kaspersky

Kaspersky
Embedded Security Systems
デフォルト拒否 許可リスト型 運用設定

2022/4/13

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

Ver. 1.3

kaspersky

目次

kaspersky

1. はじめに

1.1. 本資料の目的

Kaspersky Embedded Security Systems （以下 KESS）では、アンチウイルス機能のみでなく、デフォルト拒否・許可リスト型セキュリティの運用が可能です。
本資料では、許可リスト型セキュリティの設定について説明します。

許可リスト型セキュリティの流れは以下となります。

① Windows Embedded 上に必要な業務アプリケーションをインストール
② KESS をインストール
③ アプリケーション起動コントロールのルール作成
- ルール作成は主に 3 つの方法で行うことが出来ます。
  - ✓ 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

④ 起動コントロールタスク実行

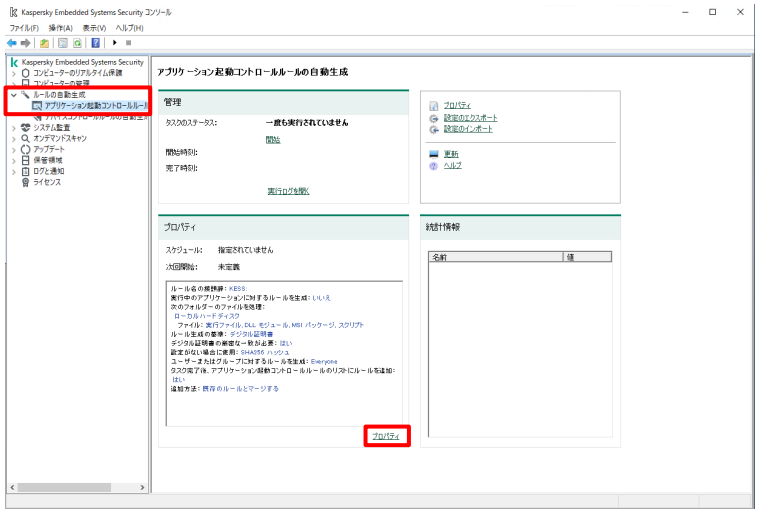
KESS をインストール後に、必要な業務アプリケーションをインストールすることも可能です。
ルールは、変更や削除が可能です。
起動コントロールのルール作成とタスク実行は、実際の作業では、前後するか、または同時に行われます。

本資料では、起動コントロールのルール作成、タスク実行について解説します。

2. アプリケーション起動コントロールルール作成

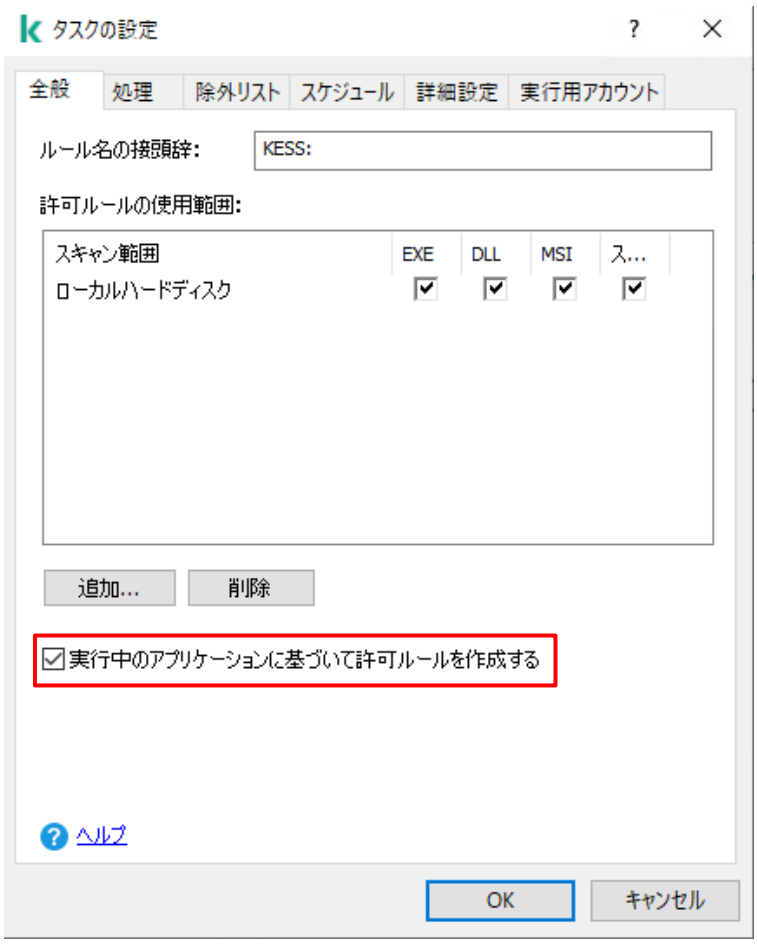
2.1. パターン①：アプリケーション起動コントロールルールの自動生成タスクからの作成

(1) 管理コンソールから「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生成」タスクを選択し、「プロパティ」をクリックします。



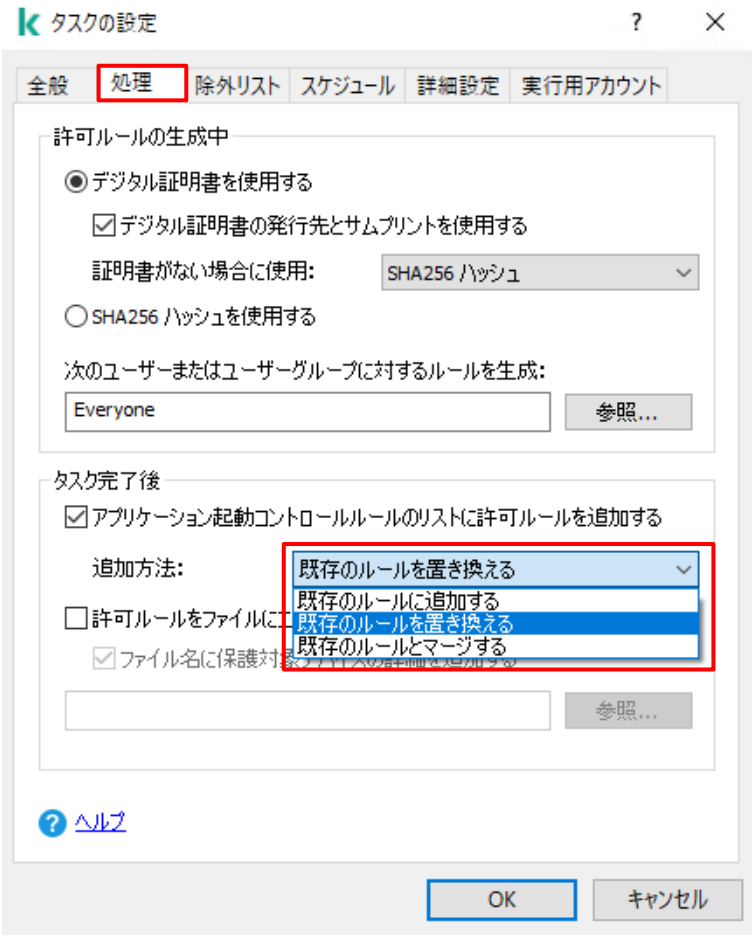
(2) 許可ルールの使用範囲を設定します。「実行中のアプリケーションに基づいて許可ルールを作成する」にチェックを入れます。

また、必要に応じてルールを自動生成するために調べるフォルダーを追加することも出来ます。



(3)「処理」タブをクリックし、許可ルールの生成及び追加方法を設定します。

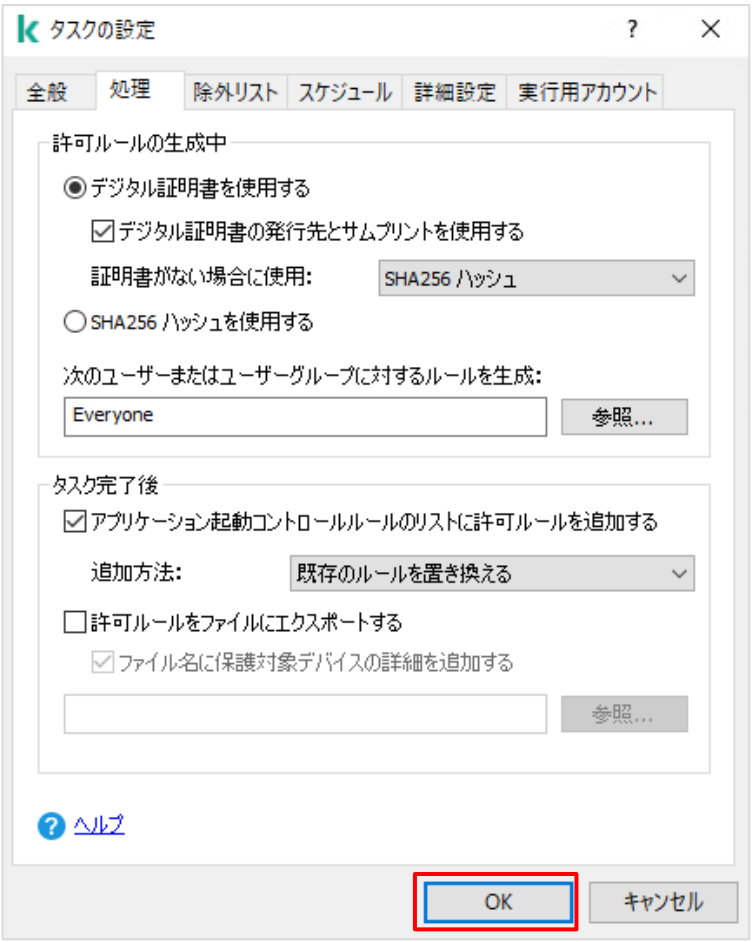
このタスクにより作成されたルールを既存ルールに追加するのか、置き換えるのか、統合するのか、選択します。
今回は初回のため、「既存のルールを置き換える」を選択します。



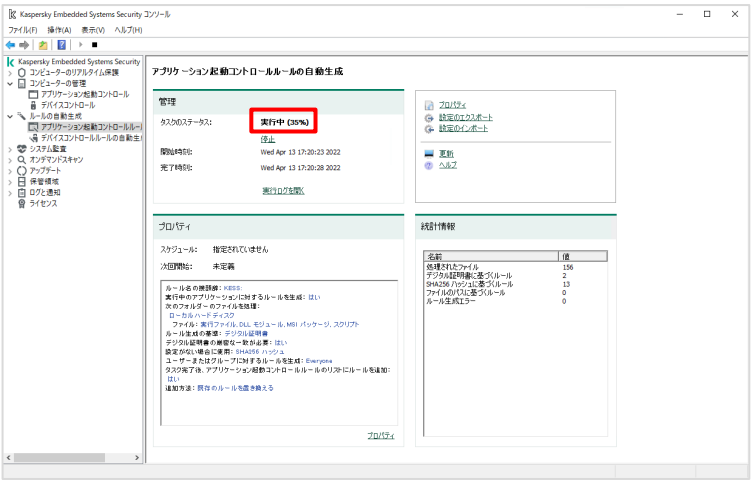
重要

デフォルトで、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）・スクリプトを許可するルールが作成されています。このルールを残したい場合は、「既存のルールとマージする」を選択してください。

(4) OK をクリックします。



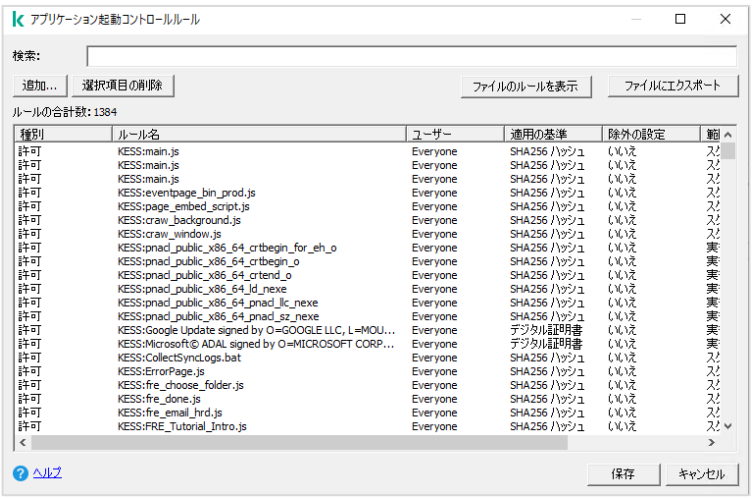
(5)「開始」をクリックし、アプリケーション起動コントロールルールの自動生成タスクを開始します。
タスクを開始すると状態が「実行中」に変わります。



(6)完了(100%)になり、完了したら「コンピューターの管理」-「アプリケーション起動コントロール」を選択します。

(7)「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。

(8)ルールが作成されていることを確認します。

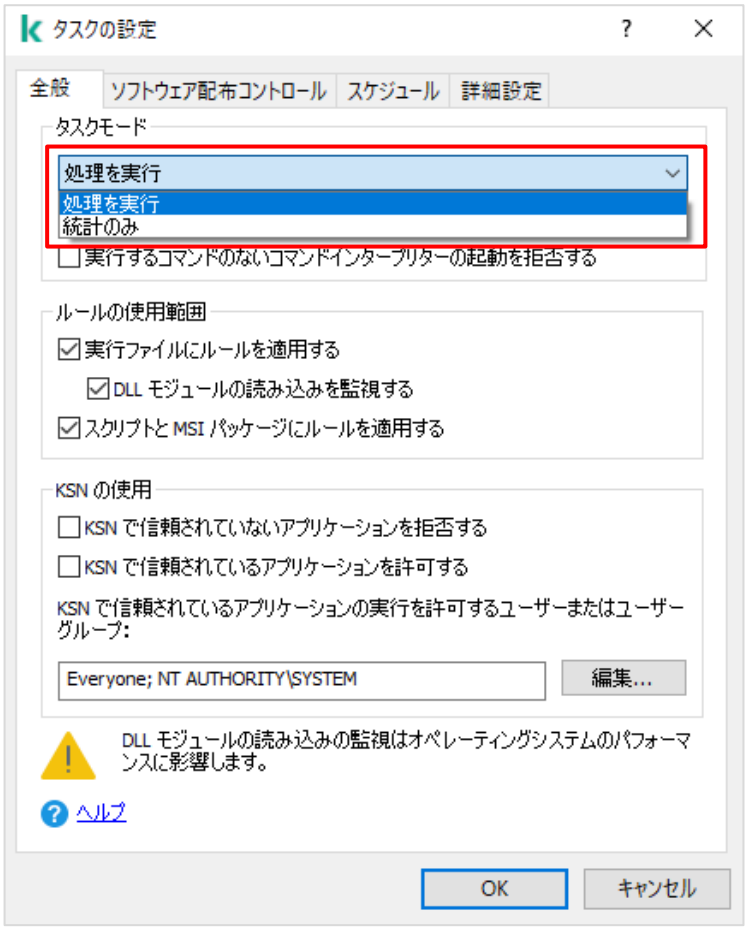


(9) アプリケーション起動コントロールタスクを、PC 起動時にスタートさせたいため、設定を変更します。
「プロパティ」をクリックします。

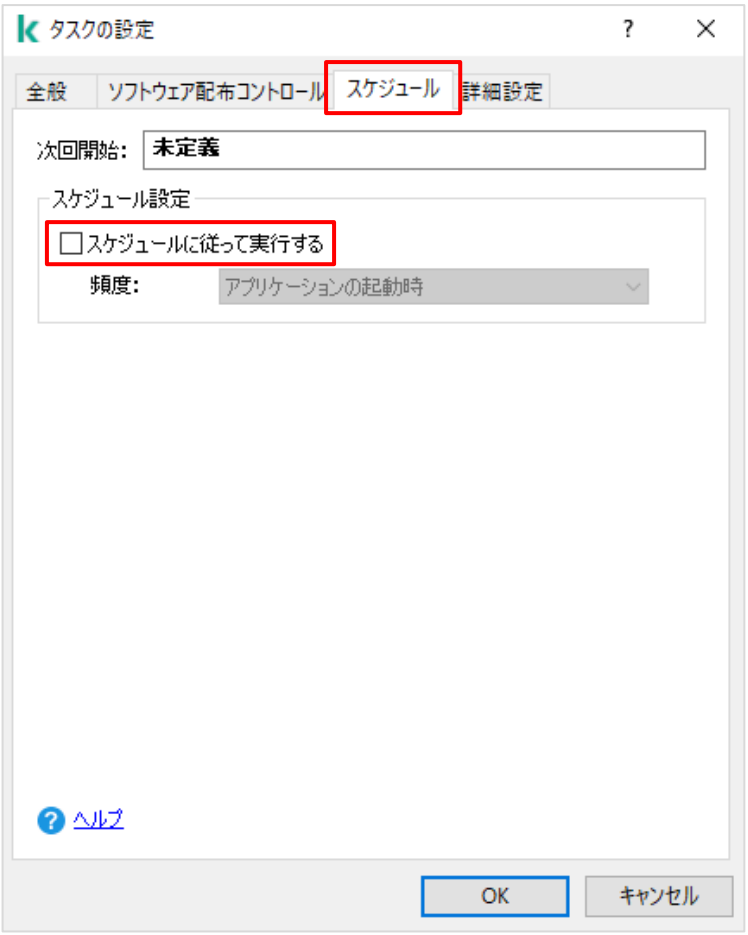
(10) タスクモードを「処理を実行」に変更します。

重要

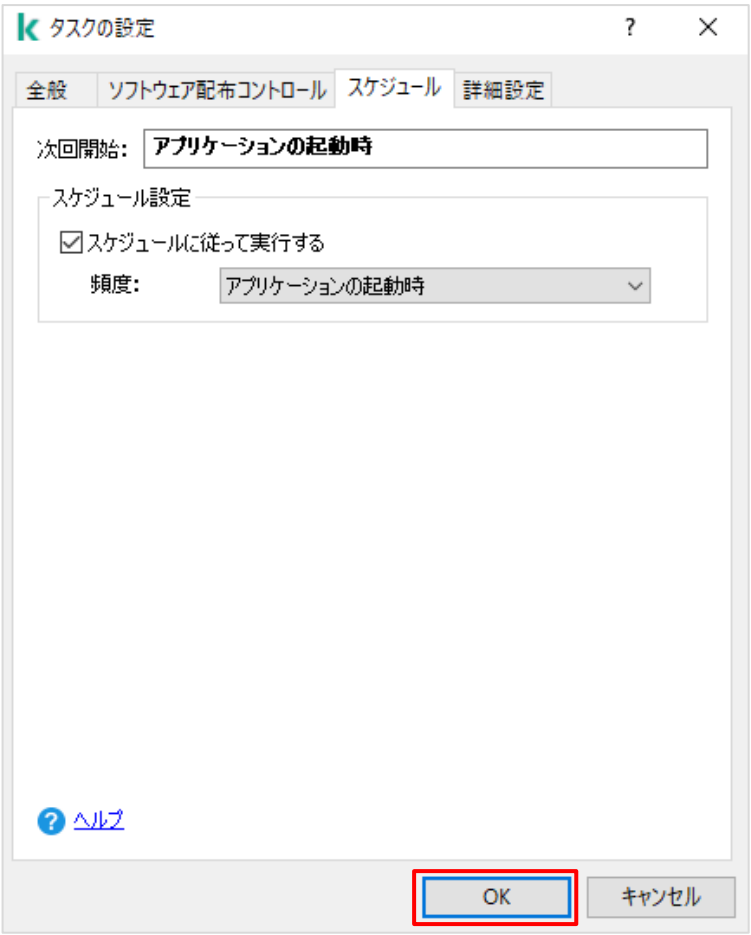
この段階でタスクモードを「統計のみ」のままでも構いません。
「統計のみ」はログに残すのみのモードです。



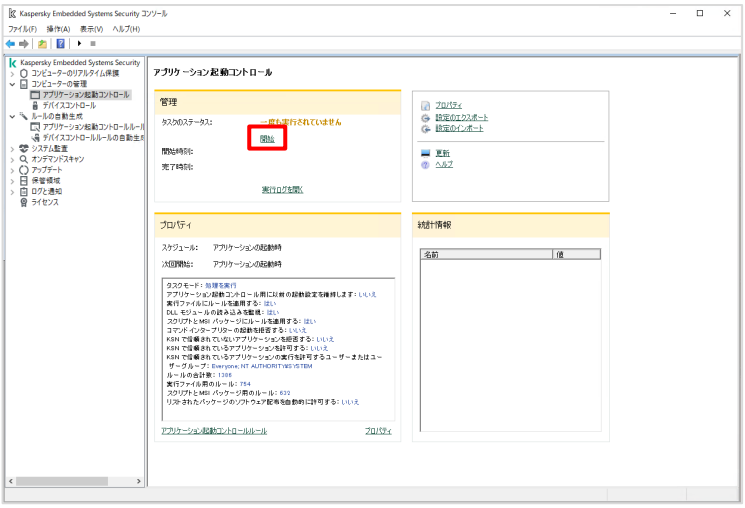
(11)　「スケジュール」タブをクリックし、「スケジュールに従って実行する」にチェックを入れます。



(12)　「OK」をクリックします。

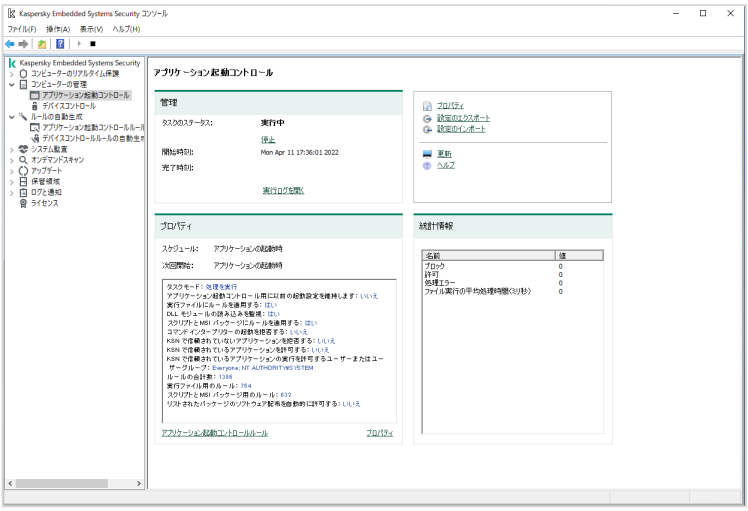


(13)　「開始」をクリックします。（再起動時には自動スタートします。）



(14)　起動されたことを確認します。

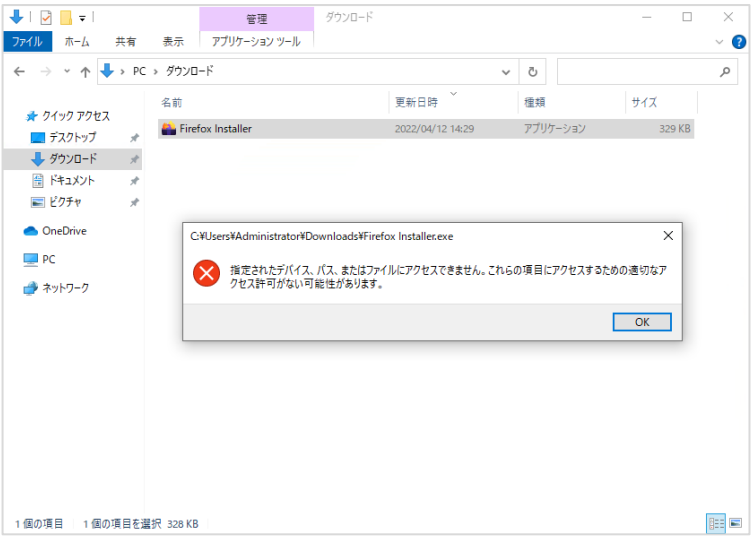
「処理を実行」モードであれば実際にブロックされ、「統計のみ」モードであればログに記録されるのみです。



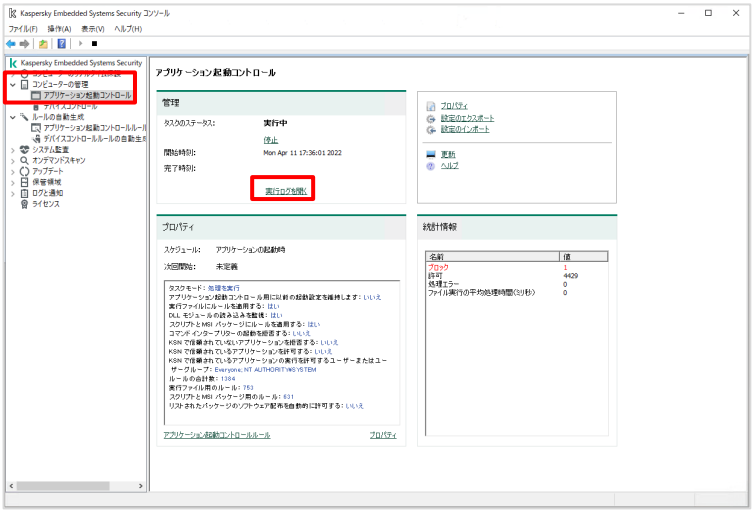
本節は以上です。

2.2. パターン②：実行ログからの作成

(1) タスクモードを「処理を実行」モードにした場合、ルールにないアプリケーションは起動できません。

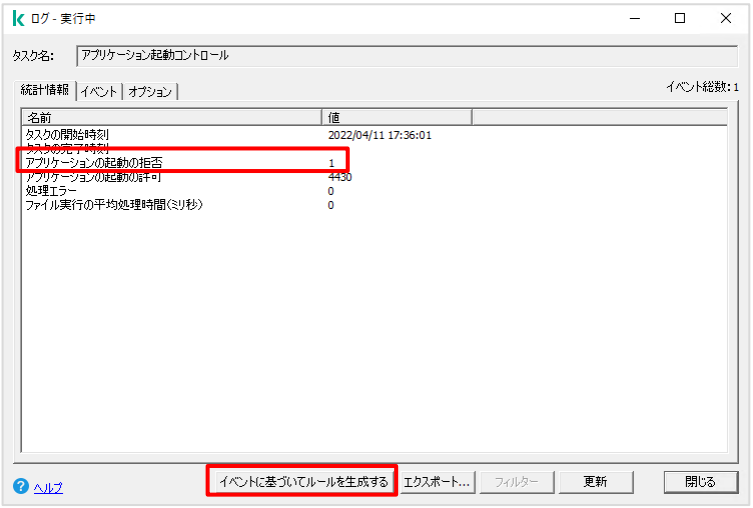


(2) 「コンピューターの管理」-「アプリケーション起動コントロール」を選択し、「実行ログを開く」をクリックします。



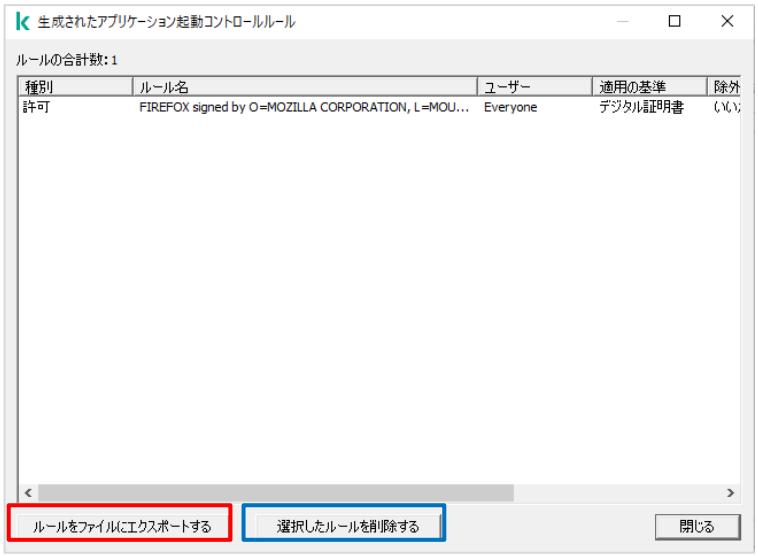
(3) 起動が拒否されたログが記録されています。「イベントに基づいてルールを生成する」をクリックします。

注）
ここでは既にルールが作成されているため、一つの拒否ログのみが記録されています。
アプリケーション起動コントロールルールの自動生成タスクによりルールを作成していなければ多数のログが記録されます。

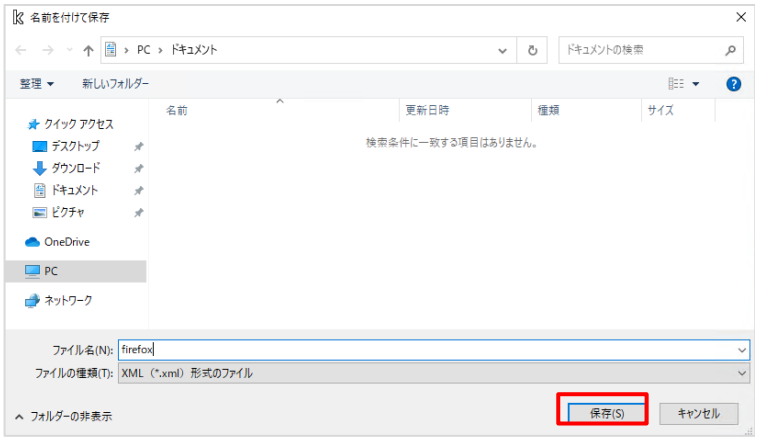


(4) 必要なルールのみを残します。
不要なルールはルールをクリックし「選択したルールを削除する」で削除します。

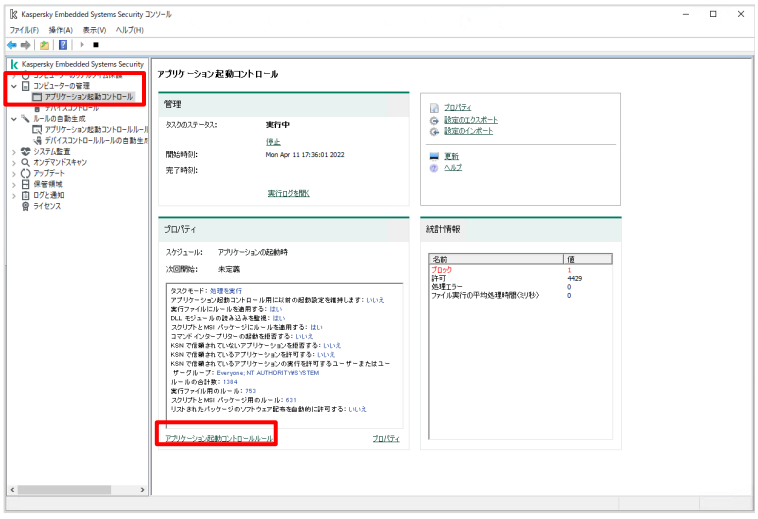
必要なルールのみを残したら、「ルールをファイルにエクスポートする」をクリックします。



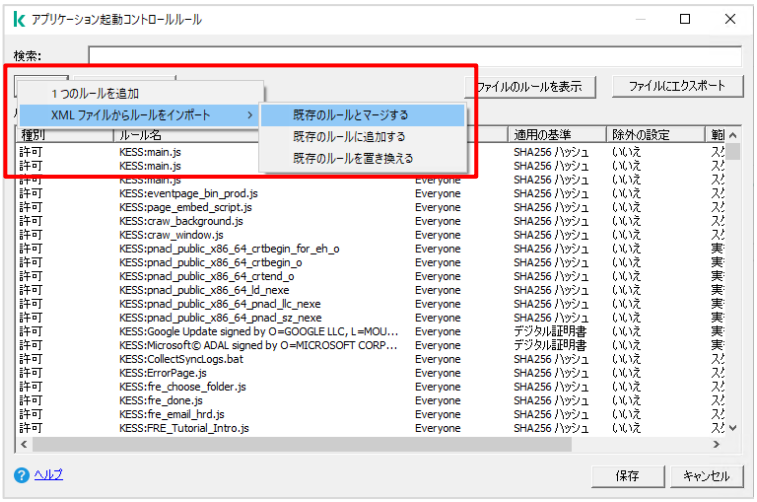
(5) 名前を付け、「保存」をクリックします。



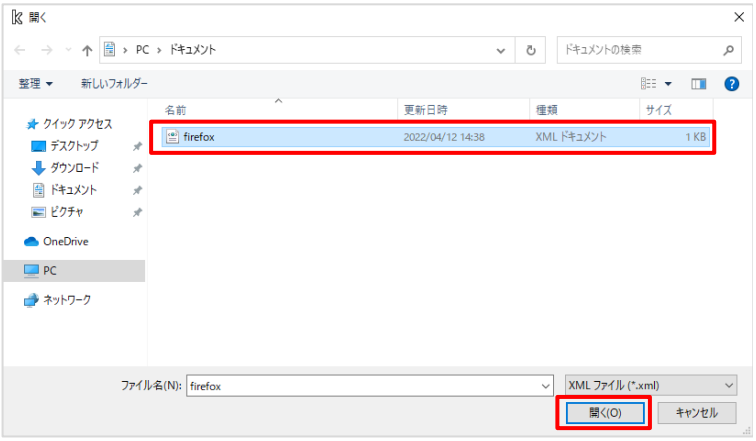
(6) 再度「コンピューターの管理」-「アプリケーション起動コントロール」を選択し、「アプリケーション起動コントロールルール」をクリックします。



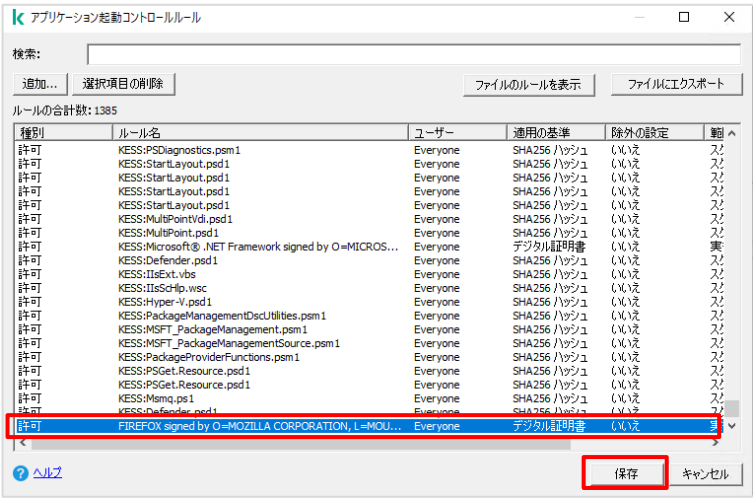
(7)「追加」をクリックし、「XML ファイルからルールをインポート」 -> 「既存のルールとマージする」を選択し、既存ルールに追加します。



(8)(５)の手順で保存した XML ファイルを指定し、「開く」をクリックします。



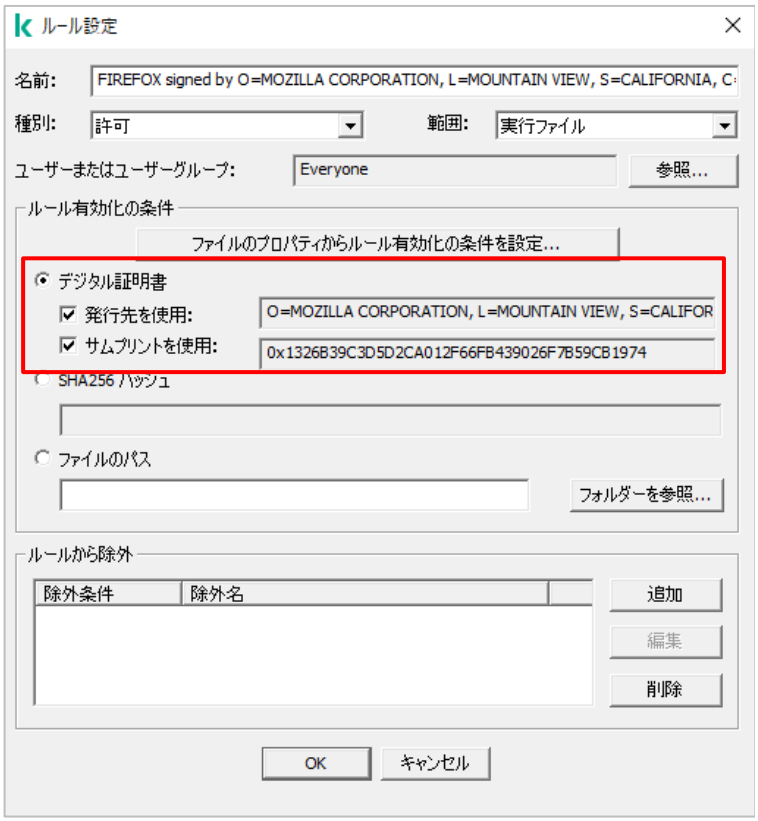
(9)ルールが追加されていることを確認します。
「保存」をクリックします。



(10)　アプリケーションが起動することを確認します。

※ **補足**

(９)で追加したルールをダブルクリックで開くと、デジタル証明書によるルールが追加されています。
そのためインストーラーだけでなく、インストール後にアプリケーションも起動可能になります。



アプリケーション起動コントロールルールを「統計のみ」モードのまま、OS 機能や業務アプリケーションを起動させ、実行ログに記録されたログからルールを作成することも可能です。

「2.1. パターン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からの作成」手順(10)-(14)のアプリケーション起動コントロールの自動起動設定と、最終的に「処理を実行」モードにすることが必要です。

本章は以上です。

kaspersky

Appendix

1. 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を許可したい場合には、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。

このルールを削除しないと、完全な許可リストになりません。

kaspersky

kaspersky

株式会社カスペルスキー

〒101-0021 東京都千代田区外神田 3-12-8 住友不動産秋葉原ビル 7F

https://www.kaspersky.co.jp/ | https://kasperskylabs.jp/biz/