェクトが変更された場合、そのオブジェクトが保存された後で再スキャンします。既定では、このオプションはオンです。
   - **ファイルのアクセス時にスキャン**：読み取り、実行、または変更のために開いているすべてのオブジェクトがスキャンされます。
   - **実行時**：ファイルが実行のためにアクセスされた時にのみ、そのファイルがスキャンされます。
7. ［**ヒューリスティック分析を使用する**］をオフまたはオンにします。
8. ［**悪意のある活動を示すセッションのネットワーク共有リソースへのアクセスをブロックする**］をオンまたはオフにします。
9. ［**アクティブな脅威の検知時に簡易スキャンを起動する**］をオフまたはオンにします。

   このチェックボックスをオンにすると、アクティブな脅威の検知時に、Kaspersky Embedded Systems Security は*簡易スキャン*の事前定義されたタスクを実行します。既定では、このチェックボックスはオンです。
10. Windows コンテナ内で実行されるファイル操作をスキャンするための設定を指定します。
11. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでファイルのウイルススキャンを有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］に移動し、［**設定**］をクリックします。
5. ［**ファイルのリアルタイム保護を有効にする**］チェックボックスをオンにします。
6. ［**オブジェクトの保護モード**］ブロックの［**全般**］タブで、ファイルのリアルタイム保護の操作モードを選択します：

   - **スマートモード**：スキャンするオブジェクトが自動的に選択されます。開いているオブジェクトがスキャンされ、オブジェクトが変更された場合は保存された後にもう一度スキャンされます。オブジェクトがプロセスによって複数回アクセスされて変更された場合、プロセスによってオブジェクトが最後に保存された後でのみオブジェクトが再スキャンされます。
   - **アクセス時と変更時**：オブジェクトが開いている時にスキャンされ、オブジェクトが変更された場合、そのオブジェクトが保存された後で再スキャンします。既定では、このオプションはオンです。
   - **ファイルのアクセス時にスキャン**：読み取り、実行、または変更のために開いているすべてのオブジェクトがスキャンされます。
   - **実行時**：ファイルが実行のためにアクセスされた時にのみ、そのファイルがスキャンされます。
7. ［**ヒューリスティック分析を使用する**］をオフまたはオンにします。
8. ［**悪意のある活動を示すネットワークセッションのネットワーク共有リソースへのアクセスをブロックする**］をオンまたはオフにします。
9. ［**アクティブな脅威の検知時に簡易スキャンを起動する**］をオフまたはオンにします。

   このチェックボックスをオンにすると、アクティブな脅威の検知時に、Kaspersky Embedded Systems Security は*簡易スキャン*の事前定義されたタスクを実行します。既定では、このチェックボックスはオンです。
10. Windows コンテナ内で実行されるファイル操作をスキャンするための設定を指定します。
11. 変更内容を保存します。

*アプリケーションコンソールでファイルのウイルススキャンを有効にする方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］の順に選択します。
2. ［**ファイルのリアルタイム保護**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: ファイルのリアルタイム保護**］ウィンドウが表示されます。
3. ［**ファイルのリアルタイム保護**］チェックボックスをオンにします。
4. ［**オブジェクトの保護モード**］ブロックの［**全般**］タブで、ファイルのリアルタイム保護の操作モードを選択します：
   - **スマートモード**：スキャンするオブジェクトが自動的に選択されます。開いているオブジェクトがスキャンされ、オブジェクトが変更された場合は保存された後にもう一度スキャンされます。オブジェクトがプロセスによって複数回アクセスされて変更された場合、プロセスによってオブジェクトが最後に保存された後でのみオブジェクトが再スキャンされます。
   - **アクセス時と変更時**：オブジェクトが開いている時にスキャンされ、オブジェクトが変更された場合、そのオブジェクトが保存された後で再スキャンします。既定では、このオプションはオンです。
   - **ファイルのアクセス時にスキャン**：読み取り、実行、または変更のために開いているすべてのオブジェクトがスキャンされます。
   - **実行時**：ファイルが実行のためにアクセスされた時にのみ、そのファイルがスキャンされます。
5. ［**ヒューリスティック分析を使用する**］をオフまたはオンにします。
6. ［**悪意のある活動を示すセッションのネットワーク共有リソースへのアクセスをブロックする**］をオンまたはオフにします。
7. ［**アクティブな脅威の検知時に簡易スキャンを起動する**］をオフまたはオンにします。
   このチェックボックスをオンにすると、アクティブな脅威の検知時に、Kaspersky Embedded Systems Security は*簡易スキャン*の事前定義されたタスクを実行します。既定では、このチェックボックスはオンです。
8. Windows コンテナ内で実行されるファイル操作をスキャンするための設定を指定します。
9. 変更内容を保存します。

# ファイルのリアルタイム保護コンポーネントの保護範囲の設定

ファイルのリアルタイム保護のコンポーネントでは、既定で保護範囲全体の共通のセキュリティ設定が使用されます。これらの設定は、定義済みのセキュリティレベル［**推奨**］に対応します。

セキュリティ設定の既定値を編集し、保護範囲全体の共通の設定として、あるいはデバイスのファイルリソースのリストの項目ごとに異なる設定として、設定することができます。

複数の保護範囲項目に同じオブジェクトが含まれており、これらの項目のセキュリティレベルが異なる場合は、リストの最後のルールが優先されます。たとえば、**すべてのハードディスク**（セキュリティレベル：**通知**）および `*\Users\*\Downloads\*`（セキュリティレベル：**カスタム**）の 2 つの項目を含む保護範囲について考えてみましょう。本製品は、フォルダー `Downloads` を除いて、通知レベルでハードディスクをスキャンします。本製品は、手動で指定された設定に従ってフォルダー `Downloads` をスキャンします。この項目は保護範囲のリストの最後にあるためです。

選択したフォルダーのセキュリティを手動で設定するには：

**Kaspersky Security Center 管理コンソールでファイルのリアルタイム保護の保護範囲を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ファイルのリアルタイム保護**］セクションで、［**設定**］をクリックします。
5. ［**保護範囲**］タブを選択します。
6. 保護対象デバイスのファイルリソースのリストで、定義済みセキュリティレベルを設定する項目を選択します。
7. ファイル共有がリストにない場合は、手動で追加します：
   a. ［**追加**］をクリックします。
   b. フォルダーツリーを使用して必要なオブジェクトへのパスを指定するか、［**オブジェクト**］フィールドにパスを入力します。

      必要に応じて、特殊文字を使用してオブジェクトのパスのマスクを入力します：

      - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。
      - 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。
      - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

コンピューターのファイルリソースのリスト内の［**このPC**］のオブジェクトには、［**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**］、［**すべてのリムーバブルドライブ**］のオブジェクトが含まれます。

c. ［**OK**］をクリックします。

8. 選択したファイルリソースが保護範囲に含まれることを確認します。

9. ［**設定**］をクリックして、選択した保護範囲に対して、定義済みのセキュリティレベルを指定します。既定では、保護範囲全体に同じセキュリティ設定が適用されます。これらの設定は、定義済みのセキュリティレベル［**推奨**］に対応します。また、既定のセキュリティ設定を編集することもできます。

10. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでファイルのリアルタイム保護の保護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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］に移動し、［**設定**］をクリックします。

5. ［**保護範囲**］タブを選択します。

6. 保護対象デバイスのファイルリソースのリストで、定義済みセキュリティレベルを設定する項目を選択します。

7. ファイル共有がリストにない場合は、手動で追加します：

a. ［**追加**］をクリックします。

b. ［**オブジェクト種別**］リストで、オプションを選択します：

［**マスク**］で、特殊文字を使用してオブジェクトのパスのマスクを入力します：

- 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

- 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。

- 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

コンピューターのファイルリソースのリスト内の［**この PC**］のオブジェクトには、［**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**］、［**すべてのリムーバブルドライブ**］のオブジェクトが含まれます。

c. ［**OK**］をクリックします。

8. リスト項目の横にあるスイッチを使用して、選択したファイルリソースが保護範囲に含まれていることを確認します。

9. ［**編集**］をクリックして、選択した保護範囲に対して、定義済みのセキュリティレベルを指定します。既定では、保護範囲全体に同じセキュリティ設定が適用されます。これらの設定は、定義済みのセキュリティレベル［**推奨**］に対応します。また、既定のセキュリティ設定を編集することもできます。

10. 変更内容を保存します。

### *アプリケーションコンソールでファイルのリアルタイム保護の保護範囲を設定する方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］の順に選択します。

2. ［**ファイルのリアルタイム保護**］フォルダーの結果ペインで、［**保護範囲の設定**］をクリックします。
［**プロパティ: ファイルのリアルタイム保護**］ウィンドウが表示されます。

3. 保護対象デバイスのファイルリソースのリストで、定義済みセキュリティレベルを設定する項目を選択します。

4. ファイル共有がリストにない場合は、手動で追加します：

a. ［**追加**］をクリックします。

b. フォルダーツリーを使用して必要なオブジェクトへのパスを指定するか、［**オブジェクト**］フィールドにパスを入力します。

必要に応じて、特殊文字を使用してオブジェクトのパスのマスクを入力します：

- 「*」（アスタリスク）文字。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「C:**.txt」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

- 2 つの連続した「*」（アスタリスク）文字。ファイル名またはフォルダー名内の、「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「C:\Folder***.txt」は、「Folder」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「C:***.txt」というマスクの指定は無効です。

- 「?」（クエスチョンマーク）。「\」および「/」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「C:\Folder\???.txt」は、「Folder」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

コンピューターのファイルリソースのリスト内の［**この PC**］のオブジェクトには、［**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**］、［**すべてのリムーバブルドライブ**］のオブジェクトが含まれます。

c. ［**OK**］をクリックします。

5. 選択したファイルリソースが保護範囲に含まれることを確認します。

6. ［**設定**］をクリックして、選択した保護範囲に対して、定義済みのセキュリティレベルを指定します。既定では、保護範囲全体に同じセキュリティ設定が適用されます。これらの設定は、定義済みのセキュリティレベル［**推奨**］に対応します。また、既定のセキュリティ設定を編集することもできます。

7. 変更内容を保存します。

# 手動でのセキュリティの設定

コンピューターのリアルタイム保護タスクでは、既定で保護範囲全体に対して共通のセキュリティ設定が使用されます。これらの設定は、定義済みのセキュリティレベル［**推奨**］に対応します。

セキュリティ設定の既定値を編集し、保護範囲全体の共通の設定として、あるいはデバイスのファイルリソースのリストの項目やツリーのフォルダーごとに異なる設定として、設定することができます。

保護対象デバイスのファイルリソースツリーで作業する場合、選択した親フォルダーに対して行ったセキュリティ設定が、すべてのサブフォルダーに自動的に適用されます。親フォルダーのセキュリティ設定は、個別に設定されたサブフォルダーに適用されません。

**Kaspersky Security Center 管理コンソールでセキュリティを手動で設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ファイルのリアルタイム保護**］セクションで、［**設定**］をクリックします。
5. ［**ファイルのリアルタイム保護**］ウィンドウで、［**保護範囲**］タブに移動します。
6. セキュリティを設定するリソースを選択します。
7. ［**設定**］をクリックします。
8. 表示されるウィンドウで、必要なセキュリティレベルを選択し、［**設定**］をクリックします。
9. ［**全般**］タブで、次の設定を行います：
   - 保護範囲に含める必要があるオブジェクト：
     - **すべてのオブジェクト**
     - **ファイル形式によってオブジェクトをスキャン**
     - **定義データベース指定の拡張子リストによってオブジェクトをスキャン**
   - ［**最適化**］ブロックで、［**作成または変更されたファイルのみをスキャン**］をオンまたはオフにします。
   - ［**複合ファイルのスキャン**］で、スキャン範囲に含める複合オブジェクトを指定します：
     - **アーカイブをスキャン**
     - **配布パッケージをスキャン**
     - **Microsoft Office 形式のファイルをスキャン**
     - **メール形式のファイルをスキャン**
10. ［**処理**］タブで、次の設定を行います：
    - 感染したオブジェクトおよびその他の検知したオブジェクトの処理を選択します：
      - **通知する**
      - **ブロック**
      - **その他の処理を実行**
        ドロップダウンリストから処理を選択します：
        - **駆除**
        - **駆除する。駆除できない場合は削除する**
        - **削除**
        - **推奨**

- 検知されたオブジェクトの種別に応じたオブジェクトの処理を設定します：

  a. ［**選択したオブジェクト種別に操作を適用する**］をオフまたはオンにします。

  b. ［**設定**］をクリックして、検知するオブジェクトの種別を選択します。

- 修正できない複合ファイルに対する処理を設定します（［**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**］をオフまたはオンにします）。

11. ［**パフォーマンス**］タブで、次の設定を行います：

- **次のサイズを超える複合ファイルをバックグラウンドで解凍する（MB）**
- **スキャン時間が次を超えたら停止する（秒）**
- **スキャンする複合オブジェクトの最大サイズ（MB）**
- **iSwift を使用する**
- **iChecker を使用する**

12. 新しいセキュリティ設定を保存します。

### Kaspersky Security Center Web コンソールでセキュリティを手動で設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］に移動し、［**設定**］をクリックします。
5. ［**保護範囲**］タブを選択します。
6. 次のいずれかを行います：

   - ［**追加**］をクリックして新しいルールを追加し、そのセキュリティ設定を指定します。
   - 既存のルールを選択し、［**編集**］をクリックします。

   ［**範囲を編集**］ウィンドウが表示されます。

7. スイッチを［**有効**］に設定します。
8. セキュリティレベルを選択して、必要に応じてセキュリティ設定を指定します。

9. ［**オブジェクトの保護モード**］セクションで、保護範囲に含めるオブジェクトの種別を選択します：

   - **すべてのオブジェクト**
   - **ファイル形式によってオブジェクトをスキャン**
   - **定義データベース指定の拡張子リストによってオブジェクトをスキャン**

10. ［**最適化**］セクションで、［**作成または変更されたファイルのみを保護**］をオンまたはオフにします。

11. ［**複合オブジェクトの保護**］で、スキャン範囲に含める複合オブジェクトを指定します：

    - **アーカイブをスキャン**
    - **配布パッケージをスキャン**
    - **Microsoft Office 形式のファイルをスキャン**
    - **メール形式のファイルをスキャン**

12. 感染したオブジェクトおよびその他の検知したオブジェクトの処理を選択します：

    - **通知**
    - **ブロック**
    - **その他の処理を実行**

      ドロップダウンリストから処理を選択します：

      - **駆除**
      - **駆除する。駆除できない場合は削除する**
      - **削除**
      - **推奨**

13. 検知されたオブジェクトの種別に応じたオブジェクトの処理を設定します：

    a. ［**選択したオブジェクト種別に操作を適用する**］をオフまたはオンにします。

    b. このチェックボックスをオンにした場合は、［**設定**］をクリックして、検知するオブジェクトの種別を選択します。

14. 修正できない複合ファイルに対する処理を設定します（［**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**］をオフまたはオンにします）。

15. ［**最適化**］セクションで、次の設定を行います：

    - **複合ファイルをバックグラウンドで展開する**
    - **スキャン時間が次を超えたら停止する（秒）**
    - **スキャンする複合オブジェクトの最大サイズ（MB）**

- iSwift を使用する
- iChecker を使用する

16. 新しいセキュリティ設定を保存します。

*アプリケーションコンソールでセキュリティを手動で設定する方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］の順に選択します。
2. ［**ファイルのリアルタイム保護**］フォルダーの結果ペインで、［**保護範囲の設定**］をクリックします。［**プロパティ: ファイルのリアルタイム保護**］ウィンドウが表示されます。
3. セキュリティを設定するリソースを選択します。
4. ［**設定**］をクリックします。
5. 表示されるウィンドウで、必要なセキュリティレベルを選択し、［**設定**］をクリックします。
6. ［**全般**］タブで、次の設定を行います：
   - 保護範囲に含める必要があるオブジェクト：
     - **すべてのオブジェクト**：すべてのオブジェクトがスキャンされます。
     - **ファイル形式によってオブジェクトをスキャン**：ファイル形式に基づいて、感染の可能性があるオブジェクトのみがスキャンされます。形式のリストがコンパイルされます。リストは、Kaspersky Embedded Systems Security の定義データベースに含まれています。
     - **定義データベース指定の拡張子リストによってオブジェクトをスキャン**：ファイル拡張子に基づいて、感染の可能性があるオブジェクトのみがスキャンされます。拡張子のリストがコンパイルされます。リストは、Kaspersky Embedded Systems Security の定義データベースに含まれています。
   - ［**最適化**］ブロックで、［作成または変更されたファイルのみを保護］をオンまたはオフにします。
   - ［**複合ファイルのスキャン**］で、スキャン範囲に含める複合オブジェクトを指定します：
     - **アーカイブをスキャン**：ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE またその他の圧縮形式をスキャンします。本製品は拡張子だけでなく、形式でもスキャンします。アーカイブのチェック中、本製品は再帰的に解凍処理を実行します。これにより、複数レベルにわたるアーカイブ（アーカイブ内のアーカイブ）の脅威を検知できます。
     - **配布パッケージをスキャン**：このチェックボックスでは、サードパーティの配布パッケージのスキャンを有効または無効にします。

- **Microsoft Office 形式の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。チェックボックスのオンオフにかかわらず、Kaspersky Embedded Systems Security は 1 MB より小さいサイズの Office 形式のファイルをスキャンします。

- **メール形式のファイルをスキャン**

7. ［**処理**］タブで、次の設定を行います：

   - 感染したオブジェクトおよびその他の検知したオブジェクトの処理を選択します：

     - **通知する**
     - **ブロック**
     - **その他の処理を実行**
       ドロップダウンリストから処理を選択します：

       - **駆除**
       - **駆除する。駆除できない場合は削除する**
       - **削除**
       - **推奨**

   - 検知されたオブジェクトの種別に応じたオブジェクトの処理を設定します：

     a. ［**選択したオブジェクト種別に操作を適用する**］をオフまたはオンにします。

     b. ［**設定**］をクリックして、検知するオブジェクトの種別を選択します。

   - 修正できない複合ファイルに対する処理を設定します（［**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**］をオフまたはオンにします）。

8. ［**パフォーマンス**］タブで、次の設定を行います：

   - **次のサイズを超える複合ファイルをバックグラウンドで解凍する（MB）**
   - **スキャン時間が次を超えたら停止する（秒）**
   - **スキャンする複合オブジェクトの最大サイズ（MB）**
   - **iSwift を使用する**
   - **iChecker を使用する**

9. 新しいセキュリティ設定を保存します。

# コンテナーのスキャン

コンテナーは、アプリケーションがオペレーティングシステムと直接やり取りすることなく実行できる分離された環境です。コンテナーを使用すると、次のようなリスクが伴います：

- ハッカーがコンテナー化の脆弱性を悪用して、コンテナー内のアプリケーションを侵害する可能性があります。
- ハッカーがコンテナー環境の安全でない設定を悪用して、コンピューター上のデータに不正にアクセスしたり、システムの整合性を侵害したりする可能性があります。
- コンテナーへの攻撃が成功すると、ハッカーがコンピューター上のデータにアクセスできるようになる可能性があります。
- ハッカーがネットワークの脆弱性を悪用してネットワークトラフィックを傍受する可能性があります。

Kaspersky Embedded Systems Security は、コンテナー内の悪意のあるアクティビティを検知するための外部ツールです。これにより、コンテナーのパフォーマンスを維持し、コンテナー内の他のアプリケーションとの競合を防ぐことができます。コンテナー内への Kaspersky Embedded Systems Security のインストールはサポートされていません。

Kaspersky Embedded Systems Security は、コンテナーのセキュリティの確保に加え、アプリケーション起動コントロールを使用したコンテナー内のアプリケーションの管理を可能にします。アプリケーション起動コントロールは、コンピューターにインストールされたアプリケーションと同じ方法でコンテナー用に設定されます。システム変更監視でもコンテナがサポートされます。

## コンテナーの要件

- コンテナーは Docker コンテナーである必要があります。その他のコンテナー化ツールはサポートされていません。
- コンテナーはプロセス分離モードで実行する必要があります。Hyper-V 分離モードはサポートされていません。
- コンテナーは、Windows Server 2016、2019、2022 サーバーのいずれかに配置する必要があります（Docker Host）。
- コンテナーには Windows イメージ（Docker Image）が含まれる必要があります。Windows 10 および 11 はサポートされていません。Linux イメージはサポートされていません。
- WSL2 モードで実行されているコンテナのスキャン - Windows Subsystem for Linux v2（Docker Wine）モードはサポートされていません。

## 脅威の検知時の処理

コンテナ内で脅威が検知された場合、ファイルのリアルタイム保護に対して選択された処理が適用されます。コンテナのスキャンには追加の設定があります（以下の手順を参照）。脅威が検知されると、悪意のある動作がブロックされて、選択した処理が実行されます（オブジェクト駆除の試行など）。Kaspersky Embedded Systems Security は、検知されたオブジェクトを駆除できない場合に、コンテナを停止できます。既定では、コンテナの停止は有効になっています。

### Kaspersky Security Center 管理コンソールでコンテナーのスキャンを設定する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ファイルのリアルタイム保護**］セクションで、［**設定**］をクリックします。
5. ［**Windows コンテナー内で実行されたファイル操作のスキャン**］ブロックで、コンテナーのスキャンを設定します：
   - **駆除できない場合はコンテナーを停止する**：本製品に、検知したオブジェクトに対する読み取りおよび書き込み権限がない可能性があります。この場合、検知したオブジェクトを駆除することも削除することもできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。
   - **Windows コンテナー内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナをリアルタイムで継続的にスキャンします。
6. 新しいセキュリティ設定を保存します。

### Kaspersky Security Center Web コンソールでコンテナーの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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］に移動し、［**設定**］をクリックします。

5. ［**Windows コンテナー内で実行されたファイル操作のスキャン**］ブロックで、コンテナーのスキャンを設定します：

   - **駆除できない場合はコンテナーを停止する**：本製品に、検知したオブジェクトに対する読み取りおよび書き込み権限がない可能性があります。この場合、検知したオブジェクトを駆除することも削除することもできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。

   - **Windows コンテナー内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナをリアルタイムで継続的にスキャンします。

6. 新しいセキュリティ設定を保存します。

***アプリケーションコンソールでコンテナーのスキャンを設定する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ファイルのリアルタイム保護**］の順に選択します。

2. ［**ファイルのリアルタイム保護**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: ファイルのリアルタイム保護**］ウィンドウが表示されます。

3. ［**Windows コンテナー内で実行されたファイル操作のスキャン**］ブロックで、コンテナーのスキャンを設定します：

   - **駆除できない場合はコンテナーを停止する**：本製品に、検知したオブジェクトに対する読み取りおよび書き込み権限がない可能性があります。この場合、検知したオブジェクトを駆除することも削除することもできません。このチェックボックスをオンにすると、本製品は検知したオブジェクトをブロックし、コンテナを停止します。このチェックボックスをオフにすると、本製品は検知したオブジェクトのブロックのみを行います。

   - **Windows コンテナー内で実行されたファイル操作をスキャンしない**：このチェックボックスをオンにすると、本製品はコンテナの起動時にのみコンテナをスキャンします。チェックボックスをオフにすると、本製品はコンテナをリアルタイムで継続的にスキャンします。

4. 変更内容を保存します。

# KSN の使用

コンピューターをより効果的に保護するために、Kaspersky Embedded Systems 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、アメリカ合衆国内にある本製品ではご利用いただけなくなる可能性があります。

*KSN（Kaspersky Security Network）*はクラウドサービスの基盤であり、ファイル、Web リソース、ソフトウェアの評価に関する情報を含む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 Kaspersky Embedded Systems Security 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。Kaspersky Security Network に参加すると、KSN サービスから Kaspersky Embedded Systems Security にスキャンしたファイルのカテゴリと評価に関する情報およびスキャンした Web アドレスの評価に関する情報を取得できます。

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。KSN への参加はいつでも開始または中止できます。

KSN に参加している間に生成されたカスペルスキー統計情報の送信や、そのような情報の保存と破棄について詳しくは、KSN 声明およびカスペルスキーの Web サイトを参照してください。Kaspersky Security Network 声明のテキストが含まれたファイル ksn_<言語 ID>.txt は製品配信キットに含まれています。

## カスペルスキーの評価データベースのインフラストラクチャ

Kaspersky Embedded Systems Security は、カスペルスキーの評価データベースと連携する、次のインフラストラクチャソリューションをサポートします：

- 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 Embedded Systems 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。

  - 国外へのデータの送信が法律などにより規制されていたり、社内のセキュリティポリシーでローカルエリアネットワーク外へのデータの送信が禁止されている。

# Kaspersky Security Network の使用の有効化

### Kaspersky Security Center 管理コンソールで Kaspersky Security Network の使用を有効にする方法

1. Kaspersky Security Network 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. Kaspersky Embedded Systems Security の目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ウィンドウが表示されるので、そのウィンドウのセクションのリストで、［**コンピューターのリアルタイム保護**］→［**KSN の使用**］の順に選択します。
4. ［**設定**］をクリックします。
5. ［**Kaspersky Security Network**］をオンにして、コンポーネントを有効にします。

   KSN の使用を有効にすると、Kaspersky Embedded Systems Security に、Kaspersky Security Network に関する声明が表示されます。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。

   既定では、Kaspersky Embedded Systems Security は Kaspersky Security Network の拡張モードを使用します。Kaspersky Security Network の拡張モードは、カスペルスキーに詳細なデータを送信するモードです。
6. 必要に応じて、［**拡張 KSN モードを有効にする**］をオフにします。
7. 変更内容を保存します。

Kaspersky Security Network の使用を有効にすると、Kaspersky Embedded Systems 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 Embedded Systems Security コンソールで Kaspersky Security Network の使用を有効にする方法*

1. アプリケーションコンソールツリーで、［**コンピューターのリアルタイム保護**］フォルダーを展開します。
2. ［**Kaspersky Security Network**］サブフォルダーを選択します。
3. 製品のメインウィンドウで、［**プロパティ**］をクリックします。
4. ［**Kaspersky Security Network**］をオンにして、コンポーネントを有効にします。

   KSN の使用を有効にすると、Kaspersky Embedded Systems Security に、Kaspersky Security Network に関する声明が表示されます。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。

   既定では、Kaspersky Embedded Systems Security は Kaspersky Security Network の拡張モードを使用します。Kaspersky Security Network の拡張モードは、カスペルスキーに詳細なデータを送信するモードです。

5. 必要に応じて、［**拡張 KSN モードを有効にする**］をオフにします。

6. 変更内容を保存します。

Kaspersky Security Network の使用を有効にすると、Kaspersky Embedded Systems 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 Security Center Web コンソールで Kaspersky Security Network 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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**KSN の使用**］セクションに移動し、［**設定**］をクリックします。

5. 表示されたウィンドウで、［**Kaspersky Security Network を有効にする**］をオンにして、コンポーネントを有効にします。

   KSN の使用を有効にすると、Kaspersky Embedded Systems Security に、Kaspersky Security Network に関する声明が表示されます。同意する場合は、Kaspersky Security Network の利用規約に同意します。

   既定では、Kaspersky Embedded Systems Security は Kaspersky Security Network の拡張モードを使用します。Kaspersky Security Network の拡張モードは、カスペルスキーに詳細なデータを送信するモードです。

6. 必要に応じて、［**拡張 KSN モードを有効にする**］をオフにします。

7. 変更内容を保存します。

Kaspersky Security Network の使用を有効にすると、Kaspersky Embedded Systems 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 Security Network の使用統計情報

*KSN の使用*タスクの実行中は、タスクが開始されてから現在までに Kaspersky Embedded Systems Security によって処理されたオブジェクトの数に関するリアルタイムの情報を確認できます。

*KSN の使用の統計情報を表示するには：*

1. コンソールツリーで、［**コンピューターのリアルタイム保護**］セクションを選択します。

2. ［**Kaspersky Security Network**］サブフォルダーを選択します。

   結果ペインの［**統計情報**］セクションでは、タスクの統計が表示されます（下の表を参照）。

| フィールド | 説明 |
| --- | --- |
| **送信されたファイル要求** | Kaspersky Embedded Systems Security から KSN に送信されたオブジェクト評価クエリの数。 |
| **KSN で信頼されていないファイル** | KSN によって信頼できない評価が割り当てられたオブジェクトの数。 |
| **要求送信エラー** | エラーで処理された KSN へのリクエストの数。 |
| **作成された統計** | KSN に送信された生成済み統計パッケージの数。 |
| **削除されたオブジェクト** | Kaspersky Embedded Systems Security によって正常に削除されたオブジェクトの数。 |
| **削除されていないオブジェクト** | 削除しようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由で削除できなかったオブジェクトの数。 |
| **バックアップに移動されました** | Kaspersky Embedded Systems Security によって正常にバックアップにコピーされたオブジェクトの数。 |
| **バックアップに移動されなかったオブジェクト** | ディスク容量不足などによりバックアップにコピーできなかったオブジェクトの数。バックアップに移動できないファイルは駆除または削除されません。 |
| **制限モード** | このステータスは、制限モードでファイル評価要求を送信するかどうかを示します。制限モードでは、カスペルスキーの推奨に従ってファイル評価の要求の一部のみが送信されます。 |

［**削除されたオブジェクト**］、［**削除されていないオブジェクト**］、［**バックアップに移動されました**］、［**バックアップに移動されなかったオブジェクト**］フィールドの値は、ファイルのリアルタイム保護コンポーネントの統計情報から生成されます。

# Kaspersky Private Security Network

*Kaspersky Private Security Network (KPSN)* は、Kaspersky Embedded Systems 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。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 Embedded Systems 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「*許可*」という評価があった場合、Kaspersky Embedded Systems 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 Embedded Systems 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 Embedded Systems 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 Embedded Systems 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。

- 製品が iSwift または iChecker などのスキャンの最適化技術を使用している、または KSN / KPSN への評価の要求をキャッシュしている場合。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。

# KSN プロキシ設定

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、KSN プロキシサービス経由で KSN と連携できます。

KSN プロキシサービスは次の機能を提供します：

- クライアントコンピューターはインターネットに直接アクセスしなくても、KSN にクエリを実行し、情報を送信できます。

- KSN プロキシ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。したがって、KSN プロキシが使用できない場合は、KSN プロキシサーバーとしてのデバイスの動作を確認する必要があります。以下の点を確認する必要があります：

- 管理サーバーで *ksnproxy* サービスが実行されている。

- コンピューターのファイアウォールがポート 13111 をブロックしていない。

KSN プロキシの使用は、KSN プロキシを有効または無効にする、また接続のポートを設定することで設定することができます。設定するためには管理サーバーのプロパティを表示する必要があります。KSN プロキシの設定について詳しくは、Kaspersky Security Center のオンラインヘルプを参照してください。Kaspersky Embedded Systems Security のポリシーで個別のコンピューターに対して KSN プロキシを有効または無効にすることも可能です。

**Kaspersky Security Center 管理コンソールで KSN プロキシを有効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. Kaspersky Embedded Systems Security の目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ウィンドウが表示されるので、そのウィンドウのセクションのリストで、［**コンピューターのリアルタイム保護**］→［**KSN の使用**］の順に選択します。
4. ［**設定**］をクリックします。
5. ［**KSN プロキシ設定**］ブロックで、［**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**］をオンにします。

   このチェックボックスをオンにすると、KSN プロキシサービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合と、サードパーティ側に配置されている場合（Kaspersky Private Security Network を使用している時）があります。

7. 変更内容を保存します。

*Kaspersky Embedded Systems Security コンソールで KSN プロキシを有効にする方法*

1. アプリケーションコンソールツリーで、［**コンピューターのリアルタイム保護**］フォルダーを展開します。
2. ［**Kaspersky Security Network**］サブフォルダーを選択します。
3. 製品のメインウィンドウで、［**プロパティ**］をクリックします。
4. ［**KSN プロキシ設定**］ブロックで、［**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 プロキシを有効または無効にします。
5. 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**］をオンにします。

   このチェックボックスをオンにすると、KSN プロキシサービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合と、サードパーティ側に配置されている場合（Kaspersky Private Security Network を使用している時）があります。

6. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで KSN プロキシを有効にする方法**

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**KSN の使用**］に移動し、［**設定**］をクリックします。
5. ［**管理サーバーを KSN プロキシサーバーとして使用する**］をオンまたはオフにして、KSN プロキシ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**］をオンにします。

   このチェックボックスをオンにすると、KSN プロキシサービスが使用できない場合は、KSN サーバーが使用されます。KSN サーバーは、カスペルスキー側に配置されている場合と、サードパーティ側に配置されている場合（Kaspersky Private Security Network を使用している時）があります。

7. 変更内容を保存します。

KSN プロキシのアドレスが管理サーバーのアドレスと一致します。管理サーバーのドメイン名が変更された場合は、KSN プロキシアドレスを手動で更新する必要があります。

# 脆弱性攻撃ブロック

Kaspersky Embedded Systems Security には、プロセスメモリを脆弱性攻撃から保護する機能があります。この機能は、脆弱性攻撃ブロックコンポーネントによって実装されます。このコンポーネントを使用してコンポーネントの動作のステータスを変更し、脆弱性攻撃からのプロセスの保護を設定することができます。

脆弱性攻撃ブロックは、コンピューター上の脆弱性を悪用して管理者権限を取得したり悪意のある活動を実行しようとするプログラムコードを検知します。たとえば、脆弱性を悪用した攻撃の例としては、バッファーオーバーフロー攻撃などがあります。この攻撃では、脆弱性のあるアプリケーションに大量のデータが送信され、このデータの処理中に、悪意のあるコードが脆弱性のあるアプリケーションによって実行されてしまいます。この攻撃により、不正にマルウェアをインストールされてしまう可能性があります。ユーザー以外の第三者が、脆弱性のあるアプリケーションから実行ファイルを実行しようとすると、Kaspersky Embedded Systems Security は、このファイルの起動をブロックしてユーザーに通知します。保護対象プロセスに外部のプロセス保護エージェント（「保護エージェント」）を挿入することによって、プロセスメモリを脆弱性攻撃から保護します。

プロセス保護エージェントは動的にロードされて保護対象プロセスに挿入される Kaspersky Embedded Systems Security モジュールで、整合性を監視し、脆弱性を攻撃されるリスクを軽減できます。

保護対象プロセス内のエージェントの操作には、プロセスの開始と停止が必要です。保護対象プロセスリストに追加されたプロセスへのエージェントの初期ロードは、プロセスが再起動された場合のみ可能です。また、プロセスが保護対象プロセスリストから削除された後にエージェントをアンロードできるのは、プロセスの再起動後のみです。

エージェントを保護対象プロセスからアンロードするには、停止する必要があります。脆弱性攻撃ブロックをアンインストールすると、環境がフリーズさせられ、エージェントが保護対象プロセスから強制的にアンロードされます。コンポーネントのアンインストール中に保護対象プロセスのいずれかにエージェントが挿入された場合、影響を受けるプロセスを終了する必要があります。保護対象デバイスの再起動が必要になることがあります（システムプロセスが保護されている場合など）。

保護対象プロセスに脆弱性攻撃の証拠が検知されると、Kaspersky Embedded Systems Security は次の処理のいずれかを実行します：

- 脆弱性攻撃が試行された場合、プロセスを終了する。
- プロセスが危険にさらされている事実を報告する。

次の方法のいずれかを使用してプロセス保護を停止できます：

- コンポーネントのアンインストール。
- 保護対象プロセスのリストからプロセスを削除して、プロセスを再起動。

# 脆弱性攻撃ブロックモード

次のモードのいずれかを選択して、保護対象プロセスの脆弱性が攻撃されるリスクを軽減するために行う処理を設定できます：

- **ブロックする**：このモードを選択すると、アクティブな脆弱性攻撃による被害の軽減技術がプロセスに適用されている場合、脆弱性攻撃試行を検知すると保護対象プロセスが終了します。

  保護されている重要なオペレーティングシステムプロセスの脆弱性に対する攻撃試行を検知した場合、脆弱性攻撃ブロック設定に示されたモードに関係なく、Kaspersky Embedded Systems Security はプロセスを終了しません。

- **通知する**（Kaspersky Security Center Web コンソールで作業する場合は、**通知する**）：このモードを適用すると、セキュリティログのイベントを使用して保護対象プロセスにおける脆弱性攻撃インスタンスに関する情報を受信します。脆弱性攻撃を受けたプロセスが実行され続けます。

  このモードを選択すると、Kaspersky Embedded Systems Security は脆弱性を攻撃するすべての試行を記録するイベントを作成します。既定で選択されています。

# 脆弱性攻撃ブロックの有効化と無効化

Kaspersky Embedded Systems Security では、脆弱性があるアプリケーションによって実行される実行ファイルを監視できます。Kaspersky Embedded Systems Security は、脆弱性があるアプリケーションの実行ファイルが、そのユーザー以外によって使用されていることを検知した場合、操作をブロックするなど、選択されている処理を行います。

**Kaspersky Security Center 管理コンソールで脆弱性攻撃ブロックを有効または無効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. Kaspersky Embedded Systems Security の目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ウィンドウが表示されるので、そのウィンドウのセクションのリストで、［**コンピューターのリアルタイム保護**］→［**脆弱性攻撃ブロック**］の順に選択します。
4. ［**設定**］をクリックします。
5. ［**脆弱性攻撃ブロック**］をオンにして、コンポーネントを有効にします。
6. ［**全般**］タブで、脆弱性攻撃ブロックモード（［**ブロックする**］または［**通知する**］）を選択します。
7. 必要に応じて、［**脆弱性攻撃ブロック**］をオフにして、コンポーネントを無効にします。
8. 変更内容を保存します。

*Kaspersky Embedded Systems Security コンソールで脆弱性攻撃ブロックを有効または無効にする方法*

1. アプリケーションコンソールツリーで、［**コンピューターのリアルタイム保護**］フォルダーを展開します。
2. ［**脆弱性攻撃ブロック**］サブフォルダーを選択します。
3. 製品のメインウィンドウで、［**プロパティ**］をクリックします。
4. ［**脆弱性攻撃ブロック**］をオンにして、コンポーネントを有効にします。
5. ［**全般**］タブで、脆弱性攻撃ブロックモード（［**ブロックする**］または［**通知する**］）を選択します。
6. 必要に応じて、［**脆弱性攻撃ブロック**］をオフにして、コンポーネントを無効にします。
7. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで脆弱性攻撃ブロック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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**脆弱性攻撃ブロック**］に移動し、［**設定**］をクリックします。
5. ウィンドウが表示されるので、そのウィンドウの［**脆弱性攻撃ブロックモード**］で、［**脆弱なプロセスに対する攻撃から防御する**］をオンにして、コンポーネントを有効にします。
6. 脆弱性攻撃ブロックモード（［**ブロックする**］または［**通知する**］）を選択します。
7. 必要に応じて、［**脆弱なプロセスに対する攻撃から防御する**］をオフにして、コンポーネントを無効にします。
8. 変更内容を保存します。

# メモリ保護の有効化と無効化

Kaspersky Embedded Systems Security は、システムプロセスへのアクセスを取得しようとする外部プロセスをブロックします。既定では、システムプロセスのメモリ保護は有効です。

### Kaspersky Security Center 管理コンソールでメモリ保護を有効または無効にする方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. Kaspersky Embedded Systems Security の目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ウィンドウが表示されるので、そのウィンドウのセクションのリストで、［**コンピューターのリアルタイム保護**］→［**脆弱性攻撃ブロック**］の順に選択します。
4. ［**設定**］をクリックします。
5. ［**全般**］タブで、［**システムプロセスのメモリ保護を有効にする**］をオンにします。
6. 必要に応じて、［**システムプロセスのメモリ保護を有効にする**］をオフにします。
7. 変更内容を保存します。

*Kaspersky Embedded Systems Security コンソールでメモリ保護を有効または無効にする方法*

1. アプリケーションコンソールツリーで、［**コンピューターのリアルタイム保護**］フォルダーを展開します。
2. ［**脆弱性攻撃ブロック**］サブフォルダーを選択します。
3. 製品のメインウィンドウで、［**プロパティ**］をクリックします。
4. ［**全般**］タブで、［**システムプロセスのメモリ保護を有効にする**］をオンにします。
5. 必要に応じて、［**システムプロセスのメモリ保護を有効にする**］をオフにします。
6. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでメモリ保護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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**脆弱性攻撃ブロック**］に移動し、［**設定**］をクリックします。
5. 開いたウィンドウの［**システムプロセスのメモリ保護**］ブロックで、［**システムプロセスのメモリ保護**］をオンにします。

6. 必要に応じて、［**システムプロセスのメモリ保護**］をオフにして、システムプロセスのメモリ保護を無効にします。

7. 変更内容を保存します。

# 保護対象プロセスのリストの作成

既定では、脆弱性攻撃ブロックコンポーネントは複数のプロセスを保護します。本製品では、保護対象プロセスのリストを自動的に生成することができます。プロセスを手動で追加または削除することもできます。

**Kaspersky Security Center 管理コンソールで保護対象プロセスのリストを管理する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。

2. Kaspersky Embedded Systems Security の目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ウィンドウが表示されるので、そのウィンドウのセクションのリストで、［**コンピューターのリアルタイム保護**］→［**脆弱性攻撃ブロック**］の順に選択します。

4. ［**設定**］をクリックします。

5. ［**保護対象プロセス**］タブで、悪意のあるコードの埋め込みからプロセスを保護するための次のいずれかのオプションをオンにします：

   - **保護対象プロセスを自動的に検出する**：このオプションをオンにすると、保護対象プロセスのリストが自動的に作成されます。

   - **下のリストのプロセスのみ保護する**：このオプションをオンにすると、保護するプロセスを選択できます。

6. ［**下のリストのプロセスのみ保護する**］をオンにした場合は、次のいずれかの方法で、保護対象プロセスのリストを編集できます：

   - 必要に応じて、［**追加**］をクリックして、保護対象プロセスのリストに追加するプロセスを選択します。

   - 保護対象プロセスの作成されたリストからプロセスを削除する場合は、リストからプロセスを選択して、［**削除**］をクリックします。

     リスト内の 1 つ以上のプロセスを選択すると、［**削除**］が使用可能になります。

7. 変更内容を保存します。

*Kaspersky Embedded Systems Security コンソールで保護対象プロセスのリストを管理する方法*

1. アプリケーションコンソールツリーで、［**コンピューターのリアルタイム保護**］フォルダーを展開します。
2. ［**脆弱性攻撃ブロック**］サブフォルダーを選択します。
3. 製品のメインウィンドウで、［**プロパティ**］をクリックします。
4. ［**保護対象プロセス**］タブで、悪意のあるコードの埋め込みからプロセスを保護するための次のいずれかのオプションをオンにします：
   - **保護対象プロセスを自動的に検出する**：このオプションをオンにすると、保護対象プロセスのリストが自動的に作成されます。
   - **下のリストのプロセスのみ保護する**：このオプションをオンにすると、保護するプロセスを選択できます。
5. ［**下のリストのプロセスのみ保護する**］をオンにした場合は、次のいずれかの方法で、保護対象プロセスのリストを編集できます：
   - 必要に応じて、［**追加**］をクリックして、保護対象プロセスのリストに追加するプロセスを選択します。
   - 保護対象プロセスの作成されたリストからプロセスを削除する場合は、リストからプロセスを選択して、［**削除**］をクリックします。

     リスト内の1つ以上のプロセスを選択すると、［**削除**］が使用可能になります。
6. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで保護対象プロセスのリストを管理する方法**

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**脆弱性攻撃ブロック**］セクションに移動し、［**設定**］をクリックします。
5. ［**保護対象プロセスのリスト**］で、悪意のあるコードの埋め込みからプロセスを保護するための次のいずれかのオプションをオンにします：
   - **保護対象プロセスを自動的に検出する**：このオプションをオンにすると、保護対象プロセスのリストが自動的に作成されます。
   - **下のリストのプロセスのみ保護する**：このオプションをオンにすると、保護するプロセスを追加、編集、削除できます。

6. ［**下のリストのプロセスのみ保護する**］をオンにした場合は、次のいずれかを実行します：

   - ［**追加**］をクリックして［**保護されているプロセス**］ウィンドウを開き、そのウィンドウで次の操作を実行します：

     a. ［**保護されているプロセス**］チェックボックスをオンにします。

     b. ［**プロセス名**］にプロセス名を入力します。

     c. 変更内容を保存します。

   - 必要に応じて、保護対象プロセスのリストでプロセスの設定を編集します。それには、次の操作を実行します：

     a. 保護対象プロセスのリストにプロセスを選択します。

     b. ［**編集**］をクリックします。リスト内の1つ以上のプロセスを選択すると、［**編集**］が使用可能になります。

     c. ［**保護されているプロセス**］ウィンドウで、［**保護されているプロセス**］をオンまたはオフにします。

     d. 必要に応じて、［**プロセス名**］フィールドでプロセスの名前を編集します。

     e. 変更内容を保存します。

   - 必要に応じて、保護対象プロセスのリストからプロセスを削除できます。それには、次の操作を実行します：

     a. 保護対象プロセスのリストで1つ以上のプロセスを選択します。

     b. ［**削除**］をクリックします。リスト内の1つ以上のプロセスを選択すると、［**削除**］が使用可能になります。

7. 変更内容を保存します。

# 修復エンジン

修復エンジンを使ってマルウェアがオペレーティングシステム内で行った動作をロールバックできます。

マルウェアがオペレーティングシステム内で行った動作をロールバックする際に、次の処理を実行します：

- **ファイルの動作**
  - マルウェアによって作成された実行ファイルを削除します（ネットワークドライブ以外のすべてのメディア上の実行ファイルが対象）。
  - マルウェアが侵入したプログラムによって作成された実行ファイルを削除します。
  - マルウェアによって変更または削除されたファイルを復元します。

  ファイルの修復機能には**いくつかの制限事項**があります。

  - 本製品では、NTFS ファイルシステムまたは FAT32 ファイルシステムを使用しているデバイス上のファイルのみを修復できます。
  - 本製品を使用して次の拡張子のファイルを修復できます：ods、odp、odm、odc、odb、doc、docx、docm、wps、xls、xlsx、xlsm、xlsb、xlk、ppt、pptx、pptm、mdb、accdb、pst、dwg、dxf、dxg、wpd、rtf、wb2、pdf、mdf、dbf、psd、pdd、eps、ai、indd、cdr、jpg、jpe、dng、3fr、arw、srf、sr2、bay、crw、cr2、dcr、kdc、erf、mef、mrw、nef、nrw、orf、raf、raw、rwl、rw2、r3d、ptx、pef、srw、x3f、der、cer、crt、pem、pfx、p12、p7b、p7c、1cd。
  - ネットワークドライブまたは再書き込み可能な CD / DVD 上に保存されているファイルは修復できません。
  - 暗号化ファイルシステム（EFS）を使用して暗号化されたファイルは修復できません。EFS の動作について詳しくは、Microsoft の Web サイトの情報を参照してください。
  - 本製品では、オペレーティングシステムのカーネルレベルのプロセスで実行されたファイル変更は監視されません。
  - 本製品では、ネットワークインターフェイスを経由して行われたファイル変更は監視されません（例：ファイルが共有フォルダーに保存されていて、プロセスが別のコンピューターからリモートで起動された場合など）。

- **レジストリの動作**
  - マルウェアによって作成されたレジストリキーを削除します。

  マルウェアによって変更または削除されたレジストリキーは復元されません。

- **システムの動作**
  - マルウェアによって開始されたプロセスを終了します。
  - 悪意のあるアプリケーションによって侵入されたプロセスを終了します。

マルウェアによって停止されたプロセスは再開しません。

- **ネットワークの動作**
  - マルウェアによるネットワーク動作をブロックします。
  - マルウェアが侵入したプロセスによるネットワーク動作をブロックします。

悪意のあるアプリケーションの処理のロールバックは、ファイルのリアルタイム保護コンポーネントによって、またはオンデマンドスキャン中に開始できます。

マルウェアの動作をロールバックすると、厳密に定義されたデータセットに影響を与えます。ロールバックは、オペレーティングシステムやコンピューターデータの整合性に悪影響を与えません。

### Kaspersky Security Center 管理コンソールで修復エンジンを有効または無効にする方法

1. **設定するポリシーの修復エンジンコンポーネントの設定を開きます**。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**ポリシー**］タブを選択します。

   d. ポリシー名をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

   e. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］をクリックします。

   f. ［**修復エンジン**］ブロックの［**設定**］をクリックします。
   ［**修復エンジン**］ウィンドウが開き、［**全般**］タブが表示されます。

2. 次のいずれかを行います：
   - 修復エンジンコンポーネントを有効にする場合は、［**修復エンジン**］をオンにします。
   - 修復エンジンコンポーネントを無効にする場合は、［**修復エンジン**］をオフにします。
3. ［**修復エンジン**］ウィンドウの［OK］をクリックします。
4. **プロパティ：<ポリシー名>**ウィンドウで、［OK］をクリックします。

*Kaspersky Embedded Systems Security コンソールで修復エンジンを有効または無効にする方法*

1. コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**修復エンジン**］セクションを選択します。
2. 結果ペインで［**プロパティ**］をクリックします。
   ［**修復エンジン**］ウィンドウが開き、［**全般**］タブが表示されます。
3. 次のいずれかを行います：
   - 修復エンジンコンポーネントを有効にする場合は、［**修復エンジン**］をオンにします。
   - 修復エンジンコンポーネントを無効にする場合は、［**修復エンジン**］をオフにします。
4. ［**修復エンジン**］ウィンドウの［**OK**］をクリックします。

**Kaspersky Security Center Web コンソールで修復エンジンを有効または無効にする方法**

1. **設定するポリシーの修復エンジンコンポーネントの設定を開きます**。
   a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
   b. Kaspersky Embedded Systems 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。
   c. ［**アプリケーション設定**］タブを選択します。
   d. ［**コンピューターのリアルタイム保護**］セクションを選択します。
   e. ［**修復エンジン**］ブロックの［**設定**］をクリックします。
      ［**修復エンジン**］ウィンドウが表示されます。
2. 次のいずれかを行います：
   - 修復エンジンコンポーネントを有効にする場合は、［**修復エンジン**］をオンにします。
   - 修復エンジンコンポーネントを無効にする場合は、［**修復エンジン**］をオフにします。
3. ［**修復エンジン**］ウィンドウの［**OK**］をクリックします。
4. ［**<ポリシー名>**］ウィンドウで、［**保存**］をクリックします。

# ふるまい検知

ふるまい検知は、コンピューター上でのアプリケーションの処理に関するデータを取得し、別のコンポーネントのパフォーマンスを向上するために、その情報を提供します。ふるまい検知は、アプリケーションの Behavior Stream Signatures（BSS）を使用します。アプリケーションの動作が BSS のシグネチャと一致する場合、選択された処理が実行されます。Kaspersky Embedded Systems Security は、Behavior Stream Signatures に基づいて、コンピューターへのプロアクティブディフェンスを実現しています。

# ローカルフォルダーの暗号化保護の有効化と無効化

**Kaspersky Security Center 管理コンソールでふるまい検知を有効または無効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ふるまい検知**］セクションで、［**設定**］をクリックします。
5. ［**ふるまい検知**］をオンまたはオフにして、コンポーネントを有効または無効にします。
6. ［**全般**］タブに移動します。
7. ［**外部からの暗号化に対するローカルフォルダーの保護を有効にする**］を使用してオプションを有効または無効にします。このチェックボックスをオンにすると、その下で指定されている処理で、悪意のある活動に対応します。
8. ［**マルウェア活動の検知時の処理**］ブロックで関連する操作を選択します。
   - **削除する**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。
   - **ブロックする**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Embedded Systems Security はそのアプリケーションを終了します。
   - **通知する**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、その活動に関する情報がアクティブな脅威のリストに追加されます。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

### Kaspersky Security Center Web コンソールでふるまい検知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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］に移動し、［**設定**］をクリックします。
   ［**ふるまい検知**］ウィンドウが表示されます。
5. ［**ふるまい検知を有効にする**］を使用して機能を有効または無効にします。
6. ［**全般**］タブに移動します。
7. ［**外部からの暗号化に対するローカルフォルダーの保護を有効にする**］を使用してオプションを有効または無効にします。このチェックボックスをオンにすると、その下で指定されている処理で、悪意のある活動に対応します。
8. ［**外部からの共有フォルダーの暗号化を検知したとき**］ブロックで関連する操作を選択します。
   - **削除する**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。
   - **ブロックする**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Embedded Systems Security はそのアプリケーションを終了します。
   - **通知する**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、その活動に関する情報がアクティブな脅威のリストに追加されます。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

### *アプリケーションコンソールでふるまい検知を有効または無効にする方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］の順に選択します。
2. ［**ふるまい検知**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: Behavior Detection**］ウィンドウが表示されます。
3. ［**ふるまい検知**］をオンにします。
4. ［**全般**］タブに移動します。
5. ［**外部からの暗号化に対するローカルフォルダーの保護を有効にする**］を使用してオプションを有効または無効にします。このチェックボックスをオンにすると、その下で指定されている処理で、悪意のある活動に対応します。

6. ［**外部からの共有フォルダーの暗号化を検知したとき**］ブロックで関連する操作を選択します。

   - **削除**：このオプションを選択した場合、悪意のある動作が検知されると、悪意のあるアプリケーションの実行ファイルを削除し、そのファイルのバックアップコピーをバックアップに作成します。
   - **ブロックする**：このオプションを選択した場合、悪意のある活動が検知されると、Kaspersky Embedded Systems Security はそのアプリケーションを終了します。
   - **通知する**：このオプションを選択した場合、アプリケーションの悪意のある活動が検知されると、その活動に関する情報がアクティブな脅威のリストに追加されます。

7. 変更内容を保存します。

# 外部からの暗号化に対する共有フォルダーの保護

このコンポーネントは、NTFS ファイルシステムを使用しており EFS で暗号化されていない大容量ストレージデバイスに保存されたファイルに対する操作のみを監視します。

外部からの暗号化に対する共有フォルダーの保護は、共有フォルダー内の操作を分析します。これらの操作が外部からの暗号化に典型的な Behavior Stream Signatures と一致する場合、選択した処理が実行されます。

共有フォルダー内のファイルの変更の試行が検知されると、Kaspersky Embedded Systems Security は次の処理を実行します：

- 悪意のある操作を開始したセッションがファイル変更へアクセスするのをブロックします（ファイルは読み取り専用になります）。
- 変更されようとしているファイルのバックアップコピーを作成します。
- ローカルの製品インターフェイスレポートに項目を追加して、検知された悪意のある動作に関する情報を Kaspersky Security Center に送信します。
- また、修復エンジンがオンの場合、変更されたファイルがバックアップコピーから復元されます。

# 外部からの暗号化に対する共有フォルダーの保護の有効化または無効化

既定では、外部からの暗号化に対する共有フォルダーの保護が有効になり、カスペルスキーの専門家が推奨するモードで機能しています。この機能を設定するには、保護範囲を作成して、必要に応じて除外リストを設定します。既定では、本製品は共有フォルダーを自動的に識別し、すべてのフォルダー内のファイルの動作を追跡します。共有フォルダー内のファイルを外部から暗号化する試行が検知されると、Kaspersky Embedded Systems Security はリモートユーザーのセッションを 1 時間（既定）ブロックします。

Kaspersky Embedded Systems Security のインストール後、コンピューターを再起動するまでは、外部からの暗号化に対する共有フォルダーの保護は制限されます。

### Kaspersky Security Center 管理コンソールで外部からの暗号化に対する共有フォルダーの保護を有効または無効にする方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ふるまい検知**］セクションで、［**設定**］をクリックします。
5. ［**ふるまい検知**］をオンまたはオフにして、コンポーネントを有効または無効にします。
6. ［**共有フォルダーの保護**］タブに移動します。
7. ［**共有フォルダーの保護**］を使用してオプションを有効または無効にします。
8. ［**外部からの暗号化に対する共有フォルダーの保護**］ブロックで関連する操作を選択します。
   - **接続をブロックする時間**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし（読み取り専用）、変更されたファイルのバックアップコピーが作成されます。

     修復エンジンが有効になっていて［**接続をブロックする時間**］が選択されている場合、変更されたファイルがバックアップコピーから復元されます。

   - **通知する**：このオプションをオンにした場合、共有フォルダーにあるファイルの変更の試行が検知されると、共有フォルダーにおけるこのファイルの変更の試行に関する情報がアクティブな脅威のリストに追加され、製品のローカルインターフェイスのレポートに記録が追加されて、悪意のある動作の検知に関する情報が Kaspersky Security Center に送信されます。
9. 必要に応じて、保護範囲を作成し、除外リストを設定します。
10. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

### Kaspersky Security Center Web コンソールで外部からの暗号化に対する共有フォルダーの保護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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］に移動し、［**設定**］をクリックします。
   ［**ふるまい検知**］ウィンドウが表示されます。
5. ［**ふるまい検知を有効にする**］を使用して機能を有効または無効にします。

6. ［**共有フォルダーの保護**］タブに移動します。

7. ［**外部からの暗号化に対する共有フォルダーの保護を有効にする**］を使用してオプションを有効または無効にします。

8. ［**外部からの暗号化の検知**］ブロックで関連する操作を選択します。

   - **接続をブロックする**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし（読み取り専用）、変更されたファイルのバックアップコピーが作成されます。

     修復エンジンが有効になっていて［**接続をブロックする**］が選択されている場合、変更されたファイルがバックアップコピーから復元されます。

   - **通知する**：このオプションをオンにした場合、共有フォルダーにあるファイルの変更の試行が検知されると、共有フォルダーにおけるこのファイルの変更の試行に関する情報がアクティブな脅威のリストに追加され、製品のローカルインターフェイスのレポートに記録が追加されて、悪意のある動作の検知に関する情報が Kaspersky Security Center に送信されます。

9. 必要に応じて、保護範囲を作成し、除外リストを設定します。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

***アプリケーションコンソールで外部からの暗号化に対する共有フォルダーの保護を有効または無効にする方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］の順に選択します。

2. ［**ふるまい検知**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: Behavior Detection**］ウィンドウが表示されます。

3. ［**ふるまい検知**］をオンにします。

4. ［**共有フォルダーの保護**］タブに移動します。

5. ［**共有フォルダーを保護する**］を使用してオプションを有効または無効にします。

6. ［**外部からの暗号化に対する共有フォルダーの保護**］ブロックで関連する操作を選択します。

   - **接続をブロックする時間**：このオプションを選択した場合、共有フォルダーにあるファイルを変更する試みが検知されると、悪意のある活動を開始したセッションのファイル変更に対するアクセスをブロックし（読み取り専用）、変更されたファイルのバックアップコピーが作成されます。

     修復エンジンが有効になっていて［**接続をブロックする時間**］が選択されている場合、変更されたファイルがバックアップコピーから復元されます。

   - **通知する**：このオプションをオンにした場合、共有フォルダーにあるファイルの変更の試行が検知されると、共有フォルダーにおけるこのファイルの変更の試行に関する情報がアクティブな脅威のリストに追加され、製品のローカルインターフェイスのレポートに記録が追加されて、悪意のある動作の検知に関する情報が Kaspersky Security Center に送信されます。

7. 必要に応じて、保護範囲を作成し、除外リストを設定します。

8. 変更内容を保存します。

# 保護範囲の作成

*保護範囲*は、Kaspersky Embedded Systems Security がファイルの動作を監視する共有フォルダーへのパスのリストです。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。既定では、本製品は共有フォルダーを自動的に識別し、すべてのフォルダーのファイルの動作を追跡します。

組織で、共有フォルダーを使用したファイルの交換時にデータ暗号化が使用されている場合、保護範囲からフォルダーを除外することで誤検知の量を減らすことができます。たとえば、ユーザーが共有フォルダーで拡張子 ENC のファイルを使用していると、ふるまい検知コンポーネントで誤検知の量が増えることがあります。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フォルダーでファイルを暗号化した場合は、そのフォルダーを除外リストに追加します。

特定のコンピューターから行われる外部からの暗号化の試行を無視する場合は、そのコンピューターを除外することもできます。

**Kaspersky Security Center 管理コンソールで保護範囲を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ふるまい検知**］セクションで、［**設定**］をクリックします。
5. ［**ふるまい検知**］をオンまたはオフにして、コンポーネントを有効または無効にします。
6. ［**共有フォルダーの保護**］タブに移動します。
7. ［**保護範囲**］ブロックの［**設定**］をクリックします。
8. 表示されたウィンドウで、［**指定した共有フォルダーのみ**］モードを選択します。
9. ［**追加**］をクリックします。
10. これにより、ウィンドウが開きます。そのウィンドウで、保護範囲に含める共有フォルダーへのパスを入力します（例：`C:\Share`）。

    共有フォルダーを保護範囲に追加するには、ローカルパスを使用します。

11. ［**OK**］をクリックします。

12. 必要に応じて、保護範囲から除外する項目を設定します：

    a. ［**除外リスト**］ブロックの［**設定**］をクリックします。

    b. 表示されたウィンドウの［**追加**］をクリックします。

    c. 表示されたウィンドウで、フォルダーまたはファイルのパスを入力します。
    マスクを使用する

    - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

    - 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。

    - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

    保護範囲内のオブジェクトのリストからオブジェクトを削除しなくても、オブジェクトをスキャンから除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。

13. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

### Kaspersky Security Center Web コンソールで保護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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］に移動し、［**設定**］をクリックします。
   ［**ふるまい検知**］ウィンドウが表示されます。

5. ［**ふるまい検知を有効にする**］を使用して機能を有効または無効にします。

6. ［**共有フォルダーの保護**］タブに移動します。

7. ［**保護範囲**］で、［**指定した共有フォルダーのみ**］モードを選択します。

8. ［**追加**］をクリックします。

9. これにより、ウィンドウが開きます。そのウィンドウで、保護範囲に含める共有フォルダーへのパスを入力します（例：`C:\Share`）。

   共有フォルダーを保護範囲に追加するには、ローカルパスを使用します。

10. ［**OK**］をクリックします。

11. 必要に応じて、保護範囲から除外する項目を設定します：

    a. ［**除外対象オブジェクト**］ブロックの［**追加**］をクリックします。

    b. 表示されたウィンドウで、フォルダーまたはファイルのパスを入力します。

    マスクを使用する

    - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

    - 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。

    - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

    保護範囲内のオブジェクトのリストからオブジェクトを削除しなくても、オブジェクトをスキャンから除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。

12. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

### *アプリケーションコンソールで保護範囲を設定する方法*

1. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。

2. ［**ふるまい検知**］セクションで、［**設定**］をクリックします。

3. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］の順に選択します。

4. ［**ふるまい検知**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。

   ［**プロパティ: Behavior Detection**］ウィンドウが表示されます。

5. ［**ふるまい検知**］をオンまたはオフにして、コンポーネントを有効または無効にします。

6. ［**共有フォルダーの保護**］タブに移動します。

7. ［**保護範囲**］ブロックの［**設定**］をクリックします。

8. 表示されたウィンドウで、［**指定した共有フォルダーのみ**］モードを選択します。

9. ［**保護範囲**］ブロックの［**追加**］をクリックします。

10. これにより、ウィンドウが開きます。そのウィンドウで、保護範囲に含める共有フォルダーへのパスを入力します（例：`C:\Share`）。

    > 共有フォルダーを保護範囲に追加するには、ローカルパスを使用します。

11. ［**OK**］をクリックします。

12. 必要に応じて、保護範囲から除外する項目を設定します：

    a. ［**除外リスト**］ブロックの［**設定**］をクリックします。

    b. 表示された［**マスクによる除外**］ウィンドウで、［**追加**］をクリックします。

    c. 表示されたウィンドウで、フォルダーまたはファイルのパスを入力します。

    マスクを使用する

    - 「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。

    - 2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。

    - 「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。

    保護範囲内のオブジェクトのリストからオブジェクトを削除しなくても、オブジェクトをスキャンから除外することができます。そのためには、オブジェクトの横にあるチェックボックスをオフにします。

13. 変更内容を保存します。

# 外部データ暗号化用の信頼できるコンピューターの追加

所属する組織がファイル交換にデータの外部からの暗号化を使用する場合、信頼できるコンピューターのリストを作成する必要があります。Kaspersky Embedded Systems Security では、信頼できるコンピューターでのデータ暗号化は監視されません。

外部からの暗号化に対する共有フォルダーの保護から除外するアドレスを設定するには、ログオンの監査サービスを有効にしておく必要があります。既定では、ログオンの監査サービスは無効です（ログオンの監査サービスの有効化に関する詳細な情報については、Microsoft の Web サイトを参照してください）。

共有フォルダーの保護からアドレスを除外する機能は、Kaspersky Embedded Systems Security が開始する前から動作しているリモートコンピューターに対しては適用されません。Kaspersky Embedded Systems Security が開始した後でリモートコンピューターを再起動することで、そのリモートコンピューターに対して共有フォルダーの保護からアドレスを除外する機能が有効になります。

**Kaspersky Security Center 管理コンソールでデータの外部からの暗号化用に信頼できるコンピューターを追加する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ふるまい検知**］セクションで、［**設定**］をクリックします。
5. ［**共有フォルダーの保護**］タブに移動します。
6. ［**IP アドレスの除外リスト**］ブロックの［**設定**］をクリックします。
7. 表示されたウィンドウの［**追加**］をクリックします。
8. 外部からの暗号化に対する処理を実行しない IP アドレスまたはコンピューター名を入力します。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

**Kaspersky Security Center Web コンソールでデータの外部からの暗号化用に信頼できるコンピューターを追加する方法**

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］に移動し、［**設定**］をクリックします。
［**ふるまい検知**］ウィンドウが表示されます。
5. ［**共有フォルダーの保護**］タブに移動します。
6. ［**除外リスト**］ブロックの［**追加**］をクリックします。
7. 外部からの暗号化に対する処理を実行しない IP アドレスまたはコンピューター名を入力します。
8. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

***アプリケーションコンソールでデータの外部からの暗号化用に信頼できるコンピューターを追加する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］の順に選択します。
2. ［**ふるまい検知**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
［**プロパティ: Behavior Detection**］ウィンドウが表示されます。
3. ［**共有フォルダーの保護**］タブに移動します。
4. ［**IP アドレスの除外リスト**］ブロックの［**設定**］をクリックします。
5. 表示されたウィンドウの［**追加**］をクリックします。
6. 外部からの暗号化に対する処理を実行しない IP アドレスまたはコンピューター名を入力します。
7. 変更内容を保存します。

# 信頼できないコンピューターのブロック期間の設定

*信頼できないコンピューター*とは、悪意のある動作やデータ暗号化に関与しているリモートコンピューターです。既定では、Kaspersky Embedded Systems Security はリモートユーザーのセッションを 1 時間ブロックします。ブロック期間が終了すると、Kaspersky Embedded Systems Security はコンピューターをブロックリストから削除し、共有フォルダーへのアクセスを復元します。

**Kaspersky Security Center 管理コンソールで信頼できないコンピューターのブロック期間を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ふるまい検知**］セクションで、［**設定**］をクリックします。

5. ［**ふるまい検知**］をオンまたはオフにして、コンポーネントを有効または無効にします。

6. ［**共有フォルダーの保護**］タブに移動します。

7. ［**外部からの共有フォルダーの暗号化を検知したとき**］で、悪意のある動作やデータ暗号化に関与している信頼できないコンピューターのブロック期間を設定します。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

**Kaspersky Security Center Web コンソールで信頼できないコンピューターのブロック期間を設定する方法**

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

2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］に移動し、［**設定**］をクリックします。
   ［**ふるまい検知**］ウィンドウが表示されます。

5. ［**ふるまい検知を有効にする**］を使用して機能を有効または無効にします。

6. ［**共有フォルダーの保護**］タブに移動します。

7. ［**外部からの暗号化の検知**］で、悪意のある動作やデータ暗号化に関与している信頼できないコンピューターのブロック期間を設定します。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

***アプリケーションコンソールで信頼できないコンピューターのブロック期間を設定する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］の順に選択します。

2. ［**ふるまい検知**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: Behavior Detection**］ウィンドウが表示されます。

3. ［**ふるまい検知**］をオンにします。

4. ［**共有フォルダーの保護**］タブに移動します。

5. ［**外部からの暗号化に対する共有フォルダーの保護**］で、悪意のある動作やデータ暗号化に関与している信頼できないコンピューターのブロック期間を設定します。

6. 変更内容を保存します。

# 外部からの暗号化に対する共有フォルダーの保護の除外リストのエクスポートおよびインポート

除外リストを XML 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、例えば同じ種別の多数のアドレス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、除外リスト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。

***Kaspersky Security Center 管理コンソールで除外リストをエクスポートおよびインポートする方法***

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］を選択します。
4. ［**ふるまい検知**］セクションで、［**設定**］をクリックします。
5. ［**共有フォルダーの保護**］タブに移動します。
6. ［**IP アドレスの除外リスト**］ブロックの［**設定**］をクリックします。
7. ルールのリストをエクスポートするには：
   a. 必要に応じて、エクスポートする除外リストを選択します。
   b. をクリックして、エクスポートモードを選択します。除外リスト全体をエクスポートするか、選択した除外リストのみをエクスポートします。
   c. 表示されたウィンドウで、除外リストをエクスポートする XML 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。
      Kaspersky Embedded Systems Security は、除外リストを XML ファイルにエクスポートします。
8. 除外リストをインポートするには：
   a. → ［**インポート**］を選択します。
      表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
   b. ファイルを開きます。
      Kaspersky Embedded Systems Security で除外リストがインポートされます。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

*Kaspersky Security Center Web コンソールで除外リスト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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］に移動し、［**設定**］をクリックします。
   ［**ふるまい検知**］ウィンドウが表示されます。
5. ［**ふるまい検知を有効にする**］を使用して機能を有効または無効にします。
6. ［**共有フォルダーの保護**］タブに移動します。
7. ［**除外リスト**］ブロックで除外リストをエクスポートするには：
   a. 必要に応じて、エクスポートする除外リストを選択します。
   b. ［**エクスポート**］をクリックして、エクスポートモードを選択します。除外リスト全体をエクスポートするか、選択した除外リストのみをエクスポートします。
   c. ファイルを保存します。
      Kaspersky Embedded Systems Security は、除外リストを XML ファイルにエクスポートします。
8. ［**除外リスト**］ブロックで除外リストをインポートするには：
   a. ［**インポート**］をクリックして、インポートモード（追加または置換）を選択します。
   b. 表示されたウィンドウで、除外リストをインポートする XML ファイルを選択します。
   c. ファイルを開きます。
      Kaspersky Embedded Systems Security で、選択したモードに従って除外リストがインポートされます。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

# ネットワーク脅威対策

ネットワーク脅威対策は、受信ネットワークトラフィックにおいて、典型的なネットワーク攻撃の活動があるかどうかをスキャンします。使用中のコンピューターを標的としてネットワーク攻撃が試行されたことが検知された場合、Kaspersky Embedded Systems Security は攻撃側コンピューターからのネットワーク活動をブロックします。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。

既定では、*ネットワーク脅威対策*タスクは、［**ブロックする**］モードで実行されます。このモードでは、Kaspersky Embedded Systems Security は、ネットワーク攻撃の典型的な動作が見られるコンピューターへの接続をブロックします。また、場合によっては、そのようなコンピューターの IP アドレスをブロック対象のネットワークセッションのリストに追加します。

ブロック対象コンピューターの保管領域で、ブロック対象コンピューターのリストを表示することができます。

Kaspersky Embedded Systems Security は、アプリケーションが再起動されたときとネットワーク脅威対策の設定が変更されたときにブロックリストを消去します。

ブロック対象コンピューターへのアクセスを復元し、ブロック対象コンピューターの保管領域を設定することで、コンピューターがブロックされた後からネットワークファイルリソースへのアクセスを回復するまでの日数および時間（時間、分）を指定できます。

ネットワーク攻撃の典型的な動作を示すコンピューターの IP アドレスが、ブロック対象コンピューターのリストから削除されるのは、次の場合です：

- Kaspersky Embedded Systems Security をアンインストールしました。
- ブロック対象コンピューターのリストから IP アドレスが手動で削除しました。
- コンピューターのブロック期間が終了しました。
- 「**ブロックする**」モードがオフになりました。

**Kaspersky Security Center 管理コンソールでネットワーク脅威対策を有効にして設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**ポリシー**］タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. ポリシーのプロパティウィンドウで、［**ネットワーク動作コントロール**］をクリックします。
6. ［**ネットワーク脅威対策**］ブロックの［**設定**］をクリックします。
   ［**ネットワーク脅威対策**］ウィンドウが開き、［**全般**］タブが表示されます。

7. ［**ネットワーク脅威対策**］をオンにして、ネットワーク脅威対策を有効にします。

8. ［**操作モード**］セクションでタスクモードを選択します：

   - **ブロックする**：このモードを選択すると、Kaspersky Embedded Systems Security は、受信ネットワークトラフィックをスキャンし、ネットワーク攻撃の典型的な動作があるかどうかをチェックして、そのような動作が見られるコンピューターへの接続をブロックします。また、場合によっては、コンピューターの IP アドレスをブロック対象のネットワークセッションのリストに追加します。さらに、検知したネットワーク攻撃の典型的な動作に関するイベントがコンポーネントログに記録されます。

   - **通知する**：このモードを選択すると、Kaspersky Embedded Systems Security は、受信ネットワークトラフィックをスキャンし、ネットワーク攻撃の典型的な動作があるかどうかをチェックしますが、そのような動作が見られるコンピューターへの接続のブロックは行いません。また、コンピューターの IP アドレスをブロック対象のネットワークセッションのリストに追加することもありません。検知したネットワーク攻撃の典型的な動作に関するイベントがコンポーネントログに記録されます。

9. 対応する攻撃の検知を有効または無効にするには、［**ポートのスキャンおよびネットワークフラッディングを攻撃として扱う**］を使用します。

10. 必要に応じて、［**攻撃元の端末をブロックする時間N 分**］をオンにします。

11. ［**MAC スプーフィング対策**］ブロックで、［**MAC スプーフィング攻撃に対する保護を有効にする**］をオンまたはオフにします。

12. 必要に応じて、**ブロックから除外する項目を追加する**ことができます。

    Kaspersky Embedded Systems 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。コミュニケーションに使用されるプロトコルとポートを選択して、特定のネットワーク活動を許可することもできます。

    > プロトコルとポートを選択して除外する機能は Kaspersky Embedded Systems Security 4.0 で追加されました。本製品と管理プラグインがバージョン 4.0 以降にアップデートされていることをご確認ください。以前のバージョンの本製品と管理プラグインを使用している場合、Kaspersky Embedded Systems Security は IP アドレスでのみネットワーク活動を許可できます。

    a. ［**除外リスト**］タブを選択します。

    b. 受信ネットワークトラフィックにおいて、除外された IP アドレスをスキャンしないように、［**除外されたアドレスを管理しない**］をオンにします。

    c. ［**追加**］をクリックします。

    d. ［**除外リスト**］ウィンドウで、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。

    e. 必要に応じて、データを転送するプロトコルとポートを選択します。

f. ［**OK**］をクリックします。

g. 追加された除外項目ごとに手順 c ～ f を実行します。

13. 変更内容を保存します。

***アプリケーションコンソールでネットワーク脅威対策を有効にして設定する方法***

1. アプリケーションコンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ネットワーク脅威対策**］フォルダーの順に選択します。
2. 結果ペインで［**プロパティ**］をクリックします。
   ［**プロパティ：ネットワーク脅威対策**］ウィンドウが表示されます。
3. ［**ネットワーク脅威対策**］をオンにして、ネットワーク脅威対策コンポーネントを有効にします。
4. ［**操作モード**］セクションでタスクモードを選択します：
   - **ブロックする**：このモードを選択すると、Kaspersky Embedded Systems Security は、受信ネットワークトラフィックをスキャンし、ネットワーク攻撃の典型的な動作があるかどうかをチェックして、そのような動作が見られるコンピューターへの接続をブロックします。また、場合によっては、コンピューターの IP アドレスをブロック対象のネットワークセッションのリストに追加します。さらに、検知したネットワーク攻撃の典型的な動作に関するイベントがコンポーネントログに記録されます。
   - **通知する**：このモードを選択すると、Kaspersky Embedded Systems Security は、受信ネットワークトラフィックをスキャンし、ネットワーク攻撃の典型的な動作があるかどうかをチェックしますが、そのような動作が見られるコンピューターへの接続のブロックは行いません。また、コンピューターの IP アドレスをブロック対象のネットワークセッションのリストに追加することもありません。検知したネットワーク攻撃の典型的な動作に関するイベントがコンポーネントログに記録されます。
5. 対応する攻撃の検知を有効または無効にするには、［**ポートのスキャンおよびネットワークフラッディングを攻撃として扱う**］を使用します。
6. 必要に応じて、［**攻撃元の端末をブロックする時間N 分**］をオンにします。
7. ［**MAC スプーフィング対策**］ブロックで、［**MAC スプーフィング攻撃に対する保護を有効にする**］をオンまたはオフにします。
8. 必要に応じて、**ブロックから除外する項目を追加する**ことができます。

Kaspersky Embedded Systems 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。コミュニケーションに使用されるプロトコルとポートを選択して、特定のネットワーク活動を許可することもできます。

プロトコルとポートを選択して除外する機能は Kaspersky Embedded Systems Security 4.0 で追加されました。本製品と管理プラグインがバージョン 4.0 以降にアップデートされていることをご確認ください。以前のバージョンの本製品と管理プラグインを使用している場合、Kaspersky Embedded Systems Security は IP アドレスでのみネットワーク活動を許可できます。

a. ［**除外リスト**］タブを選択します。

b. 受信ネットワークトラフィックにおいて、除外された IP アドレスをスキャンしないように、［**除外されたアドレスを管理しない**］をオンにします。

c. ［**追加**］をクリックします。

d. ［**除外リスト**］ウィンドウで、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。

e. 必要に応じて、データを転送するプロトコルとポートを選択します。

f. ［**OK**］をクリックします。

g. 追加された除外項目ごとに手順 c ～ f を実行します。

9. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでネットワーク脅威対策を有効にして設定する方法**

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ネットワーク動作コントロール**］→［**ネットワーク脅威対策**］の順に選択します。
5. ［**全般**］タブの［**ネットワーク脅威対策を有効にする**］をオンにして、ネットワーク脅威対策コンポーネントを有効にします。

6. タスク処理モードを選択します：

   - **ブロックする**：このモードを選択すると、Kaspersky Embedded Systems Security は、受信ネットワークトラフィックをスキャンし、ネットワーク攻撃の典型的な動作があるかどうかをチェックして、そのような動作が見られるコンピューターへの接続をブロックします。また、場合によっては、コンピューターの IP アドレスをブロック対象のネットワークセッションのリストに追加します。さらに、検知したネットワーク攻撃の典型的な動作に関するイベントがコンポーネントログに記録されます。

   - **通知する**：このモードを選択すると、Kaspersky Embedded Systems Security は、受信ネットワークトラフィックをスキャンし、ネットワーク攻撃の典型的な動作があるかどうかをチェックしますが、そのような動作が見られるコンピューターへの接続のブロックは行いません。また、コンピューターの IP アドレスをブロック対象のネットワークセッションのリストに追加することもありません。検知したネットワーク攻撃の典型的な動作に関するイベントがコンポーネントログに記録されます。

7. 対応する攻撃の検知を有効または無効にするには、［**ポートのスキャンおよびネットワークフラッディングを攻撃として扱う**］を使用します。

8. 必要に応じて、［**攻撃元の端末をブロックする時間N 分**］をオンにします。

9. ［**MAC スプーフィング攻撃に対する保護を有効にする**］をオンまたはオフにします。

10. 必要に応じて、**ブロックから除外する項目を追加する**ことができます。

    Kaspersky Embedded Systems 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。コミュニケーションに使用されるプロトコルとポートを選択して、特定のネットワーク活動を許可することもできます。

    > プロトコルとポートを選択して除外する機能は Kaspersky Embedded Systems Security 4.0 で追加されました。本製品と管理プラグインがバージョン 4.0 以降にアップデートされていることをご確認ください。以前のバージョンの本製品と管理プラグインを使用している場合、Kaspersky Embedded Systems Security は IP アドレスでのみネットワーク活動を許可できます。

    a. ［**除外リスト**］タブを選択します。

    b. 受信ネットワークトラフィックにおいて、除外された IP アドレスをスキャンしないように、［**除外されたアドレスを管理しない**］をオンにします。

    c. ［**追加**］をクリックします。

    d. ［**除外リスト**］ウィンドウで、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。

    e. 必要に応じて、データを転送するプロトコルとポートを選択します。

    f. ［**OK**］をクリックします。

    g. 追加された除外項目ごとに手順 c ～ f を実行します。

11. 変更内容を保存します。

# AMSI スキャナー

AMSI スキャナータスクの実行中、Kaspersky Embedded Systems Security は、VBScript や JScript などの Microsoft Windows スクリプト技術（Active Scripting）を使用して作成されたスクリプトの実行を制御します。本製品は、Antimalware Scan Interface（AMSI）がインストールされたオペレーティングシステム上の Microsoft Office アプリケーションで実行される PowerShell スクリプトおよびスクリプトも処理できます。

AMSI を使用すると、実行されたすべてのスクリプトがマルウェア対策によってインターセプトおよびスキャンされるように、アプリケーションとサービスをデバイスにインストールされているマルウェア対策アプリケーションと連携できます。AMSI 機能の詳細は、Microsoft の Web サイトを参照してください。

コンポーネントの設定では、危険なスクリプトの実行を許可または拒否できます。Kaspersky Embedded Systems Security は、危険なスクリプトを特定すると、選択した動作に従ってスクリプトの実行をブロックまたは許可します。［**ブロックする**］の処理を選択した場合、本製品により、危険なスクリプトがブロックされて、それ以外のスクリプトが許可されます。

Kaspersky Embedded Systems Security は、Microsoft Windows 10 および Microsoft Windows Server 2016 以降の AMSI 技術をサポートしています。

# AMSI スキャナーの有効化と無効化

**Kaspersky Security Center 管理コンソールで AMSI スキャナーを有効または無効にする方法**

1. **設定するポリシーのAMSI スキャナーの設定に移動します**。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**ポリシー**］タブを選択します。

   d. ポリシー名をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

   e. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］をクリックします。

   f. ［**AMSI スキャナー**］ブロックの［**設定**］をクリックします。
   ［**AMSI スキャナー**］ウィンドウが開き、［**全般**］タブが表示されます。

2. 次のいずれかを行います：

   - AMSI スキャナーを有効にする場合は、［**AMSI スキャナー**］をオンにします。
   - AMSI スキャナーを無効にする場合は、［**AMSI スキャナー**］をオフにします。

3. ［**AMSI スキャナー**］ウィンドウで、［**OK**］をクリックします。
4. **プロパティ：<ポリシー名>**ウィンドウで、［**OK**］をクリックします。

*Kaspersky Embedded Systems Security コンソールで AMSI スキャナーを有効にする方法*

1. コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**AMSI スキャナー**］セクションを選択します。
2. 結果ペインで［**プロパティ**］をクリックします。
   ［**AMSI スキャナー**］ウィンドウが開き、［**全般**］タブが表示されます。
3. 次のいずれかを行います：
   - AMSI スキャナーを有効にする場合は、［**AMSI スキャナー**］をオンにします。
   - AMSI スキャナーを無効にする場合は、［**AMSI スキャナー**］をオフにします。
4. ［**AMSI スキャナー**］ウィンドウで、［**OK**］をクリックします。

**Kaspersky Security Center Web コンソールで AMSI スキャナーを有効にする方法**

1. 設定するポリシーのAMSI スキャナーの設定に移動します。
   a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
   b. Kaspersky Embedded Systems 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。
   c. ［**アプリケーション設定**］タブを選択します。
   d. ［**コンピューターのリアルタイム保護**］セクションを選択します。
   e. ［**AMSI スキャナー**］ブロックの［**設定**］をクリックします。
      ［**AMSI スキャナー**］ウィンドウが表示されます。
2. 次のいずれかを行います：
   - AMSI スキャナーを有効にする場合は、［**AMSI スキャナー**］をオンにします。
   - AMSI スキャナーを無効にする場合は、［**AMSI スキャナー**］をオフにします。
3. ［**AMSI スキャナー**］ウィンドウの［**OK**］をクリックします。
4. ［**<ポリシー名>**］ウィンドウで、［**保存**］をクリックします。

# AMSI スキャナーの設定

### Kaspersky Security Center 管理コンソールでAMSI スキャナーを設定する方法

1. 設定するポリシーのAMSI スキャナーの設定に移動します。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**ポリシー**］タブを選択します。

   d. ポリシー名をダブルクリックして、ポリシーのプロパティウィンドウを開きます。

   e. ポリシーのプロパティウィンドウで、［**コンピューターのリアルタイム保護**］をクリックします。

   f. ［**AMSI スキャナー**］ブロックの［**設定**］をクリックします。
   ［**AMSI スキャナー**］ウィンドウが開き、［**全般**］タブが表示されます。

2. 危険なスクリプトが実行された際に Kaspersky Embedded Systems Security が実行する処理を選択します：

   - **通知する**：危険な可能性があるスクリプトの実行を許可します。対応するイベントが実行ログに記録されます。
   - **ブロックする**：危険な可能性があるスクリプトをブロックします。

3. ［**複合ファイルのスキャン**］ブロックで、スキャンする複合ファイル種別として、圧縮ファイル、配布パッケージ、Office 形式のファイルのいずれかを指定します。

4. ［**サイズ制限**］ブロックで、次のいずれかを実行します：

   - AMSI スキャナーを使用して大きな複合ファイルを解凍しない場合は、［**大きな複合ファイルをスキャンしない**］をオンにし、［**ファイルの最大サイズ (MB)**］に任意の値を入力します。指定された値を超えるサイズのファイルは解凍されません。
   - AMSI スキャナーを使用して大きな複合ファイルを解凍する場合は、［**大きな複合ファイルをスキャンしない**］をオフにします。

   アーカイブから展開されるサイズの大きいファイルは、［**大きな複合ファイルをスキャンしない**］がオンにされているかどうかに関係なくスキャンされます。

5. ［**AMSI スキャナー**］ウィンドウで、［**OK**］をクリックします。

6. **プロパティ：<ポリシー名>**ウィンドウで、［**OK**］をクリックします。

*Kaspersky Embedded Systems Security コンソールでAMSI スキャナーを設定する方法*

1. コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**AMSI スキャナー**］セクションを選択します。

2. 結果ペインで［**プロパティ**］をクリックします。
   ［**AMSI スキャナー**］ウィンドウが開き、［**全般**］タブが表示されます。

3. 危険なスクリプトが実行された際に Kaspersky Embedded Systems Security が実行する処理を選択します：

   - **通知する**：危険な可能性があるスクリプトの実行を許可します。対応するイベントが実行ログに記録されます。

   - **ブロックする**：危険な可能性があるスクリプトをブロックします。

4. ［**複合ファイルのスキャン**］ブロックで、スキャンする複合ファイル種別として、圧縮ファイル、配布パッケージ、Office 形式のファイルのいずれかを指定します。

5. ［**サイズ制限**］ブロックで、次のいずれかを実行します：

   - AMSI スキャナーを使用して大きな複合ファイルを解凍しない場合は、［**大きな複合ファイルをスキャンしない**］をオンにし、［**ファイルの最大サイズ (MB)**］に任意の値を入力します。指定された値を超えるサイズのファイルは解凍されません。

   - AMSI スキャナーを使用して大きな複合ファイルを解凍する場合は、［**大きな複合ファイルをスキャンしない**］をオフにします。

   > アーカイブから展開されるサイズの大きいファイルは、［**大きな複合ファイルをスキャンしない**］がオンにされているかどうかに関係なくスキャンされます。

6. ［**AMSI スキャナー**］ウィンドウで、［**OK**］をクリックします。

**Kaspersky Security Center Web コンソールでAMSI スキャナーを設定する方法**

1. 設定するポリシーのAMSI スキャナーの設定に移動します。

   a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

   b. Kaspersky Embedded Systems 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。

   c. ［**アプリケーション設定**］タブを選択します。

d. ［**コンピューターのリアルタイム保護**］セクションを選択します。

e. ［**AMSI スキャナー**］ブロックの［**設定**］をクリックします。
［**AMSI スキャナー**］ウィンドウが表示されます。

2. 危険なスクリプトが実行された際に Kaspersky Embedded Systems Security が実行する処理を選択します：

- **通知する**：危険な可能性があるスクリプトの実行を許可します。対応するイベントが実行ログに記録されます。
- **ブロックする**：危険な可能性があるスクリプトをブロックします。

3. ［**複合ファイルのスキャン**］ブロックで、スキャンする複合ファイル種別として、圧縮ファイル、配布パッケージ、Office 形式のファイルのいずれかを指定します。

4. ［**サイズ制限**］ブロックで、次のいずれかを実行します：

- AMSI スキャナーを使用して大きな複合ファイルを解凍しない場合は、［**大きな複合ファイルをスキャンしない**］をオンにし、［**ファイルの最大サイズ (MB)**］に任意の値を入力します。指定された値を超えるサイズのファイルは解凍されません。
- AMSI スキャナーを使用して大きな複合ファイルを解凍する場合は、［**大きな複合ファイルをスキャンしない**］をオフにします。

アーカイブから展開されるサイズの大きいファイルは、［**大きな複合ファイルをスキャンしない**］がオンにされているかどうかに関係なくスキャンされます。

5. ［**AMSI スキャナー**］ウィンドウの［**OK**］をクリックします。

6. ［**<ポリシー名>**］ウィンドウで、［**保存**］をクリックします。

# アプリケーション起動コントロール

アプリケーション起動コントロールタスクの実行中に、Kaspersky Embedded Systems Security はアプリケーションを起動しようとするユーザーの試行を監視し、これらのアプリケーションの開始を許可または拒否します。アプリケーション起動コントロールタスクは「既定で拒否」の原則に基づいています。これは、タスク設定で許可されていないアプリケーションはすべて自動でブロックされることを意味します。

アプリケーション起動コントロールの許可ルールを作成することで、アプリケーションの起動を許可できます。

アプリケーションを起動しようとするすべての試行は、タスク実行ログに記録されます。

アプリケーション起動コントロールタスクは、2 つのモードのいずれかで実行できます：

- **ブロックする**：Kaspersky Embedded Systems Security が、アプリケーション起動コントロールルールを使用してアプリケーションの起動を制御します。アプリケーション起動コントロールルールの範囲は、アプリケーション起動コントロールタスクの全般設定で指定されます。アプリケーションがアプリケーション起動コントロールルールを満たしているが、どのルールもアプリケーション起動コントロールルールの範囲に一致しない場合、そのアプリケーションは実行されません。

  アプリケーション起動コントロールルールの対象外のアプリケーションの実行は禁止されます。

  **アプリケーション起動コントロール**タスクは、アプリケーション起動コントロールルールが作成されていない場合、または 1 つの保護対象デバイスに対して 65,535 を超えるアプリケーション起動コントロールルールがある場合、［処理を実行］モードで起動できません。

- **通知**：Kaspersky Embedded Systems Security はすべてのアプリケーションの起動を許可します。すべてのアプリケーションの起動、起動されたアプリケーションを対象とするルール、およびタスクが**ブロックする**モードで実行されている場合に実行される処理に関する情報のみが記録されます。既定ではこのモードが設定されています。

アプリケーション起動コントロールルールの作成時に、オペレーティングシステムのアプリケーションの実行がブロックされないようにすることを推奨します。

また、Kaspersky Embedded Systems Security は、Windows Subsystem for Linux で起動されたプロセスをインターセプトします（UNIX™ シェル、またはコマンドラインインタープリターから実行されたスクリプトを除く）。そのようなプロセスに対して、アプリケーション起動コントロールタスクは現在の設定で定義されている処理を適用します。アプリケーション起動コントロールルールの自動生成タスクは、アプリケーションの起動を検出し、Windows Subsystem for Linux で動作するアプリケーションに対して対応するルールを生成します。

# アプリケーション起動コントロールルールについて

## アプリケーション起動コントロールルールの仕組み

アプリケーション起動コントロールルールの処理は、次のコンポーネントに基づきます：

- ルールの種別

  アプリケーション起動コントロールルールは、アプリケーションの起動を許可または拒否できます。それぞれ*許可*ルールまたは*拒否*ルールと呼ばれています。

- ルールの適用範囲

  アプリケーション起動コントロールルールは、*実行ファイル*や*スクリプト*、*MSI パッケージ*に適用できます。

- ルールを適用する条件

  アプリケーション起動コントロールルールは、ルール設定で指定された少なくとも1つの適用条件を満たすファイルの起動を制御します。たとえば、実行ファイルが、指定された*デジタル証明書*で署名されている、指定された *SHA256* ハッシュを持つ、指定された*パス*に配置されている、指定された*コマンドライン*引数に一致するなどです。少なくとも1つのルール適用条件を追加する必要があります。それ以外の場合、アプリケーション起動コントロールのルールは追加されません。

- ルールから除外する項目

  アプリケーション起動コントロールルールの除外項目を設定できます。除外項目は、ルールの適用条件と同じ条件に基づく場合があります。特定の許可ルールのために、アプリケーション起動コントロールルールの除外対象が必要になる場合もあります。たとえば、ユーザーが C:\Windows のパスからアプリケーションを起動することを許可する一方で、ファイル Regedit.exe の起動をブロックできます。

- ユーザーまたはユーザーのグループ

  アプリケーション起動コントロールルールは、特定のユーザーまたはユーザーグループによって指定されたアプリケーションの起動を制御できます。

アプリケーション起動コントロールルールの作成時に、新しいルールによって、オペレーティングシステムのアプリケーションの実行がブロックされないようにすることを推奨します。

## アプリケーション起動コントロールルールの管理

アプリケーション起動コントロールルールを使用して、次の処理を実行できます：

- 手動で追加する
- ルールを自動生成して追加する
- 削除する
- インポートおよびエクスポートする
- ルールのリストをフィルタリングする

# ソフトウェア配布コントロールについて

ソフトウェアの配布を制御する場合、アプリケーション起動コントロールの生成はより複雑になる可能性があります。これは、インストールされたソフトウェアが定期的に自動アップデートされる保護対象デバイスなどで行われる場合があります。この場合、ソフトウェアのアップデート後に毎回、許可ルールのリストをアップデートし、新しく作成されたファイルがアプリケーション起動コントロールタスクの設定に反映されるようにする必要があります。ソフトウェアの配布シナリオで起動コントロールを簡略化するために、ソフトウェア配布コントロールを使用できます。

*インストールパッケージ*（以降、「パッケージ」と表記）は、保護対象デバイスにインストールされる1つまたは複数のアプリケーションを表します。インストールパッケージには、アップデートや個別のコマンドも含まれる場合があります。

ソフトウェア配布コントロールのサブシステムは、追加の除外リストとして実装されます。インストールパッケージがリストに追加されると、そのパッケージは信頼済みになります。信頼済みパッケージの解凍や、信頼済みパッケージからのインストールまたはアップデートされたアプリケーションの自動起動が許可されます。抽出したファイルは、展開元の配布パッケージの信頼する属性を継承することができます。*展開元の配布パッケージ*は、ソフトウェア配布コントロールの除外リストにユーザーが追加して信頼するパッケージとなったものです。

Kaspersky Embedded Systems Security は、アプリケーションの配布のフルサイクルのみを管理します。パッケージが初めて起動された時にソフトウェア配布コントロールがオフになっている場合、またはアプリケーション起動コントロールコンポーネントがインストールされていない場合、信頼するパッケージによって変更されたファイルの起動を正しく処理できません。

ソフトウェア配布コントロールを使用するには、アプリケーション起動コントロールの全般設定で［**実行ファイルにルールを適用する**］機能を有効にする必要があります。

## ソフトウェアの配布のキャッシュ

Kaspersky Embedded Systems Security は、動的に生成されたソフトウェア配布のキャッシュ（「配布キャッシュ」とも表記）を使用して、信頼するパッケージとソフトウェアの配布中に作成されたファイルとの関連付けを確立します。パッケージの最初の起動時に、Kaspersky Embedded Systems Security はソフトウェアの配布処理中にパッケージから作成したすべてのファイルを検知し、ファイルのチェックサムとパスを配布キャッシュに保存します。既定では、その後、配布キャッシュに情報が保存されているすべてのファイルの起動が許可されます。

ユーザーインターフェイスから配布キャッシュを更新、削除、または手動で変更することはできません。キャッシュは Kaspersky Embedded Systems Security によって追加および管理されます。

コマンドラインで、配布キャッシュを設定情報ファイルに（XML 形式で）エクスポートしたり、配布キャッシュを削除したりできます。

*配布キャッシュを設定情報ファイルにエクスポートするには、次のコマンドを実行します：*

```
kavshell appcontrol /config /savetofile:<full path> /sdc
```

*配布キャッシュを削除するには、次のコマンドを実行します：*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security は、配布キャッシュを 24 時間ごとにアップデートします。前に許可されたファイルのチェックサムが変更されると、そのファイルのレコードが配布キャッシュから削除されます。アプリケーション起動コントロールタスクが［処理を実行］モードで開始された場合、このファイルのそれ以降の開始試行はブロックされます。前に許可されたファイルのフルパスが変更された場合は、チェックサムは配布キャッシュに保存されたまま残るため、それ以降のこのファイルの起動の試行はブロックされません。

## 抽出したファイルの処理

（最初のレベルでネストされる）主要な信頼する展開元の配布パッケージによって作成、抽出されたファイルとパッケージでは、除外リストに含まれるソフトウェアの配布パッケージを最初に開いてファイルとパッケージのチェックサムが配布キャッシュに追加された時に、信頼属性が継承されます。このため、配布パッケージ自体とこのパッケージから抽出されたすべてのファイルも信頼されます。

たとえば、複数のパッケージとアプリケーションを含むパッケージ test.msi が除外リストに追加された状態で［**この配布パッケージの配下のすべてのファイルを信頼済みとして起動を許可する**］機能を有効にすると、パッケージ test.msi に含まれるすべてのパッケージとアプリケーションは、他にネストされたファイルが含まれている場合でも解凍して実行できるようになります。このシナリオは、すべてのネストされたレベルで抽出されたファイルに対して有効です。

パッケージ test.msi が除外リストに追加され、［**この配布パッケージの配下のすべてのファイルを信頼済みとして起動を許可する**］機能が無効になっている場合、（最初のレベルでネストされる）信頼できるパケットから直接抽出されたパケットと実行ファイルにのみ、信頼属性が割り当てられます。そのようなファイルチェックサムは、配布キャッシュに保存されます。2 番目以降のレベルでネストされるすべてのファイルは、「既定で拒否」の原則によってブロックされます。

抽出したファイルは、オペレーティングシステムの再起動後でも信頼属性を維持します。

抽出したすべてのファイルから継承属性を削除するには、信頼できるインストールパッケージを再度実行する前に、配布キャッシュを削除し、［**この配布パッケージの配下のすべてのファイルを信頼済みとして起動を許可する**］機能を無効にする必要があります。

## アプリケーション起動コントロールルールリストとの影響関係

ソフトウェア配布コントロールの信頼するパッケージのリストは、除外のリストであり、アプリケーション起動コントロールルールの全般リストを補完しますが、置き換えるものではありません。

アプリケーション起動コントロールルールによる拒否は、最も優先されます。これらのパッケージとファイルがアプリケーション起動コントロールの拒否ルールによって影響を受けている場合、信頼するパッケージの展開と新しいファイルまたは変更されたファイルの起動がブロックされます。

アプリケーション起動コントロールリストの拒否ルールがこれらのパッケージとファイルに適用されていない場合、ソフトウェア配布コントロールの除外リストが、これらのパッケージによって作成または変更された、信頼するパッケージとファイルの両方に適用されます。

# アプリケーション起動コントロールルールの自動生成の設定

Kaspersky Security Center のタスクとポリシーを使用して、アプリケーション起動コントロールルールのリストを企業ネットワーク上の全保護対象デバイスおよび保護対象デバイスのグループに対して一度に作成できます。参照マシンが企業ネットワークになく、テンプレートマシンにインストールされているアプリケーションに基づいて許可ルールのリストを作成できない場合、以下に示すシナリオを使用してください。

アプリケーションコンソールからローカルにアプリケーション起動コントロールルールの自動生成タスクを実行して、1台の保護対象デバイスで実行するアプリケーションに基づいてルールのリストを作成できます。

Kaspersky Security Center 側でアプリケーション起動コントロールルールのリストを作成するには、次のいずれかの方法で行います：

- アプリケーション起動コントロールルールの自動生成グループタスクを使用する。

  このシナリオでは、ネットワーク上の各保護対象デバイスに対して、アプリケーション起動コントロールルールの独自のリストがグループタスクにより生成され、指定した共有フォルダーの XML ファイルにそれらのリストが保存されます。アプリケーション起動コントロールルールの自動生成タスクによって生成された XML ファイルには、タスクの開始前にアプリケーション起動コントロールのタスク設定で指定された許可ルールが含まれています。タスク設定での起動が許可されていないアプリケーションに対しては、ルールが作成されません。そのようなアプリケーションの起動は既定で拒否されます。その後、作成したルールのリストを Kaspersky Security Center のポリシーのアプリケーション起動コントロールのタスク設定に手動でインポートできます。

  生成されたルールがアプリケーション起動コントロールタスクのルールのリストへ自動的にインポートされるように、設定を編集できます。

  アプリケーション起動コントロールルールのリストを急いで作成する必要がある場合にこのシナリオを使用してください。アプリケーション起動コントロールルールの自動生成タスクのスケジュールによる開始は、適用される許可ルールの範囲に、安全であることがわかっているフォルダーとファイルのみが含まれる場合に限定して設定してください。

  ネットワークでアプリケーション起動コントロールタスクを使用する前に、すべての保護対象デバイスが共有フォルダーにアクセスできることを確認します。組織のポリシーによりネットワークで共有フォルダーを使用できない場合は、テスト用保護対象デバイスグループの保護対象デバイス上か、または共通ルールを作成する上でベースとなるような参照マシン上でアプリケーション起動コントロールルールの自動生成を開始してください。

- *通知する*モードで実行されているアプリケーション起動コントロールタスクについての、Kaspersky Security Center で生成されたイベントレポートをベースにする。

  このシナリオでは、Kaspersky Embedded Systems Security はアプリケーションの起動を拒否しません。代わりに、［*通知する*］モードでのアプリケーション起動コントロールの実行中、Kaspersky Security Center 管理サーバーフォルダーの作業領域にある［**イベント**］タブで、ネットワークの保護対象デバイス全体で許可および拒否されたすべてのアプリケーション起動が報告されます。Kaspersky Security Center は、レポートを使用して、アプリケーションの起動が拒否されたイベントの1つのリストを生成します。

タスクの実行期間を編集し、指定された期間中に保護対象デバイスおよび保護対象デバイスグループで生じうるすべてのシナリオが実行され、なおかつ再起動が1回以上実施されるようにする必要があります。タスクの実行期間の後で、保存された Kaspersky Security Center のイベントレポート（TXT 形式）からアプリケーション起動のデータをインポートし、このデータに基づいてアプリケーション起動コントロールの許可ルールをそれらのアプリケーションに対して作成できます。

企業ネットワークに用途種別の異なる保護対象デバイス（異なるソフトウェアがインストールされている保護対象デバイス）が多数存在する場合に、このシナリオを使用してください。

- 設定情報ファイルの作成やインポートは行わずに、Kaspersky Security Center を介して受け取った、拒否されたアプリケーション起動イベントをベースにする。

  この機能を使用するには、保護対象デバイス上のアプリケーション起動コントロールタスクが、アクティブな Kaspersky Security Center ポリシーの下で実行されている必要があります。この場合、保護対象デバイス上のすべてのイベントが管理サーバーに送信されます。

ネットワークの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セットが変更された場合、ルールのリストをアップデートしてください（アップデートがインストールされた場合、オペレーティングシステムが再インストールされた場合など）。ルールのリストをアップデートする際には、アプリケーション起動コントロールルールの自動生成タスクまたはアプリケーション起動コントロールタスクを、テスト管理グループの保護対象デバイス上で［*通知する*］モードで実行してください。テストの管理グループには、新しいアプリケーションをネットワークの保護対象デバイスにインストールする前にテスト起動するために必要な保護対象デバイスが含まれます。

許可ルールのリストの XML ファイルは、保護対象デバイスで開始されるタスクの分析を基に作成されます。ルールのリストの作成時にネットワーク上で使用されているすべてのアプリケーションを含めるには、アプリケーション起動コントロールルールの自動生成タスクおよびアプリケーション起動コントロールタスクを、共通ルールを作成する上でベースとなるようなテンプレートマシン上で［*通知する*］モードで開始してください。

参照マシン上で起動されたアプリケーションに基づいて許可ルールを生成する前に、テンプレートマシンがセキュアでマルウェアが存在しないことを確認してください。

許可ルールを追加する前に、利用できるルール適用モードのいずれかを選択します。Kaspersky Security Center ポリシールールのリストには、ルール適用モードに関係なく、ポリシーによって指定されたルールのみが表示されます。ローカルルールのリストには、適用されたすべてのルール（ローカルルールと、ポリシーを介して追加されたルールの両方）が表示されます。

# アプリケーション起動コントロールの有効化と設定

**Kaspersky Security Center 管理コンソールでアプリケーション起動コントロールを有効化して全般的な設定を行う方法**

1. **設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します**。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

c. ［**ポリシー**］タブを選択します。

d. 設定するポリシー名をダブルクリックします。

e. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］をクリックします。

f. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. 同じ名前のチェックボックスを使用して、**アプリケーション起動コントロール**を有効にします。

3. ［**ブロックルールの操作モード**］ブロックで、次を設定します：

- タスク処理モード：
  - **ブロックする**：Kaspersky Embedded Systems Security は、作成されたすべてのアプリケーション起動コントロールルールを適用します。
  - **通知する**：Kaspersky Embedded Systems Security は、アプリケーション起動コントロールルールを使用しません。アプリケーションの起動に関する情報のみを実行ログに記録します。すべてのアプリケーションの起動が許可されます。このモードを使用して、実行ログに記録される拒否されたアプリケーションの起動に関する情報に基づき、アプリケーション起動コントロールルールのリストを生成できます。
- **最初のファイル起動に対する処理を以降のすべての起動に対して繰り返す**
- **実行するコマンドのないコマンドインタープリターの起動を拒否する**

4. ［**ルールの使用範囲**］ブロックで、次を設定します：

- **実行ファイルにルールを適用する**
- **DLL モジュールの読み込みを監視する**

  DLL モジュールの読み込みを監視すると、オペレーティングシステムのパフォーマンスに影響を与えることがあります。

- **スクリプトと MSI パッケージにルールを適用する**

5. ［**証明書の監視**］で、［**証明書の検証時、署名にタイムスタンプがなくても無視する**］機能を有効または無効にします。

6. ［**アプリケーション起動コントロール**］ウィンドウで、［OK］をクリックして変更を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定の変更日時に関する情報と変更前と変更後のタスク設定の値は、システム監査ログに保存されます。

*Kaspersky Embedded Systems Security コンソールでアプリケーション起動コントロールを有効化して全般的な設定を行う方法*

1. コンソールツリーで、［**コンピューターコントロール**］→［**アプリケーション起動コントロール**］セクションを選択します。
2. 結果ペインで［**プロパティ**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。
3. 同じ名前のチェックボックスを使用して、**アプリケーション起動コントロール**を有効にします。
4. ［**ブロックルールの操作モード**］ブロックで、次を設定します：
   - タスク処理モード：
     - **ブロックする**：Kaspersky Embedded Systems Security は、作成されたすべてのアプリケーション起動コントロールルールを適用します。
     - **通知する**：Kaspersky Embedded Systems Security は、アプリケーション起動コントロールルールを使用しません。アプリケーションの起動に関する情報のみを実行ログに記録します。すべてのアプリケーションの起動が許可されます。このモードを使用して、実行ログに記録される拒否されたアプリケーションの起動に関する情報に基づき、アプリケーション起動コントロールルールのリストを生成できます。
   - **最初のファイル起動に対する処理を以降のすべての起動に対して繰り返す**
   - **実行するコマンドのないコマンドインタープリターの起動を拒否する**
5. ［**ルールの使用範囲**］ブロックで、次を設定します：
   - **実行ファイルにルールを適用する**
   - **DLL モジュールの読み込みを監視する**

     DLL モジュールの読み込みを監視すると、オペレーティングシステムのパフォーマンスに影響を与えることがあります。
   - **スクリプトと MSI パッケージにルールを適用する**
6. ［**証明書の監視**］で、［**証明書の検証時、署名にタイムスタンプがなくても無視する**］機能を有効または無効にします。
7. ［**アプリケーション起動コントロール**］ウィンドウで、［OK］をクリックして変更を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定の変更日時に関する情報と変更前と変更後のタスク設定の値は、システム監査ログに保存されます。

### Kaspersky Security Center Web コンソールでアプリケーション起動コントロールを有効化して全般的な設定を行う方法

1. 設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します。

   a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

   b. Kaspersky Embedded Systems 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。

   c. ［**アプリケーション設定**］タブを選択します。

   d. ［**ローカル動作コントロール**］セクションを選択します。

   e. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. 同じ名前のチェックボックスを使用して、**アプリケーション起動コントロール**を有効にします。

3. ［**ブロックルールの操作モード**］ブロックで、次を設定します：

   - タスク処理モード：

     - **ブロックする**：Kaspersky Embedded Systems Security は、作成されたすべてのアプリケーション起動コントロールルールを適用します。

     - **通知する**：Kaspersky Embedded Systems Security は、アプリケーション起動コントロールルールを使用しません。アプリケーションの起動に関する情報のみを実行ログに記録します。すべてのアプリケーションの起動が許可されます。このモードを使用して、実行ログに記録される拒否されたアプリケーションの起動に関する情報に基づき、アプリケーション起動コントロールルールのリストを生成できます。

   - 最初のファイル起動に対する処理を以降のすべての起動に対して繰り返す
   - 実行するコマンドのないコマンドインタープリターの起動を拒否する

4. ［**ルールの使用範囲**］ブロックで、次を設定します：

   - 実行ファイルにルールを適用する
   - DLL モジュールの読み込みを監視する

     DLL モジュールの読み込みを監視すると、オペレーティングシステムのパフォーマンスに影響を与えることがあります。

   - スクリプトと MSI パッケージにルールを適用する

5. ［**証明書の監視**］で、［証明書の検証時、署名にタイムスタンプがなくても無視する］機能を有効または無効にします。

6. ［**アプリケーション起動コントロール**］ウィンドウで、［**OK**］をクリックして変更を保存します。

7. 変更したポリシーを保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定の変更日時に関する情報と変更前と変更後のタスク設定の値は、システム監査ログに保存されます。

# ソフトウェア配布コントロールの設定

### Kaspersky Security Center 管理コンソールでソフトウェア配布コントロールを設定する方法

1. **設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します**。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**ポリシー**］タブを選択します。

   d. 設定するポリシー名をダブルクリックします。

   e. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］をクリックします。

   f. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ソフトウェア配布コントロール**］タブを選択します。

3. ［**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**］機能を有効にします。

   ［**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**］機能は、［**全般**］タブで［**実行ファイルにルールを適用する**］機能が有効になっている場合に、有効にすることができます。

4. 必要に応じて、［**Windows インストーラーによるソフトウェア配布を常に許可する**］機能を無効にします。

   この機能をオフにすると、オペレーティングシステムファイルのアップデートに問題が発生したり、配布パッケージから抽出したファイルを起動できなくなったりする場合があります。

5. 必要に応じて、［**バックグラウンドインテリジェント転送サービスを使用した SCCM によるソフトウェア配布を常に許可する**］機能を有効にします。

パッケージ配布からインストールやアップデートまで、保護対象デバイス上のソフトウェア配布サイクルが管理されます。配信段階のいずれかが保護対象デバイスへの Kaspersky Embedded Systems Security のインストールの前に実行された場合、プロセスは管理されません。

6. 起動を許可する実行ファイルとインストールパッケージを追加します：

- **手動で追加します。**

  a. ［**追加**］ボタンのコンテキストメニューから［**1つの配布パッケージを追加**］を選択します。

  b. 表示されたウィンドウの［**参照**］をクリックします。

  c. 実行ファイルまたは配布パッケージを選択します。

  ［**信頼の基準**］の各フィールドは、選択したファイルに関する情報が自動的に入力されます。

  d. 必要に応じて、［**この配布パッケージの配下のすべてのファイルを信頼済みとして起動を許可する**］機能を有効にします。

  e. 実行ファイルまたはインストールパッケージが信頼できるかどうかを判断する条件として、［**証明書の詳細**］または［**SHA256 ハッシュ**］を選択します。

  f. ［**OK**］をクリックします。

  実行ファイルまたはインストールパッケージがリストに追加されます。

- **ハッシュで複数のパッケージを追加**

  a. ［**追加**］ボタンのコンテキストメニューから［**ハッシュで複数のパッケージを追加**］を選択します。

  b. ウィンドウが表示されるので、そのウィンドウで、任意の数のファイルまたはインストールパッケージを選択します。

  c. ［**開く**］をクリックします。

  実行ファイルまたはインストールパッケージがリストに追加されます。SHA256 ハッシュはそのプロパティで指定されます。

- **ファイルからインポート**

  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、実行ファイルとインストールパッケージに関する情報を含む TXT ファイルを選択します。

  c. ［**開く**］をクリックします。

実行ファイルまたはインストールパッケージがリストに追加されます。SHA256 ハッシュはそのプロパティで指定されます。

実行可能ファイルに基づいて信頼できる配布パッケージを作成し、その同じ実行可能ファイルに基づいて信頼ゾーン設定にプロセスを追加し、アプリケーション起動コントロールに対して信頼できるようにした場合、信頼ゾーン設定の優先順位が高くなります。Kaspersky Embedded Systems Security は、この実行可能ファイルの起動をブロックしますが、実行可能ファイルのプロセスは信頼済みと判断されます。

7. 必要に応じて、［**編集**］をクリックして、追加された実行ファイルとインストールパッケージのリストを編集します。
8. 必要に応じて、［**削除**］をクリックして、追加された実行ファイルとインストールパッケージを削除します。この場合、解凍された実行ファイルを実行できます。

解凍された実行ファイルの実行をブロックするには、保護対象デバイスから Kaspersky Embedded Systems Security を削除するか、解凍されたファイルに対するアプリケーション起動コントロールの拒否ルールを作成する必要があります。

9. ［OK］をクリックします。

***Kaspersky Embedded Systems Security コンソールでソフトウェア配布コントロールを設定する方法***

1. コンソールツリーで、［**コンピューターコントロール**］→［**アプリケーション起動コントロール**］セクションを選択します。
2. 結果ペインで［**プロパティ**］をクリックします。

   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。
3. ［**ソフトウェア配布コントロール**］タブを選択します。
4. ［**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**］機能を有効にします。

［**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**］機能は、［**全般**］タブで［**実行ファイルにルールを適用する**］機能が有効になっている場合に、有効にすることができます。

5. 必要に応じて、［**Windows インストーラーによるソフトウェア配布を常に許可する**］機能を無効にします。

この機能をオフにすると、オペレーティングシステムファイルのアップデートに問題が発生したり、配布パッケージから抽出したファイルを起動できなくなったりする場合があります。

6. 必要に応じて、［**バックグラウンドインテリジェント転送サービスを使用した SCCM によるソフトウェア配布を常に許可する**］機能を有効にします。

パッケージ配布からインストールやアップデートまで、保護対象デバイス上のソフトウェア配布サイクルが管理されます。配信段階のいずれかが保護対象デバイスへの Kaspersky Embedded Systems Security のインストールの前に実行された場合、プロセスは管理されません。

7. 起動を許可する実行ファイルとインストールパッケージを追加します：

- **手動で追加します。**

  a. ［**追加**］ボタンのコンテキストメニューから［**1 つの配布パッケージを追加**］を選択します。

  b. 表示されたウィンドウの［**参照**］をクリックします。

  c. 実行ファイルまたは配布パッケージを選択します。

  ［**信頼の基準**］の各フィールドは、選択したファイルに関する情報が自動的に入力されます。

  d. 必要に応じて、［**この配布パッケージの配下のすべてのファイルを信頼済みとして起動を許可する**］機能を有効にします。

  e. 実行ファイルまたはインストールパッケージが信頼できるかどうかを判断する条件として、［**証明書の詳細**］または［**SHA256 ハッシュ**］を選択します。

  f. ［**OK**］をクリックします。

  実行ファイルまたはインストールパッケージがリストに追加されます。

- **ハッシュで複数のパッケージを追加**

  a. ［**追加**］ボタンのコンテキストメニューから［**ハッシュで複数のパッケージを追加**］を選択します。

  b. ウィンドウが表示されるので、そのウィンドウで、任意の数のファイルまたはインストールパッケージを選択します。

  c. ［**開く**］をクリックします。

  実行ファイルまたはインストールパッケージがリストに追加されます。SHA256 ハッシュはそのプロパティで指定されます。

- **ファイルからインポート**

  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、実行ファイルとインストールパッケージに関する情報を含む TXT ファイルを選択します。

  c. ［**開く**］をクリックします。

  実行ファイルまたはインストールパッケージがリストに追加されます。SHA256 ハッシュはそのプロパティで指定されます。

実行可能ファイルに基づいて信頼できる配布パッケージを作成し、その同じ実行可能ファイルに基づいて信頼ゾーン設定にプロセスを追加し、アプリケーション起動コントロールに対して信頼できるようにした場合、信頼ゾーン設定の優先順位が高くなります。Kaspersky Embedded Systems Security は、この実行可能ファイルの起動をブロックしますが、実行可能ファイルのプロセスは信頼済みと判断されます。

8. 必要に応じて、［**編集**］をクリックして、追加された実行ファイルとインストールパッケージのリストを編集します。
9. 必要に応じて、［**削除**］をクリックして、追加された実行ファイルとインストールパッケージを削除します。この場合、解凍された実行ファイルを実行できます。

解凍された実行ファイルの実行をブロックするには、保護対象デバイスから Kaspersky Embedded Systems Security を削除するか、解凍されたファイルに対するアプリケーション起動コントロールの拒否ルールを作成する必要があります。

10. ［**OK**］をクリックします。

**Kaspersky Security Center Web コンソールでソフトウェア配布コントロールを設定する方法**

1. **設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します**。

   a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

   b. Kaspersky Embedded Systems 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。

   c. ［**アプリケーション設定**］タブを選択します。

   d. ［**ローカル動作コントロール**］セクションを選択します。

   e. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ソフトウェア配布コントロール**］タブを選択します。

3. ［**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**］機能を有効にします。

   ［**リストされたアプリケーションとパッケージのソフトウェア配布を自動的に許可する**］機能は、［**全般**］タブで［**実行ファイルにルールを適用する**］機能が有効になっている場合に、有効にすることができます。

4. 必要に応じて、［**Windows インストーラーによるソフトウェア配布を常に許可する**］機能を無効にします。

   この機能をオフにすると、オペレーティングシステムファイルのアップデートに問題が発生したり、配布パッケージから抽出したファイルを起動できなくなったりする場合があります。

5. 必要に応じて、［**バックグラウンドインテリジェント転送サービスを使用した SCCM によるソフトウェア配布を常に許可する**］機能を有効にします。

   パッケージ配布からインストールやアップデートまで、保護対象デバイス上のソフトウェア配布サイクルが管理されます。配信段階のいずれかが保護対象デバイスへの Kaspersky Embedded Systems Security のインストールの前に実行された場合、プロセスは管理されません。

6. 起動を許可する実行ファイルとインストールパッケージを追加します：

   - **手動**

     a. ［**追加**］をクリックします。

     b. ［**信頼の基準**］で、実行ファイルまたはインストールパッケージが信頼できるかどうかを判断する条件として、［**デジタル証明書を使用する**］または［**SHA256 ハッシュを使用する**］を選択します。

     c. ［**デジタル証明書を使用する**］を選択した場合は、実行ファイルまたはインストールパッケージの署名に使用した証明書のヘッダーとサムプリント、および実行ファイルまたはインストールパッケージの名前を入力します。

     d. ［**SHA256 ハッシュを使用する**］を選択した場合は、［**参照**］をクリックして、実行ファイルまたはインストールパッケージを選択します。

     e. 必要に応じて、［**この配布パッケージの配下のすべてのファイルを信頼済みとして起動を許可する**］機能を有効にします。

     f. ［**OK**］をクリックします。

     実行ファイルまたはインストールパッケージがリストに追加されます。

- **ファイルからインポート**

  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、実行ファイルとインストールパッケージに関する情報を含む TXT ファイルを選択します。

  c. ［**開く**］をクリックします。

  実行ファイルまたはインストールパッケージがリストに追加されます。SHA256 ハッシュはそのプロパティで指定されます。

実行可能ファイルに基づいて信頼できる配布パッケージを作成し、その同じ実行可能ファイルに基づいて信頼ゾーン設定にプロセスを追加し、アプリケーション起動コントロールに対して信頼できるようにした場合、信頼ゾーン設定の優先順位が高くなります。Kaspersky Embedded Systems Security は、この実行可能ファイルの起動をブロックしますが、実行可能ファイルのプロセスは信頼済みと判断されます。

7. 必要に応じて、［**編集**］をクリックして、追加された実行ファイルとインストールパッケージのリストを編集します。
8. 必要に応じて、［**削除**］をクリックして、追加された実行ファイルとインストールパッケージを削除します。この場合、解凍された実行ファイルを実行できます。

   解凍された実行ファイルの実行をブロックするには、保護対象デバイスから Kaspersky Embedded Systems Security を削除するか、解凍されたファイルに対するアプリケーション起動コントロールの拒否ルールを作成する必要があります。

9. ［**OK**］をクリックします。
10. ［**アプリケーション起動コントロール**］ウィンドウの［**OK**］をクリックします。

# アプリケーション起動コントロールルールとの影響関係

このセクションでは、アプリケーション起動コントロールのルールのリストを作成する手順について説明します。

# アプリケーション起動コントロールルールの追加

### Kaspersky Security Center 管理コンソールでアプリケーション起動コントロールルールを追加する方法

1. **設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します**。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**ポリシー**］タブを選択します。

   d. 設定するポリシー名をダブルクリックします。

   e. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］をクリックします。

   f. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ルール**］タブを選択します。

3. ［**ルールの使用**］ドロップダウンリストで、ルール適用モードを選択します：

   - **ローカルルールにポリシールールを追加する**：ポリシーで指定したルールリストをローカルルールリストとともに適用します。
   - **ローカルルールをポリシールールで上書きする**：保護対象デバイスのグループでのアプリケーション起動コントロールを管理するかたちで、ポリシーで指定したルールリストが適用されます。ローカルルールリストは作成、編集、適用できません。

4. 必要に応じて、［**ユーザーによるローカルルールの変更を拒否する**］機能を有効にします。
   この機能が有効になっている場合、アプリケーションコンソールでアプリケーション起動コントロールルールをローカルに編集することはできません。このオプションは既定では無効になっています。

5. 次のいずれかの方法で、アプリケーション起動コントロールルールを追加します：

   - **手動**

     a. ［**追加**］をクリックします。
     ［**アプリケーション起動コントロール**］ウィンドウが表示されます。

     b. ［**名前**］にルール名を入力します。

     c. 必要に応じて、［**説明**］フィールドに、ルールの説明を入力します。

d. ［**種別**］ドロップダウンリストで、ルールの種別を選択します：

- **許可**：ルールによって、ルールで説明されたアプリケーションの実行が許可されます。
- **拒否**：ルールによって、ルールで説明されたアプリケーションの起動がブロックされます。

e. ［**範囲**］ドロップダウンリストで、起動がルールによって制御されるファイルの種別を選択します：

- **実行ファイル**：ルールによって実行ファイルの起動が制御されます。
- **スクリプトと MSI パッケージ**：ルールによってスクリプトと MSI パッケージの起動が制御されます。次の拡張子をもつファイルがサポートされます：.js、.vbs、.cmd、.bat、.py、.ps1、.pl、.msi、.msp、.mst、.com、.vbe、.jse、.psd1、.psm1、

f. ルールを適用する条件に合致するアプリケーションを信頼するアップデーターとして認識するよう設定する場合は、［**信頼するアップデーター**］をオンにします。信頼するアップデーターとは、実行ファイルの作成とそのファイルの実行が許可されているアプリケーションです。

アプリケーションが複数のルールの適用条件に一致する場合、Kaspersky Embedded Systems Security は次の条件を満たす場合に「*信頼するアップデーター*」フラグを作成します：

- すべてのルールでアプリケーションの実行が許可されている。
- ルールのうち少なくとも 1 つで［**信頼するアップデーター**］がオンになっている。

g. アプリケーション起動コントロールルールの適用条件を追加します。

h. アプリケーション起動コントロールルールの適用条件から除外する項目を追加します。

i. **ルールを満たすアプリケーションの起動を許可または禁止するユーザーまたはユーザーグループを追加します**。

a. ［**ユーザーまたはグループ**］タブを選択します。

b. ［**追加**］のコンテキストメニューで、ユーザーまたはグループを追加する方法を選択します。

c. ウィンドウが表示されるので、そのウィンドウで、ユーザーまたはユーザーグループの名前を入力または選択します。

d. ［OK］をクリックします。

e. ユーザーまたはユーザーグループごとに手順 b ～ d を実行します。

j. ［OK］をクリックします。

- **アプリケーション起動コントロールルールを含む XML ファイルをインポートする**

  a. のコンテキストメニューで、［**インポート**］→［**XML ファイルから**］の順に選択します。

  b. XML ファイルからデバイスコントロールルールをポリシーで使用可能なルールに追加する方法を選択します：

  - **既存のルールを置き換える**：既存のルールをインポートされたルールで置き換えます。
  - **既存のルールに追加する**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
  - **既存のルールとマージする**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。少なくとも 1 つのルール設定が一意である場合、ルールが追加されます。

  c. 表示されたウィンドウで、アプリケーション起動コントロールルールの自動生成のローカルタスクまたはグループタスクの完了後に作成される XML ファイルへのパスを指定します。

  d. ［**開く**］をクリックします。

- **リクエストを使用して、Kaspersky Security Center イベントに基づいて作成する**

  a. のコンテキストメニューで、［**インポート**］→［**Kaspersky Security Center イベントにもどづいて許可ルールを作成（リクエスト）**］の順に選択します。

  b. ルールを以前作成されたアプリケーション起動コントロールルールのリストに追加する方法を選択します：

  - **既存のルールに追加する**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
  - **既存のルールを置き換える**：既存のルールをインポートされたルールで置き換えます。
  - **既存のルールとマージする**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは追加されません。少なくとも 1 つのルールパラメータが他のルールと異なる場合にルールが追加されます。

  ［**アプリケーション起動コントロールルール生成**］ウィンドウが表示されます。

  c. イベント種別を、本製品が作成するアプリケーション起動コントロールルールに基づいて選択します：

  - **アプリケーションの起動が拒否されました**
  - **統計のみモード：アプリケーションの起動が拒否されました**

  d. ［**期間内に生成された要求イベント**］ドロップダウンリストから期間を選択します。

e. ［**ルール生成時のハッシュの使用を優先する**］をオフまたはオンにします。

このチェックボックスをオンにすると、Kaspersky Embedded Systems Security は、ファイルのチェックサムと証明書の両方が使用可能な場合に、ファイルのチェックサムを使用してルールを生成します。

このチェックボックスをオフにすると、Kaspersky Embedded Systems Security は、ファイルのチェックサムと証明書の両方が使用可能な場合に、ファイルのデジタル証明書を使用してルールを生成します。

f. ［**ルールの生成**］をクリックします。

g. ［OK］をクリックします。

- Kaspersky Security Center のブロック対象のアプリケーションのイベントの抽出を含む TXT ファイルをインポートする

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**ポリシー**］タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. ポリシーのプロパティウィンドウで、［**ログと通知**］をクリックします。
6. ［**実行ログ**］ブロックの［**設定**］をクリックします。
   ［**通知**］ウィンドウが表示されます。
7. ［**ローカル動作コントロール**］フォルダーを展開します。
8. ［**アプリケーション起動コントロール**］セクションを選択します。
9. アプリケーション起動コントロールイベントのリストの［**イベントを Kaspersky Security Center に送信**］列で、［*アプリケーションの起動が禁止されました*］および［*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*］の横にあるチェックボックスをオンにします。
10. 変更内容を保存します。
11. ポリシーの［**イベントの設定**］セクションで、［**管理サーバーのデータベースに保存（日）**］フィールドに指定されたイベントの保存期間が、ブロック対象のアプリケーションの起動に関する情報を収集する予定の期間（既定は 30 日）よりも長いことを確認します。

    アプリケーション起動コントロールのタスクログの保管期間が終了すると、ログに記録されたイベントは削除され、レポートに表示されなくなります。

12. 拒否されたアプリケーションの起動に関するデータを収集するように設定されたポリシーを有効にします。

13. 必要に応じて、アプリケーション起動コントロールのモードを変更します。

14. ブロック対象のアプリケーションの起動に関する情報を収集する期間が終了したら、［*アプリケーションの起動が禁止されました*］および［*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*］のイベントから抽出を行い、TXT ファイルにエクスポートします。詳細については、*Kaspersky Security Center* のヘルプの「イベントの抽出」のセクションを参照してください。

15. エクスポートされた TXT ファイルを開きます。

16. 必要に応じて、イベントのリストを編集します。

ブロック対象のアプリケーションのデータをインポートする前に、インポートするリストに、許可するアプリケーションのみが含まれており、それ以外は含まれていないことを確認してください。

a. のコンテキストメニューで、［**インポート**］→［**選択した Kaspersky Security Center のイベントの TXT ファイルに基づいて許可ルールを作成**］の順に選択します。

b. レポートから、ポリシーで既に使用可能なルールのリストにアプリケーション起動コントロールルールを追加する方法を選択します：

- **既存のルールとマージする**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。少なくとも 1 つのルール設定が一意である場合、ルールが追加されます。
- **既存のルールに追加する**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
- **既存のルールを置き換える**：既存のルールをインポートされたルールで置き換えます。

c. 表示される Windows システムウィンドウで、ブロック対象デバイスに関する Kaspersky Security Center レポートのイベントがエクスポートされた TXT ファイルへのパスを指定します。

d. ［**開く**］をクリックします。

追加されたアプリケーション起動コントロールルールがリストに表示されます。

6. 必要に応じて、手順 5 を実行して、アプリケーション起動コントロールルールをさらに追加します。

7. 必要に応じて、［**編集**］をクリックして、追加されたアプリケーション起動コントロールルールを編集します。

8. 必要に応じて、［**削除**］をクリックして、追加されたアプリケーション起動コントロールルールを削除します。

9. ［**OK**］をクリックします。

*Kaspersky Embedded Systems Security コンソールでアプリケーション起動コントロールルールを追加する方法*

1. コンソールツリーで、［**コンピューターコントロール**］→［**アプリケーション起動コントロール**］セクションを選択します。
2. 結果ペインで［**プロパティ**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。
3. ［**ルール**］タブを選択します。
4. 次のいずれかの方法で、アプリケーション起動コントロールルールを追加します：

- **手動**

  a. ［**追加**］をクリックします。
  ［**アプリケーション起動コントロール**］ウィンドウが表示されます。

  b. ［**名前**］にルール名を入力します。

  c. 必要に応じて、［**説明**］フィールドに、ルールの説明を入力します。

  d. ［**種別**］ドロップダウンリストで、ルールの種別を選択します：

  - **許可**：ルールによって、ルールで説明されたアプリケーションの実行が許可されます。
  - **拒否**：ルールによって、ルールで説明されたアプリケーションの起動がブロックされます。

  e. ［**範囲**］ドロップダウンリストで、起動がルールによって制御されるファイルの種別を選択します：

  - **実行ファイル**：ルールによって実行ファイルの起動が制御されます。
  - **スクリプトと MSI パッケージ**：ルールによってスクリプトと MSI パッケージの起動が制御されます。次の拡張子をもつファイルがサポートされます：.js、.vbs、.cmd、.bat、.py、.ps1、.pl、.msi、.msp、.mst、.com、.vbe、.jse、.psd1、.psm1、

  f. ルールを適用する条件に合致するアプリケーションを信頼するアップデーターとして認識するよう設定する場合は、［**信頼するアップデーター**］をオンにします。信頼するアップデーターとは、実行ファイルの作成とそのファイルの実行が許可されているアプリケーションです。
  アプリケーションが複数のルールの適用条件に一致する場合、Kaspersky Embedded Systems Security は次の条件を満たす場合に「*信頼するアップデーター*」フラグを作成します：

  - すべてのルールでアプリケーションの実行が許可されている。
  - ルールのうち少なくとも 1 つで［**信頼するアップデーター**］がオンになっている。

  g. アプリケーション起動コントロールルールの適用条件を追加します。

  h. アプリケーション起動コントロールルールの適用条件から除外する項目を追加します。

i. **ルールを満たすアプリケーションの起動を許可または禁止するユーザーまたはユーザーグループを追加します**。

a. ［**ユーザーまたはグループ**］タブを選択します。

b. ［**追加**］のコンテキストメニューで、ユーザーまたはグループを追加する方法を選択します。

c. ウィンドウが表示されるので、そのウィンドウで、ユーザーまたはユーザーグループの名前を入力または選択します。

d. ［**OK**］をクリックします。

e. ユーザーまたはユーザーグループごとに手順 b ～ d を実行します。

j. ［**OK**］をクリックします。

- **アプリケーション起動コントロールルールを含む XML ファイルをインポートする**

a. のコンテキストメニューで、［**インポート**］→［**XML ファイルから**］の順に選択します。

b. XML ファイルからデバイスコントロールルールをポリシーで使用可能なルールに追加する方法を選択します：

- **既存のルールを置き換える**：既存のルールをインポートされたルールで置き換えます。
- **既存のルールに追加する**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
- **既存のルールとマージする**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。少なくとも 1 つのルール設定が一意である場合、ルールが追加されます。

c. 表示されたウィンドウで、アプリケーション起動コントロールルールの自動生成のローカルタスクまたはグループタスクの完了後に作成される XML ファイルへのパスを指定します。

d. ［**開く**］をクリックします。

追加されたアプリケーション起動コントロールルールがリストに表示されます。

5. 必要に応じて、手順 5 を実行して、アプリケーション起動コントロールルールをさらに追加します。
6. 必要に応じて、［**編集**］をクリックして、追加されたアプリケーション起動コントロールルールを編集します。
7. 必要に応じて、［**削除**］をクリックして、追加されたアプリケーション起動コントロールルールを削除します。
8. ［**OK**］をクリックします。

### Kaspersky Security Center Web コンソールでアプリケーション起動コントロールルールを追加する方法

1. 設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します。

   a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

   b. Kaspersky Embedded Systems 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。

   c. ［**アプリケーション設定**］タブを選択します。

   d. ［**ローカル動作コントロール**］セクションを選択します。

   e. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ルール**］タブを選択します。

3. ［**ルールの適用**］ドロップダウンリストで、ルール適用モードを選択します：

   - **ローカルルールにポリシールールを追加する**：ポリシーで指定したルールリストをローカルルールリストとともに適用します。
   - **ローカルルールをポリシールールで上書きする**：保護対象デバイスのグループでのアプリケーション起動コントロールを管理するかたちで、ポリシーで指定したルールリストが適用されます。ローカルルールリストは作成、編集、適用できません。

4. 必要に応じて、［**ユーザーによるローカルルールの変更を拒否する**］機能を有効にします。

5. 次のいずれかの方法で、アプリケーション起動コントロールルールを追加します：

   - 手動

     a. ［**追加**］をクリックします。
     ［**ルール設定**］ウィンドウが表示されます。

     b. ［**名前**］にルール名を入力します。

     c. ［**種別**］ドロップダウンリストで、ルールの種別を選択します：

     - **許可**：ルールによって、ルールで説明されたアプリケーションの実行が許可されます。
     - **拒否**：ルールによって、ルールで説明されたアプリケーションの起動がブロックされます。

d. ［**範囲**］ドロップダウンリストで、起動がルールによって制御されるファイルの種別を選択します：

- **実行ファイル**：ルールによって実行ファイルの起動が制御されます。
- **スクリプトと MSI パッケージ**：ルールによってスクリプトと MSI パッケージの起動が制御されます。

e. ［**ユーザーまたはグループ**］タブにリストされていないすべてのユーザーに対して、ルールで説明されたアプリケーションの起動をブロックする場合は、［**他のユーザーを拒否**］をオンにします。

f. ルールを適用する条件に合致するアプリケーションを信頼するアップデーターとして認識するよう設定する場合は、［**信頼するアップデーター**］をオンにします。信頼するアップデーターとは、実行ファイルの作成とそのファイルの実行が許可されているアプリケーションです。

アプリケーションが複数のルールの適用条件に一致する場合、Kaspersky Embedded Systems Security は次の条件を満たす場合に「*信頼するアップデーター*」フラグを作成します：

- すべてのルールでアプリケーションの実行が許可されている。
- ルールのうち少なくとも 1 つで［**信頼するアップデーター**］がオンになっている。

g. アプリケーション起動コントロールルールの適用条件を追加します。

h. アプリケーション起動コントロールルールの適用条件から除外する項目を追加します。

i. **ルールを満たすアプリケーションの起動を許可または禁止するユーザーまたはユーザーグループを追加します**。

a. ［**ユーザーまたはグループ**］タブを選択します。

b. ［**追加**］をクリックします。

c. ウィンドウが表示されるので、そのウィンドウで、ユーザーまたはユーザーグループの名前を入力または選択します。

d. ［**選択**］をクリックします。

e. ユーザーまたはユーザーグループごとに手順 b ～ d を実行します。

j. ［OK］をクリックします。

追加されたアプリケーション起動コントロールルールがリストに表示されます。

- **アプリケーション起動コントロールルールを含む XML ファイルをインポートする**

a. ［**インポート**］をクリックします。

b. 表示された［**ファイルからインポート**］ウィンドウで、［**選択**］をクリックします。

c. アプリケーション起動コントロールルールの自動生成のローカルタスクまたはグループタスクの完了後に作成される XML ファイルへのパスを指定します。

d. ［**開く**］をクリックします。

e. ［**インポート**］をクリックします。

インポートされたアプリケーション起動コントロールルールが既存のルールのリストに追加されます。同一の設定を持つルールは重複します。少なくとも 1 つのルール設定が一意である場合、ルールが追加されます。

- **Kaspersky Embedded Systems Security 4.0 のアプリケーション起動コントロールルールを含む XML ファイルをインポートする**

a. ［**以前のバージョンからインポートする**］をクリックします。

b. 表示された［**ファイルからインポート**］ウィンドウで、［**選択**］をクリックします。

c. Kaspersky Embedded Systems Security 4.0 からエクスポートされたアプリケーション起動コントロールルールを含む XML ファイルへのパスを指定します。

d. ［**開く**］をクリックします。

e. ［**インポート**］をクリックします。

インポートされたアプリケーション起動コントロールルールが既存のルールのリストに追加されます。同一の設定を持つルールは重複します。少なくとも 1 つのルール設定が一意である場合、ルールが追加されます。

- **Kaspersky Security Center のレポートファイルからルールをインポートする**

a. ［**KSC レポートからインポートする**］をクリックします。

b. 表示されたウィンドウで、レポートのイベントがエクスポートされた TXT ファイルを選択します。

c. ［**開く**］をクリックします。

Kaspersky Security Center のレポートに基づくルールが、ポリシー内のルールのリストに追加されます。

- **リクエストを使用して、Kaspersky Security Center イベントに基づいて作成する**

a. ［**KSC イベントからのルールの許可**］をクリックします。
［**アプリケーション起動コントロールルールの自動生成**］ウィンドウが表示されます。

b. イベント種別を、本製品が作成するアプリケーション起動コントロールルールに基づいて選択します：

- **すべてのイベント**
- **アプリケーションの起動が拒否されました**
- **統計のみモード：アプリケーションの起動が拒否されました**

c. ［**期間内に生成されたイベントを使用する**］ドロップダウンリストから期間を選択します。

d. ［**ルール生成時のハッシュの使用を優先する**］をオフまたはオンにします。

このチェックボックスをオンにすると、Kaspersky Embedded Systems Security は、ファイルのチェックサムと証明書の両方が使用可能な場合に、ファイルのチェックサムを使用してルールを生成します。

このチェックボックスをオフにすると、Kaspersky Embedded Systems Security は、ファイルのチェックサムと証明書の両方が使用可能な場合に、ファイルのデジタル証明書を使用してルールを生成します。

e. 必要に応じて、［**管理対象デバイスのグループ用に生成されたイベントを使用する**］フィールドで管理対象デバイスのグループの名前を指定します。

f. ［**ルールの生成**］をクリックします。

g. ［**メインのリストに追加するルール**］ドロップダウンリストから、ルールを以前作成されたアプリケーション起動コントロールルールのリストに追加する方法を選択します：

- **既存のルールに追加する**：インポートされたルールを既存のルールのリストに追加します。同一の設定を持つルールは重複します。
- **既存のルールを置き換える**：既存のルールをインポートされたルールで置き換えます。

h. ポリシーのアプリケーション起動コントロールルールにエクスポートするルールを選択し、［**エクスポート**］をクリックします。

i. 変更内容を保存します。

6. 必要に応じて、手順 5 を実行して、アプリケーション起動コントロールルールをさらに追加します。
7. 必要に応じて、［**編集**］をクリックして、追加されたアプリケーション起動コントロールルールを編集します。
8. 必要に応じて、［**削除**］をクリックして、追加されたアプリケーション起動コントロールルールを削除します。
9. ［**OK**］をクリックします。

# アプリケーション起動コントロールルールの適用条件の追加

**Kaspersky Security Center 管理コンソールでアプリケーション起動コントロールルールの適用条件を追加する方法**

1. 設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**ポリシー**］タブを選択します。

   d. 設定するポリシー名をダブルクリックします。

   e. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］をクリックします。

   f. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ルール**］タブを選択します。

3. 次のいずれかを行います：

   a. 新しいアプリケーション起動コントロールルールを追加する場合は、［**追加**］をクリックします。

   b. アプリケーション起動コントロールルールのリストで、適用条件を追加するルールを選択し、［**編集**］をクリックします。

   ［**アプリケーション起動コントロール**］ウィンドウが表示されます。

4. ［**条件**］タブの［**追加**］のコンテキストメニューで、アプリケーション起動コントロールルールの適用条件を選択します：

   - **ファイルからの情報**：選択したファイルからの情報がルールの適用条件として使用されます。

     a. ［**ファイルからの情報**］ウィンドウの［**参照**］をクリックします。
     Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが表示されます。

     b. ファイルを選択します。

     c. ［**開く**］をクリックします。
     選択したファイルに関する情報が［**ファイルからの情報**］ウィンドウに表示されます。

d. オプションを少なくとも1つオンにしてください：

- **証明書の詳細**：このチェックボックスをオンにすると、ルールによって、指定されたデータを持つデジタル証明書で署名されたアプリケーションの起動が制御されません。
- **メタデータ**：このチェックボックスをオンにすると、ルールによって、指定されたメタデータを持つアプリケーションの起動が制御されません。
- **ファイルのハッシュ**：このチェックボックスをオンにすると、ルールによって、指定された SHA256 ハッシュを持つアプリケーションの起動が制御されません。
- **ファイルのパス**：このチェックボックスをオンにすると、ルールによって、指定されたパスのアプリケーションの起動が制御されません。

e. 必要に応じて、［**コマンドライン**］フィールドに、コマンドラインでアプリケーションを起動するためのコマンドを入力します。ルールによって、そのアプリケーションの起動が制御されます。マスクを入力する場合は、「?」と「*」の文字を使用できます。

> Kaspersky Embedded Systems Security は、スラッシュ「/」を含むパスを認識しません。パスにはバックスラッシュ「\」を使用してください。

f. ［OK］をクリックします。

- **ドライブの種別**：ルールによって、保護されたコンピューターに接続されているすべてのリムーバブルドライブからのアプリケーションの起動が制御されます。
- **KL カテゴリ**：ルールによって、選択した KL カテゴリに属するアプリケーションの起動が制御されます。
- **KSN により信頼されている**：ルールによって、KSN で信頼されているアプリケーションの起動が制御されます。
- **KSN により信頼されていない**：ルールによって、KSN で信頼されていないアプリケーションの起動が制御されます。
- **OS により信頼されている**：ルールによって、オペレーティングシステムで信頼されているアプリケーションの起動が制御されます。

追加した条件がリストに表示されます。

5. 必要に応じて、後続のルールを適用する条件のそれぞれで、この手順の前のステップを実行します。
6. 必要に応じて、［**編集**］をクリックして、ルールを適用する条件を編集します。
7. 変更内容を保存します。

*Kaspersky Embedded Systems Security コンソールでアプリケーション起動コントロールルールの適用条件を追加する方法*

1. コンソールツリーで、［**コンピューターコントロール**］→［**アプリケーション起動コントロール**］セクションを選択します。
2. 結果ペインで［**プロパティ**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。
3. ［**ルール**］タブを選択します。
4. 次のいずれかを行います：
   a. 新しいアプリケーション起動コントロールルールを追加する場合は、［**追加**］をクリックします。
   b. アプリケーション起動コントロールルールのリストで、適用条件を追加するルールを選択し、［**編集**］をクリックします。

   ［**アプリケーション起動コントロール**］ウィンドウが表示されます。
5. ［**条件**］タブの［**追加**］のコンテキストメニューで、アプリケーション起動コントロールルールの適用条件を選択します：
   - **ファイルからの情報**：**選択したファイルからの情報**がルールの適用条件として使用されます。

     a. ［**ファイルからの情報**］ウィンドウの［**参照**］をクリックします。
     Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが表示されます。

     b. ファイルを選択します。

     c. ［**開く**］をクリックします。
     選択したファイルに関する情報が［**ファイルからの情報**］ウィンドウに表示されます。

     d. オプションを少なくとも 1 つオンにしてください：

     - **証明書の詳細**：このチェックボックスをオンにすると、ルールによって、指定されたデータを持つデジタル証明書で署名されたアプリケーションの起動が制御されません。
     - **メタデータ**：このチェックボックスをオンにすると、ルールによって、指定されたメタデータを持つアプリケーションの起動が制御されません。
     - **ファイルのハッシュ**：このチェックボックスをオンにすると、ルールによって、指定された SHA256 ハッシュを持つアプリケーションの起動が制御されません。
     - **ファイルのパス**：このチェックボックスをオンにすると、ルールによって、指定されたパスのアプリケーションの起動が制御されません。

e. 必要に応じて、［**コマンドライン**］フィールドに、コマンドラインでアプリケーションを起動するためのコマンドを入力します。ルールによって、そのアプリケーションの起動が制御されます。マスクを入力する場合は、「?」と「*」の文字を使用できます。

> Kaspersky Embedded Systems Security は、スラッシュ「/」を含むパスを認識しません。パスにはバックスラッシュ「\」を使用してください。

f. ［**OK**］をクリックします。

- **ドライブの種別**：ルールによって、保護されたコンピューターに接続されているすべてのリムーバブルドライブからのアプリケーションの起動が制御されます。
- **KL カテゴリ**：ルールによって、選択した KL カテゴリに属するアプリケーションの起動が制御されます。
- **KSN により信頼されている**：ルールによって、KSN で信頼されているアプリケーションの起動が制御されます。
- **KSN により信頼されていない**：ルールによって、KSN で信頼されていないアプリケーションの起動が制御されます。
- **OS により信頼されている**：ルールによって、オペレーティングシステムで信頼されているアプリケーションの起動が制御されます。

追加した条件がリストに表示されます。

6. 必要に応じて、後続のルールを適用する条件のそれぞれで、この手順の前のステップを実行します。
7. 必要に応じて、［**編集**］をクリックして、ルールを適用する条件を編集します。
8. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでアプリケーション起動コントロールルールの適用条件を追加する方法

1. **設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します**。

a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

b. Kaspersky Embedded Systems 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。

c. ［**アプリケーション設定**］タブを選択します。

d. ［**ローカル動作コントロール**］セクションを選択します。

e. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ルール**］タブを選択します。

3. ［**追加**］をクリックします。
［**ルール設定**］ウィンドウが表示されます。

4. ［**条件**］タブで［**追加**］をクリックします。
［**ルール設定**］ウィンドウが表示されます。

5. アプリケーション起動コントロールルールの適用条件を選択します：

- **ファイルからの情報**：**ファイルからの情報**がルールの適用条件として使用されます。

  a. ［**ルールの適用条件**］で、少なくとも1つの条件の値を指定します：

  - **デジタル証明書**：このチェックボックスをオンにすると、ルールによって、指定されたデータを持つデジタル証明書で署名されたアプリケーションの起動が制御されません。
  - **メタデータ**：このチェックボックスをオンにすると、ルールによって、指定されたメタデータを持つアプリケーションの起動が制御されません。
  - **SHA256 ハッシュ**：このチェックボックスをオンにすると、ルールによって、指定されたSHA256ハッシュを持つアプリケーションの起動が制御されません。
  - **ファイルのパス**：このチェックボックスをオンにすると、ルールによって、指定されたパスのアプリケーションの起動が制御されません。

  b. ［**OK**］をクリックします。

- **KL カテゴリから**：ルールによって、選択したKLカテゴリに属するアプリケーションの起動が制御されます。
- **リムーバブルドライブ**：ルールによって、保護されたコンピューターに接続されているすべてのリムーバブルドライブからのアプリケーションの起動が制御されます。
- **OS により信頼されている**：ルールによって、オペレーティングシステムで信頼されているアプリケーションの起動が制御されます。

追加した条件がリストに表示されます。

6. 必要に応じて、後続のルールを適用する条件のそれぞれで、この手順のステップ4～5を実行します。

7. 必要に応じて、［**編集**］をクリックして、ルールを適用する条件を編集します。

8. 変更内容を保存します。

# アプリケーション起動コントロールルールの範囲から除外する項目の追加

**Kaspersky Security Center 管理コンソールでアプリケーション起動コントロールルールの範囲から除外する項目を追加する方法**

1. 設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**ポリシー**］タブを選択します。

   d. 設定するポリシー名をダブルクリックします。

   e. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］をクリックします。

   f. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ルール**］タブを選択します。

3. 次のいずれかを行います：

   a. 新しいアプリケーション起動コントロールルールを追加する場合は、［**追加**］をクリックします。

   b. アプリケーション起動コントロールルールのリストで、除外項目を追加するルールを選択し、［**編集**］をクリックします。

   ［**アプリケーション起動コントロール**］ウィンドウが表示されます。

4. ［**除外リスト**］タブの［**追加**］のコンテキストメニューで、アプリケーション起動コントロールルールの範囲から除外する項目を作成するための条件を選択します：

   - **ファイルからの情報**：選択したファイルからの情報が条件として使用されます。

     a. ［**ファイルからの情報**］ウィンドウの［**参照**］をクリックします。
     Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが表示されます。

     b. ファイルを選択します。

     c. ［**開く**］をクリックします。
     選択したファイルに関する情報が［**ファイルからの情報**］ウィンドウに表示されます。

d. オプションを少なくとも1つオンにしてください：

- **証明書の詳細**：このチェックボックスをオンにすると、ルールによって、指定されたデータを持つデジタル証明書で署名されたアプリケーションの起動が制御されません。
- **メタデータ**：このチェックボックスをオンにすると、ルールによって、指定されたメタデータを持つアプリケーションの起動が制御されません。
- **ファイルのハッシュ**：このチェックボックスをオンにすると、ルールによって、指定された SHA256 ハッシュを持つアプリケーションの起動が制御されません。
- **ファイルのパス**：このチェックボックスをオンにすると、ルールによって、指定されたパスのアプリケーションの起動が制御されません。

e. 必要に応じて、［**コマンドライン**］フィールドに、コマンドラインでアプリケーションを起動するためのコマンドを入力します。ルールによって、そのアプリケーションの起動が制御されません。マスクを入力する場合は、「?」と「*」の文字を使用できます。

> Kaspersky Embedded Systems Security は、スラッシュ「/」を含むパスを認識しません。パスにはバックスラッシュ「\」を使用してください。

f. ［OK］をクリックします。

- **ドライブの種別**：ルールによって、保護されたコンピューターに接続されているすべてのリムーバブルドライブからのアプリケーションの起動が制御されません。
- **KL カテゴリ**：ルールによって、選択した KL カテゴリに属するアプリケーションの起動が制御されません。
- **KSN により信頼されている**：ルールによって、KSN で信頼されているアプリケーションの起動が制御されません。
- **KSN により信頼されていない**：ルールによって、KSN で信頼されていないアプリケーションの起動が制御されません。
- **OS により信頼されている**：ルールによって、オペレーティングシステムで信頼されているアプリケーションの起動が制御されません。

追加した除外項目がリストに表示されます。

5. 必要に応じて、この手順の前のステップを実行して、アプリケーション起動コントロールルールの範囲から除外する後続の各項目を追加します。
6. 必要に応じて、［**編集**］をクリックして、除外項目を編集します。
7. 変更内容を保存します。

*Kaspersky Embedded Systems Security コンソールでアプリケーション起動コントロールルールの範囲から除外する項目を追加する方法*

1. コンソールツリーで、［**コンピューターコントロール**］→［**アプリケーション起動コントロール**］セクションを選択します。
2. 結果ペインで［**プロパティ**］をクリックします。
   ［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。
3. ［**ルール**］タブを選択します。
4. 次のいずれかを行います：
   a. 新しいアプリケーション起動コントロールルールを追加する場合は、［**追加**］をクリックします。
   b. アプリケーション起動コントロールルールのリストで、除外項目を追加するルールを選択し、［**編集**］をクリックします。

   ［**アプリケーション起動コントロール**］ウィンドウが表示されます。
5. ［**除外リスト**］タブの［**追加**］のコンテキストメニューで、アプリケーション起動コントロールルールの範囲から除外する項目を作成するための条件を選択します：
   - **ファイルからの情報**：**選択したファイルからの情報**が条件として使用されます。

     a. ［**ファイルからの情報**］ウィンドウの［**参照**］をクリックします。
     Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが表示されます。

     b. ファイルを選択します。

     c. ［**開く**］をクリックします。
     選択したファイルに関する情報が［**ファイルからの情報**］ウィンドウに表示されます。

     d. オプションを少なくとも 1 つオンにしてください：

     - **証明書の詳細**：このチェックボックスをオンにすると、ルールによって、指定されたデータを持つデジタル証明書で署名されたアプリケーションの起動が制御されません。
     - **メタデータ**：このチェックボックスをオンにすると、ルールによって、指定されたメタデータを持つアプリケーションの起動が制御されません。
     - **ファイルのハッシュ**：このチェックボックスをオンにすると、ルールによって、指定された SHA256 ハッシュを持つアプリケーションの起動が制御されません。
     - **ファイルのパス**：このチェックボックスをオンにすると、ルールによって、指定されたパスのアプリケーションの起動が制御されません。

e. 必要に応じて、［**コマンドライン**］フィールドに、コマンドラインでアプリケーションを起動するためのコマンドを入力します。ルールによって、そのアプリケーションの起動が制御されません。マスクを入力する場合は、「?」と「*」の文字を使用できます。

> Kaspersky Embedded Systems Security は、スラッシュ「/」を含むパスを認識しません。パスにはバックスラッシュ「\」を使用してください。

f. ［OK］をクリックします。

- **ドライブの種別**：ルールによって、保護されたコンピューターに接続されているすべてのリムーバブルドライブからのアプリケーションの起動が制御されません。
- **KL カテゴリ**：ルールによって、選択した KL カテゴリに属するアプリケーションの起動が制御されません。
- **KSN により信頼されている**：ルールによって、KSN で信頼されているアプリケーションの起動が制御されません。
- **KSN により信頼されていない**：ルールによって、KSN で信頼されていないアプリケーションの起動が制御されません。
- **OS により信頼されている**：ルールによって、オペレーティングシステムで信頼されているアプリケーションの起動が制御されません。

追加した除外項目がリストに表示されます。

6. 必要に応じて、この手順の前のステップを実行して、アプリケーション起動コントロールルールの範囲から除外する後続の各項目を追加します。
7. 必要に応じて、［**編集**］をクリックして、除外項目を編集します。
8. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでアプリケーション起動コントロールルールの範囲から除外する項目を追加する方法

1. 設定するポリシーのアプリケーション起動コントロールの設定の設定に移動します。

a. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

b. Kaspersky Embedded Systems 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。

c. ［**アプリケーション設定**］タブを選択します。

d. ［**ローカル動作コントロール**］セクションを選択します。

e. ［**アプリケーション起動コントロール**］ブロックの［**設定**］をクリックします。
［**アプリケーション起動コントロール**］ウィンドウが開き、［**全般**］タブが表示されます。

2. ［**ルール**］タブを選択します。

3. ［**追加**］をクリックします。
［**ルール設定**］ウィンドウが表示されます。

4. ［**除外リスト**］タブで［**追加**］をクリックします。
［**ルール設定**］ウィンドウが表示されます。

5. アプリケーション起動コントロールルールの範囲から除外する項目を作成するための基準を選択します：

- **ファイルからの情報**：このルールによって、**ファイル内のデータ**に一致するデータを持つアプリケーションの起動が制御されることはありません。

  a. ［**ルールの適用条件**］で、少なくとも1つの条件の値を指定します：

  - **デジタル証明書**：このチェックボックスをオンにすると、ルールによって、指定されたデータを持つデジタル証明書で署名されたアプリケーションの起動が制御されません。
  - **メタデータ**：このチェックボックスをオンにすると、ルールによって、指定されたメタデータを持つアプリケーションの起動が制御されません。
  - **SHA256 ハッシュ**：このチェックボックスをオンにすると、ルールによって、指定された SHA256 ハッシュを持つアプリケーションの起動が制御されません。
  - **ファイルのパス**：このチェックボックスをオンにすると、ルールによって、指定されたパスのアプリケーションの起動が制御されません。

  b. ［OK］をクリックします。

- **KL カテゴリ**：ルールによって、選択した KL カテゴリに属するアプリケーションの起動が制御されません。
- **ドライブの種別**：ルールによって、保護されたコンピューターに接続されているすべてのリムーバブルドライブからのアプリケーションの起動が制御されません。
- **OS により信頼されている**：ルールによって、オペレーティングシステムで信頼されているアプリケーションの起動が制御されません。

追加した条件がリストに表示されます。

6. 必要に応じて、この手順のステップ 4 ～ 5 を実行して、アプリケーション起動コントロールルールの範囲から除外する後続の各項目を追加します。

7. 必要に応じて、［**編集**］をクリックして、除外項目を編集します。

8. 変更内容を保存します。

# 「既定で許可」モードを有効にする

特別に設定されたアプリケーション起動コントロールの許可ルールを使用して、すべてのアプリケーションの起動を許可できます。

*すべてのアプリケーションの起動を許可するには：*

1. 次のパラメータが指定された 2 つのアプリケーション起動コントロールの許可ルールを手動で追加します：
   - ルール種別：*許可*、範囲：*実行ファイル*、ファイルのパス：`?:\`
   - ルール種別：*許可*、範囲：*スクリプトと MSI パッケージ*、ファイルのパス：`?:\`
2. アプリケーション起動コントロールの拒否ルールが追加されている場合は、これらの拒否ルールを削除します。
3. 以前に作成したすべてのアプリケーション起動コントロールの許可ルールの除外項目を削除します。
4. 変更内容を保存します。

# Kaspersky Security Center のブロック対象のアプリケーションのイベントの抽出を含む TXT ファイルの生成

Kaspersky Security Center のブロック対象のアプリケーションのイベントの抽出を TXT ファイルにエクスポートし、このデータをインポートして、設定しているポリシーにアプリケーション起動コントロールの許可ルールのリストを生成することができます。

***Kaspersky Security Center 管理コンソールを使用して Kaspersky Security Center のブロック対象のアプリケーションのイベントの抽出を含む TXT ファイルを生成する方法***

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**ポリシー**］タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. ポリシーのプロパティウィンドウで、［**ログと通知**］をクリックします。
6. ［**実行ログ**］ブロックの［**設定**］をクリックします。
   ［**通知**］ウィンドウが表示されます。
7. ［**ローカル動作コントロール**］フォルダーを展開します。
8. ［**アプリケーション起動コントロール**］セクションを選択します。

9. アプリケーション起動コントロールイベントのリストの［**イベントを Kaspersky Security Center に送信**］列で、［*アプリケーションの起動が禁止されました*］および［*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*］の横にあるチェックボックスをオンにします。

10. 変更内容を保存します。

11. ポリシーの［**イベントの設定**］セクションで、［**管理サーバーのデータベースに保存（日）**］フィールドに指定されたイベントの保存期間が、ブロック対象のアプリケーションの起動に関する情報を収集する予定の期間（既定は 30 日）よりも長いことを確認します。

    アプリケーション起動コントロールのタスクログの保管期間が終了すると、ログに記録されたイベントは削除され、レポートに表示されなくなります。

12. 拒否されたアプリケーションの起動に関するデータを収集するように設定されたポリシーを有効にします。

13. 必要に応じて、アプリケーション起動コントロールのモードを変更します。

14. ブロック対象のアプリケーションの起動に関する情報を収集する期間が終了したら、［*アプリケーションの起動が禁止されました*］および［*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*］のイベントから抽出を行い、TXT ファイルにエクスポートします。詳細については、*Kaspersky Security Center* のヘルプの「イベントの抽出」のセクションを参照してください。

15. エクスポートされた TXT ファイルを開きます。

16. 必要に応じて、イベントのリストを編集します。

***Kaspersky Security Center Web コンソールを使用して Kaspersky Security Center のブロック対象のアプリケーションのイベントの抽出を含む TXT ファイルを生成する方法***

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）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**ログと通知**］セクションを選択します。

5. ［**実行ログ**］ブロックの［**設定**］をクリックします。
   ［**実行ログ**］ウィンドウが表示されます。

6. ［**アプリケーション起動コントロール**］セクションを選択します。

7. アプリケーション起動コントロールイベントのリストの［**イベントを Kaspersky Security Center に送信**］列で、［*アプリケーションの起動が禁止されました*］および［*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*］の横にあるチェックボックスをオンにします。

8. 変更内容を保存します。

9. 設定しているポリシーの［**イベントの設定**］タブで、［**管理サーバーのデータベースに保存（日）**］フィールドに指定されたイベントの保存期間が、ブロック対象のアプリケーションの起動に関する情報を収集する予定の期間（既定は 30 日）よりも長いことを確認します。

   アプリケーション起動コントロールのタスクログの保管期間が終了すると、ログに記録されたイベントは削除され、レポートに表示されなくなります。

10. 拒否されたアプリケーションの起動に関するデータを収集するように設定されたポリシーを有効にします。

11. 必要に応じて、アプリケーション起動コントロールのモードを変更します。

12. ブロック対象のアプリケーションの起動に関する情報を収集する期間が終了したら、［*アプリケーションの起動が禁止されました*］および［*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*］のイベントから抽出を行い、TXT ファイルにエクスポートします。詳細については、*Kaspersky Security Center* のヘルプの「イベントの抽出」のセクションを参照してください。

13. エクスポートされた TXT ファイルを開きます。

14. 必要に応じて、イベントのリストを編集します。

# アプリケーション起動コントロールルールの自動生成グループタスクの設定

***Kaspersky Security Center 管理コンソールでアプリケーション起動コントロールルールの自動生成グループタスクを設定する方法***

1. **アプリケーション起動コントロールルールの自動生成タスクのプロパティを開きます**。

   a. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。

   b. タスクを設定する管理グループを選択します。

   c. ［**タスク**］タブを選択します。

   d. グループタスクのリストで、タスク名をダブルクリックして、アプリケーション起動コントロールルールの自動生成タスクを開きます。

      ［**プロパティ: アプリケーション起動コントロールルールの自動生成**］ウィンドウが表示されます。

2. ［**オプション**］に移動します。

3. 必要に応じて、［**ルール**］タブで、ルール名の接頭辞を入力します。

4. ［**許可ルールの使用範囲**］で、許可ルールの作成に使用する方法を指定します：

   - **実行中のアプリケーションに基づいて許可ルールを作成する**
   - **アプリケーション向けの許可ルールを作成する**

5. ［**設定**］タブで、アプリケーション起動コントロールの許可ルールの作成時にタスクによって適用される条件を選択します：

   - **デジタル証明書を使用する**
   - **デジタル証明書の発行先とサムプリントを使用する**
   - **証明書がない場合に次を使用する**
   - **SHA256 ハッシュを使用する**

6. ［**ハッシュ値に基づいて生成されたルールのファイルパスを追加する**］を設定します。

   このチェックボックスをオンにすると、ルールをエクスポートする際に、実行ファイルへの完全パスが XML ファイルに追加されます。完全パスは、実行ファイルがどのソフトウェアに属しているかを判断するのに役立ちます。

   チェックボックスをオフにすると、XML ファイルには実行ファイルの名前と SHA256 ハッシュのみが含まれます。既定では、このチェックボックスはオフです。

7. **タスクを使用して作成されたルールを満たすアプリケーションを起動できるようにするユーザーまたはユーザーグループを追加します**。

   a. ［**追加**］のコンテキストメニューで、ユーザーまたはグループを追加する方法を選択します。

   b. ウィンドウが表示されるので、そのウィンドウで、ユーザーまたはユーザーグループの名前を入力または選択します。

   c. ［**OK**］をクリックします。

   d. ユーザーまたはユーザーグループごとに手順 a ～ c を実行します。

8. ［**タスク完了後**］ブロックで、次を設定します：

   - **アプリケーション起動コントロールルールのリストに許可ルールを追加する**
   - **追加方法**
   - **許可ルールをファイルにエクスポートする**：［**参照**］をクリックして、アプリケーション起動コントロールルールの自動生成タスクの完了時に Kaspersky Embedded Systems Security が許可ルールをエクスポートする XML ファイルのパスを指定できます。
   - **ファイル名に保護対象デバイスの詳細を追加する**

9. 必要に応じて、［**除外リスト**］タブで、タスクの範囲から除外するオブジェクトを指定します。

10. ［**プロパティ: アプリケーション起動コントロールルールの自動生成**］ウィンドウの［**OK**］をクリックします。

### *Kaspersky Security Center Web コンソールでアプリケーション起動コントロールルールの自動生成グループ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、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
2. グループタスクのリストで、アプリケーション起動コントロールルールの自動生成タスクを開きます。
   ［**アプリケーション起動コントロールルールの自動生成**］ウィンドウが表示されます。
3. ［**アプリケーション設定**］タブを開きます。
4. 必要に応じて、［**許可ルールの使用範囲**］セクションで、ルール名の接頭辞を入力します。
5. ［**許可ルールの使用範囲**］で、許可ルールの作成に使用する方法を指定します：
   - **実行中のアプリケーションに基づいて許可ルールを作成する**
   - **アプリケーション向けの許可ルールを作成する**
6. ［**パラメータ**］タブで、アプリケーション起動コントロールの許可ルールの作成時にタスクによって適用される条件を選択します：
   - **デジタル証明書を使用する**
   - **デジタル証明書の発行先とサムプリントを使用する**
   - **証明書がない場合に次を使用する**
   - **SHA256 ハッシュを使用する**
7. ［**ハッシュ値に基づいて生成されたルールのファイルパスを追加する**］を設定します。
   このチェックボックスをオンにすると、ルールをエクスポートする際に、実行ファイルへの完全パスが XML ファイルに追加されます。完全パスは、実行ファイルがどのソフトウェアに属しているかを判断するのに役立ちます。
   チェックボックスをオフにすると、XML ファイルには実行ファイルの名前と SHA256 ハッシュのみが含まれます。既定では、このチェックボックスはオフです。
8. **タスクを使用して作成されたルールを満たすアプリケーションを起動できるようにするユーザーまたはユーザーグループを追加します**。
   a. ［**ユーザーまたはグループを選択**］をクリックします。
   b. ウィンドウが表示されるので、そのウィンドウで、ユーザーまたはユーザーグループの名前を入力または選択します。
   c. ［**選択**］をクリックします。
   d. ユーザーまたはユーザーグループごとに手順 a ～ c を実行します。

9. ［**タスク完了後**］ブロックで、次を設定します：

   - **アプリケーション起動コントロールルールのリストに許可ルールを追加する**
   - **追加方法**
   - **許可ルールはファイルにエクスポートされます。**：［**拡張子 .xml のファイルの完全パスを指定してください**］フィールドでは、アプリケーション起動コントロールルールの自動生成タスクの完了時に Kaspersky Embedded Systems Security が許可ルールをエクスポートする XML ファイルのパスを指定できます。
   - **ファイル名に保護対象デバイスの詳細を追加する**

10. 必要に応じて、［**除外リスト**］タブで、タスクの範囲から除外するオブジェクトを指定します。
11. ［**アプリケーション起動コントロールルールの自動生成**］ウィンドウの［OK］をクリックします。

# アプリケーション起動コントロールルールの自動生成グループタスクを使用したルールの作成

*アプリケーション起動コントロールルールの自動生成グループタスクを使用してルールを作成するには：*

1. *アプリケーション起動コントロールルールの自動生成グループタスク*を作成するか、既存のタスクを選択します。
2. アプリケーション起動コントロールルールの自動生成タスクを設定します。
3. アプリケーション起動コントロールルールの自動生成タスクを実行します。

タスクが完了したら、タスク設定に応じて次のようになります：

- タスクの完了時に［**アプリケーション起動コントロールルールのリストに許可ルールを追加する**］の処理を実行するよう指定した場合、生成されたアプリケーション起動コントロールルールが、アプリケーションコンソールのアプリケーション起動コントロールの設定のリストに追加されます。
- タスクの完了時に［**許可ルールはファイルにエクスポートされます。**］の処理を実行するよう指定した場合、生成されたアプリケーション起動コントロールルールが、タスク設定で指定されたパスの XML ファイルに保存されます。

リストには、アプリケーション起動コントロールルールの自動生成グループタスクの設定と同じ種別のアプリケーションの起動に対する許可ルールが含まれます。

# デバイスコントロール

デバイスコントロールは、コンピューターに内蔵ないし接続されているデバイスへのユーザーアクセスを管理します（例：ハードディスク、カメラ、Wi-Fi モジュール）。これにより、こうしたデバイスが接続されたときにコンピューターを感染から保護し、データの損失や漏洩を防ぐことができます。

デバイスコントロールは、次の機能を備えています：

- ストレージ機器（リムーバブルドライブ、携帯電話、CD/DVD ドライブなど）へのユーザーアクセス権限を管理します。
- ファイルシステムのないデバイスの接続を制御します（たとえば、外付けモデム、Bluetooth アダプター、USB キーボードなど）。
- Wi-Fi 接続を管理します。

既定では、デバイスコントロールは無効になっています。デバイスコントロールを有効にすると、Kaspersky Embedded Systems Security は既定で次のデバイス種別へのアクセスを拒否します：

- リムーバブルドライブ（USB フラッシュドライブを含む）
- フロッピーディスク
- CD/DVD ドライブ
- ポータブルデバイス（MTP）
- モデム
- スマートカードリーダー
- 外部ネットワークアダプター
- Bluetooth（入力デバイスを除く）

## デバイスコントロールのレベル

Kaspersky Embedded Systems Security は、次のレベルでデバイスアクセスを制御します：

1. **デバイス種別**

   デバイスをコンピューターに接続すると、オペレーティングシステムによってデバイス種別（プリンター、リムーバブルドライブ、CD/DVD ドライブなど）が判別されます。このレベルでは、種別ごとにデバイスの接続を許可または拒否することができます。

2. **接続バス**

   *接続バス*は、デバイスをコンピューターに接続するために使用されるインターフェイスです。一部のデバイス種別には複数の接続インターフェイスがあります。たとえば、プリンターを USB ポートまたはシリアル（COM）ポートに接続できます。

   このレベルでは、接続バスに応じてデバイスへのアクセスを許可または拒否できます。

   たとえば、USB 経由のアクセスを拒否したとします。Kaspersky Embedded Systems Security は、［**接続バスに依存**］モードの場合に USB 経由で接続されたすべてのデバイス種別へのアクセスを拒否します。

デバイスに対して［**許可**］または［**ブロック**］のアクセスモードが選択されている場合、アクセスコントロールはデバイスの接続バスを無視します。

3. **信頼するデバイス**

   「*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。

### デバイスコントロールの操作モード

デバイスコントロールは次のモードで動作します：

- **アクティブモード**

  Kaspersky Embedded Systems Security は、設定されたデバイスアクセスルールに基づいてデバイスを拒否または許可します。本製品では、信頼するデバイスへのアクセスも許可されます。本製品により、デバイスの接続イベントと切断イベントが登録されます。

- **通知**：

  Kaspersky Embedded Systems Security はすべてのデバイスを許可し、対応するイベントをログに記録します。すべてのデバイスが許可されます。既定ではこのモードが設定されています。このモードを有効にすると、組織内のデバイスの監査を実施して、この情報を使用して、信頼するデバイスのリストのドラフトを作成できます。

## デバイスアクセスルール

*デバイスアクセスルール*は、コンピューターに内蔵または接続されているデバイスに、どのユーザーがアクセスできるかを定義する複数の設定項目です。これらの設定には特定のデバイス、アクセススケジュール、読み取りまたは書き込み権限などへのアクセスが含まれます。アクセスルールで設定できる項目は、対象となるデバイスの種別に応じて異なります。

アクセスルールの設定

| デバイス | ユーザーまたはユーザーのグループの割り当て | デバイスへのアクセスのスケジュール | 読み取り／書き込み権限 | 接続バスの監視 |
|---|---|---|---|---|
| ハードディスク | ✓ | ✓ | ✓ | ✓ |
| リムーバブルドライブ（USB フラッシュドライブを含む） | ✓ | ✓ | ✓ | ✓ |
| フロッピーディスク | ✓ | ✓ | ✓ | ✓ |
| CD/DVD ドライブ | ✓ | ✓ | ✓ | ✓ |
| ポータブルデバイス（MTP） | ✓ | ✓ | ✓ | ✓ |
| ローカルプリンター | ✓ | – | – | ✓ |
| ネットワークプリンター | ✓ | – | – | – |
| モデム | – | – | – | ✓ |
| ストリーマー | – | – | – | ✓ |
| 多機能デバイス | – | – | – | ✓ |
| スマートカードリーダー | – | – | – | ✓ |
| Windows CE USB ActiveSync デバイス | – | – | – | ✓ |
| 外部ネットワークアダプター | – | – | – | ✓ |

| デバイス | ユーザーまたはユーザーのグループの割り当て | デバイスへのアクセスのスケジュール | 読み取り／書き込み権限 | 接続バスの監視 |
|---|---|---|---|---|
| Bluetooth | – | – | – | – |
| カメラとスキャナー | – | – | – | ✓ |
| Wi-Fi | – | – | – | – |
| USB キーボード | – | – | – | ✓ |
| USB マウス | – | – | – | ✓ |

# 種別ごとのデバイスアクセス制御

デバイスコントロールを使用すると、デバイス種別ごとにデバイスへのアクセスを制御できます。デバイスの種別は、デバイスの接続時にオペレーティングシステムによって決定されます。オペレーティングシステムに組み込まれているデバイスマネージャーツールを使用して、デバイス種別を確認できます。デバイスアクセスを管理するには、ルールを設定する必要があります。*デバイスアクセスルール*は、コンピューターに内蔵または接続されているデバイスに、どのユーザーがアクセスできるかを定義する複数の設定項目です。これらの設定には特定のデバイス、アクセススケジュール、読み取りまたは書き込み権限などへのアクセスが含まれます。アクセスルールで設定できる項目は、対象となるデバイスの種別に応じて異なります。

次のようにデバイスアクセスを設定できます：

- **許可**：

  Kaspersky Embedded Systems Security は、すべてのユーザーにデバイスへの完全なアクセス権を付与します。

- **ブロック**：

  Kaspersky Embedded Systems Security はデバイスの接続をブロックします。信頼するデバイスのみ接続できます。

- **接続バスに依存**：

  Kaspersky Embedded Systems Security は、デバイスの接続バスを識別し、接続バスのアクセスモードに応じてアクセス制御を実行します。また、信頼するデバイスの接続も許可します。

- **ルールに準拠**：

  一部のデバイス種別に対して、デバイスの使用、デバイスアクセススケジュールの設定、読み取り権限および書き込み権限が許可されるユーザーまたはユーザーグループを選択することができます。信頼するデバイスの接続も許可されます。

［**ハードディスク**］の種別のデバイスへのアクセスを設定する際は注意してください。システムドライブへのアクセスを禁止すると、オペレーティングシステムの起動時にクラッシュ（BSOD）が発生する可能性があります。

デバイスがデバイスコントロールの分類スキームの範囲外にある場合、そのようなデバイスへのアクセスを制限することはできません。

### Kaspersky Security Center 管理コンソールで種別ごとにデバイスへのアクセスを制御する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。
4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。
5. ［**デバイスコントロール**］チェックボックスをオンにします。
6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。
7. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。
8. デバイスアクセスルールを設定します：
   a. アクセスモード（［**許可**］、［**ブロック**］、［**接続バスに依存**］、［**ルールに準拠**］）を選択します。
      ［**ルールに準拠**］のアクセスモードを選択するには、ダブルクリックしてアクセスルールのプロパティを開く必要があります。
   b. ［**接続バスに依存**］アクセスモードを選択した場合は、［**接続バス**］タブで接続インターフェイスのアクセスルールを設定する必要があります。
   c. ストレージ機器（リムーバブルドライブなど）の場合は、個々のユーザーのアクセス権を設定することができます。また、デバイスアクセススケジュールを設定したり、読み取り権限および書き込み権限を設定したりすることもできます。
   d. 必要に応じて、印刷ルールを設定します。
   e. 必要に応じて、Wi-Fi 接続ルールを設定します。
9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

### Kaspersky Security Center Web コンソールで種別ごとにデバイスへのアクセスを制御する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。
   ［**デバイスコントロール**］ウィンドウが表示されます。

5. ［**デバイスコントロールを有効にする**］チェックボックスをオンにします。

6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

7. ［**デバイスコントロール設定**］ブロックで、［**デバイスと Wi-Fi ネットワークのアクセスルール**］をクリックします。
   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

8. デバイスアクセスルールを設定します：

   a. アクセスモード（［**許可**］、［**ブロック**］、［**接続バスに依存**］、［**ルールに準拠**］）を選択します。
      ドロップダウンメニューにアクセスモードが表示されない場合は、デバイス種別をダブルクリックしてアクセスルールのプロパティを開きます。

   b. ［**接続バスに依存**］アクセスモードを選択した場合は、一般的なデバイスコントロール設定のウィンドウに戻り、［**接続バス**］をクリックし、接続インターフェイスのアクセスルールを設定する必要があります。

   c. ストレージ機器（リムーバブルドライブなど）の場合は、個々のユーザーのアクセス権を設定することができます。また、デバイスアクセススケジュールを設定したり、読み取り権限および書き込み権限を設定したりすることもできます。

   d. 必要に応じて、印刷ルールを設定します。

   e. 必要に応じて、Wi-Fi 接続ルールを設定します。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

***アプリケーションコンソールで種別ごとにデバイスアクセスを制御する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。

2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。

3. ［**デバイスコントロール**］チェックボックスをオンにします。

4. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

5. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

6. デバイスアクセスルールを設定します：

   a. アクセスモード（［**許可**］、［**ブロック**］、［**接続バスに依存**］、［**ルールに準拠**］）を選択します。
      ［**ルールに準拠**］のアクセスモードを選択するには、ダブルクリックしてアクセスルールのプロパティを開く必要があります。

b. ［**接続バスに依存**］アクセスモードを選択した場合は、［**接続バス**］タブで接続インターフェイスのアクセスルールを設定する必要があります。

c. ストレージ機器（リムーバブルドライブなど）の場合は、個々のユーザーのアクセス権を設定することができます。また、デバイスアクセススケジュールを設定したり、読み取り権限および書き込み権限を設定したりすることもできます。

d. 必要に応じて、印刷ルールを設定します。

e. 必要に応じて、Wi-Fi 接続ルールを設定します。

7. 変更内容を保存します。

これにより、ユーザーがデバイスへのアクセスを取得しようとすると、ルールに従ってアクセスがブロックされます。さらに、Kaspersky Embedded Systems Security は対応するイベントをログに記録します。個々のデバイスへのアクセスを許可する場合は、それらのデバイスを信頼するデバイスのリストに追加することができます。

# Wi-Fi 接続の制御

デバイスコントロールを使用して、コンピューター（ターミナル）の Wi-Fi 接続を管理することができます。公衆 Wi-Fi ネットワークは安全でないことがあり、このようなネットワークを使用することによりデータ損失など問題が発生する可能性があります。デバイスコントロールを使用すると、ユーザーの Wi-Fi への接続をブロックしたり、信頼済みのネットワークのみに接続を許可することができます。例えば、セキュリティ要件を満たしている企業 Wi-Fi のネットワークにのみ接続を許可することができます。デバイスコントロールは、信頼リストで指定したもの以外のすべての Wi-Fi ネットワークへのアクセスをブロックします。

Windows 11 を実行しているコンピューターでは、Wi-Fi 接続を制御するために位置情報サービスを有効にする必要があります。これを行うには、オペレーティングシステムの設定で**位置情報サービス**を有効にする必要があります（［**設定**］→［**プライバシーとセキュリティ**］→［**位置情報**］）。位置情報サービスが無効になっている場合、Kaspersky Embedded Systems Security は Wi-Fi ネットワークへの接続を制御しません。

### Kaspersky Security Center 管理コンソールで Wi-Fi 接続を制限する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。
4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。
5. ［**デバイスコントロール**］チェックボックスをオンにします。
6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。
7. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。

8. ［**Wi-Fi**］のデバイスで、アクセスルールを設定します：

   a. アクセスモード（［**許可**］、［**ブロック**］、［**例外を除きブロック**］）を選択します。

   b. ［**例外を除きブロック**］モードを選択した場合は、信頼する Wi-Fi ネットワークのリストを作成する必要があります：

      1. ［**Wi-Fi**］のデバイス種別をダブルクリックして、信頼する Wi-Fi ネットワークのリストを開きます。

      2. 表示されたウィンドウの［**追加**］をクリックします。

      3. ウィンドウが表示されるので、そのウィンドウで信頼する Wi-Fi ネットワークを設定します：

         - **ネットワーク名**：Wi-Fi ネットワークの名前または SSID（Service Set Identifier）です。
         - **認証種別**：Wi-Fi ネットワークへの接続時に使用される認証種別です。
         - **暗号化種別**：Wi-Fi トラフィックを保護するために使用される暗号化種別です。
         - **コメント**：追加された Wi-Fi ネットワークに関する詳細情報です。

   信頼する Wi-Fi ネットワークの設定はルーターの設定で表示できます。

   すべての設定がルールで指定された設定と一致する Wi-Fi ネットワークが信頼するものとみなされます。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

### Kaspersky Security Center Web コンソールで Wi-Fi 接続を制限する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。
   ［**デバイスコントロール**］ウィンドウが表示されます。
5. ［**デバイスコントロールを有効にする**］チェックボックスをオンにします。
6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。
7. ［**デバイスコントロール設定**］ブロックで、［**デバイスと Wi-Fi ネットワークのアクセスルール**］をクリックします。
   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

8. ［**Wi-Fi**］のデバイス種別をダブルクリックして、アクセスルールのプロパティを開きます。

9. アクセスモード（［**許可**］、［**ブロック**］、［**例外を除きブロック**］）を選択します。

10. ［**例外を除きブロック**］モードを選択した場合は、信頼する Wi-Fi ネットワークのリストを作成する必要があります：

    1. ［**信頼する Wi-Fi ネットワーク**］ブロックの［**追加**］をクリックします。

    2. ウィンドウが表示されるので、そのウィンドウで信頼する Wi-Fi ネットワークを設定します：

       - **ネットワーク名**：Wi-Fi ネットワークの名前または SSID（Service Set Identifier）です。
       - **認証種別**：Wi-Fi ネットワークへの接続時に使用される認証種別です。
       - **暗号化種別**：Wi-Fi トラフィックを保護するために使用される暗号化種別です。
       - **コメント**：追加された Wi-Fi ネットワークに関する詳細情報です。

    信頼する Wi-Fi ネットワークの設定はルーターの設定で表示できます。

    > すべての設定がルールで指定された設定と一致する Wi-Fi ネットワークが信頼するものとみなされます。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

***アプリケーションコンソールで Wi-Fi 接続を制限する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。

2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。

3. ［**デバイスコントロール**］チェックボックスをオンにします。

4. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

5. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

6. ［**Wi-Fi**］のデバイスで、アクセスルールを設定します：

   a. アクセスモード（［**許可**］、［**ブロック**］、［**例外を除きブロック**］）を選択します。

   b. ［**例外を除きブロック**］モードを選択した場合は、信頼する Wi-Fi ネットワークのリストを作成する必要があります：

      1. ［**Wi-Fi**］のデバイス種別をダブルクリックして、信頼する Wi-Fi ネットワークのリストを開きます。

      2. 表示されたウィンドウの［**追加**］をクリックします。

      3. ウィンドウが表示されるので、そのウィンドウで信頼する Wi-Fi ネットワークを設定します：

         - **ネットワーク名**：Wi-Fi ネットワークの名前または SSID（Service Set Identifier）です。
         - **認証種別**：Wi-Fi ネットワークへの接続時に使用される認証種別です。
         - **暗号化種別**：Wi-Fi トラフィックを保護するために使用される暗号化種別です。
         - **コメント**：追加された Wi-Fi ネットワークに関する詳細情報です。

      信頼する Wi-Fi ネットワークの設定はルーターの設定で表示できます。

      すべての設定がルールで指定された設定と一致する Wi-Fi ネットワークが信頼するものとみなされます。

7. 変更内容を保存します。

ユーザーが信頼済みとしてリストに登録されていない Wi-Fi ネットワークに接続しようとした場合、本製品は接続をブロックします。

# プリンターのコントロール

デバイスコントロールを使用すると、ローカルとネットワークプリンターへのユーザーアクセスを設定できます。

## ローカルプリンターの管理

Kaspersky Embedded Systems Security は次のバス経由でローカルプリンターへの接続を管理します：［USB］、［シリアルポート］（COM）、［パラレルポート］（LPT）。

Kaspersky Embedded Systems Security はローカルプリンターの COM および LPT ポートへの接続をバスの 1 レベルにおいてのみコントロールします。つまり COM および LPT ポートへのプリンターの接続をブロックするには、［**ローカルプリンター**］のデバイス種別で、［**接続バスに依存**］モードを選択して、デバイスの COM および LPT バスへの接続を禁止します。

USB に接続されたプリンターについては、本製品はデバイス種別（ローカルプリンター）および接続バス（USB）の 2 レベルをコントロールします。

USB 経由でのローカルプリンターへのアクセスモードは、以下のいずれかから選択することができます：

- **許可**：Kaspersky Embedded Systems Security は、すべてのユーザーにローカルプリンターへの完全なアクセス権を付与します。ユーザーは、オペレーティングシステムに用意されている手段を使用してプリンターに接続し、文書を印刷できます。
- **ブロック**：Kaspersky Embedded Systems Security はローカルプリンターの接続をブロックします。信頼できるプリンターのみ接続できます。
- **接続バスに依存**：Kaspersky Embedded Systems Security はローカルプリンターへの接続を USB 接続バスのステータス（［**許可**］（）または［**ブロック**］（））に応じて許可します。
- **ルールに準拠**：印刷を管理するには、*印刷ルール*を追加する必要があります。ルールでは、ローカルプリンター上での文書の印刷へのアクセスを許可またはブロックするユーザーまたはユーザーグループを選択できます。

## ネットワークプリンターの管理

Kaspersky Embedded Systems Security では、ネットワークプリンター上での印刷へのアクセスを設定することができます。次のネットワークプリンターのアクセスモードのうち 1 つを選択することができます：

- ［**許可（ログ記録なし）**］（）：Kaspersky Embedded Systems Security はネットワークプリンターでの印刷をコントロールしません。すべてのユーザーに印刷へのアクセスが許可され、イベントログに印刷に関する情報は保存されません。
- ［**許可**］（）：Kaspersky Embedded Systems Security はすべてのユーザーにネットワークプリンターでの印刷へのアクセスを許可します。
- ［**ブロック**］（）：Kaspersky Embedded Systems Security はすべてのユーザーに対してネットワークプリンターへのアクセスを制限します。アクセスが許可されるのは信頼済みのプリンターのみです。
- **ルールに準拠**：印刷を管理するには、*印刷ルール*を追加する必要があります。ルールでは、ネットワークプリンター上での文書の印刷へのアクセスを許可またはブロックするユーザーまたはユーザーグループを選択できます。

## プリンターの印刷ルールを追加する

**Kaspersky Security Center 管理コンソールで印刷ルールを追加する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。
4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。
5. ［**デバイスコントロール**］チェックボックスをオンにします。

6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

7. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。

   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。

8. プリンターのアクセスルールを設定します：

   a. ［**ローカルプリンター**］と［**ネットワークプリンター**］のデバイス種別で、［**許可**］、［**ブロック**］、［**許可（ログ記録なし）**］（ネットワークプリンターのみ）、［**接続バスに依存**］（ローカルプリンターのみ）、［**ルールに準拠**］のいずれかのアクセスルールを設定します。

   b. ［**接続バスに依存**］アクセスモードを選択した場合は、［**接続バス**］タブで接続インターフェイスのアクセスルールを設定する必要があります。

   c. ［**ルールに準拠**］アクセスモードを選択した場合は、印刷ルールを設定する必要があります：

      1. ［**ローカルプリンター**］または［**ネットワークプリンター**］のデバイス種別をダブルクリックして、アクセスルールのプロパティを開きます。

      2. 印刷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。これを行うには、［**追加**］をクリックします。

         新しい印刷ルールを追加するウィンドウが開きます。

      3. *ルールの項目*に優先度を割り当てます。ルールの項目にはユーザーアカウント、操作（許可またはブロック）、優先度の属性が含まれます。

         ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Embedded Systems Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Embedded Systems Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

         例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

         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。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Embedded Systems Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

      4. ［**処理**］で、ユーザーのプリンターを使用した印刷へのアクセスを設定します。

      5. ［**ユーザーとグループ**］をクリックして、印刷にアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。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。

      6. ［OK］をクリックします。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

### Kaspersky Security Center Web コンソールで印刷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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。

   ［**デバイスコントロール**］ウィンドウが表示されます。
5. ［**デバイスコントロールを有効にする**］チェックボックスをオンにします。
6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。
7. ［**デバイスコントロール設定**］ブロックで、［**デバイスと Wi-Fi ネットワークのアクセスルール**］をクリックします。

   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。
8. プリンターのアクセスルールを設定します：

   a. ［**ローカルプリンター**］と［**ネットワークプリンター**］のデバイス種別で、［**許可**］、［**ブロック**］、［**許可（ログ記録なし）**］（ネットワークプリンターのみ）、［**接続バスに依存**］（ローカルプリンターのみ）、［**ルールに準拠**］のいずれかのアクセスモードを選択します。

   ドロップダウンメニューにアクセスモードが表示されない場合は、デバイス種別をダブルクリックしてアクセスルールのプロパティを開きます。

   b. ［**接続バスに依存**］アクセスモードを選択した場合は、一般的なデバイスコントロール設定のウィンドウに戻り、［**接続バス**］をクリックし、接続インターフェイスのアクセスルールを設定する必要があります。

   c. 印刷を設定する必要がある場合：

      1. ［**ローカルプリンター**］または［**ネットワークプリンター**］のデバイス種別をダブルクリックして、アクセスルールのプロパティを開きます。
      2. ［**ルールに準拠**］のアクセスモードを選択します。
      3. 印刷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。これを行うには、［**追加**］をクリックします。

         新しい印刷ルールを追加するウィンドウが開きます。
      4. *ルールの項目*に優先度を割り当てます。ルールの項目にはユーザーアカウント、操作（許可またはブロック）、優先度の属性が含まれます。

         ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Embedded Systems Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Embedded Systems Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

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。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Embedded Systems Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

5. ［**処理**］で、ユーザーのプリンターを使用した印刷へのアクセスを設定します。

6. ［**ユーザーとグループ**］の下にある［**追加**］をクリックして、印刷にアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。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。

7. ［**OK**］をクリックします。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

***アプリケーションコンソールで印刷ルールを追加する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。

2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。

3. ［**デバイスコントロール**］チェックボックスをオンにします。

4. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

5. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

6. プリンターのアクセスルールを設定します：

   a. ［**ローカルプリンター**］と［**ネットワークプリンター**］のデバイス種別で、［**許可**］、［**ブロック**］、［**許可（ログ記録なし）**］（ネットワークプリンターのみ）、［**接続バスに依存**］（ローカルプリンターのみ）、［**ルールに準拠**］のいずれかのアクセスルールを設定します。

   b. ［**接続バスに依存**］アクセスモードを選択した場合は、［**接続バス**］タブで接続インターフェイスのアクセスルールを設定する必要があります。

   c. ［**ルールに準拠**］アクセスモードを選択した場合は、印刷ルールを設定する必要があります：

      1. ［**ローカルプリンター**］または［**ネットワークプリンター**］のデバイス種別をダブルクリックして、アクセスルールのプロパティを開きます。

      2. 印刷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。これを行うには、［**追加**］をクリックします。
      新しい印刷ルールを追加するウィンドウが開きます。

3. *ルールの項目*に優先度を割り当てます。ルールの項目にはユーザーアカウント、操作（許可またはブロック）、優先度の属性が含まれます。

   ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Embedded Systems Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Embedded Systems Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

   例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

   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。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Embedded Systems Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

4. ［**処理**］で、ユーザーのプリンターを使用した印刷へのアクセスを設定します。

5. ［**ユーザーとグループ**］をクリックして、印刷にアクセスするユーザーまたはユーザーグループを設定します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。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。

6. ［**OK**］をクリックします。

7. 変更内容を保存します。

# 入力デバイスコントロール（HID）

入力デバイスには、キーボード、マウス、トラックボール、タッチパッドなどのデバイスが含まれます。USB、Bluetooth、PS/2 ポート、RS-232（COM）ポート、IR ポートなどのインターフェイスを使用して入力デバイスを接続できます。

Kaspersky Embedded Systems Security は、USB および Bluetooth のマウスとキーボードを制御できます。デバイスコントロールにより、入力デバイスの接続デバイスと切断デバイスが記録されます。

Bluetooth デバイスが接続または接続解除されると、本製品がそのデバイスについて複数のイベントを作成することがあります。その理由は、オペレーティングシステムが Bluetooth デバイスを異なる種別の複数のデバイスとして検出する可能性があるためです。Kaspersky Embedded Systems Security は、そのデバイスの接続に使用されている Bluetooth アダプターも別のデバイスとして管理します。そのため、本製品は検出されたデバイスごとにイベントを作成します。

Kaspersky Embedded Systems Security では、入力デバイスの使用を許可または禁止できることに加えて、信頼するデバイスのリストを作成することもできます。

**Kaspersky Security Center 管理コンソールでデバイスコントロールを有効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。

4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。

5. ［**デバイスコントロール**］チェックボックスをオンにします。

6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

7. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。

8. ［**Bluetooth**］のデバイス種別で、［**許可**］、［**ブロック**］、［**許可（ログ記録なし）**］のいずれかのアクセスモードを選択します。
   すべての Bluetooth デバイスをブロックまたは許可することも、Bluetooth 入力デバイス（HID（ヒューマンインターフェイスデバイス）クラス）のみの接続を許可することもできます。

   > 入力デバイスの接続の許可は、Kaspersky Security Center Web コンソールでのみ行うことができます。管理コンソール（MMC）または Kaspersky Embedded Systems Security コンソールで入力デバイスの接続を許可することはできません。

9. ［**USB キーボード**］および［**USB マウス**］のデバイス種別で、［**許可**］、［**ブロック**］、［**接続バスに依存**］のいずれかのアクセスモードを選択します。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

**Kaspersky Security Center Web コンソールでデバイスコントロールを有効にする方法**

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

2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。
   ［**デバイスコントロール**］ウィンドウが表示されます。

5. ［**デバイスコントロールを有効にする**］チェックボックスをオンにします。

6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

7. ［**デバイスコントロール設定**］ブロックで、［**デバイスと Wi-Fi ネットワークのアクセスルール**］をクリックします。
   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

8. ［**Bluetooth**］のデバイス種別をクリックして、アクセスルールのプロパティを開きます。

9. アクセスモード（[**許可**]、[**ブロック**]、[**許可（ログ記録なし）**]）を選択します。

   すべての Bluetooth デバイスをブロックまたは許可することも、Bluetooth 入力デバイス（HID（ヒューマンインターフェイスデバイス）クラス）のみの接続を許可することもできます。

10. [**USB キーボード**] および [**USB マウス**] のデバイス種別で、[**許可**]、[**ブロック**]、[**接続バスに依存**] のいずれかのアクセスモードを選択します。

11. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

*アプリケーションコンソールでデバイスコントロールを設定する方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、[**コンピューターコントロール**] → [**デバイスコントロール**] の順に選択します。

2. [**デバイスコントロール**] フォルダーの結果ペインで、[**プロパティ**] をクリックします。

   [**プロパティ: デバイスコントロール**] ウィンドウが表示されます。

3. [**デバイスコントロール**] チェックボックスをオンにします。

4. [**ブロックルールの操作モード**] ブロックで、[**ブロックする**] または [**通知する**] を選択します。

5. [**デバイスコントロール設定**] で、[**デバイス種別**] を選択します。

   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

6. [**Bluetooth**] のデバイス種別で、[**許可**]、[**ブロック**]、[**許可（ログ記録なし）**] のいずれかのアクセスモードを選択します。

   すべての Bluetooth デバイスをブロックまたは許可することも、Bluetooth 入力デバイス（HID（ヒューマンインターフェイスデバイス）クラス）のみの接続を許可することもできます。

   > 入力デバイスの接続の許可は、Kaspersky Security Center Web コンソールでのみ行うことができます。管理コンソール（MMC）または Kaspersky Embedded Systems Security コンソールで入力デバイスの接続を許可することはできません。

7. [**USB キーボード**] および [**USB マウス**] のデバイス種別で、[**許可**]、[**ブロック**]、[**接続バスに依存**] のいずれかのアクセスモードを選択します。

8. 変更内容を保存します。

# リムーバブルドライブの使用状況の監視

リムーバブルドライブの使用状況の監視には以下が含まれます：

- リムーバブルドライブ上のファイルの操作の監視。
- 信頼済みのリムーバブルドライブの接続および接続解除の監視。

  Kaspersky Embedded Systems Security を使用して、リムーバブルドライブだけでなくすべての信頼済みデバイスの接続および接続解除を監視できます。イベントの記録はデバイスコントロール機能の通知設定で有効にすることができます。イベントのセキュリティレベルは*情報*です。

**Kaspersky Security Center 管理コンソールでリムーバブルドライブ上のファイル操作の監視を有効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。
4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。
5. ［**デバイスコントロール**］チェックボックスをオンにします。
6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。
7. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。

   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。
8. ［**リムーバブルドライブ**］のデバイス種別を選択して、［**ログ記録**］をクリックします。

   イベントログ記録のウィンドウが表示されます。
9. ［**ログ記録を有効にする**］チェックボックスをオンにします。
10. ［**ファイル操作**］ブロックで、監視する操作を選択します：**書き込み**、**削除**。
11. ［**ファイル形式でフィルタリング**］ブロックで、デバイスコントロールで記録するファイル形式に関連付けられた操作を選択します。
12. 監視対象のリムーバブルドライブを使用するユーザーまたはユーザーグループを選択します。
13. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

### Kaspersky Security Center Web コンソールでリムーバブルドライブ上のファイル操作の監視を有効にする方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。
   ［**デバイスコントロール**］ウィンドウが表示されます。
5. ［**デバイスコントロールを有効にする**］チェックボックスをオンにします。
6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。
7. ［**デバイスコントロール設定**］ブロックで、［**デバイスと Wi-Fi ネットワークのアクセスルール**］をクリックします。
   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。
8. ［**リムーバブルドライブ**］のデバイス種別をダブルクリックして、アクセスルールのプロパティを開きます。
9. 表示されたウィンドウで、**ログ記録**タブを選択します。
10. スイッチを［**ログ記録は有効です**］に設定します。
11. ［**ファイル操作**］ブロックで、監視する操作を選択します：**書き込み**、**削除**。
12. ［**ファイル形式でフィルタリング**］ブロックで、デバイスコントロールで記録するファイル形式に関連付けられた操作を選択します。
13. 監視対象のリムーバブルドライブを使用するユーザーまたはユーザーグループを選択します。
14. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

### *アプリケーションコンソールでリムーバブルドライブ上のファイル操作の監視を有効にする方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。
2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。
3. ［**デバイスコントロール**］チェックボックスをオンにします。
4. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

5. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。
6. ［**リムーバブルドライブ**］のデバイス種別を選択して、［**ログ記録**］をクリックします。
   イベントログ記録のウィンドウが表示されます。
7. ［**ログ記録を有効にする**］チェックボックスをオンにします。
8. ［**ファイル操作**］ブロックで、監視する操作を選択します：**書き込み**、**削除**。
9. ［**ファイル形式でフィルタリング**］ブロックで、デバイスコントロールで記録するファイル形式に関連付けられた操作を選択します。
10. 監視対象のリムーバブルドライブを使用するユーザーまたはユーザーグループを選択します。
11. 変更内容を保存します。

ユーザーが、リムーバブルドライブ上のファイルに書き込みをしたりリムーバブルドライブのファイルを削除すると、その操作に関する情報がイベントログに保存され、Kaspersky Security Center にイベントが送信されます。Kaspersky Security Center コンソールに保存されているリムーバブルドライブのファイルに関するイベントは、［**管理サーバー**］ノードの作業領域内の［**イベント**］タブで確認できます。ローカルの Kaspersky Embedded Systems Security のイベントログにイベントを表示するには、デバイスコントロールの通知設定で［**ファイルの操作が実行されました**］をオンにしてください。

# Bluetooth デバイスへのアクセスの管理

Kaspersky Embedded Systems Security では、Bluetooth デバイスへのアクセスを管理できます。Bluetooth デバイスには、ワイヤレスキーボード、マウス、ヘッドセット、プリンターなどがあります。また、モバイルデバイスとの通信などにも Bluetooth を使用できます。

Bluetooth デバイスが接続または接続解除されると、本製品がそのデバイスについて複数のイベントを作成することがあります。その理由は、オペレーティングシステムが Bluetooth デバイスを異なる種別の複数のデバイスとして検出する可能性があるためです。Kaspersky Embedded Systems Security は、そのデバイスの接続に使用されている Bluetooth アダプターも別のデバイスとして管理します。そのため、本製品は検出されたデバイスごとにイベントを作成します。

Bluetooth デバイスへのアクセスには、次のモードのうち1つを選択します：

- **許可（ログ記録なし）**：Kaspersky Embedded Systems Security は、あらゆる Bluetooth デバイスの接続を許可し、接続に関する情報をイベントログに保存しません。Bluetooth 入力デバイス（キーボード、マウスなど）の接続、Bluetooth 経由でのデータ送信、その他の Bluetooth デバイス（ヘッドセット、ヘッドフォンなど）の管理が可能です。
- **許可**：Kaspersky Embedded Systems Security は、あらゆる Bluetooth デバイスの接続を許可します。Bluetooth 入力デバイス（キーボード、マウスなど）の接続、Bluetooth 経由でのデータ送信、その他の Bluetooth デバイス（ヘッドセット、ヘッドフォンなど）の管理が可能です。
- **ブロック**：Kaspersky Embedded Systems Security は、Bluetooth デバイスへのアクセスを制限します。Bluetooth 入力デバイス（ヒューマンインターフェイスデバイスクラス）のみの接続を許可できます。これらのデバイスには、キーボード、マウス、ジョイスティックなどが含まれます。

信頼する Bluetooth デバイスのリストを作成することはできません。Bluetooth デバイスへのアクセスを制限している場合、接続できるのは Bluetooth 入力デバイスのみです。

入力デバイスの接続の許可は、アプリケーションコンソールまたは Kaspersky Security Center Web コンソールでのみ行うことができます。Kaspersky Security Center 管理コンソールで入力デバイスの接続の許可を行うことはできません。

### Kaspersky Security Center 管理コンソールで Bluetooth デバイスのアクセスルールを設定する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**ローカル動作コントロール**］→［**デバイスコントロール**］の順に選択し、［**設定**］をクリックします。
4. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
5. デバイス種別［**Bluetooth**］のコンテキストメニューで、Bluetooth デバイスのアクセスモード（［**許可**］（）、［**ブロック**］（）、［**許可（ログ記録なし）**］（））を設定します。

   Bluetooth デバイスへのアクセスをブロックした場合、アプリケーションコンソールまたは Kaspersky Security Center Web コンソールでのみ、入力デバイス（キーボード、マウスなど）の接続を許可することができます。Kaspersky Security Center 管理コンソールで入力デバイスの接続の許可を行うことはできません。
6. 変更内容を保存します。

### Kaspersky Security Center Web コンソールで Bluetooth デバイスの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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ポリシーウィンドウで、［**ローカル動作コントロール**］→［**デバイスコントロール**］の順に選択し、［**設定**］をクリックします。
5. ［**デバイスコントロール設定**］セクションで、［**デバイスと Wi-Fi ネットワークのアクセスルール**］をクリックします。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
6. ［**Bluetooth**］デバイス種別を選択します。
   Bluetooth デバイスのアクセス設定が開きます。
7. Bluetooth デバイスのアクセスモード（［**許可**］、［**ブロック**］、［**許可（ログ記録なし）**］）を設定します。
8. ［**ブロック**］モードを選択した場合、Bluetooth 入力デバイス（キーボード、マウスなど）への接続のみを許可することができます。これを行うには、［**除外リスト**］の下で［**入力デバイス（マウスとキーボード）**］をオンにします。
9. 変更内容を保存します。

### *アプリケーションコンソールで Bluetooth デバイスのアクセスルールを設定する方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。
2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。
3. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   表に、デバイスコントロールの分類内に存在するすべての端末のアクセスルールが一覧表示されます。
4. ［**アクセス**］で、Bluetooth デバイスのアクセスモード（［**許可**］、［**ブロック**］、［**許可（ログ記録なし）**］）を設定します。
5. ［**ブロック**］モードを選択した場合、Bluetooth 入力デバイス（キーボード、マウスなど）への接続のみを許可することができます。これを行うには、［**除外リスト**］の下で［**入力デバイス（マウスとキーボード）**］をオンにします。
6. 変更内容を保存します。

# デバイスに対するユーザーアクセス権の区別

デバイス種別ごとにユーザーアクセス権を設定することも、信頼するデバイスへのアクセスを設定することもできます。

## デバイス種別ごとのユーザーアクセス権の区別

デバイスコントロールでは、*ストレージ機器*上のデータへのユーザーアクセス権を設定できます。このようなデバイスに対し、読み取り権限と書き込み権限を設定できます。デバイスコントロールは、次の種別のストレージ機器をサポートします：

- 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
- CD/DVD ドライブ
- ポータブルデバイス（MTP）：ポータブルデバイス（MTP）には、モバイルデバイス、写真用カメラ、メディアプレーヤーなどが含まれます。

つまり、たとえば、リムーバブルドライブの使用を管理者グループのみに許可することができます。その他のデバイス種別に対し、すべてのユーザーのアクセスを拒否または許可できます。また、プリンターへのユーザーアクセス権を設定することもできます。

**Kaspersky Security Center 管理コンソールでリムーバブルドライブ上のデータへのユーザーアクセス権を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。
4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。
5. ［**デバイスコントロール**］チェックボックスをオンにします。
6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。
7. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。
   ［**デバイス種別**］タブに、デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールが表示されます。
8. ストレージ機器のアクセスルールを設定するには、ルールのリストをダブルクリックして開きます。

9. ストレージ機器のアクセスルールを設定します：

   a. ［**アクセスルール**］ブロックの［**追加**］をクリックします。

      新しいストレージ機器のアクセスルールを追加するウィンドウが開きます。

   b. ［**優先度**］フィールドで、*ルールの項目*の優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み）、優先度。

      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Embedded Systems Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Embedded Systems Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

      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。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Embedded Systems Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

   c. ［**ユーザーとグループのルール**］で、ユーザーまたはユーザーグループを選択します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。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。

   d. ［**OK**］をクリックします。

10. ［**選択されたアクセスルールのスケジュール**］で、ユーザーのストレージ機器のアクセススケジュールを設定します。

    たとえば、勤務時間中にのみストレージ機器へのユーザーアクセスを許可できます。

11. ファイルマネージャーで、ユーザーのストレージ機器へのアクセス権を設定します（**読み取り / 書き込み**）。

12. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

**Kaspersky Security Center Web コンソールでストレージ機器上のデータへのユーザーアクセス権を設定する方法**

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

2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。

   ［**デバイスコントロール**］ウィンドウが表示されます。

5. ［**デバイスコントロールを有効にする**］チェックボックスをオンにします。

6. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

7. ［**デバイスコントロール設定**］ブロックで、［**デバイスと Wi-Fi ネットワークのアクセスルール**］をクリックします。

   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

8. ［**ストレージ機器へのアクセス**］ブロックで、ストレージ機器のアクセスルールのプロパティを開きます。

9. ストレージ機器のアクセスルールを設定します：

   a. ［**ユーザー**］ブロックの［**追加**］をクリックします。

      新しいストレージ機器のアクセスルールを追加するウィンドウが開きます。

   b. ［**優先度**］フィールドで、*ルールの項目*の優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み）、優先度。

      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Embedded Systems Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Embedded Systems Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

      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。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Embedded Systems Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

   c. ［**ユーザー**］で、ユーザーまたはユーザーグループを選択します。ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。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。

   d. ［**デバイスへのアクセスのスケジュール**］で、ユーザーのストレージ機器のアクセススケジュールを設定します。

      たとえば、勤務時間中にのみストレージ機器へのユーザーアクセスを許可できます。

   e. ファイルマネージャーで、ユーザーのストレージ機器へのアクセス権を設定します（**読み取り / 書き込み**）。

   f. ［OK］をクリックします。

10. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

***Kaspersky Embedded Systems Security コンソールでストレージ機器上のデータへのユーザーアクセス権を設定する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。

2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。

   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。

3. ［**デバイスコントロール**］チェックボックスをオンにします。

4. ［**ブロックルールの操作モード**］ブロックで、［**ブロックする**］または［**通知する**を選択します。

5. ［**デバイスコントロール設定**］で、［**デバイス種別**］を選択します。

   デバイスコントロールの分類に含まれるすべてのデバイスのアクセスルールを表示するウィンドウが開きます。

6. ストレージ機器のアクセスルールを設定するには、ルールのリストをダブルクリックして開きます。

7. ストレージ機器のアクセスルールを設定します：

   a. ［**アクセスルール**］ブロックの［**追加**］をクリックします。

      新しいストレージ機器のアクセスルールを追加するウィンドウが開きます。

   b. ［**ルールの優先度**］フィールドで、*ルールの項目*の優先度を設定します。ルールには次の属性が含まれます：ユーザーアカウント、スケジュール、権限（読み取り/書き込み）、優先度。

      ルールには特定の優先度があります。ユーザーが複数のグループに追加されている場合、Kaspersky Embedded Systems Security は優先度が一番高いルールに基づいてデバイスへのアクセスを制限します。Kaspersky Embedded Systems Security では 0 から 10,000 までの優先度を割り当てられます。値が大きいほど優先度が高くなります。言い換えると、値「0」を割り当てられた項目は優先度が一番低くなります。

      例えば Everyone グループに読み取り専用権限を付与し、管理者グループに読み取り/書き込み権限を付与するなどです。その場合、管理者グループには優先度 1 を設定し、Everyone グループには 0 を設定します。

      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。言い換えると、ユーザーが複数グループに追加されており、すべてのルールの優先度が同じ場合、Kaspersky Embedded Systems Security は既存のブロックルールに基づいてデバイスへのアクセスを制限します。

   c. ［**ユーザーとグループのルール**］で、ユーザーまたはユーザーグループを選択します。ユーザーは、Active Directory で選択することも、ローカルユーザー名を手入力することもできます。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。

   d. ［OK］をクリックします。

8. ［**選択されたアクセスルールのスケジュール**］で、ユーザーのストレージ機器のアクセススケジュールを設定します。

   たとえば、勤務時間中にのみストレージ機器へのユーザーアクセスを許可できます。

9. ファイルマネージャーで、ユーザーのストレージ機器へのアクセス権を設定します（**読み取り / 書き込み**）。

10. 変更内容を保存します。

## 信頼するデバイスに対するユーザーアクセス権の区別

「*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。信頼するデバイスのプロパティでユーザーアクセス権を設定することができます。

# 外部デバイスの監査

信頼するデバイスのリストを作成するには、組織内の外部デバイスの監査を実施する必要があります。信頼するデバイスを追加するには、接続されているデバイスを選択し、そのデバイスに「信頼」のステータスを割り当てる必要があります。デバイスのリストは次の方法で取得できます：

- 通知モードのデバイスコントロールを有効にします。

  **Kaspersky Security Center 管理コンソールで通知モードのデバイスコントロールを有効にする方法**

  1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
  2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
  3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。
  4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。
  5. ［**デバイスコントロール**］チェックボックスをオンにします。
  6. ［**ブロックルールの操作モード**］で、［**通知する**］を選択します。
  7. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

  **Kaspersky Security Center Web コンソールで通知モードのデバイスコントロールを有効にする方法**

  1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
  2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。
     ［**デバイスコントロール**］ウィンドウが表示されます。
  5. ［**デバイスコントロールを有効にする**］チェックボックスをオンにします。
  6. ［**ブロックルールの操作モード**］で、［**通知する**］を選択します。
  7. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

**アプリケーションコンソールで通知モードのデバイスコントロールを有効にする方法**

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。
2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。
3. ［**デバイスコントロール**］チェックボックスをオンにします。
4. ［**ブロックルールの操作モード**］で、［**通知する**］を選択します。
5. 変更内容を保存します。

結果として、Kaspersky Embedded Systems Security は、外部デバイスの接続イベントと切断イベントを記録します。その後、機器レポートを生成し、レポートを分析して、信頼するデバイスを追加します。

- *デバイスコントロールルールの自動生成*タスクを実行します。

**Kaspersky Security Center 管理コンソールでデバイスコントロールルールの自動生成タスクを実行する方法**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**タスク**］を選択します。
3. *デバイスコントロールルールの自動生成*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を表示します。
   必要に応じて、新しいタスクを作成します。
4. ［**モード**］セクションで、処理モードを選択します：
   - **過去に接続されたすべての外部デバイスについてシステムデータを考慮する**
     本製品は、オペレーティングシステムのメモリから、コンピューターに接続されているすべてのデバイスに関する情報を取得します。
   - **現在接続している外部デバイスだけを考慮する**
     本製品は、タスクの開始時に接続されているデバイスに関する情報を取得します。
5. データを含むファイルを保存するパスを入力します。
6. 複数のコンピューターでタスクを実行する場合は、［**ファイル名に保護対象デバイスの詳細を追加する**］をオンにすることを推奨します。
7. 変更内容を保存します。
8. タスクを実行します。

### Kaspersky Security Center Web コンソールでデバイスコントロールルールの自動生成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、［**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. *デバイスコントロールルールの自動生成*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を表示します。
   必要に応じて、新しいタスクを作成します。
3. ［**モード**］セクションで、処理モードを選択します：
   - **過去に接続されたすべての外部デバイスについてシステムデータを考慮する**
     本製品は、オペレーティングシステムのメモリから、コンピューターに接続されているすべてのデバイスに関する情報を取得します。
   - **現在接続している外部デバイスだけを考慮する**
     本製品は、タスクの開始時に接続されているデバイスに関する情報を取得します。
4. データを含むファイルを保存するパスを入力します。
5. 複数のコンピューターでタスクを実行する場合は、［**ファイル名に保護対象デバイスの詳細を追加する**］をオンにすることを推奨します。
6. 変更内容を保存します。
7. タスクを実行します。

### アプリケーションコンソールでデバイスコントロールルールの自動生成タスクを開始する方法

1. Kaspersky Embedded Systems Security コンソールツリーで、［**ルールの自動生成**］→［**デバイスコントロールルールの自動生成**］の順に選択します。
2. ［**デバイスコントロールルールの自動生成**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: デバイスコントロールルールの自動生成**］ウィンドウが表示されます。
3. ［**モード**］セクションで、処理モードを選択します：
   - **過去に接続されたすべての外部デバイスについてシステムデータを考慮する**
     本製品は、オペレーティングシステムのメモリから、コンピューターに接続されているすべてのデバイスに関する情報を取得します。
   - **現在接続している外部デバイスだけを考慮する**
     本製品は、タスクの開始時に接続されているデバイスに関する情報を取得します。
4. ［**タスク完了後**］セクションで、タスク完了後の製品の処理を選択します：
   - **デバイスコントロールルールのリストに許可ルールを追加する**：デバイスコントロールルールのリストは、デバイスコントロール設定で確認できます。

このチェックボックスをオンにすると、選択した追加方法に基づいて、タスクによって生成されたルールが、デバイスコントロールルールのリストに追加されます。

このチェックボックスをオフにすると、新しく生成された許可ルールはデバイスコントロールルールのリストに追加されません。ルールがファイルにエクスポートされるだけです。

- **追加方法**：新しく生成された許可ルールをデバイスコントロールルールのリストに追加するために使用される方法です：
  - **既存のルールに追加する**：ルールが既存のルールのリストに追加されます。この場合、同一のルールが複製されます。
  - **既存のルールを置き換える**：既存のルールに代わって新しいルールが追加されます。
  - **既存のルールとマージする**：ルールが既存のルールのリストに追加されます。この場合、同一のルールが統合されます。
- **許可ルールをファイルにエクスポートする**：許可ルールが、下のフィールドで指定されたファイルにエクスポートされます。その後、他のコンピューターの製品設定にファイルをインポートして、許可ルールを配布できます。このファイルは許可ルールをバックアップするためにも使用できます。
- **ファイル名に保護対象デバイスの詳細を追加する**：エクスポートされたファイルの名前に、日付と時刻に加えて、コンピューター名が追加されます。これは、複数のコンピューターから許可ルールを収集する場合に便利です。

5. 変更内容を保存します。

これにより、Kaspersky Embedded Systems Security は外部デバイスの監査を実施し、その情報を Kaspersky Security Center のレジストリに保存します。信頼するデバイスの追加時に、外部デバイスのリストを使用することができます。

# 信頼するデバイスの追加

「*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。

信頼するデバイスを 1000 以上追加すると、システムが不安定になる可能性があるため推奨されません。

**Kaspersky Security Center 管理コンソールで信頼するデバイスを追加する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。

4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。

5. ［**デバイス監視の設定**］で、［**信頼するデバイス**］を選択します。
   信頼するデバイスのリストが開きます。

6. 組織内のすべてのコンピューターの信頼するデバイス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デバイスのリストが統合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシー内の信頼するデバイスは子ポリシー内では読み取り専用で表示されます。親ポリシー内の信頼するデバイスは編集または削除することはできません。

7. ［**追加**］をクリックし、デバイスを信頼リストに追加する方法を選択します。

   - **接続したデバイスに基づいてルールを生成**
   - **システムデータに基づいてルールを生成**
   - **Kaspersky Security Center レジストリに基づいたルールを生成**

   デバイスのリストが空の場合は、外部デバイスの監査を実施する必要があります。これを行うには、*デバイスコントロールルールの自動生成*タスクを実行します。

   > Kaspersky Embedded Systems Security は、**フロッピーディスク**の種別のデバイスの信頼リストへの追加をサポートしていません。

8. ［**選択したデバイスにルールを追加する**］をクリックします。

9. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

### 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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。
   ［**デバイスコントロール**］ウィンドウが表示されます。

5. ［**デバイスコントロール設定**］ブロックで、［**信頼するデバイス**］をクリックします。
   信頼するデバイスのリストが開きます。

6. 組織内のすべてのコンピューターの信頼するデバイス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デバイスのリストが統合されます。［継承時に値を統合する］がオンの時にリストが統合されます。親ポリシー内の信頼するデバイスは子ポリシー内では読み取り専用で表示されます。親ポリシー内の信頼するデバイスは編集または削除することはできません。

7. ［**KSC レジストリから**］をクリックします。

   デバイスのリストが空の場合は、外部デバイスの監査を実施する必要があります。これを行うには、*デバイスコントロールルールの自動生成*タスクを実行します。

   > Kaspersky Embedded Systems Security は、**フロッピーディスク**の種別のデバイスの信頼リストへの追加をサポートしていません。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（🔒）。

***アプリケーションコンソールで信頼するデバイスを追加する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。

2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。

   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。

3. ［**デバイスコントロール設定**］で、［**信頼するデバイス**］を選択します。

   信頼するデバイスのリストが開きます。

4. ［**追加**］をクリックし、デバイスを信頼リストに追加する方法を選択します。

   - **接続したデバイスに基づいてルールを生成**
   - **システムデータに基づいてルールを生成**
   - **Kaspersky Security Center レジストリに基づいたルールを生成**

   デバイスのリストが空の場合は、外部デバイスの監査を実施する必要があります。これを行うには、*デバイスコントロールルールの自動生成*タスクを実行します。

   > Kaspersky Embedded Systems Security は、**フロッピーディスク**の種別のデバイスの信頼リストへの追加をサポートしていません。

5. ［**選択したデバイスにルールを追加する**］をクリックします。

6. 変更内容を保存します。

# 信頼するデバイスのリストのエクスポート / インポート

信頼するデバイスのリストを組織内の他のコンピューターに配布するには、エクスポート / インポート手順を使用できます。信頼するデバイスのリストを XML 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、たとえば同じ種別の多数のデバイスをファイルを編集して追加することができます。また、エクスポートまたはインポート機能を使用して、信頼するデバイスのリスト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。

Kaspersky Embedded Systems Security では、Kaspersky Endpoint Security for Windows から、信頼するデバイスのリストをインポートできます。これらの製品のファイル形式は同じ XML です。

**Kaspersky Security Center 管理コンソールで信頼するデバイスのリストをエクスポートおよびインポートする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］を選択します。
4. ［**デバイスコントロール**］セクションで、［**設定**］をクリックします。
5. ［**デバイスコントロール設定**］で、［**信頼するデバイス**］を選択します。
   信頼するデバイスのリストが開きます。
6. 信頼するデバイスのリストをエクスポートするには：
   a. 編集する信頼するデバイスを選択します。
   b. をクリックして、エクスポートモードを選択します。信頼するデバイスのリスト全体をエクスポートするか、選択した信頼するデバイスのみをエクスポートします。
   c. 表示されたウィンドウで、信頼するデバイスのリストをエクスポートする XML 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。
      Web リソースのアドレスのリストが XML ファイルでエクスポートされます。
7. 信頼するデバイスのリストをインポートするには：
   a. ［**追加**］→［**XML ファイルからルールをインポート**］の順にクリックし、インポートモード（追加、置換）を選択します。
      表示されたウィンドウで、Web リソースのリストをインポートする XML ファイルを選択します。
      マージモードでは、本製品は信頼するデバイスのリストをチェックし、重複する項目を削除します。追加モードでは、本製品は重複をチェックせずに信頼するアプリケーションリストに項目を追加します。

b. ファイルを開きます。

Kaspersky Embedded Systems Security は、選択したモードに従って信頼するデバイスをインポートします。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

**Kaspersky Security Center Web コンソールで信頼するデバイスのリスト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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］→［**デバイスコントロール**］に移動し、［**設定**］をクリックします。

［**デバイスコントロール**］ウィンドウが表示されます。

5. ［**デバイスコントロール設定**］ブロックで、［**信頼するデバイス**］をクリックします。

信頼するデバイスのリストが開きます。

6. 信頼するデバイスのリストをエクスポートするには：

a. 編集する信頼するデバイスを選択します。

b. ［**エクスポート**］をクリックして、エクスポートモードを選択します。信頼するデバイスのリスト全体をエクスポートするか、選択した信頼するデバイスのみをエクスポートします。

c. ファイルを保存します。

Web リソースのアドレスのリストが XML ファイルでエクスポートされます。

7. 信頼するデバイスのリストをインポートするには：

a. ［**インポート**］をクリックして、インポートモード（追加または置換）を選択します。

b. 表示されたウィンドウで、Web リソースのリストをインポートする XML ファイルを選択します。

c. ファイルを開きます。

Kaspersky Embedded Systems Security は、選択したモードに従って信頼するデバイスをインポートします。

8. 変更内容を保存します。コンピューターにポリシーを適用するには、ロックを閉じます（）。

## *アプリケーションコンソールで信頼するデバイスのリストをエクスポートおよびインポートする方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**デバイスコントロール**］の順に選択します。
2. ［**デバイスコントロール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: デバイスコントロール**］ウィンドウが表示されます。
3. ［**デバイスコントロール設定**］で、［**信頼するデバイス**］を選択します。
   信頼するデバイスのリストが開きます。
4. 信頼するデバイスのリストをエクスポートするには：
   a. 編集する信頼するデバイスを選択します。
   b. をクリックして、エクスポートモードを選択します。信頼するデバイスのリスト全体をエクスポートするか、選択した信頼するデバイスのみをエクスポートします。
   c. 表示されたウィンドウで、信頼するデバイスのリストをエクスポートする XML 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。
      Web リソースのアドレスのリストが XML ファイルでエクスポートされます。
5. 信頼するデバイスのリストをインポートするには：
   a. ［**追加**］→［**XML ファイルからルールをインポート**］の順にクリックし、インポートモード（追加、置換）を選択します。
      表示されたウィンドウで、Web リソースのリストをインポートする XML ファイルを選択します。
      マージモードでは、本製品は信頼するデバイスのリストをチェックし、重複する項目を削除します。追加モードでは、本製品は重複をチェックせずに信頼するアプリケーションリストに項目を追加します。
   b. ファイルを開きます。
      Kaspersky Embedded Systems Security は、選択したモードに従って信頼するデバイスをインポートします。
6. 変更内容を保存します。

# ファイアウォール

ファイアウォールコンポーネントは次のモードで動作します：

- **Windows ファイアウォールの状態を確認する**：このモードは、バージョン 3.4 以前のファイアウォール管理タスクのロジックから、バージョン 4.0 以降のフル機能のファイアウォールへのスムーズな移行を目的として使用されます。バージョン 3.4 以前をアップグレードした場合は、Windows ファイアウォールに統合されたファイアウォール管理タスクのルールが保持されます。ただし、ファイアウォールコンポーネントは Windows ファイアウォールと連携しなくなり、Windows ファイアウォールのトラフィックのフィルタリングを監視し、対応するイベントをコンポーネントの操作ログに記録するだけになります。その後、ファイアウォールルールを作成したり、Windows ファイアウォールルールをインポートしたり、ファイアウォールの操作モードを［**通知**］に変更したりすることができます。

- **通知**：本製品は、ファイアウォールルールの操作を監視して、対応するイベントをコンポーネントの操作ログに記録することだけを行います。このモードは、ファイアウォールルールのテストを目的として使用されます。ファイアウォールの操作ログを使用して、その適用性を評価できます。その後、必要に応じてファイアウォールルールを調整したり、ファイアウォールの操作モードを［**ブロック**］に変更したりすることができます。

- **ブロック**：本製品は、コンポーネント設定に従ってネットワークトラフィックをフィルタリングし、対応するイベントをコンポーネントの操作ログに記録します。

# ファイアウォールのルールについて

［**ブロック**］モードが選択されている場合、ファイアウォールコンポーネントはファイアウォールルールを使用してネットワークトラフィックをフィルタリングします。

アプリケーションのファイアウォールルールは、指定されたアプリケーションのネットワーク接続を制御します。これらのルールの有効化の条件は、実行可能なアプリケーションへのパスに基づきます。

ファイアウォールポートルールは、指定されたポートとプロトコル（TCP / UDP）のネットワーク接続を制御します。このようなルールの適用条件は、プロトコルの種別とポートまたはポート範囲です。

ポートルールには、アプリケーションルールよりも広い範囲が含まれます。ポートルールに基づく接続を許可すると、保護対象コンピューターのセキュリティレベルが低下します。

# ファイアウォールの設定

このセクションでは、ファイアウォールタスクの全般設定を指定し、ファイアウォールコンポーネントを作成および設定する手順について説明します。

# ファイアウォールの全般的な設定

### Kaspersky Security Center 管理コンソールでのファイアウォールコンポーネントの全般的な設定

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ［**ネットワーク動作コントロール**］セクションで、［**ファイアウォール**］サブセクションの［**設定**］をクリックします。

   ［**ファイアウォール**］ウィンドウが表示されます。
4. ［**ブロックルールの操作モード**］ブロックの［**全般**］タブで、機能の操作モードを選択します：

   - **Windows ファイアウォールの状態を確認する**：このモードは、バージョン 3.4 以前のファイアウォール管理タスクのロジックから、バージョン 4.0 以降のフル機能のファイアウォールへのスムーズな移行を目的として使用されます。バージョン 3.4 以前をアップグレードした場合は、Windows ファイアウォールに統合されたファイアウォール管理タスクのルールが保持されます。ただし、ファイアウォールコンポーネントは Windows ファイアウォールと連携しなくなり、Windows ファイアウォールのトラフィックのフィルタリングを監視し、対応するイベントをコンポーネントの操作ログに記録するだけになります。その後、ファイアウォールルールを作成したり、Windows ファイアウォールルールをインポートしたり、ファイアウォールの操作モードを［**通知**］に変更したりすることができます。

   - **通知**：本製品は、ファイアウォールルールの操作を監視して、対応するイベントをコンポーネントの操作ログに記録することだけを行います。このモードは、ファイアウォールルールのテストを目的として使用されます。ファイアウォールの操作ログを使用して、その適用性を評価できます。その後、必要に応じてファイアウォールルールを調整したり、ファイアウォールの操作モードを［**ブロック**］に変更したりすることができます。

   - **ブロック**：本製品は、コンポーネント設定に従ってネットワークトラフィックをフィルタリングし、対応するイベントをコンポーネントの操作ログに記録します。
5. ［**インバウンド接続**］ブロックで、受信ネットワーク接続の設定を指定します。

   - ［**インバウンド接続に対する処理**］ドロップダウンリストを使用して、受信接続のファイアウォールルールで別途定義されていない限り、本製品がすべての受信ネットワーク接続に対して実行する処理を指定します。

   - 必要に応じて、受信接続用のファイアウォールルールを追加します。

     受信接続のファイアウォールルールは、除外リストの役割を果たします。たとえば、受信ネットワーク接続の許可ルールを設定し、［**インバウンド接続に対する処理**］ドロップダウンリストで［**ブロック**］を選択すると、本製品はルールの条件を満たす受信ネットワーク接続を許可します。

6. ［**アウトバウンド接続**］ブロックで、送信ネットワーク接続の設定を指定します。

   - ［**アウトバウンド接続に対する処理**］ドロップダウンリストを使用して、送信接続のファイアウォールルールで別途定義されていない限り、本製品がすべての送信ネットワーク接続に対して実行する処理を指定します。

   - 必要に応じて、送信接続用のファイアウォールルールを追加します。

     送信接続のファイアウォールルールは、除外リストの役割を果たします。たとえば、送信ネットワーク接続のブロックルールを設定し、［**アウトバウンド接続に対する処理**］ドロップダウンリストで［**許可**］を選択すると、本製品はルールの条件を満たす送信ネットワーク接続をブロックします。

7. 変更内容を保存します。

Kaspersky Embedded Systems Security でその新しい設定が適用されます。設定を変更した日時は、システム監査ログに保存されます。

### Kaspersky Security Center Web コンソールでのファイアウォールタスクの全般的な設定

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

2. Kaspersky Embedded Systems 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. ［**ネットワーク動作コントロール**］セクションで、［**ファイアウォール**］サブセクションの［**設定**］をクリックします。

   ［**ファイアウォール**］ウィンドウが表示されます。

5. スイッチを［**ファイアウォールは有効です**］に設定します。

6. ［**ブロックルールの操作モード**］ブロックで、機能の操作モードを選択します：

   - **Windows ファイアウォールの状態を確認する**：このモードは、バージョン 3.4 以前のファイアウォール管理タスクのロジックから、バージョン 4.0 以降のフル機能のファイアウォールへのスムーズな移行を目的として使用されます。バージョン 3.4 以前をアップグレードした場合は、Windows ファイアウォールに統合されたファイアウォール管理タスクのルールが保持されます。ただし、ファイアウォールコンポーネントは Windows ファイアウォールと連携しなくなり、Windows ファイアウォールのトラフィックのフィルタリングを監視し、対応するイベントをコンポーネントの操作ログに記録するだけになります。その後、ファイアウォールルールを作成したり、Windows ファイアウォールルールをインポートしたり、ファイアウォールの操作モードを［**通知**］に変更したりすることができます。

   - **通知**：本製品は、ファイアウォールルールの操作を監視して、対応するイベントをコンポーネントの操作ログに記録することだけを行います。このモードは、ファイアウォールルールのテストを目的として使用されます。ファイアウォールの操作ログを使用して、その適用性を評価できます。その後、必要に応じてファイアウォールルールを調整したり、ファイアウォールの操作モードを［**ブロック**］に変更したりすることができます。

   - **ブロック**：本製品は、コンポーネント設定に従ってネットワークトラフィックをフィルタリングし、対応するイベントをコンポーネントの操作ログに記録します。

7. ［**インバウンド接続**］ブロックで、受信ネットワーク接続の設定を指定します。

   - ［**インバウンド接続に対する処理**］ドロップダウンリストを使用して、受信接続のファイアウォールルールで別途定義されていない限り、本製品がすべての受信ネットワーク接続に対して実行する処理を指定します。

   - 必要に応じて、受信接続用のファイアウォールルールを追加します。

     受信接続のファイアウォールルールは、除外リストの役割を果たします。たとえば、受信ネットワーク接続の許可ルールを設定し、［**インバウンド接続に対する処理**］ドロップダウンリストで［**ブロック**］を選択すると、本製品はルールの条件を満たす受信ネットワーク接続を許可します。

8. ［**アウトバウンド接続**］ブロックで、送信ネットワーク接続の設定を指定します。

   - ［**アウトバウンド接続に対する処理**］ドロップダウンリストを使用して、送信接続のファイアウォールルールで別途定義されていない限り、本製品がすべての送信ネットワーク接続に対して実行する処理を指定します。

   - 必要に応じて、送信接続用のファイアウォールルールを追加します。

     送信接続のファイアウォールルールは、除外リストの役割を果たします。たとえば、送信ネットワーク接続のブロックルールを設定し、［**アウトバウンド接続に対する処理**］ドロップダウンリストで［**許可**］を選択すると、本製品はルールの条件を満たす送信ネットワーク接続をブロックします。

9. 変更内容を保存します。

Kaspersky Embedded Systems Security でその新しい設定が適用されます。設定を変更した日時は、システム監査ログに保存されます。

### *アプリケーションコンソールでのファイアウォールコンポーネントの全般的な設定*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**ファイアウォール**］の順に選択します。

2. ［**ファイアウォール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: ファイアウォール**］ウィンドウが表示されます。

3. ［**ファイアウォール**］チェックボックスをオンにします。

4. ［**ブロックルールの操作モード**］ブロックで、機能の操作モードを選択します：

   - **Windows ファイアウォールの状態を確認する**：このモードは、バージョン 3.4 以前のファイアウォール管理タスクのロジックから、バージョン 4.0 以降のフル機能のファイアウォールへのスムーズな移行を目的として使用されます。バージョン 3.4 以前をアップグレードした場合は、Windows ファイアウォールに統合されたファイアウォール管理タスクのルールが保持されます。ただし、ファイアウォールコンポーネントは Windows ファイアウォールと連携しなくなり、Windows ファイアウォールのトラフィックのフィルタリングを監視し、対応するイベントをコンポーネントの操作ログに記録するだけになります。その後、ファイアウォールルールを作成したり、Windows ファイアウォールルールをインポートしたり、ファイアウォールの操作モードを［**通知**］に変更したりすることができます。

   - **通知**：本製品は、ファイアウォールルールの操作を監視して、対応するイベントをコンポーネントの操作ログに記録することだけを行います。このモードは、ファイアウォールルールのテストを目的として使用されます。ファイアウォールの操作ログを使用して、その適用性を評価できます。その後、必要に応じてファイアウォールルールを調整したり、ファイアウォールの操作モードを［**ブロック**］に変更したりすることができます。

   - **ブロック**：本製品は、コンポーネント設定に従ってネットワークトラフィックをフィルタリングし、対応するイベントをコンポーネントの操作ログに記録します。

5. ［**インバウンド接続**］ブロックで、受信ネットワーク接続の設定を指定します。

   - ［**インバウンド接続に対する処理**］ドロップダウンリストを使用して、受信接続のファイアウォールルールで別途定義されていない限り、本製品がすべての受信ネットワーク接続に対して実行する処理を指定します。

   - 必要に応じて、受信接続用のファイアウォールルールを追加します。

     受信接続のファイアウォールルールは、除外リストの役割を果たします。たとえば、受信ネットワーク接続の許可ルールを設定し、［**インバウンド接続に対する処理**］ドロップダウンリストで［**ブロック**］を選択すると、本製品はルールの条件を満たす受信ネットワーク接続を許可します。

6. ［**アウトバウンド接続**］ブロックで、送信ネットワーク接続の設定を指定します。

   - ［**アウトバウンド接続に対する処理**］ドロップダウンリストを使用して、送信接続のファイアウォールルールで別途定義されていない限り、本製品がすべての送信ネットワーク接続に対して実行する処理を指定します。

   - 必要に応じて、送信接続用のファイアウォールルールを追加します。

     送信接続のファイアウォールルールは、除外リストの役割を果たします。たとえば、送信ネットワーク接続のブロックルールを設定し、［**アウトバウンド接続に対する処理**］ドロップダウンリストで［**許可**］を選択すると、本製品はルールの条件を満たす送信ネットワーク接続をブロックします。

7. 変更内容を保存します。

Kaspersky Embedded Systems Security でその新しい設定が適用されます。設定を変更した日時は、システム監査ログに保存されます。

# ファイアウォールルールの作成と設定

### Kaspersky Security Center 管理コンソールでのファイアウォールルールの作成と設定

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ［**ネットワーク動作コントロール**］セクションで、［**ファイアウォール**］サブセクションの［**設定**］をクリックします。
   ［**ファイアウォール**］ウィンドウが表示されます。
4. ［**インバウンド接続**］ブロックの［**ルールリスト**］をクリックします。
   ［**インバウンド接続に対するルール**］ウィンドウが表示されます。
5. **受信接続用のファイアウォールルールを作成および設定します**。

   1. ［**アプリケーション**］タブで［**追加**］をクリックします。
      ［**アプリケーションのルール**］ウィンドウが表示されます。
   2. ルールの設定を編集します：
      a. ［**ルール名**］にルール名を入力します。

      > ルールの名前は、文字の大文字と小文字に関係なく、予約名「All」「ICMPv4」「ICMPv6」と一致してはなりません。受信ネットワーク接続のすべてのルールのリスト内で一意である必要があります。

      b. ［**処理**］リストから、次のいずれかを選択します：
      - **許可**：このオプションをオンにすると、アプリケーションの受信ネットワーク接続を許可します。
      - **ブロック**：このオプションをオンにすると、アプリケーションの受信ネットワーク接続をブロックします。

      c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。
      d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。
      e. ［**アプリケーションのパス**］フィールドに、手動で、または［**参照**］を使用して、ルールを設定するアプリケーションの実行ファイルへのパスを指定します。

f. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの受信接続が監視されます。

> IP アドレスでは IPv4 形式のみがサポートされます。

g. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

h. ［**OK**］をクリックしてルールを保存します。

3. ［**ローカルポート**］タブで［**追加**］をクリックします。
［**ポートのルール**］ウィンドウが表示されます。

4. ルールの設定を編集します：

a. ［**ルール名**］にルール名を入力します。

b. ［**処理**］リストから、次のいずれかを選択します：

- **許可**：このオプションをオンにすると、ポートへの受信ネットワーク接続を許可します。
- **ブロック**：このオプションをオンにすると、ポートへの受信ネットワーク接続をブロックします。

c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

e. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの受信接続が監視されます。

> IP アドレスでは IPv4 形式のみがサポートされます。

f. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

g. ［**OK**］をクリックしてルールを保存します。

5. ［**インバウンド接続に対するルール**］ウィンドウの［**OK**］をクリックします。

6. ［**アウトバウンド接続**］ブロックの［**ルールリスト**］をクリックします。
［**アウトバウンド接続に対するルール**］ウィンドウが表示されます。

7. **送信接続用のファイアウォールルールを作成および設定します**。

1. ［**アプリケーション**］タブで［**追加**］をクリックします。
［**アプリケーションのルール**］ウィンドウが表示されます。

2. ルールの設定を編集します：

a. ［**ルール名**］にルール名を入力します。

ルールの名前は、文字の大文字と小文字に関係なく、予約名「All」「ICMPv4」「ICMPv6」と一致してはなりません。送信ネットワーク接続のすべてのルールのリスト内で一意である必要があります。

b. ［**処理**］リストから、次のいずれかを選択します：

- **許可**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続を許可します。
- **ブロック**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続をブロックします。

c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

e. ［**アプリケーションのパス**］フィールドに、手動で、または［**参照**］を使用して、ルールを設定するアプリケーションの実行ファイルへのパスを指定します。

f. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

IP アドレスでは IPv4 形式のみがサポートされます。

g. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

h. ［OK］をクリックしてルールを保存します。

3. ［**ポート**］タブで［**追加**］をクリックします。
［**ポートのルール**］ウィンドウが表示されます。

4. ルールの設定を編集します：

a. ［**ルール名**］にルール名を入力します。

b. ［**処理**］リストから、次のいずれかを選択します：

- **許可**：このオプションをオンにすると、ポートへの発信ネットワーク接続を許可します。
- **ブロック**：このオプションをオンにすると、ポートへの発信ネットワーク接続をブロックします。

c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

e. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

IP アドレスでは IPv4 形式のみがサポートされます。

f. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

g. ［OK］をクリックしてルールを保存します。

5. ［**アウトバウンド接続に対するルール**］ウィンドウの［OK］をクリックします。

8. XML ファイルからカスタムルールをインポートまたはエクスポートする場合は、［**ルールのインポートとエクスポート**］ブロックの［**インポート**］または［**エクスポート**］を使用します。

9. 変更内容を保存します。

Kaspersky Embedded Systems Security でその新しい設定が適用されます。設定を変更した日時は、システム監査ログに保存されます。

### Kaspersky Security Center Web コンソールでのファイアウォールルールの作成と設定

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

2. Kaspersky Embedded Systems 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. ［**ネットワーク動作コントロール**］セクションで、［**ファイアウォール**］サブセクションの［**設定**］をクリックします。
［**ファイアウォール**］ウィンドウが表示されます。

5. スイッチを［**ファイアウォールは有効です**］に設定します。

6. ［**インバウンド接続**］ブロックの［**設定**］をクリックします。
［**インバウンド接続に対するルール**］ウィンドウが表示されます。

7. 受信接続用のファイアウォールルールを作成および設定します。

1. ［**ローカルポート**］タブで［**追加**］をクリックします。
［**ポートのルール**］ウィンドウが表示されます。

2. ルールの設定を編集します：

   a. ［**ルール名**］にルール名を入力します。

   b. ［**処理**］リストから、次のいずれかを選択します：

      - **許可**：このオプションをオンにすると、ポートへの発信ネットワーク接続を許可します。
      - **拒否**：このオプションをオンにすると、ポートへの発信ネットワーク接続をブロックします。

   c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

   d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

   e. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

      IP アドレスでは IPv4 形式のみがサポートされます。

   f. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

   g. ［OK］をクリックしてルールを保存します。

3. ［**アプリケーション**］タブで［**追加**］をクリックします。
   ［**アプリケーションのルール**］ウィンドウが表示されます。

4. ルールの設定を編集します：

   a. ［**ルール名**］にルール名を入力します。

      ルールの名前は、文字の大文字と小文字に関係なく、予約名「All」「ICMPv4」「ICMPv6」と一致してはなりません。送信ネットワーク接続のすべてのルールのリスト内で一意である必要があります。

   b. ［**処理**］リストから、次のいずれかを選択します：

      - **許可**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続を許可します。
      - **拒否**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続をブロックします。

   c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

   d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

e. ［**アプリケーションパス**］フィールドでルールを設定するアプリケーションの実行ファイルへのパスを手動で指定します。

f. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

> IP アドレスでは IPv4 形式のみがサポートされます。

g. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

h. ［OK］をクリックしてルールを保存します。

5. ［**インバウンド接続に対するルール**］ウィンドウの［OK］をクリックします。

8. ［**アウトバウンド接続**］ブロックの［**設定**］をクリックします。
［**アウトバウンド接続に対するルール**］ウィンドウが表示されます。

9. 送信接続用のファイアウォールルールを作成および設定します。

1. ［**ローカルポート**］タブで［**追加**］をクリックします。
［**ポートのルール**］ウィンドウが表示されます。

2. ルールの設定を編集します：

a. ［**ルール名**］にルール名を入力します。

b. ［**処理**］リストから、次のいずれかを選択します：

- **許可**：このオプションをオンにすると、ポートへの発信ネットワーク接続を許可します。
- **拒否**：このオプションをオンにすると、ポートへの発信ネットワーク接続をブロックします。

c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

e. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

> IP アドレスでは IPv4 形式のみがサポートされます。

f. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

g. ［OK］をクリックしてルールを保存します。

3. ［**アプリケーション**］タブで［**追加**］をクリックします。
［**アプリケーションのルール**］ウィンドウが表示されます。

4. ルールの設定を編集します：

a. ［**ルール名**］にルール名を入力します。

ルールの名前は、文字の大文字と小文字に関係なく、予約名「All」「ICMPv4」「ICMPv6」と一致してはなりません。送信ネットワーク接続のすべてのルールのリスト内で一意である必要があります。

b. ［**処理**］リストから、次のいずれかを選択します：

- **許可**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続を許可します。
- **拒否**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続をブロックします。

c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

e. ［**アプリケーションパス**］フィールドでルールを設定するアプリケーションの実行ファイルへのパスを手動で指定します。

f. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

IP アドレスでは IPv4 形式のみがサポートされます。

g. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

h. ［OK］をクリックしてルールを保存します。

5. ［**アウトバウンド接続に対するルール**］ウィンドウの［OK］をクリックします。

10. XML ファイルからカスタムルールをインポートまたはエクスポートする場合は、［**ルールのインポートとエクスポート**］ブロックの［**ルールのインポート**］または［**ルールのエクスポート**］を使用します。

11. 変更内容を保存します。

Kaspersky Embedded Systems Security でその新しい設定が適用されます。設定を変更した日時は、システム監査ログに保存されます。

## *アプリケーションコンソールでのファイアウォールルールの作成と設定*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**ファイアウォール**］の順に選択します。
2. ［**ファイアウォール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: ファイアウォール**］ウィンドウが表示されます。
3. ［**インバウンド接続**］ブロックの［**ルールリスト**］をクリックします。
   ［**インバウンド接続に対するルール**］ウィンドウが表示されます。
4. 受信接続用のファイアウォールルールを作成および設定します。

   1. ［**アプリケーション**］タブで［**追加**］をクリックします。
      ［**アプリケーションのルール**］ウィンドウが表示されます。
   2. ルールの設定を編集します：
      a. ［**ルール名**］にルール名を入力します。

         ルールの名前は、文字の大文字と小文字に関係なく、予約名「All」「ICMPv4」「ICMPv6」と一致してはなりません。受信ネットワーク接続のすべてのルールのリスト内で一意である必要があります。

      b. ［**処理**］リストから、次のいずれかを選択します：
         - **許可**：このオプションをオンにすると、アプリケーションの受信ネットワーク接続を許可します。
         - **ブロック**：このオプションをオンにすると、アプリケーションの受信ネットワーク接続をブロックします。

      c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。
      d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。
      e. ［**アプリケーションのパス**］フィールドに、手動で、または［**参照**］を使用して、ルールを設定するアプリケーションの実行ファイルへのパスを指定します。
      f. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの受信接続が監視されます。

         IP アドレスでは IPv4 形式のみがサポートされます。

      g. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。
      h. ［OK］をクリックしてルールを保存します。

3. ［**ローカルポート**］タブで［**追加**］をクリックします。
   ［**ポートのルール**］ウィンドウが表示されます。

4. ルールの設定を編集します：

   a. ［**ルール名**］にルール名を入力します。

   b. ［**処理**］リストから、次のいずれかを選択します：

      - **許可**：このオプションをオンにすると、ポートへの受信ネットワーク接続を許可します。
      - **ブロック**：このオプションをオンにすると、ポートへの受信ネットワーク接続をブロックします。

   c. ［**プロトコル**］をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

   d. ［**ローカルポート**］ブロックと［**リモートポート**］ブロックで、ポートまたはポートの範囲を指定します。

   e. ［**ルールの使用範囲**］フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの受信接続が監視されます。

      IP アドレスでは IPv4 形式のみがサポートされます。

   f. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

   g. ［OK］をクリックしてルールを保存します。

5. ［**インバウンド接続に対するルール**］ウィンドウの［OK］をクリックします。

5. ［**アウトバウンド接続**］ブロックの［**ルールリスト**］をクリックします。
   ［**アウトバウンド接続に対するルール**］ウィンドウが表示されます。

6. **送信接続用のファイアウォールルールを作成および設定します**。

   1. ［**アプリケーション**］タブで［**追加**］をクリックします。
      ［**アプリケーションのルール**］ウィンドウが表示されます。

   2. ルールの設定を編集します：

      a. ［**ルール名**］にルール名を入力します。

         ルールの名前は、文字の大文字と小文字に関係なく、予約名「All」「ICMPv4」「ICMPv6」と一致してはなりません。送信ネットワーク接続のすべてのルールのリスト内で一意である必要があります。

b. [**処理**] リストから、次のいずれかを選択します：

- **許可**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続を許可します。
- **ブロック**：このオプションをオンにすると、アプリケーションの送信ネットワーク接続をブロックします。

c. [**プロトコル**] をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

d. [**ローカルポート**] ブロックと [**リモートポート**] ブロックで、ポートまたはポートの範囲を指定します。

e. [**アプリケーションのパス**] フィールドに、手動で、または [**参照**] を使用して、ルールを設定するアプリケーションの実行ファイルへのパスを指定します。

f. [**ルールの使用範囲**] フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

> IP アドレスでは IPv4 形式のみがサポートされます。

g. [**ネットワークアダプター**] ブロックで、ネットワークアダプターのリストを指定します。

h. [OK] をクリックしてルールを保存します。

3. [**ポート**] タブで [**追加**] をクリックします。
[**ポートのルール**] ウィンドウが表示されます。

4. ルールの設定を編集します：

a. [**ルール名**] にルール名を入力します。

b. [**処理**] リストから、次のいずれかを選択します：

- **許可**：このオプションをオンにすると、ポートへの発信ネットワーク接続を許可します。
- **ブロック**：このオプションをオンにすると、ポートへの発信ネットワーク接続をブロックします。

c. [**プロトコル**] をオンにして、本製品が受信ネットワーク接続を制御するプロトコル種別を選択します。

d. [**ローカルポート**] ブロックと [**リモートポート**] ブロックで、ポートまたはポートの範囲を指定します。

e. [**ルールの使用範囲**] フィールドで、ネットワークアドレスを指定します。ルール設定に従って、指定されたネットワーク アドレスからの送信接続が監視されます。

> IP アドレスでは IPv4 形式のみがサポートされます。

f. ［**ネットワークアダプター**］ブロックで、ネットワークアダプターのリストを指定します。

g. ［**OK**］をクリックしてルールを保存します。

5. ［**アウトバウンド接続に対するルール**］ウィンドウの［**OK**］をクリックします。

7. XML ファイルからカスタムルールをインポートまたはエクスポートする場合は、［**ルールのインポートとエクスポート**］ブロックの［**インポート**］または［**エクスポート**］を使用します。

8. Windows ファイアウォールルールをインポートするには、［**Windows ファイアウォールルールをインポート**］をクリックします。

Windows 11 24H2 コンピューターでは、本製品が特定の Windows ファイアウォールルールをスキップする場合があります。このバージョンのオペレーティングシステムの特殊な機能により、Kaspersky Embedded Systems Security はアプリケーションパケットの一部のルールのパラメータを認識しない場合があります。

9. 変更内容を保存します。

Kaspersky Embedded Systems Security でその新しい設定が適用されます。設定を変更した日時は、システム監査ログに保存されます。

# ファイアウォールのルールの有効化と無効化

### Kaspersky Security Center 管理コンソールでのファイアウォールルールの作成と設定

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ［**ネットワーク動作コントロール**］セクションで、［**ファイアウォール**］サブセクションの［**設定**］をクリックします。
［**ファイアウォール**］ウィンドウが表示されます。

4. 表示されたウィンドウで、ステータスを変更するルールの種別に応じて、［**インバウンド接続**］または［**アウトバウンド接続**］セクションで［**ルールリスト**］をクリックします。

5. 表示されたウィンドウで、［**アプリケーション**］タブまたは［**ローカルポート**］タブを選択します。
ルールリストで、ステータスを変更するルールを選択し、次のいずれかの処理を実行します：

- 無効なルールを有効にする場合、ルール名の左側のチェックボックスをオンにします。
選択したルールが有効になります。

- 有効なルールを無効にする場合、ルール名の左側のチェックボックスをオフにします。
選択したルールが無効になります。

6. リストからルールを削除するには、ルールを選択して［**削除**］をクリックします。

7. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでのファイアウォールルールの作成と設定

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

2. Kaspersky Embedded Systems 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. ［**ネットワーク動作コントロール**］セクションで、［**ファイアウォール**］サブセクションの［**設定**］をクリックします。
   ［**ファイアウォール**］ウィンドウが表示されます。

5. 表示されたウィンドウで、ステータスを変更するルールの種別に応じて、［**インバウンド接続**］または［**アウトバウンド接続**］セクションで［**設定**］をクリックします。

6. 表示されたウィンドウで、［**ローカルポート**］タブまたは［**アプリケーション**］タブを選択します。
   ルールリストで、ステータスを変更するルールを選択し、次のいずれかの処理を実行します：

   - 無効なルールを有効にする場合、ルール名の左側のチェックボックスをオンにします。
     選択したルールが有効になります。
   - 有効なルールを無効にする場合、ルール名の左側のチェックボックスをオフにします。
     選択したルールが無効になります。

7. リストからルールを削除するには、ルールを選択して［**削除**］をクリックします。

8. 変更内容を保存します。

### *アプリケーションコンソールでのファイアウォールルールの作成と設定*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターコントロール**］→［**ファイアウォール**］の順に選択します。

2. ［**ファイアウォール**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: ファイアウォール**］ウィンドウが表示されます。

3. 表示されたウィンドウで、ステータスを変更するルールの種別に応じて、［**インバウンド接続**］または［**アウトバウンド接続**］セクションで［**ルールリスト**］をクリックします。

4. 表示されたウィンドウで、［**アプリケーション**］タブまたは［**ローカルポート**］タブを選択します。

ルールリストで、ステータスを変更するルールを選択し、次のいずれかの処理を実行します：

- 無効なルールを有効にする場合、ルール名の左側のチェックボックスをオンにします。
  選択したルールが有効になります。
- 有効なルールを無効にする場合、ルール名の左側のチェックボックスをオフにします。
  選択したルールが無効になります。

5. リストからルールを削除するには、ルールを選択して［**削除**］をクリックします。

6. 変更内容を保存します。

# 有害 USB 攻撃ブロック

有害 USB 攻撃ブロックは、既定ではインストールされません。本製品のインストール中にコンポーネントを追加することも、本製品のインストール後に一連のアプリケーションコンポーネントを変更することもできます。

ウイルスの中には、オペレーティングシステムで USB デバイスがキーボードとして検知されるように、USB デバイスのファームウェアを改竄するものがあります。ウイルスはマルウェアなどをダウンロードするためにユーザーのアカウントでコマンドを実行する可能性があります。

有害 USB 攻撃ブロックは、感染した USB デバイスがキーボードの動作を模倣してコンピューターに接続することを防ぎます。

コンピューターに接続された USB デバイスをオペレーティングシステムがキーボードとして識別した場合、製品によって生成された数値コードを、このキーボードまたは使用可能な場合はセキュリティキーボードから入力するようユーザーに要求します。この手順をキーボード承認と呼びます。

コードが正しく入力されると、識別パラメータ（キーボードの VID および PID、キーボードが接続されたポート番号）が、認証されたキーボードのリストに保存されます。キーボードが再度接続されたときやオペレーティングシステムの再起動後に、認証が繰り返されることはありません。

認証されたキーボードが別のコンピューターの USB ポートに接続されると、このキーボードの認証が再度要求されます。

数値コードが正しく入力されなかった場合、新しいコードが生成されます。数値コードの入力試行回数は指定できます。数値コードの入力を複数回誤ったりキーボードの認証ウィンドウを閉じた場合、本製品はキーボードからの入力をブロックします。USB デバイスのブロック時間の経過後もしくはオペレーティングシステムの再起動後に、キーボード認証を再度実行するようユーザーに要求します。

承認されたキーボードの使用は許可され、承認されなかったキーボードの使用はブロックされます。

有害 USB 攻撃ブロックのインストール前にオペレーティングシステムによってキーボードとして識別され、コンピューターに接続された USB デバイスは、コンポーネントのインストール後は、認証済みとみなされます。

**Kaspersky Security Center 管理コンソールで有害 USB 攻撃ブロックを有効にして設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ローカル動作コントロール**］をクリックします。
4. ［**有害 USB 攻撃ブロック**］ブロックの［**設定**］をクリックします。
   ［**有害 USB 攻撃ブロック**］ウィンドウが表示されます。
5. ［**有害 USB 攻撃ブロック**］を使用して機能を有効または無効にします。

6. ［**USB デバイスの認証**］セクションで、次の設定を行います：

   - **USB デバイスの最大認証試行回数**：認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。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 回目に失敗したあとに USB デバイスがブロックされます。Kaspersky Embedded Systems Security は USB デバイスをブロックす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。

   - **最大試行回数を超えた場合のタイムアウト（分）**：認証コードの入力の失敗回数が指定した回数を超えた後に USB デバイスをブロックする時間です。有効な値は 1 ～ 180（分）です。

7. ［**USB デバイスの接続時の認証**］セクションで、次の設定を行います：

   - **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**：このチェックボックスをオンにすると、認証用のコードが入力できない USB デバイス（バーコードスキャナーなど）の認証時に、セキュリティキーボードの使用をブロックします。

   - **USB デバイスの認証時にバーコードの使用を禁止する**：このチェックボックスをオンにすると、バーコードスキャナーの認証の通知にバーコードが表示されません。

8. コンピューターにポリシーを適用するには、南京錠（）を閉じます。

9. ［**OK**］をクリックして、変更内容を保存します。

### Kaspersky Security Center Web コンソールで有害 USB 攻撃ブロックを有効にして設定する方法

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

2. Kaspersky Embedded Systems 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. ［**ローカル動作コントロール**］セクションを選択します。

5. ［**有害 USB 攻撃ブロック**］ブロックの［**設定**］をクリックします。
   ［**有害 USB 攻撃ブロック**］ウィンドウが表示されます。

6. ［**有害 USB 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。

7. ［［**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**］**が有効です**］スイッチをオンまたはオフにして、認証用のコードが入力できない USB デバイス（バーコードスキャナーなど）の認証時に、セキュリティキーボードの使用を許可またはブロックします。

8. ［［**USB デバイスの認証時にバーコードの使用を禁止する**］**が有効です**］スイッチをオンまたはオフにして、バーコードスキャナーの認証の通知でバーコードの表示を許可またはブロックします。

9. ［**USB デバイスの認証**］セクションで、次の設定を行います：

   - **USB デバイスの最大認証試行回数（1〜10）**：認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。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 回目に失敗したあとに USB デバイスがブロックされます。Kaspersky Embedded Systems Security は USB デバイスをブロックす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。

   - **最大試行回数を超えた場合のタイムアウト（分、1〜180）**：認証コードの入力の失敗回数が指定した回数を超えた後に USB デバイスをブロックする時間です。有効な値は 1 〜 180（分）です。

10. コンピューターにポリシーを適用するには、南京錠（）を閉じます。

11. ［**OK**］をクリックして、変更内容を保存します。

***アプリケーションコンソールで有害 USB 攻撃ブロックを有効にして設定する方法***

1. コンソールツリーで、［**コンピューターコントロール**］→［**有害 USB 攻撃ブロック**］セクションを選択します。

2. 結果ペインで［**プロパティ**］をクリックします。
   ［**有害 USB 攻撃ブロック**］ウィンドウが表示されます。

3. ［**有害 USB 攻撃ブロック**］を使用して機能を有効または無効にします。

4. ［**USB デバイスの認証**］セクションで、次の設定を行います：

   - **USB デバイスの最大認証試行回数**：認証コードの入力の失敗回数が指定した回数を超えると自動的に USB デバイスがブロックされます。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 回目に失敗したあとに USB デバイスがブロックされます。Kaspersky Embedded Systems Security は USB デバイスをブロックす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。

   - **最大試行回数を超えた場合のタイムアウト（分）**：認証コードの入力の失敗回数が指定した回数を超えた後に USB デバイスをブロックする時間です。有効な値は 1 〜 180（分）です。

5. ［**USB デバイスの接続時の認証**］セクションで、次の設定を行います：

   - **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**：このチェックボックスをオンにすると、認証用のコードが入力できない USB デバイス（バーコードスキャナーなど）の認証時に、セキュリティキーボードの使用をブロックします。

   - **USB デバイスの認証時にバーコードの使用を禁止する**：このチェックボックスをオンにすると、バーコードスキャナーの認証の通知にバーコードが表示されません。

6. ［**OK**］をクリックして、変更内容を保存します。

# システム変更監視

Kaspersky Embedded Systems Security 4.0 には、ファイル変更監視コンポーネントの代わりにシステム変更監視コンポーネントが含まれるようになりました。システム変更監視コンポーネントには、ファイル変更監視のすべての機能が含まれており、さらにレジストリの変更や外部デバイスの接続を監視することもできます。

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 Embedded Systems Security は対応するイベントを生成し、管理者に警告します。システム変更監視はリアルタイムモードで動作しますが、オンデマンドでシステム変更チェックを実行することもできます。

## リアルタイムシステム変更監視

リアルタイムモードで、システム変更監視は、コンポーネントの範囲（監視範囲）に含めたオブジェクトへの変更を追跡します。システム変更監視では、このようなオブジェクトへの不正アクセスをリアルタイムでブロックすることもできます。

## オンデマンドのシステム変更チェック

オンデマンドのシステム変更チェックは、手動で実行することも、スケジュールに従って実行することもできるタスクです。**ベースラインシステム変更監視**タスクを実行するには、コンポーネントの範囲（監視範囲）を設定して、ベースラインを作成します。ベースラインとは、システム内のオブジェクトの記録された状態であり、現在の状態と比較する際に参照用に使用されます。ベースラインは、タスクが最初に開始された時に作成されます。

## ファイル変更監視の設定の移行

Kaspersky Embedded Systems Security バージョン 3.4 以前をバージョン 4.0 にアップデートすると、ファイル変更監視とレジストリアクセス監視の設定が自動的に移行されます。移行の一環として、監視ルールがシステム変更監視に移動されます。

# システム変更監視ルールについて

システム変更監視が機能するには、ルールを少なくとも 1 つ追加する必要があります。*システム変更監視ルール*とは、ファイルまたはレジストリへのユーザーのアクセスを定義する一連の条件です。システム変更監視は、指定された*監視範囲*内のファイルまたはレジストリの変更を検知します。監視範囲は、システム変更監視ルールの条件の 1 つです。

システム変更監視では、次のオブジェクトを監視できます：

- ファイル
- レジストリ
- 外部デバイス

## ファイル監視に関する特別な考慮事項

システム変更監視は、ファイルとフォルダーの変更、および監視範囲に追加されるファイルや監視範囲から削除されるファイルについて監視します。これらの変更はコンピューターのセキュリティ侵害を示す可能性があります。管理者のみがアクセス可能なオブジェクトや、めったに変更されないオブジェクトを追加することを推奨します。これにより、システム変更監視イベントの数を減らすことができます。

Kaspersky Embedded Systems Security は、リアルタイムシステム変更監視が動作を開始したときに接続されていたディスク上のファイルとフォルダーの変更のみを監視します。リアルタイムシステム変更監視が動作を開始したときにディスクが接続されていなかった場合、監視範囲にファイルとフォルダーが追加されても、本製品はそのディスク上のファイルとフォルダーの変更を監視しません。

## レジストリ監視に関する特別な考慮事項

システム変更監視はレジストリを監視します。これらの変更はコンピューターのセキュリティ侵害を示す可能性があります。

システム変更監視は、レジストリの次のルートキーを監視します：

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

システム変更監視は、HKEY_CURRENT_USER キーをサポートしません。HKEY_USERS の下に、HKEY_USERS\<user profile ID>\<key> という形式でキーを指定できます。

## 外部デバイスの監視に関する特別な考慮事項

システム変更監視は、外部デバイスの接続と接続解除を監視します。これは、それらのデバイスとのファイル交換によって生じる可能性のあるセキュリティ上の脅威からコンピューターを保護するために必要となります。システム変更監視では、外部デバイスへのアクセスを監視せず、ファイル交換もブロックしません。別のアプリケーションコンポーネントのデバイスコントロールを使用してデバイスへのアクセスを設定することができます。

ベースラインシステム変更監視タスクの実行中、外部デバイスがオペレーティングシステムで同じドライブ文字を持つ場合、本製品は外部デバイスの再接続を無視します。ログに記録するには、再接続されるデバイスのドライブ文字が異なっている必要があります。

システム変更監視は、次の種別の外部デバイスの接続を監視します：

- リムーバブルドライブ（USB フラッシュドライブを含む）
- ハードディスク
- 外部ネットワークアダプター
- CD/DVD/Blu-ray ドライブ
- スキャナーとカメラ

# リアルタイムシステム変更監視

システム変更監視により、オペレーティングシステムの変更をリアルタイムで追跡できます。コンピューターでのセキュリティ侵害を示す可能性がある変更を追跡することが可能です。このコンポーネントを使用すると、これらの変更をブロックすることも、変更イベントをただログ記録することもできます。

システム変更監視が機能するには、ルールを少なくとも 1 つ追加する必要があります。システム変更監視ルールとは、ファイルおよびレジストリへのユーザーのアクセスを定義する一連の条件です。システム変更監視は、指定された監視範囲内のファイルとレジストリの変更を検知します。監視範囲は、システム変更監視ルールの条件の 1 つです。

**Kaspersky Security Center 管理コンソールでリアルタイムシステム変更監視を有効にして設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**システム監査**］を選択します。
4. ［**システム変更監視**］セクションで、［**設定**］をクリックします。
5. ［**システム変更監視**］チェックボックスをオンにします。
6. ファイル変更監視を設定します：
   a. ［**ファイル**］タブにある［**ファイルを監視する**］をオンにします。
   b. ［**ブロックルールの操作モード**］で、ファイル変更監視のモードを選択します：
      - **ブロックする**：このモードでは、ファイル変更監視ルールに従ってファイルに対する処理が実行されて、対応するイベントがシステム変更監視ログに生成されます。
      - **通知する**：このモードでは、適用されたファイル変更監視ルールに関するイベントのみがシステム変更監視ログに生成されます。
   c. 手動で［**追加**］を使用するか、XML ファイルからインポートして、ファイル整合性監視ルールを追加します。次のテーブルでは、ファイル変更監視ルールの設定について説明します。
   d. ファイル整合性監視ルールのリストで、チェックボックスを管理して、必要なルールを有効のままにします。

7. レジストリアクセス監視を設定します：

   a. ［**レジストリ**］タブにある［**レジストリを監視する**］をオンにします。

   b. ［**ブロックルールの操作モード**］の下で、レジストリアクセス監視のモードを選択します。

      - **ブロックする**：このモードでは、レジストリアクセス監視ルールに従ってレジストリに対する処理がブロックされて、対応するイベントがシステム変更監視ログに生成されます。

      - **通知する**：このモードでは、適用されたレジストリアクセス監視ルールに関するイベントのみがシステム変更監視ログに生成されます。

   c. 手動で［**追加**］を使用するか、XML ファイルからインポートして、レジストリアクセス監視ルールを追加します。次のテーブルでは、レジストリアクセス監視ルールの設定について説明します。

   d. レジストリアクセス監視ルールのリストで、チェックボックスを管理して、必要なルールを有効のままにします。

8. 外部デバイスの監視を設定します：

   a. ［**デバイス**］タブにある［**デバイスを監視する**］をオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

      外部デバイスの監視設定を適用すると、本製品で現在の外部デバイスの接続が記憶されます。その後、外部デバイスが接続または接続解除されると、対応するイベントがシステム変更監視ログに生成されます。

9. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでリアルタイムシステム変更監視を有効にして設定する方法**

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

2. Kaspersky Embedded Systems 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. ［**システム監査**］→［**システム変更監視**］に移動し、［**設定**］をクリックします。

5. ［**システム変更監視**］チェックボックスをオンにします。

6. ファイル変更監視を設定します：

   a. ［**ファイル**］タブにある［**ファイルを監視する**］をオンにします。

   b. ［**ブロックルールの操作モード**］で、ファイル変更監視のモードを選択します：

      - **ブロックする**：このモードでは、ファイル変更監視ルールに従ってファイルに対する処理が実行されて、対応するイベントがシステム変更監視ログに生成されます。

      - **通知する**：このモードでは、適用されたファイル変更監視ルールに関するイベントのみがシステム変更監視ログに生成されます。

   c. 手動で［**追加**］を使用するか、XML ファイルからインポートして、ファイル整合性監視ルールを追加します。次のテーブルでは、ファイル変更監視ルールの設定について説明します。

   d. ファイル整合性監視ルールのリストで、［**ステータス**］列のチェックボックスを管理して、必要なルールを有効のままにします。

7. レジストリアクセス監視を設定します：

   a. ［**レジストリ**］タブにある［**レジストリを監視する**］をオンにします。

   b. ［**ブロックルールの操作モード**］の下で、レジストリアクセス監視のモードを選択します。

      - **ブロックする**：このモードでは、レジストリアクセス監視ルールに従ってレジストリに対する処理がブロックされて、対応するイベントがシステム変更監視ログに生成されます。

      - **通知する**：このモードでは、適用されたレジストリアクセス監視ルールに関するイベントのみがシステム変更監視ログに生成されます。

   c. 手動で［**追加**］を使用するか、XML ファイルからインポートして、レジストリアクセス監視ルールを追加します。次のテーブルでは、レジストリアクセス監視ルールの設定について説明します。

   d. レジストリアクセス監視ルールのリストで、［**ステータス**］列のチェックボックスを管理して、必要なルールを有効のままにします。

8. 外部デバイスの監視を設定します：

   a. ［**デバイス**］タブにある［**デバイスを監視する**］をオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

      システム変更監視は、外部デバイスの現在の接続を記録します。アプリケーション設定でコンポーネントを有効にすると、外部デバイスの接続と接続解除の監視が開始されます。その後、外部デバイスが接続または接続解除されると、対応するイベントが生成されます。

9. 変更内容を保存します。

*アプリケーションコンソールでリアルタイムシステム変更監視を有効にして設定する方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**システム監査**］→［**システム変更監視**］の順に選択します。
2. ［**システム変更監視**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: システム変更監視**］ウィンドウが表示されます。
3. ［**システム変更監視**］チェックボックスをオンにします。
4. ファイル変更監視を設定します：
   a. ［**ファイル**］タブにある［**ファイルを監視する**］をオンにします。
   b. ［**ブロックルールの操作モード**］で、ファイル変更監視のモードを選択します：
      - **ブロックする**：このモードでは、ファイル変更監視ルールに従ってファイルに対する処理が実行されて、対応するイベントがシステム変更監視ログに生成されます。
      - **通知する**：このモードでは、適用されたファイル変更監視ルールに関するイベントのみがシステム変更監視ログに生成されます。
   c. 手動で［**追加**］を使用するか、XML ファイルからインポートして、ファイル整合性監視ルールを追加します。次のテーブルでは、ファイル変更監視ルールの設定について説明します。
   d. ファイル整合性監視ルールのリストで、チェックボックスを管理して、必要なルールを有効のままにします。
5. レジストリアクセス監視を設定します：
   a. ［**レジストリ**］タブにある［**レジストリを監視する**］をオンにします。
   b. ［**ブロックルールの操作モード**］の下で、レジストリアクセス監視のモードを選択します。
      - **ブロックする**：このモードでは、レジストリアクセス監視ルールに従ってレジストリに対する処理がブロックされて、対応するイベントがシステム変更監視ログに生成されます。
      - **通知する**：このモードでは、適用されたレジストリアクセス監視ルールに関するイベントのみがシステム変更監視ログに生成されます。
   c. 手動で［**追加**］を使用するか、XML ファイルからインポートして、レジストリアクセス監視ルールを追加します。次のテーブルでは、レジストリアクセス監視ルールの設定について説明します。
   d. レジストリアクセス監視ルールのリストで、チェックボックスを管理して、必要なルールを有効のままにします。

6. 外部デバイスの監視を設定します：

   a. ［**デバイス**］タブにある［**デバイスを監視する**］をオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

      外部デバイスの監視設定を適用すると、本製品で現在の外部デバイスの接続が記憶されます。その後、外部デバイスが接続または接続解除されると、対応するイベントがシステム変更監視ログに生成されます。

7. 変更内容を保存します。

システム変更監視ルールの設定

| パラメータ | 説明 |
| --- | --- |
| **次の範囲のファイル操作を監視** | ファイル変更監視を適用する範囲。このフィールドは必須です。<br>マスクを使用する<br>Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。<br>「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。<br>2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。<br>「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。 |
| **監視対象オブジェクト** | ここで、レジストリキーの名前または値を指定できます。<br>マスクを使用する<br>Kaspersky Embedded Systems Security では、マスクの入力時の文字「`*`」および「`?`」 がサポートされます。 |
| **ファイルの操作** | • **検知**：監視範囲内のファイルに対する処理が許可されます。<br>• **検知してブロック**：本製品の動作は、選択したファイル変更監視のモードによって異なります。*ブロックするモード*を選択した場合、システム変更監視は、監視範囲内のファイルに対する操作をブロックします。*通知するモード*を選択した場合、システム変更監視は、監視範囲内のファイルに対する操作を許可します。 |
| **信頼するユーザーまたはユーザーグループ** | 信頼済みユーザーとは、監視範囲内のファイルとレジストリキーに対して操作を実行することが許可されたユーザーです。<br>Kaspersky Embedded Systems Security が信頼済みユーザーによる操作を検知すると、システム変更監視は情報イベントを生成します。<br>ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。 |
| **ファイル操作マーカー / 処理** | 本製品が監視するファイルまたはレジストリキーに対する操作を特徴付けるマーカー。 |
| **すべての認識済みマーカーに基づいてファイル操作を検出 / すべての認識済みマーカーに基づいてレジストリ操作を検出** | 既定では、使用可能なすべてのファイル / レジストリ操作マーカーが考慮されます。 |
| **次のマーカーに基づいてファイル操作を検出 / 次のマーカーに基づいてレジストリ操作を検出** | 使用可能なファイル / レジストリ操作のリストで、監視する操作の横にあるチェックボックスをオンにします。 |

| パラメータ | 説明 |
| --- | --- |
| **可能な場合はファイル操作後にチェックサムを計算します。チェックサムはタスクのログに表示されます** | チェックボックスをオンにして、少なくとも1つの選択したマーカーを持つファイル操作が検知された場合、変更したファイルのチェックサムが計算されます。<br>ファイル操作が複数のマーカーによって検知された場合、すべての変更後の最終的なファイルのチェックサムのみが計算されます。<br>このチェックボックスをオフにすると、変更したファイルのチェックサムは計算されません。<br>次の場合、チェックサムの計算は実行されません：<br>• ファイルが利用できなくなった場合（アクセス権限の変更などのため）。<br>• ファイル操作が、その後、削除されたファイル内で検知された場合。<br>既定では、このチェックボックスはオフです。 |
| **チェックサム計算アルゴリズム** | ドロップダウンリストからチェックサム計算アルゴリズムを1つ選択します：<br>• MD5 ハッシュ<br>• SHA256 ハッシュ |
| **除外リスト** | ［**除外リスト**］タブで、監視範囲から除外するオブジェクトを追加できます：<br>• ファイル変更監視ルールでは、フォルダーのリストを指定できます。<br>• レジストリアクセス監視ルールでは、レジストリキーまたは値を指定できます。<br>マスクを使用する<br>**ファイル**<br>コンポーネントによって監視されるファイルとフォルダーのリスト。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。<br>「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。<br>2つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。<br>「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の1文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が3文字のすべてのファイルのパスを含みます。<br>**レジストリ**<br>Kaspersky Embedded Systems Security は、マスクの入力時の文字「`*`」および「`?`」をサポートします。除外項目は監視範囲項目よりも優先されます。 |
| **イベントの深刻度** | Kaspersky Embedded Systems Security は、監視範囲内のファイルまたはレジストリキーが変更された場合にファイル変更イベントを記録します。**情報**、**警告**、**緊急**のイベントセキュリティレベルが利用可能です。 |

# オンデマンドのシステム変更チェック

オンデマンドのシステム変更チェックは、手動で実行することも、スケジュールに従って実行することもできるタスクです。ベースラインシステム*変更監視*タスクの実行中、本製品は監視範囲に含まれるオブジェクトの現在の状態をベースラインの状態と比較します。ベースラインは、タスクが最初に開始された時に作成されます。

システム変更監視が機能するには、ルールを少なくとも1つ追加する必要があります。システム変更監視ルールとは、ファイルおよびレジストリへのユーザーのアクセスを定義する一連の条件です。システム変更監視は、指定された監視範囲内のファイルとレジストリの変更を検知します。監視範囲は、システム変更監視ルールの条件の1つです。

# ベースラインシステム変更監視タスク用の監視範囲の設定

既定で、*ベースラインシステム変更監視*タスクの監視範囲とは、システム変更監視の監視範囲と同じです。このタスクに対して異なる監視範囲を設定できます。

システム変更監視では、*システム変更チェック*タスクへの HKEY_CURRENT_USER および HKEY_CURRENT_CONFIG のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

**Kaspersky Security Center 管理コンソールでベースラインシステム変更監視タスク用に異なる監視範囲を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**タスク**］フォルダーを選択します。
2. 必要な*ベースラインシステム変更監視*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を表示します。
3. 表示されるウィンドウで、［**設定**］を選択します。
4. ファイルの監視を設定します：
   a. ［**ファイル**］タブにある［**ファイルを監視する**］をオンにします。
   b. チェックボックスをオンにして、リスト内のルールを選択します。
   c. 必要に応じて、［**追加**］をクリックして、新しいルールを追加します。次のテーブルでは、ベースラインシステム変更監視ルールの設定について説明します。
   d. また、別のソースからルールをインポートすることもできます。
5. レジストリの監視を設定します：
   a. ［**レジストリ**］タブにある［**レジストリを監視する**］をオンにします。
   b. チェックボックスをオンにして、リスト内のルールを選択します。
   c. 必要に応じて、［**追加**］をクリックして、新しいルールを追加します。次のテーブルでは、ベースラインシステム変更監視ルールの設定について説明します。
   d. また、別のソースからルールをインポートすることもできます。

6. 外部デバイスの監視を設定します：

   a. ［**デバイス**］タブにある［**デバイスを監視する**］をオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

      ベースラインシステム変更監視タスクは、ベースラインが作成された時点で接続されていた外部デバイスに関する情報を記録します。その後、外部デバイスが接続されると、本製品は対応するイベントを生成します。タスクの実行中、外部デバイスの接続解除は監視されません。

7. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでベースラインシステム変更監視タスク用に異なる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、［**アセット（デバイス）**］→［**タスク**］の順に選択します。

2. 必要なベースラインシステム*変更監視*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を表示します。

3. 表示されるウィンドウで、［**アプリケーション設定**］を選択します。

4. ファイルの監視を設定します：

   a. ［**ファイルを監視する**］チェックボックスをオンにします。

   b. チェックボックスをオンにして、リスト内のルールを選択します。

   c. 必要に応じて、［**追加**］をクリックして、新しいルールを追加します。次のテーブルでは、ベースラインシステム変更監視ルールの設定について説明します。

   d. また、別のソースからルールをインポートすることもできます。

5. レジストリの監視を設定します：

   a. ［**レジストリを監視する**］チェックボックスをオンにします。

   b. チェックボックスをオンにして、リスト内のルールを選択します。

   c. 必要に応じて、［**追加**］をクリックして、新しいルールを追加します。次のテーブルでは、ベースラインシステム変更監視ルールの設定について説明します。

   d. また、別のソースからルールをインポートすることもできます。

6. 外部デバイスの監視を設定します：

   a. ［**デバイスを監視する**］チェックボックスをオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

      ベースラインシステム*変更監視*タスクは、ベースラインが作成された時点で接続されていた外部デバイスに関する情報を記録します。その後、外部デバイスが接続されると、本製品は対応するイベントを生成します。タスクの実行中、外部デバイスの接続解除は監視されません。

7. 変更内容を保存します。

### *アプリケーションコンソールでベースラインシステム変更監視タスク用に異なる監視範囲を設定する方法*

タスクがローカルで作成された場合、またはポリシーのプロパティの［**アプリケーション設定**］→［**ローカルシステムタスクの実行**］セクションで［**ローカルタスクの使用を許可する**］がオンになっている場合、Kaspersky Embedded Systems Security コンソールで**ベースラインシステム変更監視**タスクのプロパティを編集することができます。

1. Kaspersky Embedded Systems Security コンソールツリーで、［**システム監査**］→［**ベースラインシステム変更監視**］の順に選択します。

2. ［**ベースラインシステム変更監視**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。

   ［**プロパティ: ベースラインシステム変更監視**］ウィンドウが表示されます。

3. ファイルの監視を設定します：

   a. ［**ファイル**］タブにある［**ファイルを監視する**］をオンにします。

   b. チェックボックスをオンにして、リスト内のルールを選択します。

   c. 必要に応じて、［**追加**］をクリックして、新しいルールを追加します。次のテーブルでは、ベースラインシステム変更監視ルールの設定について説明します。

   d. また、別のソースからルールをインポートすることもできます。

4. レジストリの監視を設定します：

   a. ［**レジストリ**］タブにある［**レジストリを監視する**］をオンにします。

   b. チェックボックスをオンにして、リスト内のルールを選択します。

   c. 必要に応じて、［**追加**］をクリックして、新しいルールを追加します。次のテーブルでは、ベースラインシステム変更監視ルールの設定について説明します。

   d. また、別のソースからルールをインポートすることもできます。

5. 外部デバイスの監視を設定します：

   a. ［**デバイス**］タブにある［**デバイスを監視する**］をオンにします。

   b. ［**イベントの深刻度**］ドロップダウンリストで、外部デバイス監視イベントの重要度を選択します：*情報*、*警告*、*緊急*。

      ベースラインシステム変更監視タスクは、ベースラインが作成された時点で接続されていた外部デバイスに関する情報を記録します。その後、外部デバイスが接続されると、本製品は対応するイベントを生成します。タスクの実行中、外部デバイスの接続解除は監視されません。

6. 変更内容を保存します。

ベースラインシステム変更監視タスクルールの設定

| パラメータ | 説明 |
| --- | --- |
| **次の範囲のファイル操作を監視** | ファイル変更監視を適用する範囲。このフィールドは必須です。<br>マスクを使用する<br>Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。<br>「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。<br>2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。<br>「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。 |
| **監視対象オブジェクト** | ここで、レジストリキーの名前または値を指定できます。<br>マスクを使用する<br>Kaspersky Embedded Systems Security では、マスクの入力時の文字「`*`」および「`?`」がサポートされます。 |
| **除外リスト** | ［**除外リスト**］タブで、監視範囲から除外するオブジェクトを追加できます：<br>• ファイル変更監視ルールでは、フォルダーのリストを指定できます。<br>• レジストリアクセス監視ルールでは、レジストリキーまたは値を指定できます。<br>マスクを使用する<br>**ファイル**<br>コンポーネントによって監視されるファイルとフォルダーのリスト。Kaspersky Embedded Systems Security は環境変数とマスクの入力時の文字「`*`」および「`?`」をサポートします。<br>「`*`」（アスタリスク）文字。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の文字列に置き換えられます。たとえば、マスク「`C:\*\*.txt`」は、C: ドライブ上のフォルダーにある拡張子が txt のすべてのファイルのパスを含みますが、サブフォルダーにあるファイルのパスは含みません。<br>2 つの連続した「`*`」（アスタリスク）文字。ファイル名またはフォルダー名内の、「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を含む任意の文字列に置き換えられます。たとえば、マスク「`C:\Folder\**\*.txt`」は、「`Folder`」フォルダーおよびそのサブフォルダーにある拡張子が txt のすべてのファイルのパスを含みます。このマスクは、1 つ以上のフォルダーの下に指定する必要があります。ドライブ直下での「`C:\**\*.txt`」というマスクの指定は無効です。<br>「`?`」（クエスチョンマーク）。「`\`」および「`/`」（ファイルまたはフォルダーのパスにおけるファイル名またはフォルダー名の区切り文字）を除く任意の 1 文字に置き換えられます。たとえば、マスク「`C:\Folder\???.txt`」は、「`Folder`」フォルダーにある拡張子が txt でファイル名が 3 文字のすべてのファイルのパスを含みます。<br>**レジストリ**<br>Kaspersky Embedded Systems Security は、マスクの入力時の文字「`*`」および「`?`」をサポートします。除外項目は監視範囲項目よりも優先されます。 |
| **イベントの深刻度** | Kaspersky Embedded Systems Security は、監視範囲内のファイルまたはレジストリキーが変更された場合にファイル変更イベントを記録します。**情報**、**警告**、**緊急**のイベントセキュリティレベルが利用可能です。 |

## ベースラインシステム変更監視タスクの実行

**ベースラインシステム変更監視**タスクにより、ファイルやレジストリキーの変更を確認したり、外部デバイスの接続を確認したりできます。ファイルの変更を確認するには、**ベースラインシステム変更監視**タスクを次のいずれかのモードで実行します：

- **完全スキャン**：このモードでは、本製品はファイルのすべての属性とハッシュをチェックします。
- **簡易スキャン**：このモードでは、本製品はファイルの属性のみをチェックします。

タスクの実行モードは、レジストリまたは外部デバイスのチェックには影響しません。

***Kaspersky Security Center 管理コンソールでベースラインシステム変更監視タスクを実行する方法***

1. Kaspersky Security Center 管理コンソールツリーで、［**タスク**］フォルダーを選択します。
   タスクのリストが表示されます。
2. ［**新規タスク**］をクリックします。
   タスクウィザードが起動します。ウィザードの指示に従います。
3. ［**Kaspersky Embedded Systems Security**］→［**ベースラインシステム変更監視**］の順に選択します。
   システム変更監視モードを選択します：
   - **完全スキャン**：このモードでは、本製品はファイルのすべての属性とハッシュをチェックします。
   - **簡易スキャン**：このモードでは、本製品はファイルの属性のみをチェックします。
4. タスクを実行するコンピューターを選択します。次の設定方法があります：
   - 未割り当てデバイスなど、管理サーバーがネットワーク内で検出したデバイスを選択します。タスクの対象となるデバイスには、未割り当てデバイスだけでなく管理グループ内のデバイスも含めることができます。
   - デバイスのアドレスを手動で指定するか、リストからインポートします。タスクを割り当てるデバイスの NetBIOS 名、IP アドレス、IP サブネットを指定できます。
   - タスクを実行するデバイスの抽出を指定します。
   - 管理グループにタスクを割り当てます。この場合、作成済みの管理グループに含まれるコンピューターにタスクが割り当てられます。
5. タスクを実行するアカウントを選択します。既定では、Kaspersky Embedded Systems Security はローカルユーザーアカウントの権限でタスクを開始します。
6. タスクのスケジュールを設定します（手動や、特定の曜日など）。
7. タスク名を入力します。
8. ウィザードの操作を完了します。必要に応じて、［**ウィザードの終了後にタスクを実行**］をオンにします。タスクのプロパティでタスクの進行状況を監視できます。

### *Kaspersky Security Center Web コンソールでベースラインシステム変更監視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、［**アセット（デバイス）**］→［**タスク**］の順に選択します。
   タスクのリストが表示されます。
2. ［**追加**］をクリックします。
   タスクウィザードが起動します。
3. タスクの設定を指定します：
   a. ［**アプリケーション**］ドロップダウンリストで、［Kaspersky Embedded Systems Security］を選択します。
   b. ［**タスク種別**］から［**ベースラインシステム変更監視**］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。
4. ［**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。
5. 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。次の手順に進みます。
6. チェックサム計算アルゴリズムを選択します。
7. タスクを実行するアカウントを選択します。既定では、Kaspersky Embedded Systems Security はローカルユーザーアカウントの権限でタスクを開始します。
8. ウィザードの操作を完了します。
   タスクのリストに新しいタスクが表示されます。
9. 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。
10. ［**アプリケーション設定**］タブを選択します。
11. システム変更チェックモードを選択します：
    - **完全スキャン**：このモードでは、本製品はファイルのすべての属性とハッシュをチェックします。
    - **簡易スキャン**：このモードでは、本製品はファイルの属性のみをチェックします。
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。

# システム変更監視ルールのエクスポートとインポート

システム変更監視ルールを XML 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、例えば同じ種別の多数の記録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、システム変更監視ルールのリスト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。

システム変更監視では、*システム変更チェック*タスクへの HKEY_CURRENT_USER および HKEY_CURRENT_CONFIG のキーのインポートはサポートされていません。タスクの監視範囲にこれらのキーが含まれている場合、*監視範囲に正しくないオブジェクトが含まれています*のイベントが生成されます。

**Kaspersky Security Center 管理コンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**システム監査**］を選択します。
4. ［**システム変更監視**］セクションで、［**設定**］をクリックします。
5. ファイル / レジストリルールをエクスポートするには：
   a. ［**ファイル**］タブまたは［**レジストリ**］タブで、エクスポートするルールを選択します。
   b. ［**エクスポート**］をクリックして、［**選択したものをエクスポート**］を選択します。
   c. ルールが何も選択されていない場合、［**エクスポート**］→［**エクスポート**］の順にクリックすると、すべてのルールがエクスポートされます。
   d. 表示されたウィンドウで、ルールをエクスポートする XML 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。
   e. ファイルを保存します。

      Kaspersky Embedded Systems Security は、ルールのリスト全体を XML ファイルにエクスポートします。
6. ファイル / レジストリルールをインポートするには：
   a. ［**ファイル**］タブまたは［**レジストリ**］タブで［**インポート**］をクリックします。

      表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

b. ファイルを開きます。

コンピューターにルールのリストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

7. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでシステム変更監視ルールのリスト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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**システム監査**］→［**システム変更監視**］に移動し、［**設定**］をクリックします。

［**システム変更監視設定**］ウィンドウが表示されます。

5. ファイル / レジストリルールをエクスポートするには：

a. ［**ファイル**］タブまたは［**レジストリ**］タブで、エクスポートするルールを選択します。

b. ［**エクスポート**］をクリックします。これによりウィンドウが開きます。そのウィンドウで、選択したルールをエクスポートするか、すべてのルールをエクスポートするかを指定して、［**エクスポート**］をクリックします。

ルールが何も選択されていない場合、すべてのルールがエクスポートされます。

6. Kaspersky Embedded Systems Security は、ルールのリスト全体を XML ファイルにエクスポートします。
7. ファイル / レジストリルールをインポートするには：

a. ［**ファイル**］または［**レジストリ**］タブで、バージョン 3.4 以前の本製品で作成された XML ファイルからルールをインポートする場合は、［**以前のバージョンからインポートする**］をクリックします。

バージョン 4.0 以降で作成された XML ファイルからルールをインポートする場合は、［**インポート**］をクリックします。

b. コンピューターにルールのリストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。

c. 表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。

d. ［**インポート**］をクリックします。

8. 変更内容を保存します。

***アプリケーションコンソールでシステム変更監視ルールのリストをエクスポートおよびインポートする方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**システム監査**］→［**システム変更監視**］の順に選択します。
2. ［**システム変更監視**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: システム変更監視**］ウィンドウが表示されます。
3. ファイル / レジストリルールをエクスポートするには：
   a. ［**ファイル**］タブまたは［**レジストリ**］タブで、エクスポートするルールを選択します。
   b. ［**エクスポート**］をクリックして、［**選択したものをエクスポート**］を選択します。
   c. ルールが何も選択されていない場合、［**エクスポート**］→［**エクスポート**］の順にクリックすると、すべてのルールがエクスポートされます。
   d. 表示されたウィンドウで、ルールをエクスポートする XML 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。
   e. ファイルを保存します。
      Kaspersky Embedded Systems Security は、ルールのリスト全体を XML ファイルにエクスポートします。
4. ファイル / レジストリルールをインポートするには：
   a. ［**ファイル**］タブまたは［**レジストリ**］タブで［**インポート**］をクリックします。
      表示されたウィンドウで、ルールのリストをインポートする XML ファイルを選択します。
   b. ファイルを開きます。
      コンピューターにルールのリストが既にある場合、Kaspersky Embedded Systems Security から、既存のリストを削除するか、XML ファイルから新しいエントリを追加するよう要求されます。
5. 変更内容を保存します。

# システム変更監視レポートの表示

システム変更監視ルールのパフォーマンスを分析するには、本製品で生成されたレポートとイベントを確認できます。Kaspersky Embedded Systems Security は、コンポーネントに関して次のレポートを生成します：

- 製品インターフェイス内：
  - ベースラインアップデートレポート

  レポートにはシステム変更監視イベントが含まれます。

- Kaspersky Security Center コンソール内
  - 監視ルールの適用回数が最も多いコンピューターに関するレポート
  - 適用頻度が最も高い監視ルールに関するレポート
    最も頻繁に適用される監視ルールに関するレポートを生成するために、本製品は次のイベントをログに記録します：
    - *ファイルまたはフォルダーの変更が検知されました*
    - *統計のみ：管理領域でのファイル操作を禁止しました*
    - *信頼するユーザーによる管理領域でのファイル操作を許可しました*
    - *管理領域でのファイル操作をコントロールできません*

    > これらのイベントの保管期間を設定するには、ポリシーの［**イベントの設定**］セクションで、一般的なシステム変更監視イベント（*ファイルまたはフォルダーの変更が検知されました*）の期間を指定します。

既定では、レポートの作成日を含む過去 30 日間のレポートが作成されます。

**Kaspersky Security Center 管理コンソールでシステム変更監視レポートを表示する方法**

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［**管理サーバー**］フォルダーで、［**レポート**］タブを選択します。
3. ［**新規レポートテンプレート**］をクリックします。
   新規のレポートテンプレートウィザードが起動します。
4. レポートテンプレートウィザードの指示に従います。［**レポートテンプレートの種別の選択**］ステップで、システム変更監視レポート（［**その他**］セクション）を選択します：
   - **ファイル変更監視 / システム変更監視ルールの適用回数が多い 10 台のデバイス**
   - **デバイスで適用された回数が多い 10 個のファイル変更監視 / システム変更監視ルール**

   新規レポートテンプレートウィザードが完了すると、［**レポート**］タブのテーブルに新しいレポートテンプレートが表示されます。
5. レポートをダブルクリックして開きます。

レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

**Kaspersky Security Center Web コンソールでシステム変更監視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、［**監視とレポート**］→［**レポート**］の順に選択します。
2. ［**追加**］をクリックします。
   新規のレポートテンプレートウィザードが起動します。

3. ［**テンプレート**］の下の［**その他**］セクションで、システム変更監視レポートを選択します。

   - **ファイル変更監視 / システム変更監視ルールの適用回数が多い 10 台のデバイス**
   - **デバイスで適用された回数が多い 10 個のファイル変更監視 / システム変更監視ルール**

   新規レポートテンプレートウィザードが完了すると、テーブルに新しいレポートテンプレートが表示されます。

4. レポートを選択して実行します。

   レポートの生成プロセスが開始されます。レポートが新しいウィンドウに表示されます。

本製品で生成されたイベントを表示するには、Kaspersky Security Center コンソールのイベント選択を使用することもできます。

# Windows イベントログ監視

Windows イベントログ監視は Windows イベントログの分析に基づいて保護対象環境の整合性を監視します。通常と異なるふるまいを検知した場合、本製品は管理者にこのふるまいがサイバー攻撃の可能性を示す可能性があると通知します。

Kaspersky Embedded Systems Security はルールに従って Windows イベントログを分析して違反を検出します。コンポーネントには事前定義済みのルールが含まれます。事前定義済みのルールはヒューリスティック分析によって動作します。独自のルールを追加することもできます（カスタムルール）。ルールが適用されると、本製品は緊急ステータスのイベントを作成します。

Windows イベントログ監視を使用する場合、セキュリティ監査ポリシーが設定されており、システムが関連するイベントを記録していることを確認してください（詳細については、Microsoft のテクニカルサポートの Web サイトを参照してください）。

| パラメータ | 説明 |
| --- | --- |
| **事前定義済みのルール** | Windows イベントログ監視のリストです。事前定義済みのルールには、保護対象コンピューター上における正常でない活動のテンプレートが含まれます。正常でない活動は、攻撃の可能性を示している場合があります。 |
| **カスタムルール** | ユーザーによって追加された Windows イベントログ監視のリストです。Windows イベントログ監視のルールトリガー条件を独自に設定することができます。そのためには、イベント ID を入力してイベントソースを選択する必要があります。<br>［*Application*］、［*Security*］または［*System*］のいずれかの標準ログからイベントソースを選択できます。また、サードパーティ製のアプリケーションのログを指定することもできます。 |

# カスタムルールの追加

Windows イベントログ監視のルールトリガー条件を独自に設定することができます。そのためには、イベント ID を入力してイベントソースを選択する必要があります。イベント ID は Microsoft のテクニカルサポートの Web サイトで検索できます。［*Application*］、［*Security*］または［*System*］のいずれかの標準ログからイベントソースを選択できます。また、サードパーティ製のアプリケーションのログを指定することもできます。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（*Windows PowerShell* ログなど）に保存されています。

本製品は、指定されたログが実際に Windows イベントログ内に存在するかどうかは確認しません。ログの名前に誤りがあった場合は、そのログからのイベントは監視されません。

カスタムルールのリストには、カスペルスキーのエキスパートにより作成されたいくつかのルールが含まれています。

### Kaspersky Security Center 管理コンソールでカスタムルールを追加する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**システム監査**］を選択します。

4. ［**Windows イベントログ監視**］セクションで、［**設定**］をクリックします。
5. ［**Windows イベントログ監視**］チェックボックスをオンにします。
6. ［**カスタムルール**］タブで、［**Windows イベントログ監視にカスタムルールを適用する**］をオンにします。
7. 有効にするカスタムルールの横にあるチェックボックスをオンにします。
8. 必要に応じて、［**追加**］をクリックしてカスタムルールを作成します。
9. ウィンドウが表示されるので、そのウィンドウでカスタムルールを設定します：
   - **ルール名**
   - **ログの名前**：Windows イベントログです。*Application*、*Security*、*System* のログが利用可能です。
   - **ソース**：サードパーティ製アプリケーションのログです。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（Windows PowerShell ログなど）に保存されています。
   - **イベント ID**：Windows イベントログ内のイベント ID です。イベント ID は Microsoft のテクニカルサポートの Web サイトで検索できます。
10. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでカスタム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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**システム監査**］→［**Windows イベントログ監視**］に移動し、［**設定**］をクリックします。
5. ［**Windows イベントログ監視を有効にする**］チェックボックスをオンにします。
6. ［**カスタムルール**］タブで、［**Windows イベントログ監視にカスタムルールを適用する**］をオンにします。
7. スイッチを使用してカスタムルールを設定します：
8. 必要に応じて、［**追加**］をクリックしてカスタムルールを作成します。

9. ウィンドウが表示されるので、そのウィンドウでカスタムルールを設定します：

   - **ルール名**

   - **Windows イベントログの名前**：Windows イベントログです。*Application*、*Security*、*System* のログが利用可能です。

   - **ソース**：サードパーティ製アプリケーションのログです。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（Windows PowerShell ログなど）に保存されています。

   - **イベント ID**：Windows イベントログ内のイベント ID です。イベント ID は Microsoft のテクニカルサポートの Web サイトで検索できます。

10. 変更内容を保存します。

***アプリケーションコンソールでカスタムルールを追加する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**システム監査**］→［**Windows イベントログ監視**］の順に選択します。

2. ［**Windows イベントログ監視**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ：Windows イベントログ監視**］ウィンドウが表示されます。

3. ［**Windows イベントログ監視**］チェックボックスをオンにします。

4. ［**カスタムルール**］タブで、［**Windows イベントログ監視にカスタムルールを適用する**］をオンにします。

5. 有効にするカスタムルールの横にあるチェックボックスをオンにします。

6. 必要に応じて、［**追加**］をクリックしてカスタムルールを作成します。

7. ウィンドウが表示されるので、そのウィンドウでカスタムルールを設定します：

   - **ルール名**

   - **ログの名前**：Windows イベントログです。*Application*、*Security*、*System* のログが利用可能です。

   - **ソース**：サードパーティ製アプリケーションのログです。サードパーティ製アプリケーションのログの名前は、イベントビューアーを使用して検索することができます。サードパーティ製アプリケーションのログはアプリケーションとサービスログのフォルダー（Windows PowerShell ログなど）に保存されています。

   - **イベント ID**：Windows イベントログ内のイベント ID です。イベント ID は Microsoft のテクニカルサポートの Web サイトで検索できます。

8. 変更内容を保存します。

この結果、ルールがトリガーされると、Kaspersky Embedded Systems Security は緊急イベントを作成します。

# 事前定義済みのルールの設定

事前定義済みのルールには、保護対象コンピューター上における正常でない活動のテンプレートが含まれます。正常でない活動は、攻撃の可能性を示している場合があります。事前定義済みのルールはヒューリスティック分析によって動作します。Windows イベントログ監視には 7 つの事前定義済みのルールが使用できます。いずれのルールを有効または無効にすることができます。事前定義済みのルールを削除することはできません。

次の操作に対するイベントの監視ルールの適用条件を設定できます：

- パスワードのブルートフォース攻撃の検知
- ネットワークログオンの検知

**Kaspersky Security Center 管理コンソールで事前定義済みのルールを設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**システム監査**］を選択します。
4. ［**Windows イベントログ監視**］セクションで、［**設定**］をクリックします。
5. ［**Windows イベントログ監視**］チェックボックスをオンにします。
6. ［**事前定義済みのルール**］タブで、［**Windows イベントログ監視に事前定義済みのルールを適用する**］をオンにします。
7. チェックボックスをオンまたはオフにして、事前定義済みのルールを設定します：
   - **システムにブルートフォース攻撃の可能性を示すパターンがあります**
   - **ネットワークログオンセッション中に通常と異なる活動を検知しました**
   - **Windows イベントログの悪用の可能性を示すパターンがあります**
   - **新しくインストールしたサービスに通常と異なる活動が検出されました**
   - **明示的な資格情報を使用した通常と異なるログオンが検出されました**
   - **システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります**
   - **特権付きの組み込み管理者グループ内で疑わしい変更を検知しました**

8. 必要に応じて、［**システムにブルートフォース攻撃の可能性を示すパターンがあります**］ルールを設定します：

   a. ルールの横にある［**設定**］をクリックします。

   b. 表示されるウィンドウで、ルールが適用されるパスワードの入力試行の回数と期間を指定します。

   c. ［**OK**］をクリックします。

9. ［**ネットワークログオンセッション中に通常と異なる活動を検知しました**］ルールを選択した場合、設定を構成する必要があります：

   a. ルールの横にある［**設定**］をクリックします。

   b. 表示されたウィンドウの［**ネットワークログオンの検知**］ブロックで、間隔の開始および終了を指定します。

   Kaspersky Embedded Systems Security はこの定義された間隔で実行されたログオン試行回数を正常でない活動と認識します。

   既定では、間隔は設定されておらず、本製品はログオン試行回数を監視しません。本製品がログオン試行回数を継続的に監視するには、間隔を午前 0 時から午後 11 時 59 分に設定します。間隔の開始時間と終了時間には異なる時間を指定する必要があります。開始時間と終了時間が同じである場合、アプリケーションはログオン試行回数を監視しません。

   c. 信頼するユーザーと信頼する IP アドレス（IPv4 および IPv6）のリストを作成します。

   ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。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。Kaspersky Embedded Systems Security はこれらのユーザーおよびコンピューターのログオン試行を監視しません。

   > Windows XP で実行されているアプリケーションでは、IP アドレスによる信頼できるコンピューターの除外は機能しません。

   d. ［**OK**］をクリックします。

10. 変更内容を保存します。

**Kaspersky Security Center Web コンソールで事前定義済みの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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**システム監査**］→［**Windows イベントログ監視**］に移動し、［**設定**］をクリックします。

5. ［**Windows イベントログ監視を有効にする**］チェックボックスをオンにします。

6. ［**事前定義済みのルール**］タブで、［**Windows イベントログ監視に事前定義済みのルールを適用する**］をオンにします。

7. スイッチを使用して事前定義済みのルールを設定します：

   - **システムにブルートフォース攻撃の可能性を示すパターンがあります**
   - **ネットワークログオンセッション中に通常と異なる活動を検知しました**
   - **Windows イベントログの悪用の可能性を示すパターンがあります**
   - **新しくインストールしたサービスに通常と異なる活動が検出されました**
   - **明示的な資格情報を使用した通常と異なるログオンが検出されました**
   - **システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります**
   - **特権付きの組み込み管理者グループ内で疑わしい変更を検知しました**

8. ［**拡張**］タブで、次の設定を行います：

   - ルール［**システムにブルートフォース攻撃の可能性を示すパターンがあります**］を適用する場合は、パスワードの入力試行の回数と期間を指定します。
   - ルール［**ネットワークログオンセッション中に通常と異なる活動を検知しました**］を適用する場合は、すべてのログオン試行を正常でない活動として識別する時間間隔の開始と終了を指定します。

     既定では、間隔は設定されておらず、本製品はログオン試行回数を監視しません。本製品がログオン試行回数を継続的に監視するには、間隔を午前 0 時から午後 11 時 59 分に設定します。間隔の開始時間と終了時間には異なる時間を指定する必要があります。開始時間と終了時間が同じである場合、アプリケーションはログオン試行回数を監視しません。

9. 信頼するユーザーと信頼する IP アドレス（IPv4 および IPv6）のリストを対応するタブで作成します。

   ユーザーは、アカウントのリストで選択することも、ローカルユーザー名を手入力することもできます。

   > Windows XP で実行されているアプリケーションでは、IP アドレスによる信頼できるコンピューターの除外は機能しません。

10. 変更内容を保存します。

***アプリケーションコンソールで事前定義済みのルールを設定する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**システム監査**］→［**Windows イベントログ監視**］の順に選択します。
2. ［**Windows イベントログ監視**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。

   ［**プロパティ：Windows イベントログ監視**］ウィンドウが表示されます。
3. ［**Windows イベントログ監視**］チェックボックスをオンにします。

4. ［**事前定義済みのルール**］タブで、［**Windows イベントログ監視に事前定義済みのルールを適用する**］をオンにします。

5. チェックボックスをオンまたはオフにして、事前定義済みのルールを設定します：

   - **システムにブルートフォース攻撃の可能性を示すパターンがあります**
   - **ネットワークログオンセッション中に通常と異なる活動を検知しました**
   - **Windows イベントログの悪用の可能性を示すパターンがあります**
   - **新しくインストールしたサービスに通常と異なる活動が検出されました**
   - **明示的な資格情報を使用した通常と異なるログオンが検出されました**
   - **システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります**
   - **特権付きの組み込み管理者グループ内で疑わしい変更を検知しました**

6. 必要に応じて、［**システムにブルートフォース攻撃の可能性を示すパターンがあります**］ルールを設定します：

   a. ルールの横にある［**設定**］をクリックします。

   b. 表示されるウィンドウで、ルールが適用されるパスワードの入力試行の回数と期間を指定します。

   c. ［**OK**］をクリックします。

7. ［**ネットワークログオンセッション中に通常と異なる活動を検知しました**］ルールを選択した場合、設定を構成する必要があります：

   a. ルールの横にある［**設定**］をクリックします。

   b. 表示されたウィンドウの［**ネットワークログオンの検知**］ブロックで、間隔の開始および終了を指定します。

      Kaspersky Embedded Systems Security はこの定義された間隔で実行されたログオン試行回数を正常でない活動と認識します。

      既定では、間隔は設定されておらず、本製品はログオン試行回数を監視しません。本製品がログオン試行回数を継続的に監視するには、間隔を午前 0 時から午後 11 時 59 分に設定します。間隔の開始時間と終了時間には異なる時間を指定する必要があります。開始時間と終了時間が同じである場合、アプリケーションはログオン試行回数を監視しません。

   c. 信頼するユーザーと信頼する IP アドレス（IPv4 および IPv6）のリストを作成します。

      ユーザーは、Active Directory または Kaspersky Security Center のアカウントのリストで選択するか、ローカルユーザー名を手入力して選択することができます。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。Active Directory からユーザーのリストを作成します。Kaspersky Embedded Systems Security はこれらのユーザーおよびコンピューターのログオン試行を監視しません。

Windows XP で実行されているアプリケーションでは、IP アドレスによる信頼できるコンピューターの除外は機能しません。

d. ［**OK**］をクリックします。

8. 変更内容を保存します。

この結果、ルールがトリガーされると、Kaspersky Embedded Systems Security は緊急イベントを作成します。

# オンデマンドスキャン

このセクションでは、オンデマンドスキャンタスク、および保護対象デバイス上でのオンデマンドスキャンタスクとセキュリティの設定手順について説明します。

# オンデマンドスキャンタスクについて

Kaspersky Embedded Systems Security は、指定した領域で、ウイルスやその他のコンピューターセキュリティの脅威がないかをスキャンします。Kaspersky Embedded Systems Security では、保護対象デバイスのファイル、メモリ、および自動実行オブジェクトがスキャン対象になります。

Kaspersky Embedded Systems Security は、次のオンデマンドスキャンタスクを提供します：

- 既定では、*簡易スキャン*タスクがスケジュールに従って週単位で実行されます。オペレーティングシステムの重要な領域のオブジェクト（自動実行オブジェクト、ハードディスクやリムーバブルドライブのブートセクターやマスターブートレコード、システムメモリやプロセスのメモリなど）がスキャンされます。Kaspersky Embedded Systems Security は、［**通知**］レベルに対応するセキュリティ設定を適用します。*簡易スキャン*タスクの設定は変更できます。

- アプリケーション整合性チェックタスクは毎日実行されます。Kaspersky Embedded Systems Security モジュールの破損または変更を確認するオプションを提供します。アプリケーションのインストールフォルダーが確認されます。タスク実行の統計情報は、確認したモジュールの数と破損が見つかったモジュールの数を示します。タスクの設定の値は既定で定義され、編集できません。タスク開始スケジュール設定は編集できます。

- *リムーバブルドライブスキャン*のタスクは、リムーバブルドライブ上にあるファイルでも、実行またはコピーしたすべてのファイルをスキャンします。ウイルスやその他のマルウェアの拡散を防ぐため、リムーバブルドライブがコンピューターに接続された際に自動でスキャンされるよう設定することができます。

- *完全スキャン*が週単位で実行されます。このタスクにより、システムバックアップ保管領域、ブートセクター、メールデータベースを含む、保護対象デバイスが徹底的にスキャンされます。

さらに、カスタムのオンデマンドスキャンタスク（保護対象デバイス上の共有フォルダーをスキャンするタスクなど）を作成できます。

複数のオンデマンドスキャンタスクが同時に実行される場合があります。

# タスクのスキャン範囲とセキュリティ設定について

アプリケーションコンソールでは、選択したオンデマンドタスクのスキャン範囲は、本製品が管理可能な保護対象デバイスのファイルリソースのリストとして表示されます。

次のように、保護対象デバイスのファイルリソースのリストビューモードで項目またはフォルダーが表示されます：

☑ フォルダーがスキャン範囲に含まれています。

☐ フォルダーがスキャン範囲から除外されています。

### セキュリティ設定

選択したオンデマンドタスクでは、既定のセキュリティ設定は、保護範囲またはスキャン範囲全体の共通の設定として設定する方法、またはデバイスのファイルリソースリストのフォルダーや項目ごとに異なる設定として設定する方法で、変更することができます。

複数の保護範囲項目に同じオブジェクトが含まれており、これらの項目のセキュリティレベルが異なる場合は、リストの最後のルールが優先されます。たとえば、**すべてのハードディスク**（セキュリティレベル：**通知**）および ***\Users*\Downloads*** （セキュリティレベル：**カスタム**）の 2 つの項目を含む保護範囲について考えてみましょう。本製品は、フォルダー **Downloads** を除いて、通知レベルでハードディスクをスキャンします。本製品は、手動で指定された設定に従ってフォルダー **Downloads** をスキャンします。この項目は保護範囲のリストの最後にあるためです。

選択した親フォルダーに対するセキュリティ設定は、すべてのサブフォルダーに自動的に適用されます。親フォルダーのセキュリティ設定は、個別に設定されたサブフォルダーに適用されません。

次のいずれかの方法を使用して、選択したスキャン範囲または保護範囲の設定を実行できます：

- 3 つの定義済みセキュリティレベル（**最大のパフォーマンス**、**推奨**、**最大の保護**）のいずれかを選択する。
- 保護対象デバイスのファイルリソースのリストで、選択したフォルダーや項目のセキュリティ設定を手動で変更する（セキュリティレベルが［**カスタム**］に変更されます）。

# 定義済みのスキャン範囲

選択したオンデマンドスキャンタスクの保護対象デバイスのファイルリソースのリストが、［**スキャン範囲**］ウィンドウに表示されます。

ファイルリソースリストには、Microsoft Windows のセキュリティの設定に従って読み取りアクセス権のあるフォルダーが表示されます。

Kaspersky Embedded Systems Security には次の定義済みスキャン範囲が含まれています：

- **すべてのハードディスク**：Kaspersky Embedded Systems Security は保護対象デバイスのハードディスク上のオブジェクトをスキャンします。すべてのハードディスク、個々のディスク、フォルダー、ファイルをスキャン範囲に含めたりスキャン範囲から除外したりすることができます。
- **すべてのリムーバブルドライブ**：CD やリムーバブルドライブなどの外部デバイスのファイルがスキャンされます。すべてのリムーバブルドライブ、個々のディスク、フォルダー、ファイルをスキャン範囲に含めたりスキャン範囲から除外したりすることができます。
- **すべてのネットワークドライブ**：ネットワーク上のフォルダーやファイルのパスを UNC（ユニバーサルネーミング規約）フォーマットで指定して、スキャン範囲に追加できます。タスクの開始に使用するアカウントには、追加するネットワーク上のフォルダーやファイルのアクセス権がある必要があります。既定では、オンデマンドスキャンタスクはシステムアカウントで実行されます。

  接続されているネットワークドライブも、保護対象デバイスのファイルリソースのツリーには表示されません。ネットワークドライブ上のオブジェクトをスキャン範囲に含めるには、ネットワークドライブに対応するフォルダーへのパスを UNC フォーマットで指定します。

- **カーネルメモリ**：スキャンの開始時にオペレーティングシステムで実行されているプロセスの実行ファイルおよびモジュールがスキャンされます。

- **実行中のプロセスおよびスタートアップオブジェクト**：レジストリキーや設定情報ファイルによって参照されるオブジェクトがスキャンされます。たとえば、WIN.INI や SYSTEM.INI、および保護対象デバイスの起動時に自動的に起動されるアプリケーションのモジュールなどです。

- **ディスクブートセクター**：ハードディスクとリムーバブルメディアのブートセクターがスキャンされます。

- **メール**：データファイル（PST）、オフラインデータファイル（OST）など、Outlook メールクライアントに関連するファイルがスキャンされます。

- **システムバックアップ**：システムボリューム情報フォルダーの内容がスキャンされます。

標準スキャン範囲は、既定ではネットワークファイルリソースのツリーに表示されます。スキャン範囲設定でネットワークファイルリソースのリストを作成する時に、そのリストに追加できます。

既定では、オンデマンドスキャンタスクは次の範囲で実行されます：

- *簡易スキャンタスク*：
  - **すべてのハードディスク**（Windows フォルダーを除く）
  - **すべてのリムーバブルドライブ**
  - **カーネルメモリ**
  - **実行中のプロセスおよびスタートアップオブジェクト**
- *オンデマンドスキャンタスク*：
  - **すべてのハードディスク**（Windows フォルダーを除く）
  - **すべてのリムーバブルドライブ**
  - **カーネルメモリ**
  - **実行中のプロセスおよびスタートアップオブジェクト**
- *完全スキャンタスク*：
  - **すべてのハードディスク**（Windows フォルダーを除く）
  - **すべてのリムーバブルドライブ**
  - **カーネルメモリ**
  - **実行中のプロセスおよびスタートアップオブジェクト**
  - **システムバックアップ**
  - **ディスクブートセクター**
  - **メール**

# オンラインストレージのファイルのスキャン

## クラウドファイルについて

Kaspersky Embedded Systems Security は、Microsoft OneDrive のクラウドファイルを対象とした操作を実行できます。新機能である、OneDrive のファイルオンデマンド機能をサポートします。

Kaspersky Embedded Systems Security は、他のオンラインストレージをサポートしません。

OneDrive のファイルオンデマンド機能では、OneDrive のファイルをダウンロードすることなく、すべてのファイルにアクセスできるので、デバイスのストレージ容量を消費しません。必要に応じて、ファイルをハードディスクにダウンロードできます。

OneDrive のファイルオンデマンド機能が有効になっている場合、エクスプローラーの［**ステータス**］列の各ファイルの横にステータスアイコンが表示されます。ファイルにはそれぞれ次のいずれかのステータスが表示されます：

このステータスアイコンは、ファイルが*オンラインでのみ利用*できることを示します。オンライン専用ファイルは、ハードディスクに物理的に保存されません。オンライン専用ファイルは、デバイスがインターネットに接続していない時は開くことができません。

このステータスアイコンは、ファイルが*ローカルで利用*できることを示します。これは、オンライン専用ファイルを開いてデバイスにダウンロードした場合に発生します。インターネットにアクセスしていない場合でも、ローカルで利用できるファイルはいつでも開くことができます。容量を確保するために、ファイルを （オンライン専用）に変更できます。

このステータスアイコンは、ファイルが*ハードディスクに保存されており、いつでも利用*できることを示しています。

## クラウドファイルのスキャン

Kaspersky Embedded Systems Security は、保護対象デバイスのローカルに保存されているクラウドファイルのみをスキャンできます。そのような OneDriveファイルは と のステータスになっています。 ファイルは物理的に保護対象デバイス上にないため、スキャン中はスキップされます。

Kaspersky Embedded Systems Security は、ファイルがスキャン範囲に含まれていても、スキャン中に ファイルをクラウドから自動的にダウンロードすることはありません。

クラウドファイルはタスク種別に応じて、いくつかの Kaspersky Embedded Systems Security タスクによって様々なシナリオで処理されます：

- クラウドファイルのリアルタイムスキャン：クラウドファイルを含むフォルダーをファイルのリアルタイム保護タスクの保護範囲に追加できます。ユーザーがファイルにアクセスするとスキャンされます。ファイルにユーザーがアクセスすると、ダウンロードされてローカルで利用できるようになり、ステータスが に変更されます。これにより、ファイルのリアルタイム保護タスクによるファイルの処理が可能になります。

- クラウドファイルのオンデマンドスキャン：クラウドファイルを含むフォルダーをオンデマンドスキャンタスクのスキャン範囲に追加できます。このタスクでは、 と のステータスのファイルをスキャンします。ファイルが範囲内で見つかった場合、スキャン中はスキップされます。スキャンされたファイルはクラウドファイルの単なるプレースホルダーであり、ローカルディスクには存在しないことを示す情報イベントが実行ログに記録されます。

- アプリケーションコントロールルールの生成と使用：アプリケーション起動コントロールルールの自動生成を使用して、 と のファイルの許可および拒否のルールを作成できます。アプリケーション起動コントロールタスクは、プロセスに対しては「既定で拒否」の原則と個別に作成したルールを適用し、クラウドファイルに対してはこれをブロックします。

  > アプリケーション起動コントロールタスクは、ステータスに関係なく、すべてのクラウドファイルの起動をブロックします。ファイルはハードディスクに物理的に保存されていないため、ルール生成の範囲に含まれません。そのようなファイルに対して許可ルールを作成できないため、「既定で拒否」の原則が適用されます。

OneDrive のクラウドファイルで脅威が検知された場合、スキャンを実行するタスクの設定で指定された処理を適用します。この方法で、ファイルを削除、駆除、隔離、またはバックアップすることができます。

> 変更されたローカルファイルは、関連する Microsoft OneDrive の資料で説明されている仕様に従い、OneDrive に保存されているコピーと同期されます。

# 定義済みのセキュリティレベルについて

> ［**ヒューリスティック分析を使用する**］のセキュリティ設定は、設定済みセキュリティレベルの設定には含まれません。この設定を変更しても、選択した既定のセキュリティレベルは変更されません。

デバイスのファイルリソースリストで選択したフォルダーに対して、4 つの定義済みセキュリティレベルのいずれかを適用できます：［**最大のパフォーマンス**］、［**推奨**］、［**最大の保護**］、［**通知**］。これらのレベルにはそれぞれ、独自の定義済みセキュリティ設定が含まれます（以下の表を参照）。

**最大のパフォーマンス**

［**最大のパフォーマンス**］のセキュリティレベルは、保護対象デバイスとワークステーションでの Kaspersky Embedded Systems Security の使用に加えて、ファイアウォールや既存のポリシーなど、保護対象デバイスの追加のセキュリティ対策がネットワークに備えられている場合に使用してください。

**推奨**

［**推奨**］セキュリティレベルは、デバイスの保護とパフォーマンスへの影響が、最適な組み合わせで設定されています。カスペルスキーでは、このレベルがほとんどの企業ネットワークのデバイスの保護に十分なものとして推奨しています。既定では、［**推奨**］セキュリティレベルが選択されています。

### 最大の保護

組織のネットワークのデバイスセキュリティ要件が引き上げられた場合、［**最大の保護**］セキュリティレベルを推奨します。

### 通知

企業ネットワーク内に感染したコンピューターが多数存在する可能性があり、それらをブロックすると組織の業務に大きな支障をきたす可能性がある場合は、［**通知**］セキュリティレベルを推奨します。

定義済みセキュリティレベルと対応するセキュリティ設定値

| オプション | セキュリティレベル | | | |
|---|---|---|---|---|
| **最大のパフォーマンス** | **推奨** | **最大の保護** | **通知** | |
| **オブジェクト種別** | ファイル形式によってオブジェクトをスキャン | すべてのオブジェクト | すべてのオブジェクト | すべてのオブジェクト |
| **作成または変更されたファイルのみをスキャン** | 有効 | 無効 | 無効 | 無効 |
| **感染などの問題があるオブジェクトの処理** | 駆除。駆除できない場合は削除する | カスペルスキーが推奨する処理を実行 | 駆除。駆除できない場合は削除する | 通知 |
| **複合ファイルのスキャン** | 配布パッケージと Microsoft Office 形式のファイルをスキャン | すべてのアーカイブ、配布パッケージ、および Microsoft Office 形式のファイルをスキャン | すべてのアーカイブ、配布パッケージ、および Microsoft Office 形式のファイルをスキャン | すべてのアーカイブ、配布パッケージ、および Microsoft Office 形式のファイルをスキャン |
| システムに重大な影響があるオブジェクトは、オペレーティングシステムおよび Kaspersky Embedded Systems Security の動作に必要なファイルです。これらのファイルは削除できません。このようなオブジェクトに関連付けられたプロセスは終了できません。 | | | | |
| **選択したオブジェクト種別に操作を適用する** | 既定では、すべてのオブジェクト種別がスキャンされます。 | 既定では、すべてのオブジェクト種別がスキャンされます。 | 既定では、すべてのオブジェクト種別がスキャンされます。 | 既定では、すべてのオブジェクト種別がスキャンされます。 |
| **埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する** | なし | なし | なし | なし |
| **除外するファイル** | なし | なし | なし | なし |
| **オブジェクトを種別で検知しない** | なし | なし | なし | なし |
| **スキャン時間が次を超えたら停止する（秒）** | 60 秒 | なし | なし | なし |
| **スキャンする複合オブジェクトの最大サイズ（MB）** | 8 MB | なし | なし | なし |
| **iSwift を使用する** | 有効 | 有効 | 有効 | 有効 |
| **iChecker を使用する** | 有効 | 有効 | 有効 | 有効 |

# リムーバブルドライブスキャン

USB ポートを介して保護対象デバイスに接続されているリムーバブルドライブのスキャンを設定できます。

Kaspersky Embedded Systems Security は、オペレーティングシステムに USB 外部デバイスとして登録されている場合、接続したリムーバブルドライブをスキャンします。デバイスコントロールタスクによって接続がブロックされている場合はリムーバブルドライブをスキャンしません。

Kaspersky Embedded Systems Security は、スキャン中のリムーバブルディスクへのアクセスを許可します。

リムーバブルドライブの接続時に作成されるオンデマンドスキャンタスクの実行ログで、各ドライブのスキャン結果を参照できます。

リムーバブルドライブスキャンの設定は変更できます（次の表を参照）。

リムーバブルドライブスキャンの設定

| パラメータ | 既定値 | 説明 |
| --- | --- | --- |
| **USB 経由の接続でリムーバブルドライブをスキャンする** | オフ | USB 経由での保護対象デバイスへの接続時のリムーバブルドライブのスキャンは、オンにもオフにもできます。 |
| **サイズが指定した値以下ならリムーバブルドライブをスキャンする（MB）** | 4096 MB | スキャンされたドライブ上の最大データ容量を設定することによって、コンポーネントの対象範囲を縮小することができます。<br>格納データ容量が指定した値を上回る場合、リムーバブルドライブはスキャンされません。 |
| **次のセキュリティレベルでスキャンする** | 最大の保護 | 3 つのセキュリティレベルのいずれかを選択することによって、作成されたオンデマンドスキャンタスクを設定できます：<br>• **最大の保護**<br>• **推奨**<br>• **最大のパフォーマンス**<br>• **通知する**<br>感染したオブジェクト、感染した可能性が高いオブジェクト、およびその他のオブジェクトが検知された場合に使用されるアルゴリズムや、各セキュリティレベルに対するその他のスキャン設定は、オンデマンドスキャンタスクであらかじめ定義されたセキュリティレベルに対応しています。 |

# オンデマンドスキャンタスクの既定の設定

オンデマンドスキャンタスクでは、次の表の既定の設定が使用されます。ローカルのシステムオンデマンドスキャンタスクとカスタムオンデマンドスキャンタスクを設定できます。

オンデマンドスキャンタスクの既定の設定

| パラメータ | 既定値 | 説明 |
| --- | --- | --- |
| スキャン範囲 | ローカルのシステムタスクとカスタムタスクに適用されます：<br>• **簡易スキャン**：共有フォルダーと特定のオペレーティングシステムファイルを除いた保護対象デバイス全体が対象です。<br>• **オンデマンドスキャン**（カスタムタスク）：保護対象デバイス全体が対象です。<br>• **完全スキャン**：保護対象デバイスの徹底的なスキャン。 | スキャン範囲を変更することができます。［**リムーバブルドライブスキャン**］と［**アプリケーションの整合性チェック**］のローカルシステムタスクにはスキャン範囲を設定することはできません。 |

| パラメータ | 既定値 | 説明 |
| --- | --- | --- |
| セキュリティ設定 | スキャン範囲全体の共通の設定で、［**推奨**］セキュリティレベルに対応します。 | 保護対象デバイスのファイルリソースリストで選択したフォルダーに対して、次の操作を実行できます：<br>• 別の定義済みセキュリティレベルを選択する<br>• 手動でセキュリティ設定を変更する |
| **ヒューリスティック分析を使用する** | *簡易スキャン*、*オンデマンドスキャン*、*完全スキャン*のタスクでは［**中**］の分析レベルで適用されます。 | ヒューリスティックアナライザーを有効または無効にできます。また、分析レベルを設定できます。 |
| 特定の権限を使用したタスク開始の設定 | タスクがシステムアカウントで起動されます。 | *アプリケーション整合性チェック*タスクを除き、すべてのシステムオンデマンドスキャンタスクとカスタムオンデマンドスキャンタスクに対して、特定のアカウントの権限を使用して開始の設定を編集できます。 |
| **バックグラウンドモードでタスクを実行する** | オフ | オンデマンドスキャンタスクのレベルの優先度を設定できます。 |
| **タスクを簡易スキャンとする** | *オンデマンドスキャン*、*簡易スキャン*および*完全スキャン*に適用されます。 | オンデマンドスキャンタスクのレベルの優先度を設定できます。 |
| **同時に複数のスキャンタスクを実行しない** | オフ | オンデマンドスキャンタスクのレベルの優先度を設定できます。 |
| タスク開始スケジュール | ローカルシステムタスク（*簡易スキャン*、*アプリケーション整合性チェック*、*完全スキャン*）に適用されます – **毎月**。 | スケジュールによるタスクの開始を設定できます。 |

# オンデマンドスキャンの管理

このセクションでは、インターフェイスのナビゲーションと、保護対象デバイスでのオンデマンドスキャンタスクの設定について説明します。

# 操作方法

必要なタスクの設定を選択したインターフェイスから操作する方法について説明します。

## オンデマンドスキャンタスクウィザード

新規のオンデマンドスキャンタスクを作成するには：

**Kaspersky Security Center 管理コンソールで新規タスクウィザードに移動してオンデマンドスキャンタスクを作成する**

1. ローカルタスクを作成するには：
   a. Kaspersky Security Center の管理コンソールで［**管理対象デバイス**］フォルダーを展開します。
   b. 保護対象デバイスが所属する管理グループを選択します。
   c. 結果ペインの［**デバイス**］タブで、保護対象デバイスのコンテキストメニューを開きます。

d. ［**プロパティ**］メニューオプションをオンにします。

e. 表示されるウィンドウの［**タスク**］セクションで、［**追加**］をクリックします。

［**新規タスクウィザード**］ウィンドウが開きます。

2. グループタスクを作成するには：

a. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。

b. タスクを作成する管理グループを選択します。

c. ［**タスク**］タブを選択します。

d. ［**新規タスク**］をクリックします。

［**新規タスクウィザード**］ウィンドウが開きます。

3. 保護対象デバイスのカスタムグループ向けのタスクを作成するには：

a. Kaspersky Security Center の管理コンソールツリーの［**デバイスの抽出**］フォルダーで、［**抽出を実行**］をクリックしてデバイスの抽出を実行します。

b. ［**抽出結果「抽出名」**］タブを選択します。

c. ［**処理を実行**］ドロップダウンリストで、［**タスクの作成**］をオンにします。

［**新規タスクウィザード**］ウィンドウが開きます。

4. Kaspersky Embedded Systems Security で使用可能なタスクの一覧から、［**オンデマンドスキャン**］タスクを選択します。

5. ［**次へ**］をクリックして、必要に応じてタスクを設定します。

*既存のオンデマンドスキャンタスクの設定を編集するには：*

Kaspersky Security Center タスクのリストで、タスク名をダブルクリックします。

**オンデマンドスキャン**の**プロパティ**ウィンドウが表示されます。

**Kaspersky Security Center Web コンソールで新規タスクウィザードに移動してオンデマンドスキャンタスクを作成する**

1. Web コンソールのメインウィンドウで、［**デバイス**］→［**管理対象デバイス**］の順に選択します。

2. 保護対象デバイスの名前をクリックします。

3. 表示されたデバイスのプロパティウィンドウで、［**タスク**］タブを選択します。

4. ［**追加**］をクリックします。
   ［**新規タスクウィザード**］ウィンドウが開きます。

5. ［**アプリケーション**］ドロップダウンリストで、［**Kaspersky Embedded Systems Security**］を選択します。

6. ［**タスク種別**］ドロップダウンリストで、［**オンデマンドスキャン**］タスクを選択します。

7. ［**次へ**］をクリックします。

必要に応じてタスクを設定します。

*グループの新しいオンデマンドスキャンタスクの作成を開始するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］→［**タスク**］の順に選択します。

2. ［**グループ**］タブをクリックして、タスクを作成する管理グループを選択します。

3. ［**追加**］をクリックします。
   ［**新規タスクウィザード**］ウィンドウが開きます。

4. ［**アプリケーション**］ドロップダウンリストで、［**Kaspersky Embedded Systems Security**］を選択します。

5. ［**タスク種別**］ドロップダウンリストで、［**オンデマンドスキャン**］タスクを選択します。

6. ［**次へ**］をクリックします。

必要に応じてタスクを設定します。

*カスタムグループの新しいオンデマンドスキャンタスクの作成を開始するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］→［**デバイスの抽出**］の順に選択します。

2. タスクを作成する抽出を選択します。

3. ［**開始**］をクリックします。

4. ［**抽出結果**］ウィンドウで、タスクを作成するデバイスを選択します。

5. ［**新規タスク**］をクリックします。

6. ［**アプリケーション**］ドロップダウンリストで、［**Kaspersky Embedded Systems Security**］を選択します。

7. ［**タスク種別**］ドロップダウンリストで、［**オンデマンドスキャン**］タスクを選択します。

8. ［**次へ**］をクリックします。

必要に応じてタスクを設定します。

*既存のオンデマンドスキャンタスクの設定を編集するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］→［**タスク**］の順に選択します。
2. Kaspersky Security Center タスクのリストで、タスク名をクリックします。

   ［**<タスク名>**］ウィンドウが表示されます。

## オンデマンドスキャンタスクの設定ウィンドウ

単一の保護対象デバイスでオンデマンドスキャンタスクのアプリケーション設定を開くには：

**Kaspersky Security Center 管理コンソールでオンデマンドスキャンタスクの全般的な設定を開くには：**

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。
2. 保護対象デバイスが所属する管理グループを選択します。
3. ［**デバイス**］タブを選択します。
4. スキャン範囲を設定する保護対象デバイスの名前をダブルクリックします。
   保護対象デバイスのプロパティウィンドウが表示されます。
5. ［**タスク**］セクションを選択します。
6. デバイス用に作成されたタスクのリストで、作成したオンデマンドスキャンタスクを選択します。
7. ［**プロパティ**］をクリックします。
   **オンデマンドスキャン**の**プロパティ**ウィンドウが表示されます。

必要に応じてタスクを設定します。

**Kaspersky Security Center Web コンソールでオンデマンドスキャンタスクの全般的な設定を開くには：**

1. Web コンソールのメインウィンドウで、［**デバイス**］→［**管理対象デバイス**］の順に選択します。
2. 保護対象デバイスが所属する管理グループを選択します。
3. 保護対象デバイスの名前をクリックします。
4. 表示されたデバイスのプロパティウィンドウで、［**タスク**］タブを選択します。
5. デバイス用に作成されたタスクのリストで、作成したオンデマンドスキャンタスクを選択します。
6. ［**アプリケーションの設定**］タブを開きます。

**アプリケーションコンソールでオンデマンドスキャンタスクの全般的な設定を開くには：**

1. アプリケーションコンソールツリーで、［**オンデマンドスキャン**］フォルダーを展開します。
2. 設定するタスクに該当するサブフォルダーを選択します。
3. サブフォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ：<タスク名>**］ウィンドウが開きます。

# オンデマンドスキャンタスクの作成

### Kaspersky Security Center 管理コンソールでのオンデマンドスキャンタスクの作成

1. 新規タスクウィザードを起動します。
2. ［**タスク種別の選択**］ウィンドウで、［**オンデマンドスキャン**］を選択し、［**次へ**］をクリックします。
3. ［**スキャン範囲**］ウィンドウでスキャン範囲を作成します：

   既定では、保護対象デバイスの重要な領域がスキャン範囲に含まれます。スキャン範囲は、表では☑アイコンのマークが付きます。除外するスキャン範囲には、表で☐アイコンのマークが付きます。スキャン範囲は変更できます。特定の事前に設定されたスキャン範囲、ディスク、フォルダー、ネットワークオブジェクトおよびファイルを追加し、追加した範囲ごとに特定のセキュリティ設定を割り当てます。

   - スキャンから一部の範囲を除外するには、対応するリスト項目を選択して［**削除**］をクリックします。
   - 定義済みのスキャン範囲、ディスク、フォルダー、ネットワークオブジェクト、またはファイルをスキャン範囲に含めるには：
     a. ［**追加**］をクリックします。
     b. ［**スキャン範囲の選択**］ウィンドウで、リストから定義済みのスキャン範囲を選択し、［**OK**］をクリックします。
   - スキャン範囲からサブフォルダーまたはファイルを除外するには：
     a. ［**スキャン範囲**］ウィンドウで、追加されたフォルダー（またはディスク）を選択します。
     b. ［**編集**］をクリックします。
     c. ［**サブフォルダーを含む**］をオフにする。

- スキャン範囲のセキュリティ設定を変更するには：

  a. 設定を編集するスキャン範囲を選択し、［**設定**］をクリックします。

  b. ウィンドウが表示されるので、そのウィンドウで、定義済みのセキュリティレベルのいずれかを選択するか、［**設定**］をクリックしてセキュリティ設定を手動で設定します。

  セキュリティ設定は、ファイルのリアルタイム保護タスクと同じ方法で設定されます。

4. ヒューリスティックアナライザーと他のコンポーネントとの連携を設定します：

   - ヒューリスティックアナライザーの使用を設定します。
   - タスクが実行される作業プロセスに優先度［*低*］を割り当てる場合は［**バックグラウンドモードでタスクを実行する**］をオンにします。

     既定では、Kaspersky Embedded Systems Security タスクが実行される処理対象プロセスは、優先度［*中*］（[標準]）です。

   - タスクを*簡易スキャン*タスクとして使用する場合は［**タスクを簡易スキャンとする**］をオンにします。
   - ［**同時に複数のスキャンタスクを実行しない**］をオンにして、コンピューターの負荷を最適化します。

5. ［**タスクを割り当てるデバイスの選択**］ウィンドウで、デバイスのリストを指定して［**次へ**］をクリックします。

6. ［**タスクを実行するアカウントの選択**］ウィンドウで、アカウントを指定して、［**次へ**］をクリックします。

7. ［**タスクスケジュールの設定**］ウィンドウで、タスクスケジュールを設定して、［**次へ**］をクリックします。

8. タスク名を入力します。

   タスク名は 100 文字以内にする必要があり、" * < > & \ : | の記号は使用できません。

9. ［**タスク作成の終了**］ウィンドウが表示されます。［**終了**］をクリックしてタスクの作成を終了します。

選択した保護対象デバイスまたは保護対象デバイスグループに新規オンデマンドスキャンタスクが作成されます。

### Kaspersky Security Center Web コンソールでのオンデマンドスキャンタスクの作成

1. 新規タスクウィザードを起動します。
2. ［**新規タスク**］ウィンドウの［**アプリケーション**］ドロップダウンリストで、［**Kaspersky Embedded Systems Security**］を選択します。
3. ［**タスク種別**］で、［**オンデマンドスキャン**］を選択し、［**次へ**］をクリックします。
4. タスクの範囲を選択して、［**次へ**］をクリックします。
5. ［**タスクを実行するアカウントの選択**］ウィンドウで、アカウントを指定して、［**次へ**］をクリックします。
6. タスク名を入力します。

   タスク名は 100 文字以内にする必要があり、" * < > & \ : | の記号は使用できません。

7. ［**タスク作成の終了**］ウィンドウが表示されます。［**終了**］をクリックしてタスクの作成を終了します。

選択した保護対象デバイスまたは保護対象デバイスグループに新規オンデマンドスキャンタスクが作成されます。

***アプリケーションコンソールでのオンデマンドスキャンタスクの作成***

単一の保護対象デバイスを対象とするカスタムタスクは、［**オンデマンドスキャン**］フォルダーで作成できます。

*新規のオンデマンドスキャンタスクを作成して編集するには：*

1. アプリケーションコンソールツリーで、［**オンデマンドスキャン**］フォルダーのコンテキストメニューを開きます。
2. ［**タスクの作成**］を選択します。
   ［**タスクの作成**］ウィンドウが表示されます。
3. タスクの名前を入力して、［OK］をクリックします。

個々の保護対象デバイスのオンデマンドスキャンタスクが作成されます。

## オンデマンドスキャンタスクのバックグラウンドでの実行

既定では、Kaspersky Embedded Systems Security タスクが実行されるプロセスは、優先度［*中*］（［標準］）に割り当てられます。

オンデマンドスキャンタスクを実行するプロセスは、優先度［*低*］に割り当てることができます。プロセスの優先度を下げると、タスクの実行に必要な時間が長くなりますが、他の実行中のプログラムのプロセスのパフォーマンスは上がる可能性があります。

複数のバックグラウンドタスクを、優先度［低］で1つの処理プロセスで実行できます。

既存のオンデマンドスキャンタスクの優先度を変更するには、［**バックグラウンドモードでタスクを実行する**］をオンまたはオフにします。

構成されたタスクの設定が保存され、実行中のタスクにすぐに適用されます。タスクが実行中でない場合、変更された設定は次回の開始時に適用されます。

## 簡易スキャンの実行の登録

既定では、デバイスの保護ステータスが［**Kaspersky Embedded Systems Security**］フォルダーの結果ペインに表示され、*簡易スキャン*を実行したタイミングで週単位で更新されます。

デバイスの保護ステータスを更新する時間は、［**タスクを簡易スキャンとする**］がオンに設定されたオンデマンドタスクのスケジュールに紐付いています。

# オンデマンドスキャンタスクでのスキャン範囲の設定

*オペレーティングシステムの起動時*にスキャンタスクおよび*簡易スキャン*タスクのスキャン範囲を変更する場合は、セットアップウィザードを使用して Kaspersky Embedded Systems Security を修復することにより、これらのタスクの既定のスキャン範囲を復元できます。

**Kaspersky Security Center 管理コンソールでのオンデマンドスキャンタスクのスキャン範囲の設定**

1. ［**プロパティ：オンデマンドスキャン**］ウィンドウを開きます。
2. ［**スキャン範囲**］セクションを選択します。
3. スキャン範囲に範囲を追加するには、その横にあるチェックボックスをオンにします。
4. リストにないスキャン範囲を追加する場合：
   a. ［**追加**］をクリックします。
   b. 表示されたウィンドウで、範囲、個々のディスク、フォルダー、またはネットワークの場所を選択します。
   c. スキャン範囲にサブフォルダーを含める場合は、［**サブフォルダーを含む**］をオンにします。
5. スキャン範囲から個別のフォルダーを除外するには、これらのフォルダーの名前の横にあるチェックボックスをオフにします。
6. スキャン範囲を編集するには、リストからスキャン範囲を選択して［**編集**］をクリックします。

7. 以前に追加したスキャン範囲をネットワークファイルリソースのリストに表示されないようにするには、スキャン範囲を選択して［**削除する**］をクリックします。

   スキャン範囲がネットワークファイルリソースリストから削除された時に、オンデマンドスキャンタスクの範囲から除外されます。

8. ［**OK**］をクリックします。

   ［スキャン範囲の設定］ウィンドウを閉じます。新しい設定が保存されます。

**Kaspersky Security Center Web コンソールでのオンデマンドスキャンタスクのスキャン範囲の設定**

1. ［**オンデマンドスキャン**］ウィンドウを開きます。
2. ［**アプリケーション設定**］タブを選択します。
3. スキャン範囲に範囲を追加するには、その横にあるチェックボックスをオンにして、スイッチをオンに設定します。
4. リストにないスキャン範囲を追加する場合：
   a. ［**追加**］をクリックします。
   b. 表示されたウィンドウで、範囲、個々のディスク、フォルダー、またはネットワークの場所を選択します。
   c. スキャン範囲にサブフォルダーを含める場合は、［**サブフォルダー**］をオンにします。
5. スキャン範囲から個別のフォルダーを除外するには、これらのフォルダーの名前の横にあるチェックボックスをオフにします。
6. スキャン範囲を編集するには、リストからスキャン範囲を選択して［**範囲を編集**］をクリックします。
7. 以前に追加したスキャン範囲をネットワークファイルリソースのリストに表示されないようにするには、スキャン範囲を選択して［**削除する**］をクリックします。

   スキャン範囲がネットワークファイルリソースリストから削除された時に、オンデマンドスキャンタスクの範囲から除外されます。

8. ［**保存**］をクリックします。

   ［スキャン範囲の設定］ウィンドウを閉じます。新しい設定が保存されます。

***アプリケーションコンソールでのオンデマンドスキャンタスクのスキャン範囲の設定***

1. アプリケーションコンソールツリーで、［**オンデマンドスキャン**］フォルダーを展開します。
2. 設定するオンデマンドスキャンタスクに該当するサブフォルダーを選択します。

3. 選択したフォルダーの結果ペインで、［**保護範囲の設定**］をクリックします。

4. 表示されたウィンドウで、スキャン範囲に範囲を追加するには、その横にあるチェックボックスをオンにします。

5. リストにないスキャン範囲を追加する場合：

   a. ［**追加**］をクリックします。

   b. 表示されたウィンドウで、範囲、個々のディスク、フォルダー、またはネットワークの場所を選択します。

   c. スキャン範囲にサブフォルダーを含める場合は、［**サブフォルダーを含む**］をオンにします。

6. スキャン範囲から個別のフォルダーを除外するには、これらのフォルダーの名前の横にあるチェックボックスをオフにします。

7. スキャン範囲を編集するには、リストからスキャン範囲を選択して［**範囲を編集**］をクリックします。

8. 以前に追加したスキャン範囲をネットワークファイルリソースのリストに表示されないようにするには、スキャン範囲を選択して［**削除する**］をクリックします。

   スキャン範囲がネットワークファイルリソースリストから削除された時に、オンデマンドスキャンタスクの範囲から除外されます。

9. ［OK］をクリックします。

［スキャン範囲の設定］ウィンドウを閉じます。新しい設定が保存されます。

# オンデマンドスキャンタスクの設定

**Kaspersky Security Center 管理コンソールでオンデマンドスキャンタスクを設定する方法**

1. オンデマンドスキャンタスクのプロパティを開きます。

2. ［**オプション**］セクションを選択します。

3. ［**ヒューリスティック分析を使用する**］をオフまたはオンにします。

4. 必要に応じて分析レベルを変更します。

5. タスクが実行される作業プロセスに優先度［*低*］を割り当てる場合は［**バックグラウンドモードでタスクを実行する**］をオンにします。

   既定では、Kaspersky Embedded Systems Security タスクが実行される処理対象プロセスは、優先度［*中*］（[標準]）です。

6. タスクを*簡易スキャンタスク*として使用する場合は［**タスクを簡易スキャンとする**］をオンにします。

7. ［**同時に複数のスキャンタスクを実行しない**］をオンにして、コンピューターの負荷を最適化します。
8. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでオンデマンドスキャンタスクを設定する方法**

1. オンデマンドスキャンタスクのプロパティを開きます。
2. ［**アプリケーション設定**］セクションを選択します。
3. ［**設定**］に移動します。
4. ［**ヒューリスティック分析を使用する**］をオフまたはオンにします。
5. 必要に応じて、［**ヒューリスティック分析レベル**］ドロップダウンリストから分析レベルを選択します。
6. タスクが実行される作業プロセスに優先度［*低*］を割り当てる場合は［**バックグラウンドモードでタスクを実行する**］をオンにします。

   既定では、Kaspersky Embedded Systems Security タスクが実行される処理対象プロセスは、優先度［*中*］（[標準]）です。
7. タスクを*簡易スキャンタスク*として使用する場合は［**タスクを簡易スキャンとする**］をオンにします。
8. ［**同時に複数のスキャンタスクを実行しない**］をオンにして、コンピューターの負荷を最適化します。
9. 変更内容を保存します。

***アプリケーションコンソールでオンデマンドスキャンタスクを設定する方法***

1. アプリケーションコンソールツリーで、［**オンデマンドスキャン**］フォルダーを展開します。
2. 設定するオンデマンドスキャンタスクに該当するサブフォルダーを選択します。
3. 選択したフォルダーの結果ペインで、［**プロパティ**］をクリックします。
4. ［**タスク設定**］タブを選択します。
5. ［**ヒューリスティック分析を使用する**］をオフまたはオンにします。
6. 必要に応じて分析レベルを変更します。

7. タスクが実行される作業プロセスに優先度［*低*］を割り当てる場合は［**バックグラウンドモードでタスクを実行する**］をオンにします。

   既定では、Kaspersky Embedded Systems Security タスクが実行される処理対象プロセスは、優先度［*中*］（[標準]）です。

8. タスクを*簡易スキャンタスク*として使用する場合は［**タスクを簡易スキャンとする**］をオンにします。
9. ［**同時に複数のスキャンタスクを実行しない**］をオンにして、コンピューターの負荷を最適化します。
10. 変更内容を保存します。

# リムーバブルドライブスキャンの設定

### Kaspersky Security Center 管理コンソールでリムーバブルドライブスキャンの設定

1. Kaspersky Security Center の管理コンソールツリーで［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**ポリシー**］タブを選択します。
4. 設定するポリシー名をダブルクリックします。
   ポリシーのプロパティウィンドウで、［**詳細設定**］をクリックします。
5. ［**リムーバブルドライブスキャン**］サブセクションの［**設定**］をクリックします。
   ［**リムーバブルドライブスキャン**］ウィンドウが表示されます。
6. 次の操作を実行します：
   - 接続時に自動的にリムーバブルドライブをスキャンする場合、［**USB 経由の接続でリムーバブルドライブをスキャンする**］をオンにします。
   - 必要な場合は、［**サイズが指定した値以下ならリムーバブルドライブをスキャンする（MB）**］をオンにし、右側のフィールドに最大値を指定します。
   - ［**次のセキュリティレベルでスキャンする**］ドロップダウンリストで、リムーバブルドライブスキャンに必要な設定を持つセキュリティレベルを指定します。
7. ［OK］をクリックします。

指定された設定が保存、適用されます。

### Kaspersky Security Center Web コンソールでリムーバブルドライブスキャンの設定

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**詳細設定**］に移動します。
5. ［**リムーバブルドライブスキャン**］で、［**設定**］をクリックします。
   ［**リムーバブルドライブスキャン**］ウィンドウが表示されます。
6. 次の操作を実行します：
   - 接続時に自動的にリムーバブルドライブをスキャンする場合、［**USB 経由の接続でリムーバブルドライブをスキャンする**］をオンにします。
   - 必要な場合は、［**サイズが指定した値以下ならリムーバブルドライブをスキャンする（MB）**］をオンにし、右側のフィールドに最大値を指定します。
   - ［**次のセキュリティレベルでスキャンする**］ドロップダウンリストで、リムーバブルドライブスキャンに必要な設定を持つセキュリティレベルを指定します。
7. ［OK］をクリックします。

指定された設定が保存、適用されます。

### アプリケーションコンソールでリムーバブルドライブスキャンの設定

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューを開いて、［**リムーバブルドライブスキャン**］を選択します。
   ［**リムーバブルドライブスキャン**］ウィンドウが表示されます。
2. 次の操作を実行します：
   - 接続時に自動的にリムーバブルドライブをスキャンする場合、［**USB 経由の接続でリムーバブルドライブをスキャンする**］をオンにします。
   - 必要な場合は、［**サイズが指定した値以下ならリムーバブルドライブをスキャンする（MB）**］をオンにし、右側のフィールドに最大値を指定します。
   - ［**次のセキュリティレベルでスキャンする**］ドロップダウンリストで、リムーバブルドライブスキャンに必要な設定を持つセキュリティレベルを指定します。
3. ［OK］をクリックします。

# オンデマンドスキャンタスクの定義済みセキュリティレベルの選択

保護対象デバイスのファイルリソースリストで選択したフォルダーに対して、3 つの定義済みセキュリティレベルのいずれかを適用できます：[**最大のパフォーマンス**]、[**推奨**]、[**最大の保護**]。

**Kaspersky Security Center 管理コンソールで定義済みセキュリティレベルのいずれかを選択します。**

1. オンデマンドスキャンタスクのプロパティを開きます。
2. [**スキャン範囲**] セクションを選択します。
3. 保護対象デバイスのリストでスキャン範囲に含まれる項目を選択して、定義済みセキュリティレベルを設定します。
4. [**設定**] をクリックします。
5. ウィンドウが表示されるので、そのウィンドウの [**セキュリティレベル**] タブで、適用するセキュリティレベルを選択します。
6. [**OK**] をクリックします。
7. [**プロパティ：オンデマンドスキャン**] ウィンドウで、[**OK**] をクリックします。

構成されたタスクの設定が保存され、実行中のタスクにすぐに適用されます。タスクが実行中でない場合、変更された設定は次回の開始時に適用されます。

***アプリケーションコンソールで定義済みセキュリティレベルのいずれかを選択します。***

1. アプリケーションコンソールツリーで、[**オンデマンドスキャン**] フォルダーを展開します。
2. 設定するオンデマンドスキャンタスクに該当するサブフォルダーを選択します。
3. 選択したフォルダーの結果ペインで、[**保護範囲の設定**] をクリックします。
4. 保護対象デバイスのネットワークファイルリソースリストで、定義済みセキュリティレベルを設定するフォルダーまたは項目を選択します。
5. 選択したフォルダーや項目がスキャン範囲に含まれることを確認します。
6. [**設定**] をクリックします。
7. ウィンドウが表示されるので、そのウィンドウで、希望するセキュリティレベルを選択します。
   選択したセキュリティレベルに対応するセキュリティ設定のリストが表示されます。
8. [**OK**] をクリックします。

タスクの設定が保存され、実行中のタスクにすぐに適用されます。タスクが実行中でない場合、変更された設定は次回の開始時に適用されます。

# 手動でのセキュリティの設定

オンデマンドスキャンタスクでは、既定でスキャン範囲全体の共通のセキュリティ設定が使用されます。

これらの設定は、定義済みのセキュリティレベル［**推奨**］に対応します。

セキュリティ設定の既定値を編集し、スキャン範囲全体の共通の設定として、あるいは保護対象デバイスのファイルリソースのリストの項目やツリーのフォルダーごとに異なる設定として、設定することができます。

**Kaspersky Security Center 管理コンソールでの手動でのセキュリティ設定の管理**

1. オンデマンドスキャンタスクのプロパティを開きます。
2. ［**スキャン範囲**］セクションを選択します。
3. 保護対象デバイスのリストでスキャン範囲に含まれる項目を選択して、セキュリティ設定を管理します。
4. ［**設定**］をクリックします。
5. ウィンドウが表示されるので、そのウィンドウの［**セキュリティレベル**］タブで、適用するセキュリティレベルを選択します。
6. セキュリティを設定するリソースを選択します。
7. ［**設定**］をクリックします。
8. 表示されるウィンドウで、必要なセキュリティレベルを選択し、［**設定**］をクリックします。
9. ［**全般**］タブで、次の設定を行います：
   - 保護範囲に含める必要があるオブジェクト：
     - **すべてのオブジェクト**
     - **ファイル形式によってオブジェクトをスキャン**
     - **定義データベース指定の拡張子リストによってオブジェクトをスキャン**
   - ［**最適化**］ブロックで、［**作成または変更されたファイルのみを保護**］をオンまたはオフにします。
   - ［**複合ファイルのスキャン**］で、スキャン範囲に含める複合オブジェクトを指定します：
     - **アーカイブをスキャン**
     - **配布パッケージをスキャン**

- **Microsoft Office 形式のファイルをスキャン**
- **メール形式のファイルをスキャン**

10. ［**処理**］タブで、次の設定を行います：

- 感染したオブジェクトおよびその他の検知したオブジェクトの処理を選択します：
  - **駆除**
  - **駆除する。駆除できない場合は削除する**
  - **削除**
  - **推奨**
  - **通知する**
- 検知されたオブジェクトの種別に応じたオブジェクトの処理を設定します：
  a. ［**選択したオブジェクト種別に操作を適用する**］をオフまたはオンにします。
  b. ［**設定**］をクリックして、検知するオブジェクトの種別を選択します。
- 修正できない複合ファイルに対する処理を設定します（［**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**］をオフまたはオンにします）。

11. ［**パフォーマンス**］タブで、次の設定を行います：

- ［**除外リスト**］ブロック：
  - ［**除外するファイル**］をオフまたはオンにします。
  - ［**オブジェクトを種別で検知しない**］をオフまたはオンにします。
    除外リストを追加する設定ごとに［**編集**］をクリックします。
- ［**詳細設定**］ブロック：
  - **スキャン時間が次を超えたら停止する（秒）**
  - **スキャンする複合オブジェクトの最大サイズ（MB）**
  - **iSwift を使用する**
  - **iChecker を使用する**

12. 新しいセキュリティ設定を保存します。

1. オンデマンドスキャンタスクのプロパティを開きます。
2. ［**アプリケーション設定**］セクションを選択します。
3. ［**スキャン範囲**］に移動します。
4. 保護対象デバイスのネットワークファイルリソースリストで、セキュリティ設定を管理する項目を選択します。選択した項目がスキャン範囲に含まれることを確認します。
5. ［**編集**］をクリックします。
6. ドロップダウンリストからオブジェクトの保護モードを選択します：
   - **すべてのオブジェクト**
   - **ファイル形式によってオブジェクトをスキャン**
   - **定義データベース指定の拡張子リストによってオブジェクトをスキャン**
7. ［**作成または変更されたファイルのみを保護**］をオンまたはオフにして、スキャンにサブフォルダーを含めるかどうかを指定します。
8. 複合オブジェクトの保護設定を管理します：
   - **アーカイブをスキャン**
   - **配布パッケージをスキャン**
   - **Microsoft Office 形式のファイルをスキャン**
   - **メール形式のファイルをスキャン**
9. 感染したオブジェクトおよびその他の検知したオブジェクトの処理を選択します：
   - **駆除**
   - **駆除する。駆除できない場合は削除する**
   - **削除**
   - **推奨**
   - **通知する**
10. 検知されたオブジェクトの種別に応じたオブジェクトの処理を設定します：
    a. ［**選択したオブジェクト種別に操作を適用する**］をオフまたはオンにします。
    b. ［**設定**］をクリックして、検知するオブジェクトの種別を選択します。
11. 修正できない複合ファイルに対する処理を設定します（［**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**］をオフまたはオンにします）。

12. ［**除外リスト**］ブロック：

    - ［**除外するファイル**］をオフまたはオンにします。
    - ［**オブジェクトを種別で検知しない**］をオフまたはオンにします。

13. ［**ライセンスの追加**］ブロック：

    - **スキャン時間が次を超えたら停止する（秒）**
    - **スキャンする複合オブジェクトの最大サイズ（MB）**
    - **iSwift を使用する**
    - **iChecker を使用する**

14. 新しいセキュリティ設定を保存します。

***アプリケーションコンソールでの手動でのセキュリティ設定の管理***

1. アプリケーションコンソールツリーで、［**オンデマンドスキャン**］フォルダーを展開します。
2. 設定するオンデマンドスキャンタスクに該当するサブフォルダーを選択します。
3. 選択したフォルダーの結果ペインで、［**保護範囲の設定**］をクリックします。
4. 保護対象デバイスのネットワークファイルリソースリストで、セキュリティ設定を管理する項目を選択します。
5. 選択した項目がスキャン範囲に含まれることを確認します。
6. ［**設定**］をクリックします。
7. 表示されるウィンドウで、必要なセキュリティレベルを選択し、［**設定**］をクリックします。
8. ［**全般**］タブで、次の設定を行います：
    - 保護範囲に含める必要があるオブジェクト：
        - **すべてのオブジェクト**
        - **ファイル形式によってオブジェクトをスキャン**
        - **定義データベース指定の拡張子リストによってオブジェクトをスキャン**
    - ［**最適化**］ブロックで、［**作成または変更されたファイルのみを保護**］をオンまたはオフにします。
    - ［**複合ファイルのスキャン**］で、スキャン範囲に含める複合オブジェクトを指定します：
        - **アーカイブをスキャン**
        - **配布パッケージをスキャン**

- **Microsoft Office 形式のファイルをスキャン**
- **メール形式のファイルをスキャン**

9. ［**処理**］タブで、次の設定を行います：
   - 感染したオブジェクトおよびその他の検知したオブジェクトの処理を選択します：
     - **駆除**
     - **駆除する。駆除できない場合は削除する**
     - **削除**
     - **推奨**
     - **通知する**
   - 検知されたオブジェクトの種別に応じたオブジェクトの処理を設定します：
     a. ［**選択したオブジェクト種別に操作を適用する**］をオフまたはオンにします。
     b. ［**設定**］をクリックして、検知するオブジェクトの種別を選択します。
   - 修正できない複合ファイルに対する処理を設定します（［**埋め込みオブジェクトが検知され、修正できない場合、複合ファイルを完全に削除する**］をオフまたはオンにします）。
10. ［**パフォーマンス**］タブで、次の設定を行います：
    - ［**除外リスト**］ブロック：
      - ［**除外するファイル**］をオフまたはオンにします。
      - ［**オブジェクトを種別で検知しない**］をオフまたはオンにします。

      除外リストを追加する設定ごとに［**編集**］をクリックします。
    - ［**詳細設定**］ブロック：
      - **スキャン時間が次を超えたら停止する（秒）**
      - **スキャンする複合オブジェクトの最大サイズ（MB）**
      - **iSwift を使用する**
      - **iChecker を使用する**
11. 新しいセキュリティ設定を保存します。

# オンデマンドスキャンタスクの統計情報

オンデマンドスキャンタスクの実行中は、タスクが開始されてから処理されたオブジェクト数に関する情報を表示できます。

タスクが一時停止中であっても、この情報は使用できます。タスク実行ログで、タスクの統計情報を表示できます。

*オンデマンドスキャンタスクの統計情報を表示するには：*

1. アプリケーションコンソールツリーで、［**オンデマンドスキャン**］フォルダーを展開します。
2. 統計情報を表示するオンデマンドスキャンタスクを選択します。

   選択したフォルダーの結果ペインにある［**統計情報**］セクションに、タスクの統計情報が表示されます。

タスクが開始されてから Kaspersky Embedded Systems Security によって処理されたオブジェクトに関する情報を表示できます（次の表を参照）。

オンデマンドスキャンタスクの統計情報

| フィールド | 説明 |
| --- | --- |
| **検知** | 検知されたオブジェクトの数。たとえば、Kaspersky Embedded Systems Security が 5 つのファイルから 1 つの悪意のあるオブジェクトを検知した場合、このフィールドの値が 1 つ加算されます。 |
| **感染などの問題があるオブジェクト** | 検知され、感染として分類されたオブジェクトの数、または侵入者がデバイスや個人情報に損害を与える目的で使用する可能性がある正規のソフトウェアとして分類されたファイルの検知数（スキャンの範囲から除外されていない場合）。 |
| **駆除されていないオブジェクト** | 次の理由により、駆除されなかったオブジェクトの数：<br>• 検知したオブジェクトが、駆除できない種別である。<br>• 駆除中にエラーが発生した。 |
| **駆除されたオブジェクト** | 駆除されたオブジェクトの数。 |
| **削除されたオブジェクト** | Kaspersky Embedded Systems Security によって正常に削除されたオブジェクトの数。 |
| **スキャンされていないオブジェクト** | スキャンしようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由でスキャンできなかったオブジェクトの数。 |
| **アーカイブ** | Kaspersky Embedded Systems Security によってスキャンされたスアーカイブの数。 |
| **圧縮オブジェクト** | Kaspersky Embedded Systems Security によってスキャンされた圧縮オブジェクトの数。 |
| **パスワードで保護されているオブジェクト** | パスワードで保護されていたため、スキップされたオブジェクト（アーカイブなど）の数。 |
| **破損しているオブジェクト** | フォーマットが破損していたため、スキップされたオブジェクトの数。 |
| **処理エラー** | 処理がエラーになったオブジェクトの数。 |
| **削除されていないオブジェクト** | 削除しようとしたが、オブジェクトへのアクセスが他のアプリケーションによってブロックされたなどの理由で削除できなかったオブジェクトの数。 |
| **処理されていないオブジェクト** | 処理されていないオブジェクトの合計数。 |

オンデマンドスキャンタスクの統計情報を選択したタスク実行ログに表示するには、結果ペインの［**管理**］セクションにある［**タスクログを開く**］をクリックします。

タスクの完了時には、タスク実行ログの［**イベント**］タブに記録されているイベントを手動で処理してください。

# Kaspersky Embedded Systems Security データベースおよびソフトウェアモジュールのアップデート

このセクションでは、Kaspersky Embedded Systems Security のアップデートのアップデートタスクとロールバックに関する情報、およびタスク設定の手順について説明します。

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

## 定義データベースと製品機能のアップデート

Kaspersky Embedded Systems Security の定義データベースと製品機能をアップデートすることにより、コンピューターを最新の方法で保護することができます。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 Embedded Systems 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。脅威をすばやく検知するため、定義データベースと製品機能を定期的にアップデートしてください。

定期的なアップデートには、現在のライセンスが必要です。現在のライセンスがない場合、アップデートは一度だけ実行することができます。

Kaspersky Embedded Systems Security は、カスペルスキーの HTTP または FTP アップデートサーバー、Kaspersky Security Center 管理サーバー、またはその他のアップデート元から定義データベースやモジュールのアップデートをダウンロードします。

保護対象の各デバイスに更新プログラムをダウンロードすることも、1つの保護対象デバイスを仲介として使用することもできます。アップデートはそこにコピーされ、保護対象デバイスに配信されます。Kaspersky Security Center を使用して組織のデバイスのセキュリティを一元的に管理している場合は、アップデートをダウンロードするためのプロキシとして管理サーバーを機能させることができます。

アップデートのダウンロードプロセスが中断されたりエラーになったりすると、前回インストールしたアップデートの定義データベースの使用に自動的に切り替えられます。定義データベースが破損した場合は、以前インストールされたアップデートに手動でロールバックできます。

アップデートの実行中、次のオブジェクトがコンピューターにダウンロードされインストールされます：

- Kaspersky Embedded Systems Security の定義データベース：コンピューターの保護は、ウイルスおよびその他の脅威のシグネチャとそれらを無効化する方法についての情報を含む定義データベースを使用して実現されます。保護機能はこの情報を使用して、コンピューター上で感染したファイルを検索して無効化します。定義データベースには、定期的に、新しい脅威とそれに対処する方法のレコードが追加されます。このため、定義データベースを定期的にアップデートしてください。

  Kaspersky Embedded Systems Security の定義データベースに加えて、アプリケーションのコンポーネントでネットワークトラフィックのインターセプトを可能にするネットワークドライバーがアップデートされます。

- 製品機能：Kaspersky Embedded Systems Security の定義データベースに加えて、製品機能もアップデートできます。製品機能をアップデートすることにより、Kaspersky Embedded Systems Security の脆弱性が修正されるとともに新しい機能が追加され、さらに既存の機能が強化されます。

アップデート中、コンピューター上の製品機能と定義データベースがアップデート元にある最新のバージョンと比較されます。現在の定義データベースと製品機能がそれぞれの最新バージョンと異なる場合、アップデート内の不足している部分がコンピューター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。

Kaspersky Embedded Systems Security の定義データベース に関する情報は、メインウィンドウまたは通知領域の本製品のアイコンの上にカーソルを置いた際に表示されるツールチップに表示されます。

アップデート結果、およびアップデートタスクの実行中に発生するイベントに関する情報がアップデートのタスク実行ログに記録されます。

# アップデートタスクについて

Kaspersky Embedded Systems Security には、アップデートおよびアップデートのロールバックという 2 つのアップデートタスクがあります。

既定では、Kaspersky Embedded Systems Security は 1 時間ごとにアップデート元に接続します。アップデートのロールバックタスクを除くすべてのアップデートタスクは、設定が行えます。タスク設定が変更されると、次回のタスク開始時に新しい値が適用されます。

アップデートタスクの一時停止や再開は許可されません。

## アップデート

既定では、定義データベースと、可能な場合は製品機能は、アップデート元からデバイスにコピーされ、コンピューターのリアルタイム保護タスクの実行ですぐに使用が開始されます。オンデマンドスキャンタスクでは、次回の起動時からアップデートした定義データベースを使用します。

既定では、定義データベースのアップデートタスクは毎時間実行されます。

### アップデートのロールバック

このタスクにより、Kaspersky Embedded Systems Security は以前の定義データベースと製品機能に戻ります。

既定では、アップデートのロールバックタスクは無効になっています。

# Kaspersky Embedded Systems Security の定義データベースとモジュールのアップデートスキーム

アップデートタスクでのアップデート元の選択は、組織で使用されるデータベースおよびソフトウェアモジュールのアップデートスキームによって異なります。

Kaspersky Embedded Systems Security の定義データベースとモジュールは、次のスキームを使用して保護対象デバイスでアップデートできます：

- インターネットから各保護対象デバイスに、アップデートを直接ダウンロードする（スキーム 1）。
- インターネットから仲介デバイスにアップデートをダウンロードして、このデバイスから保護対象デバイスにアップデートを配信する。

  以下のアプリケーションがインストールされているデバイスは、仲介デバイスとして使用できます：

  - Kaspersky Embedded Systems Security（スキーム 2）
  - Kaspersky Security Center 管理サーバー（スキーム 3）

  > 仲介デバイスを使用したアップデートは、インターネットのトラフィックを軽減するだけでなく、保護対象デバイスのネットワークセキュリティも向上します。

リストされたアップデートスキームの説明を以下に記載します。

## スキーム 1：定義データベースとモジュールをインターネットから直接アップデートする

*インターネットから直接 Kaspersky Embedded Systems Security のアップデートを設定するには：*

各保護対象デバイスの定義データベースのアップデートタスクの設定で、カスペルスキーのアップデートサーバーをアップデート元として指定します。

アップデートフォルダーが置かれているその他の HTTPS サーバーや HTTP サーバーをアップデート元として設定できます。

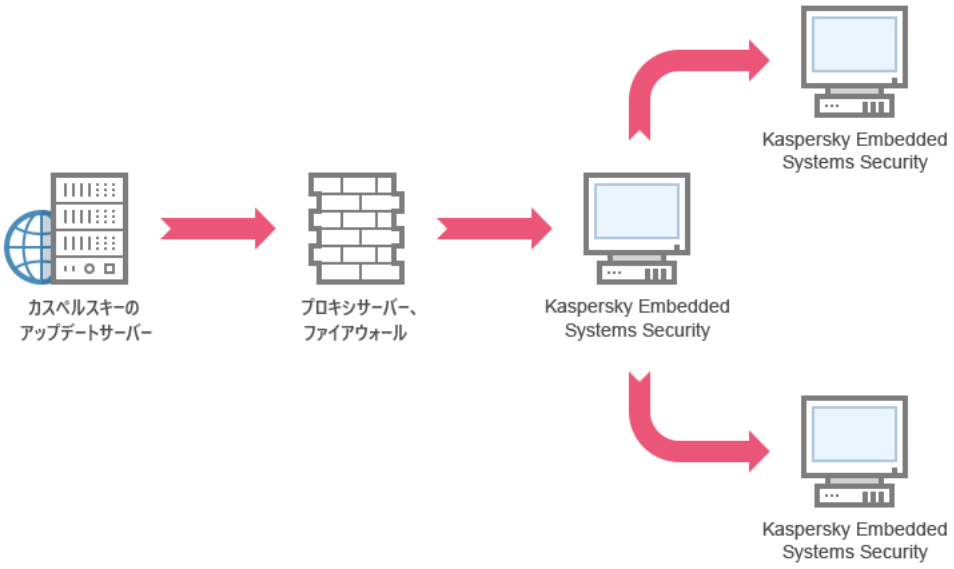
スキーム 1：定義データベースとモジュールをインターネットから直接アップデートする

# スキーム 2：定義データベースとモジュールを保護対象デバイスの 1 つを経由してアップデートする

*保護対象デバイスの 1 つを経由して Kaspersky Embedded Systems Security のアップデートを受信するよう設定するには：*

1. 選択した保護対象デバイスにアップデートをコピーします。
   - 選択した保護対象デバイスでアップデートタスクを設定します：
     a. アップデート元として、カスペルスキーのアップデートサーバーを指定します。
     b. アップデートの保存先として使用する共有フォルダーを指定します。
2. 他の保護対象デバイスにアップデートを配信します：
   - 保護対象の各デバイスでアップデートタスクを設定します。
     アップデート元として、アップデートのダウンロード先の仲介デバイスのドライブ上のフォルダーを指定します。

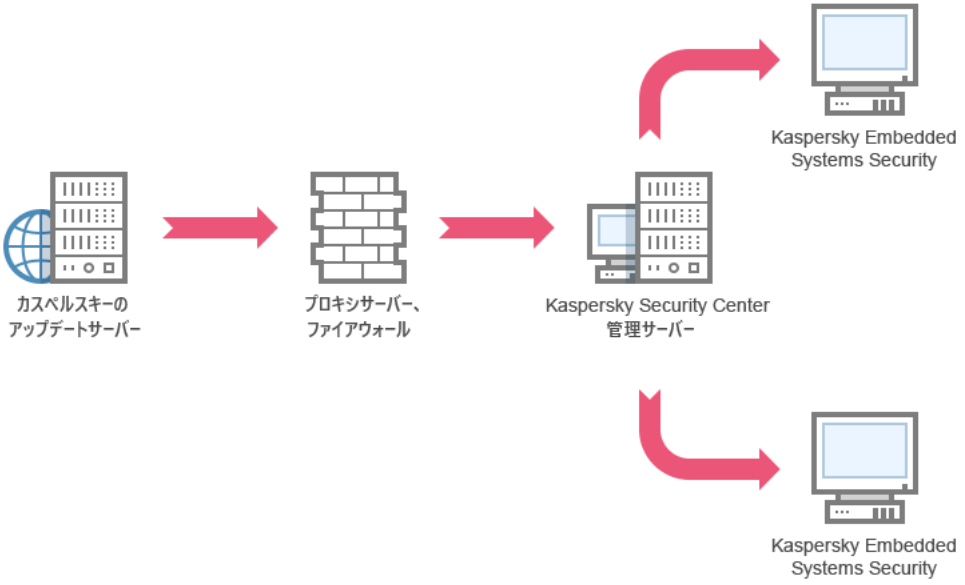
保護対象デバイスの 1 つを経由してアップデートが取得されます。




スキーム 2：定義データベースとモジュールを保護対象デバイスの 1 つを経由してアップデートする

# スキーム 3：定義データベースとモジュールを Kaspersky Security Center 管理サーバーを経由してアップデートする

Kaspersky Security Center を使用してデバイスのアンチウイルス保護を一元的に管理している場合は、ローカルネットワークにインストールされた Kaspersky Security Center 管理サーバー経由でアップデートをダウンロードできます。




スキーム 3：定義データベースとモジュールを Kaspersky Security Center 管理サーバーを経由してアップデートする

*Kaspersky Security Center 管理サーバーを経由して Kaspersky Embedded Systems Security のアップデートを受信するよう設定するには：*

1. 保護対象の各デバイスにネットワークエージェントをインストールします。ネットワークエージェントは、Kaspersky Security Center 配布キットに含まれるソフトウェアコンポーネントです。これにより、管理サーバーと Kaspersky Embedded Systems Security が保護対象デバイス上でやり取りできます。ネットワークエージェントに関する詳細と Kaspersky Security Center を使用した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 のヘルプ*を参照してください。

2. カスペルスキーのアップデートサーバーから Kaspersky Security Center 管理サーバーにアップデートをダウンロードします。

   - 指定した保護対象デバイスグループの管理サーバーでアップデートを取得するタスクを設定します。

     アップデート元として、カスペルスキーのアップデートサーバーを指定します。

3. 保護対象デバイスにアップデートを配信します。それには、次のいずれかの処理を実行します：

   - Kaspersky Security Center で、定義データベース（アプリケーションモジュール）のアップデートグループタスクを設定し、保護対象デバイスにアップデートを配信する：

   - 保護対象の各デバイスでアップデートタスクを設定します：

     a. Kaspersky Security Center 管理サーバーをアップデート元として指定します。

     b. 必要に応じて、タスクのスケジュールを設定します。

Kaspersky Security Center 管理サーバーを経由して、アップデートが取得されます。

# アップデートタスクの設定

### Kaspersky Security Center 管理コンソールでアップデートタスクを設定する方法

1. Kaspersky Security Center 管理コンソールで、設定するローカルまたはグループのアップデートタスクに移動します。
2. ［**設定**］セクションを開きます。
3. Kaspersky Security Center 管理サーバーに接続された Kaspersky Embedded Systems Security の［**ローカルモードのアップデート設定**］で、アップデート元を設定します：
   a. ［**設定**］をクリックします。
      ［**定義データベースと製品機能のアップデート**］ウィンドウが表示されます。
   b. 使用するアップデート元の横にあるチェックボックスをオンにします：
      - Kaspersky Security Center 管理サーバー
      - カスペルスキーのアップデートサーバー

      必要に応じて、［**追加**］をクリックして、カスタムのアップデート元を追加します。
   c. 複数のアップデート元を選択する場合は、［**上へ**］と［**下へ**］を使用して、アップデート元を優先度順に並べ替えます。Kaspersky Embedded Systems Security は、設定された順序に厳密に従ってアップデート元にアクセスし、最初に使用可能なアップデート元のアップデートパッケージを使用してアップデートタスクを実行します。
      既定では、Kaspersky Embedded Systems Security は Kaspersky Security Center サーバーを最初のアップデート元として使用します。これにより、アップデート時のトラフィックを節約することができます。ポリシーがコンピューターに適用されていない場合、製品が Kaspersky Security Center にアクセスできない可能性があるため、ローカルのアップデートタスクの設定でカスペルスキーサーバーが最初のアップデート元として選択されます。
   d. ［**カスペルスキーのアップデートサーバー**］をアップデート元として選択した場合は、カスペルスキーのアップデートサーバーを選択する際に Kaspersky Embedded Systems Security が従わなければならない原則を選択します：
      - **自動的に検出**：本製品は、最も近い使用可能なカスペルスキーのアップデートサーバーを使用します。
      - **リストから選択**：本製品は、リストで選択された国のカスペルスキーのアップデートサーバーを使用します。
   e. ［**定義データベースと製品機能のアップデート**］ウィンドウで、［OK］をクリックします。
4. 定義データベースのアップデートを設定します：
   a. ［**定義データベースのアップデートをダウンロードする**］をオンまたはオフにします。
   b. ［**ディスク I/O の負荷の低減**］をオンまたはオフにします。

c. ［**ディスク I/O の負荷の低減**］をオンにした場合は、［**最適化に使用するメモリ（MB）**］フィールドに、メモリの量をメガバイト単位で指定します。オペレーティングシステムは、タスクの実行中にアップデートファイルを保存するために、指定されたメモリのボリュームを一時的に割り振ります。既定のメモリのサイズは 640 MB です。最小のメモリのサイズは 400 MB です。

ディスクサブシステムの最適化機能を有効にしてアップデートタスクを実行している時に、次の問題が発生する可能性があります：

- 値が小さすぎる場合、割り当てられたメモリの量が定義データベースのアップデートタスクを完了するのに不十分である可能性があり（最初のアップデート中など）、それによってエラーが発生した状態でタスクが終了します。

  この場合、ディスクサブシステムの最適化機能でメモリの割り当てを増やしてください。

- 値が大きすぎると、定義データベースのアップデートタスクの開始時に、選択したサイズの仮想ドライブをメモリに作成できない場合があります。その結果、ディスクサブシステムの最適化機能が自動的に無効になり、定義データベースのアップデートタスクは最適化機能なしで実行されます。

  この場合、ディスクサブシステムの最適化機能でメモリの割り当てを減らしてください。

5. ソフトウェアモジュールのアップデートを設定します：

a. ［**製品機能のアップデートをダウンロードする**］をオンまたはオフにします。

b. 適用する製品機能のアップデート種別を選択します。

- **重要なアップデートおよび承認済みのアップデートをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、Kaspersky Embedded Systems Security により緊急のアップデートが自動的にインストールされ、その他すべての製品機能は、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。

- **承認済みのアップデートのみをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Embedded Systems Security によりアップデートがインストールされます。既定では、このオプションはオンです。

製品機能のアップデートで使用許諾契約書の確認と同意を要求される場合は、使用許諾契約書に同意した後で、アップデートがインストールされます。

6. ローカル保管領域のフォルダーへのアップデートのコピーを設定します：

a. ［**ローカル保管領域のフォルダーにアップデートをコピーする**］をオンまたはオフにします。

b. ローカル保管領域のフォルダーにコピーするアップデートの内容を選択します：

- **定義データベースのアップデートをコピーする**：定義データベースのアップデートのみがダウンロードされます。
- **重要な製品機能のアップデートをコピーする**：重要な製品機能のアップデートのみがダウンロードされます。
- **定義データベースとソフトウェアモジュールの重要なアップデートをコピーする**：定義データベースのアップデートと重要な製品機能のアップデートがダウンロードされます。

c. ダウンロードしたアップデートが配信されるローカルフォルダーまたはネットワークフォルダーを指定します。

7. 変更内容を保存します。

## *アプリケーションコンソールでアップデートタスクを設定する方法*

1. アプリケーションコンソールツリーで、［**アップデート**］→［**定義データベースと製品機能のアップデート**］フォルダーの順に開きます。
2. 結果ペインで［**プロパティ**］をクリックします。

   ［**プロパティ: 定義データベースと製品機能のアップデート**］ウィンドウが表示されます。
3. Kaspersky Security Center 管理サーバーに接続された Kaspersky Embedded Systems Security の［**ローカルモードのアップデート設定**］で、アップデート元を設定します：

   a. ［**設定**］をクリックします。

   ［**定義データベースと製品機能のアップデート**］ウィンドウが表示されます。

   b. 使用するアップデート元の横にあるチェックボックスをオンにします：

   - Kaspersky Security Center 管理サーバー
   - カスペルスキーのアップデートサーバー

   必要に応じて、［**追加**］をクリックして、カスタムのアップデート元を追加します。

   c. 複数のアップデート元を選択する場合は、［**上へ**］と［**下へ**］を使用して、アップデート元を優先度順に並べ替えます。Kaspersky Embedded Systems Security は、設定された順序に厳密に従ってアップデート元にアクセスし、最初に使用可能なアップデート元のアップデートパッケージを使用してアップデートタスクを実行します。

   既定では、Kaspersky Embedded Systems Security は Kaspersky Security Center サーバーを最初のアップデート元として使用します。これにより、アップデート時のトラフィックを節約することができます。ポリシーがコンピューターに適用されていない場合、製品が Kaspersky Security Center にアクセスできない可能性があるため、ローカルのアップデートタスクの設定でカスペルスキーサーバーが最初のアップデート元として選択されます。

d. ［**カスペルスキーのアップデートサーバー**］をアップデート元として選択した場合は、カスペルスキーのアップデートサーバーを選択する際に Kaspersky Embedded Systems Security が従わなければならない原則を選択します：

- **自動的に検出**：本製品は、最も近い使用可能なカスペルスキーのアップデートサーバーを使用します。
- **リストから選択**：本製品は、リストで選択された国のカスペルスキーのアップデートサーバーを使用します。

e. ［**定義データベースと製品機能のアップデート**］ウィンドウで、［**OK**］をクリックします。

4. 定義データベースのアップデートを設定します：

a. ［**定義データベースのアップデートをダウンロードする**］をオンまたはオフにします。

b. ［**ディスク I/O の負荷の低減**］をオンまたはオフにします。

c. ［**ディスク I/O の負荷の低減**］をオンにした場合は、［**最適化に使用するメモリ（MB）**］フィールドに、メモリの量をメガバイト単位で指定します。オペレーティングシステムは、タスクの実行中にアップデートファイルを保存するために、指定されたメモリのボリュームを一時的に割り振ります。既定のメモリのサイズは 640 MB です。最小のメモリのサイズは 400 MB です。

ディスクサブシステムの最適化機能を有効にしてアップデートタスクを実行している時に、次の問題が発生する可能性があります：

- 値が小さすぎる場合、割り当てられたメモリの量が定義データベースのアップデートタスクを完了するのに不十分である可能性があり（最初のアップデート中など）、それによってエラーが発生した状態でタスクが終了します。

  この場合、ディスクサブシステムの最適化機能でメモリの割り当てを増やしてください。

- 値が大きすぎると、定義データベースのアップデートタスクの開始時に、選択したサイズの仮想ドライブをメモリに作成できない場合があります。その結果、ディスクサブシステムの最適化機能が自動的に無効になり、定義データベースのアップデートタスクは最適化機能なしで実行されます。

  この場合、ディスクサブシステムの最適化機能でメモリの割り当てを減らしてください。

5. ソフトウェアモジュールのアップデートを設定します：

a. ［**製品機能のアップデートをダウンロードする**］をオンまたはオフにします。

b. 適用する製品機能のアップデート種別を選択します。

- **重要なアップデートおよび承認済みのアップデートをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、Kaspersky Embedded Systems Security により緊急のアップデートが自動的にインストールされ、その他すべての製品機能は、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。
- **承認済みのアップデートのみをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Embedded Systems Security によりアップデートがインストールされます。既定では、このオプションはオンです。

製品機能のアップデートで使用許諾契約書の確認と同意を要求される場合は、使用許諾契約書に同意した後で、アップデートがインストールされます。

6. ローカル保管領域のフォルダーへのアップデートのコピーを設定します：

   a. ［**ローカル保管領域のフォルダーにアップデートをコピーする**］をオンまたはオフにします。

   b. ローカル保管領域のフォルダーにコピーするアップデートの内容を選択します：

   - **定義データベースのアップデートをコピーする**：定義データベースのアップデートのみがダウンロードされます。
   - **重要な製品機能のアップデートをコピーする**：重要な製品機能のアップデートのみがダウンロードされます。
   - **定義データベースとソフトウェアモジュールの重要なアップデートをコピーする**：定義データベースのアップデートと重要な製品機能のアップデートがダウンロードされます。

   c. ダウンロードしたアップデートが配信されるローカルフォルダーまたはネットワークフォルダーを指定します。

7. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでアップデートタスクを設定する方法

1. Web コンソールで、設定するローカルまたはグループのアップデートタスクに移動します。
2. ［**設定**］セクションを開きます。
3. ［**ローカルモード**］タブを選択して、Kaspersky Security Center 管理サーバーに接続された Kaspersky Embedded Systems Security のアップデートタスクを設定します。
4. アップデート元を設定します：

   a. ［**アップデート元**］で、使用するアップデート元の横にあるチェックボックスをオンにします：

   - **Kaspersky Security Center 管理サーバー**
   - **カスペルスキーのアップデートサーバー**

   必要に応じて、［**追加**］をクリックして、カスタムのアップデート元を追加します。

   b. 複数のアップデート元を選択する場合は、［**上へ**］と［**下へ**］を使用して、アップデート元を優先度順に並べ替えます。Kaspersky Embedded Systems Security は、設定された順序に厳密に従ってアップデート元にアクセスし、最初に使用可能なアップデート元のアップデートパッケージを使用してアップデートタスクを実行します。

   既定では、Kaspersky Embedded Systems Security は Kaspersky Security Center サーバーを最初のアップデート元として使用します。これにより、アップデート時のトラフィックを節約することができます。ポリシーがコンピューターに適用されていない場合、製品が Kaspersky Security Center にアクセスできない可能性があるため、ローカルのアップデートタスクの設定でカスペルスキーサーバーが最初のアップデート元として選択されます。

5. 定義データベースのアップデートを設定します：

a. ［**定義データベースのアップデートをダウンロードする**］をオンまたはオフにします。

b. ［**ディスク I/O の負荷の低減**］をオンまたはオフにします。

c. ［**ディスク I/O の負荷の低減**］をオンにした場合は、［**最適化に使用するメモリ（MB）**］フィールドに、メモリの量をメガバイト単位で指定します。オペレーティングシステムは、タスクの実行中にアップデートファイルを保存するために、指定されたメモリのボリュームを一時的に割り振ります。既定のメモリのサイズは 640 MB です。最小のメモリのサイズは 400 MB です。

ディスクサブシステムの最適化機能を有効にしてアップデートタスクを実行している時に、次の問題が発生する可能性があります：

- 値が小さすぎる場合、割り当てられたメモリの量が定義データベースのアップデートタスクを完了するのに不十分である可能性があり（最初のアップデート中など）、それによってエラーが発生した状態でタスクが終了します。

  この場合、ディスクサブシステムの最適化機能でメモリの割り当てを増やしてください。

- 値が大きすぎると、定義データベースのアップデートタスクの開始時に、選択したサイズの仮想ドライブをメモリに作成できない場合があります。その結果、ディスクサブシステムの最適化機能が自動的に無効になり、定義データベースのアップデートタスクは最適化機能なしで実行されます。

  この場合、ディスクサブシステムの最適化機能でメモリの割り当てを減らしてください。

6. ソフトウェアモジュールのアップデートを設定します：

a. ［**製品機能のアップデートをダウンロードする**］をオンまたはオフにします。

b. 適用する製品機能のアップデート種別を選択します。

- **重要なアップデートおよび承認済みのアップデートをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、Kaspersky Embedded Systems Security により緊急のアップデートが自動的にインストールされ、その他すべての製品機能は、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、アップデートがインストールされます。

- **承認済みのアップデートのみをインストール**：このオプションをオンにすると、製品機能のアップデートが利用できるようになると、インストールが製品インターフェイスによってローカルで承認されるか、Kaspersky Security Center 側で承認された後でのみ、Kaspersky Embedded Systems Security によりアップデートがインストールされます。既定では、このオプションはオンです。

製品機能のアップデートで使用許諾契約書の確認と同意を要求される場合は、使用許諾契約書に同意した後で、アップデートがインストールされます。

7. ローカル保管領域のフォルダーへのアップデートのコピーを設定します：

   a. ［**アップデートをフォルダーにコピー**］をオンまたはオフにします。

   b. ローカル保管領域のフォルダーにコピーするアップデートの内容を選択します：

      - **定義データベースのアップデートをコピーする**：定義データベースのアップデートのみがダウンロードされます。
      - **重要な製品機能のアップデートをコピーする**：重要な製品機能のアップデートのみがダウンロードされます。
      - **定義データベースとソフトウェアモジュールの重要なアップデートをコピーする**：定義データベースのアップデートと重要な製品機能のアップデートがダウンロードされます。

   c. ダウンロードしたアップデートが配信されるローカルフォルダーまたはネットワークフォルダーを指定します。

8. 変更内容を保存します。

# 本製品の SMU アップデート

カスペルスキーのアップデートサービス（Seamless Update、SMU）を使用して製品をアップデートする場合、その他のアップデート方法とは異なり、インストーラを実行する必要はありません。Kaspersky Embedded Systems Security は本製品の新しいバージョンと定義データベースをを同じソースから取得します。

SMU アップデートにより、組織内のすべてのコンピューター上の本製品を最新バージョンに更新できます。SMU アップデートを適用する前に、一部のコンピューターで本製品の新しいバージョンをテストすることをお勧めします。テストする場合、テストするコンピュータ上の本製品を手動で更新する必要があります（たとえば、ローカルでセットアップウィザードを使用するなど）。SMU アップデートを実行するときに個別のコンピュータを選択することはできません。

製品のアップデートのスケジュールは、 カスペルスキーによって決定されます。新しいバージョンの製品がスムーズに実行できるよう、 カスペルスキー は段階的にアップデートを提供しています。このため、SMU アップデートは、新しいバージョンがリリースされてから最大 2 か月遅れて提供される可能性があります。

本製品の SMU アップデートは、［*定義データベースと製品機能のアップデート*］タスクを使用して管理できます。本製品の新しいバージョンを定義データベースと同じパッケージに含めるには、*製品機能*のアップデートを［*定義データベースと製品機能のアップデート*］タスクの設定で許可する必要があります。

本製品の SMU アップデートの手順

1. **本製品の新しいバージョンがリリースされる、またはモジュールがアップデートされると、 カスペルスキーはアップデートを配布します。**

2. **ユーザーが本製品のアップデートを承認します。**

   コンピュータが Kaspersky Security Center に接続されている場合、アップデートは Kaspersky Security Center の［**定義データベースとカスペルスキー製品モジュールのアップデート**］セクションで利用できます。アップデートの承認について詳しくは、Kaspersky Security Center のヘルプを参照してください。

   コンピューターが Kaspersky Security Center に接続されていない場合は、アプリケーションコンソールでアップデートを利用できます。アップデートを承認するには、［**アップデート**］-［**製品アップデート**］ の順に選択してアプリケーションのバージョンを選択し、必要に応じて契約書の条項に同意します。

3. **Kaspersky Embedded Systems Security はスケジュールに沿って［定義データベースと製品機能のアップデート］タスクを実行します。**

Kaspersky Embedded Systems Security がコンピューター上で製品をサイレントモードでアップデートします。

# Kaspersky Embedded Systems Security 定義データベースのロールバック

定義データベースのアップデートが実行される前に、過去に使用された定義データベースのバックアップコピーが作成されます。アップデートが中断されたり、エラーになったりした場合は、以前にインストールした定義データベースが自動的に使用されます。

定義データベースのアップデート後に問題が発生した場合は、*前回のアップデートのロールバック*タスクを開始して、定義データベースを以前にインストールしたアップデートにロールバックできます。

*前回のアップデートのロールバックタスクを実行するには：*

1. アプリケーションコンソールツリーで、［**アップデート**］→［**前回のアップデートのロールバック**］セクションの順に開きます。

2. 結果ペインで、［**開始**］をクリックします。

# アップデートタスクの統計情報

アップデートタスクの実行中、タスクの開始からダウンロードされたデータ量やその他のタスク実行統計情報に関するリアルタイムな情報が表示されます。

タスクの完了または停止時に、その情報をタスク実行ログで確認できます。

*アップデートタスクの統計情報を表示するには：*

アプリケーションコンソールツリーで、［**アップデート**］→［**定義データベースと製品機能のアップデート**］セクションの順に開きます。

結果パネルの［**統計情報**］では、取得したデータの総量に関する情報を確認できます。

# オブジェクトのバックアップコピーの作成

このセクションでは、検知された悪意のあるオブジェクトを駆除または削除する前にバックアップする方法について説明します。

# オブジェクトのバックアップコピーの作成：バックアップ

Kaspersky Embedded Systems Security では、駆除または削除されたオブジェクトの暗号化されたコピーがバックアップフォルダーに保存されます。

オブジェクトが複合オブジェクトの一部である場合（アーカイブの一部である場合など）は、複合オブジェクト全体がバックアップに保存されます。たとえば、メールデータベースの1つのオブジェクトの感染が検知された場合は、そのメールデータベース全体がバックアップされます。

バックアップにあるオブジェクトのサイズが大きいと、システムの速度が低下したり、ハードディスクの使用可能なディスク容量が減ったりする場合があります。

ファイルはバックアップから、元のフォルダーや、保護対象デバイスの別のフォルダーに復元できます。たとえば、感染したファイルに重要な情報が含まれていたが、整合性を損なったり情報を紛失したりすることなく駆除することができない場合に、ファイルをバックアップから復元できます。

バックアップからファイルを復元すると、保護対象デバイスが感染する可能性があります。

# バックアップ内のオブジェクトの表示

このセクションでは、バックアップ内のファイルのリストを表示する方法について説明します。

**Kaspersky Security Center 管理コンソールでバックアップのオブジェクトを表示する方法**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. コンソールの右側のペインに、バックアップ済みのオブジェクトの情報が表示されます。

**Kaspersky Security Center Web コンソールでバックアップのオブジェクトを表示する方法**

1. Web コンソールを開きます。
2. コンソールツリーで、［**操作**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. コンソールの右側のペインに、バックアップ済みのオブジェクトの情報が表示されます。

***アプリケーションコンソールでバックアップのオブジェクトを表示する方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**保管領域**］→［**バックアップ**］の順に選択します。
2. コンソールの右側のペインに、バックアップ済みのオブジェクトの情報が表示されます。

*バックアップ済みオブジェクトのリストから、重要なオブジェクトを見つけるには：*

オブジェクトの並べ替えかオブジェクトのフィルタリングを行います。

## ［バックアップ］内のファイルの並べ替え

既定では、［バックアップ］内のファイルはバックアップの日付の新しいものから順に並べ替えられます。必要なファイルを検索するために、結果ペインの任意の列の内容を基準にファイルを並べ替えることができます。

**Kaspersky Security Center 管理コンソールで［バックアップ］内のファイルを並べ替える方法**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. ファイルのリストで、オブジェクトの並べ替えに使用する列見出しを選択します。

選択した基準に基づいて、［バックアップ］内のファイルの表示順が変わります。

**Kaspersky Security Center Web コンソールで［バックアップ］内のファイルを並べ替える方法**

1. Web コンソールを開きます。
2. コンソールツリーで、［**操作**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. ファイルのリストで、オブジェクトの並べ替えに使用する列見出しを選択します。

   選択した基準に基づいて、［バックアップ］内のファイルの表示順が変わります。

***アプリケーションコンソールで［バックアップ］内のファイルを並べ替える方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**保管領域**］→［**バックアップ**］の順に選択します。
2. ファイルのリストで、オブジェクトの並べ替えに使用する列見出しを選択します。

   選択した基準に基づいて、［バックアップ］内のファイルの表示順が変わります。

## ［バックアップ］内のファイルのフィルタリング

［バックアップ］内のファイルを見つけるために、ファイルをフィルタリングして、指定したフィルタリング基準（フィルター）を満たすファイルのみがリストに表示されるようにすることができます。

**Kaspersky Security Center 管理コンソールでの［バックアップ］内のファイルのフィルタリング**

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細設定**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. 右側のペインで、［**フィルターが指定されていません**］をクリックします。
5. ［**フィルターの調整**］をクリックして、［**フィルタリング設定**］ウィンドウで、フィルタリングする列を選択します。
6. 選択した列の演算子と値を指定します。

7. 作成したフィルターが保存されます。

8. ［バックアップ］内のすべてのオブジェクトを再度表示するには、［**フィルタリング設定**］ウィンドウで、［**すべてクリア**］をクリックします。

**Kaspersky Security Center Web コンソールでの［バックアップ］内のファイルのフィルタリング**

1. Web コンソールを開きます。

2. コンソールツリーで、［**操作**］→［**保管領域**］を選択します。

3. ［**バックアップ**］フォルダーに移動します。

4. フィルターアイコンをクリックして、［**フィルター**］タブの［**追加**］をクリックします。

5. フィルター条件として使用するプロパティを選択します。

6. 選択したプロパティの条件と値を指定します。

7. ［**適用**］をクリックします。
   フィルターの設定が保存されます。

8. ［バックアップ］内のすべてのオブジェクトを再度表示するには、［**フィルター**］タブで、［**すべてクリア**］をクリックします。

***アプリケーションコンソールで［バックアップ］内のファイルをフィルタリングする方法***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**保管領域**］→［**バックアップ**］の順に選択します。

2. ファイルの表で、列見出しを選択し、左上隅にあるフィルターアイコンをクリックします。

3. フィルターを設定して、［**OK**］をクリックします。
   フィルターの設定が保存されます。

# バックアップからのファイルの復元

Kaspersky Embedded Systems Security では、発生する可能性がある危険から保護対象デバイスを保護するために、ファイルは暗号化された形式でバックアップフォルダーに保存されます。

すべてのファイルをバックアップから復元できます。

次の場合に、ファイルの復元が必要となる可能性があります。

- 感染した元のファイルに重要な情報が含まれており、Kaspersky Embedded Systems Security で整合性を保持できなかったために、ファイル内の情報が利用できなくなった場合。

- ファイルが保護対象デバイスに対して無害であると考えられ、このファイルを使用する必要がある場合。Kaspersky Embedded Systems Security でこのファイルが感染している時には、以降のスキャン時にこのファイルをファイルのリアルタイム保護タスクおよびオンデマンドスキャンタスクの処理から除外できます。

バックアップからファイルを復元すると、保護対象デバイスが感染する可能性があります。

ファイルの復元時に、復元したファイルの保管場所を選択できます。選択できるのは、元の場所（既定）、保護対象デバイスの復元したオブジェクト用の特別なフォルダー、アプリケーションコンソールがインストールされている保護対象デバイスのカスタムフォルダーです。

既定では、Kaspersky Embedded Systems Security でファイルを復元する時に、バックアップにそのファイルのコピーが作成されます。ファイルの復元後に、ファイルのコピーをバックアップから削除できます。

**Kaspersky Security Center 管理コンソールでのバックアップからのファイルの復元**

1. Kaspersky Security Center 管理コンソールツリーで、［**詳細**］→［**保管領域**］フォルダーを選択します。
2. ［**バックアップ**］フォルダーに移動します。
3. 次のいずれかを行います：
   - 1つのオブジェクトを復元するには、そのオブジェクトの名前のコンテキストメニューで［**復元**］を選択します。
   - 複数のオブジェクトを復元するには、Ctrl キーか Shift キーを使用して復元するオブジェクトを選択し、選択したオブジェクトの1つを右クリックして、コンテキストメニューから［**復元**］を選択します。
4. オブジェクトは元のフォルダーに復元されます。

**Kaspersky Security Center Web コンソールでのバックアップからのファイルの復元**

1. Web コンソールを開きます。
2. コンソールツリーで、［**操作**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. リストからオブジェクトを選択し、［**復元**］をクリックします。
5. オブジェクトは元のフォルダーに復元されます。

## *アプリケーションコンソールでのバックアップからのファイルの復元*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**保管領域**］→［**バックアップ**］の順に選択します。
2. ［**バックアップ**］フォルダーの結果ペインで、次のいずれかの処理を実行します：
   - 1つのオブジェクトを復元するには、復元するオブジェクトのコンテキストメニューから［**復元**］を選択します。
   - 複数のオブジェクトを復元するには、Ctrl キーか Shift キーを使用して復元するオブジェクトを選択し、選択したオブジェクトの1つを右クリックして、コンテキストメニューから［**復元**］を選択します。
3. ［**オブジェクトを復元**］ウィンドウで、選択したオブジェクトごとに、復元するオブジェクトの保存先のフォルダーを指定します。

   オブジェクトの名前は、ウィンドウ上部の［**オブジェクト**］に表示されます。複数のオブジェクトを選択した場合は、選択したオブジェクトのリストの最初のオブジェクトの名前が表示されます。

4. 次のいずれかを行います：
   - オブジェクトを元の場所に復元するには、［**元のフォルダーに復元**］を選択します。
   - 製品のインストール中に復元したオブジェクトの場所として指定したフォルダーにオブジェクトを復元するには、［**既定の復元用フォルダーに復元**］を選択します。
   - アプリケーションコンソールがインストールされている保護対象デバイスの別のフォルダーや共有フォルダーにオブジェクトを保存するには、［**ローカルコンピューターのフォルダーに復元**］を選択して目的のフォルダーを選択するか、そのフォルダーのパスを指定します。
5. ファイルの復元後にファイルのコピーをバックアップフォルダーに保存するには、［**復元後にオブジェクトを保管領域から削除する**］をオフにします（既定では、このチェックボックスはオフです）。
6. 指定した復元条件を残りの選択したオブジェクトに適用するには、［**選択したすべてのオブジェクトに適用する**］をオンにします。
7. ［OK］をクリックします。
8. 選択した最初のオブジェクトの復元が開始されます。
9. 指定した場所に同じ名前のオブジェクトが既に存在する場合は、［**同じ名前のオブジェクトは既に存在します**］ウィンドウが開きます。
   a. 次の Kaspersky Embedded Systems Security 処理のいずれかを選択します：
      - 既存のオブジェクトを復元されたオブジェクトに置き換えるには、［**置換**］を選択します。
      - 復元したオブジェクトを別の名前で保存するには、［**名前の変更**］を選択します。入力フィールドに、復元された新しいオブジェクトのファイル名と完全パスを入力します。
      - オブジェクトのファイル名に接尾語を追加して名前を変更するには、［**接尾語を追加して名前を変更**］を選択します。入力フィールドに接尾語を入力します。

b. 復元するオブジェクトを複数選択した場合は、［**選択したすべてのオブジェクトに適用する**］をオンにして、選択した処理（［**置換**］または［**名前の変更**］）を選択したオブジェクトの残りに適用します。［**名前の変更**］を選択した場合、［**選択したすべてのオブジェクトに適用する**］は使用できません。

c. ［**OK**］をクリックします。

オブジェクトが復元されます。復元操作に関する情報がシステム監査ログに記録されます。

［**オブジェクトを復元**］ウィンドウで［**選択したすべてのオブジェクトに適用する**］を選択しなかった場合は、［**オブジェクトを復元**］ウィンドウがもう一度開きます。このウィンドウで、選択した次のオブジェクトの保存場所を指定できます。

# バックアップからのファイルの削除

### Kaspersky Security Center 管理コンソールでのバックアップからのファイルの削除

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。右側のペインには、バックアップ済みオブジェクトのリストが表示されます。
4. 次のいずれかを行います：
   - 1つのオブジェクトを削除するには、オブジェクトのコンテキストメニューで［**削除**］を選択します。
   - 複数のオブジェクトを削除するには、Ctrl キーか Shift キーを使用して削除するオブジェクトを選択し、選択したオブジェクトの1つを右クリックして、コンテキストメニューから［**削除**］を選択します。
5. 選択したオブジェクトがバックアップから削除されます。

### Kaspersky Security Center Web コンソールでのバックアップからのファイルの削除

1. Web コンソールを開きます。
2. コンソールツリーで、［**操作**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. リストからオブジェクトを選択し、［**削除**］をクリックします。
5. 選択したオブジェクトがバックアップから削除されます。

***アプリケーションコンソールでのバックアップからのファイルの削除***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**保管領域**］→［**バックアップ**］の順に選択します。
2. 右側のペインには、バックアップ済みオブジェクトのリストが表示されます。
3. 次のいずれかを行います：
   - 1つのオブジェクトを削除するには、オブジェクトのコンテキストメニューで［**削除**］を選択します。
   - 複数のオブジェクトを削除するには、Ctrl キーか Shift キーを使用して削除するオブジェクトを選択し、選択したオブジェクトの1つを右クリックして、コンテキストメニューから［**削除**］を選択します。
4. 選択したオブジェクトがバックアップから削除されます。

# 感染の可能性があるオブジェクトを分析するためのカスペルスキーへの送信

オブジェクトのふるまいから脅威が含まれる可能性があるのに Kaspersky Embedded Systems Security で検知されない場合は、定義データベースにまだ特徴が追加されていない未知の脅威である可能性があります。このようなオブジェクトは、カスペルスキーに送信して分析してもらうことができます。カスペルスキーのアンチウイルスアナリストがこのファイルを分析し、新しい脅威が検知された場合は、その識別用レコードを定義データベースに追加します。定義データベースのアップデート後にオブジェクトを再スキャンすると、Kaspersky Embedded Systems Security によりこのオブジェクトが感染していると検知され、駆除できるようになります。オブジェクトを保持するだけでなく、ウイルスアウトブレイクを防ぐこともできます。

***Kaspersky Security Center 管理コンソールで、分析のためにオブジェクトをカスペルスキーのエキスパートに送信するには***

1. Kaspersky Security Center の管理コンソールを開きます。
2. コンソールツリーで、［**詳細**］→［**保管領域**］を選択します。
3. ［**バックアップ**］フォルダーに移動します。
4. 次のいずれかを行います：
   - 1つのオブジェクトを送信するには、そのオブジェクトの名前のコンテキストメニューで［**カスペルスキーに送信**］を選択します。
   - 複数のオブジェクトを送信するには、Ctrl キーか Shift キーを使用して送信するオブジェクトを選択し、選択したオブジェクトの1つを右クリックして、コンテキストメニューから［**カスペルスキーに送信**］を選択します。

5. コンピューター上のオブジェクトを保存するフォルダーを選択します。

6. その後、Kaspersky Threat Intelligence Portal に移動して保存したオブジェクトをアップロードして、そのオブジェクトに関する完全な情報を取得するよう要求されます。

***Kaspersky Security Center Web コンソールで、分析のためにオブジェクトをカスペルスキーのエキスパートに送信するには***

1. Web コンソールを開きます。

2. コンソールツリーで、［**操作**］→［**保管領域**］を選択します。

3. ［**バックアップ**］フォルダーに移動します。

4. リストからオブジェクトを選択し、［**カスペルスキーに送信**］をクリックします。

5. コンピューター上のオブジェクトを保存するフォルダーを選択します。

6. その後、Kaspersky Threat Intelligence Portal に移動して保存したオブジェクトをアップロードして、そのオブジェクトに関する完全な情報を取得するよう要求されます。

本製品の 3.4 以前のバージョンを 4.0 以降のバージョンにアップグレードした後でバックアップオブジェクトを移行した場合、Kaspersky Security Center Web コンソールまたは管理コンソールを使用して、分析のためにカスペルスキーにこれらのオブジェクトを送信することはできません。

# バックアップの設定

**Kaspersky Security Center 管理コンソールでバックアップを設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**詳細設定**］→［**保管領域**］の順に選択し、［**設定**］をクリックします。

4. ［**バックアップ**］タブを選択します。

5. バックアップ設定を指定します。

   - **保存期間**
   - **バックアップのサイズを制限する**
   - **空き容量のしきい値を制限する**

［バックアップ］に配置されているオブジェクトのサイズがバックアップの最大サイズを超過した場合、または空き容量のしきい値を超過した場合、その通知が表示されますが、バックアップへのオブジェクトの配置は継続されます。

6. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでバックアップを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**詳細設定**］→［**保管領域**］を選択し、［**設定**］をクリックします。
5. ［**バックアップ**］タブを選択します。
6. バックアップ設定を指定します。
   - **保存期間**
   - **バックアップのサイズを制限する**

   ［バックアップ］に配置されているオブジェクトのサイズがバックアップの最大サイズを超過した場合、その通知が表示されますが、バックアップへのオブジェクトの配置は継続されます。
7. 変更内容を保存します。

### *アプリケーションコンソールでバックアップを設定する方法*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**保管領域**］→［**バックアップ**］の順に選択します。
2. ［**バックアップ**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
3. ［**プロパティ：バックアップ**］ウィンドウで、次のバックアップ設定を指定します：
   - **保存期間**
   - **バックアップのサイズを制限する**

- **空き容量のしきい値を制限する**

  ［バックアップ］に配置されているオブジェクトのサイズがバックアップの最大サイズを超過した場合、または空き容量のしきい値を超過した場合、その通知が表示されますが、バックアップへのオブジェクトの配置は継続されます。

4. 変更内容を保存します。

# バックアップの統計情報

バックアップの現在のステータスに関する情報である、バックアップの統計情報を表示できます。

*バックアップの統計情報を表示するには：*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**保管領域**］→［**バックアップ**］の順に選択します。
2. ［**バックアップ**］フォルダーの結果ペインで、［**統計情報**］をクリックします。

   ［**バックアップ。統計情報**］ウィンドウが表示されます。［**バックアップ：統計情報**］ウィンドウに、バックアップの現在のステータスに関する情報が表示されます（次の表を参照）。

バックアップの現在のステータスに関する情報

| フィールド | 説明 |
| --- | --- |
| **現在のバックアップのサイズ** | バックアップフォルダーのデータの合計サイズ。ファイルサイズは暗号化された形式で計算されます。 |
| **オブジェクトの総数** | バックアップ内のオブジェクトの現在の合計数。 |

# ネットワークリソースへのアクセスのブロック：ブロック対象ネットワークセッション

このセクションでは、リモートデバイスをブロックし、ブロック対象ネットワークセッションのリストを設定する方法について説明します。

# ブロック対象のネットワークセッションのリスト

既定では、次のコンポーネントのいずれかがインストールされている場合、ブロック対象のネットワークセッションのリストを使用できます：ネットワーク脅威対策またはふるまい検知。コンポーネントはブロック対象ネットワークセッションのリストに従って、保護対象デバイスまたはネットワーク接続ストレージの共有フォルダーにあるオブジェクトを、リモートで暗号化したり開こうとする、あるいは実行しようとする試行を検知します。すべての保護対象デバイスのブロック対象ネットワークセッションに関する情報は、Kaspersky Security Center に送信されます。Kaspersky Embedded Systems Security は現在のセッションをブロックし、現在のセッションに関しては、共有フォルダーまたはネットワークに接続されたストレージフォルダーを使用不可にします。

ブロック対象ネットワークセッションのリストは、次のタスクのうち1つ以上のタスクが有効な状態で開始されている場合に追加されます（特定の条件下で）：

- ネットワーク脅威対策タスクの場合：ネットワーク攻撃の典型的な動作が検知された。

  Kaspersky Embedded Systems Security は、アプリケーションが再起動されたときとネットワーク脅威対策の設定が変更されたときにブロックリストを消去します。

- ふるまい検知タスクの場合：ネットワークファイルリソースにアクセスするデバイスによる悪意のある暗号化が検知された。

悪意のある活動または暗号化の試行が検知されると、タスクは攻撃しているネットワークセッションに関する情報をブロック対象ネットワークセッションのリストに送信し、本製品は攻撃しているコンピューターの現在のセッションに対して［*警告*］イベントを作成します。このセッションによる保護対象のネットワーク共有フォルダーへのアクセス試行は、すべてブロックされます。

攻撃ネットワークセッションを開始したコンピューターの LUID（ローカルで一意な識別子）がブロック対象ネットワークセッションのリストに追加されると、Kaspersky Embedded Systems Security はこの攻撃元コンピューターの IP アドレスを特定し、ブロック対象ネットワークセッションのリストに LUID の代わりにその IP アドレスを追加します。

Kaspersky Embedded Systems Security は既定で、ブロック対象ネットワークセッションがリストに追加されてから 30 分すると、そのコンピューターをリストから削除します。ブロック対象ネットワークセッションのリストからネットワークセッションが削除されると、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。ブロック対象ネットワークセッションが自動的にブロック解除されるまでの期間を設定できます。

任意のユーザーアカウントに対して保管領域の管理へのアクセスを制限する場合、ブロック対象ネットワークセッションのリストには引き続きアクセスできます。選択したユーザーアカウントが Kaspersky Embedded Systems Security を管理するための［**編集権限**］を持っていない場合に限り、ブロック対象ネットワークセッションの設定を変更することはできません。

# ブロック対象のネットワークセッションのリストの管理

悪意ある動作または暗号化動作を示すネットワークセッションを［ブロックの対象ネットワークセッションのリスト］に追加し、それらのセッションの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するには、次のコンポーネントのうち最低1つを有効にする必要があります：

- ネットワーク脅威対策
- ふるまい検知

**Kaspersky Security Center 管理コンソールでの信頼できないホストのブロックの有効化**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーウィンドウで、［**ネットワーク動作コントロール**］→［**ネットワーク脅威対策の設定**］の順に選択し、［**設定**］をクリックします。

4. 表示されたウィンドウで、［**ネットワーク脅威対策**］をオンにします。

5. ［**全般**］タブで、［**ブロックする**］モードを有効にします。

6. ［**攻撃元の端末をブロックする時間**］をオンにして、ブロック期間を指定します。

7. 変更内容を保存します。

*ポリシーのプロパティでふるまい検知の信頼できないネットワークセッションのブロックを設定するには：*

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。

2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。

3. ポリシーウィンドウで、［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］の順に選択し、［**設定**］をクリックします。

4. 表示されたウィンドウで、［**ふるまい検知**］をオンにします。

5. ［**共有フォルダーの保護**］タブに移動し、［**共有フォルダーの保護**］をオンにします。

6. ［**接続をブロックする時間**］をオンにして、ブロック期間を指定します。

7. 必要に応じて、IP アドレスとマスクで保護範囲と除外項目を指定します。

8. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでの信頼できないホストのブロックの有効化**

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

2. Kaspersky Embedded Systems 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. ［**ネットワーク動作コントロール**］→［**ネットワーク脅威対策**］に移動し、［**設定**］をクリックします。

5. 表示されたウィンドウで、［**ネットワーク脅威対策を有効にする**］をオンにします。

6. ［**ブロック**］モードを有効にします。

7. ［**攻撃元の端末をブロックする時間**］をオンにして、ブロック期間を指定します。

8. 必要に応じて、IP アドレスで除外項目を指定します。

9. 変更内容を保存します。

*ふるまい検知の信頼できないネットワークセッションのブロックを設定するには：*

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**コンピューターのリアルタイム保護**］→［**ふるまい検知**］に移動し、［**設定**］をクリックします。
5. 表示されたウィンドウで、［**ふるまい検知を有効にする**］をオンにします。
6. ［**共有フォルダーの保護**］タブに移動し、［**外部からの暗号化に対する共有フォルダーの保護を有効にする**］をオンにします。
7. ［**外部からの共有フォルダーの暗号化を検知したとき**］セクションで、［**接続をブロックする**］をオンにして、ブロック期間を指定します。
8. 必要に応じて、IP アドレスとマスクで保護範囲と除外項目を指定します。
9. 変更内容を保存します。

***アプリケーションコンソールでの信頼できないホストのブロックの有効化***

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**ネットワーク脅威対策**］の順に選択します。
2. ［**ネットワーク脅威対策**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
   ［**プロパティ: ネットワーク脅威対策**］ウィンドウが表示されます。
3. 表示されたウィンドウで、［**ネットワーク脅威対策**］をオンにします。
4. ［**全般**］タブで、［**ブロックする**］モードを有効にします。
5. ［**攻撃元の端末をブロックする時間**］をオンにして、ブロック期間を指定します。
6. 変更内容を保存します。

*ふるまい検知の信頼できないネットワークセッションのブロックを設定するには：*

1. Kaspersky Embedded Systems Security コンソールツリーで、［**コンピューターのリアルタイム保護**］→［**アンチクリプター**］の順に選択します。
2. ［**ふるまい検知**］フォルダーの結果ペインで、［**プロパティ**］をクリックします。
3. 表示されたウィンドウで、［**ふるまい検知**］をオンにします。
4. ［**共有フォルダーの保護**］タブに移動し、［**共有フォルダーの保護**］をオンにします。

5. ［**接続をブロックする時間**］をオンにして、ブロック期間を指定します。
6. 必要に応じて、IP アドレスとマスクで保護範囲と除外項目を指定します。
7. 変更内容を保存します。

***アプリケーションコンソールでのブロック対象のセッションのリストの設定***

1. アプリケーションコンソールツリーで、［**保管領域**］フォルダーを展開します。
2. ［**ブロック対象のネットワークセッション**］サブフォルダーを選択します。
3. 結果ペインで、［**プロパティ**］をクリックします。
4. 表示されたウィンドウで、［**攻撃元の端末をブロックする時間**］をオンにして、ブロック期間を指定します。
5. すべてのブロック対象のネットワークセッションへのアクセスを復元するには、ウィンドウの上部にある［**すべてブロック解除**］をクリックします。

   すべてのネットワークセッションがリストから削除されてブロック解除されます。
6. ブロック対象のネットワークセッションのリストからネットワークセッションを削除するには、結果ペインのリストで1つまたは複数のセッションを選択し、ウィンドウの上部にある［**選択項目のブロック解除**］をクリックします。

   選択したネットワークセッションのブロックが解除されます。

# イベントの登録：Kaspersky Embedded Systems Security のログ

このセクションでは、Kaspersky Embedded Systems Security ログの操作について説明します。

## Kaspersky Embedded Systems Security のイベントを登録する方法

Kaspersky Embedded Systems Security のイベントは、2 つのグループに分けられます：

- アプリケーションコンポーネントの動作や、Kaspersky Embedded Systems Security のタスクでのオブジェクトの処理に関連するイベント
- アプリケーションの起動、タスクの作成や削除、タスク設定の編集などの Kaspersky Embedded Systems Security の管理に関連するイベント

Kaspersky Embedded Systems Security では、イベントの記録に次の方法を使用します：

- **アプリケーションコンポーネントの操作ログ**：ログには、アプリケーションコンポーネントの操作中に発生したイベントに関する情報が含まれます。
- **システム監査ログ**：システム監査ログには、Kaspersky Embedded Systems Security の管理に関連するイベントの情報が含まれます。さらに、保護対象デバイスでのセキュリティ侵害や試行されたセキュリティ侵害に関連するイベントの情報が含まれます。
- **イベントログ**：イベントログには、Kaspersky Embedded Systems Security の動作エラーの診断に必要なイベントの情報が含まれます。イベントログは、Microsoft Windows イベントビューアで確認できます。

以下のリンクからダウンロードできるファイルには、次のカテゴリの Kaspersky Embedded Systems Security イベントが含まれています：

- Kaspersky Embedded Systems Security がイベントログに書き込むイベント

  WEL-EVENTS .ZIP をダウンロード
- Kaspersky Embedded Systems Security が管理サーバーに送るイベント

  KSC-EVENTS.ZIP をダウンロード

# ログ設定の指定

Kaspersky Embedded Systems Security のログの次の設定を編集できます：

- タスク実行ログとシステム監査ログのイベントの保管期間
- タスク実行ログとシステム監査ログのファイルの保存先フォルダーの場所
- ［*定義データベースがアップデートされていません*］、［*定義データベースが長期間アップデートされていません*］、および［*簡易スキャンが長期間実行されていません*］のイベント生成しきい値
- Kaspersky Embedded Systems Security によりタスク実行ログおよびシステム監査ログに保存されるイベント、イベントビューア内の Kaspersky Embedded Systems Security のイベントログ
- Syslog プロトコルにより syslog サーバーに監査イベントとタスクパフォーマンスイベントを公開するための設定

**Kaspersky Security Center 管理コンソールでログを設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ログと通知**］を選択します。
4. ［**実行ログ**］セクションで、［**設定**］をクリックします。
   ［**通知**］ウィンドウが表示されます。
5. このウィンドウで、設定するログを選択し、個々のイベントの設定を指定します：
   - イベントが保存される場所：ローカルレポートまたは Windows イベントログ
   - イベント通知：メールで通知、ターミナルサービスを使用して通知、実行ファイルを実行して通知
   - イベントを SIEM サーバーに送信するか、Kaspersky Security Center に送信するか
6. ［**イベント生成しきい値の設定**］をクリックして、イベント生成しきい値を設定します。
7. 表示されたウィンドウで、［*定義データベースがアップデートされていません*］、［*定義データベースが長期間アップデートされていません*］、および［*簡易スキャンが長期間実行されていません*］のイベントを登録する経過日数を指定します。
8. ［**SIEM 通知の設定**］をクリックして、SIEM サーバー接続を設定します。
9. ［**メール通知の設定**］をクリックして、メール通知を設定します。
10. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでログを設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ログと通知**］→［**実行ログ**］に移動し、［**設定**］をクリックします。
5. 表示されたウィンドウの［**通知**］タブで、設定するログを選択し、個々のイベントの設定を指定します：
   - イベントが保存される場所：ローカルレポートまたは Windows イベントログ
   - イベント通知：メールで通知、ターミナルサービスを使用して通知、実行ファイルを実行して通知
   - イベントを SIEM サーバーに送信するか、Kaspersky Security Center に送信するか
6. ［**メール通知の設定**］タブで、メール通知を設定します。
7. ［**SIEM 連携**］タブで、SIEM サーバー接続を設定します。
8. 変更内容を保存します。

### *アプリケーションコンソールでログを設定する方法：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーのコンテキストメニューを開きます。
2. ［**プロパティ**］を選択します。
   ［**通知**］ウィンドウが表示されます。
3. このウィンドウで、設定するログを選択し、個々のイベントの設定を指定します：
   - イベントが保存される場所：ローカルレポートまたは Windows イベントログ
   - イベント通知：メールで通知、ターミナルサービスを使用して通知、実行ファイルを実行して通知
   - イベントを SIEM サーバーに送信するか、Kaspersky Security Center に送信するか
4. ［**イベント生成しきい値の設定**］をクリックして、イベント生成しきい値を設定します。
5. 表示されたウィンドウで、［*定義データベースがアップデートされていない日数*］、［*定義データベースが長期間アップデートされていない日数*］、および［*簡易スキャンが長期間実行されていない日数*］のイベントを登録する経過日数を指定します。
6. ［**SIEM 通知の設定**］をクリックして、SIEM サーバー接続を設定します。

7. ［**メール通知の設定**］をクリックして、メール通知を設定します。

8. 変更内容を保存します。

# ログ内のイベントの並べ替え

既定では、ログのイベントは、新しいものから順に表示されます。

*ログでイベントを並べ替えるには：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーのコンテキストメニューを開きます。
2. 必要なログを選択します。
3. 結果ペインで、リストのイベントの並べ替えに使用する列の見出しを選択します。

   並べ替えの結果は、次にログを表示するまで保存されます。

# ログ内のイベントのフィルタリング

指定したフィルタリング条件を満たすイベントのレコードのみが表示されるように、ログを設定できます。

*ログでイベントをフィルタリングするには：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーを展開します。
2. フィルターを設定するログを選択し、結果ペインで［**フィルター**］をクリックします。
   ［**フィルターの設定**］ウィンドウが表示されます。
3. フィルターを追加するには、次の手順を実行します：
   a. ［**フィールド名**］リストで、イベントのフィルタリングに使用する列を選択します。
   b. ［**演算子**］リストで、フィルタリング条件を選択します。フィルタリング条件は、［**フィールド名**］リストで選択した項目によって変わります。
   c. ［**フィールド値**］リストで、フィルターの値を選択します。
   d. ［**追加**］をクリックします。

   追加したフィルターが、［**フィルターの設定**］ウィンドウのフィルターのリストに表示されます。

4. 必要に応じて、次のいずれかの処理を実行します：

   - 論理演算子「AND」を使って複数のフィルターを組み合わせるには、［**すべての条件が満たされた場合**］を選択します。
   - 論理演算子「OR」を使って複数のフィルターを組み合わせるには、［**いずれかの条件が満たされた場合**］を選択します。

5. ［**OK**］をクリックして、フィルタリング条件をログイベントに保存します。

ログのイベントのリストには、フィルタリング条件を満たすイベントのみが表示されます。フィルタリングの結果は、次にログを表示するまで保存されます。

*フィルターを無効にするには：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーを展開します。
2. フィルターを削除するログを選択し、［**フィルターの削除**］をクリックします。

この操作を実行すると、ログにはすべてのイベントが表示されます。

# ログからのイベントの削除

既定では、Kaspersky Embedded Systems Security はログ記録を 30 日間保持します。ログのレコードの保存期間は変更できます。

*ログからイベントを削除するには：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーを展開します。
2. イベントを削除するログを選択し、結果ペインで［**消去**］をクリックします。
3. 消去の操作を確認します。

ログの内容が消去されます。

# ログからの情報のエクスポート

ログから CSV ファイルまたは TXT ファイルにデータをエクスポートできます。

*ログからイベントをエクスポートするには：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーを展開します。
2. ログを選択して、結果ペインで、［**ログをエクスポート**］をクリックします。
   ［**名前を付けて保存**］ウィンドウが表示されます。

3. ログのデータのエクスポート先となるファイルの名前、場所、種別を指定します。

4. ［**保存**］をクリックします。

ログの情報が指定されたファイルに保存されます。

# システム監査ログ

Kaspersky Embedded Systems Security は、Kaspersky Embedded Systems Security の管理に関連したイベントのシステム監査を実行します。本製品の起動、Kaspersky Embedded Systems Security タスクの開始と停止、タスク設定の変更、オンデマンドスキャンタスクの作成と削除の情報がログに記録されます。本製品では、保護対象デバイスでのセキュリティ侵害や試行されたセキュリティ侵害に関連するイベントの情報もログに記録されます。アプリケーションコンソールで［**システム監査**］を選択すると、これらのすべてのイベントの記録が結果ペインに表示されます。

既定では、記録はシステム監査ログに 30 日間に保存されます。ログのレコードの保存期間は変更できます。

システム監査ログが含まれたファイルを保存するために Kaspersky Embedded Systems Security で使用するフォルダーを既定以外の場所で指定できます。

# 実行ログ

Kaspersky Embedded Systems Security のコンポーネントとタスクの操作に関する情報は、アプリケーションコンソールの［**ログと通知**］セクションで、コンポーネント名またはタスク名のフォルダーを選択すると結果ペインに表示されます。

既定では、レコードはコンポーネントとタスクのログに 30 日間に保存されます。タスクの保存期間は、タスクの完了時点から開始されます。タスク実行ログとコンポーネントログのレコードの保存期間は変更できます。

Kaspersky Embedded Systems Security で使用するフォルダーを指定して、タスク実行ログとコンポーネントログのファイルを既定以外のフォルダーに保存できます。タスク実行ログとコンポーネントログに記録されるイベントを選択することもできます。

# タスク実行ログでの Kaspersky Embedded Systems Security のタスクに関する統計と情報の表示

タスク実行ログには、タスクの開始からタスクで発生したすべてのイベントに関する詳細情報、タスク実行の統計、およびタスク設定が表示されます。

*Kaspersky Embedded Systems Security のタスクに関する統計と情報を表示するには：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーを展開します。

2. タスクを選択して、結果ペインで、［**統計情報**］タブを選択します。

# イベントビューアでの Kaspersky Embedded Systems Security のイベントログの表示

Microsoft 管理コンソールで Microsoft Windows の［イベントビューア］スナップインを使用して Kaspersky Embedded Systems Security のイベントログを表示できます。ログには、Kaspersky Embedded Systems Security で登録されている、Kaspersky Security の動作エラーの診断に必要なイベントが含まれます。

イベントログに登録されるイベントを次の基準に基づいて選択できます：

- **イベントの種別**。
- **詳細レベル**：詳細レベルは、ログに登録されるイベント（情報イベント、注意が必要なイベント、または緊急イベント）の重要度のレベルに対応しています。最も情報が多いのは情報レベルで、すべてのイベントが登録されます。最も情報が少ないのは緊急レベルで、緊急イベントのみが登録されます。

*Kaspersky Embedded Systems Security のイベントログを表示するには：*

1. ［**スタート**］をクリックし、検索バーに `mmc` コマンドを入力して、**ENTER** キーを押します。
   Microsoft 管理コンソールが開きます。
2. ［**ファイル**］>［**スナップインの追加と削除**］の順に選択します。
   ［**スナップインの追加と削除**］ウィンドウが開きます。
3. 使用可能なスナップインのリストで、［**イベントビューア**］スナップインを選択して［**追加**］をクリックします。
   ［**コンピューターの選択**］ウィンドウが開きます。
4. ［**コンピューターの選択**］ウィンドウで、Kaspersky Embedded Systems Security がインストールされている保護対象デバイスを指定し、［**OK**］をクリックします。
5. ［**スナップインの追加と削除**］ウィンドウで、［**OK**］をクリックします。
   Microsoft 管理コンソールツリーに、［**イベントビューア**］フォルダーが表示されます。
6. ［**イベントビューア**］フォルダーを展開し、［**アプリケーションとサービス ログ**］→［**Kaspersky Security**］サブフォルダーを選択します。

Kaspersky Embedded Systems Security イベントログが開きます。

# SIEM 連携について

低パフォーマンスデバイスの負荷を低下させ、アプリケーションログのサイズの肥大化によるシステムの性能低下のリスクを低減するために、Syslog プロトコルによる *syslog* サーバーへの監査イベントおよびタスクパフォーマンスイベントの公開を設定できます。

syslog サーバーは、イベント（SIEM）を集計するための外部サーバーです。受信したイベントを保管、分析し、その他のログ管理処理も実行します。

次の 2 つのモードで SIEM 連携を使用できます：

- syslog プロトコルでリモート syslog サーバーにイベントを送信する：このモードでは、ログの設定で公開が設定されたすべてのタスクパフォーマンスイベントとすべてのシステム監査イベントが、SIEM サーバーへの送信後も保護対象デバイスに引き続き格納されます。

  このモードを使用して、保護対象デバイスの負荷をできるだけ軽減してください。

- リモート syslog サーバーに送信されたイベントの場合、ローカルコピーを削除する：このモードでは、アプリケーションの操作中に登録され、SIEM サーバーに公開されたすべてのイベントが、保護対象デバイスから削除されます。

  セキュリティログのローカルバージョンは決して削除されません。

Kaspersky Embedded Systems Security はアプリケーションログのイベントを syslog サーバーでサポートされる形式に変換して、イベントを送信し SIEM サーバーが正常に認識できるようにできます。STRUCTURED-DATA 形式や JSON 形式への変換がサポートされています。

使用されている SIEM サーバーの設定に基づいて、イベントのフォーマットを選択してください。

# SIEM 連携設定

既定では、SIEM 連携は使用されません。SIEM 連携は、有効化や無効化、関連する設定ができます。

複数の SIEM サーバーへの接続を設定することで、イベントが SIEM サーバーに送信されないリスクを軽減できます。

Kaspersky Embedded Systems Security はリストの 1 番目の SIEM サーバーに接続します。接続試行が失敗した場合、Kaspersky Embedded Systems Security はリスト内の他のサーバーへの接続を 1 つずつ試行します。

Kaspersky Embedded Systems Security では、SIEM サーバーへの接続試行の失敗および SIEM サーバーへのイベント送信中のエラーについて、システム監査イベントを使用して通知することもできます。

**Kaspersky Security Center 管理コンソールで SIEM を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ［**ログと通知**］セクションを選択します。
4. ［**SIEM 連携**］ブロックの［**設定**］をクリックします。
   ［**SIEM 連携**］ウィンドウが表示されます。
5. ［**連携の設定**］ブロックで、［**SIEM サーバーへのセキュリティイベント転送を有効にする**］をオンにします。

6. ［**SIEM サーバーへの接続設定**］ブロックで、SIEM サーバー接続を設定します。

   a. ［**追加**］をクリックします。

   b. これにより、［**サーバーを追加する**］ウィンドウが開きます。そのウィンドウで、SIEM のサーバーのアドレス（IPv4、DNS）、ポート、および接続プロトコルを入力します。

   c. ［**TCP 接続のセキュリティ設定**］をクリックします。

   d. これにより、［**TCP 接続のセキュリティ設定**］ウィンドウが開きます。そのウィンドウで、SIEM サーバーの接続設定を管理します（下の表を参照）。

7. 必要に応じて、［**SIEM サーバーへのイベントの転送設定**］ブロックの［**リモート syslog サーバーに送信されたイベントのローカルコピーを削除する**］をオンにします。チェックボックスがオンの場合、SIEM サーバーに正常に公開されると、イベントのローカルコピーが削除されます。低パフォーマンスのデバイスにはこのモードをお勧めします。チェックボックスがオフの場合、ただ SIEM サーバーにイベントが送信されます。ログのコピーは、引き続きローカルに保存されます。既定では、このチェックボックスはオフです。

   セキュリティログのローカルバージョンは決して削除されません。

8. ［**イベント形式**］ブロックで、アプリケーションのイベントを SIEM サーバーに送信できるように変換する形式を選択します。既定では、［**イベントを構造化データに変換する**］オプションはオンです。使用されている SIEM サーバーの設定に基づいて、イベントのフォーマットを選択してください。

9. コンピューターにポリシーを適用するには、南京錠（）を閉じます。

10. ［**OK**］をクリックして、変更内容を保存します。

### Kaspersky Security Center Web コンソールで SIEM 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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**ログと通知**］セクションを選択します。

5. ［**SIEM 連携**］ブロックの［**設定**］をクリックします。
   ［**SIEM 連携**］ウィンドウが表示されます。

6. ［**SIEM サーバーへのセキュリティイベント転送を有効にする**］チェックボックスをオンにします。

7. ［**SIEM サーバーへの接続設定**］ブロックで、SIEM サーバー接続を設定します。

   a. ［**追加**］をクリックします。

   b. これにより、［**SIEM サーバー**］ウィンドウが開きます。そのウィンドウで、SIEM のサーバーのアドレス（IPv4、DNS）、ポート、および接続プロトコルを入力します。

   c. ［**接続の保護**］セクションで、［**SIEM サーバーへの接続設定**］をクリックします。

   d. これにより、［**SIEM サーバーへの接続設定**］ウィンドウが開きます。そのウィンドウで、SIEM サーバーの接続設定を管理します（下の表を参照）。

   e. ［**イベント形式**］ブロックで、アプリケーションのイベントを SIEM サーバーに送信できるように変換する形式を選択します。既定では、［**イベントを構造化データに変換する**］オプションはオンです。使用されている SIEM サーバーの設定に基づいて、イベントのフォーマットを選択してください。

   f. 必要に応じて、［**接続設定**］ブロックの［**リモート syslog サーバーに送信されたイベントのローカルコピーを削除する**］をオンにします。チェックボックスがオンの場合、SIEM サーバーに正常に公開されると、イベントのローカルコピーが削除されます。低パフォーマンスのデバイスにはこのモードをお勧めします。チェックボックスがオフの場合、ただ SIEM サーバーにイベントが送信されます。ログのコピーは、引き続きローカルに保存されます。既定では、このチェックボックスはオフです。

      セキュリティログのローカルバージョンは決して削除されません。

8. コンピューターにポリシーを適用するには、南京錠（🔒）を閉じます。

9. ［**OK**］をクリックして、変更内容を保存します。

**アプリケーションコンソールで SIEM 連携を設定する方法**

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーのコンテキストメニューを開きます。

2. ［**SIEM 連携**］を選択します。
   ［**SIEM 連携**］ウィンドウが表示されます。

3. ［**連携の設定**］ブロックで、［**SIEM サーバーへのセキュリティイベント転送を有効にする**］をオンにします。

4. ［**SIEM サーバーへの接続設定**］ブロックで、SIEM サーバー接続を設定します。

   a. ［**追加**］をクリックします。

   b. これにより、［**サーバーを追加する**］ウィンドウが開きます。そのウィンドウで、SIEM のサーバーのアドレス（IPv4、DNS）、ポート、および接続プロトコルを入力します。

   c. ［**TCP 接続のセキュリティ設定**］をクリックします。

   d. これにより、［**TCP 接続のセキュリティ設定**］ウィンドウが開きます。そのウィンドウで、SIEM サーバーの接続設定を管理します（下の表を参照）。

5. 必要に応じて、［**SIEM サーバーへのイベントの転送設定**］ブロックの［**リモート syslog サーバーに送信されたイベントのローカルコピーを削除する**］をオンにします。チェックボックスがオンの場合、SIEM サーバーに正常に公開されると、イベントのローカルコピーが削除されます。低パフォーマンスのデバイスにはこのモードをお勧めします。チェックボックスがオフの場合、ただ SIEM サーバーにイベントが送信されます。ログのコピーは、引き続きローカルに保存されます。既定では、このチェックボックスはオフです。

   セキュリティログのローカルバージョンは決して削除されません。

6. ［**イベント形式**］ブロックで、アプリケーションのイベントを SIEM サーバーに送信できるように変換する形式を選択します。既定では、［**イベントを構造化データに変換する**］オプションはオンです。使用されている SIEM サーバーの設定に基づいて、イベントのフォーマットを選択してください。

7. ［OK］をクリックして、変更内容を保存します。

SIEM サーバーの接続設定

| パラメータ | 説明 |
| --- | --- |
| **タイムアウト（秒）** | SIEM 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 Embedded Systems Security は別の SIEM サーバーに接続を試みます。 |
| **サーバー TLS 証明書** | SIEM サーバーと信頼済みの接続を確立するための TLS 証明書。SIEM 管理インターフェイスを使用して TLS 証明書を取得できます。 |
| **相互認証を使用する** | Kaspersky Embedded Systems Security と SIEM 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、SIEM 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。暗号化コンテナーとは、証明書と秘密鍵が含まれた PFX アーカイブです。SIEM を設定した後、チェックボックスを使用して Kaspersky Embedded Systems Security の設定で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。<br>暗号化コンテナー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ーを追加することはできません。 |

# 管理者およびユーザーへの通知方法

デバイスにアクセスする管理者とユーザーに、Kaspersky Embedded Systems Security の動作中の次のイベント、およびデバイスのアンチウイルス保護ステータスについて通知するよう設定できます。

- 管理者は、選択したイベント種別の情報を受信できます。
- デバイスにアクセスする LAN ユーザーとターミナルデバイスのユーザーは、ファイルのリアルタイム保護タスクでの［*オブジェクトが検知されました*］のイベント種別の情報を受信できます。

次の様々な方法を使用して管理者またはユーザーへの通知を有効にできます：

- ターミナルサービスツール

  保護対象デバイスがターミナルとして使用されている場合、ターミナルの保護対象デバイスのユーザーへの通知にこの方法を適用できます。

- 実行ファイルの実行

  この方法では、イベントが発生した時に、保護対象デバイスのローカルドライブに保存されている実行ファイルを実行します。

- メールで送信

  この方法では、メールを使用してメッセージを送信します。

個々のイベント種別用にメッセージのテキストを作成できます。イベントの説明を示す情報フィールドを含めることができます。既定では、既定のメッセージがユーザーへの通知に使用されます。

# 管理者およびユーザーへの通知の設定

イベント通知の設定で、メッセージテキストの設定方法と作成方法を選択できます。

**Kaspersky Security Center 管理コンソールでイベント通知を設定する方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ログと通知**］を選択します。
4. ［**実行ログ**］セクションで、［**設定**］をクリックします。

   ［**通知**］ウィンドウが表示されます。
5. 通知方法を選択するイベントを選択して、［**通知の設定**］をクリックします。

   ［**通知の設定**］ウィンドウが表示されます。
6. メールで通知する場合は、［**メール**］タブで、イベント通知メッセージのテキストを追加できます。

   イベントの情報が含まれるフィールドを追加するには、［**変数**］をクリックしてドロップダウンリストから該当するフィールドを選択します。イベントの情報が含まれるフィールドについては、このセクションの表に示しています。

   イベントメッセージの既定のテキストを復元するには、［**既定**］をクリックします。
7. 実行ファイルを実行して通知する場合は、［**実行ファイル**］タブで、保護対象デバイスのローカルドライブ上のファイルを選択するか、そのファイルへの完全パスを入力します。このファイルは、イベントの発生時に保護対象デバイス上で実行されます。ファイルを実行するために使用する、ユーザー名とパスワードを入力します。

   実行ファイルのパスを指定する時にシステム環境変数を使用できます。ユーザー環境変数は使用できません。
8. ターミナルサービスを使用して通知する場合は、［**ターミナルサービス**］タブで、イベント通知メッセージのテキストを追加できます。

   イベントの情報が含まれるフィールドを追加するには、［**変数**］をクリックしてドロップダウンリストから該当するフィールドを選択します。イベントの情報が含まれるフィールドについては、このセクションの表に示しています。

   イベントメッセージの既定のテキストを復元するには、［**既定**］をクリックします。
9. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでイベント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（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ログと通知**］→［**実行ログ**］に移動し、［**設定**］をクリックします。
5. 表示されたウィンドウで、通知方法を選択するイベントをクリックします。
   ［**通知設定**］ウィンドウが表示されます。
6. メールで通知する場合は、［**ユーザーへの通知**］セクションで、［**メールを送信**］をオンにして、イベント通知メッセージのテキストを追加します。
   イベントの情報が含まれるフィールドを追加するには、［**変数を追加する**］をクリックしてリストから該当する項目を選択します。イベントの情報が含まれるフィールドについては、このセクションの表に示しています。
   イベントメッセージの既定のテキストを復元するには、［**リセット**］をクリックします。
7. 実行ファイルを実行して通知する場合は、［**管理者への通知**］セクションで、［**実行ファイルを実行**］をオンにして、保護対象デバイスのローカルドライブ上のファイルへの完全パスを入力します。このファイルは、イベントの発生時に保護対象デバイス上で実行されます。ファイルを実行するために使用する、ユーザー名とパスワードを入力します。
   実行ファイルのパスを指定する時にシステム環境変数を使用できます。ユーザー環境変数は使用できません。
8. ターミナルサービスを使用して通知する場合は、［**管理者への通知**］セクションで、［**ターミナルサービスを使用**］をオンにして、イベント通知メッセージのテキストを追加します。
   イベントの情報が含まれるフィールドを追加するには、［**変数を追加する**］をクリックしてリストから該当する項目を選択します。イベントの情報が含まれるフィールドについては、このセクションの表に示しています。
   イベントメッセージの既定のテキストを復元するには、［**リセット**］をクリックします。
9. 変更内容を保存します。

### *アプリケーションコンソールでイベント通知を設定する方法*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーのコンテキストメニューを開きます。
2. ［**プロパティ**］を選択します。
   ［**通知**］ウィンドウが表示されます。
3. 通知方法を選択するイベントを選択して、［**通知の設定**］をクリックします。
   ［**通知の設定**］ウィンドウが表示されます。

4. メールで通知する場合は、［**メール**］タブで、イベント通知メッセージのテキストを追加できます。

   イベントの情報が含まれるフィールドを追加するには、［**変数**］をクリックしてドロップダウンリストから該当するフィールドを選択します。イベントの情報が含まれるフィールドについては、このセクションの表に示しています。

   イベントメッセージの既定のテキストを復元するには、［**既定**］をクリックします。

5. 実行ファイルを実行して通知する場合は、［**実行ファイル**］タブで、保護対象デバイスのローカルドライブ上のファイルを選択するか、そのファイルへの完全パスを入力します。このファイルは、イベントの発生時に保護対象デバイス上で実行されます。ファイルを実行するために使用する、ユーザー名とパスワードを入力します。

   実行ファイルのパスを指定する時にシステム環境変数を使用できます。ユーザー環境変数は使用できません。

6. ターミナルサービスを使用して通知する場合は、［**ターミナルサービス**］タブで、イベント通知メッセージのテキストを追加できます。

   イベントの情報が含まれるフィールドを追加するには、［**変数**］をクリックしてドロップダウンリストから該当するフィールドを選択します。イベントの情報が含まれるフィールドについては、このセクションの表に示しています。

   イベントメッセージの既定のテキストを復元するには、［**既定**］をクリックします。

7. 変更内容を保存します。

イベントの情報が含まれるフィールド

| 変数 | 説明 |
|---|---|
| %EVENT_TYPE% | イベントの種別。 |
| %EVENT_TIME% | イベントの時刻。 |
| %EVENT_SEVERITY% | 重要度 |
| %OBJECT% | オブジェクト名（コンピューターのリアルタイム保護タスクとオンデマンドスキャンタスク）。<br>ソフトウェアモジュールのアップデートタスクには、アップデートの名前、Web ページのアドレス、アップデートに関する情報が含まれます。 |
| %VIRUS_NAME% | ウイルス百科事典の分類に基づいたオブジェクトの名前。この名前は、オブジェクトの検知時に Kaspersky Embedded Systems Security によって返される、検知されたオブジェクトの完全な名前に含まれます。実行ログで、検知されたオブジェクトの名前を表示できます。 |
| %VIRUS_TYPE% | 「ウイルス」「トロイの木馬」など、カスペルスキーの分類に基づいた、検知されたオブジェクトの種別。この種別は、オブジェクトが感染しているまたは感染の可能性があることが検知されると Kaspersky Embedded Systems Security によって返される、検知されたオブジェクトの名前に含まれます。タスク実行ログで、検知されたオブジェクトの名前を表示できます。 |
| %USER_COMPUTER% | ファイルのリアルタイム保護タスクと RPC ネットワークストレージの保護タスクでは、デバイス上のオブジェクトにアクセスしたユーザーの保護対象デバイスの名前です。 |
| %USER_NAME% | ファイルのリアルタイム保護タスクと RPC ネットワークストレージの保護タスクでは、デバイス上のオブジェクトにアクセスしたユーザーの名前です。 |
| %FROM_COMPUTER% | 通知が発行された保護対象デバイスの名前。 |
| %EVENT_REASON% | イベントが発生した理由（このフィールドがないイベントもあります）。 |
| %ERROR_CODE% | エラーコード（「内部タスクエラー」イベントでのみ使用）。 |
| %TASK_NAME% | タスク名（タスク実行に関連するイベントのみ）。 |
| %PROTOCOL% | 使用されているプロトコル。 |
| %MESSAGE% | メッセージの本文 |
| %DEVICE_INSTANCEPATH% | デバイスのインスタンスへのパス。 |
| %DEVICE_VID% | デバイスの製造元 ID。 |

| 変数 | 説明 |
| --- | --- |
| %DEVICE_PID% | コントローラーの種別 |
| %DEVICE_SERIALNUMBER% | デバイスのシリアル番号 |

# メール通知の設定

### Kaspersky Security Center 管理コンソールでメール通知を設定する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ポリシーのプロパティウィンドウで、［**ログと通知**］を選択します。
4. ［**実行ログ**］セクションで、［**設定**］をクリックします。
   ［**通知**］ウィンドウが表示されます。
5. ［**メール通知の設定**］をクリックします。
6. 表示されたウィンドウで、［**イベント通知を送信する**］をオンにします。
7. ［**送信元アカウント**］で、送信者の情報（送信者のアドレス、SMTP サーバー、SMTP サーバーポート、ユーザー名とパスワード）を指定します。
8. ［**通知の受信者**］で、受信者のメールアドレスを指定します。
9. 送信方法を指定します（［**イベントの発生時**］または［**スケジュールで指定**］）。スケジュールを設定するには、［**編集**］をクリックします。
10. 変更内容を保存します。

### Kaspersky Security Center Web コンソールでメール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（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ログと通知**］→［**実行ログ**］に移動し、［**設定**］をクリックします。
5. ウィンドウが表示されるので、そのウィンドウで［**メール通知の設定**］タブを選択します。
6. ［**イベント通知を送信する**］チェックボックスをオンにします。

7. 送信者の情報（送信者のアドレス、SMTP サーバー、SMTP サーバーポート、ユーザー名とパスワード）を指定します。
8. 受信者のメールアドレスを指定します。
9. 送信方法を指定します（[**イベントの発生時**] または [**スケジュールで指定**]）。適用可能な場合はスケジュールを設定します。
10. 変更内容を保存します。

***アプリケーションコンソールでメール通知を設定する方法***

1. アプリケーションコンソールツリーで、[**ログと通知**] フォルダーのコンテキストメニューを開きます。
2. [**プロパティ**] を選択します。
   [**通知**] ウィンドウが表示されます。
3. [**メール通知の設定**] をクリックします。
4. 表示されたウィンドウで、[**イベント通知を送信する**] をオンにします。
5. [**送信元アカウント**] で、送信者の情報（送信者のアドレス、SMTP サーバー、SMTP サーバーポート、ユーザー名とパスワード）を指定します。
6. [**通知の受信者**] で、受信者のメールアドレスを指定します。
7. 送信方法を指定します（[**イベントの発生時**] または [**スケジュールで指定**]）。スケジュールを設定するには、[**編集**] をクリックします。
8. 変更内容を保存します。

# 管理サーバーとのインタラクションの設定

Kaspersky Embedded Systems Security が Kaspersky Security Center 管理サーバーに情報を送信するオブジェクトの種別を選択する必要があります。

***Kaspersky Security Center 管理コンソールで管理サーバーとのインタラクションを設定する方法***

1. Kaspersky Security Center 管理コンソールツリーで、[**ポリシー**] フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. [**ログと通知**] セクションで、[**管理サーバーとの対話**] サブセクションの [**設定**] をクリックします。

4. 表示されたウィンドウで、Kaspersky Embedded Systems Security が Kaspersky Security Center 管理サーバーに情報を送信するオブジェクトの種別を選択します：
   - **バックアップ内のファイルの情報**
   - **未処理のファイルの情報**
   - **インストールされたデバイスの情報**
   - **脅威の活動連鎖の情報**
5. 変更内容を保存します。
   選択した種別のオブジェクトに関する情報が管理サーバーに送信されます。

**Kaspersky Security Center Web コンソールで管理サーバーとのインタラクションを設定する方法**

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**ログと通知**］セクションで、［**管理サーバーとの対話**］サブセクションの［**設定**］をクリックします。
5. 表示されたウィンドウで、Kaspersky Embedded Systems Security が Kaspersky Security Center 管理サーバーに情報を送信するオブジェクトの種別を選択します：
   - **バックアップされたファイル**
   - **未処理のファイルの情報**
   - **ブロック対象のネットワークセッション**
   - **デバイスと Wi-Fi ネットワーク**
6. 変更内容を保存します。

# Managed Detection and Response

Kaspersky Embedded Systems Security は、Managed Detection and Response ソリューションとの連携をサポートしています。

Kaspersky Managed Detection and Response（MDR とも呼ばれます）は、専門知識や人材の確保に悩む組織、あるいは社内のリソースが限られている組織に対し、自動化されたセキュリティ障壁を迂回する脅威の増加から 24 時間体制で保護を提供します。市場にある類似サービスとは異なり、本サービスは効果的な標的型攻撃の調査の実績を基盤としており、最も複雑な脅威に対しても確実に継続的な防御を提供します。本サービスは、サイバー脅威に対する企業の対応力を強化すると同時に、既存リソースを解放し、他の業務に注力できるよう支援します。

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。

# MDR 連携設定

Kaspersky Managed Detection and Response を使用するには、Kaspersky Security Network コンポーネントの拡張モードを有効にする必要があります。そうしないと、Kaspersky Managed Detection and Response が正常に動作するために必要なテレメトリデータを受け取ることができません。

Kaspersky Security Center 13 Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、 新しい保護された接続であるバックグラウンド接続を確立する必要があります。Kaspersky Security Center Web コンソールを経由した管理サーバーと Kaspersky Managed Detection and Response が連携するためには、 新しい保護された接続であるバックグラウンド接続を確立する必要があります。ソリューションを配備する際に Kaspersky Managed Detection and Response はバックグラウンド接続を確立するよう求めます。バックグラウンド接続が確立されていることを確認してください。

**Kaspersky Security Center Web コンソールとのバックグラウンド接続を確立する**

1. Web コンソールのメインウィンドウで、［**設定**］→［**連携**］の順に選択します。
2. ［**連携**］に移動します。
3. ［**連携用のバックグラウンド接続が［有効］です**］をオンにします。
4. 変更内容を保存します。

Kaspersky Managed Detection and Response とは次の手順で連携されます：

1. **Managed Detection and Response コンポーネントのインストール**

   Kaspersky Embedded Systems Security と Managed Detection and Response ソリューションの連携には、Managed Detection and Response コンポーネントを使用します。このコンポーネントをインストールするには、インストールパッケージの設定内、セットアップウィザード、または Windows のコントロールパネルのアプリケーションコンポーネントのセットの変更で、コンポーネントの選択手順で［**Managed Detection and Response**］を選択します。

### 2 Kaspersky Private Security Network の設定

2025 年 7 月のアップデートから、Managed Detection and Response ソリューションは KPSN ファイルなしでの操作をサポートするようになりました。MDR ソリューションがどのように Kaspersky Security Network を使用するかに関して詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

構成が KPSN 設定ファイルなしでの実行の要件に一致しない場合は、管理サーバーのプロパティで KPSN 設定ファイルをアップロードしてください。KPSN 設定ファイルは MDR 設定ファイルの ZIP アーカイブ内に保存されています。**コマンドラインを使用して KPSN 証明書をアップロード**することもできます。

1. デバイス上で、ローカル管理者の権限でコマンドラインインタープリター（例: cmd.exe）を実行します。
2. `cd` コマンドを使用して、ファイル kavshell.exe があるフォルダーに移動します。

   例：`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0` を入力してから **ENTER** を押します。

   アプリケーションのインストールの段階で、システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。
3. 次のコマンドを実行します：

   `KAVSHELL KSN [/global] [/private <プライベート KSN 設定ファイルの完全パス>] [/login=<現在のユーザーアカウントの名前>] [/pwd=</login のパスワードまたは /login が指定されていない場合は KLAdmin パスワード>]`

   例：

   `KAVSHELL KSN /private C:\kpsn_config.pkcs7`

Kaspersky Private Security Network の設定の詳細に関しては、Kaspersky Security Center ヘルプを参照してください。

### 3 Kaspersky Managed Detection and Response をアクティベートする

Kaspersky Embedded Systems Security で Managed Detection and Response ソリューションをアクティベートするには、 Kaspersky Managed Detection and Response for Embedded Systems Security のアドオン用の別のライセンスが必要です。ソリューションのアクティベートについて詳しくは、Kaspersky Managed Detection and Response のヘルプを参照してください。

Kaspersky Embedded Systems Security は MDR 設定ファイル（BLOB ファイル）をサポートしません。すべての資産はルートのテナントに配置されます。

### 4 Managed Detection and Response コンポーネントを有効にする

**Kaspersky Security Center 管理コンソールで Managed Detection and Response を有効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**ポリシー**］フォルダーを選択します。
2. 目的のポリシーを選択し、ダブルクリックしてポリシーのプロパティを表示します。
3. ［**テレメトリ収集サーバー**］セクションを選択します。
4. ［**Managed Detection and Response**］ブロックの［**設定**］をクリックします。

   ［**Managed Detection and Response**］ウィンドウが表示されます。

5. ［**Managed Detection and Response**］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。

**Kaspersky Security Center Web コンソールで Managed Detection and Response 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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。

2. Kaspersky Embedded Systems 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. ［**テレメトリ収集サーバー**］セクションを選択します。

5. ［**Managed Detection and Response**］ブロックの［**設定**］をクリックします。
   ［**Managed Detection and Response**］ウィンドウが表示されます。

6. ［**Managed Detection and Response は無効です**］チェックボックスをオンにします。

7. 変更内容を保存します。

**アプリケーションコンソールで Managed Detection and Response を有効にする方法**

1. コンソールツリーで、［**テレメトリ収集サーバー**］→［**Managed Detection and Response**］セクションを選択します。

2. 結果ペインで［**プロパティ**］をクリックします。
   ［**Managed Detection and Response**］ウィンドウが開き、［**全般**］タブが表示されます。

3. ［**Managed Detection and Response**］チェックボックスをオンにします。

4. 変更内容を保存します。

**コマンドラインから Managed Detection and Response コンポーネントを有効にする方法**

1. デバイス上で、ローカル管理者の権限でコマンドラインインタープリター（例: cmd.exe）を実行します。

2. `cd` コマンドを使用して、ファイル kavshell.exe があるフォルダーに移動します。
   例：`cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.1.0` を入力してから **ENTER** を押します。
   アプリケーションのインストールの段階で、システム変数 %PATH% に実行ファイルのパスを追加し、アプリケーションフォルダーに移動せずにコマンドを実行することもできます。

3. 次のコマンドを実行します：

KAVSHELL MDR /<enable|disable|show> [/login:<現在のユーザーアカウントの名前>] [/pwd:</login のパスワードまたは /login が指定されていない場合は KLAdmin パスワード>]

Managed Detection and Response を有効にするためのコマンドパラメータ

| パラメータ | 説明 |
| --- | --- |
| MDR /<enable\|disable\|show> | 必須の引数です。<br>Managed Detection and Response の有効化、無効化、ステータスの表示を許可します。 |
| /LOGIN=<ユーザーアカウント名> | 省略可能な引数です。<br>十分な権限を持つユーザーアカウント名を指定することができます。<br>このオプションが指定されていない場合、次の行でユーザー名の入力が促されます。<br>KLAdmin パスワードを入力した場合はこの値を入力する必要はありません。 |
| /PWD=</login のパスワードまたは /login が指定されていない場合は KLAdmin パスワード> | KLAdmin ユーザーアカウントまたは十分な権限を持つユーザーアカウントのパスワードを指定することができます。<br>このオプションが指定されていない場合、次の行でパスワードの入力が促されます。 |

# テクニカルサポートへのお問い合わせ

このセクションでは、テクニカルサポートを受ける方法と利用条件について説明します。

## テクニカルサポートの利用方法

製品のドキュメントやその他の Kaspersky Embedded Systems Security の情報源で問題の解決法が見つからない場合、テクニカルサポートに問い合わせてください。テクニカルサポート担当者が、Kaspersky Embedded Systems Security のインストール方法や使用方法についてのお問い合わせに回答いたします。

サポート対象期間中、カスペルスキーは Kaspersky Embedded Systems Security のサポートを提供します（製品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の Web サイトにアクセスする
- カスペルスキーカンパニーアカウントポータルからカスペルスキーのテクニカルサポートに要求を送信する

## カスペルスキーカンパニーアカウントからの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ご利用の法人向けのポータルです。カスペルスキーカンパニーアカウントによって、ユーザーとカスペルスキーの担当者が、オンライン依頼によってスムーズにやり取りできます。カスペルスキーカンパニーアカウントによって、カスペルスキーの担当者によるオンライン依頼の処理の進捗を監視したり、オンライン依頼の履歴を保存したりすることができます。

カスペルスキーカンパニーアカウントの1つのユーザーアカウントで、組織のすべての従業員を登録できます。カスペルスキーカンパニーアカウントを使えば、1つのアカウントで、登録した従業員からカスペルスキーへのオンライン依頼や、これらの従業員の権限を一元的に管理できます。

カスペルスキーカンパニーアカウントは、次の言語で使用できます：

- 英語
- スペイン語
- イタリア語
- ドイツ語
- ポーランド語

- ポルトガル語
- ロシア語
- フランス語
- 日本語

カスペルスキーカンパニーアカウントの詳細については、テクニカルサポートサイトを参照してください。

# テクニカルサポートの担当者への詳細な診断情報の提供

製品の問題に対するより効果的なサポートとトラブルシューティングを行うために、テクニカルサポートの担当者は、診断中にデバッグを行う目的で、製品設定を一時的に変更するよう依頼する場合があります。そのため、次の操作が必要になる場合があります：

- 詳細な診断情報を処理および保存する機能の有効化
- 標準のユーザーインターフェイス要素からは指定できない個々のソフトウェアコンポーネントの設定の微調整
- 処理された診断情報の保存と送信の設定の変更
- ネットワークトラフィックの取得およびログの設定

リストされた処理を実行するために必要なすべての情報（手順のシーケンスの説明、変更可能な設定、設定情報ファイル、スクリプト、追加のコマンドライン機能、デバッグモジュール、特殊なユーティリティなど）、およびデバッグの目的で分析されたデータの構成は、テクニカルサポートの担当者が案内します。取得された詳細な診断情報は、クライアントコンピューターに保存されます。保存されたデータのカスペルスキーへの自動転送は実行されません。

テクニカルサポートの担当者に問題を報告した後に、担当者から Kaspersky Embedded Systems Security の操作に関する情報が含まれるレポートの生成と送信をお願いする場合があります。カスペルスキーのテクニカルサポートの担当者は、トレースファイルの作成とメモリダンプファイルの送信を依頼する場合もあります。

テクニカルサポートの担当者は、送信されたデータを分析し、AVZ スクリプトを作成してユーザーに送信できます。AVZ スクリプトによって、脅威のアクティブなプロセスの分析、コンピューターの脅威のスキャン、感染したファイルの駆除や削除、システムスキャンレポートの作成を行うことができます。

上記の処理は、テクニカルサポートの担当者の指導の下で、指示を受ける場合にのみ実行できます。製品ドキュメントやテクニカルサポートの担当者の推奨事項に記載されていない方法で製品設定を単独で変更すると、オペレーティングシステムの速度低下や誤動作、コンピューターの保護レベルの低下、処理された情報の使用可能性と整合性の侵害につながる可能性があります。

# アプリケーションの動作のトレース

*アプリケーションのトレース*とは、製品が実行する処理の詳細な記録と製品の動作中に発生したイベントに関するメッセージです。トレースプロセス中に、本製品は様々なアプリケーションコンポーネントの操作に関するデータが含まれるファイルセットを作成します。

トレースファイルを使用して、アプリケーションコマンドの実行プロセスを段階的に追跡し、エラーが発生した製品動作の段階を特定することができます。

トレースファイルは、本製品の使用中にコンピューターに保存されます。本製品が削除されると、トレースファイルは完全に削除されます。手動でトレースファイルを削除することもできます。手動でファイルを削除するには、トレースを無効にして本製品を停止する必要があります。

保存されたトレースファイルには、機密情報が含まれる可能性があります。データへのアクセスを制御するには、トレースファイルのセキュリティを個別に確保する必要があります。

既定では、認証エージェントのトレースファイルを除くトレースファイルは %ProgramData%\Kaspersky Lab\KESS.4.0\Traces のフォルダーに保存されます。

トレースファイルの命名規則は次となります：「KESS<4.0_dateXX.XX_timeXX.XX_pidXXX.><トレースファイルの種別>.log」。

**トレースファイルに保存されたデータを確認できます。**

**すべてのトレースファイルには、次の共通データが含まれます：**

- **イベントの日時**
- **実行された脅威の数**

  **認証エージェントのトレースファイルには、この情報は含まれません。**

- **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**

**Kaspersky Embedded Systems Security は、ユーザーパスワードについて、暗号化したかたちでのみトレースファイルに保存します。**

## Kaspersky Security Center 管理コンソールでアプリケーショントレースを有効にして設定する方法

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**ポリシー**］タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. ポリシーのプロパティウィンドウで、［**誤動作診断**］をクリックします。
6. ［**トラブルシューティング設定**］ブロックの［**設定**］をクリックします。
   ［**トラブルシューティング設定**］ウィンドウが開き、［**アプリケーショントレースの設定**］タブが表示されます。
7. ［**トレースを有効にする**］チェックボックスをオンにします。
8. 必要に応じて、［**トレースファイル用フォルダー**］フィールドに、Kaspersky Embedded Systems Security がトレースファイルを保存するローカルフォルダーへの完全パスを指定します。

   > フォルダーは事前に作成し、SYSTEM アカウントで書き込み可能にする必要があります。ネットワークフォルダー、ドライブ、環境変数は指定できません。

9. ［**詳細レベル**］ドロップダウンリストから、デバッグ情報の詳細レベルを選択します：
   - **緊急**：トレースファイルには、深刻なエラーに関するメッセージのみが保存されます。
   - **診断**：トレースファイルには、すべてのエラーと警告に関するメッセージが保存されます。
   - **重要**：トレースファイルには、すべてのエラー、警告、および追加情報に関するメッセージが保存されます。
   - **通常**：トレースファイルには、すべてのエラー、警告、および本製品の通常の処理に関する情報に関するメッセージが保存されます（既定）。
   - **詳細**：トレースファイルには、本製品の処理に関するすべての情報が保存されます。

   発生した問題を解決するために必要な詳細レベルは、テクニカルサポートが判断します。
10. 既定の詳細レベルは、［**通常**］に設定されています。
11. **トレースファイルの最大サイズ（MB）**を指定します。
    使用可能な値：1 ～ 4095 MB。既定では、トレースファイルの最大サイズは 100 MB に設定されています。
12. ファイルの最大数に達した時に古いトレースファイルを削除するには、［**古いトレースファイルを削除する**］をオンにします。

13. **トレースログあたりの最大ファイル数**を指定します。

    使用可能な値：1 ～ 999。既定では、ファイルの最大数は 5 に設定されています。このフィールドは、［**古いトレースファイルを削除する**］をオンにした場合に使用できます。

14. 変更内容を保存します。

15. Kaspersky Embedded Systems Security の再起動

*アプリケーションのトレースを停止するには：*

ポリシーのプロパティの［**トラブルシューティング設定**］ウィンドウの［**アプリケーショントレースの設定**］タブで、［**トレースを有効にする**］をオフにします。

*アプリケーションコンソールでアプリケーショントレースを有効にして設定する方法*

1. アプリケーションコンソールツリーで、［Kaspersky Embedded Systems Security］フォルダーを選択して、次のいずれかを行います：

   - フォルダーの結果ペインで、［**アプリケーションのプロパティ**］をクリックします。
   - フォルダーのコンテキストメニューで［**アプリケーションのプロパティ**］を選択します。

   ［**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。

2. ［**誤動作診断**］タブを選択します。

3. ［**トラブルシューティング設定**］ブロックの［**設定**］をクリックします。
   ［**トラブルシューティング設定**］ウィンドウが表示されます。

4. トレースの設定タブを選択します。

   - **アプリケーショントレースの設定**：Kaspersky Embedded Systems Security がアプリケーションのトレースを開始します。
   - **アプリケーションコンソールのトレースの設定**：アプリケーションコンソールと Kaspersky Embedded Systems Security が異なるコンピューターにインストールされている場合は、アプリケーションコンソールのトレースのみを開始できます。

5. ［**トレースを有効にする**］チェックボックスをオンにします。
   ［**トレースファイル用フォルダー**］フィールドには、Kaspersky Embedded Systems Security が既定でトレースファイルを保存するローカルフォルダーへの完全パスが含まれます。別のパスを指定することもできます。

6. ［**詳細レベル**］ドロップダウンリストから、デバッグ情報の詳細レベルを選択します：

   - **緊急**：トレースファイルには、深刻なエラーに関するメッセージのみが保存されます。
   - **診断**：トレースファイルには、すべてのエラーと警告に関するメッセージが保存されます。
   - **重要**：トレースファイルには、すべてのエラー、警告、および追加情報に関するメッセージが保存されます。

- **通常**：トレースファイルには、すべてのエラー、警告、および本製品の通常の処理に関する情報に関するメッセージが保存されます（既定）。
- **詳細**：トレースファイルには、本製品の処理に関するすべての情報が保存されます。

発生した問題を解決するために必要な詳細レベルは、テクニカルサポートが判断します。

既定の詳細レベルは、［**通常**］に設定されています。

7. **トレースファイルの最大サイズ（MB）**を指定します。

   使用可能な値：1 ～ 4095 MB。既定では、トレースファイルの最大サイズは 100 MB に設定されています。

8. ファイルの最大数に達した時に古いトレースファイルを削除するには、［**古いトレースファイルを削除する**］をオンにします。

9. **トレースログあたりの最大ファイル数**を指定します。

   使用可能な値：1 ～ 999。既定では、ファイルの最大数は 5 に設定されています。このフィールドは、［**古いトレースファイルを削除する**］をオンにした場合に使用できます。

10. 変更内容を保存します。

11. Kaspersky Embedded Systems Security の再起動

*アプリケーションのトレースを停止するには：*

アプリケーションのプロパティの［**トラブルシューティング設定**］ウィンドウの［**アプリケーショントレースの設定**］タブで、［**トレースを有効にする**］をオフにします。

### Kaspersky Security Center Web コンソールでアプリケーショントレースを有効にして設定する方法

1. Web コンソールのメインウィンドウで、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**誤動作診断**］セクションを選択します。
5. ［**トラブルシューティング設定**］ブロックで、［**アプリケーショントレースを有効にする**］をオンにします。
6. 必要に応じて、Kaspersky Embedded Systems Security がトレースファイルを保存するローカルフォルダーへの完全パスを指定します。

   > フォルダーは事前に作成し、SYSTEM アカウントで書き込み可能にする必要があります。ネットワークフォルダー、ドライブ、環境変数は指定できません。

7. ［**レベル**］ドロップダウンリストから、デバッグ情報の詳細レベルを選択します。

8. **トレースファイルの最大サイズ（MB）**を指定します。

   使用可能な値：1 ～ 4095 MB。既定では、トレースファイルの最大サイズは 100 MB に設定されています。

9. ファイルの最大数に達した時に古いトレースファイルを削除するには、［**古いトレースファイルを削除する**］をオンにします。

10. **トレースログあたりの最大ファイル数**を指定します。

    使用可能な値：1 ～ 999。既定では、ファイルの最大数は 5 に設定されています。このフィールドは、［**古いトレースファイルを削除する**］をオンにした場合に使用できます。

11. 変更内容を保存します。

12. Kaspersky Embedded Systems Security の再起動

*アプリケーションのトレースを停止するには：*

設定しているポリシーのプロパティの［**誤動作診断**］セクションで、［**アプリケーショントレースを有効にする**］をオフにします。

コンパクト診断インターフェイスでアプリケーショントレースを有効にして設定する方法

*コマンドラインを使用してアプリケーショントレースを有効にして設定する方法*

1. 管理者としてコマンドラインインタープリタ（cmd.exe）を実行します。

2. cd コマンドを使用して、ファイル klpsm.exe があるフォルダーに移動します。

   例：cd C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems Security.4.0.0

3. 次のコマンドを実行します：

   KAVSHELL TRACE /ON|/OFF /F:<トレースファイルを保存するフォルダー> [/LVL:debug|info|warning|error|critical] [/S:<トレースファイルの最大サイズ（メガバイト単位）>] [/R:<トレースファイルの最大数（この数を超えると新しいファイルに置き換えられます）>]

# メモリダンプの記録

メモリダンプファイルには、アプリケーションのエラーが発生した時点で Kaspersky Embedded Systems Security のプロセスが作業していたメモリについてのすべての情報が含まれます。

メモリダンプファイルは、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。

保存されたダンプファイルには、機密情報が含まれる可能性があります。データへのアクセスを制御するには、メモリダンプファイルのセキュリティを個別に確保する必要があります。

既定では、メモリダンプファイルは %ProgramData%¥Kaspersky Lab¥KESS.4.0¥Traces のフォルダーに保存されます。

**Kaspersky Security Center 管理コンソールでメモリダンプの記録を有効または無効にする方法**

1. Kaspersky Security Center 管理コンソールツリーで、［**管理対象デバイス**］フォルダーを展開します。
2. タスクを設定する管理グループを選択します。
3. ［**ポリシー**］タブを選択します。
4. 設定するポリシー名をダブルクリックします。
5. ポリシーのプロパティウィンドウで、［**誤動作診断**］をクリックします。
6. ［**トラブルシューティング設定**］ブロックの［**設定**］をクリックします。
   ［**トラブルシューティング設定**］ウィンドウが開き、［**アプリケーショントレースの設定**］タブが表示されます。
7. ［**アプリケーションダンプの設定**］タブを選択します。
8. ［**ダンプファイルの作成**］をオンまたはオフにして、誤動作が発生した場合のメモリダンプを有効または無効にします。
9. 必要に応じて、［**ダンプファイル用フォルダー**］フィールドに、Kaspersky Embedded Systems Security がメモリダンプファイルを保存するローカルフォルダーへの完全パスを入力します。

   フォルダーは事前に作成し、SYSTEM アカウントで書き込み可能にする必要があります。ネットワークフォルダー、ドライブ、環境変数は指定できません。

10. 変更内容を保存します。

*アプリケーションコンソールでメモリダンプの記録を有効または無効にする方法*

1. アプリケーションコンソールツリーで、［Kaspersky Embedded Systems Security］フォルダーを選択して、次のいずれかを行います：
   - フォルダーの結果ペインで、［**アプリケーションのプロパティ**］をクリックします。
   - フォルダーのコンテキストメニューで［**アプリケーションのプロパティ**］を選択します。

   ［**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。
2. ［**誤動作診断**］タブを選択します。
3. ［**トラブルシューティング設定**］ブロックの［**設定**］をクリックします。
   ［**トラブルシューティング設定**］ウィンドウが表示されます。

4. ダンプの設定タブを選択します。

   - **アプリケーションダンプの設定**：Kaspersky Embedded Systems Security は、アプリケーションのすべてのダンプを記録します。
   - **アプリケーションコンソールのダンプの設定**：アプリケーションコンソールと Kaspersky Embedded Systems Security が異なるコンピューターにインストールされている場合は、アプリケーションコンソールのダンプのみを記録できます。

5. ［**ダンプファイルの作成**］をオンまたはオフにして、誤動作が発生した場合のメモリダンプを有効または無効にします。

   既定では、メモリダンプファイルは %ProgramData%¥Kaspersky Lab¥KESS.4.0¥Traces のフォルダーに保存されます。別のパスを指定することもできます。

6. 変更内容を保存します。

**Kaspersky Security Center Web コンソールでメモリダンプの記録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、［**アセット（デバイス）**］→［**ポリシーとプロファイル**］の順に選択します。
2. Kaspersky Embedded Systems 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. ［**誤動作診断**］セクションを選択します。
5. ［**ダンプファイル設定**］で、［**ダンプファイルの作成**］をオンまたはオフにして、誤動作が発生した場合のメモリダンプを有効または無効にします。
6. 必要に応じて、Kaspersky Embedded Systems Security がメモリダンプファイルを保存するローカルフォルダーへの完全パスを指定します。

   > フォルダーは事前に作成し、SYSTEM アカウントで書き込み可能にする必要があります。ネットワークフォルダー、ドライブ、環境変数は指定できません。

7. 変更内容を保存します。

コンパクト診断インターフェイスでメモリダンプの記録を有効または無効にすることもできます。

# Kaspersky Embedded Systems Security に関する情報源

Kaspersky Embedded Systems Security についての情報は、次の場所から入手できます：

- カスペルスキーの Web サイトの Kaspersky Embedded Systems Security のページ
- テクニカルサポートサイト（ナレッジベース） - Kaspersky Embedded Systems Security のページ
- オンラインヘルプ
- フォーラムで本製品について議論する

問題の解決策が見つからない場合は、カスペルスキーのテクニカルサポートにお問い合わせください。

オンラインの情報源を使用するには、インターネット接続が必要です。

## カスペルスキーの Web サイトの Kaspersky Embedded Systems Security のページ

カスペルスキーの Web サイトの Kaspersky Embedded Systems Security のページで、本製品とその機能に関する全般的な情報を参照できます。

Kaspersky Embedded Systems Security のページにはオンラインストアへのリンクがあります。［お問い合わせ］ボタンをクリックし、表示されるフォームにご記入の上送信してください。

## ナレッジベースの Kaspersky Embedded Systems Security のページ

ナレッジベースは、テクニカルサポートサイトにあるセクションです。

ナレッジベースの Kaspersky Embedded Systems Security のページには、製品の購入、インストール、使用の方法に関する便利な情報、推奨事項、および FAQ への回答が掲載されています。

ナレッジベースの記事では、Kaspersky Embedded Systems Security だけでなく、その他のカスペルスキー製品に関する質問への回答も参照できます。また、テクニカルサポートニュースも含まれます。

## Kaspersky Embedded Systems Security のオンラインヘルプ

オンライン ヘルプには、Kaspersky Embedded Systems Security の設定と使用に関する情報が記載されています。

# フォーラムで本製品について議論する

特に緊急の対応が必要ではない場合は、カスペルスキー製品のフォーラムをご利用ください。ここでは、カスペルスキーのエキスパートやカスペルスキー製品のユーザーが、さまざまなトピックで意見交換しています。

このフォーラムでは、これまでに公開されたトピックの閲覧、コメントの書き込み、新しいトピックの作成が可能です。

# 用語解説

## Kaspersky Security Network（KSN）

ファイル、Web リソース、ソフトウェアの評判に関する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インフラストラクチャ。Kaspersky Security Networkのデータを使用することで、カスペルスキー製品による脅威への対応がより高速化され、一部の保護コンポーネントのパフォーマンスが向上し、誤検知の発生率が下がります。

## OLE オブジェクト

Object Linking and Embedding（OLE）技術を使用して別のファイルに添付されたオブジェクト、または別のファイルに埋め込まれたオブジェクト。OLE 埋め込みオブジェクトの例として、Microsoft Office Word ドキュメントに埋め込まれた Microsoft Office Excel® スプレッドシートが挙げられます。

## SIEM

Security Information and Event Management（セキュリティ情報イベント管理） の略称。組織のセキュリティシステム内の情報とイベントを管理するソリューション。

## アーカイブ

1 つの圧縮ファイルにまとめられた 1 つまたは複数のファイル。データの圧縮および回答には、アーカイバと呼ばれる専用のアプリケーションが必要です。

## アップデート

カスペルスキーのアップデートサーバーから取得した新しいファイル（定義データベースまたはソフトウェアモジュール）を差し替えまたは追加する処理。

## イベントの重要性

カスペルスキー製品の動作中に発生したイベントのプロパティ。4 つの重要度があります：

- 緊急イベント
- 機能エラー
- 警告
- 情報メッセージ

イベントの発生状況に応じて、同じ種別のイベントが異なる重要度になることがあります。

## 隔離

カスペルスキー製品が感染の可能性があるオブジェクトを検知した時に、そのオブジェクトの移動先となるフォルダー。コンピューターへの影響を防ぐために、オブジェクトは隔離に暗号化された形式で保存されます。

## 感染したオブジェクト

コードのセクションが既知の脅威のコードのセクションと完全に一致するオブジェクト。カスペルスキーのエキスパートは、このようなオブジェクトの操作を推奨していません。

## 感染の可能性があるファイル

ファイルの構造または形式により、侵入者が悪意のあるコードを保存して拡散させるための「入れ物」として使用できるファイル。一般的には、com、exe、dll などの拡張子を持つ実行ファイルです。このようなファイルには、悪意のあるコードが含まれるリスクが非常に高いです。

## 管理サーバー

Kaspersky Security Center のコンポーネントの 1 つで、企業ネットワークにインストールされているすべてのカスペルスキー製品に関する情報を一元的に保管し、管理します。

## 駆除

感染しているオブジェクトの処理方法の 1 つ。駆除の結果、データが完全に復元するかまたは部分的に復元します。感染したすべてのオブジェクトを駆除できるわけではありません。

## 現在のライセンス

製品によって現在使用されているライセンス。

## 誤検知

感染していないオブジェクトが、カスペルスキー製品によって感染しているとされる状況。オブジェクトのコードがウイルスのコードと似ているために発生します。

## スタートアップオブジェクト

コンピューターにインストールされているオペレーティングシステムとソフトウェアが正しく起動し、動作するために必要なアプリケーションのセット。これらのオブジェクトは、オペレーティングシステムが起動するたびに実行されます。そのようなオブジェクトに感染することに特化したウイルスが存在し、オペレーティングシステムの起動をブロックしたりすることがあります。

## 脆弱性

オペレーティングシステムまたはアプリケーションに侵入し、その整合性を破損させるために悪意のあるプログラムの作成者によって使用される可能性のあるオペレーティングシステムまたはアプリケーションの欠陥。オペレーティングシステムに多数の脆弱性が存在すると、その信頼性が低下します。これは、オペレーティングシステムに侵入したウイルスが、オペレーティングシステムとインストールされているアプリケーションの両方を破壊する可能性があるためです。

## セキュリティレベル

セキュリティレベルは、事前定義されたコンポーネント設定のセットです。

## タスク

カスペルスキー製品によってタスクとして実行される機能：たとえば、ファイルのリアルタイム保護、完全スキャン、定義データベースのアップデート。

## タスクの設定

各タイプのタスク特有のアプリケーション設定。

## 定義データベース

カスペルスキーが把握しているコンピューターセキュリティ上の脅威の情報が含まれるデータベース。データベースの公開時点までの情報が含まれています。定義データベースの署名は、スキャン対象のオブジェクト内の悪意のあるコードの検知に役立ちます。定義データベースは、カスペルスキーのエキスパートによって作成され、1 時間ごとにアップデートされます。

## バックアップ

オブジェクトが駆除または削除される前に、オブジェクトのバックアップコピーを保存するための特別な保管領域。

## ヒューリスティックアナライザー

カスペルスキーの定義データベースにまだ追加されていない情報について脅威を検知する技術。ヒューリスティックアナライザーは、オペレーティングシステムでの動作がセキュリティの脅威と思われるオブジェクトを検知します。ヒューリスティックアナライザーで検知されたオブジェクトは、感染の可能性があると判断されます。たとえば、悪意のあるオブジェクトに典型的なコマンドシーケンス（ファイルを開く、ファイルに書き込む）が含まれる場合、そのオブジェクトは感染の可能性があると判断されます。

## ファイル名マスク

一般的な文字を使用したファイル名の表現。ファイル名マスクで使用される基本的なワイルドカードは、* と ? です。* は任意の数の任意の文字を表します。? は任意の 1 文字を表します。

## 保護ステータス

現在の保護ステータス。デバイスのセキュリティレベルを表します。

## ポリシー

ポリシーは、アプリケーションの設定を定義し、管理グループ内のコンピューターにインストールされているアプリケーションを設定する機能を管理します。アプリケーションごとに個別のポリシーを作成する必要があります。各管理グループのコンピューターにインストールされているアプリケーションに対して複数のポリシーを作成できますが、管理グループ内の 1 つのアプリケーションにつきアクティブなポリシーとして適用できるポリシーは 1 つのみです。

## ライセンスの有効期間

本製品の機能および付加サービスをご利用いただける期間です。利用可能な機能と付加サービスの範囲は、ライセンス種別によって異なります。

## ローカルタスク

個々のクライアントコンピューター上で定義され、実行されるタスク。

# サードパーティ製のコードに関する情報

サードパーティのコードに関する情報は、本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。

Apache は Apache Software Foundation の登録商標または商標です。

Citrix、XenApp および XenDesktop は、米国およびその他の国における Cloud Software Group, Inc. およびその子会社の登録商標または商標です。

CVE は The MITRE Corporation の登録商標です。

Dell Technologies、Dell、Dell Compellent およびその他の商標は Dell Inc. およびその子会社の商標です。

EMC、Celerra、Isilon、OneFS および VNX は EMC Corporation のアメリカ合衆国およびその他の国における商標または登録商標です。

Hitachi は、株式会社日立製作所の商標です。

Linux は、米国およびその他の国における Linus Torvalds の登録商標です。

Microsoft、Active Directory、Internet Explorer、Excel, Hyper-V、JScript、MultiPoint、Outlook、PowerShell、Windows、Windows Server、Windows Vista は、Microsoft グループ企業の商標です。

NetApp および Data ONTAP ロゴはアメリカ合衆国およびその他の国における NetApp, Inc. およびその子会社の商標または登録商標です。

Oracle は Oracle およびその子会社の登録商標です。

UNIX は米国およびその他の国における登録商標で、X/Open Company Limited により独占的に認可されています。

# 補足資料

このセクションには、本ドキュメントの内容を補足する内容が含まれています。

# 簡易スキャンのファイルの拡張子

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

# アプリケーションコンポーネントルールのユーザーアカウント

一部のアプリケーションコンポーネントを設定するには、本製品によるルールの適用対象となるユーザーを選択できる特殊なルールを追加する必要があります。

次のアプリケーションコンポーネントを構成するには、ルールを追加する必要があります：

- アプリケーション起動コントロール
- デバイスコントロール
- ふるまい検知
- システム変更監視

ユーザーの追加には次の方法があります：

- Active Directory からの選択（推奨）
- Kaspersky Security Center のユーザーリストからの選択
- 手動での追加

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。ローカルアカウントを使用する際のセキュリティリスクについて詳しくは、マイクロソフトサポート技術情報を参照してください。ローカルユーザーアカウントを使用する場合、コンピューターのセキュリティに関する全責任はユーザーにあります。特に、製品の設定へのアクセスのコントロールと制限に関する責任が含まれます。

本製品はユーザーの SID（セキュリティ識別子）を使用してユーザーを識別します。Active Directory または Kaspersky Security Center ユーザーリストのユーザーアカウントを使用する場合、本製品は管理サーバーで SID を識別します。つまり、ユーザーを識別するためにコンピューターに余分な負荷をかけることはありません。1000 人以上のローカルユーザーアカウントをアプリケーションルールに追加した場合、本製品はドメインコントローラーに接続してユーザーを識別します。つまり、コンピューターへの負荷が増加します。コンピューターのパフォーマンスへの影響を最適化するには、Active Directory または Kaspersky Security Center ユーザーリストのユーザーアカウントを使用することを推奨します。

Kaspersky Embedded Systems Security は、ルール内の埋め込みユーザーアカウントとグループアカウント（「Everyone」グループなど）をサポートします。ユーザーの SID 検出の特性により、本製品では Active Directory または Kaspersky Security Center ユーザーリストから追加された埋め込みアカウントのみ使用できます。埋め込みアカウントが手動で追加されるルールは機能しません。