



# Kaspersky Endpoint Security 12 スタンドアロンインストール・設定ガイド

2023/9/5

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 3.0

1. はじめに.....	3
1.1. 本資料の目的.....	3
1.2. 前提.....	3
1.3. 製品概要.....	4
1.4. システム要件について.....	5
2. KES インストールの流れ.....	6
3. インストールファイルのダウンロード.....	7
4. インストールファイルの解凍.....	8
5. KES のインストール、アクティベーション.....	11
5.1. KES のインストール.....	11
5.2. KES のアクティベーション.....	15
6. タスク設定.....	19
6.1. アップデートタスクの設定.....	19
6.2. スキャンタスクの設定.....	24
6.2.1. 完全スキャンの設定.....	24
6.2.2. 簡易スキャンの設定.....	27
6.2.3. オブジェクトスキャンの設定.....	29
6.2.4. コンテキストメニューからのスキャンの設定.....	30
6.2.5. リムーバブルドライブのスキャンの設定.....	31
6.2.6. バックグラウンドスキャンの設定.....	32
7. パスワードによる保護設定.....	33
8. 通知設定.....	37
9. 除外設定.....	40
9.1. 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.....	40
9.2. 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.....	44
9.3. 特定の Web サイトに対するスキャンを除外する.....	47
9.4. 特定のドメインや IP アドレスとの暗号化通信を除外する.....	50
Appendix.....	53
1. オフライン環境下における定義データベースの更新.....	53

## 1. はじめに

---

### 1.1. 本資料の目的

---

本資料では、Kaspersky Endpoint Security for Windows 12 をスタンドアローン環境で使用する手順についてご説明します。

### 1.2. 前提

---

以下を前提条件とします。

- ・ 管理サーバー（Kaspersky Security Center サーバー ; KSC サーバー）が存在しない環境である。
- ・ 競合ソフトがアンインストール済みである。
- ・ ライセンスキー情報ファイル、またはアクティベーションコードを用意している。

製品の役割は以下の通りです。

### **Kaspersky Endpoint Security (KES)**

クライアントに導入するセキュリティソフトウェアです。マルウェアのスキャンや駆除を行います。ライセンスは次の 2 種類があり、それぞれ利用できる機能が異なります。(本資料で用いるのはバージョン 12.2 です)

#### Select (サーバー・クライアント)

クライアント、モバイル、サーバーOS 向けアンチウイルス、およびコントロール機能

#### Advanced (サーバー・クライアント)

Select + 脆弱性診断とパッチ配信機能、暗号化

詳細はホームページをご確認ください。

<https://www.kaspersky.co.jp/small-to-medium-business-security>

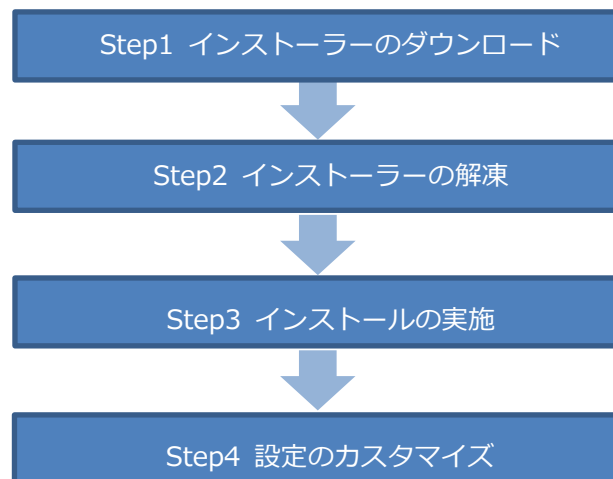
KES が適切に動作するためには、インストール先のコンピューターが下記 URL に記載されているシステム要件を満たしている必要があります。

<https://support.kaspersky.com/KESWin/12.2/ja-JP/127972.htm>

## 2. KES インストールの流れ

---

KES は以下の流れでインストールを行います。



## 3. インストールファイルのダウンロード

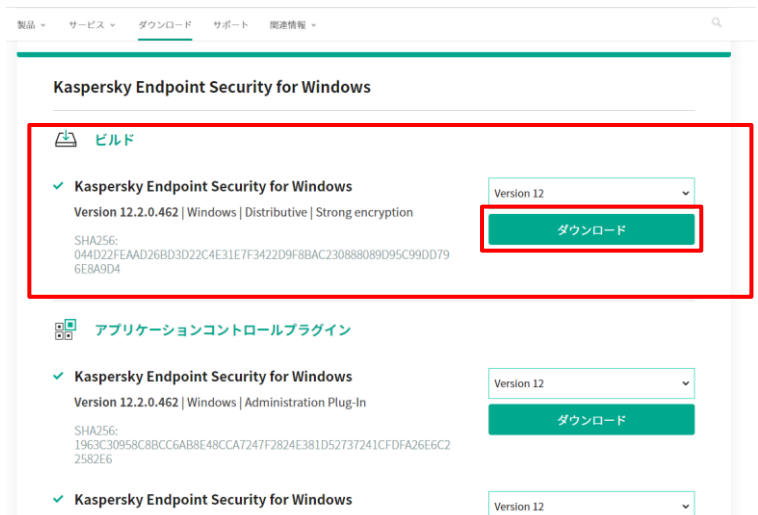
KES のインストールファイルのダウンロード手順についてご説明します。

インストールする環境がインターネットに接続できない環境の場合、接続できる環境にてダウンロードを実施してください。

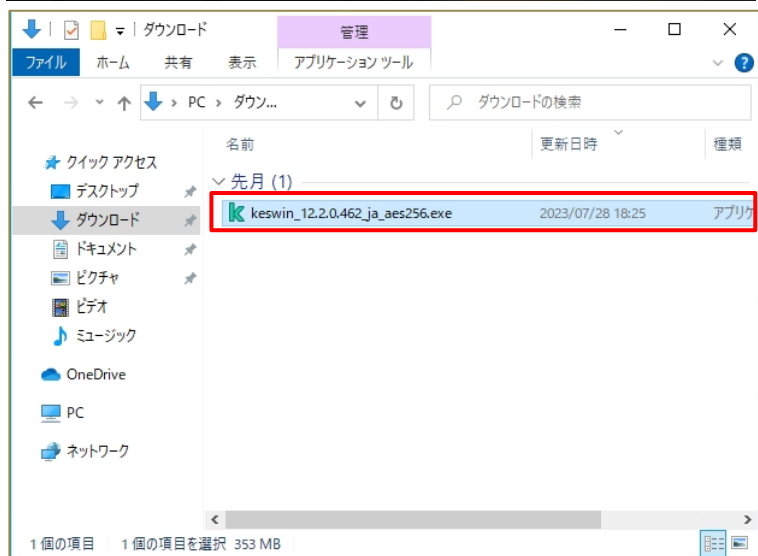
- (1) 最新版のインストーラーは下記より入手できます。

<https://www.kaspersky.co.jp/small-to-medium-business-security/downloads/endpoint>

「Kaspersky Endpoint Security for Windows」の「Distributive」にある「ダウンロード」をクリックしてください。



- (2) 正常にダウンロードされたことを確認します。

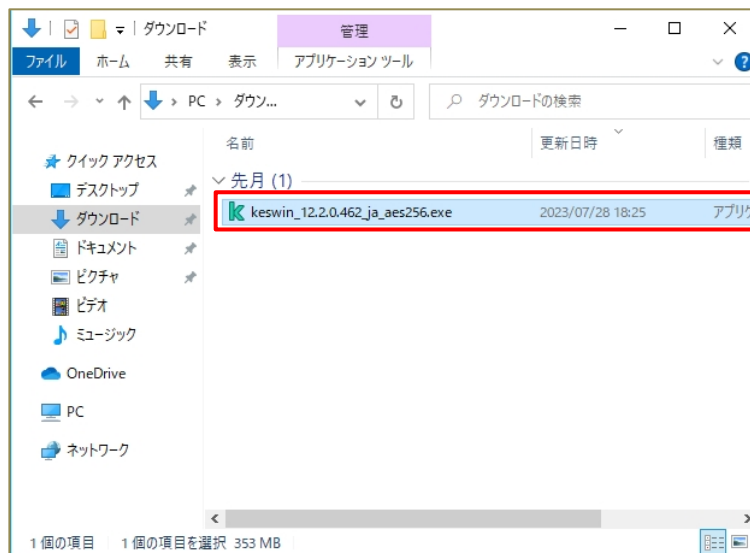


本章は以上です。

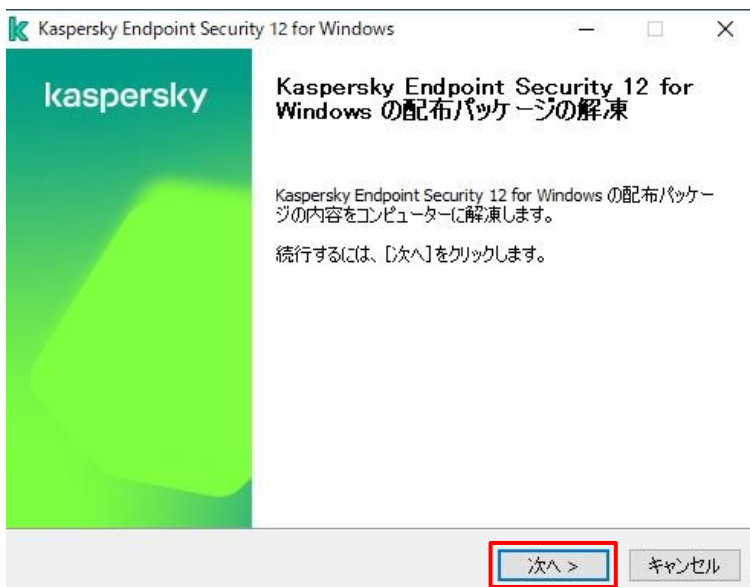
## 4. インストールファイルの解凍

KES のインストールファイルの解凍手順についてご説明します。

- (1) ダウンロードしたインストーラーを実行します。



- (2) 解凍ウィザードが起動するので「次へ」をクリックします。

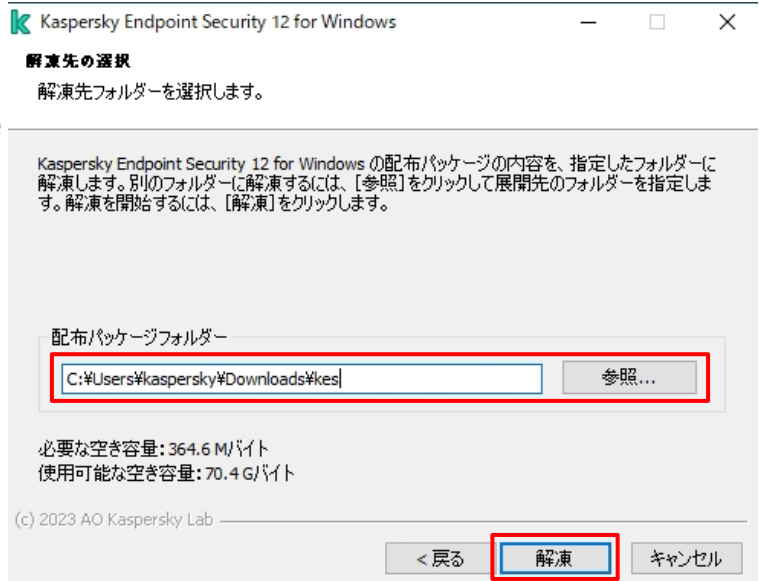




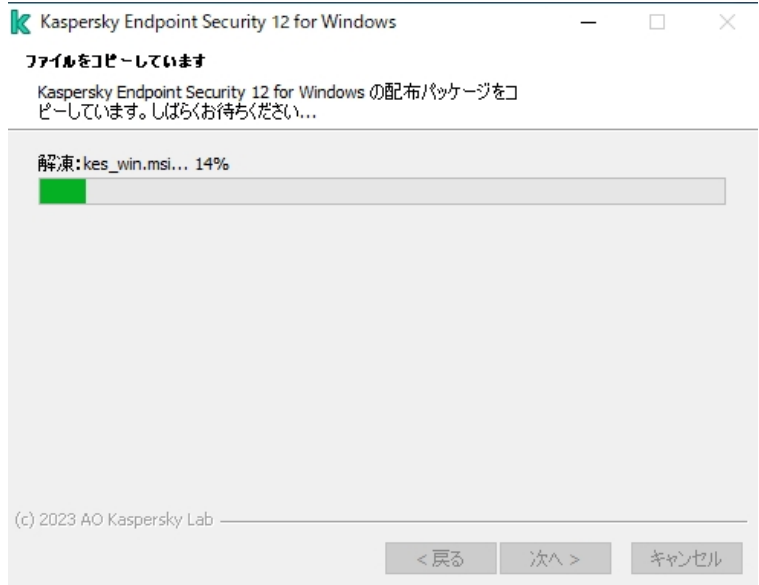
(3) 解凍先を指定し、「解凍」をクリックします。

ここでは解凍先として

「C:¥Users¥admin¥Downloads¥kaspers」を指定しています。



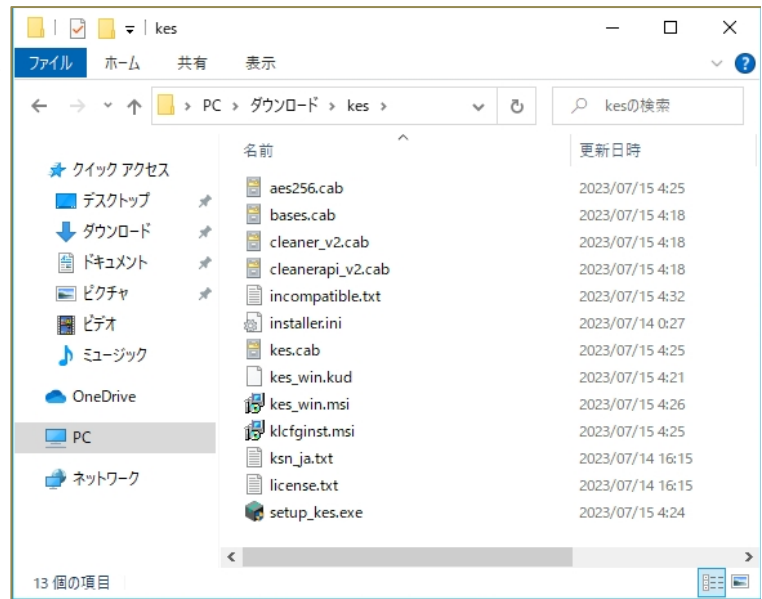
(4) 解凍が完了するまでしばらく待ちます。



(5) 正常に解凍されたことを確認し、「終了」をクリックします。



(6) エクスプローラーにて解凍先のフォルダーを開き、正常に解凍されたことを確認します。



本章は以上です。

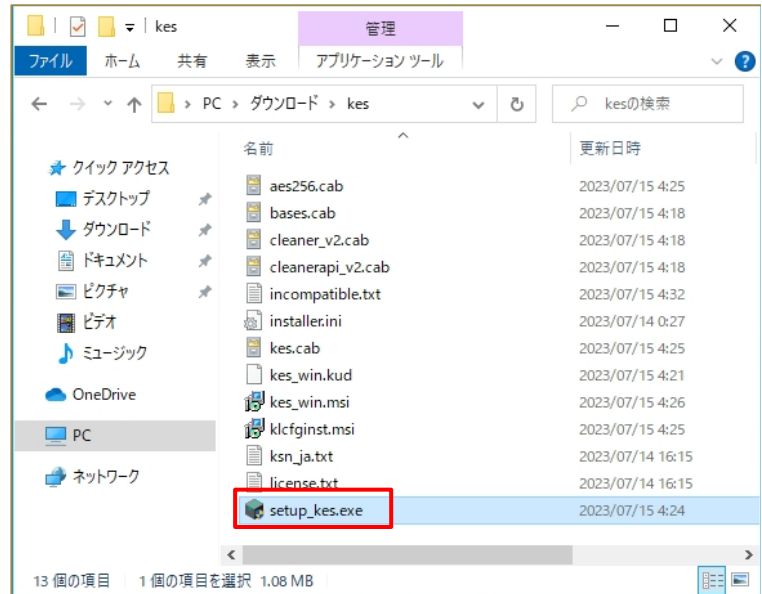
## 5. KES のインストール、アクティベーション

### 5.1. KES のインストール

KES のインストール手順についてご説明します。

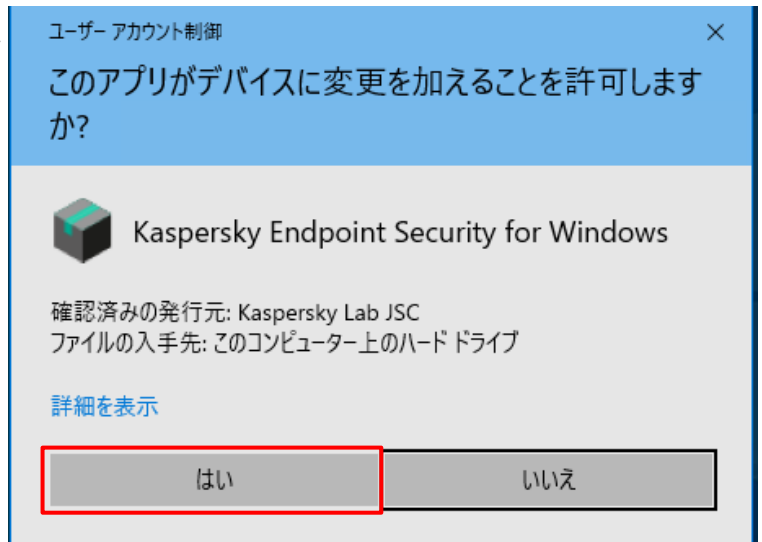
(1) 解凍先フォルダー内にある

「setup\_kes.exe」を管理者権限で実行します。

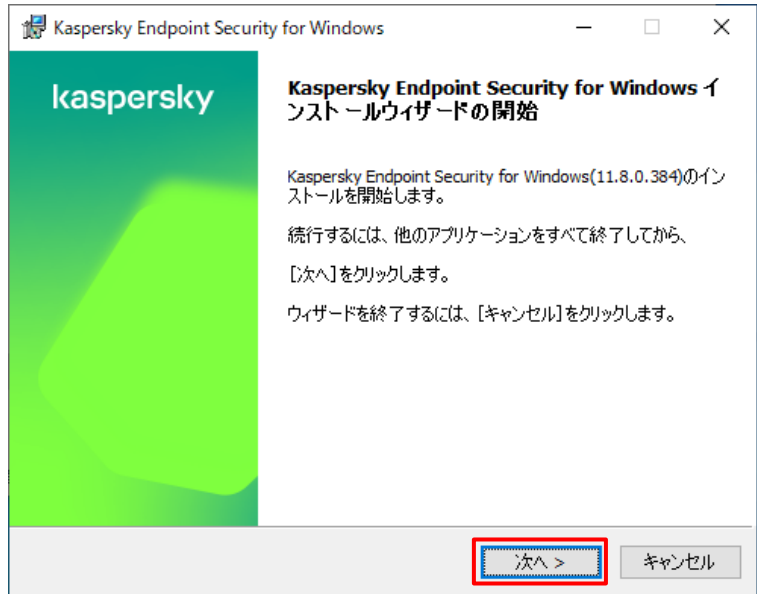


(2) ユーザーアカウント制御の警告が表示されます。

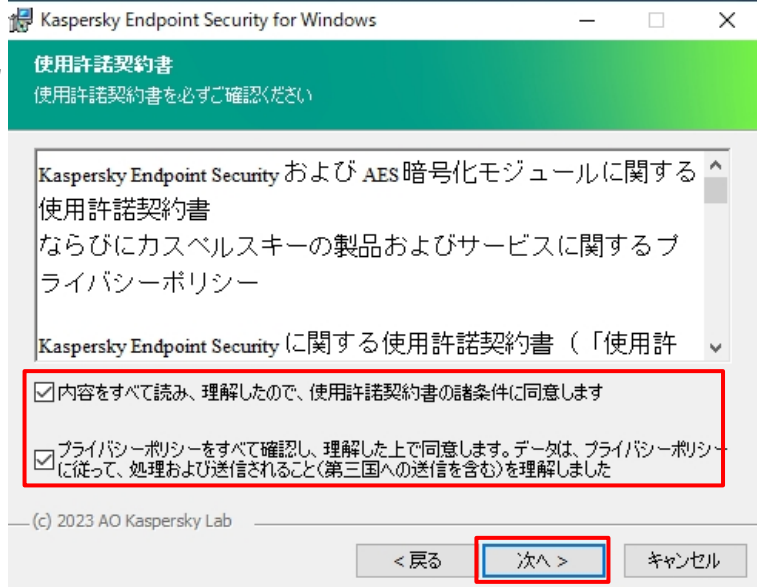
管理者権限で実行していない場合、適切なアカウント、パスワードを入力してください。



- (3) セットアップウィザードが起動するので「次へ」をクリックします。



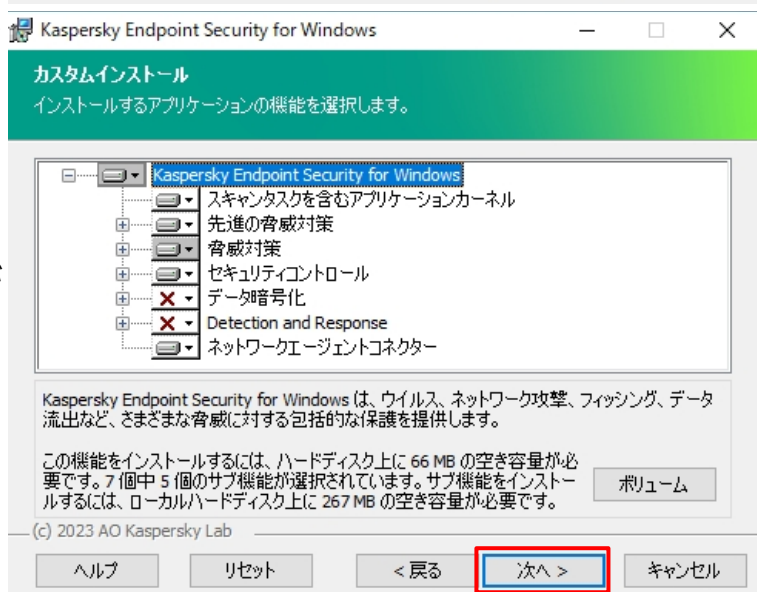
- (4) 「使用許諾契約書」、「プライバシーポリシー」の両方にチェックを入れ、「次へ」をクリックします。



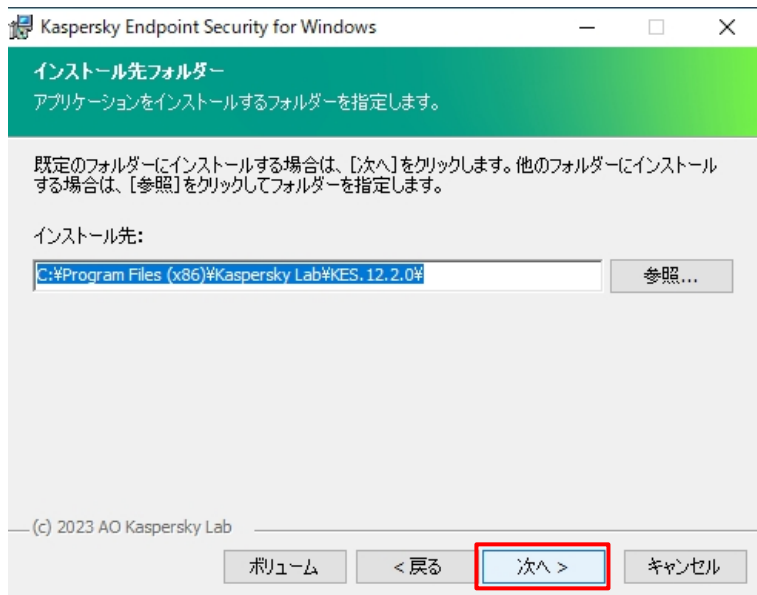
- (5) インストールするコンポーネントを選択します。ここでは既定値のまま「次へ」をクリックします。

Sa

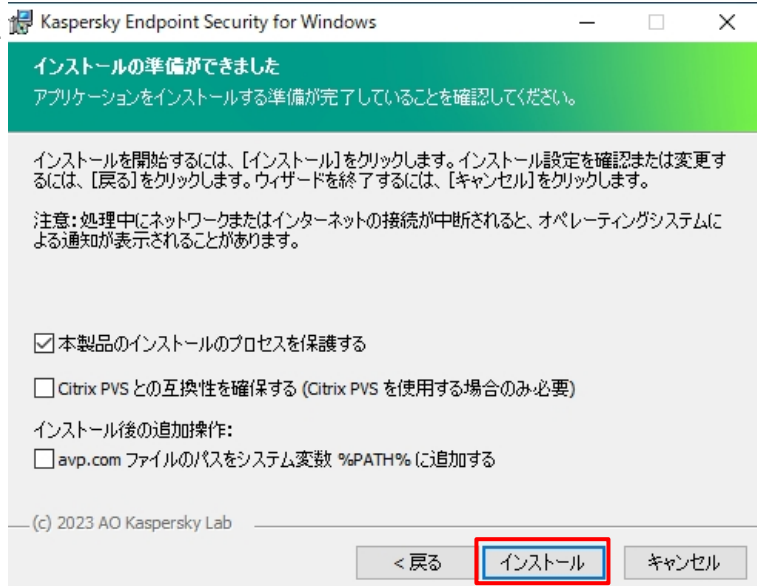
サーバーOS にインストールする場合はワークステーションとはインストールできる機能が異なるためご注意ください。



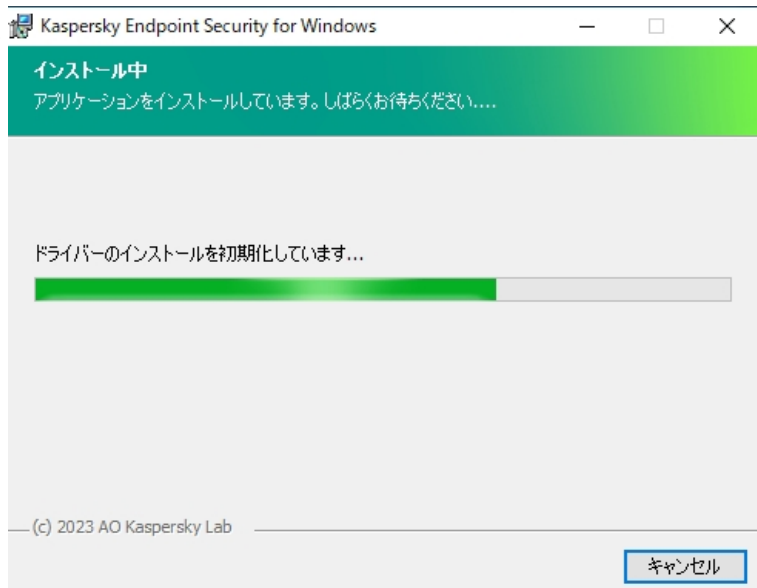
- (6) インストール先のパスを設定します。ここでは既定値のまま「次へ」をクリックします。



- (7) インストールのオプションを設定します。ここでは既定値のまま「インストール」をクリックします。



- (8) インストールが開始されるのでしばらく待ちます。



(9) セットアップウィザードが正常に完了したことを確認し、「終了」をクリックします。

※(9)と(10)は前後する場合があります。



(10) Kaspersky Security Network に関する確認画面が表示されます。「同意する」を選択し、「OK」をクリックします。

同意は任意です。同意しないを選択してもアプリケーションを使用することはできます。

※(9)と(10)は前後する場合があります。



本節は以上です。

KES のアクティベーション手順についてご説明します。

事前にライセンスを用意してください。

ここでは「ライセンス情報ファイル(.key)」を使用したアクティベーション方法をご説明します。OS 上の任意のフォルダーにライセンス情報ファイルを格納してください。

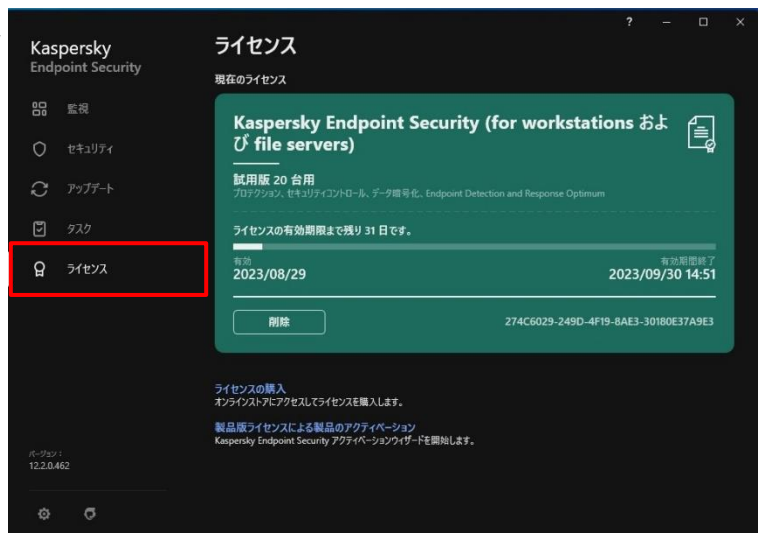
ライセンス情報ファイルは、以下のサイトにてアクティベーションコードから生成することができます。

<https://keyfile.kaspersky.com/ja>

- (1) スタートメニューから「Kaspersky Endpoint Security for Windows」を起動します。

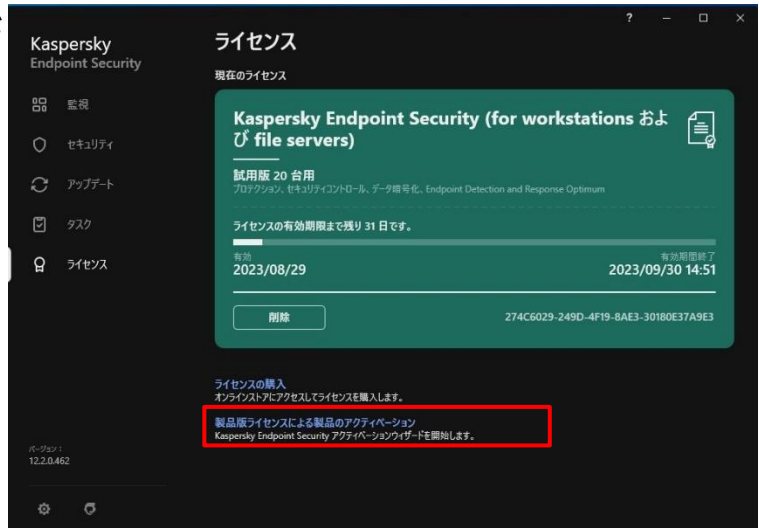


- (2) KES コンソールにて「ライセンス」をクリックします。



(3) インストール当初は試用版のライセンスが登録されています。

正規版のライセンスを登録するため「製品版ライセンスによる製品のアクティベーション」を選択します。



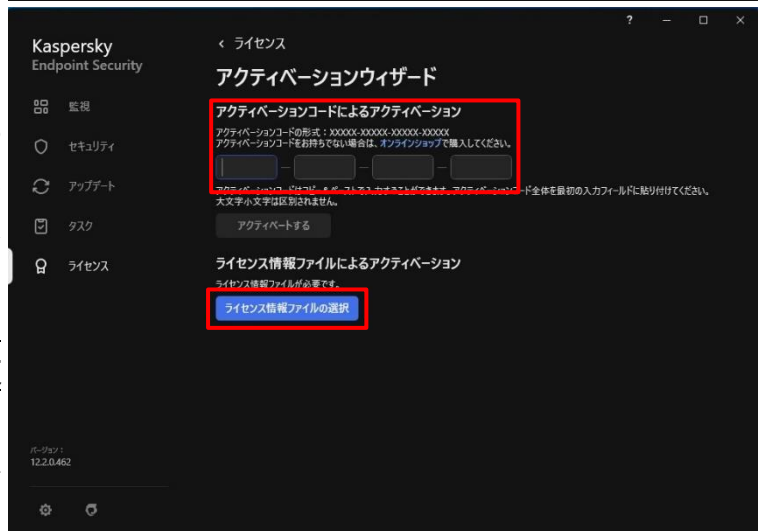
(4) ライセンス情報ファイルによるアクティベーション」を選択します。

※ アクティベーションコードを使用する場合は、「アクティベーションコードによるアクティベーション」にチェックを入れ、コードを入力してください。

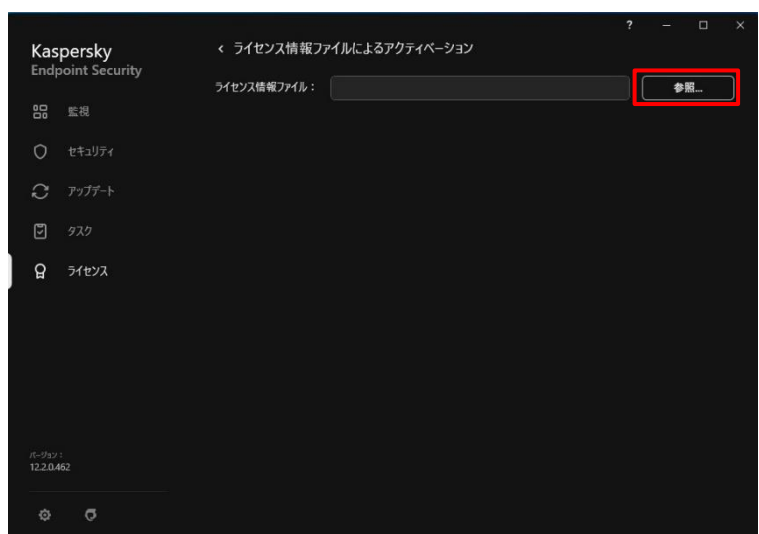
**アクティベーションコードを使用する場合はインターネット接続が必須となります。**

アクティベーションキーファイルは以下のサイトから入手します。

<https://keyfile.kaspersky.com/ja>

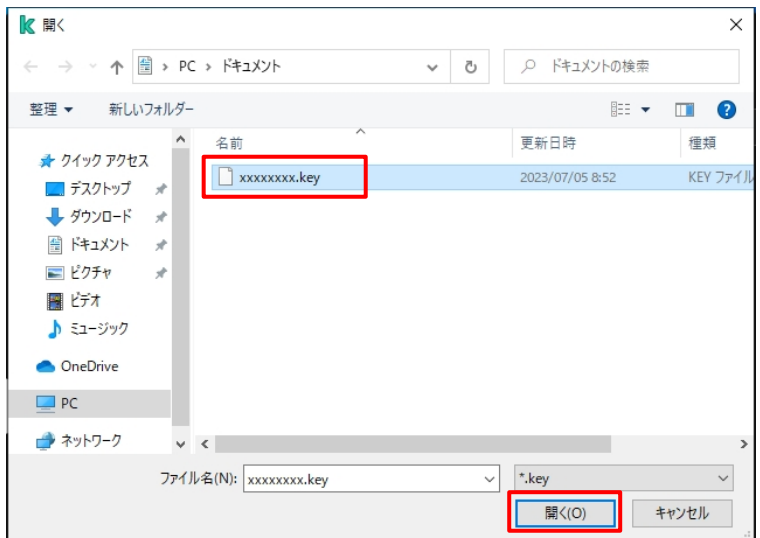


(5) 「参照」をクリックします。

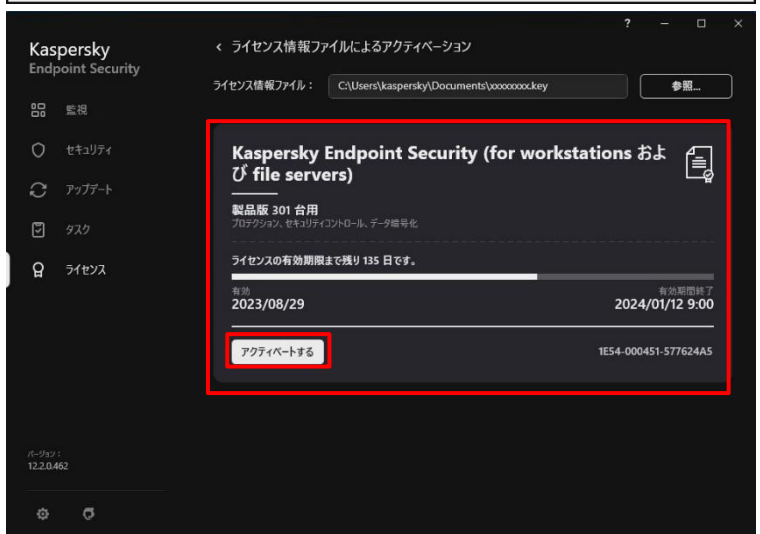




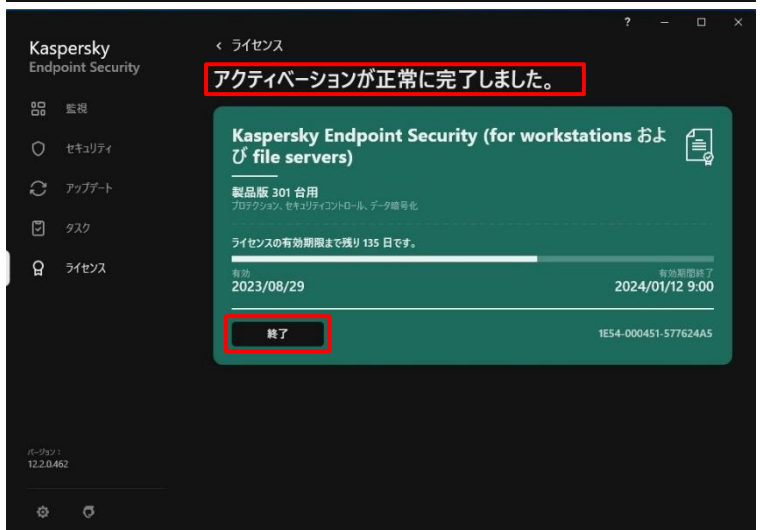
- (6) 事前に用意したライセンス情報ファイル（.key）を選択し、「開く」をクリックします。



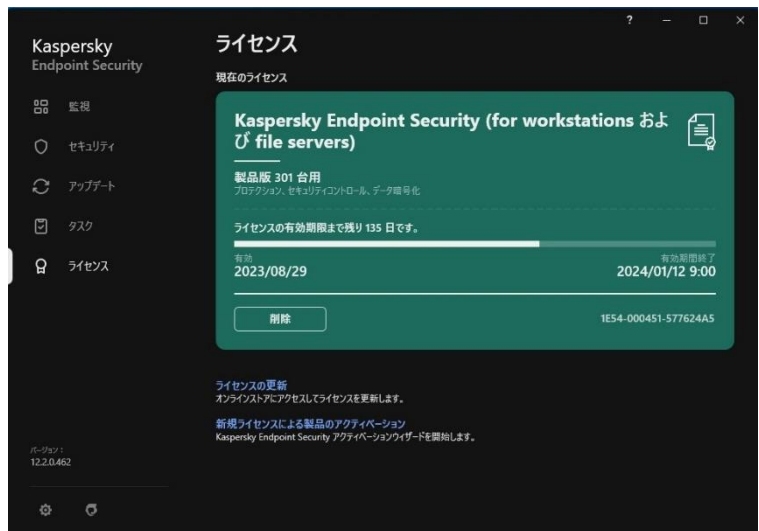
- (7) ライセンス情報が表示されることを確認し、「アクティベートする」をクリックします。



- (8) 「アクティベーションが完了しました」と表示されることを確認し、「終了」をクリックします。



(9) ご契約内容と有効期間に問題が無いことを確認します。



本節は以上です。

## 6. タスク設定

---

本章では、タスク設定についてご説明します。

タスクとは、定義データベースのアップデートやデバイスのスキャンなど、手動やスケジュールに沿って実行するアクションです。

### 6.1. アップデートタスクの設定

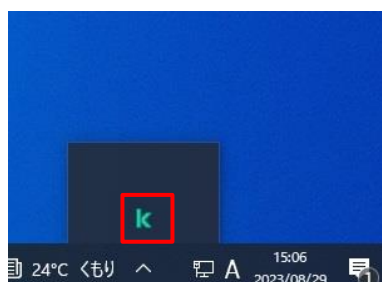
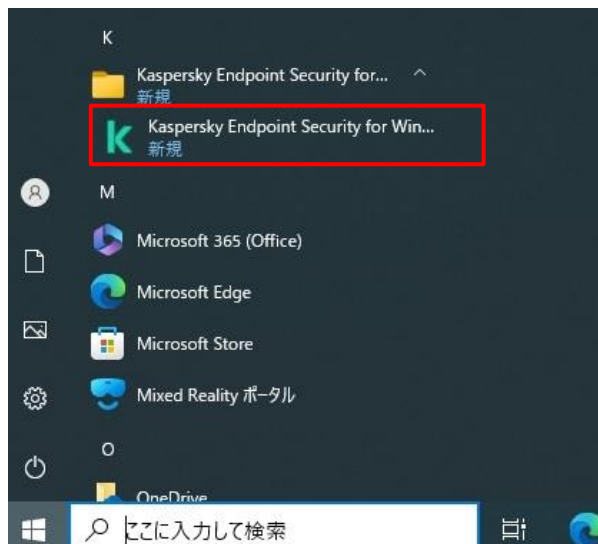
---

アップデートタスクの設定についてご説明します。


アップデートタスクとは、定義データベースをインターネットから取得しアップデートするタスクです。

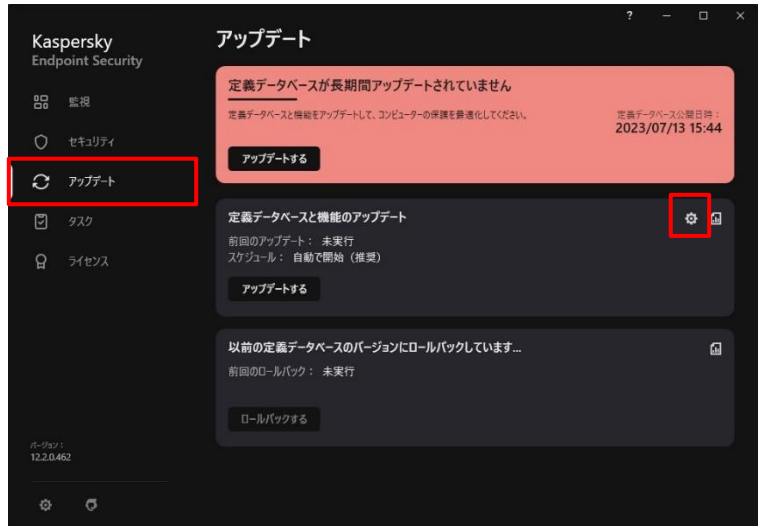
- (1). スタートメニューから「Kaspersky Endpoint Security for Windows」を起動します。

または、画面右下のタスクバーに存在するアイコンをダブルクリックします。



(2). KES コンソールにて「アップデート」をクリックします。

「定義データベースと機能のアップデート」の設定アイコン  をクリックします。



(3). アップデートの設定画面が表示されます。

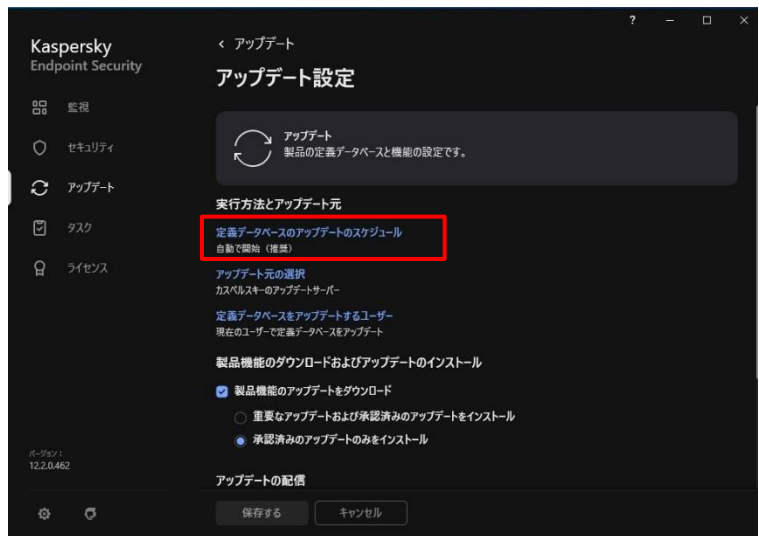
右側に設定情報が表示されます。

既定では以下の通りとなっております。

- ・実行方法：自動開始
- ・アップデート元：既定

既定値の場合、インターネット上のカスペルスキーサーバーから自動的に定義データベースをダウンロードする設定となっております。

変更する場合は「実行方法とアップデート元」から、「定義データベースのアップデートスケジュール」をクリックします。

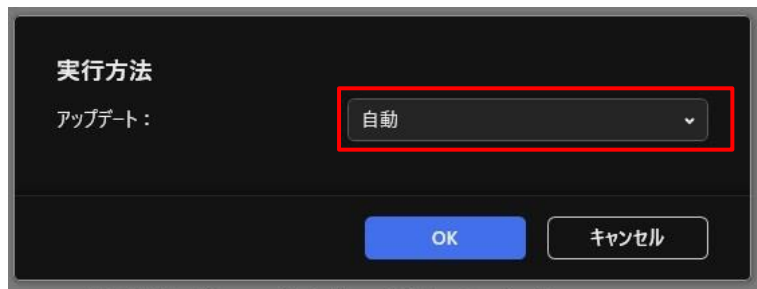


(4).プルダウンを選択し、スケジュールを設定することができます。

既定では「自動開始」となっておりますが、ここで設定を変更することができます。

**通常、変更の必要はありません。**

例は 1 時間おきに実行する設定です。



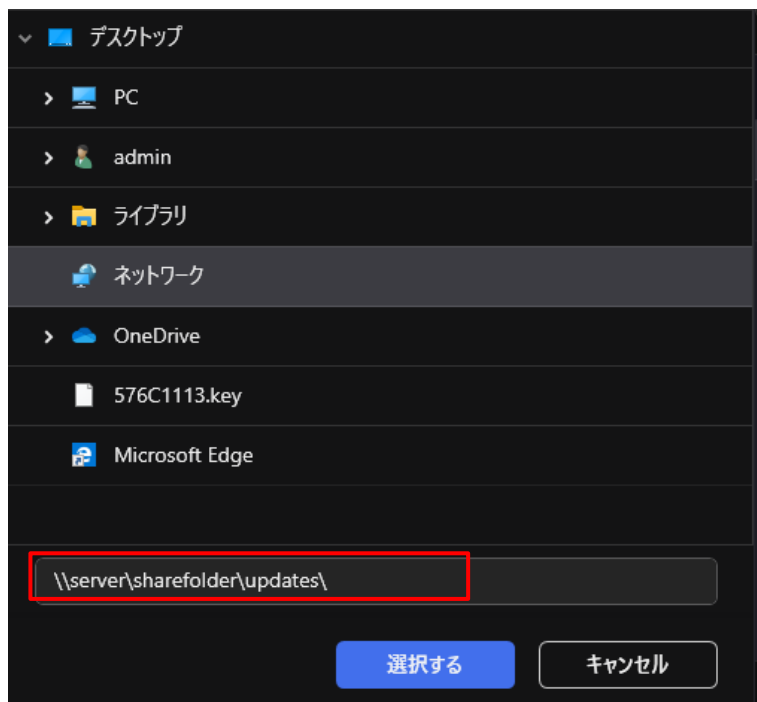
(5).次に「アップデート元」を選択します。定義データベースの取得元を設定することができます。

**通常、変更の必要はありません。**

取得元をローカルネットワーク上の共有フォルダーなどに変更する場合は「追加」ボタンをクリックします。

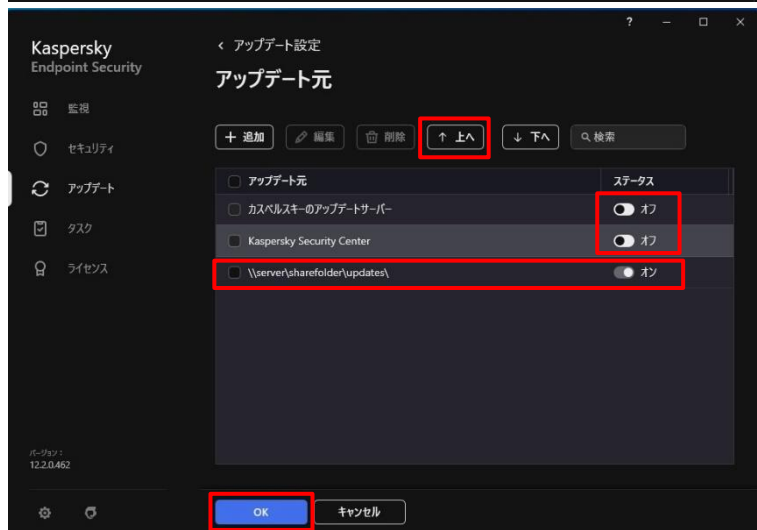


- (6). ネットワーク上の共有フォルダーを指定する場合は、パスに共有フォルダーのパスを入力します。

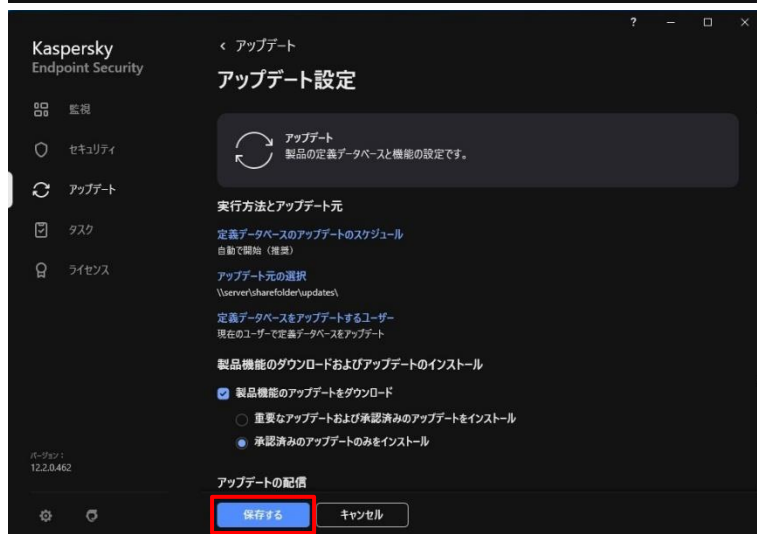


- (7). 一覧に追加されるので、↑ボタンをクリックして一番上にする事で優先順位を設定することができます。
- 不要なアップデート元がある場合は、ステータスをオフに変更するか、削除することができます。

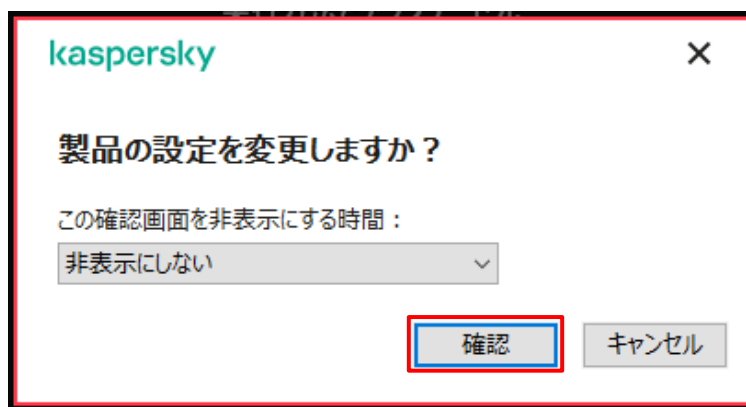
設定後、「OK」をクリックします。



- (8). 「保存する」をクリックし、設定を保存します。



(9). 確認画面が表示されるので「確認」をクリックします。



本節は以上です。

## 6.2. スキャンタスクの設定


スキャンタスクの設定についてご説明します。

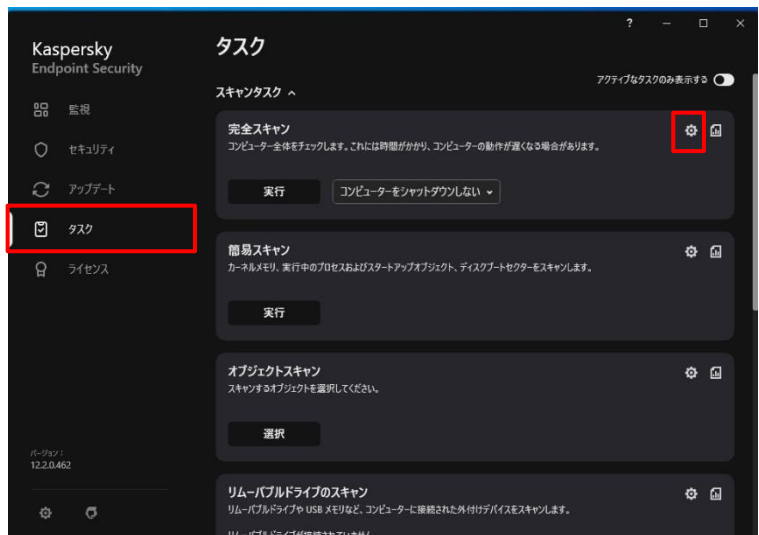
スキャンタスクとは、スケジュールに沿って OS 上のファイルやフォルダーをスキャンするタスクです。

KES では複数のスキャンタスクが登録されております。ここでは各スキャンタスクについてご説明します。

### 6.2.1. 完全スキャンの設定

「完全スキャン」タスクは、OS 上の PC のすべての領域をスキャンするタスクです。

- (1). KES コンソールにて「タスク」をクリックします。
- 「完全スキャン」の設定アイコン  をクリックします。



- (2). 現在のスキャン設定が表示されます。

「詳細設定」をクリックすると、メニューが追加表示されます。





(3)「スキャンの最適化」ではスキャンパフォーマンス調整の一部を行うことができます。

- ・作成または更新されたファイルのみスキャン  
一度スキャンされたファイルのスキャンをスキップします。
- ・スキャン時間が次を超えたファイルをスキップ  
スキャン時間が一定時間を超えるファイルについては、スキップします。既定では 30 秒です。
- ・複数のスキャンタスクを同時に実行しないでください

このスキャンタスクが実行中の場合、別のスキャンタスクを起動した場合に、そのタスクはこのタスクが完了後に自動的に開始されるようにします。



(4).スキャンスケジュールを設定することができます。

既定では「手動開始」に設定されています。

「スキャン」にて頻度や間隔を設定することが可能です。

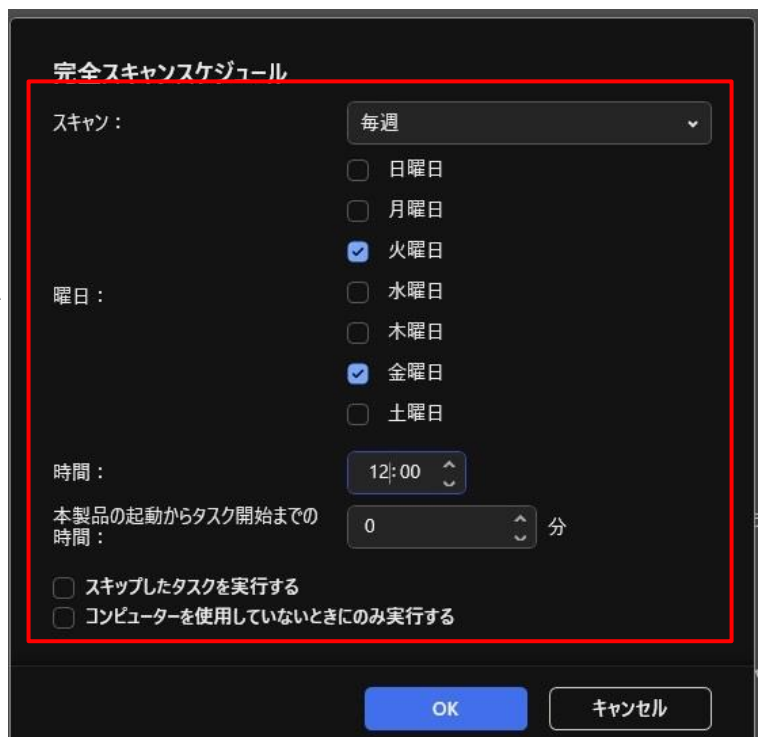
右図は毎週火曜日、金曜日の 12:00 時から開始するようにした場合の例です。



- ・スキップしたタスクを実行する  
スケジュールの時刻に OS がシャットダウンされていた場合、起動後にタスクが開始されます。

・コンピューターを使用していないときのみ実行する

スクリーンセーバー中またはロック時のみ実行されます。ロックが解除された場合は中断し、再度ロックされた場合は中断したところから自動的に開始されます。

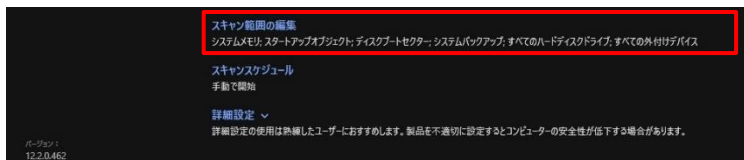


「OK」をクリックし設定を保存します。

(5).「スキャン範囲の編集」をクリックすると、このタスクでスキャンする対象を設定することができます。

完全スキャンタスクでは既定で右記の項目が選択されています。

「追加」「編集」「削除」ボタンで対象の変更や、チェックを外すことで対象外にすることができます。



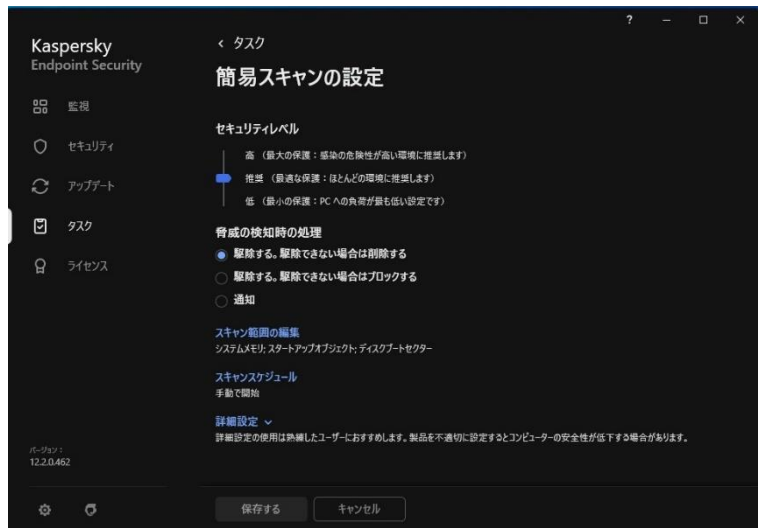
本項は以上です。

「簡易スキャン」タスクは、カーネルメモリ、ブートセクター、スタートアップオブジェクトなどをスキャンするタスクです。

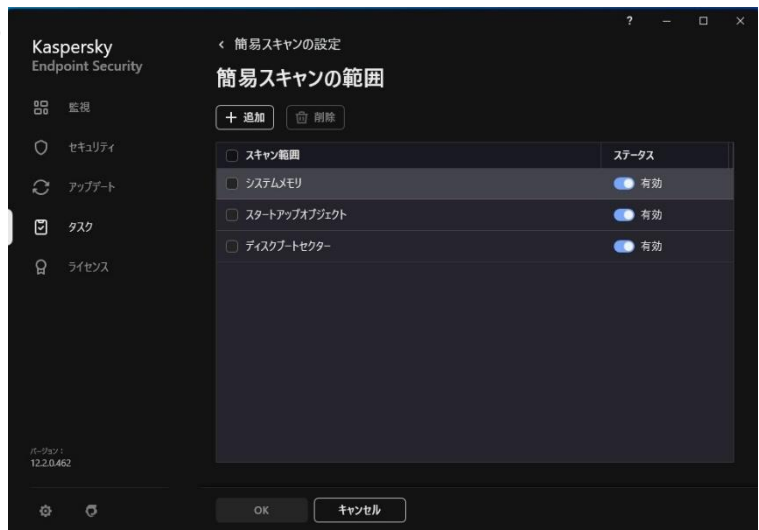
- (1). KES コンソールにて「タスク」をクリックし、  
「簡易スキャン」の設定アイコンをクリックします。



- (2). 設定方法は完全スキャン同様です。



- (3). 「スキャン範囲の編集」をクリックすると、この  
タスクでスキャンする対象を設定することができます。  
簡易スキャンタスクでは既定で右記の項目  
が選択されています。  
「追加」「編集」「削除」ボタンで対象の変更や、  
チェックを外すことで対象外にすることができます。



(4). スキャンスケジュールを設定することができます。

既定では「手動開始」と設定されております。

「スキャン」にて頻度や間隔を設定することが可能です。

右図では毎週月～金曜日の 10:00 から開始する例です。

簡易スキャンは比較的短時間で終了し、脅威対策に有効なため、毎日実施することをご検討ください。

簡易スキャンのスケジュール

スキャン： 毎週

曜日：

- ☐ 日曜日
- ☒ 月曜日
- ☒ 火曜日
- ☒ 水曜日
- ☒ 木曜日
- ☒ 金曜日
- ☐ 土曜日

時間： 10:00

本製品の起動からタスク開始までの時間： 15 分

☒ スキップしたタスクを実行する

☐ コンピューターを使用していないときにのみ実行する

OK キャンセル

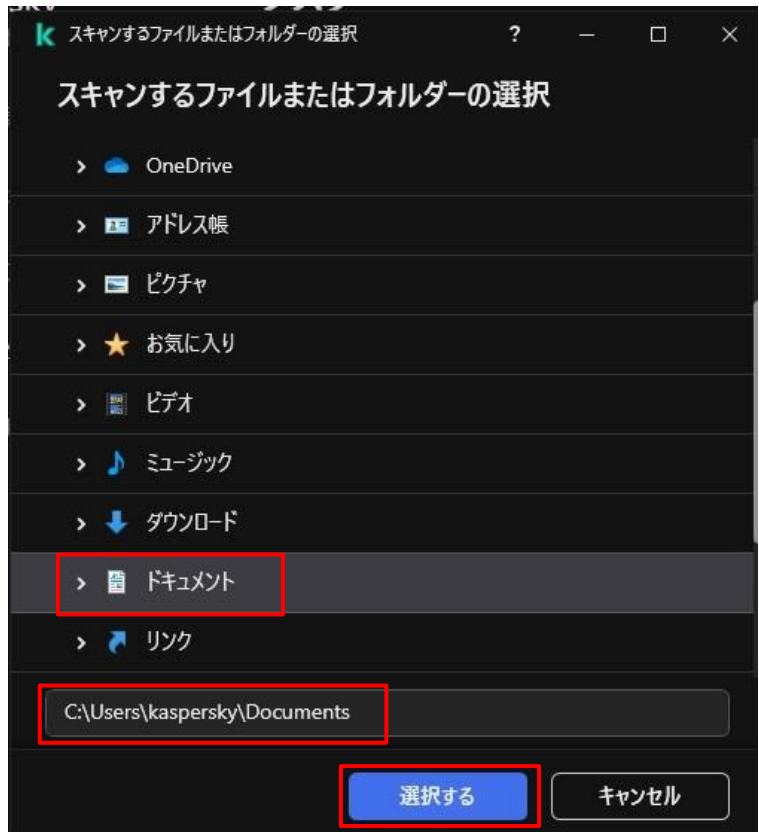
本項は以上です。

「オブジェクトスキャン」タスクは、ユーザーがスキャン範囲や開始時間を定義するタスクです。

- (1). KES コンソールにて「タスク」をクリックし、「オブジェクトスキャン」の「選択」をクリックします。



- (2). スキャンするフォルダーまたはファイルを指定します。  
スキャンするフォルダーまたはファイルは「選択」から繰り返し実施することで複数登録できます。

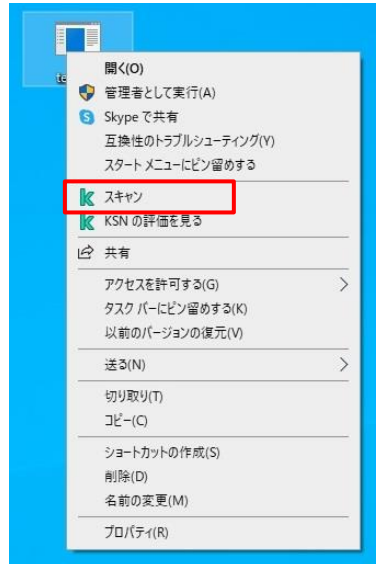


- (3). オブジェクトスキャンの設定アイコンをクリックします。  
設定方法は完全スキャンと同様です。



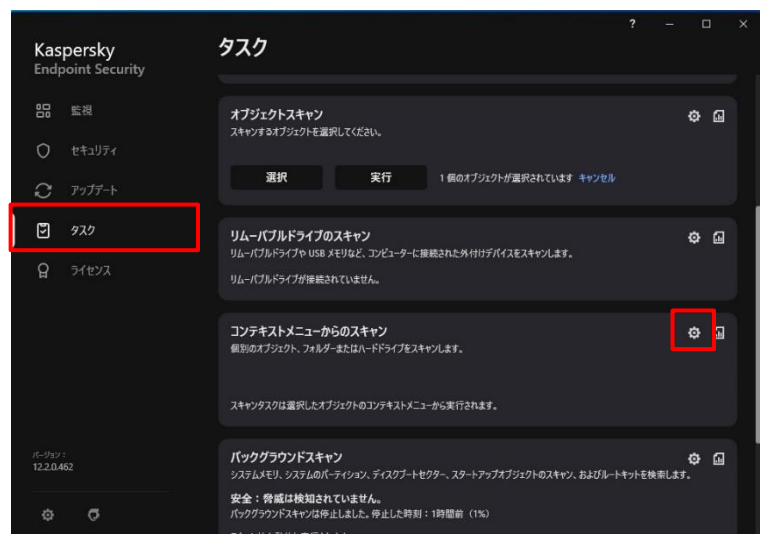
本項は以上です。

「コンテキストメニューからのスキャン」とは、ユーザーが OS 上の任意のファイルやフォルダーを右クリックして「スキャン」を選択して実行するスキャンです。



- (1). KES コンソールにてタスクをクリックし、「コンテキストメニューからのスキャン」の設定アイコンをクリックします。

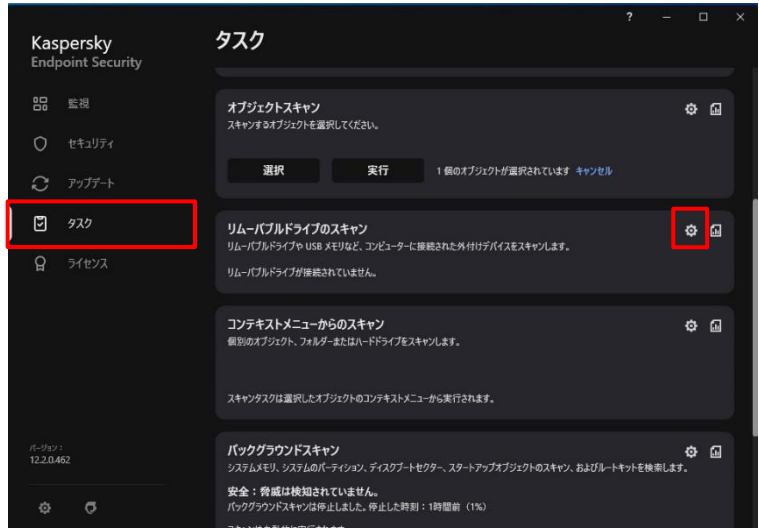
設定方法は完全スキャンと同様です。



本項は以上です。

OS に対し USB メモリなどリムーバブルメディアを接続した際のスキャンを設定します。

- (1). KES コンソールにてタスクをクリックし、「リムーバブルドライブのスキャン」の設定アイコンをクリックします。



- (2). オンに変更すると、リムーバブルドライブ接続時にスキャンを行います。

- ・リムーバブルドライブ接続時の処理：

- 簡易スキャン

感染に対して最も脆弱な特定のファイル形式のファイルのみスキャンします。(既定)

- 詳細スキャン

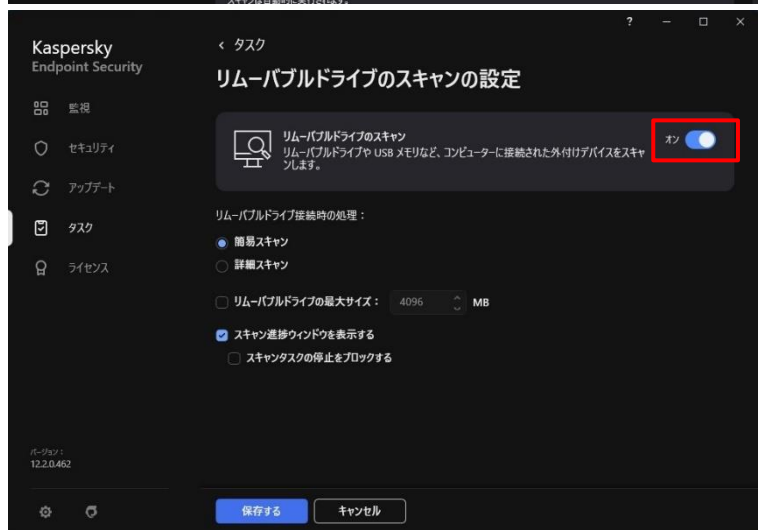
ドライブ上のすべてのファイルをスキャンします。

- ・リムーバブルドライブの最大サイズ：

スキャンするリムーバブルドライブのサイズ上限を定義します。このサイズを超えたメディアはスキャンを開始しません。

- ・スキャン進捗ウィンドを表示する：

スキャン進捗のウィンドを表示する設定です。既定では有効です。



本項は以上です。

「バックグラウンドスキャン」とは、OS が低負荷時にシステムメモリ等をスキャンするタスクの設定です。

- (1). KES コンソールにてタスクをクリックし、「バックグラウンドスキャン」の設定アイコンをクリックします。



- (2). オンになっていると有効です。詳細設定はありません。  
既定でオンになっています。



本項は以上です。



## 7. パスワードによる保護設定

本章では、パスワードによる保護設定についてご説明します。

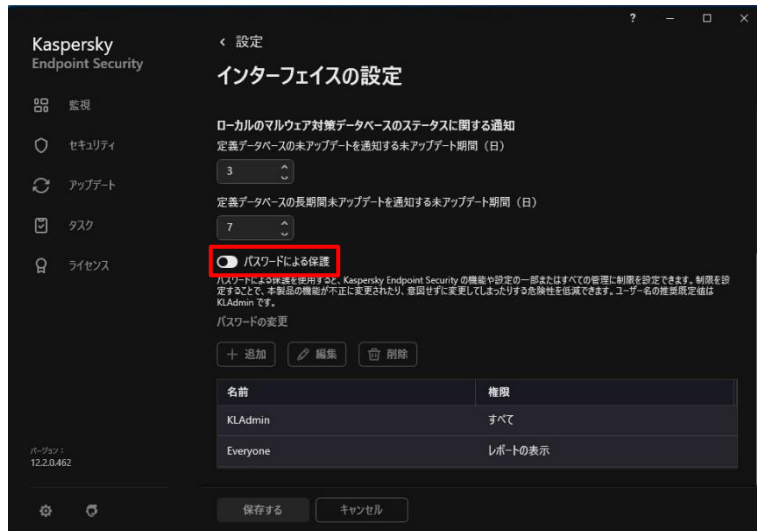
この設定を実施することで、KES の設定変更やアプリケーションの終了、アンインストール等を実施しようとした際にパスワードの入力が求められるようになります。

複数のアカウントを登録し、アカウント毎に権限を設定することができます。

- (1). KES コンソールにて設定アイコンをクリックし、「全般設定」-「インターフェイス」をクリックします。



- (2). 「パスワードによる保護」を有効にします。



(3).有効にすると、ユーザー名、パスワードの登録を求められます。

ユーザー名は「KLAdmin」とし、パスワードを登録します。

パスワードの強度が低い場合は警告が表示されます。(設定は可能です)

設定後、「保存」をクリックします。

管理者パスワードを設定してください

本製品の組み込み管理者アカウントには Kaspersky Endpoint Security のすべての機能に制限なくアクセスできる権限があります。

ユーザー名：  
KLAdmin

推奨：KLAdmin

パスワードの入力：  
●●●●●●●●

パスワードの確認：  
●●●●●●●●

パスワードの強度：中

- 8文字以上
- 1文字以上の数字
- 大文字と小文字
- 特殊文字
- パスワードの一致

保存 キャンセル

(4).ユーザーを選択した状態で、編集をクリックすると、権限が設定・確認できます。

※KLAdmin の権限は編集できません。

Kaspersky Endpoint Security

設定

### インターフェイスの設定

ローカルのマルウェア対策データベースのステータスに関する通知  
定義データベースの未アップデートを通知する未アップデート期間 (日)  
3

定義データベースの長期間未アップデートを通知する未アップデート期間 (日)  
7

☒ パスワードによる保護  
パスワードによる保護を使用すると、Kaspersky Endpoint Security の機能や設定の一部またはすべての管理に制限を設定できます。制限を設定することで、本製品の機能が不正に変更されたり、意図せずに変更してしまったりする危険性を低減できます。ユーザー名の推奨既定値は KLAdmin です。

パスワードの変更

+ 追加 **編集** 削除

名前	権限
KLAdmin	すべて
Everyone	レポートの表示

バージョン：12.2.0.462

保存する キャンセル

Kaspersky Endpoint Security

インターフェイスの設定

### ユーザーまたはグループに権限を追加

名前  
KLAdmin

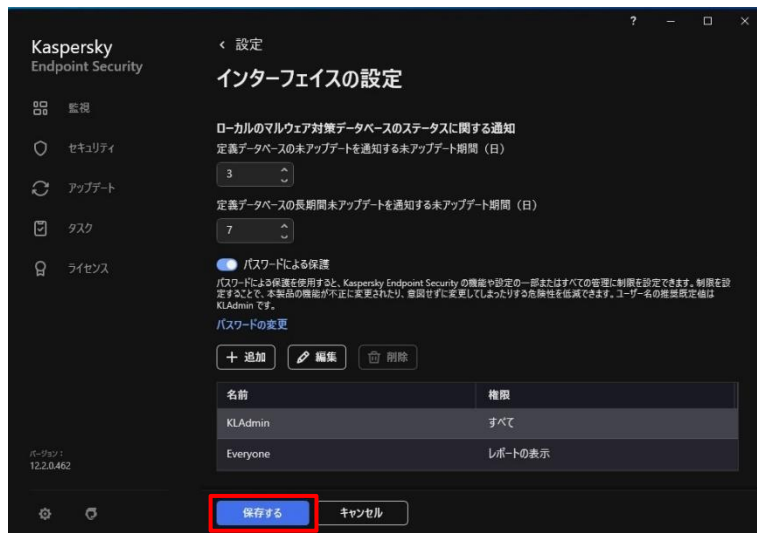
権限

- ☒ 本製品の設定
- ☒ 暗号化されたドライブ上のデータへのアクセスの復元
- ☒ バックアップから復元
- ☒ 本製品の終了
- ☒ 本製品の削除 / 変更 / 修復
- ☒ ライセンスの削除
- ☒ レポートの表示
- ☒ 保護機能の停止
- ☒ Kaspersky Security Center ポリシーを無効にする
- ☒ 管理コンポーネントの停止

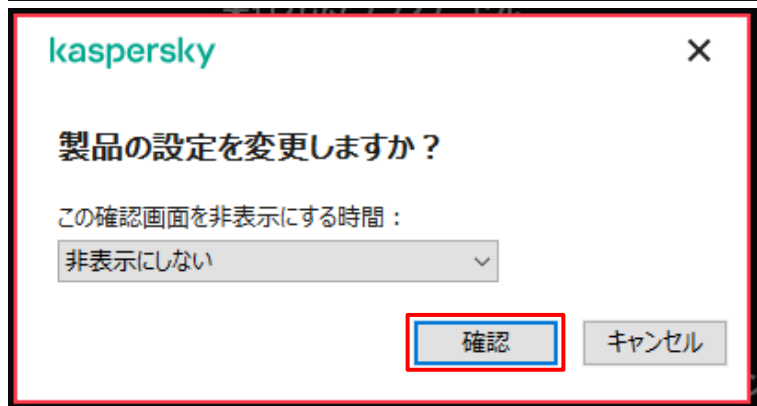
バージョン：12.2.0.462

OK キャンセル

(5).「保存する」をクリックし、設定を保存します。



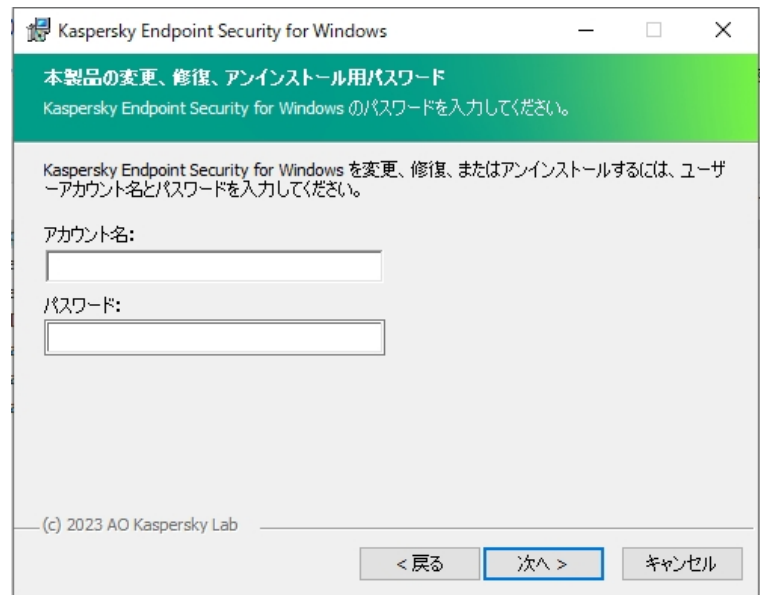
(6).確認をクリックし、設定画面を閉じます。



(7).設定後、KES の終了や設定の変更を保存しようとするすると右記のダイアログが表示されます。



(8). KES をアンインストールしようとした場合、  
右記の画面が表示されます。



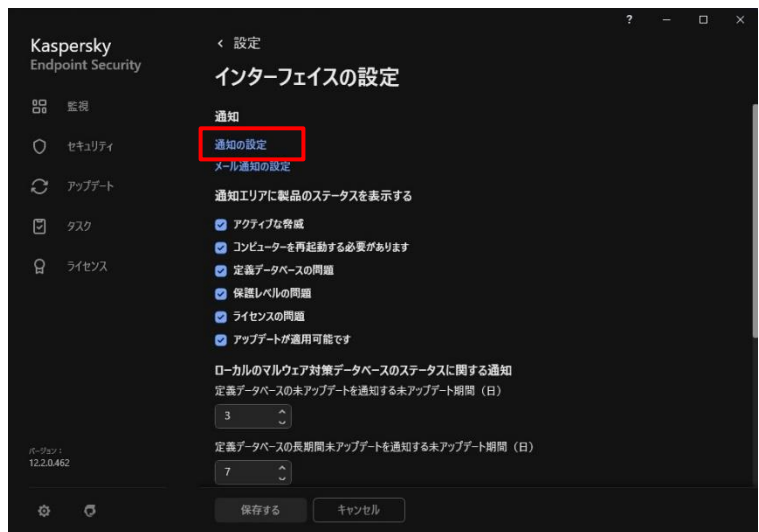
本章は以上です。

## 8. 通知設定

本章では、マルウェアの検知時など何等かのイベントが発生した際に、OS 上に通知ダイアログを表示する設定や、管理者へメールで通知する設定についてご説明します。

- (1). KES コンソールにて設定アイコンをクリックし、「全般設定」-「インターフェイス」をクリックします。

インターフェイスの設定から、「通知の設定」をクリックします。



(2).通知の設定画面が表示されます。

各保護コンポーネントやタスク毎に「緊急イベント」「重要なイベント」「情報イベント」があります。

それらのイベントに対し、以下の通知設定があります。

- ・ ローカルレポートに保存：イベント発生時に KES のログに保存します。
- ・ Windows イベントログに保存：イベント発生時に Windows のイベントログに保存します。
- ・ 画面で通知：イベント発生時に画面にダイアログメッセージを表示します。
- ・ メールで通知：イベント発生時に指定したアドレスへメール通知します。

運用に合わせ、設定を実施してください。

例えば、ファイル脅威対策にてマルウェアが検知した場合に画面に通知し、さらに管理者にメール通知する場合は、以下の設定を行います。

- 1.「ファイル脅威対策」を選択
- 2.「悪意のあるオブジェクトが検知されました」イベントの「画面で通知」「メールで通知」にチェック



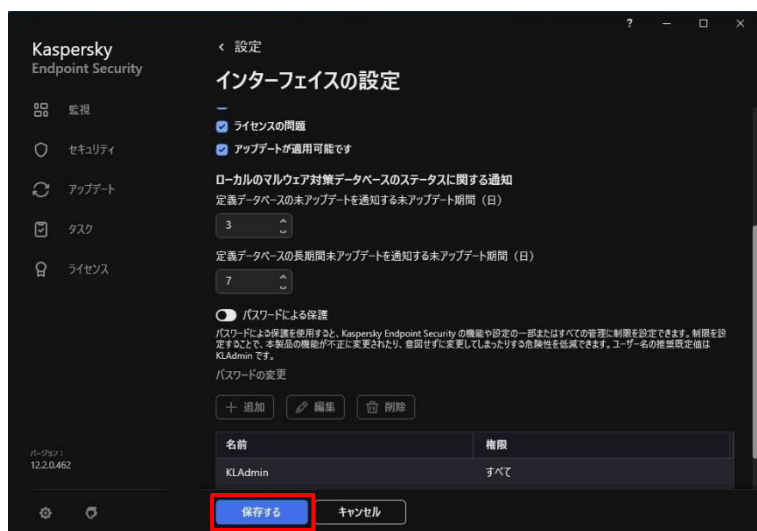
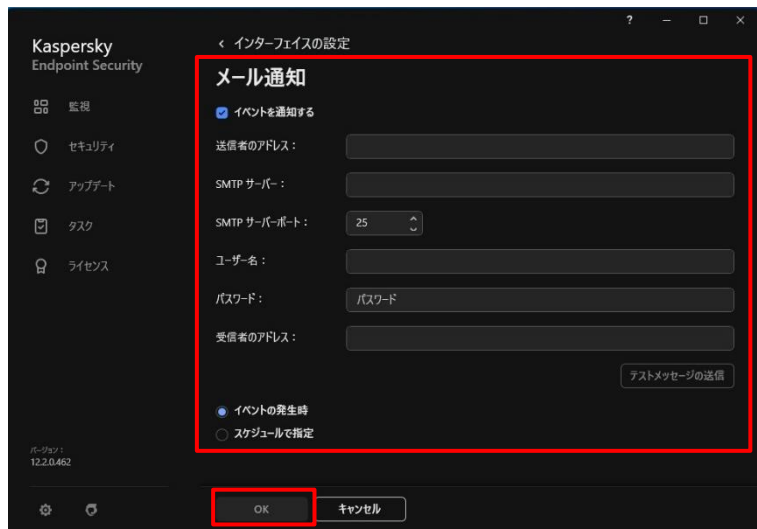
(3).メールの宛先は「メール通知の設定」から行います。



(4)。「イベントを通知する」にチェックを入れ、以下項目を入力して「OK」をクリックします

- ・ 送信者のアドレス :  
管理者に送信されるメール差出人のメールアドレスを選択します。
- ・ SMTP サーバー :  
SMTP サーバーの IP アドレスとポート番号を選択します。
- ・ ユーザー名、パスワード :  
SMTP サーバーの認証が必要なユーザー名、パスワードを選択します。
- ・ 受信者のアドレス :  
メールの送信先を設定します。
- ・ 送信方法 :  
イベントの発生時を選択します。

(5)。「保存する」をクリックし、設定を保存します。



本章は以上です。

## 9. 除外設定

本章では、除外設定についてご説明します。

資産管理、バックアップなどのアプリケーションは、その動作の性質上、KES に検知される可能性があります。

業務上必要となるアプリケーションやファイルなど、KES による影響を受けたくないものがある場合、KES の監視対象から除外設定を実施することで対応が可能です。

また、イントラネットサイトや、業務上閲覧する必要があるサイトがある場合、URL を KES の検知から除外することもできます。

### 9.1. 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。

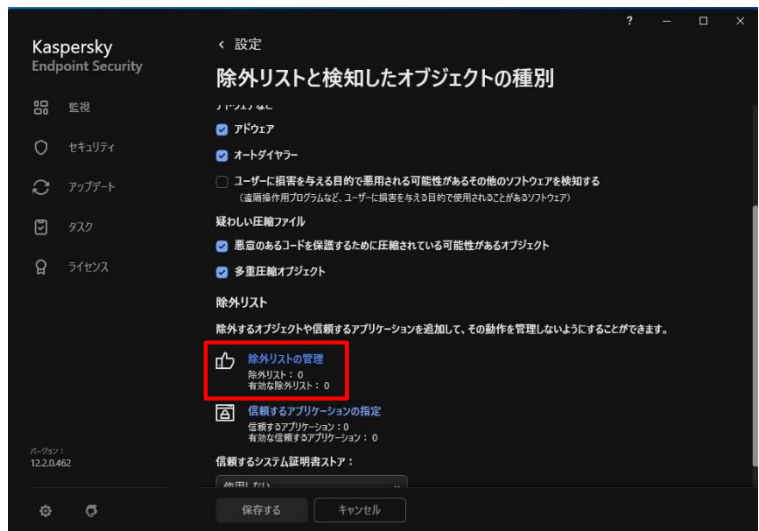
パスを指定せずファイル名を設定することで、どの場所にあってもそのファイル名のオブジェクトを除外対象とすることもできます。

- (1). KES コンソールにて設定アイコンをクリックし、「除外リストと検知したオブジェクトの種類」をクリックします。





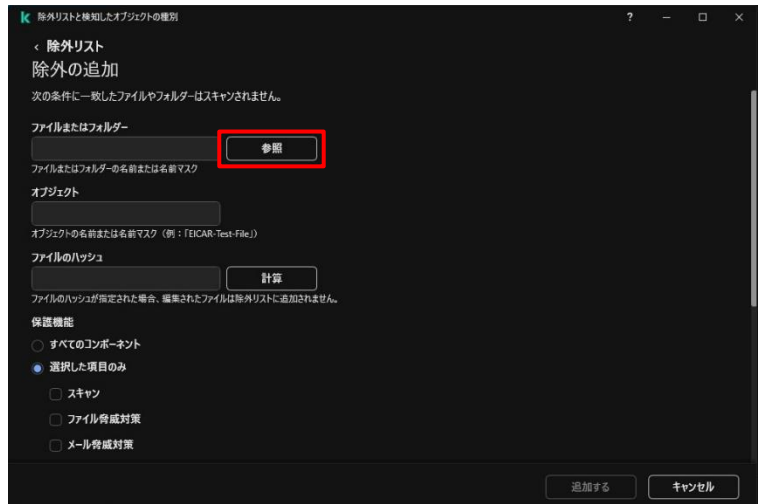
(2).「除外リストの管理」をクリックします。



(3).「追加」をクリックします。



(4). スキャンを除外したいパスを入力します。  
「ファイルまたはフォルダー」の参照ボタンをクリックします。

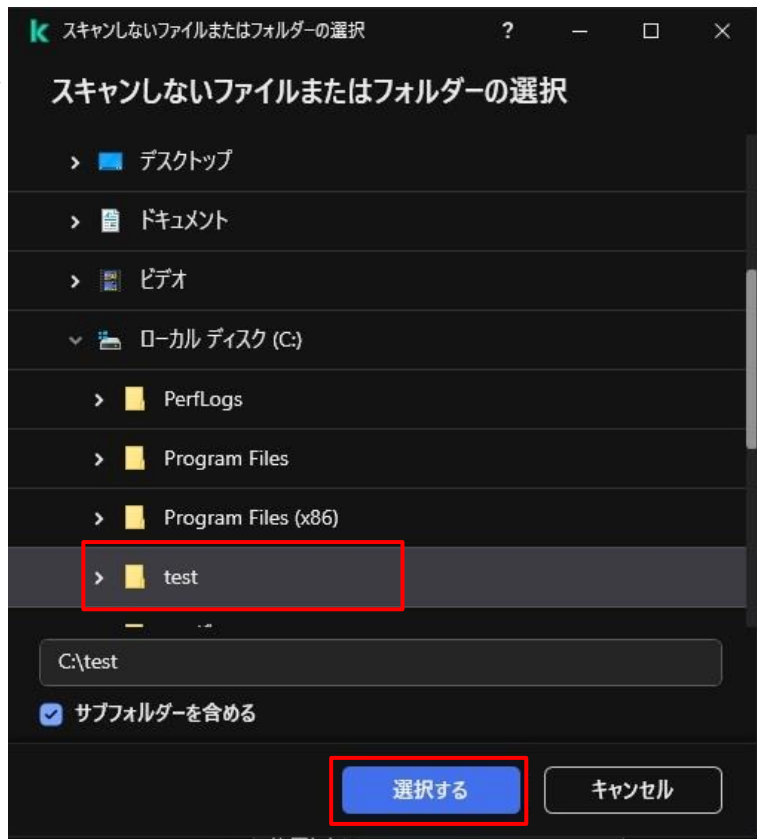


(5). スキャンを除外したいパスを入力します。

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。

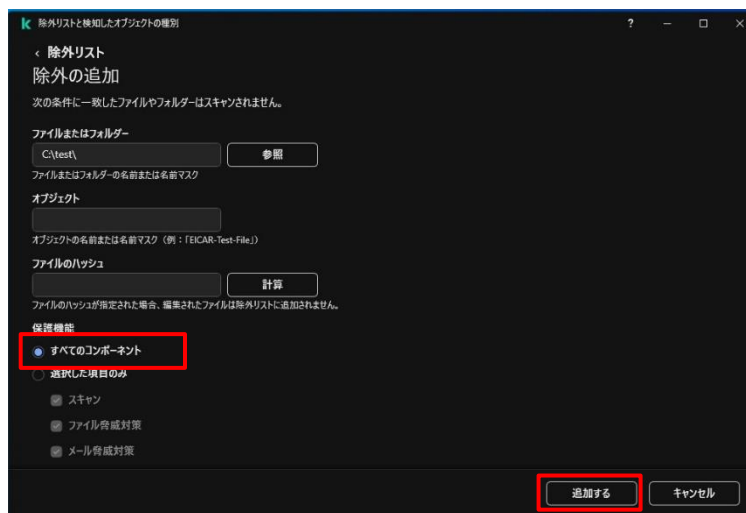
- ※ 手動で入力する場合はフォルダーの最後に¥マークを忘れずに入れてください。最後に¥マークを付けないと、フォルダーとして認識されません。
- ※ 環境変数の指定が可能です。  
(%userprofile%は不可)
- ※ パスを入力する際、「\*」や「?」を使用することができます。
  - ◆ 「C:¥test¥\*.exe」とした場合、test フォルダー配下の拡張子.exe のファイルが対象となります。
  - ◆ 「C:¥\*¥test.exe」とした場合、C ドライブ直下にある任意のフォルダー内の test.exe が対象となります。
  - ◆ 「C:¥test¥???.exe」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). スキャン除外する保護コンポーネントを指定します。

特定できない時は、「すべてのコンポーネント」を選択します。

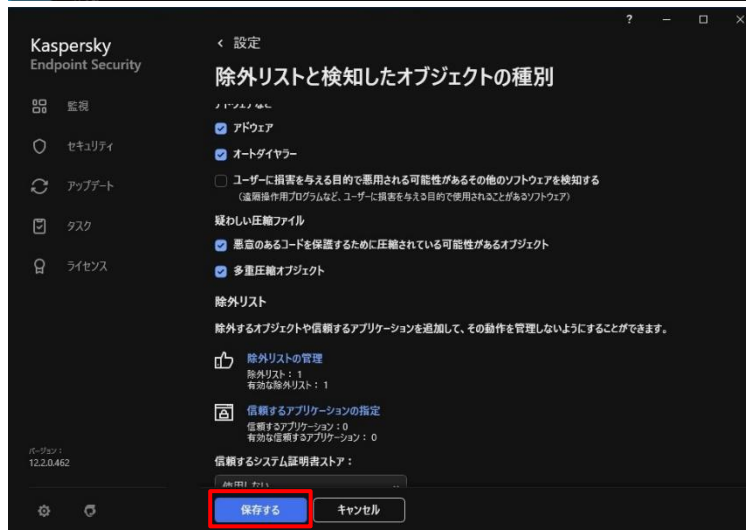
設定後、「追加する」をクリックします。



(7). 設定した内容が登録されていることを確認し、「OK」をクリックします。



(8). 「保存する」をクリックし、設定を保存します。



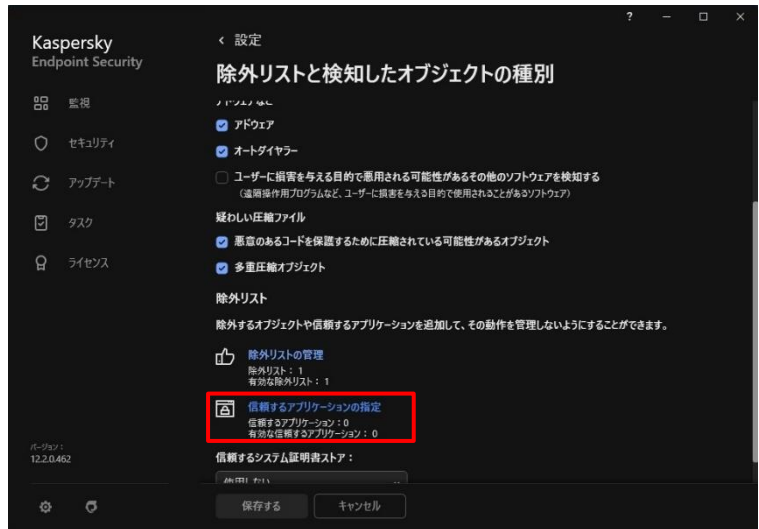
本節は以上です。

## 9.2. 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

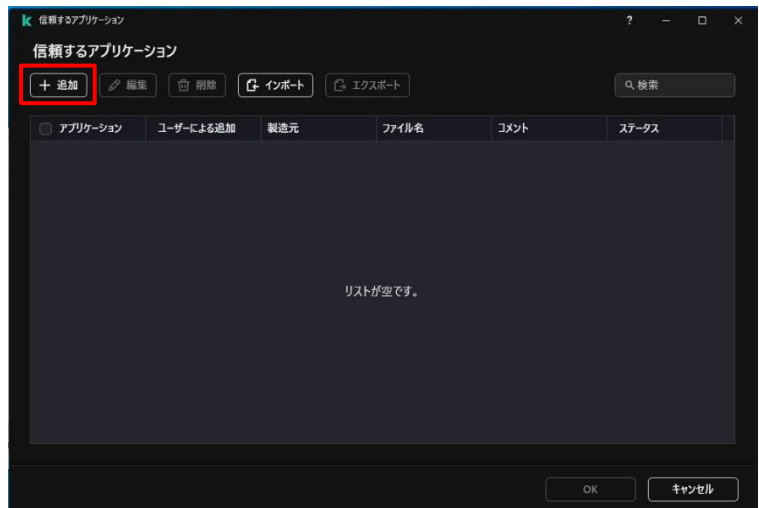
資産管理などのクライアント・サーバー型アプリケーションや自作アプリケーションなど、アプリケーションが KES に検知・ブロックされてしまう場合、実行ファイル単体ではなくアプリケーションの動作をスキャン・監視対象から除外することができます。

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). KES コンソールにて設定アイコンをクリックし、脅威と除外リストを選択します。  
「信頼するアプリケーションの指定」をクリックします。



- (2). 「追加」をクリックします。



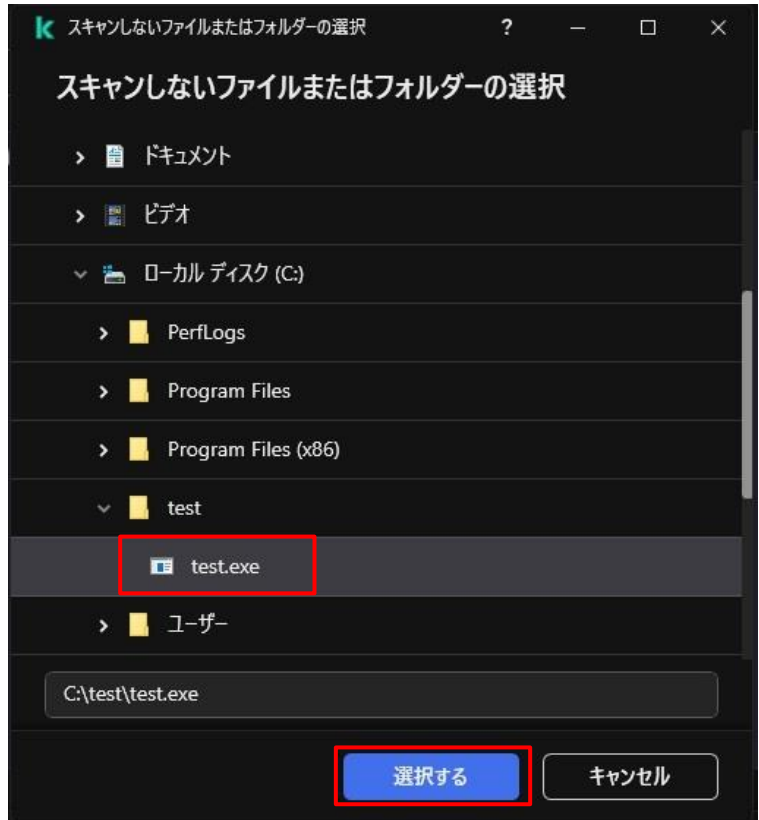
(3). 除外対象とする実行ファイルを選択します。

※ パスは手動入力も可能で、環境変数の指定が可能です。

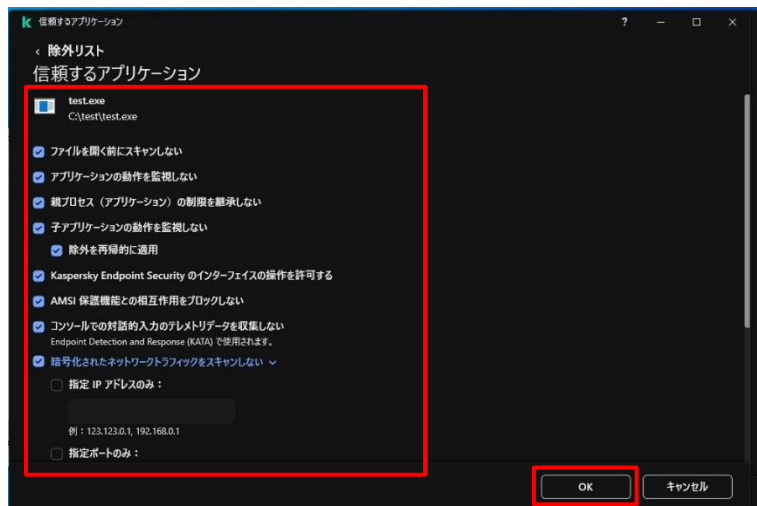
(%userprofile%は不可)

※ パスを入力する際、「\*」や「?」を使用することができます。

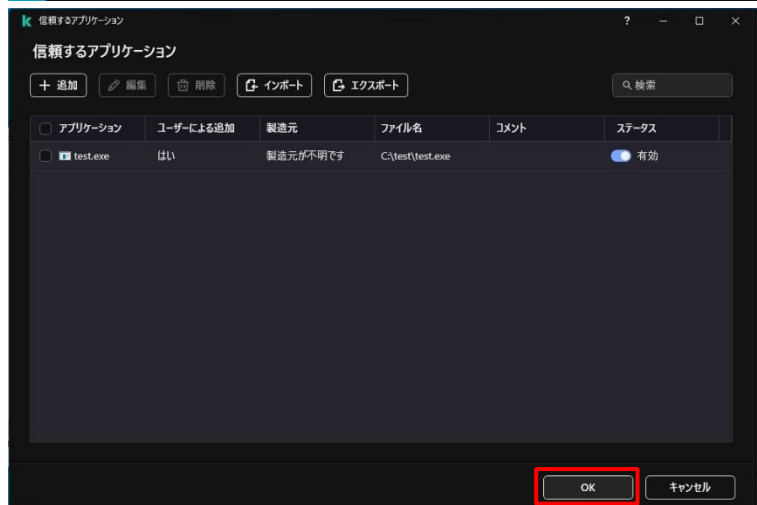
- ◆ 「C:¥test¥\*.exe」とした場合、test フォルダー配下の拡張子.exe のファイルが対象となります。
- ◆ 「C:¥\*¥test.exe」とした場合、Cドライブ直下にある任意のフォルダー内の test.exe が対象となります。
- ◆ 「C:¥test¥???.exe」とした場合、C:¥test フォルダー配下にある 3 文字のファイル名を持つ exe ファイルが対象となります。
- ◆ 「C:¥\*\*\*¥test.exe」とした場合、Cドライブ配下の全階層にある test.exe が対象となります。



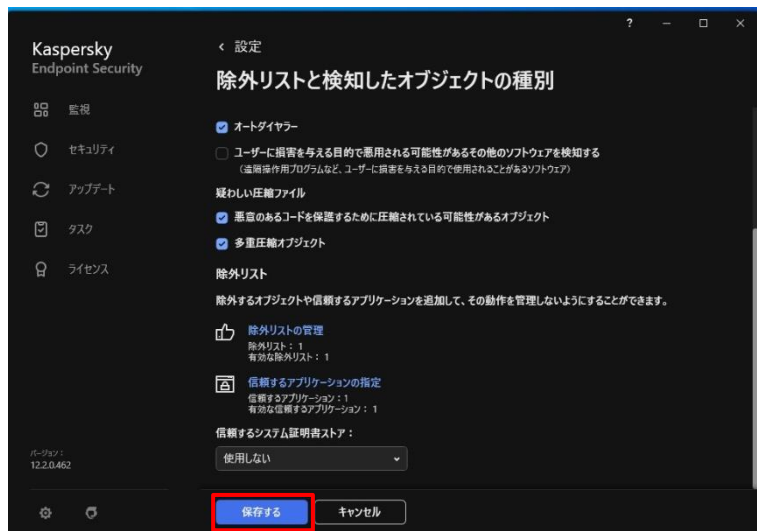
- (4).この実行ファイルに対し、除外したい動作にチェックを入れ、「OK」をクリックします。
- ※ 特定できない場合はすべての項目にチェックを入れてください。



- (5).設定した内容が登録されていることを確認し、「OK」をクリックします。



- (6).「保存する」をクリックし、設定を保存します。



本項は以上です。

## 9.3. 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。

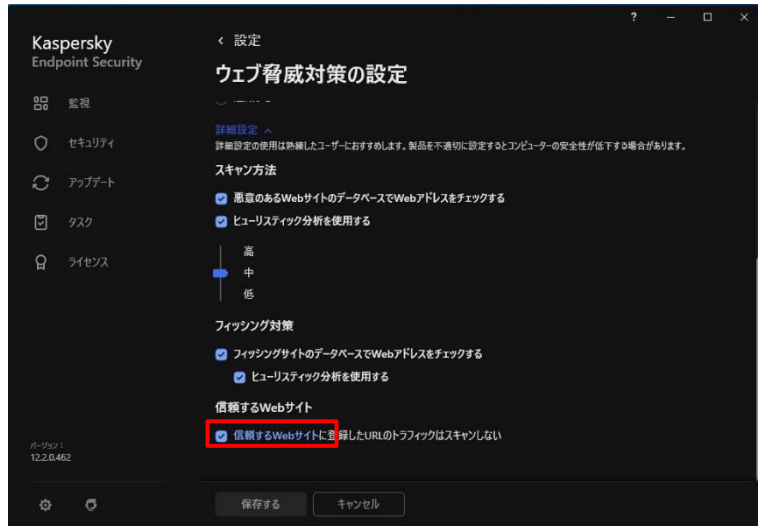
- (1). KES コンソールにて設定アイコンをクリックし、「ウェブ脅威対策」をクリックします。



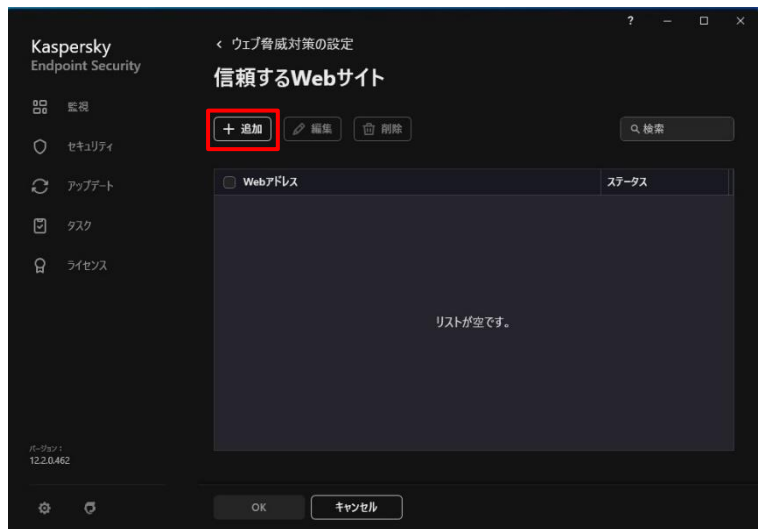
- (2). 詳細設定をクリックします。



(3).「信頼する Web サイト」をクリックします。



(4). 追加をクリックします。



(5). 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、\*.kaspersky.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、

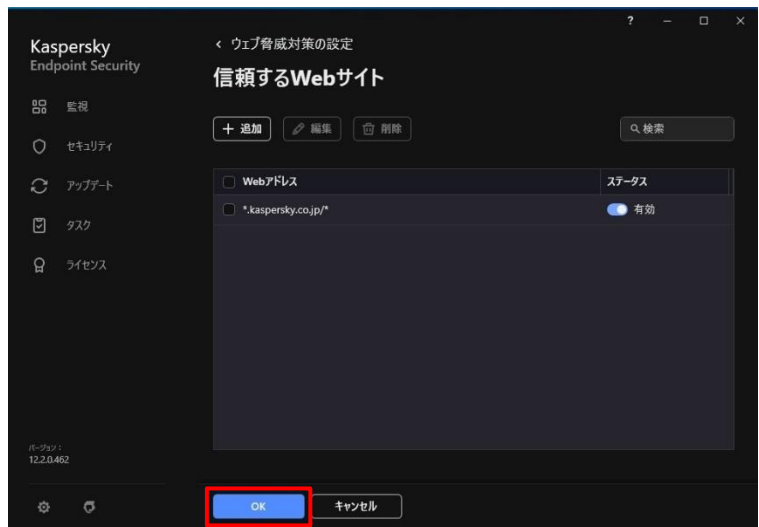
www.test.jp/dl.php¥?fl=と入力します。



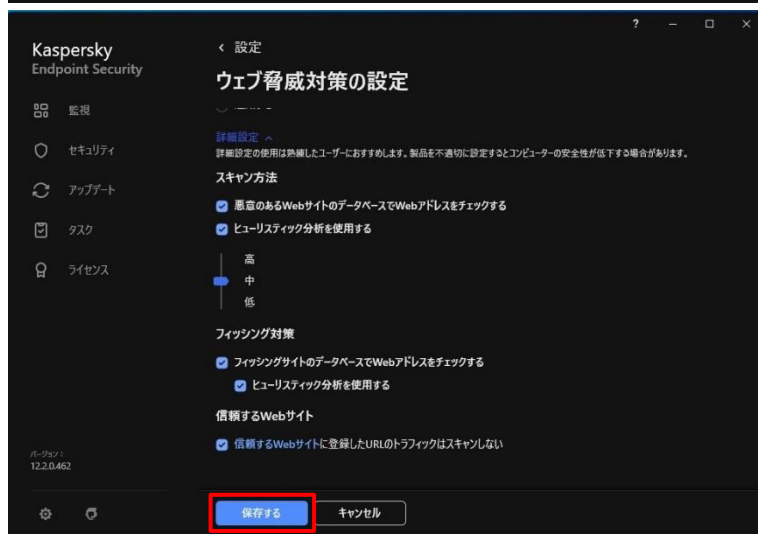




(6). 登録されていることを確認し、「OK」をクリックします。



(7). 「保存する」をクリックし、設定を保存します。



本項は以上です。

## 9.4. 特定のドメインや IP アドレスとの暗号化通信を除外する

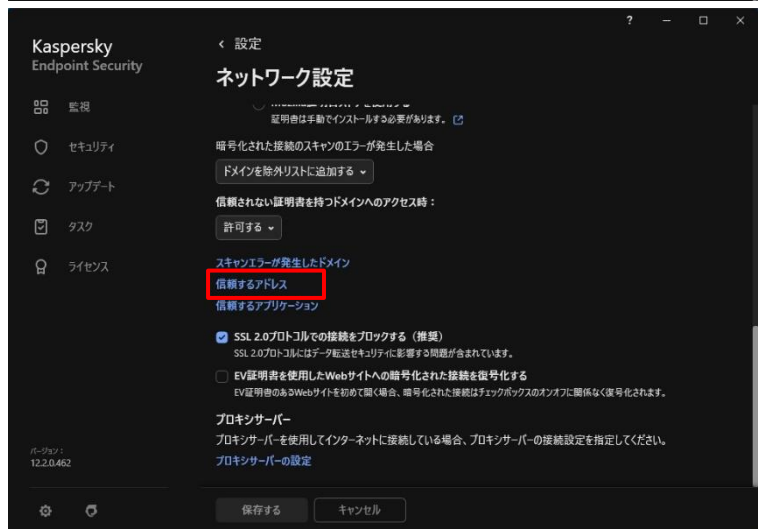
自社ポータルや特定サーバーとの暗号化通信をスキャン対象から除外することができます。

証明書エラーなどが表示される場合、この設定を実施することでエラーが表示されることがなくサイトの閲覧が可能です。

- (1). KES コンソールにて設定アイコンをクリックし、「全般設定」-「ネットワーク設定」をクリックします。



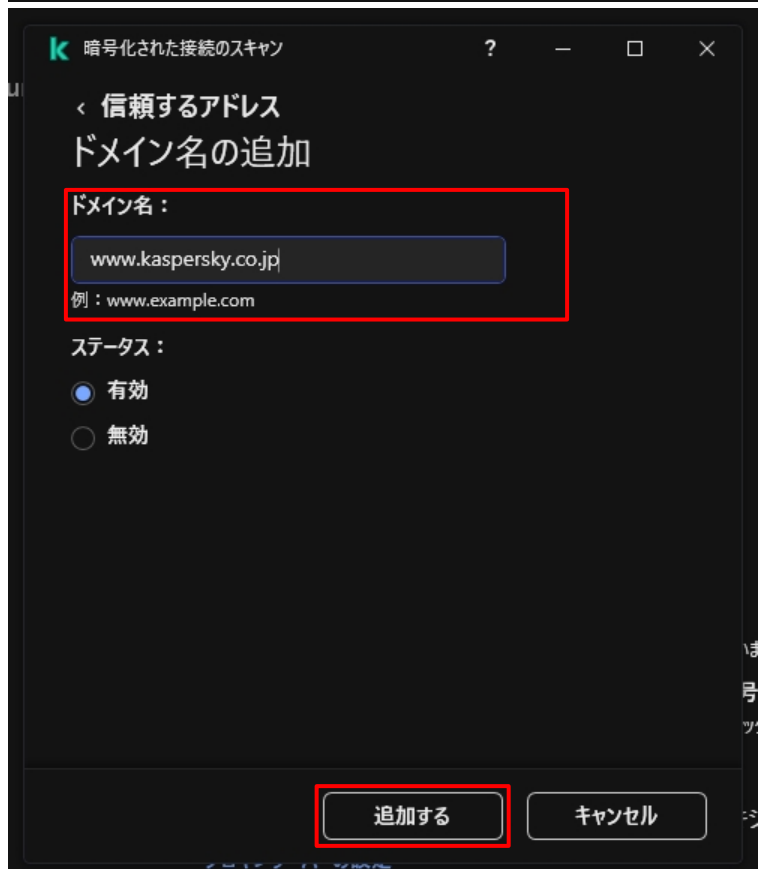
- (2). 「信頼するアドレス」をクリックします。



(3).「追加」をクリックします。



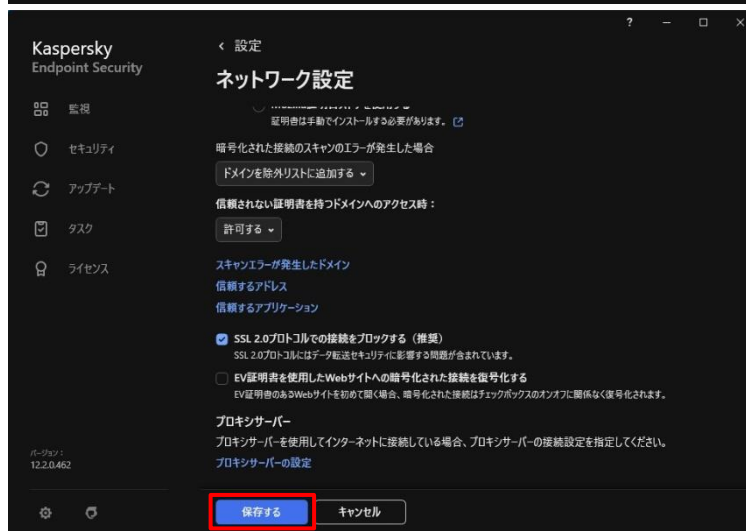
(4).「ドメイン名」に対象となるドメインを入力し、「追加する」をクリックします。



(5).ドメインが追加されていることを確認し、  
「保存する」をクリックします。



(6).「保存する」をクリックし、設定を保存します。



本章は以上です。

### 1. オフライン環境下における定義データベースの更新

---

インターネットに接続されていない環境下で KES を使用する場合があります。

カスペルスキーでは、オフライン環境においても定義データベースの更新ができるよう、定義データベースの取得ツールである「**Kaspersky Update Utility**」というツールを用意しております。

インターネットに接続されている環境でこのツールを使用して定義データベースをダウンロードし、その情報をオフライン環境下のデバイスへコピーします。KES ではそのフォルダーを定義データベースのアップデート元として指定することで定義データベースの更新が可能となります。

指定方法は「6.1 アップデートタスクの設定」をご参照ください。

Kaspersky Update Utility のダウンロード先、および使用方法については以下リンクをご確認ください。

<https://support.kaspersky.co.jp/kuu4-for-windows>



## 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/>

©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 9 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。