Kaspersky
Endpoint Detection and Response Optimum
インストールガイド

2024/02/08

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. 1.1

kaspersky

目次

1. はじめに

1.1. 本資料の目的

本資料では、Kaspersky Endpoint Detection and Response Optimum(EDR-O)を使用するために必要な手順、及び設定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

→ **「KSC 簡単インストールガイド」**をご参照ください。

STEP 3.

Web プラグイン、EDR-O コンポーネントの有効化及びポリシー設定

→ **本資料を参照し、各設定を実施してください。**

STEP 4.

EDR-O の運用

→ **「EDR-O 運用ガイド」**をご参照ください。

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/）

1.3. 用語説明

本資料で使用される用語についてご説明します。

① **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。

② **Web プラグイン：**
KSC Web コンソールによる Kaspersky 製品のリモート管理に使用されるコンポーネントです。
KSC Web コンソールと該当する Kaspersky 製品の間に仲介するインターフェイスとして機能し、Web プラグインを使用することでタスクやポリシーを設定できます。

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）

⑤ **Kaspersky Endpoint Detection and Response Optimum（以降 EDR-O）：**
KES と連携し、自動化された EDR 機能を提供するアプリケーションです。
エンドポイントからの情報を収集、根本原因分析を速やかに自動で実行し、サイバー脅威の攻撃経路と脅威の情報をわかりやすく可視化します。そして、プロセスの停止やファイルの削除、隔離などの対応アクションが実行することが可能です。

1.4. システム要件について

EDR-O 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/KEDR_Optimum/2.3/ja-JP/216855.htm

1.5. 前提条件

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 14.2 が導入されている。
- ✓ NA 及び KES11.7 以降が対象のクライアントデバイスにインストールされている。

1.6. インストール時の注意点

- ✓ **Web コンソールのインストールが必要。**
  EDR-O は MMC ベースの管理コンソール非対応の為、Web コンソールをインストールする必要があります。

- ✓ **KES for Windows の Web プラグインのインストールが必要。**
  KES for Windows を Web コンソールで設定するための Web プラグインをインストールする必要があります。

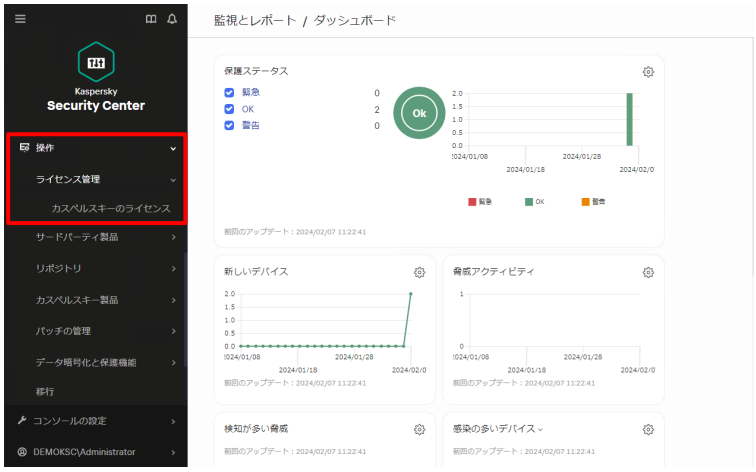
  ※KES for Windows の Web プラグインのインストール手順は「Appendix 1.KES の Web プラグインのインストール」をご参照ください。

- ✓ **100GB のハードディスク空き容量を用意。**
  EDR-O がインストールされた対象のクライアントデバイスにて収集されたデータが KSC に送信されます。
  その為、ハードディスクの空き容量として C ドライブに最低 100GB 以上の空き容量を確保してください。

2. EDR-O 用ライセンス登録

EDR-O 用のライセンスを登録します。

(1) 「操作」-「ライセンス管理」-「カスペルスキーのライセンス」を選択します。



(2) 「追加」をクリックします。

(3) アクティベーションコードを入力し、「送信」をクリックします。

(4) ライセンスの詳細が表示されます。
「管理対象デバイスにライセンスを自動的に配信する」にチェックを入れ、「閉じる」をクリックします。

注）
「管理対象デバイスにライセンスを自動的に配信する」にチェックを入れていない場合、管理下のデバイスに対しライセンスの適用が自動で行われません。
別途タスクを作成し、ライセンスを適用する必要があります。

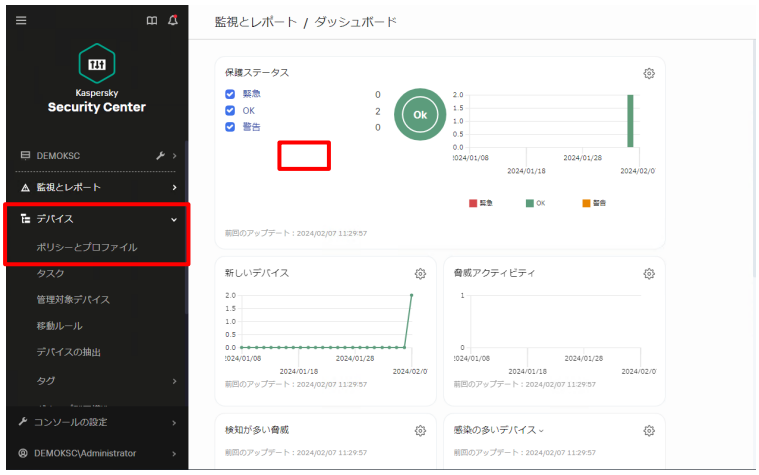
(5) ライセンス一覧に EDR-O 用のライセンスが登録されます。

以上になります。

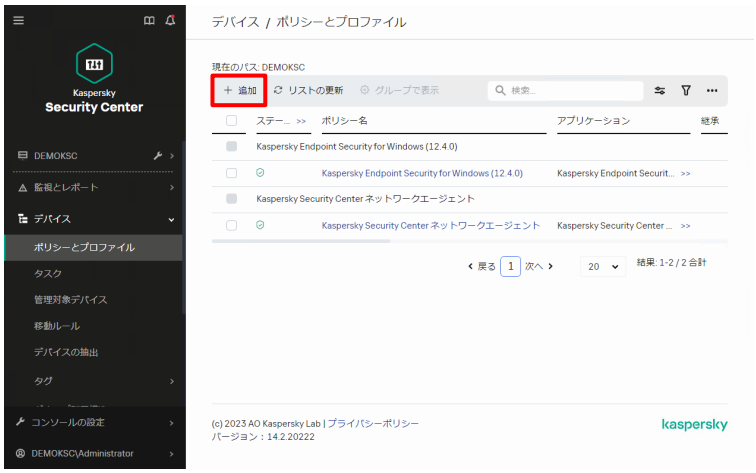
3. KES ポリシー設定

本章では KES ポリシーを設定変更し、EDR-O の各種機能をどのように適用させるか設定する方法をご説明します。

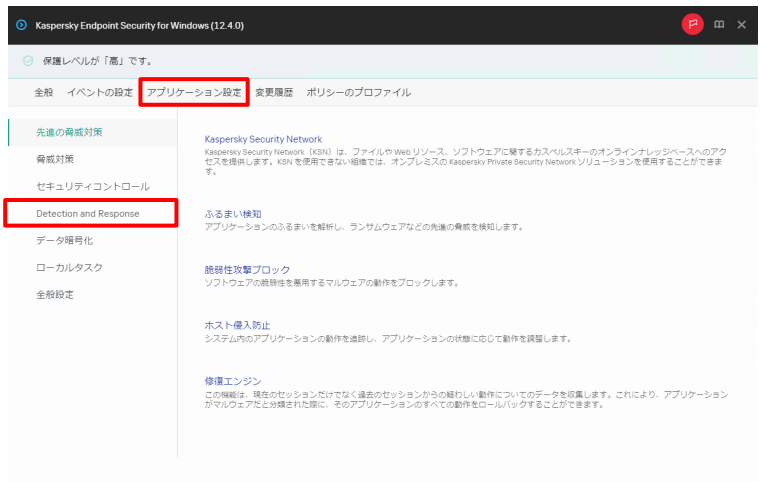
(1) 「デバイス」-「ポリシーとプロファイル」を選択します。



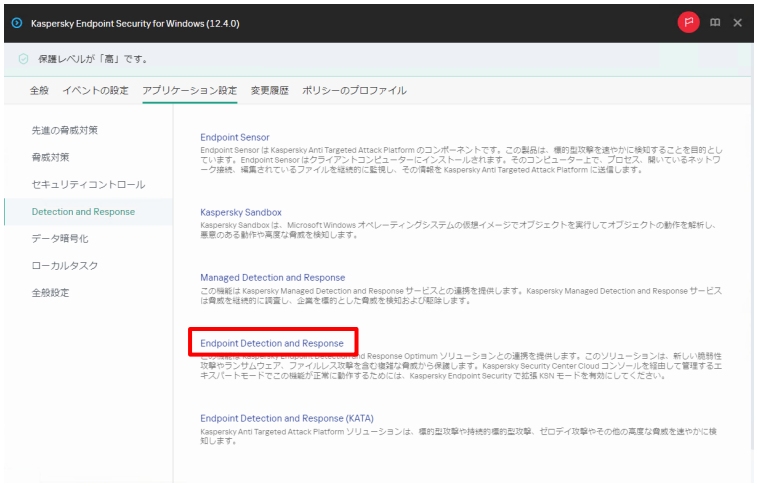
(2) 「追加」をクリックします。



(3) 「アプリケーション設定」タブ-「Detection and Response」をクリックします。



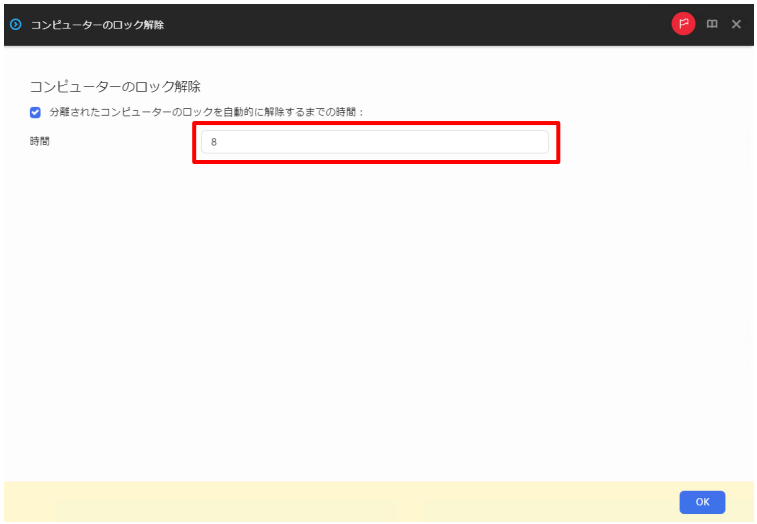
(4) 「Endpoint Detection and Response」をクリックします。



(5) トグルボタンをクリックし、Endpoint Detection and Response を有効にします。

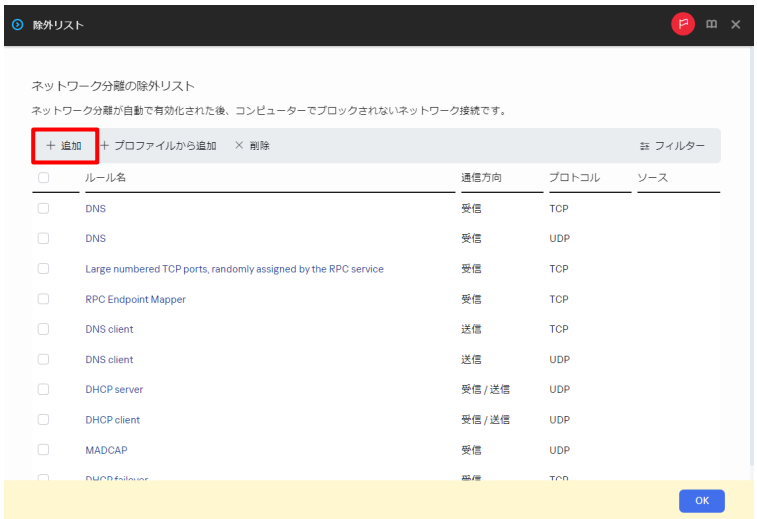
(6) ネットワーク分離時の自動ロック解除時間を設定します。
「コンピューターのロック解除を設定する」をクリックします。

(7) 任意の時間を設定し、「OK」をクリックします。
既定では、8 時間に設定されています。



(8) ネットワーク分離時に通信を遮断したくないアプリケーションなどがある場合、除外リストに追加します。
除外リストにルールを追加する場合、「除外リスト」をクリックします。

(9) 「追加」をクリックします。
追加したいプロトコルを登録し、OK をクリックします。

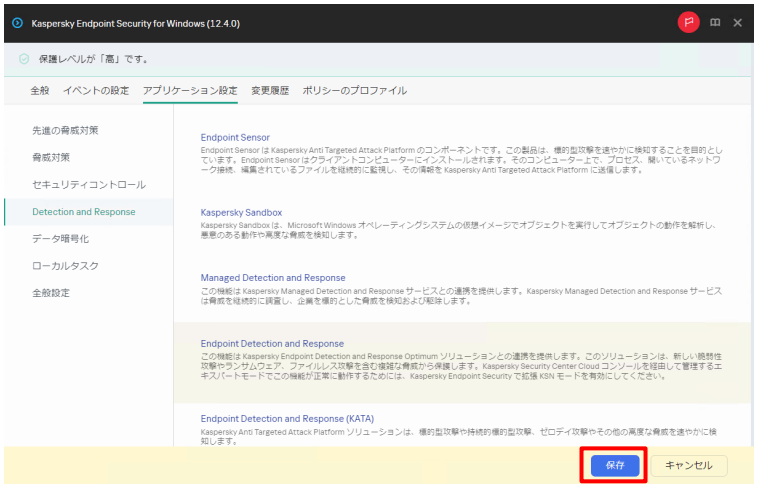


(10)　トグルボタンをクリックし、実行防止を有効にします。

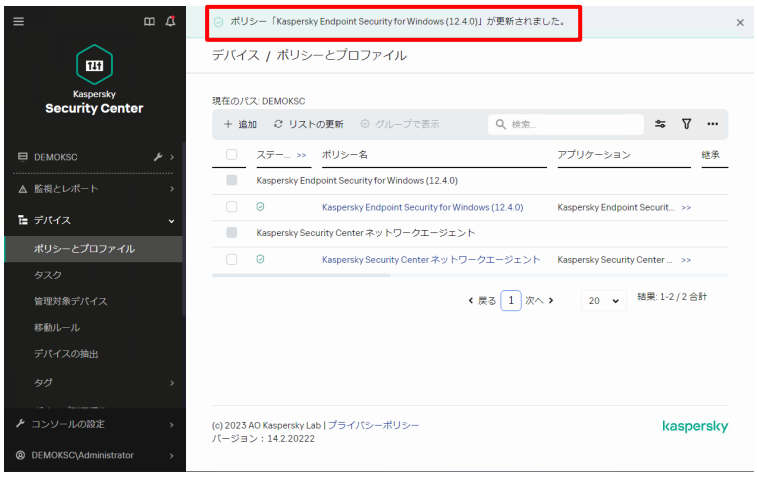
(11)　禁止されたオブジェクトが実行された場合の処理を「ブロックしてレポートに書き込む」に変更します。

(12)　トグルボタンをクリックし、Cloud Sandbox を有効にして「OK」をクリックします。

(13)　「保存」をクリックします。



(14)　KES for Windows のポリシーが更新されます。



以上になります。

4. EDR-O コンポーネントの追加

本章では対象のクライアントデバイスに EDR-O コンポーネントを追加する方法をご説明します。
インストール方法は 2 パターンあります。

パターン 1：NA、KES が導入済みのデバイスの EDR-O コンポーネントを有効化する場合

→「4.1. EDR-O コンポーネントの有効化」を参照

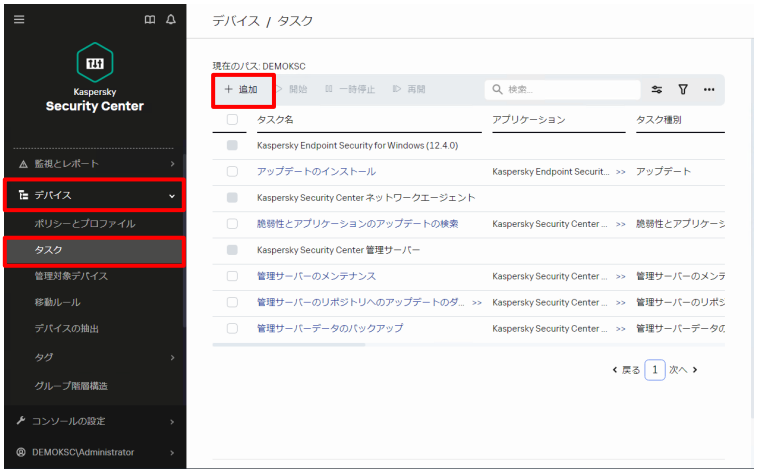
パターン 2：KES が未導入のデバイスに対し、EDR-O コンポーネントを追加した KES をリモートインストールする場合

→「4.2. EDR-O コンポーネントを有効にした KES のリモートインストール」を参照

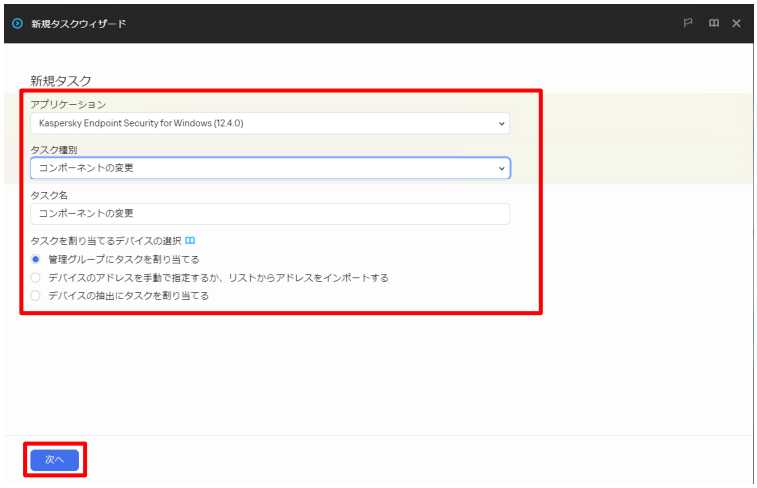
4.1.　EDR-O コンポーネントの有効化

KSC から「コンポーネントの変更」タスクを実行することでデバイスにインストール済みの KES に対し、EDR-O コンポーネントを追加することが出来ます。

(1) 「デバイス」-「タスク」を選択し、「現在のパス」が<管理サーバー名>になっていることを確認し、「追加」をクリックします。



(2) タスク追加ウィザードが表示されます。以下のアプリケーション/タスク種別/割り当てるデバイスを選択し、任意のタスク名を設定して「次へ」をクリックします。
ここではタスク名「コンポーネントの変更」とします。

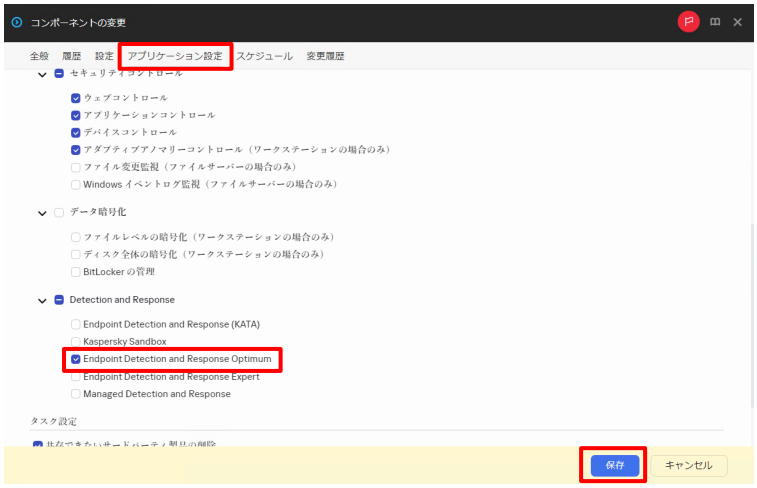


・アプリケーション：
　Kaspersky Endpoint Security for Windows (12.4.0)
・タスク種別：
　コンポーネントの変更
・タスクを割り当てるデバイスの選択：
　管理グループにタスクを割り当てる

(3) タスクを割り当てるグループを設定します。
「管理対象デバイス」にチェックを入れ、「次へ」をクリックします。

(4) 「タスクの作成が完了したらタスクの詳細を表示する」にチェックを入れ、「終了」をクリックします。

(5) タスクの作成完了後、タスクの詳細が表示されます。
「アプリケーション設定」タブを選択し、「Endpoint Detection and Response Optimum」にチェックを入れ「保存」をクリックします。

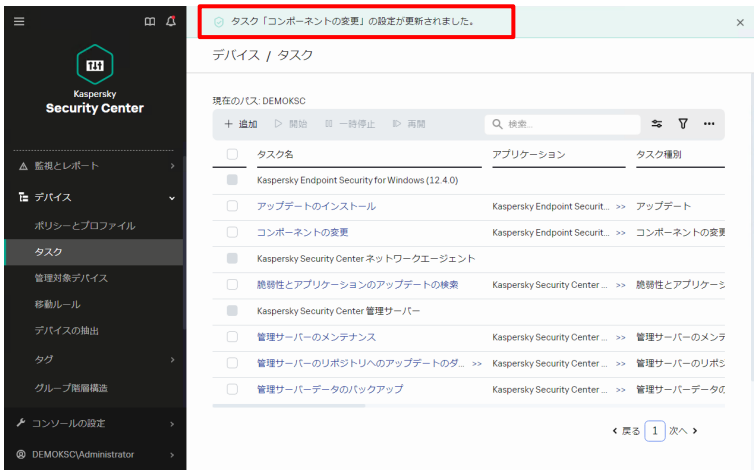


(6) タスクのスケジュールを設定します。
「スケジュール」タブをクリックし、タスクを作成した 5 分後にタスクが実行されるように設定をして「保存」をクリックします。
ここでは 2024/2/1　12:00 にタスクが実行されるよう以下の通り設定します。

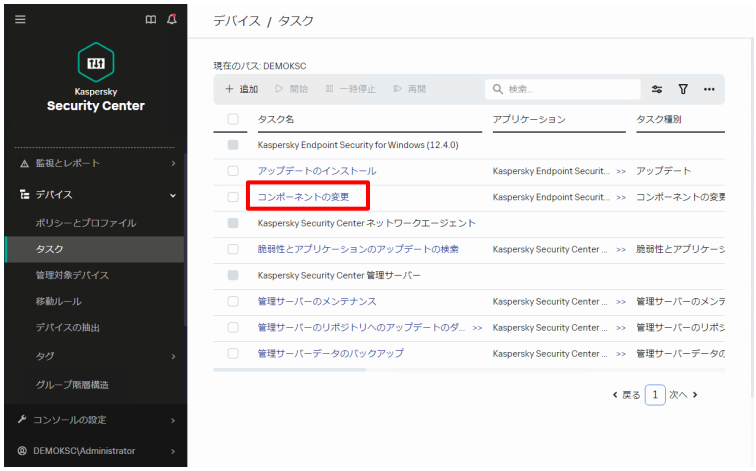
・実行予定：
　1 回
・日付：
　2024/2/1　(現在日時を設定)
・時間：
　12:00　(現在時刻の 5 分後を設定)
・タスクのその他の設定
　☑「未実行のタスクを実行する」
　☑「タスクの開始を自動的かつランダムに遅延させる」

　※上記設定で実行することで、タスク開始時にシャットダウンしていたデバイスは、起動時にタスクが開始されます。

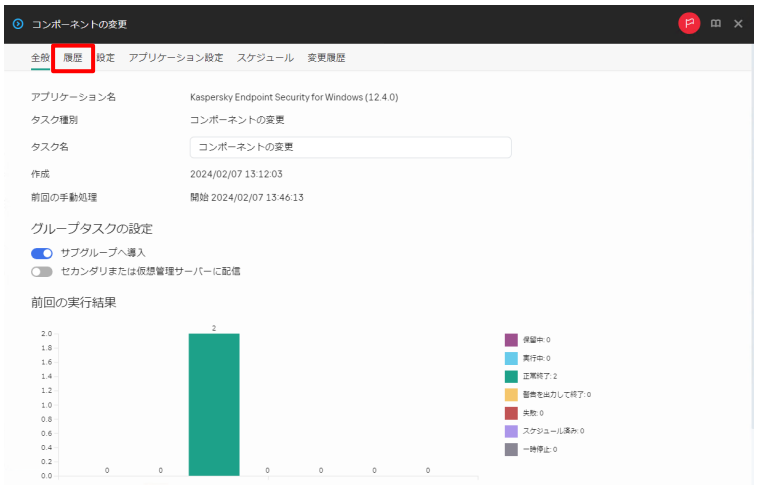
(7) 右図の通りタスクの設定が更新されたことが表示されます。



(8) 設定した時刻になるとタスクが開始されます。
タスクのステータス確認の為、「コンポーネントの変更」をクリックします。



(9) タスクのステータスが表示されます。
「履歴」タブをクリックします。



(10) 各デバイスのタスクのステータスが表示されます。
対象のデバイスのステータスがすべて「正常終了」になっていることを確認します。

以上になります。

4.2. EDR-O コンポーネントを有効にした KES のリモートインストール

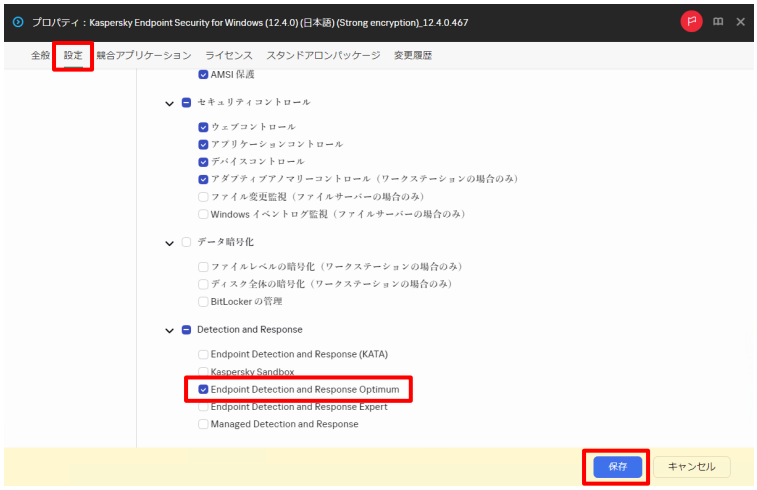
KSC で EDR-O コンポーネントを有効にした KES のインストールパッケージを作成し、リモートインストールする手順をご説明します。

※事前に NA がデバイスにインストールされている必要があります。
手順は別資料「Kaspersky Endpoint Security for Windows 12 簡単リモートインストールガイド」を参照し、実施してください。

(1) KES のインストールパッケージの設定変更をします。
「検出と製品の導入」-「導入と割り当て」-「インストールパッケージ」を選択します。

(2) KES のインストールパッケージを選択します。

(3) EDR コンポーネントを有効にします。
「設定」タブ-「保護機能」を選択し、「Endpoint Detection and Response Optimum」にチェックを入れ、「保存」をクリックします。



(4) 設定変更完了後、再度インストールパッケージの一覧画面が表示されます。

(5) KES をインストールするデバイス用のグループを作成します。
「デバイス」-「グループ階層構造」を選択し、「管理対象デバイス」にチェックを入れて「追加」をクリックします。

(6) 新しい管理グループの名前を入力して「追加」をクリックします。
ここではグループ名を「KES 未インストール」とします。

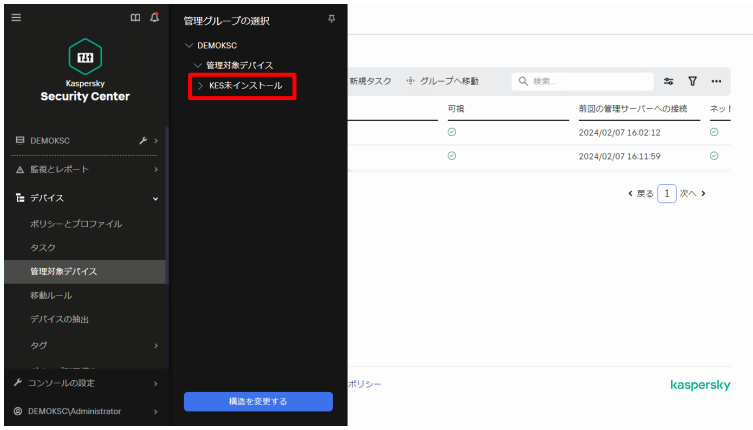
(7) 新しいグループが作成されたことを確認します。

(8) “(7)”で作成したグループに対象のクライアントデバイスを追加します。
「デバイス」-「管理対象デバイス」を選択し、移動したいクライアントデバイスにチェックを入れて「グループへ移動」をクリックします。

(9) 対象のクライアントデバイスの移動先のグループを設定します。
“(7)”で作成したグループにチェックを入れ、「移動」をクリックします。
ここでは、グループ名「KES 未インストール」を選択します。

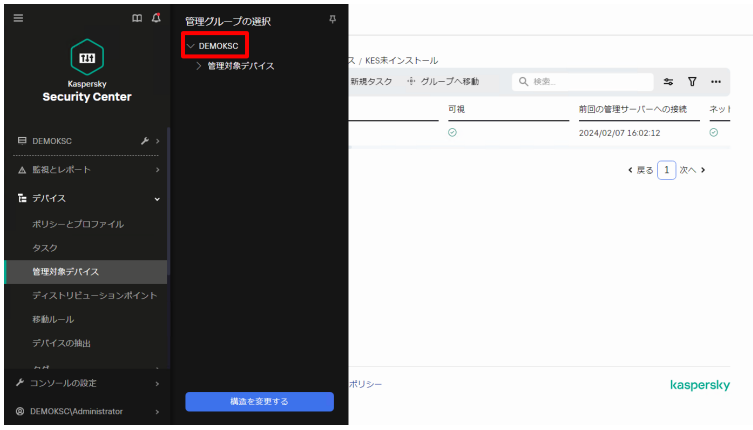
(10) 「現在のパス：<管理サーバー名>」をクリックします。

(11)　移動先のグループを選択します。
ここでは「KES 未インストール」をクリックします。

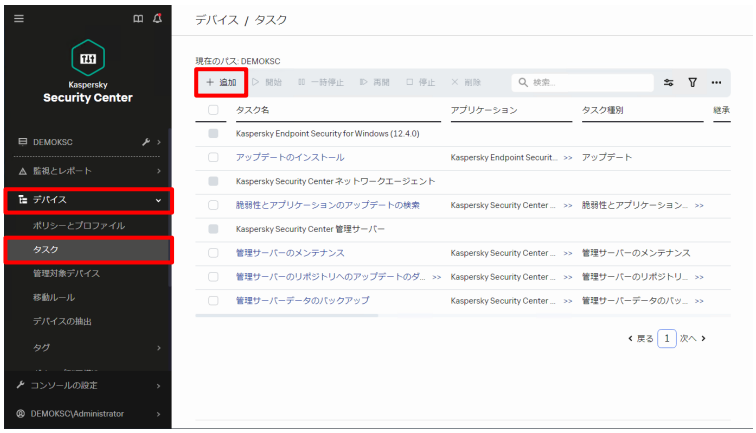


(12)　対象のクライアントデバイスがリストされていることを確認します。
確認後、「現在のパス：<管理サーバー名>/管理対象デバイス/<移動先グループ名>」をクリックします。

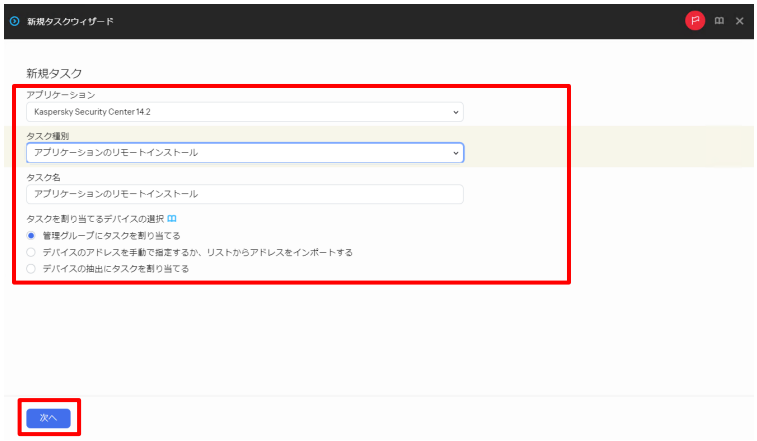
(13)　表示するグループを変更します。
「<管理サーバー名>」をクリックします。
ここでは「DEMOKSC」を選択します。



(14)　リモートインストールタスクを作成します。
「デバイス」-「タスク」を選択し、「現在のパス」が<管理サーバー名>になっていることを確認して「追加」をクリックします。



(15)　タスク追加ウィザードが表示されます。
以下のアプリケーション/タスク種別/割り当てるデバイスを選択し、任意のタスク名を設定して「次へ」をクリックします。
ここではタスク名「Kaspersky Endpoint Security for Windows のインストール」とします。



・アプリケーション：
　Kaspersky Security Center 14.2
・タスク種別：
　アプリケーションのリモートインストール
・タスクを割り当てるデバイスの選択：
　管理グループにタスクを割り当てる

(16)　タスクを割り当てるグループを設定します。
手順"(7)"で作成したグループにチェックを入れ、「次へ」をクリックします。
ここではグループ「KES 未インストール」にチェックを入れます。

(17)　インストールパッケージの設定をします。
KES のインストールパッケージを選択し、「次へ」をクリックします。

(18)　インストール後の OS 再起動方法を選択します。
ここでは「デバイスを再起動する」を選択し、「次へ」をクリックします。
競合他社製品がインストールされている場合など、KES インストール後に OS の再起動が必要となるケースがあります。

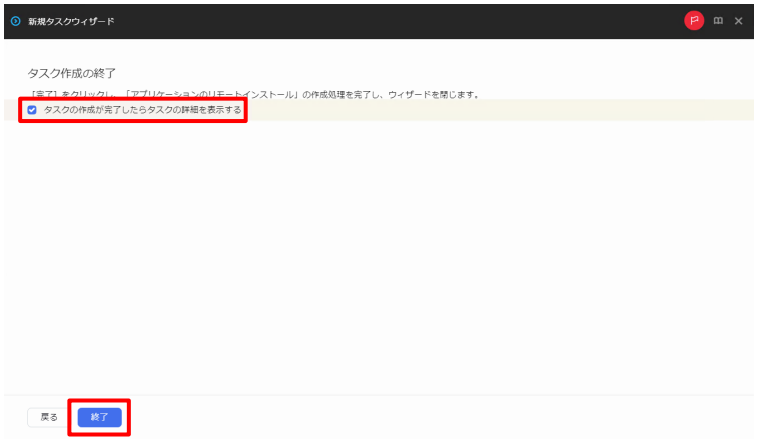
再起動について以下の設定が可能です。

- **デバイスを再起動しない**
  インストール完了後も再起動は行いません。OS が保護されない状態となりますのでご注意ください。
- **デバイスを再起動する**
  インストール完了後、60 秒のカウントダウン後 OS の再起動が強制的に行われます。
- **ユーザーに処理を確認する**
  インストール完了後、OS の再起動を選択 するダイアログが表示されます。
  既定では「延期」をすると 5 分後に再度通知され、30 分後に強制再起動が行われます。

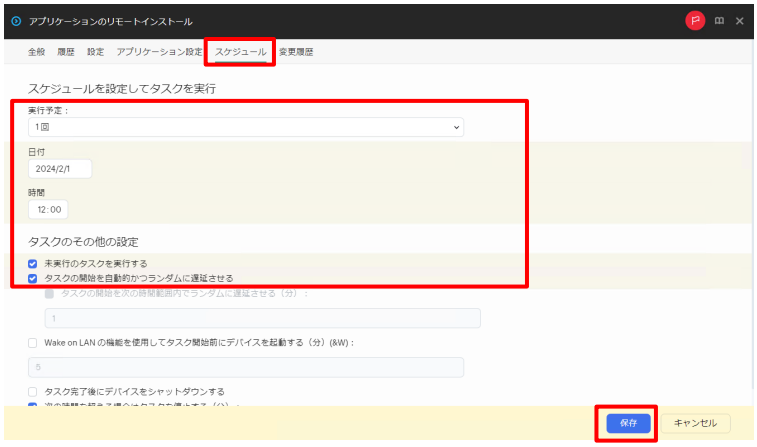
(19)　タスクの実行アカウントを指定します。
ここでは既定値のまま、「次へ」をクリックします。

既にネットワークエージェントがインストールされているデバイスに対しリモートインストールを行います。
ネットワークエージェント経由の場合、SYSTEM 権限でインストールが行われるため、アカウントの指定は不要です。

(20)　「タスクの作成が完了したらタスクの詳細を表示する」にチェックを入れ、「終了」をクリックします。



(21)　タスクのスケジュールを設定します。「スケジュール」タブをクリックし、タスクを作成した 5 分後にタスクが実行されるように設定をして「保存」をクリックします。
ここでは 2020/10/1　12:00 にタスクが実行されるよう以下の通り設定します。

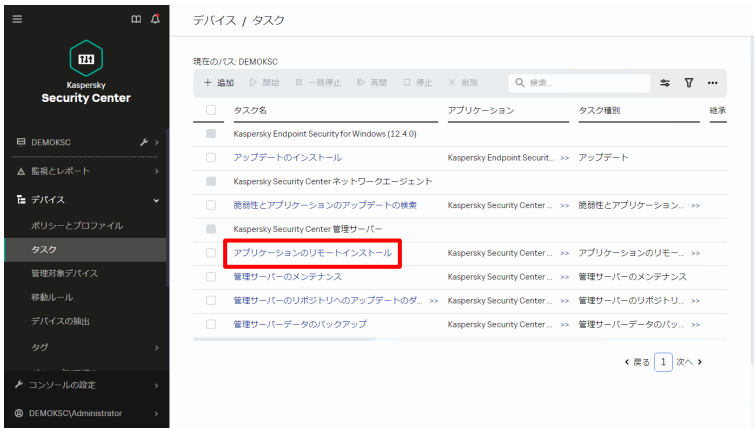


・実行予定：
　1 回
・日付：
　2024/2/1　(現在日時を設定)
・時間：
　12:00　(現在時刻の 5 分後を設定)
・タスクのその他の設定
　☑「未実行のタスクを実行する」
　☑「タスクの開始を自動的かつランダムに遅延させる」

　※上記設定で実行することで、タスク開始時にシャットダウンしていたデバイスは、起動時にタスクが開始されます。

(22)　右図の通りタスクの設定が更新されたことが表示されます。

(23)　設定した時刻になるとタスクが開始されます。
タスクのステータス確認の為、作成したリモートインストールタスクをクリックします。



(24)　「履歴」タブをクリックし、対象のデバイスのステータスが「正常終了」になっていることを確認します。

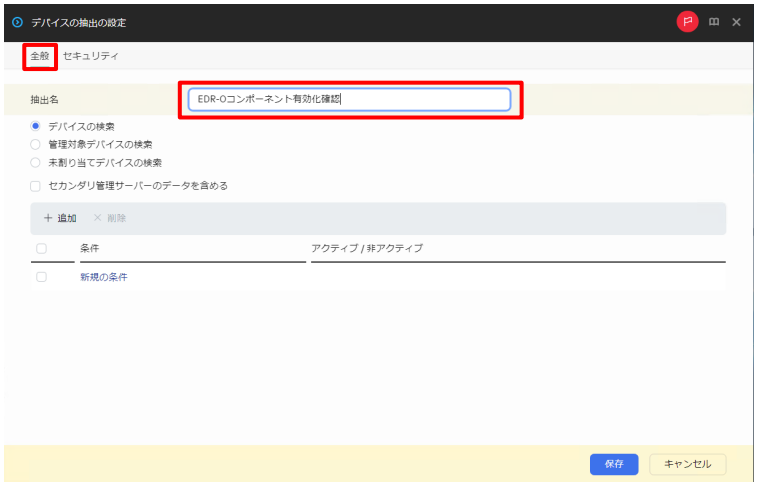
以上になります。

5. EDR-O コンポーネント有効化確認

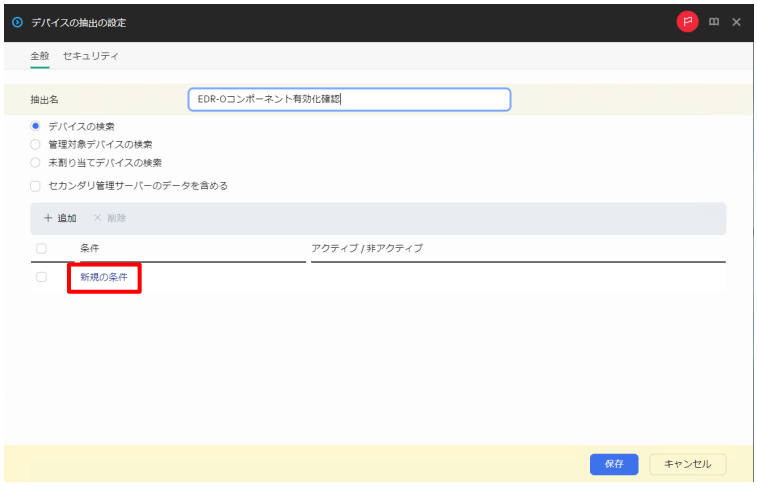
本章では対象のクライアントデバイスの EDR-O コンポーネントが有効化されているかを KSC の「デバイスの抽出」機能で確認する手順をご説明します。

(1) 「デバイス」-「デバイスの抽出」を選択し、「追加」をクリックします。

(2) デバイスの抽出の設定プロパティが表示されます。
「全般」タブを選択し、任意の抽出名を入力します。
ここでは「EDR-O コンポーネント有効化確認」とします。



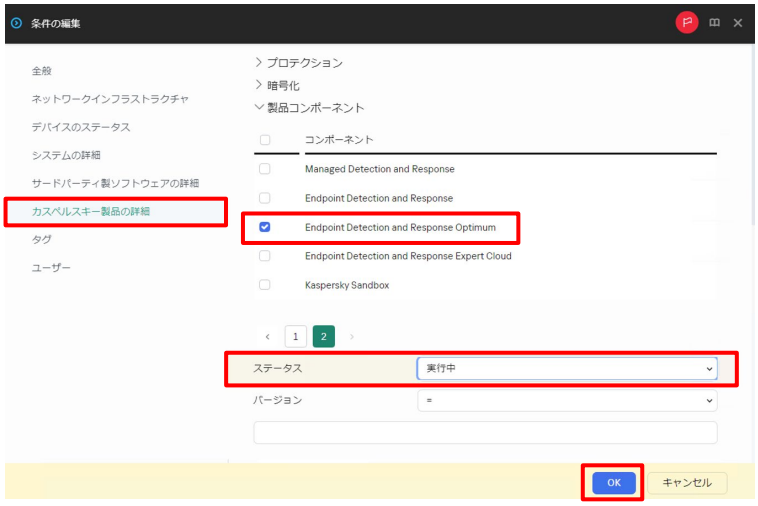
(3) デバイスの抽出条件を追加します。
「新規の条件」をクリックします。



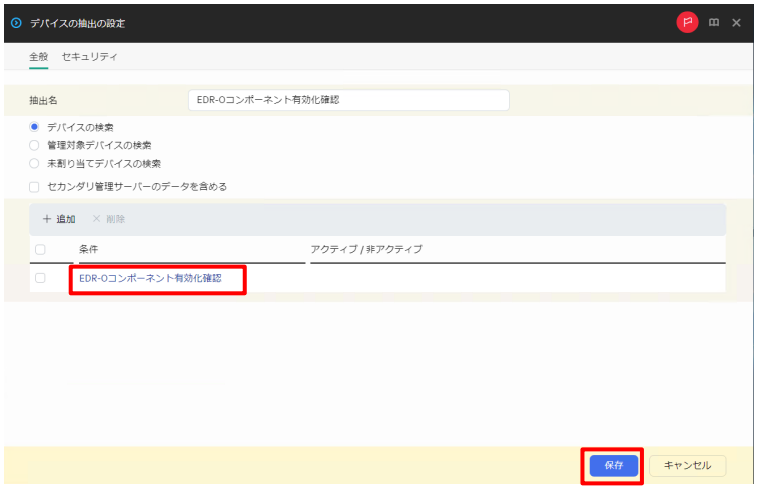
(4) 「全般」タブを選択し、任意の条件名を入力します。
ここでは「EDR-O コンポーネント有効化確認」とします。

(5) 「カスペルスキー製品の詳細」タブを選択し、条件を以下の通り設定し、「OK」をクリックます。

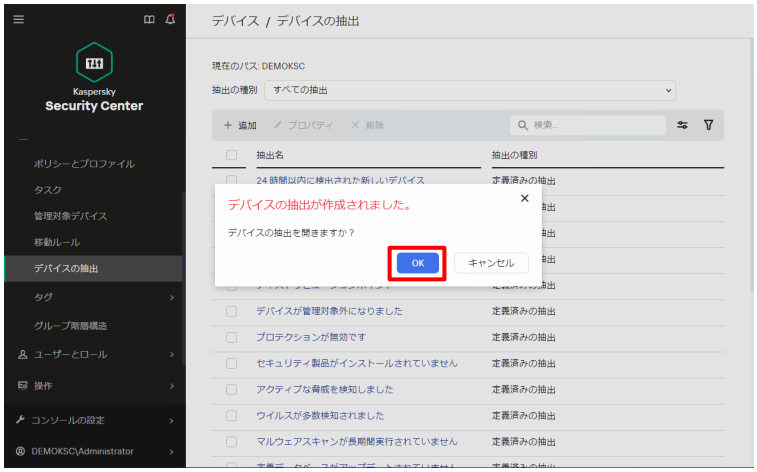
・製品コンポーネント名：
Endpoint Detection and Response Optimum
・ステータス：
実行中



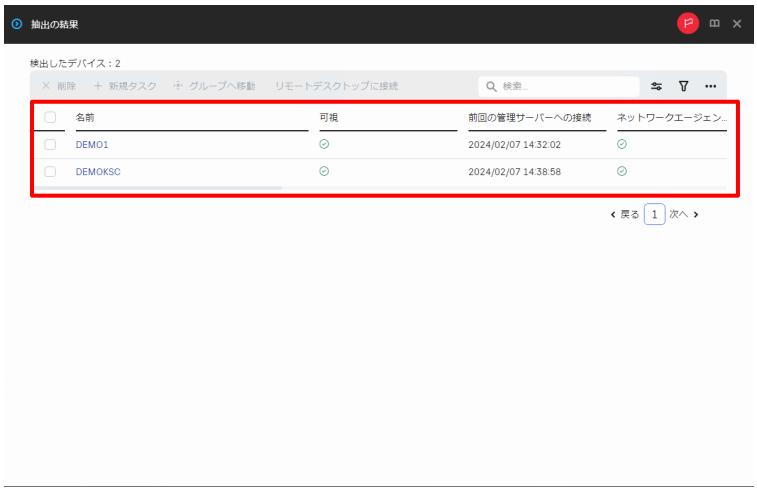
(6) 作成した抽出条件が追加されたことを確認し、「保存」をクリックします。



(7) デバイスの抽出が作成され、右図のようなポップアップが表示されるので「OK」をクリックします。



(8) EDR-O コンポーネントが実行中のクライアントデバイスが一覧表示されます。
対象のクライアントデバイスが全てリストされていることを確認します。



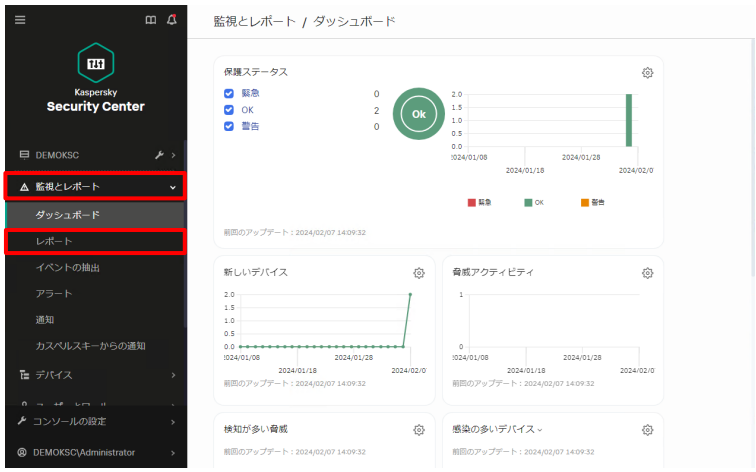
以上になります。

6.　脅威レポート設定変更

本章ではインシデントカード作成の為に必要な脅威レポートの設定変更の手順についてご説明します。

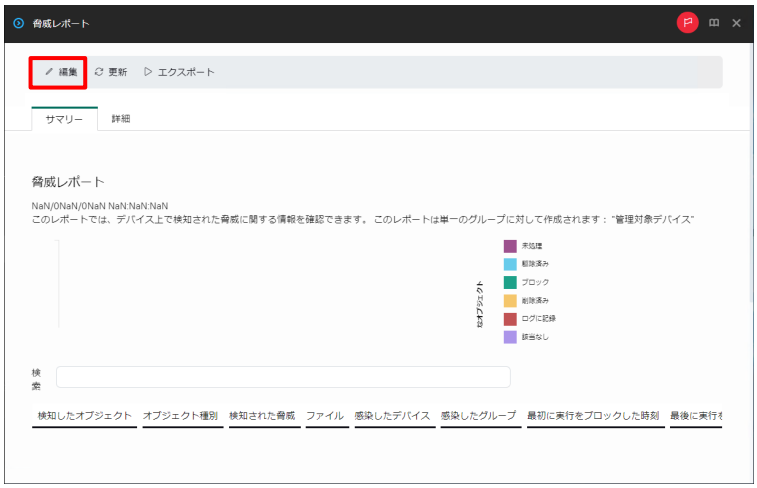
インシデントカードを表示することでインシデントの詳細情報の確認やホストの隔離、Prevent ルールの作成をすることが可能です。

(1) 脅威レポートの設定変更をします。
「監視とレポート」-「レポート」を選択します。



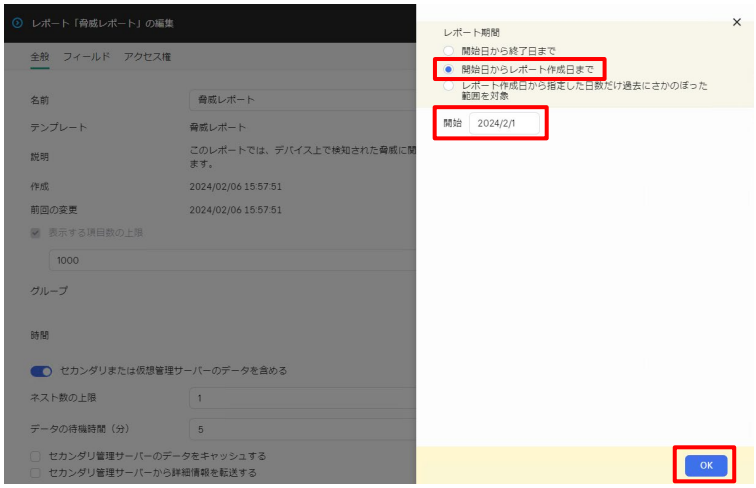
(2) 「脅威レポート」をクリックします。

(3) 「編集」をクリックします。

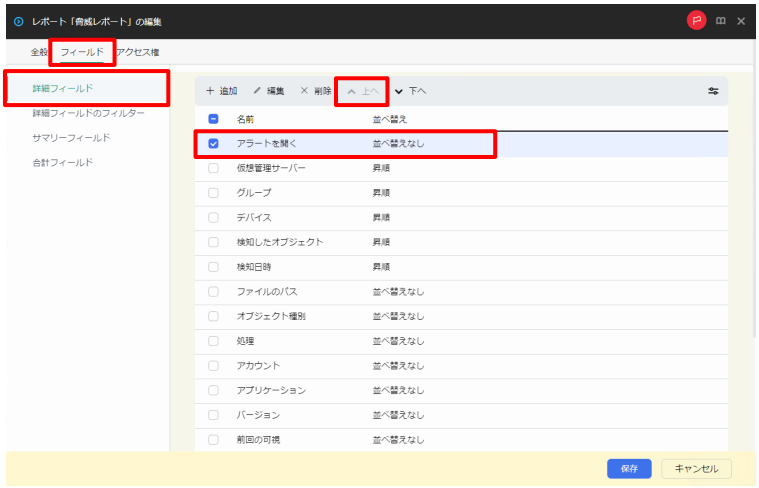


(4) レポート設定のプロパティが表示されます。「全般」タブの「時間」-「設定」を選択します。

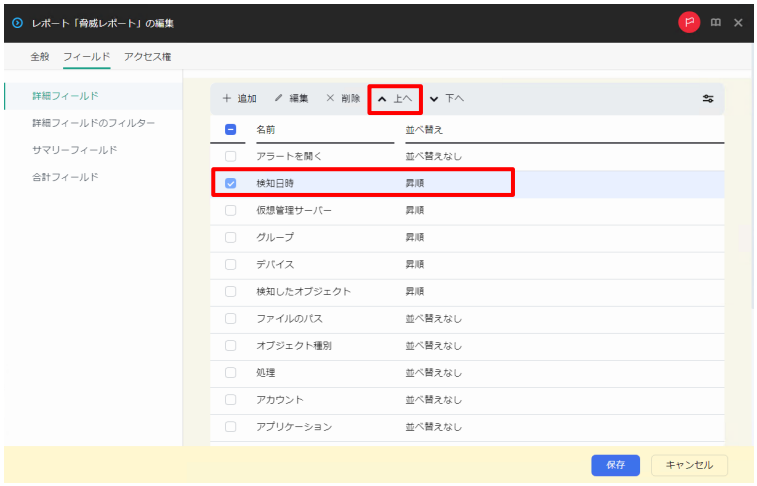
(5) レポート期間を設定します。「開始日からレポート作成日まで」を選択し、任意の開始日を設定して「OK」をクリックします。
ここでは開始日を「2024/2/1」とします。



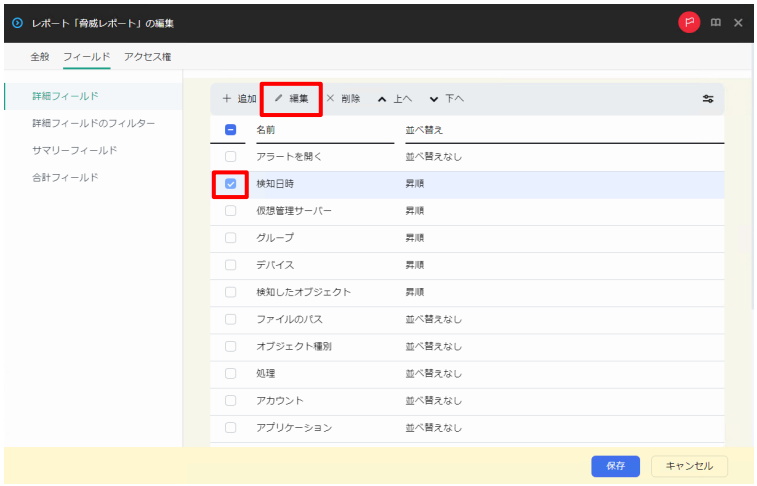
(6) 「フィールド」-「詳細フィールド」タブを選択し、「アラートを開く」にチェックを入れ、一番上になるように「上へ」をクリックして移動します。



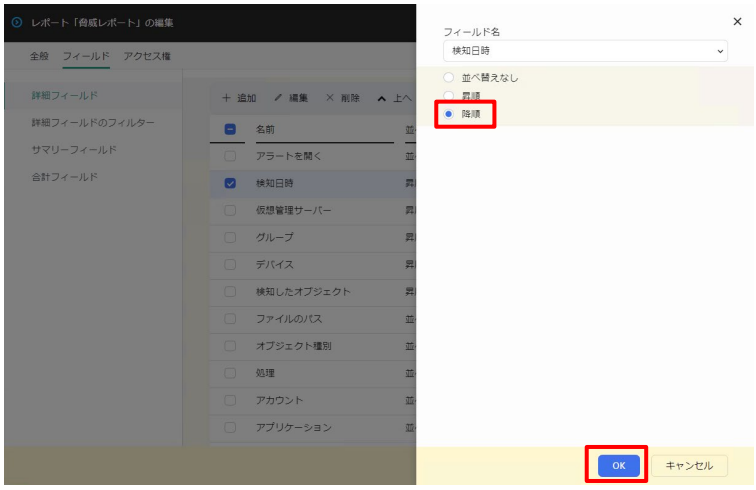
(7) 「検知日時」フィールドにチェックを入れ、上から二番目になるように「上へ」をクリックして移動します。



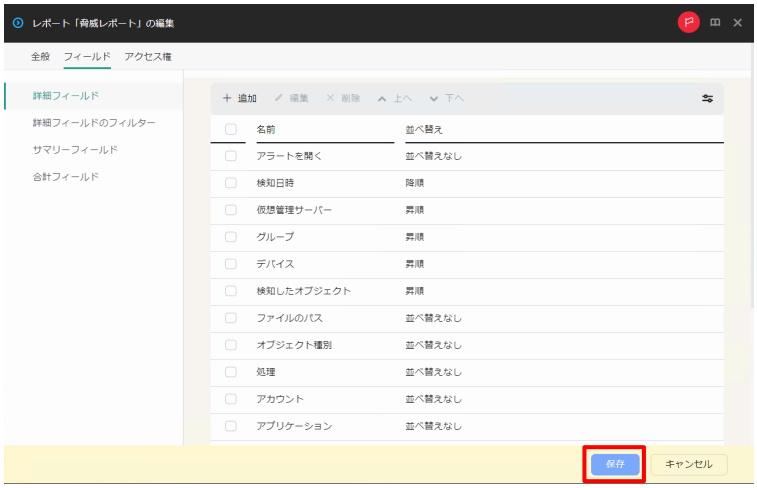
(8) フィールドの並び替えの設定をします。「検知日時」フィールドにチェックを入れ、「編集」をクリックします。



(9) 「降順」を選択し、「OK」をクリックします。



(10)　「保存」をクリックします。



(11)　脅威レポートが更新されます。

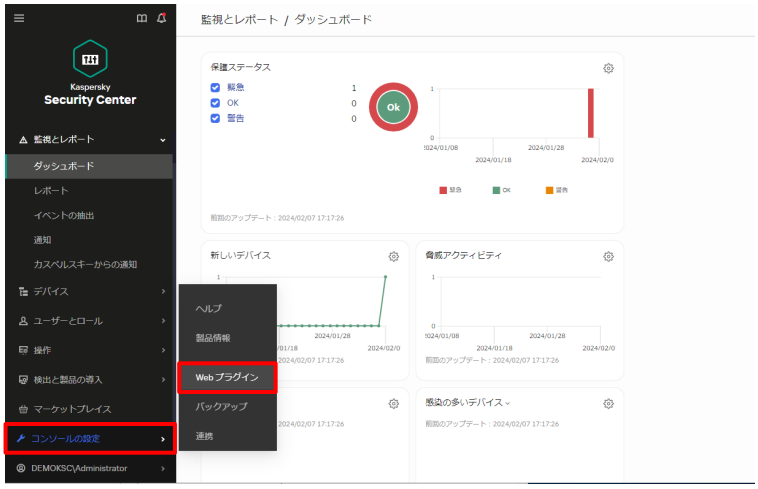
以上になります。

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。

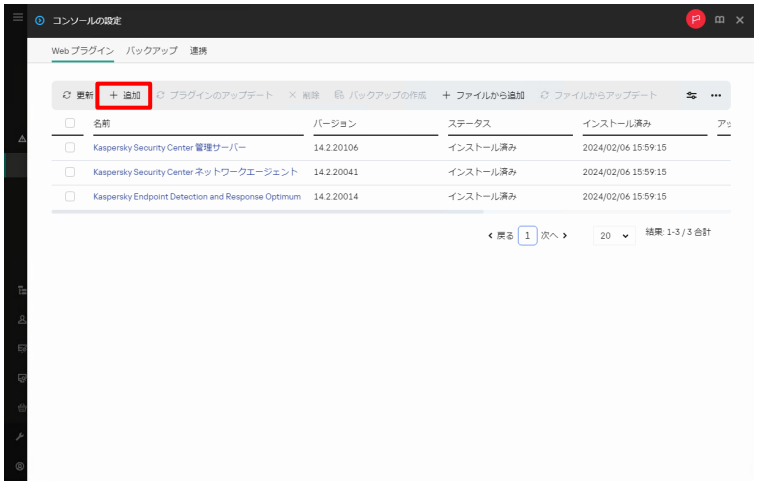
1. KES の Web プラグインのインストール

KES の Web プラグインのインストール手順についてご説明します。

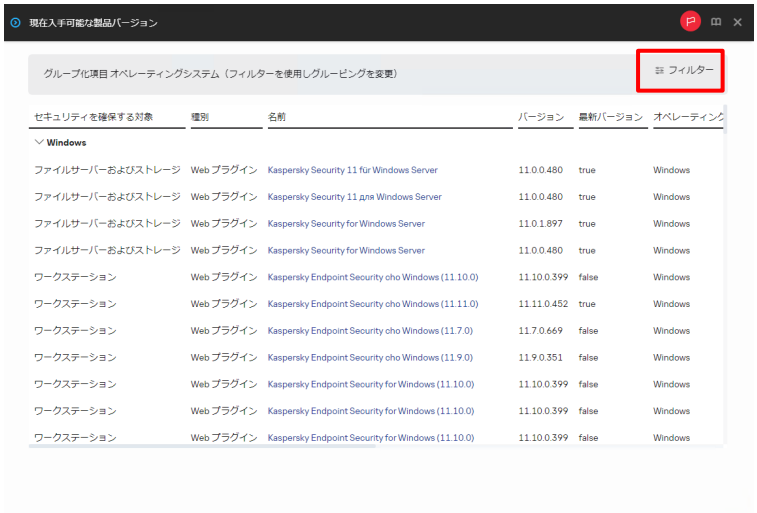
(1) Web コンソールにて「コンソールの設定」をクリックし、「Web プラグイン」を選択します。



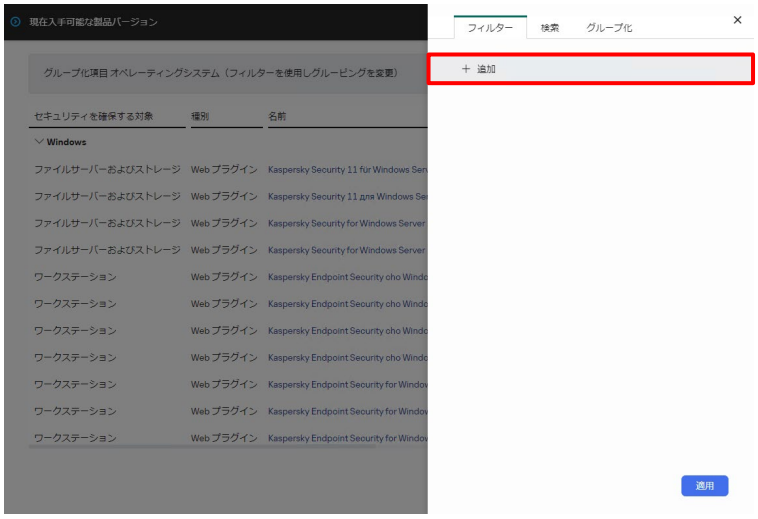
(2) 「追加」をクリックします。



(3)「フィルター」をクリックします。

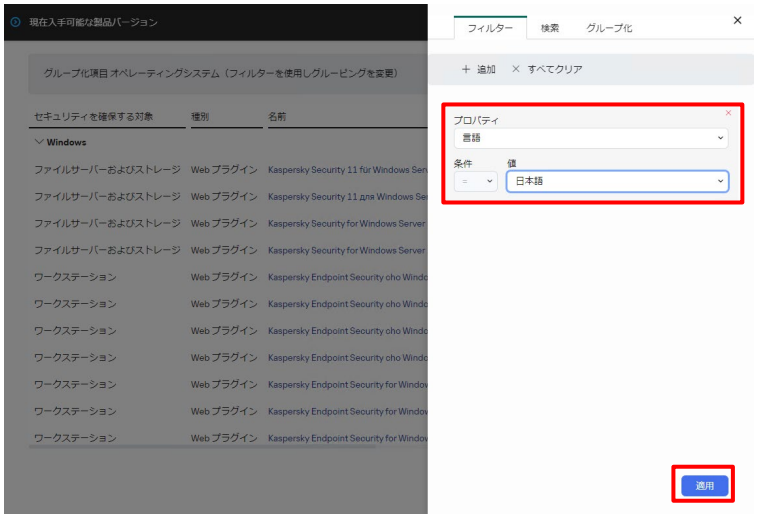


(4)「追加」をクリックします。

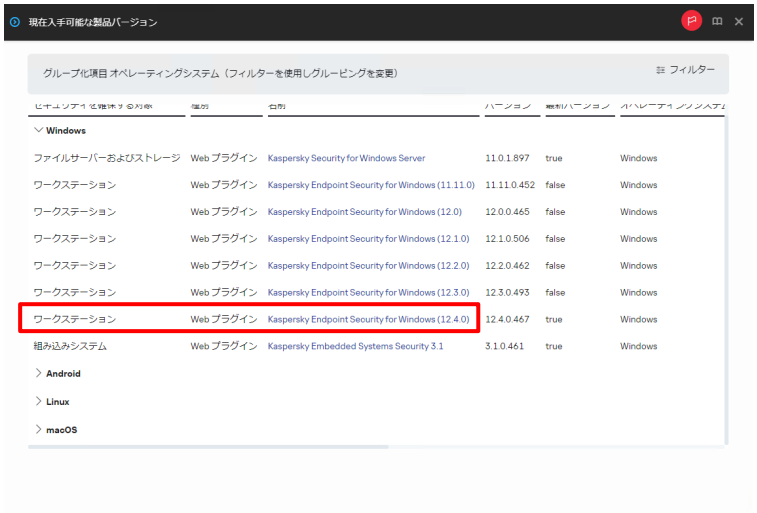


(5) 以下の条件でフィルターを設定し、「適用」をクリックします。

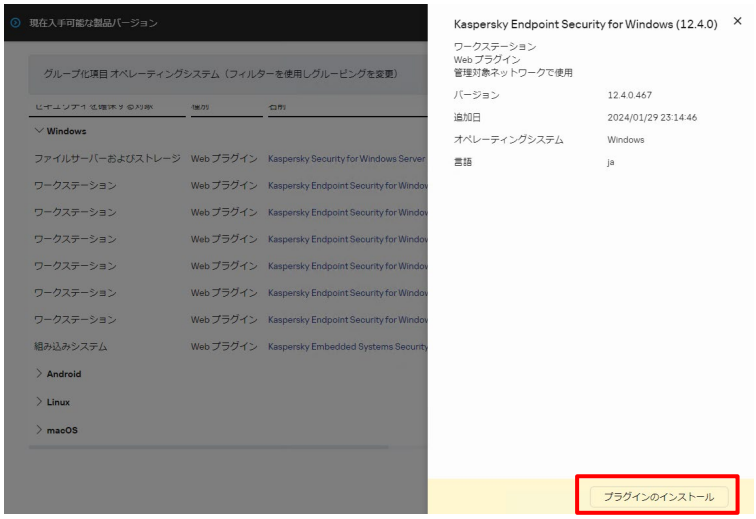
プロパティ：
「言語」
条件：
「＝」
値：
「日本語」



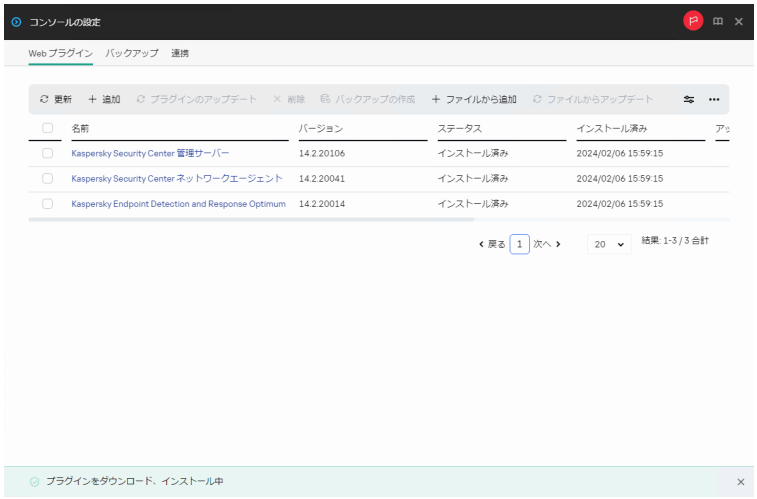
(6) 表示された Web プラグインから最新版の KES をクリックします。



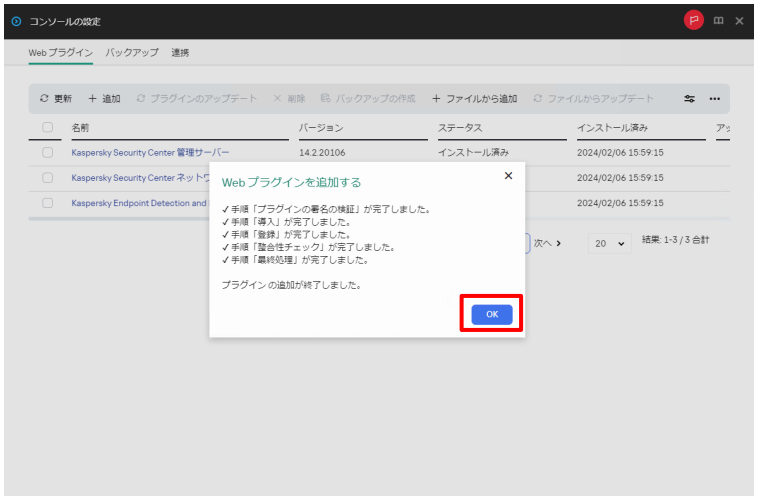
(7) 「プラグインのインストール」をクリックします。



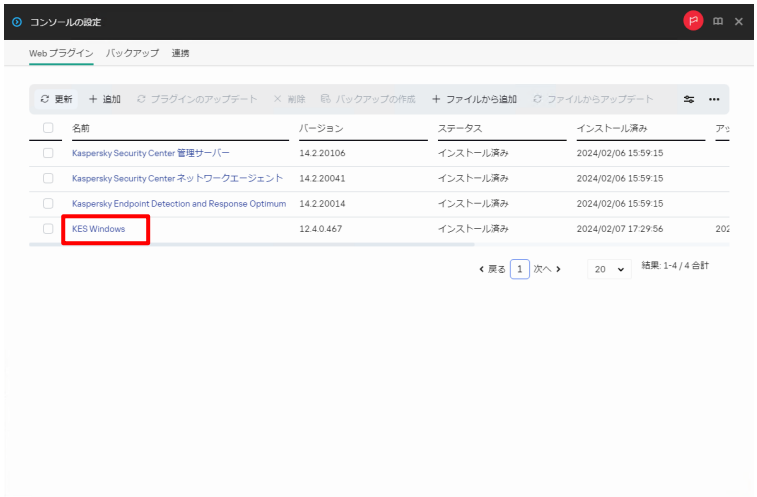
(8) インストール完了までしばらく待ちます。



(9) インストールが完了したことを確認し、「OK」をクリックします。



(10) 「Kaspersky Endpoint Security for Windows」のプラグインが追加されたことを確認します。



以上になります。

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

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