Kaspersky Endpoint Security for Windows Ver 12

2023年09月05日

株式会社カスペルスキー
セールスエンジニアリング本部

Kaspersky Endpoint Security for Windows
概要

Kaspersky Endpoint Security for Windows 12の特徴

先進的かつ高度な保護機能を持ち、多層で防御を行う。

ふるまい検知(2006年から搭載)、機械学習エンジン(2012年から搭載)
脆弱性攻撃ブロック、ホスト侵入防止
AMSI 保護プロバイダー、アダプティブアノマリコントロール（Advancedのみ）

Big Dataの活用

Kaspersky Security Network
エキスパートによる分析、機械学習アルゴリズムとビッグデータ

デバイスコントロールなど制御機能を標準装備

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（デフォルト拒否モード）
ウェブコンテンツフィルタリング、バナー広告ブロック

サーバーに特化したセキュリティ機能

イベントログ監視（KHCS サーバーのみ）
ファイル変更監視（KHCS サーバーのみ）
再起動なしのバージョンアップ

Kaspersky Endpoint Security for Windows 12 を使用可能な製品

Kaspersky Endpoint Security for Windowsはアプリケーションの名称であり、
使用する権利のある製品（ライセンス）は以下の通り。

Kaspersky Endpoint Security for Business Select、Advanced
Kaspersky Endpoint Detection and Response Optimum Bundle　*Add-onではない
Kaspersky Endpoint Detection and Response Expert
Kaspersky Hybrid Cloud Security

Kaspersky Endpoint Security Cloud

Kaspersky Endpoint Security for Windows 12 管理形態

Kaspersky Endpoint Security for Windowsは、以下の形態で使用が可能。

オンプレミス版管理サーバー Kaspersky Security Centerによる管理
クラウド管理サーバー Kaspersky Security Center Cloud Consoleによる管理（ライセンス数による条件有り）
スタンドアロン
KES Cloud購入時は、クラウドによる管理

Kaspersky Managed Detection and Response の対象として運用可能。

Kaspersky Endpoint Security for Business SelectとAdvanced

Kaspersky Hybrid Cloud Security

保護機能比較表

kaspersky

機能	Kaspersky Endpoint Security for Business			
	Select		Advanced	
	クライアントOS	サーバーOS	クライアントOS	サーバーOS
Kaspersky Security Network（KSN）	●	●	●	●
ふるまい検知	●	●	●	●
脆弱性攻撃ブロック	●	●	●	●
ホスト侵入防止	●	—	●	—
修復エンジン（ロールバック）	●	●	●	●
ファイル脅威対策	●	●	●	●
ウェブ脅威対策	●	—	●	●
メール脅威対策	●	—	●	●
ネットワーク脅威対策	●	●	●	●
ファイアウォール	●	●	●	●
有害USB攻撃ブロック	●	●	●	●
暗号化された接続のスキャン	●	●	●	●
アプリケーションコントロール	●	—	●	●
デバイスコントロール	●	—	●	●
ウェブコントロール	●	—	●	●
AMSI 保護プロバイダー	●	●	●	●
アダプティブアノマリーコントロール	—	—	●	—
ディスク全体の暗号化（Kaspersky独自）	—	—	●	—
ディスク全体の暗号化（BitLocker）	—	—	●	●
ファイルレベルの暗号化	—	—	●	—
Windowsイベントログ監視	—	—	—	—
ファイル変更監視	—	—	—	—
脆弱性管理（パッチ自動配信）	—	—	●	●

Kaspersky Endpoint Security for Windows 12 の機能

Windows10以降、
Windows Server2016以降

kaspersky

機能	Kaspersky Hybrid Cloud Security					
	Desktop Standard	Desktop Enterprise	Server Standard	Server Enterprise	CPU Standard	CPU Enterprise
	クライアントOS	クライアントOS	サーバーOS	サーバーOS	サーバーOS	サーバーOS
Kaspersky Security Network（KSN）	●	●	●	●	●	●
ふるまい検知	●	●	●	●	●	●
脆弱性攻撃ブロック	●	●	●	●	●	●
ホスト侵入防止	●	●	—	—	—	—
修復エンジン（ロールバック）	●	●	●	●	●	●
ファイル脅威対策	●	●	●	●	●	●
ウェブ脅威対策	●	●	●	●	●	●
メール脅威対策	●	●	●	●	●	●
ネットワーク脅威対策	●	●	●	●	●	●
ファイアウォール	●	●	●	●	●	●
有害USB攻撃ブロック	●	●	●	●	●	●
暗号化された接続のスキャン	●	●	●	●	●	●
アプリケーションコントロール	●	●	●	●	●	●
デバイスコントロール	●	●	●	●	●	●
ウェブコントロール	●	●	●	●	●	●
AMSI 保護プロバイダー	●	●	●	●	●	●
アダプティブアノマリーコントロール	—	●	—	—	—	—
ディスク全体の暗号化（Kaspersky独自）	—	●	—	—	—	—
ディスク全体の暗号化（BitLocker）	—	●	—	●	—	●
ファイルレベルの暗号化	—	●	—	—	—	—
Windowsイベントログ監視	—	—	—	●	—	●
ファイル変更監視	—	—	—	●	—	●

← Windows10以降、Windows Server2016以降

kaspersky

Kaspersky Endpoint Security for Windows
機能詳細

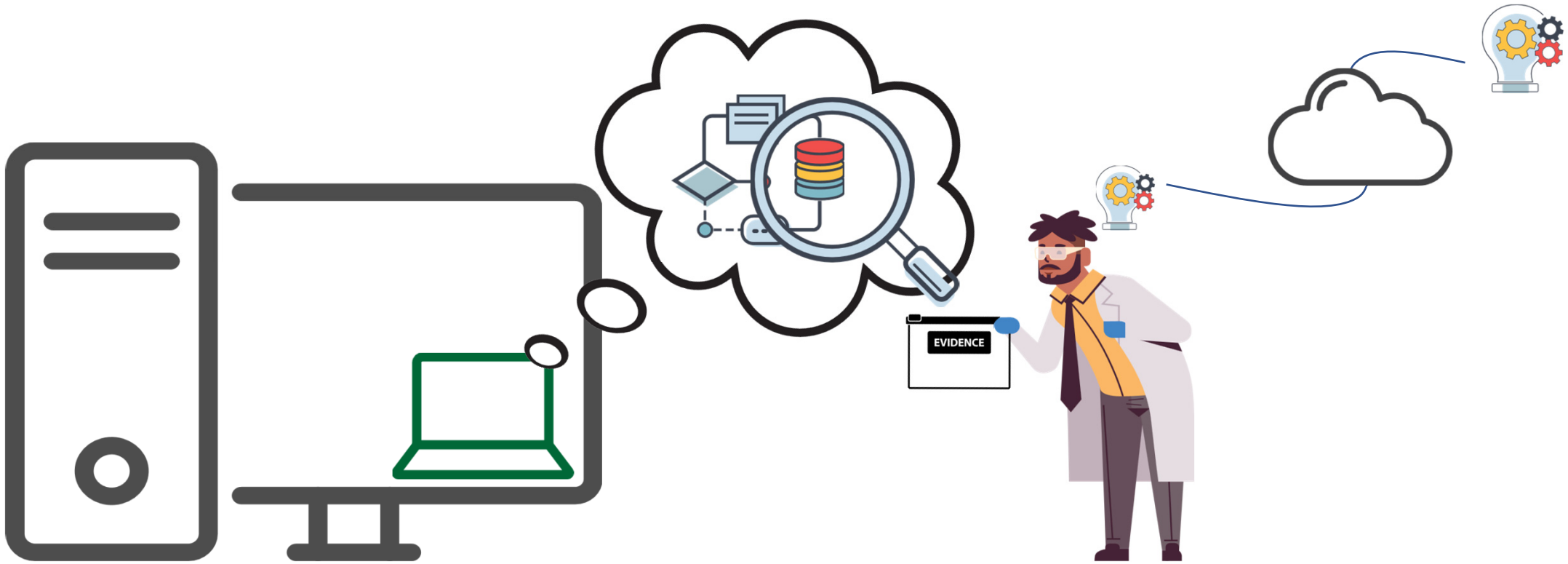
先進のセキュリティ機能

kaspersky

ファイル脅威対策：ヒューリスティック

仮想環境を立ち上げ、プログラムを実行。
ログを解析し、未知の脅威を検知する技術。
いわゆるサンドボックス技術。

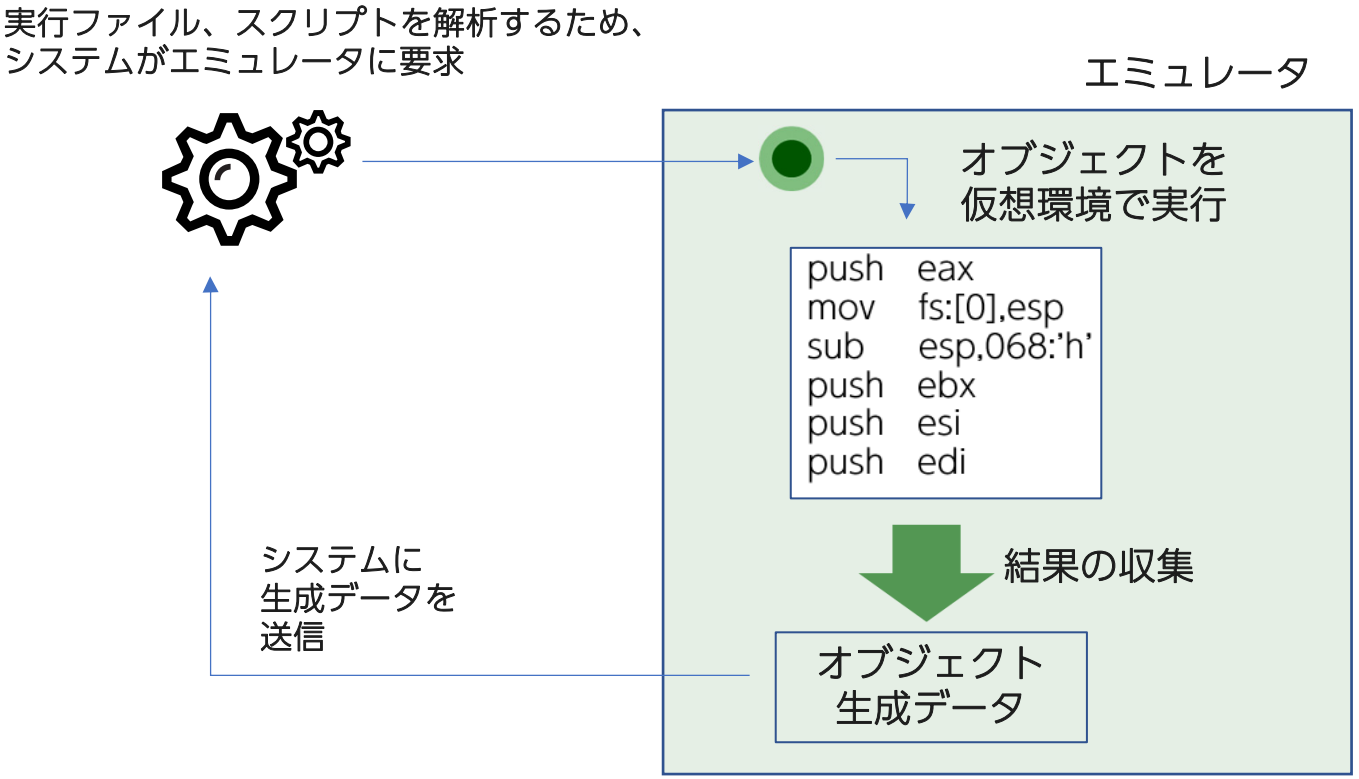
検知に必要な情報は
カスペルスキーから更新される



ファイル脅威対策：ヒューリスティック

未知の脅威を検知する技術

- *.exe, *.dll, *.sysなどの、Windows実行ファイルを実行。
- JavaScript、VBScript、 AutoITなどのファイルとしてダウンロード出来るスタンドアロンのスクリプトを処理。
- ウェブページやメールに埋め込まれたウェブリンク、PDF、MS Office ファイルに埋め込まれたスクリプトを実行。



エミュレータの更新

エミュレーション技術は、エミュレーションコアと検知レコードにより構成される。

検知レコードはコアにより提供されるデータを解析する。

検知レコードはカスペルスキーにより作成され、毎時ダウンロードされる。

ひとつの検知レコードは、同じふるまいを持つ数多くの異なるマルウェアを検討することができる。

エミュレータにより収集されるデータ

実行ファイルの一例:
- API call log
- 全てのファイルシステム、レジストリの変更
- メモリーダンプ

スクリプトの一例:
- Arguments と、文字列操作の戻り値
- 組み込み関数と環境によって提供される関数のCall
- イベント
- ファイルシステムへのドロップと子スクリプト

機械学習エンジン　機械学習モデル

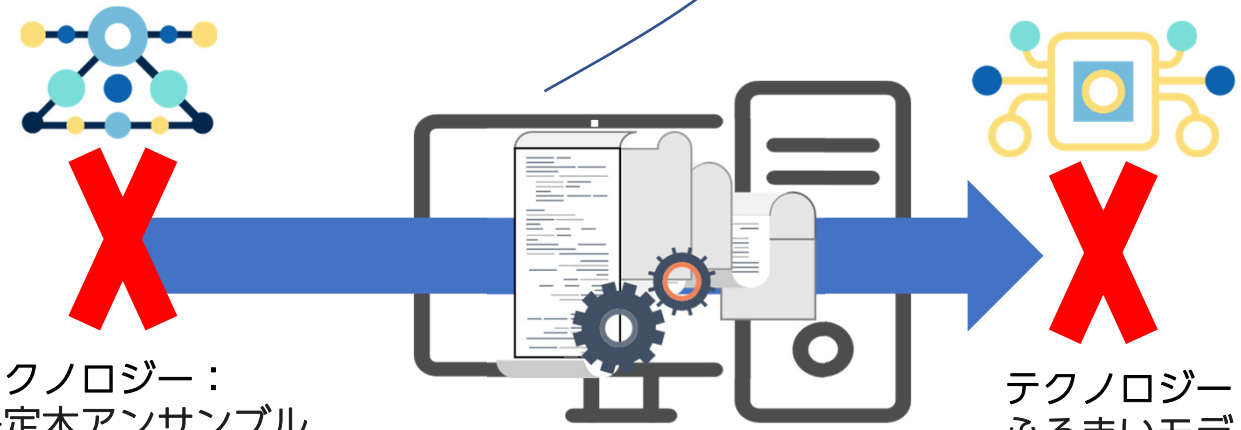
クラウド上

テクノロジー：
受信ストリームのクラスタリング、Astraea

ユーザーのコンピューターで動作

未知のプログラム実行前の
プロアクティブな保護段階で有効

未知のプログラム実行後の
プロアクティブな保護段階で有効



テクノロジー：
決定木アンサンブル、
局所性鋭敏型ハッシュ など

テクノロジー：
ふるまいモデル

教師あり学習　ユーザーのコンピューターで動作

未知のオブジェクト特徴セットX'から、正しいラベルY'を出力する式
ラベルXはコンテンツやふるまいを表す何らかの特徴(ファイル、統計、使用されたAPI関数のリストなど)、
ラベルYは「マルウェア」や「無害」(ウイルス、Trojan-Downloader、アドウェア)

[X1, X2, X3, ….]　－＞　Y

テクノロジー：未知のプログラム実行前のプロアクティブな保護段階で有効
決定木アンサンブル、局所性鋭敏型ハッシュ など

テクノロジー：未知のプログラム実行後のプロアクティブな保護段階で有効
ふるまいモデル

教師なし学習　クラウド上

データの隠れた構造を明らかにする
類似するオブジェクトや相関性の高い特徴をグループ化

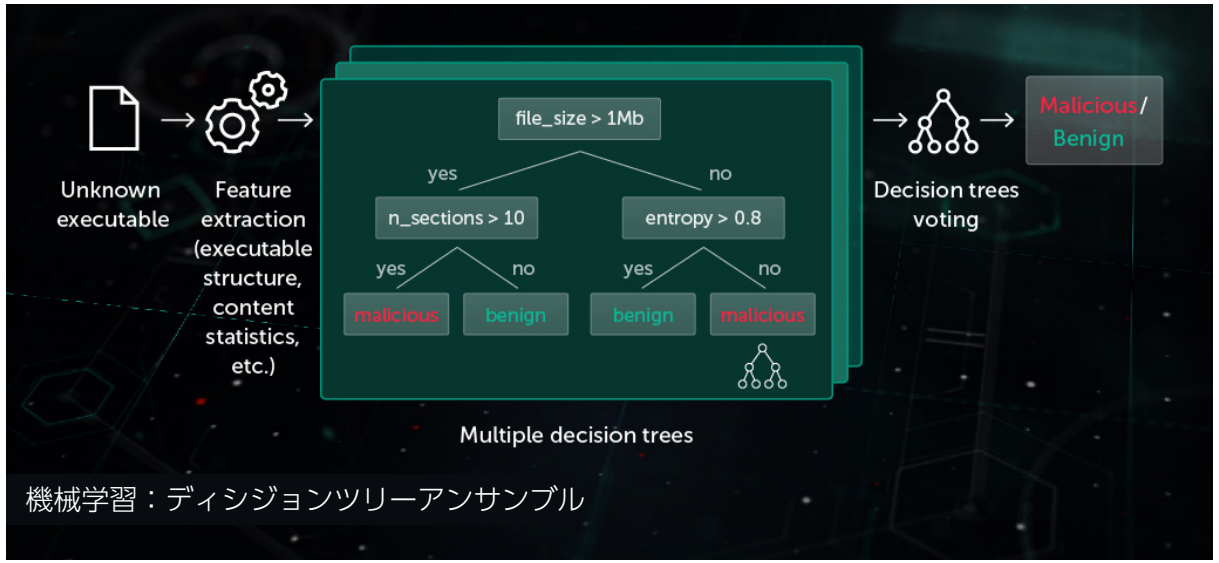
テクノロジー：受信ストリームのクラスタリング、Astraea

ユーザーコンピューターで動作する機械学習モデル

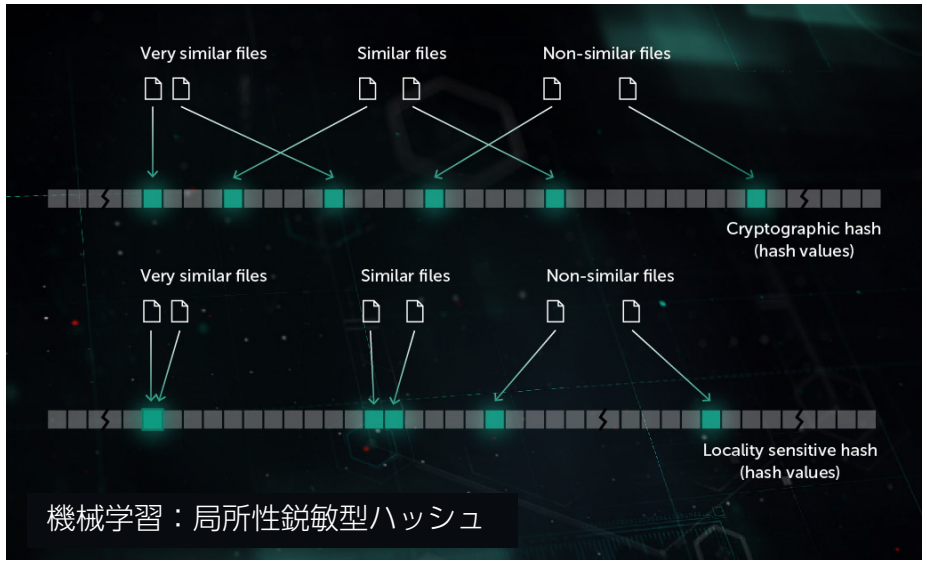
未知のプログラム実行前のプロアクティブな保護段階においてメリット

決定木アンサンブル：
各ノードの質問にオブジェクトの特徴を回答しながら、ツリーを横断。
複数のツリーの判定がアルゴリズム固有の方法で平均化され、オブジェクトに関する最終判定がなされる。

局所性鋭敏型ハッシュ：
ファイルの特徴を抽出し、直交射影学習を使用して、最も重要な特徴を選択



機械学習：ディシジョンツリーアンサンブル

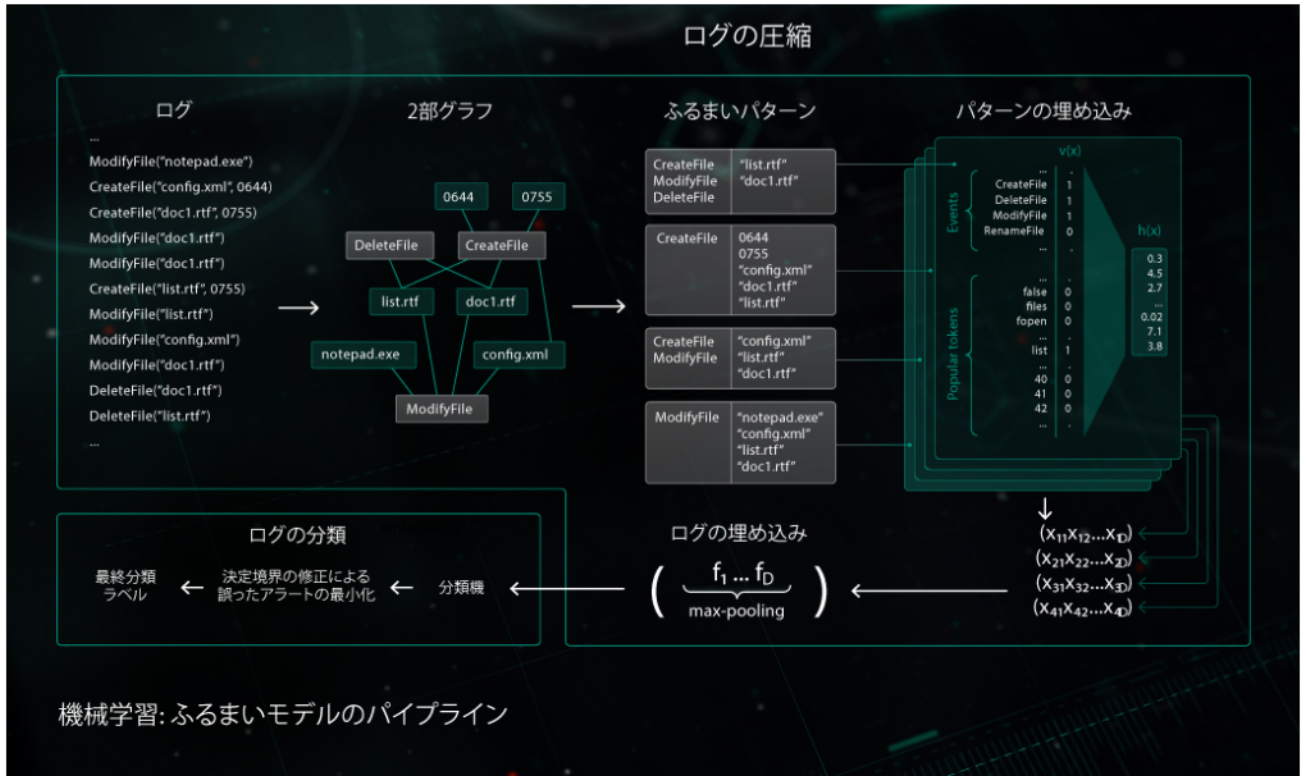


機械学習：局所性鋭敏型ハッシュ

ユーザーコンピューターで動作する機械学習モデル

未知のプログラム実行後のプロアクティブな保護段階においてメリット

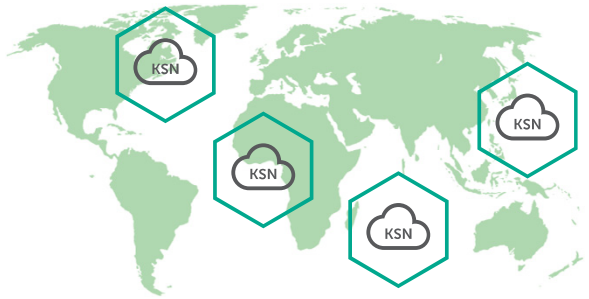
ふるまいモデル：
コンポーネント(ソフトウェア)の監視によってふるまいログを提供。
ふるまいログは、プロセス実行中に発生した一連のシステムイベントと、対応する引数。
観察されたログデータ内の悪意のあるアクティビティを検知



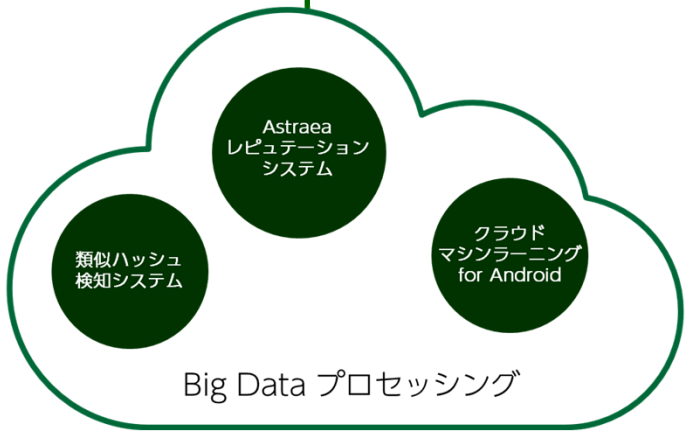
Kaspersky Security Network（KSN）

カスペルスキー製品を利用している数百万のお客様の同意を得た上でサイバーセキュリティ関連情報を収集。
収集された情報をインテリジェントに処理する専用の分散型インフラストラクチャ。
これらのデータをクラウド上で自動的に分析し、新しい未知のサイバー脅威に対して最速で対処。
Kaspersky Labの次世代の多層防御アプローチの最も重要なコンポーネントの1つ。

- 高度で未知のマルウェアの検知
- 検知エラー（誤検知）の低減
- 新たな脅威への応答時間を大幅に短縮。



KSNに接続されたクライアント



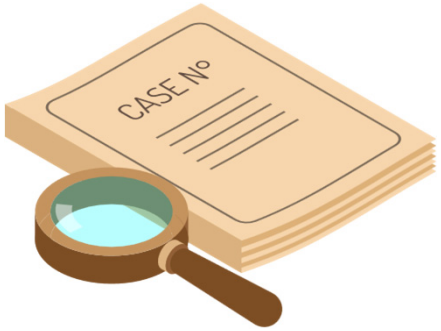
カスペルスキー
エキスパート

500TB以上の処理情報が
保存されているストレージ

kaspersky

ふるまい検知

表面上では悪意を判断出来ない未知のプログラムを、
リアルタイムに分析し、その悪意のある性質を明らかにする。



既知の情報だけでは
新しい脅威に対応出来ない。

表層では分からない真の姿を
解析する。

課題

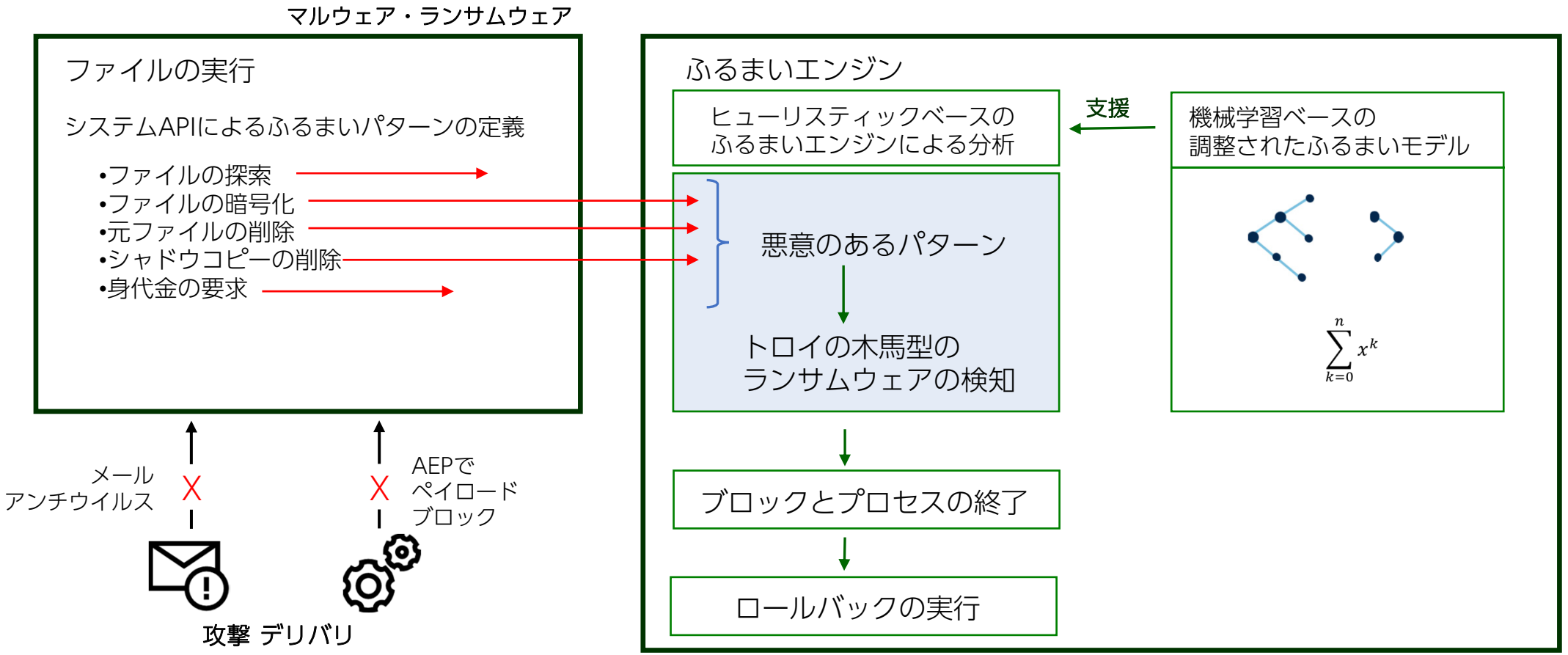
アンチエミュレーション機能を搭載した、カスタムメイドのパッカーによって圧縮された
ファイルの実行前には、ファイルをスキャンしようとしても検知は成功しない。

ふるまい検知による解決

実際のプロセスアクティビティを実行段階でリアルタイムに分析し、
その悪意のある性質を明らかにする。

- カスペルスキーの新しいふるまい検知エンジンの保護機能
  - ✓ ふるまい検知
  - ✓ 脆弱性攻撃ブロック(Automatic Exploit Prevention)
  - ✓ 修復エンジン
  - ✓ アンチロッカー（不正な画面ロックを防止）
  - ✓ 共有フォルダに対して、外部からの悪意のあるファイル操作を監視・ブロック。
- メモリ保護メカニズムを実装。
  lsass.exe のようなシステムの重要なプロセスを保護。
- ふるまいヒューリスティック記録の他に 機械学習も活用し、
  未知の悪意のある行動パターンを検知。

ふるまい検知



ふるまいヒューリスティックモデルと機械学習ベースモデルを搭載したふるまい検知エンジンを実行することで、パッカーやアンチエミュレーションの技法が使用されていても、検知が可能。

機械学習モデルには、さまざまなソースから収集されたシステムイベントが提供される。機械学習モデルは、処理の後に、分析したパターンが悪意のあるものかどうかを判定する。
たとえ悪意があると判定されなくても、機械学習モデルが生成した結果はふるまいヒューリスティックで使用され、検知に活用される。

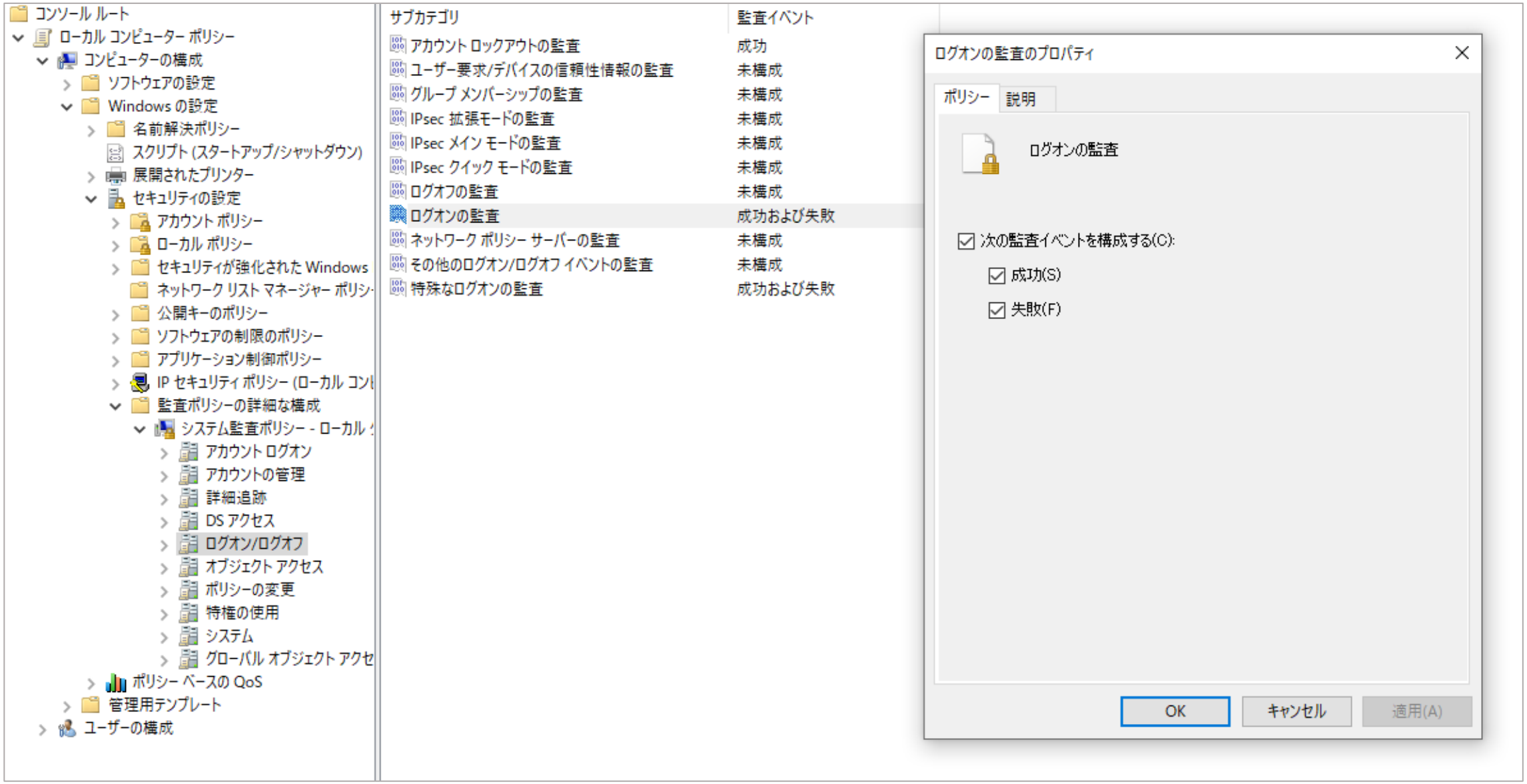
ふるまい検知：共有フォルダへの暗号化ブロック

攻撃者（ランサムウェア）がネットワーク共有越しに
データを暗号化する試みをブロック。

ランサムウェアが動作している端末ではなく、
データ側でブロックする技術。

この機能を有効にするには、Windowsセキュリティポリシーで
ログオンの監査を有効にする必要があります。
既定では、ログオンの監査は無効です。

ふるまい検知：共有フォルダへの暗号化ブロック



kaspersky

修復エンジンによるロールバック

Kaspersky Endpoint Security
ふるまい検知エンジン

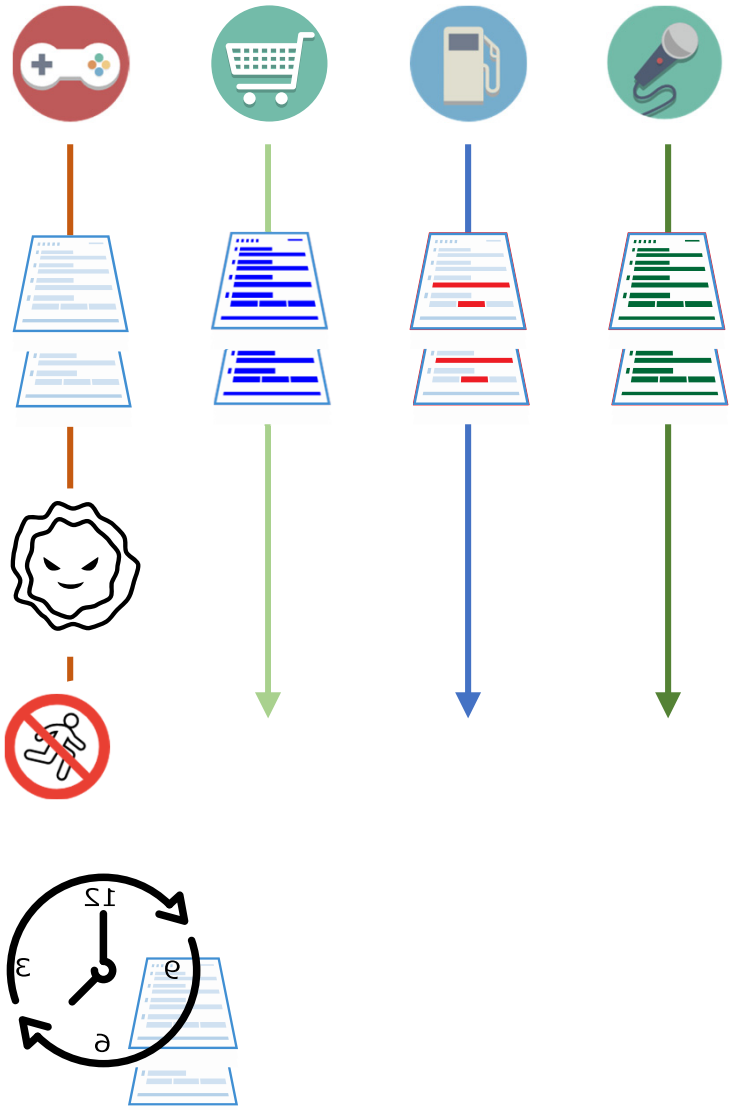
ファイル・レジストリ操作を
ログに記録

悪意あるふるまいを検知

プロセス停止

修復エンジン

ログに基づいて
ファイルレジストリ操作を
ロールバック



プログラム起動

ファイル・レジストリ操作

悪い挙動を始めるまでは、
マルウェアかどうか分からない。

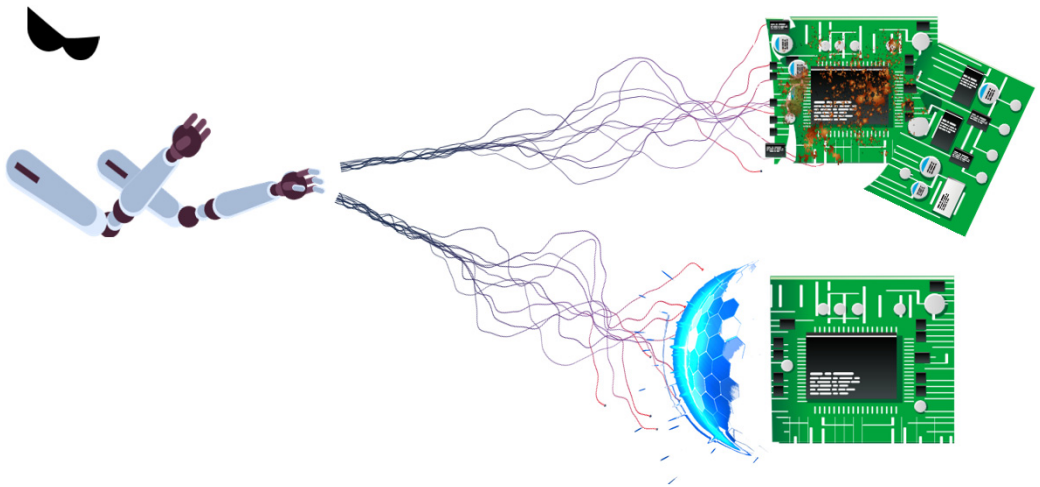
全てのアプリケーションの動作を記録しておき、悪意あるふるまいを検知したら、プロセスを停止。ファイル操作、レジストリ操作をロールバックする。

脆弱性攻撃ブロック(Automatic Exploit Prevention : AEP)

脆弱性攻撃ブロックは、カスペルスキーのふるまいベース検知の不可欠な要素。

FlashやJava、ウェブブラウザへの脆弱性、
Microsoft Office、Adobe Acrobat Readerなどの脆弱性を突くエクスプロイトを防御。

Dll Hijacking、Reflective Dll Injection、Heap Spray Allocation、Stack Pivot など
<u>エクスプロイト攻撃で用いられる様々なテクニックに対応。</u>



エクスプロイトのキルチェーン
（連続した攻撃の流れ）

例

メール開封、Webアクセス、
ネットワーク経由などで到達。

メモリーに展開。

脆弱性を突き、任意の操作を可能にする。
シェルコードを使用出来るようにする。

比較的小さなプログラム。
悪意ある動作を行う前の準備段階。

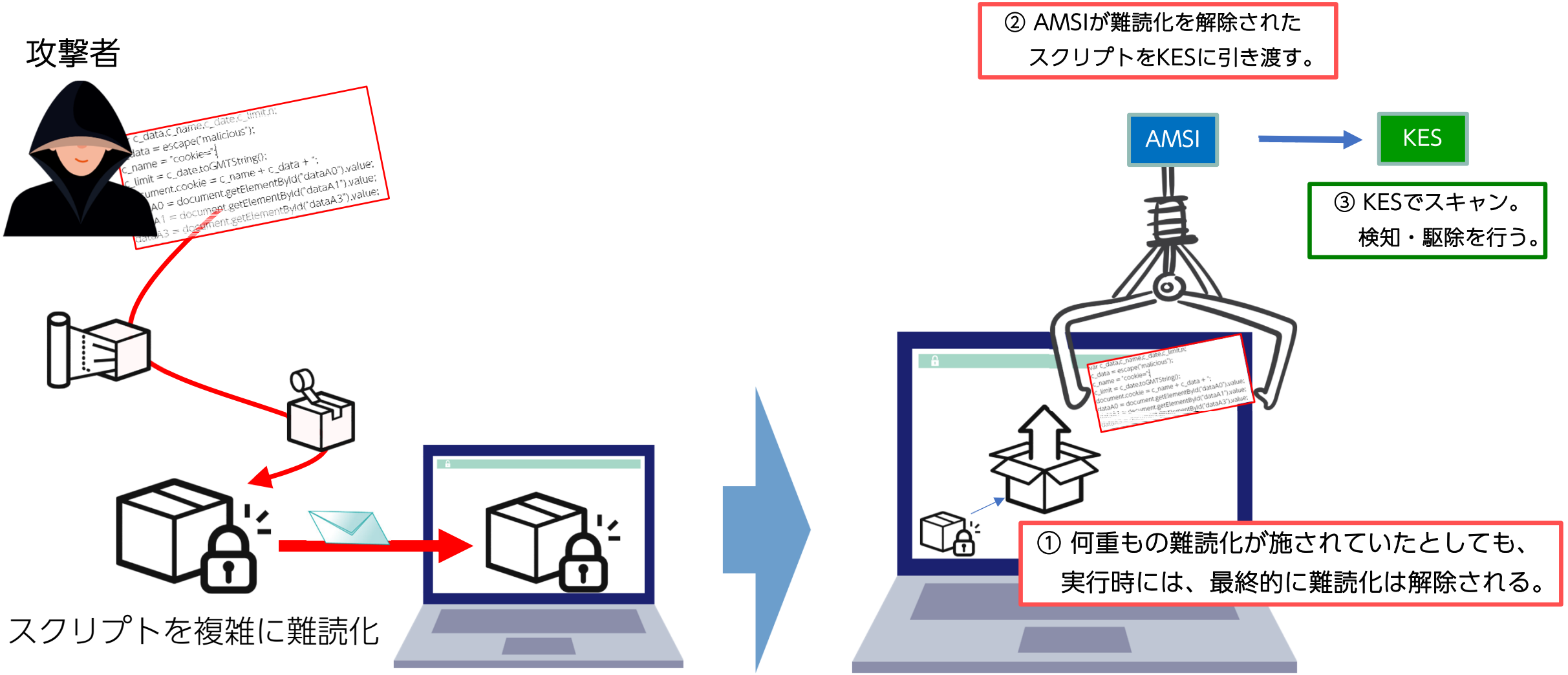
悪意ある動作。破壊、データ漏洩。

他コンポーネントで検知

脆弱性攻撃ブロックにより、
実行防止

脆弱性攻撃ブロックにより、
検知・ブロック

複雑に難読化されたスクリプトの検知能力を向上。



AMSI 保護プロバイダー

複雑に難読化されたスクリプトの検知能力を向上。
Antimalware Scan Interface（AMSI）とKESを統合。
AMSI対応アプリケーションからKESにスクリプトを引き渡し、スキャン。
ファイルレスマルウェアに対して有効。

AMSI は、Windows10以降、Windows Server2016以降 に搭載されている機能

現行AMSI対応アプリケーション

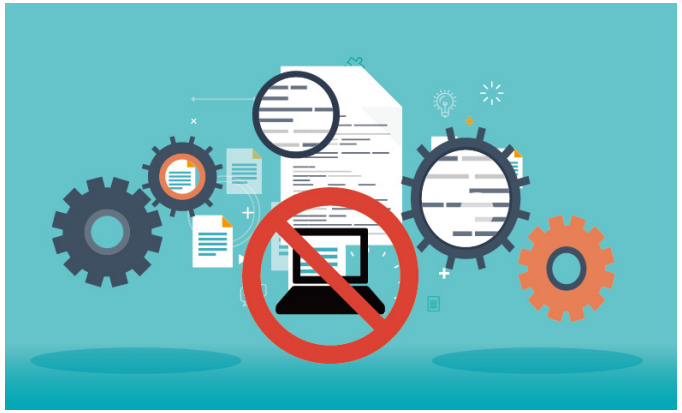
- PowerShell, JavaScript, VBScript等のスクリプトエンジン
- Office VBAマクロ

ホスト侵入防止の主機能

アプリケーションがシステムにダメージを与える可能性のある行為を防御し、
オペレーティングシステムリソースにアクセスすることを制御する。

実行中のプログラムの以下の動作を制御

- ファイルシステムへのアクセス
- レジストリへのアクセス
- 他のプログラムとのやり取り



アプリケーションは以下の４つに分類される。

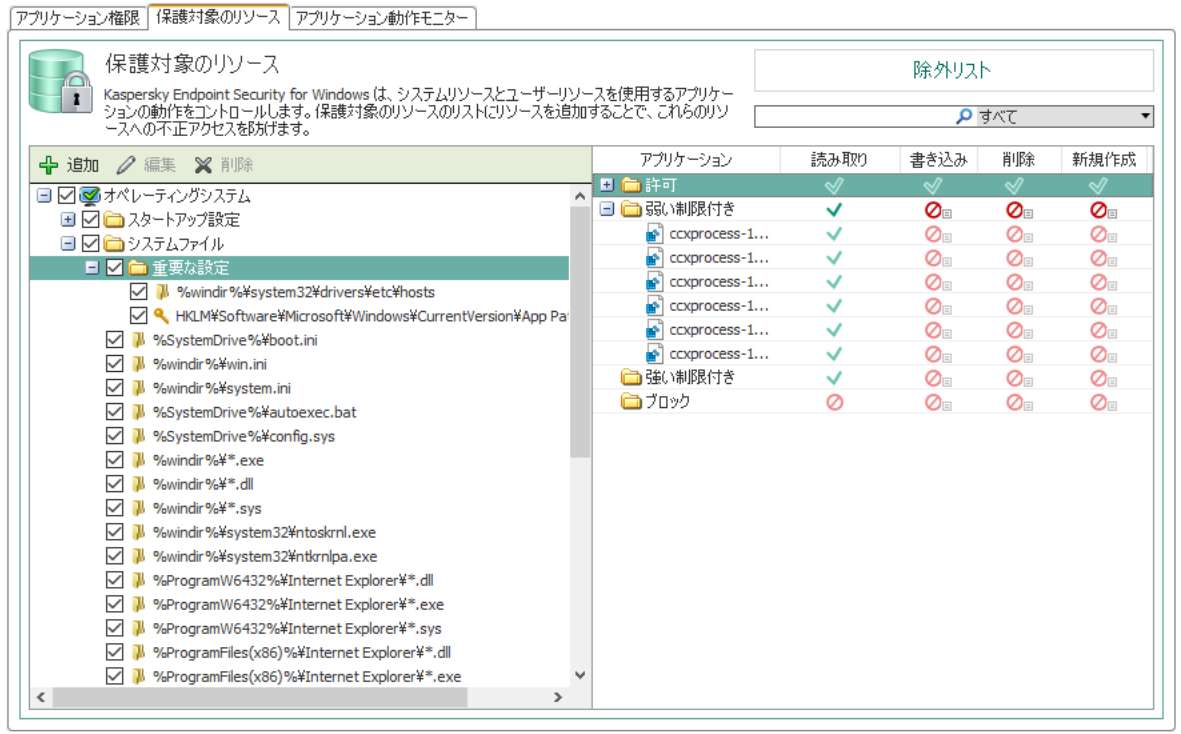
- 許可
- 弱い制限付き
- 強い制限付き
- ブロック

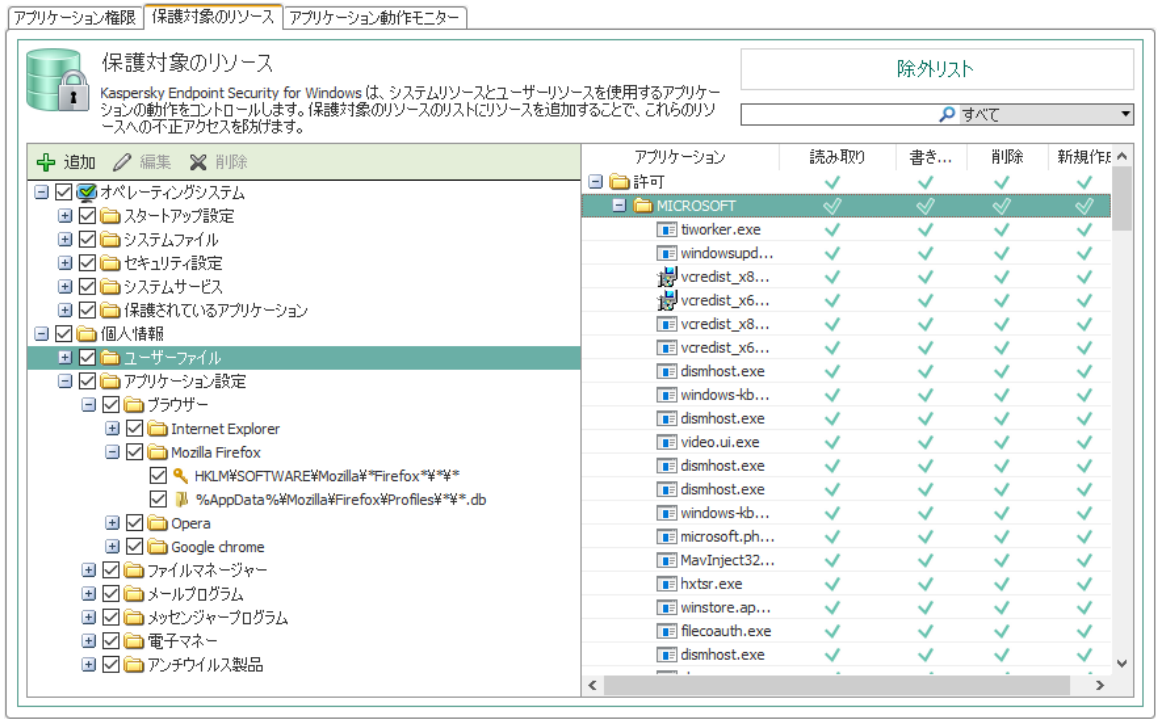
ホスト侵入防止

信頼カテゴリごとに、ルールは次のことを行うアプリケーションの機能を定義する。

- ファイル、レジストリキーの変更（読み取り、書き込み、作成、削除）
- ネットワーク接続を確立する
- Webカメラとマイクへのアクセス。
- 開いているプロセス、Windowsのシャットダウンなどのシステム操作の実行。

保護対象リソースの一部





アダプティブアノマリコントロール

PC環境に適用される”ふるまいブロック“。

定期的に更新されるヒューリスティックルール。

アプリケーションが悪性かどうかではなく、実装方法に着目。
例えば、「PowerShellによる難読化されたコードの実行」ルールでは、
コードが悪性かどうかを評価するのではなく、難読化している点を問題にしている。

ブロック処理だけでなく、通知（ログ）処理も可能。

ヒューリスティックルール 例:

- PowerShellによる難読化されたコードの実行
- スクリプトからネィティブAPIのコール
- システムディレクトリ以外に配置されているシステムファイルと同名ファイルの起動
- Officeアプリケーションからスクリプトのキック
- WMI経由でリモートからWindowsツール（mshta.exe, PowerShell等）の開始

アダプティブアノマリコントロール

ルール

スクリプトエンジンとフレームワークの動作		
PowerShell による外部コードの実行	有効	ブロック
PowerShell スクリプトによる不明な動的コードの実行	有効	ブロック
PowerShell による難読化されたコードの実行	有効	ブロック
PowerShell によるネイティブ API の呼び出し	有効	ブロック

Emotetによる難読化された
スクリプト実行をブロック

アダプティブアノマリーコントロールレポート

サマリー　詳細

詳細 1 件(1 件中)

検索

グループ	デバイス	ユーザー名	ルール名	処理	ソースプロセスのパス	ソースオブジェクトのパス
管理対象デバイス	PC01	PC01\admin	PowerShell による難読化されたコードの実行	ブロック	c:\windows\system32\windowspowershell\v1.0\powershell.exe	object://ps:CFD646BAB10A3632369D0C1BA561DEEB99559D5444897B49D4B1B49

ターゲットオブジェクトのパス

object://script:...emtype dIreCtOrY;[Net.ServicePointManager]::"SecUr`I`Ty`pR`OTocol" = (('t'+'ls')+('12'+', tl')+('s'+'11, ')+('t'+'ls'));$U33e7pj = ('Yv'+'g'+('cdua'+'_'));$Gdyii5q=('Xk'+'j1'+('s'+'ai'));$G

ルールの調整

アダプティブアノマリコントロールルールは、疑わしい挙動を定義していますが、
業務で使用されるアプリケーションがルールに合致する場合は、除外設定を行います。
そうした業務は特定のユーザーで実施されるため、最小限のユーザーを除外します。

脅威対策機能・コントロール機能

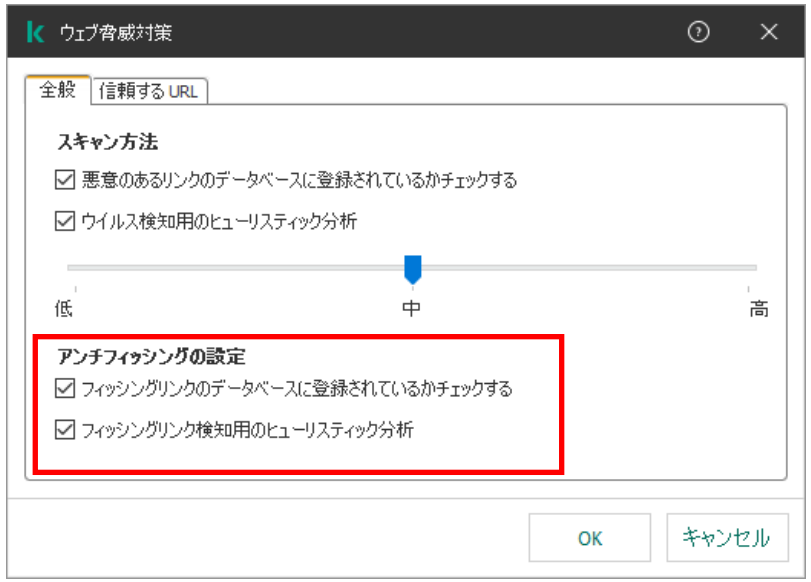
kaspersky

ウェブ脅威対策

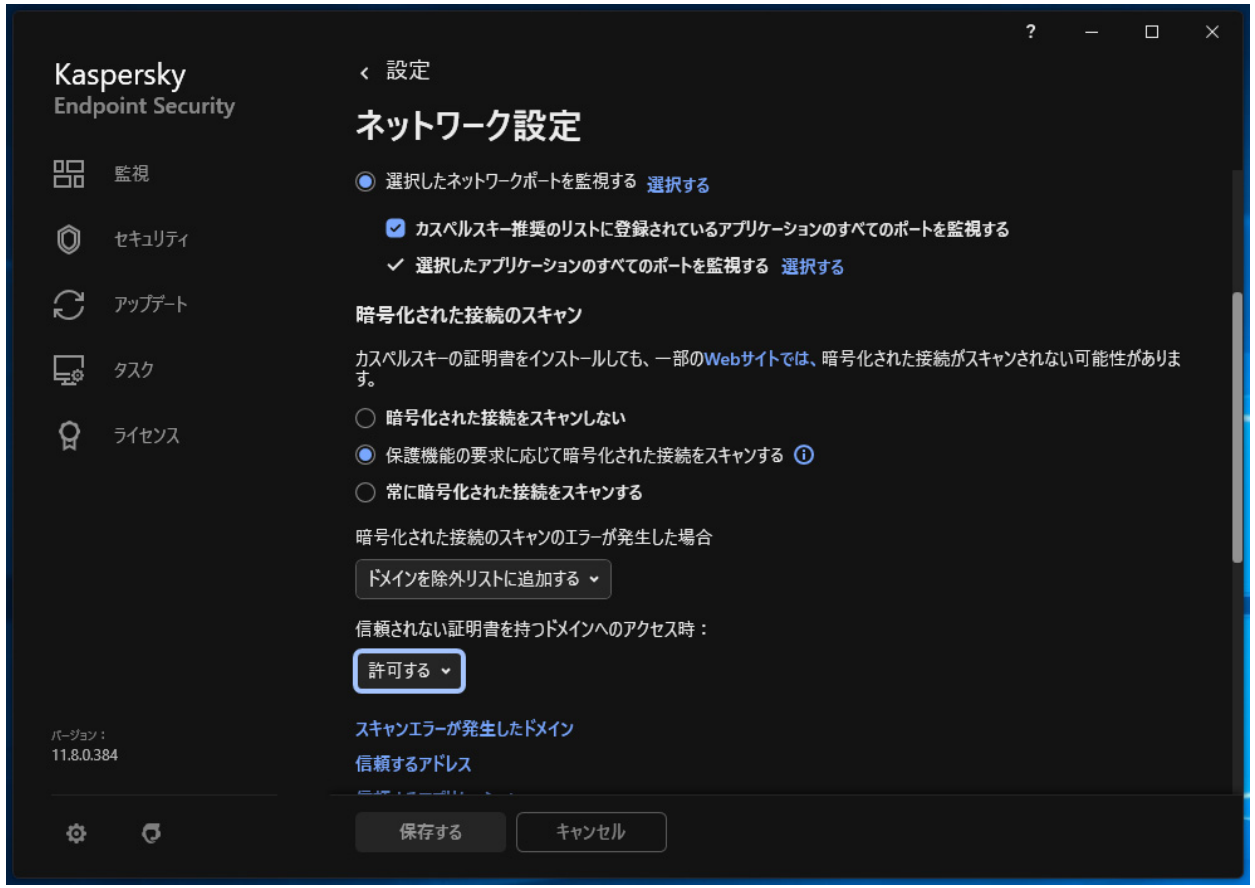
- ネットワークレベルで検知するためブラウザに依存しない。
  ブラウザのプラグインタイプの製品は、ブラウザの対応が限定され、
  対応ブラウザであっても、ブラウザの更新に追随できない問題がある。

- マルウェアだけでなく、フィッシングサイトにも対応。
  URL情報だけでなく、フィッシングサイト特有の構造を検知する。
  フィッシングサイトの解析にヒューリスティック分析を使用し、リアルタイムに解析を行う。

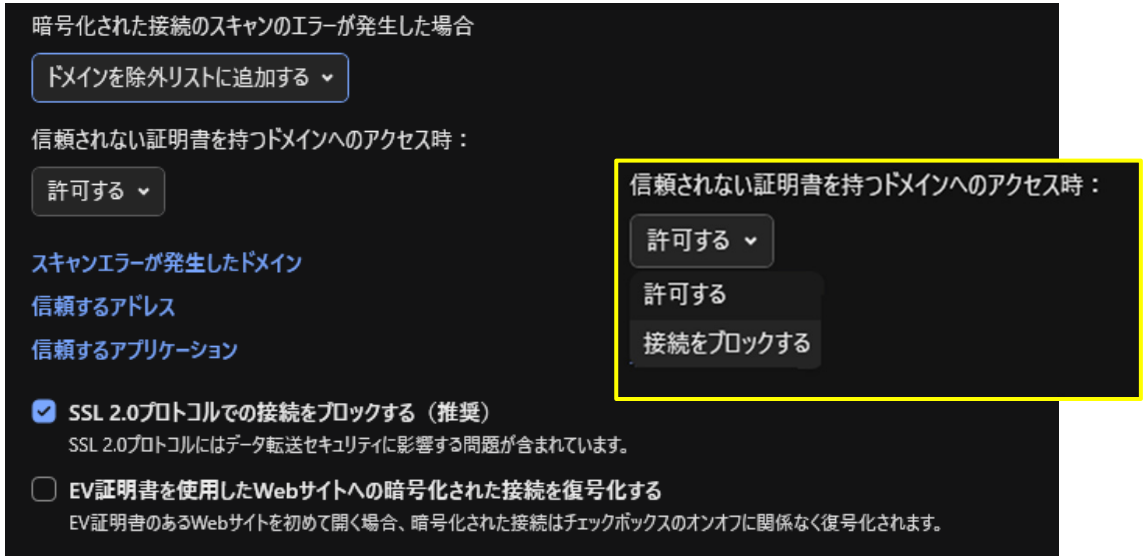
- HTTPSトラフィックのスキャンにも対応



HTTPSトラフィック：暗合化された通信のスキャン



信頼されない証明書による
HTTPS通信をブロック可能

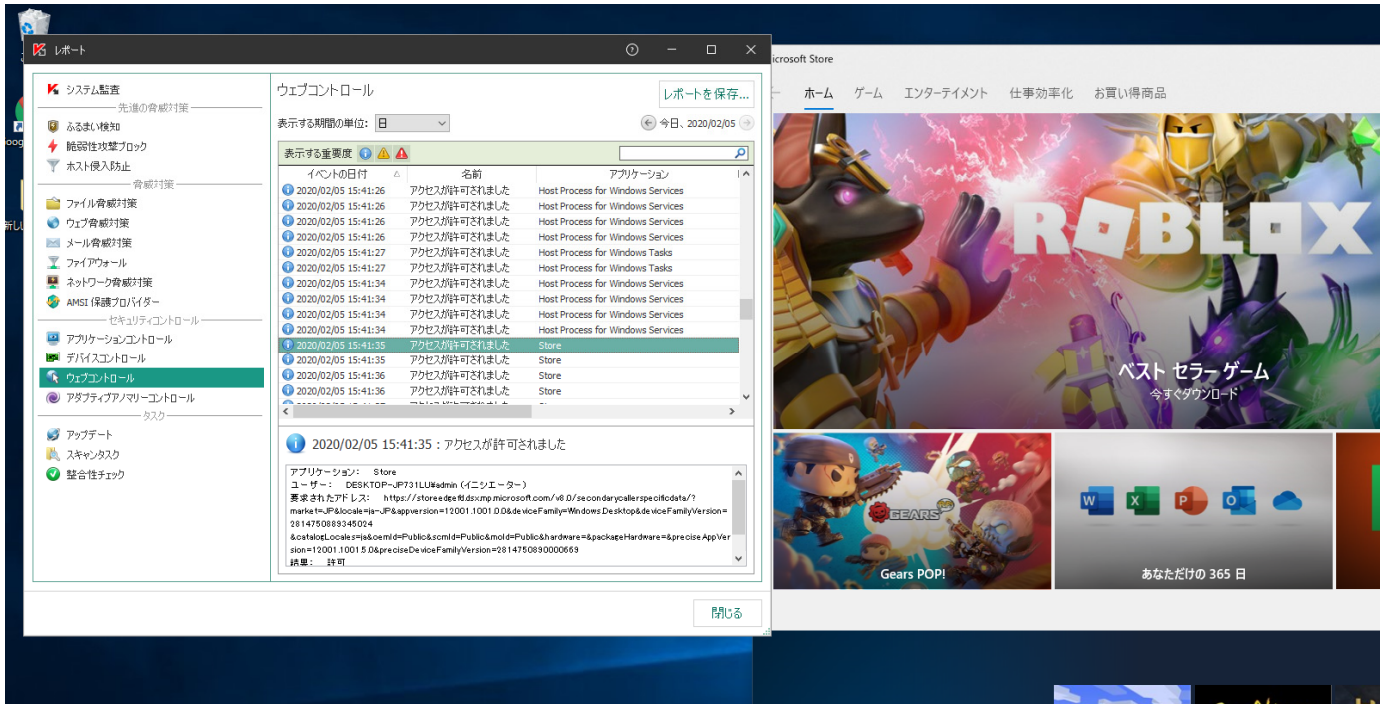


HTTP、HTTPSアクセスログ

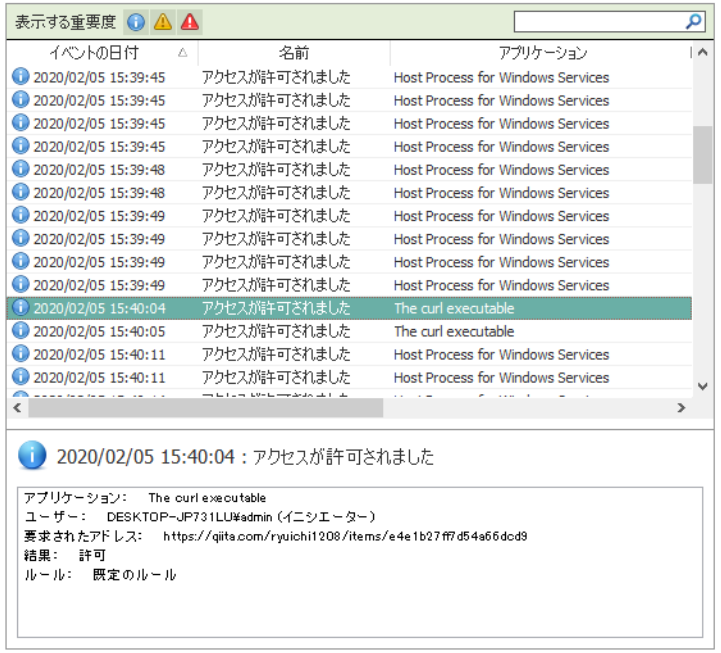
KESではブラウザのプラグインで保護するのではなく、
ネットワークトラフィックを監視するため、
ブラウザのみでなく、アプリやコマンドのアクセスが記録可能

通信ログの例

アプリによるhttp通信



Curlコマンド



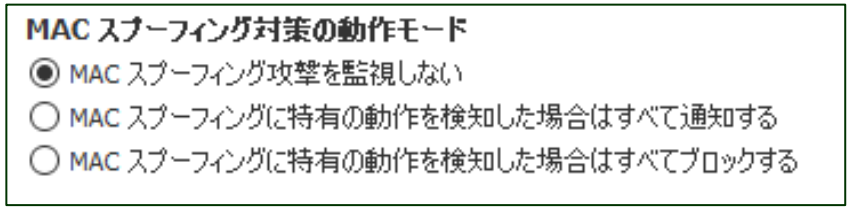
ネットワーク脅威対策

- 不正侵入防止機能、IPS (Intrusion Prevention System)

  OSやアプリケーションの脆弱性を突くネットワークからの攻撃をブロック
  攻撃を検知した端末からの接続を、一定時間すべてブロック
  近年復活したワーム型マルウェア、ランサムウェアをブロック可能

- MACアドレススプーフィング

  攻撃者の不正なARP応答をブロックし、情報搾取を防ぐ

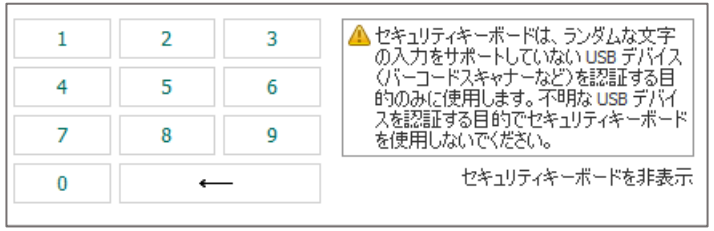


有害USB攻撃ブロック

有害USB攻撃とは；
普通のUSBメモリを改変を加えUSBキーボードに仕立て上げファイルを削除したり、
ネットワークアダプターに偽装させデータを盗聴する等、改造したUSBメモリによる攻撃。

有害USB攻撃ブロック
新たに接続したUSBデバイスは、承認しなければ使用出来ない。
ポインターなど数字キーを持たないデバイスを説明するために、
ソフトウェアキーボードの使用も有効に出来る。禁止も可能。

- 特許技術



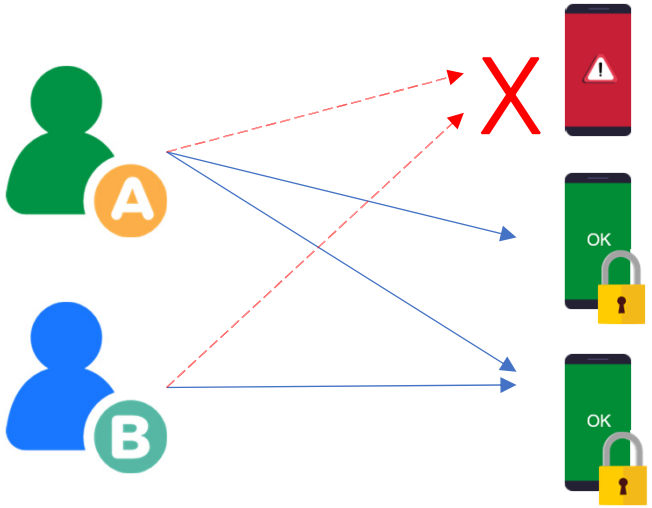
デバイスコントロール

不正なデバイスの使用を制御。
USBメモリー、マスストレージ、スマートフォンなどの不正な接続を防止。
権限のない内部犯行者からの不正な情報持ち出しを防止。

＋ ID でデバイスを追加　＋ モデルでデバイスを追加　＋ ID マスクでデバイスを追加　＋ モデルマスクでデバイスを追加　編集　削除

デバイス種別	デバイスモデル	デバイス ID	名前	ユーザー	コメント
リムーバブルドライブ	-	USBSTOR\DISK&VEN_USB_2.0&PROD_USB_FLASH_DRIVE&REV_0.00\499352C253B53B&0	USB 2.0 USB Flash Drive USB Device	Everyone	-
リムーバブルドライブ	VEN_EKM&PROD_EK-UW	-	EKM EK-UW USB Device	PC01\admin	-

- マスクを使用したデバイスの登録
  例　暗号化されたUSBメモリーだけを許可し、
  　　万が一の紛失に備える。
- ユーザーでの制御・ActiveDirectory連携



デバイスコントロール：　Wi-Fiネットワークアクセス制御

指定したアクセスポイントのみに接続を制限したり、
Wi-Fiネットワークを使用不可にする。

設定例

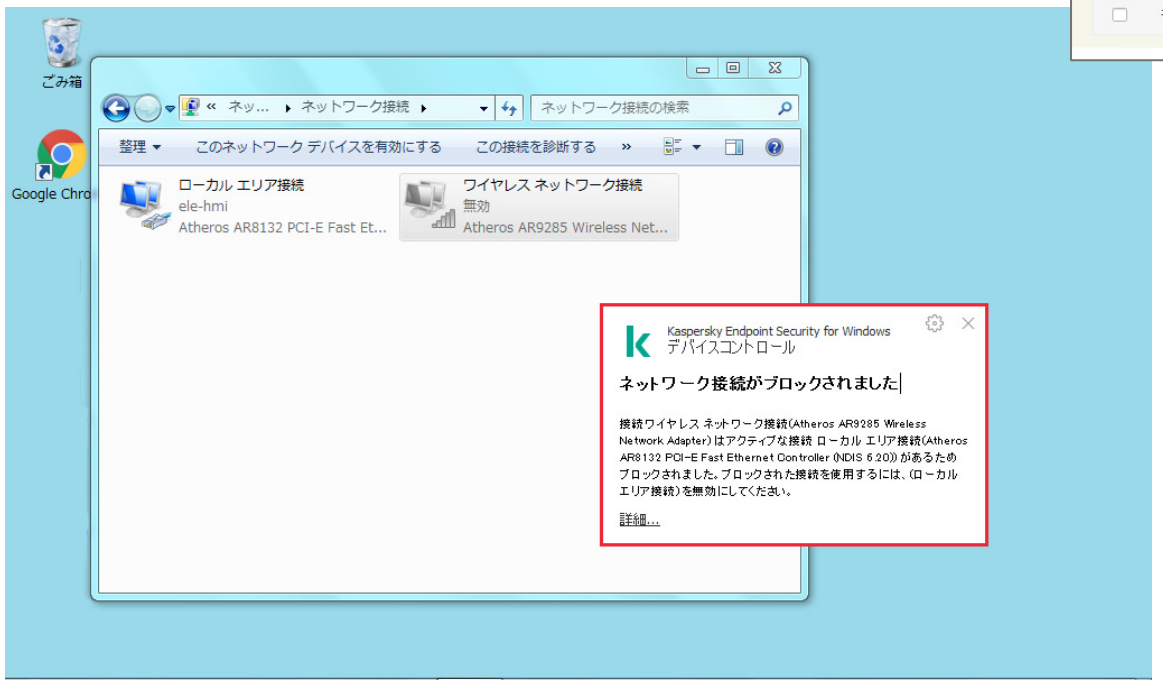
リストに無いアクセスポイントへの接続をブロック

デバイスコントロール：　アンチブリッジ

ネットワークブリッジの作成をブロックし、複数のネットワーク接続が同時に確立することを防止。
セキュリティ保護が不十分なネットワークと社内ネットワークが同時に接続されることを防止。

以下のデバイスに対して接続ルールを作成。

- ネットワークアダプター
- Wi-Fi アダプター
- モデム



偽アクセスポイント
自動接続されるフリーWi-Fi

ウェブコントロール

ウェブアンチウイルスとの違い

ウェブアンチウイルス：悪意のあるサイト、フィッシングサイトのブロック
ウェブコントロール：　コンテンツカテゴリーフィルタリング

コンテンツ、ユーザー、スケジュールと合わせた設定が可能

データ種別

無効	映像
無効	音楽
有効	Office のファイル
有効	実行ファイル
有効	アーカイブ
無効	グラフィックファイル

コンテンツカテゴリ

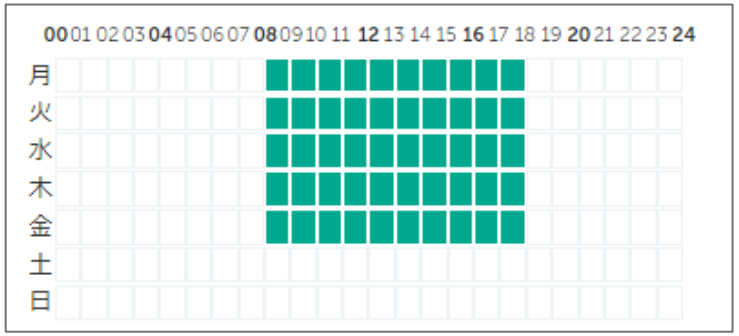
- アダルト
- アルコール、タバコ、麻薬
- 暴力
- 過激な表現、わいせつな表現
- 武器、爆発物、火工術
- 求人サイト
- アノニマイザー
- ソフトウェア、音楽、映像
- ギャンブル、宝くじ、懸賞
- インターネットコミュニケーション

ユーザー

- すべてのユーザーに適用する
- 個別のユーザー、グループ、またはその両方に適用する

＋ 追加　× 削除

ユーザーまたはグループ
EDR-O\admin
BUILTIN\Power Users



kaspersky

ウェブコントロール

シナリオ

- Webからの取得には危険が多いオフィスファイルダウンロードを、
一般ユーザーが行わないようブロック。

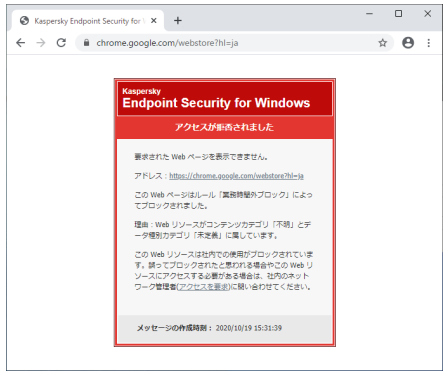
- 業務時間外の接続を禁止。不正な通信抑制にも効果。
業務に必要なサイトは除外設定が可能。

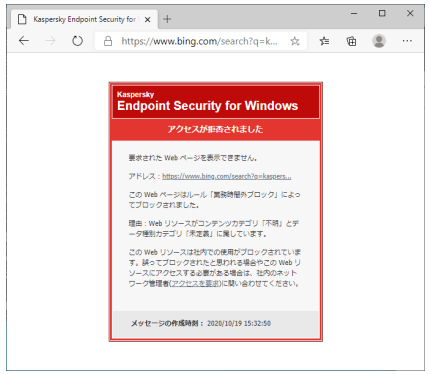
許可時間ではコマンドラインでのHTTP通信が可能

```
C:¥>curl --get http://www.kaspersky.co.jp
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

禁止時間ではコマンドラインもブロック

```
C:¥>curl --get http://www.kaspersky.co.jp
・ソ<!--Detected and blocked with Kaspersky Lab-->
```



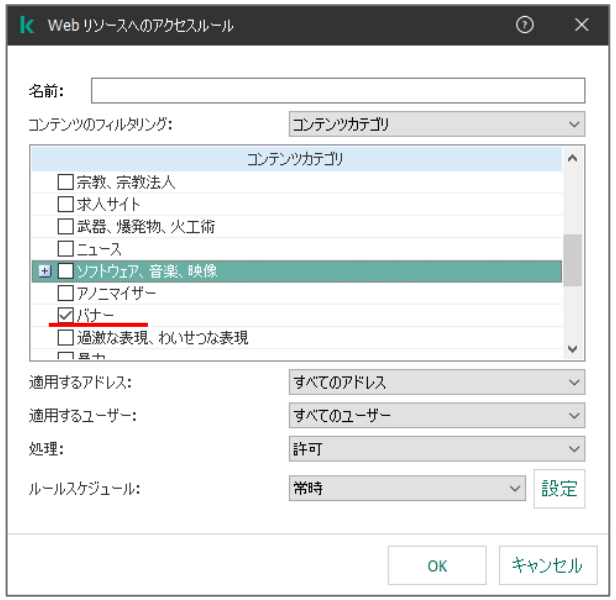


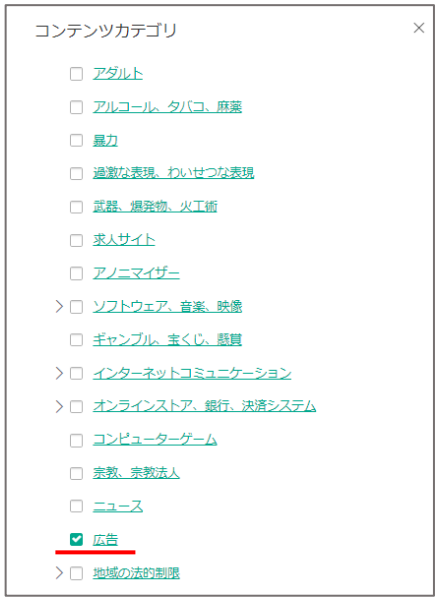
ウェブコントロール：　バナー広告ブロック

バナー広告ブロック

ウェブコントロールにあるカテゴリのひとつ。
疑わしい広告や情報収集をブロックし、セキュリティを強化する

2020/10/17 13:44:34	アクセスが拒否されました	Google Chrome	PC02¥admin	https://secu[illegible]k.net/tag/[illegible]	バナー広告
2020/10/17 13:44:35	アクセスが拒否されました	Google Chrome	PC02¥admin	https://stats.[illegible]net/j/collect?t=dc&aip=1&_r=3&...	バナー広告
2020/10/17 13:44:35	アクセスが拒否されました	Google Chrome	PC02¥admin	https://stats[illegible]net/j/collect?t=dc&aip=1&_r=3&...	バナー広告
2020/10/17 13:46:11	アクセスが拒否されました	Google Chrome	PC02¥admin	https://cas[illegible]y/0.1[illegible]id=146...	バナー広告
2020/10/17 13:46:45	アクセスが拒否されました	Google Chrome	PC02¥admin	https://stats[illegible]net/j/collect?t=dc&aip=1&_r=3&...	バナー広告
2020/10/17 13:48:06	アクセスが拒否されました	Google Chrome	PC02¥admin	https://stats[illegible]net/j/collect?t=dc&aip=1&_r=3&...	バナー広告
2020/10/17 13:48:10	アクセスが拒否されました	Google Chrome	PC02¥admin	https://fls.[illegible]/json?spot=[illegible]&rc=&var=s...	バナー広告
2020/10/17 13:50:08	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://ad.[illegible]_ad/rtb/view?url[illegible].cc&uid...	バナー広告
2020/10/17 13:50:11	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://ads.[illegible]/get-user-id?ver=2[illegible]type=i...	バナー広告
2020/10/17 13:50:12	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://jp[illegible]m/addyn/3.0/[illegible]/0/-1/all...	バナー広告
2020/10/17 13:50:12	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://contex[illegible]/dmec[illegible]p...	バナー広告
2020/10/17 13:50:12	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://[illegible]/uac/request[illegible]edSizes=728x90,948x...	バナー広告
2020/10/17 13:50:14	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://[illegible]/uac/error[illegible]es=728x90,948x25...	バナー広告
2020/10/17 13:50:14	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://[illegible]/uac/reepo[illegible]izes=728x90,94...	バナー広告
2020/10/17 13:50:16	アクセスが拒否されました	Microsoft Edge	PC02¥admin	https://[illegible]m/[illegible]?cdp=5[illegible]9...	バナー広告



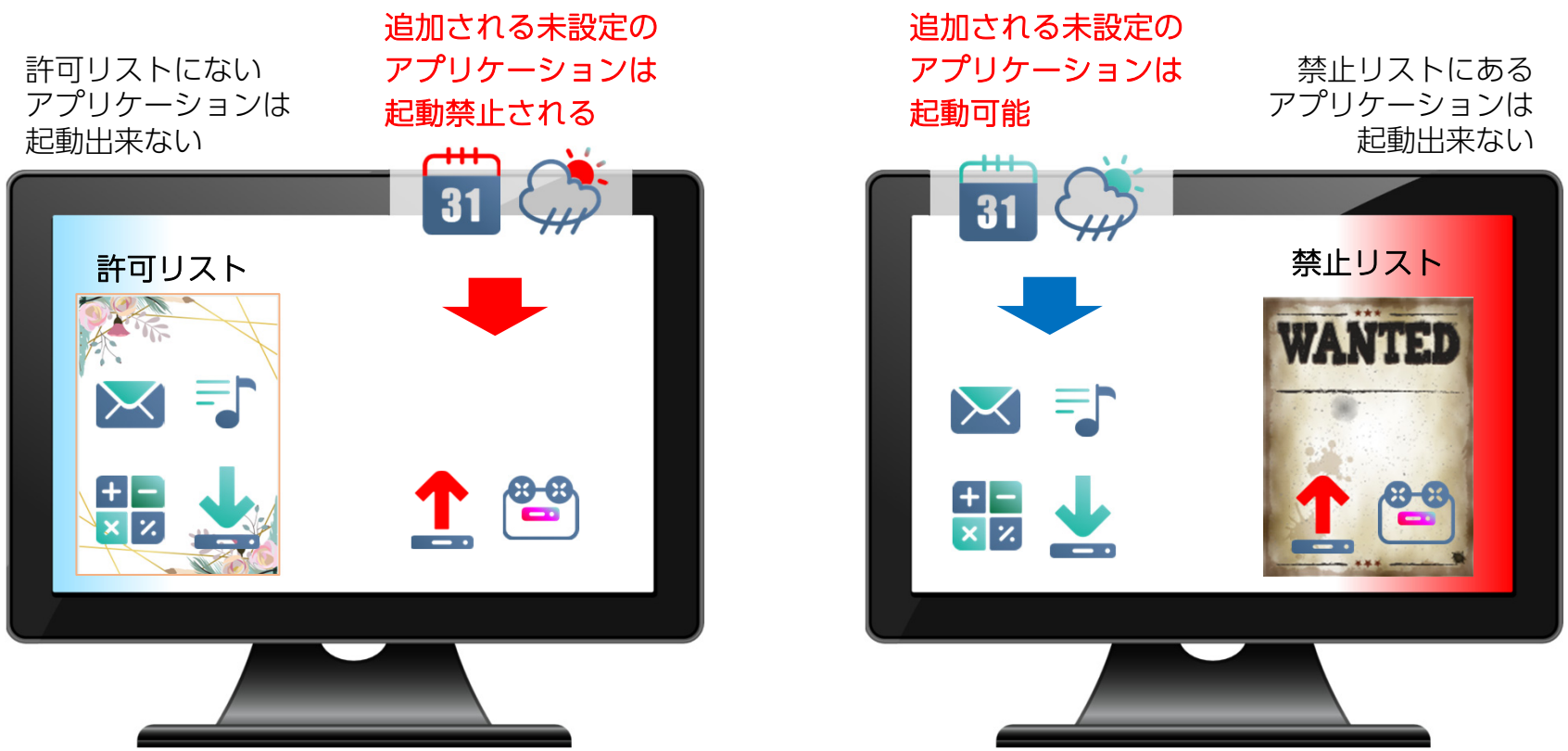


kaspersky

アプリケーションコントロール

アプリケーションの起動をコントロールする機能
許可リストでの運用・禁止リストでの運用が可能。

シナリオ
　デフォルト拒否の許可リストに基づくマスターイメージ



Windows Server向け機能強化

- Windows イベントログ監視

  Windows イベントログの分析結果に基づいて保護対象環境の整合性を監視。
  通常と異なるふるまいを検知した場合、管理者にこのふるまいがサイバー攻撃の可能性を示す可能性があると通知します。

- ファイル変更監視

  指定した監視範囲内でのオブジェクト（ファイルおよびフォルダー）に対する変更を検知。
  これらの変更はコンピューターのセキュリティ侵害を示す可能性があります。
  オブジェクトの変更が検知されると、本製品は管理者に通知します。

- 再起動せずに Kaspersky Endpoint Security をアップグレードするオプション

  製品のアップグレード時にもサーバーの動作が中断されることがありません。
  バージョン 11.11.0 から、コンピューターを再起動せずにパッチをインストールすることもできるようになりました。

Windows イベントログ監視、ファイル変更監視は、KHCS Enterprise のみで有効。

Windows Server向け機能強化

- コアモードサポート

  Ver11.8以降でコアモードをサポート。

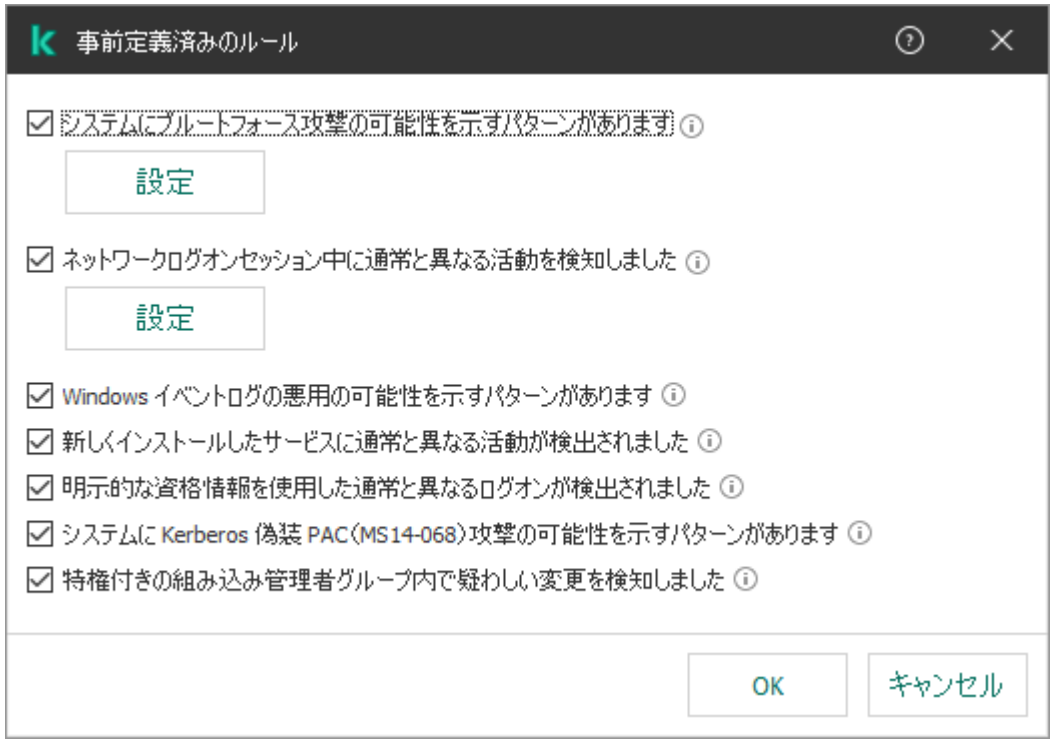
  コアモードのサーバーでの本製品の管理
  コアモードのサーバーには GUI がないため、
  KES for Windowsを管理するにはKaspersky Security Center コンソールを使用するか、
  ローカルでコマンドラインを使用する必要があります。

kaspersky

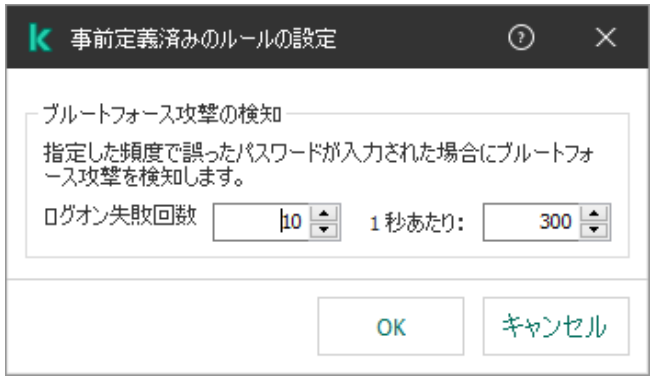
Windowsイベントログ監視

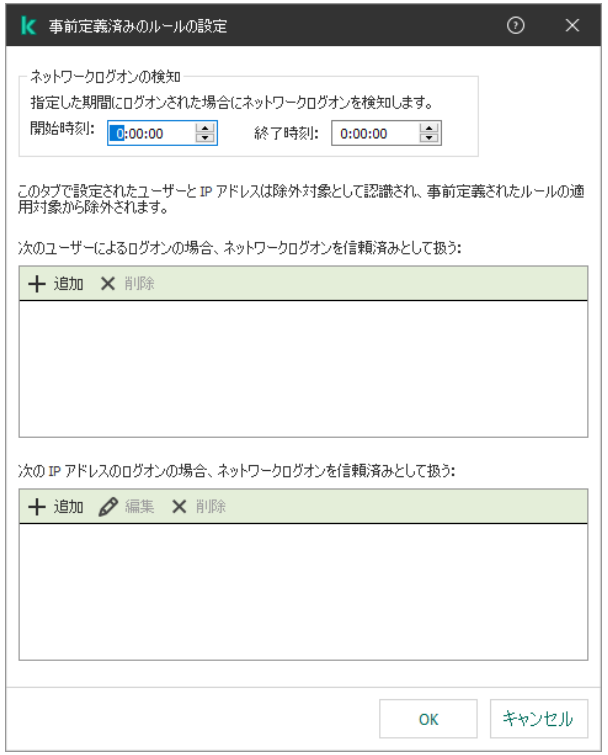
- Windows イベントログの監査結果に基づいて保護環境の整合性を監視
- サイバー攻撃の試みを示す可能性のある異常な動作がシステム内で検知し管理者に通知。
- ユーザー指定のルールまた定義済みルールに基づいて、Windowsイベントログの検討と侵入工作の特定が行われる。

◆ 定義済みのルール



ブルートフォース攻撃検知





Windowsイベントログ監視

◆ 定義済みのルール

システムにブルートフォース攻撃の可能性を示すパターンがあります

本製品は保護対象のシステム内で次のパターンを検知すると警告します：
- パスワード入力の試行が複数回失敗している
- パスワード入力の試行が複数回失敗したのちアカウントがブロックされている

設定

ネットワークログオンセッション中に通常と異なる活動を検知しました

本製品は保護対象のシステム内で次のパターンを検知すると警告します：
- 実行オブジェクトがネットワークログオンセッション中に実行された
- ネットワークログオンセッションが通常と異なる期間で開始された
- ネットワークログオンセッションが通常と異なる IP アドレスから開始された
- NTLM v.1 属性を持つネットワークログオンセッションが開始された

特権付きの組み込み管理者グループ内で疑わしい変更を検知しました

本製品は保護対象のシステム内で次のパターンを検知すると警告します：
- セキュリティグループに追加されることで昇格した権限を持つ一時的なアカウントが作成され削除された
- 短い期間内に、セキュリティグループに追加することによる新しいアカウントの権限昇格があった

明示的な資格情報を使用した通常と異なるログオンが検出されました

本製品は保護対象のシステム内で、明示的な資格情報を使用したログオンセッション中に信頼済みでないオブジェクトが開始されたことを検知すると警告します。

新しくインストールしたサービスに通常と異なる活動が検出されました

本製品は、新しくインストールしたサービス上のエクスプロイト攻撃で権限昇格による保護されたシステムが侵害された可能性を検知すると警告します。

システムに Kerberos 偽装 PAC（MS14-068）攻撃の可能性を示すパターンがあります

本製品は Kerberos の脆弱性を利用して特権を昇格する攻撃（MS14-068）により保護されたシステムが侵害された可能性を検知すると警告します。

Windows イベントログの悪用の可能性を示すパターンがあります

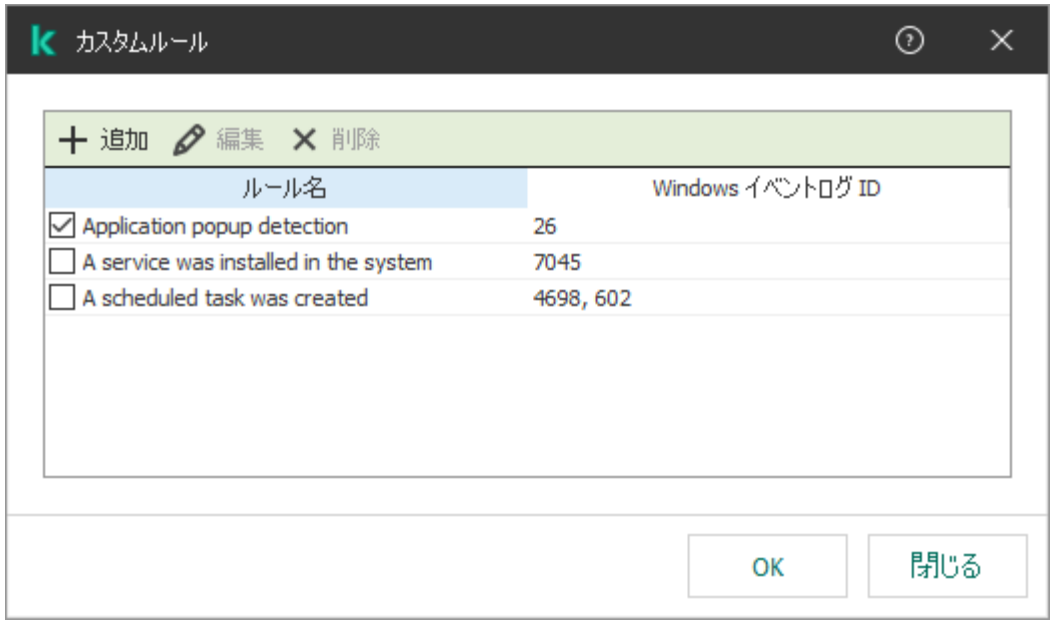
本製品は保護対象のシステム内で次のパターンを検知すると警告します：
- Windows イベントログでセキュリティジャーナルが消去される
- Windows イベントログ全体が消去される
- Windows イベントログに対するイベント記録ポリシーが変更される

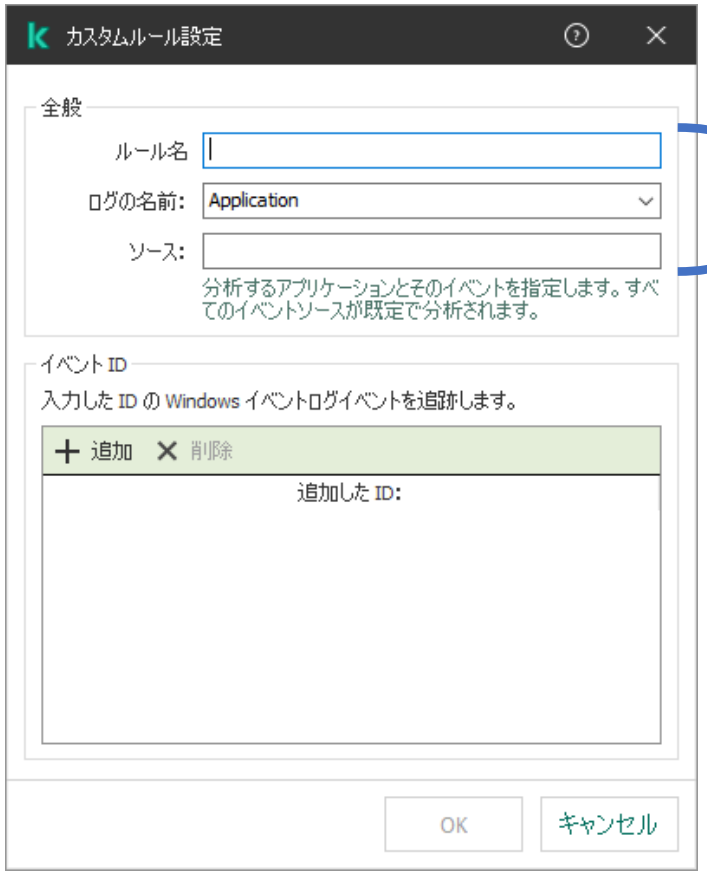
kaspersky

Windowsイベントログ監視

◆ ユーザー指定ルール

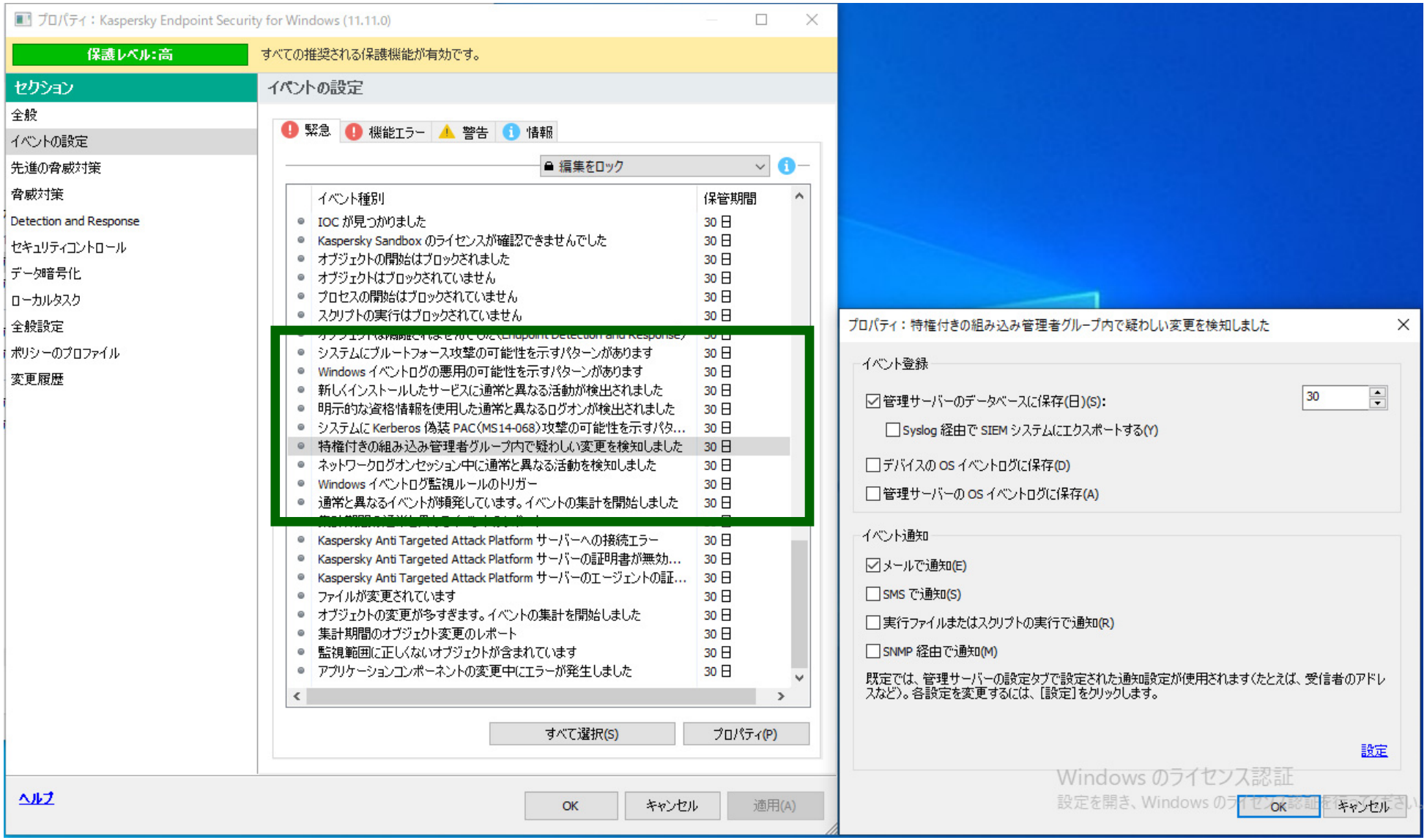
任意のログを指定可能
ソース、IDの指定が可能





プルダウンだけでなく、
手入力も可能。

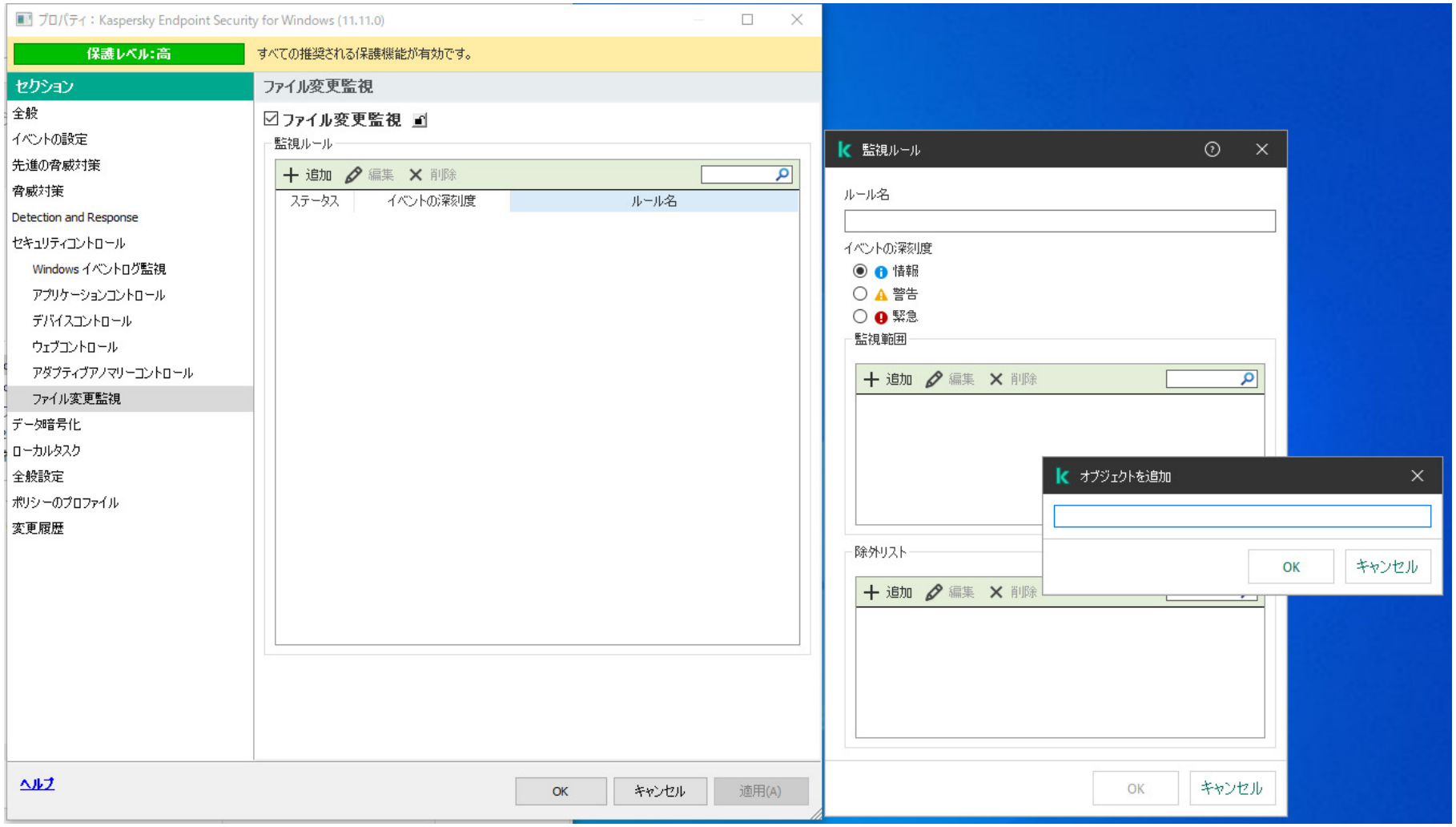
検知をメールでアラート送信



kaspersky

ファイル変更監視

- ローカル操作、ネットワーク共有からの操作、
  アプケーションによる変更等によるファイル変更を検知。（ブロックはしません）



攻撃シナリオと
保護機能

攻撃シナリオ：ファイルレス

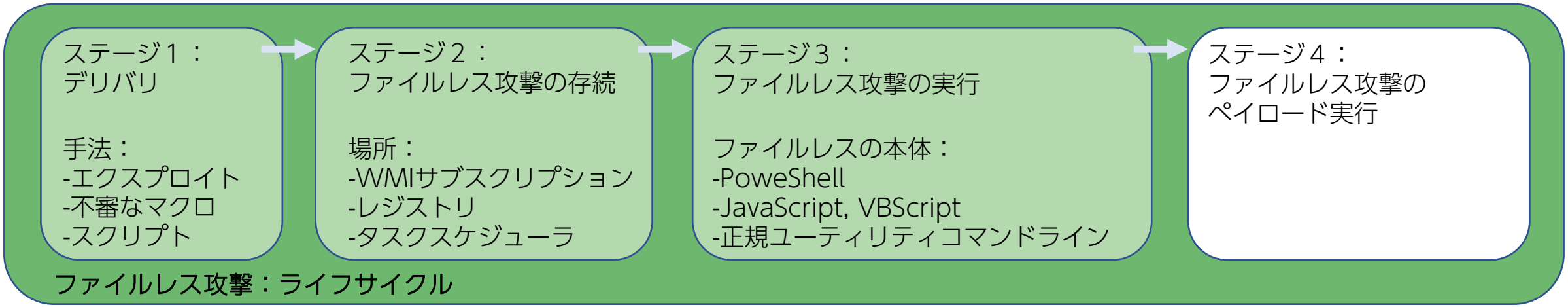
ファイルレスマルウェアはディスク上に本体を直接格納しない。
このタイプのマルウェアは、その検知と修復が複雑化していることから、2017年にはより一般的になった。

次のファイルレス手法は、攻撃で幅広く使用されている。

- Windows Management Instrumentation （WMI）サブスクリプションに保存された悪意のあるスクリプト
- コマンドラインのパラメータとしてPowerShellに直接渡される悪意のあるスクリプト
- レジストリやOSスケジューラタスクに保存されてOSスケジューラによって実行される悪意のあるスクリプト
- .Netリフレクション技術によってディスクに保存せずにメモリ内で直接抽出および実行される悪意のある実行可能ファイル

攻撃者は、次の方法でファイルレスペイロードを標的のマシンに配信。

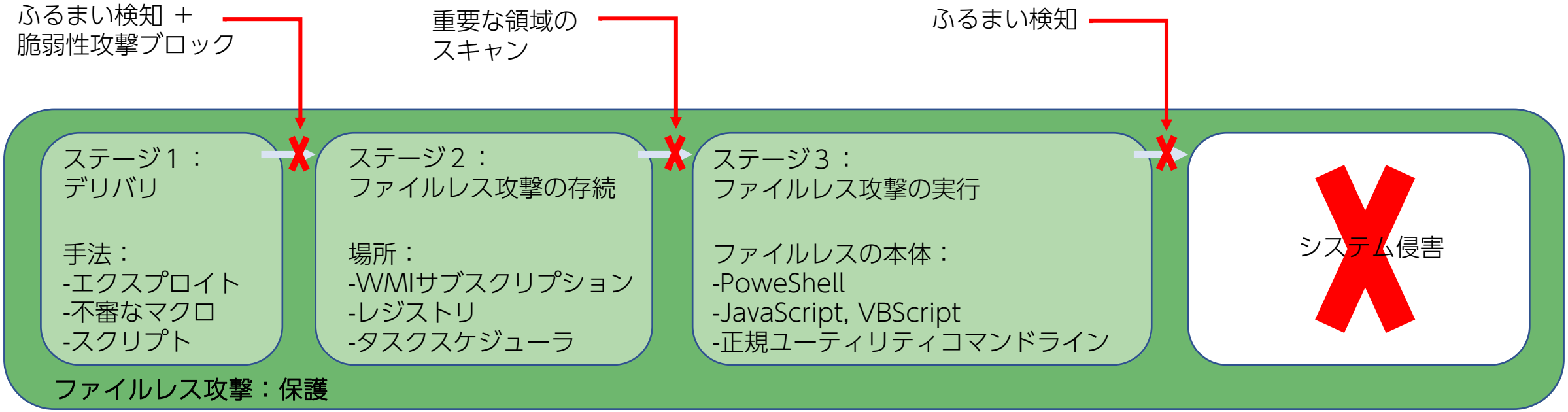
1. 脆弱性を悪用
2. マクロを含む悪意のあるドキュメント
3. シンプルな実行可能ファイル



攻撃シナリオ：ファイルレス

脅威から保護するコンポーネント

- ふるまい検知エンジン
  - ✓ ふるまい検知
  - ✓ マルウェアによる悪意のある変更からのロールバック
  - ✓ 脆弱性攻撃ブロック (AEP)
- OSスケジューラータスク、Windows Management Instrumentationサブスクリプション（WMI）、AutoRun設定、メモリー、レジストリなどの重要な領域のスキャン用エンジン
- ふるまいヒューリスティック分析
  - ✓ 実行されたプロセスのコマンドラインパラメータと実行コンテキストの分析
  - ✓ 実行したアプリケーション（オフィスアプリケーション、スクリプトホストなど）の親プロセス
  - ✓ 実行前のシステム上の動作は何であるか
  - ✓ システムに疑わしい動作（異常なネットワークアクティビティ、アプリケーションのクラッシュ、疑わしいURL要求など）があったか

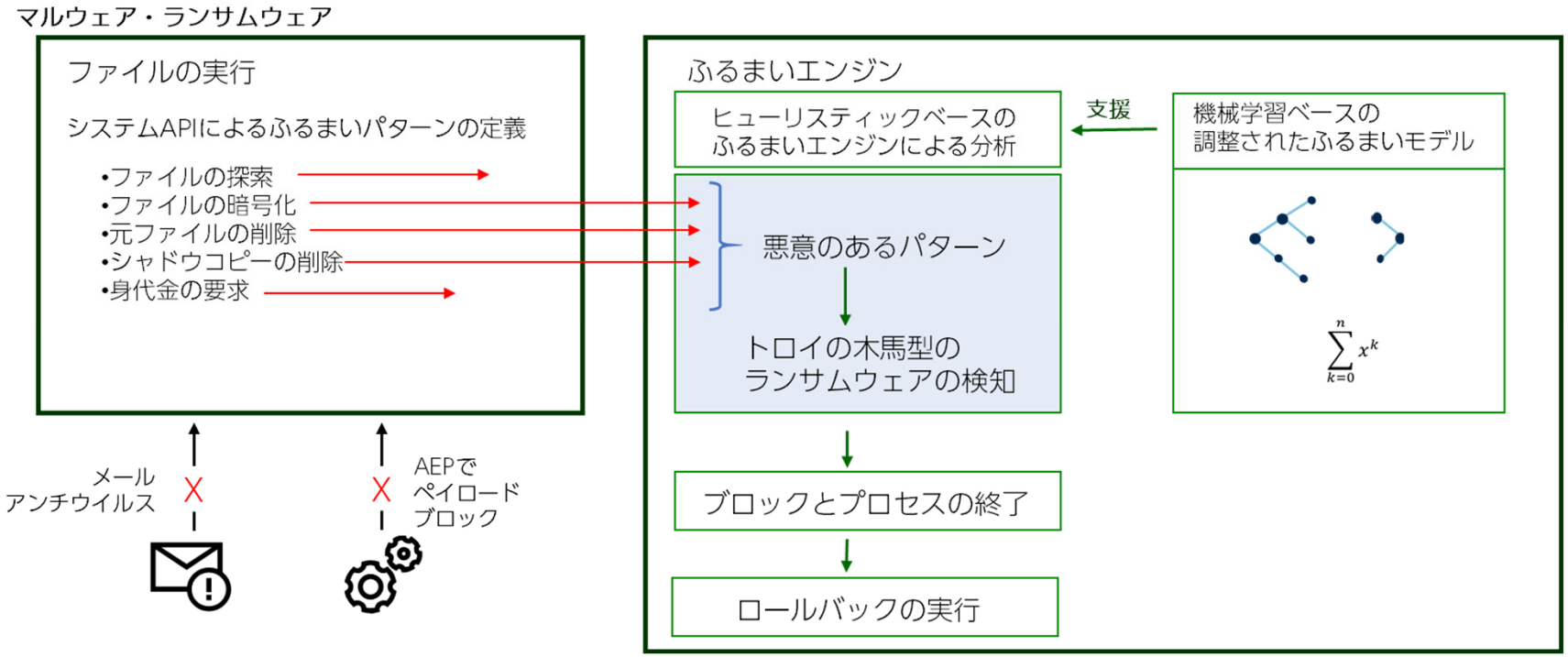


攻撃シナリオ：ランサムウェア

ランサムウェア攻撃にはいくつかの段階が存在

- 標的とするコンピューターへ**配信**
  ：スパムメールへの悪意のある添付ファイル、脆弱性の悪用、標的型攻撃の場合は侵入。
- 実行：重要なユーザーファイルの暗号化
- 身代金要求
- 暗号化されたデータの復号

ランサムウェアに対して効率的に保護するには、多層防御モデルを備えたセキュリティ製品を導入する必要がある。



攻撃シナリオ：ランサムウェア

配信段階：スパムメールに仕込まれた悪意のある添付ファイル

- メール（スパムメール）で実行可能なスクリプトを含むアーカイブを送信
- 悪意のあるマクロを含むMicrosoft Officeドキュメントをメールの添付ファイルとして使用

配信段階：脆弱性の悪用

Automatic Exploit Protection (AEP)

- ソフトウェアの脆弱性を利用したマルウェア（ランサムウェアを含む）の侵入を阻止する重要なコンポーネント。
- AEPによって保護されるアプリケーションには、Webブラウザー、MS Officeアプリケーション、Adobe Acrobat Readerなどが含まれる。
- AEPは CryptXXX やその他多くのランサムウェアをブロックするのに役立つ。

ネットワーク脅威対策（IPS = Intrusion Prevention System ）

- ランサムウェアを配信する手段としてネットワークの脆弱性が悪用される。
- 例えば、WannaCry ランサムウェアは、SMBの脆弱性を悪用して拡散する。
- このような脆弱性を悪用した攻撃は、ネットワークレベルでのみブロック可能。
- ネットワーク脅威対策は、低レベルのネットワークパケットを分析し、これらにヒューリスティック分析パターンを適用、ネットワーク上の悪意のある動作を検知。

実行段階

ふるまい検知

- サイバー犯罪者は、あるゆる手段を使って静的な検知を回避しようと試みる。
- このような場合、ふるまい検知 は、最も強力な最終防御ラインとなる。

kaspersky

攻撃シナリオ：ルートキット

ルートキット - とは
悪意のあるコードとアクティビティが検知されないようにさまざまな技法を駆使し、
自分自身の存在自体を隠し、アンチウイルスによる修復に対抗する悪意のあるプログラムのこと。

通常、ルートキットはドライバー(あるいはドライバのチェーン)を含み、
カーネルモードで動作し、以下の機能の一部またはすべてを実行する。

- ✓ ストレージ(HDD)のファイル、Windowsレジストリのキーと値、システムのプロセス、ロード済みモジュール、メモリ領域(ファイルレスマルウェアの場合)、ネットワークアクティビティ、ディスクのセクター、その他のオブジェクト、アーティファクトを隠蔽する。
- ✓ アンチウイルスによって検知されたルートキットの変更や排除に対抗する(変更されたルートキットの復元など)。
- ✓ 悪意のあるコードやアプリケーションのためにOSカーネルへのアクセス(アンチウイルスのプロセスを終了するため)、正当なプロセスへの悪意のあるコードのインジェクション、ネットワークトラフィックの傍受(スニッフィング)、プロセスキーの傍受(キーロギング)など。

システムの被害を持続させるために、
ルートキットはオペレーティングシステム起動の早い段階で実行を開始する必要があるため、
マスターブートレコード (MBR) とボリュームブートレコード (VBR) 等、ブートセクターを感染させる。
このような機能を備えたルートキットは「ブートキット」と呼ばれる。

アンチルートキットと修復テクノロジー

カスペルスキーのアンチルートキットテクノロジー

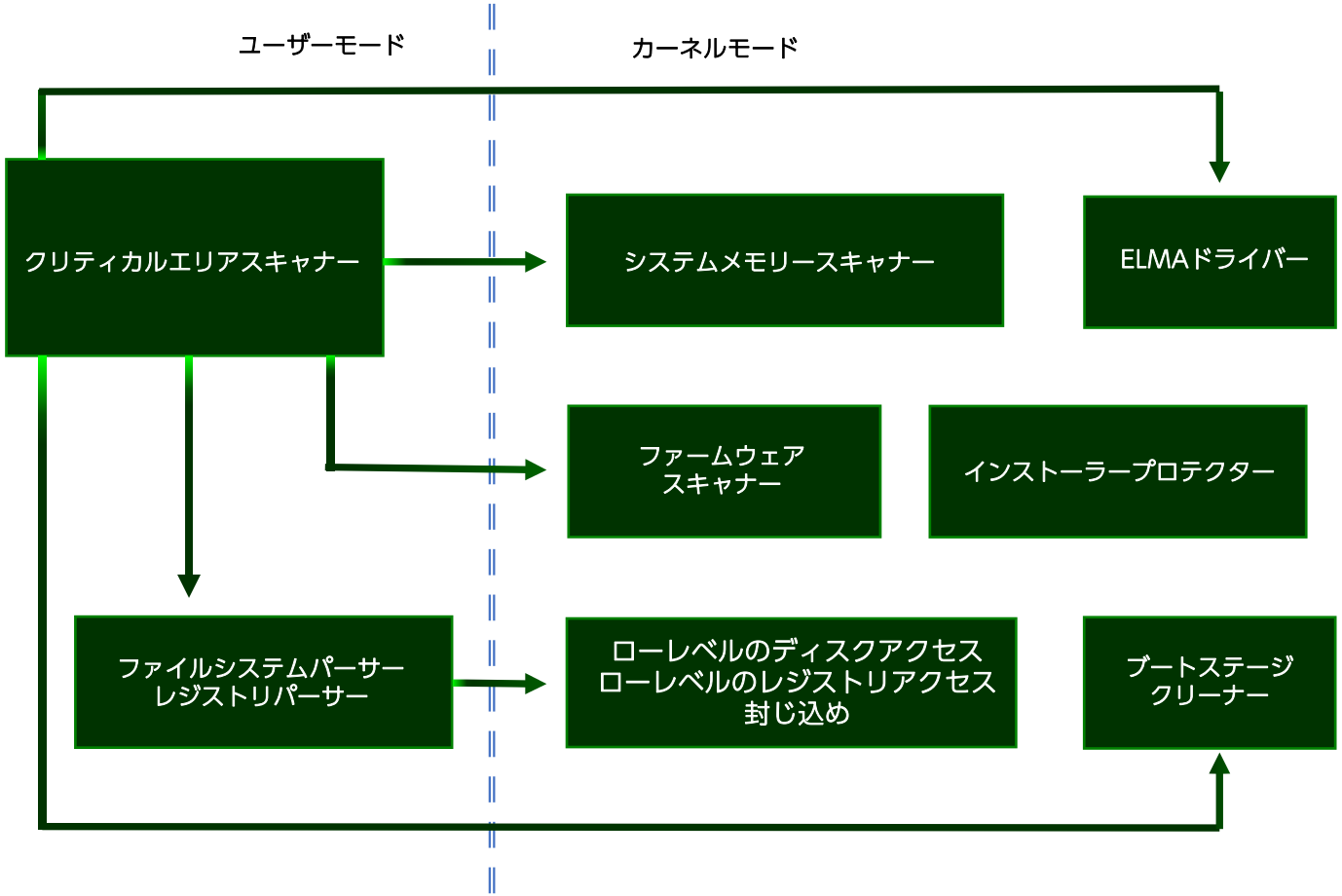
- オペレーションシステムのシステムメモリ内でアクティブな感染の調査
- 自動実行に使用される可能性のあるすべての場所をスキャン
- アクティブな感染を修復し、オペレーティングシステム起動の早期段階でのリカバリ実行
- 感染したシステムに製品をインストールする際の、アクティブな感染の封じ込め

アンチルートキットコンポーネント

- インストーラープロテクター:
  被害を受けているシステムにセキュリティ製品をインストールする際に、アクティブな感染に対抗。
- 低レベルのディスクへのアクセス、低レベルのレジストリへのアクセス、封じ込め:
  さまざまなアクセス遮断方法を回避し、ハードディスクとWindowsレジストリに低レベルでアクセス。
- ブートステージクリーナー:
  オペレーティングシステム起動の早期段階で修復を実行。
- システムメモリスキャナー:
  システムメモリ内のルートキットを探して修復。
- ファイルシステムパーサー、レジストリパーサー:
  多数の形式のファイルシステムとWindowsレジストリを解析。
- 重要な領域のスキャナー:
  前述のモジュールを活用して、自動実行オブジェクトのスキャンと修復を実行するモジュール。

攻撃シナリオ：ルートキット

アンチルートキットと修復テクノロジー



アンチルートキットのコンポーネント

- インストーラープロテクター:
  被害を受けているシステムにセキュリティ製品をインストールする際に、アクティブな感染に対抗。
- 低レベルのディスクへのアクセス、低レベルのレジストリへのアクセス、封じ込め:
  さまざまなアクセス遮断方法を回避し、ハードディスクとWindowsレジストリに低レベルでアクセス。
- ブートステージクリーナー:
  オペレーティングシステム起動の早期段階で修復を実行。
- システムメモリスキャナー:
  システムメモリ内のルートキットを探して修復。
- ファイルシステムパーサー、レジストリパーサー:
  多数の形式のファイルシステムとWindowsレジストリを解析。
- 重要な領域のスキャナー:
  前述のモジュールを活用して、自動実行オブジェクトのスキャンと修復を実行するモジュール。