Kaspersky Security Center 14
Kaspersky Endpoint Security 11
除外設定ガイド

2023/01/27

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 1.0

kaspersky

目次

1.　はじめに

1.1.　本資料の目的

Kaspersky Endpoint Security （KES）を導入すると、業務で使用しているアプリケーションやファイルがマルウェアとして検知、または、アプリケーションが意図する動作をしなくなる場合があります。
また、業務上閲覧する必要があるサイトやイントラネットのサイトがブロックされ、閲覧できない状態になる可能性があります。

本資料では、KESにて、特定のアプリケーションやフォルダー、Webサイト等をKESによる監視の対象から除外する設定についてご説明します。

以下の状態が発生した場合、または想定される場合に本資料を参考に対応を実施してください。

- **使用しているアプリケーションやファイルが検知（誤検知・過検知）した。**
- **アプリケーションメーカーより、スキャンから除外すべきフォルダー・実行ファイルの一覧が案内されている。**
- **KES 導入後、アプリケーションが正常に動作しなくなった、パフォーマンスが著しく低下した。**
- **業務遂行上必要なファイルがあり、誤検知等により削除されると問題になるファイルがある。**
  ⇒ **「2. アプリケーションの「動作(ふるまい)」に対するスキャン・監視を除外する」**
  「3. 特定のファイル・フォルダーに対するスキャン・監視を除外する」
  「4. 除外リストの継承、エンドポイント側での追加許可設定」
  を参照

- **KES 導入後、イントラネットなど、業務上閲覧する必要があるサイトがブロックされた。**
  ⇒ **「5. 特定の Web サイトに対するスキャンを除外する」を参照**

- **KES が導入されているデバイスに対し、他のデバイスから通信をすることができない。**
  ⇒ **「6. 特定の IP アドレスからの通信に対するスキャンを除外する」を参照**

- **自社ポータルなどのサイトは暗号化通信(https)をスキャンしないようにしたい。**
  ⇒ **「7. 特定のドメインや IP アドレスとの暗号化通信をスキャンしない」を参照**

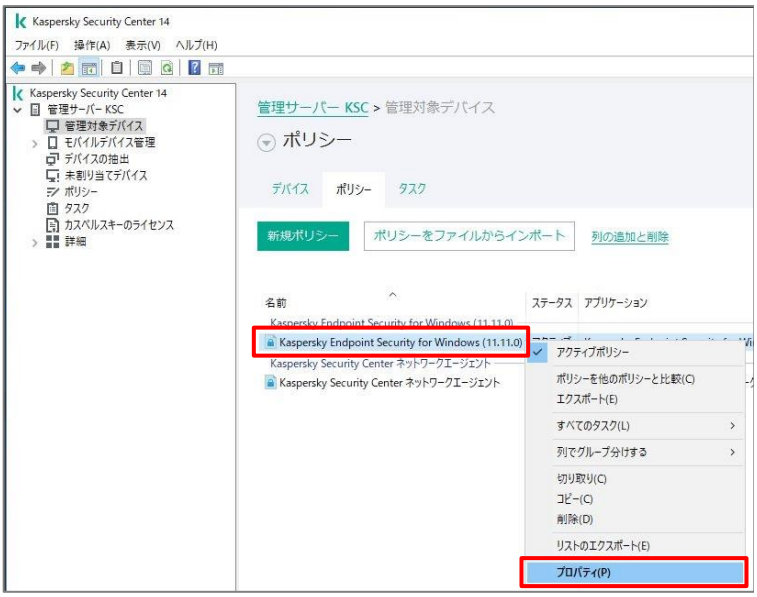
事前にこれら情報を把握し、導入前に設定することで、誤検知や過検知による運用への影響を与えずに、セキュアな環境を利用することができます。
設定は KSC にてポリシーに対し行います。基本的な設定方法は「ポリシータスク設定ガイド」をご参照ください。
法人のお客様向けダウンロード資料（https://kasperskylabs.jp/biz/）

2.　アプリケーションの「動作(ふるまい)」に対するスキャン・監視を除外する

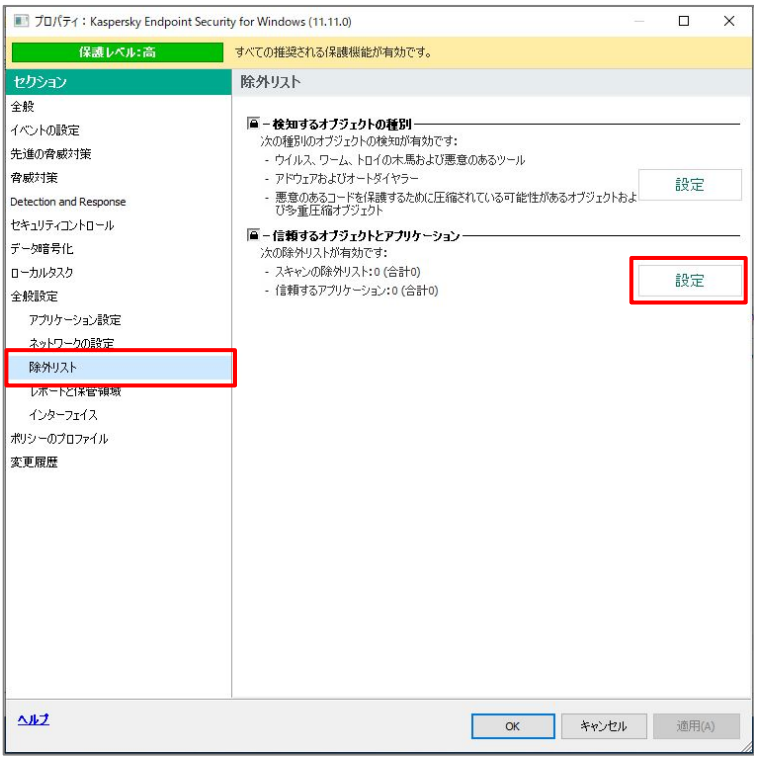
資産管理などのクライアント・サーバー型アプリケーションや自作アプリケーションなど、アプリケーションが KES に検知・ブロックされてしまう場合、実行ファイル単体ではなくアプリケーションの動作をスキャン・監視対象から除外することができます。

CAD や画像操作など、大きなサイズのファイルを扱うアプリケーションで動作が極端に遅くなった時にも、この設定が有効です。

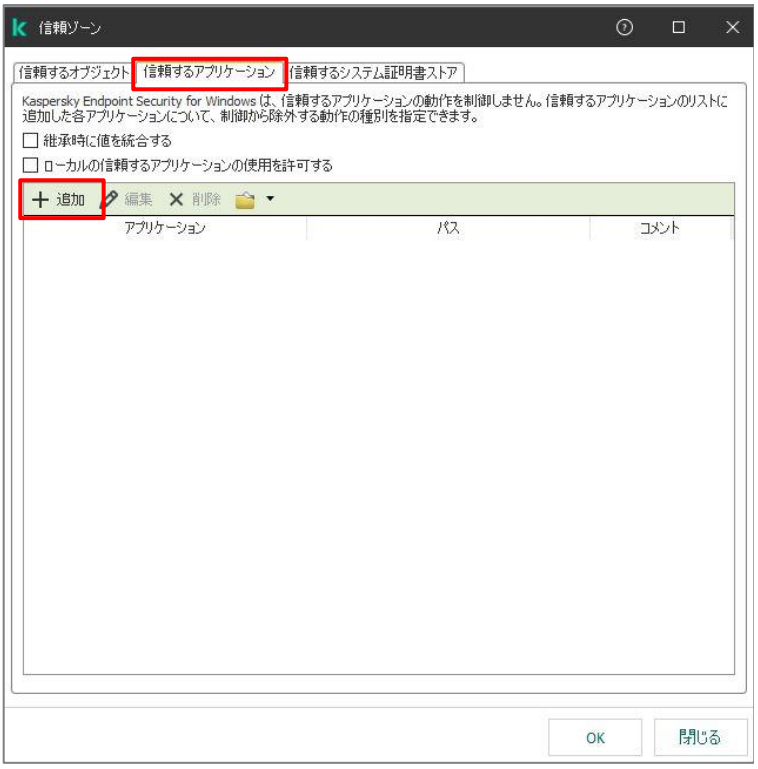
(1) 管理コンソールを開き、「管理対象デバイスにて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を選択します。



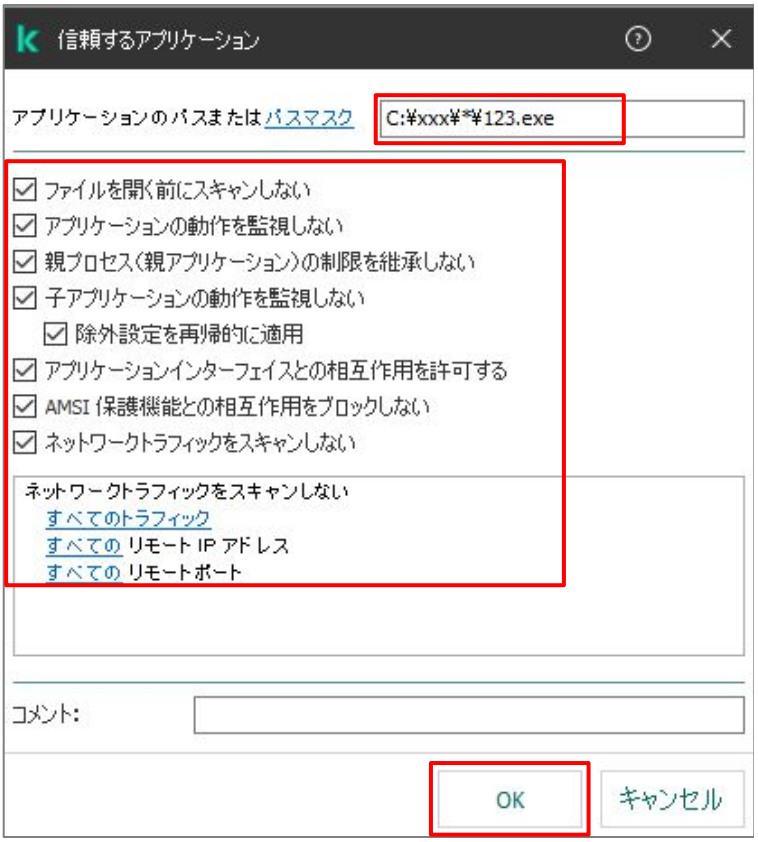
(2) 「全般設定」-「除外リスト」セクションを開き、「信頼するオブジェクトとアプリケーション」の「設定」をクリックします。



(3) 「信頼ゾーン」画面にて、「信頼するアプリケーション」タブを開き、「追加」をクリックします。



(4) 「パス」にスキャン・監視を除外したいアプリケーション（プロセス）のパスを入力し、除外する動作にチェックを入れ「OK」をクリックします。



※ **パスを入力する際、「*」や「?」を使用することができます。**

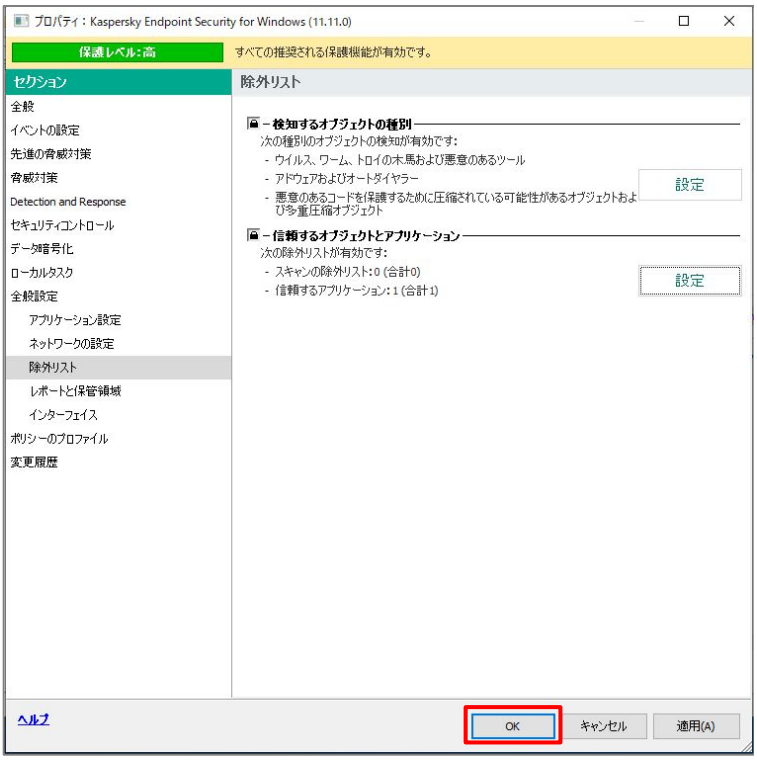
- ◆ 「C:¥test¥*.exe」とした場合、test フォルダー配下の拡張子.exe のファイルが対象となります。
- ◆ 「C:¥*¥test.exe」とした場合、C ドライブ直下にある任意のフォルダー内の test.exe が対象となります。
- ◆ 「C:¥test¥???.exe」とした場合、C:¥test フォルダー配下にある３文字のファイル名を持つ exe ファイルが対象となります。
- ◆ 「C:¥**¥test.txt」とした場合、C ドライブ配下の全階層にある test.txt が対象となります。

※ **必要に応じて各除外設定を有効にします。**

- 開いたファイルをスキャンしない
- アプリケーションの動作を監視しない
- 親プロセス(親アプリケーション)の制限を継承しない
- 子アプリケーションの動作を監視しない(除外設定を再帰的に適用)
- アプリケーションインターフェイスとの相互作用を許可する
- ASMI 保護機能との相互作用をブロックしない
- ネットワークトラフィックをスキャンしない

(5) 設定したアプリケーションが登録されている事を確認し、「OK」をクリックします。

(6) 「OK」をクリックし、ポリシーを保存します。



本章は以上です。

kaspersky

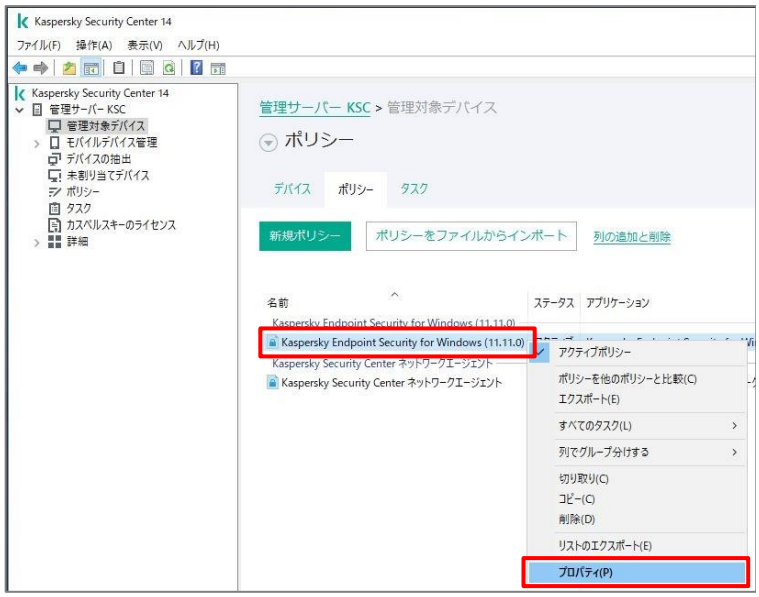
3. 特定のファイル・フォルダーに対するスキャン・監視を除外する

アプリケーションの実行ファイルや関連ファイル、または業務上 KES による検知で削除されないようにしたいファイルを、スキャン対象から除外することができます。

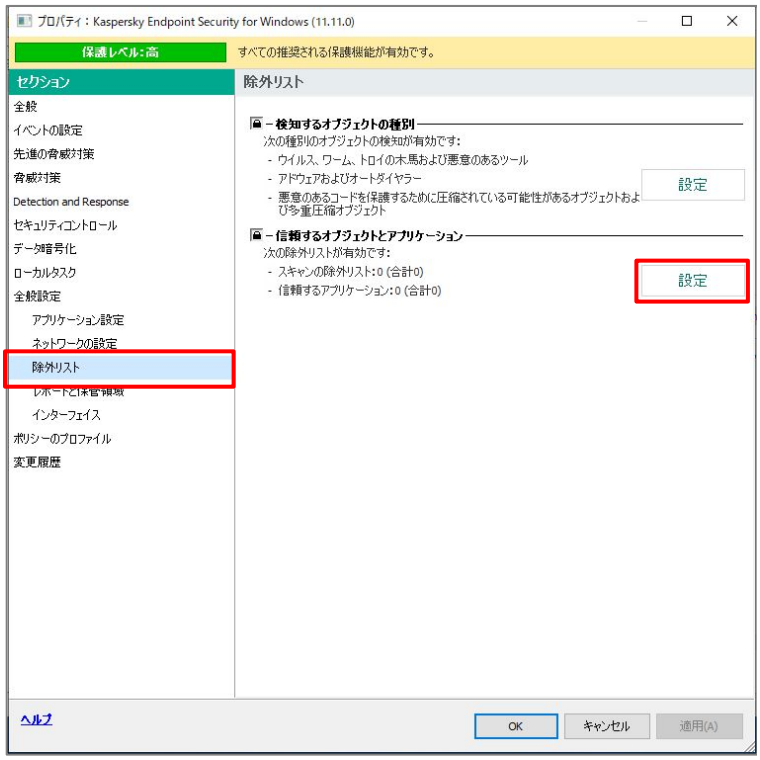
フォルダー配下に複数の除外対象ファイルがある場合、フォルダーを指定することもできます。

パスを指定せずファイル名を設定することで、どの場所にあってもそのファイル名のオブジェクトを除外対象とすることもできます。

(1) 管理コンソールを開き、「管理対象デバイスにて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を選択します。

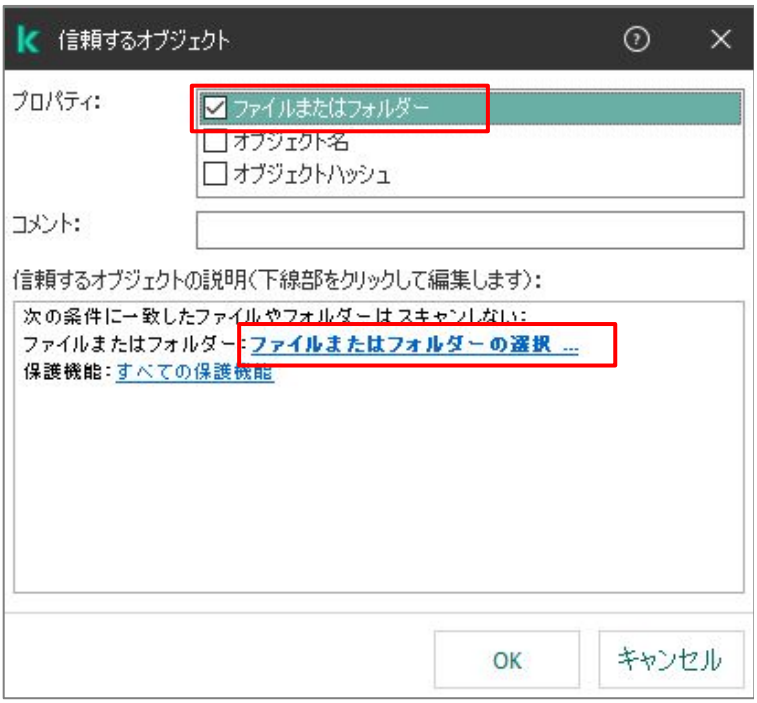


(2) 「全般設定」-「除外リスト」セクションを開き、「信頼するオブジェクトとアプリケーション」の「設定」をクリックします。

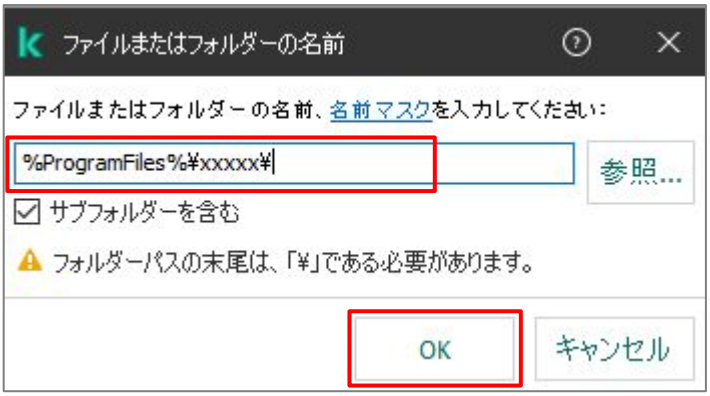


(3)「信頼ゾーン」画面にて、「信頼するオブジェクト」タブを開き、「追加」をクリックします。

(4)「ファイルまたはフォルダー」にチェックを入れ、「ファイルまたはフォルダーの選択」をクリックします。



(5)スキャンを除外したいパスを入力します。ファイルを入力する場合、ファイルまでのフルパスを入力します。
フォルダーを指定する場合、「サブフォルダーを含む」にチェックを入れ「OK」をクリックします。



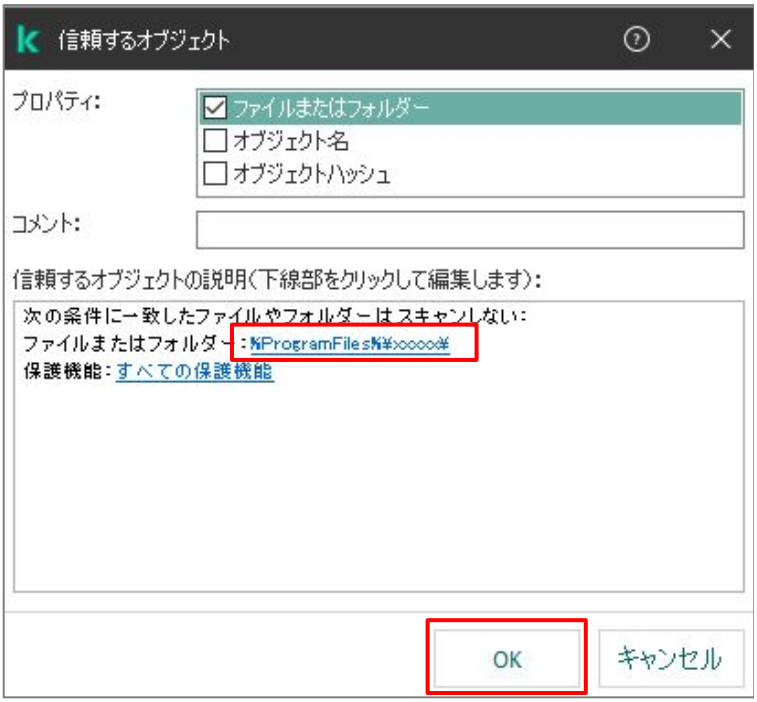
※ **フォルダーの最後に¥マークを忘れずに入れてください。**
最後に¥マークを付けないと、フォルダーとして認識されません。

※ **環境変数の指定が可能です。**
(%userprofile%は不可)

※ **パスを入力する際、「*」や「?」を使用することができます。**

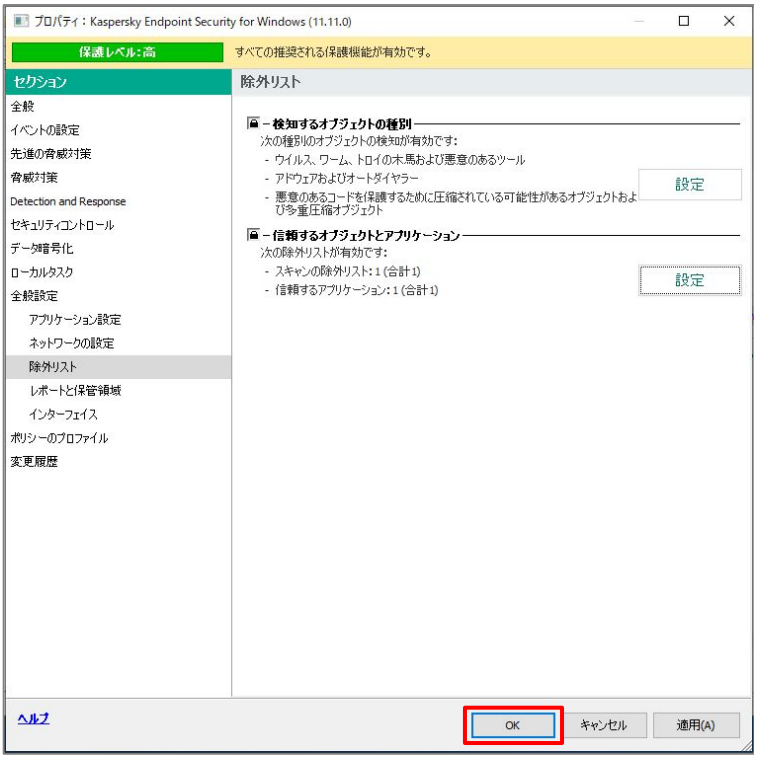
- 「C:¥test¥*.exe」とした場合、test フォルダー配下の拡張子.exe のファイルが対象となります。
- 「C:¥*¥test.exe」とした場合、C ドライブ直下にある任意のフォルダー内の test.exe が対象となります。
- 「C:¥test¥???.exe」とした場合、test フォルダー配下にある 3 文字のファイル名を持つ exe ファイルが対象となります。
- 「C:¥**¥test.txt」とした場合、C ドライブ配下の全階層にある test.txt が対象となります。

(6) 設定が表示されていることを確認し、
「OK」をクリックします。



(7) 設定したフォルダーが登録されている事を
確認し、「OK」をクリックします。

(8)「OK」をクリックし、ポリシーを保存します。



以上になります。

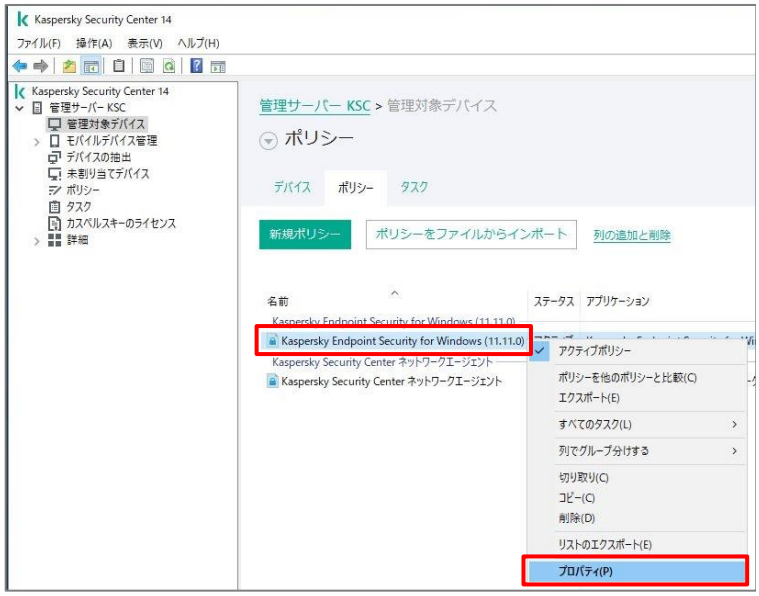
4.　除外リストの継承、エンドポイント側での追加許可設定

除外リストでは、ポリシーの継承に関する設定、ユーザーが KES 上で除外を追加できる設定があります。
各設定についてご説明します。

4.1.　除外リストの継承設定

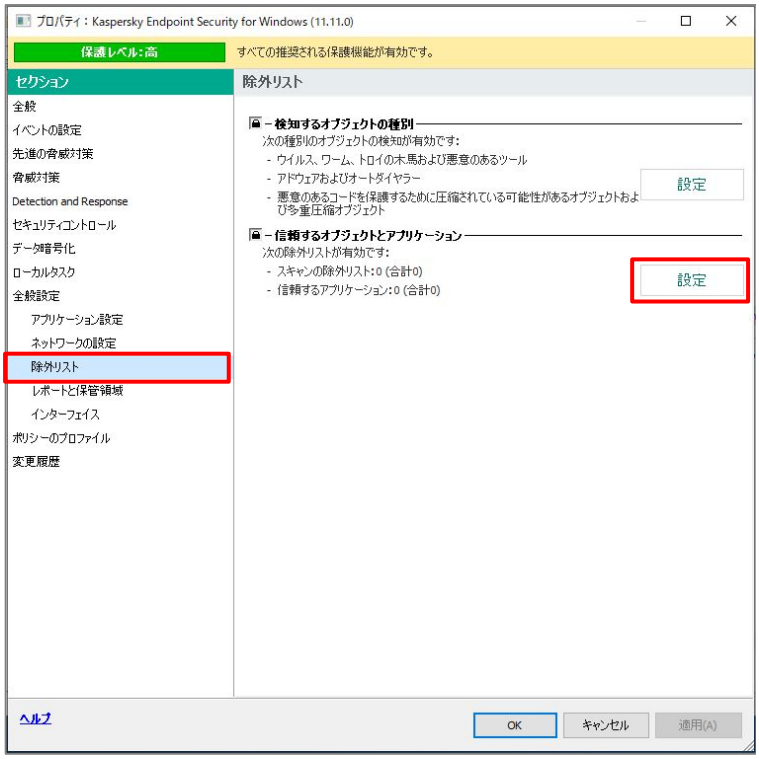
通常、グループごとにポリシーを作成し、継承を設定した場合、上位のポリシーにて設定された内容が下位のポリシーにも継承し適用されます。下位のポリシーでは内容を変更することはできません。
本設定を実施することで、上位のポリシーに設定された内容に加え、下位のポリシーでも除外設定を行うことができます。

(1) 管理コンソールを開き、「管理対象デバイスにて「ポリシー」タブを開きます。
継承元となる KES のポリシーを右クリックし、「プロパティ」を選択します。



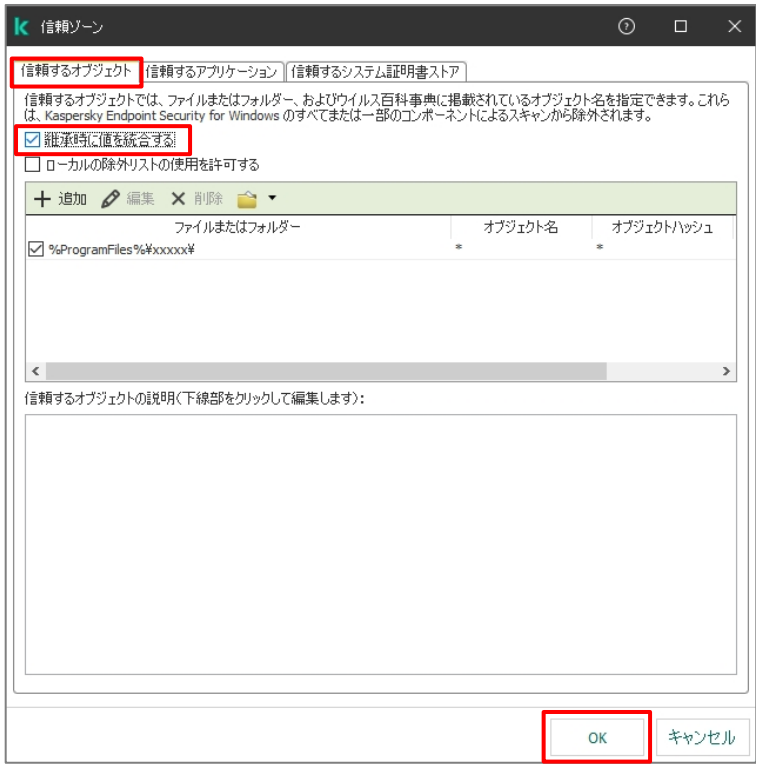
(2) 「全般設定」-「除外リスト」セクションを開き、「信頼するオブジェクトとアプリケーション」の「設定」をクリックします。

※ 「信頼するオブジェクトとアプリケーション」のロック(鍵)を無効にすると、下位のポリシーでは上位から継承されたポリシーを編集・削除することができます。

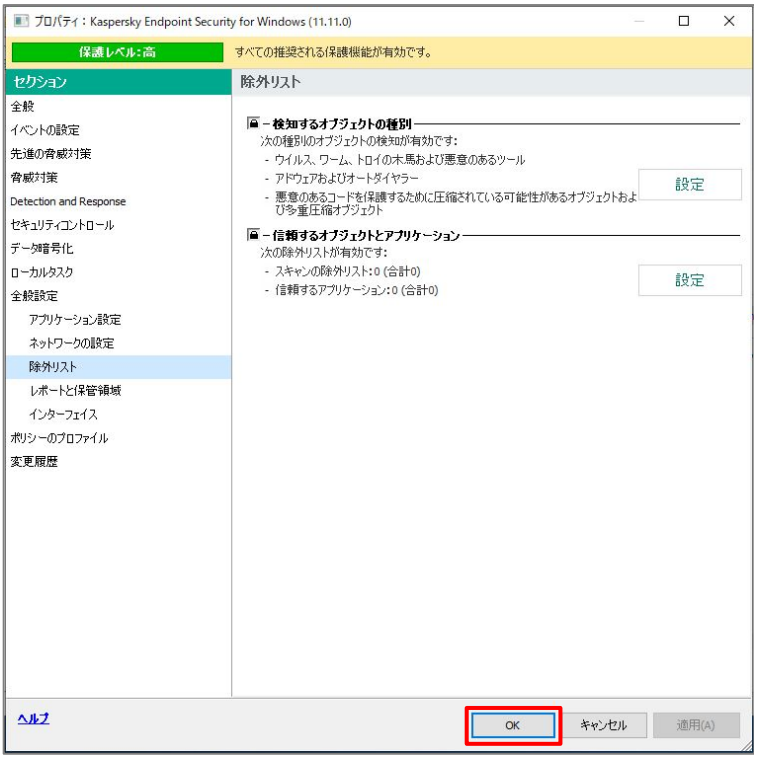


(3) 下位のポリシーに継承を設定したい除外設定タブを開きます。
（ここでは「信頼するオブジェクト」を選択しています）

「継承時に値を統合する」にチェックを入れ、「OK」をクリックします。



(4)「OK」をクリックし、ポリシーを保存します。



(5) 下位グループにてポリシーを開きます。

本設定を実施することで、上位から継承された除外設定に加え、「追加」ボタンにて除外設定を追加することができます。

本設定を実施しない場合は、「追加」ボタンはグレーアウトされクリックすることはできません。

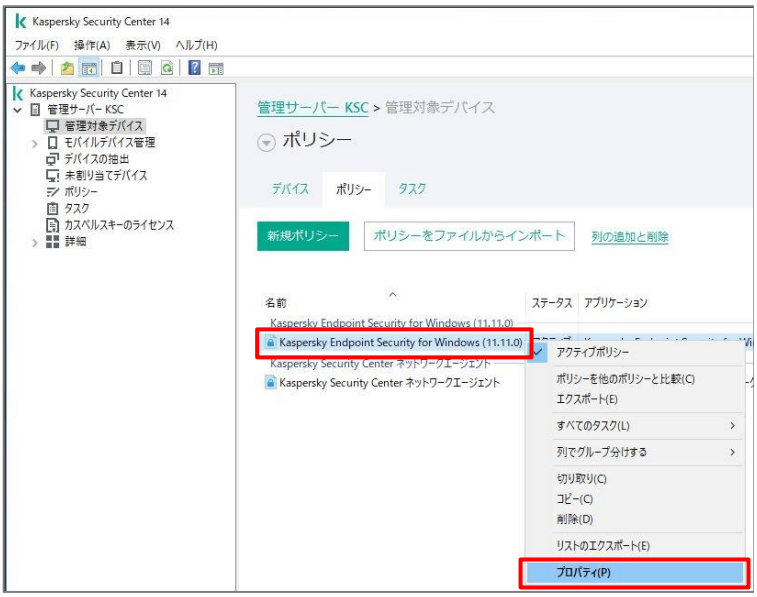
本節は以上です。

4.2. ユーザーによる除外リストの追加を許可する設定

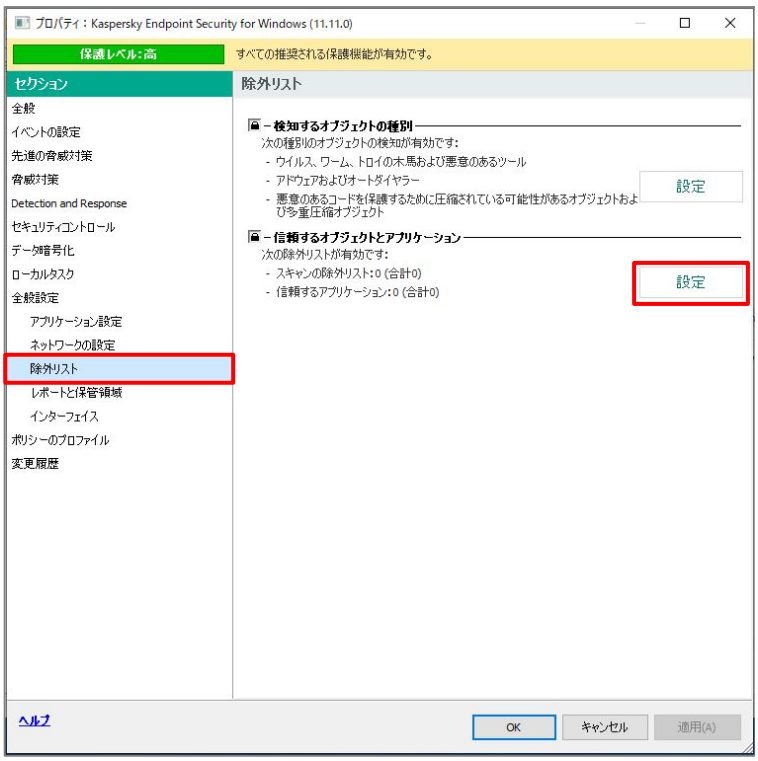
通常、ポリシーにて設定された除外リストの内容がエンドポイント側にも反映され、ユーザーは変更することができません。

本設定を実施することで、ポリシーにて設定された除外リストに加え、ユーザーが除外リストを追加することができます。

(1) 管理コンソールを開き、「管理対象デバイスにて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を選択します。

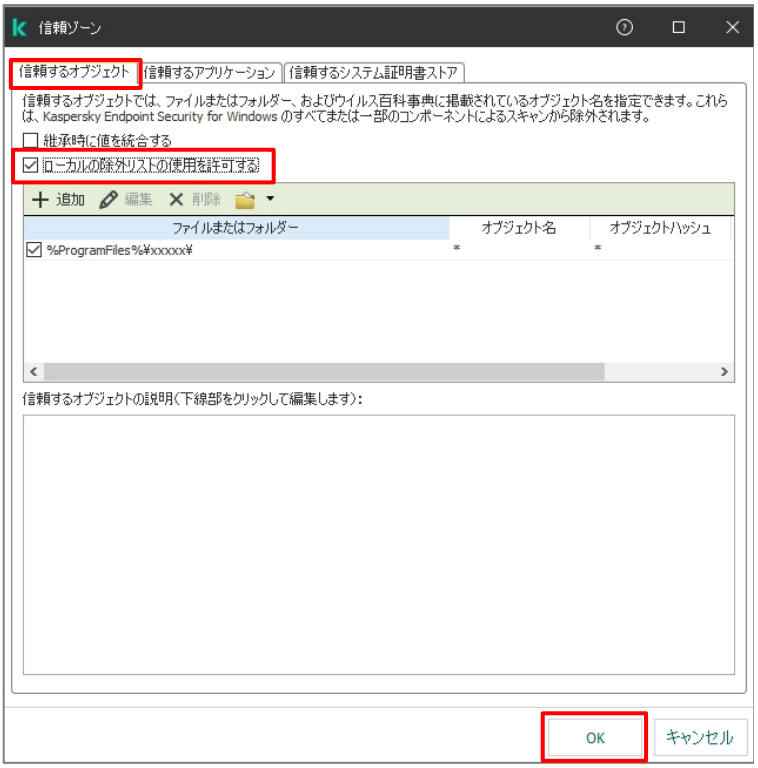


(2) 「全般設定」-「除外リスト」セクションを開き、「信頼するオブジェクトとアプリケーション」の「設定」をクリックします。

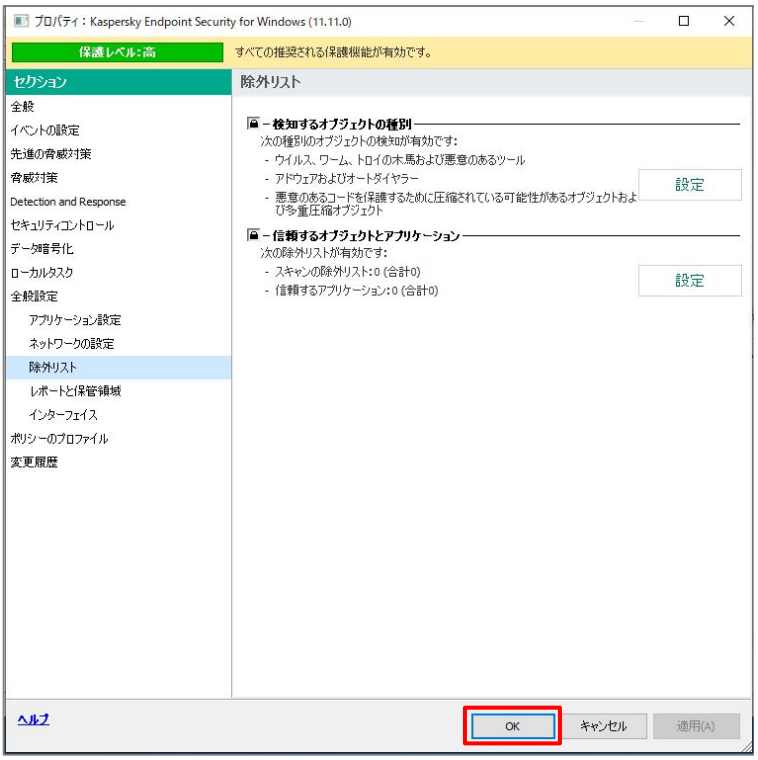


(3) ユーザーに追加を許可したい除外設定タブを開きます。
（ここでは「信頼するオブジェクト」を選択しています）

「ローカルの除外リストの使用を許可する」にチェックを入れ、「OK」をクリックします。



(4) 「OK」をクリックし、ポリシーを保存します。



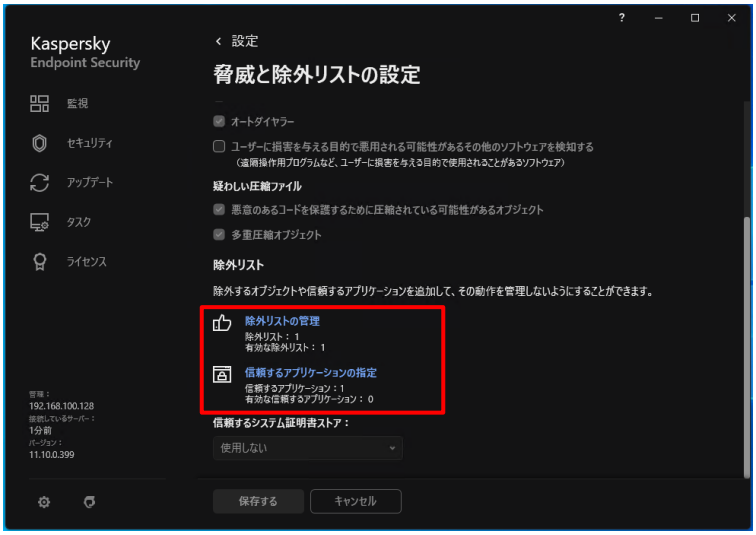
(5) クライアントデバイスにて KES のコンソールを開きます。

左下の「設定」アイコンをクリックします。

(6) 「脅威と除外リスト」をクリックします。

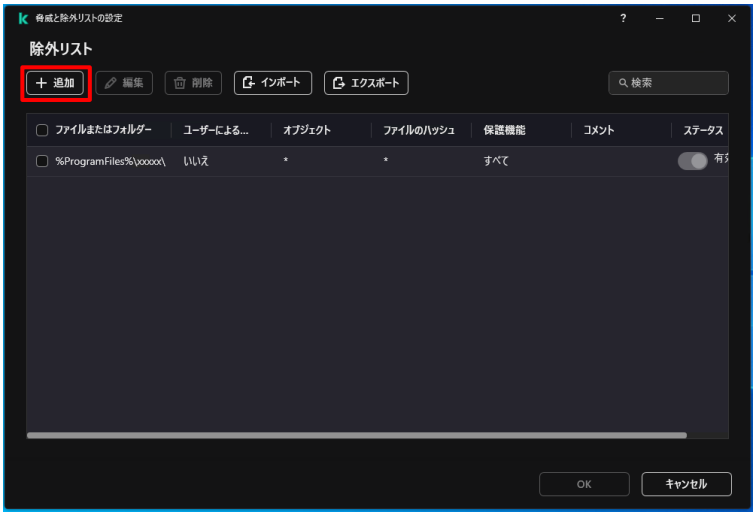
(7) 「除外リストの管理」もしくは「信頼するアプリケーションの設定」をクリックします。

ここでは「除外リストの管理」をクリックします。

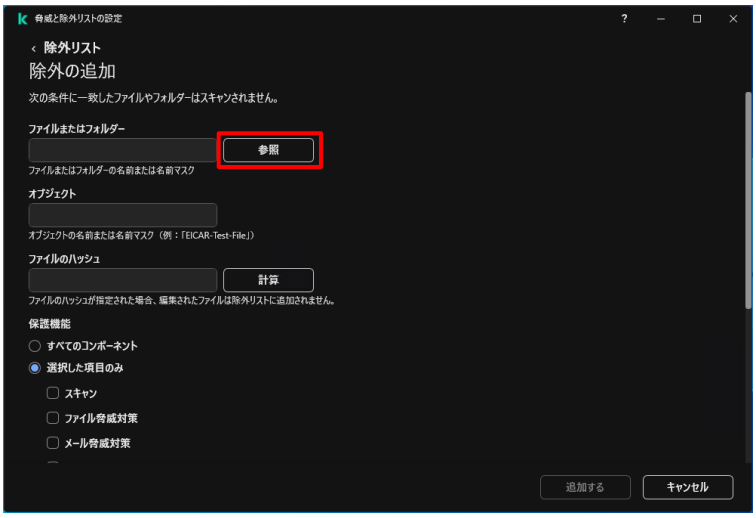


(8) リストにはポリシーにて設定された場外設定が表示されています。

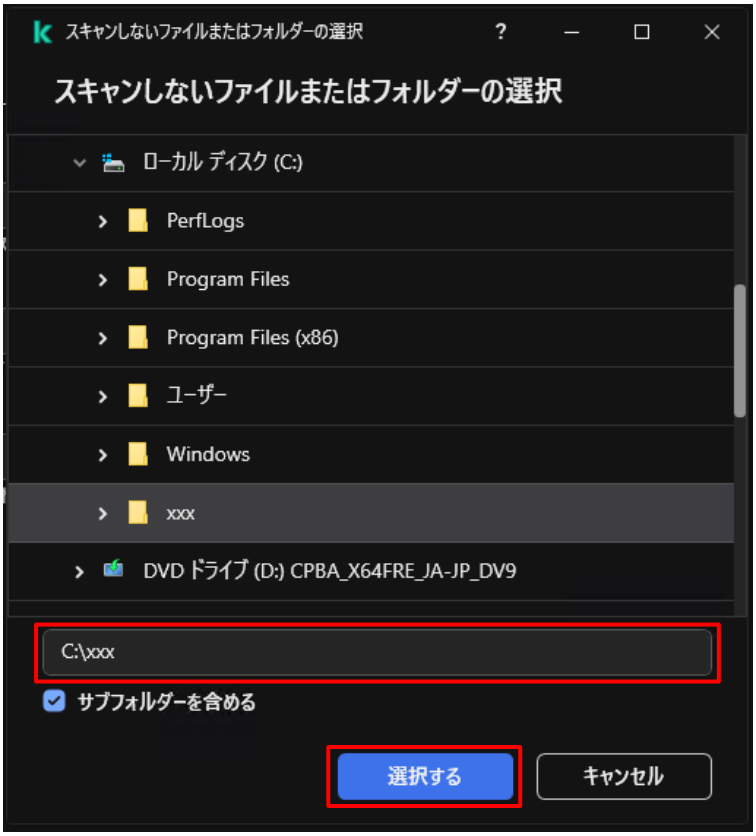
「追加」ボタンをクリックします。



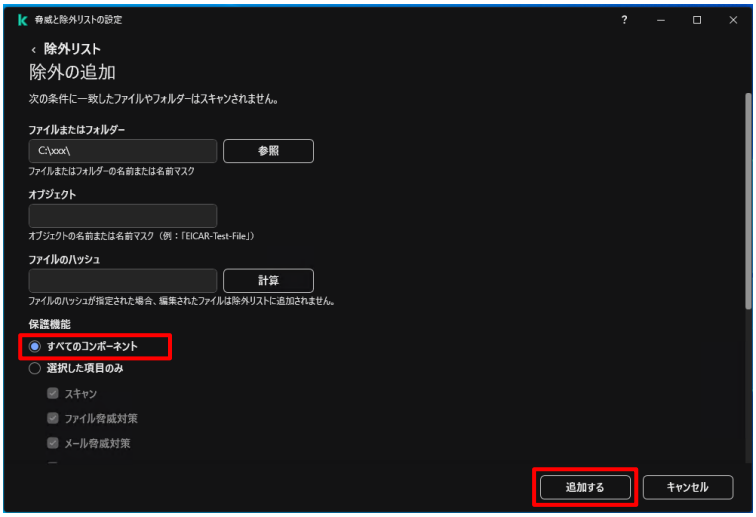
(9) 「ファイルまたはフォルダー」の「参照」ををクリックします。



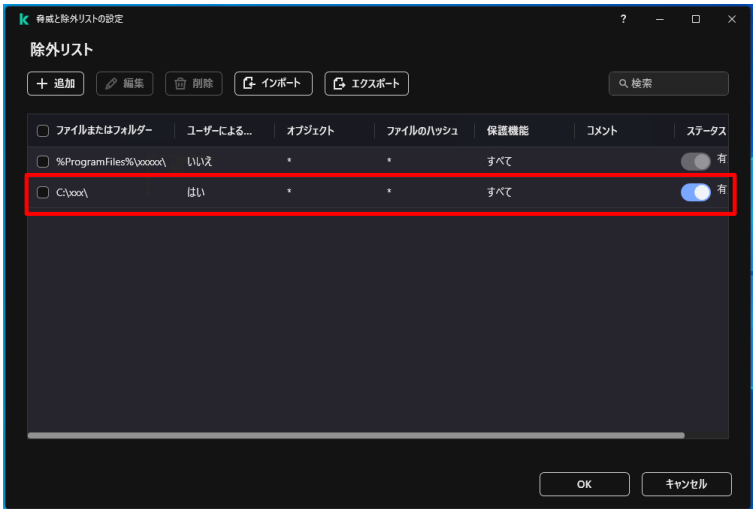
(10)　除外対象とするファイルまたはフォルダーを選択し、「選択する」をクリックします。



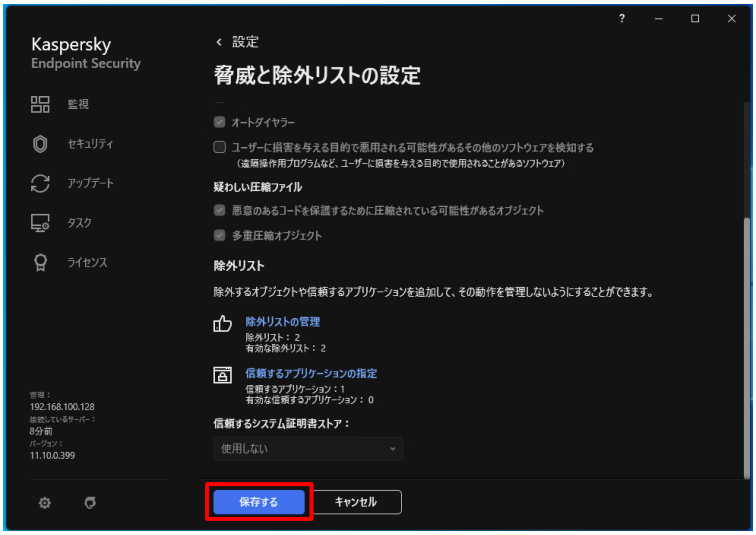
(11)　「保護機能」として「すべてのコンポーネント」にチェックを入れます。
設定後、「追加する」をクリックします。



(12)　一覧に追加した除外設定が登録されていることを確認し、「OK」をクリックします。



(13)　「保存する」をクリックし、設定を保存します。



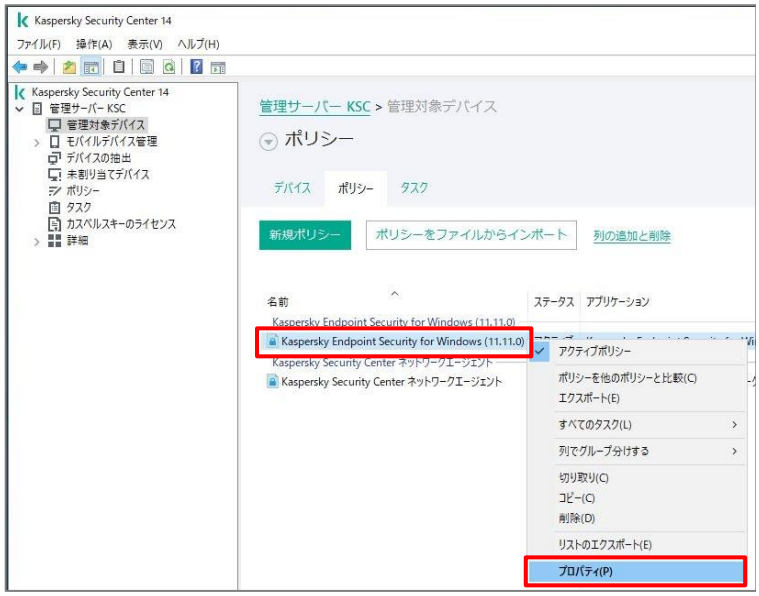
本節は以上です。

5. 特定の Web サイトに対するスキャンを除外する

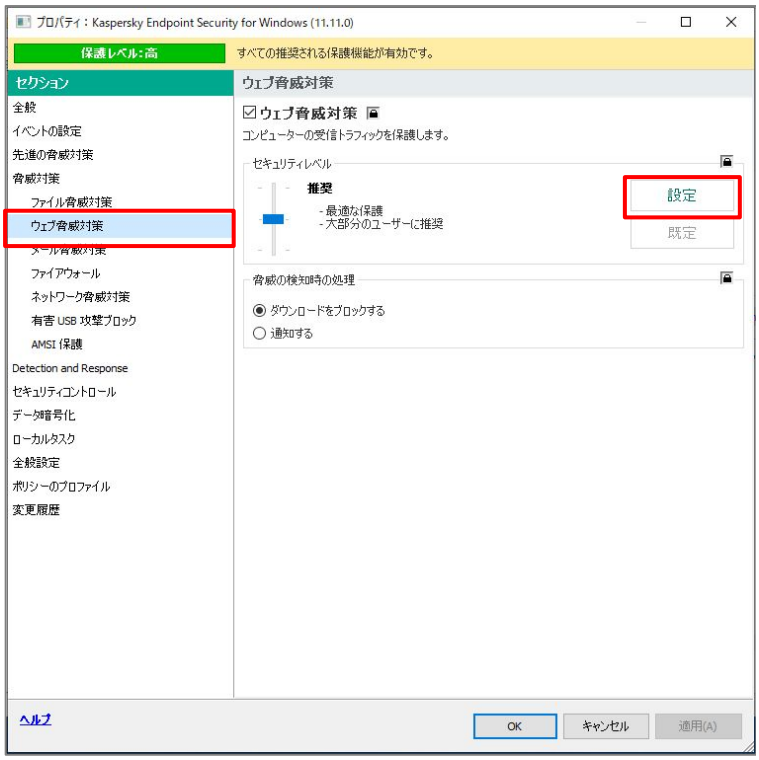
ウェブ脅威対策機能のスキャン対象から外したい Web サイトの URL を登録することができます。

イントラネットのサイトや、銀行のオンライン口座、業務上閲覧が必要なサイトをあらかじめ登録することで、KES によりブロックされることなく閲覧が可能です。

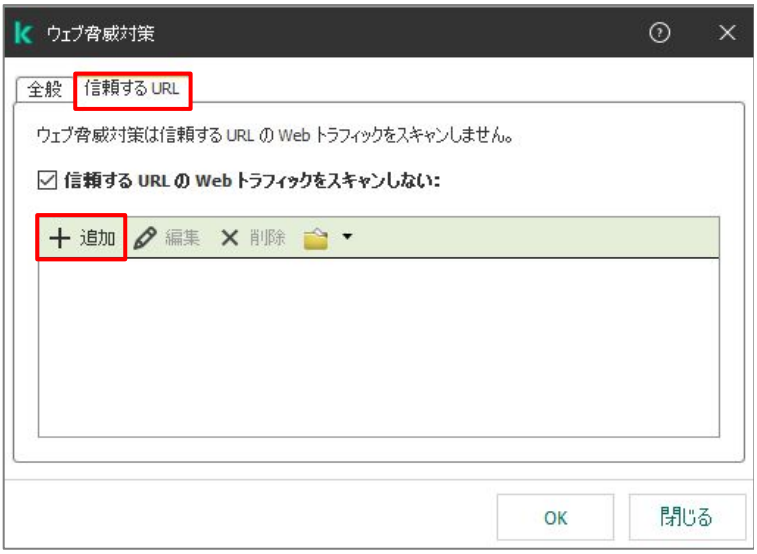
(1) 管理コンソールを開き、「管理対象デバイスにて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を選択します。



(2) 「脅威対策」-「ウェブ脅威対策」セクションを開き、「セキュリティレベル」の「設定」をクリックします。



(3) 「信頼する URL」タブを開き、「追加」をクリックします。



(4) スキャンを除外したい URL を入力し、「OK」をクリックします。

【入力規則】

以下のマスクを使用できます。

* 任意の文字列

? 任意の単一文字

例えば、

.kaspserky.co.jp/

と入力すると、以下の URL も含めて除外となります。

support.kaspersky.co.jp/

URL に「*」、「?」、「¥」、空白が含まれている場合は、それぞれの文字の前に文字「¥」を付ける必要があります。

例えば、

www.test.jp/dl.php?fl=

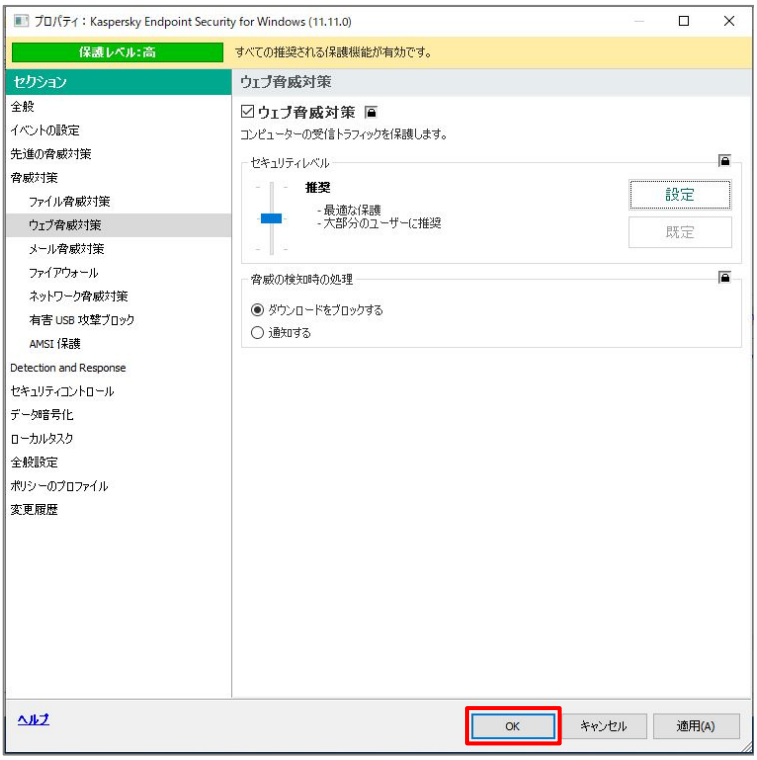
は、

www.test.jp/dl.php¥?fl=

と入力します。

(5) 一覧に URL が追加されたことを確認し、「OK」をクリックします。

(6) 「OK」をクリックし、ポリシーを保存します。

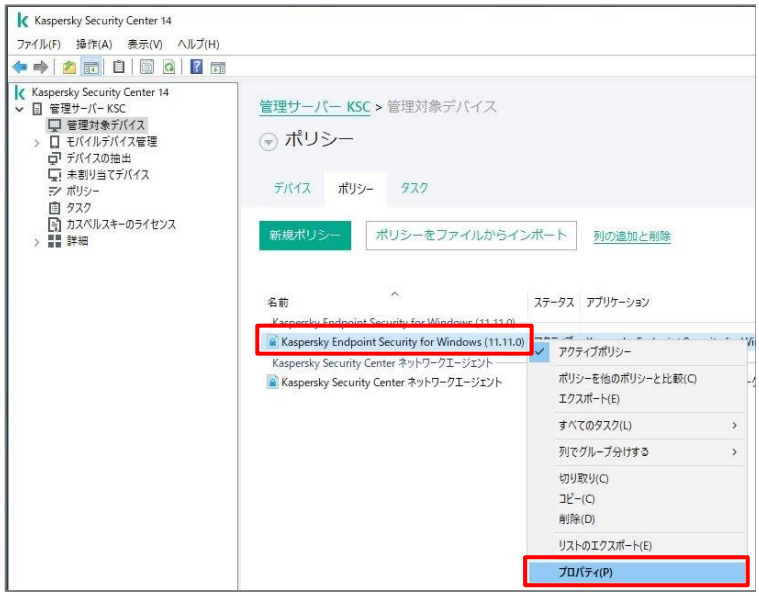


本章は以上です。

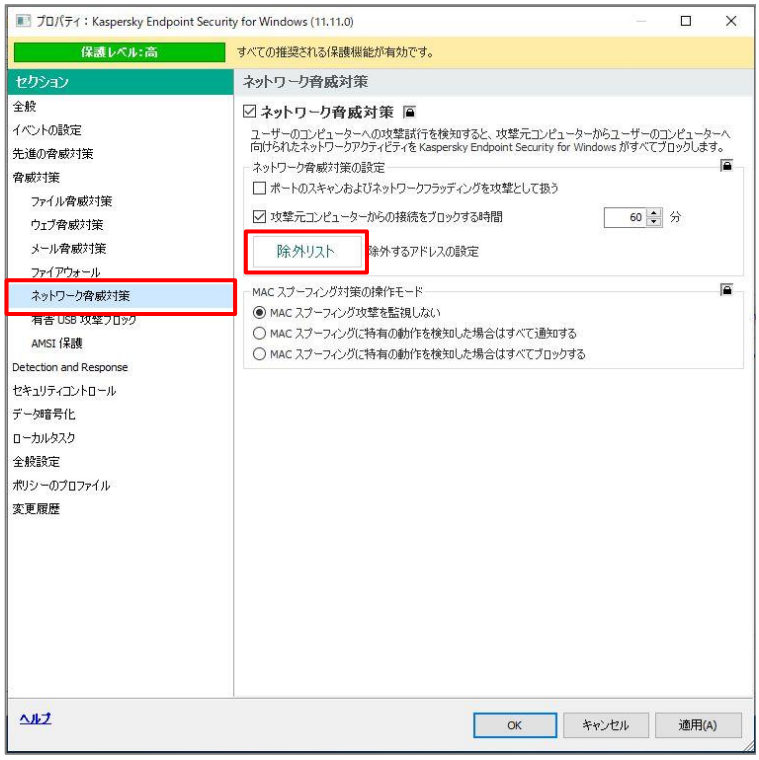
6. 特定の IP アドレスからの通信に対するスキャンを除外する

ネットワーク脅威対策機能のスキャン対象から特定の IP アドレスを除外することができます。

(1) 管理コンソールを開き、「管理対象デバイスにて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を選択します。

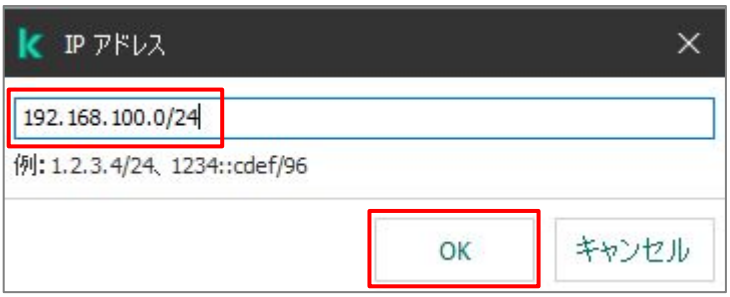


(2) 「脅威対策」-「ネットワーク攻撃防御」セクションを開き、「除外リスト」をクリックします。

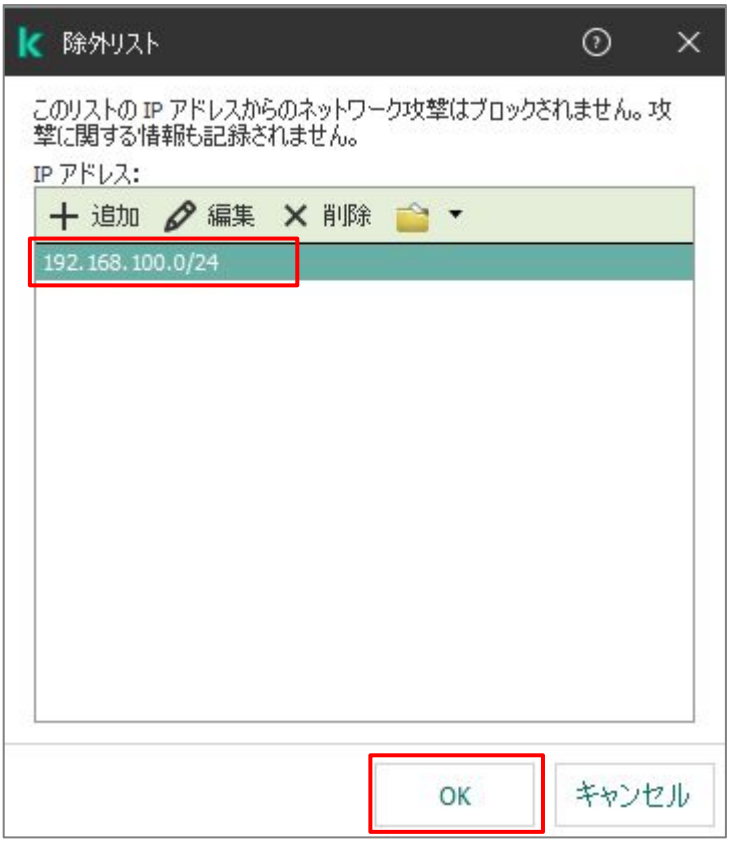


(3) 「除外リスト」画面にて「追加」をクリックします。

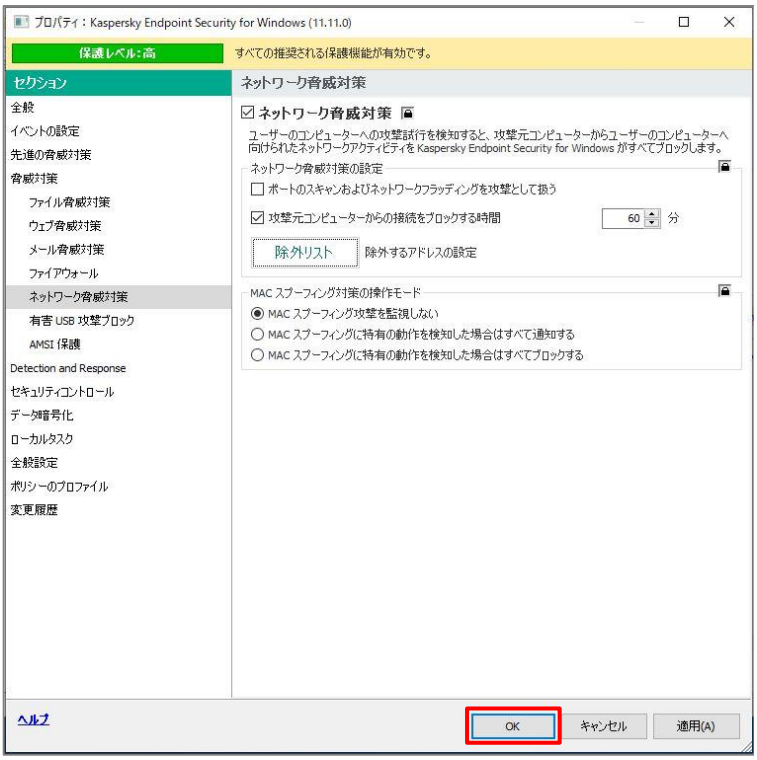
(4) ネットワークのブロックを除外したい IP アドレスを入力し、「OK」をクリックします。



(5) 追加した IP アドレスが登録されていることを確認し、「OK」をクリックします。



(6) 「OK」をクリックし、ポリシーを保存します。

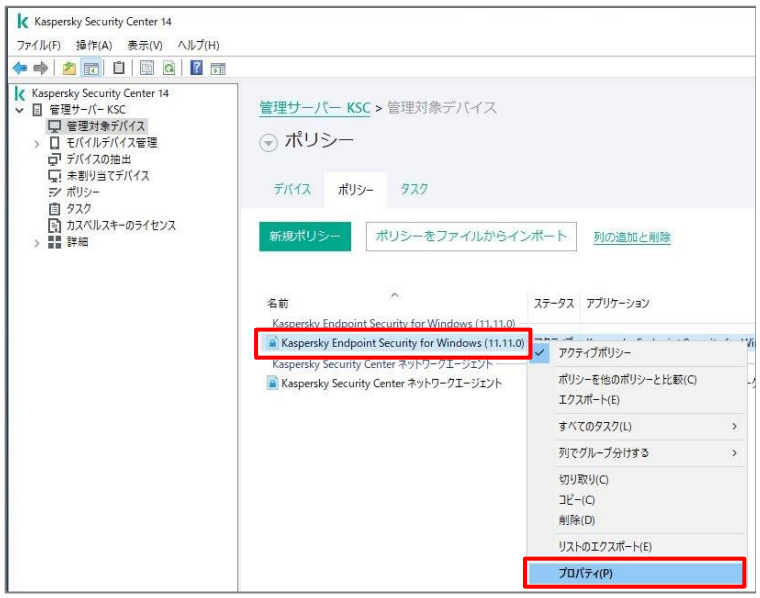


本章は以上です。

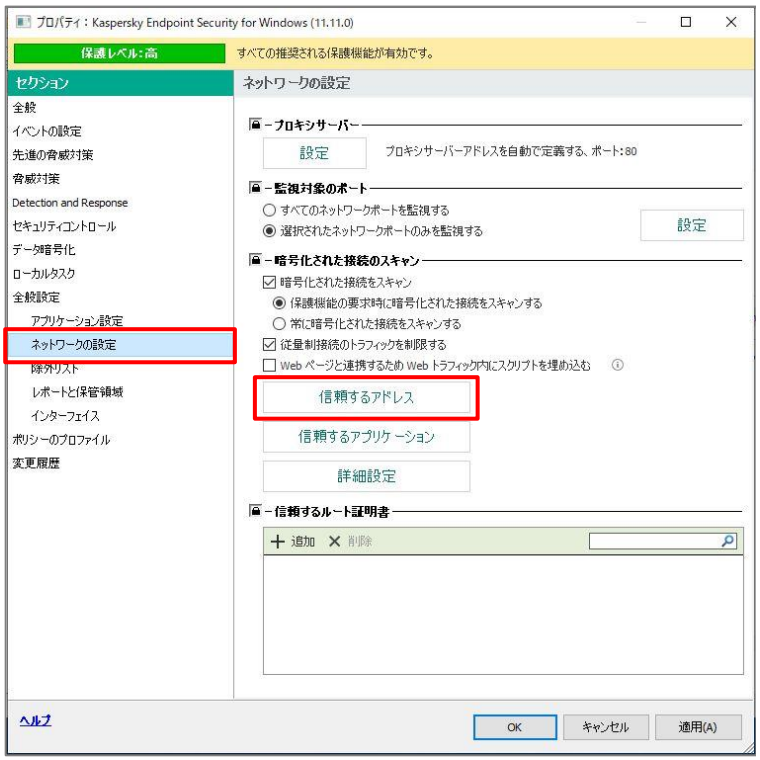
7. 特定のドメインや IP アドレスとの暗号化通信をスキャンしない

自社ポータルや特定サーバーとの暗号化通信をスキャン対象から除外することができます。
除外されるのは暗号化通信のみであり、http など暗号化されていない通信は除外されません。

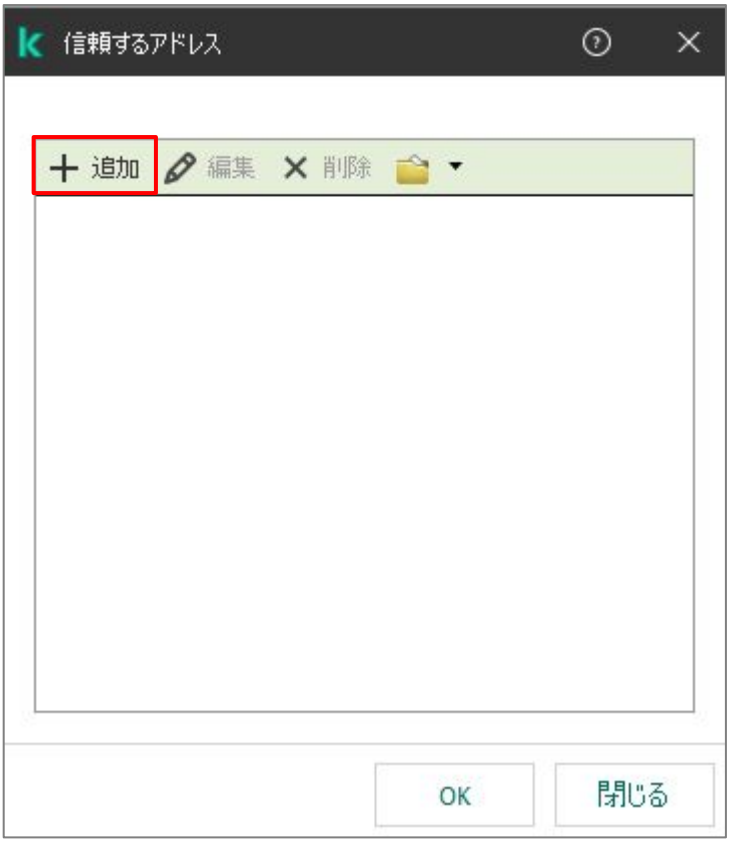
(1) 管理コンソールを開き、「管理対象デバイスにて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を選択します。



(2) 「全般設定」-「ネットワーク設定」セクションを開き、「信頼するアドレス」をクリックします。

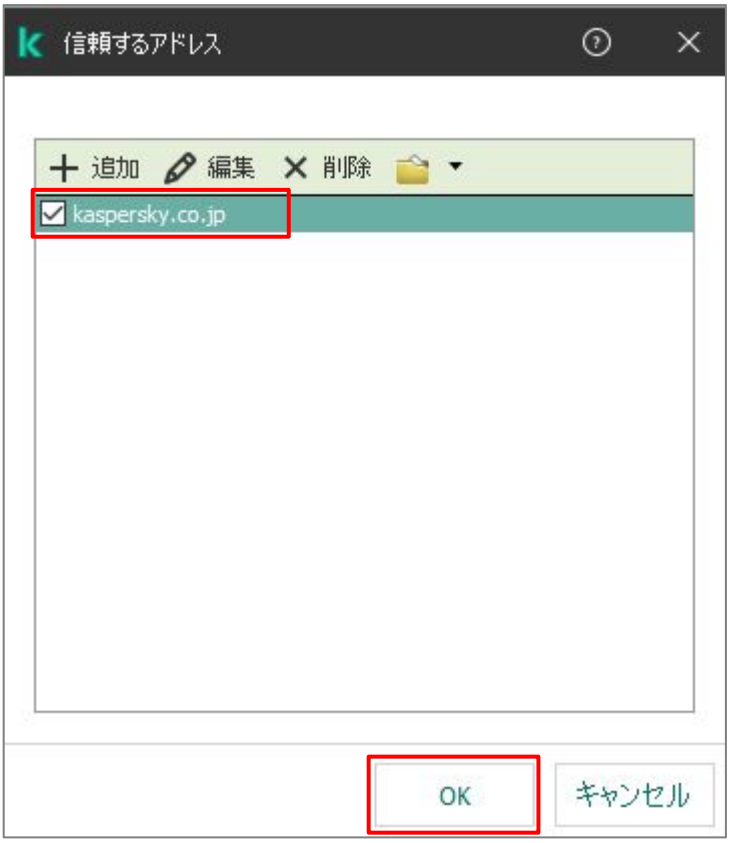


(3) 「追加」ボタンをクリックします。

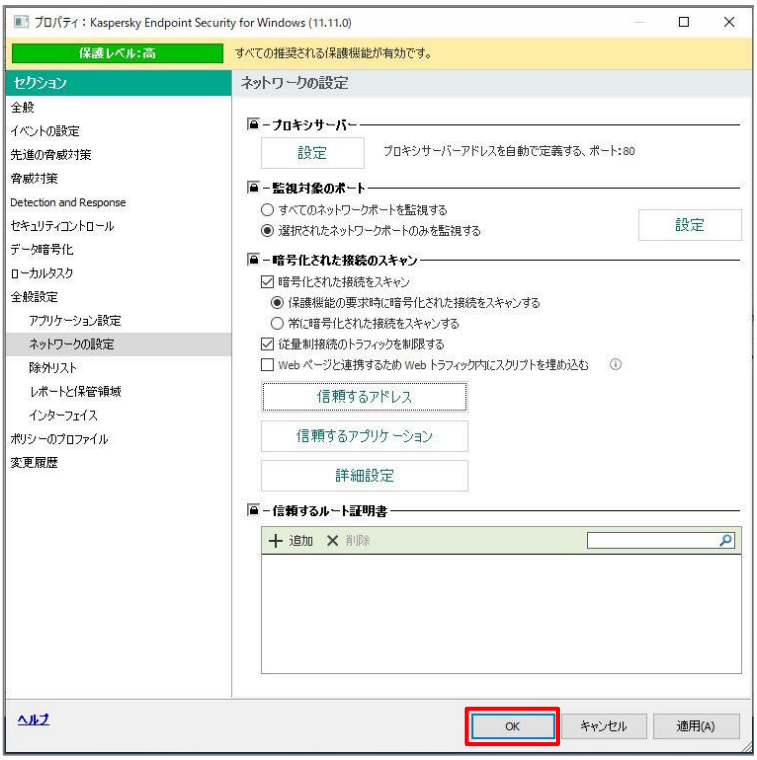


(4) 対象となるドメイン名や IP アドレスを入力し、「OK」をクリックします。

(5) 一覧に登録されていることを確認し、
「OK」をクリックします。



(6) 「OK」をクリックし、ポリシーを保存します。



本章は以上です。

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

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