

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

1.	はじめに	3
1	.1. 本資料の目的	3
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	4
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	8
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	.13
4	.1. 除外リストの継承設定	.13
4	.2. ユーザーによる除外リストの追加を許可する設定	.16
5.	特定の Web サイトに対するスキャンを除外する	.22
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	.25
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	.28

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 (<u>https://kasperskylabs.jp/biz/</u>)

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。



(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 一内の 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

🚶 信頼するアプリケーション		0 ×
アプリケーションのパスまたは <u>パスマスク</u>	C:¥xxx¥*¥123.exe	
 ファイルを開く前にスキャンしない アブリケーションの動作を監視しない 親ブロセス(親アブリケーション)の制限 子アブリケーションの動作を監視しない アブリケーションの動作を監視しない 除外設定を再別船的に適用 アブリケーションインターフェイスとの相互 AMSI 保護機能との相互作用をブロッ ネットワークトラフィックをスキャンしない ネットワークトラフィックをスキャンしない <u>すべての</u>リモート IP アドレス <u>すべての</u>リモート IP アドレス <u>すべての</u>リモート IP アドレス 	を継承しない [作用を許可する クしない	
 אַלאַב:		
	ОК	キャンセル

(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。

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。



(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。

【 ファイルまたはフォルダーの名前	0 ×
ファイルまたはフォルダーの名前、 <u>名前マスク</u> る	E入力してください:
%ProgramFiles%¥xxxxx¥	参照
🗹 サブフォルダーを含む	
🔺 フォルダーパスの末尾は、「¥」である必要が	ばあります。
0	(キャンヤル
U.	イヤノビル

(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。

ОК

キャンセル

(4)「OK」をクリックし、ポリシーを保存します。

- III プロパティ: Kaspersky Endpoint Security for Windows (11.11.0) X 保護レベル:高 すべての推奨される保護機能が有効です。 セクション 除外リスト 全般

 後知するオブジェクトの種別
 次の種別のオブジュクトの種別
 、かの種別のオブジュクトの検知が有効です:
 ・ウイルス、ワーム、トロイの木馬および悪意のあるツール
 ・アドウェアおよびオートダイヤラー

 イベントの設定 先進の脅威対策 脅威対策 設定 悪意のあるコードを保護するために圧縮されている可能性があるオブジェクトおよ び多重圧縮オブジェクト Detection and Response セキュリティコントロール 一 信頼するオブジェクトとアプリケーション 次の除外リストが有効です: デーな暗号化 - スキャンの除外リスト:0(合計0) ローカルタスク 設定 - 信頼するアプリケーション:0(合計0) 全般設定 アプリケーション設定 ネットワークの設定 除外リスト レポートと保管領域 インターフェイス ポリシーのプロファイル 変更履歴 AN7 キャンセル 適用(A) OK 🚶 信頼ゾーン 信頼するオブジェクト(信頼するアプリケーション)(信頼するシステム証明書ストア) 信頼するオブジェクトでは、ファイルまたはフォルダー、およびウイルス百科事典に掲載されているオブジェクト名を指定できます。これら は、Kaspersky Endpoint Security for Windows のすべてまたは一部のコンポーネントによるスキャンから除外されます。 ☑ 維承時に値を統合する ローカルの除外リストの使用を許可する 🕂 追加 🖉 編集 🗙 削除 🚞 🔻 ファイルまたはフォルダー オブジェクト名 オブジェクトハッシュ %ProgramEiles%¥xxxxx¥ C:¥test¥ < 信頼するオブジェクトの説明(下線部をクリックして編集します): 次の条件に一致したファイルやフォルダーはスキャンしない: ファイルまたはフォルダー:○<u>¥test¥</u> 保護機能:<u>すべての保護機能</u> ОК キャンセル
- (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。



(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。

「保存する」をクリックし、設定を保存



本節は以上です。

(13)

します。

kaspersky 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、銀行のオンラインロ座、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。



(3)「信頼する URL」タブを開き、「追加」をクリ く ウェブオ 成対策 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。

kaspersky 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。



(3)「除外リスト」画面にて「追加」をクリックしま

す。

	撃に関 IP アド	日する情 ドレス:	音楽版も言	記録を	れま1	€h₀	1000000			
	+	追加	0	編集	×	削除		•		
7.5										
								ОК	キャン	セル
k	C IP	アドレ	<u>م</u>					OK	キャン	セル 、

(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。

kaspersky 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 Kaspersky Security Center 14 ファイル(F) 操作(A) 表示(V) ヘルプ(H) 🔶 🤿 🙋 💼 📋 🗎 🖬 🙆 🖬 スにて「ポリシー」タブを開きます。 Kaspersky Security Center 14
 · □ 管理サーバーKSC
 · □ 管理対象デバイス
 · □ モバイルデバイス管理
 · □ デバイスの抽出 管理サーバー KSC > 管理対象デバイス KES のポリシーを右クリックし、「プロパティ」 🕞 ポリシー を選択します。 □ テバイスの油田 □ 未割り当てデバイス □ ポリシー デバイス ポリシー タスク デ ポリシー
 直 タスク
 ① カスペルスキーのライセンス
 > 詳細 ポリシーをファイルからインポート 列の追加と削除 2.*** ステータス アプリケーション ant Security for Windows (11.11.0 Kaspersky Endpoint Security for Windows (11.11.0) アクティブボリシー ポリシーを他のポリシーと比較(C) ■ Kaspersky Security Center ネットワークエージェント エクスポート(E) すべてのタスク(L) 列でグループ分けする 切り取り(C) コピー(C) 削除(D) リストのエクスポート(E) プロパティ(P) III プロパティ: Kaspersky Endpoint Security for Windows (11,11,0) X (2)「全般設定」-「ネットワーク設定」セクション 保護したル:高 すべての推奨される保護機能が有効です。 を開き、「信頼するアドレス」をクリックしま ネットワークの設定 全般 す。 ◎ - ブロキシサーバー イベントの設定 先進の脅威対策 設定 プロキシサーバーアドレスを自動で定義する、ポート:80 脅威対策 ◎ - 監視対象のポート-Detection and Response ○ すべてのネットワークポートを監視する セキュリティコントロール 設定 ● 選択されたネットワークボートのみを監視する データ暗号化 ◎ - 暗号化された接続のスキャン ローカルタスク ☑ 暗号化された接続をスキャン 全般設定 ● 保護機能の要求時に暗号化された接続をスキャンする アプリケーション設定 ○ 常に暗号化された接続をスキャンする ネットワークの設定 ☑ 従量制接続のトラフィックを制限する ー Web ページと連携するため Web トラフィック内にスクリプトを埋め込む ③ レポートと保管領域 信頼するアドレス インターフェイス 信頼するアプリケーション ポリシーのプロファイル 変更履歴 詳細設定 ◎-信頼するルート証明書 十追加×削弱 2 112 キャンセル 適用(A) ОК



(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。



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/

©2023 Kaspersky Labs Japan. Kaspersky Anti-Virus および Kaspersky Security は、AO Kaspersky Lab の登録商標です。 その他記載された会社名または製品名などは、各社の登録商標または商標です。なお、本文中では、TM、®マークは明記していません。 記載内容は 2023 年 1 月現在のものです。記載された内容は、改良の為に予告なく変更されることがあります。