Kaspersky Security Center 14
Kaspersky Endpoint Security for Windows
初期設定ガイド

2023/1/27

株式会社カスペルスキー
セールスエンジニアリング部

Ver. 1.0

kaspersky

目次

1. はじめに 3
1.1. 本資料の目的 3
1.2. 導入から運用開始までの流れ 4
2. 前提 5
3. 事前準備（KES のポリシー、タスク作成） 6
3.1. ポリシーの作成 7
3.2. アップデートタスクの作成 11
3.3. スキャンタスクの作成 15
4. 必要な設定項目 20
4.1. パスワードによるアプリケーションの保護 20
4.1.1. KES ポリシーの設定 20
4.1.2. NA ポリシー設定 27
4.2. 「ディストリビューションポイント」の自動割り当て解除 30
4.3. イベント通知設定 32
4.4. ウイルスアウトブレイク通知設定 38
4.5. 除外設定 42
4.6. ウェブコントロール設定（バナー広告ブロック） 43
4.7. ログオンの監査の有効化 50

Appendix 51
1. 「管理サーバークイックスタートウィザード」をキャンセルした場合 51
2. インターフェイスの設定 52

1. はじめに

1.1. 本資料の目的

本資料では、法人向け製品を使用した環境を構築後、運用を開始する前に、Kaspersky Security Center や Kaspersky Endpoint Security for Windows において、必ず設定していただきたい項目についてご説明します。

1.2. 導入から運用開始までの流れ

カスペルスキー製品の導入から運用開始までの流れ、および本資料の位置づけについてご説明します。

STEP 1.

アプリケーションの概要確認

→ **「Kaspersky Endpoint Security 製品紹介」**をご参照ください。

STEP 2.

管理サーバー機能のインストール、及びアンチウイルス製品のインストール

→ **「KSC14 簡単インストールガイド」**
「KES14 簡単リモートインストールガイド」をご参照ください。

STEP 3.

ポリシー・タスクの設定

→ **「ポリシータスクの考え方」「ポリシータスク設定 実践編」**をご参照ください。

STEP 4.

運用開始前に必要な設定の実施

→ **本資料を参照し、各設定を実施してください。**

STEP 5.

運用開始

→ **「Kaspersky 運用ガイド」を参照し、各手順に従い運用してください。**

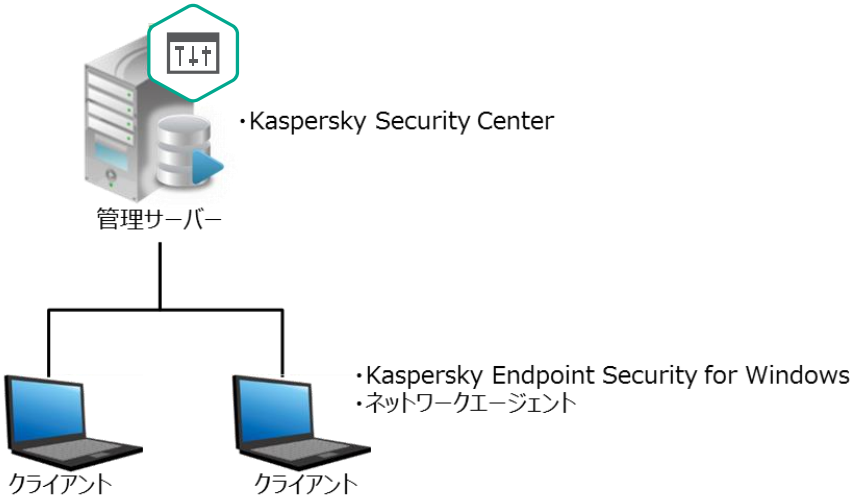
上述の各資料は、以下サイトから閲覧、ダウンロードすることができます。

- 法人のお客様向けダウンロード資料（https://kasperskylabs.jp/biz/）

2. 前提

本資料は、以下の環境構成を前提としております。

- ✓ 管理サーバーとして Kaspersky Security Center が導入されている。
- ✓ 管理下の Windows に Kaspersky Endpoint Security for Windows が導入されている。
- ✓ 管理サーバーにてデバイスが管理されている。



■ 用語説明

① **管理サーバー：**

Kaspersky Security Center がインストールされた Windows サーバーです。

② **Kaspersky Security Center（以降 KSC）：**

管理サーバーにインストールされた Kaspersky 製品を管理するアプリケーションです。

Kaspersky Security Center ネットワークエージェントがインストールされたデバイスの管理と、定義データベースの配信を行います。

③ **Kaspersky Endpoint Security for Windows（以降 KES）：**

デバイスを保護するアンチウイルスアプリケーションです。

管理サーバー及び管理下のコンピューターにインストールされます。

④ **Kaspersky Security Center ネットワークエージェント（以降 NA）：**

KSC とデバイスが通信をするために必要となるアプリケーションです。

管理下のデバイスにインストールされます。（管理サーバーは KSC に含まれています）

3. 事前準備（KES のポリシー、タスク作成）

KSC14 では KES のインストールパッケージは同梱されておらず、使用する場合は以下のうちいずれかの方法でインストールパッケージ（アプリケーション管理プラグインも同様）を登録する必要があります。

- **「管理サーバークイックスタートウィザード」内で登録**

  手順は「KSC14 簡単インストールガイド」の「3.2 KSC の初期設定」をご参照ください。

  この手順を実施した場合、KES のポリシー、および定義データベース更新タスクは自動で作成されますので、「3.1 ポリシーの作成」および「3.2 アップデートタスクの作成」は実施不要です。

  「3.3 スキャンタスクの作成」を参考に、スケジュールを設定したスキャンタスクを作成してください。

- **インストーラーをダウンロードし、「インストールパッケージ」を作成**

  手順は「KSC14 簡単インストールガイド」の「Appendix 1. KSC に対しインストールパッケージの登録」をご参照ください。

  この手順を実施した場合、ポリシー、タスクは自動的に作成されません。

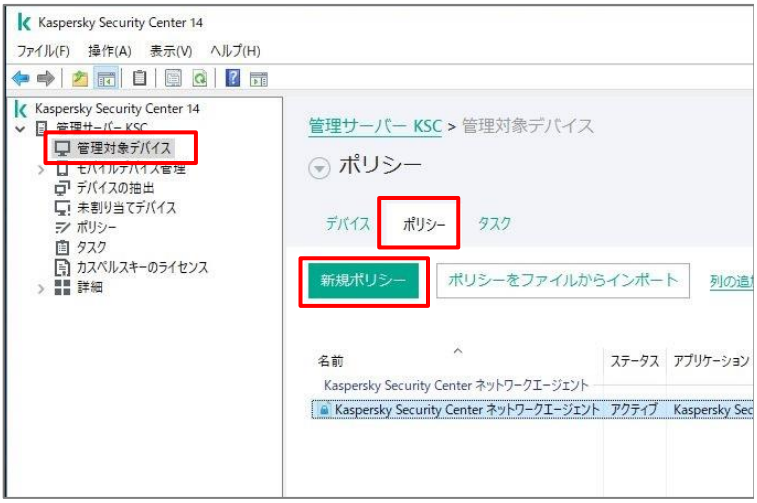
  本章の手順「3.1 ポリシーの作成」、「3.2 アップデートタスクの作成」、「3.3 スキャンタスクの作成」を実施してポリシー、各タスクを作成してください。

参考：「Kaspersky Security Center 14 簡単インストールガイド」
https://kasperskylabs.jp/biz/

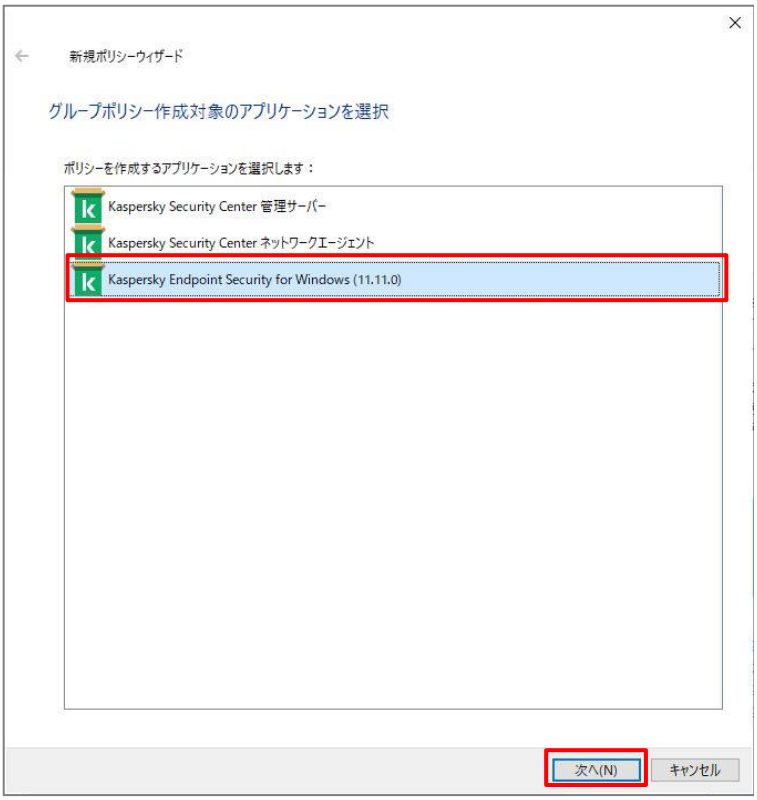
3.1.　ポリシーの作成

ここでは、KES のポリシーを作成する手順をご説明します。

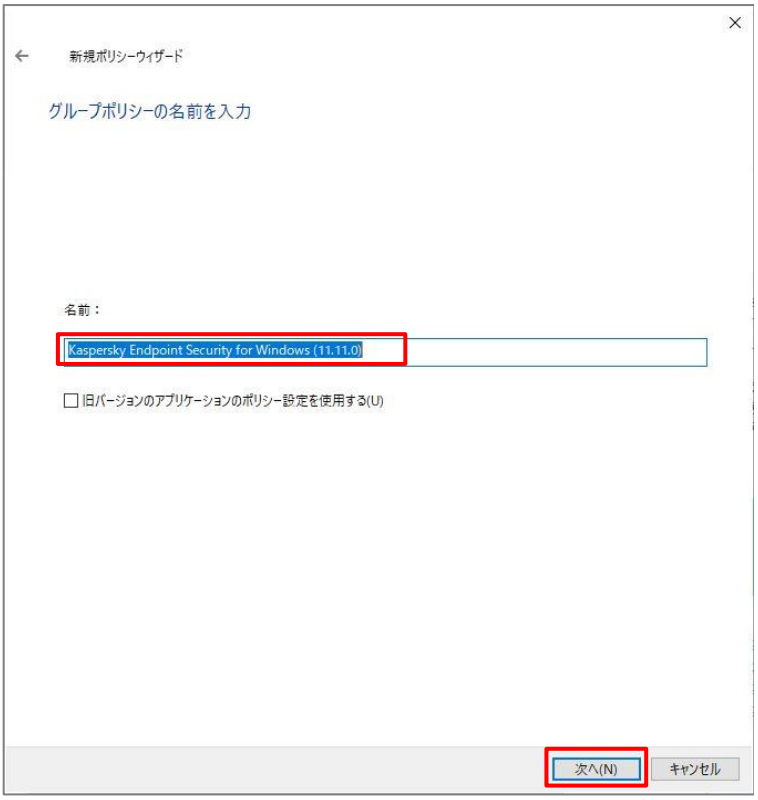
(1) 管理コンソールにて「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
「新規ポリシー」ボタンをクリックします。



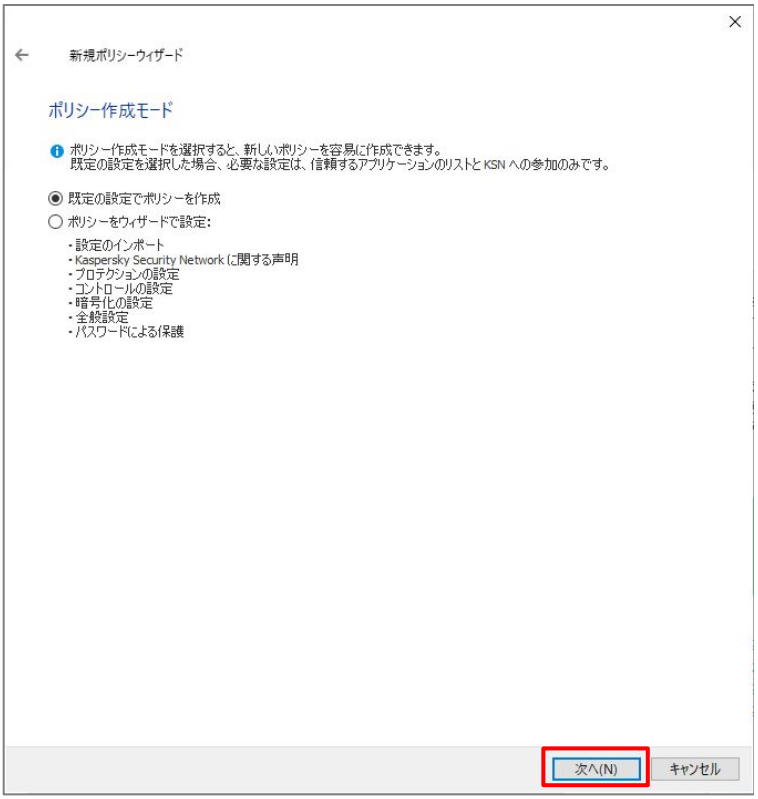
(2) 新規ポリシーウィザードが起動します。
「Kaspersky　Endpoint Security for Windows(xx.xx.xx)」を選択し、「次へ」をクリックします。



(3) 任意のポリシー名を入力し、「次へ」をクリックします。

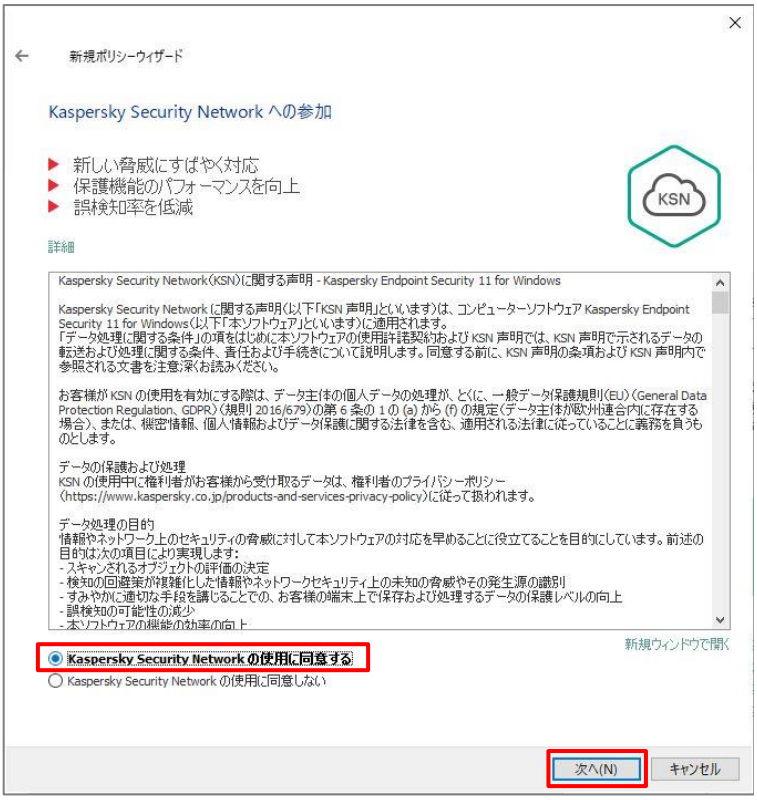


(4) 既定値のまま「次へ」をクリックします。



(5)「Kaspersky Security Network の使用に同意する」にチェックを入れ、「次へ」をクリックします。

※ インターネット接続のないクローズド環境の場合は「・・・同意しない」にチェックを入れてください。



(6)ポリシーのステータスにて「アクティブポリシー」にチェックがあることを確認し、「完了」をクリックします。

※ 作成だけ行い、デバイスに適用させたくない場合は「非アクティブポリシー」を選択して作成してください。
設定後、ポリシーのプロパティにて「アクティブ」に変更するとデバイスへ適用されます。

(7) 一覧に KES のポリシーが作成されていることを確認します。

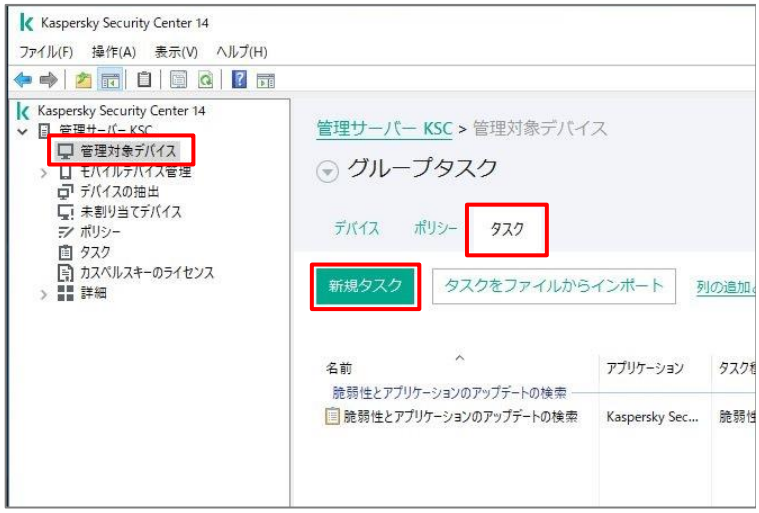
ステータスが「アクティブ」となっているポリシーがクライアントに適用されます。

本節は以上です。

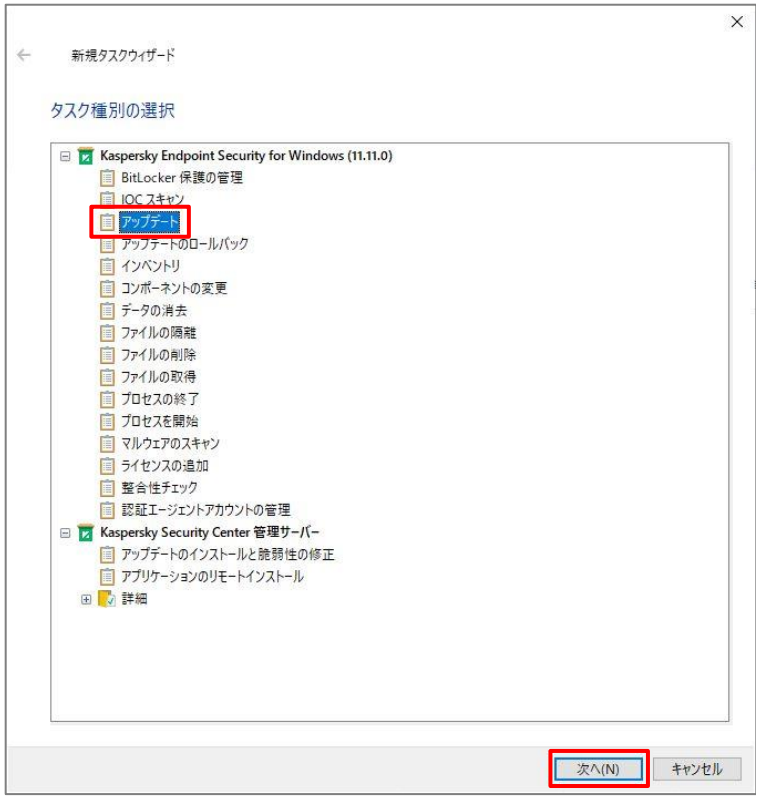
3.2. アップデートタスクの作成

ここでは、KES に対し、KSC から定義データベースを更新するためのタスクを作成する手順をご説明します。

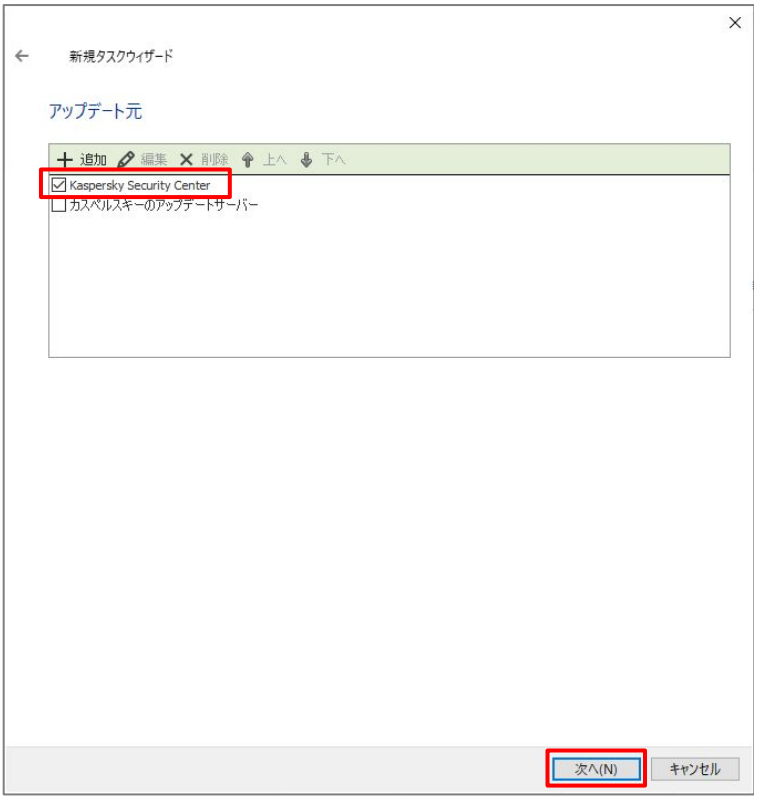
(1)「管理対象デバイス」を開き、右画面にて「タスク」タブを開きます。
「新規タスク」ボタンをクリックします。



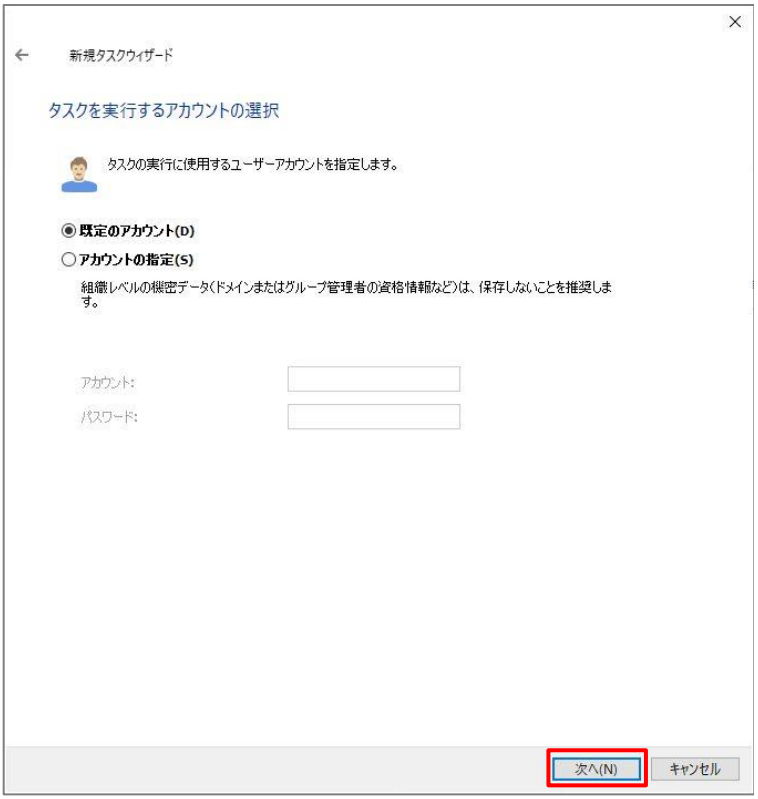
(2)新規タスクウィザードにて「Kaspersky Endpoint Security for Windows」配下の「アップデート」を選択し、「次へ」をクリックします。



(3) アップデート元として「Kaspersky Security Center」が選択されていることを確認し、「次へ」をクリックします。

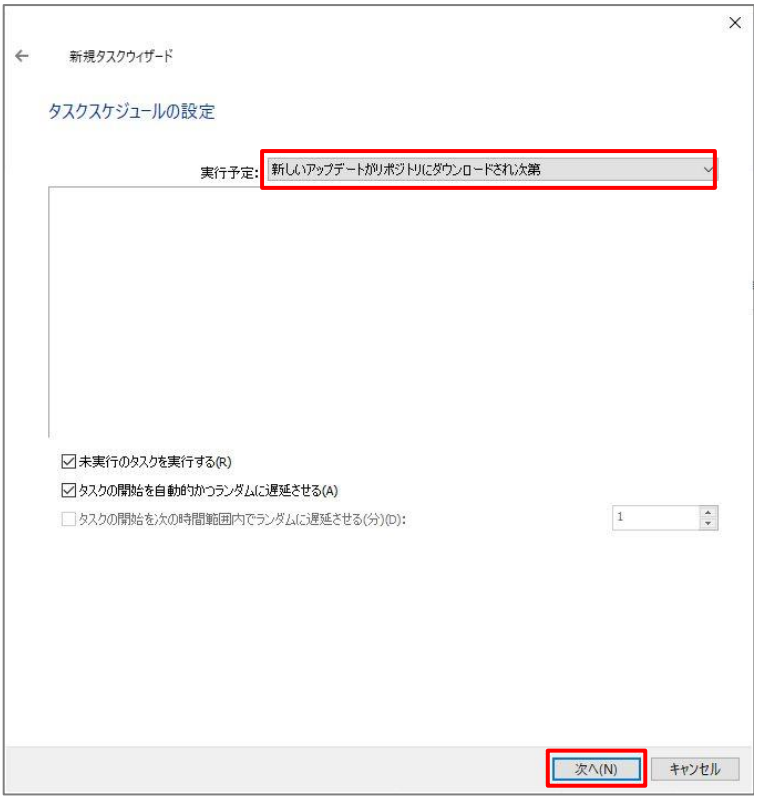


(4) タスクを実行するアカウントの選択では、既定値のまま「次へ」をクリックします。



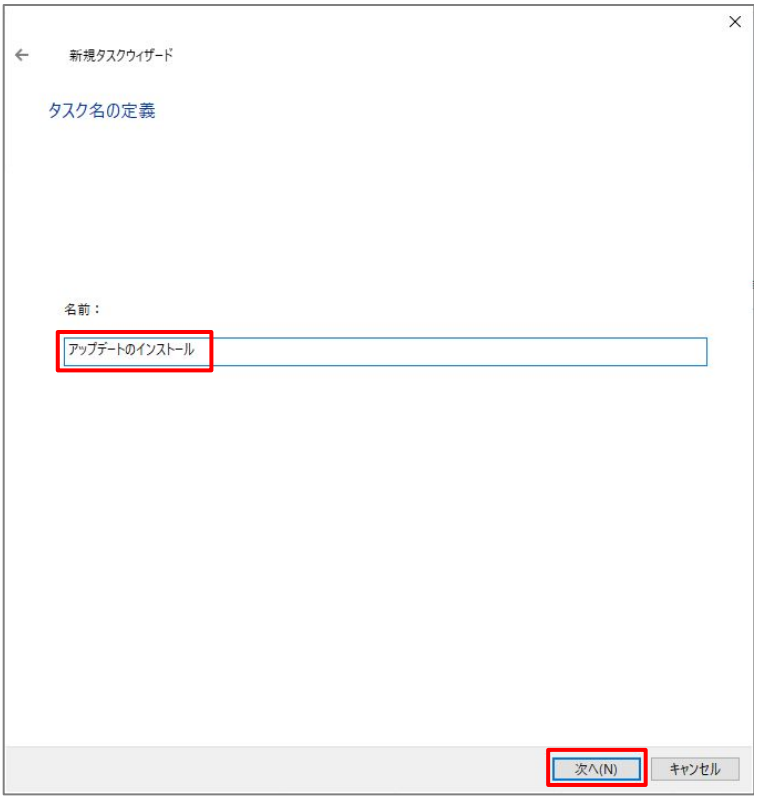
(5) タスクスケジュールの設定にて任意のスケジュールを設定し、「次へ」をクリックします。

ここでは、KSC が新しい定義データベースをダウンロードした場合に随時更新されるよう「新しいアップデートがリポジトリにダウンロードされ次第」と設定しています。

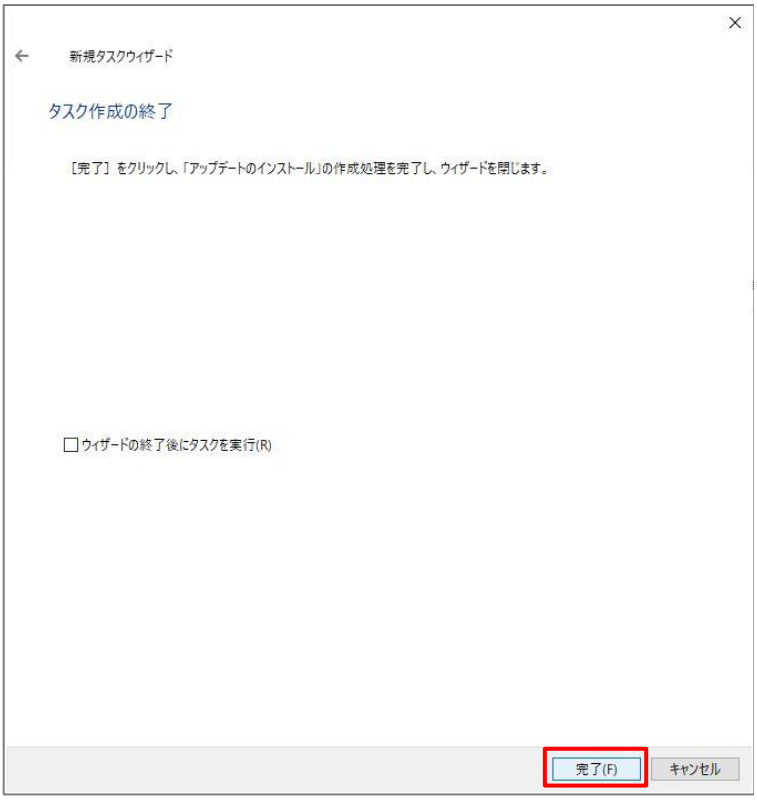


(6) 任意のタスク名を入力し、「次へ」をクリックします。

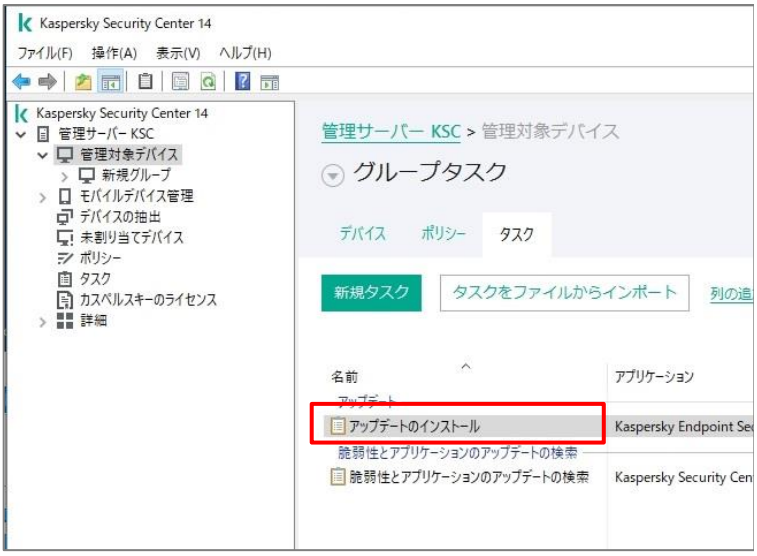
ここでは、「アップデートのインストール」という名前を設定しています。



(7) 正常に作成されたことを確認し、「完了」をクリックします。



(8) タスクの一覧に作成したタスクが表示されていることを確認します。



本節は以上です。

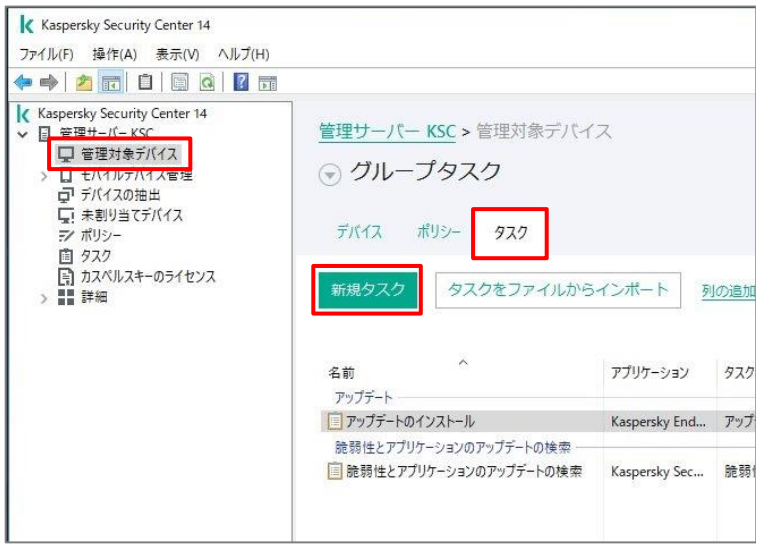
3.3. スキャンタスクの作成

ここでは、KES に対し、KSC から定義データベースを更新するためのタスクを作成する手順をご説明します。

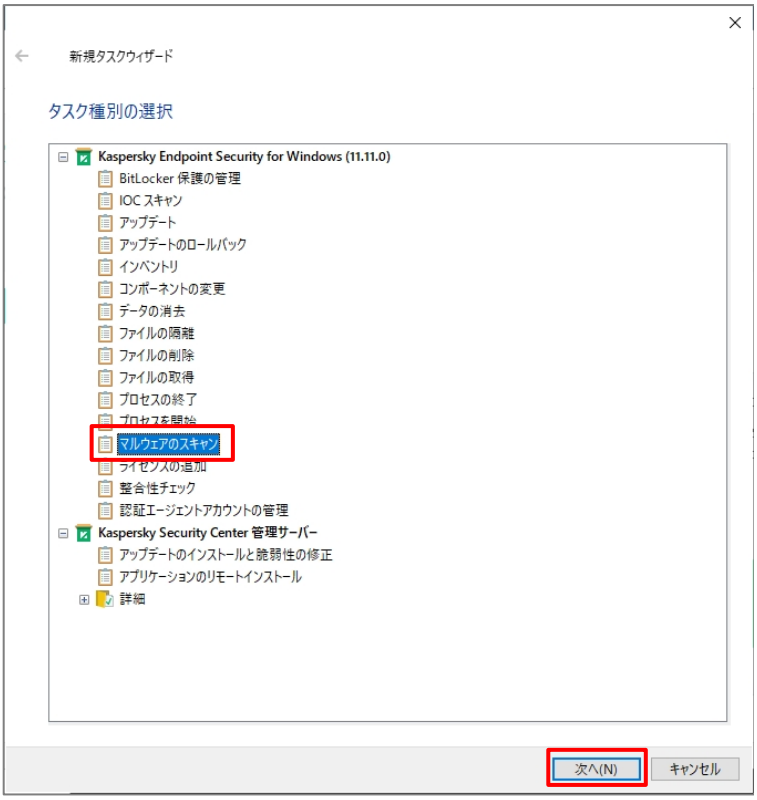
スキャンを定期的に実行することで、セキュリティレベルの設定が低いなどの理由により、保護コンポーネントで検知されない悪意のあるソフトウェアが拡散する可能性を排除できます。

KSC インストール後にクイックスタートウィザードを実行すると、KES のポリシーやタスクが自動的に作成されますが、KES のスキャンタスクは作成されないため、本手順を参照しスキャンタスクを作成してください。

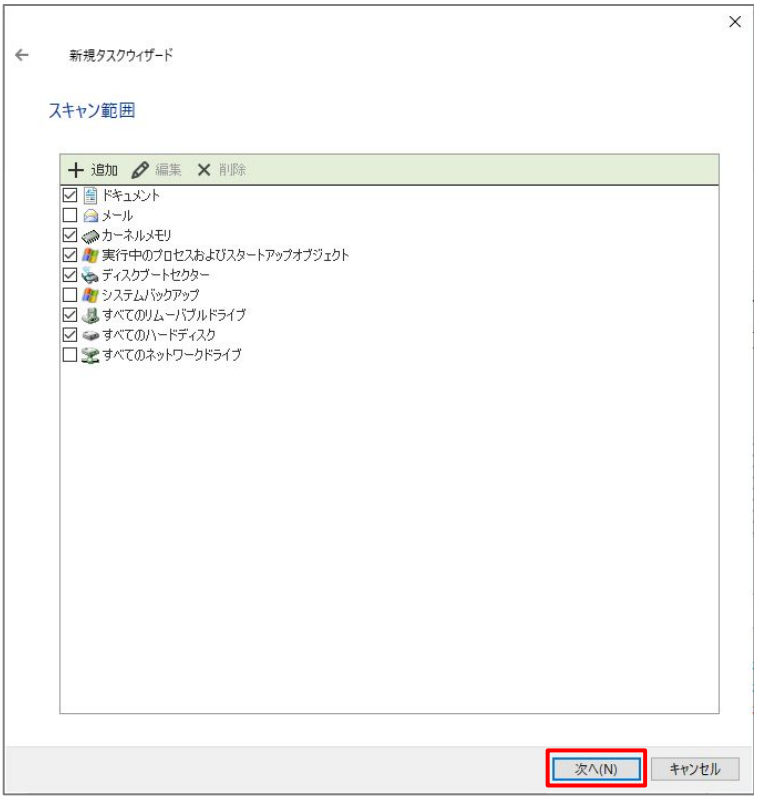
(1)「管理対象デバイス」を開き、右画面にて「タスク」タブを開きます。
「新規タスク」ボタンをクリックします。



(2)新規タスクウィザードにて「Kaspersky Endpoint Security for Windows」配下の「マルウェアのスキャン」を選択し、「次へ」をクリックします。

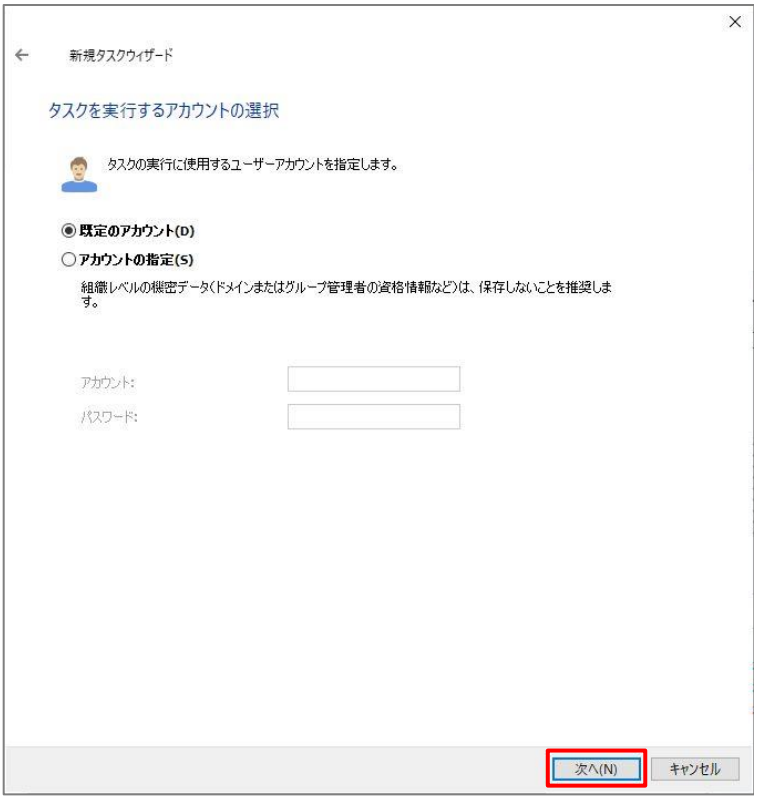


(3)任意のスキャン範囲を選択し、「次へ」をクリックします。
ここでは既定値を設定しています。



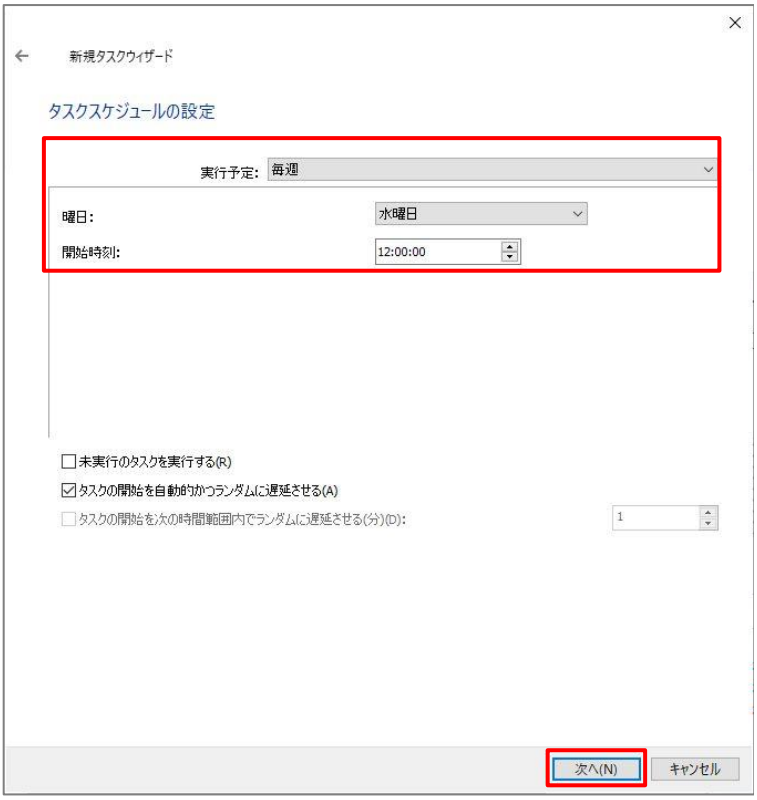
(4) 処理の設定では、既定値のまま「次へ」をクリックします。

(5) タスクを実行するアカウントの選択では、既定値のまま「次へ」をクリックします。



(6) タスクスケジュールの設定にて任意のスケジュールを設定し、「次へ」をクリックします。

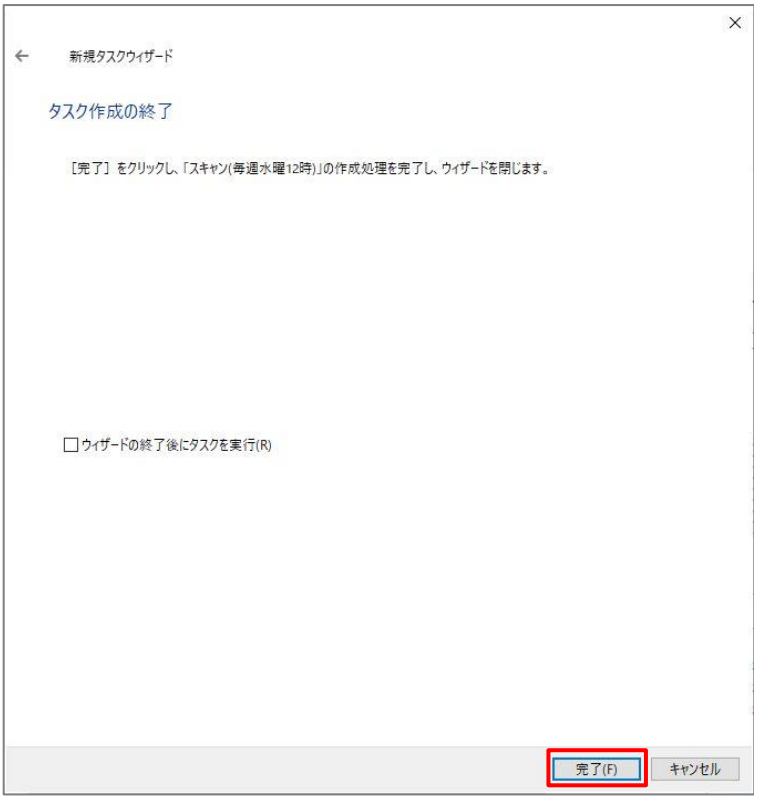
ここでは、毎週水曜日 12:00 から開始されるよう設定しています。



(7) 任意のタスク名を入力し、「次へ」をクリックします。

ここでは、「定時スキャン（毎週水曜 12 時）」という名前を設定しています。

(8) 正常に作成されたことを確認し、「完了」をクリックします。



(9) タスクの一覧に作成したタスクが表示されていることを確認します。

本章は以上です。

4.　必要な設定項目

KSC にて KES を管理している環境下において、必要な設定項目についてご説明します。
セキュリティの保護、また不要なトラブルを避けるために、以下にご案内いたします設定を必ず実施してください。

4.1.　パスワードによるアプリケーションの保護

KES、及び NA に対し、パスワードによる保護を設定することができます。（既定では無効）
パスワードによる保護を設定することで、デバイスの利用者が KES プロセスを終了しようとした場合や、アンインストールしようとした場合に、パスワード入力を求める画面が表示されます。
意図的な KES プロセスの停止やアンインストールを制限することでデバイスの保護を強固にします。

【注意】
KSC から KES のアップグレードやアンインストールを行う場合は、「パスワードによる保護」を一時的に無効化する必要があります。

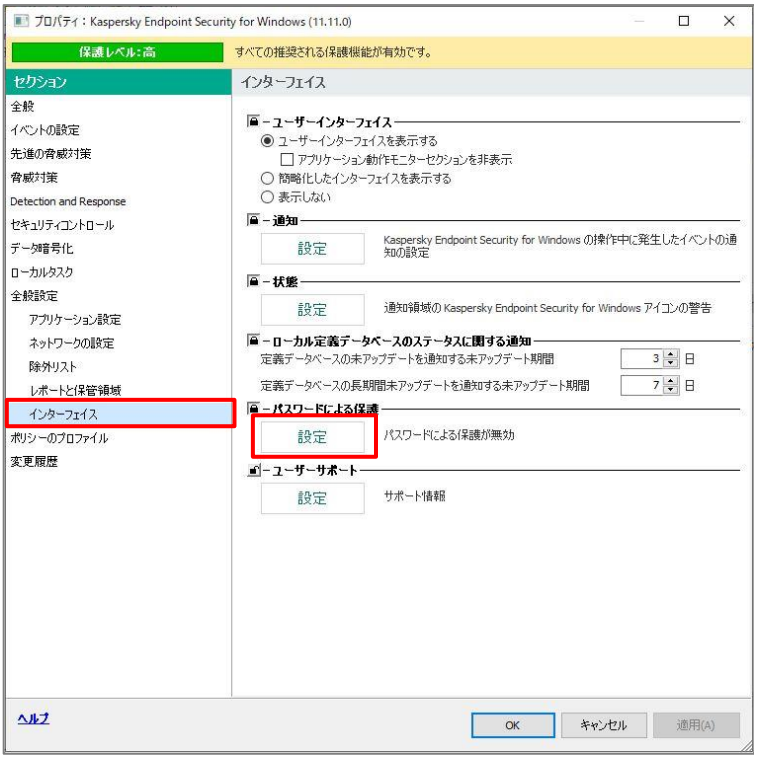
以下に KES、NA に対し、「パスワードによる保護」を有効化する手順をご説明します。

4.1.1.　KES ポリシーの設定

(1)「管理対象デバイス」を開き、右画面にて「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」を開きます。

(2)ポリシーのプロパティ画面にて、「全般設定」-「インターフェイス」セクションを開きます。

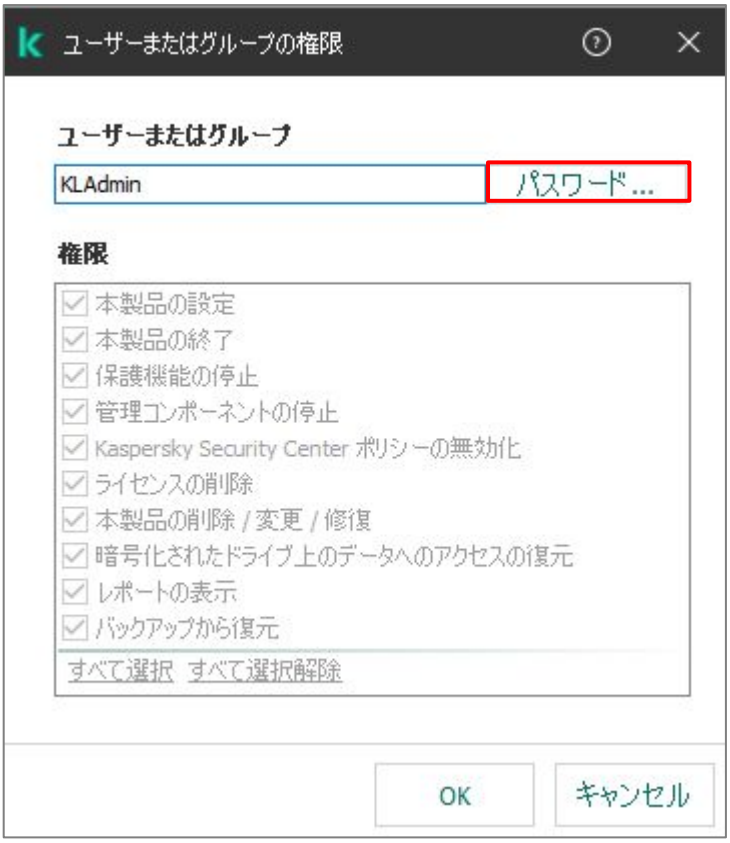
右画面にて「パスワードによる保護」の「設定」ボタンをクリックします。



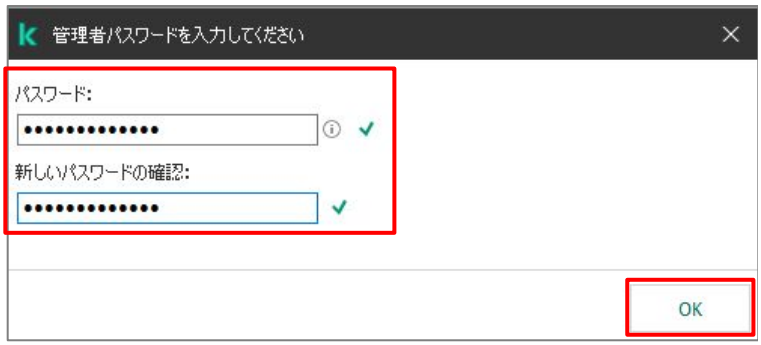
(3)「パスワードによる保護を有効にする」にチェックを入れます。
「KLAdmin」を選択し、「編集」をクリックします。

※ 「KLAdmin」は、既定で設定されているパスワード保護のアカウント名です。
(4)で変更することも可能です。

(4)「パスワード」をクリックします。



(5)「パスワード」と「新しいパスワードの確認」を入力し、「OK」をクリックします。

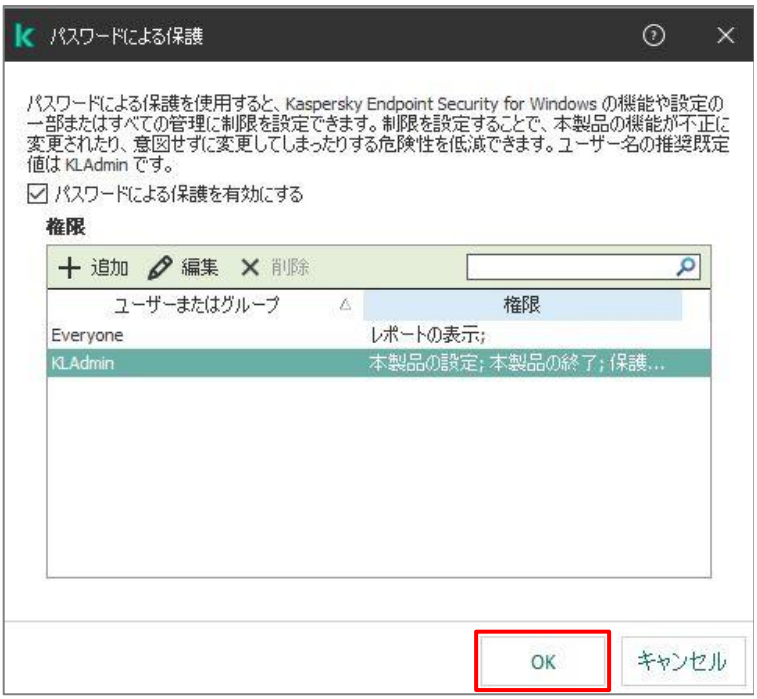


以下のパスワード要件を満たさない場合、警告が表示されます。（設定は可能）

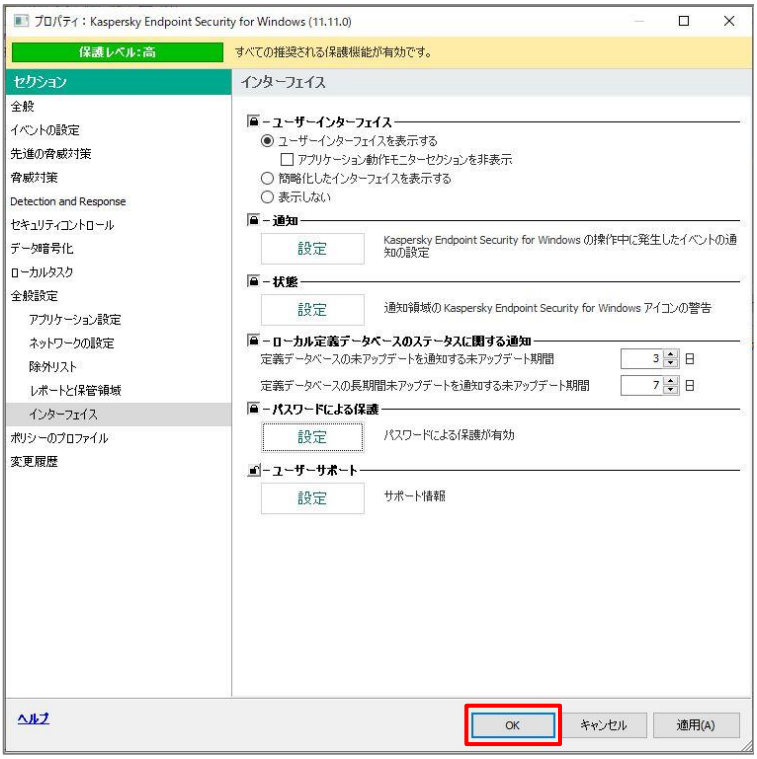
・8 文字以上
・次の各文字種別から 1 文字以上使用：
　-大文字アルファベット
　-小文字アルファベット
　-数字
　-特殊文字(~!@#%^{}[]<>?;':,/¥-_=+)

(6)「OK」をクリックし、設定を保存します。
既定では、すべての操作がパスワード保護の対象になっています。

(7)「OK」をクリックし、設定を保存します。



(8)「OK」をクリックしてポリシーのプロパティ画面を閉じます。

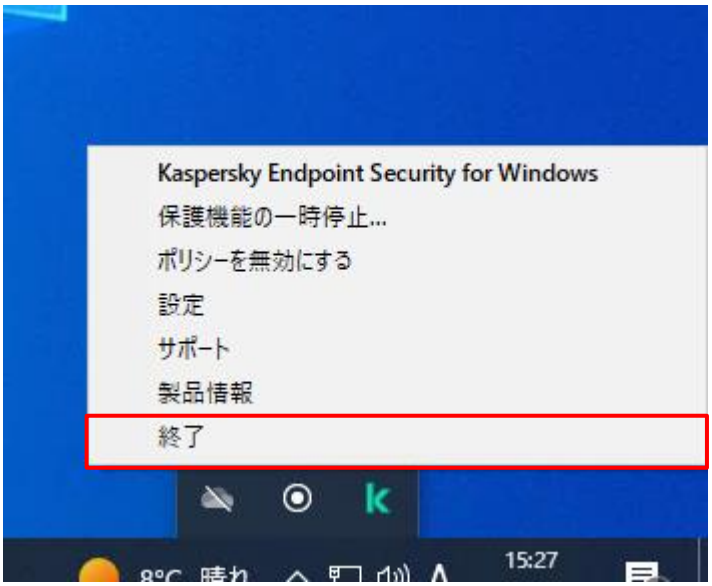


設定は以上になります。

デバイスに KES ポリシーが適用されると、パスワード保護機能が有効となります。

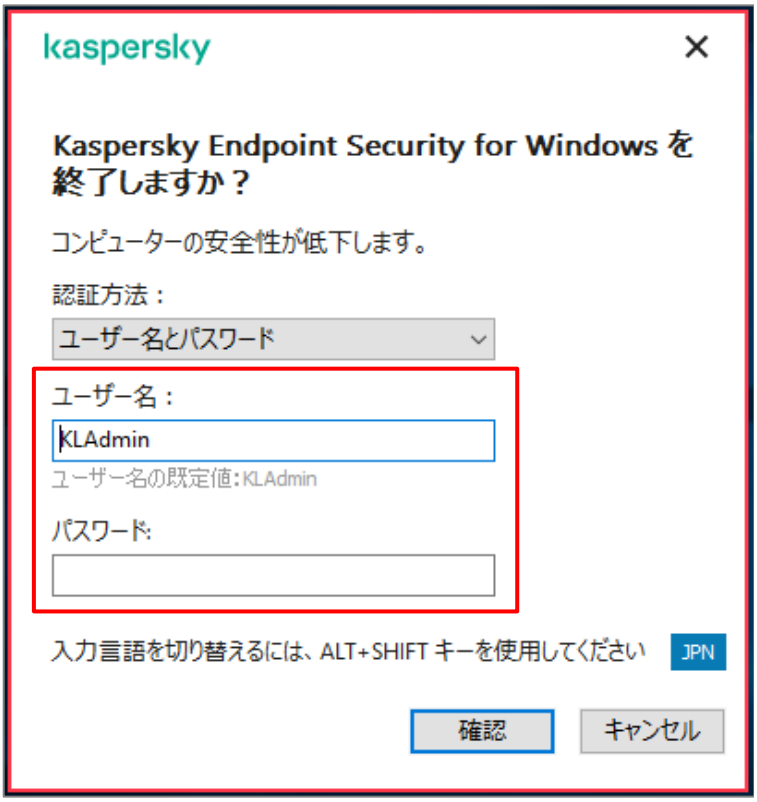
デバイス側で KES を終了しようとした場合、以下のようにダイアログが表示されます。

(1) デバイスにて、タスクバーの KES アイコンを右クリックし、「終了」を選択します。



(2) ユーザー名とパスワードの入力を求めるダイアログが表示されます。

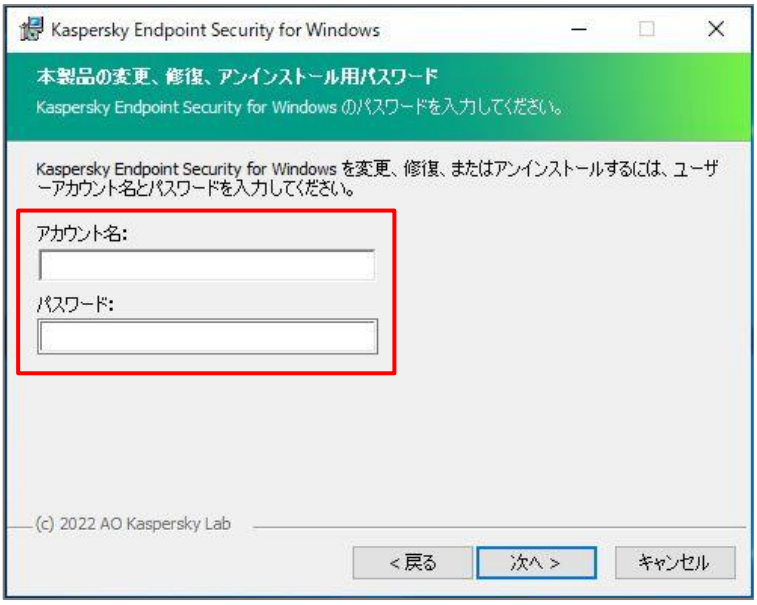
正しいユーザー名、パスワードを入力しないと、KES を終了させることはできません。



また、デバイスにて KES をアンインストールしようとした際にも、以下のようにアカウントの入力を求められます。

(1) デバイスにて「コントロールパネル」-「プログラムと機能」から KES をアンインストールしようとすると、ウィザード内で右のようにアカウントの入力を求められます。

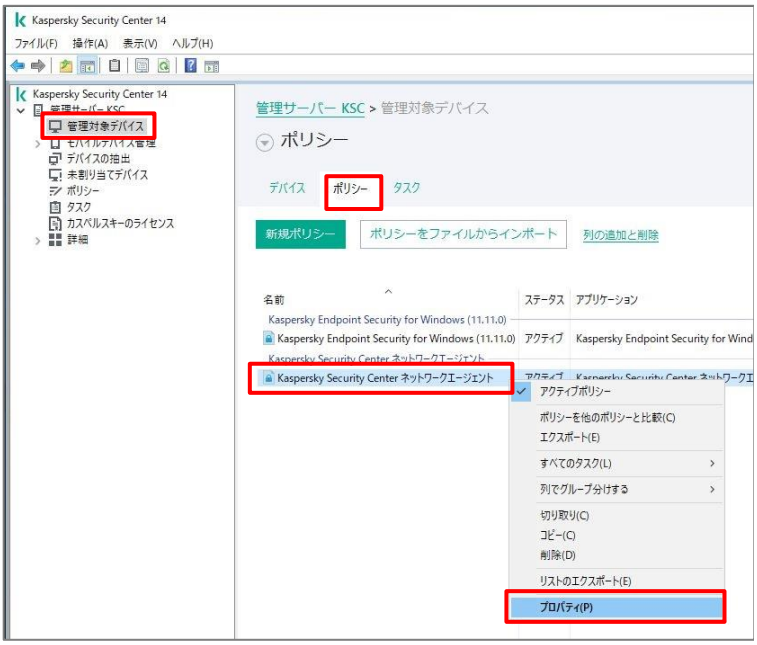
正しいユーザー名、パスワードを入力しないと、KES をアンインストールすることはできません。



本項は以上です。

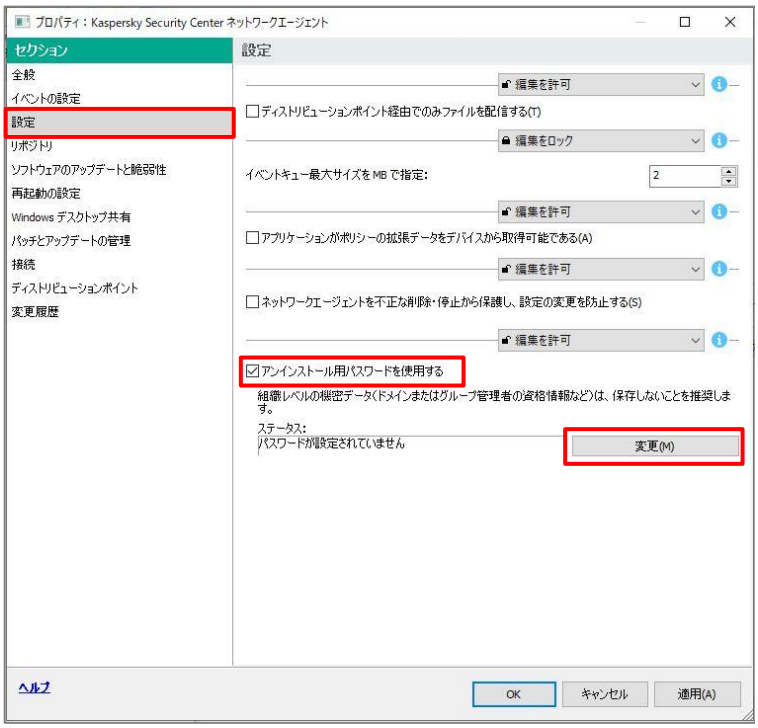
4.1.2. NA ポリシー設定

(1) 「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
NA のポリシーを右クリックし、「プロパティ」を開きます。

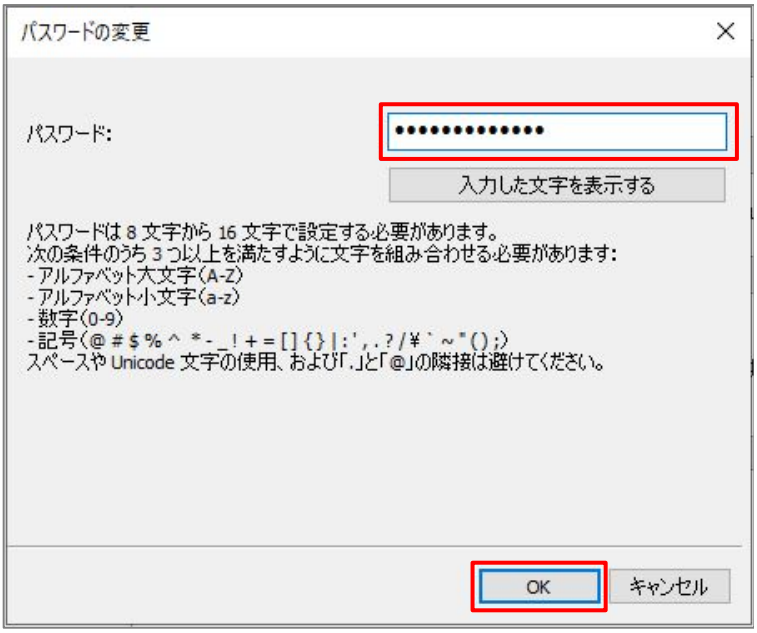


(2) 「設定」セクションを開きます。

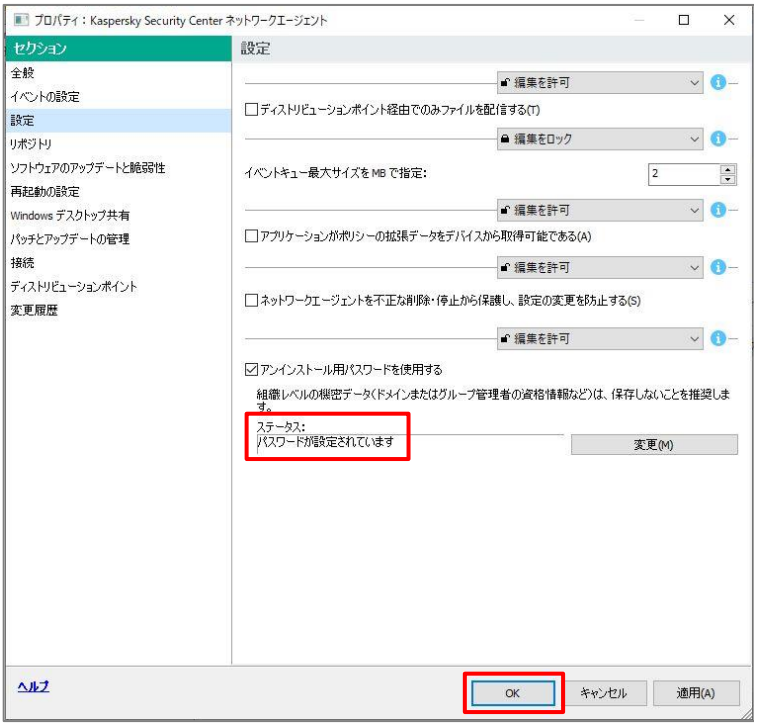
「アンインストール用パスワードを使用する」にチェックを入れ、「変更」ボタンをクリックします。



(3) ダイアログに新しいパスワードを入力し、「OK」をクリックします。



(4) ステータスに「パスワードが設定されています」と表示されていることを確認後、「OK」をクリックし、プロパティ画面を閉じます。



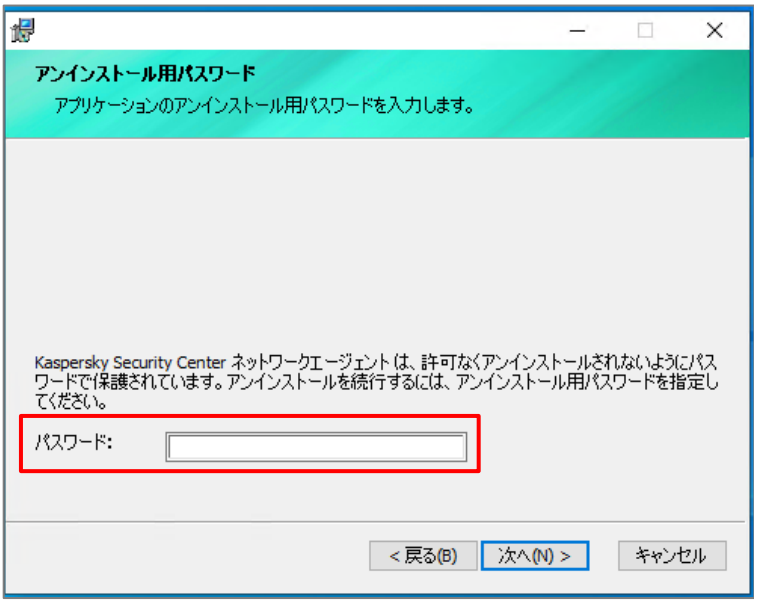
設定は以上になります。

デバイスに NA ポリシーが適用されると、パスワード保護機能が有効となります。

クライアント側で NA をアンインストールしようとした場合、以下のようにダイアログが表示されます。

(1) デバイスにて「コントロールパネル」-「プログラムと機能」から NA をアンインストールしようとすると、ウィザード内で右のようにアカウントの入力を求められます。

正しいパスワードを入力しないと、NA をアンインストールすることはできません。



本節は以上です。

4.2. 「ディストリビューションポイント」の自動割り当て解除

「ディストリビューションポイント」とは、定義データベースやインストールパッケージの配信元となる機能です。
ディストリビューションポイントを設定することで、管理下のデバイスは定義データベースをディストリビューションポイントから取得するようになるため、ネットワークトラフィックや KSC の負荷を軽減することができます。

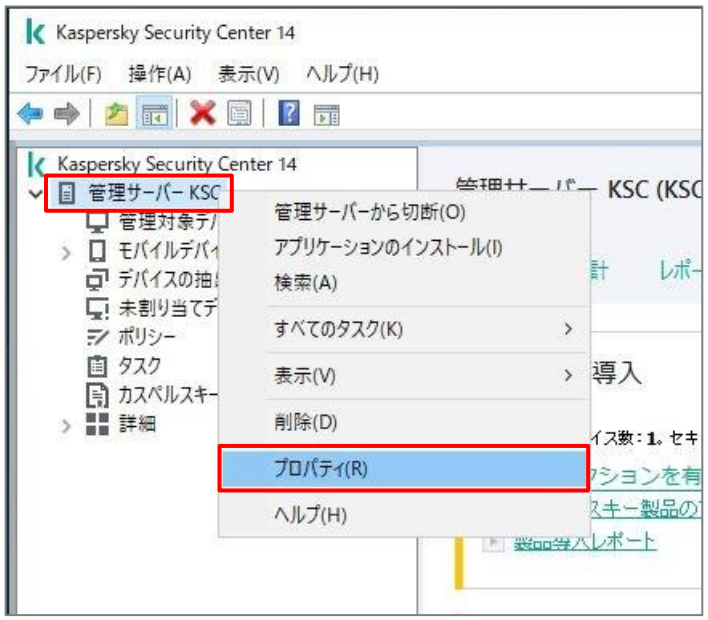
このディストリビューションポイントは、**既定で自動的に端末に対して割り当てられる設定**となっております。
そのため、業務系アプリケーションサーバーや、普段使用しているデバイスが指定される可能性があり、ディスク使用量の増加やリソースの消費、意図しない通信の発生など、予期せぬ問題が発生する可能があります。

アップデートエージェントの詳細や、手動による割り当て手順は以下サイトにある「ディストリビューションポイント設定ガイド」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/）

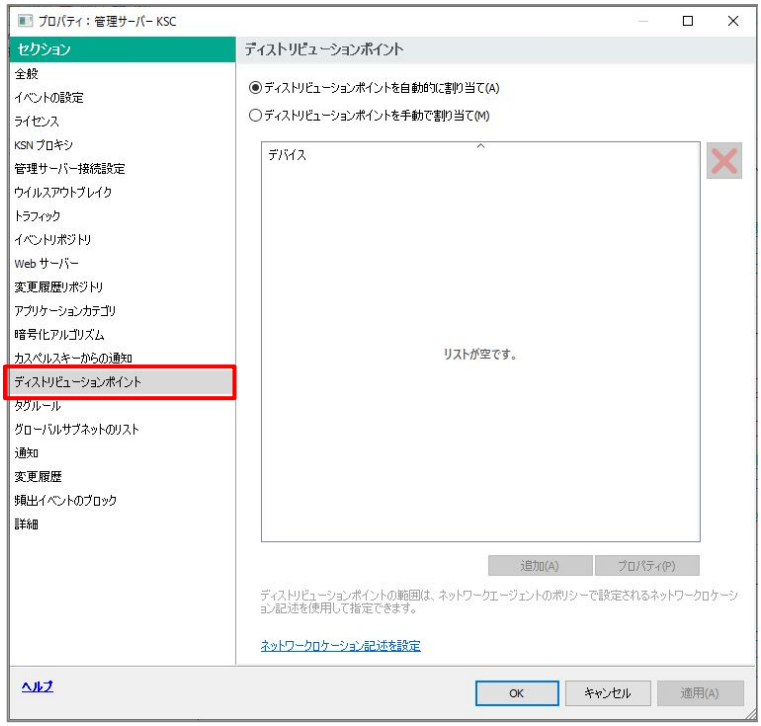
以下に、ディストリビューションポイントが割り当てられる設定を「自動」から「手動」へ変更する方法についてご説明します。

ディストリビューションポイントの自動割り当てを解除した場合、KSC 管理サーバーの管理下にある全デバイスは、直接 KSC 管理サーバーへ接続し定義データベースのダウンロードを行います。

(1) 「管理サーバー」を右クリックし、「プロパティ」を開きます。

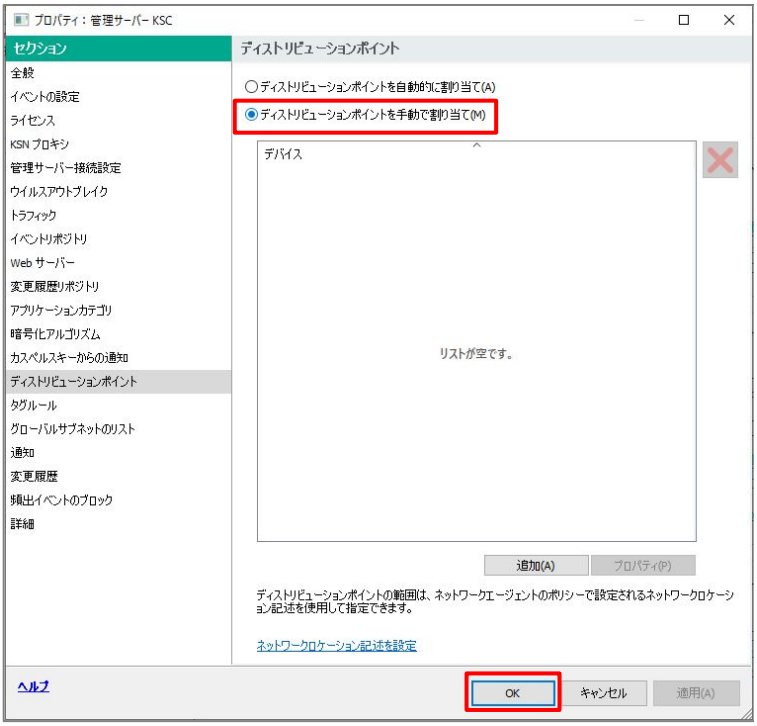


(2)「ディストリビューションポイント」セクションを開きます。



(3)「ディストリビューションポイントを手動で割り当て」にチェックを入れます。

「OK」をクリックしプロパティ画面を閉じます。



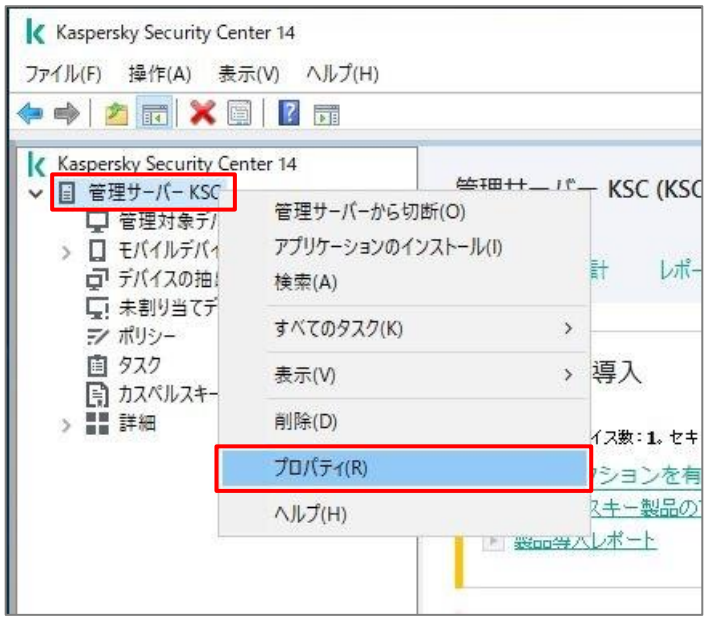
本節は以上です。

4.3. イベント通知設定

ウイルス検知など、管理下のデバイスにて重要なイベントが発生した場合、管理サーバーから管理者へメールを送信することができます。

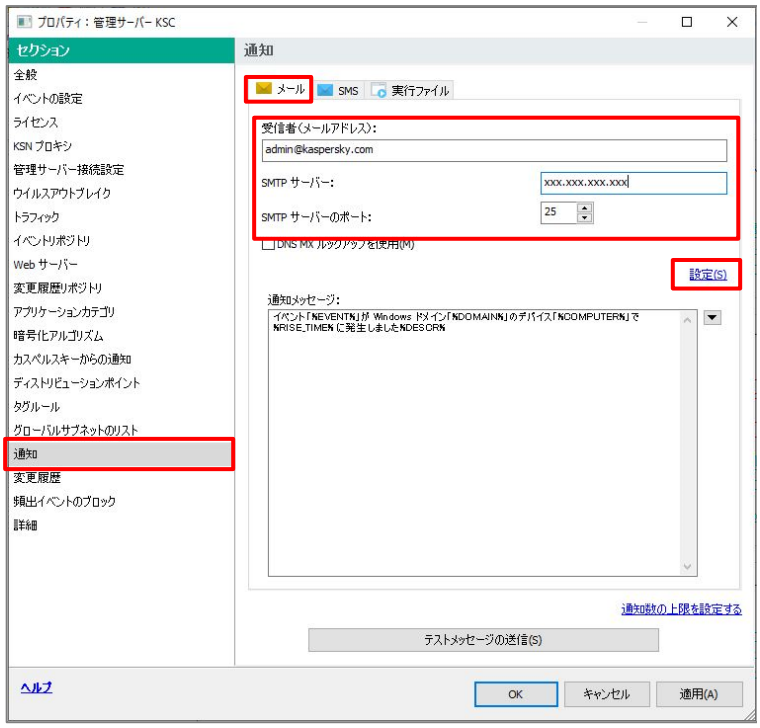
以下に、KSC にて管理者のメールアドレスを設定し、特定のイベント発生時にメール通知を行う設定についてご説明します。

(1) 「管理サーバー」を右クリックし、「プロパティ」を開きます。



(2) 「通知」セクションを開きます。
宛先に送信先となるメールアドレス、SMTP サーバーアドレス、ポートを入力します。

認証など、詳細な設定を行う場合は「設定」をクリックします。

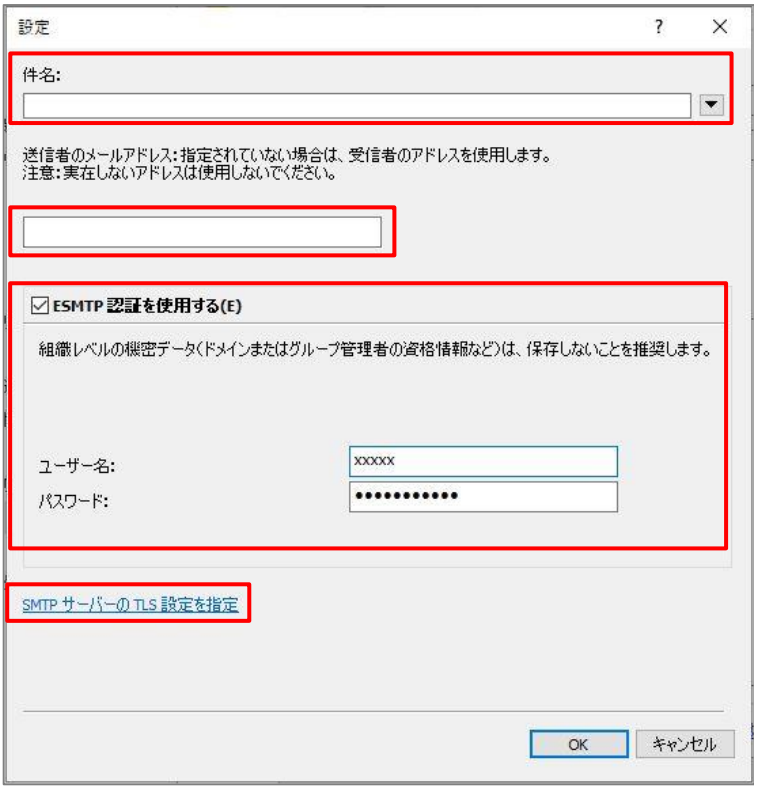


(3) 「件名」には、メール通知時の件名を設定することができます。

送信者のメールアドレスを指定したい場合は「送信者のメールアドレス」のフィールドに入力します。指定しない場合は、宛先に指定したアドレスが送信者として表示されます。

ESMTP 認証を使用する場合は、「ESMTP 認証を使用する」にチェックを入れ、「ユーザー名」「パスワード」を入力します。

SMTP サーバーの TLS 設定を指定する場合は、「SMTP サーバーの TLS 設定を指定」をクリックします。

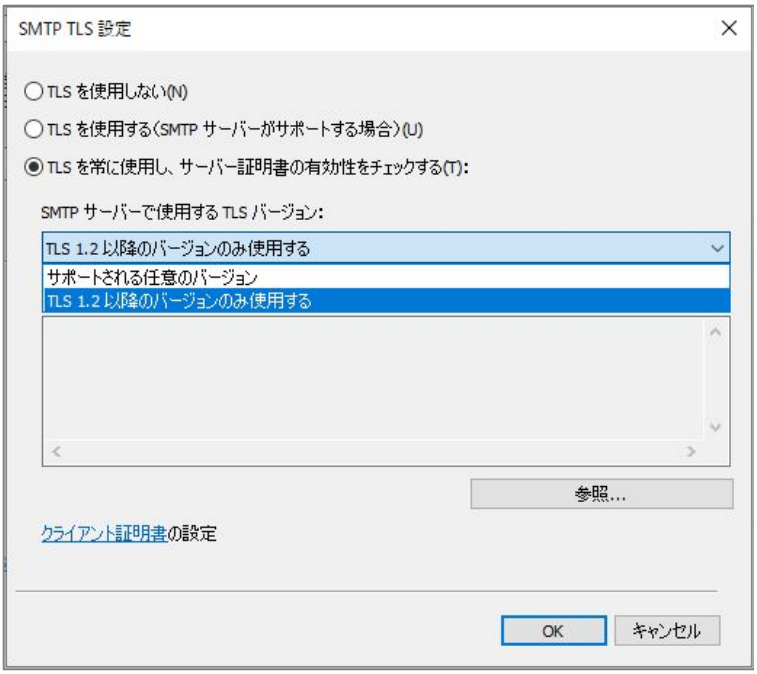


(4) SMTP サーバーの TLS 設定をします。

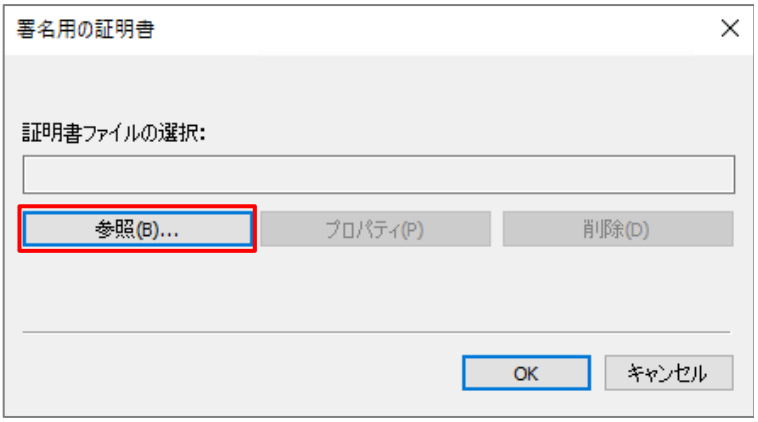
「TLS を使用する（SMTP サーバーがサポートする場合）」を選択した場合、管理サーバーは TLS をサポートしていない SMTP サーバーとは TLS を使用せずに接続します。

「TLS を常に使用し、サーバー証明書の有効性をチェックする」を選択した場合、管理サーバーは TLS をサポートしていない SMTP サーバーへ接続できません。

クライアント証明書を指定する場合は、「TLS を常に使用し、サーバー証明書の有効性をチェックする」を選択し、「クライアント証明書の設定」をクリックします。

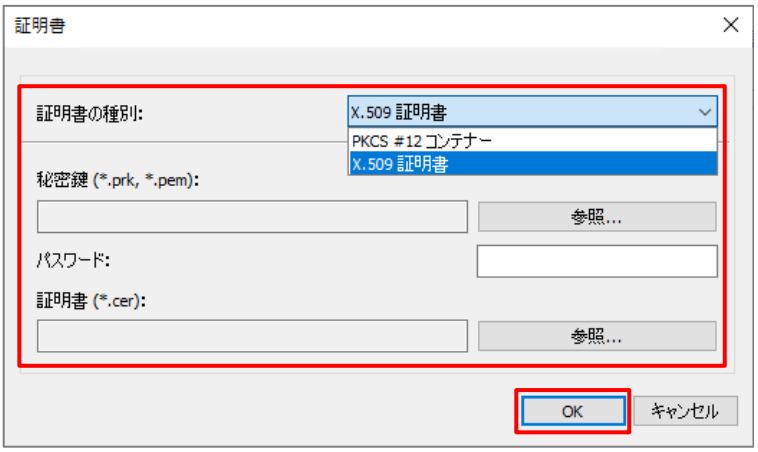


(5) 証明書を指定するため「参照」をクリックします。

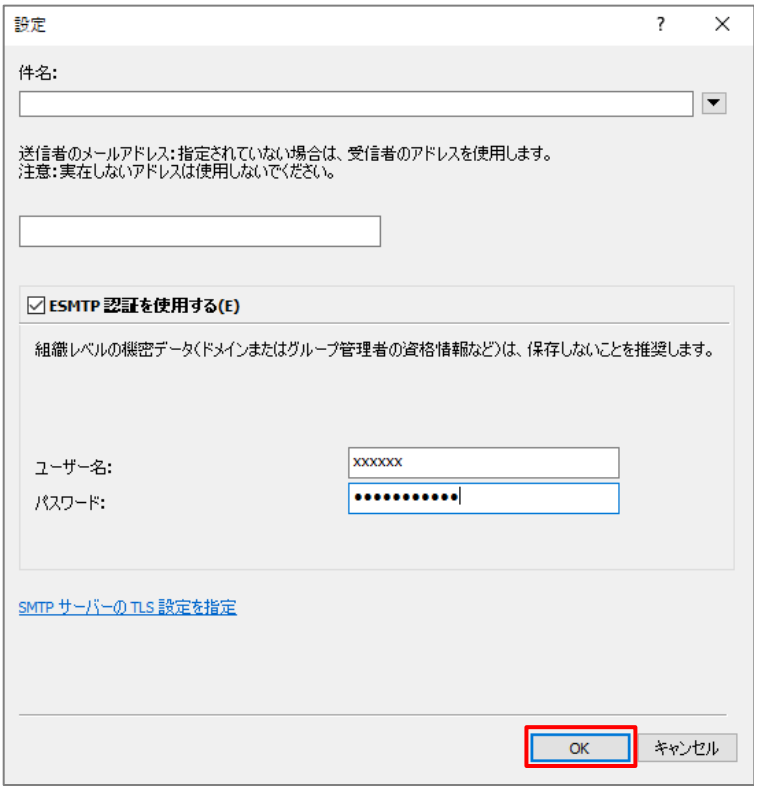


(6) 「証明書の種別」にて「x.509 証明書」か「PKCS#12 コンテナー」を選択します。

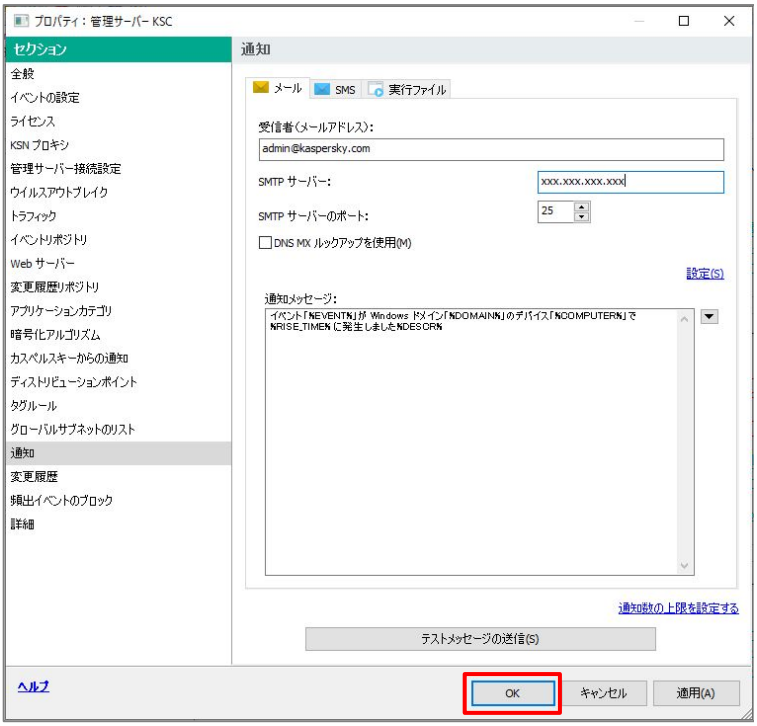
「参照」をクリックし、秘密鍵や証明書ファイルを選択します。
設定後、「OK」をクリックして設定を保存します。



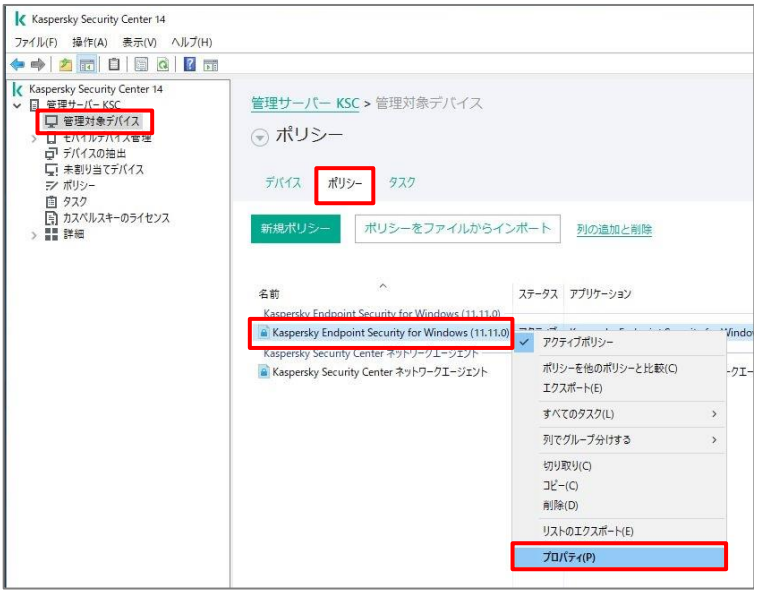
(7) 「OK」をクリックし、設定を保存します。



(8) 「OK」をクリックし、通知の設定を保存します。

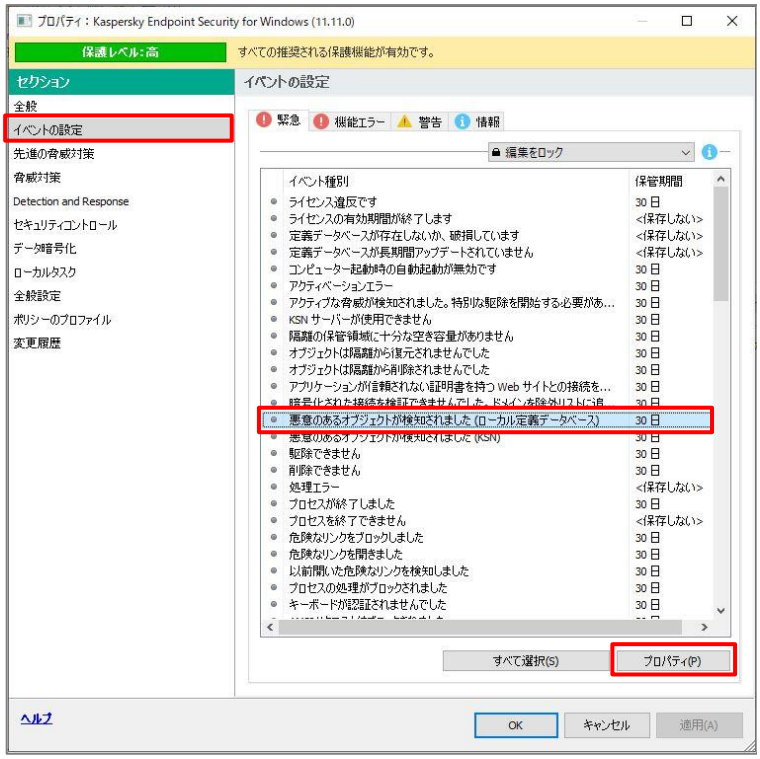


(9) 「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を開きます。



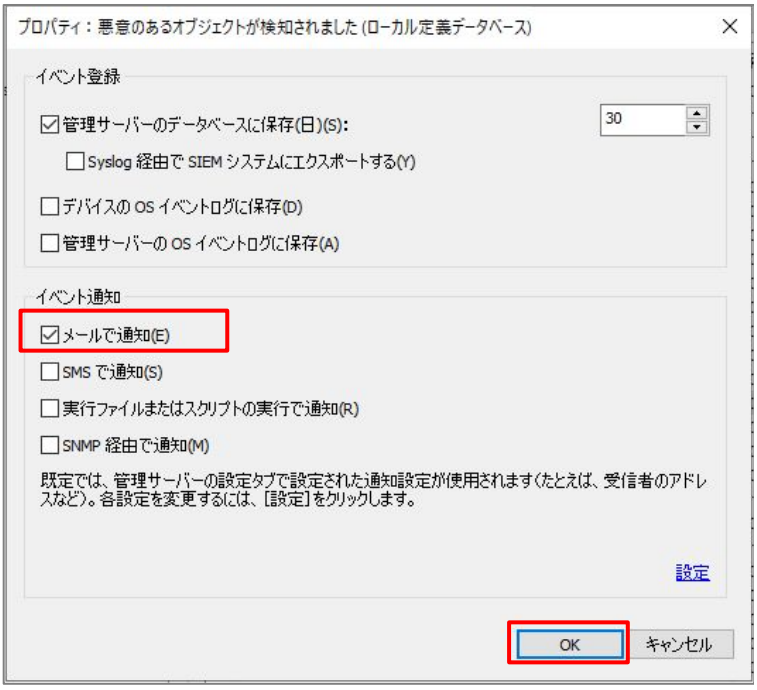
(10)　「イベントの設定」セクションを開きます。

管理者へ通知したいイベントを選択し、「プロパティ」をクリックします。
（ここでは「悪意のあるオブジェクトが検知されました」を指定しています）



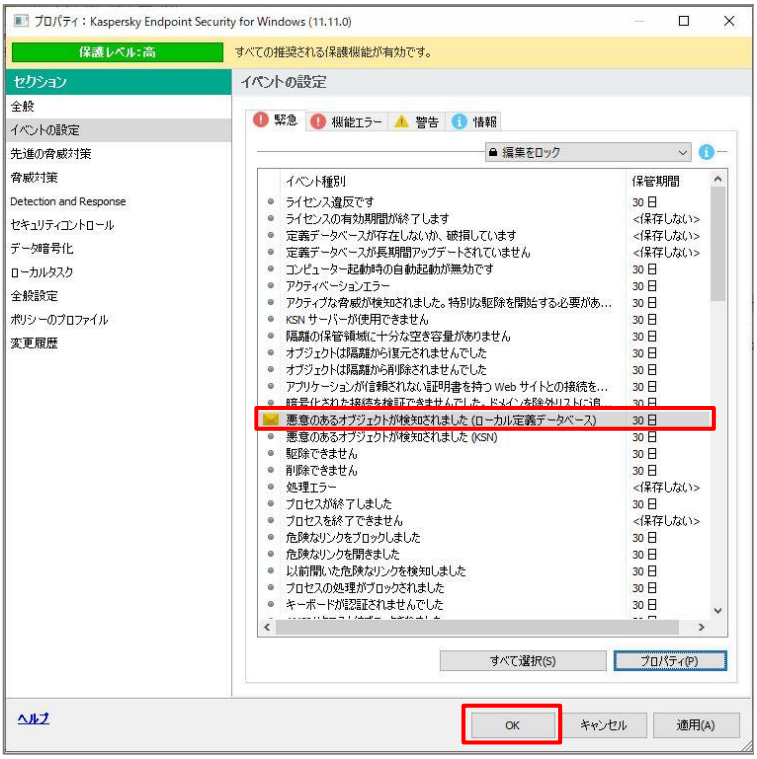
(11)　プロパティ画面にて、「メールで通知」にチェックを入れ、「OK」をクリックします。

管理サーバーで設定した宛先とは別の宛先を設定する場合、**「設定」**をクリックすることでカスタマイズが可能です。



(12)　通知設定されたイベントには、メールのアイコンが表示されます。

「OK」をクリックし設定を保存します。



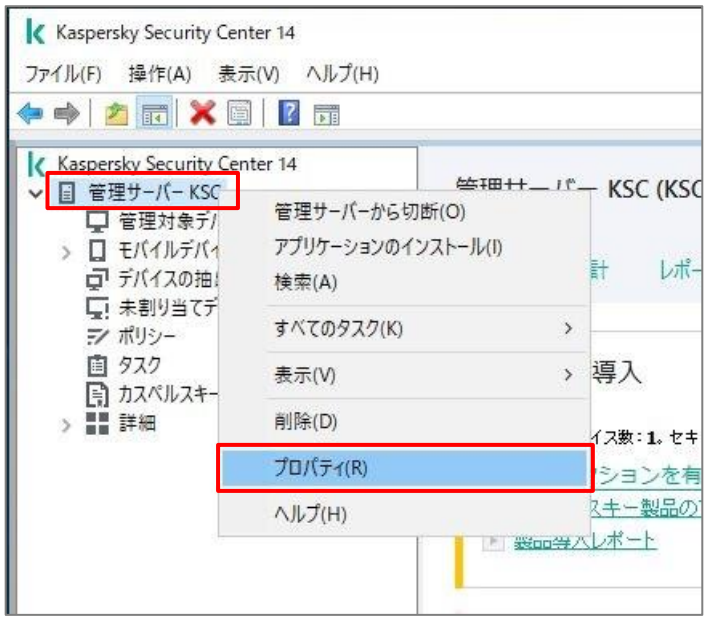
本節は以上です。

4.4.　ウイルスアウトブレイク通知設定

管理下のデバイスにて大量のウイルス検知が発生した場合、「ウイルスアウトブレイク」の通知を発信することができます。管理者は通知を受け取ることで、マルウェアの脅威に対して迅速に対応することができます。

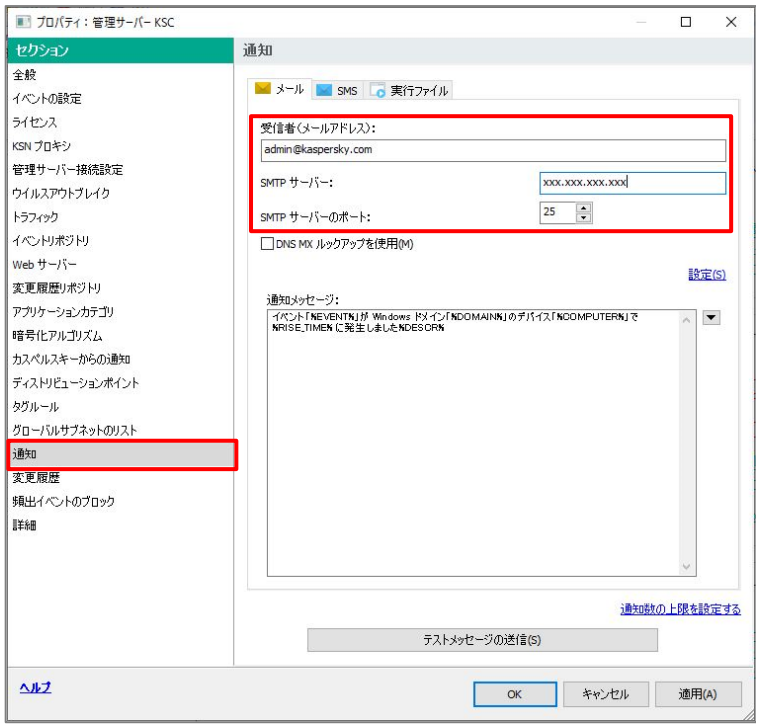
以下に、アウトブレイクの通知を有効化する設定についてご説明します。

(1) 「管理サーバー」を右クリックし、「プロパティ」を開きます。



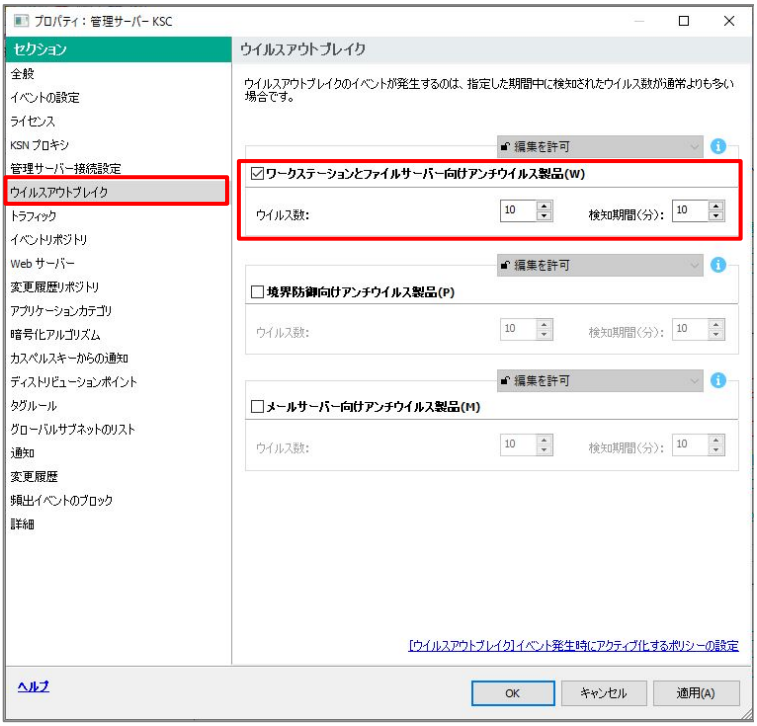
(2) 「通知」セクションを開きます。
宛先に送信先となるメールアドレス、SMTP サーバーアドレスを入力します。

※設定済みの場合、本手順は不要です。



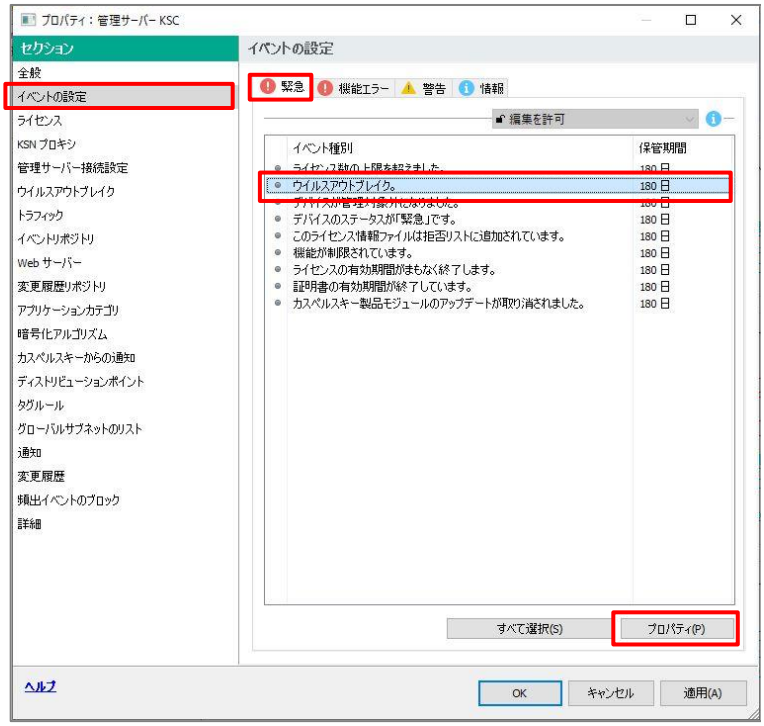
(3) 「ウイルスアウトブレイク」セクションを開きます。
「ワークステーションとファイルサーバー向けアンチウイルス」にチェックを入れます。

既定では管理下のデバイスにて**「10 分間」**に**「10 個」**のマルウェアが検知した場合、アウトブレイクを通知する設定となっております。
運用に合わせ設定を変更してください。

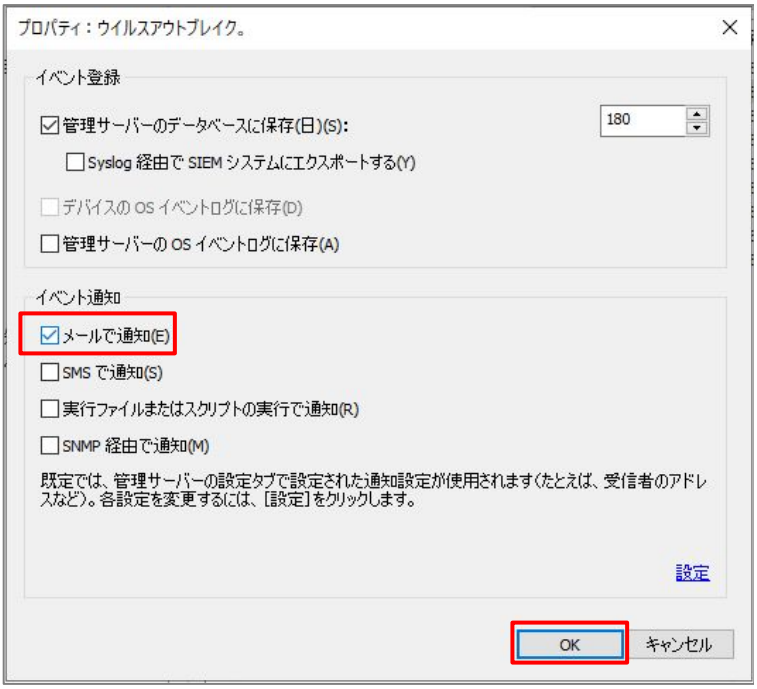


(4) 「イベントの設定」セクションを開きます。

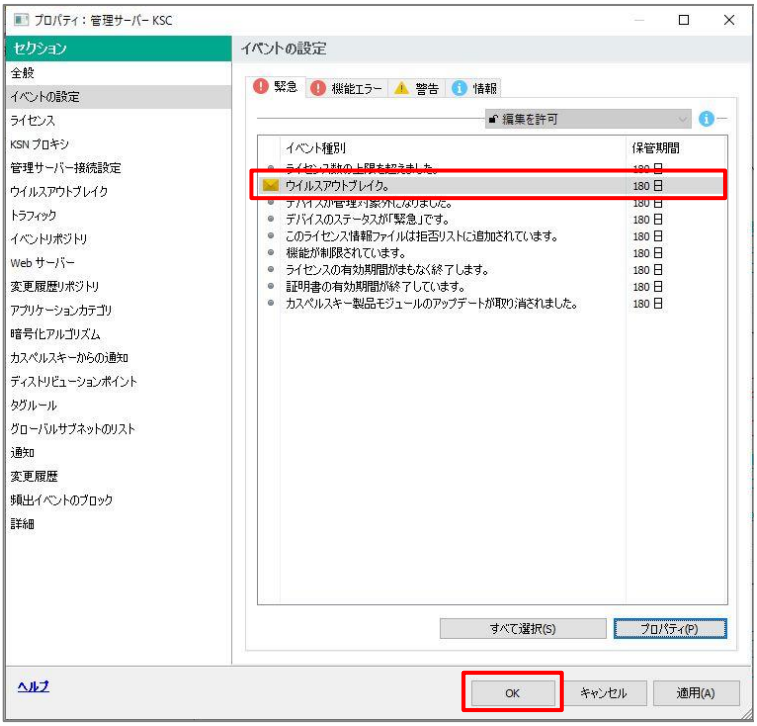
「緊急イベント」タブ内にある、「ウイルスアウトブレイク」を選択し、プロパティをクリックします。



(5)「メールで通知」にチェックを入れ、「OK」をクリックします。

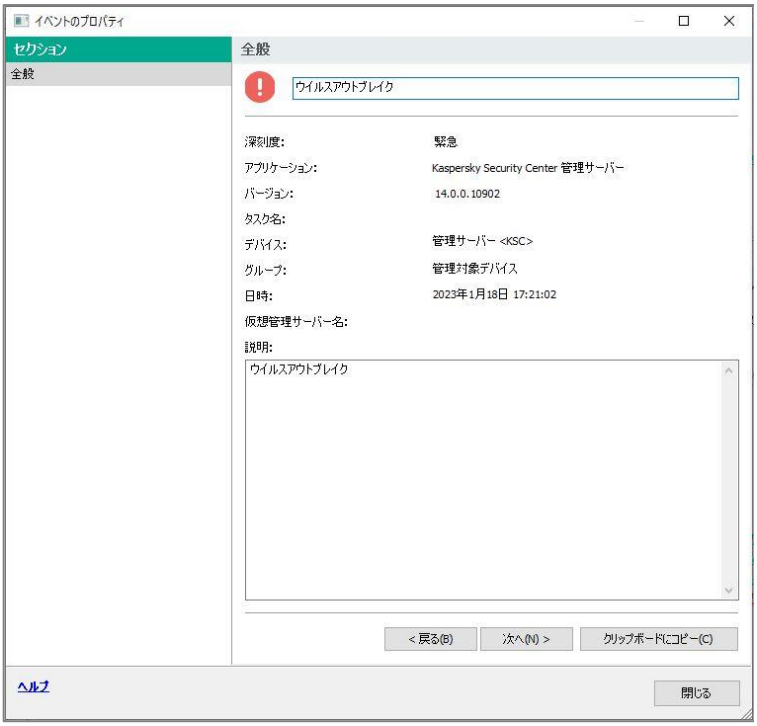


(6)「ウイルスアウトブレイク」にメールアイコンが設定されていることを確認し、「OK」をクリックします。



管理下のデバイスからのウイルス検知イベント受信数がしきい値を超えた場合、右記の「ウイルスアウトブレイク」イベントが記録されます。

同時に設定したメールアドレスへメール通知が行われます。



本節は以上です。

4.5. 除外設定

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で、検知など 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。

KES の検知対象から除外が必要なアプリケーション、ファイル、URL の確認を行い、運用開始前に設定を実施してください。

手順は以下サイトにある「除外設定ガイド」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/）

本節は以上です。

4.6. ウェブコントロール設定（バナー広告ブロック）

本章では、「ウェブコントロール」機能にて、バナー広告をブロックする設定についてご説明します。
「ウェブコントロール」とは、Web リソースへのアクセスを制限、またはブロックする機能です。ギャンブルサイトや SNS など、コンテンツを指定して制御することができます。

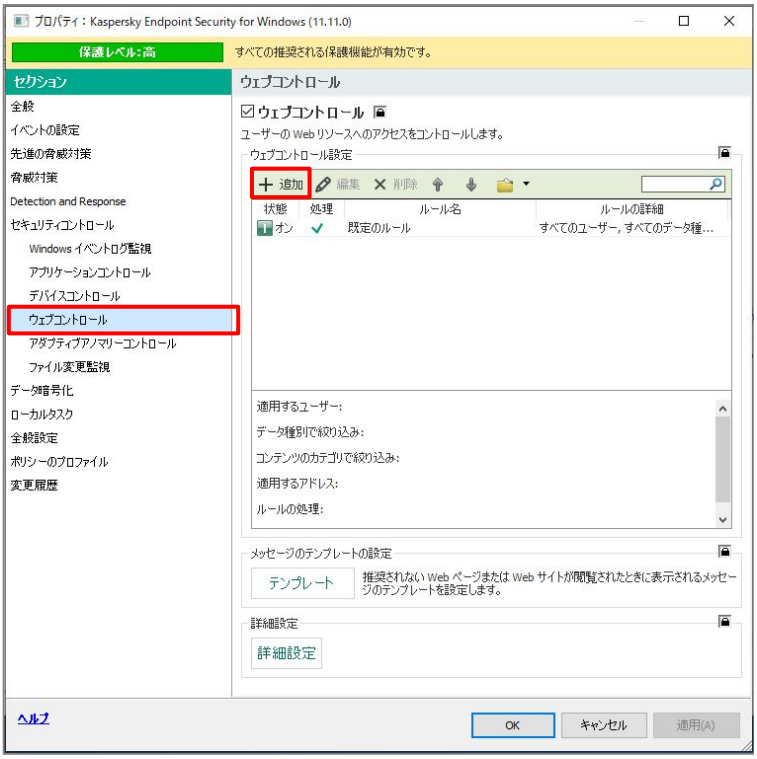
コンテンツの一つとして「バナー」を制御することができます。
不正なバナー広告にアクセスした場合、悪意のある Web サイトへの転送や、フィッシングの被害にあう可能性もありますが、本設定を実施することで不正なバナー広告自体を非表示とすることができます。

以下に、「ウェブコントロール」を使用して、バナーの表示をブロックする設定をご説明します。

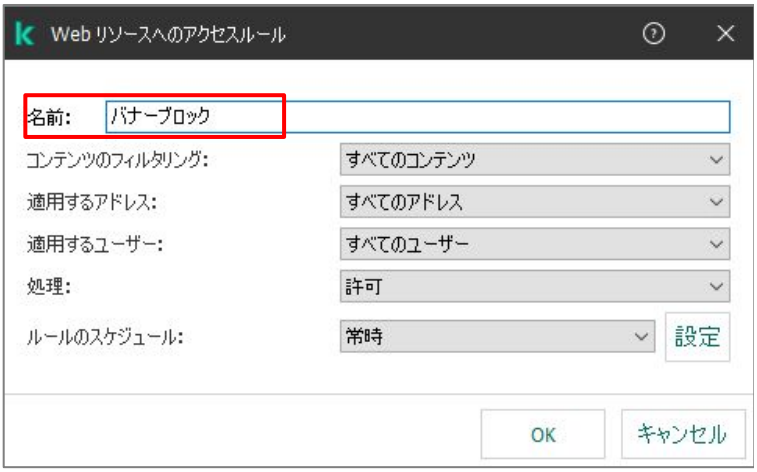
(1)「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を開きます。

(2)「セキュリティコントロール」-「ウェブコントロール」セクションを開きます。

ウェブコントロール設定画面にて「追加」をクリックします。



(3)「名前」に任意の名前を入力します。（ここでは「バナーブロック」としています）

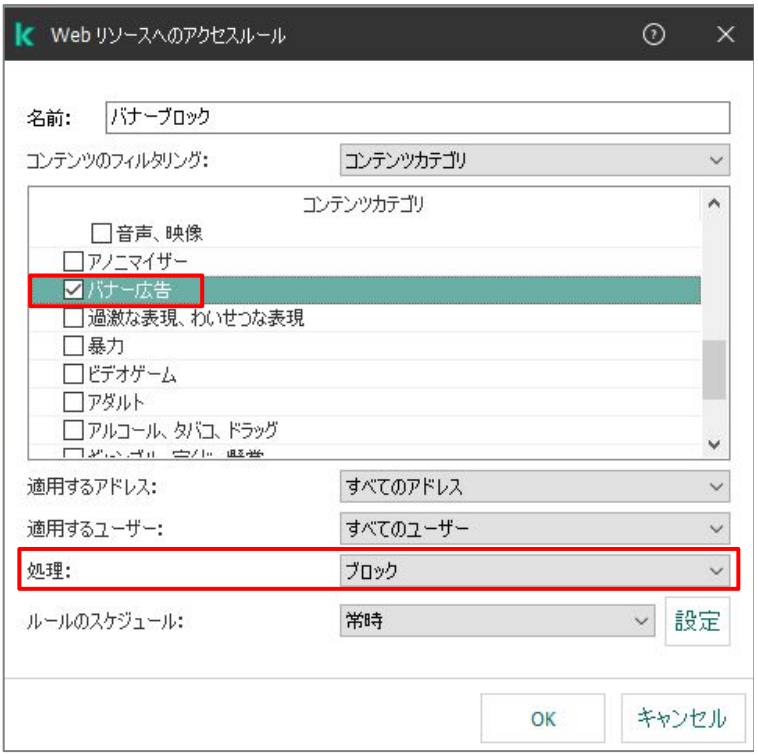


(4)「コンテンツのフィルタリング」のリストボックスから「コンテンツカテゴリ」を選択します。

(5) カテゴリを選択する画面が表示されるので、「バナー広告」にチェックを入れます。

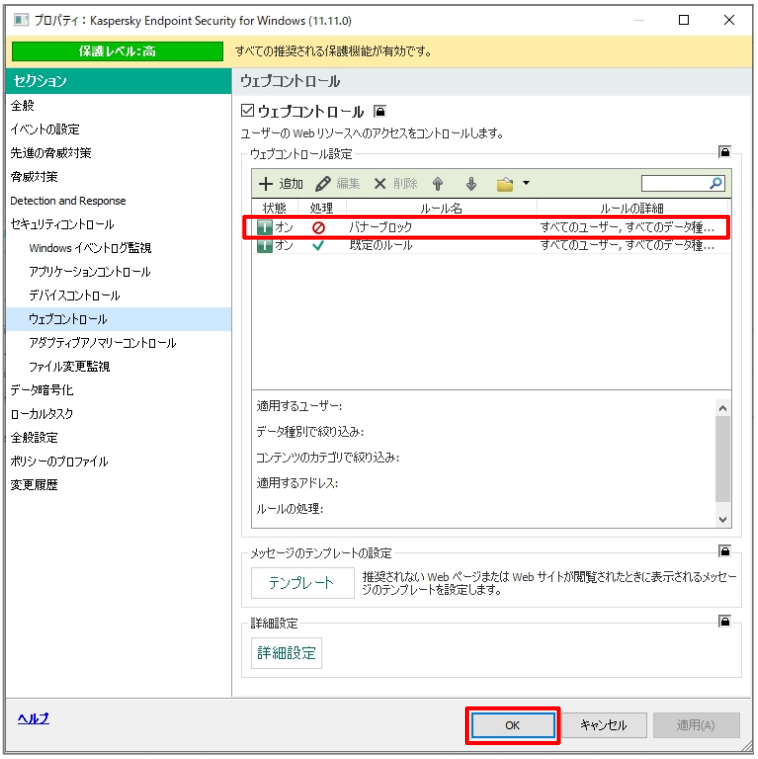
「処理」の項目を「ブロック」と設定します。

設定後、「OK」をクリックして画面を閉じます。



(6) 追加した「バナーブロック」が一番上にあることを確認します。
「OK」をクリックし設定を保存します。

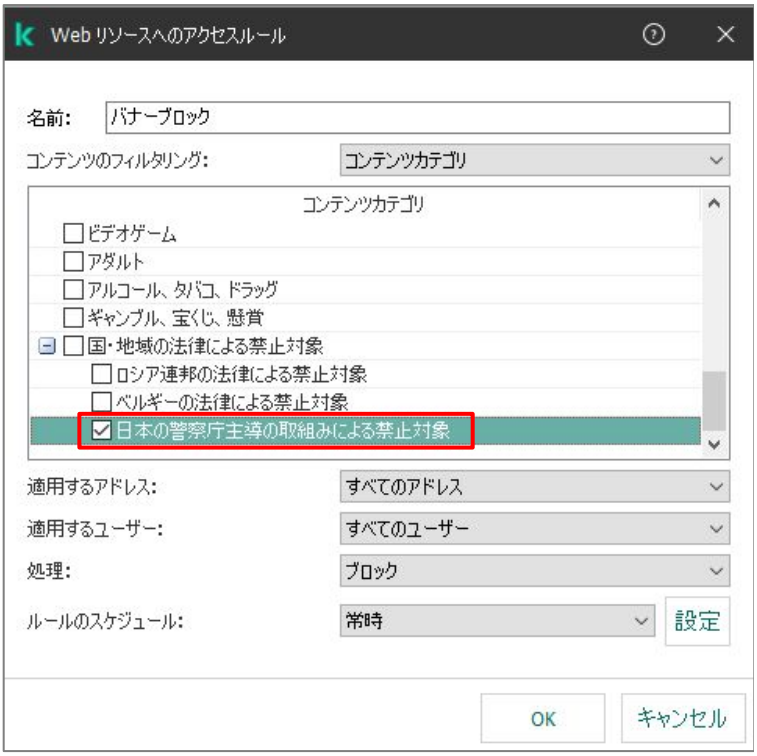
ポリシーが適用されたデバイスは、不正なバナー広告の表示がブロックされます。



kaspersky

【補足】

カテゴリの一つに、「日本の警察庁主導の取組みによる禁止対象」があります。
日本の警察庁が危険と設定したサイトの閲覧をブロックできます。
ブロックするカテゴリの一つとしてご検討ください。

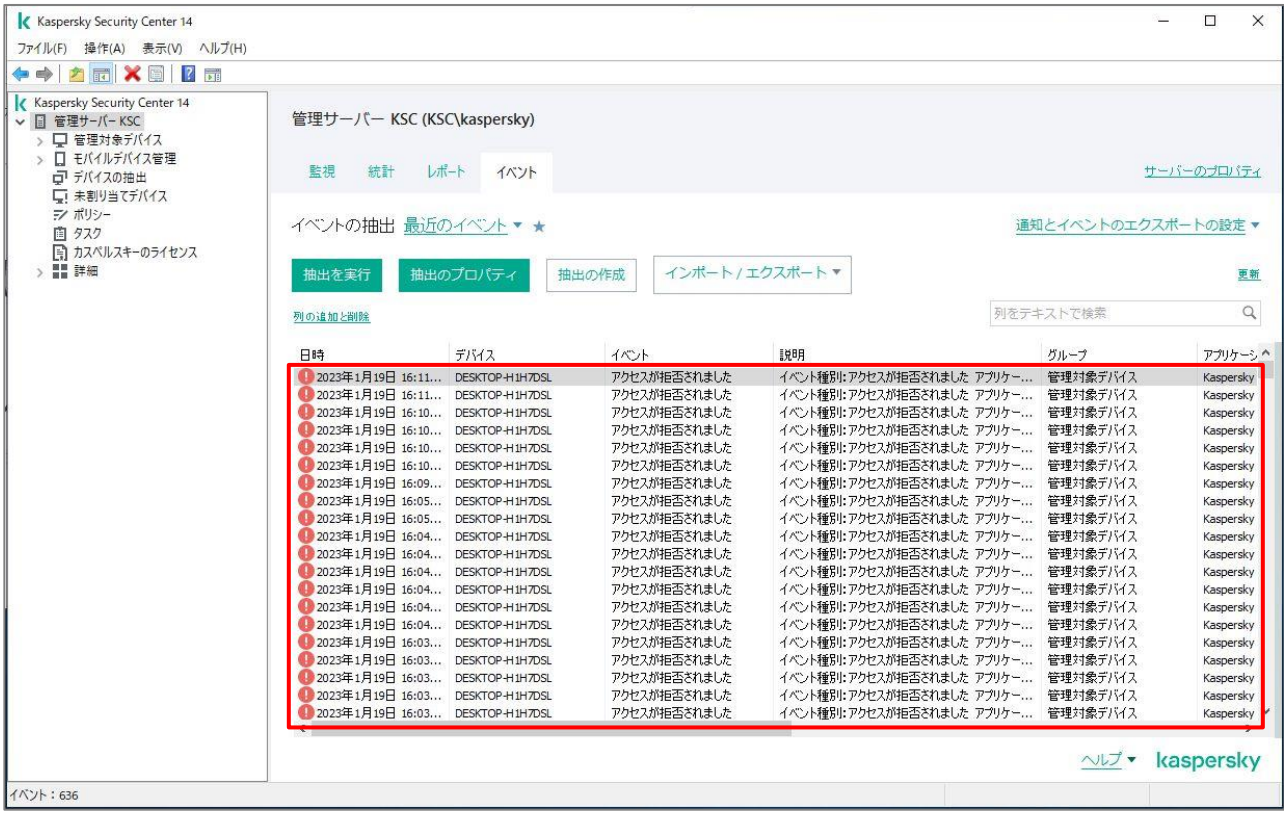


【補足】ウェブコントロールによるブロック設定後のイベント抑止

ウェブコントロールによるブロックを設定後、管理下のデバイスでブロック対象のサイトを閲覧した場合や、バナーがブロックされた場合、KSC にもブロックされた情報が通知されます。

ユーザーの利用状況により、このイベントが大量に記録され、他のイベントが埋もれてしまう可能性があります。

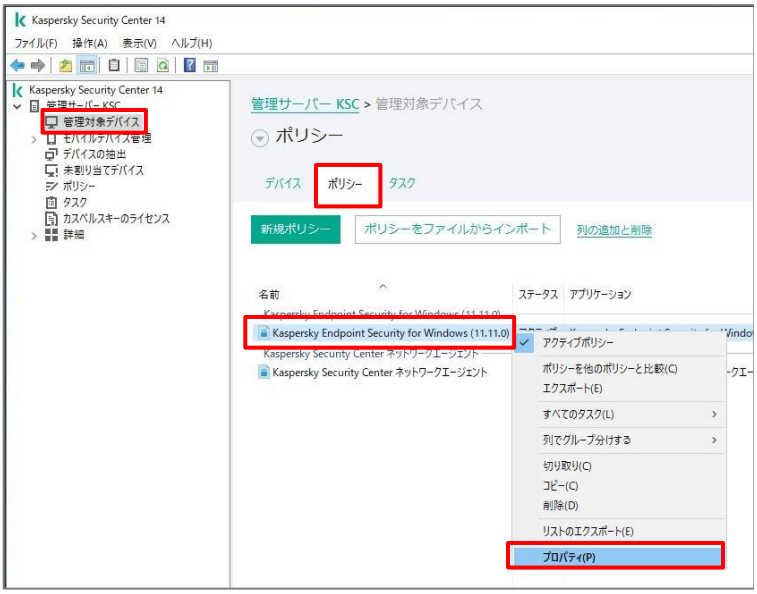
・イベント画面(例)



日時	デバイス	イベント	説明	グループ	アプリケーシ
2023年1月19日 16:11...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:11...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:10...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:10...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:10...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:10...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:09...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:05...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:05...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:04...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:04...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:04...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:04...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:04...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:04...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:03...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:03...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:03...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:03...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky
2023年1月19日 16:03...	DESKTOP-H1H7DSL	アクセスが拒否されました	イベント種別：アクセスが拒否されました アプリケー...	管理対象デバイス	Kaspersky

以下に、「ウェブコントロール」によるブロックイベントを KSC へ通知しない設定についてご説明します。

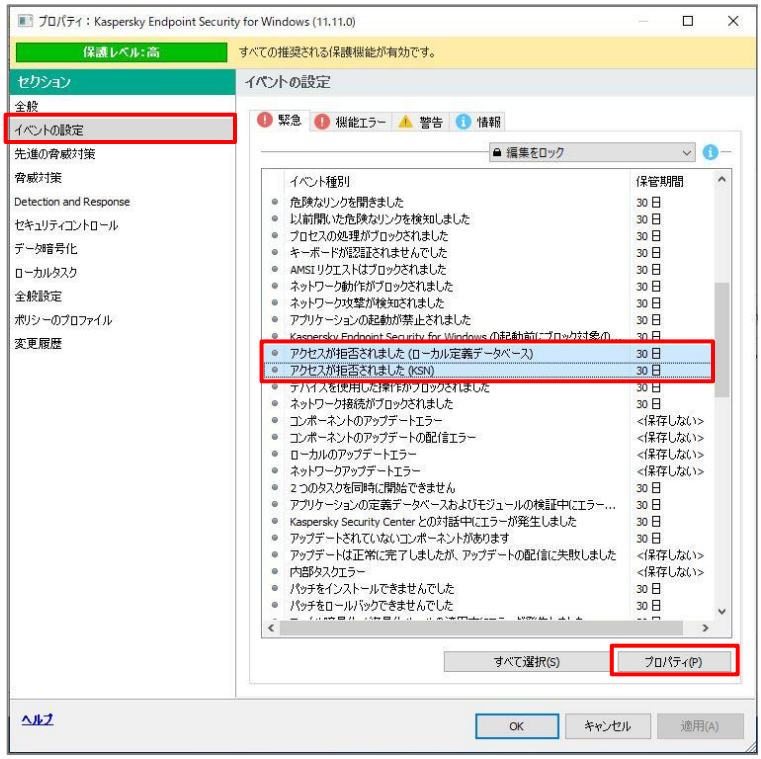
(1)「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を開きます。



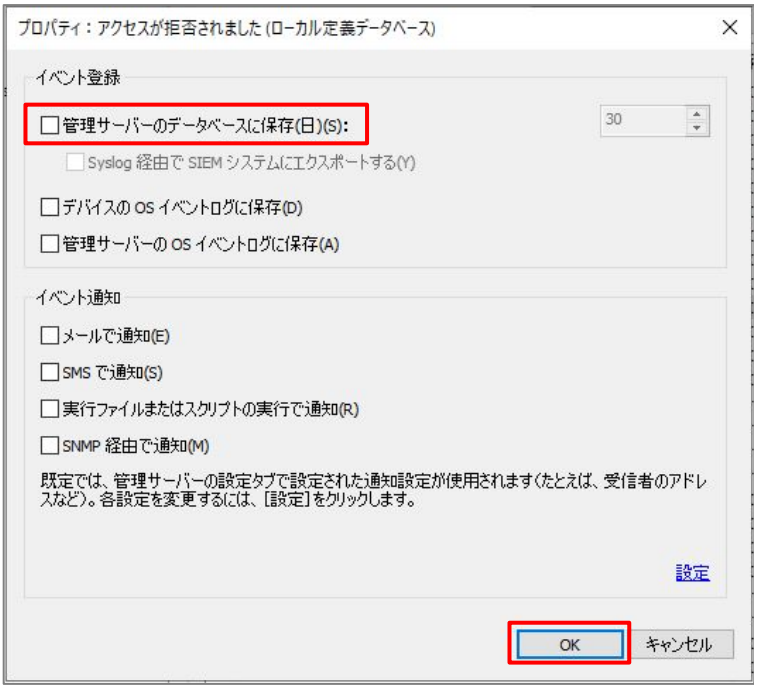
(2)「イベントの設定」セクションを開きます。

「緊急タブ」にて以下のイベントをそれぞれ選択し、「プロパティ」をクリックします。

＜設定対象イベント＞
・「アクセスが拒否されました（ローカル定義データベース）」
・「アクセスが拒否されました（KSN）」

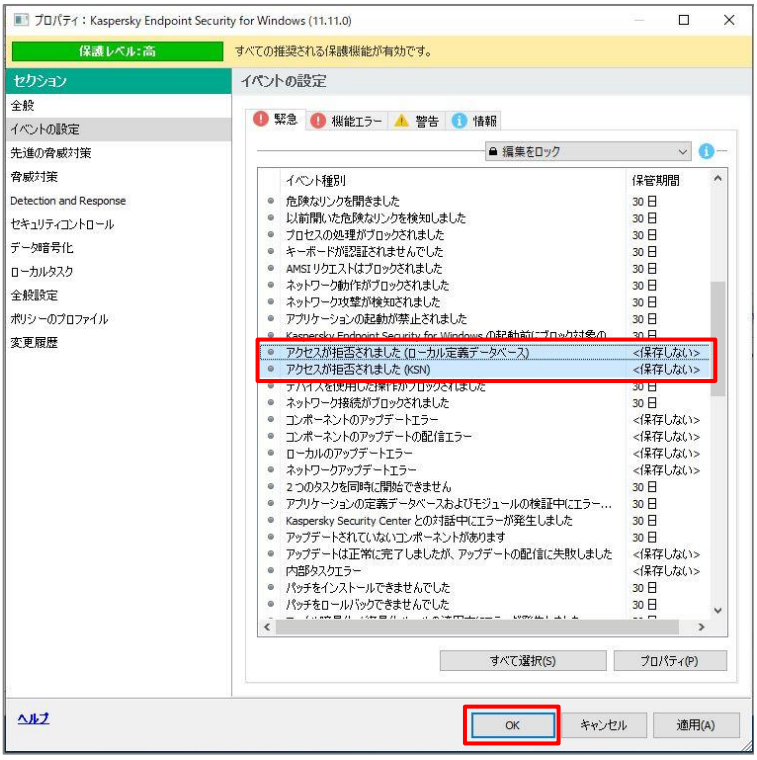


(3) 「管理サーバーのデータベースに保存」のチェックを外し、「OK」をクリックします。



(4) 設定したイベントの「保管期間」が「<保存しない>」変更されたことを確認し、「OK」をクリックしてポリシーを閉じます。

ポリシー適用後は管理サーバー上にイベントが記録されないようになります。



本節は以上です。

4.7. ログオンの監査の有効化

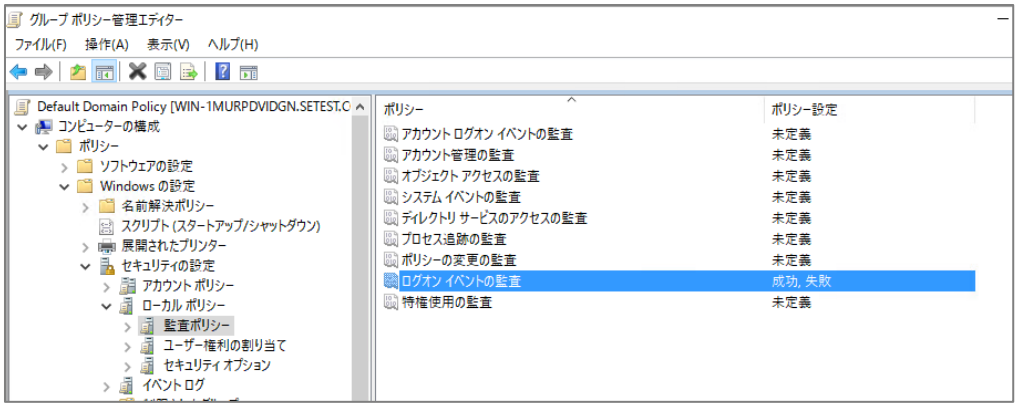
ここでは、Windows において「ログオンイベントの監査」の有効化についてご説明します。

KES の保護コンポーネントの一つである「ふるまい検知」の機能として、「外部からの暗号化に対する共有フォルダーの保護」という機能があります。

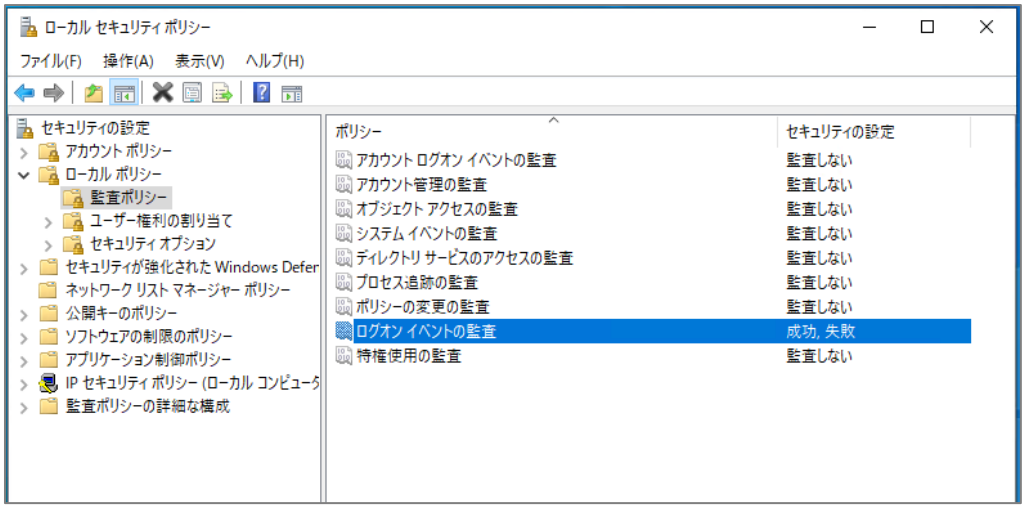
この機能において、特定デバイスからの暗号化通信は除外する設定（除外リスト）がありますが、この機能を有効にするためには、Windows において「ログオンイベントの監査」を有効化する必要があります。

参考として、Active Directory グループポリシー、ローカルセキュリティポリシーそれぞれの設定箇所をご案内します。

- Active Directory グループポリシー



- ローカルセキュリティポリシー



「ログオンイベントの監査」の詳細につきましては、以下マイクロソフト社のサイトをご参照ください。

https://learn.microsoft.com/ja-jp/windows/security/threat-protection/auditing/basic-audit-logon-events

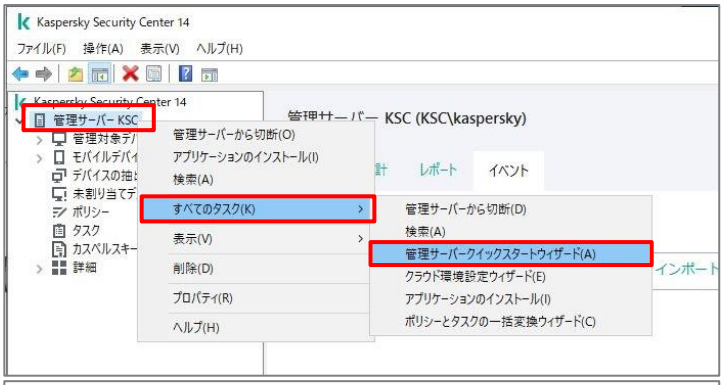
本章では、初期設定における補足事項についてご説明します。

1.「管理サーバークイックスタートウィザード」をキャンセルした場合

KSC のインストール完了後、自動的に「管理サーバークイックスタートウィザード」が起動し、KSC における初期設定や必要なタスクの作成を行うことができます。

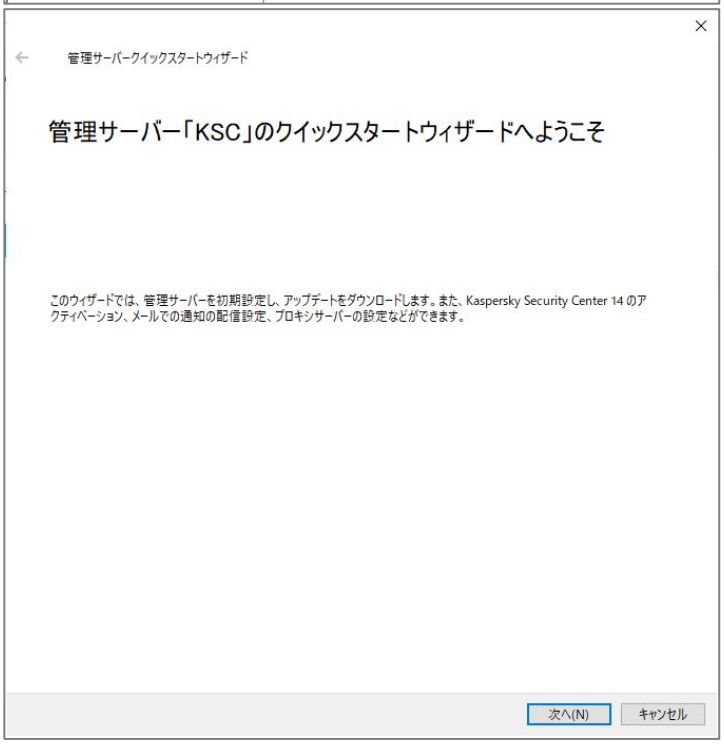
このウィザードをキャンセルした場合でも、再度ウィザードを起動することができます。

(1)「管理サーバー」を右クリックし、「すべてのタスク」-「管理サーバークイックスタートウィザード」をクリックします。



(2)「管理サーバークイックスタートウィザード」が起動します。

ウィザードに従い、初期設定を実施してください。



本節は以上です。

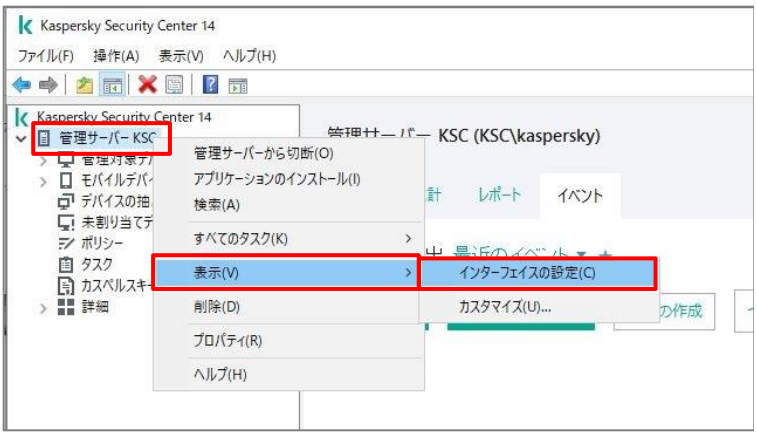
2. インターフェイスの設定

KSC の初期状態では、すべてのインターフェイスを表示する設定になっておりません。

アクセス権の設定を行う「セキュリティ」設定や、KSC をプライマリ・セカンダリと階層管理するための設定は初期状態で表示されておりません。

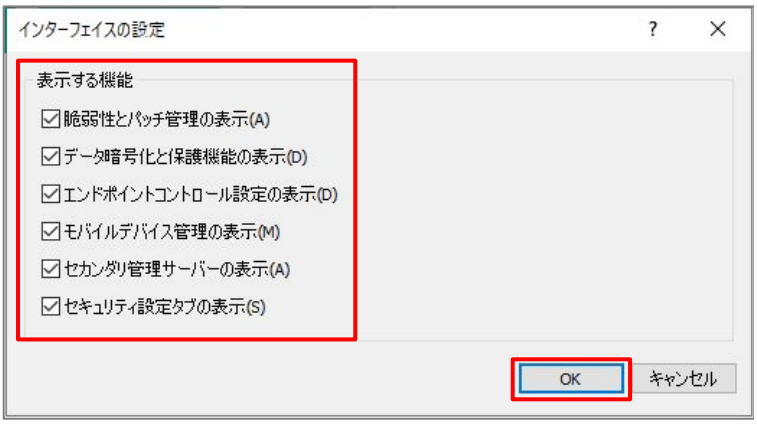
インターフェイスの設定を変更するためには以下の手順を実施します。

(1)「管理サーバー」を右クリックし、「表示」-「インターフェイスの設定」をクリックします。



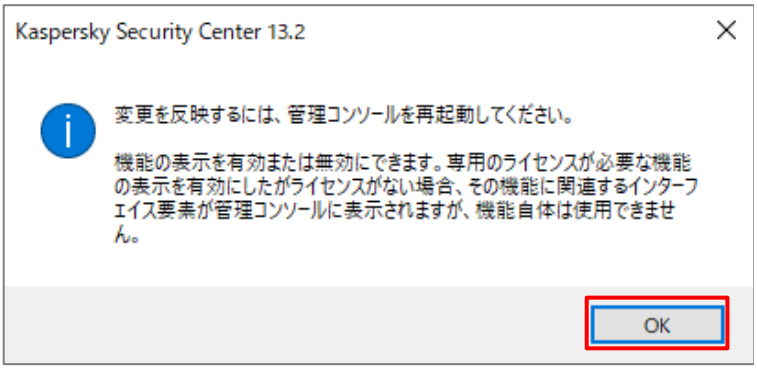
(2)「インターフェイスの設定」画面が表示されます。

必要な項目にチェックを入れ、「OK」をクリックします。



(3) 右記のダイアログが表示されるので、「OK」をクリックし、KSC 管理コンソールを閉じ、再度管理コンソールを開きます。

※OS やサービスの再起動は不要です。



(4) 管理コンソール起動後、設定したインターフェイスが表示されていることを確認します。

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/