kaspersky

# Kaspersky Embedded Systems Security

© 2024 AO Kaspersky Lab

# 目次


Kaspersky Embedded Systems Security について
新機能
Kaspersky Embedded Systems Security に関する情報源
  自分で調査する場合の情報源
  カスペルスキー製品の Web コミュニティの利用
Kaspersky Embedded Systems Security
  配布キット
  システム要件
  機能要件および制限事項
    インストールとアンインストール
    ファイル変更監視
    ファイアウォール管理
    その他の制限事項
アプリケーションのインストールと削除
  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
  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
  インストールおよびアンインストールの設定と Windows インストーラーサービスで使用するコマンドラインオプション
  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
        Windows ファイアウォールの送信ルールの追加
      Kaspersky Embedded Systems Security インストール後に実行する処理
        Kaspersky Embedded Systems Security データベース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
    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
Active Directory のグループポリシーを使用した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
アプリケーションインターフェイス
ライセンス
使用許諾契約書について
ライセンスについて
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について
データの提供について
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
ライセンスの有効期限が切れた場合の機能の制限
ライセンスの更新
ライセンスの削除
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
ポリシーでの全般的な製品設定の表示と編集
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
Kaspersky Security Center での全般的なアプリケーション設定
Kaspersky Security Center でのスケーラビリティ、インターフェイスおよびスキャン設定
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
ローカルのシステムタスクのスケジュールによる開始の設定
Kaspersky Security Center での隔離およびバックアップ設定
ポリシーの作成と編集
ポリシーの作成
Kaspersky Embedded Systems Security ポリシー設定のセクション
ポリシーの設定
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
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
Kaspersky Security Center でのグループタスクの設定
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
クラッシュの診断設定
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
Kaspersky Embedded Systems Security コンソールの使用
Kaspersky Embedded Systems Security コンソールについて
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
別のデバイスにインストールしたアプリケーションコンソールを使用した Kaspersky Embedded Systems Security の管理
アプリケーションコンソールからの全般的なアプリケーション設定
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
セキュリティ設定テンプレートの使用
セキュリティ設定テンプレートについて
セキュリティ設定テンプレートの作成
テンプレートのセキュリティ設定の表示
セキュリティ設定テンプレートの適用
セキュリティ設定テンプレートの削除
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 プラグインでのスケーラビリティ、インターフェイスおよびスキャン設定
Web プラグインでのセキュリティ設定
Web プラグインでの接続設定
ローカルのシステムタスクのスケジュールによる開始の設定
Web プラグインでの隔離とバックアップの設定

ポリシーの作成と編集
ポリシーの作成
Kaspersky Embedded Systems Security ポリシー設定のセクション
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
Web プラグインでのクラッシュの診断設定
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
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
ダンプファイルおよびトレースファイルの書き込みの設定
Kaspersky Embedded Systems Security の定義データベースとソフトウェアモジュールのアップデート
アップデートタスクについて
ソフトウェアモジュールのアップデートについて
定義データベースのアップデートについて
組織内で使用されるアンチウイルス製品の定義データベースとモジュールのアップデート方式
アップデートタスクの設定
Kaspersky Embedded Systems Security のアップデート元の使用設定
定義データベースのアップデートタスク実行中のディスク I/O の最適化
アップデートのコピータスクの設定
ソフトウェアモジュールのアップデートタスクの設定
Kaspersky Embedded Systems Security 定義データベースのロールバック
アプリケーションモジュールのアップデートのロールバック
アップデートタスクの統計情報
オブジェクトの隔離とバックアップのコピー
感染の可能性があるオブジェクトの隔離：隔離
感染の可能性があるオブジェクトの隔離について
隔離オブジェクトの表示
隔離オブジェクトの並べ替え
隔離オブジェクトのフィルタリング
隔離のスキャン
隔離されたオブジェクトの復元
オブジェクトの隔離への移動
隔離からのオブジェクトの削除
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
隔離の設定
隔離の統計情報
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
駆除または削除前のオブジェクトのバックアップについて

バックアップに保存された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
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：ブロック対象コンピューター
ブロック対象コンピューターの保管領域について
管理プラグインからブロック対象コンピューターを管理する
信頼しないコンピューターのブロックの有効化
ブロック対象コンピューターの設定
アプリケーションコンソールからブロック対象コンピューターを管理する
信頼しないコンピューターのブロックの有効化
ブロック対象コンピューターの設定
Web プラグインからブロック対象コンピューターを管理する
コンピューターのブロックの有効化
ブロック対象コンピューターの設定
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
システム監査ログ
システム監査ログでのイベントの並べ替え
システム監査ログでのイベントのフィルタリング
システム監査ログからのイベントの削除
実行ログ
タスク実行ログについて
タスク実行ログでのイベントリストの表示
タスク実行ログの並べ替え
タスク実行ログのフィルタリング
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
タスク実行ログからの情報のエクスポート
タスク実行ログの削除
セキュリティログ
イベント ビューアーでの Kaspersky Embedded Systems Security のイベントログの表示
管理プラグインでのログの設定
SIEM 統合について
SIEM 統合設定
ログと通知の設定
ログの設定
セキュリティログ
SIEM 統合設定
通知の設定
管理サーバーとのインタラクションの設定
通知の設定
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
Kaspersky Embedded Systems Security の開始と停止
Kaspersky Embedded Systems Security 管理プラグインの起動

スタートメニューからの Kaspersky Embedded Systems Security コンソールの起動
Kaspersky Security サービスの開始と停止
オペレーティングシステムのセーフモードでの Kaspersky Embedded Systems Security コンポーネントの起動
オペレーティングシステムのセーフモードでの Kaspersky Embedded Systems Security の動作について
セーフモードでの Kaspersky Embedded Systems Security の起動
Kaspersky Embedded Systems Security のセルフディフェンス機構
Kaspersky Embedded Systems Security のセルフディフェンス機構について
Kaspersky Embedded Systems Security のコンポーネントがインストールされているフォルダーの改変防止
Kaspersky Embedded Systems Security のレジストリキーの改変防止
Kaspersky Security サービスを保護対象サービスとして登録する
Kaspersky Embedded Systems Security の各種機能に対するアクセス権限の管理
Kaspersky Embedded Systems Security を管理するための権限について
登録されたサービスを管理するための権限について
Kaspersky Security 管理サービスのアクセス権限について
Kaspersky Security サービスを管理するための権限について
管理プラグインからアクセス権限を管理する
Kaspersky Embedded Systems Security と Kaspersky Security サービスのアクセス権限の設定
Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス
アプリケーションコンソールからアクセス権限を管理する
Kaspersky Embedded Systems Security と Kaspersky Security サービスを管理するためのアクセス権限の設定
Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス
Web プラグインからアクセス権限を管理する
Kaspersky Embedded Systems Security と Kaspersky Security サービスのアクセス権限の設定
Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス
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タスクについて
タスクの保護範囲とセキュリティ設定について
仮想保護範囲について
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タスク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タスクの既定の設定
管理プラグインからファイルのリアルタイム保護タスクを管理する
操作方法
ファイルのリアルタイム保護タスクのポリシーの設定ウィンドウ
ファイルのリアルタイム保護タスクのプロパティウィンドウ
ファイルのリアルタイム保護タスクの設定
保護モードの選択
ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの統合の設定
タスクのスケジュールを設定する
タスクの保護範囲の作成と編集
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
タスクの全般的な設定
処理の設定
パフォーマンスの設定
アプリケーションコンソールからファイルのリアルタイム保護タスクを管理する
操作方法

ファイルのリアルタイム保護タスクの設定ウィンドウ
ファイルのリアルタイム保護タスクの範囲の設定ウィンドウ
ファイルのリアルタイム保護タスクの設定
保護モードの選択
ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの統合の設定
タスクスケジュールの設定
保護範囲の作成
ネットワークファイルリソースのビューの設定
保護範囲の作成
保護範囲にネットワークオブジェクトを含める
仮想保護範囲の作成
手動でのセキュリティの設定
ファイルのリアルタイム保護タスクの定義済みセキュリティレベルの選択
タスクの全般的な設定
処理の設定
パフォーマンスの設定
ファイルのリアルタイム保護タスクの統計情報
Web プラグインからファイルのリアルタイム保護タスクを管理する
ファイルのリアルタイム保護タスクの設定
タスクの保護範囲の設定
KSN の使用
KSN の使用タスクについて
KSN の使用タスクの既定の設定
管理プラグインから KSN の使用を管理する
KSN の使用タスクの設定
データ処理の設定
アプリケーションコンソールから KSN の使用を管理する
KSN の使用タスクの設定
データの取り扱い方法の設定
Web プラグインから KSN の使用を管理する
追加のデータ転送の設定
KSN の使用タスクの統計情報
ネットワーク脅威対策
ネットワーク脅威対策タスクについて
ネットワーク脅威対策タスクの既定の設定
ネットワーク脅威対策タスクのアプリケーションコンソールからの設定
タスクの全般的な設定
除外の追加
ネットワーク脅威対策タスクの管理プラグインからの設定
タスクの全般的な設定
除外の追加
ネットワーク脅威対策タスクの Web プラグインからの設定
タスクの全般的な設定
除外の追加
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について
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タスクでの KSN の使用について
アプリケーション起動コントロールルールの作成について
アプリケーション起動コントロールタスクの既定の設定
管理プラグインからアプリケーション起動コントロールを管理する
操作方法
アプリケーション起動コントロールタスクのポリシーの設定ウィンドウ
アプリケーション起動コントロールルールのリスト
アプリケーション起動コントロールルールの自動作成タスクのウィザードとプロパティウィンドウ
アプリケーション起動コントロールタスクの設定
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の自動作成タスクの設定
アプリケーション起動コントロールルールの Kaspersky Security Center からの設定
アプリケーション起動コントロールルールの追加
「既定で許可」モードを有効にする
Kaspersky Security Center イベントからの許可ルールの作成
ブロックされたアプリケーションに関する Kaspersky Security Center のレポートからのルールのインポート
XML ファイルからのアプリケーション起動コントロールルールのインポート
アプリケーション起動のテスト
アプリケーション起動コントロールルールの自動作成タスクの作成
タスクの適用範囲の制限
ルールの自動作成中に実行する処理
ルールの自動作成の完了時に実行する処理
アプリケーションコンソールからアプリケーション起動コントロールを管理する
操作方法
アプリケーション起動コントロールタスクの設定ウィンドウ
アプリケーション起動コントロールルールの設定ウィンドウ
アプリケーション起動コントロールルールの自動作成タスクの設定ウィンドウ
アプリケーション起動コントロールタスクの設定
アプリケーション起動コントロールタスクのモードの選択
アプリケーション起動コントロールタスクの範囲の設定
KSN の使用の設定
ソフトウェア配布コントロール
アプリケーション起動コントロールルールの設定
アプリケーション起動コントロールルールの追加
「既定で許可」モードを有効にする
アプリケーション起動コントロールタスクイベントからの許可ルールの作成
アプリケーション起動コントロールルールのエクスポート
XML ファイルからのアプリケーション起動コントロールルールのインポート
アプリケーション起動コントロールルールの削除
アプリケーション起動コントロールルールの自動作成タスクの設定
タスクの適用範囲の制限
ルールの自動作成中に実行する処理
ルールの自動作成の完了時に実行する処理
Web プラグインからアプリケーション起動コントロールを管理する
デバイスコントロール
デバイスコントロールタスクについて
デバイスコントロールルールについて
デバイスコントロールルールの作成について

デバイスコントロールルールの自動作成タスクについて
デバイスコントロールの既定のタスク設定
管理プラグインからデバイスコントロールを管理する
操作方法
デバイスコントロールタスクのポリシーの設定ウィンドウ
デバイスコントロールルールのリスト
デバイスコントロールルールの自動作成タスクのウィザードとプロパティウィンドウ
デバイスコントロールタスクの設定
デバイスコントロールルールの自動作成タスクの設定
デバイスコントロールルールの Kaspersky Security Center からの設定
Kaspersky Security Center ポリシーでのシステムデータに基づく許可ルールの作成
接続しているデバイスのためのルール作成
ブロックされたデバイスに関する Kaspersky Security Center のレポートからのルールのインポート
デバイスコントロールルールの自動作成タスクを使用したルールの作成
デバイスコントロールルールのリストに生成されたルールを追加する
アプリケーションコンソールからデバイスコントロールを管理する
操作方法
デバイスコントロールタスクの設定ウィンドウ
デバイスコントロールルールの設定ウィンドウ
デバイスコントロールルールの自動作成タスクの設定ウィンドウ
デバイスコントロールタスクの設定
デバイスコントロールルールの設定
XML ファイルからのデバイスコントロールルールのインポート
デバイスコントロールタスクイベントに基づいたルールリストの入力
1 台以上の外部デバイスへの許可ルールの追加
デバイスコントロールルールの削除
デバイスコントロールルールのエクスポート
デバイスコントロールルールのアクティベートとアクティベート解除
デバイスコントロールルールの適用範囲の拡張
デバイスコントロールルールの自動作成タスクの設定
アプリケーションコンソール Web プラグインからデバイスコントロールを管理する
ファイアウォール管理
ファイアウォール管理タスクについて
ファイアウォールのルールについて
ファイアウォール管理タスクの既定の設定
管理プラグインからファイアウォールのルールを管理する
ファイアウォールのルールの有効化と無効化
ファイアウォールルールの手動での追加
ファイアウォールのルールの削除
アプリケーションコンソールからファイアウォールのルールを管理する
ファイアウォールのルールの有効化と無効化
ファイアウォールルールの手動での追加
ファイアウォールのルールの削除
Web プラグインからファイアウォールのルールを管理する
ファイアウォールのルールの有効化と無効化
ファイアウォールルールの手動での追加
ファイアウォールのルールの削除
ファイル変更監視

- ファイル変更監視タスクについて
- ファイル変更監視ルールについて
- ファイル変更監視タスクの既定の設定
- 管理プラグインからファイル変更監視を管理する
  - ファイル変更監視タスクの設定について
  - 監視ルールの設定
- アプリケーションコンソールからファイル変更監視を管理する
  - ファイル変更監視タスクの設定
  - 監視ルールの設定
- Web プラグインからファイル変更監視を管理する
  - ファイル変更監視タスクの設定について
  - 監視ルールの設定

レジストリアクセス監視

- レジストリアクセス監視タスクについて
- システムレジストリの監視ルールについて
- レジストリアクセス監視タスクの既定の設定
- 管理プラグインからレジストリアクセス監視を管理する
  - レジストリアクセス監視タスクの設定
  - 監視ルールの設定
- 管理コンソールからレジストリアクセス監視を管理する
  - レジストリアクセス監視タスクの設定
  - 監視ルールの設定
- Web プラグインからレジストリアクセス監視を管理する
  - レジストリアクセス監視タスクの設定
  - 監視ルールの設定

Windows イベントログ監視

- Windows イベントログ監視タスクについて
- Windows イベントログ監視タスクの既定の設定
- 管理プラグインから Windows イベントログ監視のルールを管理する
  - 定義済みタスクルールの設定
  - 管理プラグインから Windows イベントログ監視のルールを追加する
- アプリケーションコンソールから Windows イベントログ監視のルールを管理する
  - 定義済みタスクルールの設定
  - アプリケーションコンソールから Windows イベントログ監視のルールを追加する
- Web プラグインから Windows イベントログ監視のルールを管理する

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について
- ベースラインに基づくファイル変更監視タスクについて
- コンテキストメニューからオンデマンドスキャンタスクの開始を有効にする
- オンデマンドスキャンタスクの既定の設定
- 管理プラグインからオンデマンドスキャンタスクを管理する
  - 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プロパティウィンドウ
- 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への簡易スキャンのステータスの割り当て
  - 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
- タスクのスキャン範囲の設定
- 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
  - タスクの全般的な設定
  - 処理の設定
  - パフォーマンスの設定
- リムーバブルドライブスキャンの設定
- ベースラインに基づくファイル変更監視タスクの設定

アプリケーションコンソールからオンデマンドスキャンタスクを管理する
- 操作方法
  - 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範囲設定を開く
- オンデマンドスキャンタスクの作成と編集
- オンデマンドスキャンタスクのスキャン範囲
  - ネットワークファイルリソースのビューの設定
  - スキャン範囲の作成
  - スキャン範囲にネットワークオブジェクトを含める
  - 仮想スキャン範囲の作成
- セキュリティの設定
  - 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
  - タスクの全般的な設定
  - 処理の設定
  - パフォーマンスの設定
  - 階層型ストレージの設定
- リムーバブルドライブのスキャン
- オンデマンドスキャンタスクの統計情報
- ベースラインファイル変更監視タスクの作成と設定

Web プラグインからオンデマンドスキャンタスクを管理する
- 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プロパティウィンドウ
- タスクのスキャン範囲の設定
- タスクの設定

信頼ゾーン
- 信頼ゾーンについて
- 管理プラグインから信頼ゾーンを管理する
  - 操作方法
    - 信頼ゾーンのポリシーの設定を開く
    - 信頼ゾーンのプロパティウィンドウ
  - 信頼ゾーンの管理プラグインからの設定
    - 除外の追加
    - 信頼されたプロセスの追加
    - not-a-virus（非ウイルス）マスクの適用
- アプリケーションコンソールから信頼ゾーンを管理する

アプリケーションコンソールでタスクに信頼ゾーンを適用する
アプリケーションコンソールでの信頼ゾーンの設定
除外対象オブジェクトの信頼ゾーンへの追加
信頼されたプロセスの追加
not-a-virus（非ウイルス）マスクの適用
Web プラグインから信頼ゾーンを管理する
脆弱性攻撃ブロック
脆弱性攻撃ブロックについて
管理プラグインから脆弱性攻撃ブロックを管理する
操作方法
脆弱性攻撃ブロックのポリシーの設定を開く
脆弱性攻撃ブロックのプロパティウィンドウ
プロセスメモリ保護の設定
プロセスの保護範囲への追加
アプリケーションコンソールから脆弱性攻撃ブロックを管理する
操作方法
脆弱性攻撃ブロックの全般的な設定ウィンドウ
脆弱性攻撃ブロックのプロセス保護設定ウィンドウ
プロセスメモリ保護の設定
プロセスの保護範囲への追加
Web プラグインから脆弱性攻撃ブロックを管理する
プロセスメモリ保護の設定
プロセスの保護範囲への追加
脆弱性攻撃ブロック技術
サードパーティ製システムとの統合
システム監視用パフォーマンスカウンター
Kaspersky Embedded Systems Security のパフォーマンスカウンターについて
拒否された要求の合計数
スキップされた要求の合計数
システムリソースの不足が原因で処理されなかった要求の数
処理のために送信された要求の数
ファイルインターセプションディスパッチャストリームの平均数
ファイルインターセプションディスパッチャストリームの最大数
感染したオブジェクトのキュー内にある項目数。
1秒あたりの処理オブジェクト数
Kaspersky Embedded Systems Security の SNMP カウンターおよびトラップ
Kaspersky Embedded Systems Security の SNMP カウンターおよびトラップについて
Kaspersky Embedded Systems Security の SNMP カウンター
パフォーマンスカウンター
隔離カウンター
バックアップカウンター
標準カウンター
更新カウンター
ファイルのリアルタイム保護カウンター
Kaspersky Embedded Systems Security の SNMP トラップとそのオプション
Kaspersky Embedded Systems Security の SNMP トラップオプションの説明と取り得る値
WMI との統合
コマンドラインからの Kaspersky Embedded Systems Security の使用

コマンド
Kaspersky Embedded Systems Security コマンドヘルプの表示：KAVSHELL HELP
Kaspersky Security サービスの開始と停止：KAVSHELL START、KAVSHELL STOP
選択した領域のスキャン：KAVSHELL SCAN
簡易スキャンの開始：KAVSHELL SCANCRITICAL
タスクの非同期での管理：KAVSHELL TASK
PPL 属性の削除：KAVSHELL CONFIG
コンピューターのリアルタイム保護タスクの開始と停止：KAVSHELL RTP
アプリケーション起動コントロールタスクの管理：KAVSHELL APPCONTROL /CONFIG
アプリケーション起動コントロールルールの自動作成：KAVSHELL APPCONTROL /GENERATE
アプリケーション起動コントロールルールのリストの入力：KAVSHELL APPCONTROL
デバイスコントロールルールのリストの入力：KAVSHELL DEVCONTROL
定義データベースのアップデートタスクを開始する：KAVSHELL UPDATE
Kaspersky Embedded Systems Security 定義データベースのロールバック：KAVSHELL ROLLBACK
Windows イベントログ監視の管理：KAVSHELL TASK LOG-INSPECTOR
製品のアクティベート：KAVSHELL LICENSE
トレースログの有効化、設定、無効化：KAVSHELL TRACE
Kaspersky Embedded Systems Security ログファイルのデフラグ：KAVSHELL VACUUM
iSwift ベースのクリーニング：KAVSHELL FBRESET
ダンプファイル作成の有効化と無効化：KAVSHELL DUMP
設定のインポート：KAVSHELL IMPORT
設定のエクスポート：KAVSHELL EXPORT
Microsoft Operations Management Suite との統合：KAVSHELL OMSINFO
ベースラインに基づくファイル変更監視タスクの管理：KAVSHELL FIM /BASELINE
コマンドのリターンコード
KAVSHELL START および KAVSHELL STOP コマンドのリターンコード
KAVSHELL SCAN および KAVSHELL SCANCRITICAL コマンドのリターンコード
KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード
KAVSHELL TASK コマンドのリターンコード
KAVSHELL RTP コマンドのリターンコード
KAVSHELL UPDATE コマンドのリターンコード
KAVSHELL ROLLBACK コマンドのリターンコード
KAVSHELL LICENSE コマンドのリターンコード
KAVSHELL TRACE コマンドのリターンコード
KAVSHELL FBRESET コマンドのリターンコード
KAVSHELL DUMP コマンドのリターンコード
KAVSHELL IMPORT コマンドのリターンコード
KAVSHELL EXPORT コマンドのリターンコード
KAVSHELL FIM /BASELINE コマンドのリターンコード
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
トレースファイルと AVZ スクリプトの使用
用語解説
Kaspersky Security Network（KSN）
OLE 埋め込みオブジェクト
SIEM
圧縮ファイル

アップデート
イベントの重要度
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

# Kaspersky Embedded Systems Security について

Kaspersky Embedded Systems Security 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。

Kaspersky Embedded Systems Security は、Windows のさまざま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**：ユーザーによるアプリケーションの起動の試行を追跡し、保護対象デバイスでのアプリケーションの起動を制御します。
- **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。

- **ファイアウォール管理**：Windows ファイアウォールを管理する機能を提供します。設定およびオペレーティングシステムのファイアウォールのルールを設定し、外部からファイアウォール設定が編集される可能性をすべてブロックします。

- **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とおりです：

- **定義データベースのアップデート**と**ソフトウェアモジュールのアップデート**：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**：保護対象のデバイスにアクセスする管理者とユーザーに対して Kaspersky Embedded Systems Security の動作におけるイベントとデバイス上のアンチウイルスによる保護のステータスを通知するように、本製品を設定できます。

- **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**：プロセスにエージェントを注入する脆弱性攻撃から、プロセスメモリを保護できます。

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 の新バージョンでは、次の新機能と機能強化が導入されました：

- サポートされるオペレーティングシステムに、以下が追加されました：
  - Microsoft Windows 10 21H2
  - Microsoft Windows 11
- ライセンス：ライセンスの有効期限が切れても、定義データベースのアップデートコンポーネントと Kaspersky Security Network サービス以外のシステムコンポーネントは動作し続けます。
- ライセンス：アクティベーションコードがサポートされました。
- システム監査設定の改良：ファイル変更監視タスクでは、それぞれのルールを作成したあと、選択した監視領域のファイルの変更をブロックできます。また、信頼ゾーンを適用して、信頼するオブジェクトと信頼するユーザーを監視領域から除外することもできます。
- システム監査設定の改良：レジストリアクセス監視タスクでは、それぞれのルールを作成したあと、統計情報を集めたり、選択した監視領域でのレジストリキーと値の変更をブロックできます。また、信頼ゾーンを適用して、信頼するプロセスと信頼するユーザーを監視領域から除外することもできます。
- Kaspersky Embedded Systems Security サービスの早期起動のコントロールを有効にするオプションが追加されました。
- Kaspersky Security Center コンポーネントのステータスレポートで、標準ステータスのセットが拡張されました。新しいステータスでは、コンポーネントが［処理を実行］モードで動作しているか、統計を収集して脅威について通知するだけかについての情報を提供します。
- セルフディフェンスの改良：Kaspersky Embedded Systems Security コンソールおよび Kaspersky Embedded Systems Security 管理プラグインのポリシーのプロパティで、外部の脅威に対して Kaspersky Embedded Systems Security のファイルやレジストリキーの保護を有効または無効にできるようになりました。
- Kaspersky Embedded Systems Security を起動すると、本製品は保護対象デバイスに個々のタグを割り当てます。タグは、同じ名前と同じ IP アドレスで登録された保護対象デバイスのプール内で異なるデバイスを識別するのに役立ちます。
- Kaspersky Security Center のユーザーは、製品の Web プラグインの次のダイアログを使用できるようになりました：
  - ファイル変更監視
  - アプリケーション起動コントロール
  - Windows イベントログ監視
- Kaspersky Embedded Systems Security は、Kaspersky Cloud コンソールの一部として使用できるようになりました。
- Kaspersky Embedded Systems Security で、Kaspersky Security サービスに対して遅延開始モードを設定できるようになりました。このモードでは、他のすべてのオペレーティングシステムコンポーネントが読み込まれると、Kaspersky Security Service が開始されます。

- デバイスコントロールタスクの変更：統計情報を収集するか、UAS 技術をサポートする USB で接続されたデバイスをブロックするようにタスクを設定できるようになりました。

- 製品のライフサイクルの表へのリンクがオンラインヘルプで利用できるようになりました。

- 旧バージョンの不具合が一部修正されました：旧バージョンの不具合の修正が本製品に含まれています。

# Kaspersky Embedded Systems Security に関する情報源

このセクションでは、製品の情報源を示します。

問題の重要性や緊急性に応じて、情報の入手先をお選びください。

## 自分で調査する場合の情報源

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。
- ガイド。

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。

製品情報に関するお問い合わせがある場合、お問い合わせフォームから送信することができます。［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 に関する文書

『Kaspersky Embedded Systems Security 管理者用ガイド』には、アプリケーションのインストール、アンインストール、設定、および使用に関する情報が含まれます。

## カスペルスキー製品の Web コミュニティの利用

特に緊急の対応が必要ではない場合は、カスペルスキーの Web コミュニティをご利用ください。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。

オンラインコミュニティでは、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。

# Kaspersky Embedded Systems Security

このセクションでは、Kaspersky Embedded Systems Security の機能、コンポーネント、および配布キットについて説明し、Kaspersky Embedded Systems Security のシステム要件のリストを提供します。

## 配布キット

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 インストールウィザードの起動。
- Kaspersky Embedded Systems Security コンソールインストールウィザードの起動。
- Kaspersky Security Center を介して本製品を管理するための Kaspersky Embedded Systems Security 管理プラグインをインストールするインストールウィザードの起動。
- 『管理者用ガイド』をお読みください。
- 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。
- テクニカルサポートサイトにアクセスしてください。
- 最新バージョンの Kaspersky Embedded Systems Security に関する情報をお読みください。

フォルダー \console には、アプリケーションコンソール（コンポーネントの「Kaspersky Embedded Systems Security 管理ツール」のセット）をインストールするためのファイルが含まれています。

フォルダー \product には、以下のファイルが含まれています：

- 32 ビット版または 64 ビット版の Microsoft Windows オペレーティングシステムが稼働している保護対象デバイス上に Kaspersky Embedded Systems Security のコンポーネントをインストールするためのファイル。
- Kaspersky Security Center によって Kaspersky Embedded Systems Security を管理する管理プラグインをインストールするためのファイル。
- 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。
- 使用許諾契約書およびプライバシーのテキストが記載されたファイル。

フォルダー \product_no_avbases には、Kaspersky Embedded Systems Security コンポーネントと管理プラグインのインストールファイル（定義データベースは未適用）が含まれています。

フォルダー \setup には、ファイル起動用の構成プログラムが含まれています。

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 インストールウィザードの自動実行ファイル。 |
| release_notes.txt | このファイルにはリリース情報が含まれています。 |

| | |
|---|---|
| migration.txt | このファイルには、本製品の前バージョンからの移行について記載されています。 |
| setup.exe | ファイル起動用の構成プログラム（setup.hta の起動）。 |
| \console\esstools_x86.msi | Windows インストーラーパッケージ。32 ビット版 Microsoft Windows の保護対象デバイスに、アプリケーションコンソールをインストールします。 |
| \console\esstools_x64.msi | Windows インストーラーパッケージ。64 ビット版 Microsoft Windows の保護対象デバイスに、アプリケーションコンソールをインストールします。 |
| \console\setup.exe | コンポーネントの「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）用セットアップウィザードを起動するファイル。このセットアップウィザードで指定した設定を使用して、インストールパッケージファイル esstools.msi を起動します。 |
| \product\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。 |
| \product\setup.exe | ウィザードを使用して、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でインストールパッケージファイル ess.msi を実行します。 |
| \product\ess_x86.msi | Windows インストーラーパッケージ。32 ビット版 Microsoft Windows の保護対象デバイスに、Kaspersky Embedded Systems Security の **Protect computer with Anti-Virus Bases** の設定をインストールします。<br>Protect computer with Anti-Virus Bases の設定が選択されている場合、ファイアウォール管理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。<br>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 Protect computer with Anti-Virus Bases の設定をインストールすると、以下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：<br>• ファイルのリアルタイム保護<br>• オンデマンドスキャン<br>• ネットワーク脅威対策 |
| \product\ess_x64.msi | Windows インストーラーパッケージ。64 ビット版 Microsoft Windows の保護対象デバイスに、Kaspersky Embedded Systems Security の **Protect computer with Anti-Virus Bases** の設定をインストールします。 |

| | |
|---|---|
| | Protect computer with Anti-Virus Bases の設定が選択されている場合、ファイアウォール管理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。<br>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 Protect computer with Anti-Virus Bases の設定をインストールすると、以下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：<br>• ファイルのリアルタイム保護<br>• オンデマンドスキャン<br>• ネットワーク脅威対策 |
| \product\ess.kud | Kaspersky Security Center を経由した Kaspersky Embedded Systems Security 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\klcfginst.exe | Kaspersky Security Center によって Kaspersky Embedded Systems Security を管理する管理プラグイン用インストーラー。これを使用して Kaspersky Embedded Systems Security を管理する場合、Kaspersky Security Center の管理コンソールがインストールされた各保護対象デバイスに管理プラグインをインストールします。 |
| \product\license.txt | 使用許諾契約書およびプライバシーポリシーのテキスト。 |
| \product_long_term\setup.exe | ウィザードを使用して、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でインストールパッケージファイル ess.msi を実行します。 |
| \product_long_term\ess_x86.msi | Windows インストーラーパッケージ。32 ビット版 Microsoft Windows の保護対象デバイスに、Kaspersky Embedded Systems Security の Protect computer with Default Deny テクノロジーの設定をインストールします。 |

| | |
|---|---|
| | アップデートを有効にするコンポーネントは、Protect computer with Default Deny テクノロジーの設定には含まれていません。<br><br>Protect computer with Default Deny テクノロジー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、次のとおりです：<br>• Core<br>• 脆弱性攻撃ブロック<br>• アプリケーション起動コントロール<br>• システムトレイアイコン<br>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製品のバージョンに Kaspersky Embedded Systems Security の Protect computer with Default Deny テクノロジーの設定をインストールすると、以下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：<br>• ファイルのリアルタイム保護<br>• オンデマンドスキャン<br>• アップデートを有効にするコンポーネント<br>この設定は、リソースが限られているシステム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。 |
| \product_long_term\ess_x64.msi | Windows インストーラーパッケージ。64 ビット版 Microsoft Windows の保護対象デバイスに、Kaspersky Embedded Systems Security の **Protect computer with Default Deny テクノロジー**の設定をインストールします。 |

| | |
|---|---|
| | アップデートを有効にするコンポーネントは、Protect computer with Default Deny テクノロジーの設定には含まれていません。<br>Protect computer with Default Deny テクノロジー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、次のとおりです：<br>• Core<br>• 脆弱性攻撃ブロック<br>• アプリケーション起動コントロール<br>• システムトレイアイコン<br>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製品のバージョンに Kaspersky Embedded Systems Security の Protect computer with Default Deny テクノロジーの設定をインストールすると、以下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：<br>• ファイルのリアルタイム保護<br>• オンデマンドスキャン<br>• アップデートを有効にするコンポーネント<br>この設定は、リソースが限られているシステム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。 |
| \product_long_term\ess_light.kud | Kaspersky Security Center を経由した Kaspersky Embedded Systems Security 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\klcfginst.exe | Kaspersky Security Center によって Kaspersky Embedded Systems Security を管理する管理プラグイン用インストーラー。これを使用して Kaspersky Embedded Systems Security を管理する場合、Kaspersky Security Center の管理コンソールがインストールされた各保護対象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\license.txt | 使用許諾契約書およびプライバシーポリシーのテキスト。 |
| \setup\setup.hta | ファイル起動用の構成プログラム。 |

## システム要件

Kaspersky Embedded Systems Security をインストールする前に、その他のアンチウイルス製品をデバイスからアンインストールする必要があります。

## 保護対象デバイスのソフトウェア要件

Kaspersky Embedded Systems Security は、32 ビット版または 64 ビット版の Microsoft Windows が稼働しているデバイス上にインストールできます。

Windows Installer 3.1 は、Microsoft Windows XP の保護対象デバイスでアプリケーションのインストールと動作を適切に行うために必要です。

組み込みオペレーティングシステムを搭載した保護対象デバイスに Kaspersky Embedded Systems Security をインストールして使用するには、Filter Manager コンポーネントが必要です。

Kaspersky Embedded Systems Security をインストールする前に、SHA-2 サポートをカバーする必要なアップデートが、保護対象デバイスのオペレーティングシステムにインストールされていることを確認してください。SHA-2 がサポートされていない場合、インストールされているアプリケーションモジュールが正しく機能せず、オペレーティングシステムが誤動作する可能性があります。詳細については、https://support.kaspersky.com/15728 を参照してください。

Kaspersky Embedded Systems Security は、次のいずれかの 32 ビット版または 64 ビット版の Microsoft Windows が稼働しているデバイス上にインストールできます：

- Windows XP Embedded SP3（32 ビット）
- Windows Embedded POSReady 2009（32 ビット）
- Windows Embedded Standard 7 SP1（32 ビット、64 ビット）
- Windows Embedded Enterprise 7 SP1（32 ビット、64 ビット）
- Windows Embedded POSReady 7（32 ビット、64 ビット）
- Windows Embedded 8.0 Standard（32 ビット、64 ビット）
- Windows Embedded 8.1 Industry Professional / Enterprise（32 ビット、64 ビット）
- Windows 10 IoT Enterprise（32 ビット、64 ビット）
- Windows XP Professional SP2 / SP3（32 ビット）
- Windows 7 Professional / Enterprise SP1（32 ビット、64 ビット）
- Windows 8 Professional / Enterprise（32 ビット、64 ビット）
- Windows 8.1 Professional / Enterprise（32 ビット、64 ビット）
- Windows 10 Professional / Enterprise（32 ビット、64 ビット）
- Windows 10 1607 Professional / Enterprise / IoT Enterprise（32 ビット、64 ビット）
- Windows 10 1703 Professional / Enterprise / IoT Enterprise（32 ビット、64 ビット）
- Windows 10 1709 Professional / Enterprise / IoT Enterprise（32 ビット、64 ビット）

- Windows 10 1803 Professional / Enterprise / IoT Enterprise（32 ビット、64 ビット）
- Windows 10 1809 Professional / Enterprise / IoT Enterprise（32 ビット、64 ビット）
- Windows 10 19H2 Professional / Enterprise / IoT Enterprise（32 ビット、64 ビット）
- Windows 10 21H2 Professional / Enterprise / IoT Enterprise（32 ビット、64 ビット）
- Windows 10 Enterprise LTSC 2016（32 ビット、64 ビット）
- Windows 10 Enterprise LTSC 2019（32 ビット、64 ビット）
- Windows 10 Enterprise LTSC 2021（32 ビット、64 ビット）
- Windows 11 21H2 Professional / 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は、インストールされている Windows によって異なります：

- Windows XP（32 / 64 ビット）、Windows Embedded XP、Windows Embedded POSReady 2009、Windows Embedded POSReady 7 でのデバイスのハードウェア要件：
  - 最小構成：
    - 空きディスク容量：
      - アプリケーション起動コントロールコンポーネントをインストールする場合 - 50 MB
      - Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 2 GB
    - メモリ：
      - Microsoft Windows のデバイスにアプリケーション起動コントロールコンポーネントのみをインストールする場合 - 256 MB
      - すべてのコンポーネントのフルインストールを実行する場合 - 512 MB
    - プロセッサ：
      - 32 ビット Microsoft Windows の場合：

        1.4 GHz シングルコアプロセッサ

        Intel® Pentium® III
      - 64 ビット Microsoft Windows の場合：

        1.4 GHz シングルコアプロセッサ

        Intel Pentium IV
  - 推奨構成：
    - 空きディスク容量：

- アプリケーション起動コントロールコンポーネントをインストールする場合 - 2 GB
- Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 4 GB

- メモリ：2 GB
- プロセッサ：2.4 GHz クアッドコアプロセッサ

- Windows Embedded 7、Windows Embedded 8、Windows Embedded 10 でのデバイスのハードウェア要件：
  - 最小構成：
    - 空きディスク容量：
      - アプリケーション起動コントロールコンポーネントをインストールする場合 - 50 MB
      - Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 2 GB
    - メモリ：1 GB
    - プロセッサ：1.4 GHz シングルコアプロセッサ Intel Pentium IV
  - 推奨構成：
    - 空きディスク容量：
      - アプリケーション起動コントロールコンポーネントをインストールする場合 - 2 GB
      - Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 4 GB
    - メモリ：2 GB
    - プロセッサ：2.4 GHz クアッドコアプロセッサ
- Windows 7（64 ビット）、Windows 8（64 ビット）、Windows 10（64 ビット）、Windows 11（64 ビット）でのデバイスのハードウェア要件：
  - 最小構成：
    - 空きディスク容量：
      - アプリケーション起動コントロールコンポーネントをインストールする場合 - 50 MB
      - Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 2 GB
    - メモリ：
      - Microsoft Windows のデバイスにアプリケーション起動コントロールコンポーネントのみをインストールする場合 - 1 GB
      - すべてのコンポーネントのフルインストールを実行する場合 - 2 GB
    - プロセッサ：

      1.4 GHz シングルコアプロセッサ

Intel Pentium IV

- 推奨構成：
  - 空きディスク容量：
    - アプリケーション起動コントロールコンポーネントをインストールする場合 - 2 GB
    - Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 4 GB
  - メモリ：
    - Microsoft Windows のデバイスにアプリケーション起動コントロールコンポーネントのみをインストールする場合 - 2 GB
    - すべてのコンポーネントのフルインストールを実行する場合 - 4 GB
  - プロセッサ：2.4 GHz クアッドコアプロセッサ

- Windows 7（32 ビット）、Windows 8（32 ビット）、Windows 10（32 ビット）でのデバイスのハードウェア要件：
  - 最小構成：
    - 空きディスク容量：
      - アプリケーション起動コントロールコンポーネントをインストールする場合 - 50 MB
      - Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 2 GB
    - メモリ：
      - Microsoft Windows のデバイスにアプリケーション起動コントロールコンポーネントのみをインストールする場合 - 256 MB
      - すべてのコンポーネントのフルインストールを実行する場合 - 1 GB
    - プロセッサ：
      - 32 ビット Microsoft Windows の場合：

        1.4 GHz シングルコアプロセッサ

        Intel Pentium III
      - 64 ビット Microsoft Windows の場合：

        1.4 GHz シングルコアプロセッサ

        Intel Pentium IV
  - 推奨構成：
    - 空きディスク容量：
      - アプリケーション起動コントロールコンポーネントをインストールする場合 - 2 GB

- Kaspersky Embedded Systems Security のすべてのコンポーネントをインストールする場合 - 4 GB

- メモリ：2 GB
- プロセッサ：2.4 GHz クアッドコアプロセッサ

## 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。

## インストールとアンインストール

- Kaspersky Embedded Systems Security のインストールフォルダーの新しいパスに 150 以上の記号が含まれる場合、製品のインストール時に警告が表示されます。この警告はインストールプロセスには影響ありません。Kaspersky Embedded Systems Security は正常にインストールされ、稼働します。
- SNMP プロトコルサポートコンポーネントのインストールでは、SNMP サービスが実行中の場合、このサービスを再起動する必要があります。
- 組み込みオペレーティングシステムが稼働するデバイス上に Kaspersky Embedded Systems Security をインストールして機能させるには、Filter Manager コンポーネントがインストールされている必要があります。
- Kaspersky Embedded Systems Security 管理ツールを、Microsoft Active Directory® グループポリシーからインストールすることはできません。
- 定期的なアップデートを受け取ることができない古い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に製品をインストールする場合は、次のルート証明書を確認する必要があります：DigiCert Assured ID Root CA、DigiCert_High_Assurance_EV_Root_CA、DigiCertAssuredIDRootCA。これらの証明書がないと、本製品が適切に機能しない可能性があります。可能な方法でこれらの証明書をインストールしてください。

## ファイル変更監視

既定では、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は、ファイル整合性監視による監視の対象になっていません。オペレーティングシステムによって絶えず行われるファイル変更に関する情報で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手動で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。

ReFS または NTFS ファイルシステムをバイパスするファイル変更（BIOS、LiveCD などを使用したファイル変更）は監視の対象外となります。

## ファイアウォール管理

- 指定されたルール範囲が 1 つのアドレスで構成されている場合、IPv6 アドレスは使用できません。
- 設定済みのファイアウォールのポリシールールによって、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、ポートルールを手動で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（https://support.kaspersky.com/ksc10、記事 9297）を参照してください。
- 本製品のインストール時に Windows ファイアウォールルールがタスク設定に追加されていない場合、ファイアウォール管理タスクの実行中に行われたこれらのルールやルールグループの変更は、管理の対象外となります。ステータスを更新してこれらのルールを含めるには、ファイアウォール管理タスクを再起動する必要があります。
- ファイアウォール管理タスクを開始すると、オペレーティングシステムのファイアウォール設定から次の種別のルールが自動的に削除されます：

- 拒否ルール
- 送信トラフィックの監視ルール

## その他の制限事項

**オンデマンドスキャン、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。
- ［**起動プロセスのより詳細な分析（プロセスの起動は分析が終了するまでブロックされます）**］と［**KSN の使用**］サービスが同時に有効になっている場合、［統計のみ］モードが選択されていても、引数として URL を取得する起動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
  - ［**起動プロセスのより詳細な分析（プロセスの起動は分析が終了するまでブロックされます）**］を無効にする

  推奨オプション：［起動プロセスのより詳細な分析］を無効にする

**ライセンス**：

- ライセンス情報が SUBST コマンドを使用して作成されたディスクに保存されている場合、またはライセンス情報ファイル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からライセンス情報を使用して製品をアクティベートすることはできません。

**アップデート**：

- Kaspersky Embedded Systems Security の重要なモジュールのアップデートのインストール後、製品のアイコンは既定で非表示になります。
- 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。

**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。正しいマスクの使用例：「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。

**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な場合、タスクバーの通知領域にある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が開くようにするには、ユーザーアカウントを KAVWSEE 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**］から製品をアンインストールすることはできません。

**Kaspersky Security Center との連携**：

- 管理サーバーは、アップデートパッケージを受け取る時と、ネットワーク上の保護対象デバイスにアップデートを送信する前に、定義データベースのアップデートを確認します。管理サーバーは、ソフトウェアモジュールのアップデートを確認しません。

- ネットワークリストを利用して 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、管理サーバーとの通信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）。

**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で稼働している保護対象デバイスに実装されている Microsoft の EMET ユーティリティと競合します。EMET が実装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。

# アプリケーション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。

## 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

\product_long_term\ess_x86.msi ファイルと \product_long_term\ess_x64.msi ファイルは、Kaspersky Embedded Systems Security の **Protect computer with Default Deny テクノロジー** の設定をインストールするように設計されており、\product\ess_x86.msi ファイルと \product\ess_x64.msi ファイルは、**Protect computer with Anti-Virus Bases** の設定をインストールするように設計されています。

Protect computer with Anti-Virus Bases の設定が選択されている場合、ファイアウォール管理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 Protect computer with Anti-Virus Bases の設定をインストールすると、以下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、Protect computer with Default Deny テクノロジーの設定には含まれていません。

Protect computer with Default Deny テクノロジー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、次のとおりです：

- 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製品のバージョンに Kaspersky Embedded Systems Security の Protect computer with Default Deny テクノロジーの設定をインストールすると、以下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システム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。

\console\esstools_x86.msi ファイルおよび \console\esstools_x64.msi ファイルにより、「管理ツール」セットに含まれるすべてのソフトウェア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

Kaspersky Embedded Systems Security 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。

Kaspersky Embedded Systems Security ソフトウェアコンポーネントについて

| コンポーネント | 識別子 | 実行される機能 |
|---|---|---|
| 基本機能 | Core | 製品の基本的な機能のセットが含まれており、それら機能を実行します。<br>コマンドラインから Kaspersky Embedded Systems Security をインストールする際に、Core コンポーネントを指定せずに他の Kaspersky Embedded Systems Security コンポーネントを指定した場合、Core コンポーネントは自動でインストールされます。 |
| アプリケーション起動 | AppCtrl | 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従ってアプリケーシ |

| | | |
|---|---|---|
| コントロール | | ョンの開始を許可または拒否します。<br>これは、アプリケーション起動コントロールタスクに実装されています。 |
| デバイスコントロール | DevCtrl | このコンポーネントは、保護対象デバイスの外部デバイスへの接続試行を追跡し、指定したデバイスコントロールルールに従ってこれらのデバイスの使用を許可または拒否します。<br>コンポーネントは、デバイスコントロールタスクに実装されます。 |
| アンチウイルスによる保護 | AVProtection | アンチウイルスによる保護を提供するコンポーネントです。このコンポーネントには、次のコンポーネントが含まれます：<br>• オンデマンドスキャン<br>• ファイルのリアルタイム保護<br>• ネットワーク脅威対策 |
| ネットワーク脅威対策 | IDS | 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。 |
| オンデマンドスキャン | Ods | Kaspersky Embedded Systems Security システムファイルをインストールし、オンデマンドスキャンタスク（要求に基づいた保護対象デバイスにあるオブジェクトのスキャン）を実行できるようにします。 |
| ファイルのリアルタイム保護 | Oas | 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。<br>このコンポーネントにより、ファイルのリアルタイム保護タスクが実行されます。 |
| Kaspersky Security Network の使用 | Ksn | カスペルスキーのクラウド技術に基づく保護を提供します。<br>このコンポーネントにより、KSN の使用タスクが実行されます（Kaspersky Security Network サービスへの要求の送信および同サービスからの判定の受信）。 |
| ファイル変更監視 | Fim | このコンポーネントは、指定された監視範囲にあるファイル上で実行された操作を記録します。<br>このコンポーネントにより、ファイル変更監視タスクが実行されます。 |
| レジストリアクセス監視 | RegMonitor | このコンポーネントは、タスク設定で定義された監視範囲にある、指定したレジストリのブランチとキーで実行される処理を追跡します。このタスクを使用して、保護対象デバイスでセキュリティ違反を示した変更を検知できます。<br>このコンポーネントにより、レジストリアクセス監視タスクが実行されます。 |
| 脆弱性攻撃ブロック | AntiExploit | 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。 |
| ファイアウォール管理 | ファイアウォール | このコンポーネントは、Kaspersky Embedded Systems Security のグラフィカルユーザーインターフェイスを介した Windows ファイアウォールの管理を可能にします。 |

| | | |
|---|---|---|
| | | このコンポーネントにより、ファイアウォール管理タスクが実行されます。 |
| Kaspersky Security Center ネットワークエージェントとの統合モジュール | AKIntegration | Kaspersky Embedded Systems Security と Kaspersky Security Center ネットワークエージェント間の接続を提供します。<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。 |
| 「システム監視」パフォーマンスカウンターのセット | PerfMonCounters | 一連のシステム監視用パフォーマンスカウンターがインストールされます。Kaspersky Embedded Systems Security をその他のプログラムと一緒に使用する際、パフォーマンスカウンターにより、Kaspersky Embedded Systems Security のパフォーマンスが測定され、保護対象デバイスの潜在的なボトルネックが特定されます。 |
| SNMP カウンターと SNMP トラップ | SnmpSupport | Microsoft Windows の Simple Network Management Protocol（SNMP）から、Kaspersky Embedded Systems Security のカウンターとトラップを公開します。このコンポーネントは、Microsoft SNMP サービスがインストールされている保護対象デバイスにのみインストールできます。 |
| 通知領域内の Kaspersky Embedded Systems Security アイコン | TrayApp | 保護対象デバイスのタスクトレイの通知領域に Kaspersky Embedded Systems Security アイコンを表示します。Kaspersky Embedded Systems Security アイコンは、デバイス保護のステータスを示します。また、このアイコンを使用して、Microsoft 管理コンソールの Kaspersky Embedded Systems Security コンソール（インストールされている場合）と、［**製品情報**］ウィンドウを開くことができます。 |

## 「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>コマンドラインから「管理ツール」をインストールする時に、MmcSnapin コンポーネントを指定せずに他のコンポーネントを指定した場合、MmcSnapin コンポーネントは自動でインストールされます。 |

## 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 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。

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。既定のインストールフォルダーはそれぞれ次のようになります：
  - 32 ビット版の Microsoft Windows：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - 64 ビット版の Microsoft Windows：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security
- 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：
  - %Kaspersky Embedded Systems Security%\mibs
- 64 ビット版の Kaspersky Embedded Systems Security の実行ファイル（フォルダーは、64 ビット版の Microsoft Windows に Kaspersky Embedded Systems Security がインストールされる時にのみ作成されます）：
  - %Kaspersky Embedded Systems Security%\x64
- Kaspersky Embedded Systems Security サービスファイル：
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Data
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Settings
  - %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Dskm

  Windows XP の場合、「Kaspersky Lab」フォルダーへのパスは %ALLUSERSPROFILE%\Application Data です。
- アップデート元の設定を含むファイル：

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Update

- アップデートのコピー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のコピー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\Kaspersky Embedded Systems Security\3.1\Update\Distribution

- 実行ログとシステム監査ログ

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\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\Kaspersky Embedded Systems Security\3.1\Bases\Current

- 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\Kaspersky Embedded Systems Security\3.1\Bases\Backup

- 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\Kaspersky Embedded Systems Security\3.1\Bases\Temp

- 隔離されたオブジェクト（既定のフォルダー）

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Quarantine

- バックアップされたフォルダー（既定のフォルダー）

  %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Backup

- 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\Kaspersky Embedded Systems Security\3.1\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。既定のインストールフォルダーはそれぞれ次のようになります：

- 32 ビット版の Microsoft Windows：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

- 64 ビット版の Microsoft Windows：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools

## Kaspersky Embedded Systems Security サービス

次の Kaspersky Embedded Systems Security サービスでは、ローカルシステム（SYSTEM）アカウントを使用します：

- Kaspersky Security サービス（KAVFS） - Kaspersky Embedded Systems Security のタスクとワークフローを管理する、重要な Kaspersky Embedded Systems Security サービス。

- Kaspersky Security 管理サービス（KAVFSGT） - アプリケーションコンソールを介して Kaspersky Embedded Systems Security の管理を行うサービス。

- Kaspersky Security 脆弱性攻撃ブロックサービス（KAVFSSLP） - セキュリティ設定を外部セキュリティエージェントに送信し、セキュリティイベントについてのデータを受信する通信を仲介するサービス。

## 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 のプロパティ：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]
- Kaspersky Embedded Systems Security イベントログ設定（Kaspersky Event Log）：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]
- Kaspersky Embedded Systems Security 管理サービスのプロパティ：
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]
- パフォーマンスカウンターの設定：
  - 32 ビット版の Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance]
  - 64 ビット版の Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance]
- SNMP プロトコルサポートの設定：
  - 32 ビット版の Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\SnmpAgent]
  - 64 ビット版の Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\SnmpAgent]
- ダンプファイルの設定：
  - 32 ビット版の Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\CrashDump]
  - 64 ビット版の Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\CrashDump]
- トレースファイルの設定：
  - 32 ビット版の Microsoft Windows：[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\Trace]
  - 64 ビット版の Microsoft Windows：
    [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\Trace]
- 製品のタスクと機能の設定：
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1\Environment]

# 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 |
| --- | --- |
| kavfswp.exe | Kaspersky Embedded Systems Security ワークフロー |
| kavtray.exe | システムトレイアイコンのプロセス |
| kavfsmui.exe | コンパクト診断インターフェイスコンポーネントのプロセス |
| kavshell.exe | コマンドラインユーティリティのプロセス |
| kavfsrcn.exe | Kaspersky Embedded Systems Security リモート管理プロセス |
| kavfs.exe | Kaspersky Security のサービスプロセス |
| kavfsgt.exe | Kaspersky Security 管理サービスプロセス |
| kavfswh.exe | Kaspersky Security 脆弱性攻撃ブロックサービスプロセス |

# インストールおよびアンインストールの設定と Windows インストーラーサービスで使用する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 をインストールおよびアンインストールするための設定と、各設定の既定値、インストールの設定値を変更するためのキーと、設定可能な値について説明します。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。

## Windows インストーラーのインストール設定と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：Kaspersky Embedded Systems Security をインストールするには、条件に同意する必要があります。

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

  - `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件に同意：Kaspersky Embedded Systems Security をインストールするには、条件に同意する必要があります。

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

  - `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。

- KB4528760 アップデートがインストールされていない場合、Kaspersky Embedded Systems Security のインストールを許可します。KB4528760 アップデートについて詳しくは、Microsoft の Web サイトを参照してください。

SKIPCVEWINDOWS10=<値> コマンドラインオプションで取り得る値は、次のとおりです：

- 0 - KB4528760 アップデートがインストールされていない場合、Kaspersky Embedded Systems Security のインストールをキャンセルします（既定値）。
- 1 - KB4528760 アップデートがインストールされていない場合、Kaspersky Embedded Systems Security のインストールを許可します。

KB4528760 アップデートプログラムにより、CVE-2020-0601 のセキュリティの脆弱性が修正されます。CVE-2020-0601 のセキュリティの脆弱性について詳しくは Microsoft の Web サイト を参照してください。

- 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かどうか。

  PRESCAN=<値> コマンドラインオプションで取り得る値は、次のとおりです：

  - 0 - インストール中に、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の事前スキャンを実行しない（既定値）。
  - 1 - インストール中に、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の事前スキャンを実行する。

- 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、次のとおりです：

  - Kaspersky Embedded Systems Security：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security
  - 管理ツール：%ProgramFiles%\Kaspersky Lab\ Kaspersky Embedded Systems Security Admins Tools
  - Microsoft Windows 64 ビット版：%ProgramFiles(x86)%

- 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。Kaspersky Embedded Systems Security の起動時にファイルのリアルタイム保護を開始する場合は、この設定をオンにします（推奨）。

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

  - 1 - 開始する（既定値）。
  - 0 - 開始しない。

- Microsoft によって推奨される保護の除外。ファイルのリアルタイム保護タスクで、Microsoft によって除外が推奨されているオブジェクトを、デバイスの保護範囲から除外します。保護対象デバイス上で動作する一部のアプリケーションでは、使用中のファイルがアンチウイルス製品によってインターセプトまたは変更されると、動作が不安定になる場合があります。たとえば、Microsoft は、一部のドメインコントローラアプリケーションを、除外を推奨するオブジェクトのリストに含めています。

  ADDMSEXCLUSION=<値> コマンドラインオプションで取り得る値は、次のとおりです：

  - 1 - 除外する（既定値）。
  - 0 - 除外しない。

- カスペルスキーの推奨事項に従って保護範囲から除外されるオブジェクト。ファイルのリアルタイム保護タスクで、カスペルスキーによって除外が推奨されているオブジェクトを、デバイスの保護範囲から除外します。

  ADDKLEXCLUSION=<値> コマンドラインオプションで取り得る値は、次のとおりです：

  - 1 - 除外する（既定値）。
  - 0 - 除外しない。

- アプリケーションコンソールへのリモート接続を許可。既定では、保護対象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へはリモート接続できません。インストール時に接続を許可できます。Kaspersky Embedded Systems Security は、すべてのポートについて、TCP プロトコルを使用してプロセス kavfsgt.exe の許可ルールを作成します。

  ALLOWREMOTECON=<値> コマンドラインオプションで取り得る値は、次のとおりです：

  - 1 - 許可する。
  - 0 - 拒否する（既定値）。

- 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 \product フォルダーにある、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。\product フォルダーに複数のライセンス情報ファイルがある場合、Windows インストーラーによって有効期限が最も先のライセンス情報ファイルが選ばれます。ライセンス情報ファイルはあらかじめ \product フォルダーに保存できます。また［**ライセンス情報ファイルの追加**］設定を使用して、別のパスをライセンス情報ファイルに指定して保存することもできます。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=<設定ファイル名> の既定値は指定されていません。

- Kaspersky Embedded Systems Security コンソールを別のデバイスにインストールするには、アプリケーションコンソールのオプションに対してネットワーク接続を有効にします。Kaspersky Embedded Systems Security コンソールがインストールされた別のデバイスからデバイス保護をリモート管理できます。Microsoft Windows ファイアウォールでポート 135（TCP）が開き、Kaspersky Embedded Systems Security のリモート管理の実行ファイル kavfsrcn.exe に対してネットワーク接続が許可されます。また、DCOM アプリケーションへのアクセス権が付与されます。インストールが完了したらユーザーを ESS 管理者グループに追加して、リモートからのアプリケーション管理と、保護対象デバイスの Kaspersky Security 管理サービス（kavfsgt.exe ファイル）へのネットワーク接続を許可します。別のデバイスに Kaspersky Embedded Systems Security コンソールをインストールした場合の追加設定については詳細情報が用意されています。

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

  - 1 - 許可する。
  - 0 - 拒否する（既定値）。

- 非互換ソフトウェアのチェックの無効化。この設定を使用すると、保護対象デバイスへのアプリケーションのバックグラウンドインストール時に非互換ソフトウェアのチェックを有効化または無効化できます。

Kaspersky Embedded Systems Security のインストール時には、アプリケーションの他のバージョンが保護対象デバイスにインストールされている場合、この設定の値に関係なく常に警告します。

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

- 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。

### Windows インストーラーのアンインストール設定と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、次のとおりです：

  - 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 \Quarantine 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、次のとおりです：

  - 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 \Backup 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、アンインストール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%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Restored です。

## 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 をインストールまたは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。ess_v3.1_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、setup.exe ファイルを起動したアカウントのユーザーの %temp% フォルダーに保存されます。

［**変更または削除**］メニューからアプリケーションコンソールまたは Kaspersky Security for Windows Server に対して［**変更または削除**］オプションを実行すると、ess_3.1_maintenance.log というログファイルが自動的に %temp% フォルダーに作成されます。

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：*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

# 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 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統合モジュール**：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統合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 3.1 管理プラグイン**：管理コンソールを使用して、Kaspersky Security Center の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 の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 \product\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：

- 配布キットに含まれる \product\setup.exe ファイルからの保護対象デバイスの Kaspersky Embedded Systems Security コンポーネントのインストール。
- 保護対象デバイスまたは別の LAN ホストの配布キットの \console\setup.exe ファイルからの Kaspersky Embedded Systems Security コンソールのインストール。

### 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する

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アンチウイルス製品がインストールされていないことを確認します。
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 setup.exe ファイルを起動します。
2. 表示されるウィンドウの［**インストール**］セクションで、［**Protect computer with Default Deny テクノロジー**］または［**Protect computer with Anti-Virus Bases**］をクリックします。

   Protect computer with Anti-Virus Bases の設定が選択されている場合、ファイアウォール管理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 Protect computer with Anti-Virus Bases の設定をインストールすると、以下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、Protect computer with Default Deny テクノロジーの設定には含まれていません。

Protect computer with Default Deny テクノロジー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、次のとおりです：

- 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製品のバージョンに Kaspersky Embedded Systems Security の Protect computer with Default Deny テクノロジーの設定をインストールすると、以下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システム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。

   ［**使用許諾契約書とプライバシーポリシー**］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、［**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［**プライバシーポリシーに従ってデータが処理されて送信されること（第三国への送信を含む）を理解し、同意します**］をオンにします。［**プライバシーポリシーの内容をすべて確認して理解した上で同意する**］をオンにし、インストールを続行します。

   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**］ウィンドウが開きます。

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の選択**］ウィンドウで、次のように操作します：

   - 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. ［**インストールの詳細設定**］ウィンドウで、次のインストール設定を行います：

    - **製品インストール後にリアルタイム保護を有効にする**
    - **Microsoft によって推奨されているファイルを除外リストに追加する**
    - **Kaspersky Lab によって推奨されているファイルを除外リストに追加する**

      ［**次へ**］をクリックします。

11. ［**設定ファイルからのインポートの設定**］ウィンドウで、次のように操作します：

    a. 互換性のある以前のバージョンのアプリケーションで作成された既存の設定ファイルから Kaspersky Embedded Systems Security の設定をインポートする場合は、設定ファイルを指定します。

    b. ［**次へ**］をクリックします。

12. ［**製品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**］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。

      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製品に適用します。

13. ［**インストールの準備完了**］ウィンドウで、［**インストール**］をクリックします。Kaspersky Embedded Systems Security のコンポーネントのインストールが開始します。

14. 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。

15. セットアップウィザードの完了後にリリースに関する情報を確認する場合は、［**リリースノートの表示**］をオンにします。

16. ［**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 setup.exe ファイルを実行します。
   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 コンソールのインストール**］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。

4. ［**次へ**］をクリックします。

5. 表示されるウィンドウで使用許諾契約書およびプライバシーポリシーの条項を確認し、［**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**］の下にあるチェックボックスをオンにして、インストールを続行します。

6. ［**次へ**］をクリックします。
   ［**インストールの詳細設定**］ウィンドウが表示されます。

7. ［**インストールの詳細設定**］ウィンドウで、次のように操作します：

   - アプリケーションコンソールを使用してリモートデバイスにインストールされている Kaspersky Embedded Systems Security を管理する場合は、［**リモートアクセスを許可する**］をオンにします。
   - ［**カスタムインストール**］ウィンドウを開いてコンポーネントを選択するには：

     a. ［**詳細設定(d)**］をクリックします。
        ［**カスタムインストール**］ウィンドウが開きます。

     b. リストから「管理ツール」コンポーネントを選択します。
        既定では、すべてのコンポーネントがインストールされます。

     c. ［**次へ**］をクリックします。

Kaspersky Embedded Systems Security コンポーネントに関する詳細情報があります。

8. ［**インストール先フォルダーの選択**］ウィンドウで、次のように操作します：

   a. 必要に応じて、インストールするファイルの保存先として別のフォルダーを指定します。

b. ［**次へ**］をクリックします。

9. ［**インストールの準備完了**］ウィンドウで、［**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。

10. ［**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」セットが、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、詳細設定を行ってください。

# 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：

- 保護対象デバイスの ESS Administrators グループに Kaspersky Embedded Systems Security のユーザーを追加します。
- 保護対象デバイスが Windows ファイアウォールまたはサードパーティのファイアウォールを使用している場合、Kaspersky Security 管理サービス（kavfsgt.exe）のネットワーク接続を許可してください。
- Microsoft Windows が動作しているデバイスへのアプリケーションコンソールのインストール時に［**リモートアクセスを許可する**］をオンにしなかった場合、デバイスのファイアウォールを経由するアプリケーションコンソールのネットワーク接続を手動で許可してください。

リモートデバイス上のアプリケーションコンソールは、DCOM プロトコルを使用して、Kaspersky Embedded Systems Security イベントに関する情報（スキャンされたオブジェクトや完了したタスクなど）を保護対象デバイスの Kaspersky Security 管理サービスから受信します。アプリケーションコンソールと Kaspersky Security 管理サービス間の接続を確立するために、Windows ファイアウォールの設定でアプリケーションコンソールに対してネットワーク接続を許可する必要があります。

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リモートデバイス上で、次を実行します：

- COM アプリケーションへの匿名リモートアクセスが許可されていることを確認します（COM アプリケーションの遠隔起動とアクティベーションは許可しません）。
- 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の実行ファイル（kavfsrcn.exe）に対してネットワーク接続を許可します。

  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デバイスでは、保護対象デバイスへのアクセスと応答の受信に、TCP ポート 135 が使用されます。
- 接続を許可するための Windows ファイアウォールの送信ルールを設定します。

  単一のプロトコルが固定ポートを持つ従来の TCP/IP や UDP/IP とは異なり、DCOM はリモートの COM オブジェクトのポートを動的に割り当てます。ファイアウォールが、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クライアントと DCOM エンドポイント（保護対象デバイス）の間に存在する場合、広範囲のポートを開く必要があります。

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（kavfsrcn.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。
2. ［**スタート**］-［**ファイル名を指定して実行**］の順に選択します。
3. `dcomcnfg` コマンドを入力します。
4. ［**OK**］をクリックします。
5. 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。
6. ［**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。
7. ［**プロパティ**］を選択します。
8. ［**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。
9. ［**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。
10. ［**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. 次のいずれかの処理を実行します：
   - 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**］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. ［**プログラムの追加**］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。

## Windows ファイアウォールの送信ルールの追加

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 ファイアウォールの送信ルールを追加するには：*

1. ［**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。
2. ［**Windows ファイアウォール**］ウィンドウで、［**詳細設定**］をクリックします。
   ［**セキュリティが強化された Windows ファイアウォール**］ウィンドウが開きます。
3. ［**送信の規則**］サブフォルダーを選択します。
4. ［**操作**］ペインで［**新しい規則**］オプションをクリックします。
5. 表示された［**新規の送信の規則ウィザード**］ウィンドウで、［**ポート**］を選択し、［**次へ**］をクリックします。
6. ［**TCP**］プロトコルを選択します。
7. ［**特定のリモートポート**］で、送信接続を許可するための次のポートの範囲を指定します：1024-65535。
8. ［**操作**］ウィンドウで、［**接続を許可する**］を選択します。
9. 新しいルールを保存して、［**セキュリティが強化された Windows ファイアウォール**］ウィンドウを閉じます。

Windows ファイアウォールで、アプリケーションコンソールと Kaspersky Security 管理サービスの間のネットワーク接続が許可されます。

## 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リアルタイム保護を有効にする**］（既定のオプション）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。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。

### Kaspersky Embedded Systems Security データベース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. 定義データベースのアップデートタスクの設定で、アップデート元であるカスペルスキーの HTTP アップデートサーバーまたは FTP アップデートサーバーとの接続を設定します。

2. 定義データベース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. ［**プロパティ**］を選択します。
   ［**アプリケーションの設定**］ウィンドウが表示されます。

3. ［**接続設定**］タブを選択します。

4. ［**プロキシサーバーの設定**］セクションで、［**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。タスクの設定で指定されているユーザー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**ローカルシステム**（**SYSTEM**）ユーザーアカウントで実行されます）。

   - **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を適用する**：基本認証を選択できます。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. ［**アプリケーションの設定**］ウィンドウで［**OK**］をクリックします。

*カスペルスキーのアップデートサーバーとの接続を設定するには、定義データベースのアップデートタスクで次の手順を実行します：*

1. 次のいずれかの方法でアプリケーションコンソールを開始します：

   - 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。［**スタート**］ - ［**すべてのプログラム**］ - ［**Kaspersky Embedded Systems Security**］ - ［**管理ツール**］ - ［**Kaspersky Embedded Systems Security 3.1 コンソール**］の順に選択します。

   - 保護対象デバイス以外でアプリケーションコンソールを起動した場合、次の手順で保護対象デバイスに接続します：

     a. 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。

b. ［**別のコンピューターに接続**］を選択します。

c. ［**保護対象デバイスの選択**］ウィンドウで［**別のデバイス**］を選択し、入力欄に保護対象デバイスのネットワーク名を入力します。

Microsoft Windows のサインインに使用したユーザーアカウントが Kaspersky Security 管理サービスへのアクセス権を持っていない場合、必要なアクセス権のあるユーザーアカウントを指定します。

アプリケーションコンソールウィンドウが開きます。

2. 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。

3. ［**定義データベースのアップデート**］サブフォルダーを選択します。

4. 結果ペインで［**プロパティ**］をクリックします。

5. 表示される［**タスクの設定**］ウィンドウで、［**接続設定**］タブを開きます。

6. ［**プロキシサーバー設定を使用してカスペルスキーのアップデートサーバーに接続する**］を選択します。

7. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

定義データベースのアップデートタスクでのアップデート元との接続設定の内容が保存されます。

*定義データベース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を開き、［**開始**］を選択します。

定義データベースのアップデートタスクが開始されます。

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。

*重要領域の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、［**開始**］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、［**実行ログを開く**］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求められます。

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

1. ［**スタート**］メニューで、［**すべてのプログラム**］-［**Kaspersky Embedded Systems Security**］-［**Kaspersky Embedded Systems Security の変更または削除**］の順に選択します。

   セットアップウィザードの［**インストールの変更、修復、または削除**］ウィンドウが表示されます。

2. ［**コンポーネントセットの変更**］を選択します。［**次へ**］をクリックします。

   ［**カスタムインストール**］ウィンドウが開きます。

3. ［**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：

     - **コンポーネントを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

     - **コンポーネントとサブコンポーネントをローカルハードディスクにインストール**：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で、［**コンポーネントを使用しない**］を選択します。

   ［**次へ**］をクリックします。

4. ［**インストールの準備完了**］ウィンドウで［**インストール**］をクリックし、ソフトウェアコンポーネントのセットの変更を確定します。

5. 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。

   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 の修復を試みることができます。修復は、Kaspersky Embedded Systems Security の現在の設定を保存したうえで行えます。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. ［**スタート**］メニューで、［**すべてのプログラム**］を選択します。
2. ［**Kaspersky Embedded Systems Security**］を選択します。
3. ［**Kaspersky Embedded Systems Security の変更または削除**］を選択します。
   セットアップウィザードの［**インストールの変更、修復、または削除**］ウィンドウが表示されます。
4. ［**インストール済みコンポーネントの修復**］をオンにします。［**次へ**］をクリックします。
   ［**インストール済みコンポーネントの修復**］ウィンドウが表示されます。
5. アプリケーションの設定をリセットし Kaspersky Embedded Systems Security を既定値で復元する場合は、［**インストール済みコンポーネントの修復**］ウィンドウで［**製品の推奨設定を復元する**］をオンにします。［**次へ**］をクリックします。
6. ［**修復準備完了**］ウィンドウで［**インストール**］をクリックし、修復操作を確定します。
7. 修復操作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。

   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。

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。

オペレーティングシステムが UAC 機能（ユーザーアカウント制御）を使用しているか、アプリケーションへのアクセスがパスワードで保護されている場合、Windows コントロールパネルからのアプリケーションのアンインストール、修復およびインストールはできません。

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求められます。

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

1. ［**スタート**］メニューで、［**すべてのプログラム**］を選択します。
2. ［**Kaspersky Embedded Systems Security**］を選択します。
3. ［**Kaspersky Embedded Systems Security の変更または削除**］を選択します。
   セットアップウィザードの［**インストールの変更、修復、または削除**］ウィンドウが表示されます。
4. ［**ソフトウェアコンポーネントの削除**］をオンにします。［**次へ**］をクリックします。
   ［**アンインストールの詳細設定**］ウィンドウが表示されます。
5. 必要に応じて［**アンインストールの詳細設定**］ウィンドウで、次の操作を行います：
   a. 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。
   b. 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。
   c. ［**保存**］をクリックし、復元する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、オブジェクトは次のフォルダーにエクスポートされます：%ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security\Uninstall
   ［**次へ**］をクリックします。
6. ［**アンインストールの準備完了**］ウィンドウで［**アンインストール**］をクリックし、アンインストールを確定します。
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、［**OK**］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

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. ［**スタート**］メニューで、［**すべてのプログラム**］を選択します。
2. ［**Kaspersky Embedded Systems Security**］を選択します。

3. ［**Kaspersky Embedded Systems Security の変更または削除**］を選択します。
   ウィザードの［**インストールの変更、修復、または削除**］ウィンドウが表示されます。
4. ［**ソフトウェアコンポーネントの削除**］をオンにして［**次へ**］をクリックします。
5. ［**アンインストールの準備完了**］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。
   ［**アンインストールの完了**］ウィンドウが表示されます。
6. ［**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。

キーによるインストール設定の指定後、コマンドラインからインストールパッケージ \product\ess_x86.msi または \product\ess_x64.msi を実行することで、Kaspersky Embedded Systems Security のインストールやアンインストール、および Kaspersky Security コンポーネントの追加や削除が行えます。

「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 \product\ess_x86.msi または \product\ess_x64.msi のうち、予備のライセンスがない状態で、保護対象デバイスで実行されているファイルがある場合、Kaspersky Embedded Systems Security は、推奨されている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。

# 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。

32 ビット版の Microsoft Windows を実行する保護対象デバイスでは、配布キットに含まれる接尾語が「x86」のファイルを実行します。64 ビット版の Microsoft Windows を実行する保護対象デバイスでは、配布キットに含まれる接尾語が「x64」のファイルを実行します。

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。

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

*ユーザーの操作を求めずに、推奨されているインストール設定で Kaspersky Embedded Systems Security をインストールするには、次のコマンドを実行します：*

```
\product\setup.exe /s /p EULA=1 /p PRIVACYPOLICY=1
```

Kaspersky Embedded Systems Security を次の設定でインストールできます：

- 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コンポーネントのみをインストールする。
- Kaspersky Embedded Systems Security の開始時にファイルのリアルタイム保護を実行しない。
- Microsoft によってスキャン範囲からの除外が推奨されているファイルを除外しない。

*それには、次のコマンドを実行します：*

```
\product\setup.exe /p ADDLOCAL=Oas /p RUNRTP=0 /p ADDMSEXCLUSION=0
```

## インストールで使用するコマンドの例：msi ファイルを実行

*ユーザーの操作を求めずに、推奨されているインストール設定で Kaspersky Embedded Systems Security 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.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、次のコマンドを実行します：*

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

*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.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てから Kaspersky Embedded Systems Security 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.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:\ESS に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.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

*Kaspersky Embedded Systems Security をインストールして、Kaspersky Embedded Systems Security 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、次のコマンドを実行します：*

```
msiexec /i ess.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、次のコマンドを実行します：*

```
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.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、次のコマンドを実行します：*

```
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リアルタイム保護を有効にする］をオンにしていた場合、デバイス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。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実行できます：

  ```
  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

*アプリケーション起動コントロールコンポーネントは自動的にインストールされます。*

*オンデマンドスキャン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.msi ADDLOCAL=Oas,Ods /qn
```

または

```
\product\setup.exe /s /p ADDLOCAL=Oas,Ods
```

コンポーネントをリストに追加した後、Kaspersky Embedded Systems Security は既存のコンポーネントを再インストールし、指定されたコンポーネントをインストールします。

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

インストールおよび削除するコンポーネントを一覧にすると、Kaspersky Embedded SystemsSecurity はそれに応じてコンポーネントをインストールおよび削除します。

## 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.msi /qn
```

または

- 32 ビットオペレーティングシステムの場合：
  `msiexec /x {941B0F6E-2DFA-4557-90AE-D9DF81E985C2} /qn`

- 64 ビットオペレーティングシステムの場合：
  `msiexec /x {6BF23C65-7BE8-44F8-8B7F-3A6B419F6816} /qn`

*Kaspersky Embedded Systems Security コンソールをアンインストールするには、次のコマンドを実行します：*

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

または

```
msiexec /x {71FB9E57-9F23-4D72-B762-E0314EF3C814} /qn
```

*パスワードによる保護が有効であるデバイスから Kaspersky Embedded Systems Security をアンインストールするには、次のコマンドを実行します：*

- 32 ビットオペレーティングシステムの場合：
  `msiexec /x {941B0F6E-2DFA-4557-90AE-D9DF81E985C2} UNLOCK_PASSWORD=*** /qn`

- 64 ビットオペレーティングシステムの場合：
  `msiexec /x {6BF23C65-7BE8-44F8-8B7F-3A6B419F6816} UNLOCK_PASSWORD=*** /qn`

## リターンコード

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 |
|---|---|
| 1324 | インストール先のフォルダー名に無効な文字が含まれています。 |
| 25001 | Kaspersky Embedded Systems Security をインストールする権限が不十分な場合。アプリケーションをインストールするには、ローカル管理者権限でインストールウィザードを開始してください。 |
| 25003 | このバージョンの Microsoft Windows を実行しているデバイスには Kaspersky Embedded Systems Security をインストールできません。64 ビットバージョンの Microsoft Windows 用のインストールウィザードを開始してください。 |
| 25004 | 互換性のないソフトウェアが検知されました。インストールを続けるには、次のソフトウェアをアンインストールします：<非互換ソフトウェアのリスト>。 |
| 25010 | 指定したパスは、隔離されたオブジェクトの保存に使用できません。 |
| 25011 | 隔離されたオブジェクトを保存するフォルダーの名前に無効な文字が含まれています。 |
| 26251 | パフォーマンスカウンター DLL をダウンロードできません。 |
| 26252 | パフォーマンスカウンター DLL をダウンロードできません。 |
| 27300 | ドライバーをインストールできません。 |
| 27301 | ドライバーをアンインストールできません。 |

| | |
|---|---|
| 27302 | ネットワークコンポーネントをインストールできません。フィルタリングされたデバイス数の、サポートされる最大値に達しました。 |
| 27303 | 定義データベースがありません。 |

# 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

このセクションでは、Kaspersky Security Center を使用した Kaspersky Embedded Systems Security のインストールについての全般的な情報が記載されています。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方法と、製品のインストール後の処理についても説明します。

# 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 の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 \product\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 をインストールするには：*

1. Kaspersky Security Center 管理コンソールを開始します。
2. Kaspersky Security Center 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. インストールパッケージの種別として［**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. 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 ess.kud ファイルを指定します。

   ［**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、［**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［**プライバシーポリシーに従ってデータが処理されて送信されること（第三国への送信を含む）を理解し、同意します**］をオンにします。［**プライバシーポリシーの内容をすべて確認して理解した上で同意する**］をオンにし、インストールを続行します。

   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 で、［**詳細**］フォルダーの下にある［**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。

      ［**インストールするコンポーネント**］設定グループで、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。

   d. インストール先のフォルダーを既定ではないものに指定する場合、フォルダーの名前とパスを［**インストール先フォルダー**］に指定します。

      インストール先フォルダーのパスには、システム環境変数を含むことができます。フォルダーが保護対象デバイスに存在しない場合、フォルダーが作成されます。

   e. ［**インストールの詳細設定**］グループで次の設定を構成します：

      - **インストールの前にサーバーをスキャンする**
      - **製品インストール後にリアルタイム保護を有効にする**
      - **Microsoft によって推奨されているファイルを除外リストに追加する**
      - **カスペルスキーが推奨するファイルを除外リストに追加する**
      - **オペレーティングシステムの起動時に Kaspersky Security サービスの遅延開始を有効にする**

   f. インストールパッケージのプロパティウィンドウで［**OK**］をクリックします。

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 の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［**アプリケーションの設定**］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］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。新しいインストールパッケージの作成ウィザードで、次の操作を行います：

   a. ［**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。

   b. 新しいインストールパッケージ名を入力します。

   c. Kaspersky Embedded Systems Security 配布キットのフォルダーから \console\setup.exe ファイルを選択し、［**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。

   d. 必要な場合、［**実行ファイルのコマンドライン（オプション）**］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、インストール先のフォルダーを変更します。

例として、ヘルプファイルやガイドはインストールせずに、フォルダー C:\KasperskyConsole にあるアプリケーションコンソールのみをインストールする場合は、次のコマンドラインオプションを使用します：

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=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。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。

5. 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。

## Active Directory のグループポリシーを使用した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 のグループポリシーを使用した Kaspersky Embedded Systems Security のインストールとアンインストールについて説明します。グループポリシーを使用して製品をインストールした後で実行する処理についても説明します。

# 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_x86.msi or ess_x64.msi または ess_x86.msi or ess_x64.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. インストールされている Microsoft Windows オペレーティングシステムのバージョンのビット数（32 ビットまたは 64 ビット）に対応する MSI ファイルを、ドメインコントローラーのパブリック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パブリックフォルダーに、次の内容の install_props.json ファイルを作成します。これにより、使用許諾契約書の条件とプライバシーポリシーに同意したことになります。

   ```
   {
   "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してください。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。

eicar.com ファイルには、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、次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出を確認できます。これを確認するには、テスト用ウイルス EICAR 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パブリック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、eicar.com ファイル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、実行ログに「*緊急*」のステータスが割り当てられている。ファイル eicar.com 内の脅威に関する情報がログの新しい行に記録される（実行ログを確認するには、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、**ファイルのリアルタイム保護**タスクを選択します。結果パネルで［**実行ログを開く**］をクリックします）。

  - 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パブリック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ます。

3. 次の操作を実行します：

   a. 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。

   b. ［**簡易スキャン**］サブフォルダーを選択します。

   c. ［**スキャン範囲の設定**］タブで、［**ネットワーク**］フォルダーのコンテキストメニューを開いて、［**ネットワークファイルの追加**］を選択します。

   d. リモートデバイスで、ファイル eicar.com のネットワークパスを UNC（ユニバーサルネーミング規約）形式で入力します。

   e. チェックボックスをオンにして、追加したネットワークのパスをスキャン範囲に含めます。

   f. 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、実行ログに「*緊急*」のステータスが割り当てられている。ファイル eicar.com 内の脅威に関する情報が簡易スキャンタスクのログの新しい行に記録される（実行ログを確認するには、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**］サブフォルダーを展開し、簡易スキャンタスクを選択します。結果パネルで［**実行ログを開く**］をクリックします）。

# アプリケーションインターフェイス

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：

- ローカル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 Cloud 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 の Web コンソールと Cloud 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。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 Cloud コンソール（以降「Cloud コンソール」とも表記）は、組織のネットワークを保護および管理するためのクラウドベースのソリューションです。Kaspersky Security Center Cloud コンソールの詳細については、*Kaspersky Security Center Cloud コンソールのヘルプ*を参照してください。

Web コンソールと Cloud コンソールでは、次のことができます：

- 組織のセキュリティシステムのステータスを監視します。
- ネットワーク内のデバイスにカスペルスキー製品をインストールします。
- インストールされているアプリケーションを管理します。
- セキュリティシステムのステータスに関するレポートを表示します。

# 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。

使用許諾契約書の条件は、次のような方法で確認できます：

- Kaspersky Embedded Systems Security インストール時。
- ファイル license.txt で確認できます。使用許諾契約書は、本製品の配布キットに含まれています。

本製品のインストール中に使用許諾契約書に同意すると、使用許諾契約書の条件に同意したことになります。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。

## ライセンスについて

*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。

有効なライセンスを取得すると、次のサービスを利用できます：

- 使用許諾契約書の条件に基づいた製品の使用
- テクニカルサポート

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*は、製品の購入時に提供される有償のライセンスです。

購入できるライセンスは、Kaspersky Embedded Systems Security 標準ライセンスか、Kaspersky Embedded Systems Security Compliance Edition 拡張ライセンスです。拡張ライセンスには、ファイル変更監視、Windows イベントログ監視、レジストリアクセス監視の 3 つの追加システム検査コンポーネントが含まれています。

製品版ライセンスの有効期間が終了した場合、製品は継続して機能しますが、以下の機能が使用できなくなります：

- Kaspersky Security Network との連携
- Kaspersky Embedded Systems Security の定義データベースのアップデート

試用ライセンスの有効期限が切れても、製品は継続して機能します。**オンデマンドスキャン**と**ファイルのリアルタイム保護**タスクは引き続き使用できますが、これら以外のすべてのタスクと 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ません。ライセンスを削除した場合や、ライセンスが拒否リストに追加された場合も同様に、2 つの機能以外使用できなくなります。

Kaspersky Embedded Systems Security のすべての機能を継続して使用するには、ライセンスを更新する必要があります。

デバイスを最大限に保護するには、有効期間が終了する前にライセンスを更新してください。

予備のライセンスの有効期限が現在のライセンスの有効期限よりも後に設定されていることを確認してください。

## 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（該当する場合）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、現在のライセンスに関する次の情報が含まれます：

- 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製品に関する情報
- ライセンス単位数の上限（たとえば、提供されるライセンスの下でアプリケーションを使用できるデバイス）
- 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、「現在のライセンス」と「予備のライセンス」があります。

*現在のライセンス*は、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または試用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。本製品で使用できる現在のライセンスは、1つのみです。

*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適用されてい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、カスペルスキーによって提供される .key という拡張子の付いたファイルです。ライセンス情報ファイルを使って、ライセンスを追加して製品をアクティベートします。

ライセンス情報ファイルは、Kaspersky Embedded Systems Security の購入時、または Kaspersky Embedded Systems Security の試用版の注文時に、メールで提供されます。

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。

ライセンス情報ファイルは、誤って削除してしまっても復元できます。ライセンス情報ファイルは、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。

ライセンス情報ファイルを復元するには、次のいずれかの操作を行います：

- ご購入元の販売代理店へ問い合わせる。
- カスペルスキーの Web サイトにアクセスし、有効なアクティベーションコードを使用してライセンス情報ファイルを取得します。

## アクティベーションコードについて

*アクティベーションコード*は、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。アクティベーションコードは、Kaspersky Embedded Systems Security の購入時、または Kaspersky Embedded Systems Security の試用版の注文時に、メールで提供されます。

アクティベーションコードを使用して製品をアクティベートするには、Kaspersky のアクティベーションサーバーに接続するためにインターネットアクセスが必要です。

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復元するには、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。

## 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、Kaspersky Embedded Systems Security のインストールの途中で確認できます。インストール後は、配布キット、または［**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を実行している時に、Kaspersky Embedded Systems Security は、一連のデータをローカルで処理し、保護対象コンピューターに保存します。

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、次の表のとおりです。

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 Embedded Systems Security\<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 | アクセスコントロールリスト。 |

| | |
|---|---|
| ティ対策 | |
| 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。
- 保護対象コンピューター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。
- 保護対象コンピューター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、次の表のとおりです。

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 | Kaspersky Embedded Systems Security のすべての機能 |

| | |
|---|---|
| の領域 | |
| 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 Embedded Systems Security\<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、データの処理と保存を行います。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（Kaspersky Embedded Systems Security の各種機能に対するアクセス権限の管理、イベントの登録、Kaspersky Embedded Systems Security のログ）。たとえば、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。

ただし例外として、診断情報のファイル（トレースファイル、ダンプファイル）、Windows イベントログに記録された本製品のイベント、およびエクスポートされた Kaspersky Embedded Systems Security 設定を含むファイルは削除されずに残ります。これらのファイルを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。

Kaspersky Embedded Systems Security のプログラムイベントを含む Windows イベントログは、オペレーティングシステムの標準の方法で削除できます。

## 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設定したパラメータ、Kaspersky Security Center のポリシーのパラメータ、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、次の表のとおりです。

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。

ただし例外として、補助コンポーネントのトレースファイルは削除されずに残ります。これらのファイルを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 がコンピューター上で実行する処理。
- 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。

## 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。

Kaspersky Embedded Systems Security 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。

Kaspersky Embedded Systems Security 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。

Kaspersky Embedded Systems Security 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。

*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、［**ライセンス情報ファイルの追加**］をクリックします。
3. 表示されたウィンドウで、［**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。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規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に連絡することを促されます。

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 プラグインから製品のアクティベーショング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**］をオンにします。
   - ライセンス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。ライセンス情報が［**ライセンス情報**］セクションに表示されます。
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

## ライセンス情報の表示

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。ライセンスには、次のステータスがあります：

- **ライセンスのステータスを確認中** - Kaspersky Embedded Systems Security は、適用された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チェックして、現在のライセンスのステータスに関する応答を待ちます。

- **ライセンスの有効期限** - Kaspersky Embedded Systems Security は指定された日時までアクティベートされています。次の場合にライセンスの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 14 日で、予備のライセンスが適用されていない。
  - 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。
- **ライセンスの有効期間が終了しました** - 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** | アクティベーションコード。アクティベーションコードを使用して製品をアクティベートした場合に、表示されます。 |
| **アクティベーションステータス** | 製品のアクティベーションのステータス情報。［**アクティベーションステータス**］フォルダーの詳細ペインの［**ライセンス**］には、次のステータスが表示されます：<br>• **適用済み** - アクティベーションコードまたはライセンス情報ファイルを使用して製品をアクティベートした場合。<br>• **アクティベーション** - アクティベーションコードを適用してアプリケーション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** | 本製品のアクティベーションに使用されたライセンス。 |
| **ライセンス種別** | ライセンスの種別（製品版または試用版）。 |
| **有効期限** | 現在のライセンスの有効期限の日時。 |
| **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：*処理を実行*または*追加*。 |

*ライセンスの詳細情報を表示するには：*

［**ライセンス**］フォルダーの、展開するライセンスデータの行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。

**ライセンスのプロパティ**ウィンドウの［**全般**］タブでは、現在のライセンスの詳細情報が表示されます。［**詳細設定**］タブでは、お客様の情報と、カスペルスキーまたは Kaspersky Embedded Systems Security を購入した販売店の問い合わせ先の詳細が表示されます（下の表を参照）。

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のプロパティウィンドウで表示されるライセンスの詳細情報

| フィールド | 説明 |
|---|---|
| ［全般］タブ | |
| **識別 ID** | 本製品のアクティベーションに使用されたライセンス。 |
| **ライセンス追加日** | 本製品にライセンスが追加された日付。 |
| **ライセンス種別** | ライセンスの種別（製品版または試用版）。 |
| **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。 |
| **有効期限** | 現在のライセンスの有効期限の日時。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*と表示されます。 |
| **アプリケーション** | その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でアクティベートされたアプリケーションの名前。 |
| **使用範囲** | ライセンスの使用における制限（存在する場合）。 |
| **テクニカルサポート利用可能** | 使用許諾契約書に従ってカスペルスキーまたはいずれかのパートナー企業からテクニカルサポートが提供されるかどうかに関する情報。 |
| ［詳細設定］タブ | |
| **ライセンス情報** | 現在のライセンスの情報。 |
| **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のことがあります。 |
| **所有者情報** | ライセンス所有者の情報：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。 |

## ライセンスの有効期限が切れた場合の機能の制限

現在のライセンスの有効期限が切れた場合、機能コンポーネントに以下の制限が適用されます：

- ファイルのリアルタイム保護タスク、オンデマンドスキャンタスク、およびアプリケーションの整合性チェックタスク以外のすべてのタスクが停止します。
- ファイルのリアルタイム保護、オンデマンドスキャン、およびアプリケーションの整合性チェック以外のすべてのタスクを起動できません。これらのタスクは、古い定義データベースで引き続き実行されます。
- 脆弱性攻撃ブロックが制限されます：

- プロセスは再起動されるまで保護されます。
- 新しいプロセスを保護範囲に追加することはできません。

その他の機能（リポジトリ、ログ、診断情報）は引き続き利用可能です。

## ライセンスの更新

既定で、ライセンスの有効期限までの日数が 14 日になると、期限がまもなく切れる旨の通知が表示されます。この時、［**Kaspersky Embedded Systems Security**］フォルダーの結果ペインの、［**ライセンスの有効期限**］のステータスが黄色にハイライト表示されます。

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**］フォルダーを開きます。
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. ［**ライセンス情報ファイルの追加**］をクリックします。
     b. 表示されたウィンドウで、［**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**］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**］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**］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できます。

Kaspersky Embedded Systems Security に予備のライセンスが追加されている場合、現在のライセンスを削除すると、予備のライセンスが自動的に現在のライセンスになります。

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。

*追加され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。

# 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、管理グループに含ま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することで集中管理できます。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 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 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、アプリケーションの全般的な設定、コンピューターのリアルタイム保護タスクの設定、ローカルアクティビティの管理タスクの設定、およびスケジュールによるローカルシステムタスクの開始設定を編集できます。

- **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作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。

Kaspersky Security Center を使用すると、アプリケーションや高度な機能を設定し、ログや通知を利用できます。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。

# 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 Web 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の情報が記載されています。

# 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。

# 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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］セクションを選択します。
6. 設定のサブセクションで、［**設定**］をクリックします。

# 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、保護対象デバイスのプロパティ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コンテキストメニューで［**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 3.1**］を選択します。

6. ［**プロパティ**］をクリックします。
［**Kaspersky Embedded Systems Security 3.1 のアプリケーション設定**］ウィンドウが表示されます。

7. ［**アプリケーションの設定**］セクションを選択します。

## 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 でのスケーラビリティ、インターフェイスおよびスキャン設定

*スケーラビリティ、インターフェイスおよびスキャン設定を構成するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。

   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**アプリケーションの設定**］セクションの［**スケーラビリティ、インターフェイス、スキャンの設定**］ブロックで、［**設定**］をクリックします。

5. ［**製品の詳細設定**］ウィンドウの［**全般**］タブで、次の設定を行います：

   - ［**スケーラビリティ設定**］セクションで、Kaspersky Embedded Systems Security で使用される処理対象プロセスの数を定義する設定を行います：

     - **スケーラビリティ設定を自動的に検出する**

     - **処理対象プロセスの数を手動で設定する**

       - **実行中プロセスの最大数**

       - **リアルタイム保護の対象プロセスの数**

       - **バックグラウンドのオンデマンドスキャンタスクの対象プロセスの数**

- ［**ユーザーインターフェイス**］セクションで、［**タスクバーにシステムトレイアイコンを表示する**］をオンまたはオフにして、製品のシステムトレイアイコンを通知領域に表示するかどうかの設定を行います。

6. ［**スキャン設定**］タブで、次の設定を行います：
   - **スキャン後にファイル属性を復元する**
   - **スレッドのスキャン時に CPU の使用を制限する**
     - **上限（パーセント）**
   - **スキャン中に作成された一時ファイルのフォルダー**
7. ［**階層型ストレージ**］タブで、階層型ストレージへのアクセスのオプションを選択します。
8. ［**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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**アプリケーションの設定**］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**］ウィンドウで、次の設定を行います：
   - ［**パスワードによる保護の設定**］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**］を有効または無効にします。
   - ［**パスワードによる保護の設定**］セクションで、Kaspersky Embedded Systems Security 機能へのアクセスを保護するパスワードを入力します。
   - ［**セルフディフェンス**］セクションで、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合の、Kaspersky Embedded Systems Security のタスクの復元を設定します。

- **タスク復元を実行する**
- **信頼性設定**

- ［**オンデマンドスキャンタスクの復元回数上限（回）**］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**
  - **現在のスキャンタスクを中止する**
- ［**パスワードによる保護の設定**］セクションで、Kaspersky Embedded Systems Security 機能へのアクセスを保護するパスワードを入力します。

6. ［**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 サービスと統合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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**アプリケーションの設定**］セクションで、［**接続**］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：
   - ［**プロキシサーバーの設定**］セクションで、プロキシサーバーの使用設定を選択します：
     - **プロキシサーバーを使用しない**
     - **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
- **ローカルアドレスへの接続時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、認証設定を指定します：
  - 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。既定では、このモードが選択されます。
    - **NTLM 認証を使用する** - 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。
    - **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を適用する** - ユーザー名とパスワードを使用して認証が行われます。
  - 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。

6. ［**OK**］をクリックします。

接続設定の内容が保存されます。

## ローカルのシステム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、管理グループの各保護対象デバイスで、ローカルで設定されたスケジュールに基づくローカルシステムのオンデマンドスキャンタスクおよびアップデートタスクの起動を許可またはブロックできます：

- 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。

グループ更新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、隔離のスキャン、オペレーティングシステムの起動時にスキャン、アプリケーションの整合性チェック、ベースラインに基づくファイル変更監視。
- アップデートタスク：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、アップデートのコピー。

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. 管理コンソールツリーの［**管理対象デバイス**］フォルダーで、目的のグループを展開し、［**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、［**アプリケーションの設定**］セクションを開きます。［**ローカルシステムタスクの実行**］セクションで［**設定**］をクリックして、次のように実行します：
   - ［**オンデマンドスキャンタスク**］と［**アップデートタスクとアップデートのコピータスク**］をオンにし、リストのタスクに対するスケジュールによる開始を許可します。
   - ［**オンデマンドスキャンタスク**］と［**アップデートタスクとアップデートのコピータスク**］をオフにし、リストのタスクに対するスケジュールによる開始を無効にします。

   チェックボックスをオンにしてもオフにしても、この種のローカルカスタムタスクの開始設定に影響はありません。
4. 設定するポリシーがアクティブで、選択された保護対象デバイスのグループに適用されることを確認します。
5. ［OK］をクリックします。

設定されたタスクのスケジュールの設定が、選択したタスクに適用されます。

## Kaspersky Security Center での隔離およびバックアップ設定

*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**ポリシーのプロパティ**ウィンドウを開きます。

- 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

  Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**詳細設定**］セクションで、［**保管領域**］サブセクションの［**設定**］をクリックします。

5. 必要に応じて、［**バックアップ**］ウィンドウの［**保管領域の設定**］タブを使用して、次のバックアップ設定を行います：

   - バックアップフォルダーを指定するには、［**バックアップフォルダー**］を使用して保護対象デバイスのローカルドライブ上の目的のフォルダーを選択するか、フォルダーの絶対パスを入力します。
   - バックアップの最大サイズを設定するには、［**バックアップの最大サイズ（MB）**］をオンにして、入力フィールドに該当する値（メガバイト単位）を指定します。
   - バックアップの空き容量のしきい値を設定するには：
     - ［**バックアップの最大サイズ（MB）**］の設定値を定義します。
     - ［**空き容量のしきい値（MB）**］を選択します。
     - バックアップフォルダーの空き容量の最小値をメガバイト単位で指定します。
   - 復元されたオブジェクトのフォルダーを指定するには、次のいずれかを実行してください：
     - ［**復元設定**］セクションで、保護対象デバイスのローカルドライブ内の対応するフォルダーを選択します。
     - ［**オブジェクトの復元先フォルダー**］フィールドにフォルダー名と完全パスを入力します。

6. ［**保管領域の設定**］ウィンドウの［**隔離**］タブで、次の隔離設定を行います：

   - 隔離フォルダーを変更するには、［**隔離フォルダー**］で保護対象デバイスのローカルドライブ上のフォルダーへの完全パスを指定します。
   - 隔離の最大サイズを設定するには、［**隔離の最大サイズ（MB）**］をオンにして、入力フィールドにこのパラメータの値（メガバイト単位）を指定します。
   - 隔離の保管領域の最小空き容量を設定するには、［**隔離の最大サイズ（MB）**］と［**空き容量のしきい値（MB）**］をオンにして、入力フィールドにこのパラメータの値（メガバイト単位）を指定します。
   - 隔離されたオブジェクトの復元先フォルダーを変更するには、［**オブジェクトの復元先フォルダー**］で保護対象デバイスのローカルドライブ上のフォルダーへの絶対パスを指定します。

7. ［**OK**］をクリックします。

隔離およびバックアップの設定内容が保存されます。

## 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、および指定され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［**システム監査ログ**］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 アイコンが選択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（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。

また、アクティブポリシーで設定し 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。

ポリシーでコンピューターのリアルタイム保護タスクの設定を定義しており、そのタスクが現在実行中の場合、ポリシーによって定義された設定のいずれかが、ポリシーの適用後すぐに変更されます。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

ポリシーの作成プロセスには、次の手順が含まれます：

1. ポリシーウィザードを使用したポリシーの作成：ウィザードダイアログを使用して、コンピューターのリアルタイム保護タスクを設定できます。

2. ポリシーの設定：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タスクの設定、Kaspersky Embedded Systems Security の全般設定、隔離とバックアップの設定、実行ログの詳細レベル、および Kaspersky Embedded Systems Security のイベントに関するユーザー通知と管理者への通知を定義することができます。

*インストールした Kaspersky Embedded Systems Security を実行す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：*

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詳細ペインで［**ポリシー**］タブを選択し、［**ポリシーの作成**］をクリックして、ウィザードを開始してポリシーを作成します。

   ［**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 を選択して［**次へ**］をクリックします。

4. ［**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：" * < : > ? \ | 。

5. 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**］をオンにします。

   b. ［**選択**］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。

6. ［**処理の選択**］ウィンドウで、次の値のいずれかを選択します：

   - ［**新規**］：既定の設定を使用した新しいポリシーを作成します。
   - **旧バージョンの Kaspersky Embedded Systems Security で作成したポリシーをインポート**：インポートしたポリシーをテンプレートとして使用します。
   - ［**参照**］をクリックして、既存のポリシーの設定ファイルを選択します。

7. ［**コンピューターのリアルタイム保護**］ウィンドウで、必要に応じてファイルのリアルタイム保護と KSN の使用タスク、脆弱性攻撃ブロックとスクリプト監視の設定を行います。ネットワークにある保護対象デバイスでの設定済みのポリシータスクの使用を許可またはブロックします：

   - をクリックすると、ネットワークの保護対象デバイスのタスク設定の変更を許可し、ポリシーで編集されたタスク設定の適用をブロックします。
   - をクリックすると、ネットワークの保護対象デバイスのタスク設定の変更を拒否し、ポリシーで編集されたタスク設定の適用を許可します。

   新たに作成されたポリシーでは、コンピューターのリアルタイム保護タスクの既定の設定を使用します。

   - ファイルのリアルタイム保護タスクの既定の設定を編集するには、［**設定**］サブセクションの［**ファイルのリアルタイム保護**］をクリックします。表示されるウィンドウで、要件に応じてタスクの設定を行います。［**OK**］をクリックします。
   - KSN の使用タスクの既定の設定を編集するには、［**設定**］サブセクションの［**KSN の使用**］をクリックします。表示されるウィンドウで、要件に応じてタスクの設定を行います。［**OK**］をクリックします。

     KSN の使用タスクを開始するには、［**KSN データの取り扱い**］ウィンドウで KSN に関する声明に同意する必要があります。

- 脆弱性攻撃ブロックコンポーネントの既定の設定を編集するには、［**設定**］サブセクションの［**脆弱性攻撃ブロック**］をクリックします。表示されるウィンドウで、必要に応じて機能の設定を行います。［OK］をクリックします。

8. ［**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。

   - ［**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。

9. ［**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。

# Kaspersky Embedded Systems Security ポリシー設定のセクション

## 全般

［**全般**］セクションでは、次のポリシー設定を編集できます：

- ポリシーのステータスの指定。
- 親ポリシーから子ポリシーへ継承する設定の指定。

## イベント通知

［**イベントの設定**］セクションでは、次のイベントカテゴリの設定を行えます：

- *緊急*
- *機能エラー*
- *警告*
- *情報*
  ［**プロパティ**］を使用して、選択したイベントに対して次を設定できます：
- 記録したイベントの保管場所と保管期間の指定
- 記録したイベントの通知方法の指定

## アプリケーションの設定

［アプリケーションの設定］セクションの設定

| | |
|---|---|

| セクション | オプション |
| --- | --- |
| **スケーラビリティ、インターフェイス、スキャンの設定** | ［**スケーラビリティ、インターフェイス、スキャンの設定**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• スケーラビリティ設定を自動と手動のいずれで設定するかを選択<br>• 製品アイコンの表示設定 |
| **セキュリティと信頼性** | ［**セキュリティと信頼性**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• タスク実行の設定<br>• UPS 電源による保護対象デバイスの実行時のアプリケーションの挙動の指定<br>• アプリケーション機能のパスワードによる保護の有効化または無効化 |
| **接続** | ［**接続**］サブセクションで［**設定**］を使用して、アップデートサーバー、アクティベーションサーバー、および KSN に接続するためのプロキシサーバーの次の設定を行えます：<br>• プロキシサーバーの設定<br>• プロキシサーバーの認証設定の指定 |
| **ローカルシステムタスクの実行** | ［**ローカルシステムタスクの実行**］サブセクションで［**設定**］をクリックして、保護対象デバイスで設定されているスケジュールに応じた次のシステムタスクの起動を許可またはブロックできます：<br>• オンデマンドスキャンタスク<br>• アップデートタスクおよびアップデートのコピータスク |

## 詳細設定

［詳細設定］セクションの設定

| セクション | オプション |
| --- | --- |
| **信頼ゾーン** | ［**信頼ゾーン**］サブセクションの［**設定**］をクリックして、次の信頼ゾーンの設定を編集します：<br>• 信頼ゾーンの除外リストの作成<br>• ファイルのバックアップ処理のスキャンの有効化または無効化<br>• 信頼するプロセスのリストの作成 |
| **リムーバブルドライブスキャン** | ［**リムーバブルドライブスキャン**］サブセクションで［**設定**］をクリックして、リムーバブルドライブのスキャンを設定できます。 |
| **アプリケーション管理用のユーザーアクセス権限** | ［**アプリケーション管理用のユーザーアクセス権限**］サブセクションで、ユーザー権限およびユーザーグループ権限を設定して Kaspersky Embedded Systems Security を管理できます。 |
| **Kaspersky Security サービス管理用のユーザ** | ［**Kaspersky Security サービス管理用のユーザーアクセス権限**］サブセクションで、ユーザー権限およびユーザーグループ権限を設定して Kaspersky |

| | |
|---|---|
| **ーアクセス権限** | Security サービスを管理できます。 |
| **保管領域** | ［**保管領域**］サブセクションで［**設定**］をクリックして、次の隔離設定、バックアップ設定、ブロック対象コンピューターの設定を編集します：<br>• 隔離オブジェクトまたはバックアップオブジェクトを配置するフォルダーのパスの指定<br>• バックアップと隔離の最大サイズの設定および空き容量のしきい値の指定<br>• 隔離またはバックアップから復元するオブジェクトの配置先となるフォルダーのパスの指定<br>• ホストがブロックされる時間の設定 |

## コンピューターのリアルタイム保護

［コンピューターのリアルタイム保護］セクションの設定

| セクション | オプション |
|---|---|
| **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**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• 保護範囲の指定<br>• ヒューリスティックアナライザーの使用設定<br>• 信頼ゾーンの使用設定<br>• 保護範囲の指定<br>• 選択した保護範囲のセキュリティレベルの設定（定義済みのセキュリティレベルの選択または手動によるセキュリティレベルの設定）<br>• タスク開始の設定 |
| **KSN の使用** | ［**KSN の使用**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• KSN で信頼されていないオブジェクトに対する処理の指定。<br>• データ転送と、Kaspersky Security Center の KSN プロキシサーバーとしての使用を設定します。<br>［**データの処理**］をクリックして、KSN 声明に同意するか同意しないかを選択し、データ交換方法を設定します。 |
| **脆弱性攻撃ブロック** | ［**脆弱性攻撃ブロック**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• プロセスメモリの保護モードを選択<br>• 脆弱性攻撃リスクを低下させる処理を指定<br>• 保護対象プロセスのリストを追加して編集 |

## ローカル活動の管理

［ローカルアクティビティの管理］セクションの設定

| セクション | オプション |
| --- | --- |
| **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**］サブセクションで［**設定**］を使用して、次のタスク設定を行えます：<br>• タスク処理モードの選択<br>• 次回以降のアプリケーション起動に対するコントロールの適用設定<br>• アプリケーション起動コントロールルールの範囲の指定<br>• KSN の使用設定<br>• タスク開始の設定 |
| **デバイスコントロール** | ［**デバイスコントロール**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• タスク処理モードの選択<br>• タスク開始の設定 |

## ネットワーク活動の管理

［ネットワークアクティビティの管理］セクションの設定

| セクション | オプション |
| --- | --- |
| **ファイアウォール管理** | ［**ファイアウォール管理**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• ファイアウォールのルールの設定<br>• タスク開始の設定 |

## システム監査

［システム監査］セクションの設定

| セクション | オプション |
| --- | --- |
| **ファイル変更監視** | ［**ファイル変更監視**］サブセクションで、保護対象デバイスにおける、セキュリティ侵害の可能性があるファイル変更の管理を設定できます。 |
| **Windows イベントログ監視** | ［**Windows イベントログ監視**］セクションで、Windows イベントログ分析の結果に基づいて、保護対象デバイスの整合性管理を設定できます。 |

## ログと通知

［ログと通知の設定］セクションの設定

| セクション | オプション |
| --- | --- |

| | |
|---|---|
| **実行ログ** | ［**実行ログ**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• 選択したソフトウェアコンポーネントの記録されたイベントに対する重要度の指定<br>• 実行ログのストレージ設定の指定<br>• Kaspersky Security Center 設定と SIEM との統合の指定 |
| **イベント通知** | ［**イベント通知**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• ［*オブジェクトが検知されました*］イベント、［*信頼しない外部デバイスが検出および制限されました*］イベント、［*コンピューターが信頼しないリストに追加されました*］イベントのユーザーへの通知設定の指定<br>• ［**通知設定**］セクションのイベントリストで選択したイベントの管理者への通知設定の指定 |
| **管理サーバーとのインタラクション** | ［**管理サーバーとのインタラクション**］セクションで［**設定**］をクリックして、Kaspersky Embedded Systems Security が管理サーバーに報告するオブジェクトの種別（隔離オブジェクトとバックアップのオブジェクトを含む）を選択できます。 |

### 変更履歴

［**変更履歴**］セクションでは、次のようにしてリビジョンを管理できます：現在のリビジョンや他のポリシーとの比較、リビジョンの説明の追加、ファイルへのリビジョンの保存、ロールバックの実行など。

## ポリシーの設定

既存のポリシーの［**プロパティ： <ポリシー名>**］ウィンドウで、以下を設定することができます：

- 全般的な Kaspersky Embedded Systems Security の設定
- 隔離とバックアップの設定
- 信頼ゾーン、コンピューターのリアルタイム保護、ローカルアクティビティの管理設定
- タスクログの詳細レベル
- Kaspersky Embedded Systems Security イベントに関するユーザーおよび管理者への通知
- 製品および Kaspersky Security サービスを管理するためのアクセス権限

*ポリシー設定を行うには：*

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. 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. 次の方法の 1 つを使用して、設定するポリシーを選択し、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。

- 選択したポリシーの右の詳細ペインで、［**ポリシーの設定**］をクリックする。
- 選択されたポリシーをダブルクリックする。

4. ［**全般**］セクションの［**ポリシーのステータス**］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。
   - **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。

   **モバイルユーザーポリシー**は、Kaspersky Embedded Systems Security を管理している場合は使用できません。

5. ［**イベントの設定**］、［**アプリケーションの設定**］、［**詳細設定**］、［**ログと通知**］、［**変更履歴**］の各セクションで、アプリケーション設定を変更できます（次の表を参照）。
6. ［**コンピューターのリアルタイム保護**］、［**ローカル活動の管理**］、［**ネットワーク活動の管理**］、および［**システム監査**］の各セクションで、アプリケーション設定およびアプリケーション起動設定を設定します（次の表を参照）。

   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。

7. ［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。

## 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。

- 製品のアクティベーション
- 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
- 定義データベースのロールバック
- オンデマンドスキャン
- アプリケーションの整合性チェック
- ベースラインファイル変更監視
- アプリケーション起動コントロールルールの自動作成
- デバイスコントロールルールの自動作成

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：

- 1台の保護対象デバイスの場合、保護対象デバイスのプロパティウィンドウの［**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結果ペインの［**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**］フォルダーの結果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、保護対象デバイス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。
   - 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、［**タスクの作成**］を選択します。

- 保護対象デバイスのカスタムセットに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. 保護対象デバイスを含む管理グループを選択します。

  c. 保護対象デバイスまたは保護対象デバイスのカスタムセットを選択します。

  d. ［**処理を実行**］ドロップダウンリストで、［**タスクの作成**］オプションを選択します。

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 3.1**］ヘッダーで、作成するタスクの種別を選択します。

3. 定義データベースのロールバック、アプリケーションの整合性チェック、製品のアクティベーションのいずれか以外のタスク種別を選択した場合、［**設定**］ウィンドウが開きます。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**］ウィンドウでアップデート元を選択します。

  b. ［**接続設定**］をクリックします。［**接続設定**］ウィンドウが表示されます。

  c. ［**接続設定**］ウィンドウで：

  保護対象デバイスに接続するための FTP サーバーモードを指定します。

  必要に応じて、アップデート元に接続する際の接続のタイムアウトを変更します。

  アップデート元に接続する際のプロキシサーバーアクセス設定を行います。

  保護対象デバイスの場所を指定し、アップデートのダウンロードを最適化します。

- ソフトウェアモジュールのアップデートタスクを作成するには、［**ソフトウェアモジュールのアップデートの設定**］ウィンドウで、必要なアプリケーションモジュールのアップデート設定を行います：

  a. 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してインストールするか、インストールはせずに使用可能かどうかのチェックだけを行うかを選択します。

  b. ［**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しインストールする**］を選択すると、インストールされたソフトウェアモジュールを適用するために、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。タスクの完了時に保護対象デバイスが自動的に再起動するようにしたい場合は、［**システムの再起動を許可する**］をオンにします。

  c. Kaspersky Embedded Systems Security のモジュールのアップグレードに関する情報を入手するには、［**適用可能になったソフトウェアモジュールの定期アップデートの情報を受信する**］をオンにします。

  カスペルスキーは、自動インストール用の定期的なアップデートパッケージをアップデートサーバーで公開していません。これらのパッケージは、カスペルスキーの Web サイトから手動でダウンロードできます。［**ソフトウェアモジュールの新しい定期アップデートが適用可能です**］イベントに関する管理者への通知を設定できます。これには、定期アップデートをダウンロードできるカスペルスキーの Web サイトの URL が含まれます。

- アップデートのコピータスクを作成するには、［**アップデートのコピーの設定**］ウィンドウでアップデートとインストール先フォルダーを指定します。
- 製品のアクティベーション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、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。
  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作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作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。
   ［定義データベースのロールバック］以外のすべてのタスク種別のスケジュールを設定できます。
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、タスクを実行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. ［**タスクの作成を終了**］ウィンドウで以下の処理を実行します：
   a. 作成された後すぐにタスクを開始する場合は［**ウィザードの完了後にタスクを実行する**］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。

## 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

*1 台のネットワークの保護対象デバイスに対してローカルタスクの設定またはアプリケーション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、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、保護対象デバイスのプロパティ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。

4. ローカルタスクを設定するには、次の手順を実行します：

   a. ［**タスク**］セクションに進みます。

   b. タスクのリストで、設定するローカルタスクを選択します。

   - タスクのリストで、タスク名をダブルクリックします。
   - タスク名を選択して［**プロパティ**］をクリックします。
   - 選択されたタスクのコンテキストメニューで、［**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。

5. アプリケーションの設定を行うには、次の手順を実行します：

   a. ［**アプリケーション**］セクションに進みます。

   b. インストール済みのアプリケーションのリストで、設定するアプリケーションを選択します。

   - インストール済みのアプリケーションのリストで、アプリケーション名をダブルクリックします。
   - インストール済みのアプリケーションのリストで、アプリケーション名を選択して［**プロパティ**］をクリックします。
   - インストール済みのアプリケーションのリストで、アプリケーション名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。

   ［**<アプリケーション名> の設定**］ウィンドウが表示されます。

   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、［**<アプリケーション名> の設定**］ウィンドウでこれらの設定を編集することはできません。

## Kaspersky Security Center でのグループタスクの設定

Kaspersky Security Center Cloud コンソールから Kaspersky Embedded Systems Security を管理する場合、カスタム HTTP や 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することはできません。

*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、タスクのプロパティ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。

［**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方法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. 設定したタスクの種別に従って、次のいずれかの処理を実行します：
   - オンデマンドスキャン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。
     - ［**オプション**］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統合を設定します。
   - 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行います：
     - ［**設定**］セクションで、アップデート元の設定とディスクサブシステムの最適化を設定します。
     - ［**接続設定**］をクリックして、アップデート元の接続を設定します。
   - ソフトウェアモジュールのアップデートタスクを設定するには：
     - ［**ソフトウェアモジュールのアップデートの設定**］セクションに移動します。
     - 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。
   - アップデートのコピータスクを設定する場合は、［**アップデートのコピーの設定**］セクションでアップデートとインストール先フォルダーを指定します。
   - 製品のアクティベーションタスクを設定するには：
     - ［**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作成を設定するには、［**設定**］セクションで、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。
6. ［**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。定義データベースのロールバック以外のすべてのタスク種別にスケジュールを設定することができます。
7. ［**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。
8. 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。

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。

新たに設定したタスクの内容が保存されます。

設定可能なグループタスクの設定について、次の表に概要を示します。

Kaspersky Embedded Systems Security グループタスクの設定

| Kaspersky Embedded Systems Security タスクの種別 | タスクのプロパティウィンドウ内のセクション | 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作成 | **設定** | アプリケーション起動コントロールルールの自動作成タスクの設定時に、許可ルールの作成方法を選択できます：<br>• **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**<br>• **次のフォルダーにあるアプリケーションに対する許可ルールを作成する** |
| | **オプション** | アプリケーション起動コントロール許可ルールの作成中に実行する処理を指定できます：<br>• **デジタル証明書を使用する**<br>• **デジタル証明書の発行先とサムプリントを使用する**<br>• **証明書がない場合に使用**<br>• **SHA256 ハッシュを使用する**<br>• **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作成**<br>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、設定ファイルの設定ができます。 |
| | **スケジュール** | タスクのスケジュールを設定できます。 |
| デバイスコントロールルールの自動作成 | **設定** | • 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。<br>• 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、設定ファイルを設定します。 |
| | **スケジュール** | スケジュールでタスクを開始する設定を指定できます。 |
| 製品のアクティベーション | **アクティベーション設定** | 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を追加します。 |
| | **スケジュ** | スケジュールでタスクを開始する設定を指定できます。 |

| | | |
|---|---|---|
| | **ール** | |
| アップデートのコピー | **アップデート元** | 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。<br>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。 |
| | ［**接続設定**］ウィンドウ | ［**アップデート元**］セクションからリンクされた［**接続設定**］ウィンドウで、カスペルスキーのアップデートサーバーまたはその他のサーバーへの接続を確立するために、プロキシサーバーを使用すべきかどうかを指定できます。 |
| | **アップデートのコピーの設定** | コピーするアップデートを指定できます。<br>［**コピーしたアップデートのローカル用保存フォルダー**］で、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。 |
| | **スケジュール** | スケジュールでタスクを開始する設定を指定できます。 |
| 定義データベースのアップデート | **設定** | ［**アップデート元**］セクションで、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。<br>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。<br>［ディスク I/O 使用の最適化］セクションで、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：<br>• **ディスク I/O の負荷の低減**<br>• **最適化に使用するメモリ（MB）** |
| | ［**接続設定**］ウィンドウ | ［**アップデート元**］セクションからリンクされた［**接続設定**］ウィンドウで、カスペルスキーのアップデートサーバーまたはその他のサーバーへの接続を確立するために、プロキシサーバーを使用すべきかどうかを指定できます。 |
| | **スケジュール** | スケジュールでタスクを開始する設定を指定できます。 |
| ソフトウェアモジュールのアップデート | **アップデート元** | 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。 |
| | ［**接続設定**］ウィンドウ | ［**アップデート元への接続設定**］セクションで、カスペルスキーのアップデートサーバーまたはその他のサーバーへの接続を確立するために、プロキシサーバーを使用すべきかどうかを指定できます。 |
| | **ソフトウェアモジュールのアップデートの設定** | ソフトウェアモジュールの重要なアップデートが適用可能な場合または既にインストール済みの場合に実行する処理を指定できます。定期アップデートに関する情報を受信するかどうかの指定も行えます。 |
| | **スケジュール** | 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の設定 | **スキャン範囲** | 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。 |
| | ［**オンデマンドスキャンの設定**］ウィンドウ | ［**スキャン範囲**］セクションからリンクされた［**オンデマンドスキャンの設定**］ウィンドウでは、定義済みのセキュリティレベルのいずれかを選択したり、セキュリティレベルを手動でカスタマイズできます。 |
| | **オプション** | ［**ヒューリスティックアナライザー**］セクションで、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できます。また、スライダーを使用して分析レベルを設定できます。<br>［**他のコンポーネントとの連携**］セクションで、次の設定を行えます：<br>• オンデマンドスキャンタスクでの信頼ゾーンの適用。<br>• オンデマンドスキャンタスクでの KSN の使用の適用。<br>• オンデマンドスキャンタスクの優先度の設定：バックグラウンドモードでタスクを実行する（優先度「低」）か、またはタスクを簡易スキャンとします。 |
| | **スケジュール** | 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 | **スケジュール** | スケジュールでタスクを開始する設定を指定できます。 |

| | | |
|---|---|---|
| の整合性チェック | | |
| ベースラインファイル変更監視 | **スケジュール** | 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。

## 製品のアクティベーションタスク

*製品のアクティベーション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、タスクのプロパティ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。

   ［**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方法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。ライセンスを延長するためにライセンスを追加する時は、［**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（定義データベース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）。
7. ［**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。
8. 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。

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。

   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

*アップデートのコピー、定義データベースのアップデート、またはソフトウェアモジュールのアップデートの各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、タスクのプロパティ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。

［**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方法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. ［**アップデート元**］セクションで、次の操作を実行します：

   a. 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. ［**接続設定**］をクリックします。

c. 表示された［**接続設定**］セクションで、カスペルスキーのアップデートサーバーおよびその他のサーバーに接続するためのプロキシサーバーの使用を設定します。

d. 定義データベースのアップデートタスクは、［**ディスク I/O 使用の最適化**］セクションで、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 使用の最適化**］セクションは定義データベースのアップデートタスクに対してのみ使用可能です。

- **ディスク I/O の負荷の低減**
- **最適化に使用するメモリ（MB）**

6. ソフトウェアモジュールのアップデートの設定については、［**ソフトウェアモジュールのアップデートの設定**］セクションで、重要なアップデートが適用可能なとき、またはアップデートが適用予定であることを示す情報があるときに Kaspersky Embedded Systems Security が実行する操作を指定します。

重要なアップデートがインストールされたときに Kaspersky Embedded Systems Security が実行する操作を指定することも可能です。

［**ソフトウェアモジュールのアップデートの設定**］セクションは、ソフトウェアモジュールのアップデートタスクに対してのみ使用可能です。

7. アップデートのコピータスクには、［**アップデートのコピーの設定**］セクションでアップデートとコピー先フォルダーを指定します。

［**アップデートのコピーの設定**］セクションはアップデートのコピータスクに対してのみ使用可能です。

8. ［**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（定義データベース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）。

9. ［**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。

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。

定義データベース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

*アプリケーションの整合性チェック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、タスクのプロパティ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。

   ［**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方法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. ［**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。
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（定義データベース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）。
7. ［**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。
8. 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。
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。

   新たに設定したタスクの内容が保存されます。

## クラッシュの診断設定

Kaspersky Embedded Systems Security の動作中に、製品がクラッシュするなどの問題が発生した場合、診断することができます。診断するには、Kaspersky Embedded Systems Security プロセスのトレースファイルやダンプファイルの作成を有効にし、作成したファイルを解析のため Kaspersky Technical Support に提出します。

Kaspersky Embedded Systems Security からは、トレースファイルまたはダンプファイルは自動的に送信されません。診断データは、必要な権限を持つユーザーのみが送信できます。

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ユーザーが選択し、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。

*クラッシュの診断を設定するには：KAVSHELL DUMP コマンドを使用するか、アプリケーションコンソール上で次の操作を実行します。*

1. Kaspersky Security Center 管理コンソールで、［**アプリケーションの設定**］を開きます。
2. ［**トラブルシューティング**］セクションを開きます。
3. デバッグ情報をファイルに書き込む場合は、［**デバッグ情報をトレースファイルに書き込む**］をオンにします。
4. 下にあるフィールドで、トレースファイルを保存するフォルダーを指定します。
5. デバッグ情報の詳細レベルを設定します。
6. トレースファイルの最大サイズを指定します。
7. 1つのトレースログの最大ファイル数を指定します。

   Kaspersky Embedded Systems Security は、デバッグするコンポーネントごとに最大数のトレースファイルを作成します。

8. デバッグするコンポーネントを指定します。コンポーネントコードを複数指定する場合は、セミコロンで区切る必要があります。コードは大文字と小文字が区別されます（次の表を参照）。

Kaspersky Embedded Systems Security サブシステムコード

| コンポーネントコード | コンポーネントの名前 |
|---|---|
| * | すべてのコンポーネント |
| gui | ユーザーインターフェイスサブシステム、Microsoft 管理コンソール形式の Kaspersky Embedded Systems Security スナップイン |
| ak_conn | ネットワークエージェントと Kaspersky Security Center の統合のためのサブシステム |
| bl | コントロールプロセス、Kaspersky Embedded Systems Security コントロールタスクの実装 |
| wp | アンチウイルスによる保護タスクを処理する処理対象プロセス |
| blgate | Kaspersky Embedded Systems Security リモート管理プロセス |
| ods | オンデマンドスキャンサブシステム |
| oas | ファイルのリアルタイム保護サブシステム |
| qb | 隔離およびバックアップのサブシステム |
| scandll | スキャンのための補助モジュール |
| core | アンチウイルス基本機能のためのサブシステム |
| avscan | アンチウイルス処理サブシステム |

| | |
|---|---|
| avserv | アンチウイルスのカーネルの管理のためのサブシステム |
| prague | 基本機能のためのサブシステム |
| updater | 定義データベースとソフトウェアモジュールをアップデートするためのサブシステム |
| snmp | SNMP プロトコルサポートサブシステム |
| perfcount | パフォーマンスカウンターサブシステム |

Kaspersky Embedded Systems Security スナップインのトレース設定（gui）および Kaspersky Security Center の管理プラグインのトレース設定（ak_conn）は、それらのコンポーネントの再起動後に適用されます。SNMP プロトコルサポートサブシステムのトレース設定（snmp）は、SNMP サービスが再起動された後に適用されます。パフォーマンスカウンターサブシステムのトレース設定（perfcount）は、パフォーマンスカウンターを使用するすべてのプロセスが再起動された後に適用されます。その他の Kaspersky Embedded Systems Security サブシステムのトレース設定は、クラッシュの診断設定が保存されるとすぐに適用されます。

既定値で、Kaspersky Embedded Systems Security は、すべての Kaspersky Embedded Systems Security コンポーネントのデバッグ情報をログに記録します。

この入力フィールドは、［**デバッグ情報をトレースファイルに書き込む**］をオンにすると使用可能になります。

9. ダンプファイルを作成する場合は、［**ダンプファイルの作成**］をオンにしてください。
10. 下にあるフィールドで、ダンプファイルを保存するフォルダーを指定します。
11. ［**OK**］をクリックします。

アプリケーションの設定内容が保護対象デバイスに適用されます。

# 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、タスクのプロパティ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. ［**スケジュール設定**］セクションで、［**スケジュールに従って実行する**］をオンにします。

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。

7. 要件に従ってスケジュールを設定します。それには、次の操作を実行します：

a. ［**頻度**］リストでは、次の値のいずれかを選択します：

- ［**時間単位**］：指定された時間間隔でタスクを実行する場合は、［**間隔：<数字> 時間**］で時間数を指定します。
- ［**日単位**］：指定された日間隔でタスクを実行する場合は、［**間隔：<数字> 日**］で日数を指定します。
- ［**週単位**］：指定された週間隔でタスクを実行する場合は、［**間隔：<数字> 週**ごと］で週数を指定します。タスクを開始する曜日を指定します（既定では、タスクは月曜日に実行されます）。
- ［**アプリケーションの起動時**］：Kaspersky Embedded Systems Security が起動するたびにタスクを実行します。
- ［**定義データベースのアップデート後**］：定義データベースのアップデート後にタスクを実行します。

b. ［**開始時刻**］にタスクを最初に開始する時刻を指定します。

c. ［**開始日**］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、［**タスクの設定**］ウィンドウを開きます。ウィンドウの上部にある［**次回開始**］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、［**次回開始**］には［**ポリシーによりブロック**］と表示されます。

8. ［**詳細設定**］タブを使用して、要件に従って以下のスケジュール設定を指定します：

- ［**タスクの停止設定**］セクション：

a. ［**経過時間**］をオンにして、タスクの最長実行時間を時間と分で右側のフィールドに入力します。

b. ［**一時停止**］をオンにして、タスクの実行が一時停止される時間帯の開始と終了の値（24 時間で指定）を右側のフィールドに入力します。

- ［**詳細設定**］セクション：

a. ［**スケジュール終了日**］をオンにして、スケジュールの適用を停止する日付を指定します。

b. ［**スキップしたタスクを実行する**］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。

c. ［**タスクの開始時刻を次の期間内でランダム化する**］をオンにして、値を分で指定します。

9. ［**OK**］をクリックします。

10. ［**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、タスクのプロパティ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. 次のいずれかを行います：
   - 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、［**スケジュールに従って実行する**］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無効にする場合は、［**スケジュールに従って実行する**］をオフにします。

     設定されたタスク開始のスケジュール設定は削除されず、次回のタスク開始スケジュールで適用されます。
7. ［**OK**］をクリックします。
8. ［**適用する**］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*、*誤動作*、*未インストール*、*開始中*。

［*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**］タブを開きます。

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（統計のみ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。

*統計のみ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統計のみ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**］タブを開きます。

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**］タブを開きます。

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。

## Kaspersky Embedded Systems Security コンソールについて

Kaspersky Embedded Systems Security コンソールは、Microsoft 管理コンソールに追加できる独立したスナップインです。

アプリケーションの管理は、企業ネットワーク内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を使用して行えます。

アプリケーションコンソールの別のデバイスへのインストール後に、追加の設定が必要です。

別のドメインに割り当てられた保護対象デバイスにアプリケーションコンソールおよび Kaspersky Embedded Systems Security をインストールすることができます。この場合、本製品からアプリケーションコンソールへの情報の送信に制限が発生する可能性があります。たとえば、アプリケーションタスクが開始されても、アプリケーションコンソールではそのステータスが変更されないままの場合があります。

アプリケーションコンソールのインストール時に、インストールウィザードによって、インストールフォルダーにファイル kavfs.msc が作成され、Kaspersky Embedded Systems Security スナップインが独立した Microsoft Windows スナップインのリストに追加されます。

アプリケーションコンソールは、［**スタート**］メニューから起動できます。Kaspersky Embedded Systems Security スナップインである msc ファイルを実行したり、Microsoft 管理コンソールにツリーの新しい要素として追加したりすることができます。

64 ビット版の Microsoft Windows では、Kaspersky Embedded Systems Security スナップインを 32 ビット版の Microsoft 管理コンソールにのみ追加できます。Kaspersky Embedded Systems Security スナップインを追加するには、コマンドラインから「mmc.exe /32」というコマンドを実行して Microsoft 管理コンソールを開きます。

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することができます。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。

## 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

Kaspersky Embedded Systems Security コンソールは、Microsoft 管理コンソールツリーにフォルダーの形式で表示されます。

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、アプリケーションがインストールされた保護対象デバイスの名前、および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>**。アプリケーション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。

## アプリケーションコンソールツリー

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**：コンピューターのリアルタイム保護タスクと KSN サービスを管理します。［**コンピューターのリアルタイム保護**］フォルダーでは、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**
  - **KSN の使用**
  - **脆弱性攻撃ブロック**
- **コンピューターの管理**：保護対象デバイスにインストールされたアプリケーションの起動や外部デバイスの接続を制御します。［**コンピューターコントロール**］フォルダーでは、次のタスクを設定できます：
  - **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**
  - **ファイアウォール管理**
- **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作成を設定します。
  - **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**
  - ルール作成グループタスク **<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。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することはできません。
- **システム監査**：ファイル動作コントロールと Windows イベントログ監視を設定します。
  - **ファイル変更監視**
  - **Windows イベントログ監視**
- **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：
  - **オペレーティングシステムの起動時にスキャン**
  - **簡易スキャン**

- **隔離のスキャン**
- **アプリケーションの整合性チェック**
- 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 データベースおよびモジュールのアップデートを管理し、アップデートをローカルアップデートソースフォルダーにコピーします。このフォルダーには、各アップデートタスクを管理するためのサブフォルダーと、最後の**定義データベースのロールバック**が含まれています：
  - **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**
  - **アップデートのコピー**
  - **定義データベースのロールバック**

  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**：隔離とバックアップの設定を管理します。
  - **隔離**
  - **バックアップ**
- **ログと通知**：ローカルタスクログ、セキュリティログ、および Kaspersky Embedded Systems Security システム監査ログを管理します。
  - **セキュリティログ**
  - **システム監査ログ**
  - **実行ログ**
- **ライセンス**：Kaspersky Embedded Systems Security のライセンス情報ファイル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の有効期限日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、次の操作を行えます：

- **別のコンピューターに接続**：別のデバイスにインストールされている Kaspersky Embedded Systems Security を管理するには、そのデバイスに接続します。［**Kaspersky Embedded Systems Security**］フォルダーの詳細ペインの右下にあるリンクをクリックして、この操作を実行することもできます。
- **サービスの起動 / サービスの停止**：アプリケーションまたは選択したタスクを開始または停止します。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。また、これらの操作をアプリケーションの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。
- **リムーバブルドライブスキャンを設定**：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。
- **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。
- **アプリケーション管理のユーザー権限の変更**：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 サービス管理のユーザー権限の変更**：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。
- **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。
- **アプリケーションと使用可能なモジュールアップデートの情報**：Kaspersky Embedded Systems Security や、現在使用可能なアプリケーションモジュールのアップデートに関する情報を参照してください。
- **最新の情報に更新**：アプリケーションコンソール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。
- **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。

  また、［**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**］を使用するか、ツールバーにあるボタン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 タスクを、アプリケーションコンソールツリーにある各タスクのコンテキストメニューの項目を使用して管理できます。

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：

- **開始 / 停止**：タスクの実行を開始または停止します。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。

- **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、コンピューター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で使用できます。
- **タスクの追加**：新しいカスタムタスクを作成します。この操作は、オンデマンドスキャンタスクで使用できます。
- **ログを開く**：実行ログを表示および管理します。この操作は、すべてのタスクで使用できます。
- **タスクを削除**：カスタムタスクを削除します。この操作は、オンデマンドスキャンタスクで使用できます。
- **設定のテンプレート**：テンプレートを管理します。この操作は、ファイルのリアルタイム保護およびオンデマンドスキャンに対して使用できます。

## 通知領域のシステムトレイアイコン

保護対象デバイスの再起動後に Kaspersky Embedded Systems Security が自動的に起動されるたびに、システムトレイアイコン がツールバーの通知領域に表示されます。このアイコンは、本製品のセットアップ時にシステムトレイアイコンがインストールされた場合に、既定で表示されます。

システムトレイアイコンの外観は、デバイス保護の現在のステータスを反映します。ステータスには 2 種類あります：

| | |
|---|---|
|  | アクティブ（カラーのアイコン）- 次のタスクのうち少なくとも 1 つが現在実行中である場合：ファイルのリアルタイム保護、アプリケーション起動コントロール |
|  | 非アクティブ（白黒のアイコン）- 次のタスクのいずれも現在実行中でない場合：ファイルのリアルタイム保護、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** | 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**］ - ［**システムトレイアイコン**］を選択します。

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。

Kaspersky Embedded Systems Security の全般設定で、保護対象デバイスの再起動後にアプリケーションが自動起動するたびに、システムトレイアイコンの表示を有効または無効にできます。

# 別のデバイスにインストールしたアプリケーションコンソールを使用した Kaspersky Embedded Systems Security の管理

リモート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から Kaspersky Embedded Systems Security を管理できます。

リモートデバイスで Kaspersky Embedded Systems Security コンソールを使用して本製品を管理するには、次の点を確認してください：

- リモートデバイスのアプリケーションコンソールのユーザーが、保護対象デバイスの［ESS Administrators］グループに追加されている。
- 保護対象デバイスで Windows ファイアウォールが有効な場合、Kaspersky Security 管理サービスプロセス（kavfsgt.exe）に対してネットワーク接続が許可されている。
- Kaspersky Embedded Systems Security のインストール中、インストールウィザードで［**リモートアクセスを許可する**］がオンになっている。

リモートデバイス上の Kaspersky Embedded Systems Security がパスワードで保護されている場合は、パスワードを入力して、アプリケーションコンソールからアプリケーション管理にアクセスします。

# アプリケーションコンソールからの全般的なアプリケーション設定

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、アプリケーション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 を設定するには：*

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：

- フォルダーの詳細ペインにある［**アプリケーションのプロパティ**］をクリックする。
- フォルダーのコンテキストメニューで［**プロパティ**］を選択する。

［**アプリケーションの設定**］ウィンドウが表示されます。

2. 表示されたウィンドウで、必要に応じて Kaspersky Embedded Systems Security の全般設定を設定します：

- ［**スケーラビリティとインターフェイス**］タブでは、次を設定できます：
  - ［**スケーラビリティ設定**］セクション：
    - Kaspersky Embedded Systems Security で実行可能な処理対象プロセスの最大数
    - コンピューターのリアルタイム保護の対象プロセスの数
    - バックグラウンドのオンデマンドスキャンタスクの処理対象プロセスの数
- ［**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ている場合に選択します。
- ［**セキュリティと信頼性**］タブでは、次を設定できます：
  - ［**パスワードによる保護の設定**］セクションで、アプリケーションプロセスの保護を設定します。
  - ［**パスワードによる保護の設定**］セクションで、アプリケーション機能のパスワードによる保護を設定します。
  - クラッシュした場合、［**セルフディフェンス**］セクションで、オンデマンドスキャンタスクの復元を試行する回数を指定します。
- ［**オンデマンドスキャンタスクの復元回数上限（回）**］セクションで、UPS 電源への切り替え後に Kaspersky Embedded Systems Security により実行される動作を指定します。
- ［**スキャン設定**］タブ：
  - **スキャン後にファイル属性を復元する**
  - **スレッドのスキャン時に CPU の使用を制限する**
    - **上限（パーセント）**
  - **スキャン中に作成された一時ファイルのフォルダー**
- ［**接続設定**］タブ：
  - ［**プロキシサーバーの設定**］セクションで、プロキシサーバーの設定を指定します。
  - ［**プロキシサーバーの認証設定**］セクションで、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。
  - ［**ライセンス**］セクションで、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。
- ［**トラブルシューティング**］タブ：

- デバッグ情報をファイルに書き込む場合は、［**デバッグ情報をトレースファイルに書き込む**］をオンにします。
  - 下にあるフィールドで、トレースファイルを保存するフォルダーを指定します。
  - デバッグ情報の詳細レベルを設定します。
  - トレースファイルの最大サイズを指定します。
  - 1つのトレースログの最大ファイル数を指定します。Kaspersky Embedded Systems Security は、デバッグするコンポーネントごとに最大数のトレースファイルを作成します。
  - デバッグするコンポーネントを指定します。
- ダンプファイルを作成する場合は、［**クラッシュダンプファイルの作成**］をオンにしてください。

Kaspersky Embedded Systems Security からは、トレースファイルまたはダンプファイルは自動的に送信されません。診断データは、該当する権限を持つユーザーのみが送信できます。

- 下にあるフィールドで、ダンプファイルを保存するフォルダーを指定します。

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ユーザーが選択し、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。

3. ［**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 では、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、オンデマンドスキャン、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。

タスクは、アプリケーションコンソールツリー、ツールバー、およびクイックアクセスバーでタスクのコンテキストメニュー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。隔離のスキャンおよび定義データベースのロールバック以外のすべてのローカルシステムタスクの設定を編集できます。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を作成できます。Kaspersky Security Center で、オンデマンドスキャンタスク、定義データベースのアップデートタスク、定義データベースのロールバックタスク、およびアップデートのコピータスクを作成できます。カスタムタスクは、名前の変更や設定変更、削除ができます。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

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のみ、一時停止および再開することができます。その他のタスクは手動で一時停止および再開はできません。

*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. 次のいずれかを選択します：［**開始**］、［**一時停止**］、［**再開**］、［**停止**］。

   操作が実行され、システム監査ログに記録されます。

オンデマンドスキャンタスクを再開した場合、Kaspersky Embedded Systems Security はスキャンが停止したオブジェクトからスキャンを開始します。

## 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. スケジュールを設定するタスク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。
   ［**タスクの設定**］ウィンドウが表示されます。
3. 表示されたウィンドウの［**スケジュール**］タブで、［**スケジュールに従って実行する**］をオンにします。
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**］ドロップダウンメニューでは、次のいずれかを選択します：
      - ［**時間単位**］：1時間間隔でタスクを実行します。指定された時間間隔でタスクを実行する場合は、［**間隔 <number> 時間**］で時間数を指定します。
      - ［**日単位**］：日単位でタスクを実行します。指定された日間隔でタスクを実行する場合は、［**間隔 <number> 日**］で日数を指定します。
      - ［**週単位**］：週単位でタスクを実行します。指定された週間隔でタスクを実行する場合は、［**間隔 <number> 週ごと、曜日**］で週数を指定します。タスクが開始される曜日を指定します（既定では、タスクは月曜日に実行されます）。
      - ［**アプリケーションの起動時**］：Kaspersky Embedded Systems Security が起動するたびにタスクを実行します。
      - ［**定義データベースのアップデート後**］：定義データベースのアップデート後にタスクを実行します。
   b. ［**開始時刻**］フィールドに、タスクの初回開始時刻を指定します。
   c. ［**開始日**］フィールドに、タスクの初回開始日を指定します。

   タスクの開始頻度、タスクが最初に開始される時刻、およびスケジュールの適用開始日を指定したら、ウィンドウ上部の［**次回開始**］に、計算された次回のタスク開始時間が表示されます。［**タスクの設定**］ウィンドウの［**スケジュール**］タブを開くたびに、次回タスクが開始される予定の日時が更新されて、表示されます。

   Kaspersky Security Center の有効な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、［**次回開始**］には［**ポリシーによりブロック**］と表示されます。

5. ［**詳細設定**を使用して次のスケジュールを指定します。
   - ［**タスクの停止設定**］セクション：
     a. ［**経過時間**］を選択します。右側のフィールドに、最大タスク期間を時間と分単位で入力します。
     b. ［**一時停止**］をオンにします。右側のフィールドに、タスクを一時停止および再開する時間を入力します（24時間以内）。

- ［**詳細設定**］セクション：

  a. ［**スケジュール終了日**］を選択してタスクのスケジュールの終了日を指定します。

  b. ［**スキップしたタスクを実行する**］をオンにして、スキップしたタスクを開始します。

  c. ［**タスク開始を次の期間内でランダム化する**］をオンにして、値を分で指定します。

6. ［**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、スケジュールを設定するタスク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。
   ［**タスクの設定**］ウィンドウが表示されます。
3. 表示されたウィンドウの［**スケジュール**］タブで、次のいずれかのオプションを選択します：
   - 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、［**スケジュールに従って実行する**］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無効にする場合は、［**スケジュールに従って実行する**］をオフにします。

   > タスクの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。

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作成

- デバイスコントロールルールの自動作成
- オンデマンドスキャン
- 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パブリック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
- **オンデマンドスキャン**タスク：システムアカウントがスキャン対象オブジェクトに対するアクセス権限を所有していない場合（例：保護対象デバイスの共有フォルダーのファイルなど）
- **アプリケーション起動コントロールルールの自動作成**タスク：システムアカウントがアクセスできない設定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）

システムアカウント権限を使用して、アップデートタスク、オンデマンドスキャンタスク、およびルールの自動作成タスクを実行できます。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

*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、特定のアカウントを使用して実行するタスク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。
   ［**タスクの設定**］ウィンドウが表示されます。
3. 表示されたウィンドウの［**実行用アカウント**］タブで次の手順に従います：
   a. ［**ユーザー名**］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。

   c. パスワードを確認します。

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、特定の製品設定を XML 設定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
- KSN の使用
- デバイスコントロール
- 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ルールの自動作成
- アプリケーション起動コントロールルールの自動作成
- オンデマンドスキャンタスク
- ファイル変更監視
- ログ監査
- 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
- 隔離
- バックアップ
- ログ
- 管理者およびユーザーへの通知
- 信頼ゾーン
- 脆弱性攻撃ブロック
- パスワードによる保護

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。別の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

*設定ファイルに設定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、次のいずれかの操作を行います：

   - ［**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**］を選択してすべての Kaspersky Embedded Systems Security 設定をエクスポートする。
   - 特定のタスクでコンテキストメニューを開き、［**設定のエクスポート**］を選択して、本製品の個別の機能コンポーネントの設定をエクスポートする。
   - 信頼ゾーンの設定をエクスポートするには：

     a. 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。

     b. ［**信頼ゾーンの設定**］を選択します。
     ［**信頼ゾーン**］ウィンドウが開きます。

     c. ［**エクスポート**］をクリックします。
     設定のエクスポートウィザードが開きます。

2. ［**設定のエクスポートウィザード**］の手順に従い、設定を保存する設定ファイルの名前とパスを指定します。
   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. ［**アプリケーション設定のエクスポートが完了しました**］ウィンドウで［**閉じる**］をクリックします。

設定のエクスポートウィザードが終了し、エクスポートされた設定が保存されます。

## 設定のインポート

*保存された設定ファイルから設定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、次のいずれかの操作を行います：

   - ［**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**］を選択してすべての Kaspersky Embedded Systems Security 設定をインポートする。
   - 特定のタスクでコンテキストメニューを開き、［**設定のインポート**］を選択して、本製品の個別の機能コンポーネントの設定をインポートする。
   - 信頼ゾーンの設定をインポートするには：

     a. 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。

     b. ［**信頼ゾーンの設定**］を選択します。
     ［**信頼ゾーン**］ウィンドウが開きます。

     c. ［**インポート**］をクリックします。
     設定のインポートウィザードが開きます。

2. ［**設定のインポートウィザード**］の手順に従い、設定をインポートする設定ファイルを指定します。

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。

3. ［**アプリケーション設定のインポートが完了しました**］ウィンドウにある［**閉じる**］をクリックします。
設定のインポートウィザードが終了し、インポートされた設定が保存されます。

4. アプリケーションコンソールのツールバーで、［**最新の情報に更新**］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。

# セキュリティ設定テンプレートの使用

このセクションでは、Kaspersky Embedded Systems Security の保護タスクとスキャンタスクでのセキュリティ設定テンプレートの使用について説明します。

# セキュリティ設定テンプレートについて

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。

テンプレートを使用して、次の Kaspersky Embedded Systems Security タスクのセキュリティ設定を行うことができます：

- ファイルのリアルタイム保護
- オペレーティングシステムの起動時にスキャン
- 簡易スキャン
- オンデマンドスキャンタスク

保護対象デバイスのファイルリソースツリーでテンプレートから親フォルダーに適用されるセキュリティ設定は、すべてのサブフォルダーに適用されます。次の場合、親フォルダーのテンプレートはサブフォルダーには適用されません：

- 子フォルダーのセキュリティ設定を個別に設定した場合。
- サブフォルダーが仮想の場合。この場合、仮想フォルダーごとにテンプレートを個別に適用する必要があります。

# セキュリティ設定テンプレートの作成

*フォルダーのセキュリティ設定を手動でテンプレートに保存するには：*

1. アプリケーションコンソールツリーで、セキュリティ設定テンプレートを作成するタスクを選択します。
2. 選択したタスクの詳細ペインにある［**保護範囲の設定**］または［**スキャン範囲の設定**］をクリックします。
3. 保護対象デバイスのネットワークファイルリソースのツリーまたはリストで、表示するテンプレートを選択します。
4. ［**セキュリティレベル**］タブで、［**テンプレートとして保存**］をクリックします。
   ［**テンプレートのプロパティ**］ウィンドウが開きます。
5. ［**テンプレート名**］で、テンプレートの名前を入力します。

6. ［**説明**］フィールドで、テンプレートの情報を入力します。

7. ［**OK**］をクリックします。

セキュリティ設定テンプレートが保存されます。

## テンプレートのセキュリティ設定の表示

*作成したテンプレートのセキュリティ設定を表示するには：*

1. アプリケーションコンソールツリーで、表示するセキュリティ設定テンプレートのあるタスクを選択します。

2. 選択したタスクのコンテキストメニューで、［**設定のテンプレート**］を選択します。
   ［**テンプレート**］ウィンドウが開きます。

3. テンプレートリストで、表示するテンプレートを選択します。

4. ［**表示**］をクリックします。

［**<テンプレート名>**］ウィンドウが開きます。［**全般**］タブにはテンプレートの名前とテンプレートに関する情報が表示されます。［**オプション**］タブにはテンプレートに保存されたセキュリティ設定がリストで表示されます。

## セキュリティ設定テンプレートの適用

*選択したフォルダーにテンプレートからセキュリティ設定を適用するには：*

1. アプリケーションコンソールツリーで、セキュリティ設定テンプレートを適用するタスクを選択します。

2. 選択したタスクの詳細ペインにある［**保護範囲の設定**］または［**スキャン範囲の設定**］をクリックします。

3. 保護対象デバイスのネットワークファイルリソースのツリーまたはリストで、テンプレートを適用するフォルダーまたは項目のコンテキストメニューを開きます。

4. ［**テンプレートの適用**］-［**<テンプレート名>**］の順に選択します。

5. ［**保存**］をクリックします。

保護対象デバイスのファイルリソースツリーで選択されたフォルダーにセキュリティ設定のテンプレートを適用します。選択されたフォルダーの［**セキュリティレベル**］タブの値が［**カスタム**］に変更されます。

保護対象デバイスのファイルリソースツリーの親フォルダーにテンプレートのセキュリティ設定が適用される場合、この設定はすべての子フォルダーに適用されます。

保護対象デバイスのファイルリソースツリー内で個別に子フォルダーの保護またはスキャン範囲を設定することができます。この場合、親フォルダーに適用されたテンプレートのセキュリティ設定は自動では子フォルダーに適用されません。

*選択したすべてのフォルダーにテンプレートからセキュリティ設定を適用するには：*

1. アプリケーションコンソールツリーで、セキュリティ設定テンプレートを適用するタスクを選択します。
2. 選択したタスクの詳細ペインにある［**保護範囲の設定**］または［**スキャン範囲の設定**］をクリックします。
3. 選択したフォルダーおよびそのサブフォルダーにテンプレートを適用するには、保護対象デバイスのネットワークファイルリソースのツリーまたはリストで親フォルダーを選択します。
4. 右クリックしてコンテキストメニューを開き、［**テンプレートの適用**］-［**<テンプレート名>**］の順に選択します。
5. ［**保存**］をクリックします。

セキュリティ設定テンプレートが、保護対象デバイスのファイルリソースツリーの親フォルダーとすべてのサブフォルダーに適用されます。選択されたフォルダーの［**セキュリティレベル**］タブの値が［**カスタム**］に変更されます。

## セキュリティ設定テンプレートの削除

*セキュリティ設定テンプレートを削除するには：*

1. アプリケーションコンソールツリーで、削除するセキュリティ設定テンプレートのあるタスクを選択します。
2. 選択したタスクのコンテキストメニューで、［**設定のテンプレート**］を選択します。
   ［**テンプレート**］ウィンドウが開きます。

   ［**オンデマンドスキャン**］親フォルダーの結果ペインで、オンデマンドスキャンタスクの設定テンプレートを表示できます。
3. テンプレートリストで、削除するテンプレートを選択します。
4. ［**削除**］をクリックします。
   削除を確認するウィンドウが開きます。
5. 表示されたウィンドウで、［**はい**］をクリックします。

選択したテンプレートが削除されます。

セキュリティ設定のテンプレートを適用して保護対象デバイスのファイルリソースツリーのスキャンを実行したり保護したりできます。この場合、これらのフォルダーに対するセキュリティ設定はテンプレートの削除後に変更されません。

## 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：*

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。

既定では、アプリケーション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［**最新の情報に更新**］コマンドを選択します。

アプリケーション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。
- ライセンス情報。
- Kaspersky Security Center との統合のステータス：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。

保護動作ステータスを示すために、異なる色で表示されます：

- *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。

［**Kaspersky Security Network の使用**］セクションには、*実行中*、*停止済み*、または*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：

- 緑色は、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。
- 黄色は、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。

## コンピューターの保護

［**コンピューターの保護**］セクション（下の表を参照）には、デバイスの現在の保護ステータス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

| ［保護］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** | セクション名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 - 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>• 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ません。<br>• 赤色 - ファイルのリアルタイム保護タスクが実行されていません。 |
| **ファイルのリアルタイム保護** | **タスクのステータス** - 「*実行中*」や「*停止済み*」など、現在のタスクのステータス。<br>**検知** - Kaspersky Embedded Systems Security が検知し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 つの悪意のあるアプリケーションを検知した場合、このフィールドの値が 1 つ加算されます。検知された悪意のあるアプリケーションの数が 0 を超えると、値が赤色で表示されます。 |
| **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付。<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。 |
| **脆弱性攻撃ブロック** | **ステータス** - 脆弱性攻撃ブロックの現在のステータス。例：「*適用済み*」または「*未適用*」。<br>**防御モード** - 使用可能な 2 つのモードのうちの 1 つで、プロセスメモリ保護の設定時に選択します：［**脆弱性攻撃時に終了する**］または［**統計のみ**］。<br>**保護したプロセス** - 保護範囲に追加され、選択したモードに従って処理されたプロセスの合計数。 |
| **バックアップされたオブジェクト** | *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* - このイベントは、バックアップの空き容量が指定のサイズに達しそうになると発生します。オブジェクトのバックアップ保管領域への移動を継続します。この場合、［**使用済みのサイズ**］の値が黄色で表示されます。<br>*バックアップの最大サイズを超過しました* - このイベントは、バックアップのサイズが指定のサイズに達すると発生します。オブジェクトのバックアップ保管領域への移動を継続します。この場合、［**使用済みのサイズ**］の値が赤色で表示されます。<br>**バックアップされたオブジェクト** - バックアップに現在保存されているオブジェクトの数。<br>**使用済みのサイズ** - バックアップ領域の使用済みのサイズ。 |

## 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アプリケーション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

| ［アップデート］セクション | 情報 |
| --- | --- |
| **定義データベースとソフトウェアモジュールのステータスインジケーター** | セクション名が表示されたパネルの色は、定義データベースとモジュール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 - 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のアップデートが正常に完了したことを示します。<br>• 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のアップデートが失敗したことを示します。<br>• 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*］または［*定義データベースが破損しています*］のいずれかのイベントが発生したことを示します。 |
| **定義データベースのアップデート**と**ソフトウェアモジュールのアップデート** | **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>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す。<br>*［定義データベースは最新です］*イベントおよび［*定義データベースが長期間アップデートされていません*］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リリースされた日時。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ステータス** - 前回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。このフィールドは、［*失敗*］イベントが発生すると赤色になります。<br>**利用可能なモジュールのアップデートの数** - ダウンロードしてインストールできる Kaspersky Embedded Systems Security モジュールのアップデートの数。<br>**インストールされたモジュールのアップデートの数** - インストール済みの Kaspersky Embedded Systems Security モジュールのアップデートの数。 |

## 管理

［**管理**］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管理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

| ［管理］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** | セクション名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： |

| | |
|---|---|
| | • 緑色 - この色は既定で表示されます。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、タスクが処理を実行モードで実行中であること、脆弱性攻撃ブロック機能がインストールされ、［**処理を実行**］モードで実行中であることを示します。<br>• 黄色 - アプリケーション起動コントロールが［**統計のみ**］モードで実行中であることを示します。<br>• 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、失敗したことを示します。 |
| **アプリケーション起動コントロール** | **タスクのステータス** - 「*実行中*」や「*停止済み*」など、現在のタスクのステータス。<br>**動作モード** - 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：［**処理を実行**］または［**統計のみ**］。<br>**アプリケーションの起動の拒否** - 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 によってブロックされたアプリケーション起動の試行数。ブロックされたアプリケーション起動の数が 0 を超えると、フィールドは赤色になります。<br>**平均処理時間（ミリ秒）** - Kaspersky Embedded Systems Security が保護対象デバイスのアプリケーション起動の試行処理にかかった時間。 |
| **デバイスコントロール** | **タスクのステータス** - 「*実行中*」や「*停止済み*」など、現在のタスクのステータス。<br>**動作モード** - 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：［**処理を実行**］または［**統計のみ**］。<br>**ブロック対象デバイス** - デバイスコントロールタスク時に Kaspersky Embedded Systems Security によってブロックされた、外部デバイスへの接続試行の合計数。ブロックされた外部デバイスの数が 0 を超えると、フィールドの値は赤色になります。 |
| **ファイアウォール管理** | **タスクのステータス** - 「*実行中*」や「*停止済み*」など、現在のタスクのステータス。<br>**接続をブロックしました** - 指定されたファイアウォールのルールによってブロックされた、保護対象デバイスへの接続数。 |

## 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

| ［診断］セクション | 情報 |
|---|---|
| **診断ステータスのインジケーター** | セクション名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 - この色は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。 |
| **ファイル変** | **タスクのステータス** - 「*実行中*」や「*停止済み*」など、現在のタスクのステータス。 |

| | |
|---|---|
| **更監視** | **認可されていないファイル操作** - 監視範囲のファイルへの変更数。この変更数は、保護対象デバイスのセキュリティが侵害されていることを示す場合があります。 |
| **Windows イベントログ監視** | **タスクのステータス** - 「*実行中*」や「*停止済み*」など、現在のタスクのステータス。<br>**設定済みルール違反** - Windows イベントログからのデータに基づく、記録された違反の数。この数は、指定されたタスクルールに基づいて、またはヒューリスティックアナライザーを使用して決定されます。 |

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、［**別の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、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、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集中管理できます。Kaspersky Security Center Web コンソールおよび Kaspersky Security Center 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、アプリケーションの全般的な設定、コンピューターのリアルタイム保護タスクの設定、ローカルアクティビティの管理タスクの設定、およびスケジュールによるローカルシステムタスクの開始設定を編集できます。

- **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作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 Kaspersky Security Center 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、ログや通知を利用できます。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：

- ユーザーまたはユーザーグループを追加するには、セキュリティ記述子定義言語（SDDL）を使用して SDDL 文字列を指定する必要があります。
- ファイルのリアルタイム保護タスクでは、定義済みセキュリティレベルを変更することはできません。
- 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 Web 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の情報が記載されています。

## 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 プラグインでのスケーラビリティ、インターフェイスおよびスキャン設定

*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. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**アプリケーションの設定**］セクションを選択します。
5. ［**スケーラビリティ、インターフェイス、スキャンの設定**］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。

スケーラビリティ設定

| 設定 | 説明 |
| --- | --- |
| スケーラビリティ設定を自動的に検出する | 使用するプロセス数が自動的にコントロールされます。<br>これが既定値です。 |
| 処理対象プロセスの数を手動で設定する | Kaspersky Embedded Systems Security で、指定した値に従ってアクティブな処理対象プロセスの数がコントロールされます。 |
| 実行中プロセスの最大数 | Kaspersky Embedded Systems Security が使用するプロセスの最大数。この入力フィールドは、［**処理対象プロセスの数を手動で設定する**］をオンにすると使用可能になります。 |
| リアルタイム保護の対象プロセスの数 | コンピューターのリアルタイム保護タスクが使用するプロセスの最大数。この入力フィールドは、［**処理対象プロセスの数を手動で設定する**］をオンにすると使用可能になります。 |
| バックグラウンドのオンデマンドスキャンタスクの対象プロセスの数 | バックグラウンドでオンデマンドスキャンタスクを実行している時に、オンデマンドスキャンで使用されるプロセスの最大数。この入力フィールドは、［**処理対象プロセスの数を手動で設定する**］をオンにすると使用可能になります。 |
| タスクバーにシステムトレイアイコンを表示する | システムトレイアイコンを通知領域に表示するかどうかを設定します。 |
| **スキャン後にファイル属性を復元する** | Kaspersky Embedded Systems Security がオンデマンドスキャンタスクを実行すると、スキャンされた各ファイルの最終アクセス時刻が更新されます。スキャン後、Kaspersky Embedded Systems Security は、ファイルの最終アクセス時刻を初期値にリセットします。<br><br>この動作は、変更されていないファイルのバックアップコピーを作成することにより、バックアップシステムの動作に影響を与える可能性があります。これにより、ファイル変更追跡アプリケーションで誤検出が発生する可能性もあります。<br><br>既定では、このオプションは有効です。 |
| スレッドのスキャン時に CPU の使用を制限する | 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（パーセント）**］で指定した値に制限されます。<br><br>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。<br><br>既定では、このオプションは無効です。 |
| 上限（パーセント） | Kaspersky Embedded Systems Security による CPU 使用率の最大許容値。<br><br>この入力フィールドは、［**スレッドのスキャン時に CPU の使用を制限する**］がオンの場合にのみ使用できます。 |
| **スキャン中に作成された一時ファイルのフォルダー** | Kaspersky Embedded Systems Security がスキャン中にアーカイブファイルを解凍するフォルダー。<br><br>既定では、C:\Windows\Temp フォルダーが使用されます。 |
| HSM システムの設定 | 階層型ストレージへのアクセスのオプションを選択します。 |

# Web プラグインでのセキュリティ設定

*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、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**アプリケーションの設定**］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。

セキュリティ設定

| 設定 | 説明 |
| --- | --- |
| **アプリケーションプロセスを外部の脅威から保護する** | ［**アプリケーションプロセスを外部の脅威から保護する**］がオンの場合、本製品はコードインジェクションまたはデータ処理へのアクセスから本製品のプロセスを保護します。<br><br>このオプションを有効または無効にする際、変更を適用するために本製品のサービスを再起動する必要はありません。<br><br>既定では、このオプションは有効です。 |
| **タスク復元を実行する** | このチェックボックスにより、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合の、Kaspersky Embedded Systems Security タスクの復元を有効または無効に設定できます。<br>このチェックボックスをオンにすると、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合に、Kaspersky Embedded Systems Security によって Kaspersky Embedded Systems Security タスクが自動的に復元されます。<br>このチェックボックスをオフにすると、アプリケーションでエラーが返された場合、またはアプリケーションが終了した場合に、Kaspersky Embedded Systems Security タスクは自動的に復元されません。<br>既定では、このチェックボックスはオンです。 |
| オンデマンドスキャンタスクの復元回数上限（範囲：1～10回） | アプリケーションでエラーが返された後に、オンデマンドスキャンタスクの復元を試行する回数。この入力フィールドは、［**タスク復元を実行する**］をオンにすると使用可能になります。 |
| スケジュール設定済みのスキャンタスクを開始しない | このチェックボックスにより、保護対象デバイス UPS 電源に切り替えられてから通常の電源供給が復元されるまでの間における定期スキャンタスクの開始を有効にするか、無効にするかを設定できます。<br>このチェックボックスをオンにすると、保護対象デバイスで UPS 電源に切り替えられてから標準の電源供給が復元されるまで、定期スキャンタスクは開始されません。<br>このチェックボックスをオフにすると、電源供給に関係なく、Kaspersky Embedded Systems Security により定期スキャンタスクが開始されます。<br>既定では、このチェックボックスはオンです。 |

| | |
|---|---|
| 現在のスキャンタスクを中止する | このチェックボックスにより、保護対象デバイスの UPS 電源への切り替え後のスキャンタスクの実行を有効または無効に設定できます。<br>このチェックボックスをオンにすると、保護対象デバイスで UPS 電源に切り替えられた後で、Kaspersky Embedded Systems Security によりスキャンタスクの実行が一時停止されます。<br>このチェックボックスをオフにすると、保護対象デバイスで UPS 電源に切り替えられた後でも、Kaspersky Embedded Systems Security により引き続きスキャンタスクが実行されます。<br>既定では、このチェックボックスはオンです。 |
| パスワードによる保護を適用する | Kaspersky Embedded Systems Security 機能へのアクセスを保護するパスワードを設定します。 |

## 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 サービスと統合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、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**アプリケーションの設定**］セクションを選択します。
5. ［**スケーラビリティ、インターフェイス、スキャンの設定**］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。

接続設定

| 設定 | 説明 |
|---|---|
| プロキシサーバーを使用しない | このオプションをオンにすると、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。 |
| 指定したプロキシサーバー設定を使用する | このオプションを選択すると、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。 |
| ローカルアドレスへの接続時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。既定では、このモードが選択されます。 |
| **NTLM 認証を使用する** | 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。 |
| **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を適用する** | ユーザー名とパスワードを使用して認証が行われます。 |

## ローカルのシステム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、隔離のスキャン、オペレーティングシステムの起動時にスキャン、アプリケーションの整合性チェック、ベースラインに基づくファイル変更監視。
- アップデートタスク：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、アップデートのコピー。

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、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**アプリケーションの設定**］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。

ローカルシステムタスクのスケジュールによる開始の設定

| 設定 | 説明 |
|---|---|
| オンデマンドスキャンタスクの実行を許可 | チェックボックスをオンまたはオフにして、オンデマンドスキャンタスクのスケジュールされた起動を許可または禁止します。 |
| アップデートタスクとアップデートのコピータスクの実行を許可 | チェックボックスをオンまたはオフにして、アップデートタスクとアップデートのコピータスクのスケジュールされた起動を許可または禁止します。 |

## Web プラグインでの隔離とバックアップの設定

Kaspersky Security Center で隔離および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、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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。

隔離とバックアップの設定

| 設定 | 説明 |
|---|---|
| **バックアップフォルダー** | バックアップのフォルダーを指定します。 |
| **バックアップの最大サイズ** | バックアップの最大サイズを設定します。 |

| | |
|---|---|
| （MB） | |
| **空き容量のしきい値（MB）** | バックアップフォルダーの空き容量の最小値を指定します。 |
| **オブジェクトの復元先フォルダー** | 復元されたオブジェクトのフォルダーを指定します。 |
| **隔離フォルダー** | バックアップのフォルダーを指定します。 |
| **隔離の最大サイズ（MB）** | バックアップの最大サイズを設定します。 |
| **空き容量のしきい値（MB）** | バックアップフォルダーの空き容量の最小値を指定します。 |
| **オブジェクトの復元先フォルダー** | 復元されたオブジェクトのフォルダーを指定します。 |
| **コンピューターのブロック期間** | ブロック対象コンピューターが、ネットワークファイルリソースに再びアクセスできるようになるまでの日数および時間（時間、分）を指定します。 |

## 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、指定された Kaspersky Embedded Systems Security の設定、機能、および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［**システム監査ログ**］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。

また、アクティブポリシーで設定し 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。

ポリシーでコンピューターのリアルタイム保護タスクのいずれかの設定を定義しており、そのタスクが現在実行中の場合、ポリシーによって定義された設定は、ポリシーの適用後すぐに変更されます。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には：*

1. Web コンソールのメインウィンドウで、［**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**］ウィンドウが開きます。
4. ［**アプリケーションの選択**］セクションで、Kaspersky Embedded Systems Security を選択して［**次へ**］をクリックします。
5. ［**全般**］セクションでは、次の操作を行えます：
   - ポリシーの名前を変更します。

     次の記号をポリシー名に含めることはできません：`" * < : > ? \ |` 。
   - ポリシーのステータスを選択します：
     - **処理を実行**：次の同期後、このポリシーはコンピューター上の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**：バックアップポリシーとして使用されます。必要に応じて、非アクティブポリシーをアクティブステータスに切り替えることができます。
     - **モバイルユーザー**：コンピューターが組織のネットワークを離れると、このポリシーがアクティブになります。
   - 継承の設定を指定します：
     - **親ポリシーから設定を継承する**：この切り替えボタンをオンにすると、ポリシーの設定値はトップレベルのポリシーから継承されます。🔒が親ポリシーに設定されている場合、ポリシー設定は編集できません。
     - **子ポリシーへ設定を強制的に継承する**：この切り替えボタンをオンにすると、ポリシーの設定値は子ポリシーに継承されます。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。🔒が親ポリシーに設定されている場合、子ポリシーの設定は編集できません。
6. ［**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。
7. ［**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。

# Kaspersky Embedded Systems Security ポリシー設定のセクション

## 全般

［**全般**］セクションでは、次のポリシー設定を編集できます：

- ポリシーのステータスの指定。
- 親ポリシーから子ポリシーへ継承する設定の指定。

## イベントの設定

［**イベントの設定**］セクションでは、次のイベントカテゴリを設定できます：

- *緊急*
- *機能エラー*
- *警告*
- *情報*
  ［**プロパティ**］を使用して、選択したイベントに対して次を設定できます：
- 記録したイベントの保管場所と保管期間の指定
- 記録したイベントの通知方法の指定

## アプリケーションの設定

［アプリケーションの設定］セクションの設定

| セクション | オプション |
| --- | --- |
| **スケーラビリティ、インターフェイス、スキャンの設定** | ［**スケーラビリティ、インターフェイス、スキャンの設定**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• スケーラビリティ設定を自動と手動のいずれで設定するかを選択<br>• 製品アイコンの表示設定 |
| **セキュリティと信頼性** | ［**セキュリティと信頼性**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• タスク実行の設定<br>• UPS 電源による保護対象デバイスの実行時のアプリケーションの挙動の指定<br>• アプリケーション機能のパスワードによる保護の有効化または無効化 |
| **接続** | ［**接続**］サブセクションで［**設定**］を使用して、アップデートサーバー、アクティベーションサーバー、および KSN に接続するためのプロキシサーバーの次の設定を行えます： |

| | |
|---|---|
| | • プロキシサーバーの設定<br>• プロキシサーバーの認証設定の指定 |
| **ローカルシステムタスクの実行** | ［**ローカルシステムタスクの実行**］サブセクションで［**設定**］をクリックして、保護対象デバイスで設定されているスケジュールに応じた次のシステムタスクの起動を許可またはブロックできます：<br>• オンデマンドスキャンタスク<br>• アップデートタスクおよびアップデートのコピータスク |

## 詳細設定

［詳細設定］セクションの設定

| セクション | オプション |
|---|---|
| **信頼ゾーン** | ［**信頼ゾーン**］サブセクションの［**設定**］をクリックして、次の信頼ゾーンの設定を編集します：<br>• 信頼ゾーンの除外リストの作成<br>• ファイルのバックアップ処理のスキャンの有効化または無効化<br>• 信頼するプロセスのリストの作成 |
| **リムーバブルドライブスキャン** | ［**リムーバブルドライブスキャン**］サブセクションで［**設定**］をクリックして、リムーバブルドライブのスキャンを設定できます。 |
| **アプリケーション管理用のユーザーアクセス権限** | ［**アプリケーション管理用のユーザーアクセス権限**］サブセクションで、ユーザー権限およびユーザーグループ権限を設定して Kaspersky Embedded Systems Security を管理できます。 |
| **Kaspersky Security サービス管理用のユーザーアクセス権限** | ［**Kaspersky Security サービス管理用のユーザーアクセス権限**］サブセクションで、ユーザー権限およびユーザーグループ権限を設定して Kaspersky Security サービスを管理できます。 |
| **保管領域** | ［**保管領域**］サブセクションで［**設定**］をクリックして、次の隔離設定、バックアップ設定、ブロック対象コンピューターの設定を編集します：<br>• 隔離オブジェクトまたはバックアップオブジェクトを配置するフォルダーのパスの指定<br>• バックアップと隔離の最大サイズの設定および空き容量のしきい値の指定<br>• 隔離またはバックアップから復元するオブジェクトの配置先となるフォルダーのパスの指定<br>• 隔離オブジェクトおよびバックアップオブジェクトに関する情報の管理サーバーへの送信設定<br>• ホストがブロックされる時間の設定 |

## コンピューターのリアルタイム保護

［サーバーのリアルタイム保護］セクションの設定

| セクション | オプション |
| --- | --- |
| **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**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• 保護範囲の指定<br>• ヒューリスティックアナライザーの使用設定<br>• 信頼ゾーンの使用設定<br>• 保護範囲の指定<br>• 選択した保護範囲のセキュリティレベルの設定（定義済みのセキュリティレベルの選択または手動によるセキュリティレベルの設定）<br>• タスク開始の設定 |
| **KSN の使用** | ［**KSN の使用**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• KSN で信頼されていないオブジェクトに対する処理の指定。<br>• データ転送と、Kaspersky Security Center の KSN プロキシサーバーとしての使用を設定します。 |
| **脆弱性攻撃ブロック** | ［**脆弱性攻撃ブロック**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• プロセスメモリの保護モードを選択<br>• 脆弱性攻撃リスクを低下させる処理を指定<br>• 保護対象プロセスのリストを追加して編集 |

## ローカル活動の管理

［ローカルアクティビティの管理］セクションの設定

| セクション | オプション |
| --- | --- |
| **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**］サブセクションで［**設定**］を使用して、次のタスク設定を行えます：<br>• タスク処理モードの選択<br>• 次回以降のアプリケーション起動に対するコントロールの適用設定<br>• アプリケーション起動コントロールルールの範囲の指定<br>• KSN の使用設定<br>• タスク開始の設定 |
| **デバイスコントロール** | ［**デバイスコントロール**］サブセクションで［**設定**］をクリックして、次の |

| | |
|---|---|
| | タスク設定を行えます：<br>• タスク処理モードの選択<br>• タスク開始の設定 |

## ネットワーク活動の管理

［ネットワークアクティビティの管理］セクションの設定

| セクション | オプション |
|---|---|
| **ファイアウォール管理** | ［**ファイアウォール管理**］サブセクションで［**設定**］をクリックして、次のタスク設定を行えます：<br>• ファイアウォールのルールの設定<br>• タスク開始の設定 |

## システム監査

［システム監査］セクションの設定

| セクション | オプション |
|---|---|
| **ファイル変更監視** | ［**ファイル変更監視**］サブセクションで、保護対象デバイスにおける、セキュリティ侵害の可能性があるファイル変更の管理を設定できます。 |
| **Windows イベントログ監視** | ［**Windows イベントログ監視**］セクションで、Windows イベントログ分析の結果に基づいて、保護対象デバイスの整合性管理を設定できます。 |

## ログと通知

［ログと通知の設定］セクションの設定

| セクション | オプション |
|---|---|
| **実行ログ** | ［**実行ログ**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• 選択したソフトウェアコンポーネントの記録されたイベントに対する重要度の指定<br>• 実行ログのストレージ設定の指定<br>• Kaspersky Security Center 設定と SIEM との統合の指定 |
| **イベント通知** | ［**イベント通知**］サブセクションで［**設定**］をクリックして、次の設定を行えます：<br>• ［*オブジェクトが検知されました*］イベント、［*信頼しない大容量ストレージが検出および制限されました*］イベント、［*コンピューターが信頼しないリストに追加されました*］イベントのユーザーへの通知設定の指定<br>• ［**通知設定**］セクションのイベントリストで選択したイベントの管理者への通知設定の指定 |
| **管理サーバ** | ［**管理サーバーとのインタラクション**］サブセクションで［**設定**］をクリックして、 |

| | |
|---|---|
| **ーとのインタラクション** | Kaspersky Embedded Systems Security が管理サーバーに報告するオブジェクトの種別を選択できます。 |

変更履歴

［**変更履歴**］セクションでは、次のようにしてリビジョンを管理できます：現在のリビジョンや他のポリシーとの比較、リビジョンの説明の追加、ファイルへのリビジョンの保存、ロールバックの実行など。

## 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

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。次の種別のタスクが作成できます：

- 製品のアクティベーション
- 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
- 定義データベースのロールバック
- オンデマンドスキャン
- アプリケーションの整合性チェック
- ベースラインファイル変更監視
- アプリケーション起動コントロールルールの自動作成
- デバイスコントロールルールの自動作成

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：

- 1台の保護対象デバイスの場合、保護対象デバイスのプロパティウィンドウの［**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 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. 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。

     b. ［**グループ**］タブをクリックして、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. 保護対象デバイスの名前をクリックします。

     d. 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。

     e. ［**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、［**デバイス**］ - ［**管理対象デバイス**］の順に選択します。

     b. ［**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。

     c. ［**追加**］をクリックします。

   - 保護対象デバイスのカスタムセットに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、［**デバイス**］ - ［**デバイスの抽出**］の順に選択します。

     b. タスクを作成する抽出を選択します。

     c. ［**開始**］をクリックします。

     d. ［**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。

     e. ［**新規タスク**］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。

   定義データベースのロールバック、アプリケーションの整合性チェック、製品のアクティベーションのいずれか以外のタスク種別を選択した場合、［設定］ウィンドウが開きます。

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. ［**定義データベースのアップデート元**］セクションでアップデート元を選択します。

  b. ［**接続設定**］ウィンドウで、プロキシサーバーを設定します。

- ソフトウェアモジュールのアップデートタスクの作成後、［**ソフトウェアモジュールのアップデート**］ウィンドウで、必要なアプリケーションモジュールのアップデート設定を行います：

  a. 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してインストールするか、インストールはせずに使用可能かどうかのチェックだけを行うかを選択します。

  b. ［**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しインストールする**］を選択すると、インストールされたソフトウェアモジュールを適用するために、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。タスクの完了時に保護対象デバイスが自動的に再起動するようにしたい場合は、［**システムの再起動を許可する**］をオンにします。

  c. Kaspersky Embedded Systems Security のモジュールのアップグレードに関する情報を入手するには、［**適用可能になったソフトウェアモジュールの定期アップデートの情報を受信する**］をオンにします。

  カスペルスキーは、自動インストール用の定期的なアップデートパッケージをアップデートサーバーで公開していません。これらのパッケージは、カスペルスキーの Web サイトから手動でダウンロードできます。［**ソフトウェアモジュールの新しい定期アップデートが適用可能です**］イベントに関する管理者への通知を設定できます。これには、定期アップデートをダウンロードできるカスペルスキーの Web サイトの URL が含まれます。

- アップデートのコピータスクを作成するには、［**アップデートのコピー**］ウィンドウでアップデートとインストール先フォルダーを指定します。
- 製品のアクティベーションタスクを作成するには：

  a. ［**Kaspersky Security Center の保管領域にあるライセンスのリスト**］ウィンドウで、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。

  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作成タスクを作成して編集します。
- デバイスコントロールのルール生成タスクを作成して編集します。

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. タスクを設定する場合、［**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. ［**完了**］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、［**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。
   タスクのプロパティウィンドウが表示されます。
3. 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、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統合を設定します。
   - 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行います：
     a. ［**アップデート元**］セクションで、アップデート元とプロキシサーバーの設定を行います。
     b. ［**最適化**］セクションで、ディスクサブシステムの最適化を設定します。
   - ソフトウェアモジュールのアップデートタスクを設定する場合は、［**詳細設定**］セクションで、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してインストールするか、ソフトウェアモジュールの重要なアップデートの有無のみを確認します。
   - アップデートのコピータスクを設定する場合は、［**アップデートのコピーの設定**］セクションでアップデートとインストール先フォルダーを指定します。
   - 製品のアクティベーション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作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。
4. ［**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（定義データベース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）。
5. ［**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。
6. ［**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 プラグインでの製品のアクティベーションタスクの設定

*製品のアクティベーション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。
   タスクのプロパティウィンドウが表示されます。
3. ［**一般**］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。ライセンスを延長するためにライセンスを追加する時は、［**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、［**OK**］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

*アップデートのコピー、定義データベースのアップデート、またはソフトウェアモジュールのアップデートの各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。
   タスクのプロパティウィンドウが表示されます。
3. ［**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：
   - ［**定義データベースのアップデート元**］セクションで、製品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。

     > 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。

     > Cloud コンソールを使用してアップデートタスクを設定する場合、アップデート元に指定できるのは、［**ディストリビューションポイント**］と［**カスペルスキーのアップデートサーバー**］のみです。

   - ［**接続設定**］セクションで、カスペルスキーのアップデートサーバーおよびその他のサーバーに接続するためのプロキシサーバーの使用を設定します。
4. 定義データベースのアップデートタスクの［**最適化**］セクションでは、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 使用の最適化**
   - **最適化に使用するメモリ（400～9999 MB）**

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（定義データベース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。

## Web プラグインでのクラッシュの診断設定

Kaspersky Embedded Systems Security の使用中に Kaspersky Embedded Systems Security のクラッシュなどの問題が発生し、その問題を診断する場合、Kaspersky Embedded Systems Security プロセスのトレースファイルおよびダンプファイルの作成を有効にし、それらのファイルを解析するためにカスペルスキーのテクニカルサポートに送信することができます。

Kaspersky Embedded Systems Security からは、トレースファイルまたはダンプファイルは自動的に送信されません。診断データは、必要な権限を持つユーザーのみが送信できます。

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ユーザーが選択し、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。

*クラッシュの診断を設定するには：KAVSHELL DUMP コマンドを使用するか、アプリケーションコンソール上で次の操作を実行します。*

1. Kaspersky Security Center 管理コンソールで、［**アプリケーションの設定**］を開きます。

2. ［**トラブルシューティング**］タブで次の操作を実行します：

   - デバッグ情報をファイルに書き込む場合は、［**デバッグ情報をトレースファイルに書き込む**］をオンにします。

     - 下にあるフィールドで、トレースファイルを保存するフォルダーを指定します。
     - デバッグ情報の詳細レベルを設定します。
     - トレースファイルの最大サイズを指定します。
     - 1つのトレースログの最大ファイル数を指定します。

       Kaspersky Embedded Systems Security は、デバッグするコンポーネントごとに最大数のトレースファイルを作成します。

     - デバッグするコンポーネントを指定します。コンポーネントコードを複数指定する場合は、セミコロンで区切る必要があります。コードは大文字と小文字が区別されます（次の表を参照）。

Kaspersky Embedded Systems Security サブシステムコード

| コンポーネントコード | コンポーネントの名前 |
|---|---|
| * | すべてのコンポーネント |

| | |
|---|---|
| gui | ユーザーインターフェイスサブシステム、Microsoft 管理コンソール形式の Kaspersky Embedded Systems Security スナップイン |
| ak_conn | ネットワークエージェントと Kaspersky Security Center の統合のためのサブシステム |
| bl | コントロールプロセス、Kaspersky Embedded Systems Security コントロールタスクの実装 |
| wp | アンチウイルスによる保護タスクを処理する処理対象プロセス |
| blgate | Kaspersky Embedded Systems Security リモート管理プロセス |
| ods | オンデマンドスキャンサブシステム |
| oas | ファイルのリアルタイム保護サブシステム |
| qb | 隔離およびバックアップのサブシステム |
| scandll | スキャンのための補助モジュール |
| core | アンチウイルス基本機能のためのサブシステム |
| avscan | アンチウイルス処理サブシステム |
| avserv | アンチウイルスのカーネルの管理のためのサブシステム |
| prague | 基本機能のためのサブシステム |
| updater | 定義データベースとソフトウェアモジュールをアップデートするためのサブシステム |
| snmp | SNMP プロトコルサポートサブシステム |
| perfcount | パフォーマンスカウンターサブシステム |

Kaspersky Embedded Systems Security スナップインのトレース設定（gui）および Kaspersky Security Center の管理プラグインのトレース設定（ak_conn）は、それらのコンポーネントの再起動後に適用されます。SNMP プロトコルサポートサブシステムのトレース設定（snmp）は、SNMP サービスが再起動された後に適用されます。パフォーマンスカウンターサブシステムのトレース設定（perfcount）は、パフォーマンスカウンターを使用するすべてのプロセスが再起動された後に適用されます。その他の Kaspersky Embedded Systems Security サブシステムのトレース設定は、クラッシュの診断設定が保存されるとすぐに適用されます。

既定値で、Kaspersky Embedded Systems Security は、すべての Kaspersky Embedded Systems Security コンポーネントのデバッグ情報をログに記録します。

この入力フィールドは、［**デバッグ情報をトレースファイルに書き込む**］をオンにすると使用可能になります。

- ダンプファイルを作成する場合は、［**ダンプファイルの作成**］をオンにしてください。
  - 下にあるフィールドで、ダンプファイルを保存するフォルダーを指定します。

3. ［**OK**］をクリックします。

アプリケーションの設定内容が保護対象デバイスに適用されます。

## タスクスケジュールの管理

Kaspersky Embedded Systems Security タスクの開始スケジュールを設定して、スケジュールに従ってタスクを実行するための設定を行うことができます。

# 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をスケジュールするには：*

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. ［**アプリケーションの設定**］セクションを選択します。
4. ［**スケジュール**］セクションで、［**スケジュールに従って実行する**］をオンにします。

   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。

5. 要件に従ってスケジュールを設定します。それには、次の操作を実行します：
   a. ［**頻度**］リストでは、次の値のいずれかを選択します：
      - ［**時間単位**］：指定された時間間隔でタスクを実行する場合は、［**間隔：<数字> 時間**］で時間数を指定します。
      - ［**日単位**］：指定された日間隔でタスクを実行する場合は、［**間隔：<数字> 日**］で日数を指定します。
      - ［**週単位**］：指定された週間隔でタスクを実行する場合は、［**間隔：<数字> 週**ごと］で週数を指定します。タスクが開始される曜日を指定します（既定では、タスクは月曜日に実行されます）。
      - ［**アプリケーションの起動時**］：Kaspersky Embedded Systems Security が起動するたびにタスクを実行します。
      - ［**定義データベースのアップデート後**］：定義データベースのアップデート後にタスクを実行します。
   b. ［**開始時刻**］にタスクを最初に開始する時刻を指定します。
   c. ［**開始日**］にスケジュールの開始日を指定します。
6. ［**タスクの停止設定**］セクション：
   a. ［**経過時間**］をオンにして、タスクの最長実行時間を時間と分で右側のフィールドに入力します。
   b. ［**タスクを一時停止する**］をオンにして、タスクの実行が一時停止される時間帯の開始と終了の値（24時間で指定）を右側のフィールドに入力します。
7. ［**スケジュールの詳細設定**］セクション：

a. ［**スケジュールをキャンセルする**］をオンにして、スケジュールの適用を停止する日付を指定します。

b. ［**スキップしたタスクを実行する**］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。

c. ［**タスクの開始時刻を次の期間内でランダム化する**］をオンにして、値を分で指定します。

8. ［**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. 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. ［**アプリケーションの設定**］セクションを選択します。
4. ［**スケジュール**］セクションを選択します。
5. 次のいずれかを行います：
   - 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、［**スケジュールに従って実行する**］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無効にする場合は、［**スケジュールに従って実行する**］をオフにします。

     設定されたタスク開始のスケジュール設定は削除されず、次回のタスク開始スケジュールで適用されます。
6. ［**保存**］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*、*誤動作*、*未インストール*、*開始中*。

［*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。

*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. 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. ［**全般**］タブで、［**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。

脆弱性攻撃ブロックコンポーネントのステータスに関する情報は、このテーブルにはありません。

*Kaspersky Security Center Web コンソールの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、［**レポートの表示**］をクリックします。
   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（統計のみ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。

*統計のみ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統計のみモードで開始します。
2. ［**監視とレポート**］ - ［**レポート**］を選択します。
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**］リストの項目の上で、［**レポートの表示**］をクリックします。
   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**］を選択します。
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**］リストの項目の上で、［**レポートの表示**］をクリックします。
   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。

# コンパクト診断インターフェイス

このセクションでは、保護対象デバイスのステータスまたは現在のアプリケーションの動作を確認するためにコンパクト診断インターフェイスを使用する方法や、ダンプファイルおよびトレースファイルの書き込みを設定する方法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。CDI 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 kavfsmui.exe を実行することでも起動できます。

CDI ウィンドウからは、以下の操作が可能です：

- 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。
- ［**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。

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、CDI は使用可能です。パスワードは必要ありません。

CDI 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

*［コンパクトな診断インターフェイス］ウィンドウを開くには、次の処理を実行します：*

1. ツールバーの通知領域の Kaspersky Embedded Systems Security システムトレイアイコンを右クリックします。
2. ［**コンパクト診断インターフェイスを開く**］を選択します。
   ［**コンパクト診断インターフェイス**］ウィンドウが表示されます。

［**保護ステータス**］タブで、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）。

| セクション | ステータス |
| --- | --- |
| **リアルタイム保護ステータス** | 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**処理を実行**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［**統計のみ**］モードで開始されている。<br>• 脆弱性攻撃からの保護とアプリケーション起動コントロールが［**統計のみ**］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［**統計のみ**］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14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>• *製品が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ました。*<br>• *使用許諾契約書に違反しています。* |

| | |
|---|---|
| | • *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

［**統計情報**］タブには、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。

*統計情報を確認するには：*

1. ツールバーの通知領域の Kaspersky Embedded Systems Security システムトレイアイコンを右クリックします。
2. ［**コンパクト診断インターフェイスを開く**］を選択します。
   ［**コンパクト診断インターフェイス**］ウィンドウが表示されます。
3. ［**統計情報**］タブを開きます。
4. 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

このタブでは、現在のタスクおよびアプリケーションプロセスのステータスを確認し、発生する重要なイベントに関する通知をすぐに取得できます。

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る。

- *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。

*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. ツールバーの通知領域の Kaspersky Embedded Systems Security システムトレイアイコンを右クリックします。
2. ［**コンパクト診断インターフェイスを開く**］を選択します。
   ［**コンパクト診断インターフェイス**］ウィンドウが表示されます。
3. ［**現在のアプリケーションの動作**］タブを開きます。
4. ［**タスク**］セクションで次の情報を確認します：
   - **重要領域の簡易スキャンが長期間実行されていません。**

     このフィールドは、簡易スキャンに関する警告が表示された場合にのみ表示されます。

   - **現在実行中**
   - **実行できませんでした**
   - **スケジュールで定義された次の開始**
5. ［**Kaspersky Security Network**］セクションで、次の情報を確認します：
   - **KSN は有効です。ファイル評価サービスが使用可能です。**］または［**保護が無効です**］。
   - **KSN は有効です。ファイル評価サービスが使用可能です。**］、［**アプリケーションの統計情報が KSN に送信されています**］。

     リアルタイムのファイル保護タスクおよびオンデマンドスキャンタスクの実行時に検知したマルウェア（詐欺ソフトウェアなど）に関する情報や、スキャン時のエラーについてのデバッグ情報を送信します。

     フィールドが表示されるのは、KSN の使用タスクの設定で［**Kaspersky Security Network に統計情報を送信**］がオンになっている場合です。
6. ［**Kaspersky Security Center との連携**］セクションで次の情報を確認します：
   - **ローカル管理は許可されています。**
   - **ポリシーが適用されます：<管理サーバー名>。**

## ダンプファイルおよびトレースファイルの書き込みの設定

CDI を使用してダンプファイルおよびトレースファイルの書き込みを設定できます。

アプリケーションコンソールを使用して、トラブルシューティングを設定することもできます。

*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するには、次の処理を実行します：*

1. ツールバーの通知領域の Kaspersky Embedded Systems Security システムトレイアイコンを右クリックします。
2. ［**コンパクト診断インターフェイスを開く**］を選択します。
   ［**コンパクト診断インターフェイス**］ウィンドウが表示されます。
3. ［**トラブルシューティング**］タブを開きます。
4. 必要に応じて、次のトレース設定を変更します：
   a. ［**デバッグ情報をこのフォルダーのトレースファイルに書き込む**］をオンにします。
   b. ［**参照**］ボタンをクリックして、トレースファイルを保存するフォルダーを指定します。
      すべてのコンポーネントで、ログ記録の詳細レベルは［デバッグ］レベル、ログの最大サイズは 50 MB の既定値の設定でトレースが有効になります。
5. 必要に応じて、次のダンプファイル設定を変更します：
   a. ［**誤動作時のダンプファイルをこのフォルダーに作成する**］をオンにします。
   b. ［**参照**］ボタンをクリックして、ダンプファイルを保存するフォルダーを指定します。
6. ［**適用**］をクリックします。
   新しい設定が適用されます。

# Kaspersky Embedded Systems Security の定義データベースとソフトウェアモジュールのアップデート

このセクションでは、Kaspersky Embedded Systems Security の定義データベースとソフトウェアモジュールのアップデートタスク、Kaspersky Embedded Systems Security のアップデートのコピーと定義データベースのアップデートのロールバック、および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タスクを設定する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）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。

## アップデートタスクについて

Kaspersky Embedded Systems Security には、4 つのシステムアップデートタスクが用意されています：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、アップデートのコピー、および定義データベースのロールバック。

既定では、Kaspersky Embedded Systems Security は 1 時間ごとにアップデート元（カスペルスキーのアップデートの保護対象デバイスの 1 つ）に接続します。定義データベース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。

### 定義データベースのアップデート

既定では、定義データベース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。

### ソフトウェアモジュールのアップデート

既定では、利用可能なソフトウェアモジュールのアップデートがアップデート元にあるかどうかチェックされます。インストールしたソフトウェアモジュールの使用を開始するには、保護対象デバイスや Kaspersky Embedded Systems Security の再起動が必要です。

既定では、ソフトウェアモジュールのアップデートタスクは、毎週金曜日の午後 4 時に実行されます（時刻は、保護対象デバイスの地域設定に準じます）。タスクの実行中、適用可能なソフトウェアモジュールの重要なアップデートおよび定期アップデートの有無をチェックします。アップデートは配信されません。

### アップデートのコピー

既定では、タスクの実行中に、定義データベースのアップデートファイルをダウンロードし、指定したネットワークフォルダーやローカルフォルダーに保存します。アップデートファイルは適用されません。

既定では、アップデートのコピータスクは無効になっています。

### 定義データベースのロールバック

タスクの実行中に、以前にインストールしたアップデートの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ロールバックタスクは無効になっています。

## ソフトウェアモジュールのアップデートについて

カスペルスキーから、Kaspersky Embedded Systems Security モジュールのアップデートパッケージが発行される場合があります。アップデートパッケージは、*緊急*（または*重要*）や定期的の場合があります。重要なアップデートパッケージでは、脆弱性やエラーが修正されます。定期的なパッケージでは、新規機能の追加や既存機能の拡張が行われます。

緊急（重要）アップデートパッケージは、カスペルスキーのアップデートサーバーにアップロードされます。ソフトウェアモジュールのアップデートタスクを使用して、これらのパッケージの自動インストールを設定できます。既定では、ソフトウェアモジュールのアップデートタスクは、毎週金曜日の午後 4 時に実行されます（時刻は、保護対象デバイスの地域設定に準じます）。

カスペルスキーは、自動アップデート用の定期的なアップデートパッケージをアップデートサーバーで公開していません。これらのパッケージは、カスペルスキーの Web サイトから手動でダウンロードできます。ソフトウェアモジュールのアップデートタスクを使用して、Kaspersky Embedded Systems Security の定期アップデートのリリースに関する情報を受信できます。

重要なアップデートは、インターネットから取得されて各保護対象デバイスに適用できます。または、1台の保護対象デバイスを仲介として使用して、このデバイスにすべてのアップデートをコピーし、ネットワークの保護対象デバイスに配信することもできます。アップデートをインストールせずにコピーおよび保存するには、アップデートのコピータスクを使用します。

モジュールのアップデートのインストール前に、以前にインストールしたモジュールのバックアップコピーが作成されます。ソフトウェアモジュールのアップデートプロセスが中断されたり、エラーになったりした場合は、以前にインストールしたソフトウェアモジュールが自動的に使用されます。ソフトウェアモジュールは、以前にインストールしたアップデートに手動でロールバックできます。

ダウンロードしたアップデートのインストール中は Kaspersky Security サービスが自動的に停止され、その後再開されます。

## 定義データベースのアップデートについて

保護対象デバイス上に保存されている Kaspersky Embedded Systems Security の定義データベースは、すぐに未アップデートの状態になります。カスペルスキーのウイルスアナリストは、毎日数百個もの新しい脅威を検知し、その識別レコードを作成して、定義データベースのアップデートに追加しています。定義データベースのアップデートは、前回のアップデートの作成以降に検知された脅威の識別用レコードが含まれるファイルやファイルセットです。必要なデバイス保護レベルを維持するには、定義データベースのアップデートを定期的に受信してください。

既定では、インストールされている Kaspersky Embedded Systems Security の定義データベースのアップデートが作成されてから1週間以内に定義データベースがアップデートされない場合、［*定義データベースがアップデートされていません*］イベントが発生します。定義データベースが 2 週間アップデートされていない場合、［*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*］イベントが発生します。データベースの最新のステータスに関する情報は、アプリケーションコンソールツリーの［**Kaspersky Embedded Systems Security**］フォルダーの結果ペインに表示されます。Kaspersky Embedded Systems Security の全般設定を使用して、これらのイベントが発生するまでの個別の日数を指定できます。また、これらのイベントに関する管理者への通知を設定できます。

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。

アップデートは、インターネットからすべての保護対象デバイスにダウンロードできます。または、1台の保護対象デバイスを仲介として使用して、このデバイスにすべてのアップデートをコピーし、保護対象デバイスに配信することもできます。組織で Kaspersky Security Center を使用してデバイスの保護を一元管理する場合、Kaspersky Security Center 管理サーバーをアップデートのダウンロードの仲介として使用できます。

定義データベースのアップデートタスクは手動またはスケジュールに基づいて開始できます。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。

## 組織内で使用されるアンチウイルス製品の定義データベースとモジュールのアップデート方式

アップデートタスクのアップデート元の選択は、組織での定義データベースとプログラムモジュールのアップデートに使用されるスキームに応じて異なります。

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。

  以下のソフトウェア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およびソフトウェアモジュール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 HTTP サーバーや FTP サーバーをアップデート元として設定できます。

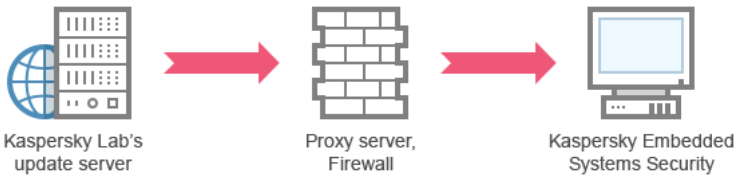


図 1：定義データベースとモジュールをインターネットから直接アップデートする

## 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。それには、次の操作を実行します：
   - 選択した保護対象デバイスで［アップデートのコピー］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。それには、次の操作を実行します：
   - 各保護対象デバイスで、定義データベースのアップデートタスクとソフトウェアモジュールのアップデートタスクを設定します（次の図を参照）：
     a. 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。

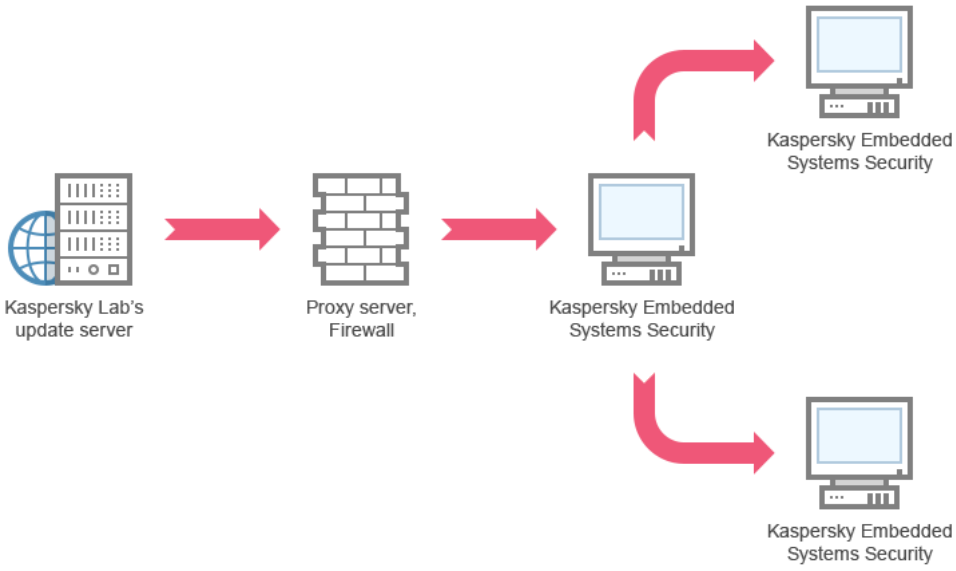


図 2：定義データベースとモジュールを保護対象デバイスの 1 つを経由してアップデートする

## 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 を使用してアンチウイルスによるデバイスの保護を一元的に管理している場合、ローカルエリアネットワークにインストールされている 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（次の図を参照）。

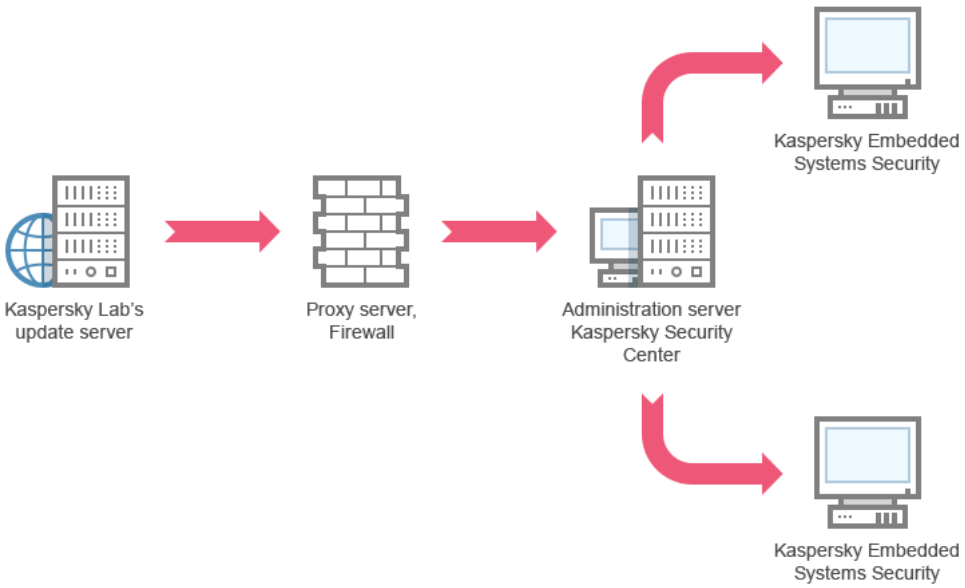


図 3：定義データベースとモジュールを Kaspersky Security Center 管理サーバーを経由してアップデートする

*Kaspersky Security Center 管理サーバーを経由して Kaspersky Embedded Systems Security のアップデートを設定するには：*

1. 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。それには、次の操作を実行します：
   - 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：
     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。
2. 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：
     a. タスクのスケジュールで、開始の頻度として［**管理サーバーがアップデートを取得した後**］を指定します。
     管理サーバーでは、アップデートを受信するたびにタスクが開始されます（推奨の方法です）。

     ［**管理サーバーがアップデートを取得した後**］の開始頻度をアプリケーションコンソールで指定することはできません。
   - 各保護対象デバイスで、定義データベースのアップデートタスクとソフトウェアモジュールのアップデートタスクを設定する：
     a. Kaspersky Security Center の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 Embedded Systems Security 定義データベースをまれにしかアップデートしない場合（1か月に1回から1年に1回）、脅威を検知する可能性が低くなり、アプリケーションコンポーネントによる誤検知が発生する頻度が高くなります。

Kaspersky Security Center の管理サーバーを経由して、アップデートが取得されます。

Kaspersky Security Center 管理サーバーをアップデート配信に使用する予定の場合は、Kaspersky Security Center の配布キットに含まれるアプリケーションコンポーネントであるネットワークエージェントを各保護対象デバイスにインストールします。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。

## アップデートタスクの設定

このセクションでは、Kaspersky Embedded Systems Security のアップデートタスクの設定方法について説明します。

## Kaspersky Embedded Systems Security のアップデート元の使用設定

定義データベースのロールバックタスクを除く各アップデートタスクに対して、1つ以上のアップデート元の指定や、ユーザー定義のアップデート元の追加、指定されたアップデート元との接続設定が行えます。

アップデートタスク設定の変更後、実行中のアップデートタスクに対して新しい設定はすぐには適用されません。設定の内容は、タスクを再起動した時にのみ適用されます。

*アップデート元の種別を指定するには：*

1. アプリケーションコンソールツリーで、［**アップデート**］フォルダーを展開します。
2. 設定するアップデート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。
   ［**タスクの設定**］ウィンドウが開き、［**全般**］タブが表示されます。
4. ［**アップデート元**］セクションで、Kaspersky Embedded Systems Security のアップデート元の種別を選択します：
   - **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**
5. 必要に応じて、ユーザー定義のアップデート元の詳細設定を行います：
   a. ［**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**］をクリックします。

1. 表示される［**アップデートサーバー**］ウィンドウで、ユーザー定義のアップデート元の横にあるチェックボックスをオンまたはオフにして、そのアップデート元を使用するかどうかを指定します。

2. ［OK］をクリックします。

b. ［**全般**］タブの［**アップデート元**］セクションで、［**指定したサーバーが使用できない場合はカスペルスキーのアップデートサーバーを使用する**］をオンまたはオフにします。

6. ［**タスクの設定**］ウィンドウで［**接続設定**］タブを選択して、アップデート元に接続するための設定を行います：

- ［**プロキシサーバー設定を使用してカスペルスキーのアップデートサーバーに接続する**］をオンまたはオフにします。
- ［**プロキシサーバー設定を使用して他のサーバーに接続する**］をオンまたはオフにします。

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方法について詳しくは、「Kaspersky Embedded Systems Security データベースのアップデートタスクの開始と設定」を参照してください。

7. ［OK］をクリックします。

Kaspersky Embedded Systems Security のアップデート元の設定内容が保存され、次回のタスクの起動時に適用されます。

Kaspersky Embedded Systems Security のユーザー定義のアップデート元のリストを管理できます。

*アプリケーションのユーザー定義のアップデート元のリストを編集するには：*

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. 設定するアップデート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。
［**タスクの設定**］ウィンドウが開き、［**全般**］タブが表示されます。

4. ［**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**］をクリックします。
［**アップデートサーバー**］ウィンドウが開きます。

5. 次の操作を実行します：

- 新しいユーザー定義のアップデート元を追加するには、［**追加**］をクリックし、入力フィールドに FTP サーバーまたは HTTP サーバーのアップデートファイルが置かれているフォルダーのアドレスを指定します。ローカルフォルダーまたはネットワークフォルダーは、UNC（ユニバーサルネーミング規約）フォーマットで指定します。**ENTER** キーを押します。
既定では、追加されたフォルダーはアップデート元として使用されます。
- ユーザー定義のアップデート元の使用を無効にするには、リストのアップデート元の横にあるチェックボックスをオフにします。
- ユーザー定義のアップデート元の使用を有効にするには、リストの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 Embedded Systems Security がユーザー定義のアップデート元にアクセスする順序を変更するには、［**上に移動**］および［**下に移動**］を使用し、選択したアップデート元を他のアップデート元より先に使用するか後に使用するかに応じて、リストの先頭の方向または末尾の方向に移動します。

- アップデート元へのパスを変更するには、リストからアップデート元を選択し、［**編集**］をクリックします。入力フィールドで必要な変更を行ったら、**ENTER** キーを押します。

- ユーザー定義のアップデート元を削除するには、リストからアップデート元を選択し、［**削除**］をクリックします。

  ユーザー定義のアップデート元がリストに1つしか残っていない場合、削除することはできません。

6. ［**OK**］をクリックします。

ユーザー定義のアップデート元のリストの変更が保存されます。

## 定義データベースのアップデートタスク実行中のディスク I/O の最適化

定義データベースのアップデートタスクの実行中に、アップデートファイルが保護対象デバイスのローカルディスクに保存されます。アップデートタスクの実行中に、メモリの仮想ドライブにアップデートファイルを保存することで、保護対象デバイスのディスク I/O サブシステムに関する負荷を軽減できます。

この機能は、Microsoft Windows 7 以降のオペレーティングシステムで使用できます。

定義データベースのアップデートタスクの実行中にこの機能を使用すると、余分な論理ドライブがオペレーティングシステムに表示されることがあります。この論理ドライブは、タスクの完了後にオペレーティングシステムから削除されます。

*定義データベースのアップデートタスクの実行中に、保護対象デバイスのディスク I/O サブシステムに関する負荷を軽減するには：*

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**］サブフォルダーを選択します。
3. ［**定義データベースのアップデート**］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。
   ［**タスクの設定**］ウィンドウが開き、［**全般**］タブが表示されます。
4. ［**ディスク I/O 使用の最適化**］セクションで、次の設定を定義します：

   - ［**ディスク I/O の負荷の低減**］をオンまたはオフにします。

   - ［**最適化に使用するメモリ（MB）**］で、メモリのボリューム（MB 単位）を指定します。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 512 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定義データベースのアップデートタスクを実行している時に、機能に割り当てられたメモリの量に応じて、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。

- 値が大きすぎる場合、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することができません。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が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. ［**OK**］をクリックします。

設定の内容が保存され、次回のタスク開始時に適用されます。

## アップデートのコピータスクの設定

*アップデートのコピータスクを設定するには：*

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. ［**アップデートのコピー**］サブフォルダーを選択します。
3. ［**アップデートのコピー**］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。
   ［**タスクの設定**］ウィンドウが表示されます。
4. ［**全般**］タブおよび［**接続設定**］タブで、アップデート元を使用するための設定を行います
5. ［**全般**］タブの［**アップデートのコピーの設定**］セクション：
   - アップデートのコピーの条件を指定します：
     - **定義データベースのアップデートをコピーする**
     - **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**
   - 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。
6. ［**スケジュール**］タブと［**詳細設定**］タブで、タスクの開始スケジュールを設定します。
7. ［**実行用アカウント**］タブで、特定のユーザーアカウントを使用して起動するタスクを設定します。
8. ［**OK**］をクリックします。

設定の内容が保存され、次回のタスク開始時に適用されます。

## ソフトウェアモジュールのアップデートタスクの設定

*ソフトウェアモジュールのアップデートタスクを設定するには：*

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. ［**ソフトウェアモジュールのアップデート**］サブフォルダーを選択します。
3. ［**ソフトウェアモジュールのアップデート**］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。
   ［**タスクの設定**］ウィンドウが表示されます。
4. ［**全般**］タブおよび［**接続設定**］タブで、アップデート元を使用するための設定を行います
5. ［**全般**］タブの［**アップデートの設定**］セクションで、ソフトウェアモジュールをアップデートするための設定を行います：
   - **適用可能になったソフトウェアモジュールの重要なアップデートを確認する**
   - **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しインストールする**
   - **システムの再起動を許可する**
   - **適用可能になったソフトウェアモジュールの定期アップデートの情報を受信する**
6. ［**スケジュール**］タブと［**詳細設定**］タブで、タスクの開始スケジュールを設定します。既定では、ソフトウェアモジュールのアップデートタスクは、毎週金曜日の午後 4 時に実行されます（時刻は、保護対象デバイスの地域設定に準じます）。
7. ［**実行用アカウント**］タブで、特定のユーザーアカウントを使用して起動するタスクを設定します。
8. ［OK］をクリックします。

   設定の内容が保存され、次回のタスク開始時に適用されます。

カスペルスキーは、自動インストール用の定期的なアップデートパッケージをアップデートサーバーで公開していません。これらのパッケージは、カスペルスキーの Web サイトから手動でダウンロードできます。［*新しい重要なアップデートと定期アップデートがあります*］イベントに関する管理者の通知を設定できます。この通知には、定期的なアップデートがダウンロードできる Web ページの URL が含まれます。

## 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適用される前に、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、定義データベース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。

*定義データベースのロールバックタスクを開始するには：*

［**定義データベースのロールバック**］フォルダーの結果ペインで［**開始**］をクリックします。

## アプリケーションモジュールのアップデートのロールバック

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。

ソフトウェアモジュールのアップデートの適用前に、現在使用中のモジュールのバックアップコピーが作成されます。モジュールのアップデート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モジュールが自動的に使用されるようになります。

ソフトウェアモジュールをロールバックするには、Microsoft Windows の**アプリケーションのインストールと削除**機能を使用します。

## 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：*

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. 統計情報を確認するタスクに該当するサブフォルダーを選択します。

   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。

定義データベースのアップデートタスクまたはアップデートのコピータスクを表示している場合、［**統計情報**］セクションには現時点で Kaspersky Embedded Systems Security によってダウンロードされたデータのボリュームが表示されます（**受信したデータ**）。

次の表に、ソフトウェアモジュールのアップデートタスクの詳細を示します。

ソフトウェアモジュールのアップデートタスクに関する情報

| フィールド | 説明 |
|---|---|
| **受信したデータ** | ダウンロードしたデータの総量。 |
| **適用可能な重要なアップデート** | インストール可能な重要なアップデートの数。 |
| **適用可能な定期アップデート** | インストール可能な定期的なアップデートの数。 |
| **アップデート適用中のエラー** | このフィールドの値がゼロ以外の場合、アップデートは適用されませんでした。エラーが発生したアップデートの名前は、タスク実行ログで確認できます。 |

# オブジェクトの隔離とバックアップのコピー

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が駆除されたり削除される前のバックアップや、感染の可能性のあるオブジェクトの隔離について説明します。

# 感染の可能性があるオブジェクトの隔離：隔離

このセクションでは、感染の可能性があるオブジェクトを隔離して分離する方法、および隔離の設定を行う方法について説明します。

# 感染の可能性があるオブジェクトの隔離について

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。

# 隔離オブジェクトの表示

隔離されたオブジェクトは、アプリケーションコンソールの［**隔離**］フォルダーで確認できます。

*隔離されたオブジェクトを表示するには、*

1. アプリケーションコンソールツリーで、［**保管領域**］フォルダーを展開します。
2. ［**隔離**］サブフォルダーを選択します。

   選択したフォルダーの結果ペインに、隔離されたオブジェクトの情報が表示されます。

*隔離されたオブジェクトのリストで目的の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。

# 隔離オブジェクトの並べ替え

既定では、隔離されたオブジェクトリスト内のオブジェクトは、隔離された日付の新しい順に表示されます。目的のオブジェクトを見つけるため、オブジェクトに関する情報の列でオブジェクトを並べ替えることができます。［**隔離**］フォルダーを閉じて再度開いた場合、並べ替えの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

*オブジェク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、［**保管領域**］フォルダーを展開します。
2. ［**隔離**］サブフォルダーを選択します。

3. ［**隔離**］フォルダーの結果ペインで、リストのオブジェクトの並べ替えに使用する列の見出しを選択します。

選択した設定に基づいて、リストのオブジェクトの表示順が変わります。

## 隔離オブジェクトのフィルタリング

目的の隔離されたオブジェクトを検索するために、リストでオブジェクトをフィルタリングして、指定したフィルタリング条件（フィルター）を満たすオブジェクトのみ表示することができます。［**隔離**］フォルダーを閉じて再度開いた場合、フィルタリングの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

*1 つまたは複数のフィルターを指定するには：*

1. アプリケーションコンソールツリーで、［**保管領域**］フォルダーを展開します。
2. ［**隔離**］サブフォルダーを選択します。
3. ファイル名の上でコンテキストメニューを開き、［**フィルター**］を選択します。
   ［**フィルターの設定**］ウィンドウが表示されます。
4. 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、フィルターの基準となるフィールドを選択します。
   b. ［**演算子**］リストで、フィルタリング条件を選択します。リストのフィルタリング条件は、［**フィールド名**］リストで選択した値に応じて異なる場合があります。
   c. ［**フィールド値**］にフィルターの値を入力するか、リストから選択します。
   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。追加するフィルターごとにこれらの手順を繰り返します。フィルターの使用時は、次のガイドラインに従います：

   - 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。
   - フィルターを削除するには、フィルターのリストから削除するフィルターを選択し、［**削除**］をクリックします。
   - フィルターを編集するには、［**フィルターの設定**］ウィンドウのリストからフィルターを選択します。次に、［**フィールド名**］、［**演算子**］、または［**フィールド値**］で、対象の値を変更して、［**置換**］をクリックします。
5. すべてのフィルターが追加されたら、［**適用**］をクリックします。

作成したフィルターが保存されます。

*隔離されたすべてのオブジェクトの表示に戻るには：*

［**隔離**］フォルダーのコンテキストメニューで、［**フィルターの削除**］を選択します。

## 隔離のスキャン

既定では、定義データベースをアップデートするごとに、隔離のスキャンローカルシステムタスクが実行されます。以下の表に、タスクの設定を示します。隔離のスキャンタスクの設定は変更できません。

タスクの起動スケジュールの設定、手動でのタスクの開始、タスクの開始に使用するアカウント権限の変更が可能です。

定義データベースのアップデート後に隔離されたオブジェクトがスキャンされると、Kaspersky Embedded Systems Security により一部のオブジェクトが感染していないとして再分類されることがあります。それらのオブジェクトのステータスは「**誤検知**」に変更されます。その他のオブジェクトは、感染しているとして再分類されます。この場合、そのようなオブジェクトは隔離のスキャンタスクの設定に従い、駆除または駆除できない場合は削除されます。

隔離のスキャンタスクの設定

| 隔離のスキャンタスクの設定 | 値 |
|---|---|
| スキャン範囲 | 隔離フォルダー |
| セキュリティ設定 | スキャン範囲全体で同一。これらの値は次の表に示されています。 |

隔離のスキャンタスクのスキャン設定

| セキュリティ設定 | 値 |
|---|---|
| **オブジェクトをスキャン** | スキャン範囲に含まれているすべてのオブジェクト |
| **パフォーマンス** | 無効 |
| **感染などの問題があるオブジェクトの処理** | 駆除する。駆除できない場合は削除する |
| **感染の可能性があるオブジェクトの処理** | スキップ |
| **除外するファイル** | なし |
| **検知しない** | なし |
| **スキャン時間が次を超えたら停止する（秒）** | 設定なし |
| **次のサイズより大きいオブジェクトはスキャンしない（MB）** | 設定なし |
| **NTFS 代替データストリームをスキャン** | 有効 |
| **ディスクのブートセクターと MBR をスキャン** | 無効 |
| **iChecker を使用する** | 無効 |
| **iSwift を使用する** | 無効 |
| **複合オブジェクトをスキャンします** | • **アーカイブ***<br>• **SFX アーカイブ***<br>• **圧縮されたオブジェクト***<br>• **OLE 埋め込みオブジェクト***<br>* **作成または変更されたファイルのみをスキャン**することはできません。 |

| | |
|---|---|
| **ファイルの Microsoft の署名をチェックする** | 実行されていません |
| **ヒューリスティックアナライザーを使用する** | 有効（分析レベル［**高**］） |
| **信頼ゾーン** | オフ |

## 隔離されたオブジェクトの復元

Kaspersky Embedded Systems Security では、感染の可能性があるオブジェクトを暗号化して隔離に移動し、あらゆる有害な影響から保護対象デバイスを保護します。

オブジェクトは隔離から復元できます。これは、次の場合に必要となる可能性があります：

- アップデートした定義データベースによる隔離のスキャンの後に、オブジェクトのステータスが［**誤検知**］や［**駆除済み**］に変更された場合。
- 保護対象デバイスに対してオブジェクトが無害であると思われ、使用したい場合。その後のスキャンで、このオブジェクトを隔離したくない場合は、ファイルのリアルタイム保護タスクやオンデマンドスキャンタスクの処理から、このオブジェクトを除外できます。この操作を実行するには、それらのタスクのセキュリティ設定でこのオブジェクトを［**除外するファイル**］（ファイル名）または［**検知しない**］に指定するか、信頼ゾーンに追加します。

オブジェクトの復元時に、復元したオブジェクト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やネットワーク上のその他のデバイスのカスタムフォルダーです。

保護対象デバイスで復元されたオブジェクトを保管するために使用されるフォルダーを指定できます。このスキャン対象のオブジェクト用に、特別なセキュリティ設定を設定できます。このフォルダーのパスは、［隔離］設定で設定されます。

隔離からオブジェクトを復元すると、保護対象デバイスが感染する可能性があります。

オブジェクトを復元して、そのコピーを隔離に保存して後で使用できます。たとえば、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場合です。

隔離されたオブジェクトがアーカイブなどの複合オブジェクトに含まれる場合、そのオブジェクトは復元中の複合オブジェクトの中には含まれず、選択したフォルダーに個別に保存されます。

1つまたは複数のオブジェクトを復元できます。

*隔離されたオブジェクトを復元するには、次の手順を実行します：*

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. ［**隔離**］サブフォルダーを選択します。
3. ［**隔離**］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。

［**オブジェクトを復元**］ウィンドウが開きます。

4. ［**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。

5. 次のいずれかの処理を実行します：

- 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。
- この設定で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。

6. オブジェクトの復元後にこのオブジェクトのコピーを*隔離*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。

7. 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。

選択したすべてのオブジェクトが復元され、指定された場所に保存されます。［**元のフォルダーに復元**］を選択した場合、各オブジェクトは前の場所に保存されます。［**既定の復元用フォルダーに復元**］または［**ローカルコンピューターのフォルダーに復元**］を選択した場合、すべてのオブジェクトは指定したフォルダーに保存されます。

8. ［**OK**］をクリックします。

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あり**］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（この処理の手順 4 を参照してください）。

## オブジェクトの隔離への移動

ファイルを手動で隔離できます。

*ファイルを隔離するには：*

1. アプリケーションコンソールツリーで、［**隔離**］フォルダーのコンテキストメニューを開きます。
2. ［**追加**］を選択します。
3. ［**ファイルを開く**］ウィンドウで、ディスク上の隔離するファイルを選択します。
4. ［**OK**］をクリックします。

選択したファイルが隔離されます。

## 隔離からのオブジェクトの削除

アップデートされた定義データベースで隔離のスキャン中にステータスが「*感染*」に変更され、駆除できなかった場合には、隔離のスキャンタスクの設定に基づき、隔離フォルダーからオブジェクトが自動的に削除されます。他のオブジェクトは隔離から削除されません。

1つまたは複数のオブジェクトを隔離から削除できます。

*1 つまたは複数のオブジェクトを隔離から削除するには：*

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. ［**隔離**］サブフォルダーを選択します。
3. 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削除するには、そのオブジェクトの名前の上でコンテキストメニューを開き［**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** キーまたは **Shift** キーを使用して削除対象のオブジェクトを選択し、選択したいずれかのオブジェクトのコンテキストメニューを開いて、［**削除**］を選択します。
4. 確認ウィンドウで［**はい**］をクリックして操作を確認します。

選択したオブジェクトが隔離から削除されます。

## 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

ファイル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。このようなファイルは、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。

分析用に送信できるのは、隔離されたファイルだけです。隔離されたファイルは暗号化された形式で保管され、送信の際、メールサーバーにインストールされている Kaspersky Security によって削除されません。

ライセンスの有効期間終了後に、隔離されたオブジェクトを分析のためにカスペルスキーに送信することはできません。

*ファイルを分析のためにカスペルスキーに送信するには：*

1. ファイルが隔離されていない場合は、まず［**隔離**］に移動します。
2. ［**隔離**］フォルダーで分析用に送信するファイルのコンテキストメニューを開き、［**オブジェクトを解析用に送信**］を選択します。
3. 選択したオブジェクトを分析に送信する場合は、表示される確認ウィンドウで［**はい**］をクリックします。
4. 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でメールクライアントが設定されている場合は、新しいメールメッセージが作成されます。このメッセージを確認して［**送信**］をクリックします。

   ［**受信者**］にはカスペルスキーのメールアドレス（newvirus@kaspersky.com）が含まれます。［件名］には「隔離されたオブジェクト」というテキストが含まれます。

   メッセージの本文には、次のテキストが含まれます：「オブジェクトがカスペルスキーに送信されて解析されます」。メッセージ本文に、ファイルに関する追加情報（感染の可能性や危険性があると思われる理由や、ファイルの動作、システムへ与えた影響など）を含めることができます。

   アーカイブ <オブジェクト名>.cab がメッセージに添付されます。このアーカイブには、暗号化されたオブジェクトが含まれるファイル <uuid>.klq、抽出されたオブジェクトに関する情報が含まれるファイル <uuid>.txt、および保護対象デバイスにインストールされている Kaspersky Embedded Systems Security とオペレーティングシステムに関する情報が含まれるファイル Sysinfo.txt が含まれます。Sysinfo.txt に含まれる情報は、次のとおりです：

   - オペレーティングシステムの名前とバージョン。
   - Kaspersky Embedded Systems Security の名前とバージョン。
   - インストールされている最新の定義データベースのアップデートの公開日時。
   - 現在のライセンス。

   この情報は、カスペルスキーのアンチウイルスアナリストがファイルをより早く効率的に分析するのに必要です。ただし、この情報を送信したくない場合は、アーカイブからファイル Sysinfo.txt を削除できます。

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にメールクライアントがインストールされていない場合、選択した暗号化されているオブジェクトのファイル保存を確認するウィンドウが表示されます。このファイルは、手動でカスペルスキーに送信できます。

*暗号化されたオブジェクトをファイルに保存するには：*

1. オブジェクトの保存について確認するウィンドウが表示されたら、［**OK**］をクリックします。
2. 保護対象デバイスのドライブ上のフォルダーか、オブジェクトが含まれるファイルの保存先のネットワークフォルダーを選択します。

オブジェクトが CAB ファイルに保存されます。

## 隔離の設定

隔離の設定を行えます。新しい隔離設定は、保存後即座に適用されます。

*隔離の設定を行うには：*

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. ［**隔離**］サブフォルダーのコンテキストメニューを開きます。
3. ［**プロパティ**］を選択します。
4. ［**隔離**］ウィンドウで、要件に従って、必要な隔離設定を行います：
   - ［**隔離設定**］セクション：
     - **隔離フォルダー**
     - **隔離の最大サイズ（MB）**
     - **空き容量のしきい値（MB）**

     ［隔離］に配置されているオブジェクトのサイズが隔離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、隔離へのオブジェクトの配置は継続されます。
   - ［**復元設定**］セクション：
     - **オブジェクトの復元先フォルダー**
5. ［**OK**］をクリックします。

新しい隔離の設定が保存されます。

## 隔離の統計情報

隔離されたオブジェクトの数に関する情報である、隔離の統計情報を確認できます。

*隔離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、［**隔離**］フォルダーのコンテキストメニューを開き、［**統計情報**］を選択します。

［**隔離の統計情報**］ウィンドウに、隔離に現在保存されているオブジェクトの数に関する情報が表示されます（次の表を参照）：

| フィールド | 説明 |
| --- | --- |
| **感染の可能性があるオブジェクト** | Kaspersky Embedded Systems Security が感染の可能性を検知したオブジェクトの数。 |
| **使用済み隔離領域** | 隔離内のデータの合計サイズ。 |
| **誤検知** | アップデートされた定義データベースを使用した隔離スキャン時に感染していないと分類されたために、*誤検知*ステータスを受け取ったオブジェクトの数。 |
| **駆除されたオブジェクト** | 隔離のスキャン後に*駆除済み*ステータスを受け取ったオブジェクトの数。 |
| **オブジェクトの合計数** | 隔離内のオブジェクトの合計数。 |

## 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

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のバックアップと、バックアップの設定方法に関する情報を提供します。

## 駆除または削除前のオブジェクトのバックアップについて

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。

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、保護対象デバイスまたはローカルエリアネットワークの他の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。

## バックアップに保存されたオブジェクトの表示

オブジェクトをバックアップフォルダーで表示する唯一の方法は、［**バックアップ**］フォルダーでアプリケーションコンソールを使用することです。これらのファイルを Microsoft Windows ファイルマネージャーで表示することはできません。

*オブジェクトをバックアップで表示するには：*

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. ［**バックアップ**］サブフォルダーを選択します。

   選択したフォルダーの結果ペインに、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。目的の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。

［**バックアップ**］フォルダーを閉じて再度開いた場合、並べ替えの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

*［バックアップ］内のファイルを並べ替えるには：*

1. アプリケーションコンソールツリーで、［**保管領域**］フォルダーを展開します。
2. ［**バックアップ**］サブフォルダーを選択します。
3. ［**バックアップ**］内の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］内の目的のファイルを検索するために、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条件（フィルター）を満たすファイルのみを［**バックアップ**］フォルダーに表示することができます。

［**バックアップ**］フォルダーを閉じて再度開いた場合、並べ替えの結果は保存されています。アプリケーションコンソールを閉じる場合は、msc ファイルを保存して、その msc ファイルから再度開きます。

*［バックアップ］内のファイル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、［**バックアップ**］フォルダーのコンテキストメニューを開き、［**フィルター**］を選択します。

   ［**フィルターの設定**］ウィンドウが表示されます。
2. 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、フィルターの基準となるフィールドを選択します。

b. ［**演算子**］リストで、フィルタリング条件を選択します。リストのフィルタリング条件は、［**フィールド名**］で選択した値に応じて異なる場合があります。

c. ［**フィールド値**］にフィルターの値を入力するか、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。追加するフィルターごとにこれらの手順を繰り返します。フィルターの使用時は、次のガイドラインに従います：

- 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。
- フィルターを削除するには、フィルターのリストから削除するフィルターを選択し、［**削除**］をクリックします。
- フィルターを編集するには、［**フィルターの設定**］ウィンドウのフィルターリストからフィルターを選択して、［**フィールド名**］、［**演算子**］、または［**フィールド値**］で、対象の値を変更して、［**置換**］をクリックします。

すべてのフィルターが追加されたら、［**適用**］をクリックします。指定したフィルターに一致するファイルのみがリストに表示されます。

*［バックアップ］に格納されているオブジェクトのリストに含まれるすべてのファイルを表示するには：*

［**バックアップ**］フォルダーのコンテキストメニューで、［**フィルターの削除**］を選択します。

## 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または感染の可能性があると判断されないようにする時には、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。除外するには、対応するタスクの［**除外するファイル**］設定または［**検知しない**］設定で、このファイルを指定します。

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やネットワーク上のその他のデバイスのカスタムフォルダーです。

保護対象デバイスで復元されたオブジェクトを保管するためのフォルダーを指定できます。このスキャン対象のオブジェクト用に、特別なセキュリティ設定を設定できます。このフォルダーへのパスは、バックアップ設定で指定します。

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。

*バックアップからのファイルを復元するには：*

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. ［**バックアップ**］サブフォルダーを選択します。
3. ［**バックアップ**］フォルダーの結果ペインで、次のいずれかの操作を実行します：
   - 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。

   ［**オブジェクトを復元**］ウィンドウが開きます。
4. ［**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。

5. 次のいずれかの処理を実行します：
   - 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。
   - この設定で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。
6. 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）。
7. 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。

   選択したすべてのオブジェクトが復元され、指定された場所に保存されます。［**元のフォルダーに復元**］を選択した場合、各オブジェクトは前の場所に保存されます。［**既定の復元用フォルダーに復元**］または［**ローカルコンピューターのフォルダーに復元**］を選択した場合、すべてのオブジェクトは指定したフォルダーに保存されます。

8. ［**OK**］をクリックします。

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あり**］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（この処理の手順 4 を参照してください）。

## バックアップからのファイルの削除

*1 つまたは複数のファイルをバックアップから削除するには：*

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. ［**バックアップ**］サブフォルダーを選択します。
3. 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削除するには、そのオブジェクトの名前の上でコンテキストメニューを開き［**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** キーまたは **Shift** キーを使用して削除対象のオブジェクトを選択し、選択したいずれかのオブジェクトのコンテキストメニューを開いて、［**削除**］を選択します。

4. 確認ウィンドウで［**はい**］をクリックして操作を確認します。

選択したファイルが［バックアップ］から削除されます。

## バックアップの設定

*バックアップの設定を行うには：*

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. ［**バックアップ**］サブフォルダーのコンテキストメニューを開きます。
3. ［**プロパティ**］を選択します。
4. ［**バックアップのプロパティ**］ウィンドウで、要件に従って、必要なバックアップ設定を行います：
   ［**バックアップ設定**］セクション：
   - **バックアップフォルダー**
   - **バックアップの最大サイズ（MB）**
   - **空き容量のしきい値（MB）**

     ［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。

   ［**復元設定**］セクション：
   - **オブジェクトの復元先フォルダー**
5. ［OK］をクリックします。

設定したバックアップの内容が保存されます。

## 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：*

アプリケーションコンソールツリーで、［**バックアップ**］フォルダーのコンテキストメニューを開き、［**統計情報**］を選択します。［**バックアップの統計情報**］ウィンドウが開きます。

［**バックアップの統計情報**］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量。ファイルサイズは暗号化された形式で計算されます。 |
| **オブジェクトの合計数** | 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：ブロック対象コンピューター

このセクションでは、リモートデバイスをブロックする方法と、ブロック対象コンピューターの保管領域を設定する方法について説明します。

# ブロック対象コンピューターの保管領域について

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、次のブロック対象コンピューターの保管領域が既定でインストールされます：ファイルのリアルタイム保護、ネットワーク脅威対策。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、リモートコンピューターから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出します。すべての保護対象デバイスのブロック対象コンピューターに関する情報は、Kaspersky Security Center に送信されます。Kaspersky Embedded Systems Security は、ブロック対象コンピューターのリストにあるすべてのリモートコンピューターによる、保護対象デバイスの共有フォルダーまたはネットワーク接続ストレージのフォルダーへのアクセスをブロックします。

ブロック対象コンピューターの保管領域は、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）：

- ファイルのリアルタイム保護タスクの場合：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動作が検知され、ファイルのリアルタイム保護タスク設定で［**悪意のある活動を示すコンピューター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**］がオンにされている。

- 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。

悪意のある動作または暗号化の試行が検知されると、タスクは攻撃元のコンピューターに関する情報をブロック対象コンピューターの保管領域に送信し、コンピューターのブロックに関する*警告*イベントが作成されます。このコンピューター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。

攻撃元のコンピューターの LUID（ローカルで一意な識別子）がブロック対象コンピューター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、ブロック対象コンピューターのリストに 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、ブロック対象コンピューター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。ブロック対象コンピューターのリストから削除されると、ネットワークファイルリソースへのコンピューターのアクセスは自動的に復元されます。ブロック対象コンピューター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、ブロック対象コンピューターの保管領域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、ブロック対象コンピューターの設定を変更することはできません。

# 管理プラグインからブロック対象コンピューターを管理する

このセクションでは、管理プラグインインターフェイスからブロック対象コンピューターの保管領域を設定する方法について説明します。

# 信頼しないコンピューターのブロックの有効化

悪意ある動作または暗号化動作を示すコンピューターを［**ブロック対象コンピューター**］の保管領域に追加し、これらのコンピューター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、次のタスクのうち最低1つを有効な状態で実行する必要があります：

- ファイルのリアルタイム保護
- ネットワーク脅威対策

*ファイルのリアルタイム保護タスクの設定：*

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. ［**ポリシー**］タブを選択して、［**<ポリシー名>**］ - ［**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**］ブロックの［**設定**］を順に開きます。
   ［**コンピューターのリアルタイム保護**］ウィンドウが開きます。
3. ［**他のコンポーネントとの連携**］セクションで、ファイルのリアルタイム保護タスクの実行中に悪意のある動作が検知されたコンピューターに対して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、［**悪意のある動作を示すコンピューターを信頼しないリストに追加する**］をオンにします。
4. タスクが開始されていない場合、［**タスク管理**］タブを開きます：
   a. ［**スケジュールに従って実行する**］をオンにします。
   b. ドロップダウンリストから［**アプリケーションの起動時**］の頻度を選択します。
5. ［**コンピューターのリアルタイム保護**］ウィンドウで［**OK**］をクリックします。

新しい設定が保存されます。

*ネットワーク脅威対策タスクの設定：*

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。
5. 表示された［**プロパティ：<ポリシー名>**］ウィンドウで、セクションを選択します。
6. ［**ネットワーク脅威対策**］サブセクションで［**設定**］をクリックします。
   ［**ネットワーク脅威対策**］ウィンドウが開きます。
7. ［**全般**］タブを開きます。
8. ［**処理モード**］セクションで、［**攻撃の検知時に接続をブロックする**］の処理モードを選択します。

このチェックボックスでは、ブロック対象コンピューターのリストに、ネットワーク攻撃の典型的な活動を示すコンピューターの追加を有効または無効にします。

このモードでは、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、検知された動作に関するイベントが記録されて、ブロック対象コンピューターのリストにネットワーク攻撃の典型的な活動を示すコンピューターの IP アドレスが追加されます。

既定では、このモードが選択されます。

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。

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。

9. タスクが開始されていない場合、［**タスク管理**］タブを開きます：
   a. ［**スケジュールに従って実行する**］をオンにします。
   b. ドロップダウンリストから［**アプリケーションの起動時**］の頻度を選択します。
10. ウィンドウで、［OK］をクリックします。
11. 新しい設定が保存されます。

## ブロック対象コンピューターの設定

*ブロック対象コンピューターの保管領域を設定するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**詳細設定**］セクションで、［**保管領域**］サブセクションの［**設定**］をクリックします。
   ［**保管領域の設定**］ウィンドウが表示されます。
5. ［**ブロック対象コンピューターの保管領域**］タブの［**コンピューターのブロック期間**］セクションで、ブロック対象コンピューターが、ブロックされてからネットワークファイルリソースに再びアクセスできるようになるまでの日数および時間（時間、分）を指定します。

6. ［**OK**］をクリックします。

# アプリケーションコンソールからブロック対象コンピューターを管理する

このセクションでは、アプリケーションコンソールのインターフェイスからブロック対象コンピューターの保管領域を設定する方法について説明します。

## 信頼しないコンピューターのブロックの有効化

悪意ある動作または暗号化動作を示すコンピューターを［**ブロック対象コンピューター**］の保管領域に追加し、これらのコンピューター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、次のタスクのうち1つ以上のタスクを有効な状態で実行する必要があります：

- ファイルのリアルタイム保護
- ネットワーク脅威対策

*ファイルのリアルタイム保護タスクの設定：*

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. ［**ファイルのリアルタイム保護**］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。
   ［**タスクの設定**］ウィンドウが表示されます。
4. ［**高**］セクションで、［**悪意のある活動を示すコンピューター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**］をオンにすると、ファイルのリアルタイム保護の実行中に悪意ある活動が検知されたコンピューターをブロックできます。
5. タスクが開始されていない場合、［**スケジュール**］タブを開きます：
   a. ［**スケジュールに従って実行する**］をオンにします。
   b. ドロップダウンリストから［**アプリケーションの起動時**］の頻度を選択します。
6. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

新しい設定が保存されます。

*ネットワーク脅威対策タスクの設定：*

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. ［**ネットワーク脅威対策**］サブフォルダーを選択します。
3. ［**ネットワーク脅威対策**］フォルダーの詳細ペインで、［**プロパティ**］をクリックします。

4. ［**タスクの設定**］ウィンドウが表示されます。

5. ［**全般**］タブを開きます。

6. ［**処理モード**］セクションで、［**攻撃の検知時に接続をブロックする**］の処理モードを選択します。

   このチェックボックスでは、ブロック対象コンピューターのリストに、ネットワーク攻撃の典型的な活動を示すコンピューターの追加を有効または無効にします。

   このモードでは、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、検知された動作に関するイベントが記録されて、ブロック対象コンピューターのリストにネットワーク攻撃の典型的な活動を示すコンピューターの IP アドレスが追加されます。

   既定では、このモードが選択されます。

   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。

   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。

7. ［**タスクが実行されていない時にトラフィック分析を停止しない**］をオンまたはオフにします。

   このチェックボックスをオンにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、攻撃しているコンピューターからのネットワーク活動が選択された処理モードに応じてブロックされます。

   このチェックボックスをオフにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作はスキャンされず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

   既定では、このチェックボックスはオフです。

8. タスクが開始されていない場合、［**スケジュール**］タブを開きます：

   a. ［**スケジュールに従って実行する**］をオンにします。

   b. ドロップダウンリストから［**アプリケーションの起動時**］の頻度を選択します。

9. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

新しい設定が保存されます。

## ブロック対象コンピューターの設定

*ブロック対象コンピューターの保管領域を設定するには：*

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. ［**ブロック対象コンピューター**］サブフォルダーのコンテキストメニューを開きます。

3. ［**プロパティ**］メニューオプションを選択します。
   ［**ブロック対象コンピューターの保管領域の設定**］ウィンドウが表示されます。

4. ［**コンピューターのブロック期間**］セクションで、ブロック対象コンピューターが、ブロックされてからネットワークファイルリソースに再びアクセスできるようになるまでの日数および時間（時間、分）を指定します。

5. ［**OK**］をクリックします。

6. すべてのブロック対象コンピューターへのアクセスを復元するには：

   a. ［**ブロック対象コンピューター**］サブフォルダーのコンテキストメニューを開きます。

   b. ［**すべてブロック解除**］オプションを選択します。
   すべてのコンピューターがリストから削除されてブロック解除されます。

7. ブロック対象コンピューターのリストからいくつかのコンピューターを削除するには：

   a. 結果ペインに表示されるブロック対象コンピューターのリストで、1つ以上のコンピューターを選択します。

   b. ［**ブロック対象コンピューター**］サブフォルダーのコンテキストメニューを開きます。

   c. ［**選択項目のブロック解除**］オプションを選択します。
   選択したコンピューターがブロック解除されます。

## Web プラグインからブロック対象コンピューターを管理する

このセクションでは、Web プラグインのインターフェイスからブロック対象コンピューターの保管領域を設定する方法について説明します。

## コンピューターのブロックの有効化

悪意ある動作または暗号化動作を示すコンピューターを［**ブロック対象コンピューター**］の保管領域に追加し、これらのコンピューター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、次のタスクのうち最低1つを有効な状態で実行する必要があります：

- ファイルのリアルタイム保護
- ネットワーク脅威対策

*ファイルのリアルタイム保護タスクの設定：*

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。

5. ［**ファイルのリアルタイム保護**］サブセクションで［**設定**］をクリックします。

6. ［**他のコンポーネントとの連携**］セクションで、［**悪意のある活動を示すコンピューター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**］をオンにすると、ファイルのリアルタイム保護タスクの実行中に悪意ある動作が検知されたコンピューター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できます。

7. タスクが開始されていない場合、［**タスク管理**］タブを開きます：

   a. ［**スケジュールに従って実行する**］をオンにします。

   b. ドロップダウンリストから［**アプリケーションの起動時**］の頻度を選択します。

8. ［**保存**］をクリックします。

新しい設定が保存されます。

## ブロック対象コンピューターの設定

*ブロック対象コンピューターの保管領域を設定するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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. ［**詳細設定**］セクションで、［**保管領域**］サブセクションの［**設定**］をクリックします。
   ［**保管領域**］ウィンドウが表示されます。

7. ［**ブロック対象コンピューターの保管領域**］タブの［**コンピューターのブロック期間**］セクションで、ブロック対象コンピューターが、ブロックされてからネットワークファイルリソースに再びアクセスできるようになるまでの日数および時間（時間、分）を指定します。

8. ［**OK**］をクリックします。

# 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 のログ（システム監査ログ、タスク実行ログ、イベントログ）の使用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：

- 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：

- **実行ログ**：タスク実行ログには、タスクの現在のステータスとタスクの実行中に発生したイベントの情報が含まれます。
- **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。
- **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 ビューアーで確認できます。
- **セキュリティログ**：セキュリティログには、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が含まれています。

Kaspersky Embedded Systems Security の使用中に、Kaspersky Embedded Systems Security または個々のタスクが異常終了したり、開始されなかったりする問題が発生した場合、その問題を診断するために、Kaspersky Embedded Systems Security プロセスのトレースファイルとダンプファイルを作成し、この情報が含まれるファイルをカスペルスキーのテクニカルサポートに送信できます。

Kaspersky Embedded Systems Security からは、トレースファイルまたはダンプファイルは自動的に送信されません。診断データは、必要な権限を持つユーザーのみが送信できます。

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ユーザーが選択し、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。

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

  KESS-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

KESS-KSC-EVENTS.ZIP をダウンロード

## 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などの情報がログに記録されます。アプリケーションコンソールで［**システム監査ログ**］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無期限に保存されます。システム監査ログでの記録の保存期間を指定します。

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。

## システム監査ログでのイベントの並べ替え

既定では、システム監査ログノードのイベントは、新しいものから順に表示されます。

イベントは、［**イベント**］列以外の列の内容で並べ替えできます。

*システム監査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**］フォルダーを展開します。
2. ［**システム監査ログ**］サブフォルダーを選択します。
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、次にシステム監査ログを表示する時まで保存されます。

## システム監査ログで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、システム監査ログを設定できます。

*システム監査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. ［**システム監査ログ**］サブフォルダーのコンテキストメニューを開き、［**フィルター**］を選択します。
   ［**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**］で、イベントをフィルタリング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. ［**適用**］をクリックして、フィルタリング条件をシステム監査ログに保存します。

システム監査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、次にシステム監査ログを表示する時まで保存されます。

*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. ［**システム監査ログ**］サブフォルダーのコンテキストメニューを開き、［**フィルターの削除**］を選択します。

システム監査ログのイベントのリストに、すべてのイベントが表示されます。

## システム監査ログからのイベントの削除

既定では、記録はシステム監査ログに無期限に保存されます。システム監査ログでの記録の保存期間を指定できます。

システム監査ログからすべてのイベントを手動で削除できます。

*システム監査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. ［**システム監査ログ**］サブフォルダーのコンテキストメニューを開き、［**クリア**］を選択します。
3. 次のいずれかの処理を実行します：

- システム監査ログからイベントを削除する前に、ログの内容を CSV 形式や TXT 形式のファイルとして保存するには、削除の確認ウィンドウで［**はい**］をクリックします。ウィンドウが開いたら、ファイルの名前と場所を指定します。
- ログの内容をファイルとして保存しない場合は、削除の確認ウィンドウで［**いいえ**］をクリックします。

システム監査ログがクリアされます。

# 実行ログ

このセクションでは、Kaspersky Embedded Systems Security のタスク実行ログに関する情報、およびタスク実行ログの管理方法について説明します。

## タスク実行ログについて

アプリケーションコンソールで［**実行ログ**］フォルダーを選択すると、結果ペインに Kaspersky Embedded Systems Security タスクの実行に関する情報が表示されます。

各タスクのログでは、タスク実行の統計、タスクの開始時から本製品で処理された各オブジェクトの詳細、およびタスクの設定を表示できます。

既定では、レコードはタスクの完了から 30 日間、タスク実行ログに保存されます。タスク実行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イベントリストの表示

*タスク実行ログを表示するには：*

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. ［**実行ログ**］を選択します。

   Kaspersky Embedded Systems Security のタスク実行ログに保存されているイベントのリストが、結果ペインに表示されます。

イベントは、列で並べ替えたりフィルタリングしたりすることができます。

## タスク実行ログの並べ替え

既定では、タスク実行ログは新しいものから順に表示されます。イベントは、列で並べ替えることができます。

*タスク実行ログを並べ替えるには：*

1. アプリケーションコンソールツリーで、［**ログと通知**］フォルダーを展開します。
2. ［**実行ログ**］を選択します。
3. 結果ペインで、タスク実行ログ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、次にタスク実行ログを表示するまで保存されます。

# タスク実行ログのフィルタリング

指定したフィルタリング条件を満たすタスク実行ログのみが表示されるように、タスク実行ログのリストを設定できます。

*タスク実行ログ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. ［**実行ログ**］サブフォルダーのコンテキストメニューを開き、［**フィルター**］を選択します。
   ［**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**］で、タスク実行ログをフィルタリング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. ［**適用**］をクリックして、フィルタリング条件をタスク実行ログのリストに保存します。

タスク実行ログのリストには、フィルタリング条件を満たすタスク実行ログのみが表示されます。フィルタリングの結果は、次にタスク実行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. ［**実行ログ**］サブフォルダーのコンテキストメニューを開き、［**フィルターの削除**］を選択します。

タスク実行ログのリストにすべてのタスク実行ログが表示されます。

# 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. ［**実行ログ**］を選択します。
3. 結果ペインで、次のいずれかの方法で［**ログ**］ウィンドウを開きます：
   - 表示するタスク実行ログをダブルクリックします。
   - 表示するタスク実行ログのコンテキストメニューを開き、［**ログを表示**］を選択します。
4. ウィンドウが開いて、次の詳細が表示されます：
   - ［**統計情報**］タブには、タスクの開始時間と完了時間、およびタスクの統計が表示されます。
   - ［**イベント**］タブには、タスクの実行中に記録されたイベントのリストが表示されます。
   - ［**オプション**］タブには、タスクの設定が表示されます。
5. 必要に応じて、［**フィルター**］をクリックしてタスク実行ログのイベントをフィルタリングします。
6. 必要に応じて、［**エクスポート**］をクリックして、タスク実行ログのデータを CSV 形式または TXT 形式のファイルでエクスポートします。
7. ［**閉じる**］をクリックします。

［**ログ**］ウィンドウが終了します。

## タスク実行ログからの情報のエクスポート

タスク実行ログから CSV 形式または TXT 形式のファイルにデータをエクスポートできます。

*タスク実行ログからデータ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. ［**実行ログ**］を選択します。
3. 結果ペインで、次のいずれかの方法で［**ログ**］ウィンドウを開きます：
   - 表示するタスク実行ログをダブルクリックします。
   - 表示するタスク実行ログのコンテキストメニューを開き、［**ログを表示**］を選択します。
4. ［**ログ**］ウィンドウ下部の［**エクスポート**］をクリックします。
   ［**名前を付けて保存**］ウィンドウが開きます。
5. タスク実行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、エンコーディングを指定します。
6. ［**保存**］をクリックします。

指定された設定が保存されます。

## タスク実行ログの削除

既定では、レコードはタスクの完了から 30 日間、タスク実行ログに保存されます。タスク実行ログのレコードの保存期間は変更できます。

既に完了したタスク実行ログを手動で削除できます。

現在実行中のタスクと他のユーザーが使用しているタスクのログのイベントは、削除されません。

*タスク実行ログを削除するには：*

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. ［**実行ログ**］を選択します。
3. 次のいずれかの処理を実行します：
   - 完了しているすべてのタスクのログを削除するには、［**実行ログ**］サブフォルダーのコンテキストメニューを開き、［**クリア**］を選択します。
   - 個々のタスクのログをクリアするには、結果ペインでクリアするタスク実行ログのコンテキストメニューを開き、［**削除**］を選択します。
   - 複数のタスク実行ログをクリアするには：
     a. 結果ペインで、**Ctrl** キーか **Shift** キーを使用して、クリアするタスク実行ログを選択します。
     b. 選択したタスク実行ログのコンテキストメニューを開き、［**削除**］を選択します。
4. 削除の確認ウィンドウで［**はい**］をクリックし、ログを削除することを確認します。

選択したタスク実行ログがクリアされます。タスク実行ログの削除は、システム監査ログに記録されます。

## セキュリティログ

Kaspersky Embedded Systems Security 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ログが保持されています。このログには次のイベントが記録されます：

- 脆弱性攻撃ブロックイベント
- 重要な Windows イベントログ監視イベント
- 試行されたセキュリティ侵害を示す重要なイベント（コンピューターのリアルタイム保護タスク、オンデマンドスキャンタスク、ファイル変更監視タスク、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用）

セキュリティログとシステム監査ログでは記録内容を削除できます。さらに Kaspersky Embedded Systems Security では、セキュリティログがクリアされた時にシステム監査イベントが記録されます。

# イベント ビューアーでの 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 ビューアー］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 ビューアー**］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、［**イベントビューアー**］フォルダーが表示されます。
6. ［**イベント ビューアー**］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。

# 管理プラグインでのログの設定

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*］の各イベントの発生のしきい値

- 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 ビューアー内の 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 Embedded Systems Security ログを設定するには、次の手順を実行します：*

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、［**プロパティ**］を選択します。
   ［**ログと通知の設定**］ウィンドウが開きます。
2. ［**ログと通知の設定**］ウィンドウで、要件に従ってログを設定します。それには、次の操作を実行します：
   - ［**全般**］タブで、必要に応じて、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 ビューアー内の Kaspersky Embedded Systems Security のイベントログを選択します。それには、次の操作を実行します：
     - ［**コンポーネント**］リストで、詳細レベルを設定する Kaspersky Embedded Systems Security のコンポーネントを選択します。

       ファイルのリアルタイム保護、オンデマンドスキャン、およびアップデートの各コンポーネントのイベントは、タスク実行ログとイベントログに記録されます。これらのコンポーネントの場合、イベントのテーブルには［**実行ログ**］と［**Windows イベントログ**］の列が含まれます。隔離とバックアップのイベントは、システム監査ログおよびイベントログに登録されます。これらのコンポーネントの場合、イベントのテーブルには［**監査**］と［**Windows イベントログ**］の列が含まれます。

     - ［**重要度**］リストで、選択したコンポーネントのタスク実行ログ、システム監査ログ、イベントログのイベントの詳細レベルを選択します。
       イベントのリストが含まれる次のテーブルでは、タスク実行ログ、システム監査ログ、イベントログと一緒に登録されるイベントの横のチェックボックスが、現在の詳細レベルに従ってオンになります。
     - 選択したコンポーネントの特定のイベントの登録を手動で有効にするには、次の操作を実行します：
       a. ［**重要度**］リストで［**カスタム**］を選択します。
       b. イベントのリストが含まれるテーブルで、タスク実行ログ、システム監査ログ、イベントログに登録するイベントの横のチェックボックスをオンにします。
   - ［**詳細設定**］タブで、デバイス保護ステータスに対するログの保管領域設定とイベント発生のしきい値を設定します：
     - ［**ログの保管領域**］セクション：
       - **ログフォルダー**
       - **実行ログの保管日数**
       - **システム監査ログ内のイベントの保管日数**
     - ［**イベント生成しきい値**］セクション：

- ［*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*］、［*簡易スキャンが長期間実行されていません*］の各イベントが発生するまでの日数を指定します。

- ［**SIEM 連携**］タブで、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を行います。

3. ［**OK**］をクリックして、変更内容を保存します。

# SIEM 統合について

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 統合を使用できます：

- 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。

## 信頼性設定

SIEM サーバーへのイベントの送信に失敗するリスクを軽減するために、ミラー syslog サーバーへの接続設定を指定できます。

ミラー syslog サーバーは追加の syslog サーバーで、メインの syslog サーバーに接続できないか、メインのサーバーが使用できない場合に、自動的に切り替えられます。

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。

# SIEM 統合設定

既定では、SIEM 統合は使用されません。SIEM 統合は、有効化や無効化、関連する設定ができます（次の表を参照）。

SIEM 統合設定

| 設定 | 既定値 | 説明 |
|---|---|---|
| **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** | オフ | それぞれ、チェックボックスをオンまたはオフにすることによって、SIEM 統合を有効または無効にできます。 |
| **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** | オフ | チェックボックスをオンまたはオフにすることによって SIEM サーバーに送信されたログのローカルコピーの保存設定を行うことができます。 |
| **イベント形式** | STRUCTURED-DATA | これらのイベントを syslog サーバーに送信して SIEM サーバーで良好に認識するために、イベントの変換形式には 2 つのいずれかを選択できます。 |
| **接続プロトコル** | TCP | ドロップダウンリストを使用して、メインおよびミラー syslog サーバーへの接続プロトコルに UDP または TCP を設定できます。 |
| **メイン syslog サーバー接続設定** | IP アドレス：127.0.0.1<br>ポート：514 | 適切なフィールドを使用して、メインの syslog サーバーへの接続に使用する IP アドレスおよびポートを設定できます。<br>IP アドレスは IPv4 形式でのみ指定できます。 |
| **メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する** | オフ | チェックボックスを使用してミラー syslog サーバーの使用を有効または無効にできます。 |
| **ミラー syslog サーバー接続設定** | IP アドレス：127.0.0.1<br>ポート：514 | 適切なフィールドを使用して、ミラー syslog サーバーへの接続に使用する IP アドレスおよびポートを設定できます。<br>IP アドレスは IPv4 形式でのみ指定できます。 |

*SIEM 統合設定を設定するには：*

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。
   ［**ログと通知の設定**］ウィンドウが開きます。
3. ［**SIEM 連携**］タブを選択します。
4. ［**連携の設定**］セクションで、［**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**］をオンにします。
5. 必要に応じて、［**連携の設定**］セクションの［**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**］をオンにします。

   ［**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**］の状態は、セキュリティログのイベントを保存する設定に影響を及ぼしません。セキュリティログイベントが自動的に削除されることはありません。

6. ［**イベント形式**］セクションで、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指定します。
   既定では、STRUCTURED-DATA 形式に変換されます。

7. ［**接続設定**］セクション：

   - SIEM 接続プロトコルを指定します。
   - メインの syslog サーバーに接続する設定を指定します。

     IP アドレスは IPv4 形式でのみ指定できます。
   - メインの syslog サーバーにイベントを送信できない場合にその他の接続設定を使用するようにするには、［**メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する**］をオンにします。

     ミラー syslog サーバーに接続する設定を指定します：［**アドレス**］および［**ポート**］。

     ［**メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する**］がオフの場合、ミラー syslog サーバーの［**アドレス**］および［**ポート**］は編集できません。

     IP アドレスは IPv4 形式でのみ指定できます。

8. ［**OK**］をクリックします。

   設定済みの SIEM 統合設定が適用されます。

## ログと通知の設定

Kaspersky Security Center の管理コンソールを使用して、Kaspersky Embedded Systems Security や、デバイスのアンチウイルスによる保護のステータスに関する次のイベントについて、管理者やユーザー向けの通知を設定できます：

- 管理者は、選択したイベント種別の情報を受信できます。
- 保護対象デバイスにアクセスする LAN ユーザーとターミナル保護対象デバイスのユーザーは、*オブジェクトが検知されました*イベントに関する情報を受信できます。

Kaspersky Embedded Systems Security イベントに関する通知は、選択した保護対象デバイスのプロパティウィンドウを使用して選択した個別の保護対象デバイスに対して設定するか、選択した管理グループのポリシーのプロパティウィンドウ内で保護対象デバイスのグループに対して設定することができます。

［**イベント通知**］セクション、または［**通知設定**］ウィンドウで、次の種類の通知を設定できます：

- 選択した種別のイベントに関する管理者通知は、［**イベント通知**］セクション（Kaspersky Security Center の標準タブ）を使用して設定できます。通知方法の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。
- 管理者通知とユーザー通知は、両方とも［**通知設定**］ウィンドウで設定できます。

一部の種別のイベントの通知は、［通知の設定］ウィンドウまたは［イベント通知］セクションでしか設定できません。その他の種別のイベントの通知は、［通知の設定］ウィンドウと［イベント通知］セクションの両方で設定できます。

同じ種別のイベントに関する通知を、同じモードで、［**イベント通知**］セクションと［**通知設定**］ウィンドウで設定すると、システム管理者はこれらのイベントの通知を同じモードで 2 回受信します。

## ログの設定

*Kaspersky Embedded Systems Security ログを設定するには、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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**ログと通知**］セクションで、［**実行ログ**］サブセクションの［**設定**］をクリックします。
5. ［**ログの設定**］ウィンドウで、要件に従って Kaspersky Embedded Systems Security の次の設定を定義します：
   - ログのイベント詳細レベルの設定を設定します。それには、次の操作を実行します：
     a. ［**コンポーネント**］リストで、詳細レベルを設定する Kaspersky Embedded Systems Security のコンポーネントを選択します。
     b. 選択したコンポーネントのタスク実行ログとシステム監査ログの詳細レベルを定義するには、［**重要度**］から必要なレベルを選択します。
   - ログの既定の場所を変更するには、フォルダーの完全パスを指定するか、［**参照**］をクリックして選択します。
   - タスク実行ログの保存日数を指定します。
   - ［**システム監査ログ**］フォルダーに表示される情報の保存日数を指定します。
6. ［OK］をクリックします。

ログの設定が保存されます。

## セキュリティログ

Kaspersky Embedded Systems Security 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ログが保持されています。このログには次のイベントが記録されます：

- 脆弱性攻撃ブロックイベント

- 重要な Windows イベントログ監視イベント
- 試行されたセキュリティ侵害を示す重要なイベント（コンピューターのリアルタイム保護タスク、オンデマンドスキャンタスク、ファイル変更監視タスク、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用）

セキュリティログとシステム監査ログでは記録内容を削除できます。さらに Kaspersky Embedded Systems Security では、セキュリティログがクリアされた時にシステム監査イベントが記録されます。

## SIEM 統合設定

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 統合を使用できます：

- 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。

SIEM サーバーへのイベントの送信に失敗するリスクを軽減するために、ミラー syslog サーバーへの接続設定を指定できます。

ミラー syslog サーバーは追加の syslog サーバーで、メインの syslog サーバーに接続できないか、メインのサーバーが使用できない場合に、自動的に切り替えられます。

既定では、SIEM 統合は使用されません。SIEM 統合は、有効化や無効化、関連する設定ができます（次の表を参照）。

SIEM 統合設定

| 設定 | 既定値 | 説明 |
| --- | --- | --- |
| **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** | オフ | それぞれ、チェックボックスをオンまたはオフにすることによって、SIEM 統合を有効または無効にできます。 |
| **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** | オフ | チェックボックスをオンまたはオフにすることによって SIEM サーバーに送信されたログのローカルコピーの保存設定を行うことができます。 |

| | | |
|---|---|---|
| イベント形式 | STRUCTURED-DATA | これらのイベントを syslog サーバーに送信して SIEM サーバーで良好に認識するために、イベントの変換形式には 2 つのいずれかを選択できます。 |
| 接続プロトコル | TCP | ドロップダウンリストを使用して、メイン syslog サーバーへの接続プロトコルに UDP または TCP を設定できます。ミラー syslog サーバーへの接続プロトコルには TCP を設定できます。 |
| メイン syslog サーバー接続設定 | IP アドレス：127.0.0.1<br>ポート：514 | 適切なフィールドを使用して、メインの syslog サーバーへの接続に使用する IP アドレスおよびポートを設定できます。<br>IP アドレスは IPv4 形式でのみ指定できます。 |
| **メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する** | オフ | チェックボックスを使用してミラー syslog サーバーの使用を有効または無効にできます。 |
| ミラー syslog サーバー接続設定 | IP アドレス：127.0.0.1<br>ポート：514 | 適切なフィールドを使用して、ミラー syslog サーバーへの接続に使用する IP アドレスおよびポートを設定できます。<br>IP アドレスは IPv4 形式でのみ指定できます。 |

*SIEM 統合設定を設定するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**ログと通知**］セクションで、［**実行ログ**］サブセクションの［**設定**］をクリックします。
   ［**ログと通知の設定**］ウィンドウが開きます。
5. ［**SIEM 連携**］タブを選択します。
6. ［**連携の設定**］セクションで、［**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**］をオンにします。
7. 必要に応じて、［**連携の設定**］セクションの［**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**］をオンにします。

   ［**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**］の状態は、セキュリティログのイベントを保存する設定に影響を及ぼしません。セキュリティログイベントが自動的に削除されることはありません。

8. ［**イベント形式**］セクションで、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指定します。

   既定では、STRUCTURED-DATA 形式に変換されます。

9. ［**接続設定**］セクション：

   - SIEM 接続プロトコルを指定します。
   - メインの syslog サーバーに接続する設定を指定します。

     IP アドレスは IPv4 形式でのみ指定できます。
   - メインの syslog サーバーにイベントを送信できない場合にその他の接続設定を使用するようにするには、［**メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する**］をオンにします。

     ミラー syslog サーバーに接続する設定を指定します：［**アドレス**］および［**ポート**］。

     ［**メインのサーバーにアクセスできない場合、ミラー syslog サーバーを使用する**］がオフの場合、ミラー syslog サーバーの［**アドレス**］および［**ポート**］は編集できません。

     IP アドレスは IPv4 形式でのみ指定できます。

10. ［**OK**］をクリックします。

設定済みの SIEM 統合設定が適用されます。

## 通知の設定

*Kaspersky Embedded Systems Security 通知を設定するには、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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     > Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**ログと通知**］セクションで、［**イベント通知**］サブセクションの［**設定**］をクリックします。
5. ［**通知設定**］ウィンドウで、要件に従って Kaspersky Embedded Systems Security の次の設定を定義します：

   - ［**通知設定**］リストより、設定を編集する通知の種別を選択します。

- ［**ユーザーへの通知**］セクションで、ユーザーへの通知方法を設定します。必要に応じて、通知メッセージのテキストを入力します。
- ［**管理者への通知**］セクションで、管理者への通知方法を設定します。必要に応じて、通知メッセージのテキストを入力します。必要に応じて［**設定**］をクリックし、通知の詳細設定を行います。
- ［**イベント生成しきい値**］セクションでは、Kaspersky Embedded Systems Security が［*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*］の各イベントを記録する時間間隔を指定できます。
  - **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**
  - **簡易スキャンが長期間実行されていない日数**

6. ［**OK**］をクリックします。

通知の設定内容が保存されます。

## 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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**ログと通知**］セクションで、［**管理サーバーとのインタラクション**］サブセクションの［**設定**］をクリックします。
   ［**管理サーバーのネットワークリスト**］ウィンドウが開きます。
5. ［**管理サーバーのネットワークリスト**］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：
   - 隔離されたオブジェクト
   - バックアップされたオブジェクト
6. ［**OK**］をクリックします。

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。

# 通知の設定

このセクションでは、Kaspersky Embedded Systems Security のユーザーと管理者に対して本製品のイベントとデバイスの保護ステータスを通知する方法、および通知を設定する方法について説明します。

# 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 の操作、およびデバイスのアンチウイルスによる保護のステータスに関するイベントについて通知するよう設定できます。

次のタスクが実行されます：

- 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。

アプリケーションコンソールで、次のさまざま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：

- ユーザーのへ通知方法：
  a. 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。
  b. メッセージサービスツール
     Microsoft Windows メッセージサービスを使用した通知にこの方法を適用できます。
- 管理者への通知方法：
  a. メッセージサービスツール
     Microsoft Windows メッセージサービスを使用した通知にこの方法を適用できます。
  b. 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。
  c. 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。

*イベント通知を設定するには：*

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。

   ［**ログと通知の設定**］ウィンドウが開きます。

2. ［**通知**］タブで、通知モードを選択します：

   a. ［**イベント種別**］リストから、通知方法を選択するイベントを選択します。

   b. ［**管理者への通知**］または［**ユーザーへの通知**］グループ設定で、設定する通知方法の横にあるチェックボックスをオンにします。

   次のイベントのユーザーへの通知のみを設定できます：［**オブジェクトが検知されました**］イベント、［**信頼しない外部デバイスが検出および制限されました**］イベント、［**コンピューターが信頼しないリストに追加されました**］。

3. メッセージのテキストを追加するには：

   a. ［**メッセージのテキスト**］をクリックします。

   b. 表示されたウィンドウに、対応するイベントメッセージに表示するテキストを入力します。

   複数のイベントの種別に同じメッセージを作成できます。1つのイベント種別の通知方法を選択してから、**Ctrl** キーまたは **Shift** キーを使用して、同じメッセージを使用する他のイベント種別を選択し、［**メッセージのテキスト**］をクリックします。

   a. イベントの情報が含まれるフィールドを追加するには、［**マクロ**］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。

   b. イベントメッセージの既定のテキストを復元するには、［**既定値**］をクリックします。

4. 選択したイベントの管理者通知方法を設定するには、［**通知**］タブを選択して［**管理者への通知**］セクションの［**設定**］をクリックし、［**詳細設定**］ウィンドウで通知方法を設定します。それには、次の操作を実行します：

   a. メール通知の場合、［**メール**］タブを開いて、該当するフィールドに受信者のメールアドレス（アドレスをセミコロンで区切ります）、SMTP サーバーの名前またはネットワークアドレス、およびポート番号を指定します。必要に応じて、［**発行先**］と［**送信者**］に表示するテキストを指定します。［**発行先**］のテキストに、イベントの情報が含まれる変数を含めることもできます（以下の表を参照）。

   SMTP サーバーへの接続時にユーザーアカウント認証を適用するには、［**認証設定**］グループの［**SMTP 認証を使用する**］を選択し、認証対象のユーザーアカウントのユーザー名とパスワードを指定します。

   b. Windows Messenger サービスを使用して通知するには、［**Windows Messenger サービス**］タブで通知を受信する保護対象デバイスのリストを作成します。追加する保護対象デバイスごとに、［**追加**］をクリックして入力フィールドにネットワークの名前を入力します。

   c. 実行ファイルを実行するには、イベントが発生した時に保護対象デバイスで実行される保護対象デバイスのローカルドライブのファイルを選択するか、［**実行ファイル**］タブのフルパスを入力します。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。

一定の期間に1つのイベント種別のメッセージ数を制限するには、［**詳細設定**］タブで［**同じ通知の最大送信回数**］を選択し、回数と時間の間隔を指定します。

5. ［**OK**］をクリックします。

通知の設定内容が保存されます。

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。 |
| %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）。 |

# Kaspersky Embedded Systems Security の開始と停止

このセクションでは、アプリケーションコンソールの起動に関する情報および Kaspersky Security サービスの開始と停止に関する情報について説明します。

# Kaspersky Embedded Systems Security 管理プラグインの起動

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プラグインは Kaspersky Security Center と同時に開始されます。Kaspersky Security Center の開始についての詳細情報は、*Kaspersky Security Center のヘルプ*を参照してください。

# スタートメニューからの Kaspersky Embedded Systems Security コンソールの起動

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。

*［**スタート**］メニューからアプリケーションコンソールを起動するには：*

1. ［**スタート**］メニューから、［**すべてのプログラム**］ - ［**Kaspersky Embedded Systems Security**］ - ［**管理ツール**］ - ［**Kaspersky Embedded Systems Security コンソール**］の順に選択します。

アプリケーションコンソールに他のスナップインを追加するには、作成者モードでアプリケーションコンソールを起動します。

*作成者モードでアプリケーションコンソールを起動するには：*

1. ［**スタート**］メニューから、［**すべてのプログラム**］ - ［**Kaspersky Embedded Systems Security**］ - ［**管理ツール**］の順に選択します。
2. アプリケーションコンソールのコンテキストメニューで、［**作成者**］を選択します。

   アプリケーションコンソールが作成者モードで起動します。

保護対象デバイスでアプリケーションコンソールを起動した場合、アプリケーションコンソールウィンドウが開きます。

保護対象デバイス以外でアプリケーションコンソールを起動した場合は、保護対象デバイスに接続します。

*保護対象デバイスに接続するには：*

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. ［**別のコンピューターに接続**］コマンドを選択します。
   ［**保護対象デバイスの選択**］ウィンドウが開きます。
3. 表示されたウィンドウで、［**別のデバイス**］を選択します。

4. 右側にある入力フィールドで保護対象デバイスのネットワーク名を指定します。

5. ［OK］をクリックします。

アプリケーションコンソールが、保護対象デバイスに接続されます。

Microsoft Windows のログイン用のユーザーアカウントの権限では保護対象デバイス上の Kaspersky Security 管理サービスにアクセスできない場合は、［**次のユーザーとして接続する**］をオンにして、必要な権限を持つ別のユーザーアカウントを指定します。

## Kaspersky Security サービスの開始と停止

既定では、Kaspersky Security サービスはオペレーティングシステムの起動直後に自動で開始します。Kaspersky Security サービスは、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、オンデマンドスキャン、およびアップデートタスクを実行する処理対象プロセスを管理します。

既定では、Kaspersky Embedded Systems Security の開始時に、ファイルのリアルタイム保護タスク、およびオペレーティングシステムの起動時のスキャンタスクが開始されます。さらに、**アプリケーションの起動時**に開始するようにスケジュールされたその他のタスクも開始されます。

Kaspersky Security サービスが停止されると、実行中のすべてのタスクが停止されます。Kaspersky Security サービスの再起動後には、［**アプリケーションの起動時**］に実行するようスケジュールが設定されたタスクのみが自動的に開始されます。それ以外のタスクは手動で開始する必要があります。

Kaspersky Security サービスは、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューまたは Microsoft Windows の［サービス］スナップインを使用して開始および停止することもできます。

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。

*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停止または開始するには：*

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. 次のいずれかの項目を選択します：

   - **サービスの停止**
   - **サービスの起動**

Kaspersky Security サービスが開始または停止します。

## オペレーティングシステムのセーフモードでの Kaspersky Embedded Systems Security コンポーネントの起動

このセクションでは、オペレーティングシステムのセーフモードで Kaspersky Embedded Systems Security を動作させる方法について説明しています。

# オペレーティングシステムのセーフモードでの Kaspersky Embedded Systems Security の動作について

オペレーティングシステムをセーフモードで読み込んだ時に、Kaspersky Embedded Systems Security のコンポーネントを起動できます。Kaspersky Security サービス（kavfs.exe）に加えて、klam.sys ドライバーも読み込まれます。オペレーティングシステムの起動中に Kaspersky Security サービスを保護対象サービスとして登録するために使用されます。詳しくは、「Kaspersky Security サービスを保護対象サービスとして登録する」セクションを参照してください。

Kaspersky Embedded Systems Security は、オペレーティングシステムの次の種別のセーフモードで起動できます：

- セーフモード（最小限）：オペレーティングシステムのセーフモードの標準のオプションを選択すると起動されます。この場合、Kaspersky Embedded Systems Security は次のコンポーネントを起動できます：
  - ファイルのリアルタイム保護
  - オンデマンドスキャン
  - アプリケーション起動コントロールとアプリケーション起動コントロールルールの自動作成
  - Windows イベントログ監視
  - ファイル変更監視
  - ベースラインに基づくファイル変更監視
  - アプリケーションの整合性チェック

セーフモードとネットワーク：このモードでは、オペレーティングシステムがネットワークドライバーとともにセーフモードで読み込まれます。セーフモード（最小限）で起動されるコンポーネントに加えて、Kaspersky Embedded Systems Security はこのモードで次のコンポーネントを起動できます：

- 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

# セーフモードでの Kaspersky Embedded Systems Security の起動

既定では、オペレーティングシステムをセーフモードで読み込んだ時、Kaspersky Embedded Systems Security は起動されません。

*オペレーティングシステムのセーフモードで Kaspersky Embedded Systems Security を起動するには：*

1. Windows のレジストリエディター（C:\Windows\regedit.exe）を起動します。
2. システムレジストリの [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] キーを開きます。
3. 「LoadInSafeMode」パラメータを開きます。

4. 値を「1」に設定します。

5. ［OK］をクリックします。

*オペレーティングシステムのセーフモードでの Kaspersky Embedded Systems Security の起動を取り消すには：*

1. Windows のレジストリエディター（C:\Windows\regedit.exe）を起動します。

2. システムレジストリの [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam\Parameters] キーを開きます。

3. 「LoadInSafeMode」パラメータを開きます。

4. 値を「0」に設定します。

5. ［OK］をクリックします。

# Kaspersky Embedded Systems Security のセルフディフェンス機構

このセクションでは、Kaspersky Embedded Systems Security のセルフディフェンス機構について説明します。

## Kaspersky Embedded Systems Security のセルフディフェンス機構について

Kaspersky Embedded Systems Security 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 のコンポーネントがインストールされているフォルダーの改変防止

Kaspersky Embedded Systems Security では、コンポーネントがインストールされているフォルダーの名前変更と削除は、いかなるユーザーアカウントによるものであってもブロックされます。既定のインストールフォルダーはそれぞれ次のようになります：

- 32 ビット版の Microsoft Windows：%ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\
- 64 ビット版の Microsoft Windows：%ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security\

## Kaspersky Embedded Systems Security のレジストリキーの改変防止

Kaspersky Embedded Systems Security では、本製品のドライバーとサービスの読み込みを容易にする、次のレジストリブランチとレジストリキーへのアクセス権が制限されます：

- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfs]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsgt]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kavfsslp]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klam]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klelaml]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klfltdev]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\klramdisk]
- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\CrashDump]
- [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\3.1]（64 ビット版の Microsoft Windows 製品の場合）

- [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\3.1\Trace]

これらのレジストリブランチとレジストリキーの変更権限は、ローカルシステム（SYSTEM）アカウントにのみ付与されます。ユーザーアカウントと管理者アカウントには読み取り権限が付与されます。

### プログラムサービス部分へのメモリの変更からの保護

サードパーティプロセスからプログラムサービス部分を保護するために、Kaspersky Embedded Systems Security のドライバーにより、次の実行ファイルへのアクセスが制限されます：

- kavfs.exe
- kavfswp.exe
- kavfswh.exe
- kavfsgt.exe

既定では、Kaspersky Embedded Systems Security サービス部分のメモリへのアクセスは、サードパーティプロセスに対して制限されています。

Kaspersky Embedded Systems Security コンソールおよび Kaspersky Embedded Systems Security 管理用プラグインの、ポリシーのプロパティでセルフディフェンス機能を有効にできます。

## Kaspersky Security サービスを保護対象サービスとして登録する

*Protected Process Light*（または「PPL」とも表記）技術により、オペレーティングシステムが信頼するサービスとプロセスのみを読み込みます。サービスを保護対象サービスとして実行するには、*起動時マルウェア対策*ドライバーを保護対象デバイスにインストールする必要があります。

*起動時マルウェア対策*（または「ELAM」とも表記）ドライバーは、ネットワーク上のデバイスが起動すると保護を開始し、他のサードパーティ製ドライバーが起動する前の保護を提供します。

Kaspersky Embedded Systems Security のインストール中に ELAM ドライバーが自動的にインストールされ、オペレーティングシステムの起動時に Kaspersky Security サービスを PPL として登録するために使用されます。Kaspersky Security Service（KAVFS）がシステムの保護対象プロセスとして起動される場合、システム上のその他の保護されていないプロセスはスレッドの注入、保護対象プロセスの仮想メモリへの書き込み、またはサービスの停止を行うことはできません。

PPL として開始されたプロセスは、ユーザーの持つ権限に関係なく、ユーザーが管理することはできません。ELAM ドライバーを使用した Kaspersky Security Service の PPL としての登録は、Microsoft Windows 10 以降のオペレーティングシステムでサポートされます。Kaspersky Embedded Systems Security を、PPL をサポートするオペレーティングシステムのサーバーにインストールする場合、Kaspersky Security サービス（KAVFS）の権限の管理は使用できません。

*Kaspersky Embedded Systems Security を PPL として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_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

# Kaspersky Embedded Systems Security の各種機能に対するアクセス権限の管理

このセクションでは、Kaspersky Embedded Systems Security を管理するための権限およびアプリケーションによって登録されるオペレーティングシステムのサービスを管理するための権限に関する情報と、それらの権限の設定方法について説明します。

## Kaspersky Embedded Systems Security を管理するための権限について

既定では、保護対象デバイスの管理者グループのユーザー、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 グループのユーザー、および SYSTEM グループに、Kaspersky Embedded Systems Security の全機能に対するアクセス権が付与されます。

Kaspersky Embedded Systems Security の［編集］権限のアクセスレベルを持つユーザーは、保護対象デバイスに登録された他のユーザー、またはドメイン内の他のユーザーに対し、Kaspersky Embedded Systems Security の各種機能へのアクセス権を付与することができます。

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。

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アクセス権限レベルを選択できます：

- **フルコントロール** - 製品のすべての機能に対するアクセス。Kaspersky Embedded Systems Security の全般的な設定、コンポーネントの設定、および Kaspersky Embedded Systems Security ユーザーの権限を表示および編集でき、さらに Kaspersky Embedded Systems Security の統計情報を表示できます。

- **変更** - ユーザー権限の編集以外のすべての製品の機能へのアクセス。Kaspersky Embedded Systems Security の全般的な設定と、Kaspersky Embedded Systems Security コンポーネントの設定を表示および編集できます。

- **読み取り** - Kaspersky Embedded Systems Security の全般的な設定、Kaspersky Embedded Systems Security コンポーネントの設定、Kaspersky Embedded Systems Security の統計情報、Kaspersky Embedded Systems Security ユーザーの権限を表示できます。

また、詳細なアクセス権限を設定して、Kaspersky Embedded Systems Security の特定の機能へのアクセスを許可したりブロックしたりすることもできます。

ユーザーまたはグループのアクセス権限を手動で設定した場合、該当のユーザーまたはグループには［**特殊なアクセス許可**］のアクセスレベルが設定されます。

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。 |
| オンデマンドスキャン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>• 設定ファイルからの Kaspersky Embedded Systems Security の設定のインポート。 |

| | |
|---|---|
| | • 製品設定の編集。 |
| 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。 |
| リポジトリの管理 | 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。 |
| 統計情報の読み取り | 各 Kaspersky Embedded Systems Security タスクの統計情報を表示できます。 |
| ライセンス | Kaspersky Embedded Systems Security のアクティベーションを実行できます。 |
| アプリケーション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。 |
| 権限の読み取り | 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。 |
| 権限の編集 | 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。 |

## 登録されたサービスを管理するための権限について

Kaspersky Embedded Systems Security では、インストール時に Kaspersky Security サービス（KAVFS）、Kaspersky Security 管理サービス（KAVFSGT）、および Kaspersky Security 脆弱性攻撃ブロック（KAVFSSLP）が Windows に登録されます。

Microsoft Windows 10 以降のオペレーティングシステムで ELAM ドライバーを使用して、Kaspersky Security サービスを Protected Process Light として登録できます。PPL として開始されたプロセスは、ユーザーの持つ権限に関係なく、ユーザーが管理することはできません。PPL をサポートするオペレーティングシステムが稼働する保護対象デバイスに Kaspersky Embedded Systems Security をインストールする場合、Kaspersky Security サービス（KAVFS）の権限の管理は使用できません。

### Kaspersky Security サービス

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、保護対象デバイスで管理者グループに登録されているユーザー、読み取り権限を持つ SERVICE および INTERACTIVE のグループ、および読み取りと実行権限を持つ SYSTEM のグループに付与されます。

［編集権限］レベルのアクセス権限を持つユーザーは、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 管理サービス

別の保護対象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から本製品を管理するには、Kaspersky Embedded Systems Security への接続に使用される権限を持つアカウントが、保護対象デバイスの Kaspersky Security 管理サービスへのフルアクセス権を持っている必要があります。

既定では、保護対象デバイスの管理者グループのユーザーと、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］グループのユーザーに、すべての Kaspersky Security 管理サービスへのアクセス権が付与されます。

Kaspersky Security 管理サービスは、Microsoft Windows の［サービス］スナップインでのみ管理できます。

### Kaspersky Security 脆弱性攻撃ブロック

既定では、Kaspersky Security 脆弱性攻撃ブロックサービスを管理するためのアクセス権限は、保護対象デバイスで管理者グループに登録されているユーザー、および読み取りと実行権限を持つ SYSTEM のグループに付与されます。

## Kaspersky Security 管理サービスのアクセス権限について

Kaspersky Embedded Systems Security サービスのリストを確認できます。

Kaspersky Embedded Systems Security はインストール時に Kaspersky Security 管理サービス（KAVFSGT）を登録します。別の保護対象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から本製品を管理するには、Kaspersky Embedded Systems Security への接続に使用されるアカウントが、保護対象デバイスの Kaspersky Security 管理サービスへのフルアクセス権を持っている必要があります。

既定では、保護対象デバイスの管理者グループのユーザーと、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］グループのユーザーに、すべての Kaspersky Security 管理サービスへのアクセス権が付与されます。

Kaspersky Security 管理サービスは、Microsoft Windows の［サービス］スナップインでのみ管理できます。

Kaspersky Embedded Systems Security の設定では、Kaspersky Security 管理サービスへのユーザーアクセスを許可またはブロックできません。

ユーザー名とパスワードがローカルアカウントと同じアカウントが保護対象デバイスに登録されている場合、ローカルアカウントから Kaspersky Embedded Systems Security に接続できます。

# Kaspersky Security サービスを管理するための権限について

Kaspersky Embedded Systems Security はインストール中に Kaspersky Security サービス（KAVFS）を Windows に登録し、オペレーティングシステムの起動時に機能コンポーネントを内部で起動できるようにします。Kaspersky Security サービスの管理を介して第三者によって保護対象デバイスのアプリケーション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、ローカルのアプリケーションコンソールや管理プラグインから 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 のユーザーやユーザーグループに対し、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。
- **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。
- **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）。

ユーザーまたはグループのアクセス権限を手動で設定した場合、該当のユーザーまたはグループには［**特殊なアクセス許可**］のアクセスレベルが設定されます。

Kaspersky Security サービスの各機能に対するアクセス権限

| 機能 | 説明 |
| --- | --- |
| サービスの設定の表示 | 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。 |
| サービスからのステータスの要求 | 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。 |
| サービスの設定の編集 | 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。 |

| | |
|---|---|
| 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。 |
| 権限の読み取り | 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。 |
| 権限の編集 | 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。 |

## 管理プラグインからアクセス権限を管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの1つまたはすべての保護対象デバイスのアクセス権を設定する方法について説明します。

## Kaspersky Embedded Systems Security と Kaspersky Security サービスのアクセス権限の設定

Kaspersky Embedded Systems Security の機能にアクセスして Kaspersky Security サービスを管理することが許可されているユーザーとユーザーグループのリストを編集できます。さらに、こ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することもできます。

*リストでユーザーまたはグループを追加または削除するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**詳細設定**］セクションで、次のいずれかの手順を実行します：

   - Kaspersky Embedded Systems Security の機能を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**アプリケーション管理用のユーザーアクセス権限**］サブセクションにある［**設定**］をクリックします。

   - Kaspersky Security サービスを管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**Kaspersky Security サービス管理用のユーザーアクセス権限**］の［**設定**］をクリックします。

     ［**Kaspersky Embedded Systems Security 3.1 のアクセス許可**］ウィンドウが開きます。

5. 表示されたウィンドウで、次の操作を行います：

   - ユーザーまたはグループをリストに追加するには、［**追加**］をクリックして権限を付与するユーザーまたはグループを選択します。

   - ユーザーまたはグループをリストから削除するには、アクセスを制限するユーザーまたはグループを選択して、［**削除**］をクリックします。

6. ［**OK**］をクリックします。

選択されたユーザー（グループ）が追加または削除されます。

*Kaspersky Embedded Systems Security または Kaspersky Security サービスを管理するユーザーまたはグループの権限を編集するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。

   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**詳細設定**］セクションで、次のいずれかの手順を実行します：

   - Kaspersky Embedded Systems Security の機能を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**アプリケーション管理用のユーザーアクセス権限**］サブセクションにある［**設定**］をクリックします。

   - Kaspersky Security サービスから本製品を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**Kaspersky Security サービス管理用のユーザーアクセス権限**］の［**設定**］をクリックし

ます。

［**Kaspersky Embedded Systems Security のアクセス許可**］ウィンドウが開きます。

5. 表示されたウィンドウにある［**グループ名またはユーザー名**］リストで、権限を変更するユーザーまたはユーザーのグループを選択します。

6. 次のアクセスレベルに対して、［**アクセス許可**］セクションにある［**許可**］または［**拒否**］を選択します：

   - **フルコントロール**：Kaspersky Embedded Systems Security または Kaspersky Security サービスを管理する権限のフルセット。
   - **読み取り**：
     - 次の権限で Kaspersky Embedded Systems Security を管理します：［**統計情報の取得**］、［**設定の読み取り**］、［**ログの読み取り**］、［**読み取り権限**］。
     - 次の権限で Kaspersky Security サービスを管理します：［**サービスの設定の読み込み**］、［**Service Control Manager からのステータスの要求**］、［**サービスからのステータスの要求**］、［**依存するサービスのリストの読み込み**］、［**読み取り権限**］。
   - **変更**：
     - ［**編集権限**］を除く、Kaspersky Embedded Systems Security を管理するための権限すべて。
     - 次の権限で Kaspersky Security サービスを管理します：［**サービス設定の変更**］、［**読み取り権限**］。
   - **特殊なアクセス許可**：次の権限で Kaspersky Security サービスを管理します：［**サービスを開始中**］、［**サービスの停止**］、［**サービスの一時停止/再開**］、［**読み取り権限**］、［**サービスへのユーザー定義要求**］。

7. ユーザーまたはグループの権限の詳細を設定するには（**特殊なアクセス許可**）、［**詳細設定**］をクリックします。

   a. 表示された［**Kaspersky Embedded Systems Security のセキュリティの詳細設定**］ウィンドウで、目的のユーザーまたはグループを選択します。

   b. ［**編集**］をクリックします。

   c. ウィンドウの上部にあるドロップダウンリストで、アクセスコントロールの種別を選択します（［**許可**］または［**拒否**］）。

   d. 選択したユーザーまたはグループに対して許可または拒否する機能の横にあるチェックボックスをオンにします。

   e. ［**OK**］をクリックします。

   f. ［**Kaspersky Embedded Systems Security のセキュリティ詳細設定**］ウィンドウで、［**OK**］をクリックします。

8. ［**Kaspersky Embedded Systems Security のアクセス許可**］ウィンドウで、［**適用**］をクリックします。

Kaspersky Embedded Systems Security または Kaspersky Security サービスを管理するために設定された権限が保存されます。

# Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス

ユーザー権限の設定によって、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。

次のアプリケーション機能にアクセスしようとすると、Kaspersky Embedded Systems Security はパスワードを要求します：

- アプリケーションコンソールへの接続
- Kaspersky Embedded Systems Security のアンインストール
- Kaspersky Embedded Systems Security コンポーネントの変更
- コマンドラインによるコマンドの実行

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）
  - 記号：感嘆符（!）、ドル（$）、ハッシュ（#）、パーセント（%）

パスワードで保護するアプリケーションの設定をエクスポートおよびインポートできます。保護対象アプリケーション設定をエクスポートすると作成される設定ファイルには、パスワードチェックサムおよびパスワード文字列の空白を埋めるために使用される修飾子の値が含まれています。

設定ファイルのチェックサムや修飾子は変更しないでください。手動で変更されたパスワードによる保護の設定をインポートすると、アプリケーションへのアクセスが完全にブロックされる場合があります。

*Kaspersky Embedded Systems Security 機能へのアクセスを保護するには：*

1. Kaspersky Security Center 管理コンソールのツリーで、［**管理対象デバイス**］フォルダーを展開します。アプリケーションの設定を行う保護対象デバイスがあ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、次のいずれかを実行します：

   - 保護対象デバイスのグループのポリシーの設定を行うには、［**ポリシー**］タブを選択し、コンテキストメニューを使用して **<ポリシー名>** のプロパティを開きます。

   - 1 台の保護対象デバイスのアプリケーションの設定を行う場合、Kaspersky Security Center の［**アプリケーションの設定**］ウィンドウで必要な設定を開きます。

3. ［**アプリケーションの設定**］タブの［**セキュリティと信頼性**］セクションで、［**設定**］ボタンをクリックします。

   ［**セキュリティ設定**］ウィンドウが表示されます。

4. ［**パスワードによる保護の設定**］セクションで、［**パスワードによる保護を適用する**］をオンにします。

   ［**パスワード**］および［**パスワードの確認**］がアクティブになります。

5. ［**パスワード**］で、Kaspersky Embedded Systems Security 機能へのアクセスを保護するために使用するパスワードを入力します。

6. ［**パスワードの確認**］にもう一度パスワードを入力します。

7. ［**OK**］をクリックします。

指定された設定が保存されます。保護対象機能へのアクセスに、指定したパスワードが要求されるようになります。

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アプリケーションをアンインストールできなくなります。

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［**パスワードによる保護を適用する**］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。

## アプリケーションコンソールからアクセス権限を管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、保護対象デバイスのアクセス権の設定を行う方法について説明します。

## Kaspersky Embedded Systems Security と Kaspersky Security サービスを管理するためのアクセス権限の設定

Kaspersky Embedded Systems Security の機能にアクセスして Kaspersky Security サービスを管理することが許可されているユーザーとユーザーグループのリストを編集できます。さらに、こ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することもできます。

*リストでユーザーまたはグループを追加または削除するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**詳細設定**］セクションで、次のいずれかの手順を実行します：
   - Kaspersky Embedded Systems Security の機能を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**アプリケーション管理用のユーザーアクセス権限**］サブセクションにある［**設定**］をクリックします。
   - Kaspersky Security サービスを管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**Kaspersky Security サービス管理用のユーザーアクセス権限**］の［**設定**］をクリックします。

     ［**Kaspersky Embedded Systems Security 3.1 のアクセス許可**］ウィンドウが開きます。
5. 表示されたウィンドウで、次の操作を行います：
   - ユーザーまたはグループをリストに追加するには、［**追加**］をクリックして権限を付与するユーザーまたはグループを選択します。
   - ユーザーまたはグループをリストから削除するには、アクセスを制限するユーザーまたはグループを選択して、［**削除**］をクリックします。
6. ［**OK**］をクリックします。

選択されたユーザー（グループ）が追加または削除されます。

*Kaspersky Embedded Systems Security または Kaspersky Security サービスを管理するユーザーまたはグループの権限を編集するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**詳細設定**］セクションで、次のいずれかの手順を実行します：

   - Kaspersky Embedded Systems Security の機能を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**アプリケーション管理用のユーザーアクセス権限**］サブセクションにある［**設定**］をクリックします。

   - Kaspersky Security サービスから本製品を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**Kaspersky Security サービス管理用のユーザーアクセス権限**］の［**設定**］をクリックします。

     ［**Kaspersky Embedded Systems Security のアクセス許可**］ウィンドウが開きます。

5. 表示されたウィンドウにある［**グループ名またはユーザー名**］リストで、権限を変更するユーザーまたはユーザーのグループを選択します。

6. 次のアクセスレベルに対して、［**アクセス許可**］セクションにある［**許可**］または［**拒否**］を選択します：

   - **フルコントロール**：Kaspersky Embedded Systems Security または Kaspersky Security サービスを管理する権限のフルセット。

   - **読み取り**：

     - 次の権限で Kaspersky Embedded Systems Security を管理します：［**統計情報の取得**］、［**設定の読み取り**］、［**ログの読み取り**］、［**読み取り権限**］。

     - 次の権限で Kaspersky Security サービスを管理します：［**サービスの設定の読み込み**］、［**Service Control Manager からのステータスの要求**］、［**サービスからのステータスの要求**］、［**依存するサービスのリストの読み込み**］、［**読み取り権限**］。

   - **変更**：

     - ［**編集権限**］を除く、Kaspersky Embedded Systems Security を管理するための権限すべて。

     - 次の権限で Kaspersky Security サービスを管理します：［**サービス設定の変更**］、［**読み取り権限**］。

   - **特殊なアクセス許可**：次の権限で Kaspersky Security サービスを管理します：［**サービスを開始中**］、［**サービスの停止**］、［**サービスの一時停止/再開**］、［**読み取り権限**］、［**サービスへのユーザー定義要求**］。

7. ユーザーまたはグループの権限の詳細を設定するには（**特殊なアクセス許可**）、［**詳細設定**］をクリックします。

   a. 表示された［**Kaspersky Embedded Systems Security のセキュリティの詳細設定**］ウィンドウで、目的のユーザーまたはグループを選択します。

   b. ［**編集**］をクリックします。

   c. ウィンドウの上部にあるドロップダウンリストで、アクセスコントロールの種別を選択します（［**許可**］または［**拒否**］）。

d. 選択したユーザーまたはグループに対して許可または拒否する機能の横にあるチェックボックスをオンにします。

e. ［**OK**］をクリックします。

f. ［**Kaspersky Embedded Systems Security のセキュリティ詳細設定**］ウィンドウで、［**OK**］をクリックします。

8. ［**Kaspersky Embedded Systems Security のアクセス許可**］ウィンドウで、［**適用**］をクリックします。

9. Kaspersky Embedded Systems Security または Kaspersky Security サービスを管理するために設定された権限が保存されます。

## Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス

ユーザー権限の設定によって、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。

次のアプリケーション機能にアクセスしようとすると、Kaspersky Embedded Systems Security はパスワードを要求します：

- アプリケーションコンソールへの接続
- Kaspersky Embedded Systems Security のアンインストール
- Kaspersky Embedded Systems Security コンポーネントの変更
- コマンドラインによるコマンドの実行

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。

パスワードで保護するアプリケーションの設定をエクスポートおよびインポートできます。保護対象アプリケーション設定をエクスポートすると作成される設定ファイルには、パスワードチェックサムおよびパスワード文字列の空白を埋めるために使用される修飾子の値が含まれています。

設定ファイルのチェックサムや修飾子は変更しないでください。手動で変更されたパスワードによる保護の設定をインポートすると、アプリケーションへのアクセスが完全にブロックされる場合があります。

*Kaspersky Embedded Systems Security 機能へのアクセスを保護するには：*

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にある［**アプリケーションのプロパティ**］をクリックする。
   - フォルダーのコンテキストメニューで［**プロパティ**］を選択する。

   ［**アプリケーションの設定**］ウィンドウが表示されます。

2. ［**セキュリティと信頼性**］タブの［**パスワードによる保護の設定**］セクションで、［**パスワードによる保護を適用する**］をオンにします。

   ［**パスワード**］および［**パスワードの確認**］がアクティブになります。

3. ［**パスワード**］で、Kaspersky Embedded Systems Security 機能へのアクセスを保護するために使用するパスワードを入力します。

4. ［**パスワードの確認**］にもう一度パスワードを入力します。

5. ［OK］をクリックします。

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アプリケーションをアンインストールできなくなります。

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［**パスワードによる保護を適用する**］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。

## Web プラグインからアクセス権限を管理する

このセクションでは、Web プラグインインターフェイスを操作して、ネットワークの 1 つまたはすべての保護対象デバイスのアクセス権を設定する方法について説明します。

## Kaspersky Embedded Systems Security と Kaspersky Security サービスのアクセス権限の設定

ユーザーまたはグループのアクセス権限を設定するには、セキュリティ記述子定義言語（SDDL）を使用して SDDL 文字列を指定する必要があります。SDDL 文字列について詳しくは、Microsoft の Web サイトを参照してください。

*ユーザーまたはグループのアクセス権限を設定するには：*

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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. 次のいずれかの処理を実行します：

   - Kaspersky Embedded Systems Security の機能を管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**アプリケーション管理用のユーザーアクセス権限**］サブセクションにある［**設定**］をクリックします。

   - Kaspersky Security サービスを管理するためのアクセス権限を持つユーザーのリストを編集する場合は、［**Kaspersky Security サービス管理用のユーザーアクセス権限**］の［**設定**］をクリックします。

6. ［**アプリケーション管理用のユーザーアクセス権限**］ウィンドウまたは［**Kaspersky Security サービス管理用のユーザーアクセス権限**］ウィンドウで、SDDL 文字列を指定してユーザーまたはグループを追加します。

7. ［**OK**］をクリックします。

## Kaspersky Embedded Systems Security 機能へのパスワードで保護されたアクセス

ユーザー権限の設定によって、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。

次のアプリケーション機能にアクセスしようとすると、Kaspersky Embedded Systems Security はパスワードを要求します：

- アプリケーションコンソールへの接続
- Kaspersky Embedded Systems Security のアンインストール
- Kaspersky Embedded Systems Security コンポーネントの変更
- コマンドラインによるコマンドの実行

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。

パスワードで保護するアプリケーションの設定をエクスポートおよびインポートできます。保護対象アプリケーション設定をエクスポートすると作成される設定ファイルには、パスワードチェックサムおよびパスワード文字列の空白を埋めるために使用される修飾子の値が含まれています。

設定ファイルのチェックサムや修飾子は変更しないでください。手動で変更されたパスワードによる保護の設定をインポートすると、アプリケーションへのアクセスが完全にブロックされる場合があります。

*Kaspersky Embedded Systems Security 機能へのアクセスを保護するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］-［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**アプリケーションの設定**］セクションを選択します。
5. ［アプリケーションの設定］セクションの［**セキュリティと信頼性**］セクションで、［**設定**］をクリックします。
6. ［**パスワードによる保護の設定**］セクションで、［**パスワードによる保護を適用する**］をオンにします。
7. ［**パスワード**］で、Kaspersky Embedded Systems Security 機能へのアクセスを保護するために使用するパスワードを入力します。

8. ［**OK**］をクリックします。

指定された設定が保存されます。保護対象機能へのアクセスに、指定したパスワードが要求されるようになります。

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アプリケーションをアンインストールできなくなります。

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［**パスワードによる保護を適用する**］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。

# ファイルのリアルタイム保護

このセクションでは、ファイルのリアルタイム保護タスクとその設定方法について説明します。

## ファイルのリアルタイム保護タスクについて

ファイルのリアルタイム保護タスクが実行されている場合、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 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

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 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。

## 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タスク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。セキュリティ要件でファイルシステムのオブジェクトすべてを保護することまでは求められていない場合、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ツリーまたはリストとして表示されます。既定では、デバイスのネットワークファイルリソースがリストで表示されます。

管理プラグインでは、リストビューのみ使用できます。

*ネットワークファイルリソースをアプリケーションコンソールのツリーで表示するには：*

［**保護範囲の設定**］ウィンドウの左上部にあるドロップダウンリストを開き、［**ツリービュー**］を選択します。

保護対象デバイスのファイルリソースがリストまたはツリーで表示される場合に、フォルダーアイコンは次の意味を持ちます：

☑フォルダーが保護範囲に含まれています。

☐フォルダーが保護範囲から除外されています。

☑このフォルダーの1つ以上の子フォルダーが保護範囲から除外されています。または、この子フォルダーと親フォルダーのセキュリティ設定が異なります（ツリービューの場合のみ）。

☑ アイコンは、親フォルダーを除くすべてのサブフォルダーが選択されている場合に表示されます。この場合、親フォルダーのファイルとフォルダーの構成の変更は、選択した子フォルダーの保護範囲の作成中には自動的に無視されます。

アプリケーションコンソールを使用して、［仮想ドライブ］を保護範囲に追加することもできます。仮想フォルダーの名前は、青色で表示されます。

### 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ツリーまたは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。
- ファイルリソースツリーまたは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）。

フォルダーや項目の一連の設定をテンプレートに保存して、後で他のフォルダーや項目に適用することができます。

## 仮想保護範囲について

Kaspersky Embedded Systems Security では、ハードディスクとリムーバブルドライブ上の既存のフォルダーとファイルだけでなく、さまざまなアプリケーションやサービスによって保護対象デバイス上に動的に作成されたドライブもスキャンすることができます。

保護範囲にすべてのデバイスオブジェクトが含まれている場合、これらのダイナミックフォルダーも自動的に保護範囲に含まれます。ただし、これらのダイナミックフォルダーのセキュリティ設定に特定の値を指定する場合、または保護の対象としてデバイスの一部のみを選択した後で、仮想ドライブ、ファイル、またはフォルダーを保護範囲に追加する場合は、最初にそれらをアプリケーションコンソールで作成する（つまり、仮想保護範囲を指定する）必要があります。作成されたドライブ、ファイル、およびフォルダーはアプリケーションコンソールにのみ存在します。保護対象デバイスのファイル構造内には存在しません。

保護範囲の作成中に、親フォルダーを選択せずにすべてのサブフォルダーまたはファイルを選択した場合は、そこに表示されるすべての仮想フォルダーまたはファイルが自動的に保護範囲に含まれることはありません。これらの「仮想コピー」をアプリケーションコンソールで作成し、保護範囲に追加する必要があります。

## 定義済みの保護範囲

ファイルリソースのツリーまたはリストには、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。
- **仮想ドライブ**：共有のクラスタードライブなどの、一時的にデバイスに接続される仮想フォルダー、ファイル、およびドライブを保護範囲に含めることができます。

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。

既定では、仮想ドライブを除くすべての定義済みの領域が保護範囲に含まれます。

SUBST コマンドを使用して作成した仮想ドライブは、アプリケーションコンソールの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。仮想ドライブ上のオブジェクトを保護範囲に含めるには、仮想ドライブと関連付けられているデバイスのフォルダーを保護範囲に含めます。

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 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：［**最高のパフォーマンス**］、［**推奨**］、［**最大の保護**］。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）。

## 最高のパフォーマンス

［**最高のパフォーマンス**］ セキュリティレベルは、保護対象デバイスでの 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で高い水準のデバイスセキュリティ要件が求められる場合、［**最大の保護**］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 | | |
|---|---|---|---|
| | **最高のパフォーマンス** | **推奨** | **最大の保護** |
| **オブジェクトの保護** | 拡張子に基づく | 形式に基づく | 形式に基づく |
| **作成または変更されたファイルのみを保護** | 有効 | 有効 | 無効 |
| **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 | 通知のみ | アクセスをブロックして駆除、駆除できない場合は削除 |
| **感染の可能性があるオブジェクトの処理** | アクセスをブロックして隔離 | 通知のみ | アクセスをブロックして隔離 |
| **除外するファイル** | なし | なし | なし |
| **検知しない** | 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 | 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 |
| **NTFS 代替データストリームをスキャン** | 有効 | 有効 | 有効 |
| **ディスクのブートセクターと MBR をスキャン** | 有効 | 有効 | 有効 |
| **複合オブジェクトの保護** | • 圧縮されたオブジェクト*<br><br>*新規および変更されたオブジェクトのみ | • SFX アーカイブ*<br>• 圧縮されたオブジェクト*<br>• OLE 埋め込みオブジェクト*<br><br>*新規および変更されたオブジェクトのみ | • SFX アーカイブ*<br>• 圧縮されたオブジェクト*<br>• OLE 埋め込みオブジェクト*<br><br>* すべてのオブジェクト |
| **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 | 有効 |

［**オブジェクトの保護**］、［**iChecker を使用する**］、［**iSwift を使用する**］、および［**ヒューリスティックアナライザーを使用する**］の設定は、定義済みのセキュリティレベルの設定に含まれていません。事前に設定されたセキュリティレベルのいずれかを選択した後で、［**オブジェクトの保護**］、［**iChecker を使用する**］、［**iSwift を使用する**］、または［**ヒューリスティックアナライザーを使用する**］のセキュリティ設定を編集しても、選択したセキュリティレベルは変更されません。

# ファイルのリアルタイム保護タスク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、次のとおりです：

- *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タスクの既定の設定

既定では、ファイルのリアルタイム保護タスクでは、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タスクの既定の設定

| 設定 | 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。 | 保護範囲を変更することができます。 |
| 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** | 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指定できます。 |
| **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。 |
| **信頼ゾーンを適用する** | 適用されます。 | 選択したタスクで使用できる一般的な信頼するオブジェクト。 |
| **保護に KSN を使用する** | 適用されます。 | Kaspersky Security Network のクラウドサービスを使用して、デバイスの保護を改善することができます（KSN に関する声明に同意している場合に利用できます）。 |
| タスク開始スケジュール | アプリケーション開始時 | タスク開始スケジュールを設定できます。 |
| **悪意のある活動を示すコンピューター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。 | 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すコンピューターを追加できます。 |
| **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、一時的な簡易スキャンタスクが作成され、起動します。 |

## 管理プラグインからファイルのリアルタイム保護タスクを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの1つまたはすべての保護対象デバイスのタスクを設定する方法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。

## ファイルのリアルタイム保護タスクのポリシーの設定ウィンドウ

*Kaspersky Security Center のポリシーからファイルのリアルタイム保護タスクの設定を開くには：*

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. 表示された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**］セクションを選択します。
6. ［**ファイルのリアルタイム保護**］サブセクションで［**設定**］をクリックします。

［**ファイルのリアルタイム保護**］ウィンドウが開きます。

保護対象デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、アプリケーションコンソールでこれらの設定を編集することはできません。

## ファイルのリアルタイム保護タスクのプロパティウィンドウ

*1 つのネットワークデバイスのファイルのリアルタイム保護タスクの設定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、保護対象デバイスのプロパティ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コンテキストメニューで［**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. ［**タスク**］セクションで、［**ファイルのリアルタイム保護**］タスクを選択します。
6. ［**プロパティ**］をクリックします。
   **ファイルのリアルタイム保護**のプロパティウィンドウが開きます。

## ファイルのリアルタイム保護タスクの設定

*ファイルのリアルタイム保護タスクの設定を編集するには：*

1. ［**ファイルのリアルタイム保護**］ウィンドウを開きます。
2. 次のタスクの設定を指定します：
   - ［**全般**］タブ：
     - **監視パラメータ**
     - **ヒューリスティックアナライザー**
     - **他のコンポーネントとの連携**
   - ［**タスク管理**］タブ：
     - タスク開始スケジュール設定

3. ［**保護範囲**］タブを選択し、次の操作を行います：

- ［**追加**］または［**編集**］をクリックして保護範囲を編集します。
  - 表示されたウィンドウで、タスクの保護範囲に含めるものを選択します：
    - **定義済みの範囲**
    - **ディスク、フォルダー、またはネットワークの場所**
    - **ファイル**
  - 定義済みのセキュリティレベルの1つを選択するか、またはスキャンの設定を手動で行います。

4. ［**ファイルのリアルタイム保護**］ウィンドウで［OK］をクリックします。

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、および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。

## 保護モードの選択

ファイルのリアルタイム保護タスクでは、保護モードを選択できます。［**オブジェクトの保護モード**］セクションでは、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指定できます。

［**オブジェクトの保護モード**］設定の値は、タスクで指定された保護範囲全体に適用されます。保護範囲内の個別のフォルダーの設定に対して、別の値を指定することはできません。

*保護モードを選択するには：*

1. ［**ファイルのリアルタイム保護**］ウィンドウを開きます。
2. 表示されたウィンドウの［**全般**］タブで、設定する保護モードを選択します：
   - **スマートモード**
   - **アクセス時と変更時**
   - **アクセス時**
   - **実行時**
   - **起動プロセスのより詳細な分析（プロセスの起動は分析が終了するまでブロックされます）**
3. ［OK］をクリックします。

選択された保護モードが有効になります。

## ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの統合の設定

KSN の使用タスクを開始するには、Kaspersky Security Network に関する声明に同意する必要があります。

*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統合を設定するには：*

1. ［**ファイルのリアルタイム保護**］ウィンドウを開きます。
2. ［**全般**］タブで、［**ヒューリスティックアナライザーを使用する**］をオフまたはオンにします。
3. 必要に応じて、スライダーを使用して分析のレベルを調整します。
4. ［**他のコンポーネントとの連携**］セクションで、次の設定を行います：
   - ［**信頼ゾーンを適用する**］をオンまたはオフにします。
   - ［**保護に KSN を使用する**］をオンまたはオフにします。

     ［KSN の使用］タスクの設定で、［**スキャンしたファイルに関するデータを送信**］をオンにする必要があります。

   - ［**悪意のある活動を示すコンピューター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。
   - ［**アクティブな脅威の検知時に簡易スキャンを起動する**］をオンまたはオフにします。
5. ［**OK**］をクリックします。

構成されたタスクの設定は、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。

## 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、タスクのプロパティ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. ［**スケジュール設定**］セクションで、［**スケジュールに従って実行する**］をオンにします。

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。

7. 要件に従ってスケジュールを設定します。それには、次の操作を実行します：

a. ［**頻度**］リストでは、次の値のいずれかを選択します：

- ［**時間単位**］：指定された時間間隔でタスクを実行する場合は、［**間隔：<数字> 時間**］で時間数を指定します。
- ［**日単位**］：指定された日間隔でタスクを実行する場合は、［**間隔：<数字> 日**］で日数を指定します。
- ［**週単位**］：指定された週間隔でタスクを実行する場合は、［**間隔：<数字> 週**ごと］で週数を指定します。タスクを開始する曜日を指定します（既定では、タスクは月曜日に実行されます）。
- ［**アプリケーションの起動時**］：Kaspersky Embedded Systems Security が起動するたびにタスクを実行します。
- ［**定義データベースのアップデート後**］：定義データベースのアップデート後にタスクを実行します。

b. ［**開始時刻**］にタスクを最初に開始する時刻を指定します。

c. ［**開始日**］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、［**タスクの設定**］ウィンドウを開きます。ウィンドウの上部にある［**次回開始**］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、［**次回開始**］には［**ポリシーによりブロック**］と表示されます。

8. ［**詳細設定**］タブを使用して、要件に従って以下のスケジュール設定を指定します：

- ［**タスクの停止設定**］セクション：

a. ［**経過時間**］をオンにして、タスクの最長実行時間を時間と分で右側のフィールドに入力します。

b. ［**一時停止**］をオンにして、タスクの実行が一時停止される時間帯の開始と終了の値（24 時間で指定）を右側のフィールドに入力します。

- ［**詳細設定**］セクション：

a. ［**スケジュール終了日**］をオンにして、スケジュールの適用を停止する日付を指定します。

b. ［**スキップしたタスクを実行する**］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。

c. ［**タスクの開始時刻を次の期間内でランダム化する**］をオンにして、値を分で指定します。

9. ［**OK**］をクリックします。

10. ［**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。

## タスクの保護範囲の作成と編集

*Kaspersky Security Center からタスクの保護範囲を作成して編集するには：*

1. ［**ファイルのリアルタイム保護**］ウィンドウを開きます。

2. ［**保護範囲**］タブを選択します。
タスクによって既に保護されているすべての項目は、［**保護範囲**］テーブルに表示されます。

3. ［**追加**］をクリックして、新しい項目をリストに追加します。
［**保護範囲にオブジェクトを追加**］ウィンドウが開きます。

4. 保護範囲に追加するオブジェクトの種別を選択します：

- **定義済みの範囲**：いずれかの定義済み範囲をデバイスの保護範囲に含めます。ドロップダウンリストで、目的の保護範囲を選択します。
- **ディスク、フォルダー、またはネットワークの場所**：個別のドライブ、フォルダー、またはネットワークオブジェクトを保護範囲に含めます。［**参照**］をクリックして目的の保護範囲を選択します。
- **ファイル**：個別のファイルを保護範囲に含めます。［**参照**］をクリックして目的の保護範囲を選択します。

オブジェクトが既に保護範囲からの除外対象として追加されている場合、保護範囲には追加できません。

5. 保護範囲から個別の項目を除外するには、これらの項目の名前の横にあるチェックボックスをオフにするか、次の手順を実行します：

a. 保護範囲を右クリックして、コンテキストメニューを開きます。

b. コンテキストメニューで、［**除外の追加**］を選択します。

c. ［**除外の追加**］ウィンドウで、保護範囲にオブジェクトを追加する時に使用する手順に従い、保護範囲からの除外対象として追加するオブジェクトの種別を選択します。

6. 保護範囲または既存の除外対象を変更するには、該当する保護範囲のコンテキストメニューで［**範囲の編集**］を選択します。

7. ネットワークファイルリソースのリストに以前追加した保護範囲または除外対象を非表示にするには、該当する保護範囲のコンテキストメニューで［**範囲の削除**］を選択します。

保護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、ファイルのリアルタイム保護タスクの範囲から除外されます。

8. ［**OK**］をクリックします。

［保護範囲の設定］ウィンドウが閉じます。新しい設定が保存されます。

**ファイルのリアルタイム保護**タスクは、デバイスのファイルリソースツリーのフォルダーが1つ以上保護範囲に含まれている場合に開始できます。

## 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

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：［**最高のパフォーマンス**］、［**推奨**］、［**最大の保護**］。

*事前に定義されたセキュリティレベルのいずれかを選択するには：*

1. **ファイルのリアルタイム保護**のプロパティウィンドウが開きます。
2. ［**保護範囲**］タブを選択します。
3. 保護対象デバイスのリストで保護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。
   ［**ファイルのリアルタイム保護の設定**］ウィンドウが開きます。
5. ［**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。
   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。
6. ［**OK**］をクリックします。
7. **ファイルのリアルタイム保護**のプロパティウィンドウで［**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。

## 手動でのセキュリティの設定

ファイルのリアルタイム保護タスクでは、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。

*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：*

1. ［**ファイルのリアルタイム保護**］ウィンドウを開きます。
2. ［**保護範囲**］タブでセキュリティ設定を行うフォルダーを選択し、［**設定**］をクリックします。
   ［**ファイルのリアルタイム保護の設定**］ウィンドウが開きます。
3. ［**セキュリティレベル**］タブで、［**設定**］をクリックして設定をカスタマイズします。
4. 要件に従って、選択したフォルダーのカスタムのセキュリティ設定を行えます：
   - 全般設定
   - 処理
   - パフォーマンス
5. ［**ファイルのリアルタイム保護**］ウィンドウで［**OK**］をクリックします。

新しい保護範囲の設定が保存されます。

## タスクの全般的な設定

*ファイルのリアルタイム保護タスクのセキュリティの全般設定を行うには：*

1. ［**ファイルのリアルタイム保護の設定**］ウィンドウを開きます。
2. ［**全般**］タブを選択します。
3. ［**オブジェクトの保護**］セクションで、保護範囲に含めるオブジェクトの種別を指定します：
   - 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**
   - **指定の拡張子リストによってオブジェクトをスキャン**
   - **ディスクのブートセクターと MBR をスキャン**
   - **NTFS 代替データストリームをスキャン**
4. ［**パフォーマンス**］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。

   チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の［すべての / 新しい（～のみ）］をクリックします。

5. ［**複合オブジェクトの保護**］で、保護範囲に含める複合オブジェクトを指定します：

- すべてのアーカイブ / **新しい アーカイブのみ** / アーカイブ
- すべての SFX アーカイブ / **新しい SFX アーカイブのみ** / SFX アーカイブ
- すべてのメールデータベース / **新しい メールデータベースのみ** / メールデータベース
- すべての圧縮されたオブジェクト / **新しい 圧縮されたオブジェクトのみ** / 圧縮されたオブジェクト
- すべての通常のメール / **新しい 通常のメールのみ** / 通常のメール
- すべての OLE 埋め込みオブジェクト / **新しい OLE 埋め込みオブジェクトのみ** / OLE 埋め込みオブジェクト

6. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## 処理の設定

*ファイルのリアルタイム保護タスク中に、感染したオブジェクトおよびその他の検知されたオブジェクトの処理を設定するには：*

1. ［**ファイルのリアルタイム保護の設定**］ウィンドウを開きます。
2. ［**処理**］タブを選択します。
3. 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：
   - **通知のみ**
   - **アクセスをブロック**
   - **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。駆除できない場合は削除**
     - **削除**
     - **推奨**
4. 感染の可能性があるオブジェクトの処理を選択します：
   - **通知のみ**
   - **アクセスをブロック**
   - **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：
     - **隔離**

- **削除**
- **推奨**

5. 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. ［**検知したオブジェクトの種別に応じて処理を実行**］をオンまたはオフにします。

   b. ［**設定**］をクリックします。

   c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理（最初の処理が失敗した場合に実行）を選択します。

   d. ［**OK**］をクリックします。

6. 修正できない複合ファイルに対して実行する処理を選択します：［**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**］をオンまたはオフにします。

7. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## パフォーマンスの設定

*ファイルのリアルタイム保護タスクのパフォーマンスを設定するには：*

1. ［**ファイルのリアルタイム保護の設定**］ウィンドウを開きます。
2. ［**パフォーマンス**］タブを選択します。
3. ［**除外リスト**］セクション：
   - ［**除外するファイル**］をオフまたはオンにします。
   - ［**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。
4. ［**詳細設定**］セクション：
   - **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**

## アプリケーションコンソールからファイルのリアルタイム保護タスクを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、保護デバイスのタスクの設定を行う方法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。

## ファイルのリアルタイム保護タスクの設定ウィンドウ

*タスクの全般的な設定のウィンドウを開くには：*

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. ［**ファイルのリアルタイム保護**］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。
   ［**タスクの設定**］ウィンドウが表示されます。

## ファイルのリアルタイム保護タスクの範囲の設定ウィンドウ

*ファイルのリアルタイム保護タスクの保護範囲の設定ウィンドウを開くには：*

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. ［**ファイルのリアルタイム保護**］サブフォルダーを選択します。
3. 結果ペインで［**保護範囲の設定**］をクリックします。
   ［**保護範囲の設定**］ウィンドウが開きます。

## ファイルのリアルタイム保護タスクの設定

*ファイルのリアルタイム保護タスクの設定を編集するには：*

1. ［**タスクの設定**］ウィンドウを開きます。
2. ［**全般**］タブで、次のタスク設定を行います：
   - オブジェクトの保護モード
   - **ヒューリスティックアナライザー**
   - **他のコンポーネントとの連携**

3. ［**スケジュール**］タブと［**詳細設定**］タブで、開始スケジュールを設定します。

4. ［**タスクの設定**］ウィンドウで［OK］をクリックします。
   変更された設定が保存されます。

5. ［**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。

6. 次の操作を実行します：

   - デバイスのファイルリソースのツリーまたはリストで、タスクの保護範囲に含めるフォルダーや項目を選択します。
   - 定義済みのセキュリティレベルから1つを選択するか、オブジェクトの保護を手動で設定します。

7. ［**保護範囲の設定**］ウィンドウで、［**保存**］をクリックします。

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、および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。

## 保護モードの選択

ファイルのリアルタイム保護タスクでは、保護モードを選択できます。［**オブジェクトの保護モード**］セクションでは、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指定できます。

［**オブジェクトの保護モード**］設定の値は、タスクで指定された保護範囲全体に適用されます。保護範囲内の個別のフォルダーの設定に対して、別の値を指定することはできません。

*保護モードを選択するには：*

1. ［**タスクの設定**］ウィンドウを開きます。

2. 表示されたウィンドウの［**全般**］タブで、設定する保護モードを選択します：

   - **スマートモード**
   - **アクセス時と変更時**
   - **アクセス時**
   - **実行時**
   - **起動プロセスのより詳細な分析（プロセスの起動は分析が終了するまでブロックされます）**

3. ［OK］をクリックします。

選択された保護モードが有効になります。

## ヒューリスティックアナライザーと他のアプリケーションコンポーネントとの統合の設定

KSN の使用タスクを開始するには、Kaspersky Security Network に関する声明に同意する必要があります。

*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統合を設定するには：*

1. ［**タスクの設定**］ウィンドウを開きます。
2. ［**全般**］タブで、［**ヒューリスティックアナライザーを使用する**］をオフまたはオンにします。
3. 必要に応じて、スライダーを使用して分析のレベルを調整します。
4. ［**他のコンポーネントとの連携**］セクションで、次の設定を行います：
   - ［**信頼ゾーンを適用する**］をオンまたはオフにします。
     ［**信頼ゾーン**］をクリックして、信頼ゾーンの設定を開きます。
   - ［**保護に KSN を使用する**］をオンまたはオフにします。

     ［KSN の使用］タスクの設定で、［**スキャンしたファイルに関するデータを送信**］をオンにする必要があります。
   - ［**悪意のある活動を示すコンピューター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。
   - ［**アクティブな脅威の検知時に簡易スキャンを起動する**］をオンまたはオフにします。
5. ［**OK**］をクリックします。

新しい設定が適用されます。

## 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. スケジュールを設定するタスク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。
   ［**タスクの設定**］ウィンドウが表示されます。
3. 表示されたウィンドウの［**スケジュール**］タブで、［**スケジュールに従って実行する**］をオンにします。
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**］ドロップダウンメニューでは、次のいずれかを選択します：
      - ［**時間単位**］：1 時間間隔でタスクを実行します。指定された時間間隔でタスクを実行する場合は、［**間隔 <number> 時間**］で時間数を指定します。

- ［**日単位**］：日単位でタスクを実行します。指定された日間隔でタスクを実行する場合は、［**間隔 <number> 日**］で日数を指定します。
- ［**週単位**］：週単位でタスクを実行します。指定された週間隔でタスクを実行する場合は、［**間隔 <number> 週ごと、曜日**］で週数を指定します。タスクが開始される曜日を指定します（既定では、タスクは月曜日に実行されます）。
- ［**アプリケーションの起動時**］：Kaspersky Embedded Systems Security が起動するたびにタスクを実行します。
- ［**定義データベースのアップデート後**］：定義データベースのアップデート後にタスクを実行します。

b. ［**開始時刻**］フィールドに、タスクの初回開始時刻を指定します。

c. ［**開始日**］フィールドに、タスクの初回開始日を指定します。

タスクの開始頻度、タスクが最初に開始される時刻、およびスケジュールの適用開始日を指定したら、ウィンドウ上部の［**次回開始**］に、計算された次回のタスク開始時間が表示されます。［**タスクの設定**］ウィンドウの［**スケジュール**］タブを開くたびに、次回タスクが開始される予定の日時が更新されて、表示されます。

Kaspersky Security Center の有効な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、［**次回開始**］には［**ポリシーによりブロック**］と表示されます。

5. ［**詳細設定**を使用して次のスケジュールを指定します。

- ［**タスクの停止設定**］セクション：
  a. ［**経過時間**］を選択します。右側のフィールドに、最大タスク期間を時間と分単位で入力します。
  b. ［**一時停止**］をオンにします。右側のフィールドに、タスクを一時停止および再開する時間を入力します（24時間以内）。
- ［**詳細設定**］セクション：
  a. ［**スケジュール終了日**］を選択してタスクのスケジュールの終了日を指定します。
  b. ［**スキップしたタスクを実行する**］をオンにして、スキップしたタスクを開始します。
  c. ［**タスク開始を次の期間内でランダム化する**］をオンにして、値を分で指定します。

6. ［**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。

## 保護範囲の作成

このセクションでは、ファイルのリアルタイム保護タスクの保護範囲の作成と管理について説明します。

## ネットワークファイルリソースのビューの設定

*保護範囲設定時のネットワークファイルリソースのビューを選択するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストを開き、次のオプションのいずれかを選択します：
   - ［**ツリービュー**］を選択し、ネットワークファイルリソースをツリーで表示する。
   - ［**リストビュー**］を選択し、ネットワークファイルリソースをリストで表示する。

   既定では、保護対象デバイスのネットワークファイルリソースがリストで表示されます。
3. ［**保存**］をクリックします。

## 保護範囲の作成

ファイルのリアルタイム保護のタスク範囲を作成する手順は、ネットワークファイルリソースのビューに応じて異なります。ネットワークファイルリソースをツリーまたはリストとして表示できます（既定として設定）。

タスクに新しい保護範囲設定を適用するには、ファイルのリアルタイム保護タスクを再起動する必要があります。

*ネットワークファイルリソースツリーを使用して保護範囲を作成するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左側のセクションでネットワークファイルリソースツリーを開き、すべてのフォルダーとサブフォルダーを表示します。
3. 次の操作を実行します：
   - 保護範囲から個別のフォルダーを除外するには、除外したい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。
   - 個別のフォルダーを保護範囲に含めるには、［**マイコンピューター**］をオフにして、次の操作を行います：
     - 同じ種別のすべてのドライブを保護範囲に含める場合は、対象のディスク種別の名前の横にあるチェックボックスをオンにします。たとえば、デバイス上のすべてのリムーバブルドライブを追加する場合は、［**リムーバブルドライブ**］をオンにします。
     - 特定の種別の個々のディスクを保護範囲に含める場合は、その種別のドライブのリストを含むフォルダーを展開し、対象のドライブの名前の横にあるチェックボックスをオンにします。たとえば、リムーバブルドライブ F: を選択する場合は、［**リムーバブルドライブ**］フォルダーを展開し、ドライブ **F:** のチェックボックスをオンにします。

- ドライブ上のフォルダーまたはファイルを1つのみ含める場合は、そのフォルダーまたはファイルの名前の横にあるチェックボックスをオンにします。

4. ［**保存**］をクリックします。

［**保護範囲の設定**］ウィンドウが閉じます。新しい設定が保存されます。

*ネットワークファイルリソースリストを使用して保護範囲を作成するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. 個別のフォルダーを保護範囲に含めるには、［**マイコンピューター**］をオフにして、次の操作を行います：
   a. 保護範囲を右クリックして、コンテキストメニューを開きます。
   b. ボタンのコンテキストメニューで、［**保護範囲の追加**］を選択します。
   c. ［**保護範囲の追加**］ウィンドウでオブジェクトの種別を選択し、保護範囲に追加します：
      - **定義済みの範囲**：いずれかの定義済み範囲をデバイスの保護範囲に含めます。ドロップダウンリストで、目的の保護範囲を選択します。
      - **ディスク、フォルダー、またはネットワークの場所**：個別のドライブ、フォルダー、またはネットワークオブジェクトを保護範囲に含めます。［**参照**］をクリックして目的の範囲を選択します。
      - **ファイル**：個別のファイルを保護範囲に含めます。［**参照**］をクリックして目的の範囲を選択します。

   オブジェクトが既に保護範囲からの除外対象として追加されている場合、保護範囲には追加できません。

3. 保護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するか、次の手順を実行します：
   a. 保護範囲を右クリックして、コンテキストメニューを開きます。
   b. コンテキストメニューで、［**除外の追加**］を選択します。
   c. ［**除外の追加**］ウィンドウで、保護範囲にオブジェクトを追加する時に使用する手順に従い、保護範囲からの除外対象として追加するオブジェクトの種別を選択します。
4. 保護範囲または既存の除外対象を変更するには、該当する保護範囲のコンテキストメニューで［**範囲の編集**］を選択します。
5. ネットワークファイルリソースのリストに以前追加した保護範囲または除外対象を非表示にするには、該当する保護範囲のコンテキストメニューで［リストから削除］を選択します。

   保護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、ファイルのリアルタイム保護タスクの範囲から除外されます。

6. ［**保存**］をクリックします。

［**保護範囲の設定**］ウィンドウが閉じます。新しい設定が保存されます。

ファイルのリアルタイム保護タスクは、デバイスのファイルリソースツリーのフォルダーが1つ以上保護範囲に含まれている場合に開始できます。

複雑な保護範囲が指定されている場合（たとえば、デバイスのファイルリソースツリーで複数のフォルダーが指定され、それらのセキュリティ設定の値が異なる場合）、オブジェクトがアクセスされた時のスキャン速度が低下する場合があります。

## 保護範囲にネットワークオブジェクトを含める

UNC（ユニバーサルネーミング規約）フォーマットでパスを指定して、ネットワークドライブや、フォルダー、ファイルを保護範囲に追加することができます。

システムアカウントでネットワークフォルダーをスキャンできます。

*ネットワークの場所を保護範囲に追加するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストを開き、［**ツリービュー**］を選択します。
3. ［**ネットワーク**］フォルダーのコンテキストメニューを開きます：
   - 保護範囲にネットワークフォルダーを追加する場合は、［**ネットワークフォルダーの追加**］を選択します。
   - 保護範囲にネットワークファイルを追加する場合は、［**ネットワークファイルの追加**］を選択します。
4. ネットワークフォルダーまたはファイルへのパスを UNC フォーマットで入力します。
5. **ENTER** キーを押します。
6. 新しく追加されたネットワークオブジェクトの横にあるチェックボックスをオンにして、保護範囲に含めます。
7. 必要に応じて、追加したネットワークオブジェクトのセキュリティ設定を変更します。
8. ［**保存**］をクリックします。

変更されたタスクの設定が保存されます。

## 仮想保護範囲の作成

ファイルリソースのツリーとして保護範囲またはスキャン範囲が表示されている場合に限り、個別の仮想ドライブ、フォルダー、またはファイルを追加して、保護範囲またはスキャン範囲を拡張することができます。

*仮想ドライブを保護範囲に追加するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストより、［**ツリービュー**］を選択します。
3. ［**仮想ドライブ**］フォルダーのコンテキストメニューを開きます。
4. ［**仮想ドライブの追加**］オプションを選択します。
5. 選択可能な名前のリストから、作成中の仮想ドライブの名前を選択します。
6. ドライブの横のチェックボックスをオンにすると、そのドライブが保護範囲に追加されます。
7. ［**保護範囲の設定**］ウィンドウで、［**保存**］をクリックします。

新しい設定が保存されます。

*仮想フォルダーまたは仮想ファイルを保護範囲に追加するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストを開き、［**ツリービュー**］を選択します。
3. フォルダーまたはファイルを追加する仮想ドライブのコンテキストメニューを開き、次のいずれかを選択します：
   - **仮想フォルダーの追加**：保護範囲に仮想フォルダーを追加する場合に選択します。
   - **仮想ファイルの追加**：スキャン範囲に仮想ファイルを追加する場合に選択します。
4. 入力フィールドに、フォルダーまたはファイルの名前を指定します。
5. 作成されたフォルダーまたはファイルの名前と同じチェックボックスをオンにして、このフォルダーまたはファイルを保護範囲に追加します。
6. ［**保護範囲の設定**］ウィンドウで、［**保存**］をクリックします。

変更されたタスクの設定が保存されます。

## 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。

*手動でセキュリティを設定するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左側のセクションで、セキュリティ設定を行うフォルダーを選択します。

   セキュリティ設定を含む定義済みのテンプレートは、保護範囲内の選択したフォルダーまたは項目に適用できます。

   ウィンドウの左側で、ネットワークファイルリソースのビューを選択、保護範囲を作成、または仮想保護範囲を作成できます。
3. ウィンドウの右側で、次のいずれかを行います：
   - ［**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。
   - 要件に従って、次のタブで、選択したフォルダーや項目に必要なセキュリティを設定します：
     - **全般**
     - **処理**
     - **パフォーマンス**
4. ［**保護範囲の設定**］ウィンドウで、［**保存**］をクリックします。

新しい保護範囲の設定が保存されます。

## ファイルのリアルタイム保護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ツリーまたは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：［**最高のパフォーマンス**］、［**推奨**］、［**最大の保護**］。

*事前に定義されたセキュリティレベルのいずれかを選択するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. 保護対象デバイスのネットワークファイルリソースツリーまたはリストで、定義済みセキュリティレベルを設定するフォルダーや項目を選択します。
3. 選択したフォルダーや項目が保護範囲に含まれることを確認します。
4. ウィンドウの右側の［**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。

   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。
5. ［**保存**］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。

## タスクの全般的な設定

*ファイルのリアルタイム保護タスクのセキュリティの全般設定を行うには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ［**全般**］タブを選択します。
3. ［**オブジェクトの保護**］セクションで、保護範囲に含めるオブジェクトを指定します：
   - **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**
   - **指定の拡張子リストによってオブジェクトをスキャン**
   - **ディスクのブートセクターと MBR をスキャン**
   - **NTFS 代替データストリームをスキャン**
4. ［**パフォーマンス**］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。

   チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の［**すべての / 新しい（～のみ）**］をクリックします。

5. ［**複合オブジェクトの保護**］で、保護範囲に含める複合オブジェクトを指定します：
   - **すべてのアーカイブ** / **新しい アーカイブのみ** / アーカイブ
   - **すべての SFX アーカイブ** / **新しい SFX アーカイブのみ** / SFX アーカイブ
   - **すべてのメールデータベース** / **新しい メールデータベースのみ** / メールデータベース
   - **すべての圧縮されたオブジェクト** / **新しい 圧縮されたオブジェクトのみ** / 圧縮されたオブジェクト
   - **すべての通常のメール** / **新しい 通常のメールのみ** / 通常のメール
   - **すべての OLE 埋め込みオブジェクト** / **新しい OLE 埋め込みオブジェクトのみ** / OLE 埋め込みオブジェクト
6. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## 処理の設定

*ファイルのリアルタイム保護タスクで、感染したオブジェクトおよびその他の検知されたオブジェクトの処理を設定するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ［**処理**］タブを選択します。
3. 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：
   - **通知のみ**
   - **アクセスをブロック**
   - **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。駆除できない場合は削除**
     - **削除**
     - **推奨**
4. 感染の可能性があるオブジェクトの処理を選択します：
   - **通知のみ**
   - **アクセスをブロック**
   - **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：
     - **隔離**
     - **削除**
     - **推奨**
5. 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. ［**検知したオブジェクトの種別に応じて処理を実行**］をオンまたはオフにします。
   b. ［**設定**］をクリックします。
   c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理（最初の処理が失敗した場合に実行）を選択します。
   d. ［**OK**］をクリックします。
6. 修正できない複合ファイルに対して実行する処理を選択します：［**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**］をオンまたはオフにします。
7. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## パフォーマンスの設定

*ファイルのリアルタイム保護タスクのパフォーマンスを設定するには：*

1. ［**保護範囲の設定**］ウィンドウを開きます。
2. ［**パフォーマンス**］タブを選択します。
3. ［**除外リスト**］セクション：
   - ［**除外するファイル**］をオフまたはオンにします。
   - ［**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。
4. ［**詳細設定**］セクション：
   - **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**

## ファイルのリアルタイム保護タスクの統計情報

ファイルのリアルタイム保護タスクの実行中は、タスクが開始されてから処理されたオブジェクト数の詳細をリアルタイムで表示できます。

*ファイルのリアルタイム保護タスクの統計を表示するには：*

1. アプリケーションコンソールツリーで、［**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. ［**ファイルのリアルタイム保護**］サブフォルダーを選択します。

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）。

ファイルのリアルタイム保護タスクの統計情報

| 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の検知** | 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ファイルの検知数。 |
| **感染の可能性があるオブジェクトの検知** | Kaspersky Embedded Systems Security が感染の可能性を検知したオブジェクトの数。 |
| **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。 |
| **隔離されていないオブジェクト** | 隔離に移動しようとしたが、ディスク容量不足などにより移動できなか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。 |
| **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。 |
| **バックアップされていないオブジェクト** | バックアップにコピーを保存しようとしたが、ディスク容量不足などにより保存できなかっ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。 |
| **駆除されたオブジェクト** | 駆除されたオブジェクトの数。 |
| **隔離済み** | 隔離されたオブジェクトの数。 |
| **バックアップ済み** | バックアップに保存されたオブジェクトコピーの数。 |
| **削除されたオブジェクト** | 削除されたオブジェクトの数。 |
| **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、スキャンできなかったオブジェクト（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。 |
| **処理されたオブジェクト** | 処理されたオブジェクトの合計数。 |

ファイルのリアルタイム保護タスクの統計情報をタスク実行ログに表示するには、詳細ペインの［**管理**］セクションにある［**実行ログを開く**］をクリックします。

ファイルのリアルタイム保護実行ログウィンドウの［**イベント総数**］の値が 0 を超えている場合は、［**イベント**］タブのタスク実行ログのイベントを手動で処理してください。

## Web プラグインからファイルのリアルタイム保護タスクを管理する

このセクションでは、Web プラグインのインターフェイスからファイルのリアルタイム保護タスクを管理する方法について説明します。

# ファイルのリアルタイム保護タスクの設定

Web プラグインからのファイルのリアルタイム保護タスクでは、定義済みセキュリティレベルを変更することはできません。

*Web プラグインからファイルのリアルタイム保護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**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。
5. ［**ファイルのリアルタイム保護**］サブセクションで［**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。

ファイルのリアルタイム保護タスクの設定

| 設定 | 説明 |
| --- | --- |
| **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** | 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。 |
| **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。<br>既定では、このオプションはオンです。 |
| **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。 |
| **起動プロセスのより詳細な分析（プロセスの起動は分析が終了するまでブロックされます）** | Kaspersky Embedded Systems Security は、起動プロセスの分析により時間をかけることで脅威を検知する可能性を高めます。プロセスの起動は、分析が終了するまでブロックされます。 |
| **ヒューリスティックアナライザーを使用する** | このチェックボックスでは、オブジェクトのスキャン中の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。<br>このチェックボックスをオンにすると、ヒューリスティックアナライザーが有効になります。 |

| | |
|---|---|
| | このチェックボックスをオフにすると、ヒューリスティックアナライザーが無効になります。<br>既定では、このチェックボックスはオンです。 |
| **ヒューリスティック分析レベル** | このヒューリスティック分析のレベルによって、脅威の検知の徹底度、オペレーティングシステムのリソースにかかる負荷、スキャンの所要時間の間のバランスを調整します。<br>次のレベルを設定できます：<br>• **低**：実行ファイル内のスクリプトは少数しか実行されません。脅威が検知される可能性はやや低くなります。スキャンの速度は速く、システムリソースの消費は軽度です。<br>• **中**：カスペルスキーが推奨する実行ファイルのスクリプトが実行されます。<br>既定では、このレベルが選択されています。<br>• **高**：実行ファイル内のスクリプトが多数実行されます。脅威が検知される可能性は非常に高くなります。スキャンには、より多くのシステムリソースを消費し、より多くの時間がかかります。また、非常に多くの誤検知を引き起こす可能性があります。<br>設定は、［**ヒューリスティックアナライザーを使用する**］をオンにすると使用可能になります。 |
| **信頼ゾーンを適用する** | このチェックボックスにより、タスクに対する信頼ゾーン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、信頼するプロセスのファイル操作が、タスクの設定で指定されたスキャンの除外対象に追加されます。<br>チェックボックスをオフにすると、タスクの保護範囲を判定する時に、信頼するプロセスのファイル操作が無視されます。<br>既定では、このチェックボックスはオンです。 |
| **保護に KSN を使用する** | このチェックボックスで KSN サービス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 Security Network データを使用して、新しい脅威に対する応答時間を迅速化し、誤検知の可能性を減少させます。<br>このチェックボックスをオフにすると、タスクは KSN サービスを使用しません。<br>既定では、このチェックボックスはオンです。 |
| **悪意のある活動を示すコンピューター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** | このチェックボックスでは、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すコンピューターの追加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すると、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すコンピューターが追加されます。<br>このチェックボックスをオフすると、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すコンピューターは追加されません。<br>既定では、このチェックボックスはオフです。<br>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。 |

| | |
|---|---|
| | 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。 |
| **アクティブな脅威の検知時に簡易スキャンを起動する** | チェックボックスをオンにすると、アクティブな感染が検知された際に、一時的な簡易スキャンタスクが作成され、起動します。簡易スキャンの一時タスクが完了すると、この一時タスクは削除されます。<br>チェックボックスをオフにすると、アクティブな感染が検知されても、簡易スキャンタスクが作成されず、起動しません。<br>既定では、このチェックボックスはオンです。 |
| **保護範囲** | 保護範囲のセキュリティ設定を指定できます。 |

## タスクの保護範囲の設定

*ファイルのリアルタイム保護タスクの保護範囲を設定するには：*

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。
5. ［**ファイルのリアルタイム保護**］サブセクションで［**設定**］をクリックします。
6. ［**保護範囲**］セクションを選択します。
7. 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ます。
   - 既存のルールを選択し、［**編集**］をクリックします。

   ［**範囲の編集**］ウィンドウが開きます。
8. スイッチを［**使用中**］切り替えて、オブジェクトの種別を選択します。
9. ［**オブジェクトの保護**］セクションで、次の設定を行います：
   - **オブジェクトの保護モード**：
     - **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**
     - **指定の拡張子リストによってオブジェクトをスキャン**

- **ディスクのブートセクターと MBR をスキャン**
- **NTFS 代替データストリームをスキャン**

10. ［**オブジェクトの保護**］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**
    - **SFX アーカイブ**
    - **圧縮されたオブジェクト**
    - **メールデータベース**
    - **通常のメール**
    - **OLE 埋め込みオブジェクト**
    - 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
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：
    - **通知のみ**
    - **アクセスをブロック**
    - **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。駆除できない場合は削除**
      - **削除**
      - **推奨**
13. 感染の可能性があるオブジェクトの処理を選択します：
    - **通知のみ**
    - **アクセスをブロック**
    - **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：
      - **隔離**
      - **削除**
      - **推奨**

14. 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. ［**検知したオブジェクトの種別に応じて処理を実行**］をオンまたはオフにします。

    b. ［**設定**］をクリックします。

    c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理（最初の処理が失敗した場合に実行）を選択します。

    d. ［**OK**］をクリックします。

15. ［**除外リスト**］セクションで、次の設定を行います：

- ［**除外するファイル**］をオフまたはオンにします。
- ［**検知しない**］をオフまたはオンにします。

16. ［**パフォーマンス**］セクションで、次の設定を行います：

- **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**

17. ［**OK**］をクリックします。

# KSN の使用

このセクションでは、KSN の使用タスクとその設定方法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）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。

## KSN の使用タスクについて

*Kaspersky Security Network*（「KSN」とも表記）は、カスペルスキーが運用する、ファイル評価、Web リソース、およびプログラムに関するナレッジベースにアクセスできるオンラインサービスのインフラストラクチャです。Kaspersky Security Network により、Kaspersky Embedded Systems Security が新しい脅威に迅速に対応でき、いくつかの保護コンポーネントのパフォーマンスを改善し、誤検知の可能性を低下させます。

KSN の使用タスクを開始するには、Kaspersky Security Network に関する声明に同意する必要があります。

Kaspersky Embedded Systems Security が Kaspersky Security Network から受信するのは、プログラムの評価に関する情報のみです。

KSN に参加することで、カスペルスキーが新しい脅威の種別と発生源に関する情報をリアルタイムで受信して、無効化する方法を開発し、コンポーネントでの誤検知の数を減少させます。

製品が使用する情報の転送、処理、保管、破棄に関する詳細情報は、KSN の使用タスクの［**データの取り扱い**］ウィンドウと、カスペルスキーの Web サイトのプライバシーポリシーで確認できます。

Kaspersky Security Network への参加は任意です。Kaspersky Security Network への参加に関する決定は、Kaspersky Embedded Systems Security のインストール後に行います。Kaspersky Security Network への参加についての決定は、いつでも変更できます。

Kaspersky Security Network は、次の Kaspersky Embedded Systems Security 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
- アプリケーション起動コントロール

### Kaspersky Private Security Network

Kaspersky Private Security Network（以降、「プライベート KSN」と表記）の設定方法の詳細は、Kaspersky Security Center のヘルプを参照してください。

デバイスでプライベート KSN を使用する場合は、KSN の使用タスクの［**データの取り扱い**］ウィンドウで、KSN 声明を確認し、［Kaspersky Security Network の参加条項に同意する］をオンにすることにより、タスクを有効にします。条件を承諾することで、KSN 声明で説明しているあらゆる種別のデータ（セキュリティの要求、統計情報データ）を KSN サービスに送信することに同意します。

プライベート KSN の条件を承諾すると、グローバル KSN の使用を調整するチェックボックスは表示されなくなります。

KSN の使用タスクの実行中にプライベート KSN を無効にすると、*ライセンス違反*エラーが発生し、タスクが停止します。コンピューターを継続して保護するには、［**データの取り扱い**］ウィンドウで KSN 声明に同意し、タスクを再起動する必要があります。

### KSN に関する声明の同意の撤回

Kaspersky Security Network の同意はいつでも撤回して、データ交換を停止することができます。次の処理は KSN に関する声明に対する同意の完全または部分的な撤回と判断されます：

- ［**スキャンしたファイルに関するデータを送信**］をオフにする：分析のためにスキャンしたファイルのチェックサムを KSN サービスに送信することを停止します。
- ［**Kaspersky Security Network に統計情報を送信**］をオフにする：追加の KSN の統計情報のデータ処理を停止します。
- ［**Kaspersky Security Network の参加条項に同意する**］のオフ：すべての KSN 関連のデータ処理を停止し、KSN の使用タスクが停止します。
- KSN の使用コンポーネントのアンインストール：すべての KSN 関連のデータ処理が停止します。
- Kaspersky Embedded Systems Security のアンインストール：すべての KSN 関連のデータ処理が停止します。
- Kaspersky Embedded Systems Security のライセンスをアンインストール、またはライセンスの一時停止：すべての KSN 関連のデータ処理が停止します。

## KSN の使用タスクの既定の設定

KSN の使用タスクの既定の設定を変更できます（次の表を参照）。

KSN の使用タスクの既定の設定

| 設定 | 既定値 | 説明 |
|---|---|---|
| **KSN で信頼されていないオブジェクトに対する処理** | 削除 | KSN によって信頼しないと認識されたオブジェクトに対して Kaspersky Embedded Systems Security が実行する処理を指定できます。 |
| **データ転送** | サイズが 2 MB を超えないファイルのチェックサム（MD5 のハッシュ）が計算されます。 | KSN に提供するために MD5 アルゴリズムを使用してチェックサムが計算されるファイルの最大サイズを指定できます。チェックボックスをオフにすると、Kaspersky Embedded Systems Security はすべてのサイズのファイルに対して MD5 のハッシュを計算します。 |

| | | |
|---|---|---|
| **タスク開始スケジュール** | 最初の実行がスケジュール設定されていません。 | タスクは手動で開始するか、開始スケジュールを設定することもできます。 |
| **Kaspersky Security Center を KSN プロキシとして使用する** | オン | 既定では、データは Kaspersky Security Center を経由して KSN に送信されます。<br>この設定は管理プラグインからのみ変更できます。 |
| **Kaspersky Security Network の参加条項に同意する** | オフ | オンにすると、インストール後の KSN の使用に同意します。この決定は、いつでも変更できます。 |
| **Kaspersky Security Network の統計情報を送信** | オン（KSN に関する声明に同意した場合にのみ適用されます） | KSN 声明に同意すると、このチェックボックスをオフにしない限り、KSN 統計情報が自動的に送信されます。 |
| **スキャンしたファイルに関するデータを送信** | オン（KSN に関する声明に同意した場合にのみ適用されます） | KSN に関する声明に同意すると、タスクが開始されてからスキャンおよび分析したファイルに関するデータが送信されます。チェックボックスはいつでもオフにできます。 |

## 管理プラグインから KSN の使用を管理する

このセクションでは、管理プラグインからの KSN の使用タスクの設定方法とデータの取り扱い方法について説明します。

## KSN の使用タスクの設定

*KSN の使用タスクを設定するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**コンピューターのリアルタイム保護**］セクションで、［**KSN の使用**］サブセクションの［**設定**］をクリックします。

   ［**KSN の使用**］ウィンドウが開きます。

5. ［**全般**］タブで、次のタスク設定を行います：

   - ［**KSN で信頼されていないオブジェクトに対する処理**］セクションで、KSN によって信頼しないと判定されたオブジェクトを検知した場合に Kaspersky Embedded Systems Security が実行する処理を指定します：

     - **削除**
     - **情報を記録**

   - ［**データ転送**］セクションで、チェックサムが計算されるファイルのサイズを制限します：

     - ［**ファイルサイズが次の値を超えたら KSN に送信する前にチェックサムを計算しない（MB）**］をオフまたはオンにします。
     - 必要に応じて、右側のフィールドで、Kaspersky Embedded Systems Security がチェックサムを計算するファイルの最大サイズを変更します。

   - ［**KSN プロキシ**］セクションで、［**Kaspersky Security Center を KSN プロキシとして使用する**］をオフまたはオンにします。

     KSN プロキシを有効にするには、KSN 声明に同意し、Kaspersky Security Center を適切に設定する必要があります。詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

6. 必要に応じて、［**タスク管理**］タブでタスクの実行スケジュールを設定します。たとえば、保護対象デバイスが再起動した時にタスクを自動的に実行する場合は、スケジュールによるタスク開始を有効にし、頻度として［**アプリケーションの起動時**］を指定します。

   KSN の使用タスクがスケジュールによって自動的に開始されます。

7. タスクを開始する前にデータの取り扱い方法を設定してください。

8. ［**OK**］をクリックします。

変更された設定が適用されます。設定を変更した日時、および変更前と変更後のタスクの設定に関する情報が、システム監査ログに保存されます。

## データ処理の設定

*KSN サービスによって処理されるデータを設定して KSN 声明に同意するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
- 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

  Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**コンピューターのリアルタイム保護**］セクションで、［**KSN の使用**］サブセクションの［**データの処理**］をクリックします。
   ［**KSN データの取り扱い**］ウィンドウが開きます。
5. ［**統計とサービス**］タブで、声明の内容を確認し、［**Kaspersky Security Network の参加条項に同意する**］をオンにします。
6. 保護レベルを上げるため、次のチェックボックスが自動的にオンになります：
   - **スキャンしたファイルに関するデータを送信**
   - **Kaspersky Security Network の統計情報を送信**

   いつでもこれらのチェックボックスをオフにして、追加データの送信を停止できます。
7. ［**Kaspersky Security Network に統計情報を送信**］は、既定ではオンです。追加の統計情報をカスペルスキーに送信しないようにする場合は、いつでもこのチェックボックスをオフにできます。
8. ［**OK**］をクリックします。
   データ処理の設定が保存されます。

# アプリケーションコンソールから KSN の使用を管理する

このセクションでは、KSN の使用タスクとデータの取り扱い方法を、アプリケーションコンソールから設定する方法について説明します。

## KSN の使用タスクの設定

*KSN の使用タスクを設定するには：*

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. ［**KSN の使用**］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。
   ［**タスクの設定**］ウィンドウが開き、［**全般**］タブが表示されます。
4. タスクを設定するには：

- ［**KSN で信頼されていないオブジェクトに対する処理**］セクションで、KSN によって信頼しないと判定されたオブジェクトを検知した場合に Kaspersky Embedded Systems Security が実行する処理を指定します：
  - **削除**
  - **情報を記録**
- ［**データ転送**］セクションで、チェックサムが計算されるファイルのサイズを制限します：
  - ［**ファイルサイズが次の値を超えたら KSN に送信する前にチェックサムを計算しない（MB）**］をオフまたはオンにします。
  - 必要に応じて、右側のフィールドで、Kaspersky Embedded Systems Security がチェックサムを計算するファイルの最大サイズを変更します。

5. 必要に応じて、［**スケジュール**］タブと［**詳細設定**］タブでタスク開始スケジュールを設定します。たとえば、保護対象デバイスが再起動した時にタスクを自動的に実行する場合は、スケジュールによるタスク開始を有効にして、［**アプリケーションの起動時**］の開始の頻度を指定します。

   KSN の使用タスクがスケジュールによって自動的に開始されます。

6. タスクを開始する前にデータの取り扱い方法を設定してください。

7. ［**OK**］をクリックします。

変更された設定が適用されます。設定を変更した日時、および変更前と変更後のタスクの設定に関する情報が、システム監査ログに保存されます。

## データの取り扱い方法の設定

*KSN サービスによって処理されるデータを設定して KSN 声明に同意するには：*

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. ［**KSN の使用**］サブフォルダーを選択します。
3. 結果ペインで［**データの処理**］をクリックします。

   ［**データの取り扱い**］ウィンドウが開きます。
4. ［**統計とサービス**］タブで、声明の内容を確認し、［**Kaspersky Security Network の参加条項に同意する**］をオンにします。
5. 保護レベルを上げるため、次のチェックボックスが自動的にオンになります：
   - **スキャンしたファイルに関するデータを送信**
   - **Kaspersky Security Network の統計情報を送信**

   いつでもこれらのチェックボックスをオフにして、追加データの送信を停止できます。
6. ［**Kaspersky Security Network に統計情報を送信**］は、既定ではオンです。追加の統計情報をカスペルスキーに送信しないようにする場合は、いつでもこのチェックボックスをオフにできます。

7. ［**OK**］をクリックします。

データ処理の設定が保存されます。

## Web プラグインから KSN の使用を管理する

*Web プラグインから KSN の使用タスクとデータの取り扱い方法を設定するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。
5. ［**KSN の使用**］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。

管理プラグインからの KSN の使用タスクとデータの取り扱い方法の設定

| 設定 | 説明 |
| --- | --- |
| **削除** | Kaspersky Embedded Systems Security は、KSN の信頼しないステータスが設定されているオブジェクトを削除し、バックアップにコピーを配置します。<br>既定では、このオプションはオンです。 |
| **情報を記録** | Kaspersky Embedded Systems Security は、実行ログで KSN の信頼しないステータスが設定されているオブジェクトに関する情報を記録します。信頼しないオブジェクトは削除しません。 |
| **ファイルサイズが次の値を超えたら KSN に送信する前にチェックサムを計算しない** | このチェックボックスにより、KSN サービスにこの情報を送信するための、指定されたサイズのファイルのチェックサムの計算を有効または無効にします。<br>チェックサムの計算にかかる時間は、ファイルサイズによって異なります。<br>このチェックボックスをオンにすると、指定された値（MB）を超えるサイズのファイルに対してチェックサムを計算しません。<br>チェックボックスをオフにすると、すべてのサイズのファイルに対してチェックサムを計算します。<br>既定では、このチェックボックスはオンです。 |
| **Kaspersky Security Network の参加条項をすべて確認し、理解した上で同意する** | このチェックボックスをオンにすることにより、Kaspersky Security Network に関する声明の条項を読んで同意することを確認します。 |
| **スキャンしたファイルに関** | このチェックボックスをオンにすると、スキャンしたファイルのチェックサムがカスペルスキーに送信されます。各ファイルのセキュリティに関する判定は、KSN から取得した評価に基づいています。 |

| | |
|---|---|
| **するデータを送信** | チェックボックスをオフにすると、ファイルのチェックサムは KSN に送信されません。<br>ファイル評価の要求が制限モードで送信されることがあるので、注意してください。制限は、DDoS 攻撃からカスペルスキーの評価サーバーを保護するために使用されます。このシナリオでは、送信中のファイル評価要求のパラメータは、カスペルスキーが確立したルールや方法によって定義され、保護対象デバイスでユーザーが設定することはできません。これらのルールと方法のアップデートは、定義データベースのアップデートとともに受信されます。制限が適用されると、［*KSN サーバーを DDoS 攻撃から保護するためにカスペルスキーにより有効にされました*］ステータスが KSN の使用タスクの統計情報に表示されます。<br>既定では、このチェックボックスはオンです。 |
| **Kaspersky Security Network の統計情報の一部としてデータが処理されることに同意する** | このチェックボックスをオンにすると、個人情報を含む可能性のある追加の統計情報が送信されます。KSN の統計情報として送信されるすべてのデータのリストは、KSN に関する声明で示されています。カスペルスキーが受信したデータは、製品の品質改善と脅威の検知レベルの向上のために使用されます。<br>チェックボックスをオフにすると、追加の統計情報は送信されません。<br>既定では、このチェックボックスはオンです。 |
| タスク管理 | スケジュールでタスクを開始する設定を指定できます。 |

## 追加のデータ転送の設定

Kaspersky Embedded Systems Security では、以下のデータをカスペルスキーに送信するよう設定できます：

- スキャンされたファイルのチェックサム（［**スキャンしたファイルに関するデータを送信**］）。
- 個人情報を含む追加の統計情報（［**Kaspersky Security Network に統計情報を送信**］）。

カスペルスキーに送信されるデータの詳細情報については、このガイドの「ローカルでのデータ取り扱い方法」を参照してください。

［**Kaspersky Security Network の参加条項に同意する**］をオンにした場合にのみ、該当するチェックボックスをオンまたはオフにできます。

既定では、Kaspersky Embedded Systems Security は KSN に関する声明に同意した後で、ファイルのチェックサムとスキャンした URL に関するデータ、追加の統計情報を送信します。

［**Kaspersky Security Network の参加条項に同意する**］は、Kaspersky Security Center のポリシーでデータの取り扱い方法の設定の変更がブロックされている場合にのみ編集できません。

使用可能なチェックボックスの状態と該当する条件

| チェックボックスの状態 | ［スキャンしたファイルに関するデータを送信］の状態 | ［Kaspersky Security Network の統計情報を送信］の状態 | ［Kaspersky Security Network の参加条項に同意する］の状態 |
|---|---|---|---|
| ☑ | • 評価の要求が送信され | • 追加の統計情報が送信さ | • Kaspersky Security Network |

| | | | |
|---|---|---|---|
| | る<br>• チェックボックスが編集できる | れる<br>• チェックボックスが編集できる | に関する声明の内容に同意する<br>• チェックボックスが編集できる |
| ☑ | • 評価の要求が送信される<br>• チェックボックスが編集できない | • 追加の統計情報が送信される<br>• チェックボックスが編集できない | • Kaspersky Security Network に関する声明の内容に同意する<br>• チェックボックスが編集できない |
| ☐ | • 評価の要求が送信されない<br>• チェックボックスが編集できる | • 追加の統計情報が送信されない<br>• チェックボックスが編集できる | • Kaspersky Security Network に関する声明の内容に同意しない<br>• チェックボックスが編集できる |
| ☐ | • 評価の要求が送信されない<br>• チェックボックスが編集できない | • 追加の統計情報が送信されない<br>• チェックボックスが編集できない | • Kaspersky Security Network に関する声明の内容に同意しない<br>• チェックボックスが編集できない |

## KSN の使用タスクの統計情報

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ついての詳細情報を、リアルタイムで表示することができます。タスクの実行中に発生したすべてのイベントに関する情報は、タスク実行ログに記録されます。

*KSN の使用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、［**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. ［**KSN の使用**］サブフォルダーを選択します。

選択したフォルダーの詳細ペインにある［**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。

タスクの開始以降、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）。

KSN の使用タスクの統計情報

| フィールド | 説明 |
|---|---|
| **要求送信エラー** | 処理の結果がタスクエラーになった KSN 要求の数。 |

| | |
|---|---|
| **生成された統計** | 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** | KSN の使用タスクを実行している時に削除されたオブジェクトの数。 |
| **バックアップ済み** | バックアップに保存されたオブジェクトコピーの数。 |
| **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。そのようなオブジェクトの情報は、タスク実行ログに記録されます。 |
| **バックアップされていないオブジェクト** | バックアップにコピーを保存しようとしたが、ディスク容量不足などにより保存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。そのようなオブジェクトの情報は、タスク実行ログに記録されます。 |
| **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。 |

# ネットワーク脅威対策

このセクションでは、ネットワーク脅威対策タスクとその設定方法について説明します。

## ネットワーク脅威対策タスクについて

ネットワーク脅威対策は、Microsoft Windows 7 以降または Windows Server 2008 R2 以降のバージョンを実行しているデバイスにのみインストールできます。

ネットワーク脅威対策タスクは、受信ネットワークトラフィックにおいて、ネットワーク攻撃に特有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。画面にネットワーク攻撃が試行されたことを示す警告が表示され、攻撃しているコンピューターに関する情報が表示されます。

既定では、ネットワーク脅威対策タスクは、［**攻撃の検知時に接続をブロックする**］モードで実行されます。このモードでは、ブロック対象コンピューターのリストに、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 アドレスが追加されます。

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。

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。
- ネットワーク脅威対策タスクが停止され、［**タスクが実行されていない時にトラフィック分析を停止しない**］がオフになっています。
- ［**攻撃の検知時に接続をブロックする**］モードがオフになりました。

## ネットワーク脅威対策タスクの既定の設定

ネットワーク脅威対策タスクでは、次の表の既定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。

ネットワーク脅威対策タスクの既定の設定

| 設定 | 既定値 | 説明 |
| --- | --- | --- |
| **処理モード** | **攻撃の検知時に接続をブロックする** | ネットワーク脅威対策タスクは、［**処理しない**］、［**ネットワーク攻撃の通知のみ行う**］または［**攻撃の検知時に接続をブロックする**］のモードで開始されます。 |

| | | |
|---|---|---|
| | | このチェックボックスでは、ブロック対象コンピューターのリストに、ネットワーク攻撃の典型的な活動を示すコンピューターの追加を有効または無効にします。<br>このモードでは、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、検知された動作に関するイベントが記録されて、ブロック対象コンピューターのリストにネットワーク攻撃の典型的な活動を示すコンピューターの IP アドレスが追加されます。<br>既定では、このモードが選択されます。<br>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。<br>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。<br>このモードをオンにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされ、検知された動作に関するイベントが記録されますが、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。<br>このモードをオフにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされますが、検知された動作に関するイベントが記録されず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。<br>たとえば、保護対象デバイスのパフォーマンスが低下した場合に、このモードを使用できます。 |
| **除外リスト** | 除外リストは適用されません。 | タスクの保護範囲から除外する領域を指定します。 |
| **スケジュール設定** | 既定では、ネットワーク脅威対策タスクは Kaspersky Embedded Systems Security の起動時に自動的に開始されます。 | スケジュールは設定できます。 |

## ネットワーク脅威対策タスクのアプリケーションコンソールからの設定

このセクションでは、アプリケーションコンソールのインターフェイスからネットワーク脅威対策タスクを管理する方法について説明します。

# タスクの全般的な設定

*タスクの全般的な設定を行うには：*

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. ［**ネットワーク脅威対策**］サブフォルダーを選択します。
3. ［**ネットワーク脅威対策**］フォルダーの詳細ペインで、［**プロパティ**］をクリックします。
   ［**タスクの設定**］ウィンドウが表示されます。
4. ［**全般**］タブを開きます。
5. ［**処理モード**］セクションで、処理モードを選択します：
   - **処理しない**

     このモードをオフにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされますが、検知された動作に関するイベントが記録されず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

     たとえば、保護対象デバイスのパフォーマンスが低下した場合に、このモードを使用できます。

   - **ネットワーク攻撃の通知のみ行う**

     このモードをオンにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされ、検知された動作に関するイベントが記録されますが、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

   - **攻撃の検知時に接続をブロックする**

     このチェックボックスでは、ブロック対象コンピューターのリストに、ネットワーク攻撃の典型的な活動を示すコンピューターの追加を有効または無効にします。

     このモードでは、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、検知された動作に関するイベントが記録されて、ブロック対象コンピューターのリストにネットワーク攻撃の典型的な活動を示すコンピューターの IP アドレスが追加されます。

     既定では、このモードが選択されます。

     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。

     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。

6. ［**タスクが実行されていない時にトラフィック分析を停止しない**］をオンまたはオフにします。

このチェックボックスをオンにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、攻撃しているコンピューターからのネットワーク活動が選択された処理モードに応じてブロックされます。

このチェックボックスをオフにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作はスキャンされず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

既定では、このチェックボックスはオフです。

7. ［**OK**］をクリックします。

## 除外の追加

*ネットワーク脅威対策タスクの除外を追加するには、次の手順を実行します：*

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. ［**ネットワーク脅威対策**］サブフォルダーを選択します。
3. ［**ネットワーク脅威対策**］フォルダーの詳細ペインで、［**プロパティ**］をクリックします。
   ［**タスクの設定**］ウィンドウが表示されます。
4. ［**除外リスト**］タブで、［**除外された IP アドレスを管理しない**］をオンにします。

   このチェックボックスをオンにすると、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ません。

   このチェックボックスをオフにすると、除外リストは適用されません。

5. IP アドレスを指定し、［**追加**］をクリックします。
6. ［**OK**］をクリックします。

## ネットワーク脅威対策タスクの管理プラグインからの設定

このセクションでは、管理プラグインインターフェイスからネットワーク脅威対策タスクを管理する方法について説明します。

## タスクの全般的な設定

*タスク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**ポリシーのプロパティ**ウィンドウを開きます。
- 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

> Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**コンピューターのリアルタイム保護**］セクションで、［**ネットワーク脅威対策**］サブセクションの［**設定**］をクリックします。

［**ネットワーク脅威対策**］ウィンドウが開きます。

5. ［**全般**］タブを開きます。

6. ［**処理モード**］セクションで、処理モードを選択します：

- **処理しない**

> このモードをオフにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされますが、検知された動作に関するイベントが記録されず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。
>
> たとえば、保護対象デバイスのパフォーマンスが低下した場合に、このモードを使用できます。

- **ネットワーク攻撃の通知のみ行う**

> このモードをオンにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされ、検知された動作に関するイベントが記録されますが、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

- **攻撃の検知時に接続をブロックする**

> このチェックボックスでは、ブロック対象コンピューターのリストに、ネットワーク攻撃の典型的な活動を示すコンピューターの追加を有効または無効にします。
>
> このモードでは、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、検知された動作に関するイベントが記録されて、ブロック対象コンピューターのリストにネットワーク攻撃の典型的な活動を示すコンピューターの IP アドレスが追加されます。
>
> 既定では、このモードが選択されます。
>
> 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。
>
> 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。

7. ［**タスクが実行されていない時にトラフィック分析を停止しない**］をオンまたはオフにします。

このチェックボックスをオンにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、攻撃しているコンピューターからのネットワーク活動が選択された処理モードに応じてブロックされます。

このチェックボックスをオフにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作はスキャンされず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

既定では、このチェックボックスはオフです。

8. ［**OK**］をクリックします。

## 除外の追加

*ネットワーク脅威対策タスクの除外を追加するには、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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**コンピューターのリアルタイム保護**］セクションで、［**ネットワーク脅威対策**］サブセクションの［**設定**］をクリックします。

   ［**ネットワーク脅威対策**］ウィンドウが開きます。
5. ［**除外リスト**］タブで、［**除外された IP アドレスを管理しない**］をオンにします。

   このチェックボックスをオンにすると、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ません。

   このチェックボックスをオフにすると、除外リストは適用されません。
6. IP アドレスを指定し、［**追加**］をクリックします。
7. ［**OK**］をクリックします。

## ネットワーク脅威対策タスクの Web プラグインからの設定

このセクションでは、Web プラグインのインターフェイスからネットワーク脅威対策タスクを管理する方法について説明します。

## タスクの全般的な設定

*タスク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、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。
5. ［**ネットワーク脅威対策**］サブセクションで［**設定**］をクリックします。
6. ［**全般**］タブを開きます。
7. ［**処理モード**］セクションで、処理モードを選択します：

   - **処理しない**

     このモードをオフにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされますが、検知された動作に関するイベントが記録されず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

     たとえば、保護対象デバイスのパフォーマンスが低下した場合に、このモードを使用できます。

   - **ネットワーク攻撃の通知のみ行う**

     このモードをオンにすると、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作がスキャンされ、検知された動作に関するイベントが記録されますが、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

   - **攻撃の検知時に接続をブロックする**

     このチェックボックスでは、ブロック対象コンピューターのリストに、ネットワーク攻撃の典型的な活動を示すコンピューターの追加を有効または無効にします。

     このモードでは、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、検知された動作に関するイベントが記録されて、ブロック対象コンピューターのリストにネットワーク攻撃の典型的な活動を示すコンピューターの IP アドレスが追加されます。

     既定では、このモードが選択されます。

     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。

     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。

8. ［**タスクが実行されていない時にトラフィック分析を停止しない**］をオンまたはオフにします。

このチェックボックスをオンにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な活動がスキャンされ、攻撃しているコンピューターからのネットワーク活動が選択された処理モードに応じてブロックされます。

このチェックボックスをオフにすると、ネットワーク脅威対策タスクが停止した時に、受信ネットワークトラフィックでネットワーク攻撃の典型的な動作はスキャンされず、攻撃しているコンピューターからのネットワークアクティビティはブロックされません。

既定では、このチェックボックスはオフです。

9. ［**OK**］をクリックします。

## 除外の追加

*ネットワーク脅威対策タスクの除外を追加するには、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、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。
5. ［**ネットワーク脅威対策**］サブセクションで［**設定**］をクリックします。
6. ［**除外リスト**］タブで、［**除外された IP アドレスを管理しない**］をオンにします。

このチェックボックスをオンにすると、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ません。

このチェックボックスをオフにすると、除外リストは適用されません。

7. IP アドレスを指定し、［**追加**］をクリックします。
8. ［**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

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タスクとその設定方法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タスクについて

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。

次のいずれかの方法により、アプリケーションの起動を許可できます：

- 信頼するアプリケーションの許可ルールを設定する。
- 起動時に KSN において信頼するアプリケーションの評価について確認する。

アプリケーションの起動の拒否には最大の優先度が指定されます。たとえば、いずれかのブロックルールによってアプリケーションの起動が阻止された場合、KSN による信頼の判定には関係なく、アプリケーションの起動が拒否されます。その時に、アプリケーションが許可ルールの範囲に含まれているにもかかわらず、KSN サービスによって信頼されていない場合、このアプリケーションの起動は拒否されます。

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：

- **処理を実行**：アプリケーション起動コントロールルールの範囲に該当するアプリケーションについて、起動をコントロールするルールを使用します。アプリケーション起動コントロールルールの範囲は、このタスクの設定で指定されます。アプリケーションはアプリケーション起動コントロールルールの適用範囲に該当し、そのタスク設定が指定されたルールに適合していない場合、そのアプリケーションの起動は拒否されます。

  アプリケーション起動コントロールタスクの設定で指定されたルールの範囲に該当しないアプリケーションは、アプリケーション起動コントロールタスクの設定に関係なく、起動が拒否されます。

  **アプリケーション起動コントロール**タスクは、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 を超えるルールがある場合に、［処理を実行］モードで起動できません。

- **統計のみ**：Kaspersky Embedded Systems Security は、アプリケーションの起動を許可まはた拒否するために、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。代わりに、アプリケーションの起動に関する情報、アプリケーションの開始を実行するルール、**処理を実行**モードでタスクを開始した場合に実行される処理に関する情報を記録します。すべてのアプリケーションの起動が許可されます。既定ではこのモードが設定されています。

  このモードを使用して、実行ログに記録される情報に基づき、アプリケーション起動コントロールルールを作成できます。

次のいずれかのシナリオに従って、アプリケーション起動コントロールタスクを設定できます：

- 詳細なルール設定およびアプリケーション起動コントロールにおけるそのルールの使用
- アプリケーション起動コントロールにおける基本的なルール設定および KSN の使用

オペレーティングシステムの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範囲に該当する場合、アプリケーション起動コントロールルールを作成する時、そのアプリケーションが新たに作成したルールによって許可されていることを確認してください。許可されていない場合、オペレーティングシステムが起動しないことがあります。

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作成タスクは、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しくみ

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。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作成するには、ルールの自動生成を使用して許可ルールを作成するか、アプリケーション起動コントロールタスクで**統計のみ**モードを使用します。また、許可ルールを手動で追加することもできます。

- ユーザーまたはユーザーグループ

  アプリケーション起動コントロールルールは、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。

- 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。

- ルール有効化の条件

  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基準のいずれかを満たすファイルの起動を制御します。指定された*デジタル証明書*によってファイルが署名されていること、指定された*SHA256 ハッシュ*とファイルが一致していること、指定された*パス*にファイルがあることが、ルール設定で指定される基準です。

  ルール有効化の条件に**デジタル証明書**を設定すると、オペレーティングシステムで信頼されているすべてのアプリケーションの起動が、作成したルールによって制御されます。次のチェックボックスを使用して、より厳しい有効化の条件を設定することもできます：

  - **発行先を使用**
  - **サムプリントを使用**

ムプリントはデジタル証明書を一意に識別し、デジタル証明書の発行先と違って偽造できないため、デジタル証明書に基づくアプリケーション起動ルールの適用では、最も基準が正確になっています。

アプリケーション起動コントロールルールに対して除外対象を指定することもできます。アプリケーション起動コントロールルールの除外対象は、ルール有効化の条件と同様、デジタル証明書、SHA256 ハッシュ、ファイルのパスに基づきます。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。

オペレーティングシステムの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範囲に該当する場合、アプリケーション起動コントロールルールを作成する時、そのアプリケーションが新たに作成したルールによって許可されていることを確認してください。許可されていない場合、オペレーティングシステムが起動しないことがあります。

### 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：

- ルールを手動で追加する
- ルールを自動作成して追加する
- ルールを削除する
- ルールをファイルにエクスポートする
- 選択したファイルの実行を許可するルールに適合しているかどうか、これらのファイルをチェックする
- 指定した基準に従って、リストのルール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

保護対象デバイスでのソフトウェア配布も制御する必要がある場合、アプリケーション起動コントロールルールの生成は複雑になる可能性があります。たとえば、保護対象デバイス上に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などの特性を考慮する必要があります。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のサブシステムを使用できます。

*ソフトウェアの配布パッケージ*は、保護対象デバイスにインストールされるソフトウェアアプリケーションを表します。各パッケージには1つ以上のアプリケーションが含まれており、特にソフトウェアアプリケーションまたはアップデートをインストールしている場合は、アプリケーションに加えて個々のファイル、アップデート、さらに個々のコマンドが含まれることもあります。

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。ソフトウェアの配布パッケージをこのリストに追加すると、これらの信頼するパッケージの展開、および信頼するパッケージによってインストールまたは変更されるソフトウェア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、ソフトウェア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。

アプリケーション起動コントロールタスクの設定で、［**実行ファイルにルールを適用する**］がオフになっている場合は、ソフトウェア配布コントロールは使用できません。

## 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。その後、既定では、配布キャッシュの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、クリア、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。

コマンドラインのオプションを使用して配布キャッシュを設定ファイルに（XML 形式で）エクスポートしたり、キャッシュをクリアできます。

*配布キャッシュを設定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:<フルパス> /sdc
```

*配布キャッシュをクリアするには、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

信頼するパッケージから抽出したすべてのファイルでは、パッケージの最初の起動時に信頼属性が継承されます。最初の起動後にチェックボックスをオフにした場合、このパッケージから抽出されたすべてのファイルでは継承された属性が維持されます。抽出されたすべてのファイルで継承された属性をリセットするには、配布キャッシュをクリアして、［**この配布パッケージから作成されたプログラムの今後の配布を許可する**］をオフにしてから信頼する配布パッケージをもう一度起動する必要があります。

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。既定では、信頼属性を継承するレベルの数に制限はありません。

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。

［**この配布パッケージから作成されたプログラムの今後の配布を許可する**］のオンまたはオフによって、ファイルの処理がソフトウェア配布コントロール設定で指定されます。

たとえば、他のパッケージやアプリケーションをいくつか含むテスト用の .msi パッケージを除外リストに追加してチェックボックスをオンにします。この場合、テスト用の .msi パッケージに含まれるすべてのパッケージとアプリケーションは、他のファイルを含む場合に、実行または抽出が許可されます。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。

テスト用の .msi パッケージを除外リストに追加して［**この配布パッケージから作成されたプログラムの今後の配布を許可する**］をオフにすると、（最初のレベルでネストされる）展開元の信頼するパッケージから直接抽出したパッケージ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。

### 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サブシステム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。

### KSN の判定の利用

ファイルを信頼しないという KSN の判定は、ソフトウェア配布コントロールの除外リストよりも優先されます。これらのファイルを信頼しないとの判定を KSN から受け取っている場合、信頼するパッケージの展開、またはこのパッケージによって作成または変更されたファイルの起動はブロックされます。

この場合、信頼するパッケージから展開された後で、すべての子ファイルはアプリケーション起動コントロールの範囲内で KSN の使用に関係なく実行が許可されます。さらに、［**KSN で信頼されていないアプリケーションを拒否する**］および［**KSN で信頼されているアプリケーションを許可する**］の状態は、［**この配布パッケージから作成されたプログラムの今後の配布を許可する**］の操作に影響します。

## アプリケーション起動コントロールタスクでの KSN の使用について

KSN の使用タスクを開始するには、KSN 声明に同意する必要があります。

アプリケーションの評価に関する KSN のデータがアプリケーション起動コントロールタスクによって使用される場合、KSN でのアプリケーションの評価は該当するアプリケーションの起動を許可または拒否する際の基準と判断されます。アプリケーション起動の試行時に Kaspersky Embedded Systems Security が KSN から信頼しないとの判定を受け取った場合、このアプリケーションの起動は拒否されます。アプリケーション起動の試行時に Kaspersky Embedded Systems Security が KSN から信頼するとの判定を受け取った場合、このアプリケーションの起動は許可されます。KSN は、アプリケーション起動コントロールルールとともに使用するか、あるいはアプリケーションの起動を拒否するための独立した 1 つの基準として使用できます。

### アプリケーションの起動を拒否するための独立した基準として KSN の判定を使用する

このシナリオでは、ルールリストの詳細な設定を使用しなくても、保護対象デバイスでアプリケーションの起動を安全に管理できます。

Kaspersky Embedded Systems Security に対して、KSN の判定と指定したルールのみを適用できます。KSN で信頼されているアプリケーション、あるいは特定のルールで許可されているアプリケーションの起動のみが許可されます。

このようなシナリオでは、デジタル証明書に基づいてアプリケーションの起動を許可するルールを設定してください。

その他のアプリケーションはすべて、「既定で拒否」の原則に従って起動が拒否されます。ルールが適用されていない時に KSN を使用すると、KSN が脅威であると判定したアプリケーションからデバイスが保護されます。

### アプリケーション起動コントロールルールと同時に KSN の判定を使用する

KSN の判定をアプリケーション起動コントロールルールと同時に使用すると、次の条件が適用されます：

- アプリケーションが 1 つ以上の拒否ルールの範囲に含まれている場合、Kaspersky Embedded Systems Security では常にこのアプリケーションの起動が拒否されます。アプリケーションが KSN によって信頼されると判断されている場合、この判定の優先度は低く、考慮されません。アプリケーションの起動は拒否されます。これにより、ブロックされたアプリケーションとして起動を拒否するアプリケーションの対象範囲を拡大できます。

- KSN で信頼されていないアプリケーションの起動が禁止されており、アプリケーションが KSN で信頼されていない場合、Kaspersky Embedded Systems Security では常にこのアプリケーションの起動が拒否されます。アプリケーションで許可ルールが設定されている場合も、その優先度は低く、考慮されないため、アプリケーションの起動は拒否されます。これにより、ルールの初期設定時には考慮されていなかったが現在では KSN が脅威であると判定したアプリケーションからデバイスが保護されます。

## アプリケーション起動コントロールルールの作成について

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作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。

アプリケーション起動コントロールコンポーネントは、事前設定された 2 つの許可ルールとともにインストールされます：

- オペレーティングシステムの信頼する証明書を使用したスクリプトと Windows Installer パッケージの許可ルール。

- オペレーティングシステムの信頼する証明書を使用した実行ファイルの許可ルール。

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作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作成タスクによって生成される XML ファイルには、タスクを開始する前のタスクの設定で指定した許可ルールが含まれます。指定されたタスクの設定で起動が許可されていないアプリケーションに対してルールは作成されません。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タスクに手動でインポートできます。

  作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作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で、または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アプリケーション起動コントロールルールの自動作成タスクを開始してください。

- **統計のみ**モードで実行されるアプリケーション起動コントロールタスクにより、Kaspersky Security Center で生成されるタスクイベントの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、［**統計のみ**］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 の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作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［**統計のみ**］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作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［**統計のみ**］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の作成する前に、テンプレートマシンが安全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タスクの既定の設定

アプリケーション起動コントロールタスクでは、次の表の既定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。

アプリケーション起動コントロールタスクの既定の設定

| 設定 | 既定値 | 説明 |
|---|---|---|
| **タスクモード** | **統計のみ**：設定されたルールに基づき、拒否された起動イベントおよび許可された起動イベントを記録します。アプリケーション起動は実際には拒否されません。 | 最終的なルールのリストの生成後、［**処理を実行**］モードを選択できます。 |
| **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** | オフ | 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ことができます。 |
| **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** | 適用されません。 | 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できます。 |
| **ルールの管理** | **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と保護対象デバイス上のルールを合わせて適用するモードを選択できます。 |
| **ルールの使用範囲** | タスクでは、実行ファイル、スクリプト、および MSI パッケージの起動を制御します。さらに、DLL モジュールの読み込みも監視します。 | ルールによって起動が制御されるファイルの種別を指定できます。 |
| **KSN の使用** | KSN アプリケーション評価データは使用されません。 | アプリケーション起動コントロールタスクの実行時、KSN アプリケーション評価データを使用できます。 |
| **リストされたアプリケーションとパッケ** | 適用されません。 | 設定で指定したインストーラーおよびアプリケーションを使用するソフトウェア配布 |

| | | |
|---|---|---|
| **ージのソフトウェア配布を自動的に許可する** | | を許可できます。既定では、ソフトウェア配布は Windows インストーラーサービスを使用する場合のみ許可されます。 |
| **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** | 適用されます（［**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**］の設定が有効になっている場合のみ変更できます）。 | Windows インストーラーによって実行されるすべてのソフトウェアインストールまたはアップデートを許可することができます。 |
| **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** | 適用されません（［**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**］の設定が有効になっている場合のみ変更できます）。 | システムセンター設定マネージャーを使用した自動ソフトウェア配布をオンまたはオフにできます。 |
| **タスク開始** | 最初の実行がスケジュール設定されていません。 | アプリケーション起動コントロールタスクは、Kaspersky Embedded Systems Security の起動時に自動的には開始されません。タスクは手動で開始するか、開始スケジュールを設定することもできます。 |

アプリケーション起動コントロールルールの自動作成タスクの既定の設定

| 設定 | 既定値 | 説明 |
|---|---|---|
| 許可ルール名の接頭辞 | Kaspersky Embedded Systems Security がインストールされている保護対象デバイスの名前と同一にします。 | 許可ルールの名前の接頭辞を変更できます。 |
| 許可ルールの適用範囲 | 許可ルールの適用範囲には、次の既定のファイルのカテゴリが含まれます：<br>• C:\Windows、C:\Program Files (x86)、および C:\Program Files の各フォルダーにある EXE 拡張子を持つファイル<br>• C:\Windows フォルダーにある MSI パッケージ<br>• C:\Windows フォルダーに保存されているスクリプト<br>このタスクは、場所や形式に関係なく、実行中のすべてのアプリケーションのルールも作成します。 | 自動生成されるルールによって起動が許可されるフォルダーのパスを追加や削除したり、ファイルの種別を指定したりすることで、保護範囲を変更できます。また、許可ルールを作成する時に、実行中のアプリケーションを無視することもできます。 |
| 許可ルールの生成の基準 | デジタル証明書の発行先とサムプリントが使用されます。ルールはすべてのユーザーとユーザーグループに対して生成されます。 | 許可ルールを生成する時に、SHA256 ハッシュを使用できます。<br>許可ルールを自動的に生成する必要があるユーザーおよびユーザーグループを選択できます。 |
| タスク完了後 | 許可ルールが、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されます。新しいルールが既存の | ルールの結合や重複するルールの削除をしないで既存のルールに追加したり、既存のルールを新しい許可ルールに置き換えたりすることもできます。さらに、許可ルールをファイルへエクスポートする設定も可能です。 |

| | | |
|---|---|---|
| の処理 | ルールに結合され、重複するルールは削除されます。 | |
| 権限を指定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。 | システムアカウントや指定したユーザーの権限を使用して、アプリケーション起動コントロールルールの自動作成タスクの起動を許可できます。 |
| タスク開始スケジュール | 最初の実行がスケジュール設定されていません。 | アプリケーション起動コントロールルールの自動作成タスクは、Kaspersky Embedded Systems Security 起動時に自動的には開始されません。タスクは手動で開始するか、開始スケジュールを設定することもできます。 |

## 管理プラグインからアプリケーション起動コントロールを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの1つまたはすべての保護対象デバイスのタスクを設定する方法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。

## アプリケーション起動コントロールタスクのポリシーの設定ウィンドウ

*Kaspersky Security Center のポリシーからアプリケーション起動コントロールタスクの設定を開くには：*

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. 表示されたポリシーのプロパティウィンドウで、［**ローカル活動の管理**］セクションを選択します。
6. ［**アプリケーション起動コントロール**］サブセクションの［**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**］ウィンドウが開きます。

必要に応じてポリシーを設定します。

## アプリケーション起動コントロールルールのリスト

*Kaspersky Security Center からアプリケーション起動コントロールのリストを開くには：*

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. 表示されたポリシーのプロパティウィンドウで、［**ローカル活動の管理**］セクションを選択します。
6. ［**アプリケーション起動コントロール**］サブセクションの［**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**］ウィンドウが開きます。
7. ［**全般**］タブで、［**ルールリスト**］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**］ウィンドウが開きます。

必要に応じてルールリストを設定します。

## アプリケーション起動コントロールルールの自動作成タスクのウィザードとプロパティウィンドウ

*アプリケーション起動コントロールルールの自動作成タスクの作成を開始するには：*

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. タスクを設定する管理グループを選択します。
3. ［**タスク**］タブを選択します。
4. ［**タスクの作成**］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. ［**アプリケーション起動コントロールルールの自動生成**］タスクを選択します。
6. ［**次へ**］をクリックします。
   ［**設定**］ウィンドウが開きます。

*アプリケーション起動コントロールルールの自動作成の既存タスクを編集するには：*

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. タスクを設定する管理グループを選択します。
3. ［**タスク**］タブを選択します。
4. 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。
   **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**プロパティ**ウィンドウが開きます。

タスクの設定に関する詳細は、セクション「アプリケーション起動コントロールルールの自動作成タスクの設定」を参照してください。

## アプリケーション起動コントロールタスクの設定

*アプリケーション起動コントロールタスクの全般的な設定を行うには：*

1. ［**アプリケーション起動コントロール**］ウィンドウを開きます。
2. ［**全般**］タブの［**タスクモード**］セクションで、次の設定を選択します：
   - ［**タスクモード**］ドロップダウンリストで、タスクモードを指定します。
   - ［**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**］をオフまたはオンにします。
   - ［**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**］をオフまたはオンにします。
3. ［**ルールの管理**］セクションで、ルールの適用を設定します：
   a. アプリケーション起動コントロールタスクの許可ルールを追加するには、［**ルールリスト**］をクリックします。

      Kaspersky Embedded Systems Security は、スラッシュ「/」を含むパスを認識しません。パスを正しく入力するには、円記号「\」を使用してください。

   b. ルール適用のモードを選択します：
      - **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一元管理するかたちで、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。
      - **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。アプリケーション起動コントロールルールの自動作成タスクを使用してローカルルールリストを編集できます。
4. ［**ルールの使用範囲**］セクションで、次の設定を行います：
   - **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. ［**KSN の使用**］セクションで、次のアプリケーション起動を設定します：

- **KSN で信頼されていないアプリケーションを拒否する**。
- **KSN で信頼されているアプリケーションを許可する**。
- KSN で信頼されているアプリケーションの起動を許可するユーザーまたはユーザーグループ。

6. ［**ソフトウェア配布コントロール**］タブでソフトウェア配布コントロールを設定します。
7. ［**タスク管理**］タブで、タスクの開始スケジュールを設定します。
8. ［**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

*信頼する配布パッケージを追加するには：*

1. ［**アプリケーション起動コントロール**］ウィンドウを開きます。
2. ［**ソフトウェア配布コントロール**］タブで、［**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**］をオンにします。

［**アプリケーション起動コントロール**］タスクの設定で［**全般**］タブの［**実行ファイルにルールを適用する**］がオンになっている場合、［**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**］をオンにできます。

3. 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**］をオフにします。

［**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**］をオフにすることは、どうしても必要な場合以外お勧めできません。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。

4. 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**］をオンにします。

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本製品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。

5. 信頼する配布パッケージのリストを編集するには、［**パッケージリストの変更**］をクリックし、表示されたウィンドウで次の方法のいずれかを選択します：
   - **1 つの配布パッケージを追加**
     a. ［**参照**］をクリックします。
     b. 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**］セクションには、選択したファイルに関するデータが自動的に読み込まれます。

c. ［**この配布パッケージから作成されたプログラムの今後の配布を許可する**］をオンまたはオフにします。

d. ファイルまたは配布パッケージを信頼するかどうかを決定するのに使用する基準について、2 つのオプションのいずれかを選択します：

- **デジタル証明書を使用する**
- **SHA256 ハッシュを使用する**

- **ハッシュで複数のパッケージを追加**

  実行ファイルおよび配布パッケージを数の制限なく選択して、すべて同時にリストに追加できます。Kaspersky Embedded Systems Security はハッシュを検査し、オペレーティングシステムが指定ファイルを開始するのを可能にします。

- **選択したパッケージを変更**

  異なる実行ファイルまたは配布パッケージを選択するか、信頼の基準を変更するには、このオプションを使用します。

- **ファイルから配布パッケージリストをインポート**

  ［開く］ウィンドウで、信頼する配布パッケージのリストを含む設定ファイルを指定します。

6. 以前に追加されたアプリケーションまたは信頼するリストの配布パッケージを削除するには、［**配布パッケージの削除**］をクリックします。抽出したファイルの実行が許可されます。

   抽出したファイルの起動を防ぐには、保護対象デバイス上でアプリケーションをアンインストールするか、アプリケーション起動コントロールタスクの設定で拒否ルールを作成します。

7. ［OK］をクリックします。

新しい設定が保存されます。

## アプリケーション起動コントロールルールの自動作成タスクの設定

*アプリケーション起動コントロールルールの自動作成タスクを設定するには：*

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**の**プロパティ**ウィンドウを開きます。
2. ［**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。

3. ［**設定**］セクションでは、次の設定を行うことができます：

   - ルール名の接頭辞を追加します。

- 許可ルールの作成方法を選択します：
  - **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**
  - **次のフォルダーにあるアプリケーションに対する許可ルールを作成する**

4. ［**オプション**］セクションでは、アプリケーション起動コントロールの許可ルール作成時に実行する処理を指定できます：
   - **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使用**
     - **SHA256 ハッシュ**：ルールの作成に使用されるファイルのチェックサムが、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。指定されたチェックサムを持つファイルを使用して起動されるプログラムの開始が許可されます。
     - **ファイルのパス**：ルールの作成に使用されるファイルのパスが、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。［**設定**］セクションの［**次のフォルダーにあるアプリケーションに対する許可ルールを作成する**］テーブルで指定されたフォルダーにあるファイルを使用して起動されるプログラムの開始が許可されます。
   - **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作成**

   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、設定ファイルの設定ができます。

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（定義データベース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。

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。

## アプリケーション起動コントロールルールの Kaspersky Security Center からの設定

さまざまな条件に基づいてルールのリストを生成する方法、またはアプリケーション起動コントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法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

*アプリケーション起動コントロールルールを追加するには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。
2. ［**追加**］をクリックします。
3. ボタンのコンテキストメニューで、［**1つのルールを追加**］を選択します。
   ［**ルール設定**］ウィンドウが開きます。
4. 次の設定を指定します：
   a. ［**名前**］で、ルールの名前を入力します。
   b. ［**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**：ルール設定で指定された基準に従って、ルールがアプリケーションの起動を許可します。
      - **拒否**：ルール設定で指定された基準に従って、ルールがアプリケーションの起動をブロックします。
   c. ［**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。
   d. ［**ユーザーまたはユーザーグループ**］で、ルールの種別に従って、プログラムの起動が許可されるユーザーまたは許可されないユーザーを指定します。それには、次の操作を実行します：
      1. ［**参照**］をクリックします。
      2. Microsoft Windows 標準の［ユーザーまたはグループの選択］ウィンドウが開きます。
      3. ユーザーまたはユーザーグループのリストを指定します。
      4. ［OK］をクリックします。
   e. ［**ルール有効化の条件**］セクションにリストされたルール有効化の条件の値を、特定のファイルから取得する場合：
      1. ［**ファイルのプロパティからルール有効化の条件を設定**］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。
      2. ファイルを選択します。
      3. ［開く］をクリックします。
         ファイルの基準の値が［**ルール有効化の条件**］セクションのフィールドに表示されます。ファイルのプロパティで指定できるデータの基準が既定で選択されています。
   f. ［**ルール有効化の条件**］セクションで、次のいずれかを選択します：

- **デジタル証明書**：デジタル証明書で署名されたファイルを使用して起動されるアプリケーションの開始が、ルールによって制御されます：
  - 指定したヘッダーを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、［**発行先を使用**］をオンにします。
  - 指定したサムプリントを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、［**サムプリントを使用**］をオンにします。
- **SHA256 ハッシュ**：チェックサムが指定されたものと一致するファイルを使用して起動されるプログラムの開始が、ルールによって制御されます。
- **ファイルのパス**：指定されたパスにあるファイルを使用して起動されるプログラムの開始が、ルールによって制御されます。

  Kaspersky Embedded Systems Security は、スラッシュ「/」を含むパスを認識しません。パスを正しく入力するには、円記号「\」を使用してください。

  オブジェクトを指定する時は、ファイルマスク（?、* を使用）と次の環境変数が使用できます：%WINDIR%、%SYSTEM32%、%OSDRIVE%、%PROGRAMFILES%。

g. ルールの除外対象を追加するには：

1. ［**ルールから除外**］セクションで、［追加］をクリックします。
   ［**ルールから除外**］ウィンドウが開きます。
2. ［**名前**］で、除外の名前を入力します。
3. アプリケーション起動コントロールルールからアプリケーションのファイルを除外する設定を指定します。［**ファイルのプロパティに基づいて除外を設定**］をクリックして、ファイルのプロパティから設定フィールドに入力できます。
   - デジタル証明書
   - **発行先を使用**
   - **サムプリントを使用**
   - **SHA256 ハッシュ**
   - **ファイルのパス**
4. ［OK］をクリックします。
5. 必要に応じて、手順（i）～（iv）を繰り返し、除外を追加します。

5. ［**ルール設定**］ウィンドウで［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**］ウィンドウのリストに、作成されたルールが表示されます。

## 「既定で許可」モードを有効にする

アプリケーションがルールまたはKSNの信頼しない判定によってブロックされていない場合、「既定で許可」モードですべてのアプリケーションの起動が許可されます。「既定で許可」モードは、以下で記載している設定の許可ルールを追加することによって有効にできます。「既定で許可」は、スクリプトまたはすべての実行可能なファイルに対してのみ有効にできます。

*「既定で許可」ルールを追加するには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。
2. ［**追加**］をクリックして、ボタンのコンテキストメニューで［**1つのルールを追加**］を選択します。
   ［**ルール設定**］ウィンドウが開きます。
3. ［**名前**］で、ルールの名前を入力します。
4. ［**種別**］ドロップダウンリストで、**許可**ルールを選択します。
5. ［**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。
6. ［**ルール有効化の条件**］セクションで、［**ファイルのパス**］を選択します。
7. 次のマスクを入力します：`?:\`
8. ［**ルール設定**］ウィンドウで［**OK**］をクリックします。

「既定で許可」モードが適用されます。

## Kaspersky Security Centerイベントからの許可ルールの作成

*アプリケーション起動コントロールのKaspersky Security Centerイベントからアプリケーションの許可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**］ウィンドウを開きます。
2. ［**追加**］をクリックし、コンテキストメニューで［**Kaspersky Security Centerイベントからアプリケーションの許可ルールを作成**］を選択します。
3. 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作成**］ウィンドウが開きます。

4. ルール作成タスクで使用するイベントの種別を選択します：

   - ［**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**］。
   - ［**アプリケーションの起動が拒否されました**］。

5. ［**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、時間間隔を選択します。

6. ［**ルール生成時のハッシュの使用を優先する**］をオンまたはオフにします。

   このチェックボックスをオンにすると、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。

7. ［**ルールの生成**］をクリックします。

8. ［**アプリケーション起動コントロールルール**］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タスクのルールリストには、Kaspersky Security Center 管理コンソールがインストールされた保護対象デバイスからのシステムデータに基づいて生成される新しいルールが反映されます。

   アプリケーション起動コントロールルールのリストがポリシーで既に指定されている場合、Kaspersky Embedded Systems Security は選択したルールをブロックイベントから既に指定したルールに追加します。リスト内のすべてのルールは一意である必要があるため、同じハッシュを持つルールは追加されません。

## ブロックされたアプリケーションに関する Kaspersky Security Center のレポートからのルールのインポート

［**統計のみ**］モードでアプリケーション起動コントロールタスクを実行後、Kaspersky Security Center で生成されるレポートからブロックされたアプリケーションの起動のデータをインポートできます。そのデータを使用して、設定中のポリシーで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できます。

アプリケーション起動コントロールタスクの実行中に発生したイベントのレポートの生成時に、起動がブロックされたアプリケーションを確認することができます。

ブロックされたアプリケーションのレポートのデータをポリシー設定にインポートする場合は、使用するリストには起動を許可するアプリケーションのみが含まれていることを確認してください。

*Kaspersky Security Center からのブロックされたアプリケーションのレポートに従い、保護対象デバイスのグループに対してアプリケーション起動コントロールの許可ルールを指定するには：*

1. ［**アプリケーション起動コントロール**］ウィンドウを開きます。
2. ［**タスクモード**］セクションで、［**統計のみ**］モードを選択します。

3. ポリシーのプロパティの［**イベント通知**］セクションで、次の内容を確認します：

   - ［**緊急イベント**］で、［**アプリケーションの起動が拒否されました**］イベントの実行ログの保管期間が［**統計のみ**］モードのタスクの実行で計画された期間を超えている（既定値は 30 日）。
   - 重要度が［**警告**］のイベントで、［**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**］イベントの実行ログの保管期間が［**統計のみ**］モードのタスクの実行で計画された期間を超えている（既定値は 30 日）。

   イベントの保管期間が経過すると、記録されたイベントに関する情報が削除され、レポートファイルに反映されません。**統計のみ**モードでアプリケーション起動コントロールタスクを実行する前に、タスクの実行時間が、指定のイベントに対して設定されている期間を超えていないことを確認してください。

4. タスクが完了すると、記録されたイベントを TXT ファイルにエクスポートします：

   a. Kaspersky Security Center の［**管理サーバー**］フォルダーの作業領域で、［**イベント**］タブを選択します。

   b. ［**抽出の作成**］をクリックし、［ブロック］の基準に基づいてイベントの抽出を作成し、アプリケーション起動コントロールタスクによって起動がブロックされるアプリケーションを表示します。

   c. 抽出の結果ペインで、［**イベントをファイルにエクスポート**］をクリックして、ブロックされたアプリケーション起動のレポートを TXT ファイルに保存します。

   生成したレポートをポリシーにインポートして適用する前に、レポートには起動を許可するアプリケーションのデータしか含まれていないことを確認してください。

5. ブロックされたアプリケーション起動のデータをアプリケーション起動コントロールタスクにインポートします。それには、アプリケーション起動コントロールタスク設定のポリシーのプロパティで、次の手順を実行します：

   a. ［**全般**］タブで、［**ルールリスト**］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**］ウィンドウが開きます。

   b. ［**追加**］をクリックし、コンテキストメニューで［**Kaspersky Security Center のレポートから、ブロックされたアプリケーションのデータをインポート**］を選択します。

   c. Kaspersky Security Center のレポートを基に作成されたリストから以前設定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ルールを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。

   d. 表示される Microsoft Windows の標準のウィンドウで、ブロックされたアプリケーション起動のレポートから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。

   e. ［**アプリケーション起動コントロールルール**］ウィンドウで［**保存**］をクリックします。

ブロックされたアプリケーションに関する Kaspersky Security Center のレポートに従って作成されたルールが、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されます。

## XML ファイルからのアプリケーション起動コントロールルールのインポート

アプリケーション起動コントロールルールの自動作成グループタスクによって生成されるレポートをインポートし、許可ルールのリストとして設定中のポリシーに適用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作成グループタスクが終了すると、作成した許可ルールは、指定された共有フォルダーに保存してある XML ファイルにエクスポートされます。ルールのリストの各ファイルは、企業ネットワーク上のそれぞれの保護対象デバイスで実行されたファイルと起動されたアプリケーションの分析に基づいて作成されます。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作成グループタスクで指定された種別と同じ種別のファイルとアプリケーションに対する許可ルールが含まれます。

*自動で生成された許可ルールのリストに従って保護対象デバイスのグループに対してアプリケーション起動コントロールの許可ルールを指定するには：*

1. 設定中の保護対象デバイスグループの詳細ペインの［**タスク**］タブで、アプリケーション起動コントロールルールの自動作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. 作成したアプリケーション起動コントロールルールの自動作成グループタスクのプロパティで、次の設定を行います：

   - ［**通知**］セクションで、タスクの実行レポートの保存設定を行います。

     このセクションでの設定方法の詳細については、*Kaspersky Security Center のヘルプ*を参照してください。

   - ［**設定**］セクションで、作成したルールで起動が許可されるアプリケーションの種別を指定します。タスクの範囲から既定のフォルダーを除外したり、新しいフォルダーを手動で追加したりして、許可されるアプリケーションを含むフォルダーとして指定するフォルダーを編集できます。

   - ［**オプション**］セクションで、タスクの実行中と完了後の処理を指定します。ルールが生成される基準と、生成されるルールのエクスポート先のファイル名を指定します。

   - ［**スケジュール**］セクションで、タスクの開始スケジュールを設定します。

   - ［**アカウント**］セクションで、タスクが実行されるユーザーアカウントを指定します。

   - ［**タスク範囲からの除外**］セクションで、タスク範囲から除外する保護対象デバイスのグループを指定します。

     除外対象の保護対象デバイスで起動されるアプリケーションに対して許可ルールは作成されません。

3. 設定中の保護対象デバイスグループの詳細ペインにある、［**タスク**］タブのグループタスクのリストで、作成したアプリケーション起動コントロールルールの自動作成タスクを選択し、［**開始**］をクリックしてタスクを開始します。

   タスクが完了すると、自動で生成された許可ルールのリストは XML ファイルとして共有フォルダーに保存されます。

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で、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作成タスクを開始してください。

4. 生成された許可ルールのリストをアプリケーション起動コントロールタスクに追加するには：

   a. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。

   b. ［**追加**］をクリックして、表示されるリストで［**XML ファイルからルールをインポート**］を選択します。

   c. 自動で生成された許可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。

   d. 表示される Microsoft Windows の標準のウィンドウで、アプリケーション起動コントロールルールの自動作成グループタスクの完了後に作成される XML ファイルを選択します。

   e. ［**アプリケーション起動コントロールルール**］ウィンドウで［**保存**］をクリックします。

5. 作成したルールを適用してアプリケーションの起動を管理する場合は、アプリケーション起動コントロールタスクのプロパティのポリシーでタスクに対して［**処理を実行**］モードを選択します。

各保護対象デバイスで実行されるタスクに基づいて自動で生成される許可ルールは、設定中のポリシーの範囲となっているすべてのネットワークサーバーに適用されます。これらの保護対象デバイスでは、許可ルールが作成されたアプリケーションに対してのみ起動が許可されます。

## アプリケーション起動のテスト

設定したアプリケーション起動コントロールルールを適用する前に、任意のアプリケーションのテスト起動を試行して、各アプリケーションにどのアプリケーション起動コントロールルールが適用されているかを判断できます。

既定では、起動がいずれかのルールによって許可されないアプリケーションの起動は拒否されます。重要なアプリケーションの起動を拒否しないようにするには、許可ルールを作成する必要があります。

アプリケーションの起動が、種別の異なる複数のルールで管理されている場合、拒否ルールが優先されます。1 つ以上の拒否ルールの対象になっている場合、アプリケーションの起動は拒否されます。

*アプリケーション起動コントロールルールをテストするには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。

2. 表示されたウィンドウで、［**ファイルのルールを表示**］をクリックします。

Microsoft Windows 標準のウィンドウが表示されます。

3. 起動コントロールをテストするファイルを選択します。

指定されたファイルへのパスが検索フィールドに表示されます。リストには、選択されたファイルの起動時に適用されるルールすべてが含まれます。

## アプリケーション起動コントロールルールの自動作成タスクの作成

*アプリケーション起動コントロールルールの自動作成タスクを作成して編集するには：*

1. ［新規タスクウィザード］で、［**設定**］ウィンドウを開きます。
2. 以下を設定します：
   - ルール名の接頭辞を指定します。
   - 許可ルールの適用範囲を設定します。
3. ［次へ］をクリックします。
4. Kaspersky Embedded Systems Security が実行する処理を指定します：
   - 許可ルールの作成時
   - タスクの完了時
5. ［**スケジュール**］ウィンドウで、タスクの開始スケジュールを設定します。
6. ［次へ］をクリックします。
7. ［タスクを実行するアカウントの選択］ウィンドウで、使用するアカウントを指定します。
8. ［次へ］をクリックします。
9. タスク名を指定します。
10. ［次へ］をクリックします。

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。

［タスクの作成を終了］ウィンドウが開きます。

11. オプションで［ウィザード完了後にタスクを実行する］をオンにすると、ウィザードの終了後にタスクを実行することができます。
12. ［完了］をクリックしてタスクの作成を終了します。

*Kaspersky Security Center で既存のルールを編集するには：*

**アプリケーション起動コントロールルールの自動生成**ウィンドウを開き、上記の設定を編集します。

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。

## タスクの適用範囲の制限

*アプリケーション起動コントロールルールの自動作成タスクの範囲を制限するには：*

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**の**プロパティ**ウィンドウを開きます。
2. 許可ルールの作成方法を選択します：
   - **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**
   - **次のフォルダーにあるアプリケーションに対する許可ルールを作成する**
3. ［OK］をクリックします。

   指定された設定が保存されます。

## ルールの自動作成中に実行する処理

*アプリケーション起動コントロールルールの自動作成タスクの実行時に Kaspersky Embedded Systems Security が行う処理を設定するには：*

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**の**プロパティ**ウィンドウを開きます。
2. ［**オプション**］タブを開きます。
3. ［**許可ルールの生成中**］セクションで、次の設定を行います：
   - **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使用**
     - **SHA256 ハッシュ**：ルールの作成に使用されるファイルのチェックサムが、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。指定されたチェックサムを持つファイルを使用して起動されるプログラムの開始が許可されます。
     - **ファイルのパス**：ルールの作成に使用されるファイルのパスが、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。［**設定**］セクションの［**次のフォルダーにあるアプリケーションに対する許可ルールを作成する**］テーブルで指定されたフォルダーにあるファイルを使用して起動されるプログラムの開始が許可されます。
   - **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作成**
4. ［OK］をクリックします。

   指定された設定が保存されます。

## ルールの自動作成の完了時に実行する処理

*アプリケーション起動コントロールルールの自動作成タスクの完了後に Kaspersky Embedded Systems Security が行う処理を設定するには：*

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**の**プロパティ**ウィンドウを開きます。
2. ［**オプション**］タブを開きます。
3. ［**タスク完了後**］セクションで、次の設定を行います：
   - **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**
   - **ファイル名に保護対象デバイスの詳細を追加する**
4. ［OK］をクリックします。

指定された設定が保存されます。

# アプリケーションコンソールからアプリケーション起動コントロールを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、保護デバイスのタスクの設定を行う方法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。

## アプリケーション起動コントロールタスクの設定ウィンドウ

*アプリケーションコンソールからアプリケーション起動コントロール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、［**コンピューターの管理**］フォルダーを展開します。
2. ［**アプリケーション起動コントロール**］サブフォルダーを選択します。
3. ［**アプリケーション起動コントロール**］サブフォルダーの詳細ペインで、［**プロパティ**］をクリックします。

［**タスクの設定**］ウィンドウが表示されます。

## アプリケーション起動コントロールルールの設定ウィンドウ

*アプリケーションコンソールからアプリケーション起動コントロールルールのリストを開くには：*

1. アプリケーションコンソールツリーで、［**コンピューターの管理**］フォルダーを展開します。
2. ［**アプリケーション起動コントロール**］サブフォルダーを選択します。
3. ［**アプリケーション起動コントロール**］フォルダーの結果ペインで、［**アプリケーション起動コントロールルール**］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**］ウィンドウが開きます。
4. 必要に応じてルールリストを設定します。

## アプリケーション起動コントロールルールの自動作成タスクの設定ウィンドウ

*アプリケーション起動コントロールルールの自動作成タスクを設定するには：*

1. アプリケーションコンソールツリーで、［**ルールの自動生成**］フォルダーを展開します。
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**］サブフォルダーを選択します。
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**］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。
   ［**タスクの設定**］ウィンドウが表示されます。
4. 必要に応じてタスクを設定します。

## アプリケーション起動コントロールタスクの設定

*アプリケーション起動コントロールタスクの全般的な設定を行うには：*

1. ［**タスクの設定**］ウィンドウを開きます。
2. 次のタスクの設定を指定します：
   - ［**全般**］タブ：
     - アプリケーション起動コントロールタスクのモード
     - タスクのルールの適用範囲
     - KSN の使用
   - ［**ソフトウェア配布コントロール**］タブのソフトウェア配布コントロールの設定

- ［**スケジュール**］タブおよび［**詳細設定**］タブのタスク開始スケジュール設定

3. ［**タスクの設定**］ウィンドウで［OK］をクリックします。

   変更された設定が保存されます。

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。

## アプリケーション起動コントロールタスクのモードの選択

*アプリケーション起動コントロールタスクのモードを設定するには：*

1. ［**タスクの設定**］ウィンドウを開きます。
2. ［**全般**］タブの［**タスクモード**］ドロップダウンリストで、タスクモードを指定します。
3. ［**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**］をオフまたはオンにします。

   Kaspersky Embedded Systems Security では、アプリケーション起動コントロールタスク設定を変更するたびに、キャッシュイベントの新しいリストが作成されます。これは、現在のセキュリティ設定に従って、アプリケーション起動コントロールが実行されることを意味します。

4. ［**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**］をオフまたはオンにします。
5. ［**タスクの設定**］ウィンドウで［OK］をクリックします。

指定された設定が保存されます。

アプリケーションを起動しようとするすべての試行は、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の範囲の設定

*アプリケーション起動コントロールタスクの範囲を定義するには：*

1. ［**タスクの設定**］ウィンドウを開きます。
2. ［**ルールの使用範囲**］セクションの［**全般**］タブで、次の設定を行います：
   - **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**

3. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

指定された設定が保存されます。

## KSN の使用の設定

*アプリケーション起動コントロールタスクで KSN サービスの使用を設定するには：*

1. ［**タスクの設定**］ウィンドウを開きます。
2. ［**全般**］タブの［**KSN の使用**］セクションで、KSN サービスの使用の設定を行います：
   - 必要に応じて、［**KSN で信頼されていないアプリケーションを拒否する**］をオンにします。
   - 必要に応じて、［**KSN で信頼されているアプリケーションを許可する**］をオンにします。
   - ［**KSN で信頼されているアプリケーションを許可する**］をオンにする場合、KSN で信頼されているアプリケーションの起動が許可されるユーザーまたはユーザーグループを指定します。それには、次の操作を実行します：
     a. ［**編集**］をクリックします。
     Microsoft Windows 標準の［**ユーザーまたはグループの選択**］ウィンドウが開きます。

     > 既定では、KSN で信頼されているプログラムへのアクセスは、すべてのユーザーに許可されています。

     b. ユーザーまたはユーザーグループのリストを指定します。
     c. ［**OK**］をクリックします。
3. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

指定された設定が保存されます。

## ソフトウェア配布コントロール

*信頼する配布パッケージを追加するには：*

1. ［**タスクの設定**］ウィンドウを開きます。
2. ［**ソフトウェア配布コントロール**］タブで、［**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**］をオンにします。

> ［**アプリケーション起動コントロール**］タスクの設定で［**全般**］タブの［**実行ファイルにルールを適用する**］がオンになっている場合、［**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**］をオンにできます。

3. 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**］をオフにします。

［**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**］をオフにすることは、どうしても必要な場合以外お勧めできません。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。

4. 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**］をオンにします。

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本製品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。

5. 信頼する配布パッケージのリストを編集するには、［**パッケージリストの変更**］をクリックし、表示されたウィンドウで次の方法のいずれかを選択します：

- **1 つの配布パッケージを追加**

  a. ［**参照**］をクリックします。

  b. 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**］セクションには、選択したファイルに関するデータが自動的に読み込まれます。

  c. ［**この配布パッケージから作成されたプログラムの今後の配布を許可する**］をオンまたはオフにします。

  d. ファイルまたは配布パッケージを信頼するかどうかを決定するのに使用する基準について、2 つのオプションのいずれかを選択します：

  - **デジタル証明書を使用する**
  - **SHA256 ハッシュを使用する**

- **ハッシュで複数のパッケージを追加**

実行ファイルおよび配布パッケージを数の制限なく選択して、すべて同時にリストに追加できます。Kaspersky Embedded Systems Security はハッシュを検査し、オペレーティングシステムが指定ファイルを開始するのを可能にします。

- **選択したパッケージを変更**

異なる実行ファイルまたは配布パッケージを選択するか、信頼の基準を変更するには、このオプションを使用します。

- **ファイルから配布パッケージリストをインポート**

［**開く**］ウィンドウで、信頼する配布パッケージのリストを含む設定ファイルを指定します。

6. 以前に追加されたアプリケーションまたは信頼するリストの配布パッケージを削除するには、［**配布パッケージの削除**］をクリックします。抽出したファイルの実行が許可されます。

抽出したファイルの起動を防ぐには、保護対象デバイス上でアプリケーションをアンインストールするか、アプリケーション起動コントロールタスクの設定で拒否ルールを作成します。

7. ［**OK**］をクリックします。

新しい設定が保存されます。

## アプリケーション起動コントロールルールの設定

ルールのリストを生成やインポート / エクスポートする方法、またはアプリケーション起動コントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法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

*アプリケーション起動コントロールルールを追加するには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。
2. ［**追加**］をクリックします。
3. ボタンのコンテキストメニューで、［**1つのルールを追加**］を選択します。
   ［**ルール設定**］ウィンドウが開きます。
4. 次の設定を指定します：
   a. ［**名前**］で、ルールの名前を入力します。
   b. ［**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**：ルール設定で指定された基準に従って、ルールがアプリケーションの起動を許可します。
      - **拒否**：ルール設定で指定された基準に従って、ルールがアプリケーションの起動をブロックします。
   c. ［**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。
   d. ［**ユーザーまたはユーザーグループ**］で、ルールの種別に従って、プログラムの起動が許可されるユーザーまたは許可されないユーザーを指定します。それには、次の操作を実行します：
      1. ［**参照**］をクリックします。
      2. Microsoft Windows 標準の［ユーザーまたはグループの選択］ウィンドウが開きます。
      3. ユーザーまたはユーザーグループのリストを指定します。
      4. ［OK］をクリックします。
   e. ［**ルール有効化の条件**］セクションにリストされたルール有効化の条件の値を、特定のファイルから取得する場合：

1. ［**ファイルのプロパティからルール有効化の条件を設定**］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。

2. ファイルを選択します。

3. ［開く］をクリックします。

   ファイルの基準の値が［**ルール有効化の条件**］セクションのフィールドに表示されます。ファイルのプロパティで指定できるデータの基準が既定で選択されています。

f. ［**ルール有効化の条件**］セクションで、次のいずれかを選択します：

- **デジタル証明書**：デジタル証明書で署名されたファイルを使用して起動されるアプリケーションの開始が、ルールによって制御されます：
  - 指定したヘッダーを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、［**発行先を使用**］をオンにします。
  - 指定したサムプリントを持つデジタル証明書を使用して署名されたファイルの起動のみを、ルールの制御対象にする場合は、［**サムプリントを使用**］をオンにします。
- **SHA256 ハッシュ**：チェックサムが指定されたものと一致するファイルを使用して起動されるプログラムの開始が、ルールによって制御されます。
- **ファイルのパス**：指定されたパスにあるファイルを使用して起動されるプログラムの開始が、ルールによって制御されます。

  Kaspersky Embedded Systems Security は、スラッシュ「/」を含むパスを認識しません。パスを正しく入力するには、円記号「\」を使用してください。

  オブジェクトを指定する時は、ファイルマスク（?、* を使用）と次の環境変数が使用できます：%WINDIR%、%SYSTEM32%、%OSDRIVE%、%PROGRAMFILES%。

g. ルールの除外対象を追加するには：

1. ［**ルールから除外**］セクションで、［追加］をクリックします。

   ［**ルールから除外**］ウィンドウが開きます。

2. ［**名前**］で、除外の名前を入力します。

3. アプリケーション起動コントロールルールからアプリケーションのファイルを除外する設定を指定します。［**ファイルのプロパティに基づいて除外を設定**］をクリックして、ファイルのプロパティから設定フィールドに入力できます。

   - **デジタル証明書**
   - **発行先を使用**
   - **サムプリントを使用**
   - **SHA256 ハッシュ**
   - **ファイルのパス**

4. ［**OK**］をクリックします。

5. 必要に応じて、手順（i）～（iv）を繰り返し、除外を追加します。

5. ［**ルール設定**］ウィンドウで［**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**］ウィンドウのリストに、作成されたルールが表示されます。

## 「既定で許可」モードを有効にする

アプリケーションがルールまたはKSNの信頼しない判定によってブロックされていない場合、「既定で許可」モードですべてのアプリケーションの起動が許可されます。「既定で許可」モードは、以下で記載している設定の許可ルールを追加することによって有効にできます。「既定で許可」は、スクリプトまたはすべての実行可能なファイルに対してのみ有効にできます。

*「既定で許可」ルールを追加するには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。

2. ［**追加**］をクリックします。

3. ボタンのコンテキストメニューで、［**1つのルールを追加**］を選択します。
［**ルール設定**］ウィンドウが開きます。

4. ［**名前**］で、ルールの名前を入力します。

5. ［**種別**］ドロップダウンリストで、**許可**ルールを選択します。

6. ［**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。

7. ［**ルール有効化の条件**］セクションで、［**ファイルのパス**］を選択します。

8. 次のマスクを入力します：**?:**

9. ［**ルール設定**］ウィンドウで［**OK**］をクリックします。

「既定で許可」モードが適用されます。

## アプリケーション起動コントロールタスクイベントからの許可ルールの作成

*アプリケーション起動コントロールタスクイベントから生成された許可ルールを含む設定ファイルを作成するには：*

1. アプリケーション起動コントロールタスクを［**統計のみ**］モードで開始し、保護対象デバイスでのすべてのアプリケーション起動に関する情報をタスク実行ログに記録します。

2. **統計のみ**モードで実行しているタスクの完了後、［**アプリケーション起動コントロール**］フォルダーの詳細ペインの［**管理**］セクションにある［**実行ログを開く**］をクリックして、実行ログを開きます。

3. ［**ログ**］ウィンドウで、［**イベントに基づいてルールを作成する**］をクリックします。

**統計のみ**モードのアプリケーション起動コントロールタスクで発生したイベントに基づくルールリストを含んだ XML 設定ファイルが作成されます。アプリケーション起動コントロールタスクで、このルールリストを適用できます

記録されたタスクイベントから作成されたルールリストを適用する前に、リストを確認して手動で処理し、指定したルールにより重要なファイル（たとえば、システムファイルなど）の実行が許可されていることを確認してください。

すべてのタスクイベントが、タスクモードに関係なく実行ログに記録されます。**処理を実行**モードでタスクが実行中に作成されたログに基づいたルールリストが含まれる設定ファイルを作成できます。タスクが適切に動作するには、タスクが［**処理を実行**］モードで実行される前に最終的なルールのリストを作成しておく必要があります。そのため、緊急の場合を除いてこのシナリオは推奨されません。

## アプリケーション起動コントロールルールのエクスポート

*アプリケーション起動コントロールルールを設定ファイルにエクスポートするには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。

2. ［**ファイルにエクスポート**］をクリックします。
Microsoft Windows 標準のウィンドウが表示されます。

3. 表示されたウィンドウで、ルールをエクスポートするファイルを指定します。ファイルが存在しない場合は作成されます。指定した名前のファイルが既に存在する場合、ルールをエクスポートするとファイルの内容が上書きされます。

4. ［**保存**］をクリックします。

ルール設定が指定されたファイルにエクスポートされます。

## XML ファイルからのアプリケーション起動コントロールルールのインポート

*アプリケーション起動コントロールルールをインポートするには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。

2. ［**追加**］をクリックします。

3. 表示されるコンテキストメニューで、［**XML ファイルからルールをインポート**］を選択します。

4. インポートされるルールを追加する方法を指定します。そのためには、［**XML ファイルからルールをインポート**］のコンテキストメニューからいずれかのオプションを選択します：

- **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。

Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが表示されます。

5. ［**ファイルを開く**］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を含む XML ファイルを選択します。
6. ［**開く**］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**］ウィンドウのリストに、インポートされたルールが表示されます。

## アプリケーション起動コントロールルールの削除

*アプリケーション起動コントロールルールを削除するには：*

1. ［**アプリケーション起動コントロールルール**］ウィンドウを開きます。
2. リストで削除するルールを1つ以上選択します。
3. ［**選択項目の削除**］をクリックします。
4. ［**保存**］をクリックします。

選択したアプリケーション起動コントロールルールが削除されます。

## アプリケーション起動コントロールルールの自動作成タスクの設定

*アプリケーション起動コントロールルールの自動作成タスクを設定するには：*

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**］タスクの**タスクの設定**ウィンドウを開きます。
2. 次の設定を指定します：
   - ［**全般**］タブ：
     - **ルール名の接頭辞**を指定します。
     - 許可ルールの適用範囲を設定します。
   - ［**処理**］タブで、Kaspersky Embedded Systems Security が実行する処理を指定します。
   - ［**スケジュール**］タブと［**詳細設定**］タブで、タスクの開始スケジュールを設定します。
   - ［**実行用アカウント**］タブで、アカウント権限を使用して起動するタスクを設定します。
3. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

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。

## タスクの適用範囲の制限

*アプリケーション起動コントロールルールの自動作成タスクの範囲を制限するには：*

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**］タスクの**タスクの設定**ウィンドウを開きます。
2. 許可ルールの作成方法を選択します：
   - **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**
   - **次のフォルダーにあるアプリケーションに対する許可ルールを作成する**
3. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

   指定された設定が保存されます。

## ルールの自動作成中に実行する処理

*アプリケーション起動コントロールルールの自動作成タスクの実行時および完了時に Kaspersky Embedded Systems Security が行う処理を設定するには：*

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**］タスクの**タスクの設定**ウィンドウを開きます。
2. ［**オプション**］タブを開きます。
3. ［**許可ルールの生成中**］セクションで、次の設定を行います：
   - **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使用**
     - **SHA256 ハッシュ**：ルールの作成に使用されるファイルのチェックサムが、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。指定されたチェックサムを持つファイルを使用して起動されるプログラムの開始が許可されます。
     - **ファイルのパス**：ルールの作成に使用されるファイルのパスが、アプリケーション起動コントロールの許可ルールを適用する基準として設定されます。［**設定**］セクションの［**次のフォルダーにあるアプリケーションに対する許可ルールを作成する**］テーブルで指定されたフォルダーにあるファイルを使用して起動されるプログラムの開始が許可されます。
   - **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作成**
4. ［**タスク完了後**］セクションで、次の設定を行います：
   - **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**
- **ファイル名に保護対象デバイスの詳細を追加する**

5. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

指定された設定が保存されます。

## ルールの自動作成の完了時に実行する処理

*アプリケーション起動コントロールルールの自動作成タスクの完了後に Kaspersky Embedded Systems Security が行う処理を設定するには：*

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**］タスクの**タスクの設定**ウィンドウを開きます。
2. ［**オプション**］タブを開きます。
3. ［**タスク完了後**］セクションで、次の設定を行います：
   - **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**
   - **ファイル名に保護対象デバイスの詳細を追加する**
4. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。

指定された設定が保存されます。

## Web プラグインからアプリケーション起動コントロールを管理する

*Web プラグインからアプリケーション起動コントロール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**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**ローカル活動の管理**］セクションを選択します。
5. ［**アプリケーション起動コントロール**］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。

アプリケーション起動コントロールタスクの設定

| 設定 | 説明 |
| --- | --- |
| **タスクモード** | このドロップダウンリストで、アプリケーション起動コントロールタスクのモード |

| | |
|---|---|
| | を選択できます：<br>• **処理を実行**：指定されたルールを使用して、アプリケーションの起動を管理します。<br>• **統計のみ**：アプリケーションの起動を管理するために指定されたルールは使用されません。代わりに、実行ログに起動イベントに関する情報が記録されます。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。<br>既定では、アプリケーション起動コントロールタスクは**統計のみ**モードで動作します。 |
| **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** | このチェックボックスでは、2 回目以降のアプリケーションの起動試行に対して、キャッシュに保存されたイベント情報に基づく起動コントロール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、アプリケーションの初回起動に関するタスクの判定を基にして、アプリケーションの以降の起動が許可または拒否されます。たとえば、アプリケーションの初回起動がルールにより許可された場合、この判定に関する情報がキャッシュに保存され、2 回目以降の起動はすべて許可されて、追加の再チェックは行われません。<br>このチェックボックスをオフにすると、アプリケーションが起動を試行するたびに毎回アプリケーションが分析されます。<br>既定では、このチェックボックスはオフです。 |
| **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** | チェックボックスをオンにすると、インタープリターの起動が許可された場合でもコマンドラインインタープリターの起動が拒否されます。コマンドのないコマンドインタープリターは、以下の両方の条件が満たされた場合のみ起動されます：<br>• コマンドラインインタープリターの起動が許可されている。<br>• 実行対象のコマンドが許可されている。<br>チェックボックスをオフにすると、コマンドラインインタープリターを起動する時に許可ルールのみが考慮されます。許可ルールが適用されていない、または実行プロセスが KSN によって信頼されていない場合、起動は拒否されます。許可ルールが適用されているか、プロセスが KSN によって信頼されている場合、コマンドラインインタープリターは実行コマンドがある場合でもない場合でも起動できます。<br>Kaspersky Embedded Systems Security は次のコマンドラインインタープリターを認識します：<br>• cmd.exe<br>• powershell.exe<br>• python.exe<br>• perl.exe<br>既定では、このチェックボックスはオフです。 |
| **実行ファイルにルールを適用する** | このチェックボックスでは、実行ファイルの起動コントロール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、**実行ファイル**を範囲として設定する、指定されたルールを使用して実行ファイルの起動を許可またはブロックします。 |

| | |
|---|---|
| | このチェックボックスをオフにすると、指定されたルールによる実行ファイルの起動は制御されません。実行ファイルの起動が許可されます。<br>既定では、このチェックボックスはオンです。 |
| **DLL モジュールの読み込みを監視する** | このチェックボックスでは、DLL モジュールの読み込みの監視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、**実行ファイル**を範囲として設定する、指定されたルールを使用して DLL モジュールの読み込みを許可またはブロックします。<br>このチェックボックスをオフにすると、指定されたルールを使用して DLL モジュールの読み込みを監視しません。DLL モジュールの読み込みが許可されます。<br>［**実行ファイルにルールを適用する**］がオンになっている場合に、このチェックボックスを選択できます。<br>既定では、このチェックボックスはオンです。 |
| **スクリプトと MSI パッケージにルールを適用する** | このチェックボックスでは、スクリプトと MSI パッケージの起動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、スクリプトと MSI パッケージを範囲として設定する、指定されたルールを使用して、スクリプトおよび MSI パッケージの開始を許可またはブロックします。<br>このチェックボックスをオフにすると、指定されたルールを使用したスクリプトおよび MSI パッケージの起動のコントロールは実行されません。スクリプトおよび MSI パッケージの起動は許可されます。<br>既定では、このチェックボックスはオンです。 |
| **KSN で信頼されていないアプリケーションを拒否する** | このチェックボックスでは、KSN でのアプリケーション評価データに従ってアプリケーション起動コントロール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、アプリケーションが KSN で信頼されていない場合に、そのアプリケーションの実行をブロックします。KSN で信頼しないアプリケーションに適用されるアプリケーション起動コントロールの許可ルールは適用されません。チェックボックスをオンにすると、マルウェアに対する保護も提供されます。<br>このチェックボックスをオフにすると、KSN の信頼しないアプリケーションの評価は考慮されず、そのようなアプリケーションに適用するルールに従って起動を許可またはブロックします。<br>既定では、このチェックボックスはオフです。 |
| **KSN で信頼されているアプリケーションを許可する** | このチェックボックスでは、KSN でのアプリケーション評価データに従ってアプリケーション起動コントロールを有効または無効にします。<br>チェックボックスをオンにすると、アプリケーションが KSN で信頼されている場合に、そのアプリケーションの実行を許可します。アプリケーションが KSN で信頼されていても、同じアプリケーションに適用されるアプリケーション起動コントロールの拒否ルールの方が、高い優先度を持っています：アプリケーションが KSN サービスによって信頼されている場合でも、このアプリケーションの起動は拒否されます。<br>このチェックボックスをオフにすると、KSN の信頼するアプリケーションの評価は考慮されず、そのようなアプリケーションに適用するルールに従って起動を許可またはブロックします。<br>既定では、このチェックボックスはオフです。 |
| **KSN で信頼されているアプリケーションの実行を許可** | ［**KSN で信頼されているアプリケーションを許可する**］がオンの場合、KSN で信頼されているアプリケーションの開始を許可するユーザーまたはユーザーグループをここで指定できます。 |

| | |
|---|---|
| **するユーザーまたはユーザーグループ** | 既定では、次のユーザーが指定されています：**Everyone** および **NT AUTHORITY\SYSTEM** |
| **ルール** | アプリケーション起動コントロールタスクの許可または拒否ルールを設定します。 |
| **ソフトウェア配布コントロール** | 信頼する配信パッケージを追加します。 |
| **タスク管理** | 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

このセクションでは、デバイスコントロールタスクとその設定方法について説明します。

## デバイスコントロールタスクについて

Kaspersky Embedded Systems Security では外部デバイスおよび CD / DVD ドライブ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セキュリティ脅威からデバイスを保護します。

Kaspersky Embedded Systems Security は、次の USB 外部デバイス接続を制御します：

- USB 接続フラッシュドライブ
- CD/DVD ROM ドライブ
- USB 接続フロッピーディスクドライブ
- USB 接続ネットワークアダプター
- USB 接続 MTP モバイルデバイス

Kaspersky Embedded Systems Security は、USB で接続されたすべてのデバイスについて、実行ログおよびイベントログの対応するイベントとともに通知します。イベント詳細には、デバイスの種別と接続パスが含まれます。デバイスコントロールタスクが開始されると、Kaspersky Embedded Systems Security は USB で接続されたすべてのデバイスをチェックしてリストします。通知は、Kaspersky Security Center の通知の設定セクションで設定できます。

デバイスコントロールタスクでは保護対象デバイスに USB で接続されている外部デバイスのすべての試行が監視されており、このデバイスの許可ルールが存在しない場合は接続がブロックされます。接続がブロックされると、そのデバイスは使用できなくなります。

本製品は、接続された外部デバイスごとに次のいずれかのステータスを付与します：

- *信頼する*：ファイル交換を許可するデバイス。ルールリストが作成されると、1つ以上のルールに対して*デバイスインスタンスパス*値が適用範囲に含められます。
- *信頼しない*：ファイル交換を制限するデバイス。デバイスインスタンスパスは、許可ルールの適用範囲には含められません。

外部デバイスの許可ルールを作成し、デバイスコントロールルールの自動作成タスクを使用すると、データ交換を許可できます。また、既に指定したルールの適用範囲を拡張することもできます。許可ルールは手動では作成できません。

Kaspersky Embedded Systems Security ではデバイスインスタンスパス値を使用して、システムに登録されている外部デバイスが識別されます。デバイスインスタンスパスは、外部デバイスごとに一意に指定された既定の機能です。デバイスインスタンスパス値は外部デバイスごとに Windows プロパティで指定され、ルール作成時に Kaspersky Embedded Systems Security によって自動的に判別されます。

デバイスコントロールタスクは、2 つのモードで実行できます：

- **処理を実行**：Kaspersky Embedded Systems Security ではフラッシュドライブやその他の外部デバイスの接続を制御するためにいくつかのルールが適用され、「既定で拒否」の原則と個別に指定した許可ルールに従って、各デバイスの使用が許可またはブロックされます。信頼する外部デバイスの使用は許可されます。信頼しない外部デバイスの使用は既定でブロックされます。

  デバイスコントロールタスクが［**処理を実行**］モードで実行される前に、信頼しないと判断される外部デバイスが保護対象デバイスに接続されていた場合、そのデバイスは製品によってブロックされません。信頼しないデバイスを手動で切断するか、保護対象デバイスを再起動してください。そうしない場合、このデバイスに「既定で拒否」の原則は適用されません。

- **統計のみ**：Kaspersky Embedded Systems Security ではフラッシュドライブやその他の外部デバイスの接続は制御されず、保護対象デバイス上での外部デバイスの接続と登録に関する情報、および接続されたデバイスによって適用されるデバイスコントロールの許可ルールに関する情報が記録されるのみです。すべての外部デバイスの使用が許可されます。既定ではこのモードが設定されています。

  このモードは、タスク実行時に記録されたデバイスのブロックに関する情報を基にしてルールを作成する際に適用できます。

# デバイスコントロールルールについて

Kaspersky Embedded Systems Security は、MTP 接続したモバイルデバイスに対して許可ルールを適用しません。

このルールは、現在保護対象デバイスに接続されているデバイスまたは接続されていたことがあるデバイスごとに一意に作成されます。ただし、このデバイスに関する情報がシステムレジストリに格納されている場合です。

デバイスコントロールの許可ルールを作成するには：

- デバイスコントロールルールの自動作成タスクの適用
- デバイスコントロールタスクの統計のみモードでの実行
- 以前接続されていたデバイスに関するシステム情報の適用
- 既に指定されているルールの適用範囲の拡張

Kaspersky Embedded Systems Security でサポートされるデバイスコントロールルールの最大数は 3072 です。

デバイスコントロールルールの説明を以下に記載します。

## ルールの種別

ルールの種別は常に［*許可*］です。既定では、デバイスが許可ルールの適用範囲に含まれていない場合、デバイスコントロールタスクにより、すべてのフラッシュドライブおよびその他の外部デバイスの接続がブロックされます。

## ルール有効化の条件とルールの適用範囲

デバイスコントロールルールでは、*デバイスインスタンスパス*に基づいてフラッシュドライブおよびその他の外部デバイスが識別されます。デバイスインスタンスパスは、デバイスが接続されて外部デバイスまたは CD / DVD ドライブ（たとえば、IDE または SCSI）として登録された時に、システムによってデバイスに割り当てられる一意の基準です。

Kaspersky Embedded Systems Security では、接続に使用されているバスには関係なく、CD / DVD ドライブの接続が制御されます。このようなデバイスを USB 経由でマウントする際には、オペレーティングシステムにより、外部デバイスおよび CD / DVD ドライブ（たとえば、IDE または SCSI）という 2 つのデバイスインスタンスのパス値が登録されます。このようなデバイスを正常に接続するには、インスタンスの各パス値に対して許可ルールを設定する必要があります。

Kaspersky Embedded Systems Security ではデバイスインスタンスパスが自動的に定義され、得られた値が次の要素に構文解析されます：

- デバイスの製造元（VID）
- デバイスコントローラーの種別（PID）
- デバイスのシリアルナンバー

デバイスインスタンスパスは手動では設定できません。許可ルールの有効化の条件では、ルールの適用範囲が定義されます。既定では、新しく作成されたルールの適用範囲には、Kaspersky Embedded Systems Security がルール作成の基準としてプロパティを参照した初期デバイスが 1 台含まれています。作成したルールの値を設定するには、ルールの適用範囲を拡張するマスクを使用します。

## 初期デバイス値

Kaspersky Embedded Systems Security で許可ルールの作成に使用され、接続されているデバイスごとに Windows デバイス マネージャーに表示されるデバイスプロパティ。

初期デバイス値には次の情報が含まれています：

- **デバイスインスタンスパス**：Kaspersky Embedded Systems Security は、このプロパティに基づいてルール有効化の条件を定義し、次のフィールドに記入します：［**製造元（VID）**］、［**コントローラーの種別（PID）**］、［**ルールのプロパティ**］ウィンドウの［**ルールの使用範囲**］セクションにある［**シリアルナンバー**］。
- **説明的名称**：製造元がデバイスのプロパティで設定するデバイスの説明的名称。

Kaspersky Embedded Systems Security では、ルールの作成時に初期デバイス値が自動的に定義されます。後でこれらの値を使用して、ルール作成の基本として使用されたデバイスを認識できます。初期デバイス値は編集できません。

## 説明

作成したデバイスコントロールルールごとに、［**説明**］で情報を追加できます。たとえば、接続されているフラッシュドライブの名前を記録したり、その所有者を定義したりできます。この説明は、［**デバイスコントロールルール**］ウィンドウの対応する図に表示されます。

説明と初期デバイス値はルール適用での使用は許可されず、ユーザーがデバイスを簡単に識別する目的のみで規定されます。

# デバイスコントロールルールの作成について

デバイスコントロールタスクまたはデバイスコントロールルールの自動作成タスクの実行時に自動的に作成された XML ファイルからデバイスコントロールの許可ルールをインポートできます。

既定では、Kaspersky Embedded Systems Security ではフラッシュドライブおよびその他の外部デバイスが、指定したデバイスコントロールルールの適用範囲に含まれていない場合、それらのドライブやデバイスの接続が制限されます。

デバイスコントロールルールの作成の対象とシナリオ

| ルール作成シナリオ | 対象 |
| --- | --- |
| デバイスコントロールルールの自動作成タスク | • デバイスコントロールタスクの初回開始前に、以前接続されていた信頼するデバイスに許可ルールを追加します。<br>• 保護対象デバイスネットワークで信頼されるデバイスのルールリストを生成します。 |
| システムデータに基づいてルールを作成 | データがシステムに格納されている 1 台以上の外部デバイスに許可ルールを追加します。 |
| 現在接続しているデバイスに関するデータに基づくルール作成 | 少数の新しい外部デバイスを信頼する必要がある際に、既に指定されているルールリストを更新します。 |
| **統計のみ**モードのデバイスコントロールタスク | 大量の信頼するデバイスの許可ルールを生成します。 |

## デバイスコントロールルールの自動作成タスクの使用

デバイスコントロールルールの自動作成タスクの完了時に作成された XML ファイルには、システムレジストリにデータが格納されているフラッシュドライブおよびその他の外部デバイスの許可ルールが含まれています。

すべてのネットワークの保護対象デバイス上のシステムによって登録されている、これまでに接続したすべての外部デバイスを考慮に入れる場合、または、すべてのネットワーク保護対象デバイスに現在接続されているデバイスに関するデータのみを考慮する場合は、ルール作成プロセス時にこのシナリオを使用します。また、タスクでは、タスク実行時に接続されているすべての外部デバイスが考慮されます。グループタスク完了時に、Kaspersky Embedded Systems Security は、ネットワーク内で登録されているすべて外部デバイスの許可ルールリストを作成し、そのリストを、指定したフォルダーに XML ファイルとして保存します。これで、作成されたルールをデバイスコントロールタスク設定に手動でインポートできます。保護対象デバイスのタスクと異なり、ポリシーでは、デバイスコントロールルールの自動作成グループタスク完了時に、作成したルールをデバイスコントロールルールのリストに自動で追加する設定はできません。

デバイスコントロールタスクの初回開始前に許可ルールリストを作成する場合はこのシナリオを使用し、作成した許可ルールにより保護対象デバイスで使用されているすべての信頼する外部デバイスに対応するようにしてください。

## 接続されているすべてのデバイスに関するシステムデータの使用

タスクの実行時に、Kaspersky Embedded Systems Security では保護対象デバイスに以前接続されていたことがあるまたは現在接続されているすべての外部デバイスに関するシステムデータが受信され、［**システム情報に基づいてルールを生成する**］ウィンドウのリストに検知されたデバイスが表示されます。

Kaspersky Embedded Systems Security では、検知された各デバイスの製造元（VID）、コントローラーの種別（PID）、説明的名称、シリアルナンバー、およびデバイスインスタンスパスが構文解析されます。システムにデータが格納されている外部デバイスの許可ルールを作成し、デバイスコントロールのルールリストに新しく作成されたルールを追加できます。

このシナリオでは、Kaspersky Embedded Systems Security は、Kaspersky Security Center がインストールされている保護対象デバイスにこれまでに接続されたか現在接続されている外部デバイスのための許可ルールを作成します。

少数の新しい外部デバイスを信頼する必要がある際に、既に指定されているルールリストを更新する場合はこのシナリオを使用してください。

### 現在接続しているデバイスに関するデータの使用

このシナリオでは、Kaspersky Embedded Systems Security は現在接続している外部デバイスのみを対象とする許可ルールを作成します。許可ルールを作成する 1 つ以上の外部デバイスを選択できます。

### 統計のみモードのデバイスコントロールタスクの使用

**統計のみ**モードのデバイスコントロールタスクの完了時に受信した XML ファイルは、実行ログに基づいて作成されます。

タスクの実行時に、Kaspersky Embedded Systems Security では保護対象デバイスに接続されたすべてのフラッシュドライブおよびその他の外部デバイスに関する情報が記録されます。タスクのイベントに基づいて許可ルールを作成し、XML ファイルにエクスポートすることができます。［**統計のみ**］モードでタスクを開始する前にタスク実行期間を設定し、指定した期間中に保護対象デバイスにすべての使用可能なデバイスが接続されるようにしてください。

大量の新しい外部デバイスを許可する必要があり、既に生成されているルールリストを更新する場合は、このシナリオを使用してください。

テンプレートマシンでこのシナリオに従ってルールリストを作成する場合は、Kaspersky Security Center でデバイスコントロールタスクを設定する際に、作成された許可ルールリストを適用できます。この方法により、すべての保護対象デバイスでテンプレートマシンに接続されている外部デバイスの使用を許可できます。

## デバイスコントロールルールの自動作成タスクについて

デバイスコントロールルールの自動作成では、保護対象デバイスに以前接続されていたことがあるすべての外部デバイスに関するシステムデータに基づいて、接続されているフラッシュドライブおよびその他の外部デバイスの許可ルールのリストを自動的に作成できます。

デバイスコントロールルールの自動作成設定に応じて、タスクの完了時に、検知されたすべての外部デバイスの許可ルールリストを含む XML 設定ファイルが作成されるかあるいはデバイスコントロールタスクに作成されたルールが直接追加されます。自動的に生成された許可ルールでデバイスが許可されます。

タスクで作成されて追加されたルールは、［**デバイスコントロールルール**］ウィンドウに表示されます。

# デバイスコントロールの既定のタスク設定

デバイスコントロールタスクでは、次の表の既定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。

既定のデバイスコントロールタスクの設定

| 設定 | 既定値 | 説明 |
| --- | --- | --- |
| **タスクモード** | **統計のみ** | 指定したルールに従ってブロックまたは許可された外部デバイスに関するタスク実行ログ情報。外部デバイスは実際にはブロックされません。<br>外部デバイスの使用を実際にブロックするには、デバイス保護として［**処理を実行**］モードを選択します。 |
| **デバイスコントロールタスクが実行されていない時にすべての外部デバイスの使用を許可する** | オフ | Kaspersky Embedded Systems Security ではデバイスコントロールタスクの状態に関係なく、外部デバイスの使用がブロックされます。これにより、外部デバイスとファイルを交換する際に発生するコンピューターのセキュリティ脅威に対して、最大の保護レベルが実現されます。<br>デバイスコントロールタスクが実行されていない時に、Kaspersky Embedded Systems Security がすべての外部デバイスの使用を許可するように設定を編集できます。 |
| タスク開始スケジュール | 最初の実行がスケジュール設定されていません。 | デバイスコントロールタスクは、Kaspersky Embedded Systems Security の起動時に自動的には開始されません。<br>この場合、タスク開始スケジュールを設定できます。 |

デバイスコントロールルールの自動作成タスクの既定の設定

| 設定 | 既定値 | 説明 |
| --- | --- | --- |
| **タスクモード** | **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** | タスクの処理モード。<br>［**現在接続している外部デバイスだけを考慮する**］タスクモードを選択できます。 |
| タスク完了後の処理 | 処理は実行されません。 | ルールを結合しないで既存のルールに追加して重複したルールを削除しないようにしたり、既存のルールを新しい許可ルールに置き換えたりすることができます。許可ルールのファイルへのエクスポートを設定することも可能です。 |
| タスク開始スケジュール | 最初の実行がスケジュール設定されていません。 | デバイスコントロールルールの自動作成タスクは、Kaspersky Embedded Systems Security の起動時に自動的には開始されません。タスクは手動で開始するか、開始スケジュールを設定することもできます。 |

# 管理プラグインからデバイスコントロールを管理する

このセクションでは、管理プラグインインターフェイスを操作し、保護対象デバイスのグループに対して Kaspersky Security Center を介してルールのリストを作成することによって、ネットワーク上のすべての保護対象デバイスへの外部デバイスの接続を管理する方法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。

## デバイスコントロールタスクのポリシーの設定ウィンドウ

*Kaspersky Security Center のポリシーからデバイスコントロールタスクの設定を開くには：*

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. 表示されたポリシーのプロパティウィンドウで、［**ローカル活動の管理**］セクションを選択します。
6. ［**デバイスコントロール**］サブセクションの［**設定**］をクリックします。
   ［**デバイスコントロール**］ウィンドウが開きます。
7. 必要に応じてポリシーを設定します。

## デバイスコントロールルールのリスト

*Kaspersky Security Center からデバイスコントロールルールのリストを開くには：*

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. 表示されたポリシーのプロパティウィンドウで、［**ローカル活動の管理**］セクションを選択します。
6. ［**デバイスコントロール**］サブセクションの［**設定**］をクリックします。
   ［**デバイスコントロール**］ウィンドウが開きます。
7. ［**全般**］タブで、［**ルールリスト**］をクリックします。
   ［**デバイスコントロールルール**］ウィンドウが開きます。

8. 必要に応じてポリシーを設定します。

## デバイスコントロールルールの自動作成タスクのウィザードとプロパティウィンドウ

*デバイスコントロールルールの自動作成タスクの作成を初期化するには：*

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. タスクを設定する管理グループを選択します。
3. ［**タスク**］タブを選択します。
4. ［**タスクの作成**］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. ［**デバイスコントロールルールの自動生成**］タスクを選択します。
6. ［**次へ**］をクリックします。
   ［**設定**］ウィンドウが開きます。

*既存のデバイスコントロールルールの自動作成タスクの設定を編集するには：*

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. タスクを設定する管理グループを選択します。
3. ［**タスク**］タブを選択します。
4. 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。
   **デバイスコントロールルールの自動生成**の**プロパティ**ウィンドウが開きます。

タスクの設定に関する詳細は、セクション「デバイスコントロールルールの自動作成タスクの設定」を参照してください。

## デバイスコントロールタスクの設定

*デバイスコントロールタスクの設定を行うには：*

1. ［**デバイスコントロール**］ウィンドウを開きます。
2. ［**全般**］タブで、次のタスク設定を行います：
   - ［**タスクモード**］セクションで、次のいずれかのタスクモードを選択します：
     - **処理を実行**：

デバイスコントロールタスクが［処理を実行］モードで実行される前に、信頼しないと判断される外部デバイスが保護対象デバイスに接続されていた場合、そのデバイスは製品によってブロックされません。信頼しないデバイスを手動で切断するか、保護対象デバイスを再起動してください。そうしない場合、このデバイスに「既定で拒否」の原則は適用されません。

- **統計のみ**：

- ［**デバイスコントロールタスクが実行されていない時にすべての外部デバイスの使用を許可する**］をオンまたはオフにします。

3. デバイスコントロールルールのリストを編集するには、［**ルールリスト**］をクリックします。

4. 必要に応じて、［**タスク管理**］タブでタスク開始スケジュールを設定します。

5. ［**デバイスコントロール**］ウィンドウで、［OK］をクリックします。

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。

## デバイスコントロールルールの自動作成タスクの設定

*デバイスコントロールルールの自動作成タスクを設定するには：*

1. **デバイスコントロールルールの自動生成**の**プロパティ**ウィンドウを開きます。

2. ［**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。

3. ［**設定**］セクションでは、次の設定を行うことができます：

- 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、設定ファイルを設定します。

4. ［**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（定義データベース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）。

5. ［**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。

6. 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。

7. 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。

## デバイスコントロールルールの Kaspersky Security Center からの設定

さまざまな条件に基づいてルールのリストを生成する方法、またはデバイスコントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法について説明します。

## Kaspersky Security Center ポリシーでのシステムデータに基づく許可ルールの作成

*デバイスコントロールタスクの［**システムデータに基づいてルールを作成**］オプションを使用して許可ルールを指定するには：*

1. 必要に応じて、信頼する外部デバイスを、Kaspersky Security Center 管理コンソールがインストールされた保護対象デバイスに接続します。
2. ［**デバイスコントロールルール**］ウィンドウを開きます。
3. ［**追加**］をクリックし、表示されたコンテキストメニューで、［**システムデータに基づいてルールを作成**］オプションを選択します。
4. ［**システム情報に基づいてルールを生成する**］ウィンドウのデバイスリストで、デバイスを選択します。
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. ［**デバイスコントロールルール**］ウィンドウで、［**保存**］をクリックします。

デバイスコントロールタスクのルールリストには、Kaspersky Security Center 管理コンソールがインストールされた保護対象デバイスのシステムデータに基づいて生成される新しいルールが反映されます。

## 接続しているデバイスのためのルール作成

*デバイスコントロールタスクの［**接続したデバイスに基づいてルールを作成**］オプションを使用して許可ルールを指定するには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。
2. ［**追加**］をクリックし、コンテキストメニューで［**接続したデバイスに基づいてルールを作成**］を選択します。

   ［**システム情報に基づいてルールを生成する**］ウィンドウが開きます。
3. 保護対象デバイスに接続されている検知されたデバイスのリストで、許可ルールを作成するデバイスを選択します。
4. ［**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。
5. ［**デバイスコントロールルール**］ウィンドウで、［**保存**］をクリックします。

デバイスコントロールタスクのルールリストには、Kaspersky Security Center 管理コンソールがインストールされた保護対象デバイスのシステムデータに基づいて生成される新しいルールが反映されます。

## ブロックされたデバイスに関する Kaspersky Security Center のレポートからのルールのインポート

**統計のみ**モードでデバイスコントロールタスクを実行後、Kaspersky Security Center で生成されるレポートからブロックされたデバイスの接続のデータをインポートできます。そのデータを使用して、設定中のポリシーでデバイスコントロールの許可ルールのリストを生成できます。

デバイスコントロールタスクの実行中に発生したイベントのレポートの生成時に、接続が制限されたデバイスを確認することができます。

*ブロックされたデバイスに関する Kaspersky Security Center レポートに基づいて、保護対象デバイスのグループに対してデバイス接続のための許可ルールを指定するには：*

1. ポリシーのプロパティの［**イベント通知**］セクションで、次の内容を確認します：
   - 重要度が［**緊急イベント**］のイベントに対して、［*信頼しない外部デバイスが検出および制限されました*］イベントの実行ログを保存する期間が、［**統計のみ**］モードのタスクの実行で計画された期間を超えている（既定値は 30 日）。
   - 重要度が［**警告**］のイベントに対して、［*統計のみ：信頼しない外部デバイスが検出されました*］イベントの実行ログを保存する期間が、［**統計のみ**］モードのタスクの実行で予定された期間を超えている（既定値は 30 日）。

   イベントの保管期間が経過すると、記録されたイベントに関する情報が削除され、レポートファイルに反映されません。**統計のみ**モードでデバイスコントロールタスクを実行する前に、タスクの実行時間が、指定のイベントに対して設定されている保管時間を超えていないことを確認してください。
2. **統計のみ**モードのデバイスコントロールタスクを開始します。
   a. Kaspersky Security Center の［**管理サーバー**］フォルダーの作業領域で、［**イベント**］タブを選択します。
   b. ［**抽出の作成**］をクリックし、［*信頼しない外部デバイスが検出および制限されました*］の基準に基づいてベントの抽出を作成し、デバイスコントロールタスクによって接続が制限されるデバイスを表示します。
   c. ［インポート / エクスポート］ドロップダウンリストで、［**イベントをファイルにエクスポート**］をクリックして、制限された接続のレポートを TXT ファイルに保存します。

   生成したレポートとポリシーにインポートして適用する前に、レポートには接続を許可するデバイスのデータしか含まれていないことを確認してください。
3. 制限されたデバイス接続に関するデータをデバイスコントロールタスクにインポートします：
   a. ［**デバイスコントロールルール**］ウィンドウを開きます。
   b. ［**追加**］をクリックし、コンテキストメニューで［**Kaspersky Security Center のレポートから、ブロック対象デバイスのデータをインポート**］を選択します。

c. Kaspersky Security Center のレポートを基に作成されたリストから以前設定されたデバイスコントロールルールのリストにルールを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。

d. 表示される Microsoft Windows の標準のウィンドウで、制限されたデバイスについてのレポートから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。

e. ［**デバイスコントロールルール**］ウィンドウで、［**保存**］をクリックします。

4. ［**デバイスコントロール**］ウィンドウで、［OK］をクリックします。

制限されたデバイスに関する Kaspersky Security Center のレポートに従って作成されたルールが、デバイスコントロールルールのリストに追加されます。

## デバイスコントロールルールの自動作成タスクを使用したルールの作成

*デバイスコントロールルールの自動作成タスクを使用して保護対象デバイスのグループのためのデバイスコントロールルールを指定するには：*

1. ［新規タスクウィザード］で、［**設定**］ウィンドウを開きます。
2. 以下を設定します：
   - ［**モード**］セクション：
     - **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**
     - **現在接続している外部デバイスだけを考慮する**
   - ［**タスク完了後**］セクション：
     - **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**
     - **追加方法**
     - **許可ルールをファイルにエクスポートする**
     - **ファイル名に保護対象デバイスの詳細を追加する**
3. ［次へ］をクリックします。
4. ［**スケジュール**］ウィンドウで、タスクの開始スケジュールを設定します。
5. ［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、使用するアカウントを指定します。

7. ［次へ］をクリックします。

8. タスク名を指定します。

9. ［次へ］をクリックします。

   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。

   ［タスクの作成を終了］ウィンドウが開きます。

10. オプションで［ウィザード完了後にタスクを実行する］をオンにすると、ウィザードの終了後にタスクを実行することができます。

11. ［完了］をクリックしてタスクの作成を終了します。

12. 設定中の保護対象デバイスグループの作業領域にある、［タスク］タブのグループタスクのリストで、作成したデバイスコントロールルールの自動作成タスクを選択します。

13. ［開始］をクリックして、タスクを開始します。

    タスクが完了すると、自動で生成された許可ルールのリストは XML ファイルとして共有フォルダーに保存されます。

    ネットワークでデバイスコントロールポリシーを使用する前に、すべての保護対象デバイスがネットワーク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ネットワーク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上、またはテンプレートマシン上で保護対象デバイスコントロールのルール生成タスクを開始してください。

## デバイスコントロールルールのリストに生成されたルールを追加する

*生成された許可ルールのリストをデバイスコントロールタスクに追加するには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。

2. ［**追加**］をクリックします。

3. ［**追加**］をクリックし、コンテキストメニューで［**XML ファイルからルールをインポート**］を選択します。

4. 自動で生成された許可ルールを以前作成されたデバイス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。

5. 表示される Microsoft Windows の標準のウィンドウで、デバイスコントロールルールの自動作成グループタスクの完了後に作成される XML ファイルを選択します。

6. ［ファイルを開く］をクリックします。

   XML ファイルから生成されたすべてのルールは、選択した方法に応じてリストに追加されます。

7. ［**デバイスコントロールルール**］ウィンドウで、［**保存**］をクリックします。

8. 作成したデバイスコントロールルールを適用する場合、ポリシー設定の［ローカルアクティビティの管理］セクションの［**デバイスコントロール**］の設定で［**処理を実行**］タスクモードを選択します。

各保護対象デバイス上のシステムデータに基づいて自動で生成される許可ルールは、設定中のポリシーの範囲となっているすべてのネットワークの保護対象デバイスに適用されます。これらの保護対象デバイスでは、許可ルールが作成されたデバイスに対してのみ接続が許可されます。

# アプリケーションコンソールからデバイスコントロールを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、保護デバイスのタスクの設定を行う方法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。

## デバイスコントロールタスクの設定ウィンドウ

*アプリケーションコンソールからデバイスコントロールタスクの設定を開くには：*

1. アプリケーションコンソールツリーで、［**コンピューターの管理**］フォルダーを展開します。

2. ［**デバイスコントロール**］サブフォルダーを選択します。

3. ［**デバイスコントロール**］サブフォルダーの詳細ペインで、［**プロパティ**］をクリックします。
   ［**タスクの設定**］ウィンドウが表示されます。

4. 必要に応じてタスクを設定します。

## デバイスコントロールルールの設定ウィンドウ

*アプリケーションコンソールからデバイスコントロールルールのリストを開くには：*

1. アプリケーションコンソールツリーで、［**コンピューターの管理**］フォルダーを展開します。

2. ［**デバイスコントロール**］サブフォルダーを選択します。

3. ［**デバイスコントロール**］フォルダーの結果ペインで、［**デバイスコントロールルール**］をクリックします。
   ［**デバイスコントロールルール**］ウィンドウが開きます。

4. 必要に応じてルールリストを設定します。

## デバイスコントロールルールの自動作成タスクの設定ウィンドウ

*デバイスコントロールルールの自動作成タスクを設定するには：*

1. アプリケーションコンソールツリーで、［**ルールの自動生成**］フォルダーを展開します。

2. ［**デバイスコントロールルールの自動生成**］サブフォルダーを選択します。

3. ［**デバイスコントロールルールの自動生成**］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。
   ［**タスクの設定**］ウィンドウが表示されます。

4. 必要に応じてタスクを設定します。

## デバイスコントロールタスクの設定

*デバイスコントロールタスクの設定を行うには：*

1. ［**タスクの設定**］ウィンドウを開きます。

2. ［**全般**］タブで、次のタスク設定を行います：

   - ［**タスクモード**］セクションで、次のいずれかのタスクモードを選択します：

     - 処理を実行：

       デバイスコントロールタスクが［処理を実行］モードで実行される前に、信頼しないと判断される外部デバイスが保護対象デバイスに接続されていた場合、そのデバイスは製品によってブロックされません。信頼しないデバイスを手動で切断するか、保護対象デバイスを再起動してください。そうしない場合、このデバイスに「既定で拒否」の原則は適用されません。

     - **統計のみ**：

   - ［**デバイスコントロールタスクが実行されていない時にすべての外部デバイスの使用を許可する**］をオンまたはオフにします。

3. 必要に応じて、［**スケジュール**］タブと［**詳細設定**］タブでタスクの開始スケジュールを設定します。

4. デバイスコントロールルールのリストを編集するには、［**デバイスコントロール**］フォルダーの結果ペインの下部にある［**デバイスコントロールルール**］をクリックします。

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。

# デバイスコントロールルールの設定

ルールのリストを生成やインポート / エクスポートする方法、またはデバイスコントロールタスクを使用して許可ルールや拒否ルールを手動で作成する方法について説明します。

## XML ファイルからのデバイスコントロールルールのインポート

*デバイスコントロールルールをインポートするには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。
2. ［**追加**］をクリックします。
3. 表示されるコンテキストメニューで、［**XML ファイルからルールをインポート**］を選択します。
4. インポートされるルールを追加する方法を指定します。そのためには、［**XML ファイルからルールをインポート**］のコンテキストメニューからいずれかのオプションを選択します：
   - **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。

   Microsoft Windows 標準の［**ファイルを開く**］ウィンドウが表示されます。
5. ［**ファイルを開く**］ウィンドウで、［デバイスコントロールルール］の設定を含む XML ファイルを選択します。
6. ［**開く**］をクリックします。

［**デバイスコントロールルール**］ウィンドウのリストに、インポートされたルールが表示されます。

## デバイスコントロールタスクイベントに基づいたルールリストの入力

*デバイスコントロールルールのリストが含まれている設定ファイルを、デバイスコントロールタスクイベントに基づいて作成するには：*

1. デバイスコントロールタスクを［**統計のみ**］モードで開始し、保護対象デバイスに接続されているフラッシュドライブおよびその他の外部デバイスのすべてのイベントを記録します。
2. **統計のみ**モードで実行したタスクの完了後、［**デバイスコントロール**］フォルダーの結果ペインの［**管理**］セクションにある［**実行ログを開く**］をクリックして、実行ログを開きます。
3. ［**ログ**］ウィンドウで、［**イベントに基づいてルールを作成する**］をクリックします。

**統計のみ**モードのデバイスコントロールタスクで発生したイベントに基づくルールリストを含んだ XML 設定ファイルが作成されます。このリストはデバイスコントロールタスクで適用できます。

タスクイベントに基づいて作成されたルールリストを適用する前に、このルールリストを確認してから手動で処理し、指定されたルールで許可された信頼しないデバイスが存在しないことを確認してください。

アプリケーションでは、タスクイベントにより XML ファイルをルールリストに変換する際に、登録されたすべてのイベントの許可ルール（デバイスの制限を含む）が作成されます。

すべてのタスクイベントが、タスクモードに関係なくタスク実行ログに登録されます。**処理を実行**モードで実行したタスクで発生したイベントに基づくルールリストを含んだ設定ファイルが作成されます。タスクが適切に動作するには、タスクが「処理を実行」モードで実行される前にルールリストの最終バージョンを作成しておく必要があります。そのため、緊急の場合を除いてこのシナリオは推奨されません。

## 1 台以上の外部デバイスへの許可ルールの追加

デバイスコントロールタスクでは、ルールを 1 つずつ手動で追加する機能はサポートされていません。ただし、1 台以上の新しい外部デバイスにルールを追加する必要がある場合は、［**システムデータに基づいてルールを作成**］を使用できます。このシナリオを適用すると、アプリケーションでは以前接続されていたすべての外部デバイスに関する Windows データが使用され、現在接続されているデバイスに対しても許可ルールリストを入力できます。

*現在接続されている 1 台以上の外部デバイスに許可ルールを追加するには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。
2. ［**追加**］をクリックします。
3. 表示されたコンテキストメニューで、［**システムデータに基づいてルールを作成**］をオンにします。
4. 表示されたウィンドウで検知されたデバイスのリストを確認し、保護対象デバイスで信頼する 1 台以上のデバイスを選択します。
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。

新しいルールが作成され、デバイスコントロールルールのリストに追加されます。

## デバイスコントロールルールの削除

*デバイスコントロールルールを削除するには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。
2. リストで削除するルールを 1 つ以上選択します。
3. ［**選択項目の削除**］をクリックします。
4. ［**保存**］をクリックします。

選択したデバイスコントロールルールが削除されます。

## デバイスコントロールルールのエクスポート

*デバイスコントロールルールを設定ファイルにエクスポートするには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。
2. ［**ファイルにエクスポート**］をクリックします。
   Microsoft Windows 標準のウィンドウが表示されます。
3. 表示されたウィンドウで、ルールをエクスポートするファイルを指定します。ファイルが存在しない場合は作成されます。指定した名前のファイルが既に存在する場合、ルールをエクスポートするとファイルの内容が書き換えられます。
4. ［**保存**］をクリックします。

ルールとその設定が指定されたファイルにエクスポートされます。

## デバイスコントロールルールのアクティベートとアクティベート解除

作成したデバイスコントロールルールは、削除しなくてもアクティベートおよびアクティベート解除できます。

*作成したデバイスコントロールのルールをアクティベートまたはアクティベート解除するには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。
2. 指定したルールのリストで、プロパティを設定するルールをダブルクリックして［**ルールのプロパティ**］ウィンドウを開きます。
3. 表示されたウィンドウで、［**ルールを適用する**］をオンまたはオフにします。
4. ［**OK**］をクリックします。

ルールの適用ステータスが保存され、指定したルールに表示されます。

## デバイスコントロールルールの適用範囲の拡張

自動作成された各デバイスコントロールルールが対応しているのは、1台の外部デバイスのみです。ルールの適用範囲を手動で拡張するには、指定したルールのプロパティでデバイスインスタンスパスのマスクを設定します。

デバイスインスタンスパスのマスクを適用すると、指定するルールの合計数を減らすことができ、ルールの処理の複雑さを低減できます。ただし、ルールの適用範囲を拡張すると、外部デバイスの制御効率が低下する可能性があります。

*デバイスコントロールルールのプロパティでデバイスインスタンスパスのマスクを適用するには：*

1. ［**デバイスコントロールルール**］ウィンドウを開きます。

2. 表示されたウィンドウでルールを選択し、マスク適用でそのプロパティを使用します。

3. 選択したデバイスコントロールルールをダブルクリックして、［**ルールのプロパティ**］ウィンドウを開きます。

4. 表示されたウィンドウで、次の操作を行います：

   - 選択したルールにより、デバイスの製造元とコントローラーの種別で指定された情報に適合するすべての外部デバイスへの接続を許可する場合は、［**コントローラーの種別（PID）**］の横にある［**マスクを使用**］をオンにします。

   - 選択したルールにより、デバイスの製造元とデバイスのシリアルナンバーで指定された情報に適合するすべての外部デバイスへの接続を許可する場合は、［**シリアルナンバー**］の横にある［**マスクを使用**］をオンにします。

   - 選択したルールにより、デバイスの製造元、およびコントローラーの種別とデバイスのシリアルナンバーの両方で指定された情報に適合するすべての外部デバイスへの接続を許可する場合は、［**コントローラーの種別（PID）**］および［**シリアルナンバー**］の横にある［**マスクを使用**］をオンにします。

   1つ以上のフィールドで［**マスクを使用**］をオンにすると、チェックボックスがオンのフィールドのデータが「*」記号で置き換えられ、ルールの適用時に考慮されなくなります。

5. 必要に応じて、ルールに関する追加情報を［**説明**］に入力します。たとえば、ルールによって影響を受けるデバイスの情報を入力します。

6. ［**OK**］をクリックします。

新しく設定されたルールのプロパティが保存されます。ルールの適用範囲は、指定されたデバイスインスタンスパスのマスクに従って拡張されます。

## デバイスコントロールルールの自動作成タスクの設定

*デバイスコントロールルールの自動作成タスクを設定するには：*

1. アプリケーションコンソールツリーで、［**ルールの自動生成**］フォルダーを展開します。

2. ［**デバイスコントロールルールの自動生成**］サブフォルダーを選択します。

3. ［**デバイスコントロールルールの自動生成**］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。

   ［**タスクの設定**］ウィンドウが表示されます。

4. ［**全般**］タブの［**タスクモード**］セクションで、タスクの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**

   - **現在接続している外部デバイスだけを考慮する**

5. ［**タスク完了後**］セクションで、タスクの完了時に Kaspersky Embedded Systems Security が実行する処理を指定します：

   - **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**

   - **追加方法**

- **許可ルールをファイルにエクスポートする**
- **ファイル名に保護対象デバイスの詳細を追加する**

6. ［**スケジュール**］タブと［**詳細設定**］タブで、タスクの開始スケジュールを設定します。
7. ［**タスクの設定**］ウィンドウで［OK］をクリックします。

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。

## アプリケーションコンソール Web プラグインからデバイスコントロールを管理する

このセクションでは、Web プラグインコンソールインターフェイスを操作して、保護デバイスのタスクの設定を行う方法について説明します。

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**ローカル活動の管理**］セクションを選択します。
5. ［**デバイスコントロール**］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。

デバイスコントロールタスクの設定

| 設定 | 説明 |
| --- | --- |
| **処理を実行** | Kaspersky Embedded Systems Security ではリムーバブルドライブやその他の外部デバイスの接続を制御するためにいくつかのルールが適用され、「既定で拒否」の原則と個別に指定した許可ルールに従って、各デバイスの使用が許可またはブロックされます。信頼する外部デバイスの使用は許可されます。信頼しない外部デバイスの使用は既定でブロックされます。 |
| **統計のみ** | Kaspersky Embedded Systems Security ではリムーバブルドライブやその他の外部デバイスの接続は制御されず、保護対象デバイス上での外部デバイスの接続と登録に関する情報、および接続されたデバイスによって適用されるデバイスコントロールの許可ルールに関する情報が記録されるのみです。すべての外部デバイスの使用が許可されます。既定ではこのモードが設定されています。 |
| **デバイスコントロールタスクが実行されていない時にすべての外部デバイスの使用を許可する** | このチェックボックスにより、デバイスコントロールタスクが実行されていない時に外部デバイスの使用が許可またはブロックされます。<br>このチェックボックスがオンにされており、デバイスコントロールタスクが実行されていない場合、保護対象デバイス上のすべての外部デバイスの使用が許可されます。<br>このチェックボックスがオフにされており、デバイスコントロールタスクが実行されていない、あるいは Kaspersky Security サービスがオフの場合、保護対象デバイス上の信頼しない外部デバイスの使用がブロックされます。これにより、外部デバイスとファイルを交換する際に発生するコンピューターのセキュリティ脅威に対して、最大の保護レベルが実現されます。<br>既定では、このチェックボックスはオフです。 |

| | |
|---|---|
| **デバイスコントロールのルール** | デバイスコントロールルールのリストを編集できます。 |
| タスク管理 | スケジュールでタスクを開始する設定を指定できます。 |

# ファイアウォール管理

このセクションでは、ファイアウォール管理タスクとその設定方法について説明します。

## ファイアウォール管理タスクについて

Kaspersky Embedded Systems Security は、ファイアウォール管理タスクを使用してネットワーク接続を保護するための信頼性と利便性にすぐれたソリューションを提供します。

ファイアウォール管理タスクは独立したネットワークトラフィックフィルタリングを実行しませんが、Kaspersky Embedded Systems Security グラフィックインターフェイスを介して Windows ファイアウォールを管理できます。ファイアウォール管理タスク時に Kaspersky Embedded Systems Security はオペレーティングシステムのファイアウォールの設定およびポリシーの管理を引き継ぎ、外部からファイアウォールを設定しようとする試行をすべてブロックします。

アプリケーションのインストール時にファイアウォール管理は、Windows ファイアウォールステータスと指定されたすべてのルールを読み取ってコピーします。その後、Kaspersky Embedded Systems Security ではルールとルールパラメータのセットのみが変更可能で、ファイアウォールはオンまたはオフにできるだけです。

Windows ファイアウォールが Kaspersky Embedded Systems Security のインストール時にオフにされた場合、インストールの完了後にファイアウォール管理タスクは実行されません。アプリケーションのインストール時に Windows ファイアウォールをオンにした場合、インストールが完了すると、ファイアウォール管理タスクが実行され、指定したルールによって許可されないすべてのネットワーク接続をブロックします。

ファイアウォール管理は既定でインストールされません。推奨インストールのコンポーネントセットに含まれていないためです。

ファイアウォール管理タスクは、タスクの指定したルールによって許可されないすべての送受信接続を強制的にブロックします。

タスクは定期的に Windows ファイアウォールをポーリングしてステータスを監視します。既定のポーリング間隔は 1分に設定されており、変更できません。Kaspersky Embedded Systems Security が Windows ファイアウォール設定とファイアウォール管理タスク設定の不一致を検知すると、オペレーティングシステムファイアウォールにタスク設定が強制的に適用されます。

Windows Firewall を 1分ごとにポーリングすることで、Kaspersky Embedded Systems Security は次を監視します：

- Windows ファイアウォールの動作状況。
- Kaspersky Embedded Systems Security のインストール後に他のアプリケーションまたはツールによって追加されたルールのステータス（たとえば、wf.msc を使用したポートやアプリケーションのための新しいアプリケーションルールの追加）。

Windows ファイアウォールに新しいルールを適用すると、Kaspersky Embedded Systems Security は［Windows ファイアウォール］スナップインに設定される Kaspersky Security グループルールを作成します。このルールセットには、ファイアウォール管理タスクを使用して Kaspersky Embedded Systems Security によって作成されるルールがすべて含まれます。Kaspersky Security グループルールは、ポーリング時にはアプリケーションにより監視されず、ファイアウォール管理タスク設定で指定されたルールのリストに自動的には同期しません。

*手動で Kaspersky Security グループルールをアップデートするには：*

Kaspersky Embedded Systems Security ファイアウォール管理タスクを再起動します。

Windows ファイアウォールスナップインを手動で使用して Kaspersky Security グループルールを編集することもできます。

Windows ファイアウォールが Kaspersky Security Center グループポリシーによって管理されている場合、ファイアウォール管理タスクは開始できません。

## ファイアウォールのルールについて

ファイアウォール管理タスクは、タスク実行時に Windows ファイアウォールに強制的に適用される許可ルールを使用して送受信ネットワークトラフィックのフィルタリングを管理します。

タスクが初めて開始された時に、Kaspersky Embedded Systems Security は Windows ファイアウォール設定で指定されたすべての着信ネットワークトラフィックルールを読み取ってファイアウォール管理タスク設定にコピーします。続いて、アプリケーションは次のルールに従って動作します：

- Windows ファイアウォール設定に新しいルールが作成された場合（手動で、または新しいアプリケーションのインストール時に自動的に）、Kaspersky Embedded Systems Security はそのルールを削除します。
- Windows ファイアウォール設定から既存のルールが削除された場合、タスクが再起動された時に Kaspersky Embedded Systems Security はそのルールを復元します。
- Windows ファイアウォール設定で既存のルールのパラメータが変更された場合、Kaspersky Embedded Systems Security はその変更をロールバックします。
- ファイアウォール管理設定に新しいルールが作成された場合、Kaspersky Embedded Systems Security は Windows ファイアウォールにルールを強制的に適用します。
- ファイアウォール管理設定から既存のルールが削除された場合、Kaspersky Embedded Systems Security は Windows ファイアウォール設定からルールを強制的に削除します。

Kaspersky Embedded Systems Security は、送信ネットワークトラフィックを管理するブロックルールを使用しません。ファイアウォール管理タスクの開始時に、Kaspersky Embedded Systems Security は Windows ファイアウォール設定からそのようなルールをすべて削除します。

着信ネットワークトラフィックのフィルタリングルールを設定、削除、編集することはできます。

ファイアウォール管理タスク設定に新しいルールを指定して送信ネットワークトラフィックを管理することはできません。Kaspersky Embedded Systems Security で指定されているすべてのファイアウォールルールは、着信ネットワークトラフィックのみを管理します。

アプリケーションやポートを対象とするさまざまな種別のファイアウォールのルールを管理できます。

### アプリケーションルール

この種のルールは、指定したアプリケーションを標的とするネットワーク接続を許可します。これらのルールの有効化の条件は、実行ファイルへのパスに基づきます。

アプリケーションルールは管理できます：

- ルールの追加
- 既存のルールの削除
- 指定したルールの有効化と無効化
- 指定したルールのパラメータの編集：ルール名、実行ファイルへのパス、およびルール使用範囲の指定

### ポートルール

この種のルールは、指定したポートおよびプロトコル（TCP/UDP）によるネットワーク接続を許可します。これらのルールの有効化の条件は、ポート番号およびプロトコルの種別に基づきます。

ポートルールは管理できます：

- ルールの追加
- 既存のルールの削除
- 指定したルールの有効化と無効化
- 指定したルールのパラメータの編集：ルール名、ポート番号、プロトコルの種別、およびルールの適用範囲の設定

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、保護対象デバイスのセキュリティレベルは低下します。

## ファイアウォール管理タスクの既定の設定

ファイアウォール管理タスクでは、次の表の既定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。

ファイアウォール管理タスクの既定の設定

| 設定 | 既定値 | 説明 |
| --- | --- | --- |
| アプリケーションを対象とするファイアウォールのルール | アプリケーションを対象とする 2 つの既定のルールが有効です | 既定のルールを無効にしたり、新しいツールを追加できます。 |
| ポートを対象とするファイアウォールのルール | ポートを対象とする 6 つの既定のルールが有効です | 既定のルールを無効にしたり、新しいツールを追加できます。 |
| タスク開始スケジュール | 最初の実行がスケジュール設定されていません。 | ファイアウォール管理タスクは、Kaspersky Embedded Systems Security の起動時に自動的には開始されません。<br>この場合、タスク開始スケジュールを設定できます。 |

# 管理プラグインからファイアウォールのルールを管理する

このセクションでは、管理プラグインインターフェイスからファイアウォールのルールを管理する方法について説明します。

## ファイアウォールのルールの有効化と無効化

*着信ネットワークトラフィックをフィルタリングする既存のルールを有効または無効にするには、次の処理を実行します：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**ネットワーク活動の管理**］セクションで、［**ファイアウォール管理**］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の［**ルールリスト**］をクリックします。
   ［**ファイアウォールのルール**］ウィンドウが開きます。
6. ステータスを変更するルールの種別に応じて、［**アプリケーション**］または［**ポート**］タブを選択します。
7. 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。
8. ［**ファイアウォールのルール**］ウィンドウで［OK］をクリックします。
9. ［**ファイアウォール管理**］ウィンドウで［OK］をクリックします。
10. ポリシーのプロパティウィンドウで、［OK］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## ファイアウォールルールの手動での追加

アプリケーションおよびポートのルールは、追加と編集のみ可能です。新しいグループルールを追加したり既存のグループルールを編集したりすることはできません。

*着信ネットワークトラフィックをフィルタリングする既存のルールを追加または編集するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**ネットワーク活動の管理**］セクションで、［**ファイアウォール管理**］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の［**ルールリスト**］をクリックします。
   ［**ファイアウォールのルール**］ウィンドウが開きます。
6. 追加するルールの種別に応じて［**アプリケーション**］または［**ポート**］タブを選択し、次の処理のいずれかを実行します：
   - 既存のルールを編集するには、ルールリストで編集するルールを選択し、［**編集**］をクリックします。
   - 新しいルールを追加するには［**追加**］をクリックします。
     設定するルールの種別に応じて、［**アプリケーションルール**］ウィンドウまたは［**ポートルール**］ウィンドウが開きます。
7. 表示されたウィンドウで、次の操作を行います：
   - アプリケーションルールを使用する場合、次を行います：
     a. ［**ルール名**］で、編集したルールの名前を入力します。
     b. このルールを変更して接続を許可するアプリケーションの実行ファイルへの［**アプリケーションパス**］を指定します。
     パスは、手動で、または［**参照**］を使用して設定できます。

c. ［**ルール適用範囲**］で、変更したルールを適用するネットワークアドレスを指定します。

IPv4 アドレスのみ使用できます。

- ポートルールを使用する場合、次を行います：

  a. ［**ルール名**］で、編集したルールの名前を入力します。

  b. 接続を許可する**ポート番号**を指定します。

  c. 接続を許可する種類のプロトコル（TCP / UDP）を選択します。

  d. ［**ルール適用範囲**］で、変更したルールを適用するネットワークアドレスを指定します。

  IPv4 アドレスのみ使用できます。

8. ［**アプリケーションルール**］または［**ポートルール**］ウィンドウで［OK］をクリックします。
9. ［**ファイアウォール管理**］ウィンドウで［OK］をクリックします。
10. ポリシーのプロパティウィンドウで、［OK］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## ファイアウォールのルールの削除

削除できるのはアプリケーションルールおよびポートルールのみです。既存のグループルールを削除することはできません。

*着信ネットワークトラフィックをフィルタリングする既存のルールを削除するには、次の処理を実行します：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

   Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**ネットワーク活動の管理**］セクションで、［**ファイアウォール管理**］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の［**ルールリスト**］をクリックします。
   ［**ファイアウォールのルール**］ウィンドウが開きます。

6. ステータスを変更するルールの種別に応じて、［**アプリケーション**］または［**ポート**］タブを選択します。

7. ルールリストで、削除するルールを選択します。

8. ［**削除**］をクリックします。
   選択したルールが削除されます。

9. ［**ファイアウォールのルール**］ウィンドウで［**OK**］をクリックします。

10. ［**ファイアウォール管理**］ウィンドウで［**OK**］をクリックします。

11. ポリシーのプロパティウィンドウで、［**OK**］をクリックします。

指定したファイアウォール管理タスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## アプリケーションコンソールからファイアウォールのルールを管理する

このセクションでは、アプリケーションコンソールインターフェイスからファイアウォールのルールを管理する方法について説明します。

## ファイアウォールのルールの有効化と無効化

*着信ネットワークトラフィックをフィルタリングする既存のルールを有効または無効にするには、次の処理を実行します：*

1. アプリケーションコンソールツリーで、［**コンピューターの管理**］フォルダーを展開します。

2. ［**ファイアウォール管理**］サブフォルダーを選択します。

3. ［**ファイアウォール管理**］フォルダーの詳細ペインで、［**ファイアウォールのルール**］をクリックします。
   ［**ファイアウォールのルール**］ウィンドウが開きます。

4. ステータスを変更するルールの種別に応じて、［**アプリケーション**］または［**ポート**］タブを選択します。

5. 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. ［**ファイアウォールのルール**］ウィンドウで［**保存**］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## ファイアウォールルールの手動での追加

*着信ネットワークトラフィックをフィルタリングする既存のルールを追加または編集するには：*

1. アプリケーションコンソールツリーで、［**コンピューターの管理**］フォルダーを展開します。
2. ［**ファイアウォール管理**］サブフォルダーを選択します。
3. ［**ファイアウォール管理**］フォルダーの詳細ペインで、［**ファイアウォールのルール**］をクリックします。
   ［**ファイアウォールのルール**］ウィンドウが開きます。
4. 追加するルールの種別に応じて［**アプリケーション**］または［**ポート**］タブを選択し、次の処理のいずれかを実行します：
   - 既存のルールを編集するには、ルールリストで編集するルールを選択し、［**編集**］をクリックします。
   - 新しいルールを追加するには［**追加**］をクリックします。
     設定するルールの種別に応じて、［**アプリケーションルール**］ウィンドウまたは［**ポートルール**］ウィンドウが開きます。
5. 表示されたウィンドウで、次の操作を行います：
   - アプリケーションルールを使用する場合、次を行います：
     a. ［**ルール名**］で、編集したルールの名前を入力します。
     b. このルールを変更して接続を許可するアプリケーションの実行ファイルへの［**アプリケーションパス**］を指定します。
     パスは、手動で、または［**参照**］を使用して設定できます。
     c. ［**ルール適用範囲**］で、変更したルールを適用するネットワークアドレスを指定します。

     IPv4 アドレスのみ使用できます。

   - ポートルールを使用する場合、次を行います：
     a. ［**ルール名**］で、編集したルールの名前を入力します。
     b. 接続を許可する**ポート番号**を指定します。
     c. 接続を許可する種類のプロトコル（TCP / UDP）を選択します。
     d. ［**ルール適用範囲**］で、変更したルールを適用するネットワークアドレスを指定します。

IPv4 アドレスのみ使用できます。

6. ［**アプリケーションルール**］または［**ポートルール**］ウィンドウで［OK］をクリックします。
7. ［**ファイアウォールのルール**］ウィンドウで［**保存**］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## ファイアウォールのルールの削除

削除できるのはアプリケーションルールおよびポートルールのみです。既存のグループルールを削除することはできません。

*着信ネットワークトラフィックをフィルタリングする既存のルールを削除するには、次の処理を実行します：*

1. アプリケーションコンソールツリーで、［**コンピューターの管理**］フォルダーを展開します。
2. ［**ファイアウォール管理**］サブフォルダーを選択します。
3. ［**ファイアウォール管理**］フォルダーの詳細ペインで、［**ファイアウォールのルール**］をクリックします。
   ［**ファイアウォールのルール**］ウィンドウが開きます。
4. ステータスを変更するルールの種別に応じて、［**アプリケーション**］または［**ポート**］タブを選択します。
5. ルールリストで、削除するルールを選択します。
6. ［**削除**］をクリックします。
   選択したルールが削除されます。
7. ［**ファイアウォールのルール**］ウィンドウで［**保存**］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## Web プラグインからファイアウォールのルールを管理する

*Web プラグインからファイアウォールのル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、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**ネットワーク活動の管理**］セクションを選択します。

5. ［**ファイアウォール管理**］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。

ファイアウォール管理タスクの設定

| 設定 | 説明 |
| --- | --- |
| **アプリケーションルール** | アプリケーションルールは管理できます。<br>この種のルールは、指定したアプリケーションを標的とするネットワーク接続を許可します。これらのルールの有効化の条件は、実行ファイルへのパスに基づきます。 |
| **ポートルール** | ポートルールは管理できます。<br>この種のルールは、指定したポートおよびプロトコル（TCP/UDP）によるネットワーク接続を許可します。これらのルールの有効化の条件は、ポート番号およびプロトコルの種別に基づきます。 |
| **タスク管理** | スケジュールでタスクを開始する設定を指定できます。 |

## ファイアウォールのルールの有効化と無効化

*着信ネットワークトラフィックをフィルタリングする既存のルールを有効または無効にするには、次の処理を実行します：*

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。

4. ［**ネットワーク活動の管理**］セクションを選択します。

5. ［**ファイアウォール管理**］サブセクションの［**設定**］をクリックします。

6. ステータスを変更するルールの種別に応じて、［**アプリケーションルール**］または［**ポートルール**］タブを選択します。

7. 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、ルール名の左側の切り替えボタンをオンにします。
   - 有効なルールを無効にする場合、ルール名の左側の切り替えボタンをオフにします。

8. ［**OK**］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## ファイアウォールルールの手動での追加

*着信ネットワークトラフィックをフィルタリングする既存のルールを追加または編集するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。

4. ［**ネットワーク活動の管理**］セクションを選択します。

5. ［**ファイアウォール管理**］サブセクションの［**設定**］をクリックします。

6. ステータスを変更するルールの種別に応じて［**アプリケーションルール**］または［**ポートルール**］タブを選択し、次の処理のいずれかを実行します：

   - 既存のルールを編集するには、編集するルールを選択し、［**編集**］をクリックします。
   - 新しいルールを追加するには［**追加**］をクリックします。

7. 画面の右側で、次の操作を実行します：

   - アプリケーションルールを使用する場合、次を行います：

     a. ［**ルール名**］で、編集したルールの名前を入力します。

     b. このルールを変更して接続を許可するアプリケーションの実行ファイルへの［**アプリケーションパス**］を指定します。

     c. ［**ルール適用範囲**］で、変更したルールを適用するネットワークアドレスを指定します。

     IPv4 アドレスのみ使用できます。

   - ポートルールを使用する場合、次を行います：

     a. ［**ルール名**］で、編集したルールの名前を入力します。

     b. 接続を許可するポート番号を指定します。

     c. 接続を許可する種類のプロトコル（TCP / UDP）を選択します。

     d. ［**ルール適用範囲**］で、変更したルールを適用するネットワークアドレスを指定します。

     IPv4 アドレスのみ使用できます。

8. ［OK］をクリックします。

9. ［**ファイアウォール管理**］ウィンドウで［OK］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

## ファイアウォールのルールの削除

削除できるのはアプリケーションルールおよびポートルールのみです。既存のグループルールを削除することはできません。

*着信ネットワークトラフィックをフィルタリングする既存のルールを削除するには、次の処理を実行します：*

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**ネットワーク活動の管理**］セクションを選択します。
5. ［**ファイアウォール管理**］サブセクションの［**設定**］をクリックします。
6. 削除するルールの種別に応じて、［**アプリケーションルール**］または［**ポートルール**］タブを選択します。
7. ルールリストで、削除するルールを選択します。
8. ［**削除**］をクリックします。
   選択したルールが削除されます。
9. ［**OK**］をクリックします。

指定したタスクの設定が保存されます。新しいルールパラメータが Windows ファイアウォールに送信されます。

# ファイル変更監視

このセクションには、ファイル変更監視タスクの開始と設定に関する情報が含まれています。

## ファイル変更監視タスクについて

ファイル変更監視タスクは、タスク設定で指定した監視範囲にある指定したファイルおよびフォルダーで実行される処理を追跡します。このタスクを使用して、保護対象デバイスでセキュリティ違反を示した可能性があるファイル変更を検知できます。監視中断期間のファイル変更を追跡するよう設定することもできます。

*監視の中断*は、監視範囲が一時的にタスク範囲を外れる、たとえばタスクが停止された場合や、外部デバイスが保護対象デバイスに物理的に存在しない場合に発生します。外部デバイスが再接続されるとすぐに、Kaspersky Embedded Systems Security は監視範囲で検知したファイル操作を報告します。

ファイル変更監視の再インストールのためにタスクが指定した監視範囲で実行を停止した場合は、監視の中断は発生しません。この場合、ファイル変更監視タスクは実行されません。

### 環境に関する要件

ファイル変更監視タスクを開始するには、次の条件が満たされている必要があります：

- ReFS または NTFS ファイルシステムを、保護対象デバイスに使用する必要があります。
- Windows USN ジャーナルが有効である。このコンポーネントはこのジャーナルに対してクエリを行って、ファイル操作に関する情報を受け取ります。

  ボリュームに対してルールが作成され、ファイル変更監視タスクが開始された後で USN ジャーナルを有効化した場合、タスクを再起動する必要があります。そうでない場合、ルールは監視時に適用されません。

### 除外された監視範囲

監視範囲の除外を作成できます。除外は別々のルール各々に対して指定され、指定した監視範囲に対してのみ機能します。各ルールに対して個数の制限なく除外を指定できます。

指定したフォルダーまたはファイルが監視範囲内の場合でも、除外は監視範囲より優先度が高いため、タスクによって監視されません。ルールのいずれかの設定が、除外で指定したフォルダーより下位のレベルで監視範囲を指定している場合、タスクの実行時に監視範囲は考慮されません。

除外を指定するために、監視範囲を指定するために使用したのと同じマスクを使用できます。

## ファイル変更監視ルールについて

ファイル変更監視タスクは、ファイル変更監視ルールに基づいて実行されます。ルール有効化の条件を使用してタスクを起動させる条件を設定し、実行ログに記録された検知されたファイル操作イベントに対して重要性レベルを調整することができます。

ファイル変更監視ルールは、各監視範囲に対して指定されます。

次のルール有効化の条件を設定できます：

- 信頼するユーザー
- ファイル操作マーカー

## 信頼するユーザー

既定では、すべてのユーザーアクションが潜在的なセキュリティ違反と判断されます。信頼するユーザーのリストは空です。ファイル変更監視ルール設定に信頼するユーザーのリストを作成することで、イベントの重要性レベルを設定できます。

*信頼しないユーザー*とは、監視範囲ルール設定の信頼するユーザーリストに示されていないすべてのユーザーに割り当てられるステータスです。信頼しないユーザーによって行われたファイル操作を検知すると、ファイル変更監視タスクが実行ログに緊急イベントを記録します。

*信頼するユーザー*とは、指定した監視範囲でファイル操作を行う許可を与えられているユーザーのユーザーまたはグループに割り当てられるステータスです。信頼するユーザーによって行われたファイル操作を検知すると、ファイル変更監視タスクが実行ログに情報イベントを記録します。

Kaspersky Embedded Systems Security は、監視の中断中に操作を開始したユーザーを特定できません。この場合、ユーザーステータスは不明と判断されます。

*不明なユーザー*は、タスク中断、またはデータ同期ドライバーや USN ジャーナルの障害のために Kaspersky Embedded Systems Security がユーザーに関する情報を受け取ることができない場合に、ユーザーに割り当てられるステータスです。不明なユーザーによって行われたファイル操作を検知すると、ファイル変更監視タスクが実行ログに*警告*イベントを記録します。

## ファイル操作マーカー

ファイル変更監視タスクが実行されている時、Kaspersky Embedded Systems Security はファイル操作マーカーを使用して、ファイル上で処理が実行されたと判定します。

ファイル操作マーカーは、ファイル操作を特徴づけることができる一意の記述子です。

各ファイル操作は、単一の処理であることも、ファイルを使用した処理の連鎖であることもあります。この種類の各処理は、ファイル操作マーカーに対応します。ルール有効化の条件として指定するマーカーがファイル操作チェーンで検知された場合、所定のファイル操作が実行されたことを示すイベントが記録されます。

記録されたイベントの重要性レベルは、選択されたファイル操作マーカーまたはイベントの数に依存しません。

既定で、Kaspersky Embedded Systems Security は利用できるすべてのファイル操作マーカーを考慮します。タスクのルール設定で、手動でファイル操作マーカーを選択できます。

ファイル操作マーカー

| ファイル操作 ID | ファイル操作マーカー | サポートされて |
| --- | --- | --- |

| | | いるファイルシステム |
|---|---|---|
| BASIC_INFO_CHANGE | ファイルまたはフォルダーの属性または時間マーカーが変更されました | NTFS、ReFS |
| COMPRESSION_CHANGE | ファイルまたはフォルダーの圧縮が変更されました | NTFS、ReFS |
| DATA_EXTEND | ファイルまたはフォルダーのサイズが増加しました | NTFS、ReFS |
| DATA_OVERWRITE | ファイルまたはフォルダー内のデータが上書きされました | NTFS、ReFS |
| DATA_TRUNCATION | ファイルまたはフォルダーが切り詰められました | NTFS、ReFS |
| EA_CHANGE | 拡張されたファイルまたはフォルダーの属性が変更されました | NTFS のみ |
| ENCRYPTION_CHANGE | ファイルまたはフォルダーの暗号化ステータスが変更されました | NTFS、ReFS |
| FILE_CREATE | ファイルまたはフォルダーが初めて作成されました | NTFS、ReFS |
| FILE_DELETE | SHIFT+DEL を同時に押して、ファイルまたはフォルダーが完全に削除されました | NTFS、ReFS |
| HARD_LINK_CHANGE | ファイルまたはフォルダーにハードリンクが作成または削除されました | NTFS のみ |
| INDEXABLE_CHANGE | ファイルまたはフォルダーの索引ステータスが変更されました | NTFS、ReFS |
| INTEGRITY_CHANGE | 名前付きファイルストリームの整合性属性が変更されました | ReFS のみ |
| NAMED_DATA_EXTEND | 名前付きファイルストリームのサイズが増加しました。 | NTFS、ReFS |
| NAMED_DATA_OVERWRITE | 名前付きファイルストリームが上書きされました | NTFS、ReFS |
| NAMED_DATA_TRUNCATION | 名前付きファイルストリームが切り詰められました | NTFS、ReFS |
| OBJECT_ID_CHANGE | ファイルまたはフォルダー ID が変更されました | NTFS、ReFS |
| RENAME_NEW_NAME | ファイルまたはフォルダーに新しい名前が割り当てられました | NTFS、ReFS |
| REPARSE_POINT_CHANGE | 新しい再解析ポイントが作成されたか、ファイルまたはフォルダーに対する既存の再解析ポイントが変更されました | NTFS、ReFS |
| SECURITY_CHANGE | ファイルまたはフォルダーのアクセス権が変更されました | NTFS、ReFS |
| STREAM_CHANGE | 新しい名前付きファイルストリームが作成されたか、既存の名前付きファイルストリームが変更されました | NTFS、ReFS |
| TRANSACTED_CHANGE | 名前付きファイルストリームが TxF トランザクションによって変更されました | ReFS のみ |

## ファイル変更監視タスクの既定の設定

ファイル変更監視タスクでは、次の表の既定の設定が使用されます。設定の値を変更できるのは、以下のコンポーネントです：

- 管理プラグイン
- アプリケーションコンソール
- Web プラグイン

ファイル変更監視タスクの既定の設定

| 設定 | 既定値 | 説明 |
|---|---|---|
| **監視範囲** | 設定なし | このオプションを使用して、処理が監視されるフォルダーとファイルを指定します。監視イベントは、指定した監視範囲のフォルダーおよびファイルに対して作成されます。 |
| ［**信頼するユーザー**］リスト | 設定なし | このオプションを使用して、指定したフォルダーにおける処理がコンポーネントにより安全なものと判断されるユーザーやユーザーのグループを指定します。 |
| **監視中断期間におけるファイル操作の情報を記録する** | 使用 | このオプションを使用して、タスクが実行されていない期間に、指定した監視範囲で実行されたファイル操作の記録を有効または無効にします。<br><br>既定では、設定されたルールに関係なく、信頼するユーザーの統計が収集されます。 |
| **USN ログを不正に利用しようとする動作をブロックする** | 使用 | このオプションを使用して、USN ログの保護を有効または無効にします。 |
| **信頼ゾーンを適用する** | 無効 | ルールに設定されている監視範囲に加えて、除外を［**信頼ゾーン**］に適用するために、［**信頼ゾーンを適用する**］をオンまたはオフにします。 |
| **選択したファイル操作を検知してブロックする** | 無効 | 選択した監視領域のすべての変更をブロックする場合は、［**選択したファイル操作を検知してブロックする**］をオンまたはオフにします。 |
| **次のフォルダーをコントロールから除外する** | オフ | このオプションを使用して、ファイル操作を監視する必要がないフォルダーに対する除外の使用を確認します。ファイル変更監視タスクが実行されている場合、Kaspersky Embedded Systems Security は除外として指定された監視範囲をスキップします。 |
| **チェックサムの計算** | オフ | このオプションを使用して、ファイル変更後のファイルチェックサム計算を設定します。 |
| **ファイル操作マーカーの設定** | 使用可能なすべてのファイル操作マーカーが考慮されます | このオプションを使用して、ファイル操作マーカーのセットを指定します。監視範囲で実行されたファイル操作に、1つ以上の指定したマーカーが付けられている場合、Kaspersky Embedded Systems Security は監査イベントを作成します。 |
| タスク開始スケジュール | 最初の実行がスケジュール設定されていません | スケジュールによるタスクの開始を設定できます。 |

## 管理プラグインからファイル変更監視を管理する

このセクションでは、管理プラグインからファイル変更監視タスクを設定する方法について説明します。

## ファイル変更監視タスクの設定について

ファイル変更監視タスク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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**ファイル変更監視**］セクションの［**システム監査**］サブセクションで、［**設定**］をクリックします。
   ［**ファイル変更監視**］ウィンドウが開きます。
5. 表示されたウィンドウの［**ファイル変更監視の設定**］タブで、次の設定を行います：
   - ［**監視中断期間におけるファイル操作の情報を記録する**］をオンにします。

     このチェックボックスで、なんらかの理由でタスクが実行されていない場合（ハードディスクの取り外し、ユーザーによるタスク停止、ソフトウェアエラー）における、ファイル変更監視タスク設定で指定したファイル操作の監視を有効または無効にできます。

     このチェックボックスをオンにすると、ファイル変更監視タスクが実行されていない時、Kaspersky Embedded Systems Security はすべての監視範囲のイベントを記録します。

     このチェックボックスをオフにすると、タスクが実行中でない時には、監視範囲のファイル操作を記録しません。

     既定では、このチェックボックスはオンです。
   - ［**USN ログを不正に利用しようとする動作をブロックする**］をオフまたはオンにします。

     USN ログの保護を有効または無効にできます。

     このチェックボックスをオンにすると、Kaspersky Embedded Systems Security は USN ログの削除、または USN ログの内容への不正アクセスをブロックします。

     このチェックボックスをオフにすると、USN ログの変更は監視されません。

     既定では、このチェックボックスはオンです。
   - 必要に応じて、［**信頼ゾーンを適用する**］をオンまたはオフにします。

［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］に設定された［**除外**］と［**信頼するプロセス**］が、設定されたルールに加えて監視範囲に適用されます。

［**信頼ゾーンを適用する**］がオフの場合、［**信頼ゾーン**］に設定された［**除外**］と［**信頼するプロセス**］は監視範囲に適用されません。

既定では、このチェックボックスはオフです。

- タスクによって監視される監視範囲を追加します。

6. ［**タスク管理**］タブで、スケジュールに基づくタスク開始の設定を行います。
7. ［**OK**］をクリックして、変更内容を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定変更の日時に関する情報は、システム監査ログに保存されます。

## 監視ルールの設定

*監視範囲を追加するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**ファイル変更監視**］セクションの［**システム監査**］サブセクションで、［**設定**］をクリックします。
   ［**ファイル変更監視**］ウィンドウが開きます。
5. ［**監視範囲**］セクションで、［**追加**］をクリックします。
   ［**ファイル変更監視ルール**］ウィンドウが表示されます。
6. 次のいずれかの方法で、監視範囲を追加します：
   - 標準の Microsoft Windows ダイアログを使用してフォルダーを選択する場合：
     a. ［**参照**］をクリックします。
        Microsoft Windows 標準の［**フォルダーを参照**］ウィンドウが表示されます。

b. 表示された［**フォルダーを参照**］ウィンドウで操作を監視するフォルダーを選択し、［**OK**］をクリックします。

- 手動で監視範囲を指定する場合、サポートされているマスクを使用してパスを追加します：
  - <*.ext> - 場所に関係なく、拡張子 <ext> を持つすべてのファイル
  - <*\name.ext> - 場所に関係なく、名前 <name> と拡張子 <ext> を持つすべてのファイル
  - <\dir*> - フォルダー <\dir> にあるすべてのファイル
  - <\dir*\name.ext> - フォルダー <\dir> とそのすべてのサブフォルダーにある、名前 <name> と拡張子 <ext> を持つすべてのファイル

手動で監視範囲を指定する場合、パスが次の形式であることを確認してください：<ボリューム文字>:\<マスク>。ボリューム文字がない場合、Kaspersky Embedded Systems Security は指定した監視範囲を追加しません。

7. ［**信頼するユーザー**］タブで、［**追加**］をクリックします。

   Microsoft Windows 標準の［**ユーザーまたはグループの選択**］ウィンドウが開きます。

8. 選択した監視範囲でのファイル操作が許可されたユーザーまたはユーザーのグループを選択し、［**OK**］をクリックします。

既定では、Kaspersky Embedded Systems Security においては信頼するユーザーリストに記載されていないすべてのユーザーを信頼しないユーザーとして取り扱い、重要なイベントを作成します。信頼するユーザーの場合、統計が収集されます。

9. ［**ファイル操作マーカー**］タブを選択します。

10. 必要に応じて、次の処理を実行して複数のマーカーを選択します：

    a. ［**次のマーカーに基づいてファイル操作を検出する**］オプションを選択します。

    b. 使用可能なファイル操作のリストで、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。

既定では、Kaspersky Embedded Systems Security によりすべてのファイル操作マーカーが検知され、［**認識可能なすべてのマーカーに基づいてファイル操作を検出する**］がオンになります。

11. 選択した領域のすべてのファイル操作をブロックする場合は、［**選択したファイル操作を検知してブロックする**］をオンにします。

12. 操作の実行後に Kaspersky Embedded Systems Security がファイルチェックサムを計算するようにするには、次の手順を実行します：

    a. ［**可能な場合、ファイルのチェックサムを計算する。チェックサムはタスクレポートで表示できます**］をオンにします。

    b. ［**チェックサム種別**］ドロップダウンリストで、次のいずれかのオプションを選択します：

    - **MD5 ハッシュ**

- **SHA256 ハッシュ**

13. 利用できるファイル操作のリストにあるすべてのファイル操作を監視するのでない場合は、監視する操作の隣にあるチェックボックスをオンにします。

14. 必要に応じて、除外された監視範囲を追加します：

    a. ［**除外リスト**］タブを選択します。

    b. ［**次のフォルダーをコントロールから除外する**］をオンにします。

    c. ［**追加**］をクリックします。
    ［**追加するフォルダーの選択**］ウィンドウが開きます。

    d. 表示されたウィンドウで、監視範囲から除外するフォルダーを指定します。

    e. ［**OK**］をクリックします。
    指定したフォルダーが、除外される範囲のリストに追加されます。

15. ［**ファイル変更監視ルール**］ウィンドウで［**OK**］をクリックします。
指定したルール設定は、［ファイル変更監視］タスクの、選択した監視範囲に適用されます。

## アプリケーションコンソールからファイル変更監視を管理する

このセクションでは、アプリケーションコンソールからファイル変更監視タスクを設定する方法について説明します。

## ファイル変更監視タスクの設定

*ファイル変更監視タスクの全般的な設定を行うには：*

1. アプリケーションコンソールツリーで、［**システム監査**］フォルダーを展開します。

2. ［**ファイル変更監視**］サブフォルダーを選択します。

3. ［**ファイル変更監視**］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。
［**タスクの設定**］ウィンドウが表示されます。

4. 表示されたウィンドウの［**全般**］タブで、次の設定を行います：

    a. ［**監視中断期間におけるファイル操作の情報を記録する**］をオフまたはオンにします。

このチェックボックスで、なんらかの理由でタスクが実行されていない場合（ハードディスクの取り外し、ユーザーによるタスク停止、ソフトウェアエラー）における、ファイル変更監視タスク設定で指定したファイル操作の監視を有効または無効にできます。

このチェックボックスをオンにすると、ファイル変更監視タスクが実行されていない時、Kaspersky Embedded Systems Security はすべての監視範囲のイベントを記録します。

このチェックボックスをオフにすると、タスクが実行中でない時には、監視範囲のファイル操作を記録しません。

既定では、このチェックボックスはオンです。

b. ［**USN ログを不正に利用しようとする動作をブロックする**］をオフまたはオンにします。

USN ログの保護を有効または無効にできます。

このチェックボックスをオンにすると、Kaspersky Embedded Systems Security は USN ログの削除、または USN ログの内容への不正アクセスをブロックします。

このチェックボックスをオフにすると、USN ログの変更は監視されません。

既定では、このチェックボックスはオンです。

c. 必要に応じて、［**信頼ゾーンを適用する**］をオンまたはオフにします。

［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］に設定された［**除外**］と［**信頼するプロセス**］が、設定されたルールに加えて監視範囲に適用されます。

［**信頼ゾーンを適用する**］がオフの場合、［**信頼ゾーン**］に設定された［**除外**］と［**信頼するプロセス**］は監視範囲に適用されません。

既定では、このチェックボックスはオフです。

5. ［**スケジュール**］タブと［**詳細設定**］タブで、タスクの開始スケジュールを設定します。

6. ［**OK**］をクリックして、変更内容を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定変更の日時に関する情報は、システム監査ログに保存されます。

## 監視ルールの設定

*監視範囲を追加するには：*

1. アプリケーションコンソールツリーで、［**システム監査**］フォルダーを展開します。

2. ［**ファイル変更監視**］サブフォルダーを選択します。

3. ［**ファイル変更監視**］フォルダーの結果ペインで、［**ファイル変更監視ルール**］をクリックします。
［**ファイル変更監視**］ウィンドウが表示されます。

4. 次のいずれかの方法で、監視範囲を追加します：

- 標準の Microsoft Windows ダイアログを使用してフォルダーを選択する場合：

a. ウィンドウの左側にある［**参照**］をクリックします。

Microsoft Windows 標準の［**フォルダーを参照**］ウィンドウが表示されます。

b. ［**フォルダーを参照**］ウィンドウで操作を監視するフォルダーを選択し、［**OK**］をクリックします。

c. ［**追加**］をクリックし、指定した監視範囲で Kaspersky Embedded Systems Security によるファイル操作の監視を開始します。

- 手動で監視範囲を指定する場合、サポートされているマスクを使用してパスを追加します：
  - <*.ext> - 場所に関係なく、拡張子 <ext> を持つすべてのファイル
  - <*\name.ext> - 場所に関係なく、名前 <name> と拡張子 <ext> を持つすべてのファイル
  - <\dir*> - フォルダー <\dir> にあるすべてのファイル
  - <\dir*\name.ext> - フォルダー <\dir> とそのすべてのサブフォルダーにある、名前 <name> と拡張子 <ext> を持つすべてのファイル

手動で監視範囲を指定する場合、パスが次の形式であることを確認してください：<ボリューム文字>:\<マスク>。ボリューム文字がない場合、Kaspersky Embedded Systems Security は指定した監視範囲を追加しません。

ウィンドウの右側にある［**ルールの説明**］タブに、この監視範囲で選択した信頼するユーザーとファイル操作マーカーが表示されます。

5. 追加した監視範囲のリストで、設定を実行する範囲を選択します。
6. ［**信頼するユーザー**］タブを選択します。
7. ［**追加**］をクリックします。

Microsoft Windows 標準の［**ユーザーまたはグループの選択**］ウィンドウが開きます。

8. 選択した監視範囲で Kaspersky Embedded Systems Security が信頼すると判断するユーザーまたはユーザーグループを選択します。
9. ［**OK**］をクリックします。

既定では、Kaspersky Embedded Systems Security においては信頼するユーザーリストに記載されていないすべてのユーザーを信頼しないユーザーとして取り扱い、重要なイベントを作成します。信頼するユーザーの場合、統計が収集されます。

10. ［**ファイル操作マーカーの設定**］タブを選択します。
11. 必要に応じて、次の処理を実行して複数のマーカーを選択します：

a. ［**次のマーカーに基づいてファイル操作を検出する**］オプションを選択します。

b. 使用可能なファイル操作のリストで、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。

既定では、Kaspersky Embedded Systems Security によりすべてのファイル操作マーカーが検知され、［**認識可能なすべてのマーカーに基づいてファイル操作を検出する**］がオンになります。

12. 選択した領域のすべてのファイル操作をブロックする場合は、［**選択したファイル操作を検知してブロックする**］をオンにします。

13. 操作の実行後に Kaspersky Embedded Systems Security がファイルチェックサムを計算するようにするには、次の手順を実行します：

    a. ［**チェックサムの計算**］セクションで、［**可能な場合、ファイルの変更後にファイル最終版のチェックサムを計算する。チェックサムは実行ログに表示されます。**］をオンまたはオフにします。

    b. ［**アルゴリズムを使用してチェックサムを計算する**］ドロップダウンリストで、次のいずれかのオプションを選択します：

    - **MD5 ハッシュ**：
    - **SHA256 ハッシュ**：

14. 必要に応じて、除外された監視範囲を追加します：

    a. ［**除外の設定**］タブを選択します。

    b. ［**除外された監視範囲を検討する**］をオンにします。

    c. ［**参照**］をクリックします。
    Microsoft Windows 標準の［**フォルダーを参照**］ウィンドウが表示されます。

    d. ［**フォルダーを参照**］ウィンドウで、監視範囲から除外するフォルダーを指定します。

    e. ［**OK**］をクリックします。

    f. ［**追加**］をクリックします。
    指定したフォルダーが、除外される範囲のリストに追加されます。

    また、監視範囲の指定に使用されたのと同じマスクを使用して、除外された監視範囲を手動で追加することもできます。

15. ［**保存**］をクリックして、新しいルール設定を適用します。

指定したルール設定は、［**ファイル変更監視**］タスクの定義した監視範囲にただちに適用されます。

## Web プラグインからファイル変更監視を管理する

このセクションでは、Web プラグインからファイル変更監視タスクを設定する方法について説明します。

## ファイル変更監視タスクの設定について

*Web プラグインからファイル変更監視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**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**システム監査**］セクションを選択します。
5. ［**ファイル変更監視**］サブセクションの［**設定**］をクリックします。
6. 表示された［**ファイル変更監視**］ウィンドウの［**ファイル変更監視の設定**］タブで、次の設定を行います：

   a. ［**監視中断期間におけるファイル操作の情報を記録する**］をオフまたはオンにします。

   このチェックボックスで、なんらかの理由でタスクが実行されていない場合（ハードディスクの取り外し、ユーザーによるタスク停止、ソフトウェアエラー）における、ファイル変更監視タスク設定で指定したファイル操作の監視を有効または無効にできます。

   このチェックボックスをオンにすると、ファイル変更監視タスクが実行されていない時、Kaspersky Embedded Systems Security はすべての監視範囲のイベントを記録します。

   このチェックボックスをオフにすると、タスクが実行中でない時には、監視範囲のファイル操作を記録しません。

   既定では、このチェックボックスはオンです。

   b. ［**USN ログを不正に利用しようとする動作をブロックする**］をオフまたはオンにします。

   USN ログの保護を有効または無効にできます。

   このチェックボックスをオンにすると、Kaspersky Embedded Systems Security は USN ログの削除、または USN ログの内容への不正アクセスをブロックします。

   このチェックボックスをオフにすると、USN ログの変更は監視されません。

   既定では、このチェックボックスはオンです。

   c. 必要に応じて、［**信頼ゾーンを適用する**］をオンまたはオフにします。

   ［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］に設定された［**除外**］と［**信頼するプロセス**］が、設定されたルールに加えて監視範囲に適用されます。

   ［**信頼ゾーンを適用する**］がオフの場合、［**信頼ゾーン**］に設定された［**除外**］と［**信頼するプロセス**］は監視範囲に適用されません。

   既定では、このチェックボックスはオフです。

7. ［**タスク管理**］タブで、タスクの開始スケジュールを設定します。
8. ［**OK**］をクリックして、変更内容を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定変更の日時に関する情報は、システム監査ログに保存されます。

# 監視ルールの設定

*監視範囲を追加するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**システム監査**］セクションを選択します。
5. ［**ファイル変更監視**］サブセクションの［**設定**］をクリックします。
6. 表示される［**ファイル変更監視**］ウィンドウで、［**ファイル変更監視の設定**］タブを開きます。
7. ［**USN ログ**］セクションで、［**追加**］をクリックします。
   ［**ファイル変更監視ルール**］ウィンドウが表示されます。
8. ［**次の範囲のファイル操作を監視**］で、サポートされているマスクを使用してパスを指定します：
   - <*.ext> - 場所に関係なく、拡張子 <ext> を持つすべてのファイル
   - <*\name.ext> - 場所に関係なく、名前 <name> と拡張子 <ext> を持つすべてのファイル
   - <\dir*> - フォルダー <\dir> にあるすべてのファイル
   - <\dir*\name.ext> - フォルダー <\dir> とそのすべてのサブフォルダーにある、名前 <name> と拡張子 <ext> を持つすべてのファイル

   手動で監視範囲を指定する場合、パスが次の形式であることを確認してください：<ボリューム文字>:\<マスク>。ボリューム文字がない場合、Kaspersky Embedded Systems Security は指定した監視範囲を追加しません。
9. ［**信頼するユーザー**］タブで、次のいずれかを実行します：
   - ［**追加**］をクリックし、表示されたウィンドウの［**ユーザー名**］に SID を使用してユーザー名を指定します。
   - ［**管理サーバーから追加する**］をクリックし、表示されたウィンドウでリストからユーザーを選択します。

   既定では、Kaspersky Embedded Systems Security においては信頼するユーザーリストに記載されていないすべてのユーザーを信頼しないユーザーとして取り扱い、重要なイベントを作成します。信頼するユーザーの場合、統計が収集されます。
10. ［**OK**］をクリックします。
11. ［**ファイル操作マーカー**］タブを選択します。

12. 必要に応じて、次の処理を実行して複数のマーカーを選択します：

    a. ［**次のマーカーに基づいてファイル操作を検出する**］オプションを選択します。

    b. 使用可能なファイル操作のリストで、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。

    既定では、Kaspersky Embedded Systems Security によりすべてのファイル操作マーカーが検知され、［**認識可能なすべてのマーカーに基づいてファイル操作を検出する**］がオンになります。

13. 選択した領域のすべてのファイル操作をブロックする場合は、［**選択したファイル操作を検知してブロックする**］をオンにします。

14. 操作の実行後に Kaspersky Embedded Systems Security がファイルチェックサムを計算するようにするには：

    a. ［**可能な場合、ファイルのチェックサムを計算する。チェックサムはタスクレポートで表示できます**］をオンにします。

    b. ［**チェックサム種別**］ドロップダウンリストで、次のいずれかのオプションを選択します：

    - **SHA256 ハッシュ**
    - **MD5 ハッシュ**

15. 利用できるファイル操作のリストにあるすべてのファイル操作を監視するのでない場合は、監視する操作の隣にあるチェックボックスをオンにします。

16. 必要に応じて、除外された監視範囲を追加します：

    a. ［**除外リスト**］タブを選択します。

    b. ［**次のフォルダーをコントロールから除外する**］をオンにします。

    c. ［**追加**］をクリックします。
    ［**追加するフォルダーの選択**］ウィンドウが開きます。

    d. 右に表示されるペインで、監視範囲から除外するフォルダーを指定します。

    e. ［**OK**］をクリックします。
    指定したフォルダーが、除外される範囲のリストに追加されます。

17. ［**ファイル変更監視ルール**］ウィンドウで［**OK**］をクリックします。
    指定したルール設定は、［ファイル変更監視］タスクの、選択した監視範囲に適用されます。

# レジストリアクセス監視

このセクションでは、レジストリアクセス監視タスクの開始と設定の方法について説明します。

# レジストリアクセス監視タスクについて

レジストリアクセス監視タスクは、タスク設定で定義された監視範囲にある、指定したレジストリのブランチとキーで実行される処理を追跡します。このタスクを使用して、保護対象デバイスでセキュリティ違反を示した変更を検知できます。

レジストリアクセス監視タスクを開始するには、少なくとも1つの監視ルールを設定する必要があります。

# システムレジストリの監視ルールについて

レジストリアクセス監視タスクは、システムレジストリの監視ルールに基づいて実行されます。ルール有効化の条件を使用してタスクを起動させる条件を設定し、実行ログに記録された検知したイベントに対して重要性レベルを設定することができます。

システムレジストリの監視ルールは、各監視範囲に対して指定されます。

次のルール有効化の条件を設定できます：

- **処理**
- **レジストリ値**
- **信頼するユーザー**

## 処理

レジストリアクセス監視タスクが開始されると、Kaspersky Embedded Systems Security は処理のリストを使用してレジストリを監視します（以下の表を参照）。

ルール有効化の条件として指定された処理が検知されると、それぞれのイベントがログに記録されます。

記録されたイベントの重要性レベルは、選択された処理またはイベントの数に依存しません。

既定では、Kaspersky Embedded Systems Security はすべての処理を考慮します。タスクのルール設定で処理のリストを手動で設定できます。

処理

| 処理 | 制限 | オペレーティングシステム |
|---|---|---|
| **キー** | | Windows |

| | | |
|---|---|---|
| **を作成** | • Windows XP および Windows Server 2003 の場合、［**処理**］のリストに［**キーを作成**］を追加し、［**ルールに従って操作をブロックする**］モードを選択すると、システムの制限により、指定されたオペレーティングシステムでキーの作成がブロックされません。キーは、イベントのログに送信されるそれぞれの通知で作成されます。<br><br>• レジストリエディターを使用して特定のキーを作成することを禁止する場合は、親レジストリキーのルールを作成し、［**サブキーを作成**］を［**処理**］のリストに必ず追加してください。次に［**ルールに従って操作をブロックする**］モードを選択します。 | XP 以降 |
| **キーを削除** | 親キーを削除する場合は、設定したレジストリキーの監視する［**処理**］のリストで、［**キーの削除**］と［**サブキーの削除**］オプションの両方を必ず取り除いてください。削除できるのは、サブキーを持つ親キーのみです。 | Windows XP 以降 |
| **キーの名前を変更** | N/A | Windows XP 以降 |
| **キーのセキュリティ設定を変更** | N/A | Windows Vista 以降 |
| **値を削除** | N/A | Windows XP 以降 |
| **値を設定** | ［**処理**］のリストに［**値を設定**］を追加し、キーのルールで既定の［**値の名前**］を定義して、［**ルールに従って操作をブロックする**］モードを選択すると、キーは作成されません。新しいキーは、既定値でのみ作成できます。 | Windows XP 以降 |
| **サブキーを作成** | N/A | Windows XP 以降 |
| **サブキーを削除** | N/A | Windows XP 以降 |
| **サブキーの名前を変更** | N/A | Windows XP 以降 |
| **サブキーのセキュリティ設定を変更** | N/A | Windows Vista 以降 |

### レジストリ値

レジストリキーの監視のほかに、既存のレジストリ値の変更をブロックまたは監視できます。次のオプションを使用できます：

- **値を設定** - 新しいレジストリ値を作成するか、既存のレジストリ値を変更します。
- **値を削除** - 既存のレジストリ値を削除します。

セキュリティ設定の名前や設定内容の変更は、レジストリ値には適用されません。

### 信頼するユーザー

既定では、すべてのユーザーアクションが潜在的なセキュリティ違反と判断されます。信頼するユーザーのリストは空です。システムレジストリの監視ルール設定に信頼するユーザーのリストを作成することで、イベントの重要性レベルを設定できます。

*信頼しないユーザー*は、監視範囲ルール設定の信頼するユーザーリストに示されていないすべてのユーザーです。信頼しないユーザーによって実行された処理を検知すると、レジストリアクセス監視タスクが実行ログに緊急イベントを記録します。

*信頼するユーザー*は、指定した監視範囲で処理を行う許可を与えられているユーザーやユーザーグループです。信頼するユーザーによって実行された処理を検知すると、レジストリアクセス監視タスクが実行ログに情報イベントを記録します。

## レジストリアクセス監視タスクの既定の設定

［レジストリアクセス監視］タスクの既定の設定について、次の表で説明します。設定の値を変更できるのは、以下のコンポーネントです：

- 管理プラグイン
- アプリケーションコンソール
- Web プラグイン

レジストリアクセス監視タスクの既定の設定

| 設定 | 既定値 | 説明 |
|---|---|---|
| **監視範囲** | 未定義 | このオプションを使用して、監視する親レジストリキーとサブキーを定義します。指定された監視範囲内の親レジストリキーとサブキーに対して監視イベントが生成されます。 |
| **処理** | 処理のリストのすべての項目が選択 | このオプションを使用して、それぞれのチェックボックスをオンまたはオフにすることで、必要に応じて処理のリストを設定します。 |
| **レジストリ値** | 未定義 | このオプションを使用して、定義された監視範囲に対して、監視するレジストリ値の追加や変更、削除を行います。 |
| **信頼するユーザー** | 未定義 | このオプションを使用して、指定したレジストリキーに対して定義された処理を実行することを許可するユーザーやユーザーグループを指定します。 |
| | | |

| | | |
|---|---|---|
| **タスクモード** | 統計のみ | タスクモードを［**ルールに従って操作をブロックする**］に選択するか、または［**統計のみ**］モードを選択して、通知を受信できます。 |
| **信頼ゾーンを適用する** | 無効 | ルールに設定されているものに加えて、除外を［**信頼ゾーン**］に適用するために、［**信頼ゾーン**］をオンまたはオフにします。 |
| タスク開始スケジュール | 未定義 | スケジュールによるタスクの開始を設定できます。 |

## 管理プラグインからレジストリアクセス監視を管理する

このセクションでは、管理プラグインからレジストリアクセス監視タスクを設定する方法について説明します。

## レジストリアクセス監視タスクの設定

*レジストリアクセス監視タスク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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**システム監査**］セクションの［**レジストリアクセス監視**］サブセクションで、［**設定**］をクリックします。
   ［**レジストリアクセス監視**］ウィンドウが表示されます。
5. ［**レジストリアクセス監視の設定**］タブで、次の設定を行います：
   - ［**タスクモード**］グループで、リストから必要なオプションを選択します：
     - **ルールに従って操作をブロックする**

［**ルールに従って操作をブロックする**］モードを選択した場合、監視範囲に定義されている［**処理**］がブロックされます。また、［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］で定義されたプロセスはブロックされません。

既定では、［**統計のみ**］モードが適用されます。

- **統計のみ**

  監視範囲に対して［**統計のみ**］モードが選択されている場合、設定されたルールに従ってレジストリキーの処理の統計が収集されます。また、［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］で定義されたプロセスの統計は収集されません。

  既定では、［**統計のみ**］モードが適用されます。

- 必要に応じて、［**信頼ゾーンを適用する**］をオンまたはオフにします。

  ［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］に設定された［**信頼するプロセス**］が、設定されたルールに加えて監視範囲に適用されます。

  ［**信頼ゾーンを適用する**］がオフの場合、［**信頼ゾーン**］に設定された［**信頼するプロセス**］は監視範囲に適用されません。

  既定では、このチェックボックスはオフです。

6. タスクによって監視される監視範囲を追加します。
7. ［**タスク管理**］タブで、タスクのスケジュールを設定します。
8. ［**OK**］をクリックして、変更内容を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定変更の日時に関する情報は、システム監査ログに保存されます。

## 監視ルールの設定

監視ルールは、設定されたルールのリストの位置に沿って、連続して適用されます。

*監視範囲を追加するには：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**システム監査**］セクションの［**レジストリアクセス監視**］サブセクションで、［**設定**］をクリックします。
   ［**レジストリアクセス監視**］ウィンドウが表示されます。

5. ［**範囲のレジストリ変更の監視**］セクションで、［**追加**］をクリックします。

6. ［**レジストリアクセス監視領域**］ウィンドウで、**サポートされているマスク**を使用してパスを指定し、監視範囲を追加します。

   パスを入力する際に、マスクとして ？ と * を使用できます。

   ルートレジストリキーへのパスを入力する場合は、「HKEY_USERS」のように、マスクを使わずに完全パスで指定してください。以下は、有効なルートレジストリキーのリストです：

   - HKEY_LOCAL_MACHINE
   - HKLM
   - HKEY_CURRENT_USER
   - HKCU
   - HKEY_USERS
   - HKUS
   - HKU
   - HKEY_CURRENT_CONFIG
   - HKEY_CLASSES_ROOT
   - HKCR

   ルールを作成するときは、ルートキーにサポートされているマスクを使用しないでください。HKEY_CURRENT_USER などのルートキーのみを指定するか、HKEY_CURRENT_USER* などのすべての子キーのマスクを持つルートキーのみを指定すると、指定された子キーのアドレス指定に関する大量の通知が生成され、システムパフォーマンスに問題が生じます。HKEY_CURRENT_USER などのルートキー、または HKEY_CURRENT_USER* などのすべての子キーのマスクを持つルートキーを指定し、［**ルールに従って操作をブロックする**］モードをオンにすると、システムは OS の機能に必要なキーの読み取りや変更ができずに応答できなくなります。

7. ［**追加**］タブで、必要に応じて処理のリストを設定します。

8. 特定の［**レジストリ値**］を監視する場合、次の操作を行います：

   - ［**レジストリ値**］タブで、［**追加**］をクリックします。

- ［**レジストリ値のルール**］ウィンドウで、［**値のマスク**］を入力し、［**管理された処理**］を設定します。
- ［**OK**］をクリックして、変更内容を保存します。

9. ［**信頼するユーザー**］を定義するには、次の操作を行います：
   - ［**信頼するユーザー**］タブで、［**追加**］をクリックします。
   - ［**ユーザーまたはグループの選択**］ウィンドウで、定義された処理の実行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。
   - ［**OK**］をクリックして、変更内容を保存します。

   既定では、Kaspersky Embedded Systems Security においては信頼するユーザーリストに記載されていないすべてのユーザーを信頼しないユーザーとして取り扱い、重要なイベントを作成します。信頼するユーザーの場合、統計が収集されます。

10. ［**レジストリアクセス監視領域**］ウィンドウで［**OK**］をクリックします。

指定したルール設定は、［**レジストリアクセス監視**］タスクの定義した監視範囲にただちに適用されます。

## 管理コンソールからレジストリアクセス監視を管理する

このセクションでは、アプリケーションコンソールからレジストリアクセス監視タスクを設定する方法について説明します。

## レジストリアクセス監視タスクの設定

*レジストリアクセス監視タスクの全般的な設定を行うには：*

1. アプリケーションコンソールツリーで、［**システム監査**］フォルダーを展開します。
2. ［**レジストリアクセス監視**］サブフォルダーを選択します。
3. ［**レジストリアクセス監視**］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。
   ［**タスクの設定**］ウィンドウが表示されます。
4. ［**タスクの設定**］ウィンドウの［**全般**］タブで、次の設定を行います：
   - ［**タスクモード**］グループで、リストから必要なオプションを選択します：
     - **ルールに従って操作をブロックする**

［**ルールに従って操作をブロックする**］モードを選択した場合、監視範囲に定義されている［**処理**］がブロックされます。また、［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］で定義されたプロセスはブロックされません。

既定では、［**統計のみ**］モードが適用されます。

- **統計のみ**

  監視範囲に対して［**統計のみ**］モードが選択されている場合、設定されたルールに従ってレジストリキーの処理の統計が収集されます。また、［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］で定義されたプロセスの統計は収集されません。

  既定では、［**統計のみ**］モードが適用されます。

- 必要に応じて、［**信頼ゾーンを適用する**］をオンまたはオフにします。

  ［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］に設定された［**信頼するプロセス**］が、設定されたルールに加えて監視範囲に適用されます。

  ［**信頼ゾーンを適用する**］がオフの場合、［**信頼ゾーン**］に設定された［**信頼するプロセス**］は監視範囲に適用されません。

  既定では、このチェックボックスはオフです。

5. ［**スケジュール**］タブと［**詳細設定**］タブで、タスクの開始スケジュールを設定します。
6. ［**OK**］をクリックして、変更内容を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定変更の日時に関する情報は、システム監査ログに保存されます。

## 監視ルールの設定

監視ルールは、設定されたルールのリストの位置に沿って、連続して適用されます。

*監視範囲を追加するには：*

1. アプリケーションコンソールツリーで、［**システム監査**］フォルダーを展開します。
2. ［**レジストリアクセス監視**］サブフォルダーを選択します。
3. ［**レジストリアクセス監視**］フォルダーの結果ペインで、［**レジストリアクセスの監視ルール**］をクリックします。

   ［**レジストリアクセスの監視**］ウィンドウが表示されます。
4. ［**レジストリアクセスの監視**］ウィンドウで、サポートされているマスクを使用して［**監視するシステムレジストリキーを追加する**］にパスを指定し、［**追加**］をクリックします。

ルールを作成するときは、ルートキーにサポートされているマスクを使用しないでください。HKEY_CURRENT_USER などのルートキーのみを指定するか、HKEY_CURRENT_USER* などのすべての子キーのマスクを持つルートキーのみを指定すると、指定された子キーのアドレス指定に関する大量の通知が生成され、システムパフォーマンスに問題が生じます。
HKEY_CURRENT_USER などのルートキー、または HKEY_CURRENT_USER* などのすべての子キーのマスクを持つルートキーを指定し、［**ルールに従って操作をブロックする**］モードをオンにすると、システムは OS の機能に必要なキーの読み取りや変更ができずに応答できなくなります。

5. 選択した監視領域の［**処理**］タブで、必要に応じて処理のリストを設定します。
6. 特定の［**レジストリ値**］を監視する場合、次の操作を行います：
   a. ［**レジストリ値**］タブで、［**追加**］をクリックします。
   b. ［**レジストリ値のルール**］ウィンドウで、［**値のマスク**］を入力し、必要な［**管理された処理**］を設定します。
   c. ［**OK**］をクリックして、変更内容を保存します。
7. ［**信頼するユーザー**］を定義するには、次の操作を行います：
   a. ［**信頼するユーザー**］タブで、［**追加**］をクリックします。
   b. ［**ユーザーまたはグループの選択**］ウィンドウで、定義された処理の実行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。
   c. ［**OK**］をクリックして、変更内容を保存します。

既定では、Kaspersky Embedded Systems Security においては信頼するユーザーリストに記載されていないすべてのユーザーを信頼しないユーザーとして取り扱い、重要なイベントを作成します。信頼するユーザーの場合、統計が収集されます。

8. ［**レジストリアクセス監視領域**］ウィンドウで、［**保存**］をクリックします。
   指定したルール設定は、［**レジストリアクセス監視**］タスクの定義した監視範囲にただちに適用されます。

# Web プラグインからレジストリアクセス監視を管理する

このセクションでは、Web プラグインからレジストリアクセス監視タスクを設定する方法について説明します。

## レジストリアクセス監視タスクの設定

*Web プラグインからレジストリアクセス監視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**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。

4. ［**システム監査**］セクションを選択します。

5. ［**レジストリアクセス監視**］サブセクションの［**設定**］をクリックします。

6. ［**レジストリアクセス監視**］ウィンドウの［**レジストリアクセス監視の設定**］タブで、次の設定を行います：

   - ［**タスクモード**］グループで、リストから必要なオプションを選択します：

     - **ルールに基づき操作をブロック**

       ［**ルールに従って操作をブロックする**］モードを選択した場合、監視範囲に定義されている［**処理**］がブロックされます。また、［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］で定義されたプロセスはブロックされません。

       既定では、［**統計のみ**］モードが適用されます。

     - **統計のみ**

       監視範囲に対して［**統計のみ**］モードが選択されている場合、設定されたルールに従ってレジストリキーの処理の統計が収集されます。また、［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］で定義されたプロセスの統計は収集されません。

       既定では、［**統計のみ**］モードが適用されます。

   - 必要に応じて、［**信頼ゾーンを適用する**］をオンまたはオフにします。

     ［**信頼ゾーンを適用する**］がオンの場合、［**信頼ゾーン**］に設定された［**信頼するプロセス**］が、設定されたルールに加えて監視範囲に適用されます。

     ［**信頼ゾーンを適用する**］がオフの場合、［**信頼ゾーン**］に設定された［**信頼するプロセス**］は監視範囲に適用されません。

     既定では、このチェックボックスはオフです。

7. ［**タスク管理**］タブで、タスクの開始スケジュールを設定します。

8. ［**OK**］をクリックして、変更内容を保存します。

新しい設定は、実行中のタスクにすぐに適用されます。設定変更の日時に関する情報は、システム監査ログに保存されます。

## 監視ルールの設定

監視ルールは、設定されたルールのリストの位置に沿って、連続して適用されます。

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。

4. ［**システム監査**］セクションを選択します。

5. ［**レジストリアクセス監視**］サブセクションの［**設定**］をクリックします。

6. 表示される［**レジストリアクセス監視**］ウィンドウで、［**レジストリアクセス監視の設定**］タブを開きます。

7. ［**レジストリアクセス監視ルール**］セクションで、［**追加**］をクリックします。

8. ［**レジストリアクセス監視領域**］ウィンドウで、**サポートされているマスク**を使用して、［**範囲内のレジストリ操作を監視する**］にパスを指定します。

   パスを入力する際に、マスクとして ？ と * を使用できます。

   ルートレジストリキーへのパスを入力する場合は、「HKEY_USERS」のように、マスクを使わずに完全パスで指定してください。以下は、有効なルートレジストリキーのリストです：

   - HKEY_LOCAL_MACHINE
   - HKLM
   - HKEY_CURRENT_USER
   - HKCU
   - HKEY_USERS
   - HKUS
   - HKU
   - HKEY_CURRENT_CONFIG
   - HKEY_CLASSES_ROOT
   - HKCR

   ルールを作成するときは、ルートキーにサポートされているマスクを使用しないでください。HKEY_CURRENT_USER などのルートキーのみを指定するか、HKEY_CURRENT_USER* などのすべての子キーのマスクを持つルートキーのみを指定すると、指定された子キーのアドレス指定に関する大量の通知が生成され、システムパフォーマンスに問題が生じます。
   HKEY_CURRENT_USER などのルートキー、または HKEY_CURRENT_USER* などのすべての子キーのマスクを持つルートキーを指定し、［**ルールに基づき操作をブロック**］モードをオンにすると、システムは OS の機能に必要なキーの読み取りや変更ができずに応答できなくなります。

9. 選択した監視領域の［**処理**］タブで、必要に応じて処理のリストを設定します。

10. 特定の［**レジストリ値**］を監視する場合、次の操作を行います：

    a. ［**レジストリ値**］タブで、［**追加**］をクリックします。

b. ［**レジストリ値のルール**］ウィンドウで、［**値のマスク**］を入力し、必要な［**操作のリスト**］を設定します。

c. ［**OK**］をクリックして、変更内容を保存します。

11. ［**信頼するユーザー**］を定義するには、次の操作を行います：

a. ［**信頼するユーザー**］タブで、［**追加**］をクリックします。

b. ［**ユーザー名**］を入力するか［**セキュリティ識別子（SID）を Everyone に設定**］をクリックし、選択した処理の実行を許可するユーザーを定義します。

c. ［**OK**］をクリックして、変更内容を保存します。

既定では、Kaspersky Embedded Systems Security においては信頼するユーザーリストに記載されていないすべてのユーザーを信頼しないユーザーとして取り扱い、重要なイベントを作成します。信頼するユーザーの場合、統計が収集されます。

12. ［**レジストリアクセス監視領域**］ウィンドウで［**OK**］をクリックして変更を保存します。

指定したルール設定は、［**レジストリアクセス監視**］タスクの定義した監視範囲にただちに適用されます。

# Windows イベントログ監視

このセクションでは、Windows イベントログ監視タスクとタスク設定に関する情報について説明します。

# Windows イベントログ監視タスクについて

Windows イベントログ監視タスクの実行時に、Windows イベントログの監査結果に基づいて保護環境の整合性を監視します。サイバー攻撃の試みを示す可能性のある異常な動作が検知されると、管理者に通知されます。

Kaspersky Embedded Systems Security では、Windows イベントログ監視タスクによって使用される、ユーザー指定のルールまたはヒューリスティックアナライザーの設定で指定されたルールに基づいて、Windows イベントログの分析と侵入工作の特定が行われます。

## 定義済みのルールとヒューリスティック分析

既存のヒューリスティックに基づき、定義済みのルールを適用することにより、Windows イベントログ監視タスクを使用して保護対象システムの状態を監視できます。ヒューリスティックアナライザーは、攻撃の試みを示す可能性のある異常な活動を保護対象デバイス上で特定します。異常な動作を特定するテンプレートは、定義済みのルール設定で使用可能なルールに含まれています。

Windows イベントログ監視タスク用のルールリストには、7 つのルールが含まれています。各ルールを有効または無効にできます。既存のルールを削除したり、新しいルールを作成したりすることはできません。

以下の操作に対して、イベントを監視するルールの有効化の条件を設定できます：

- ブルートフォース攻撃の検知
- ネットワークログイン検知

タスク設定内で除外を設定することもできます。信頼するユーザーまたは信頼する IP アドレスからのログイン実施時は、ヒューリスティックアナライザーは起動しません。

> Kaspersky Embedded Systems Security では、ヒューリスティックアナライザーがタスクで使用されない場合、Windows ログの監視にヒューリスティックを使用しません。ヒューリスティックアナライザーは既定で有効化されています。

ルールが適用されると、Windows イベントログ監視タスクのログに*緊急イベント*が記録されます。

## Windows イベントログ監視タスクのルールのカスタマイズ

ルール設定を使用して、指定した Windows ログ内で選択したイベントを検知する際のルール有効化条件を指定および変更できます。Windows イベントログ監視のルールのリストには、既定で 4 つのルールがあります。これらのルールの有効化および無効化、ルールの削除、およびルール設定の編集が行えます。

各ルールに対して、次のルール有効化の条件を設定できます：

- Windows イベントログ内の記録 ID のリスト

ルールで指定されたイベント ID がイベントプロパティに含まれる場合、Windows イベントログ内で新しいレコードが作成された際にルールが有効化されます。各指定ルールに対する ID の追加と削除もできます。

- イベントソース

  各ルールに対して、Windows イベントログ内のログを指定できます。このログのみで、指定されたイベント ID を含む記録が検索されます。標準ログ（アプリケーション、セキュリティ、システム）のいずれかを選択するか、ソース選択フィールドに名前を入力してカスタムのログを指定できます。

  > 指定されたログが実際に Windows イベントログに存在するかは検証されません。

ルールが適用されると、Windows イベントログ監視タスクのログに緊急イベントが記録されます。

既定では、Windows イベントログ監視タスクでカスタムルールが適用されます。

> Windows イベントログ監視タスクを開始する前に、システム監査ポリシーが正しく設定されていることを確認してください。詳細は、Microsoft の記事を参照してください。

## Windows イベントログ監視タスクの既定の設定

Windows イベントログ監視タスクでは、次の表の既定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。

Windows イベントログ監視タスクの既定の設定

| 設定 | 既定値 | 説明 |
| --- | --- | --- |
| **Windows イベントログ監視にカスタムルールを適用する** | 適用されません。 | カスタムルールの追加や変更を行ったり、各ルールの有効と無効を切り替えることができます。 |
| **Windows イベントログ監視に定義済みのルールを適用する** | 適用されます。 | 保護対象デバイスで通常とは異なるふるまいを検知する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。 |
| **ブルートフォース攻撃の検知** | 300 秒でログオンの失敗回数が 10 回 | ヒューリスティックアナライザーの適用基準として使用する、試行の数と期間を指定できます。 |
| **ネットワークログオン** | 12:00:00 AM. | Kaspersky Embedded Systems Security がサインインの試行を異常なふるまいとして扱う時間帯の開始と終了を指定します。 |
| **除外リスト** | 適用されません。 | ヒューリスティックアナライザーを適用しないユーザーと IP アドレスを指定できます。 |
| タスク開始スケジュール | 最初の実行がスケジュール設定されていません。 | スケジュールでタスクを開始する設定を指定できます。 |

## 管理プラグインから Windows イベントログ監視のルールを管理する

このセクションでは、管理プラグインから Windows イベントログ監視のルールを追加または編集する方法について説明します。

# 定義済みタスクルールの設定

*Windows イベントログ監視タスクに対して定義済みのルールを設定するには、次の処理を実行します：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。
4. ［**システム監査**］セクションで、［**Windows イベントログ監視**］サブセクションの［**設定**］をクリックします。
   ［**Windows イベントログ監視**］ウィンドウが開きます。
5. ［**定義済みのルール**］タブを選択します。
6. ［**Windows イベントログ監視に定義済みのルールを適用する**］をオンまたはオフにします。

   タスクを実行するには、少なくとも 1 つの Windows イベントログ監視のルールを選択する必要があります。
7. 定義済みのルールのリストから、適用するルールを選択します：
   - システムにブルートフォース攻撃の可能性があるパターンがあります
   - Windows イベントログ悪用の可能性があるパターンがあります
   - インストールされた新しいサービスによる異常処理が検出されました
   - 明示的な資格証明を使用する異常ログオンが検出されました
   - システムに Kerberos 偽造 PAC（MS14-068）攻撃の可能性があるパターンがあります
   - 組み込みの特権グループ Administrators に向けた異常なアクションが検出されました
   - ネットワークログオンセッション時に異常な活動が検出されました
8. 選択したルールを設定するには、［**詳細設定**］をクリックします。
   ［**Windows イベントログ監視**］ウィンドウが開きます。

9. ［**ブルートフォース攻撃の検知**］セクションで、ヒューリスティックアナライザーの適用基準として使用する、試行の数と期間を設定します。

10. ［**ネットワークログオンの検出**］セクションで、Kaspersky Embedded Systems Security がサインインの試行を異常な動作として扱う時間帯の開始と終了を指定します。

11. ［**除外リスト**］タブを選択します。

12. 信頼するユーザーを追加するため、次の処理を実行します：

    a. ［**参照**］をクリックします。

    b. ユーザーを選択します。

    c. ［**OK**］をクリックします。
    選択したユーザーが、信頼するユーザーのリストに追加されます。

13. 信頼する IP アドレスを追加するため、次の処理を実行します：

    a. IP アドレスを入力します。

    b. ［**追加**］をクリックします。

14. 入力した IP アドレスが、信頼する IP アドレスのリストに追加されます。

15. ［**タスク管理**］タブで、タスクの開始スケジュールを設定します。

16. ［**Windows イベントログ監視**］ウィンドウで［**OK**］をクリックします。

Windows イベントログ監視のタスク設定が保存されます。

## 管理プラグインから Windows イベントログ監視のルールを追加する

*新しい Windows イベントログ監視のカスタムルールを追加および設定するには、次の処理を実行します：*

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**ポリシーのプロパティ**ウィンドウを開きます。
   - 単一の保護対象デバイスに対してアプリケーションを設定するには、［**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。

     Kaspersky Security Center のアクティブポリシーがデバイスに適用され、アプリケーションの設定の変更がブロックされている場合、［**アプリケーションの設定**］ウィンドウでこれらの設定を編集することはできません。

4. ［**システム監査**］セクションで、［**Windows イベントログ監視**］サブセクションの［**設定**］をクリックします。

［**Windows イベントログ監視**］ウィンドウが開きます。

5. ［**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**］をオンまたはオフにします。

   事前設定ルールを Windows イベントログ監視のルールに適用するかどうかをコントロールできます。Windows イベントログ監視に適用するルールに該当するチェックボックスをオンにします。

6. 新しいカスタムルールを追加するには［**追加**］をクリックします。
   ［**Windows イベントログ監視のカスタムルール**］ウィンドウが開きます。

7. ［**全般**］セクションで新しいルールに関する次の情報を指定します：

   - **ルール名**
   - **ソース**

8. ［**ルール有効化の条件**］セクションで、ルールを有効化するイベント ID を指定します：

   a. ID を入力します。

   b. ［**追加**］をクリックします。
      入力したイベント ID がリストに追加されます。各ルールに対して個数の制限なく ID を追加できます。

9. ［**OK**］をクリックします。
   Windows イベントログ監視ルールがルールのリストに追加されます。

## アプリケーションコンソールから Windows イベントログ監視のルールを管理する

このセクションでは、アプリケーションコンソールから Windows イベントログ監視のルールを追加または編集する方法について説明します。

## 定義済みタスクルールの設定

*ヒューリスティックアナライザーを Windows イベントログ監視タスクに対して設定する次の処理を行います：*

1. アプリケーションコンソールツリーで、［**システム監査**］フォルダーを展開します。

2. ［**Windows イベントログ監視**］サブフォルダーを選択します。

3. ［**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。
   ［**タスクの設定**］ウィンドウが表示されます。

4. ［**定義済みのルール**］タブを選択します。

5. ［**Windows イベントログ監視に定義済みのルールを適用する**］をオンまたはオフにします。

タスクを実行するには、少なくとも 1 つの Windows イベントログ監視のルールを選択する必要があります。

6. 定義済みのルールのリストから、適用するルールを選択します：
   - システムにブルートフォース攻撃の可能性があるパターンがあります
   - Windows イベントログ悪用の可能性があるパターンがあります
   - インストールされた新しいサービスによる異常処理が検出されました
   - 明示的な資格証明を使用する異常ログオンが検出されました
   - システムに Kerberos 偽造 PAC（MS14-068）攻撃の可能性があるパターンがあります
   - 組み込みの特権グループ Administrators に向けた異常なアクションが検出されました
   - ネットワークログオンセッション時に異常な活動が検出されました
7. 選択したルールを設定するには、［**拡張**］タブに移動します。
8. ［**ブルートフォース攻撃の検知**］セクションで、ヒューリスティックアナライザーの適用基準として使用する、試行の数と期間を設定します。
9. ［**ネットワークログオン**］セクションで、Kaspersky Embedded Systems Security がサインインの試行を異常な動作として扱う時間帯の開始と終了を指定します。
10. ［**除外リスト**］タブを選択します。
11. 信頼するユーザーを追加するため、次の処理を実行します：
    a. ［**参照**］をクリックします。
    b. ユーザーを選択します。
    c. ［**OK**］をクリックします。
    選択したユーザーが、信頼するユーザーのリストに追加されます。
12. 信頼する IP アドレスを追加するため、次の処理を実行します：
    a. IP アドレスを入力します。
    b. ［**追加**］をクリックします。
    入力した IP アドレスが、信頼する IP アドレスのリストに追加されます。
13. ［**スケジュール**］タブと［**詳細設定**］タブを選択し、タスクの開始スケジュールを設定します。
14. ［**タスクの設定**］ウィンドウで［**OK**］をクリックします。
    Windows イベントログ監視のタスク設定が保存されます。

# アプリケーションコンソールから Windows イベントログ監視のルールを追加する

*新しい Windows イベントログ監視のカスタムルールを追加および設定するには：*

1. アプリケーションコンソールツリーで、［**システム監査**］フォルダーを展開します。
2. ［**Windows イベントログ監視**］サブフォルダーを選択します。
3. ［**Windows イベントログ監視**］フォルダーの結果ペインで、［**Windows イベントログ監視のルール**］をクリックします。
4. ［**Windows イベントログ監視のルール**］ウィンドウが開きます。
5. ［**Windows イベントログ監視にカスタムルールを適用する。設定されたルールはチェックボックスをオンにするまで適用されません。**］をオンまたはオフにします。

   定義済みのルールを Windows イベントログ監視タスクに適用するかどうかをコントロールできます。Windows イベントログ監視に適用するルールに該当するチェックボックスをオンにします。

6. 新しいカスタムルールを作成するには：
   a. 新しいルール名を入力します。
   b. ［**追加**］をクリックします。
      作成されたルールは、一般ルールリストに追加されます。
7. 任意のルールを設定するには：
   a. リストからルールを選択します。
      ウィンドウの右の領域にある［**説明**］タブに、ルールに関する一般情報が表示されます。

      新しいルールの説明は空白です。

   b. ［**ルールの説明**］タブを選択します。
8. ［**全般**］セクションで新しいルールに関する次の情報を指定します：
   - **ルール名**
   - **ログの名前**
   - **ソース**
9. ［**イベント ID**］セクションで、ルールを有効化するイベント ID を指定します：
   a. イベント ID を入力します。
   b. ［**追加**］をクリックします。

入力したイベント ID がリストに追加されます。各ルールに対して個数の制限なく ID を追加できます。

10. ［**保存**］をクリックします。
    設定された Windows イベントログ監視ルールが適用されます。

## Web プラグインから Windows イベントログ監視のルールを管理する

*Web プラグインから Windows イベントログ監視のルールを追加して設定するには：*

1. Web コンソールのメインウィンドウで、［**デバイス**］-［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］タブを選択します。
4. ［**システム監査**］セクションを選択します。
5. ［**Windows イベントログ監視**］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。

Windows イベントログ監視タスクの設定

| 設定 | 説明 |
| --- | --- |
| **Windows イベントログ監視にカスタムルールを適用する** | カスタムルールの追加や変更を行ったり、各ルールの有効と無効を切り替えることができます。<br>この設定は、カスタムルールのリストにある表で使用できます。 |
| **Windows イベントログ監視に定義済みのルールを適用する** | 保護対象デバイスで通常とは異なるふるまいを検知する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。<br>この設定は、カスタムルールのリストにある表で使用できます。 |
| **誤ったパスワードが指定の頻度で入力された場合にブルートフォース攻撃として検知します** | ヒューリスティックアナライザーの適用基準として使用する、試行の数と期間を指定できます。 |
| **定義された期間内のネットワークログオンを検出します。** | Kaspersky Embedded Systems Security がサインインの試行を異常なふるまいとして扱う時間帯の開始と終了を指定します。 |
| **ユーザーによる除外** | ヒューリスティックアナライザーを適用しないユーザーを指定できます。 |
| **除外された IP アドレス** | ヒューリスティックアナライザーを適用しない IP アドレスを指定できます。 |
| **タスク管理** | 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

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：

- ［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、Kaspersky Embedded Systems Security の起動のたびに実行されます。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、およびプロセスのメモリがスキャンされます。このタスクが実行されるたびに、感染していないブートセクターのコピーが作成されます。次回のタスク起動時にこれらのセクターで脅威が検知された場合は、バックアップコピーと置き換えられます。

  保護対象デバイスがスリープモードまたは休止状態モードから復帰した後、［オペレーティングシステムの起動時にスキャン］タスクが実行されない場合があります。このタスクは、保護対象バイスの再起動時または完全なシャットダウン後の起動時にのみ実行されます。

- 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。%windir%\system32 などのシステムフォルダーのファイルがスキャンされます。Kaspersky Embedded Systems Security は、［推奨］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。

- 隔離のスキャンタスクは、定義データベースのアップデートのたびに、スケジュールに従って既定で実行されます。隔離のスキャンタスクの対象範囲は変更できません。

- アプリケーションの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。

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、Kaspersky Embedded Systems Security が操作できる保護対象デバイスのファイルリソースのツリーまたはリストとして表示されます。既定では、保護対象デバイスのネットワークファイルリソースがリストビューモードで表示されます。

リストビューは管理プラグインでのみ使用できます。

*ネットワークファイルリソースをアプリケーションコンソールのツリービューモードで表示するには：*

［**スキャン範囲の設定**］ウィンドウの左上部にあるドロップダウンリストより、［**ツリービュー**］を選択します。

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またはツリー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。

☑ このフォルダーの1つ以上のサブフォルダーがスキャン範囲から除外されます。または、このサブフォルダーと親フォルダーのセキュリティ設定が異なります（ツリービューモードの場合のみ）。

☑アイコンは、親フォルダーを除くすべてのサブフォルダーが選択されている場合に表示されます。この場合、親フォルダーのファイルとフォルダーの構成の変更は、選択したサブフォルダーのスキャン範囲の作成中は自動的に無視されます。

アプリケーションコンソールを使用して、［仮想ドライブ］をスキャン範囲に追加することもできます。仮想フォルダーの名前は、青色のフォントで表示されます。

### 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、あるいはデバイスのファイルリソースツリーまたは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。

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（**最高のパフォーマンス**、**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ツリーまたはリストで、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）。

フォルダーの一連の設定をテンプレートに保存して、後で他のフォルダーに適用することができます。

## 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ツリーまたはリストが、［**スキャン範囲の設定**］ウィンドウに表示されます。

ファイルリソースのツリーまたはリストには、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：

- **マイコンピューター**：Kaspersky Embedded Systems Security は保護対象デバイス全体をスキャンします。
- **ローカルハードディスク**：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。
- **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。
- **ネットワーク**：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。

- **システムメモリ**：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。
- **スタートアップオブジェクト**：レジストリキーや設定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。
- 共有フォルダー：保護対象デバイスにある共有フォルダーをスキャン範囲に含めることができます。
- **仮想ドライブ**：共有のクラスタードライブなどの、保護対象デバイスに接続される仮想フォルダー、ファイル、およびドライブを保護範囲に含めることができます。

  SUBST コマンドを使用して作成した仮想ドライブは、アプリケーションコンソールの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。仮想ドライブのオブジェクトをスキャンするには、仮想ドライブに関連付けられた保護対象デバイスのフォルダーをスキャン範囲に含めます。

既定では、ネットワークファイルリソースツリーで定義済みスキャン範囲を表示して設定できます。また、その構成時にスキャン範囲設定のネットワークファイルリソースリストに定義済みの範囲を追加することもできます。

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：

- オペレーティングシステムの起動時にスキャン：
  - **ローカルハードディスク**
  - **リムーバブルドライブ**
  - **システムメモリ**
- 簡易スキャン：
  - **ローカルハードディスク**（Windows フォルダーを除く）
  - **リムーバブルドライブ**

- **システムメモリ**
- **スタートアップオブジェクト**

- その他のタスク：
  - **ローカルハードディスク**（Windows フォルダーを除く）
  - **リムーバブルドライブ**
  - **システムメモリ**
  - **スタートアップオブジェクト**
  - **共有フォルダー**

# 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 タスクによってさまざま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作成と利用：アプリケーション起動コントロールルールの自動作成を使用して、 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、ルール作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

［**iChecker を使用する**］、［**iSwift を使用する**］、［**ヒューリスティックアナライザーを使用する**］、［**ファイルの Microsoft の署名をチェックする**］のセキュリティ設定は、事前設定のセキュリティレベルには含まれません。［**iChecker を使用する**］、［**iSwift を使用する**］、［**ヒューリスティックアナライザーを使用する**］、［**ファイルの Microsoft の署名をチェックする**］の設定が変更されても、選択した事前設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ツリーで選択したフォルダーに対して、次の 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：［**最高のパフォーマンス**］、［**推奨**］、［**最大の保護**］。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）。

### 最高のパフォーマンス

［**最高のパフォーマンス**］セキュリティレベルは、保護対象デバイスでの 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で高い水準のデバイスセキュリティ要件が求められる場合、［**最大の保護**］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 | | |
|---|---|---|---|
| | 最高のパフォーマンス | 推奨 | 最大の保護 |
| **オブジェクトのスキャン** | 形式に基づく | 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 |
| **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 | 推奨処理を実行（駆除、駆除できない場合は削除） | 駆除、駆除できない場合は削除 |
| **感染の可能性があるオブジェクトの処理** | 隔離 | 推奨処理を実行（隔離） | 隔離 |
| **除外するファイル** | なし | なし | なし |
| **検知しない** | 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 |
| **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 |
| **NTFS 代替データストリームをスキャン** | 有効 | 有効 | 有効 |
| **ディスクのブートセクターと MBR をスキャン** | 有効 | 有効 | 有効 |
| **複合オブジェクトのスキャン** | • SFX アーカイブ*<br>• 圧縮されたオブジェクト*<br>• OLE 埋め込みオブジェクト*<br>* 新規および変更されたオブジェクトのみ | • SFX アーカイブ*<br>• 圧縮されたオブジェクト*<br>• OLE 埋め込みオブジェクト*<br>* すべてのオブジェクト | • アーカイブ*<br>• SFX アーカイブ*<br>• メールデータベース*<br>• 通常のメール* |

| | | | |
|---|---|---|---|
| | | | • 圧縮されたオブジェクト*<br>• OLE 埋め込みオブジェクト*<br>* すべてのオブジェクト |

## リムーバブルドライブスキャンについて

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 では、オンデマンドスキャンタスクを使用してリムーバブルドライブをスキャンします。リムーバブルドライブが接続されると、アプリケーションは自動的に新しいオンデマンドスキャンタスクを作成し、スキャンの完了後にタスクを削除します。作成されたタスクは、リムーバブルドライブスキャンに対してあらかじめ定義されたセキュリティレベルで実行されます。一時的なオンデマンドスキャンタスクの設定は変更できません。

Kaspersky Embedded Systems Security を定義データベースなしでインストールする場合、リムーバブルドライブスキャンは利用できません。

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。MTP 接続したモバイルデバイスはスキャンしません。

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、各リムーバブルドライブのオンデマンドスキャンタスクのスキャン結果はログにあります。

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

| 設定 | 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** | チェックボックスはオフです | 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。 |
| **格納データ容量がこの値以下ならリムーバブルドライブをスキャンする（MB）** | 8192 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** | 最大 | 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 |

| | | |
|---|---|---|
| **ィレベルでスキャンする** | の保護 | 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>• **最高のパフォーマンス**<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。 |

## ベースラインに基づくファイル変更監視タスクについて

ベースラインに基づくファイル変更監視タスクが実行中の場合、Kaspersky Embedded Systems Security はロックされたファイルやフォルダー、ファイルのショートカット、およびクラウドファイルをチェックしません。

ベースラインに基づくファイル変更監視タスクは、ファイルのハッシュ（MD5 ハッシュまたは SHA256 ハッシュ）とベースラインを比較することで、監視範囲のファイルの整合性を監視します。

最初のベースラインに基づくファイル変更監視タスクの実行時に、Kaspersky Embedded Systems Security はタスクの監視範囲でファイルのハッシュを計算 / 保存して、ベースラインを作成します。ベースラインに基づくファイル変更監視タスクの監視範囲が変更された場合、Kaspersky Embedded Systems Security はタスクの監視範囲でファイルのハッシュを計算 / 保存して、次のベースラインに基づくファイル変更監視タスクの実行時にベースラインをアップデートします。ベースラインに基づくファイル変更監視タスクが削除された場合、Kaspersky Embedded Systems Security はこのベースラインに基づくファイル変更監視タスクのベースラインを削除します。

コマンドラインを使用することで、ベースラインに基づくファイル変更監視タスクを削除せずにベースラインを削除できます。

ベースラインに基づくファイル変更監視タスクは、監視範囲でファイルの次の変更を管理します：

- ベースラインに存在しないファイルが監視範囲に含まれている
- ベースラインに存在するファイルが監視範囲に含まれていない
- 監視範囲のファイルのハッシュが、ベースラインのそのファイルのハッシュと異なる

ベースラインに基づくファイル変更監視タスクは、ファイルの属性と代替のストリームの変更を追跡しません。

ファイルまたはフォルダーがアクセスできない場合、ベースラインの作成中に Kaspersky Embedded Systems Security はこのファイルまたはフォルダーを追加せず、ベースラインに基づくファイル変更監視タスクの実行中に、ファイルのチェックサムの計算失敗に関するイベントを作成します。

ファイルまたはフォルダーは、次の理由でアクセスできないことがあります：

- 指定されたパスが存在しない
- マスクによって指定されたファイルの種別が指定されたパスに存在しない
- 指定されたファイルがロックされている
- 指定されたファイルが空である

## コンテキストメニューからオンデマンドスキャンタスクの開始を有効にする

Microsoft Windows エクスプローラーのコンテキストメニューから、1つまたは複数のファイルのオンデマンドスキャンタスクの開始を有効にできます。

*コンテキストメニューからオンデマンドスキャンタスクの開始を有効にするには：*

1. REG ファイルを次のように作成します：

```
Windows Registry Editor Version 5.0.0

[HKEY_CLASSES_ROOT\Directory\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\*\shell\kess\command]

@="C:\\Temp\\scan.cmd \"%1\""

[HKEY_CLASSES_ROOT\Directory\shell\kess]

@="Scan with Kaspersky Embedded Systems Security\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\Directory\shell\kess\DefaultIcon]

@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess]

@="Scan with Kaspersky Embedded Systems Security\"

"Icon"="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_CLASSES_ROOT\*\shell\kess\DefaultIcon]
@="\"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavtrayr.dll\",0"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers]

"C:\\Program Files (x86)\\Kaspersky Lab\\Kaspersky Embedded Systems Security\\kavshell.exe"="~ RUNASADMIN"
```

> Kaspersky Embedded Systems Security インストールフォルダーの実際の場所を指定する必要があります。

2. `scan.cmd` ファイルを次の内容で作成します：

```
@echo off
set LOGNAME=%RANDOM%

"C:\Program Files (x86)\Kaspersky Lab\Kaspersky Embedded Systems
Security\kavshell.exe" scan "%~1" /W:c:\temp\%LOGNAME%.txt

echo Scanning is in progress...
type c:\temp\%LOGNAME%.txt
del c:\temp\%LOGNAME%.txt

timeout /t -1
```

scan.cmd ファイルには、次の情報を含める必要があります：

- kavshell.exe ファイルの場所。
- スキャン結果を含む一時ファイルの場所。
- KAVSHELL SCAN コマンドのパラメータ。
- タスクが完了した時にコンソールウィンドウを閉じるためのタイムアウト値。

3. scan.cmd ファイルを、REG ファイル [HKEY_CLASSES_ROOT\Directory\shell\kess\command] で指定されたフォルダーにコピーします。

   例では、C:\Temp フォルダーを使用しています。

オペレーティングシステムを再起動する必要はありません。

## 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

| 設定 | 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>• **オペレーティングシステムの起動時にスキャン**：共有フォルダーと自動実行オブジェクトを除いた保護対象デバイス全体が対象です。<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>• カスタムの**オンデマンドスキャン**タスク：保護対象デバイス全体が対象です。 | スキャン範囲を変更することができます。スキャン範囲は、**隔離のスキャン**および**アプリケーションの整合性チェック**ックのシステムタスクでは設定できません。 |

| | | |
|---|---|---|
| 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。 |
| **ヒューリスティックアナライザーを使用する** | 簡易スキャン、オペレーティングシステムの起動時のスキャン、カスタムタスクでは**中**の分析レベルで使用されます。<br>隔離のスキャンタスクでは**高**の分析レベルで使用されます。 | 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。隔離のスキャンタスクの分析レベルは変更できません。<br>ヒューリスティクスアナライザーは、アプリケーションの整合性チェックおよびベースラインに基づくファイル変更監視タスクでは使用されません。 |
| **信頼ゾーンを適用する** | 適用されます（隔離のスキャンタスクには適用されません）。 | 選択したタスクで使用できる一般的な信頼するオブジェクト。 |
| **スキャンに KSN を使用する** | 適用されます。 | Kaspersky Security Network のクラウドサービスのインフラストラクチャを使用して、デバイスの保護を改善することができます。 |
| 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。 | 隔離のスキャンタスクとアプリケーションの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**（優先度「低」） | 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に適用されます：<br>• オペレーティングシステムの起動時にスキャン - **アプリケーションの起動時**<br>• 簡易スキャン - **週単位**<br>• 隔離のスキャン - **定義データベースのアップデート後**<br>• アプリケーションの整合性チェック - **日単位**<br>新しく作成されたカスタムタスクでは使用されません。 | スケジュールによるタスクの開始を設定できます。 |
| スキャンの実行の登録とデバイスの保護ステ | デバイスの保護ステータスは、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。 | 簡易スキャンの実行の登録は、次の方法で設定できます：<br>• 簡易スキャンタスクの開始スケジュール設定を編集する。 |

| | | |
|---|---|---|
| ータスの更新 | | • 簡易スキャンタスクのスキャン範囲を編集する。<br>• カスタムオンデマンドスキャンタスクを作成する。 |

## 管理プラグインからオンデマンドスキャンタスクを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの1つまたはすべての保護対象デバイスのタスクを設定する方法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

*新しいカスタムオンデマンドスキャンタスクの作成を開始するには：*

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選択します。
   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**］タブを開きます。
   d. ［**タスクの作成**］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に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」**］タブを開きます。

c. ［**処理を実行**］ドロップダウンリストで、［**新規タスク**］オプションを選択します。

［**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**］をクリックします。
［**設定**］ウィンドウが開きます。

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：*

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。

## オンデマンドスキャンタスクのプロパティウィンドウ

*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プロパティを開くには：*

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。

## オンデマンドスキャンタスクの作成

*カスタムオンデマンドスキャンタスクを作成するには：*

1. ［新規タスクウィザード］で、［**設定**］ウィンドウを開きます。

2. 目的の［**タスクの作成方法**］を選択します。

3. ［**次へ**］をクリックします。

4. ［**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。

- すべての重要な領域をスキャン対象から除外するには、各行のコンテキストメニューを開いて［範囲の削除］を選択します。
- 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. ［**スキャン範囲**］テーブルを右クリックし、［**範囲の追加**］を選択するか、［**追加**］をクリックします。
  b. ［**スキャン範囲にオブジェクトを追加**］の［**定義済みの範囲**］リストで定義済みの範囲を選択し、保護対象デバイスまたはその他のネットワーク保護対象デバイスの保護対象デバイスディスク、フォルダー、ネットワークオブジェクト、またはファイルを指定して［**OK**］をクリックします。
- サブフォルダーまたはファイルをスキャンから除外するには、ウィザードの［**スキャン範囲**］ウィンドウで追加されたフォルダー（ディスク）を選択します。
  a. コンテキストメニューを開いて、［**設定**］を選択します。
  b. ［**セキュリティレベル**］タブの［**設定**］をクリックします。
  c. ［**オンデマンドスキャンの設定**］ウィンドウの［**全般**］タブで、［**サブフォルダー**］と［**サブファイル**］をオフにします。
- スキャン範囲のセキュリティ設定を変更するには：
  a. 設定を行う範囲のコンテキストメニューを開き、［**設定**］を選択します。
  b. ［**オンデマンドスキャンの設定**］ウィンドウで、定義済みのセキュリティレベルの1つを選択するか、［**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と同じ方法で設定されます。
- 追加されたスキャン範囲内で埋め込みオブジェクトをスキップするには：
  a. ［**スキャン範囲**］テーブルのコンテキストメニューを開き、［**除外の追加**］を選択します。
  b. 除外するオブジェクトを指定します：［**定義済みの範囲**］リスト内で定義済み範囲を選択し、保護対象デバイスまたは別のネットワーク保護対象デバイス上の保護対象デバイスディスク、フォルダー、ネットワークオブジェクト、またはファイルを指定します。
  c. ［**OK**］をクリックします。

5. ［**オプション**］ウィンドウで、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統合を設定します。

   - ヒューリスティックアナライザーの使用を設定します。
   - 信頼ゾーンのリストに追加されたオブジェクトをタスクのスキャン範囲から除外する場合は、［**信頼ゾーンを適用する**］をオンにします。
   - Kaspersky Security Network クラウドサービスをタスクに使用するには、［**スキャンに KSN を使用する**］をオンにします。
   - タスクが実行される処理対象プロセスに優先度［*低*］を割り当てるには、［**オプション**］ウィンドウで［**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。

   - 作成したタスクを簡易スキャンタスクとして使用する場合、［**オプション**］ウィンドウで［**タスクを簡易スキャンとする**］をオンにしてください。

6. ［**次へ**］をクリックします。
7. ［**スケジュール**］ウィンドウで、タスクの開始スケジュールを設定します。
8. ［**次へ**］をクリックします。
9. ［**タスクを実行するアカウントの選択**］ウィンドウで、使用するアカウントを指定します。
10. ［**次へ**］をクリックします。
11. タスク名を指定します。
12. ［**次へ**］をクリックします。

    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。

    ［**タスクの作成を終了**］ウィンドウが開きます。

13. オプションで［**ウィザード完了後にタスクを実行する**］をオンにすると、ウィザードの終了後にタスクを実行することができます。
14. ［**完了**］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。

## オンデマンドスキャンタスクへの簡易スキャンのステータスの割り当て

既定では、簡易スキャンタスクの実行頻度が Kaspersky Embedded Systems Security のイベント生成しきい値の［*簡易スキャンが長期間実行されていません*］設定より低い場合に、Kaspersky Security Center により保護対象デバイスに対して*警告*の状態が割り当てられます。

*1 つの管理グループですべての保護対象デバイスのスキャンを設定するには：*

1. グループのオンデマンドスキャンタスクを作成します。
2. タスクウィザードの［**オプション**］ウィンドウで、［**タスクを簡易スキャンとする**］をオンにします。指定したタスク設定（スキャン範囲およびセキュリティ設定）が、グループ内のすべての保護対象デバイスに適用されます。タスクのスケジュールを設定します。

   ［**タスクを簡易スキャンとする**］は、保護対象デバイスのグループに対してオンデマンドスキャンタスクを作成する時、または**タスクのプロパティ**ウィンドウでオンにできます。

3. 新しいポリシーまたは既存のポリシーを使用して、グループの保護対象デバイスのローカルシステムオンデマンドスキャンタスクのスケジュールによる開始を無効にします。

Kaspersky Security Center 管理サーバーによって、保護対象デバイスのセキュリティの状態が評価され、簡易スキャンのローカルシステムタスクの結果ではなく、前回のタスク実行結果と簡易スキャンの状態に基づいて、その状態が通知されます。

*簡易スキャン*の状態は、オンデマンドスキャンのグループタスクと、保護対象デバイスのグループのタスクの両方に割り当てることができます。

アプリケーションコンソールを使用して、オンデマンドスキャンタスクが簡易スキャンタスクであるかを確認できます。

アプリケーションコンソールで、タスクのプロパティに［**タスクを簡易スキャンとする**］チェックボックスが表示されますが、この設定を編集することはできません。

## 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。バックグラウンドのオンデマンドスキャンタスクのプロセスの最大数を指定できます。

*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：*

1. **オンデマンドスキャンのプロパティ**ウィンドウを開きます。
2. ［**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。
3. ［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。

## 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。既定では、このチェックボックスは簡易スキャンタスクでのみオンになっており、このタスクでは変更できません。

デバイスの保護ステータスに結果を反映させるオンデマンドスキャンタスクの選択は、Kaspersky Security Center からのみ実行できます。

## タスクのスキャン範囲の設定

オペレーティングシステム起動時の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、Kaspersky Embedded Systems Security 自体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（［**スタート**］ - ［**すべてのプログラム**］ - ［**Kaspersky Embedded Systems Security**］ - ［**Kaspersky Embedded Systems Security の変更または削除**］の順に選択します）。セットアップウィザードで、［**インストール済みコンポーネントの修復**］をオンにして、［**次へ**］をクリックします。次に、［**製品の推奨設定を復元する**］をオンにします。

*既存のオンデマンドスキャンタスクのスキャン範囲を編集するには：*

1. **オンデマンドスキャンのプロパティ**ウィンドウを開きます。
2. ［**スキャン範囲**］タブを選択します。
3. スキャン範囲に項目を含めるには：
   a. スキャン範囲のリストの空白部分でコンテキストメニューを開きます。
   b. コンテキストメニューで［**範囲の追加**］を選択します。
   c. 表示された［**スキャン範囲にオブジェクトを追加**］ウィンドウで、追加するオブジェクトの種別を選択します：
      - **定義済みの範囲**：保護対象デバイスでいずれかの定義済み範囲を追加します。ドロップダウンリストで、目的のスキャン範囲を選択します。
      - **ディスク、フォルダー、またはネットワークの場所**：個別のドライブ、フォルダー、またはネットワークオブジェクトをスキャン範囲に含めます。［**参照**］をクリックして目的の範囲を選択します。
      - **ファイル**：個別のファイルをスキャン範囲に含めます。［**参照**］をクリックして目的の範囲を選択します。

オブジェクトが既にスキャン範囲からの除外対象として追加されている場合、スキャン範囲には追加できません。

4. 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するか、次の手順を実行します：

   a. スキャン範囲を右クリックして、コンテキストメニューを開きます。

   b. コンテキストメニューで、［**除外の追加**］を選択します。

   c. ［**除外の追加**］ウィンドウで、スキャン範囲にオブジェクトを追加する時に使用する手順に従い、スキャン範囲からの除外対象として追加するオブジェクトの種別を選択します。

5. スキャン範囲または追加する除外対象を変更するには、該当するスキャン範囲のコンテキストメニューで［**範囲の編集**］を選択します。

6. ネットワークファイルリソースのリストに以前追加したスキャン範囲または除外対象を非表示にするには、該当するスキャン範囲のコンテキストメニューで［**範囲の削除**］を選択します。

   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。

7. ［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：［**最高のパフォーマンス**］、［**推奨**］、［**最大の保護**］。

*事前に定義されたセキュリティレベルのいずれかを選択するには：*

1. **オンデマンドスキャン**の**プロパティ**ウィンドウを開きます。
2. ［**スキャン範囲**］タブを選択します。
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。
   ［**オンデマンドスキャンの設定**］ウィンドウが開きます。
5. ［**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。
   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。
6. ［OK］をクリックします。
7. **オンデマンドスキャン**の**プロパティ**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。

## 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。

*手動でセキュリティを設定するには：*

1. **オンデマンドスキャンのプロパティ**ウィンドウを開きます。
2. ［**スキャン範囲**］タブを選択します。
3. セキュリティ設定を行うスキャン範囲のリストから項目を選択します。

   セキュリティ設定を含む定義済みのテンプレートは、スキャン範囲内の選択したフォルダーまたは項目に適用できます。

4. ［**設定**］をクリックします。
   ［**オンデマンドスキャンの設定**］ウィンドウが開きます。
5. 要件に従って、選択したフォルダーや項目のセキュリティ設定を、次のタブで指定します：
   - **全般**
   - **処理**
   - **パフォーマンス**
   - **階層型ストレージ**
6. ［**オンデマンドスキャンの設定**］ウィンドウで［**OK**］をクリックします。
7. ［**スキャン範囲**］ウィンドウで、［**OK**］をクリックします。

新しいスキャン範囲の設定が保存されます。

## タスクの全般的な設定

*オンデマンドスキャンタスクの全般的な設定を行うには：*

1. **オンデマンドスキャン**の**プロパティ**ウィンドウを開きます。
2. ［**スキャン範囲**］タブを選択します。
3. ［**設定**］をクリックします。
   ［**オンデマンドスキャンの設定**］ウィンドウが開きます。
4. ［**設定**］をクリックします。

5. ［**全般**］タブの［**オブジェクトのスキャン**］セクションで、スキャンの範囲に含めるオブジェクト種別を指定します：

   - **スキャン対象オブジェクト**：
     - **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**
     - **指定の拡張子リストによってオブジェクトをスキャン**
   - **サブフォルダー**
   - **サブファイル**
   - **ディスクのブートセクターと MBR をスキャン**
   - **NTFS 代替データストリームをスキャン**

6. ［**パフォーマンス**］セクションで、［**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。

   チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の［**すべての / 新しい（～のみ）**］をクリックします。

7. ［**複合オブジェクトのスキャン**］セクションで、スキャンの範囲に含める複合オブジェクトを指定します：

   - **すべてのアーカイブ** / **新しい アーカイブのみ** / アーカイブ
   - **すべての SFX アーカイブ** / **新しい SFX アーカイブのみ** / SFX アーカイブ
   - **すべてのメールデータベース** / **新しい メールデータベースのみ** / メールデータベース
   - **すべての圧縮されたオブジェクト** / **新しい 圧縮されたオブジェクトのみ** / 圧縮されたオブジェクト
   - **すべての通常のメール** / **新しい 通常のメールのみ** / 通常のメール
   - **すべての OLE 埋め込みオブジェクト** / **新しい OLE 埋め込みオブジェクトのみ** / OLE 埋め込みオブジェクト

8. ［**OK**］をクリックします。

新しいタスクの設定が保存されます。

## 処理の設定

*オンデマンドスキャンタスク実行中の、感染したオブジェクトおよびその他の検知されたオブジェクトに対する処理を設定するには：*

1. **オンデマンドスキャン**の**プロパティ**ウィンドウを開きます。

2. ［**スキャン範囲**］タブを選択します。
3. ［**設定**］をクリックします。
   ［**オンデマンドスキャンの設定**］ウィンドウが開きます。
4. ［**設定**］をクリックします。
5. ［**処理**］タブを選択します。
6. 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：
   - **通知のみ**
   - **駆除**
   - **駆除。駆除できない場合は削除**
   - **削除**
   - **推奨処理を実行**
7. 感染の可能性があるオブジェクトの処理を選択します：
   - **通知のみ**
   - **隔離**
   - **削除**
   - **推奨処理を実行**
8. 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. ［**検知したオブジェクトの種別に応じて処理を実行**］をオンまたはオフにします。
   b. ［**設定**］をクリックします。
   c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理（最初の処理が失敗した場合に実行）を選択します。
   d. ［**OK**］をクリックします。
9. 修正できない複合オブジェクトに対して実行する処理を選択します：［**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**］をオンまたはオフにします。
10. ［**OK**］をクリックします。

新しいタスクの設定が保存されます。

## パフォーマンスの設定

*オンデマンドスキャンタスクのパフォーマンスを設定するには：*

1. **オンデマンドスキャン**の**プロパティ**ウィンドウを開きます。

2. ［**スキャン範囲**］タブを選択します。
3. ［**設定**］をクリックします。
   ［**オンデマンドスキャンの設定**］ウィンドウが開きます。
4. ［**設定**］をクリックします。
5. ［**パフォーマンス**］タブを選択します。
6. ［**除外リスト**］セクション：
   - ［**除外するファイル**］をオフまたはオンにします。
   - ［**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。
7. ［**詳細設定**］セクション：
   - **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**
8. ［**OK**］をクリックします。

新しいタスクの設定が保存されます。

## リムーバブルドライブスキャンの設定

*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. 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。
   表示されたポリシーのプロパティウィンドウで、［**詳細設定**］セクションを選択します。
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**］ウィンドウが開きます。
6. ［**接続時スキャン**］セクションで次の操作を行います：
   - 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、［**格納データ容量がこの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。

## ベースラインに基づくファイル変更監視タスクの設定

*ベースラインに基づくファイル変更監視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、タスクのプロパティ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。

   ［**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方法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. ［**スキャン範囲**］セクションで、次の操作を実行します：

   a. ベースラインに基づくファイル変更監視タスクの範囲にフォルダーを含めるには：

      1. ［**追加**］をクリックします。
         ［**スキャン領域のプロパティ**］ウィンドウが開きます。

      2. ［**この領域をスキャン**］をオンまたはオフにします。

      3. ［**参照**］をクリックして、ベースラインに基づくファイル変更監視タスクの範囲に含めるフォルダーを指定します。

      4. ベースラインファイル変更監視タスクの範囲のすべてのサブフォルダーを含めるには、［**サブフォルダーもスキャンする**］をオンにします。

   b. ベースラインに基づくファイル変更監視タスクの範囲に以前追加したフォルダーを含めるか、または除外するには、［**スキャン範囲**］表のフォルダーのパスの左側にあるチェックボックスをオンまたはオフにします。

   c. ベースラインに基づくファイル変更監視タスクの範囲に以前追加したフォルダーを削除するには、［**スキャン範囲**］の表でそのフォルダーを選択して、［**削除**］をクリックします。

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（定義データベース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）。

7. ［**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。

8. 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。

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。

   新たに設定したタスクの内容が保存されます。

# アプリケーションコンソールからオンデマンドスキャンタスクを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、保護デバイスのタスクの設定を行う方法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の設定ウィンドウ

*アプリケーションコンソールから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。

   ［**タスクの設定**］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範囲設定を開く

*アプリケーションコンソールからスキャン範囲の設定ウィンドウを開くには：*

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、［**スキャン範囲の設定**］をクリックします。
［**スキャン範囲の設定**］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と編集

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。Kaspersky Embedded Systems Security のその他の機能コンポーネントでは、カスタムタスクを作成できません。

*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. ［**タスクの追加**］を選択します。
［**タスクの追加**］ウィンドウが開きます。
3. 次のタスクの設定を指定します：
   - **名前** - 100 文字以内で構成されるタスク名。次の記号を除くすべての記号を使用できます：**" * < > & \ :**

     > タスク名が指定されていないと、［**スケジュール**］タブ、［**詳細設定**］タブ、および［**実行用アカウント**］タブで、タスクの保存および新しいタスクの設定は行えません。

   - **説明** - タスクに関する追加情報。2000 文字以内です。この情報は、タスクのプロパティウィンドウに表示されます。
   - **ヒューリスティックアナライザーを使用する**
   - **バックグラウンドモードでタスクを実行する**
   - **信頼ゾーンを適用する**
   - **タスクを簡易スキャンとする**
   - **スキャンに KSN を使用する**
4. ［**スケジュール**］タブおよび［**詳細設定**］タブでタスク開始スケジュール設定を指定します。
5. ［**実行用アカウント**］タブで、特定のアカウントの権限を使用してタスクの起動の設定を行います。
6. ［**タスクの追加**］ウィンドウで［OK］をクリックします。
新しいカスタムオンデマンドスキャンタスクが作成されます。新しいタスクの名前が付いたフォルダーがアプリケーションコンソールツリーに表示されます。操作が、システム監査ログに記録されます。
7. 必要に応じて、選択したフォルダーの結果ペインで、［**スキャン範囲の設定**］を選択します。
［**スキャン範囲の設定**］ウィンドウが開きます。
8. 保護対象デバイスのファイルリソースツリーまたはリストで、スキャンの範囲に含めるフォルダーや項目を選択します。

9. 定義済みのセキュリティレベルの1つを選択するか、またはスキャンの設定を手動で行います。

10. ［**スキャン範囲の設定**］ウィンドウで、［**保存**］をクリックします。

設定の内容は、次回のタスク開始時に適用されます。

## オンデマンドスキャンタスクのスキャン範囲

このセクションでは、オンデマンドスキャンタスクのスキャン範囲の作成と使用について説明します。

## ネットワークファイルリソースのビューの設定

*スキャン範囲設定時のネットワークファイルリソースのビューを選択するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストを開き、次のオプションのいずれかを選択します：
   - ［**ツリービュー**］を選択し、ネットワークファイルリソースをツリーで表示する。
   - ［**リストビュー**］を選択し、ネットワークファイルリソースをリストで表示する。

   既定では、保護対象デバイスのネットワークファイルリソースがリストで表示されます。
3. ［**保存**］をクリックします。

## スキャン範囲の作成

管理者のワークステーション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、保護対象デバイス上の Kaspersky Embedded Systems Security をリモートで管理している場合は、保護対象デバイス上のフォルダーを表示できるように、保護対象デバイスの管理者グループのメンバーである必要があります。

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。

オペレーティングシステム起動時の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、Kaspersky Embedded Systems Security 自体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（［**スタート**］ - ［**すべてのプログラム**］ - ［**Kaspersky Embedded Systems Security**］ - ［**Kaspersky Embedded Systems Security の変更または削除**］の順に選択します）。セットアップウィザードで、［**インストール済みコンポーネントの修復**］をオンにして、［**次へ**］をクリックします。次に、［**製品の推奨設定を復元する**］をオンにします。

オンデマンドスキャンタスク範囲を作成する手順は、ネットワークファイルリソースの選択したビューに応じて異なります。ネットワークファイルリソースのビューは、ツリーまたはリストとして設定できます（既定のビュー）。

*ネットワークファイルリソースツリーを使用してスキャン範囲を作成するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。

2. ウィンドウの左側のセクションでネットワークファイルリソースツリーを開き、すべてのフォルダーとサブフォルダーを表示します。

3. 次の操作を実行します：

   - 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。

   - 個別のフォルダーをスキャン範囲に含めるには、［**マイコンピューター**］をオフにして、次の操作を行います：

     - 特定の種別のすべてのドライブをスキャン範囲に含める場合は、対象のドライブ種別の名前の横にあるチェックボックスをオンにします。たとえば、保護対象デバイス上のすべてのリムーバブルドライブを追加する場合は、［**リムーバブルドライブ**］をオンにします。

     - 特定の種別の個々のドライブをスキャン範囲に含める場合は、その種別のドライブを含むフォルダーを展開し、対象のドライブの名前の横にあるチェックボックスをオンにします。たとえば、リムーバブルドライブの **F:** ドライブを選択する場合は、［**リムーバブルドライブ**］フォルダーを展開し、**F:** ドライブのチェックボックスをオンにします。

     - ドライブ上のフォルダーまたはファイルを1つのみ含める場合は、そのフォルダーまたはファイルの名前の横にあるチェックボックスをオンにします。

4. ［**保存**］をクリックします。

［**スキャン範囲の設定**］ウィンドウが終了します。新しい設定が保存されます。

*ネットワークファイルリソースリストを使用してスキャン範囲を作成するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。

2. 個別のフォルダーをスキャン範囲に含めるには、［**マイコンピューター**］をオフにして、次の操作を行います：

   a. スキャン範囲を右クリックして、コンテキストメニューを開きます。

   b. ボタンのコンテキストメニューで、［**スキャン範囲を追加**］を選択します。

   c. 表示された［**スキャン範囲を追加**］ウィンドウで、追加するオブジェクトの種別を選択します：

      - **定義済みの範囲**：保護対象デバイスでいずれかの定義済み範囲を追加します。ドロップダウンリストで、目的のスキャン範囲を選択します。

      - **ディスク、フォルダー、またはネットワークの場所**：個別のドライブ、フォルダー、またはネットワークオブジェクトをスキャン範囲に含めます。［**参照**］をクリックして目的の範囲を選択します。

      - **ファイル**：個別のファイルをスキャン範囲に含めます。［**参照**］をクリックして目的の範囲を選択します。

      オブジェクトが既にスキャン範囲からの除外対象として追加されている場合、スキャン範囲には追加できません。

3. 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するか、次の手順を実行します：

   a. スキャン範囲を右クリックして、コンテキストメニューを開きます。

   b. コンテキストメニューで、［**除外の追加**］を選択します。

   c. ［**除外の追加**］ウィンドウで、スキャン範囲にオブジェクトを追加する手順と同様に、スキャン範囲からの除外対象として追加するオブジェクトの種別を選択します。

4. スキャン範囲または追加する除外対象を変更するには、該当するスキャン範囲のコンテキストメニューで［**範囲の編集**］を選択します。

5. ネットワークファイルリソースのリストに以前追加したスキャン範囲または除外対象を非表示にするには、該当するスキャン範囲のコンテキストメニューで［**リストから削除**］を選択します。

   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。

6. ［**保存**］をクリックします。

［**スキャン範囲の設定**］ウィンドウが終了します。新しい設定が保存されます。

## スキャン範囲にネットワークオブジェクトを含める

UNC（ユニバーサルネーミング規約）フォーマットでパスを指定して、ネットワークドライブ、フォルダー、またはファイルをスキャン範囲に追加することができます。

システムアカウントでネットワークフォルダーをスキャンできます。

*ネットワーク上の場所をスキャン範囲に追加するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。

2. ウィンドウの左上部にあるドロップダウンリストを開き、［**ツリービュー**］を選択します。

3. ［**ネットワーク**］フォルダーのコンテキストメニューを開きます：

   - スキャン範囲にネットワークフォルダーを追加する場合は、［**ネットワークフォルダーの追加**］を選択します。

   - スキャン範囲にネットワークファイルを追加する場合は、［**ネットワークファイルの追加**］を選択します。

4. ネットワークフォルダーまたはネットワークファイルへのパスを UNC フォーマットで入力して、**ENTER** キーを押します。

5. 新しく追加されたネットワークオブジェクトの横にあるチェックボックスをオンにして、スキャン範囲に含めます。

6. 必要に応じて、追加したネットワークオブジェクトのセキュリティ設定を変更します。

7. ［**保存**］をクリックします。

変更されたタスクの設定が保存されます。

## 仮想スキャン範囲の作成

仮想ドライブ、フォルダー、およびファイルは、仮想スキャン範囲を作成するためにスキャン範囲に含めることができます。

ファイルリソースのツリーとしてスキャン範囲が表示されている場合に限り、個別の仮想ドライブ、フォルダー、またはファイルを追加して、スキャン範囲を拡張することができます。

*仮想ドライブをスキャン範囲に追加するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストを開き、［**ツリービュー**］を選択します。
3. 保護対象デバイスのファイルリソースのツリーで、［**仮想ドライブ**］フォルダーのコンテキストメニューを開き、［**仮想ドライブの追加**］をクリックして、使用可能な名前のリストから仮想ドライブの名前を選択します。
4. 追加したドライブの横のチェックボックスをオンにして、ドライブをスキャン範囲に含めます。
5. ［**保存**］をクリックします。

変更されたタスクの設定が保存されます。

*仮想フォルダーまたは仮想ファイルをスキャン範囲に追加するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左上部にあるドロップダウンリストを開き、［**ツリービュー**］を選択します。
3. 保護対象デバイスのファイルリソースツリーでフォルダーまたはファイルを追加するフォルダーのコンテキストメニューを開き、次のいずれかを選択します：
   - **仮想フォルダーの追加**：スキャン範囲に仮想フォルダーを追加する場合に選択します。
   - **仮想ファイルの追加**：スキャン範囲に仮想ファイルを追加する場合に選択します。
4. 入力フィールドに、フォルダーまたはファイルの名前を指定します。
5. フォルダーまたはファイルの名前と同じチェックボックスをオンにして、このフォルダーまたはファイルをスキャン範囲に追加します。
6. ［**保存**］をクリックします。

変更されたタスクの設定が保存されます。

## 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。

ネットワーク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。

*手動でセキュリティを設定するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. ウィンドウの左側で、目的のセキュリティ設定のフォルダーまたは項目を選択します。

   セキュリティ設定を含む定義済みのテンプレートは、スキャン範囲内の選択したフォルダーまたは項目に適用できます。

   ウィンドウの左側では、ネットワークファイルリソースのビューの選択や、スキャン範囲の作成、または仮想スキャン範囲の作成が行えます。
3. ウィンドウの右側で、次のいずれかを行います：
   - ［**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。
   - 要件に従って、選択したフォルダーや項目の必要なセキュリティ設定を、次のタブで指定します：
     - **全般**
     - **処理**
     - **パフォーマンス**
     - **階層型ストレージ**
4. ［**スキャン範囲の設定**］ウィンドウで、［**保存**］をクリックします。

新しいスキャン範囲の設定が保存されます。

## 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ツリーまたは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：［**最高のパフォーマンス**］、［**推奨**］、［**最大の保護**］。

*事前に定義されたセキュリティレベルのいずれかを選択するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. 保護対象デバイスのネットワークファイルリソースツリーまたはリストで、定義済みセキュリティレベルを設定するフォルダーや項目を選択します。
3. 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。

4. ウィンドウの右側の［**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。
   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。

5. ［**保存**］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。

## タスクの全般的な設定

*オンデマンドスキャンタスクのセキュリティの全般設定を行うには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。

2. ［**全般**］タブを選択します。

3. ［**オブジェクトのスキャン**］セクションで、スキャンの範囲に含めるオブジェクト種別を指定します：

   - **スキャン対象オブジェクト**：
     - **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**
     - **指定の拡張子リストによってオブジェクトをスキャン**
   - **ディスクのブートセクターと MBR をスキャン**
   - **NTFS 代替データストリームをスキャン**

4. ［**パフォーマンス**］セクションで、［**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。

   > チェックボックスがオフの場合に使用可能なオプションを切り替えるには、各複合オブジェクトの種別の［**すべての / 新しい（～のみ）**］をクリックします。

5. ［**複合オブジェクトのスキャン**］セクションで、スキャンの範囲に含める複合オブジェクトを指定します：

   - **すべてのアーカイブ** / **新しい アーカイブのみ** / アーカイブ
   - **すべての SFX アーカイブ** / **新しい SFX アーカイブのみ** / SFX アーカイブ
   - **すべてのメールデータベース** / **新しい メールデータベースのみ** / メールデータベース
   - **すべての圧縮されたオブジェクト** / **新しい 圧縮されたオブジェクトのみ** / 圧縮されたオブジェクト
   - **すべての通常のメール** / **新しい 通常のメールのみ** / 通常のメール

- **すべての OLE 埋め込みオブジェクト** / **新しい OLE 埋め込みオブジェクトのみ** / OLE 埋め込みオブジェクト

6. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## 処理の設定

*オンデマンドスキャンタスクで、感染したオブジェクトおよびその他の検知されたオブジェクトの処理を設定するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. ［**処理**］タブを選択します。
3. 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：
   - **通知のみ**
   - **駆除**
   - **駆除。駆除できない場合は削除**
   - **削除**
   - **推奨処理を実行**
4. 感染の可能性があるオブジェクトの処理を選択します：
   - **通知のみ**
   - **隔離**
   - **削除**
   - **推奨処理を実行**
5. 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. ［**検知したオブジェクトの種別に応じて処理を実行**］をオンまたはオフにします。
   b. ［**設定**］をクリックします。
   c. 表示されたウィンドウで、検知したオブジェクトのそれぞれの種別に対して最初の処理と 2 番目の処理（最初の処理が失敗した場合に実行）を選択します。
   d. ［**OK**］をクリックします。
6. 修正できない複合オブジェクトに対して実行する処理を選択します：［**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**］をオンまたはオフにします。
7. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## パフォーマンスの設定

*オンデマンドスキャンタスクのパフォーマンスを設定するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. ［**パフォーマンス**］タブを選択します。
3. ［**除外リスト**］セクション：
   - ［**除外するファイル**］をオフまたはオンにします。
   - ［**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。
4. ［**詳細設定**］セクション：
   - **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**
5. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## 階層型ストレージの設定

*オンデマンドスキャンタスクで、感染したオブジェクトおよびその他の検知されたオブジェクトに実行する処理を設定するには：*

1. ［**スキャン範囲の設定**］ウィンドウを開きます。
2. ［**階層型ストレージ**］タブを選択します。
3. ファイルに対して実行する処理を選択します：
   - **スキャンしない**
   - **ファイルの常駐部分のみスキャン**
   - **ファイル全体をスキャン**
     この処理を選択すると、次のオプションを指定できます：
     - ［**指定した期間（日数）にアクセスされた場合のみ**］をオンまたはオフにして、オンの場合は日数を指定します。

- ［**可能な場合はローカルのハードディスクにファイルをコピーしない**］をオンまたはオフにします。

4. ［**保存**］をクリックします。

新しいタスクの設定が保存されます。

## リムーバブルドライブのスキャン

*アプリケーションコンソールから、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を設定するには：*

1. アプリケーションコンソールツリーで、［**Kaspersky Embedded Systems Security**］フォルダーのコンテキストメニューを開き、［**リムーバブルドライブスキャンを設定**］を選択します。

   ［**リムーバブルドライブスキャン**］ウィンドウが開きます。

2. ［**接続時スキャン**］セクションで次の操作を行います：

   - 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、［**格納データ容量がこの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。

指定された設定が保存、適用されます。

## 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の検知** | 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）。 |
| **感染の可能性があるオブジェクトの検知** | Kaspersky Embedded Systems Security が感染の可能性を検知したオブジェクトの数。 |
| **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。 |
| **隔離されていないオブジェクト** | 隔離に移動しようとしたが、ディスク容量不足などにより移動できなか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。 |
| **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。 |
| **バックアップされていないオブジェクト** | バックアップにコピーを保存しようとしたが、ディスク容量不足などにより保存できなかっ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。 |
| **駆除されたオブジェクト** | 駆除されたオブジェクトの数。 |
| **隔離済み** | 隔離されたオブジェクトの数。 |
| **バックアップ済み** | バックアップに保存されたオブジェクトコピーの数。 |
| **削除されたオブジェクト** | 削除されたオブジェクトの数。 |
| **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。 |
| **処理されたオブジェクト** | 処理された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［**実行ログを開く**］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。

# ベースラインファイル変更監視タスクの作成と設定

*新しいベースラインファイル変更監視タスクを作成または設定するには：*

1. アプリケーションコンソールツリーで、［**システム監査**］フォルダーのコンテキストメニューを開きます。
2. ［**ベースラインファイル変更監視タスクを作成する**］を選択します。
   ［**タスクの追加**］ウィンドウが開きます。
3. ［**ハッシュ計算アルゴリズム**］ドロップダウンリストで、次のいずれかのオプションを選択します：
   - **MD5**
   - **SHA256**
4. ［**スキャン領域**］の表で、以下の操作を実行します：
   a. ベースラインファイル変更監視タスクの範囲でファイルまたはフォルダーを作成するには：
      1. ［**追加**］をクリックします。
         ［**スキャン領域のプロパティ**］ウィンドウが開きます。
      2. ［**この領域をスキャン**］をオンまたはオフにします。
      3. ［**参照**］をクリックして、ベースラインファイル変更監視タスクの範囲に含めるファイルまたはフォルダーを指定します。
      4. ベースラインファイル変更監視タスクの範囲のすべてのサブフォルダーを含めるには、［**サブフォルダーもスキャンする**］をオンにします。
      5. ［**OK**］をクリックします。
   b. ベースラインファイル変更監視タスクの範囲に以前追加されたファイルまたはフォルダーを変更するには：
      1. ［**変更**］をクリックします。
         ［**スキャン領域のプロパティ**］ウィンドウが開きます。
      2. ［**この領域をスキャン**］をオンまたはオフにします。
      3. ［**参照**］をクリックして、ベースラインファイル変更監視タスクの範囲に含めるファイルまたはフォルダーを指定します。
      4. ベースラインファイル変更監視タスクの範囲にすべてのサブフォルダーを含めるか、または除外するには、［**サブフォルダーもスキャンする**］をオンまたはオフにします。
      5. ［**OK**］をクリックします。
   c. ベースラインファイル変更監視タスクの範囲に以前追加されたファイルまたはフォルダーを削除するには、［**スキャン領域**］の表でそのファイルまたはフォルダーを選択して、［**削除**］をクリックします。
5. ［**スケジュール**］タブおよび［**詳細設定**］タブでタスク開始スケジュール設定を指定します。

6. ［**実行用アカウント**］タブで、特定のアカウントの権限を使用してタスクの起動の設定を行います。

7. ［**タスクの追加**］ウィンドウで［**OK**］をクリックします。

   ベースラインファイル変更監視の新しいカスタムタスクが作成されます。新しいタスクの名前が付いたフォルダーがアプリケーションコンソールツリーに表示されます。操作が、システム監査ログに記録されます。

*ベースラインファイル変更監視タスクの設定を開くには：*

1. アプリケーションコンソールツリーで、［**システム監査**］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。

   ［**タスクの設定**］ウィンドウが表示されます。

# Web プラグインからオンデマンドスキャンタスクを管理する

このセクションでは、ネットワークの1つまたはすべての保護対象デバイスに対して Web プラグインインターフェイスを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

*ローカル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**］ - ［**管理対象デバイス**］の順に選択します。

2. ［**グループ**］タブをクリックして、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. ［**追加**］をクリックします。

   ［**タスク追加ウィザード**］ウィンドウが開きます。

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。

*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。
［**タスク追加ウィザード**］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。

タスクのプロパティ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プロパティウィンドウ

*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プロパティを開くには：*

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. ［**グループ**］タブをクリックして、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。

## タスクのスキャン範囲の設定

*既存のオンデマンドスキャンタスクのスキャン範囲を編集するには：*

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. 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ます。
   - 既存のルールを選択し、［**編集**］をクリックします。

   ［**範囲の編集**］ウィンドウが開きます。
4. スイッチを［**使用中**］切り替えて、オブジェクトの種別を選択します。
5. ［**オブジェクトの保護**］セクションで、次の設定を行います：
   - **オブジェクトの保護モード**：
     - **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**
     - **指定の拡張子リストによってオブジェクトをスキャン**
   - **サブフォルダー**
   - **サブファイル**
   - **ディスクのブートセクターと MBR をスキャン**
   - **NTFS 代替データストリームをスキャン**
   - 作成または変更されたファイルのみを保護
6. ［**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**
   - **SFX アーカイブ**
   - **圧縮されたオブジェクト**
   - **メールデータベース**

- **通常のメール**
- **OLE 埋め込みオブジェクト**

7. ［**感染などの問題があるオブジェクトの処理**］セクションで、感染したオブジェクトや検知されたその他のオブジェクトに対して実行する処理を選択します：
   - **通知のみ**
   - **駆除**
   - **駆除。駆除できない場合は削除**
   - **削除**
   - **推奨**
8. ［**感染の可能性があるオブジェクトの処理**］セクションで、感染の可能性があるオブジェクトに対して実行する処理を選択します：
   - **通知のみ**
   - **隔離**
   - **削除**
   - **推奨**
9. ［**感染の可能性があるオブジェクトの処理**］セクションで、［**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**］をオンまたはオフにします。
10. ［**除外リスト**］セクションで、次の設定を行います：
    - ［**除外するファイル**］をオフまたはオンにします。
    - ［**検知しない**］をオフまたはオンにします。
11. ［**詳細設定**］セクションで、次の設定を行います：
    - **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. ［**オフラインファイルの処理**］セクションで、ファイルに対して実行する処理を選択します：
    - **スキャンしない**
    - **ファイルの常駐部分のみスキャン**
    - **ファイル全体をスキャン**
      この処理を選択すると、次のオプションを指定できます：

- ［**指定した期間（日数）にアクセスされた場合のみ**］をオンまたはオフにして、オンの場合は日数を指定します。
- ［**可能な場合はローカルのハードディスクにファイルをコピーしない**］をオンまたはオフにします。

13. ［**OK**］をクリックします。

## タスクの設定

*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. 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アナライザーを使用する**］をオフまたはオンにします。
4. 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。
5. ［**他のコンポーネントとの連携**］セクションで、次の設定を行います：
   - 信頼ゾーンのリストに追加されたオブジェクトをタスクのスキャン範囲から除外する場合は、［**信頼ゾーンを適用する**］をオンにします。
   - Kaspersky Security Network クラウドサービスをタスクに使用するには、［**スキャンに KSN を使用する**］をオンにします。
   - タスクが実行される処理対象プロセスに優先度［*低*］を割り当てるには、［**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。

   - 作成したタスクを簡易スキャンタスクとして使用する場合、［**タスクを簡易スキャンとする**］をオンにします。

# 信頼ゾーン

このセクションでは、Kaspersky Embedded Systems Security の信頼ゾーンに関する情報、およびタスク実行時に信頼ゾーンにオブジェクトを追加する手順について説明します。

# 信頼ゾーンについて

信頼ゾーンは、保護範囲またはスキャン範囲から除外するリストで、各タスクに対して生成して適用できます。対象となるタスクは、オンデマンドスキャンタスクとファイルのリアルタイム保護タスク、新しく作成されたカスタムオンデマンドスキャンタスク、およびすべてのシステムのオンデマンドスキャンタスク（隔離のスキャンタスクは対象外）です。

既定では、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に適用されます。

信頼ゾーンを生成するためのルールのリストは、XML 形式の設定ファイルにエクスポートして、別の保護対象デバイスで実行されている Kaspersky Embedded Systems Security にインポートできます。

## 信頼するプロセス

ファイルのリアルタイム保護タスクに適用されます。

一部の保護対象デバイス上のアプリケーションは、アクセスするファイルが Kaspersky Embedded Systems Security によってインターセプトされると、不安定になる場合があります。そのようなアプリケーションには、システムドメインコントローラーアプリケーションなどがあります。

そのようなアプリケーションの動作を妨害しないように、それらのアプリケーションが実行するプロセスによってアクセスされるファイルの保護を無効にすることができます（これにより、信頼ゾーン内に信頼するプロセスのリストが作成されます）。

Microsoft の推奨事項に基づいて、ファイルのリアルタイム保護から、一部の Microsoft Windows オペレーティングシステムファイルと Microsoft アプリケーションファイルを、感染しないプログラムとして除外してください。これらの一部は、Microsoft の Web サイト に名前が記載されています（記事コード：KB822158）。

信頼ゾーンの信頼するプロセスの使用は、有効にすることも無効にすることもできます。

> 更新などで実行ファイルが変更された場合、信頼するプロセスのリストからそのファイルが除外されます。

本製品では、プロセスを信頼するために保護対象デバイスのファイルのパスを使用することはありません。保護対象デバイスのファイルへのパスは、ファイルの検索、チェックサムの計算、およびユーザーに対する実行ファイルのソースに関する情報の提供のみに使用されます。

## バックアップ処理

コンピューターのリアルタイム保護タスクに適用されます。

ハードディスクに格納されているデータを外部デバイスにバックアップする際には、バックアップ処理時にアクセスされるオブジェクトの保護を無効にできます。Kaspersky Embedded Systems Security では、バックアップのアプリケーションで開いて読み取られる FILE_FLAG_BACKUP_SEMANTICS 属性のオブジェクトがスキャンされます。

除外

- ファイルのリアルタイム保護に適用。
- 保護対象デバイスの指定された領域内で、検知可能なすべてのオブジェクト。
- 保護範囲またはスキャン範囲全体で、名前または名前マスクで指定された検知可能なオブジェクト。

## 管理プラグインから信頼ゾーンを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの1つまたはすべての保護対象デバイスの信頼ゾーンを設定する方法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。

## 信頼ゾーンのポリシーの設定を開く

*Kaspersky Security Center のポリシーから信頼ゾーンを開くには：*

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. 表示されたポリシーのプロパティウィンドウで、［**詳細設定**］セクションを選択します。
6. ［**信頼ゾーン**］サブセクションの［**設定**］をクリックします。
   ［**信頼ゾーン**］ウィンドウが開きます。

必要に応じて信頼ゾーンを設定します。

保護対象デバイスが Kaspersky Security Center のアクティブポリシーで管理されており、このポリシーでアプリケーション設定の変更がブロックされている場合、アプリケーションコンソールでこれらの設定を編集することはできません。

## 信頼ゾーンのプロパティウィンドウ

*［アプリケーションのプロパティ］ウィンドウで信頼ゾーンを設定するには：*

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. 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、保護対象デバイスのプロパティ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コンテキストメニューで［**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 3.1**］を選択します。
6. ［**プロパティ**］をクリックします。
   ［**Kaspersky Embedded Systems Security 3.1 のアプリケーション設定**］ウィンドウが開きます。
7. ［**詳細設定**］セクションを選択します。
8. ［**信頼ゾーン**］サブセクションの［**設定**］をクリックします。
   ［**信頼ゾーン**］ウィンドウが開きます。

必要に応じて信頼ゾーンを設定します。

## 信頼ゾーンの管理プラグインからの設定

既定では、新しく作成されたすべてのポリシーとタスクに信頼ゾーンが適用されます。

*信頼ゾーンを設定するには：*

1. ［**除外リスト**］タブで、タスクの実行時にスキップするオブジェクトを指定できます。
2. ［**信頼するプロセス**］タブで、タスクの実行時にスキップするプロセスを指定できます。
3. not-a-virus（非ウイルス）マスクを適用します。

## 除外の追加

*Kaspersky Security Center のポリシーから信頼ゾーンに除外を追加するには：*

1. ［**信頼ゾーン**］ウィンドウを開きます。
2. ［**除外リスト**］タブで、スキャンと保護をスキップするオブジェクトを指定します：
   - 推奨信頼リストを作成するには、［推奨除外リストを追加］をクリックします。
   - 定義済みの除外をインポートするには、［**インポート**］をクリックし、表示されるウィンドウで、デバイスに保存されている XML 形式の設定ファイルを選択します。

     除外が XML ファイルから除外リストに追加されます。

- オブジェクトを信頼すると判断する条件を手動で指定するには、［**追加**］をクリックして次のステップに進みます。

  ［**除外**］ウィンドウが開きます。

3. ［**追加**］をクリックした場合は、［**次の条件が満たされた場合はオブジェクトをスキャンしない**］セクションで、保護範囲またはスキャン範囲から除外するオブジェクトと、検知可能なオブジェクトから除外するオブジェクトを指定します：

   - 保護範囲またはスキャン範囲からオブジェクトを除外するには：

     a. ［**スキャン対象オブジェクト**］をオンにします。

     b. ［**編集**］をクリックします。

     ［**オブジェクトを選択**］ウィンドウが開きます。

     c. スキャンの範囲から除外するオブジェクトを指定します。

     > オブジェクトを指定する時に、名前マスク（? と * の文字を使用）およびすべての種別の環境変数を使用できます。環境変数の解決（変数を値で置き換え）は、タスクを起動する時または新しいタスクを実行中のタスクに適用する時に、Kaspersky Embedded Systems Security によって実行されます（オンデマンドスキャンタスクには適用されません）。Kaspersky Embedded Systems Security は、タスクの起動に使用されるアカウントで環境設定を解決します。環境変数について詳しくは、Microsoft のナレッジベースを参照してください。

     d. ［**OK**］をクリックします。

     e. 指定されたオブジェクトの下位に置かれているすべてのファイルとフォルダーを保護範囲またはスキャン範囲から除外する場合は、［**サブフォルダーに適用**］をオンにします。

   - 検知可能なオブジェクトの名前を指定するには：

     a. ［**検知対象オブジェクト**］をオンにします。

     b. ［**編集**］をクリックします。

     ［**オブジェクトのリスト**］ウィンドウが開きます。

     c. ウイルス百科事典の分類に従い、検知可能なオブジェクトの名前または名前のマスクを指定します。

     d. ［**追加**］をクリックします。

     e. ［**OK**］をクリックします。

4. ［**除外の適用範囲**］セクションで、除外を適用するタスクの名前の横にあるチェックボックスをオンにします。

5. ［**OK**］をクリックします。

［**信頼ゾーン**］ウィンドウの［**除外リスト**］タブのリストに、除外対象オブジェクトが表示されます。

## 信頼されたプロセスの追加

*信頼するプロセスのリストにプロセスを 1 つ以上追加するには：*

1. ［**信頼ゾーン**］ウィンドウを開きます。
2. ［**信頼するプロセス**］タブを選択します。
3. ファイルの読み取り操作のスキャンをスキップするには、［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。
4. 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。
5. 信頼するプロセスのリストにプロセスを追加するには、次のいずれかを行います：
   - 定義済みの信頼するプロセスをインポートするには、［**インポート**］をクリックし、表示されるウィンドウで、デバイスに保存されている XML 形式の設定ファイルを選択します。

     プロセスが XML ファイルから信頼するプロセスのリストに追加されます。
   - プロセスを手動で指定するには、［**追加**］をクリックして、次の手順に進みます。
6. ［**追加**］をクリックした場合、そのコンテキストメニューで、次のいずれかのオプションを選択します：
   - **複数のプロセス**

     表示された［**信頼するプロセスの追加**］ウィンドウで、次を設定します：

     a. **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**。

     b. **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**。

     c. 実行可能プロセスに基づいてデータを追加するには、［**参照**］をクリックします。

     d. 表示されたウィンドウで、実行ファイルを選択します。

     > 一度に追加できる実行ファイルは 1 つのみです。他の実行ファイルを追加するには手順 c と d を繰り返してください。

     e. 実行中のプロセスに基づいてデータを追加するには、［**プロセス**］をクリックします。

     f. 表示されたウィンドウで、プロセスを選択します。複数のプロセスを選択するには、［CTRL］を押したまま選択します。

     g. ［OK］をクリックします。

     > 実行中のプロセスのリストを表示できるようにするには、ファイルのリアルタイム保護タスクが実行されたアカウントに、Kaspersky Embedded Systems Security がインストールされているデバイスの管理者権限が必要です。実行中のプロセスのリスト内のプロセスは、ファイル名、プロセス識別子（PID）、または保護対象デバイス上のプロセスの実行ファイルのパスで並べ替えることができます。実行中のプロセスを選択するには、保護対象デバイスでアプリケーションコンソールのみを使用するか、あるいは Kaspersky Security Center から指定されたコンピューター設定内で、［**プロセス**］をクリックします。

   - **ファイル名とパスに基づく 1 つのプロセス**

     ［**プロセスの追加**］ウィンドウで、次を実行します：

     a. 実行ファイルへのパスを入力します（ファイル名を含む）。

オブジェクトを指定する時に、名前マスク（? と * の文字を使用）およびすべての種別の環境変数を使用できます。環境変数の解決（変数を値で置き換え）は、タスクを起動する時または新しいタスクを実行中のタスクに適用する時に、Kaspersky Embedded Systems Security によって実行されます（オンデマンドスキャンタスクには適用されません）。Kaspersky Embedded Systems Security は、タスクの起動に使用されるアカウントで環境設定を解決します。環境変数について詳しくは、Microsoft のナレッジベースを参照してください。

b. ［**OK**］をクリックします。

- **オブジェクトのプロパティに基づく 1 つのプロセス**
  表示された［**信頼するプロセスの追加**］ウィンドウで、次を設定します：

  a. ［**参照**］をクリックしてプロセスを選択します。

  b. **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**。

  c. **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**。

  d. ［**OK**］をクリックします。

  選択したプロセスを信頼できるプロセスのリストに追加するには、少なくとも 1 つの信頼の基準を選択する必要があります。

7. ［**信頼ゾーン**］ウィンドウで［OK］をクリックします。

選択したファイルまたはプロセスが、［**信頼ゾーン**］ウィンドウの信頼するプロセスのリストに追加されます。

## not-a-virus（非ウイルス）マスクの適用

not-a-virus（非ウイルス）マスクを使用すると、有害と判断される可能性がある正規のソフトウェアのファイルや Web リソースのスキャンをスキップできます。マスクが影響を与えるタスクは、次の通りです：

- ファイルのリアルタイム保護
- オンデマンドスキャン

マスクが除外リストに追加されていない場合、Kaspersky Embedded Systems Security はこのカテゴリに分類されるソフトウェアに対して、タスク設定に指定された処理を適用します。

*not-a-virus（非ウイルス）マスクを適用するには：*

1. ［**信頼ゾーン**］ウィンドウを開きます。
2. チェックボックスがオフの場合、［**除外リスト**］タブの［**検知対象オブジェクト**］列でリストをスクロールして、「not-a-virus:*」（非ウイルス）の行を選択します。
3. ［OK］をクリックします。

新しい設定が適用されます。

# アプリケーションコンソールから信頼ゾーンを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、保護対象デバイスの信頼ゾーンを設定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でタスクに信頼ゾーンを適用する

既定では、信頼ゾーンは、ファイルのリアルタイム保護タスク、新しく作成されたカスタムオンデマンドスキャンタスク、すべてのシステムのオンデマンドスキャンタスク（隔離のスキャンタスクを除く）に適用されます。

信頼ゾーンを有効化または無効化すると、指定された除外対象オブジェクトに即座に適用されるか、あるいは実行中のタスクでの適用が終了します。

*Kaspersky Embedded Systems Security タスクで信頼ゾーンの使用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、信頼ゾーンの使用を設定するタスク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。
   ［**タスクの設定**］ウィンドウが表示されます。
3. ウィンドウが表示されたら［**全般**］タブを選択し、次のいずれかの操作を実行します：
   - タスクで信頼ゾーンを適用するには、［**信頼ゾーンを適用する**］をオンにします。
   - タスクで信頼ゾーンを無効にするには、［**信頼ゾーンを適用する**］をオフにします。
4. 信頼ゾーンを設定するには、［**信頼ゾーンを適用する**］のリンク部分をクリックします。
   ［**信頼ゾーン**］ウィンドウが開きます。
   ［**信頼ゾーン**］ウィンドウで、［除外］と［信頼するプロセス］を設定し、［**OK**］をクリックします。
5. ［**タスクの設定**］ウィンドウで、［**OK**］をクリックして変更を保存します。

# アプリケーションコンソールでの信頼ゾーンの設定

信頼ゾーンを設定するには：

1. ［**除外リスト**］タブで、タスクの実行時にスキップするオブジェクトを指定できます。
2. ［**信頼するプロセス**］タブで、タスクの実行時にスキップするプロセスを指定できます。
3. 製品のタスクに信頼ゾーンを適用します。
4. not-a-virus（非ウイルス）マスクを適用します。

# 除外対象オブジェクトの信頼ゾーンへの追加

*アプリケーションコンソールを使用して、除外するオブジェクトを信頼ゾーンに手動で追加するには：*

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**］メニューオプションを選択します。
   ［**信頼ゾーン**］ウィンドウが開きます。
3. ［**除外リスト**］タブを選択します。
4. スキャンと保護でスキップするオブジェクトを指定します：
   - 定義済みの除外をインポートするには、［**インポート**］をクリックし、表示されるウィンドウで、デバイスに保存されている XML 形式の設定ファイルを選択します。
     除外が XML ファイルから除外リストに追加されます。
   - オブジェクトを信頼すると判断する条件を手動で指定するには、［**追加**］をクリックして次のステップに進みます。
     ［**除外**］ウィンドウが開きます。
5. ［**追加**］をクリックした場合は、［**次の条件が満たされた場合はオブジェクトをスキャンしない**］セクションで、保護範囲またはスキャン範囲から除外するオブジェクトと、検知可能なオブジェクトから除外するオブジェクトを指定します：
   - 保護範囲またはスキャン範囲からオブジェクトを除外するには：
     a. ［**スキャン対象オブジェクト**］をオンにします。
     b. ［**編集**］をクリックします。
     ［**オブジェクトを選択**］ウィンドウが開きます。
     c. スキャンの範囲から除外するオブジェクトを指定します。

     > オブジェクトを指定する時に、名前マスク（? と * の文字を使用）およびすべての種別の環境変数を使用できます。環境変数の解決（変数を値で置き換え）は、タスクを起動する時または新しいタスクを実行中のタスクに適用する時に、Kaspersky Embedded Systems Security によって実行されます（オンデマンドスキャンタスクには適用されません）。Kaspersky Embedded Systems Security は、タスクの起動に使用されるアカウントで環境設定を解決します。環境変数について詳しくは、Microsoft のナレッジベースを参照してください。

     d. ［**OK**］をクリックします。
     e. 指定されたオブジェクトの下位に置かれているすべてのファイルとフォルダーを保護範囲またはスキャン範囲から除外する場合は、［**サブフォルダーに適用**］をオンにします。
   - 検知可能なオブジェクトの名前を指定するには：
     a. ［**検知対象オブジェクト**］をオンにします。

b. ［**編集**］をクリックします。
［**オブジェクトのリスト**］ウィンドウが開きます。

c. ウイルス百科事典の分類に従い、検知可能なオブジェクトの名前または名前のマスクを指定します。

d. ［**追加**］をクリックします。

e. ［**OK**］をクリックします。

6. ［**除外の適用範囲**］セクションで、除外を適用するタスクの名前の横にあるチェックボックスをオンにします。

7. ［**OK**］をクリックします。

［**信頼ゾーン**］ウィンドウの［**除外リスト**］タブのリストに、除外対象オブジェクトが表示されます。

## 信頼されたプロセスの追加

次のいずれかの方法を使用して、信頼するプロセスのリストにプロセスを追加できます：

- 保護対象デバイスで実行中のプロセスのリストから、対象のプロセスを選択する方法。
- プロセスの実行ファイルを選択する方法。この方法では、プロセスが現在実行されているかどうかは関係ありません。

プロセスの実行ファイルが変更されている場合、信頼するプロセスのリストからこのプロセスが除外されます。

*信頼するプロセスのリストにプロセスを 1 つ以上追加するには：*

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**］メニューオプションを選択します。
［**信頼ゾーン**］ウィンドウが開きます。

3. ［**信頼するプロセス**］タブを選択します。

4. ファイルの読み取り操作のスキャンをスキップするには、［**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。

5. 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。

6. 信頼するプロセスのリストにプロセスを追加するには、次のいずれかを行います：

- 定義済みの信頼するプロセスをインポートするには、［**インポート**］をクリックし、表示されるウィンドウで、デバイスに保存されている XML 形式の設定ファイルを選択します。
プロセスが XML ファイルから信頼するプロセスのリストに追加されます。

- プロセスを手動で指定するには、［**追加**］をクリックして、次の手順に進みます。

7. ［**追加**］をクリックした場合、そのコンテキストメニューで、次のいずれかのオプションを選択します：

- **複数のプロセス**

  表示された［**信頼するプロセスの追加**］ウィンドウで、次を設定します：

  a. **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**。

  b. **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**。

  c. 実行可能プロセスに基づいてデータを追加するには、［**参照**］をクリックします。

  d. 表示されたウィンドウで、実行ファイルを選択します。

  一度に追加できる実行ファイルは1つのみです。他の実行ファイルを追加するには手順 c と d を繰り返してください。

  e. 実行中のプロセスに基づいてデータを追加するには、［**プロセス**］をクリックします。

  f. 表示されたウィンドウで、プロセスを選択します。複数のプロセスを選択するには、［**CTRL**］を押したまま選択します。

  g. ［**OK**］をクリックします。

  実行中のプロセスのリストを表示できるようにするには、ファイルのリアルタイム保護タスクが実行されたアカウントに、Kaspersky Embedded Systems Security がインストールされているデバイスの管理者権限が必要です。実行中のプロセスのリスト内のプロセスは、ファイル名、プロセス識別子（PID）、または保護対象デバイス上のプロセスの実行ファイルのパスで並べ替えることができます。実行中のプロセスを選択するには、保護対象デバイスでアプリケーションコンソールのみを使用するか、あるいは Kaspersky Security Center から指定されたコンピューター設定内で、［**プロセス**］をクリックします。

- **ファイル名とパスに基づく1つのプロセス**

  ［**プロセスの追加**］ウィンドウで、次を実行します：

  a. 実行ファイルへのパスを入力します（ファイル名を含む）。

  オブジェクトを指定する時に、名前マスク（**?** と ***** の文字を使用）およびすべての種別の環境変数を使用できます。環境変数の解決（変数を値で置き換え）は、タスクを起動する時または新しいタスクを実行中のタスクに適用する時に、Kaspersky Embedded Systems Security によって実行されます（オンデマンドスキャンタスクには適用されません）。Kaspersky Embedded Systems Security は、タスクの起動に使用されるアカウントで環境設定を解決します。環境変数について詳しくは、Microsoft のナレッジベースを参照してください。

  b. ［**OK**］をクリックします。

- **オブジェクトのプロパティに基づく1つのプロセス**

  表示された［**信頼するプロセスの追加**］ウィンドウで、次を設定します：

  a. ［**参照**］をクリックしてプロセスを選択します。

  b. **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**。

c. **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**。

d. ［**OK**］をクリックします。

選択したプロセスを信頼できるプロセスのリストに追加するには、少なくとも1つの信頼の基準を選択する必要があります。

8. ［**信頼ゾーン**］ウィンドウで［**OK**］をクリックします。

選択したファイルまたはプロセスが、［**信頼ゾーン**］ウィンドウの信頼するプロセスのリストに追加されます。

## not-a-virus（非ウイルス）マスクの適用

not-a-virus（非ウイルス）マスクを使用すると、有害と判断される可能性がある正規のソフトウェアのファイルや Web リソースのスキャンをスキップできます。マスクが影響を与えるタスクは、次の通りです：

- ファイルのリアルタイム保護
- オンデマンドスキャン

マスクが除外リストに追加されていない場合、Kaspersky Embedded Systems Security はこのカテゴリに分類されるソフトウェアまたは Web リソースに対して、タスク設定に指定された処理を適用します。

*not-a-virus（非ウイルス）マスクを適用するには：*

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**］メニューオプションを選択します。
   ［**信頼ゾーン**］ウィンドウが開きます。
3. ［**除外リスト**］タブを選択します。
4. リストをスクロールして「*not-a-virus:**」の値を探します。
5. 該当するチェックボックスがオフになっている場合はオンにします。
6. ［**OK**］をクリックします。

新しい設定が適用されます。

## Web プラグインから信頼ゾーンを管理する

Web プラグインから信頼ゾーンを管理するには：

1. Web コンソールのメインウィンドウで、［**デバイス**］ - ［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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. ［**信頼ゾーン**］サブセクションの［**設定**］をクリックします。

6. 必要に応じて信頼ゾーンを設定します。

# 脆弱性攻撃ブロック

このセクションでは、プロセスメモリ保護を設定する方法について説明します。

# 脆弱性攻撃ブロックについて

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で実装されます。コンポーネントのアクティビティステータスを変更し、プロセスメモリ保護を設定できます。

コンポーネントは、保護対象プロセスに外部のプロセス保護エージェント（「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。

## Kaspersky Security 脆弱性攻撃ブロックサービス

脆弱性攻撃ブロックの効果を最も高めるためには、保護対象デバイスに Kaspersky Security 脆弱性攻撃ブロックサービスが必要です。このサービスおよび脆弱性攻撃ブロックは、推奨インストールの一部です。kavfswh プロセスは保護対象デバイスのサービスのインストール時に作成、開始されます。これは、コンポーネントからセキュリティエージェントに、保護対象プロセスに関する情報を送信します。

Kaspersky Security 脆弱性攻撃ブロックサービスの停止後、Kaspersky Embedded Systems Security は、保護対象プロセスリストに追加されたプロセスを引き続き保護し、新しく追加されたプロセスにもロードされ、使用可能なすべての脆弱性攻撃ブロック技術を適用してプロセスメモリを保護します。

デバイスが Windows 10 以降のオペレーティングシステムで稼働している場合、Kaspersky Security 脆弱性攻撃ブロックサービスが停止した後は、プロセスとプロセスのメモリが保護されません。

Kaspersky Security 脆弱性攻撃ブロックサービスが停止した場合、アプリケーションは保護対象プロセスに発生したイベントに関する情報を受信しません（脆弱性攻撃およびプロセスの終了に関する情報を含む）。さらに、エージェントは新しい保護設定および保護対象プロセスリストへの新しいプロセスの追加に関する情報を受信できません。

### 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：

- **脆弱性攻撃時に終了する**：このモードを適用すると、脆弱性攻撃が行われた場合にプロセスを終了します。

  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。

- **通知のみ**：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。

  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。

## 管理プラグインから脆弱性攻撃ブロックを管理する

このセクションでは、管理プラグインインターフェイスを操作して、ネットワークの1つまたはすべての保護対象デバイスのコンポーネントの設定を行う方法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。

## 脆弱性攻撃ブロックのポリシーの設定を開く

*脆弱性攻撃ブロックの設定を Kaspersky Security Center のポリシーから開くには：*

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. 表示された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**］セクションを選択します。

6. ［**脆弱性攻撃ブロック**］サブセクションの［**設定**］をクリックします。
［**脆弱性攻撃ブロック**］ウィンドウが表示されます。

必要に応じて脆弱性攻撃ブロックを設定します。

## 脆弱性攻撃ブロックのプロパティウィンドウ

*脆弱性攻撃ブロック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、保護対象デバイスのプロパティ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コンテキストメニューで［**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 3.1**］を選択します。

6. ［**プロパティ**］をクリックします。
［**Kaspersky Embedded Systems Security 3.1 のアプリケーション設定**］ウィンドウが開きます。

7. ［**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。

8. ［**脆弱性攻撃ブロック**］サブセクションの［**設定**］をクリックします。
［**脆弱性攻撃ブロック**］ウィンドウが表示されます。

必要に応じて脆弱性攻撃ブロックを設定します。

## プロセスメモリ保護の設定

*保護対象プロセスのリストに追加されたプロセスのメモリを保護するように設定するには、次の処理を実行します：*

1. ［**脆弱性攻撃ブロック**］ウィンドウを開きます。

2. ［**脆弱性攻撃ブロックモード**］セクションで、次の設定を行います：

   - **脆弱なプロセスに対する攻撃から防御する**。

- **脆弱性攻撃時に終了する**。
- **通知のみ**

3. ［**防御処理**］セクションで、次の設定を行います：
   - **脆弱性攻撃を受けたプロセスについてターミナルサービスから通知する**。
   - **Kaspersky Security サービスが無効の場合にも脆弱なプロセスに対する攻撃を防御する**。
4. ［**脆弱性攻撃ブロック**］ウィンドウで［**OK**］をクリックします。

Kaspersky Embedded Systems Security では、設定したプロセスメモリ保護が保存されて適用されます。

## プロセスの保護範囲への追加

脆弱性攻撃ブロックは、既定で複数のプロセスを保護します。リストの該当するチェックボックスをオフにすることで、処理を保護範囲から除外できます。

*保護されているプロセスのリストにプロセスを追加するには：*

1. ［**脆弱性攻撃ブロック**］ウィンドウを開きます。
2. ［**保護対象プロセス**］タブで、［**参照**］をクリックします。
   Microsoft Windows のエクスプローラーのウィンドウが表示されます。
3. リストに追加するプロセスを選択します。
4. ［**開く**］をクリックします。
   プロセス名が表示されます。
5. ［**追加**］をクリックします。
   プロセスが保護対象プロセスのリストに追加されます。
6. 追加したプロセスを選択します。
7. ［**脆弱性攻撃ブロック技術の設定**］をクリックします。
   ［**脆弱性攻撃ブロック技術**］ウィンドウが開きます。
8. 次のいずれかのオプションを選択して、脆弱性攻撃による被害の軽減技術を適用します：
   - **使用可能なすべての脆弱性攻撃ブロック技術を適用する。**
     このオプションを選択すると、リストは編集できません。既定では、利用可能なすべての技術がプロセスに適用されます。
   - **選択した脆弱性攻撃ブロック技術を適用する。**
     このオプションを選択すると、適用されている脆弱性攻撃による被害の軽減技術のリストを編集できます：
     a. 選択したプロセスを保護するには、適用する技術の隣にあるチェックボックスをオンにします。
     b. ［**Attack Surface Reduction 技術を適用する**］をオンまたはオフにします。

9. Attack Surface Reduction 技術を設定します：

- ［**次のモジュールを拒否する**］に、起動後に保護対象プロセスからブロックされるモジュールの名前を入力します。
- ［**インターネットゾーンで起動した場合、モジュールを拒否しない**］で、モジュールの起動を許可するオプションの隣にあるチェックボックスをオンにします：
  - **インターネット**
  - **ローカルイントラネット**
  - **信頼する URL**
  - **制限された URL**
  - **コンピューター**

これらの設定は、Internet Explorer® にのみ適用されます。

10. ［**OK**］をクリックします。

プロセスがタスクの保護範囲に追加されます。

## アプリケーションコンソールから脆弱性攻撃ブロックを管理する

このセクションでは、アプリケーションコンソールインターフェイスを操作して、保護対象デバイスのコンポーネントの設定を行う方法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。

## 脆弱性攻撃ブロックの全般的な設定ウィンドウ

*［**脆弱性攻撃ブロックの設定**］ウィンドウを開くには：*

1. アプリケーションコンソールにある［**ファイル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**］フォルダーを選択します。
3. ［**プロセス保護設定**］セクションで、［**プロパティ**］をクリックします。
   ［**脆弱性攻撃ブロックの設定**］ウィンドウが開きます。

必要に応じて脆弱性攻撃ブロックの全般的な設定を指定します。

## 脆弱性攻撃ブロックのプロセス保護設定ウィンドウ

*［**プロセス保護設定**］ウィンドウを開くには：*

1. アプリケーションコンソールにある［**ファイル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**］フォルダーを選択します。

［**プロセス保護設定**］セクションで、［**プロセス保護のパラメータ**］をクリックします。

［**プロセス保護設定**］ウィンドウが表示されます。

必要に応じて脆弱性攻撃ブロックのプロセス保護設定を指定します。

## プロセスメモリ保護の設定

*保護されているプロセスのリストにプロセスを追加するには：*

1. ［**脆弱性攻撃ブロックの設定**］ウィンドウを開きます。
2. ［**脆弱性攻撃ブロックモード**］セクションで、次の設定を行います：
   - **脆弱なプロセスに対する攻撃から防御する**。
     - **脆弱性攻撃時に終了する**。
     - **通知のみ**
3. ［**防御処理**］セクションで、次の設定を行います：
   - **脆弱性攻撃を受けたプロセスについてターミナルサービスから通知する**。
   - **Kaspersky Security サービスが無効の場合にも脆弱なプロセスに対する攻撃を防御する**。
4. ［**脆弱性攻撃ブロックの設定**］ウィンドウで［**OK**］をクリックします。

Kaspersky Embedded Systems Security では、設定したプロセスメモリ保護が保存されて適用されます。

## プロセスの保護範囲への追加

脆弱性攻撃ブロックは、既定で複数のプロセスを保護します。保護しないプロセスは、保護対象プロセスのリストでチェックをオフにします。

*保護されているプロセスのリストにプロセスを追加するには：*

1. ［**プロセス保護設定**］ウィンドウを開きます。
2. プロセスを追加して悪用から保護し、脆弱性攻撃の影響を受ける可能性を軽減するには、次の処理を実行します：

a. ［**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. 表示されたウィンドウで、リストに追加するプロセスを選択します。

c. ［**開く**］をクリックします。

d. ［**追加**］をクリックします。
プロセスが保護対象プロセスのリストに追加されます。

3. リストでプロセスを選択します。

4. 現在の設定が［**プロセス保護設定**］タブに表示されます：

- **プロセス名**
- **実行中**
- **適用される脆弱性攻撃ブロック技術**
- **Attack Surface Reduction の設定**

5. プロセスに適用される脆弱性攻撃ブロック技術を変更するには、［**脆弱性攻撃ブロック技術**］タブを選択します。

6. 次のいずれかのオプションを選択して、脆弱性攻撃による被害の軽減技術を適用します：

- **利用できるすべての脆弱性攻撃ブロック技術を適用する**。
このオプションを選択すると、リストは編集できません。既定では、利用可能なすべての技術がプロセスに適用されます。
- **プロセスに対してリストされた脆弱性攻撃ブロック技術を適用する**。
このオプションを選択すると、適用されている脆弱性攻撃による被害の軽減技術のリストを編集できます：

  a. 選択したプロセスを保護するには、適用する技術の隣にあるチェックボックスをオンにします。

7. Attack Surface Reduction 技術を設定します：

- ［**次のモジュールを拒否する**］に、起動後に保護対象プロセスからブロックされるモジュールの名前を入力します。
- ［**インターネットゾーンで起動した場合、モジュールを拒否しない**］セクションで、モジュールの起動を許可するオプションの隣にあるチェックボックスをオンにします：
  - **インターネット**
  - **ローカルイントラネット**
  - **信頼する URL**
  - **制限されたサイト**
  - **コンピューター**

これらの設定は、Internet Explorer® にのみ適用されます。

8. ［**保存**］をクリックします。

プロセスがタスクの保護範囲に追加されます。

## Web プラグインから脆弱性攻撃ブロックを管理する

このセクションでは、Web プラグインインターフェイスを操作して、保護対象デバイスのコンポーネントの設定を行う方法について説明します。

## プロセスメモリ保護の設定

*保護対象プロセスのリストに追加されたプロセスのメモリを保護するように設定するには、次の処理を実行します：*

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。
5. ［**脆弱性攻撃ブロック**］サブセクションの［**設定**］をクリックします。
6. ［**脆弱性攻撃ブロックの設定**］タブを開きます。
7. ［**脆弱性攻撃ブロックモード**］セクションで、次の設定を行います：
   - **脆弱なプロセスに対する攻撃から防御する**。
     - **脆弱性攻撃時に終了する**。
     - **通知のみ**
8. ［**防御処理**］セクションで、次の設定を行います：
   - **脆弱性攻撃を受けたプロセスについてターミナルサービスから通知する**。
   - **Kaspersky Security サービスが無効の場合にも脆弱なプロセスに対する攻撃を防御する**。
9. ［**脆弱性攻撃ブロック**］ウィンドウで［**OK**］をクリックします。

Kaspersky Embedded Systems Security では、設定したプロセスメモリ保護が保存されて適用されます。

## プロセスの保護範囲への追加

*保護対象プロセスのリストに追加されたプロセスのメモリを保護するように設定するには、次の処理を実行します：*

1. Web コンソールのメインウィンドウで、［**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. 表示されたポリシーのプロパティウィンドウで、［**アプリケーションの設定**］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**］セクションを選択します。
5. ［**脆弱性攻撃ブロック**］サブセクションの［**設定**］をクリックします。
6. ［**保護対象プロセス**］タブを開きます。
7. ［**追加**］をクリックします。
8. ［**脆弱性攻撃ブロック技術**］ウィンドウが開きます。
9. プロセス名を指定します。
10. 次のいずれかのオプションを選択して、脆弱性攻撃による被害の軽減技術を適用します：

    - **使用可能なすべての脆弱性攻撃ブロック技術を適用する。**

      このオプションを選択すると、リストは編集できません。既定では、利用可能なすべての技術がプロセスに適用されます。

    - **選択した脆弱性攻撃ブロック技術を適用する。**

      このオプションを選択すると、適用されている脆弱性攻撃による被害の軽減技術のリストを編集できます：

      a. 選択したプロセスを保護するには、適用する技術の隣にあるチェックボックスをオンにします。

      b. ［**Attack Surface Reduction 技術を適用する**］をオンまたはオフにします。

11. Attack Surface Reduction 技術を設定します：

    - ［**次のモジュールを拒否する**］に、起動後に保護対象プロセスからブロックされるモジュールの名前を入力します。
    - ［**インターネットゾーンで起動した場合、モジュールを拒否しない**］で、モジュールの起動を許可するオプションの隣にあるチェックボックスをオンにします：
      - **インターネット**
      - **ローカルイントラネット**
      - **信頼する URL**
      - **制限された URL**
      - **コンピューター**

      これらの設定は、Internet Explorer® にのみ適用されます。

12. ［OK］をクリックします。

プロセスがタスクの保護範囲に追加されます。

# 脆弱性攻撃ブロック技術

脆弱性攻撃ブロック技術

| 脆弱性攻撃ブロック技術 | 説明 |
| --- | --- |
| Data Execution Prevention（DEP） | Data Execution Prevention は、保護されたメモリ領域でのすべてのコードの実行をブロックします。 |
| Address Space Layout Randomization（ASLR） | プロセスのアドレス空間におけるデータ構造の配置に対する変更。 |
| Structured Exception Handler Overwrite Protection（SEHOP） | 例外レコードの置換または例外ハンドラの置換。 |
| NULL ページの割り当て | NULL ポインタのリダイレクト防止。 |
| LoadLibrary のネットワークコールチェック（Anti ROP） | ネットワークパスからの DLL ロードに対する保護。 |
| Executable Stack（ROP 対策） | スタックの領域の無許可実行のブロック。 |
| アンチ RET チェック（ROP 対策） | CALL インストラクションが安全に起動するかどうか確認します。 |
| アンチスタックピボット（ROP 対策） | 実行可能アドレスへの ESP スタックポインタの再配置に対する保護。 |
| 単純な Export Address Table Access 監視（EAT Access 監視とデバッグレジスタによる EAT Access 監視） | kernel32.dll、kernelbase.dll および ntdll.dll でのエクスポートアドレステーブルに対する読み込みアクセスの保護 |
| ヒープスプレーの割り当て（Heapspray） | 悪意のあるコードを実行するためのメモリ割り当てに対する保護。 |
| 実行フローシミュレーション（Return Oriented Programming 対策） | Windows API コンポーネントにおいて潜在的な危険性があるインストラクション連鎖（ROP ガジェットの可能性あり）の検知。 |
| IntervalProfile コールの監視（Ancillary Function Driver Protection（AFDP）） | AFD ドライバーの脆弱性を使用した権限の昇格に対する保護（QueryIntervalProfile のコールによる Ring 0 におけるすべてのコードの実行）。 |
| Attack Surface Reduction（ASR） | 保護対象プロセスを介した脆弱なアドインの起動のブロック。 |
| Anti Process Hollowing（Hollowing） | 信頼するプロセスの悪意のあるコピーの作成と実行に対する保護。 |
| Anti AtomBombing（APC） | 非同期プロシージャーコールを経由したグローバルアトムテーブルの悪用（APC）。 |
| Anti CreateRemoteThread（RThreadLocal） | 保護対象のプロセスに、別のプロセスがスレッドを作成しました。 |
| Anti CreateRemoteThread（RThreadRemote） | 保護対象のプロセスが、別のプロセスにスレッドを作成しました。 |

# サードパーティ製システムとの統合

このセクションでは、Kaspersky Embedded Systems Security とサードパーティ製の機能および技術との統合について説明します。

# システム監視用パフォーマンスカウンター

このセクションでは、インストールの際に Kaspersky Embedded Systems Security によって登録される Microsoft Windows システム監視用のパフォーマンスカウンターについて説明します。

# Kaspersky Embedded Systems Security のパフォーマンスカウンターについて

既定では、パフォーマンスカウンターは、インストールされた Kaspersky Embedded Systems Security のコンポーネントに含まれます。インストールの際、Kaspersky Embedded Systems Security 独自の Microsoft Windows システム監視用パフォーマンスカウンターが登録されます。

Kaspersky Embedded Systems Security のカウンターを使用すれば、コンピューターのリアルタイム保護タスクの実行中に製品のパフォーマンスを監視できます。他のアプリケーションとともに実行している際のボトルネックやリソース不足について解析できます。Kaspersky Embedded Systems Security のクラッシュを診断して、推奨されない設定を特定できます。

Kaspersky Embedded Systems Security パフォーマンスカウンターを参照するには、Windows のコントロールパネルの［**管理ツール**］セクションにある［**パフォーマンス**］コンソールを開きます。

以下のセクションで、カウンターの定義、推奨読み取り間隔、しきい値、カウンター値がしきい値を超えた場合の Kaspersky Embedded Systems Security の推奨される設定について示します。

# 拒否された要求の合計数

拒否された要求の合計数

| | |
|---|---|
| **名前** | 拒否された要求の合計数 |
| **定義** | ファイルインターセプションドライバーによるオブジェクト処理要求のうち、アプリケーションプロセスによって受け入れられなかった要求の合計数。この数は、Kaspersky Embedded Systems Security が最後に起動された時点からカウントされます。<br>Kaspersky Embedded Systems Security のプロセスによって処理の要求が拒否されたオブジェクトをスキップします。 |
| **目的** | このカウンターの値により、次の状況を検出できます：<br>• Kaspersky Embedded Systems Security のプロセスの過負荷による、コンピューターのリアルタイム保護の低下。<br>• ファイルインターセプションディスパッチャの障害発生による、コンピューターのリアルタイム保護の中断。 |
| **標準値 / しきい値** | 0 / 1 |

| | |
|---|---|
| **推奨読み取り間隔** | 1時間 |
| **値がしきい値を超えた場合の設定の推奨事項** | 拒否された処理要求の数は、スキップされたオブジェクトの数に対応します。<br>カウンターの動作によって、次のいずれかの状況になっている可能性があります：<br>• カウンターに、長時間拒否されているいくつかの要求が表示されます：Kaspersky Embedded Systems Security のすべてのプロセスが完全に読み込まれるため、Kaspersky Embedded Systems Security はオブジェクトをスキャンできませんでした。オブジェクトのスキップを防ぐには、コンピューターのリアルタイム保護タスク用のアプリケーションプロセスの数を増やしてください。［**実行中プロセスの最大数**］、［**リアルタイム保護の対象プロセスの数**］などの Kaspersky Embedded Systems Security の設定を使用できます。<br>• 拒否された要求の数が重大レベルのしきい値を上回り、急増している場合は、ファイルインターセプションディスパッチャがクラッシュしている。Kaspersky Embedded Systems Security はオブジェクトがアクセスされている時にはスキャンを行いません。Kaspersky Embedded Systems Security の再起動 |

## スキップされた要求の合計数

スキップされた要求の合計数

| | |
|---|---|
| **名前** | スキップされた要求の合計数 |
| **定義** | Kaspersky Embedded Systems Security が受け取ったが処理完了を示すイベントを生成しなかったファイルインターセプションドライバーによるオブジェクト処理要求の合計数。この数は、アプリケーションが最後に起動された時点からカウントされます。<br>オブジェクト処理要求が処理対象プロセスのいずれによって受け入れられているが、処理完了を示すイベントが送信されなかった場合、ドライバーがその要求を別のプロセスに転送し、**スキップされた要求の合計数**カウンターの値が1つ加算されます。ドライバーがすべての処理対象プロセスに要求を転送し、どのプロセスも処理要求を受け取らなかったか（すべてビジー）、どのプロセスも処理完了のイベントを送信しなかった場合、Kaspersky Embedded Systems Security はこのオブジェクトをスキップし、**スキップされた要求の合計数**カウンターの値が1つ加算されます。 |
| **目的** | このカウンターの値により、ファイルインターセプションディスパッチャのエラーによるパフォーマンスの低下を検出できます。 |
| **標準値 / しきい値** | 0 / 1 |
| **推奨読み取り間隔** | 1時間 |
| **値がしきい値を超えた場合の設定の推奨事項** | カウンターがゼロ以外の場合は、1つ以上のファイルインターセプションディスパッチャストリームがフリーズしてダウンしていることを意味します。このカウンターの値は、現在ダウンしているストリームの数に対応します。<br>スキャン速度が十分でない場合は、Kaspersky Embedded Systems Security を再起動してオフラインストリームを復元してください。 |

# システムリソースの不足が原因で処理されなかった要求の数

システムリソースの不足が原因で処理されなかった要求の数

| | |
|---|---|
| **名前** | リソースの不足が原因で処理されなかった要求の数 |
| **定義** | システムリソース（メモリなど）が不足しているため処理されなかったファイルインターセプションドライバーからの要求の合計数。この数は、Kaspersky Embedded Systems Security が最後に起動された時点からカウントされます。<br>Kaspersky Embedded Systems Security は、ファイルインターセプションドライバーによって処理されていないオブジェクト処理要求をスキップします。 |
| **目的** | このカウンターは、システムリソースの不足が原因で発生する、コンピューターのリアルタイム保護の品質低下の可能性を検出して除去するために使用できます。 |
| **標準値 / しきい値** | 0 / 1 |
| **推奨読み取り間隔** | 1時間 |
| **値がしきい値を超えた場合の設定の推奨事項** | カウンターの値がゼロ以外の場合は、Kaspersky Embedded Systems Security 処理対象プロセスが要求を処理するために、より多くのメモリを必要としています。<br>他のアプリケーションの実行中プロセスが利用可能なメモリをすべて使用している可能性があります。 |

# 処理のために送信された要求の数

処理のために送信された要求の数

| | |
|---|---|
| **名前** | 処理のために送信された要求の数 |
| **定義** | 処理対象プロセスによる処理を待っているオブジェクトの数。 |
| **目的** | このカウンターは、Kaspersky Embedded Systems Security の処理対象プロセスの負荷および保護対象デバイス上のファイル動作の全体的なレベルを監視するために使用できます。 |
| **標準値 / しきい値** | このカウンターは、保護対象デバイス上のファイル動作のレベルによって変化します。 |
| **推奨読み取り間隔** | 1分 |
| **値がしきい値を超えた場合の設定の推奨事項** | N/A |

# ファイルインターセプションディスパッチャストリームの平均数

ファイルインターセプションディスパッチャストリームの平均数

| | |
|---|---|
| **名前** | ファイルインターセプションディスパッチャストリームの平均数 |
| **定義** | 1つのプロセス内のファイルインターセプションディスパッチャストリームの数、およびコンピューターのリアルタイム保護タスクに現在関わっているすべてのプロセスの平均値。 |
| **目的** | このカウンターは、Kaspersky Embedded Systems Security プロセスでの過負荷による、コン |

| | |
|---|---|
| | ピューターのリアルタイム保護の潜在的な低下を検出して除去するために使用できます。 |
| **標準値 / しきい値** | 可変 / 40 |
| **推奨読み取り間隔** | 1分 |
| **値がしきい値を超えた場合の設定の推奨事項** | 各処理対象プロセスで最大 60 のファイルインターセプションディスパッチャストリームを作成できます。このカウンターが 60 に近い場合、いずれの処理対象プロセスも、現在のキューにあるファイルインターセプションドライバーからの次の要求を処理できず、Kaspersky Embedded Systems Security がそのオブジェクトをスキップする危険性があります。<br>コンピューターのリアルタイム保護タスク用の Kaspersky Embedded Systems Security プロセスの数を増やしてください。［**実行中プロセスの最大数**］、［**リアルタイム保護の対象プロセスの数**］などの Kaspersky Embedded Systems Security の設定を使用できます。 |

## ファイルインターセプションディスパッチャストリームの最大数

ファイルインターセプションディスパッチャストリームの最大数

| | |
|---|---|
| **名前** | ファイルインターセプションディスパッチャストリームの最大数 |
| **定義** | 1つのプロセス内のファイルインターセプションディスパッチャストリームの数、およびコンピューターのリアルタイム保護タスクに現在関わっているすべてのプロセスの最大値。 |
| **目的** | このカウンターの値により、実行中のプロセスでの不均等な負荷分散を原因としたパフォーマンス低下を検出して除去できます。 |
| **標準値 / しきい値** | 可変 / 40 |
| **推奨読み取り間隔** | 1分 |
| **値がしきい値を超えた場合の設定の推奨事項** | このカウンターの値が**ファイルインターセプションディスパッチャストリームの平均数**カウンターの値を継続的に大きく上回る場合は、Kaspersky Embedded Systems Security の実行中プロセスへの負荷分散が不均等になっています。<br>Kaspersky Embedded Systems Security の再起動 |

## 感染したオブジェクトのキュー内にある項目数。

感染したオブジェクトのキュー内にある項目数。

| | |
|---|---|
| **名前** | 感染したオブジェクトのキュー内にある項目数。 |
| **定義** | 現在処理（駆除または削除）を待っている感染したオブジェクトの数。 |
| **目的** | このカウンターの値により、次の状況を検出できます：<br>• ファイルインターセプションディスパッチャの障害発生の可能性によるコンピューターのリアルタイム保護の中断<br>• さまざまな処理対象プロセスと Kaspersky Embedded Systems Security 間のプロセッサ時間の配分が不均等であるためにプロセスが過負荷状態であること<br>• ウイルスアウトブレイク |

| | |
|---|---|
| **標準値 / しきい値** | この値は、Kaspersky Embedded Systems Security が感染したオブジェクトまたは感染の可能性があるオブジェクトを処理している間はゼロ以外の値を返し、その処理が終了した後はゼロを返します。ゼロ以外の値が返される状況が長時間続きます。 |
| **推奨読み取り間隔** | 1分 |
| **値がしきい値を超えた場合の設定の推奨事項** | ゼロ以外のカウンターの値が返される状況が長時間続く場合：<br>• Kaspersky Embedded Systems Security はオブジェクトを処理していない（ファイルインターセプションディスパッチャがクラッシュした可能性がある）。<br>Kaspersky Embedded Systems Security の再起動<br>• オブジェクトを処理するためのプロセッサ時間が不十分である可能性がある。<br>Kaspersky Embedded Systems Security に追加のプロセッサ時間が割り当てられるようにしてください（保護対象デバイス上の他のアプリケーションの負荷を減らすなど）。<br>• ウイルスアウトブレイクが発生した。<br>ファイルのリアルタイム保護タスクで多数の感染したオブジェクトまたは感染の可能性があるオブジェクトが発生している場合も、ウイルスアウトブレイクの兆候を示しています。タスク統計または実行ログで検知されたオブジェクト数に関する情報を表示できます。 |

## 1秒あたりの処理オブジェクト数

1秒あたりの処理オブジェクト数

| | |
|---|---|
| **名前** | 1秒あたりの処理オブジェクト数。 |
| **定義** | 処理されたオブジェクト数を、オブジェクトの処理にかかった時間で割った数（等しい時間間隔で計算します）。 |
| **目的** | このカウンターはオブジェクトの処理速度を示します。これを使用して、Kaspersky Embedded Systems Security プロセスに割り当てられたプロセッサ時間が不十分であるか、Kaspersky Embedded Systems Security の動作エラーによって発生した、保護対象デバイスのパフォーマンスが低下したポイントを検出して除去できます。 |
| **標準値 / しきい値** | 不定 / なし |
| **推奨読み取り間隔** | 1分 |
| **値がしきい値を超えた場合の設定の推奨事項** | このカウンターの値は、Kaspersky Embedded Systems Security の設定の値と、保護対象デバイス上の他のアプリケーションプロセスの負荷に応じて異なります。<br>カウンターの平均値を長期的に監視してください。通常のカウンター値が低下した場合、次のいずれかの状況が考えられます：<br>• Kaspersky Embedded Systems Security プロセスに、オブジェクトを処理するための十分なプロセッサ時間が割り当てられていない。<br>Kaspersky Embedded Systems Security に追加のプロセッサ時間が割り当てられるようにしてください（保護対象デバイス上の他のアプリケーションの負荷を減らすなど）。<br>• Kaspersky Embedded Systems Security でエラーが発生している（複数のストリームがアイドル状態である）。<br>Kaspersky Embedded Systems Security の再起動 |

# Kaspersky Embedded Systems Security の SNMP カウンターおよびトラップ

このセクションでは、Kaspersky Embedded Systems Security のカウンターおよびトラップについて説明します。

# Kaspersky Embedded Systems Security の SNMP カウンターおよびトラップについて

アンチウイルスコンポーネントセットの SNMP カウンターおよび SNMP トラップをインストールに追加した場合、Simple Network Management Protocol（SNMP）を使用して Kaspersky Embedded Systems Security のカウンターおよびトラップを参照できます。

管理者のワークステーションから Kaspersky Embedded Systems Security のカウンターおよびトラップを参照するには、保護対象デバイスで SNMP サービスを開始し、さらに管理者のワークステーションで SNMP サービスおよび SNMP トラップサービスを開始します。

# Kaspersky Embedded Systems Security の SNMP カウンター

このセクションでは Kaspersky Embedded Systems Security SNMP カウンターの設定の概要を表で説明します。

## パフォーマンスカウンター

パフォーマンスカウンター

| カウンター | 定義 |
| --- | --- |
| currentRequestsAmount | 処理のために送信された要求の数 |
| currentInfectedQueueLength | 感染したオブジェクトのキュー内にある項目数。 |
| currentObjectProcessingRate | 1 秒あたりの処理オブジェクト数 |
| currentWorkProcessesNumber | Kaspersky Embedded Systems Security で使用される処理対象プロセスの現在の数 |

## 隔離カウンター

隔離カウンター

| カウンター | 定義 |
| --- | --- |
| totalObjects | 現在隔離にあるオブジェクトの数 |
| totalSuspiciousObjects | 現在隔離にある感染の可能性があるオブジェクトの数 |
| | |

| | |
|---|---|
| currentStorageSize | 隔離内のデータの合計サイズ（MB） |

## バックアップカウンター

バックアップカウンター

| カウンター | 定義 |
|---|---|
| currentBackupStorageSize | バックアップ内のデータの合計サイズ（MB） |

## 標準カウンター

標準カウンター

| カウンター | 定義 |
|---|---|
| lastCriticalAreasScanAge | 保護対象デバイスの重要な領域の前回のスキャンが完了してからの「経過時間」（前回の簡易スキャンタスクが完了してからの経過時間）。 |
| licenseExpirationDate | ライセンスの有効期限。現在のライセンスと予備のライセンスが追加されている場合、予備のライセンスに関連付けられたライセンスの有効期限日が表示されます。 |
| currentApplicationUptime | 前回の開始以降の Kaspersky Embedded Systems Security の実行時間（100 分の 1 秒単位） |

## 更新カウンター

更新カウンター

| カウンター | 定義 |
|---|---|
| avBasesAge | 定義データベースが作成されてからの「経過時間」（前回インストールされた定義データベースのアップデートの作成日以降の経過時間（100 分の 1 秒単位））。 |

## ファイルのリアルタイム保護カウンター

ファイルのリアルタイム保護カウンター

| カウンター | 定義 |
|---|---|
| totalObjectsProcessed | 前回のファイルのリアルタイム保護タスクの実行以降にスキャンされたオブジェクトの合計数 |
| totalInfectedObjectsFound | 前回のファイルのリアルタイム保護タスクの実行以降に検知された、感染したオブジェクトとその他のオブジェクトの合計数 |
| totalSuspiciousObjectsFound | 前回のファイルのリアルタイム保護タスクの実行以降に検知された、感染の可能性があるオブジェクトの合計数 |
| totalVirusesFound | 前回のファイルのリアルタイム保護タスクの実行以降に検知されたオブジェクトの合計数 |
| totalObjectsQuarantined | 隔離に入れられた、感染したオブジェクトと感染の可能性があるオブジ |

| | |
|---|---|
| | ェクト、およびその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |
| totalObjectsNotQuarantined | 隔離しようとしたができなかった、感染したオブジェクトまたは感染の可能性があるオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |
| totalObjectsDisinfected | 駆除が成功した、感染したオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |
| totalObjectsNotDisinfected | 駆除しようとしたができなかった、感染したオブジェクトとその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |
| totalObjectsDeleted | 削除が成功した、感染したオブジェクトと感染の可能性があるオブジェクト、およびその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |
| totalObjectsNotDeleted | 削除しようとしたができなかった、感染したオブジェクトと感染の可能性があるオブジェクト、およびその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |
| totalObjectsBackedUp | バックアップに入れられた、感染したオブジェクトとその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |
| totalObjectsNotBackedUp | バックアップに入れようとしたができなかった、感染したオブジェクトとその他のオブジェクトの合計数。前回のファイルのリアルタイム保護タスクの開始時から計算 |

## Kaspersky Embedded Systems Security の SNMP トラップとそのオプション

Kaspersky Embedded Systems Security の SNMP トラップオプションについて、以下に概要を示します：

- eventThreatDetected：オブジェクトが検知されました。
  トラップには次のオプションがあります：
  - eventDateAndTime
  - eventSeverity
  - computerName
  - userName
  - objectName
  - threatName
  - detectType
  - detectCertainty
- eventBackupStorageSizeExceeds：バックアップの最大サイズを超過しました。バックアップ内のデータの合計サイズが［**バックアップの最大サイズ（MB）**］で指定した値を超過しました。感染したオブジェクトのバックアップを継続します。

トラップには次のオプションがあります：

- eventDateAndTime
- eventSeverity
- eventSource

- eventThresholdBackupStorageSizeExceeds：バックアップの空き容量がしきい値に達しました。バックアップの空き容量が［**空き容量のしきい値（MB）**］で指定された値以下になりました。感染したオブジェクトのバックアップを継続します。

  トラップには次のオプションがあります：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventQuarantineStorageSizeExceeds：隔離の最大サイズを超過しました。隔離フォルダー内のデータの合計サイズが［**隔離の最大サイズ（MB）**］で指定した値を超過しました。感染の可能性があるオブジェクトの隔離を継続します。

  トラップには次のオプションがあります：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventThresholdQuarantineStorageSizeExceeds：隔離の空き容量がしきい値に達しました。［**空き容量のしきい値（MB）**］で割り当てられた隔離内の空き容量が、指定された値以下になりました。感染したオブジェクトのバックアップを継続します。

  トラップには次のオプションがあります：

  - eventDateAndTime
  - eventSeverity
  - eventSource

- eventObjectNotQuarantined：隔離中にエラーが発生しました。

  トラップには次のオプションがあります：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - userName
  - computerName
  - objectName

- storageObjectNotAddedEventReason

- eventObjectNotBackuped：バックアップでのオブジェクトコピーの保存中にエラーが発生しました。
  トラップには次のオプションがあります：
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - objectName
  - userName
  - computerName
  - storageObjectNotAddedEventReason
- eventQuarantineInternalError：隔離中に内部エラーが発生しました。
  トラップには次のオプションがあります：
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventBackupInternalError：バックアップでエラーが発生しました。
  トラップには次のオプションがあります：
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - eventReason
- eventAVBasesOutdated：定義データベースがアップデートされていません。前回の定義データベースのアップデートタスク（ローカルタスク、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）が実行されてから経過した日数。
  トラップには次のオプションがあります：
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventAVBasesTotallyOutdated：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。前回の定義データベースのアップデートタスク（ローカルタスク、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）が実行されてから経過した日数。

  トラップには次のオプションがあります：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventApplicationStarted：Kaspersky Embedded Systems Security が実行中です。

  トラップには次のオプションがあります：

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventApplicationShutdown：Kaspersky Embedded Systems Security が停止しました。

  トラップには次のオプションがあります：

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventCriticalAreasScanWasntPerformForALongTime：重要領域の簡易スキャンが長期間実行されていません。前回の簡易スキャンタスクが実行されてから経過した日数。

  トラップには次のオプションがあります：

  - eventSeverity
  - eventDateAndTime
  - eventSource
  - days

- eventLicenseHasExpired：ライセンスの有効期間が終了しました。

  トラップには次のオプションがあります：

  - eventSeverity
  - eventDateAndTime
  - eventSource

- eventLicenseExpiresSoon：ライセンスの有効期間がまもなく終了します。ライセンスの有効期限までの日数として計算されます。

トラップには次のオプションがあります：

- eventSeverity
- eventDateAndTime
- eventSource
- days

- eventTaskInternalError：タスクの実行中にエラーが発生しました。
  トラップには次のオプションがあります：
  - eventSeverity
  - eventDateAndTime
  - eventSource
  - errorCode
  - knowledgeBaseId
  - taskName
- eventUpdateError：アップデートタスクの実行中にエラーが発生しました。
  トラップには次のオプションがあります：
  - eventSeverity
  - eventDateAndTime
  - taskName
  - updaterErrorEventReason

## Kaspersky Embedded Systems Security の SNMP トラップオプションの説明と取り得る値

トラップオプションとその可能な値は、次のとおりです：

- eventDateAndTime：イベントの発生日時。
- eventSeverity：重要度。
  オプションとして、次の値が使用されます：
  - critical (1) - 重要。
  - warning (2) - 警告。
  - info (3) - 情報。

- userName：ユーザー名（例：感染したファイルにアクセスしようとしたユーザーの名前）。
- computerName：保護対象デバイス名（例：感染したファイルにアクセスしようとしたユーザーの保護対象デバイスの名前）。
- eventSource：イベントが生成された機能コンポーネント。
  オプションとして、次の値が使用されます：
  - unknown (0) - 不明な機能コンポーネント。
  - quarantine (1) - 隔離。
  - backup (2) - バックアップ。
  - reporting (3) - 実行ログ。
  - updates (4) - アップデート。
  - realTimeProtection (5) - ファイルのリアルタイム保護。
  - onDemandScanning (6) - オンデマンドスキャン。
  - product (7) - 個々のコンポーネントの操作ではなく Kaspersky Embedded Systems Security 全体の操作に関連するイベント。
  - systemAudit (8) - システム監査ログ。
- eventReason：イベントトリガー：イベントを引き起こすもの。
  オプションとして、次の値が使用されます：
  - reasonUnknown(0) - 不明な理由。
  - reasonInvalidSettings (1) - バックアップイベントと隔離イベントのみ。隔離またはバックアップが利用できない場合に表示される（アクセス権限が不十分か、ネットワークパスが指定されているなど、隔離設定でのフォルダー指定に誤りがある）。この場合、既定のバックアップフォルダーまたは隔離フォルダーが使用される。
- objectName：オブジェクト名（例：ウイルスが検知されたファイルの名前）。
- threatName：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。
- detectType：検知したオブジェクトの種別。
  オプションとして、次の値が使用されます：
  - undefined (0) - 未定義。
  - virware - 古典的なウイルスおよびネットワークワーム。
  - trojware - トロイの木馬。
  - malware - その他の悪意のあるアプリケーション。
  - adware - 広告目的のソフトウェア。

- pornware - アダルトソフトウェア。
- riskware：ユーザーのデバイスまたはデータを損傷させるために侵入者が使用している可能性がある正規アプリケーション。

- detectCertainty：検知された脅威が実際の脅威であるかの検知の信頼度。
  オプションとして、次の値が使用されます：
  - Suspicion（感染の可能性あり） - Kaspersky Embedded Systems Security により、オブジェクトコードのセクションと既知の悪意のあるコードのセクションの部分一致が検知されている。
  - Sure（感染） - Kaspersky Embedded Systems Security により、オブジェクトコードのセクションと既知の悪意のあるコードのセクションの完全一致が検知されている。
- days：日数（例：ライセンスの有効期限までの日数）。
- errorCode：エラーコード。
- knowledgeBaseId：ナレッジベースの記事のアドレス（例：特定のエラーについて説明している記事のアドレス）。
- taskName：タスク名。
- updaterErrorEventReason：アップデートエラーの理由。
  オプションとして、次の値が使用されます：
  - reasonUnknown(0) - 不明な理由。
  - reasonAccessDenied - アクセスが拒否された。
  - reasonUrlsExhausted - アップデート元リストにあるどのアップデート元にも接続できなかった。
  - reasonInvalidConfig - 設定ファイルが無効。
  - reasonInvalidSignature - 署名が無効。
  - reasonCantCreateFolder - フォルダーを作成できない。
  - reasonFileOperError - ファイルのエラー。
  - reasonDataCorrupted - オブジェクトが破損している。
  - reasonConnectionReset - 接続がリセットされた。
  - reasonTimeOut - 接続がタイムアウトした。
  - reasonProxyAuthError - プロキシの認証エラー。
  - reasonServerAuthError - サーバーの認証エラー。
  - reasonHostNotFound - デバイスが見つからない。
  - reasonServerBusy - サーバーを使用できない。
  - reasonConnectionError - 接続エラー。

- reasonModuleNotFound - オブジェクトが見つからない。
- reasonBlstCheckFailed(16) - ライセンス情報の拒否リストを確認中にエラーが発生した。アップデート時点でデータベースのアップデートが公開中であった可能性があります。数分後に再度アップデートを実行してください。

- storageObjectNotAddedEventReason：オブジェクトのバックアップまたは隔離が実行されなかった理由。

  オプションとして、次の値が使用されます：

  - reasonUnknown(0) - 不明な理由。
  - reasonStorageInternalError - データベースのエラー。Kaspersky Embedded Systems Security を復元する必要があります。
  - reasonStorageReadOnly - データベースが読み取り専用になっている。Kaspersky Embedded Systems Security を復元する必要があります。
  - reasonStorageIOError - 入力-出力エラー：a) Kaspersky Embedded Systems Security が破損している。Kaspersky Embedded Systems Security を復元する必要があります。b) Kaspersky Embedded Systems Security ファイルのディスクが破損している。
  - reasonStorageCorrupted - 保管領域が破損している。Kaspersky Embedded Systems Security を復元する必要があります。
  - reasonStorageFull - データベースの空き容量がない。空きディスク容量が必要です。
  - reasonStorageOpenError - データベースファイルを開けない。Kaspersky Embedded Systems Security を復元する必要があります。
  - reasonStorageOSFeatureError - 一部のオペレーティングシステム機能が Kaspersky Embedded Systems Security の要件を満たしていない。
  - reasonObjectNotFound - 隔離に配置しようとしたオブジェクトがディスク上に存在しない。
  - reasonObjectAccessError - Backup API を使用する十分な権限がない。操作を行うために使用されているアカウントには、Backup Operator 権限がありません。
  - reasonDiskOutOfSpace - ディスクの空き容量が不十分。

## WMI との統合

Kaspersky Embedded Systems Security は、Windows Management Instrumentation（WMI）との統合をサポートしています：Web-Based Enterprise Management（WBEM）標準でデータを受信し、Kaspersky Embedded Systems Security とそのコンポーネントの情報を受信する目的で WMI を使用するクライアントシステムを使用できます。

Kaspersky Embedded Systems Security のインストール時に、システムに専用モジュールが登録されます。このモジュールは、保護対象デバイスに Kaspersky Embedded Systems Security の名前空間を作成します。Kaspersky Embedded Systems Security の名前空間により、Kaspersky Embedded Systems Security のクラス、インスタンス、プロパティが使用できるようになります。

一部のインスタンスのプロパティの値は、タスク種別に依存します。

*定期的でないタスク*は時間の制約がないタスクで、常に実行させておくことも停止することも可能です。これらのタスクでは、実行時の進捗が表示されません。タスクの結果は、タスクが単一のイベントとして実行されている間（例：任意のコンピューターのリアルタイム保護タスクで感染したオブジェクトを検知した場合など）は、継続的にログに記録されます。この種別のタスクは、Kaspersky Security Center のポリシーで管理されます。

*定期的なタスク*は時間の制約があるタスクで、実行時の進捗がパーセンテージで表示されます。タスクの結果は、タスクの完了時に生成され、単一のアイテムまたは変更されたアプリケーションのステータスとして表示されます（例：定義データベースのアップデートの完了、ルールの自動生成タスクの設定ファイルの生成など）。同じ種別の定期的なタスクのいくつかが、単一の保護対象デバイス上で同時に実行できます（例：オンデマンドスキャンを異なるタスク範囲で 3 つ実行するなど）。定期的なタスクは、Kaspersky Security Center のグループタスクとして管理されます。

WMI 名前空間のクエリの生成や、企業ネットワークの WMI 名前空間からの動的データの受信にツールを使用する場合、現在の本製品の状態に関する情報を受信できます（次の表を参照）。

本製品の状態に関する情報

| インスタンスのプロパティ | 説明 | 値 |
|---|---|---|
| ProductName | インストールされた本製品の名前。 | 本製品の名前（バージョン番号なし）。 |
| ProductVersion | インストールされた本製品のバージョン。 | 本製品のバージョン番号（ビルド番号を含む）。 |
| InstalledPatches | インストールされたパッチの表示名のセット。 | 本製品にインストールされた重要な修正のリスト。 |
| IsLicenseInstalled | 本製品のアクティベーションのステータス。 | 本製品のアクティベーションに使用されたライセンスの状態。<br>取りうる値：<br>• False - ライセンス情報ファイルが本製品に追加されていません。<br>• True - ライセンス情報ファイルが本製品に追加されています。 |
| LicenseDaysLeft | 現在のライセンスの有効期間が終了するまでの日数を表示します。 | 現在のライセンスの有効期間が終了するまでの日数。<br>取りうる 0 以下の値：<br>• 0 - ライセンスの有効期間が終了しています。<br>• -1 - 現在のライセンスに関する情報が取得できないか、指定されたライセンス情報が本製品のアクティベーションに使用できません（例：ライセンスの拒否リストに掲載されているため、ブロックされているなど）。 |
| AVBasesDatetime | 現在の定義データベースのバージョンのタイムスタンプ。 | 現在使用されている定義データベースの作成日時。<br>インストール済みの本製品が定義データベースを使用していない場合、フィールドの値は「未インストール」になります。 |
| IsExploitPreventionEnabled | 脆弱性攻撃ブロックコンポーネントの状態。 | 脆弱性攻撃ブロックコンポーネントの状態。<br>取りうる値： |

| | | |
|---|---|---|
| | | • True - 脆弱性攻撃ブロックコンポーネントが有効で、保護を提供しています。<br>• False - 脆弱性攻撃ブロックコンポーネントが保護を提供していません。例：無効にされている、未インストールである、使用許諾契約書に違反している、など。 |
| ProtectionTasksRunning | 現在実行中の保護タスクのセット。 | 現在実行中の保護、管理、監視などのタスク。このフィールドには、実行中のすべての定期的でないタスクが表示されます。<br>定期的でないタスクが1つも実行されていない場合は、フィールドの値は「None」になります。 |
| IsAppControlRunning | アプリケーション起動コントロールタスクの状態。 | アプリケーション起動コントロールタスクの状態。<br>• True - アプリケーション起動コントロールタスクが現在実行中です。<br>• False - アプリケーション起動コントロールタスクが現在実行されていないか、コンポーネントがインストールされていません。 |
| AppControlMode | アプリケーション起動コントロールタスクのモード。 | アプリケーション起動コントロールコンポーネントの現在の状態の説明と、そのタスクで選択されたモードの説明。<br>取りうる値：<br>• Active - ［**処理を実行**］モードがタスク設定で選択されています。<br>• Statistics Only - ［**統計のみ**］モードがタスク設定で選択されています。<br>• Not installed - アプリケーション起動コントロールコンポーネントが未インストールです。 |
| AppControlRulesNumber | アプリケーション起動コントロールルールの総数。 | アプリケーション起動コントロールルールタスクの設定で現在指定されているルールの数。 |
| AppControlLastBlocking | アプリケーション起動コントロールタスクが任意のモードで起動をブロックした最後のタイムスタンプ。 | アプリケーション起動コントロールコンポーネントがアプリケーションの起動を最後にブロックした日時。このフィールドには、ブロックされたアプリケーションのすべてが、タスクのモードに関係なく表示されます。<br>WMI クエリが処理された時点でアプリケーションの起動のブロックのインスタンスが記録されていない場合、このフィールドの値は「None」になります。 |
| PeriodicTasksRunning | 現在実行中の定期的なタスクのセット。 | 現在実行中のオンデマンドスキャン、アップデート、インベントリを使用するタスクのリスト。このフィールドには、実行中のすべての定期的なタスクが表示されます。 |

| | | |
|---|---|---|
| | | 定期的なタスクが1つも実行されていない場合は、フィールドの値は「None」になります。 |
| ConnectionState | WMI プロバイダーコンポーネントと Kaspersky Security サービス（KAVFS）間の接続の状態。 | WMI プロバイダーコンポーネントと Kaspersky Security サービス間の接続に関する情報。<br>取りうる値：<br>• Success - 接続が正常に確立されています：WMI クライアントがアプリケーションの状態を受信可能な状態です。<br>• Failed.Error Code: <コード> - 特定のコードを持つエラーにより、接続が確立されていません。 |

このデータは、次のインスタンスのプロパティで表示されます：
KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security

- KasperskySecurity_ProductInfo：Kaspersky Embedded Systems Security のクラスの名前
- .ProductName=Kaspersky Embedded Systems Security：Kaspersky Embedded Systems Security のキープロパティ

インスタンスは、名前空間 ROOT\Kaspersky\Security に作成されます。

# コマンドラインからの Kaspersky Embedded Systems Security の使用

このセクションでは、コマンドラインからの Kaspersky Embedded Systems Security の使用について説明します。

## コマンド

Kaspersky Embedded Systems Security ソフトウェアコンポーネントグループに含まれるコマンドラインユーティリティコンポーネントを使用して、保護対象デバイスのコマンドラインから基本的な Kaspersky Embedded Systems Security 管理コマンドを実行できます。

コマンドを使用すると、Kaspersky Embedded Systems Security で自分に割り当てられた権限に基づいてアクセス可能な機能のみを管理できます。

特定の Kaspersky Embedded Systems Security のコマンドは次のモードで実行されます：

- 同期モード：コマンドが完了するまで、コンソールでの操作はできません。
- 非同期モード：コマンドが開始された直後から、コンソールでの操作が可能です。

*同期モードでのコマンドの実行を中断するには：*

キーボードショートカット **Ctrl+C** を押します。

Kaspersky Embedded Systems Security のコマンド入力時は、次のルールに従います：

- 修飾子とコマンドの入力には、大文字と小文字を使用する。
- 修飾子をスペースで区切る。
- 値として指定するファイルまたはフォルダーのパスに空白文字が含まれる場合は、パスを引用符で囲む。例：`"C:\TEST\test cpp.exe"`
- 必要に応じて、ファイル名またはパスにワイルドカードを使用する。例：「`C:\Temp\Temp*\`」、「`C:\Temp\Temp???.doc`」、「`C:\Temp\Temp*.doc`」

Kaspersky Embedded Systems Security の管理に必要な操作はすべてコマンドラインを使用して実行できます（次の表を参照）。

Kaspersky Embedded Systems Security のコマンド

| コマンド | 説明 |
| --- | --- |
| KAVSHELL APPCONTROL | 選択したインポートルールに従ってルールリストを更新します。 |
| KAVSHELL APPCONTROL /CONFIG | アプリケーション起動コントロールタスクの処理モードを設定します。 |
| KAVSHELL APPCONTROL /GENERATE | アプリケーション起動コントロールルールの自動作成タスクを開始します。 |
| KAVSHELL VACUUM | Kaspersky Embedded Systems Security のログファイルのデフラグを実行します。 |

| | |
|---|---|
| KAVSHELL PASSWORD | パスワードによる保護の設定を管理します。 |
| KAVSHELL HELP | Kaspersky Embedded Systems Security のコマンドヘルプを表示します。 |
| KAVSHELL START | Kaspersky Security サービスを開始します。 |
| KAVSHELL STOP | Kaspersky Security サービスを停止します。 |
| KAVSHELL SCAN | 一時的なオンデマンドスキャンタスクを作成または開始します。スキャン範囲とセキュリティ設定については、コマンドラインのオプションで指定します。 |
| KAVSHELL SCANCRITICAL | 簡易スキャンのローカルシステムタスクを開始します。 |
| KAVSHELL TASK | 指定したタスクを非同期で開始、一時停止、再開、停止します。さらに、現在のタスクの状態または統計を表示します。 |
| KAVSHELL RTP | すべてのコンピューターのリアルタイム保護タスクを開始または停止します。 |
| KAVSHELL UPDATE | 定義データベースのアップデートタスクを開始します。設定については、コマンドラインのオプションで指定します。 |
| KAVSHELL ROLLBACK | 以前のバージョンの定義データベースにロールバックします。 |
| KAVSHELL LICENSE | ライセンスを追加または削除します。追加されたライセンスに関する情報を表示します。 |
| KAVSHELL TRACE | トレースログを有効または無効にします。トレースログの設定を管理します。 |
| KAVSHELL DUMP | Kaspersky Embedded Systems Security のプロセスが異常終了した時に、ダンプファイルの作成を有効または無効にします。 |
| KAVSHELL IMPORT | 一般的な Kaspersky Embedded Systems Security 設定、機能、およびタスクを設定ファイルからインポートします。 |
| KAVSHELL EXPORT | Kaspersky Embedded Systems Security のすべての設定および既存タスクを設定ファイルにエクスポートします。 |
| KAVSHELL DEVCONTROL | 選択した方法に応じて、作成されたデバイスコントロールルールのリストに追加します。 |

## Kaspersky Embedded Systems Security コマンドヘルプの表示：KAVSHELL HELP

すべての Kaspersky Embedded Systems Security コマンドのリストを表示するには、次のコマンドのいずれかを実行します：

```
KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

コマンドの説明とその構文を表示するには、次のコマンドのいずれかを実行します：

```
KAVSHELL HELP <コマンド>
```

```
KAVSHELL <コマンド> /?
```

### KAVSHELL HELP examples

KAVSHELL SCAN コマンドの詳細情報を表示するには、次のコマンドを実行します：

```
KAVSHELL HELP SCAN
```

## Kaspersky Security サービスの開始と停止：KAVSHELL START、KAVSHELL STOP

Kaspersky Security サービスを実行するには、次のコマンドを実行します：

```
KAVSHELL START
```

既定では、Kaspersky Security サービスの起動時に、ファイルのリアルタイム保護、オペレーティングシステムの起動時にスキャンといったタスクに加え、**アプリケーションの起動時**に開始するようにスケジュールされたその他のタスクが開始されます。

Kaspersky Security サービスを停止するには、次のコマンドを実行します：

```
KAVSHELL STOP
```

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、`[/pwd:<パスワード>]` を使用します。

## 選択した領域のスキャン：KAVSHELL SCAN

`KAVSHELL SCAN` を使用すると、保護対象デバイスの特定領域をスキャンするタスクを開始できます。このコマンドラインオプションでは、選択したフォルダーのスキャン範囲とセキュリティ設定を指定します。

`KAVSHELL SCAN` コマンドを使用して起動したオンデマンドスキャンタスクは、一時的なタスクです。このタスクは実行している時のみアプリケーションコンソールに表示されます（タスク設定をアプリケーションコンソールで確認することはできません）。ただし、タスク実行ログが生成されてアプリケーションコンソールの［**実行ログ**］フォルダーの下に表示されます。

スキャンタスク内で特定領域のパスを指定する際には、環境変数を使用できます。ユーザー環境変数を使用する場合は、該当するユーザーで `KAVSHELL SCAN` コマンドを実行します。

`KAVSHELL SCAN` コマンドは、同期モードで実行されます。

既存のオンデマンドスキャンタスクをコマンドラインから開始するには、KAVSHELL TASK コマンドを使用します。

### KAVSHELL SCAN コマンドの構文

```
KAVSHELL SCAN <スキャン範囲> [/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:<スキャン範囲のリストが含まれるファイルのパス>] [/F<A|C|E>] [/NEWONLY] [/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>] [/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>] [/EM:<"マスク">] [/ES:<サイズ>] [/ET:<秒数>] [/TZOFF] [/OF:<SKIP|RESIDENT|SCAN[=<日数>] [NORECALL]>] [/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL] [/NOCHECKMSSIGN][/W:<タスク実行ログのファイルのパス>] [/ANSI] [/ALIAS:<タスクのエイリアス>]
```

KAVSHELL SCAN コマンドには、必須のパラメータ / オプションと選択可能なパラメータ / オプションの両方があります（以下の表を参照）。

## KAVSHELL SCAN コマンドの例

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe "\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA /E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1 /NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

KAVSHELL SCAN コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
|---|---|
| **スキャン範囲**：必須のパラメータ。 | |
| <ファイル> | スキャン範囲（ファイル、フォルダー、ネットワークパス、および定義済み領域のリスト）を指定します。<br>ネットワークパスをユニバーサルネーミング規約（UNC）形式で指定します。<br>次の例では、Folder4 フォルダーはパスなしで指定されています。このフォルダーは、KAVSHELL コマンドを実行するフォルダー内にあることを示します：<br>KAVSHELL SCAN Folder4<br>スキャンするオブジェクトの名前に空白が含まれている場合は、この名前を引用符で囲む必要があります。<br>フォルダーが指定されている場合、そのすべてのサブフォルダーもスキャンされます。<br>* 記号または ? 記号はファイルのグループをスキャンするために使用できます。 |
| <フォルダー> | |
| <ネットワークパス> | |
| /MEMORY | メモリ内のオブジェクトをスキャンします。 |
| /SHARED | 保護対象デバイスにある共有フォルダーをスキャンします。 |
| /STARTUP | 自動実行オブジェクトをスキャンします。 |
| /REMDRIVES | リムーバブルドライブをスキャンします。 |
| /FIXDRIVES | ハードディスクをスキャンします。 |
| /MYCOMP | 保護対象デバイスのすべての領域をスキャンします。 |
| /L:<スキャン範囲のリストを含むファイルのパス> | スキャン範囲のリストを含むファイルの絶対パス。<br>ファイル内でスキャン範囲を区切るには、改行を使用します。スキャン範囲のリストを含む次のファイル例の内容で示すように、定義済みのスキャン範囲を指定できます。<br>C:\<br>D:\Docs*.doc<br>E:\My Documents |

| | |
|---|---|
| | /STARTUP<br>/SHARED |
| **オブジェクトのスキャン**（ファイル種別）：このオプションを指定しない場合は、形式に基づくオブジェクトのスキャンが実行されます。 | |
| /FA | すべてのオブジェクトをスキャンします。 |
| /FC | オブジェクトを形式に基づいてスキャンします（既定）。感染の可能性があるオブジェクト形式のリストに含まれている形式のオブジェクトのみスキャンします。 |
| /FE | オブジェクトを拡張子に基づいてスキャンします。感染の可能性があるオブジェクト拡張子のリストに含まれている拡張子を持つオブジェクトのみスキャンします。 |
| /NEWONLY | 作成または変更されたファイルのみスキャン<br>このオプションを指定しない場合は、すべてのオブジェクトがスキャンされます。 |
| **感染などの問題があるオブジェクトの処理**：この修飾子の値を指定しない場合は、**スキップ**処理が実行されます。 | |
| DISINFECT | 駆除し、駆除できない場合はスキップします。<br>DISINFECT オプションと DELETE オプションは、以前のバージョンとの互換性を確保するために、現在のバージョンの Kaspersky Embedded Systems Security で維持されています。これらの設定は、/AI オプションと /AS オプションの代わりに使用できます。この場合、感染の可能性があるオブジェクトは処理されません。 |
| DISINFDEL | 駆除し、駆除できない場合は削除します。 |
| DELETE | 削除<br>DISINFECT オプションと DELETE オプションは、以前のバージョンとの互換性を確保するために、現在のバージョンの Kaspersky Embedded Systems Security で保存されています。これらの設定は、/AI オプションと /AS オプションの代わりに使用できます。この場合、感染の可能性があるオブジェクトは処理されません。 |
| REPORT | レポートを送信（既定） |
| AUTO | 推奨処理を実行 |
| /AS: **感染の可能性があるオブジェクトの処理**。このオプションを指定しない場合は、**スキップ**処理が実行されます。 | |
| QUARANTINE | 隔離 |
| DELETE | 削除 |
| REPORT | レポートを送信（既定） |
| AUTO | 推奨処理を実行 |
| **除外リスト** | |
| /E:ABMSPO | 次の種別の複合オブジェクトを除外します：<br>A - アーカイブ（SFX アーカイブのみスキャン）<br>B - メールデータベース<br>M - 通常のメール<br>S - アーカイブと SFX アーカイブ<br>P - 圧縮されたオブジェクト<br>O - OLE 埋め込みオブジェクト |
| /EM:<"マスク"> | ファイルをマスクに基づいて除外します。<br>複数のマスクを指定できます。例：`EM:"*.txt; *.png; C\Videos\*.avi"` |
| | |

| | |
|---|---|
| /ET:<秒数> | この <秒数> に指定した秒数よりも長くオブジェクトの処理が続いた場合に、オブジェクトの処理を停止します。<br>既定では、時間制限はありません。 |
| /ES:<サイズ> | <サイズ> の値に指定したサイズ（MB 単位）よりも大きい複合オブジェクトはスキャンしません。<br>既定では、すべてのサイズのオブジェクトをスキャンします。 |
| /TZOFF | 信頼ゾーンの除外指定を無効にします。 |
| **詳細設定**（オプション） | |
| /NOICHECKER | iChecker の使用を無効にします（既定では有効）。 |
| /NOISWIFT | iSwift の使用を無効にします（既定では有効）。 |
| /ANALYZERLEVEL:<ヒューリスティック分析のレベル> | ヒューリスティックアナライザーを有効にし、分析レベルを設定します。<br>以下のヒューリスティック分析レベルを設定できます：<br>1 - 低<br>2 - 中<br>3 - 高<br>このオプションを省略した場合、ヒューリスティックアナライザーは使用されません。 |
| /ALIAS:<タスクエイリアス> | オンデマンドスキャンタスクに一時的な名前を割り当てることができます。タスクの実行中に、TASK コマンドを使用して統計を確認する際などに、参照できます。タスクのエイリアスは、Kaspersky Embedded Systems Security のすべてのコンポーネントのタスクエイリアスの間で一意である必要があります。<br>このオプションを指定しない場合、scan_<kavshell_pid> という形式の一時的な名前が使用されます（例：scan_1234）。アプリケーションコンソールで、「スキャンオブジェクトの名前 <日時>」がタスクに割り当てられます（例：Scan objects 8/16/2007 5:13:14 PM）。 |
| タスク実行ログの設定（レポート設定） | |
| /W:<タスク実行ログファイルのパス> | このパラメータを指定すると、Kaspersky Embedded Systems Security によって、パラメータの値で指定された名前を使用したタスクログファイルが保存されます。<br>ログファイルには、タスクの実行統計情報、タスクの開始時刻と完了（停止）時刻、およびタスク中に発生したイベントに関する情報が含まれます。<br>このログを使用して、「イベント ビューアー」のタスク実行ログの設定および Kaspersky Embedded Systems Security イベントログの設定で定義されたイベントが登録されます。<br><br>ログファイルの絶対パスまたは相対パスを指定できます。ファイル名のみを指定し、そのパスを指定しなかった場合、ログファイルは現在のフォルダーに作成されます。<br>同じログ設定でコマンドを再度開始すると、既存のログファイルが上書きされます。<br>タスクの実行中にログファイルを表示できます。<br>ログは、アプリケーションコンソールの［実行ログ］に表示されます。<br>Kaspersky Embedded Systems Security でログファイルを作成できない場合、エラーメッセージが表示されますが、コマンドは実行されます。 |
| /ANSI | このオプションは ANSI エンコーディングを使用して、イベントをタスク実行ログに記録します。<br>W パラメータを指定していない場合、この ANSI オプションは適用されません。 |

| | |
|---|---|
| | ANSI オプションが指定されていない場合、UNICODE が使用されてタスク実行ログが生成されます。 |

# 簡易スキャンの開始：KAVSHELL SCANCRITICAL

KAVSHELL SCANCRITICAL コマンドを使用すると、アプリケーションコンソールで定義された設定に従って簡易スキャンタスクを開始します。

## KAVSHELL SCANCRITICAL コマンドの構文

```
KAVSHELL SCANCRITICAL [/W:<path to task log file>]
```

## KAVSHELL SCANCRITICAL コマンドの例

簡易スキャンタスクを実行し、現在のフォルダーにタスク実行ログの scancritical.log を保存するには、次のコマンドを実行します：

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

/W パラメータを使用して、タスク実行ログの場所を設定できます（次の表を参照）。

KAVSHELL SCANCRITICAL コマンドの /W パラメータの構文

| パラメータとオプション | 説明 |
|---|---|
| /W:<タスク実行ログファイルのパス> | このパラメータを指定すると、Kaspersky Embedded Systems Security によって、パラメータの値で指定された名前を使用したタスクログファイルが保存されます。<br>ログファイルには、タスクの実行統計情報、タスクの開始時刻と完了（停止）時刻、およびタスク中に発生したイベントに関する情報が含まれます。<br>このログを使用して、「イベント ビューアー」のタスク実行ログの設定および Kaspersky Embedded Systems Security イベントログの設定で定義されたイベントが登録されます。<br>ログファイルの絶対パスまたは相対パスを指定できます。ファイル名のみを指定し、そのパスを指定しなかった場合、ログファイルは現在のフォルダーに作成されます。<br>同じログ設定でコマンドを再度開始すると、既存のログファイルが上書きされます。<br>タスクの実行中にログファイルを表示できます。<br>ログは、アプリケーションコンソールの［**実行ログ**］に表示されます。<br>Kaspersky Embedded Systems Security でログファイルを作成できない場合、エラーメッセージが表示されますが、コマンドは実行されます。 |

# タスクの非同期での管理：KAVSHELL TASK

KAVSHELL TASK コマンドを使用すると、指定のタスクを管理できます。タスクの実行、一時停止、再開、停止、およびタスクの現在のステータスと統計情報の表示を実行できます。コマンドは非同期モードで実行されます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

## KAVSHELL TASK コマンドの構文

```
KAVSHELL TASK [<タスク名のエイリアス> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

## KAVSHELL TASK コマンドの例

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE

KAVSHELL TASK network-attack-blocker /START
```

KAVSHELL TASK コマンドは、パラメータやオプションなしでも、1つ以上のパラメータやオプションを指定しても実行できます（次の表を参照）。

KAVSHELL TASK コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
|---|---|
| パラメータなし | 既存のすべての Kaspersky Embedded Systems Security タスクのリストが確認できます。リストには、次のフィールドが含まれます：タスクのエイリアス、タスクカテゴリ（システムまたはカスタム）、タスクの現在のテータス。 |
| <タスクのエイリアス> | SCAN TASK コマンドでは、タスク名の代わりに、Kaspersky Embedded Systems Security によってタスクに割り当てられた追加の省略されたの名前である、タスクのエイリアスが使用されます。Kaspersky Embedded Systems Security タスクのエイリアスを表示するには、パラメータを指定せずに KAVSHELL TASK コマンドを入力します。 |
| /START | 指定のタスクを非同期モードで開始します。 |
| /STOP | 指定のタスクを停止します。 |
| /PAUSE | 指定のタスクを一時停止します。 |
| /RESUME | 指定のタスクを非同期モードで再開します。 |
| /STATE | タスクの現在のステータス（*実行中*、*完了*、*一時停止済み*、*停止済み*、*失敗*、*開始中*、*再開中*など）を返します。 |
| /STATISTICS | タスクの統計情報（タスクが開始されてから処理されたオブジェクトの数に関する情報）を取得します。 |

すべての Kaspersky Embedded Systems Security タスクが /PAUSE、/RESUME、/STATE パラメータをすべてサポートするわけではないことに注意してください。

# PPL 属性の削除：KAVSHELL CONFIG

KAVSHELL CONFIG コマンドを使用すると、製品のインストール時にインストールされた ELAM ドライバーを使用して、Kaspersky Security サービスの PPL（Protected Process Light）属性を削除できます。

## KAVSHELL CONFIG コマンドの構文

```
KAVSHELL CONFIG /PPL:<OFF>
```

KAVSHELL CONFIG コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
| --- | --- |
| /PPL:OFF | Kaspersky Security サービスの PPL 属性を削除します。 |

# コンピューターのリアルタイム保護タスクの開始と停止：KAVSHELL RTP

KAVSHELL RTP コマンドを使用すると、すべてのコンピューターのリアルタイム保護タスクを開始または停止できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

## KAVSHELL RTP コマンドの構文

```
KAVSHELL RTP {/START | /STOP}
```

## KAVSHELL RTP コマンドの例

すべてのコンピューターのリアルタイム保護タスクを開始するには、次のコマンドを実行します：

```
KAVSHELL RTP /START
```

KAVSHELL RTP コマンドは、2 つのオプションのいずれかを含める必要があります（次の表を参照）。

KAVSHELL RTP コマンドラインオプション

| パラメータとオプション | 説明 |
| --- | --- |
| /START | すべてのコンピューターのリアルタイム保護タスクを開始します：ファイルのリアルタイム保護、KSN の使用。 |
| /STOP | すべてのコンピューターのリアルタイム保護タスクを停止します。 |

# アプリケーション起動コントロールタスクの管理：KAVSHELL APPCONTROL /CONFIG

KAVSHELL APPCONTROL/CONFIG コマンドを使用して、アプリケーション起動コントロールタスクが DLL モジュールの読み込みを実行、監視するモードを設定できます。

## KAVSHELL APPCONTROL /CONFIG コマンドの構文

/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config /savetofile:<XML ファイルの完全パス>

## KAVSHELL APPCONTROL /CONFIG コマンドの例

*アプリケーション起動コントロールタスクを、DLL の読み込みを監視せずに［**処理を実行**］モードで実行し、完了時にタスク設定を保存するには、次のコマンドを実行します：*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

コマンドラインのパラメータを使用して、アプリケーション起動コントロールタスク設定を設定できます（次の表を参照）。

KAVSHELL APPCONTROL /CONFIG コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
|---|---|
| /mode:<applyrules\|statistics> | アプリケーション起動コントロールタスクの処理モード<br>次のいずれかのモードを選択できます：<br>• active - アプリケーション起動コントロールルールを適用。<br>• statistics - 統計のみを生成します。 |
| /dll:<no\|yes> | DLL の読み込みの監視を有効または無効にします。 |
| /savetofile: <XML ファイルのパス> | 指定したルールを指定したファイルに XML 形式でエクスポートします。 |
| /savetofile: <xml ファイルの完全名> | ルールのリストをファイルに保存します。 |
| /savetofile: <xml ファイルの完全名> /sdc | ソフトウェア配布コントロールルールのリストをファイルに保存します。 |
| /clearsdc | すべてのソフトウェア配布コントロールルールをリストから削除します。 |

# アプリケーション起動コントロールルールの自動作成：KAVSHELL APPCONTROL /GENERATE

KAVSHELL APPCONTROL /GENERATE コマンドを使用して、アプリケーション起動コントロールルールリストを作成できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

## KAVSHELL APPCONTROL /GENERATE コマンドの構文

KAVSHELL APPCONTROL /GENERATE <フォルダーのパス> | /source:<フォルダーリストを含むファイルのパス> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<ユーザーまたはユーザーのグループ>] [/export:<XML ファイルのパス>] [/import:<a|r|m>] [/prefix:<ルール名の接頭辞>] [/unique]

## KAVSHELL APPCONTROL /GENERATE コマンドの例

*指定したフォルダーからファイルのルールを作成するには、次のコマンドを実行します：*

```
KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
/export:c:\rules\appctrlrules.xml
```

*指定したフォルダーにある、すべての拡張子の実行ファイルのルールを作成し、タスク完了時に、指定した XML ファイルに作成したルールを保存するには、次のコマンドを実行します：*

```
KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms /export:c\rules\appctrlrules.xml
```

コマンドラインのパラメータやオプションを使用して、アプリケーション起動コントロールタスクのルールの自動生成を設定できます（次の表を参照）。

KAVSHELL APPCONTROL /GENERATE コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
|---|---|
| **許可ルールの範囲** | |
| <フォルダーのパス> | 許可ルールが自動生成される実行ファイルのあるフォルダーへのパスを指定します。 |
| /source: <フォルダーリストを含むファイルのパス> | 許可ルールが自動生成される実行ファイルのあるフォルダーのリストを含む TXT ファイルへのパスを指定します。 |
| /masks: <edms> | 許可ルールが自動生成される実行ファイルの拡張子を指定します。<br>ルールの範囲に次の拡張子のファイルを含めることができます：<br>• e - EXE ファイル<br>• d - DLL ファイル<br>• m - MSI ファイル<br>• s - スクリプト |

| | |
|---|---|
| /runapp | 許可ルールの生成時に、保護対象デバイスで現在実行中のアプリケーションのアカウント。 |
| **許可ルールを自動的に作成する時の処理** | |
| /rules: <ch\|cp\|h> | アプリケーション起動コントロールタスクの許可ルールを生成する間に実行する処理を指定します：<br>• ch - デジタル証明書を使用する。証明書がない場合は SHA256 ハッシュを使用します。<br>• cp - デジタル証明書を使用する。証明書がない場合は、実行ファイルへのパスを使用します。<br>• h - SHA256 ハッシュを使用する。 |
| /strong | アプリケーション起動コントロールタスクの許可ルールを自動作成する時に、デジタル証明書の発行先とサムプリントを使用します。/rules: <ch\|cp> パラメータが指定されている場合、コマンドが実行されます。 |
| /user: <ユーザーまたはユーザーのグループ> | ルールを適用するユーザーまたはユーザーのグループを指定します。指定されたユーザーまたはユーザーグループによって実行されるアプリケーションを監視します。 |
| **アプリケーション起動コントロールルールの自動作成タスクの完了時の処理** | |
| /export <XML ファイルのパス> | 作成したルールを XML ファイルに保存します。 |
| /unique | アプリケーション起動コントロールの許可ルール作成の基礎となるアプリケーションがインストールされた保護対象デバイスに関する情報を追加します。 |
| /prefix: <ルール名の接頭辞> | アプリケーション起動コントロール許可ルールの名前の接頭辞を指定します。 |
| /import: <a\|r\|m> | 選択したインポートルールに従って作成したルールを、指定したアプリケーション起動コントロールのルールのリストにインポートします：<br>• a - **既存のルールに追加する**（同一の設定を持つルールは重複します）<br>• r - **既存のルールを置き換える**（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つのルールの設定が他のルールと異なる場合にルールが追加されます）<br>• m - **既存のルールとマージする**（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つのルールの設定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のリストの入力：KAVSHELL APPCONTROL

KAVSHELL APPCONTROL を使用すると、選択したインポートルールに従って XML ファイルからアプリケーション起動コントロールタスクのルールリストにルールを追加し、リストから既存のルールをすべて削除できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

### KAVSHELL APPCONTROL コマンドの構文

KAVSHELL APPCONTROL /append <XML ファイルのパス> | /replace <XML ファイルのパス> | /merge <XML ファイルのパス> | /clear

### KAVSHELL APPCONTROL コマンドの例

*［既存のルールに追加する］インポートルールに従って、XML ファイルから既存のアプリケーション起動コントロールルールにルールを追加するには、次のコマンドを実行します：*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

コマンドラインパラメータを使用して、指定した XML ファイルから新しいルールをアプリケーション起動コントロールのルールの定義済みのリストに追加する方法を選択できます（次の表を参照）。

KAVSHELL APPCONTROL コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
|---|---|
| /append <XML ファイルのパス> | 指定した XML ファイルに基づい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更新します。インポートルール - **既存のルールに追加する**（同一の設定を持つルールは重複します）。 |
| /replace <XML ファイルのパス> | 指定した XML ファイルに基づい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更新します。インポートルール - **既存のルールを置き換える**（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 つのルール設定が他のルールと異なる場合にルールが追加されます）。 |
| /merge <XML ファイルのパス> | 指定した XML ファイルに基づい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更新します。インポートルール - **既存のルールとマージする**（新しいルールは、既存のルールと重複しません）。 |
| /clear | アプリケーション起動コントロールルールのリストのクリア |

## デバイスコントロールルールのリストの入力：KAVSHELL DEVCONTROL

KAVSHELL DEVCONTROL コマンドを使用すると、選択したインポートルールに従って XML ファイルからデバイスコントロールタスクのルールリストにルールを追加し、リストから既存のルールをすべて削除できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

### KAVSHELL DEVCONTROL コマンドの構文

```
KAVSHELL DEVCONTROL /append <XML ファイルのパス> | /replace <XML ファイルのパス> | /merge <XML ファイルのパス> | /clear
```

### KAVSHELL DEVCONTROL コマンドの例

*［既存のルールに追加する］インポートルールに従って、XML ファイルからルールをデバイスコントロールタスクの既存のルールに追加するには、次のコマンドを実行します：*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

コマンドラインパラメータを使用して、指定した XML ファイルから新しいルールをデバイスコントロールのルールの定義済みのリストに追加するインポートルールを選択できます（次の表を参照）。

KAVSHELL DEVCONTROL コマンドラインのパラメータとオプション

| ライセンス | 説明 |
|---|---|
| /append <XML ファイルのパス> | 指定した XML ファイルに基づいてデバイスコントロールルールのリストを更新します。インポートルール - **既存のルールに追加する**（同一の設定を持つルールは重複します）。 |
| /replace <XML ファイルのパス> | 指定した XML ファイルに基づいてデバイスコントロールルールのリストを更新します。インポートルール - **既存のルールを置き換える**（同一のパラメータを持つルールは追加されません。少なくとも 1 つのルールの設定が他のルールと異なる場合にルールが追加されます）。 |
| /merge <XML ファイルのパス> | 指定した XML ファイルに基づいてデバイスコントロールルールのリストを更新します。インポートルール - **既存のルールとマージする**（新しいルールは、既存のルールと重複しません）。 |
| /clear | デバイスコントロールルールのリストのクリア |

## 定義データベースのアップデートタスクを開始する：KAVSHELL UPDATE

KAVSHELL UPDATE コマンドを使用すると、Kaspersky Embedded Systems Security 定義データベースのアップデートタスクを同期モードで開始できます。

KAVSHELL UPDATE コマンドを使用して起動した定義データベースのアップデートタスクは、一時的なタスクです。実行中にのみアプリケーションコンソールに表示されます。ただし、タスク実行ログが生成されてアプリケーションコンソールの［**実行ログ**］に表示されます。Kaspersky Security Center のポリシーを、KAVSHELL UPDATE コマンドを使用して作成および開始されたアップデートタスクとアプリケーションコンソールで作成されたアップデートタスクに適用できます。Kaspersky Security Center を使用して保護対象デバイス上の Kaspersky Embedded Systems Security を管理する方法については、「Kaspersky Security Center を使用した Kaspersky Embedded Systems Security の管理」を参照してください。

このタスクでアップデート元のパスを指定する際は、環境変数を使用できます。ユーザー環境変数を使用する場合は、該当するユーザーで KAVSHELL UPDATE コマンドを実行します。

## KAVSHELL UPDATE コマンドの構文

KAVSHELL UPDATE <アップデート元のパス | /AK | /KL> [/NOUSEKL] [/PROXY:<アドレス>:<ポート>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<ユーザー名>] [/PROXYPWD:<パスワード>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM] [/NOFTPPASSIVE] [/TIMEOUT:<秒>] [/REG:<ISO3166 コード>] [/W:<タスク実行ログファイルのパス>] [/ALIAS:<タスクのエイリアス>]

KAVSHELL UPDATE コマンドには、必須のパラメータ / オプションと選択可能なパラメータ / オプションの両方があります（以下の表を参照）。

## KAVSHELL UPDATE コマンドの例

*カスタムの定義データベースのアップデートタスクを開始するには、次のコマンドを実行します：*

```
KAVSHELL UPDATE
```

*ネットワークフォルダー「\\server\databases」のアップデートファイルを使用して定義データベースのアップデートタスクを実行するには、次のコマンドを実行します：*

```
KAVSHELL UPDATE \\server\databases
```

*FTP サーバー ftp://dnl-ru1.kaspersky-labs.com/ から定義データベースのアップデートタスクを開始し、すべてのタスクイベントをファイル c:\update_report.log に記録するには、次のコマンドを実行します：*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

*カスペルスキーのアップデートサーバーから Kaspersky Embedded Systems Security 定義データベースのアップデートをダウンロードするには、プロキシサーバー（プロキシサーバーアドレス：proxy.company.com、ポート：8080）を介してアップデート元に接続します。組み込みの Microsoft Windows NTLM 認証（ユーザー名：inetuser、パスワード：123456）を使用してサーバーにアクセスするには、次のコマンドを実行します：*

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

KAVSHELL UPDATE コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
|---|---|
| **アップデート元**（必須のパラメータ）。1つ以上のアップデート元を指定します。Kaspersky Embedded Systems Security は、表示されている順序でアップデート元にアクセスします。アップデート元をスペースで区切ります。 | |
| <UNC フォーマットのパス> | ユーザー定義のアップデート元。UNC フォーマットのネットワークアップデートフォルダーのパス。 |
| <URL> | ユーザー定義のアップデート元。アップデートフォルダーが配置されている HTTP または FTP サーバーのアドレス。 |
| <ローカルフォルダー> | ユーザー定義のアップデート元。保護対象デバイス上のフォルダー。 |
| /AK | Kaspersky Security Center の管理サーバーをアップデート元として使用します。 |
| /KL | 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使用します。 |
| /NOUSEKL | 他のアップデート元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を使用しません（既定で使用）。 |

| プロキシサーバーの設定 | |
|---|---|
| /PROXY:<アドレス>:<ポート> | プロキシサーバーおよびそのポートのネットワーク名または IP アドレス。このパラメータを指定しない場合、ローカルエリアネットワークで使用されているプロキシサーバーの設定が Kaspersky Embedded Systems Security によって自動的に検出されます。 |
| /AUTHTYPE:<0-2> | このパラメータで、プロキシサーバーにアクセスするための認証方法を指定します。次の値が使用されます：<br>**0** - Microsoft Windows NTLM 認証。**ローカルシステム**（**SYSTEM**）アカウントを使用して Kaspersky Embedded Systems Security がプロキシサーバーに接続します。<br>**1** - Microsoft Windows NTLM 認証。パラメータ /PROXYUSER と /PROXYPWD で指定したユーザー名とパスワードを使用して Kaspersky Embedded Systems Security がプロキシサーバーに接続します。<br>**2** - パラメータ /PROXYUSER と /PROXYPWD で指定したユーザー名とパスワードを使用した認証（基本認証）。<br>プロキシサーバーが認証を必要としない場合、このパラメータを指定する必要はありません。 |
| /PROXYUSER:<ユーザー名> | プロキシサーバーへのアクセスに使用するユーザー名。/AUTHTYPE:0 を指定すると、/PROXYUSER:<ユーザー名> と /PROXYPWD:<パスワード> パラメータは無視されます。 |
| /PROXYPWD:<パスワード> | プロキシサーバーへのアクセスに使用するユーザーのパスワード。/AUTHTYPE:0 を指定すると、/PROXYUSER:<ユーザー名> と /PROXYPWD:<パスワード> パラメータは無視されます。/PROXYUSER パラメータを指定し、/PROXYPWD パラメータを省略すると、パスワードは空の文字列と判断されます。 |
| /NOPROXYFORKL | カスペルスキーのアップデートサーバーへの接続にプロキシサーバー設定を使用しません（既定で使用）。 |
| /USEPROXYFORCUSTOM | ユーザー定義のアップデート元への接続にプロキシサーバー設定を使用します（既定では使用しない）。 |
| /USEPROXYFORLOCAL | ローカルのアップデート元への接続にプロキシサーバー設定を使用します。指定しない場合、［**ローカルアドレスへの接続時はプロキシサーバーを使用しない**］の設定が適用されます。 |
| **FTP サーバーと HTTP サーバーの全般設定** | |
| /NOFTPPASSIVE | このパラメータを指定すると、保護対象デバイスへの接続に Kaspersky Embedded Systems Security は FTP のアクティブモードを使用します。このパラメータを指定しない場合、Kaspersky Embedded Systems Security は FTP のパッシブモードを使用します（可能な場合）。 |
| /TIMEOUT:<秒数> | FTP サーバーまたは HTTP サーバーの接続タイムアウト。このパラメータを指定しない場合、Kaspersky Security は既定値の 10 秒を使用します。値は整数である必要があります。 |
| /REG:<iso3166 コード> | 地域の設定。このパラメータは、カスペルスキーのアップデートサーバーからアップデートを受信する場合に使用します。Kaspersky Embedded Systems Security は最も近いアップデートサーバーを選択して、保護対象デバイスの負荷を最小限に抑えます。<br>このパラメータの値は、保護対象デバイスがある国の ISO 3166-1 alpha-2 コードを指定してください（例：/REG: gr、/REG:US）。パラメータを省略した場合や無効な国コードを指定した場合、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地域の設定に基づいて、保護対象デバイスの場所が検出されます。 |
| /ALIAS:<タスクエイリア | このパラメータによって、一時的な名前をタスクに割り当てて、実行中のタ |

| | |
|---|---|
| ス> | スクを参照できます。たとえば、TASK コマンドを使用してタスクの統計情報を表示できます。タスクのエイリアスは、Kaspersky Embedded Systems Security のすべてのコンポーネントのタスクエイリアスの間で一意である必要があります。<br>このパラメータを指定しない場合、update_<kavshell_pid> という形式の一時的な名前が使用されます（例：update_1234）。アプリケーションコンソールで、タスクに「Update-databases <日時>」という名前が割り当てられます（例：Update-databases 8/16/2007 5:41:02 PM）。 |
| /W:<タスク実行ログファイルのパス> | このパラメータを指定すると、Kaspersky Embedded Systems Security によって、パラメータの値で指定された名前を使用したタスクログファイルが保存されます。<br>ログファイルには、タスクの実行統計情報、タスクの開始時刻と完了（停止）時刻、およびタスク中に発生したイベントに関する情報が含まれます。<br>このログを使用して、「イベント ビューアー」のタスク実行ログの設定および Kaspersky Embedded Systems Security イベントログの設定で定義されたイベントが登録されます。<br>ログファイルの絶対パスまたは相対パスを指定できます。ファイル名のみを指定し、そのパスを指定しなかった場合、ログファイルは現在のフォルダーに作成されます。<br>同じログ設定でコマンドを再度開始すると、既存のログファイルが上書きされます。<br>タスクの実行中にログファイルを表示できます。<br>ログは、アプリケーションコンソールの［**実行ログ**］に表示されます。<br>Kaspersky Embedded Systems Security でログファイルを作成できない場合、エラーメッセージが表示されますが、コマンドは実行されます。 |

KAVSHELL UPDATE コマンドのリターンコード。

## Kaspersky Embedded Systems Security 定義データベースのロールバック：KAVSHELL ROLLBACK

`KAVSHELL ROLLBACK` コマンドを使用すると、定義データベースのアップデートのロールバックローカルシステムタスク（Kaspersky Embedded Systems Security 定義データベースを、以前にインストールしたバージョンにロールバック）を実行できます。コマンドは同期的に実行されます。

### コマンドの構文：

```
KAVSHELL ROLLBACK
```

KAVSHELL ROLLBACK コマンドのリターンコード

## Windows イベントログ監視の管理：KAVSHELL TASK LOG-INSPECTOR

`KAVSHELL TASK LOG-INSPECTOR` コマンドを使用すると、Windows イベントログ分析に基づいて環境の整合性を監視できます。

### コマンドの構文

KAVSHELL TASK LOG-INSPECTOR

### コマンドの例

KAVSHELL TASK LOG-INSPECTOR /stop

KAVSHELL TASK LOG-INSPECTOR コマンドラインのオプション

| オプション | 説明 |
|---|---|
| /START | 指定のタスクを非同期モードで開始します。 |
| /STOP | 指定のタスクを停止します。 |
| /STATE | タスクの現在のステータス（*実行中*、*完了*、*一時停止済み*、*停止済み*、*失敗*、*開始中*、*再開中*など）を返します。 |
| /STATISTICS | タスクの統計情報（タスクが開始されてから処理されたオブジェクトの数に関する情報）を取得します。 |

KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード。

## 製品のアクティベート：KAVSHELL LICENSE

Kaspersky Embedded Systems Security のライセンスおよびアクティベーションコードは、KAVSHELL LICENSE コマンドを使用して管理できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

### KAVSHELL LICENSE コマンドの構文

KAVSHELL LICENSE [/ADD:<ライセンス情報ファイル | アクティベーションコード> [/R] | /DEL:<ライセンス情報 | アクティベーションコード番号>]

### KAVSHELL LICENSE コマンドの例

*製品をアクティベートするには、次のコマンドを実行します：*

KAVSHELL.EXE LICENSE / ADD: <アクティベーションコードまたはライセンス情報>

*追加したライセンスの情報を表示するには、次のコマンドを実行します：*

KAVSHELL LICENSE

*識別 ID 0000-000000-00000001 の追加したライセンスを削除するには、次のコマンドを実行します：*

KAVSHELL LICENSE /DEL:0000-000000-00000001

KAVSHELL LICENSE コマンドは、ライセンスを指定してもしなくても実行できます（次の表を参照）。

KAVSHELL LICENSE コマンドラインのパラメータとオプション

| パラメータ | 説明 |
| --- | --- |
| キーの指定なし | コマンドを実行すると、追加したライセンスの次の情報が返されます：<br>• ライセンス情報。<br>• ライセンスの種別（製品版）。<br>• ライセンスの期間。<br>• ライセンスのステータス（現在のライセンスまたは予備のライセンス）。ステータスが * の場合、ライセンスは予備のライセンスとして追加されました。 |
| /ADD:<ライセンス情報ファイル名またはアクティベーションコード> | 指定のファイルまたはアクティベーションコードを使用してライセンスを追加します。<br>ライセンス情報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。 |
| /R | /R のアクティベーションコードまたはライセンスは /ADD のアクティベーションコードまたはライセンスに加えて使用でき、追加されたアクティベーションコードまたはライセンスが予備のアクティベーションコードまたはライセンスであることを示します。 |
| /DEL:<ライセンス情報またはアクティベーションコード> | 指定した番号のライセンスまたはアクティベーションコードを削除します。 |

KAVSHELL LICENSE コマンドのリターンコード。

# トレースログの有効化、設定、無効化：KAVSHELL TRACE

KAVSHELL TRACE コマンドを使用すると、Kaspersky Embedded Systems Security のすべてのサブシステムのトレースログの有効化と無効化、およびログの詳細レベルの設定を行うことができます。

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。

## KAVSHELL TRACE コマンドの構文

```
KAVSHELL TRACE </ON /F:<path to trace log file folder> [/S:<maximum log size in megabytes>] [/LVL:debug|info|warning|error|critical] | /OFF>
```

トレースログが有効化されている場合に設定を変更するには、/ON オプションを使用して KAVSHELL TRACE コマンドを入力し、/S パラメータと /LVL パラメータを使用してトレースログの設定を指定します（次の表を参照）。

KAVSHELL TRACE コマンドのキー

| ライセンス | 説明 |
| --- | --- |
| /ON | トレースログの有効化。 |
| /F:<トレースログファイルを保存するフォルダー> | このパラメータで、トレースログファイルを保存するフォルダーの絶対パスを指定します（必須）。 |

| | |
|---|---|
| | 存在しないフォルダーのパスを指定すると、トレースログは作成されません。他の保護対象デバイスのネットワークドライブ上のフォルダーへのパスは指定できません。<br>パラメータによって指定されたパスに空白文字が含まれる場合は、引用符で囲む必要があります（例：/F:"C:\Trace Folder"）。<br>トレースログ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。 |
| /S: <メガバイト単位でのログファイルの最大サイズ> | このキーで、単一のトレースログファイルの最大サイズを設定します。ログファイルが最大サイズに達するとすぐに、Kaspersky Embedded Systems Security によって情報は新しいファイルに記録され、前のログファイルは保存されます。<br>このパラメータの値を指定しない場合、1 つのログファイルの最大サイズは 50 MB です。 |
| /LVL:debug\|info\|warning\|error\|critical | このパラメータで、すべてのイベントがログに記録される最大（**すべてのデバッグ情報**）から緊急イベントのみ記録される最小（**緊急イベント**）まで、ログの詳細レベルを設定します。<br>このパラメータを指定しない場合、詳細レベル「**すべてのデバッグ情報**」に含まれるすべてのイベントがトレースログに記録されます。 |
| /OFF | このオプションで、トレースログを無効にします。 |

### KAVSHELL TRACE コマンドの例

*詳細レベル「**すべてのデバッグ情報**」を使用してログの最大サイズ 200 MB でトレースログを有効にし、ログファイルを「C:\Trace Folder」フォルダーに保存するには、次のコマンドを実行します：*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

*詳細レベル「**注意が必要なイベント**」を使用してトレースログを有効にし、ログファイルを「C:\Trace Folder」フォルダーに保存するには、次のコマンドを実行します：*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

*トレースログを無効にするには、次のコマンドを実行します：*

```
KAVSHELL TRACE /OFF
```

KAVSHELL TRACE コマンドのリターンコード

## Kaspersky Embedded Systems Security ログファイルのデフラグ：KAVSHELL VACUUM

KAVSHELL VACUUM コマンドを使用すると、アプリケーションのログファイルをデフラグできます。これにより、アプリケーションのイベントを含む大量のログファイルの保管によるシステムエラーおよびアプリケーションエラーを回避することができます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

オンデマンドスキャンおよびアップデートタスクが頻繁に開始される場合、KAVSHELL VACUUM コマンドを適用してログファイル保管領域を最適化してください。このコマンドにより、Kaspersky Embedded Systems Security は、保護対象デバイスの指定したパスに保存されるアプリケーションのログファイルの論理構造を更新します。

既定で、アプリケーションのログファイルは「C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security\3.1\Reports」に保存されます。ログの保管として別のパスを手動で指定した場合、KAVSHELL VACUUM コマンドは、Kaspersky Embedded Systems Security ログ設定で指定したフォルダーにあるファイルのデフラグを実行します。

ファイルサイズが大きいと、KAVSHELL VACUUM コマンドがデフラグ操作を完了するのに必要となる時間が増えます。

リアルタイム保護タスクとコンピューターコントロールタスクは、KAVSHELL VACUUM コマンドの実行中は実行できません。デフラグプロセスにより、Kaspersky Embedded Systems Security ログへのアクセスが制限され、イベントログ記録は行われません。保護の低下を回避するには、KAVSHELL VACUUM コマンドの実行タイミングを計画的に行ってください。

*Kaspersky Embedded Systems Security ログファイルをデフラグするには、次のコマンドを実行します：*

```
KAVSHELL VACUUM
```

このコマンドは、ローカルシステムアカウント権限が必要です。

## iSwift ベースのクリーニング：KAVSHELL FBRESET

Kaspersky Embedded Systems Security では iSwift テクノロジーが使用されており、前回のスキャン以降に変更されていないファイルがスキャンされないようにすることができます（**iSwift を使用する**）。

Kaspersky Embedded Systems Security により、klamfb.dat ファイルと klamfb2.dat ファイルが「%SYSTEMDRIVE%\System Volume Information」フォルダーに作成されます。これらのファイルには、スキャン済みのクリーンなオブジェクトに関する情報が含まれます。klamfb.dat（klamfb2.dat）ファイルのサイズは、スキャン済みのファイル数が増えるにつれて大きくなります。ファイルには、システムに存在するファイルに関する現在の情報のみが含まれます。ファイルが削除されると、klamfb.dat から対応する情報が消去されます。

ファイルをクリアするには、KAVSHELL FBRESET コマンドを使用します。

KAVSHELL FBRESET コマンドを使用する場合は、次の特性にご注意ください：

- KAVSHELL FBRESET コマンドを使用して klamfb.dat ファイルをクリアする時に、Kaspersky Embedded Systems Security は保護を一時停止しません（klamfb.dat を手動で削除した時に起こることとは異なります）。
- klamfb.dat のデータがクリアされると、保護対象デバイスの負荷が増える場合があります。この場合、すべてのファイルに対して、klamfb.dat をクリアした後の最初のアクセス時にスキャンが実行されます。スキャンの後に、スキャン済みの各オブジェクトに関する情報が klamfb.dat に再度追加されます。オブジェクトに新しくアクセスしようとすると、iSwift テクノロジーによって、変更のないファイルは再スキャンされません。

KAVSHELL FBRESET コマンドは、コマンドラインインタープリターが SYSTEM アカウントで開始された場合のみ実行できます。

# ダンプファイル作成の有効化と無効化：KAVSHELL DUMP

KAVSHELL DUMP コマンドを使用して、Kaspersky Embedded Systems Security が異常終了した場合に Kaspersky Embedded Systems Security のプロセスのスナップショット（ダンプファイル）の作成を有効または無効にできます（以下の表を参照）。また、Kaspersky Embedded Systems Security のプロセス実行のダンプファイルはいつでも作成できます。

ダンプファイルを正常に作成するには、KAVSHELL DUMP コマンドをローカルシステムアカウント（SYSTEM）で実行する必要があります。

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。

KAVSHELL DUMP コマンドは、64 ビットのプロセスには使用できません。

## KAVSHELL DUMP コマンドの構文

```
KAVSHELL DUMP </ON /F:<ダンプファイルのフォルダー>|/SNAPSHOT /F:<ダンプファイルのフォルダー> /P:<PID> | /OFF>
```

KAVSHELL DUMP コマンドラインのパラメータとオプション

| ライセンス | 説明 |
|---|---|
| /ON | プロセスが異常終了した場合の、ダンプファイルの作成を有効にします。 |
| /F:<ダンプファイルを保存するフォルダーのパス> | これは必須のパラメータです。このパラメータで、ダンプファイルを保存するフォルダーのパスを指定します。保護対象でない他のデバイスのネットワークドライブ上のフォルダーへのパスは許可されません。<br>ダンプファイルを保存するフォルダー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。 |
| /SNAPSHOT | 指定した PID を持つ実行中のプロセスのメモリのスナップショットを作成し、ダンプファイルを /F パラメータで指定したフォルダーに保存します。 |
| /P | プロセス識別子（PID）が Microsoft Windows タスクマネージャーに表示されます。 |
| /OFF | プロセスが異常終了した場合の、ダンプファイルの作成を無効にします。 |

KAVSHELL DUMP コマンドのリターンコード

## KAVSHELL DUMP コマンドの例

*ダンプファイルの作成を有効にするには、ダンプファイルを C:\Dump Folder フォルダーに保存して、次のコマンドを実行します：*

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

*ID 1234 のプロセスのダンプを「C:/Dumps」フォルダーに作成するには、次のコマンドを実行します：*

```
KAVSHELL DUMP /SNAPSHOT /F:C:\dumps /P:1234
```

*ダンプファイルの生成を無効にするには、次のコマンドを実行します：*

```
KAVSHELL DUMP /OFF
```

# 設定のインポート：KAVSHELL IMPORT

KAVSHELL IMPORT コマンドを使用すると、Kaspersky Embedded Systems Security の設定および現在のタスクを設定ファイルから保護対象デバイスの Kaspersky Embedded Systems Security のコピーにインポートできます。設定ファイルを作成するには、KAVSHELL EXPORT コマンドを使用します。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

## KAVSHELL IMPORT コマンドの構文

```
KAVSHELL IMPORT <設定ファイルの名前とファイルのパス>
```

## KAVSHELL IMPORT コマンドの例

```
KAVSHELL IMPORT Host1.xml
```

KAVSHELL IMPORT コマンドラインパラメータ

| パラメータ | 説明 |
| --- | --- |
| <設定ファイルの名前とファイルのパス> | 設定のインポート元として使用する設定ファイルの名前。<br>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。 |

KAVSHELL IMPORT コマンドのリターンコード

# 設定のエクスポート：KAVSHELL EXPORT

KAVSHELL EXPORT コマンドを使用すると、他の保護対象デバイスにインストールされた Kaspersky Embedded Systems Security のコピーに後でインポートするために、Kaspersky Embedded Systems Security のすべての設定と現在のタスクを設定ファイルにエクスポートできます。

## KAVSHELL EXPORT コマンドの構文

```
KAVSHELL EXPORT <設定ファイルの名前とファイルのパス>
```

### KAVSHELL EXPORT コマンドの例

```
KAVSHELL EXPORT Host1.xml
```

KAVSHELL EXPORT コマンドラインパラメータ

| パラメータ | 説明 |
| --- | --- |
| <設定ファイルの名前とファイルのパス> | 設定が含まれる設定ファイルの名前。<br>設定ファイルに任意のファイル拡張子を割り当てることができます。<br>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。 |

KAVSHELL EXPORT コマンドのリターンコード

## Microsoft Operations Management Suite との統合：KAVSHELL OMSINFO

KAVSHELL OMSINFO コマンドを使用すると、製品のステータスや、定義データベースおよび KSN サービスによって検知された脅威に関する情報を確認できます。脅威に関する情報は、使用可能なイベントログから取得されます。

### KAVSHELL OMSINFO コマンドの構文

```
KAVSHELL OMSINFO <生成されるファイルの完全パスとファイル名>
```

### KAVSHELL OMSINFO コマンドの例

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

KAVSHELL OMSINFO コマンドラインパラメータ

| パラメータ | 説明 |
| --- | --- |
| <生成されるファイルのパスとファイル名> | 製品のステータスと検知された脅威に関する情報が含まれる、生成されるファイルの名前。 |

## ベースラインに基づくファイル変更監視タスクの管理：KAVSHELL FIM /BASELINE

KAVSHELL FIM /BASELINE コマンドを使用して、アプリケーション起動コントロールタスクが DLL モジュールの読み込みを実行、監視するモードを設定できます。

コマンドの実行にパスワードが必要になることがあります。現在のパスワードを入力するには、[/pwd:<パスワード>] を使用します。

### KAVSHELL FIM /BASELINE コマンドの構文

KAVSHELL FIM /BASELINE [/CREATE: [<監視範囲> | /L:<監視範囲のリストを含む TXT ファイルへのパス>] [/MD5 | /SHA256] [/SF]] | [/CLEAR [/BL:<ベースライン ID> | /ALIAS:<既存のエイリアス>]] | [/EXPORT:<TXT ファイルへのパス> [/BL:<ベースライン ID> | /ALIAS:<既存のエイリアス>]] | [/SHOW [/BL:<ベースライン ID> | /ALIAS:<既存のエイリアス>]] | [/SCAN [/BL:<ベースライン ID> | /ALIAS:<既存のエイリアス>]] | [/PWD:<パスワード>]

## KAVSHELL FIM /BASELINE コマンドの例

*ベースラインを削除するには、次のコマンドを実行します：*

```
KAVSHELL FIM /BASELINE /CLEAR /BL:<ベースライン ID>
```

コマンドラインのパラメータを使用して、ベースラインファイル変更監視タスク設定を設定できます（次の表を参照）。

KAVSHELL FIM/ BASELINE コマンドラインのパラメータとオプション

| パラメータとオプション | 説明 |
|---|---|
| /CREATE | 新しいベースラインに基づくファイル変更監視タスクを作成します。<br><br>ベースラインを作成するため、Kaspersky Embedded Systems Security によって新しいベースラインに基づくファイル変更監視タスクが開始されます。 |
| /L | 監視領域のリストを含む TXT ファイルへのパスを指定します。 |
| /MD5 | チェックサムを計算するための MD5 アルゴリズムを指定します（オプションのパラメータ）。<br>/MD5 パラメータを /SHA256 と一緒に使用することはできません。<br>既定では、MD5 アルゴリズムが使用されています。 |
| /SHA256 | チェックサムを計算するための SHA256 アルゴリズムを指定します（オプションのパラメータ）。<br>/SHA256 パラメータを /MD5 と一緒に使用することはできません。<br>既定では、MD5 アルゴリズムが使用されています。 |
| /SF | ベースラインに基づくファイル変更監視タスクの範囲のすべてのサブフォルダーが含まれます（オプションのパラメータ）。<br>既定では、すべてのサブフォルダーがベースラインに基づくファイル変更監視タスクの範囲から除外されます。 |
| /CLEAR | 指定された <ベースライン ID> を持つベースライン、または指定された <既存のエイリアス> を持つタスクのベースラインを削除します。<br><ベースライン ID> または <既存のエイリアス> のいずれも指定されていない場合は、すべてのベースラインを削除します。<br>オプションのパラメータ。 |
| /BL | ベースラインの一意の ID を指定します（オプションのパラメータ）。 |
| /EXPORT | TXT ファイルのすべてのベースラインに関するデータをエクスポートします。 |
| /SHOW | すべてのベースライン関するデータを表示します。 |
| /SCAN | 指定された <ベースライン ID> または指定された <既存のエイリアス> を持つ新しいベースラインに基づくファイル変更監視タスクを開始します。 |
| /ALIAS | 既存のタスクの名前、または新しいタスクの名前を指定します。 |

| | |
|---|---|
| <監視範囲> | ベースラインに基づくファイル変更監視タスクの範囲に含めるファイルまたはフォルダーを指定します。<br><br>このパラメータにより、1つの領域のみを指定できます。 |
| <監視領域のリストを含む TXT ファイルへのパス> | 監視領域のリストを含む TXT ファイルへのパスを指定します。<br>ファイルは UTF-8 でエンコードされ、監視領域へのそれぞれのパスは別の行で指定する必要があります。 |
| <TXT ファイルのパス> | すべてのベースラインに関するデータのエクスポート先となるファイルのパスを指定します。 |
| <ベースライン ID> | ベースラインの一意の ID を指定します。<br>/SHOW パラメータを使用して、ベースラインの ID を学習できます。 |
| <既存のエイリアス> | 既存のタスクの名前を指定します。 |
| <新しいエイリアス> | 新しいタスクの名前を指定します。 |

# コマンドのリターンコード

## KAVSHELL START および KAVSHELL STOP コマンドのリターンコード

KAVSHELL START および KAVSHELL STOP コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -3 | 権限エラー |
| -5 | コマンド構文が無効である |
| -6 | 操作が無効である（Kaspersky Security サービスが既に実行されている、既に停止されているなど） |
| -7 | サービスが登録されていない |
| -8 | サービスの自動スタートアップが無効 |
| -9 | 別のユーザーアカウントでの保護対象デバイスの起動に失敗した（既定では、Kaspersky Security サービスはローカルシステムユーザーアカウントで実行されます） |
| -99 | 不明なエラー |

## KAVSHELL SCAN および KAVSHELL SCANCRITICAL コマンドのリターンコード

KAVSHELL SCAN および KAVSHELL SCANCRITICAL コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した（脅威が検知されなかった） |

| | |
|---|---|
| 1 | 操作がキャンセルされた |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -4 | オブジェクトが見つからない（スキャン範囲のリストを含むファイルが見つからない） |
| -5 | コマンド構文が無効であるか、スキャン範囲が定義されていない |
| -80 | 感染などの問題があるオブジェクトの検知 |
| -81 | 感染の可能性があるオブジェクトの検知 |
| -82 | 処理エラーが検知された |
| -83 | スキャンされていないオブジェクトが検知された |
| -84 | 破損したオブジェクトが検知された |
| -85 | タスク実行ログの作成に失敗した |
| -99 | 不明なエラー |
| -301 | ライセンスが無効である |

## KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード

KAVSHELL TASK LOG-INSPECTOR コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -6 | 操作が無効である（Kaspersky Security サービスが既に実行されている、既に停止されているなど） |
| 402 | タスクが既に実行されている（/STATE オプションの場合） |

## KAVSHELL TASK コマンドのリターンコード

KAVSHELL TASK コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -4 | オブジェクトが見つからない（タスクが見つからない） |
| -5 | コマンド構文が無効である |
| -6 | 操作が無効である（タスクが実行されていない、既に実行されている、一時停止できないなど） |
| -99 | 不明なエラー |

| | |
|---|---|
| -301 | ライセンスが無効である |
| 401 | タスクが実行されていない（/STATE オプションの場合） |
| 402 | タスクが既に実行されている（/STATE オプションの場合） |
| 403 | タスクが既に一時停止されている（/STATE オプションの場合） |
| -404 | 操作に失敗した（タスクステータスの変更によりクラッシュした） |

## KAVSHELL RTP コマンドのリターンコード

KAVSHELL RTP コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -4 | オブジェクトが見つからない（1つまたはすべてのコンピューターのリアルタイム保護が見つからない） |
| -5 | コマンド構文が無効である |
| -6 | 操作が無効である（タスクが既に実行されている、既に停止されているなど） |
| -99 | 不明なエラー |
| -301 | ライセンスが無効である |

## KAVSHELL UPDATE コマンドのリターンコード

KAVSHELL UPDATE コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| 200 | すべてのオブジェクトが最新である（定義データベースまたはプログラムのコンポーネントが最新である） |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -5 | コマンド構文が無効である |
| -99 | 不明なエラー |
| -206 | 拡張ファイルが指定されたアップデート元にないか、不明な形式である |
| -209 | アップデート元への接続エラー |
| -232 | プロキシサーバーへの接続時の認証エラー |
| -234 | Kaspersky Security Center への接続エラー |
| -235 | アップデート元への接続時に Kaspersky Embedded Systems Security が認証されなかった |

| | |
|---|---|
| -236 | 定義データベースが破損した |
| -301 | ライセンスが無効である |

## KAVSHELL ROLLBACK コマンドのリターンコード

KAVSHELL ROLLBACK コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -99 | 不明なエラー |
| -221 | 定義データベースのバックアップコピーが見つからないか、破損している |
| -222 | 定義データベースのバックアップコピーが破損している |

## KAVSHELL LICENSE コマンドのリターンコード

KAVSHELL LICENSE コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | ライセンスを管理する権限が不十分である |
| -4 | 指定した番号のライセンスが見つからない |
| -5 | コマンド構文が無効である |
| -6 | 操作が無効である（ライセンスが既に追加されている） |
| -99 | 不明なエラー |
| -301 | ライセンスが無効である |
| -303 | 別のアプリケーション用のライセンスである |

## KAVSHELL TRACE コマンドのリターンコード

KAVSHELL TRACE コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -4 | オブジェクトが見つからない（トレースログフォルダーに指定されたパスが見つからな |

| | |
|---|---|
| | い） |
| -5 | コマンド構文が無効である |
| -6 | 操作が無効である（トレースログが既に無効になっている時に KAVSHELL TRACE /OFF コマンドの実行が試行された） |
| -99 | 不明なエラー |

## KAVSHELL FBRESET コマンドのリターンコード

KAVSHELL FBRESET コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -99 | 不明なエラー |

## KAVSHELL DUMP コマンドのリターンコード

KAVSHELL DUMP コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -4 | オブジェクトが見つからない（ダンプファイルフォルダーに指定されたパスが見つからない、指定した PID のプロセスが見つからない） |
| -5 | コマンド構文が無効である |
| -6 | 操作が無効である（ダンプファイルの作成が既に無効化されている場合に KAVSHELL DUMP/OFF コマンドの実行が試みられた） |
| -99 | 不明なエラー |

## KAVSHELL IMPORT コマンドのリターンコード

KAVSHELL IMPORT コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -4 | オブジェクトが見つからない（インポートできる設定ファイルが見つからない） |
| -5 | 構文が無効である |

| | |
|---|---|
| -99 | 不明なエラー |
| 501 | 操作は正常に完了したが、エラー / コメントが発生した（たとえば、いくつかの機能コンポーネントのパラメータがインポートされなかった） |
| -502 | インポート対象のファイルがないか、認識できない形式である |
| -503 | 設定に互換性がない（異なるプログラムまたは互換性のない Kaspersky Embedded Systems Security 上位バージョンからエクスポートされた設定ファイル） |

## KAVSHELL EXPORT コマンドのリターンコード

KAVSHELL EXPORT コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -5 | 構文が無効である |
| -10 | 設定ファイルを作成できない（たとえば、ファイルパスで指定されたフォルダーにアクセスできない） |
| -99 | 不明なエラー |
| 501 | 操作は正常に完了したが、エラー / コメントが発生した（たとえば、いくつかの機能コンポーネントのパラメータがエクスポートされなかった） |

## KAVSHELL FIM /BASELINE コマンドのリターンコード

KAVSHELL FIM /BASELINE コマンドのリターンコード

| リターンコード | 説明 |
|---|---|
| 0 | 操作が正常に完了した |
| -2 | サービスが実行されていない |
| -3 | 権限エラー |
| -4 | オブジェクトが見つからない（タスクが見つからない） |
| -5 | コマンド構文が無効である |
| -6 | 操作が無効である（例：ベースラインがすでに削除されている） |
| -10 | 設定ファイルを作成できない（たとえば、ファイルパスで指定されたフォルダーにアクセスできない） |
| -12 | パスワードが無効である |
| -80 | 検知されたベースラインオブジェクトとの不一致 |
| -85 | タスク実行ログの作成に失敗した |
| -99 | 内部エラー |

| | |
|---|---|
| -303 | 無効なライセンス |
| -502 | タスクが実行されていない |
| 200 | すべてのオブジェクトがベースラインと一致 |
| 501 | タスクは正常に完了したが、エラー / コメントが発生した |

# 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

製品のガイドや製品に関する情報源で問題の解決法が見つからない場合は、テクニカルサポートにお問い合わせください。テクニカルサポートの担当者が、製品のインストール方法または使用方法についての質問に答えます。

テクニカルサポートは、製品版ライセンスを購入したお客様のみが利用できます。試用版のお客様は、テクニカルサポートを利用できません。

製品のサポートは、アプリケーションライフサイクルに従って提供されます（アプリケーションライフサイクルのページを参照）。

テクニカルサポートにご連絡いただく前に、「サポートサービス規約」をお読みください。

カスペルスキーカンパニーアカウントポータルを使用してリクエストを送信することで、カスペルスキーのテクニカルサポートにお問い合わせいただくことが可能です。

## 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。

## トレースファイルと AVZ スクリプトの使用

カスペルスキーの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。また、トレースファイルの作成をお願いする場合もあります。トレースファイルによって、アプリケーションコマンドの実行プロセスを段階ごとに追跡し、どの操作段階でエラーが発生したかを特定できます。

カスペルスキーの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、保護対象デバイスの脅威のスキャン、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。

# 用語解説

## Kaspersky Security Network（KSN）

カスペルスキーのデータベースへのアクセスを提供するクラウドサービスのインフラストラクチャ。ファイル、Web リソース、ソフトウェアの評価に関する情報が絶えず更新されています。Kaspersky Security Network により、カスペルスキー製品は新しい脅威に迅速に対応でき、保護コンポーネントのパフォーマンスを改善し、誤検知の可能性を低下させます。

## OLE 埋め込みオブジェクト

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

各種ネットワークデバイスおよびアプリケーションから開始されるセキュリティイベントを分析する技術。

## 圧縮ファイル

圧縮によって1つまたは複数のファイルを単一のファイルにパッケージ化したもの。データの圧縮と展開には、アーカイバーと呼ばれる専用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製品モジュール）を差し替えまたは追加する処理。

## イベントの重要度

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。次の重要度があります：

- 緊急イベント
- 機能エラー
- 警告
- 情報

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

そのコードの一部が既知の悪意のあるソフトウェアのコードの一部と完全に一致するオブジェクト。そのようなオブジェクトにはアクセスしないでください。

## 感染の可能性があるファイル

その構造や形式のため、悪意のあるコードを保管し拡散するための「容器」として犯罪者に使用される可能性のあるファイル。通常、これらは実行ファイルであり、.com、.exe、.dll のようなファイル拡張子を持ちます。このようなファイルは、悪意のあるコードが侵入するリスクが極めて高くなります。

## 管理サーバー

Kaspersky Security Center の機能の 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ます。これらのカスペルスキー製品の管理にも使用できます。

## 駆除

感染したオブジェクトの処理方法のひとつ。データを完全に復元または一部復元します。感染したすべてのオブジェクトを駆除できるわけではありません。

## 現在のライセンス

本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侵入するウイルスは、オペレーティングシステム自体とインストール済みアプリケーションで障害を発生させるので、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、オペレーティングシステムが信頼できないものになります。

## セキュリティレベル

セキュリティレベルは、製品コンポーネント設定を事前に構成したセットとして定義されます。

## タスク

カスペルスキー製品によって実行される機能は、タスクとして実装されています。例：ファイルのリアルタイム保護、コンピューターの完全スキャン、定義データベースのアップデート。

## タスクの設定

各タスク種別に対して固有の製品設定。

## 定義データベース

定義データベースの公開日時点でのセキュリティ上の既知の脅威に関する情報が含まれるデータベース。定義データベースのエントリーによって、スキャン対象のオブジェクトに含まれる悪意のあるコードを検知できます。定義データベースは、カスペルスキーによって作成され、1時間ごとにアップデートされます。

## バックアップ

ファイルのバックアップコピーのための特別な保管領域。駆除または削除が試行される前に作成されます。

## 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

ワイルドカードを使用したファイル名の表示。ファイル名マスクで使用される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。コンピューターセキュリティのレベルを反映します。

## 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

製品機能へのアクセスとその他のサービスを使用する権利を持つ期間。使用できるサービスはライセンスの種別により異なります。

## ローカルタスク

単一のクライアントコンピューターで定義され、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

サードパーティ製のコードに関する情報は、アプリケーションのインストールフォルダーにある legal_notices.txt という名前のファイルに入っています。

# 商標に関する通知

登録商標およびサービスマークは、それぞれの所有者に属しています。

CVE は MITRE Corporation の登録商標です。

Core、Intel、Pentium は、米国およびその他の国における Intel Corporation の商標です。

Linux は、米国およびその他の国における Linus Torvalds の登録商標です。

Microsoft、Active Directory、Excel、Internet Explorer、Outlook、Windows、Windows Server、Windows Vista は、米国およびその他の国における Microsoft Corporation 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。