

kaspersky

Kaspersky Embedded Security System 3.1

デフォルト拒否 許可リスト型 挙動説明（初期値 起動拒否）

2022年4月13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

V1.1



アプリケーション起動コントロール

起動コントロールには二つのモードがあります。

- 統計のみ（ログのみで起動を止めない）
- 処理を実行（ルール通りに、起動とブロックを制御）

- アプリケーション起動コントロールルールに記述されたルールに従って、アプリケーションの起動がコントロールされます。

- ルールは証明書、ハッシュ値、ファイルパスなどで指定します。
- ルール作成は主に3つの方法で行うことができます。
 - ✓ アプリケーション起動コントロールルールの自動生成タスク
 - ✓ ログから自動作成
 - ✓ 手動

アプリケーション起動コントロールルール



Kaspersky
Embedded
Systems
Security

アプリケーション起動コントロールルール

検索:

追加... 選択項目の削除

ファイルのルールを表示 ファイルにエクスポート

ルールの合計数: 1384

種別	ルール名	ユーザー	適用の基準	除外の設定	範囲
許可	KESS:main.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:main.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:main.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:eventpage_bin_prod.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:page_embed_script.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:craw_background.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:craw_window.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:pnad_public_x86_64_crtbegin_for_ah_o	Everyone	SHA256 ハッシュ	はい	実
許可	KESS:pnad_public_x86_64_crtbegin_o	Everyone	SHA256 ハッシュ	はい	実
許可	KESS:pnad_public_x86_64_crtend_o	Everyone	SHA256 ハッシュ	はい	実
許可	KESS:pnad_public_x86_64_ld_nexe	Everyone	SHA256 ハッシュ	はい	実
許可	KESS:pnad_public_x86_64_pnad_llc_nexe	Everyone	SHA256 ハッシュ	はい	実
許可	KESS:pnad_public_x86_64_pnad_sz_nexe	Everyone	SHA256 ハッシュ	はい	実
許可	KESS:Google Update signed by O=GOOGLE LLC, L=MOU...	Everyone	デジタル証明書	はい	実
許可	KESS:Microsoft@ ADAL signed by O=MICROSOFT CORP...	Everyone	デジタル証明書	はい	実
許可	KESS:CollectSyncLogs.bat	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:ErrorPage.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:fre_choose_folder.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:fre_done.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:fre_email_hrd.js	Everyone	SHA256 ハッシュ	はい	ス
許可	KESS:FRE_Tutorial_Intro.js	Everyone	SHA256 ハッシュ	はい	ス

ヘルプ 保存 キャンセル



アプリケーション起動コントロールルール 詳細

名前: FIREFOX signed by O=MOZILLA CORPORATION, L=MOUNTAIN VIEW, S=CALIFORNIA, C...

種別: 許可 範囲: 実行ファイル

ユーザーまたはユーザーグループ: Everyone 参照...

ルール有効化の条件

ファイルのプロパティからルール有効化の条件を設定...

デジタル証明書

発行先を使用: O=MOZILLA CORPORATION, L=MOUNTAIN VIEW, S=CALIFOR...

サムプリントを使用: 0x1326B39C3D5D2CA012F66FB439026F7B59CB1974

SHA256 ハッシュ

ファイルのパス

ルールから除外

除外条件	除外名
------	-----

追加
編集
削除

OK キャンセル

「実行ファイル」、
「MSI・スクリプト」の指定

証明書による指定

ハッシュ値による指定

除外ルール

例えば、ルールを許可で証明書を指定し、
同じ証明書を使う特定のアプリケーションだけを
ブロックする



**Kaspersky
Embedded
Systems
Security**

デフォルトで作成されているルールについて



アプリケーション起動コントロールルール

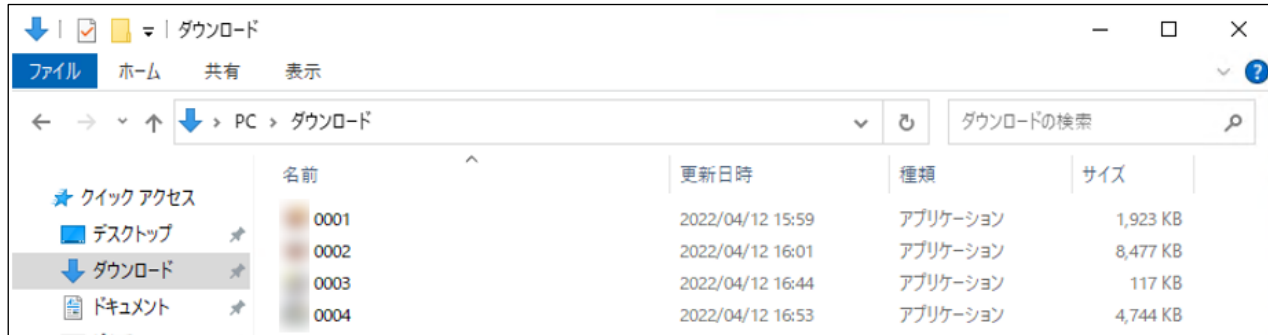
デフォルトで作成されているルールについて

デジタル署名がされているアプリケーション(インストーラーを含む)・スクリプトは、このルールにより実行可能になります。

デジタル署名があるアプリケーションは許可する場合には、このルールを残し、明示的に許可したアプリケーションのみを許可する場合には、このルールを削除します。削除する場合は、必要なルールで置き換えるか、ルールを追加した後に削除します。

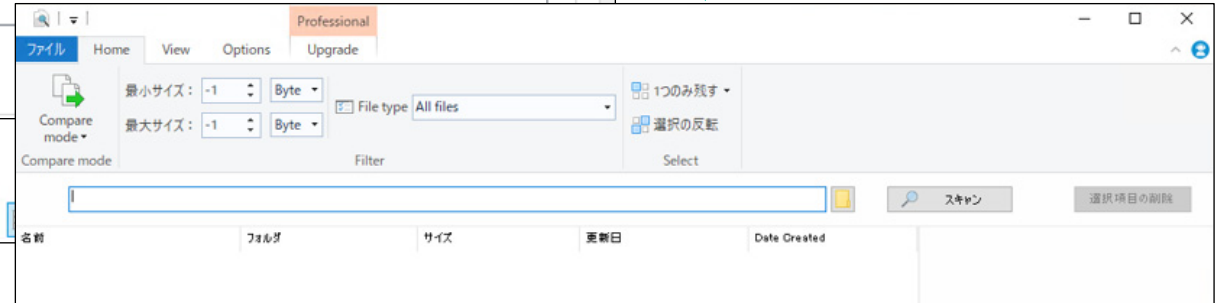
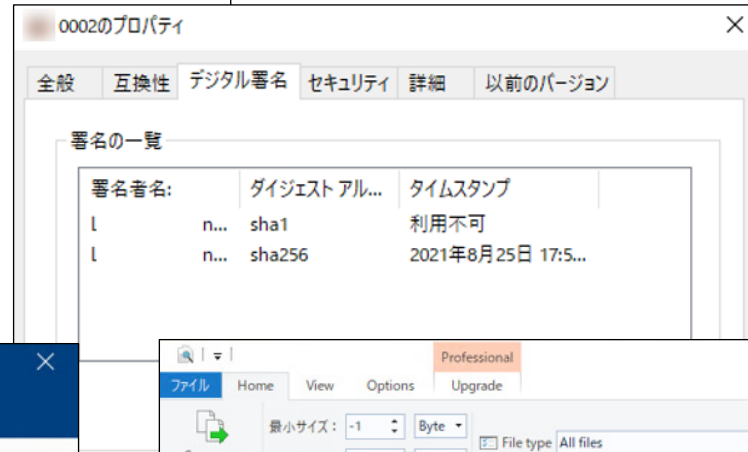
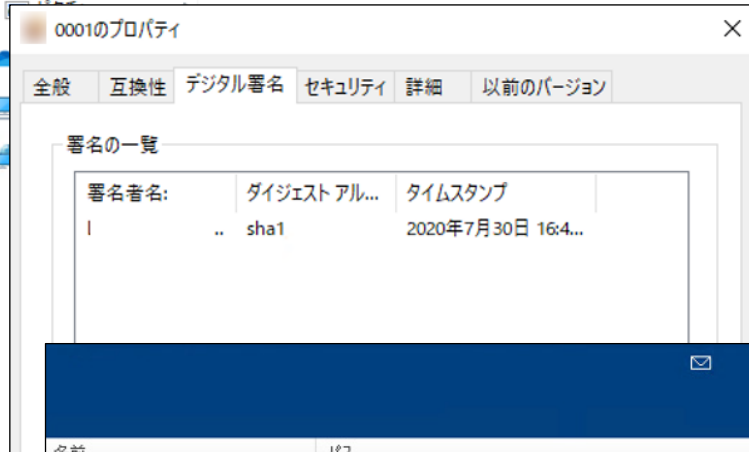


デフォルトで作成されているルール 挙動例



4つのインストーラーがあります。

0001.exeと0002.exeにはデジタル署名があります



0001.exeと0002.exeは起動に成功します。

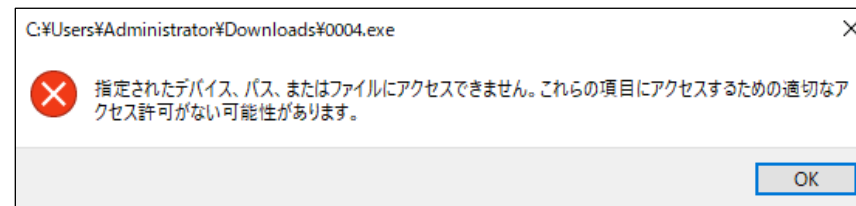
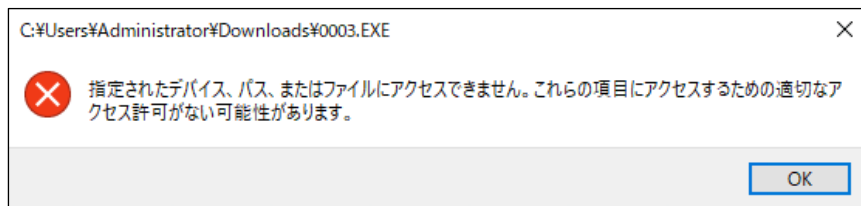


デフォルトで作成されているルール 挙動例

0003.exeと0004.exeには
デジタル署名がありません。



0003.exeと0004.exeは、起動がブロックされます。



kaspersky