Kaspersky Security Center 14.2
Kaspersky Endpoint Security for Windows
運用ガイド

2023/08/18

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. 1.1

kaspersky

目次

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、運用を開始するにあたり、Kaspersky Security Center において定期的に確認すべき項目、及び効果的な使用方法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」**
「KSC を使用した KES 展開ガイド」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

→ **「KSC14 ポリシータスク初期設定ガイド」をご参照ください。**

STEP 5.

運用開始

→ **本資料を参照し、各手順に従い運用してください。**

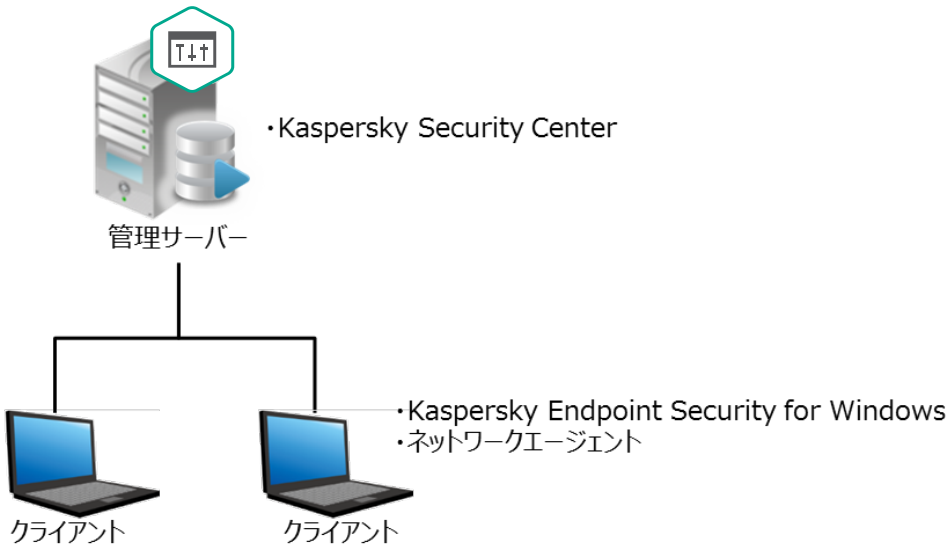
上述の各資料は、以下サイトから閲覧、ダウンロードすることができます。

- 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

- **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。

- **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 14 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。

- **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デバイスにインストールされます。

- **Kaspersky Security Center 14 ネットワークエージェント（以降 NA）：**
  KSC とクライアント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. タスクの確認と手順

本章では、運用に必要なタスクと、その確認手順についてご説明します。

3.1. 定義データベースの更新タスクについて

カスペルスキーでは、コンピューターセキュリティへの脅威に関する情報をデータベースとして公開しております。
保護システムの信頼性を維持するためには、定義データベースのアップデートを実施する必要があります。

3.1.1. KSC における定義データベースの更新

既定では、KSC がインターネット上のカスペルスキーサーバーから定義データベースのダウンロードを行い、管理下のクライアントへ展開するよう設定されております。
KSC をインストールし、「管理サーバークイックスタートウィザード」を実行すると、KSC が定義データベースをダウンロードするタスクである**「管理サーバーのリポジトリへのアップデートのダウンロード」**が作成されます。

既定では、以下のように設定されております。

スケジュール：1 時間毎
アップデート元：Kaspersky Lab のアップデートサーバー

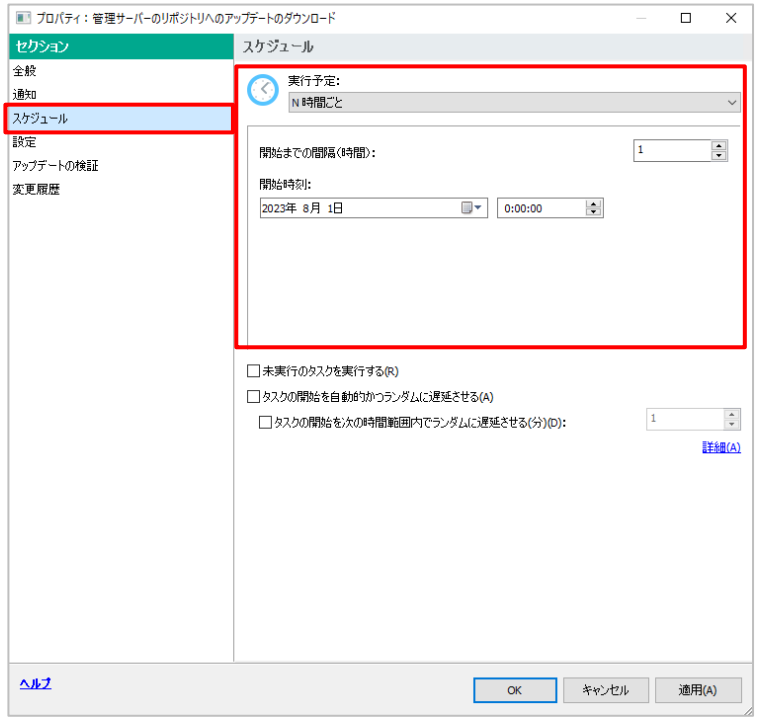
kaspersky

・「管理サーバーのリポジトリへのアップデートのダウンロード」タスクの設定確認

(1) KSC にて「タスク」を開きます。
一覧から「管理サーバーのリポジトリへのアップデートのダウンロード」を右クリックし、プロパティを選択します。

(2) 「スケジュール」セクションを開きます。

ここでは、このタスクが実行する間隔を設定します。
既定では、**1 時間毎**に実行するようスケジュールされております。
1 時間毎にサーバーへ問い合わせを行い、更新があった場合はダウンロードを行います。



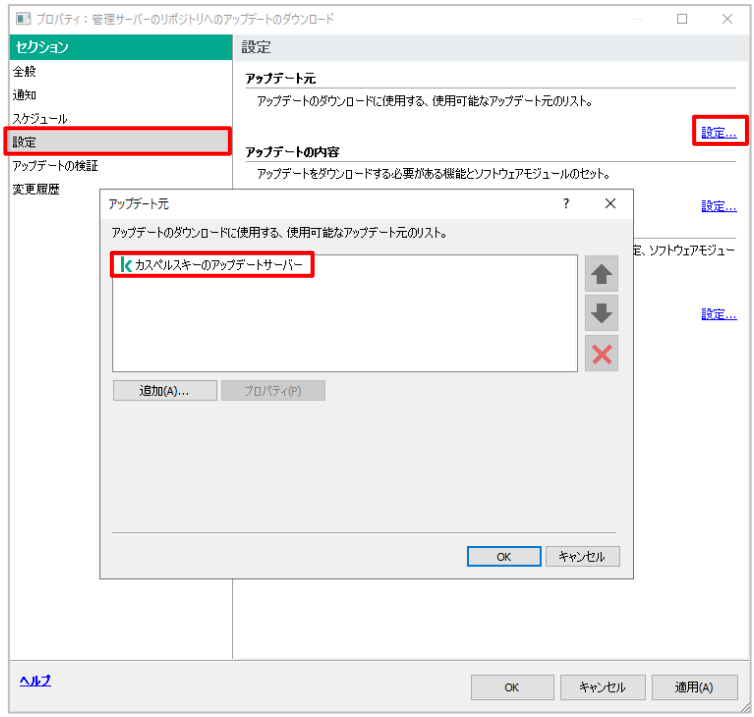
(3) 「設定」セクションを開きます。

右画面にて「アップデート元」の「設定」をクリックします。

アップデート元となる宛先が設定されております。

既定では、**「Kaspersky Lab のアップデートサーバー」**が指定されております。

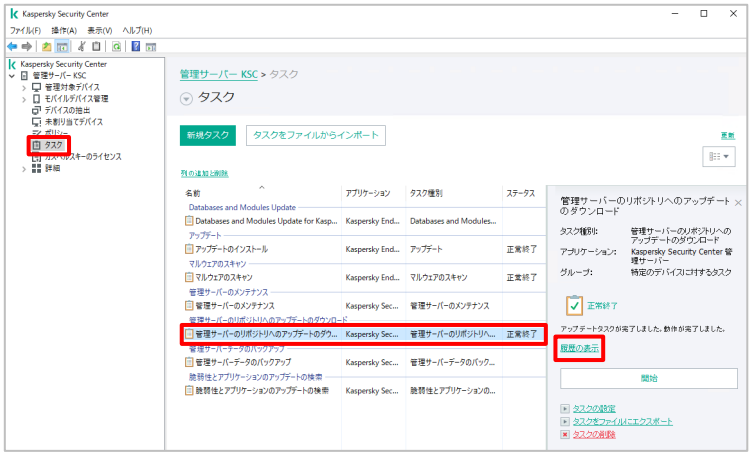
宛先を変更する場合は、「追加」をクリックすることで別の URL や共有フォルダーなど指定することも可能です。



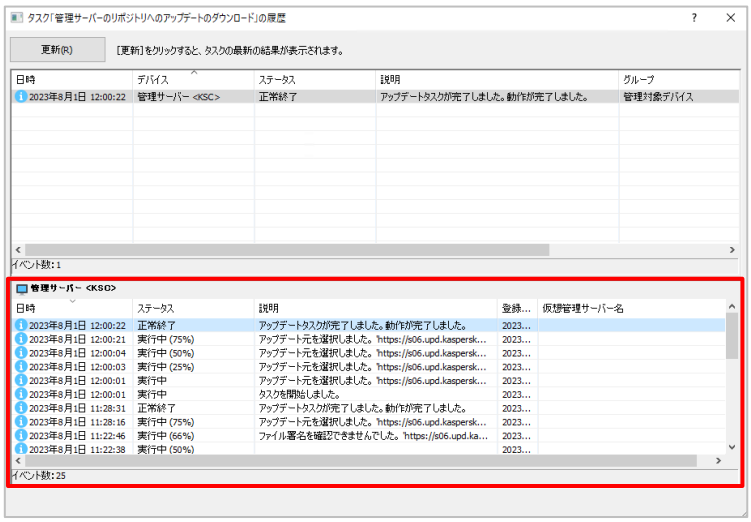
本項は以上です。

・「リポジトリへのアップデートのダウンロード」タスクの実行状態確認

(1) KSC にて「タスク」を開きます。
一覧から「リポジトリへのアップデートのダウンロード」を選択し、右に表示される「履歴の表示」をクリックします。
（または、タスクを右クリックし、「履歴」を選択します）



(2) タスクの実行履歴画面が表示されます。
右記のように、「アップデートタスクが完了しました。正常に完了しました」と表示されていることを確認してください。



本項は以上です。

3.1.2. KES に対する定義データベースの更新

KSC をインストールし、「管理サーバークイックスタートウィザード」を実行すると、KES に対する定義データベース更新タスクである**「アップデートのインストール」**が自動的に作成されます。

既定では、以下のように設定されております。

スケジュール：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

「未実行のタスクを実行する」：オン

この設定が有効である場合、スケジュールされた時刻にデバイスがシャットダウンされていると、デバイスの起動後にタスクが実行されます。

「タスクの開始を自動的かつランダムに遅延させる」：インストール時の設定による

この設定が有効である場合、タスクの実行対象デバイス数により、ランダムにタスクが開始されます。

KSC のインストール時に管理対象デバイス数の設定を、「101-1,000 台」以上とした場合、自動的に有効となります。

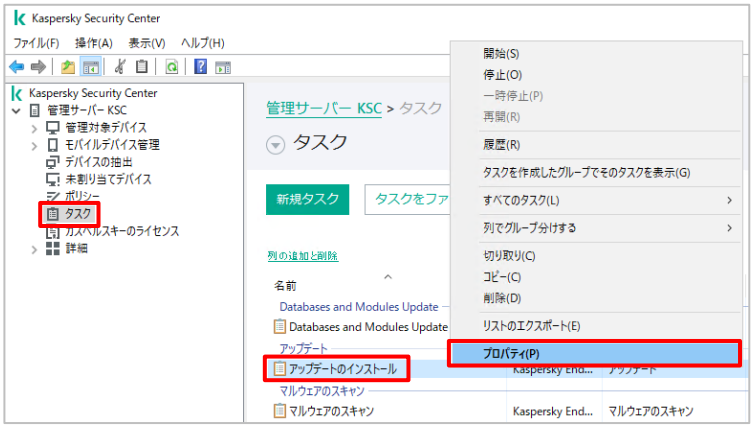
手動で間隔を設定する場合はこのチェックを外し、「タスクを次の時間内にランダムに実行する」にチェックを入れ、時間範囲(分)を入力します。

アップデート元：Kaspersky Security Center

kaspersky

・「アップデートのインストール」タスクの設定確認

(1) KSC にて「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。
一覧から「アップデートのインストール」を右クリックし、プロパティを選択します。

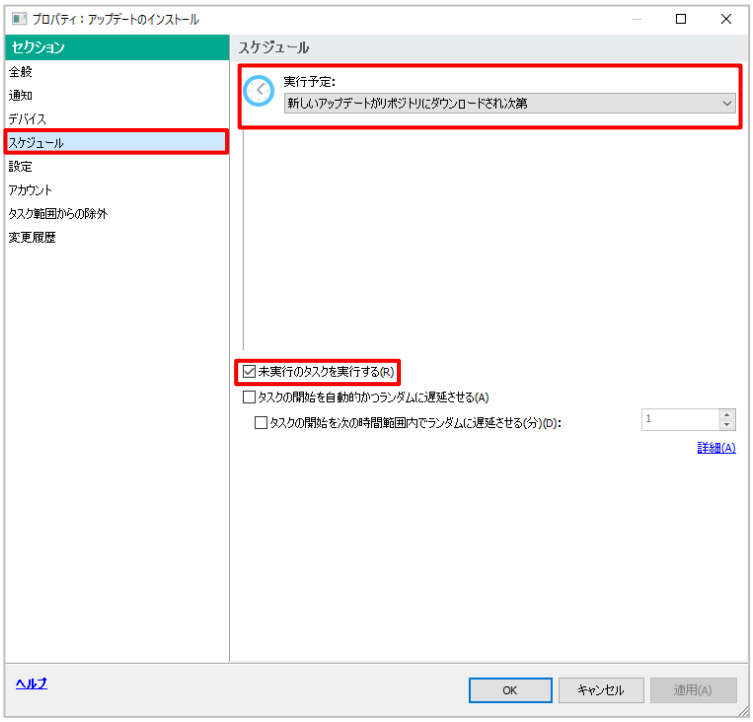


(2) 「スケジュール」セクションを開きます。

既定では、KSC 上の定義データベース情報が更新された場合に開始するよう、「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」にスケジュールされております。
運用に合わせ、スケジュールを設定してください。

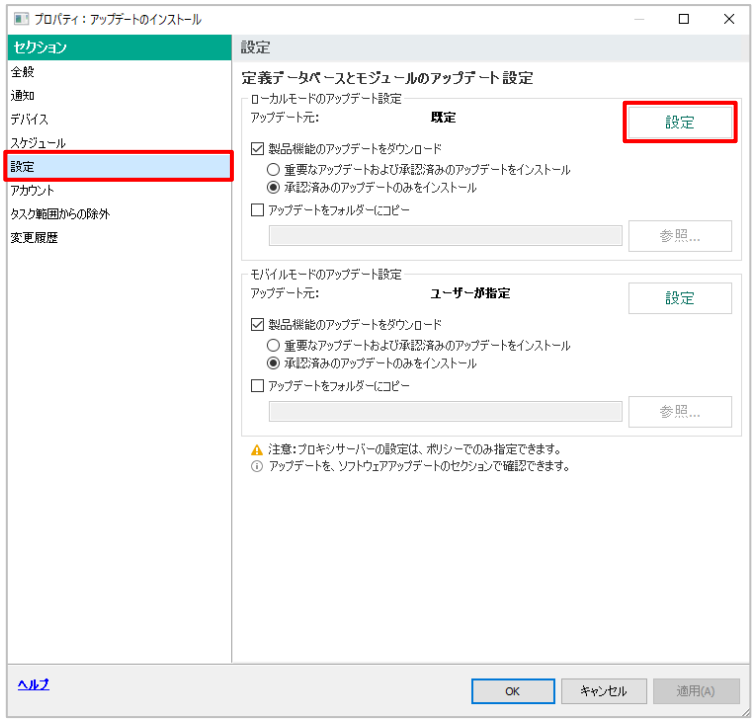
また、以下設定も有効となっております。
・未実行のタスクを実行する。

以下は、インストール時に指定したデバイス数により変わります。
・タスクの開始を自動的かつランダムに遅延させる



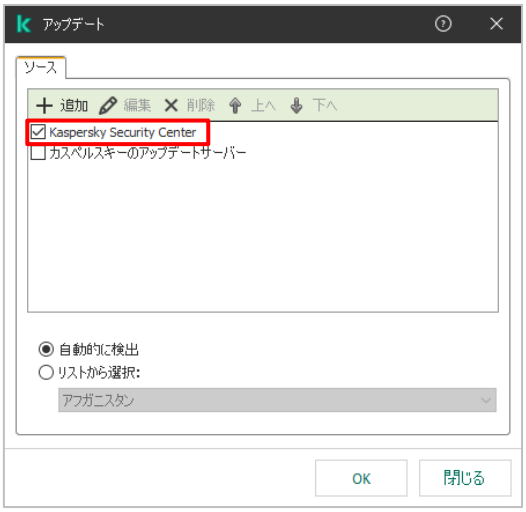
(3) 「オプション」セクションを開きます。

「ローカルモードのアップデート設定」にある「設定」ボタンをクリックします。



(4) アップデート元の設定を確認することができます。

既定では、「Kaspersky Security Center」が指定されており、定義データベースを KSC からダウンロードするよう設定されております。



本項は以上です。

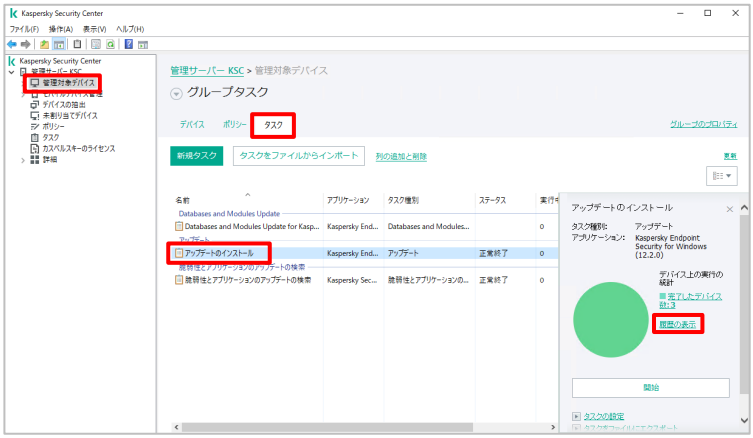
kaspersky

・「アップデートのインストール」タスクの実行状態確認

(1) KSC にて「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。

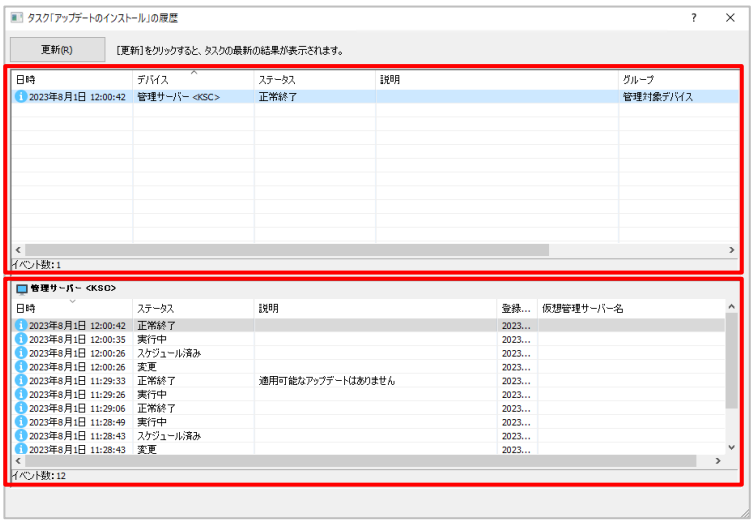
一覧から「アップデート」を選択します。
実行中の場合、右側に実行状態が表示されます。

一覧を表示する場合は、「履歴の表示」をクリックします。



(2) デバイス毎のタスク実行状態が表示されます。

画面上段には、デバイス毎のステータス一覧が表示されます。
上段にてデバイスを選択すると、下段に該当デバイスのステータス詳細が表示されます。



本節は以上です。

3.2. スキャンタスクについて

KSC14 では、既定で KES をスキャンするタスクは作成されません。デバイスをスキャンする場合、タスクを手動で作成する必要があります。

スキャンタスクの作成方法は、以下サイトにある**「初期設定ガイド」**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/）

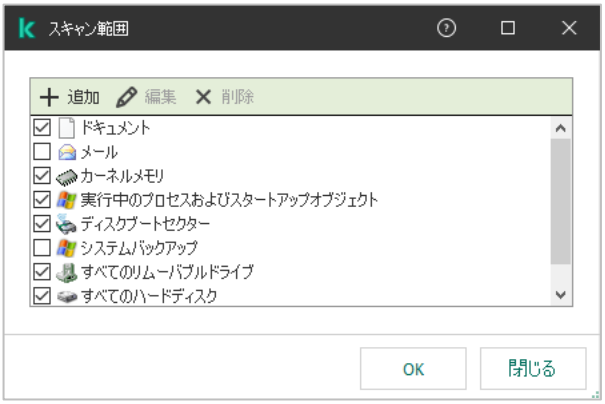
KSC では既定で、7 日上スキャンされていないデバイスを「警告」、14 日以上スキャンされていないデバイスを「緊急」としてステータスを設定しております。（ステータスに関する詳細は**「4.5. 保護ステータスの確認」**をご参照ください）

以下の範囲がスキャンされている場合、スキャン済みとして認識され、デバイスのステータスは変わりません。

●スキャン範囲

- カーネルメモリ
- 実行中のプロセスおよびスタートアップオブジェクト
- ディスクブートセクター
- すべてのハードディスク

[スキャン範囲]



スキャンによるステータスの変更を無効化したい場合、**「4.5.3 保護ステータスの設定」**をご参照ください。

kaspersky

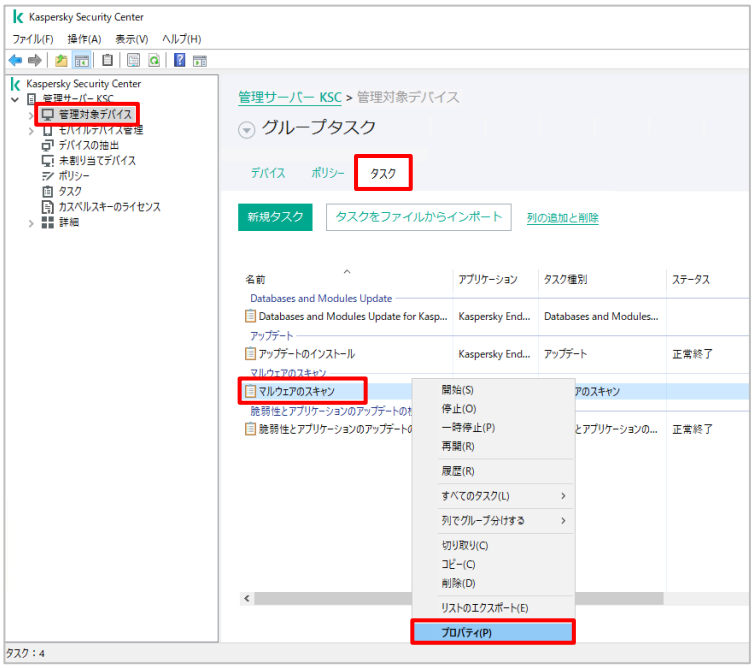
・「スキャン」タスクの確認

※スキャンタスクが作成されていることを前提とします。

(1) KSC にて「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。

「マルウェアのスキャン」という名前のスキャンタスクを右クリックし、「プロパティ」をクリックします。

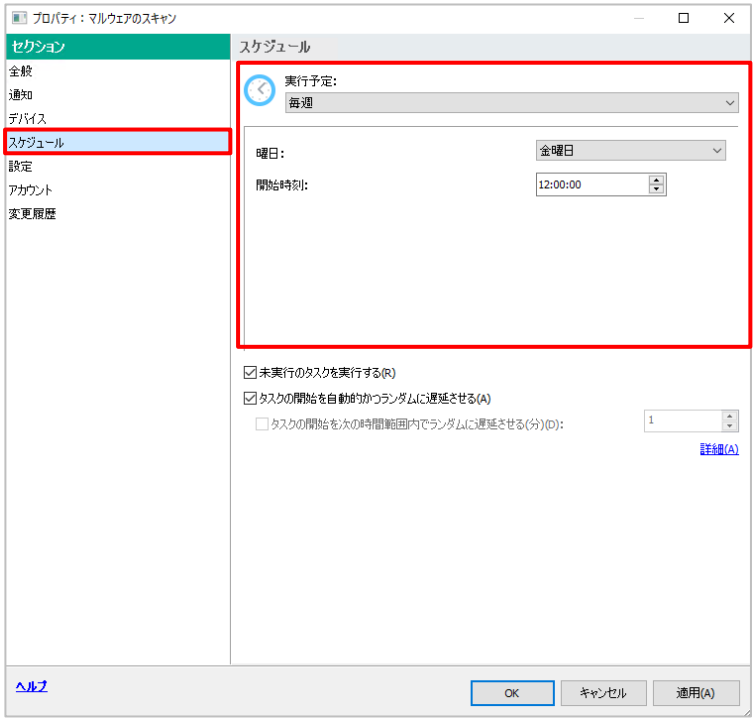
※ ここでは、「スキャン」という名前でスキャンタスクを作成しています。



(2) 「スケジュール」セクションを開きます。

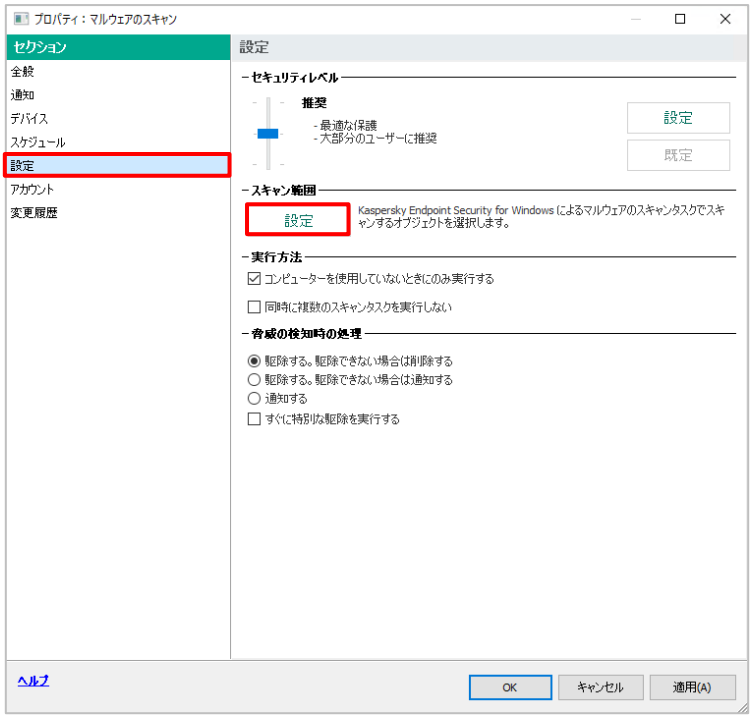
ここでは、スキャンを開始するスケジュールが設定できます。
また、以下の設定も可能です。
・未実行のタスクを実行する。
・タスクの開始を自動的かつランダムに遅延させる
・タスクの開始を次の時間範囲内でランダムに遅延させる

運用に合わせ設定を実施してください。



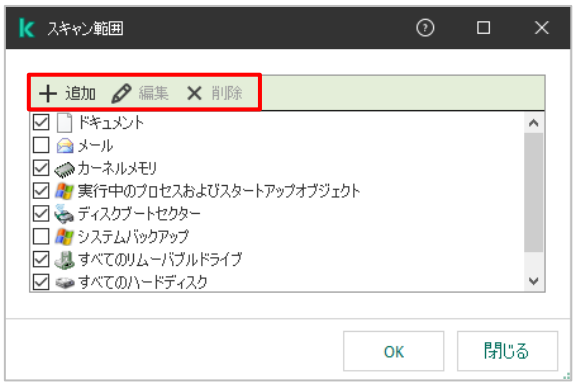
(3) 「オプション」セクションを開きます。

「スキャン範囲」にある「設定」ボタンをクリックします。



(4) スキャン範囲を確認できます。

「追加」「削除」ボタンにてスキャン範囲を設定することができます。



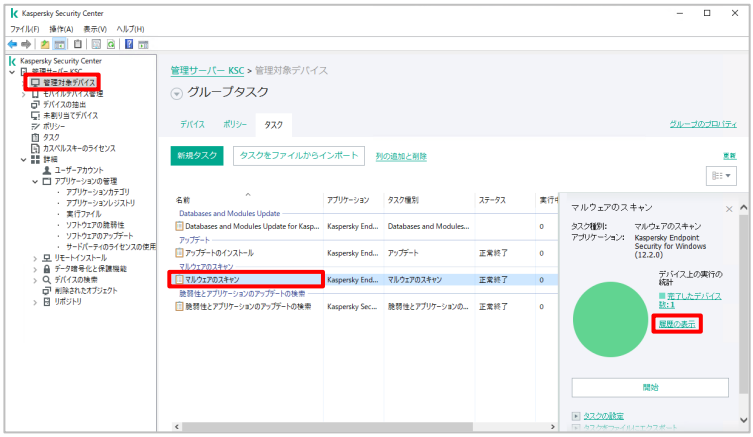
kaspersky

・「スキャン」タスクの実行状態確認

(1) KSC にて「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。

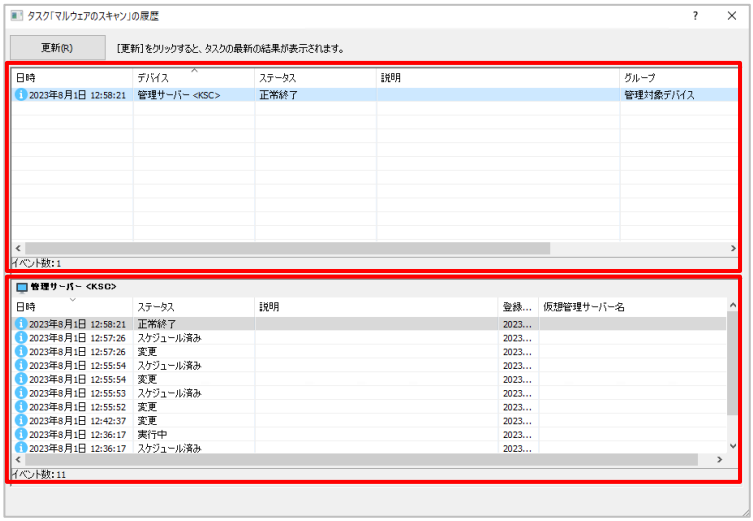
一覧から「マルウェアのスキャン」を選択します。
実行中の場合、右側に実行状態が表示されます。

一覧を表示する場合は、「履歴の表示」をクリックします。



(2) デバイス毎のタスク実行状態が表示されます。

画面上段には、デバイス毎のステータス一覧が表示されます。
デバイスを選択すると、下段にステータスの詳細が表示されます。



本節は以上です。

3.3. 「脆弱性とアプリケーションのアップデートの検索」タスクについて

KSC をインストールし、「管理サーバークイックスタートウィザード」を実行すると、**「脆弱性とアプリケーションのアップデートの検索」**タスクが作成されます。

このタスクは、デバイスにインストールされている OS やサードパーティ製アプリケーションにおける脆弱性のリスト、また、導入できるすべてのソフトウェアアップデート（アプリケーションの新しいバージョンなど）などの情報を収集し、KSC にて表示します。

収集した情報の確認方法は、本資料内の以下手順をご確認ください。

5.2. ソフトウェア、OS に関する脆弱性情報の確認

5.3. ソフトウェア、OS に関するアップデート情報の確認

本タスクは既定で、以下のように設定されております。

スケジュール：毎週火曜日 19:00

「未実行のタスクを実行する」：オン

この設定が有効である場合、スケジュールされた時刻にデバイスがシャットダウンされていると、デバイスの起動後にタスクが実行されます。

「タスクの開始を自動的かつランダムに遅延させる」：インストール時の設定による

この設定が有効である場合、タスクの実行対象デバイス数により、ランダムにタスクが開始されます。

KSC のインストール時に管理対象デバイス数の設定を、「101-1,000 台」以上とした場合、自動的に有効となります。

手動で間隔を設定する場合はこのチェックを外し、「タスクを次の時間内にランダムに実行する」にチェックを入れ、時間範囲(分)を入力します。

kaspersky

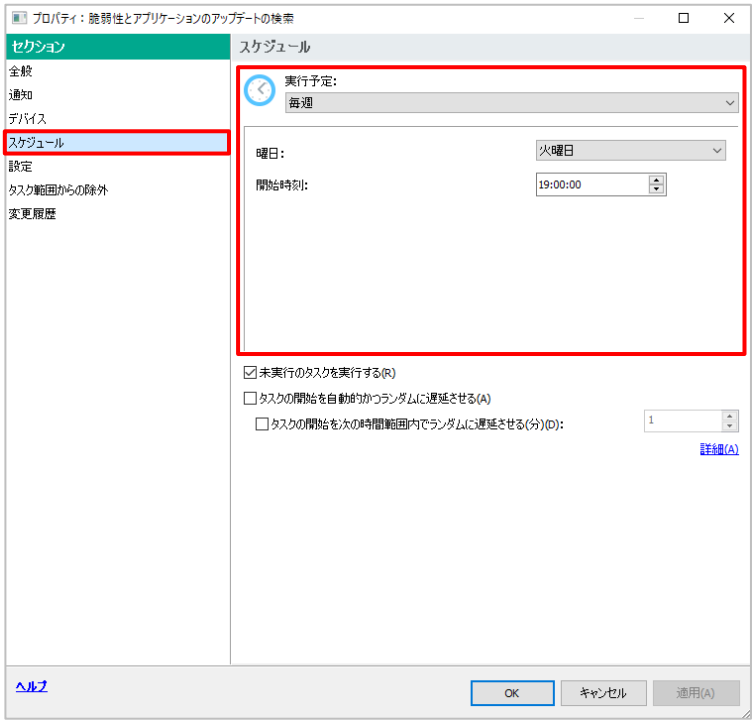
・「脆弱性とアプリケーションのアップデートの検索」タスクの確認

(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。

「脆弱性とアプリケーションのアップデートの検索」タスクを右クリックし、「プロパティ」を開きます。

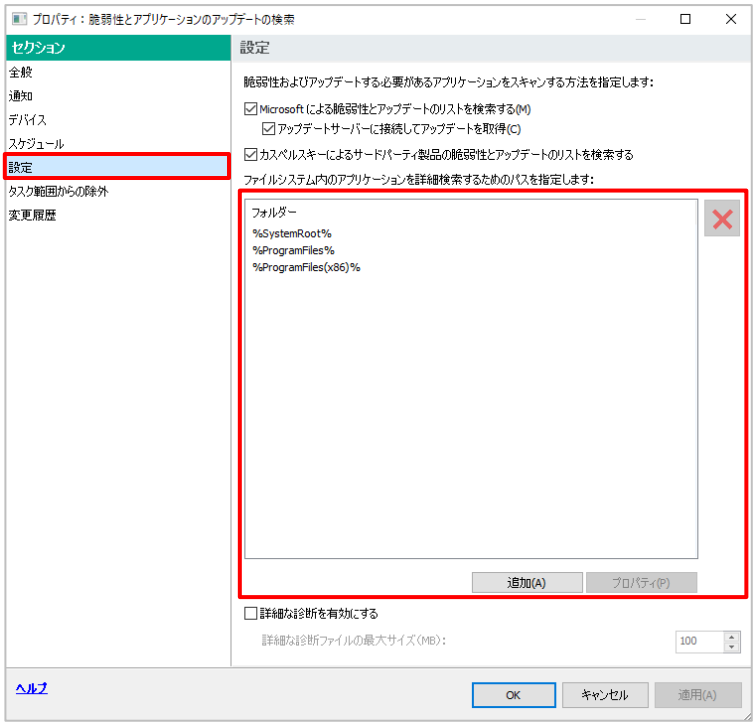
(2) 「スケジュール」セクションを開きます。

既定では、**毎週火曜日 19:00** に開始するようスケジュールされております。
運用に合わせ、設定を変更してください。



(3) 「設定」セクションを開きます。
アプリケーションを検索するためのパスを指定する場所があります。

右画面の「フォルダー」以外のパスにアプリケーションがインストールされている場合、「追加」ボタンにてパスを追加することができます。



本節は以上です。

3.4. 「管理サーバーデータのバックアップ」タスクについて

KSC をインストールし、「管理サーバークイックスタートウィザード」を実行すると、**「管理サーバーデータのバックアップ」**タスクが作成されます。

このタスクを実行すると、管理サーバーに関する主要な設定とオブジェクト情報がバックアップされます。

- **管理サーバーの情報データベース（管理サーバーに保存されているポリシー、タスク、アプリケーション設定、イベント）**
- **管理グループとクライアントデバイスの構造についての設定情報**
- **リモートインストール用アプリケーション配信パッケージのリポジトリ**
- **管理サーバー証明書**
- **ライセンス情報**

バックアップデータは、KSC の移行や障害復旧時に使用することができます。

このタスクは、既定で 2 日毎に 4:00 に実行するよう、スケジュールされております。

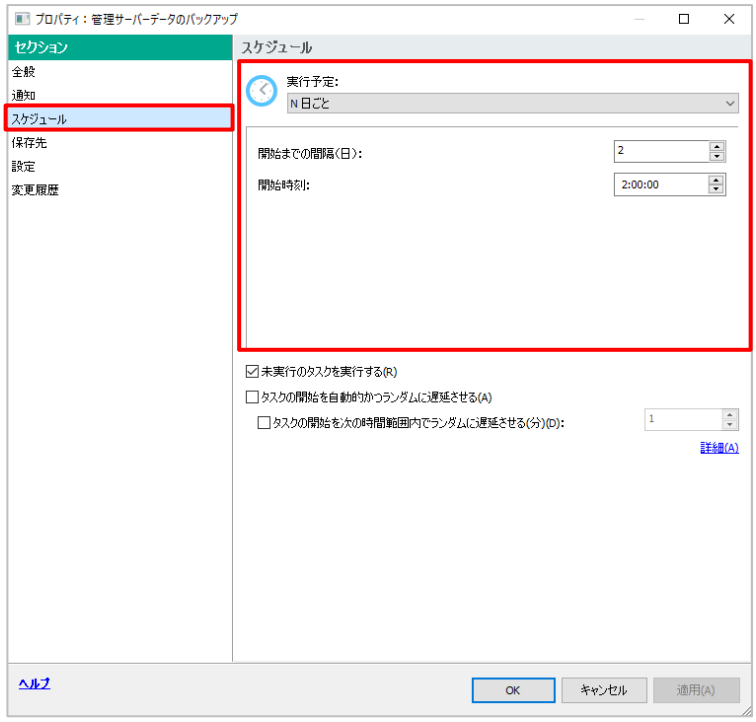
・「管理サーバーデータのバックアップ」タスクの確認

(1) 「タスク」を開きます。

「管理サーバーデータのバックアップ」タスクを右クリックし、「プロパティ」を開きます。

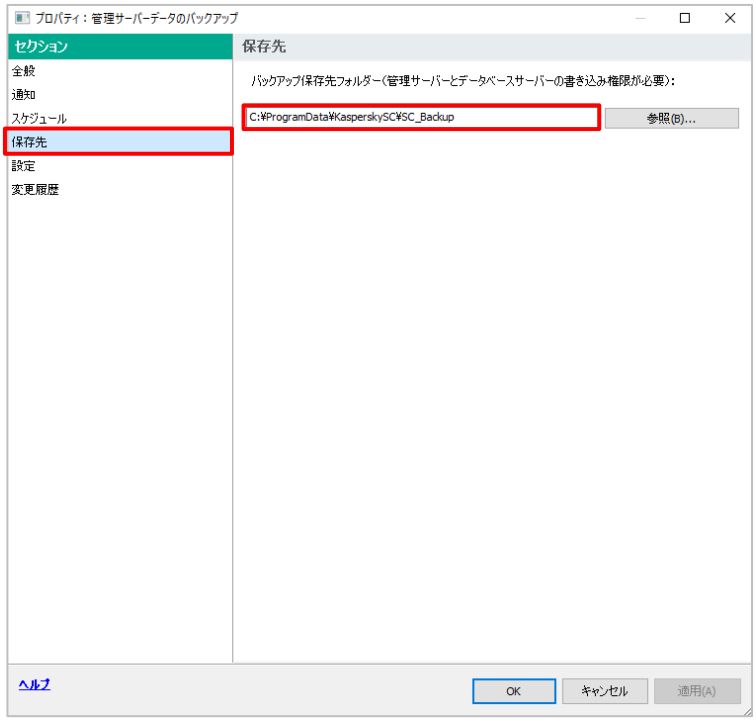
(2)「スケジュール」セクションを開きます。

既定では、**2日間隔で2:00**に開始するようスケジュールされております。
運用に合わせ、設定を変更してください。



(3)「保存先」セクションを開きます。

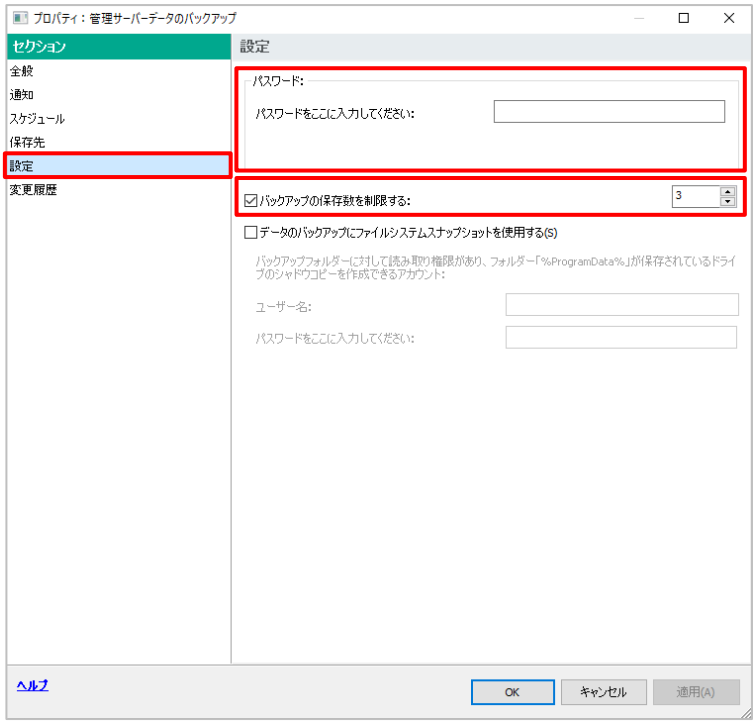
既定では、以下のパスに保存するよう設定されております。
C:¥ProgramData¥KasperskySC¥SC_Backup



(4)「設定」セクションを開きます。

バックアップに指定するパスワードを設定することができます。

また、保存する数は既定で 3 世代と設定されており、上限に達すると古いものから削除されます。
運用に合わせ、設定を変更してください。



本章は以上です。

4.　管理対象デバイスのステータス、情報の確認

本章では、管理下にあるデバイスのステータスや、KSC が収集した情報の確認方法についてご説明します。

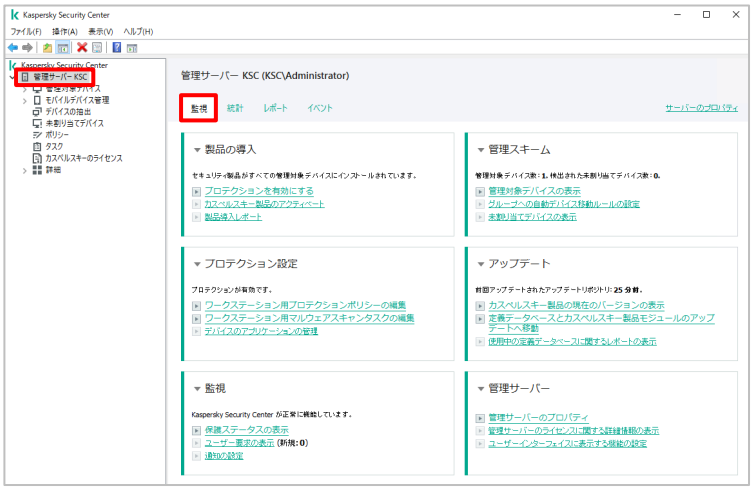
4.1.　監視機能

KSC によって管理されているアプリケーションやデバイスのステータスに関する情報は、「監視」にて確認することができます。

脆弱性に関するメッセージや検知されたウイルス情報など重要な情報は、管理者が分かりやすいよう強調表示されます。

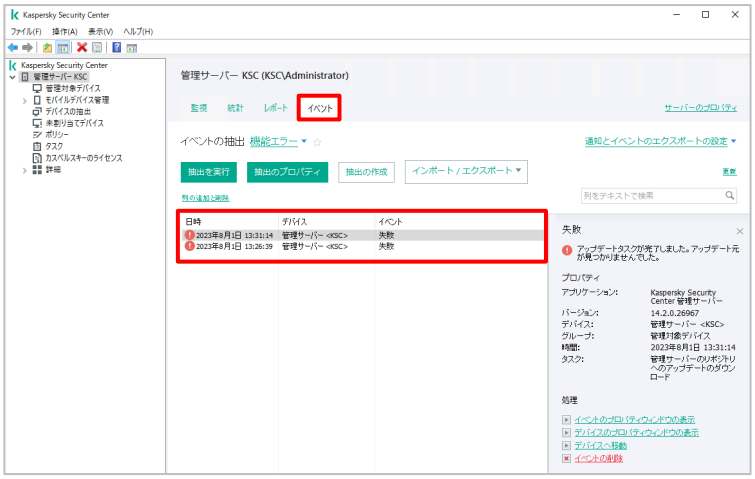
メッセージやリンクをクリックすることで、KSC コンソールの他フォルダーに移動することができます。

(1) 監視を確認するには、「管理サーバー」をクリックし、「監視」タブを開きます。



(2) 例として、「監視」内にある「エラーが管理サーバーのイベントに登録されました。」をクリックします。

(3) 自動的に「イベント」タブが開き、「緊急イベント」の一覧を確認することができます。



本節は以上です。

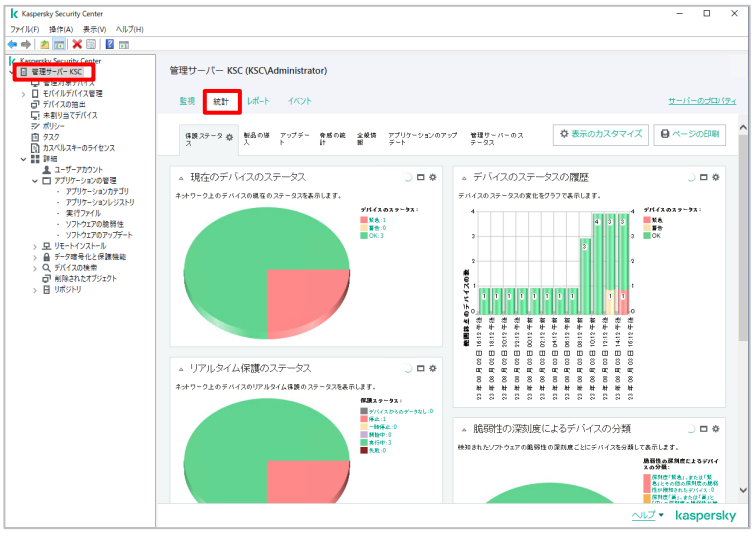
4.2. 統計機能

KSC にて収集されている情報（保護ステータス、アンチウイルス統計など）を図表化されたものを「統計」にて確認することができます。

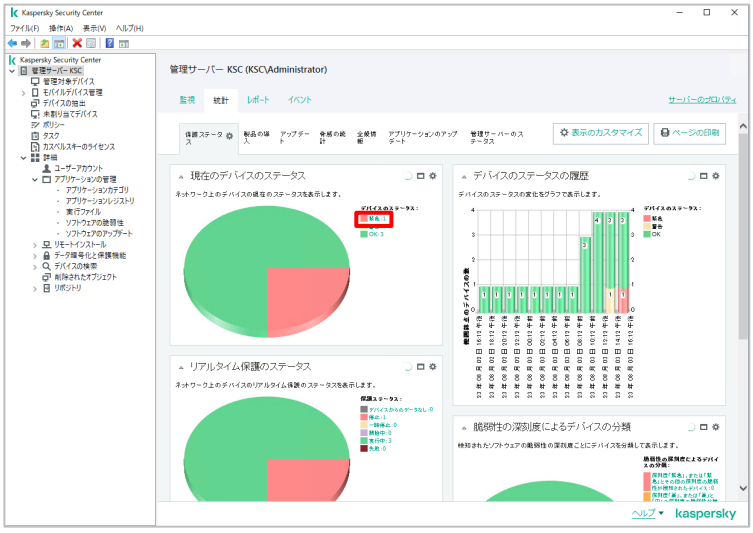
ステータスをクリックすると、該当するデバイス情報を確認することができます。

(1) 監視を確認するには、「管理サーバー」をクリックし、「統計」タブを開きます。

配下に「保護ステータス」「導入」「アップデート」などのタブがあり、図表化した情報を確認することができます。

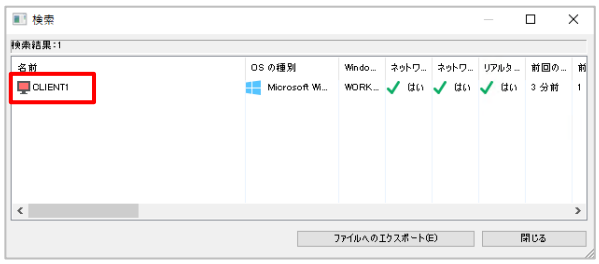


(2) 例として、「現在のデバイスのステータス」情報内にある「緊急」ステータスをクリックします。



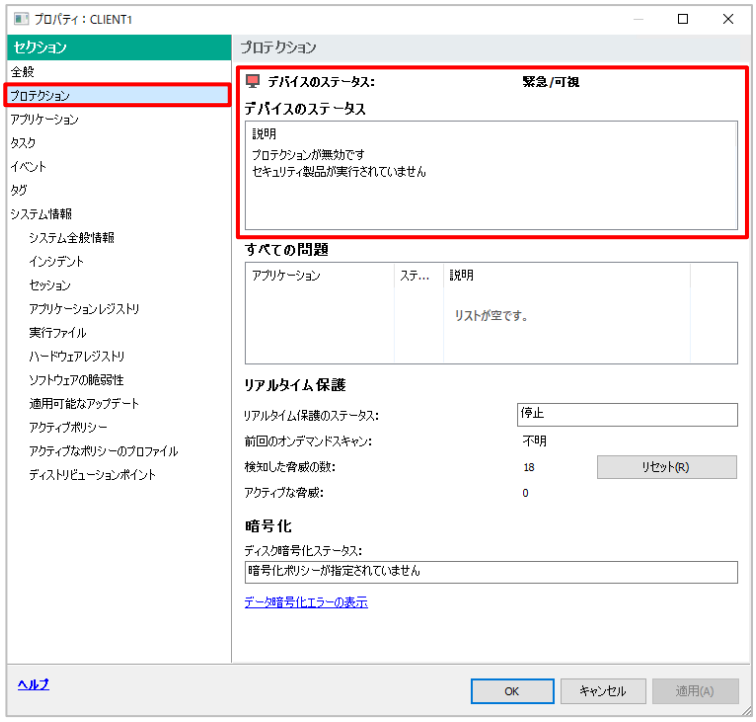
(3) 「緊急」に該当するデバイスの一覧が表示されます。

デバイスの詳細を確認するには、対象のデバイスをダブルクリックします。



(4) デバイスのプロパティが表示されます。

「プロテクション」セクションを開くと、「緊急」ステータスの理由が確認できます。



本節は以上です。

4.3. レポート機能

4.3.1. レポートの確認

KSC では、管理下にあるデバイスのステータスやウイルス検知、デバイス情報などをレポートとして出力することができます。レポートは、管理サーバーに保存されている最新の情報を元に生成されます。

例えば、以下のようなレポートを生成することができます。

・**脅威レポート**： 検知したマルウェア、検知デバイス、日時、オブジェクト名など。
・**カスペルスキー製品バージョンレポート：**管理下のデバイスに導入されているカスペルスキー製品情報一覧
・**ハードウェアレジストリレポート：**デバイス毎のマザーボード、CPU、メモリ、ディスク容量など。
・**脆弱性レポート：**管理下のデバイスにおける OS、アプリケーションに存在する脆弱性の一覧。

上記以外にも、多くのレポートテンプレートが用意されております。
レポートのプロパティにて表示項目や抽出期間などカスタマイズすることができます。
また、テンプレートを元に新しいレポートを作成することも可能です。

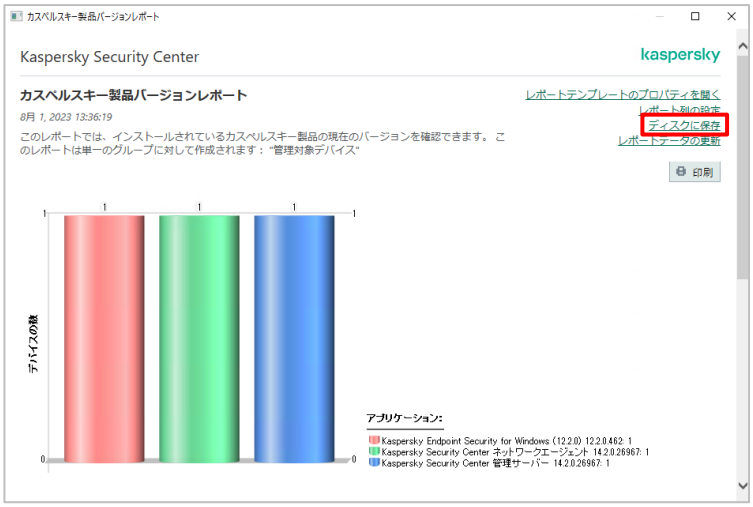
(1) レポートを確認するには、「管理サーバー」をクリックし、「レポート」タブを開きます。

(2) レポートを開く場合、レポートをダブルクリックします。

ここでは、例として「カスペルスキー製品バージョンレポート」を開きます。

(3) ブラウザーによる別のウィンドウが開き、レポートが表示されます。

「ディスクに保存」を選択することで、レポートを HTML、xls、pdf 形式で保存することができます。



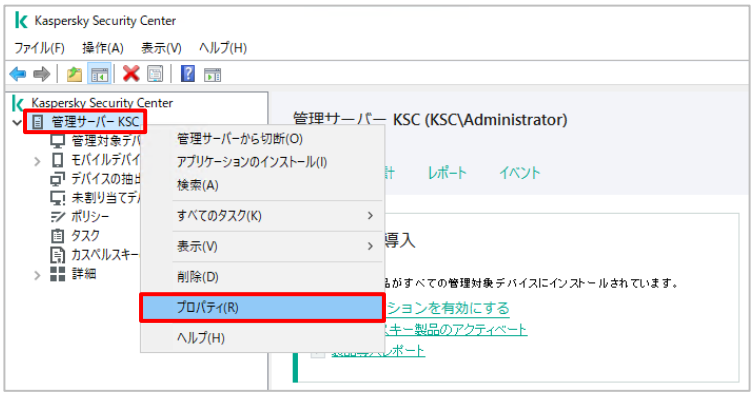
本項は以上です。

4.3.2. レポートの送信

KSC で生成するレポートは、スケジュールを設定しメール送信することができます。管理者は KSC へ接続することなく、受信したレポートを元にデバイスの状態を把握することができます。

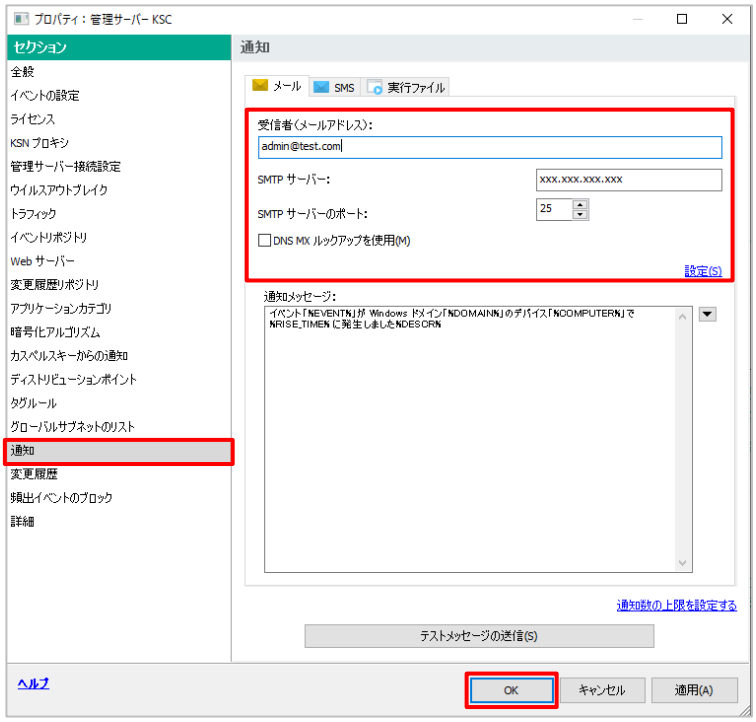
本手順では、管理者に対し、スケジュールを設定してレポートを送信するタスクを作成する手順についてご説明します。

(1) 「管理サーバー」を右クリックし、「プロパティ」を開きます。

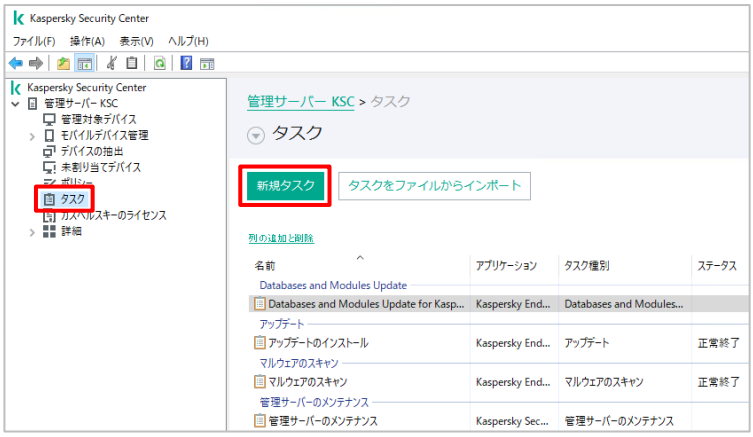


(2) 「通知」セクションを開きます。
宛先に送信先となるメールアドレス、SMTP サーバーアドレス、ポートを入力し、「OK」をクリックします。

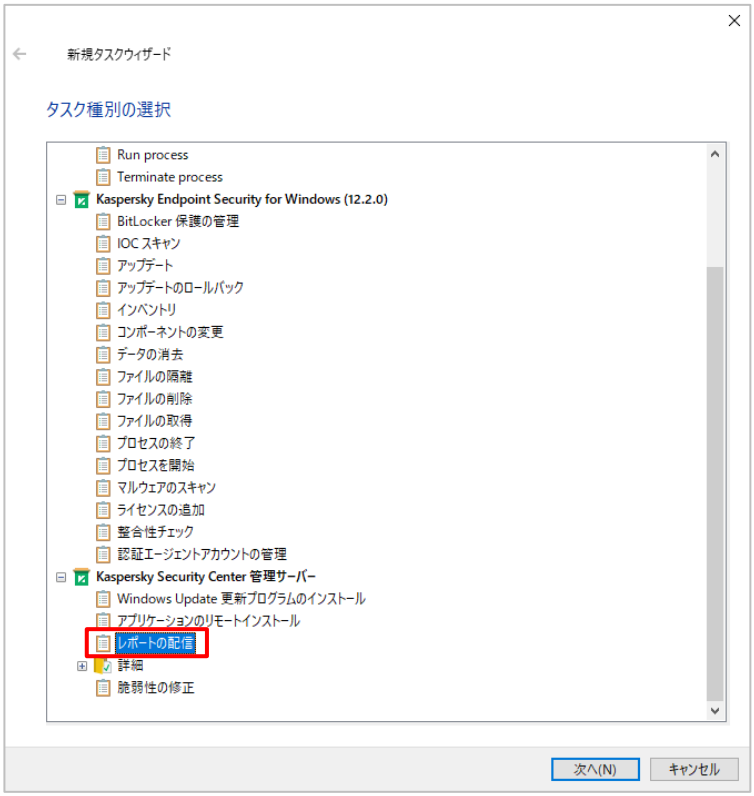
設定後、「OK」をクリックして保存します。



(3) 管理サーバーにて「タスク」を選択します。
右画面にて「新規タスク」をクリックします。



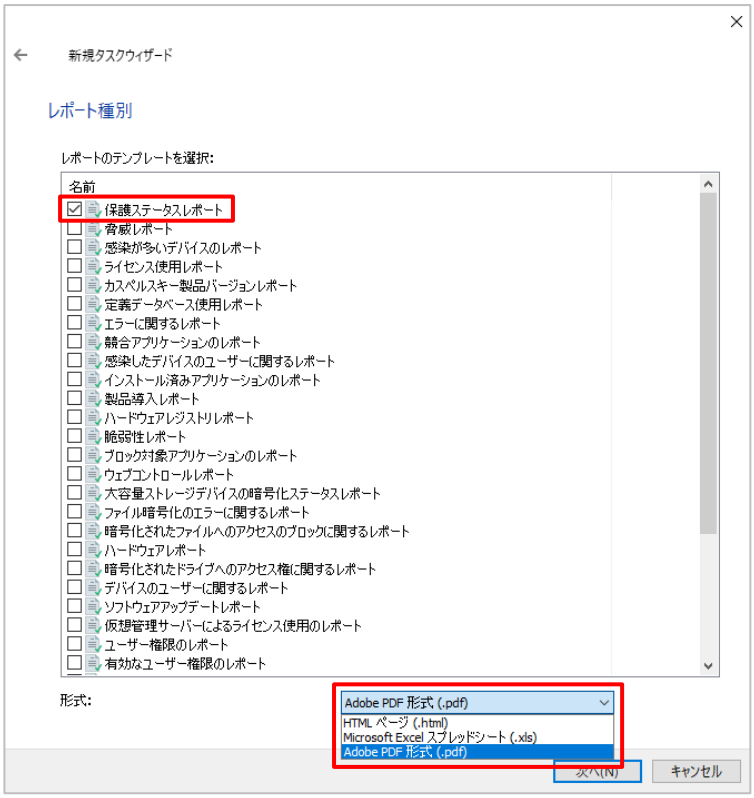
(4) 新規タスク作成ウィザードが表示されるので、「Kaspersky Security Center 管理サーバー」配下にある「レポートの配信」を選択し、ウィザードを進めます。



(5) 作成するレポートと添付形式を選択し、「次へ」をクリックします。

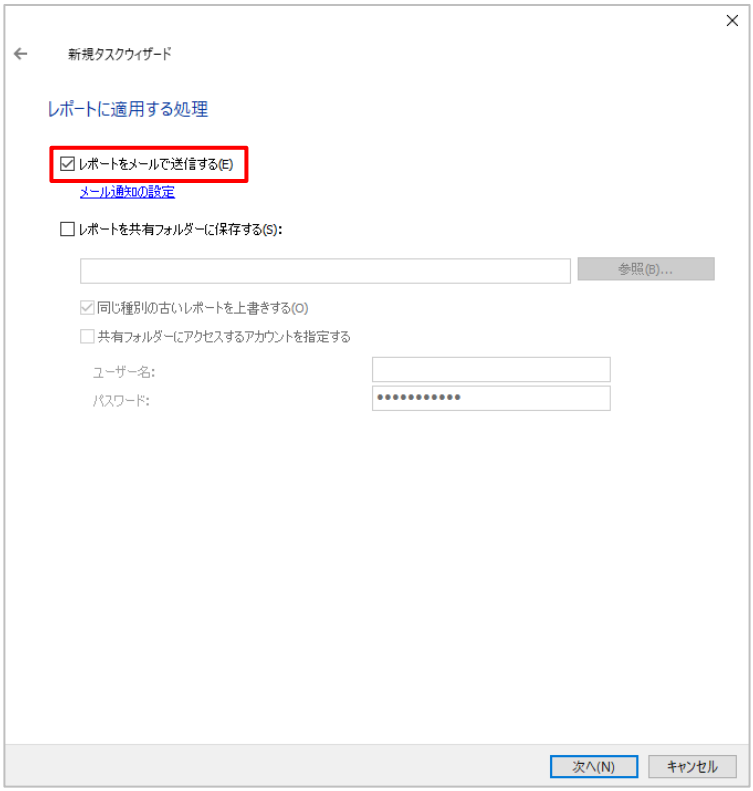
ここでは「保護ステータスレポート」を選択し、添付形式は pdf としています。

複数レポートを選択することができますが、1 メール 1 レポートとなります。

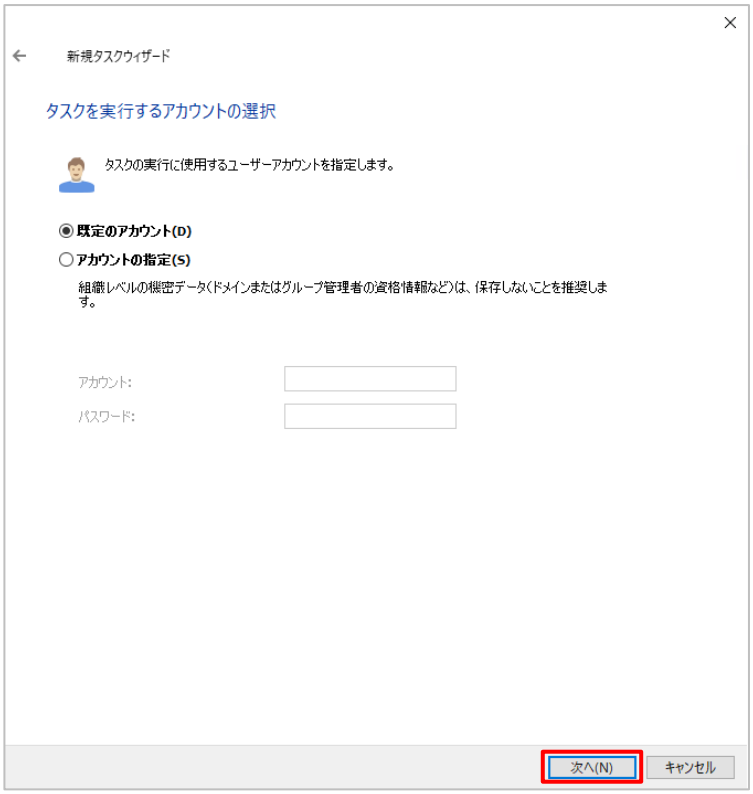


(6) メールで送信するため「レポートをメールで送信する」にチェックを入れ、「次へ」をクリックします。

個別に送信先を設定したい場合は「メール通知の設定」にて設定できます。

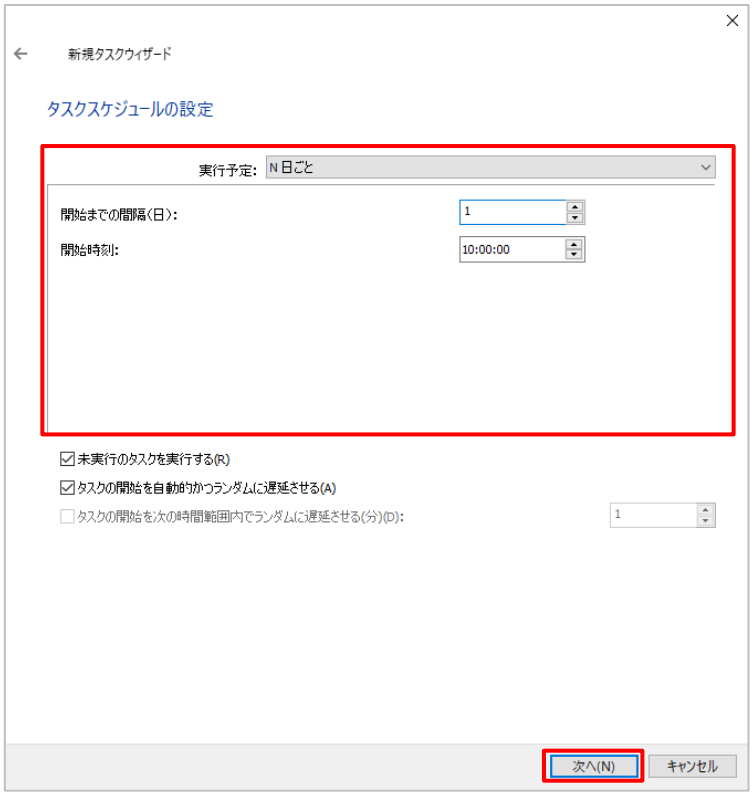


(7) 「タスクを実行するアカウントの選択」にて「次へ」をクリックします。

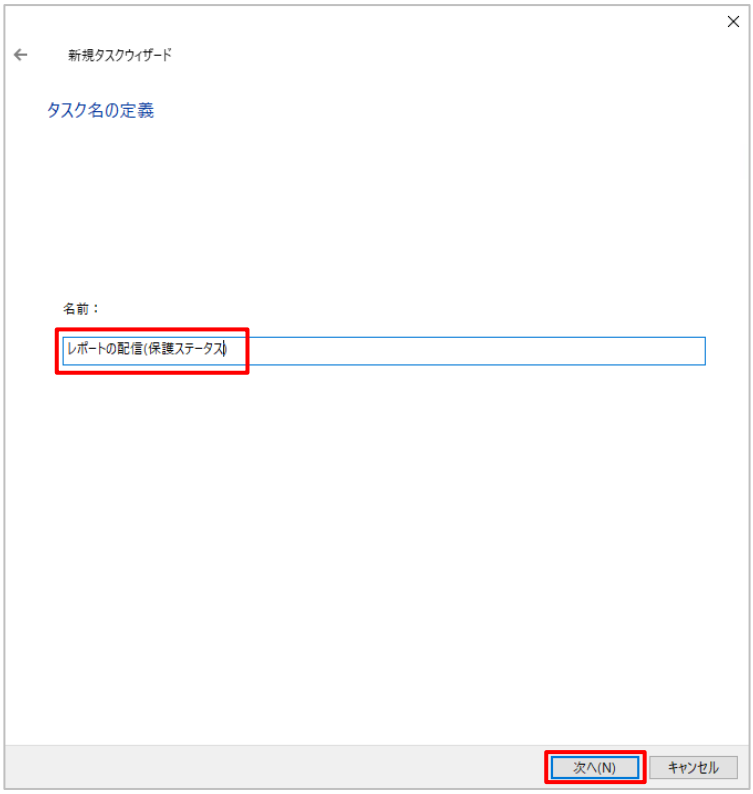


(8) タスクの実行スケジュールを設定し、「次へ」をクリックします。

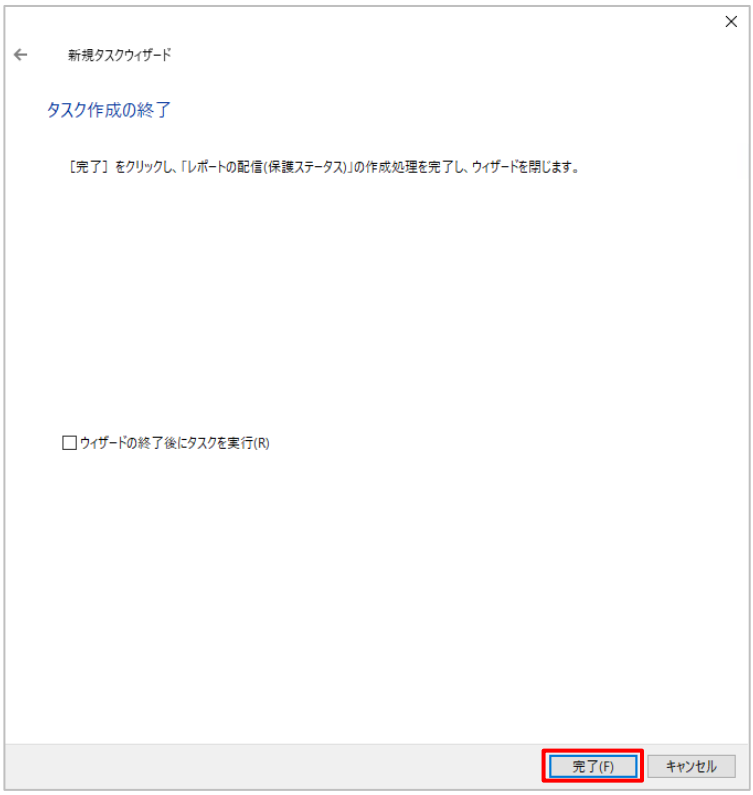
ここでは毎日 10:00 に実行されるよう設定しております。



(9) 任意のタスク名を設定し、「次へ」をクリックします。



(10) 正常に作成されたことを確認し「完了」をクリックします。



本節は以上です。
スケジュールに設定した時間に、最新のレポートが送信されます。

4.4. イベント機能

4.4.1. イベントの確認

KSC で発生したイベント、また管理下のデバイスにて発生したイベントは、KSC 上のデータベースに格納されます。イベントにはそれぞれ種別と重要度（緊急イベント、機能エラー、警告、情報）という属性があります。

・イベントの確認方法

(1) イベントを確認するには、「管理サーバー」をクリックし、「イベント」タブを開きます。

(2) イベントには抽出条件が予め定義されています。
「抽出イベント」の右側にあるリストボックスから抽出条件を選択すると、該当するイベントが出力されます。

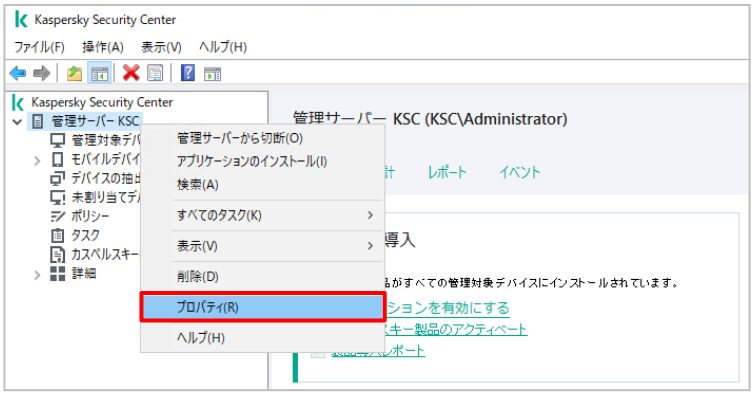
※
「抽出の作成」ボタンをクリックすることで、カスタマイズした抽出条件を作成することができます。

<抽出の作成>

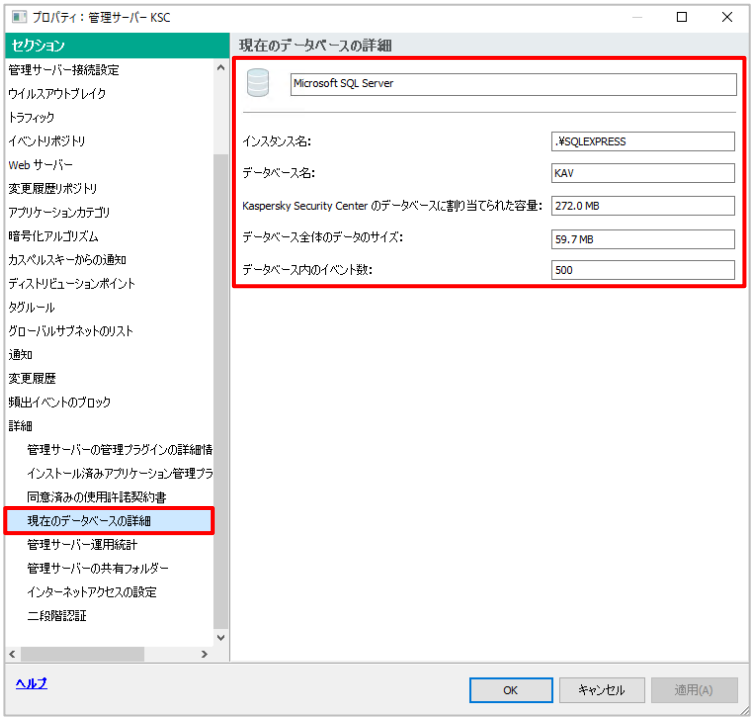
kaspersky

・保管されているイベント数、データベースサイズの確認

(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) 「詳細」-「現在のデータベース情報」セクションを開きます。
右側に、データベースに関する情報が表示されます。



・インスタンス
インスタンス名が表示されます。

・データベース名
データベース名が表示されます。

・データベースのサイズ
データベースのサイズが表示されます。
（トランザクションログ含む）

・データベース内のデータのサイズ
データベース内のデータサイズが表示されます。
（トランザクションログは含まない）

・データベース内のイベント数
データベース内に登録されているイベント数が表示されます。

本項は以上です。

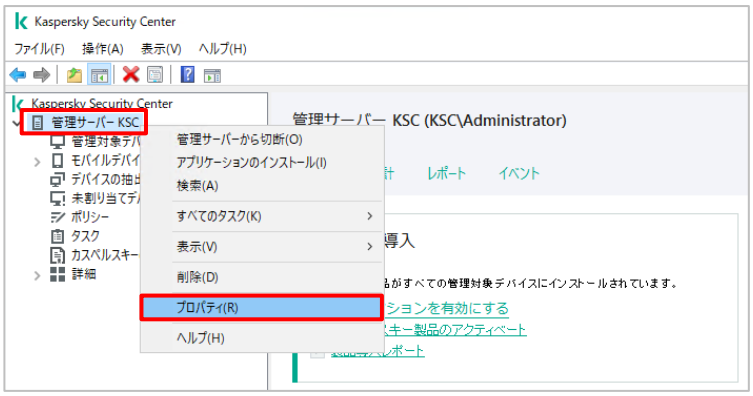
4.4.2. 保管イベントのローテーション

イベントには**「イベントの保管数」**と**「イベントの保管日数」**という 2 種類のしきい値があり、いずれかのしきい値に達したイベントは、古いものから順にデータベース上から削除されます。

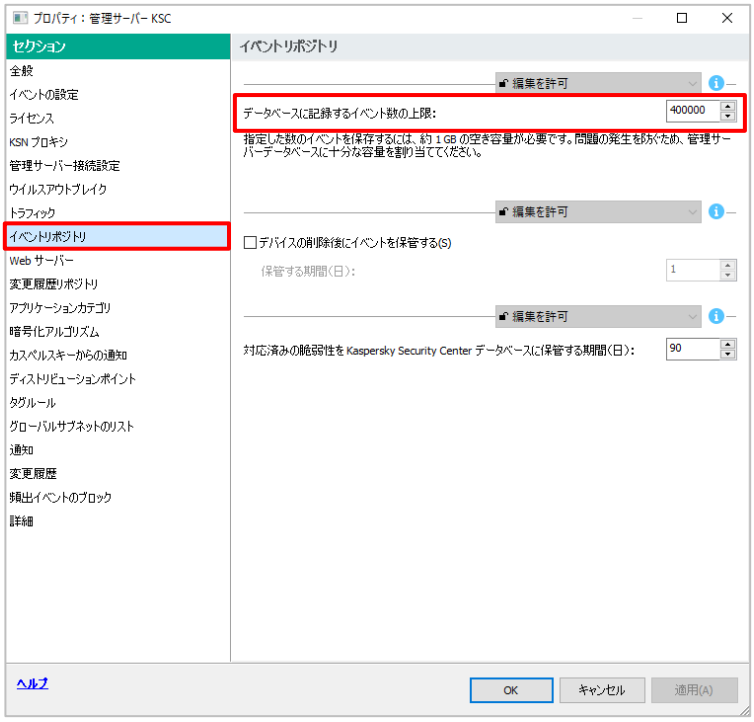
(1). イベント保管数

既定では、**400,000 件**が上限として設定されております。上限に達した場合は、古いイベントから順に削除されます。

(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) 「イベントの保管」セクションを開きます。「データベースに記録するイベント数の上限」に上限値が設定されております。設定可能な値は最大 **15,000,000 件**です。上限数を設定する場合は、データベースサイズやディスクサイズを考慮し、様子を見ながら徐々に設定してください。

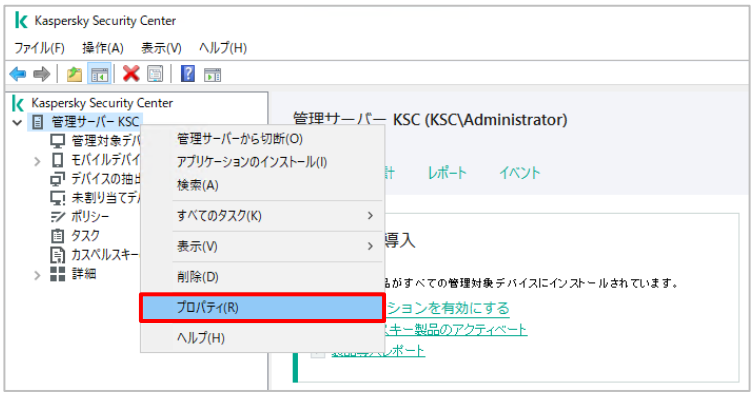


(2). イベント保管日数

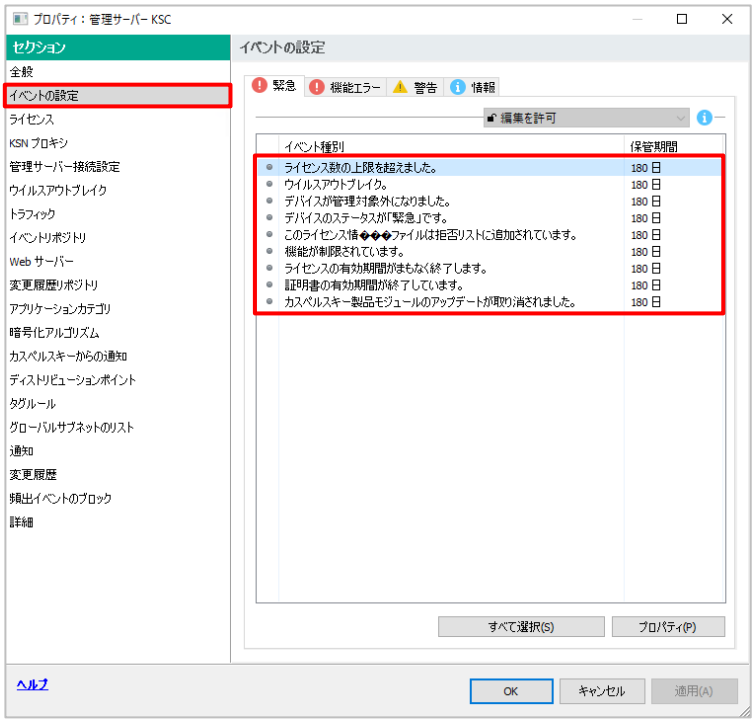
イベント毎に KSC 上に保存する日数が設定されております。これはイベント毎に異なり、保存日数が過ぎたイベントはデータベースから削除されます。

・KSC のイベント確認

(1) 「管理サーバー」を右クリックし、「プロパティ」を開きます。

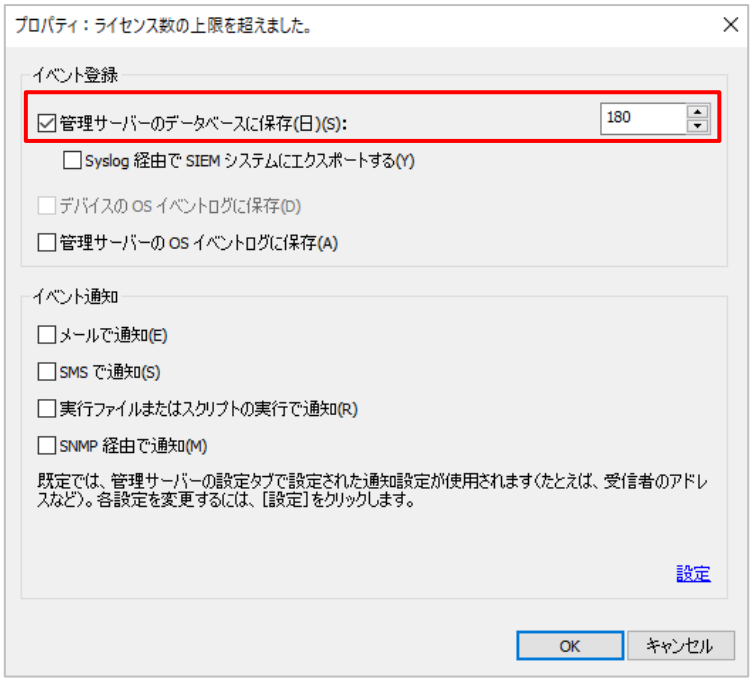


(2) 「イベントの設定」セクションを開きます。
各イベントに設定されている「保管期間」が、データベースに保管される日数となります。
設定を変更する場合はイベントをダブルクリックします。



(3) 「管理サーバー上に保存」にチェックがあることを確認し、保管期間を設定してください。

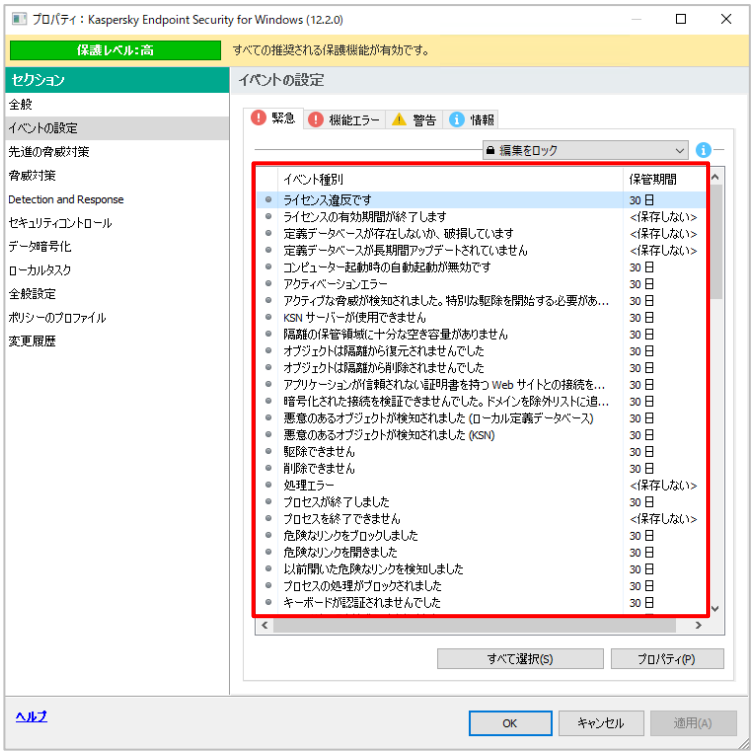
保管する必要が無いと判断したイベントは、このチェックを外すことでデータベースに保管されないようになります。



・KES のイベント確認

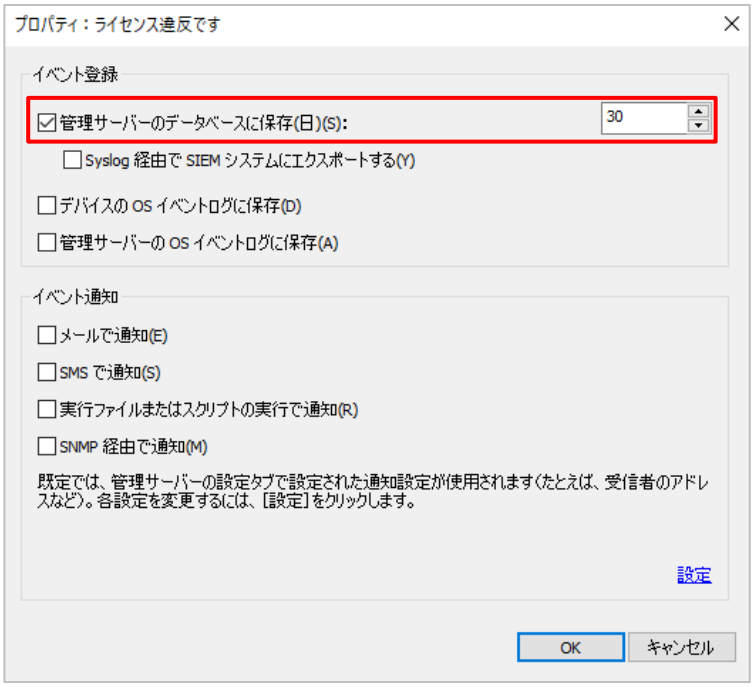
(1) 「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を開きます。

(2) 「イベント通知」セクションを開きます。
各イベントに設定されている「保管期間」が、データベースに保管される日数となります。
設定を変更する場合はイベントをダブルクリックします。



(3) 「管理サーバー上に保存」にチェックがあることを確認し、保管期間を設定してください。

保管する必要が無いと判断したイベントは、このチェックを外すことでデータベースに保管されないようになります。



本節は以上です。

4.5.　保護ステータスの確認

KSC では定期的に管理下にあるデバイス情報を収集しており、デバイスの状態をアイコンの色で表しています。

(1) KSC にて「管理対象デバイス」を開き、「デバイス」タブをクリックします。

デバイスの左にあるアイコンでステータスを表しております。

本節は以上です。

4.5.1. 保護ステータスの種類

保護ステータスのアイコンについてご説明します。
保護ステータスのアイコンは以下の種類があります。

(1) Windows ワークステーション OS、Linux OS におけるアイコン情報

	KSC で検出されたが、どこの管理グループにも所属していないデバイス
	管理グループに所属しており、ステータスが「OK」であるデバイス
	管理グループに所属しており、ステータスが「警告」であるデバイス
	管理グループに所属しており、ステータスが「緊急」であるデバイス
	管理グループに所属しており、KSC との接続が失われたデバイス

(2) Windows サーバーOS におけるアイコン情報

	KSC で検出されたが、どこの管理グループにも所属していないデバイス
	管理グループに所属しており、ステータスが「OK」であるデバイス
	管理グループに所属しており、ステータスが「警告」であるデバイス
	管理グループに所属しており、ステータスが「緊急」であるデバイス
	管理グループに所属しており、KSC との接続が失われたデバイス

(3) モバイルデバイスにおけるアイコン情報

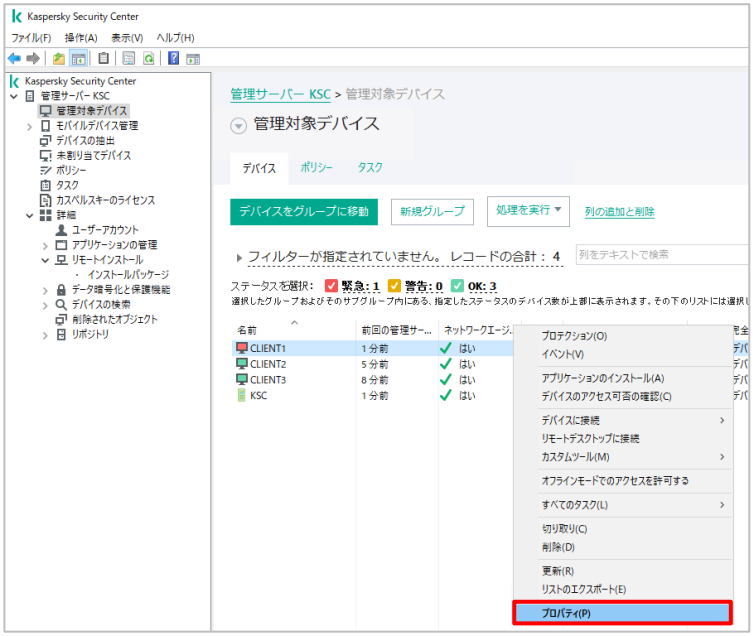
	KSC で検出されたが、どこの管理グループにも所属していないデバイス
	管理グループに所属しており、ステータスが「OK」であるデバイス
	管理グループに所属しており、ステータスが「警告」であるデバイス
	管理グループに所属しており、ステータスが「緊急」であるデバイス
	管理グループに所属しており、KSC との接続が失われたデバイス

本項は以上です。

4.5.2. ステータスの詳細確認

各デバイスのステータス詳細を確認する場合は、デバイスのプロパティを表示します。

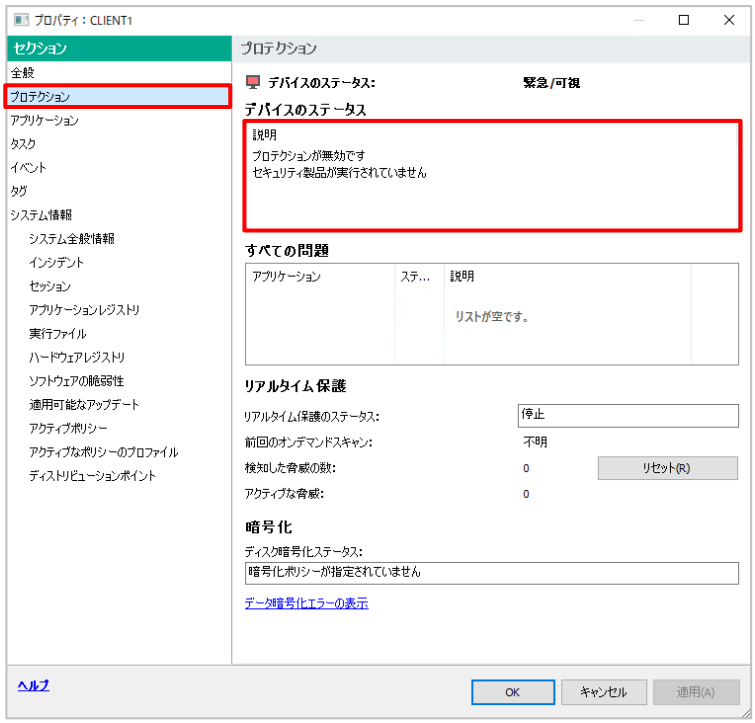
(1) 任意のデバイスを選択して右クリックし、「プロパティ」を選択します。



(2) 「プロテクション」を開きます。

「デバイスの状態」内に、警告、または緊急ステータスとなっている要因が記載されております。
各要因に対する対応を実施してください。

もしくは、「4.5.3. 保護ステータスの設定」を参考に、要因によるステータス変更がされないよう設定を実施してください。



本項は以上です。

4.5.3. 保護ステータスの設定

保護ステータスの設定はカスタマイズすることができます。
上位グループで設定した内容が下位グループへ継承されますが、グループ毎に設定することも可能です。
運用に合わせ、設定を変更してください。

【設定例】

・定期的なスキャンを実行しない場合 → 「長期間スキャンされていない」設定を無効化
・脆弱性の管理は行わない場合 → 「ソフトウェアの脆弱性が検知されました」設定を無効化
・定義データベースを 3 日更新しないと警告を出したい → ステータスのしきい値を変更

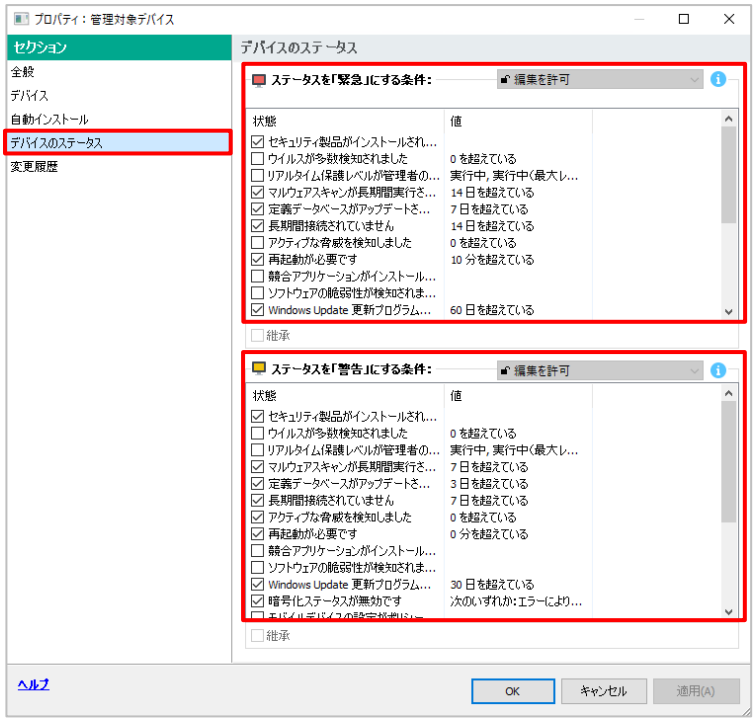
・ステータスの設定

(1) 「管理対象デバイス」を右クリックし、「プロパティ」を選択します。

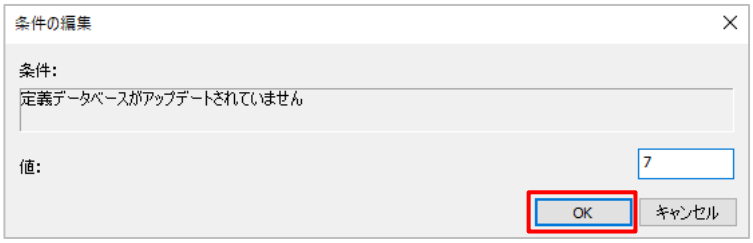
(2) 「デバイスのステータス」セクションを開きます。

右画面の上にステータスを「緊急」とする条件、下にステータスを「警告」とする条件が設定されております。
チェックのある項目が有効な条件となります。

条件の値を変更する場合は、条件をダウブルクリックします。



(3) 「条件の編集」画面が表示されます。
条件が変更される際の値を入力し、「OK」をクリックします。



本節は以上です。

4.6. KSC と管理対象デバイス間の接続（ネットワークエージェントの確認）

KSC と管理下にあるデバイスは、「Kaspersky Security Center 13 ネットワークエージェント（NA）」を介して通信を行っております。

KSC で設定したポリシー、タスクの反映、デバイスのステータス、イベント通知など、すべての情報はネットワークエージェントを介して行われます。

ネットワークエージェントは既定で 15 分に 1 回、KSC に対して同期を行います。この間隔はポリシーにて変更できます。（**「4.6.2. ネットワークエージェント同期間隔の設定」**参照）

既定では、7 日以上 KSC と接続していないデバイスは**「長期間接続されていない」**デバイスとして**警告**ステータスとなり、14 日以上接続されていない場合は**緊急**ステータスになります。
このしきい値は変更することができます。（**「4.5.3 保護ステータスの設定」**参照）

なお、デバイス側でウイルス検知など重要なイベントが発生した場合は、この同期間隔に関係なく、即時に KSC へイベントが通知されます。

ネットワークエージェントの導入、展開方法については、以下サイトにある**「簡単インストールガイド」**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/）

4.6.1. KSC 上で管理対象デバイスの接続状態を確認する

KSC 上で管理下にあるデバイスの接続状態を確認することができます。

(1) 「管理対象デバイス」を開き、右画面にてデバイス」タブを開きます。

(2) 以下の列に、ネットワークエージェントを介した接続状態を確認することができます。

・前回の管理サーバーへの接続

前回の同期からどのくらい時間が経過しているか表示されます。

・ネットワークエージェントインストールがインストール済み

ネットワークエージェントがインストール済みかどうか表示されます。

・リアルタイム保護のステータス

デバイスにカスペルスキーによる保護アプリケーションがインストールされているかどうか表示されます。

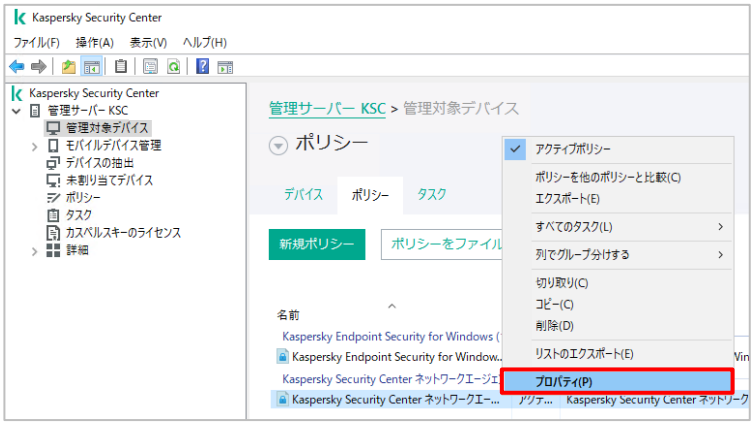
この表示項目は、「列の追加と削除」にてカスタマイズすることができます。

本項は以上です。

4.6.2. ネットワークエージェント同期間隔の設定

ネットワークエージェントによる同期間隔は、ポリシーにて変更することができます。

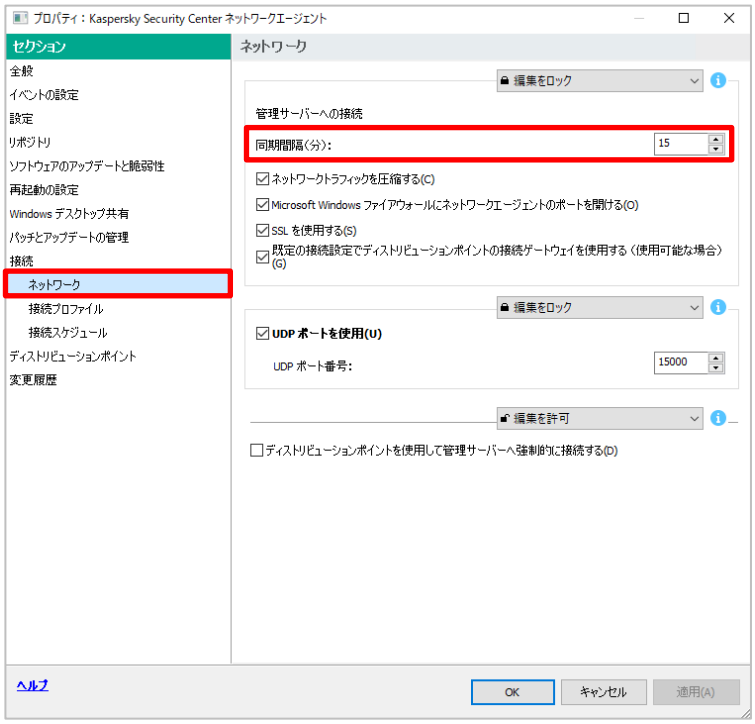
(1) 「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
NA のポリシーを右クリックし、「プロパティ」を開きます。



(2) 「ネットワーク」-「ネットワーク」セクションを開きます。

右画面にて「同期間隔」を確認します。
既定で **15 分**が設定されております。

管理下のデバイス数により、NA の同期が原因で KSC のパフォーマンスに影響を及ぼす可能性があります。
その場合は、この同期間隔を変更して事象が改善されるかどうかご確認ください。



本項は以上です。

4.6.3. デバイスから KSC への接続状態を確認

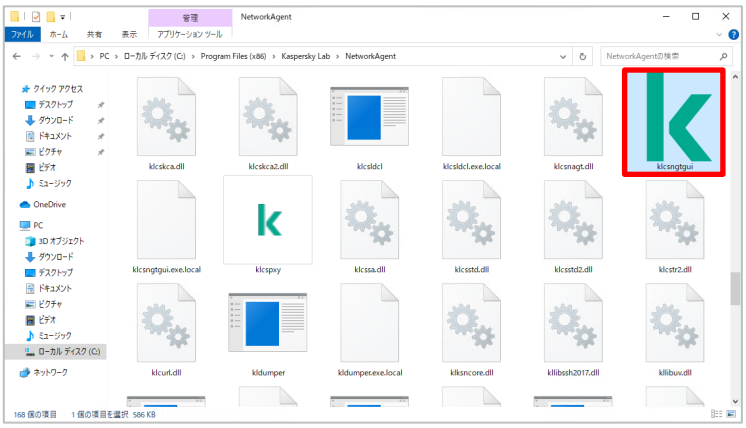
ネットワークエージェントでは、KSC との接続状態を確認するためのツールがあります。
デバイスにネットワークエージェントをインストール後、KSC との疎通を確認する際に使用してください。

※ **このツールは、デバイスの管理者権限が必要となります。**

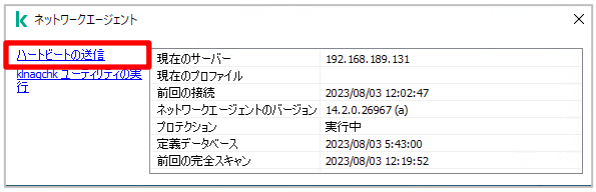
(1) エクスプローラーを起動し、ネットワークエージェントのインストールパスへ移動します。
既定では以下パスになります。

・32bit
C:¥Program Files¥Kaspersky Lab¥NetworkAgent
・64bit
C:¥Program Files (x86)¥Kaspersky Lab¥NetworkAgent

(2) 「klcsngtgui.exe」を起動します。

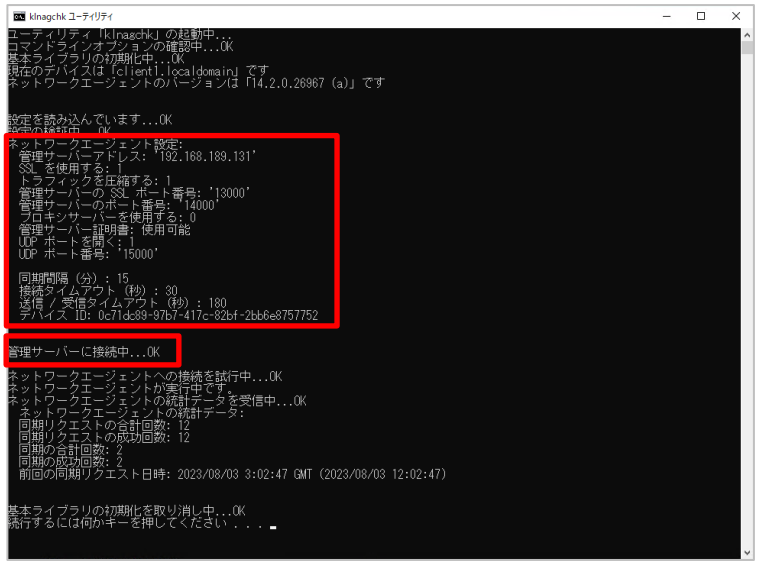


(3) 「ネットワークエージェント」のツールが起動します。
「ハートビートの送信」をクリックすると、KSC に対する同期の通信を手動で実行することができます。



(4) 接続状態を確認するためには、
「klnagchk ユーティリティの実行」をクリックします。

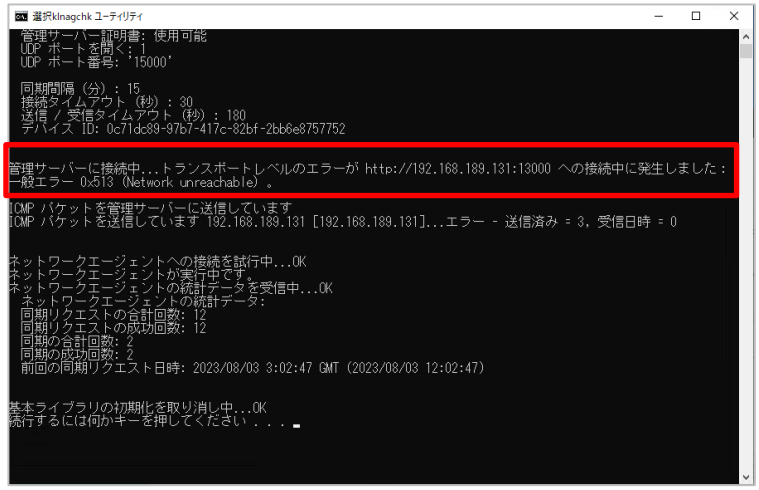
(5) コマンドプロンプトが起動し、ネットワークエージェント設定情報や、KSC への接続状態を確認することができます。



「管理サーバーアドレス」では、ネットワークエージェントに設定されている KSC のアドレスが表示されます。
KSC と接続できない場合、この値に誤りがないかご確認ください。

管理サーバーに正常に接続できている場合は、「管理サーバーに接続中」が「OK」と表示されます。

(6) 管理サーバーとの接続に失敗する場合、「管理サーバーへ接続中」が何らかの理由により失敗します。



管理サーバーのアドレスに誤りがないか、ネットワークやファイアウォール等の設定に問題はないかどうかご確認ください。

本章は以上です。

デバイス上で管理サーバーの宛先を変更する手順は、**「9.4. ネットワークエージェントの管理サーバーアドレス変更」**をご参照ください。

5.　導入アプリケーション、脆弱性情報、アップデート情報の確認

本章では、KSC 上で確認できるデバイスの情報についてご説明します。

KSC ではアンチウイルスの管理の他、デバイスに導入されているアプリケーション、脆弱性、アップデートなどの情報を確認することができます。

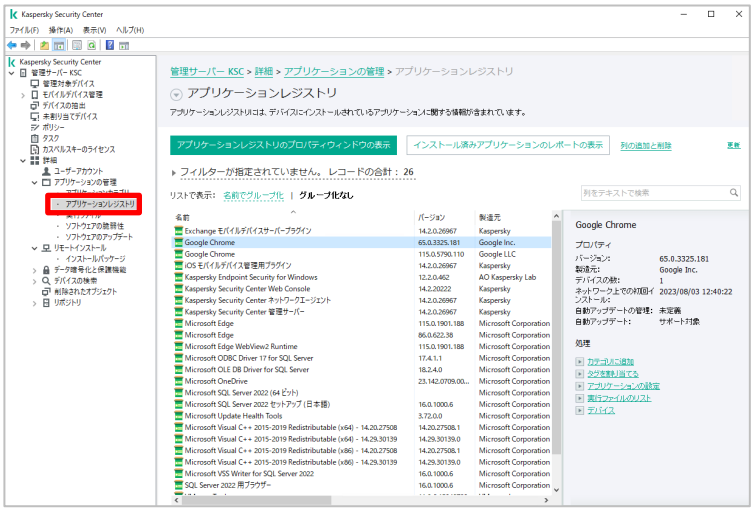
※デバイスに対し「脆弱性とアプリケーションのアップデートの検索」タスクが実行されている必要があります。

5.1.　導入アプリケーション情報の確認

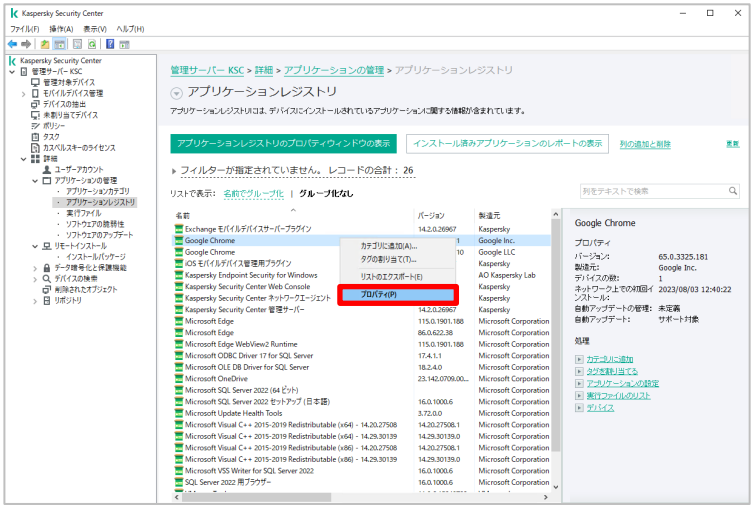
管理下にあるデバイス（Windows OS が対象）にインストールされているアプリケーション情報を収集し、一覧として表示することができます。

(1) 「詳細」-「アプリケーションの管理」-「アプリケーションレジストリ」を開きます。

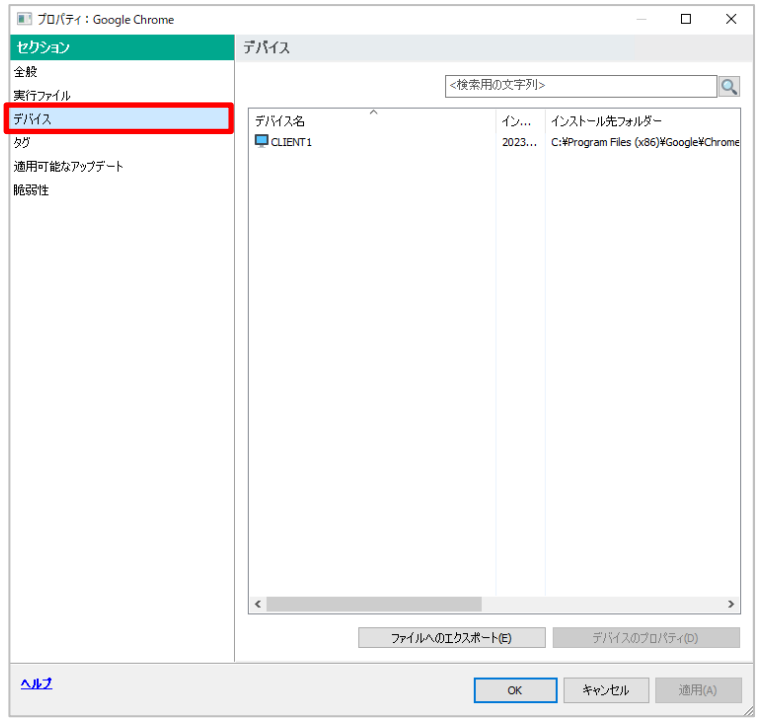
管理下のデバイスにインストールされているアプリケーションの情報を確認することができます。



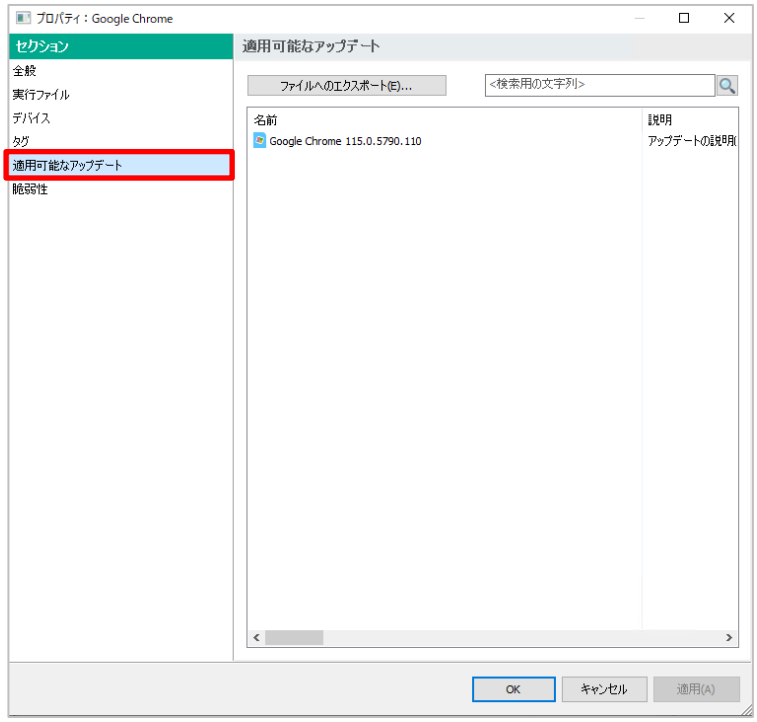
(2) 詳細を確認する場合は、アプリケーションを選択し、「プロパティ」を選択します。



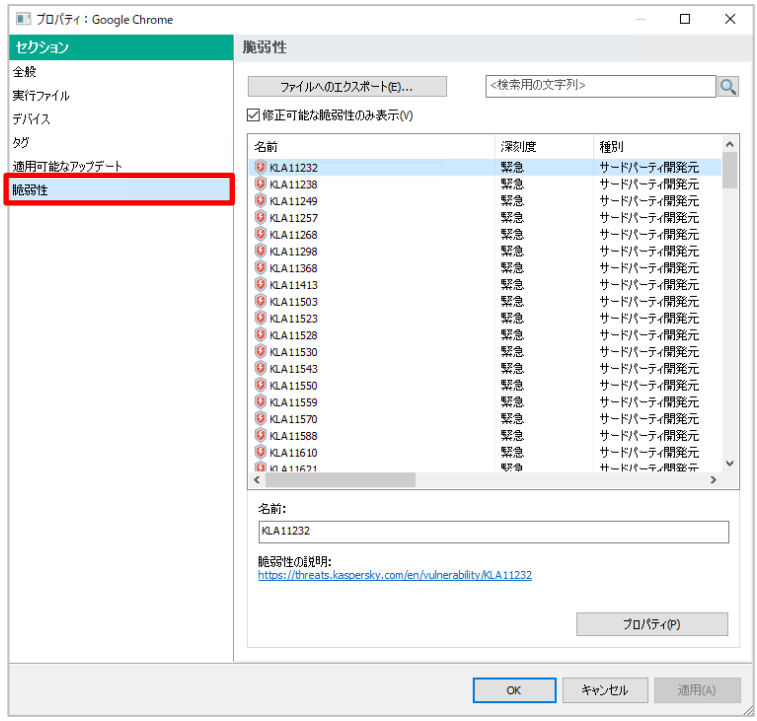
(3) 「デバイス」セクションでは、このアプリケーションがインストールされているデバイスを確認することができます。



(4) 「適用可能なアップデート」セクションでは、アプリケーションのアップデート情報を確認することができます。



(5)「脆弱性」セクションでは、このアプリケーションにおける脆弱性の情報を確認することができます。



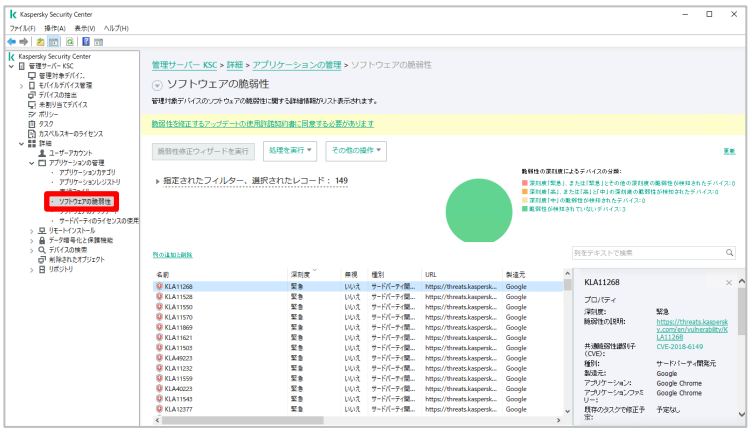
本節は以上です。

5.2.　ソフトウェア、OS に関する脆弱性情報の確認

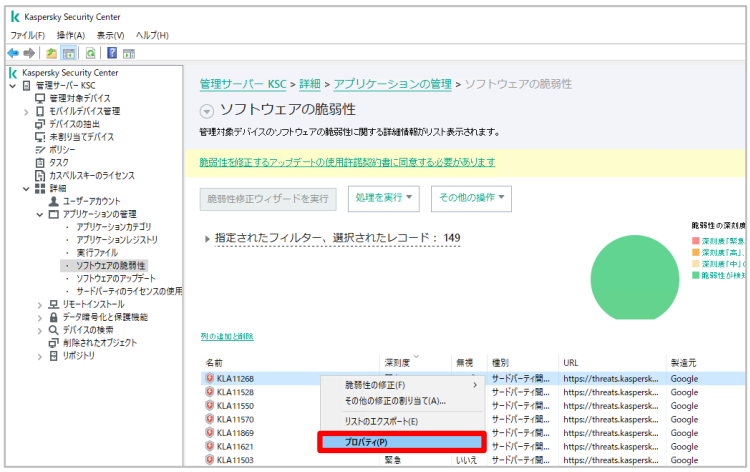
管理下にあるデバイス（Windows OS が対象）の OS、またサードパーティ製アプリケーションに関する脆弱性情報を確認することができます。

(1) 「詳細」-「アプリケーションの管理」-「ソフトウェアの脆弱性」を開きます。

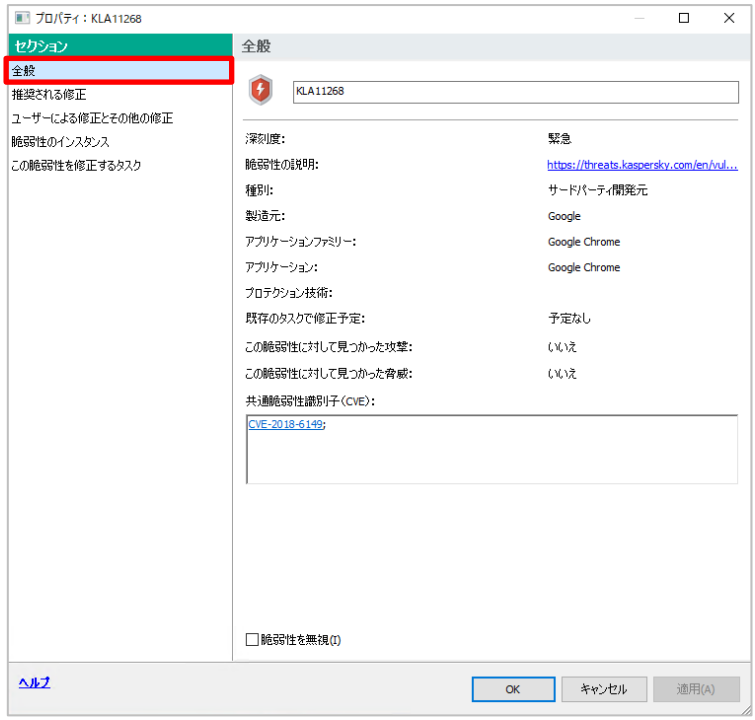
管理下のデバイスにインストールされている OS、アプリケーションの脆弱性情報を確認することができます。



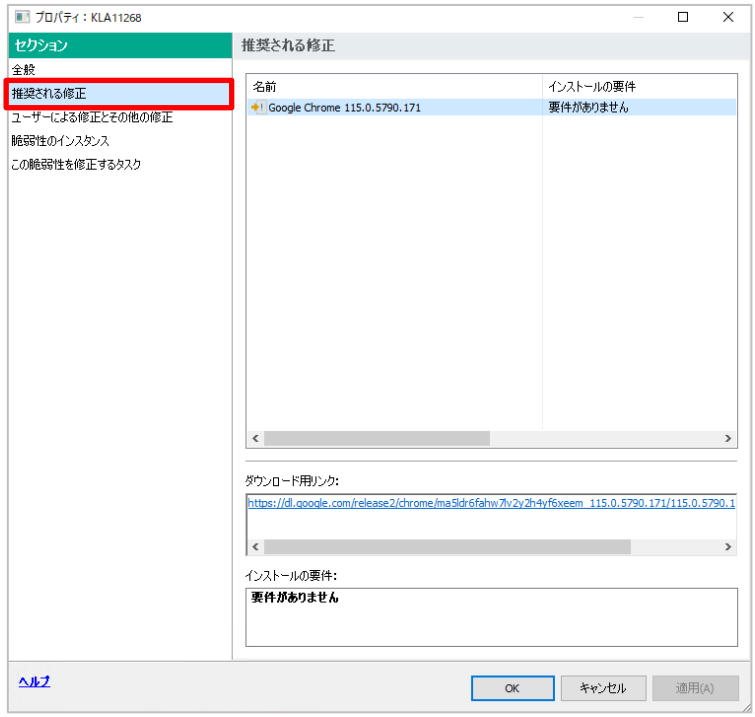
(2) 詳細を確認する場合は、項目を選択し、「プロパティ」を選択します。



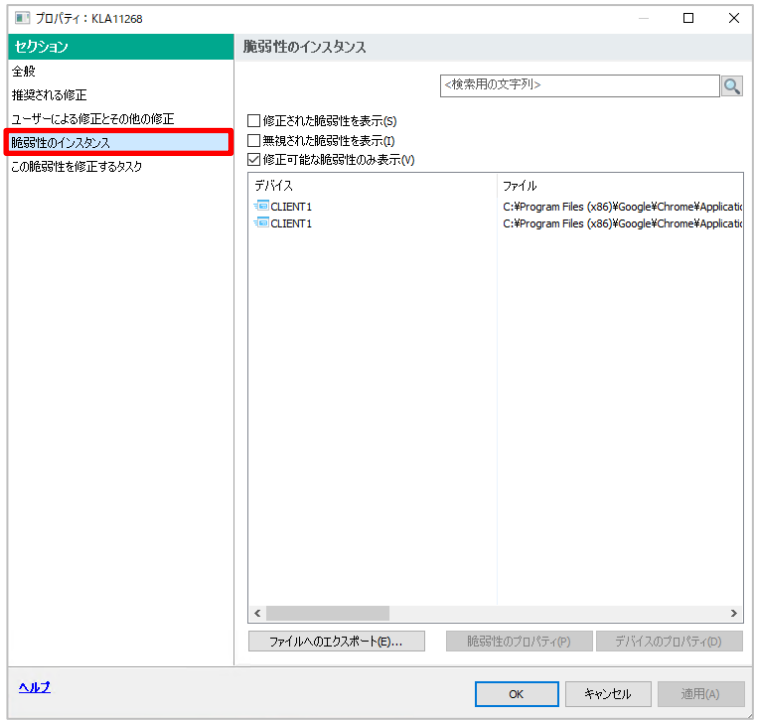
(3) 「全般」セクションでは、何のアプリケーションに関する脆弱性なのか、また、共通脆弱性識別子（CVE）を確認することができます。



(4) 「推奨される修正」セクションでは、その脆弱性を修正するためのパッチ、またはアップデート情報を確認することができます。



(5) 「脆弱性のインスタンス」セクションでは、脆弱性を保持するデバイスを確認することができます。



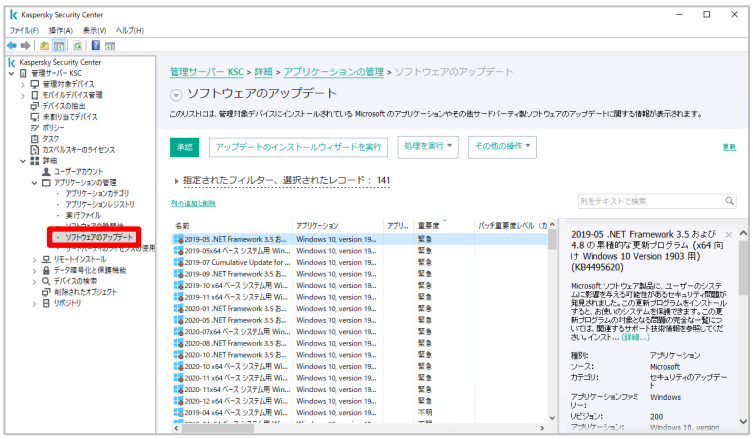
本節は以上です。

5.3. ソフトウェア、OS に関するアップデート情報の確認

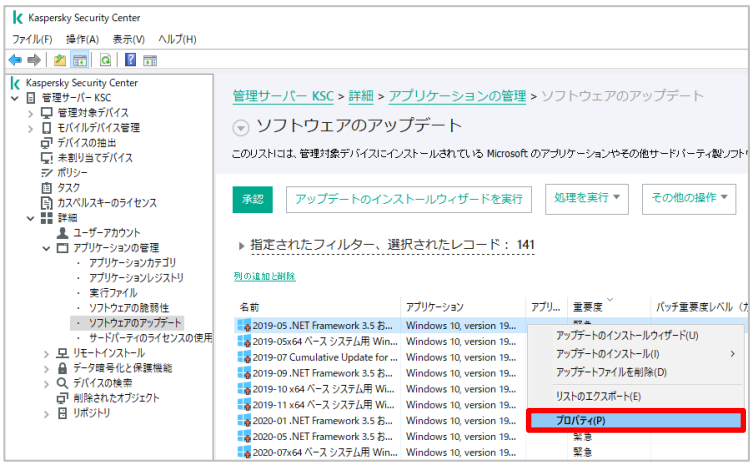
管理下にあるデバイス（Windows OS が対象）の OS、またサードパーティ製アプリケーションにおけるパッチ情報、またアップデート情報を確認することができます。

(1) 「詳細」-「アプリケーションの管理」-「ソフトウェアのアップデート」を開きます。

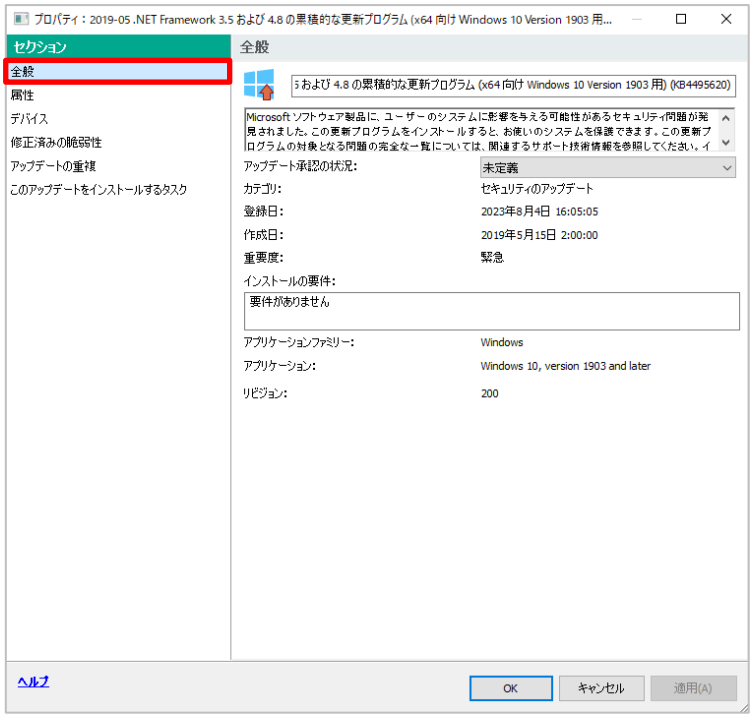
管理下のデバイスにインストールされている OS のパッチ、アプリケーションのアップデート情報を確認することができます。



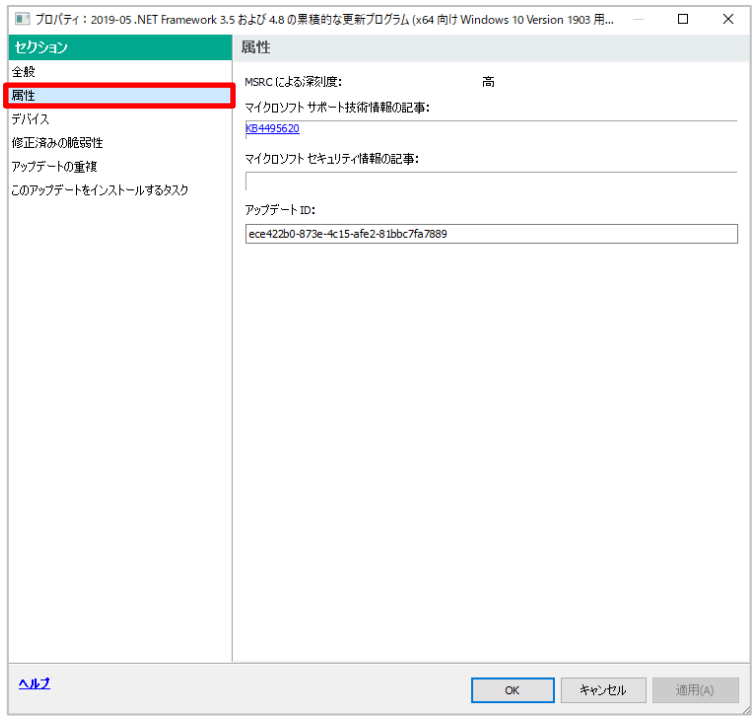
(2) 詳細を確認する場合は、項目を選択し、「プロパティ」を選択します。



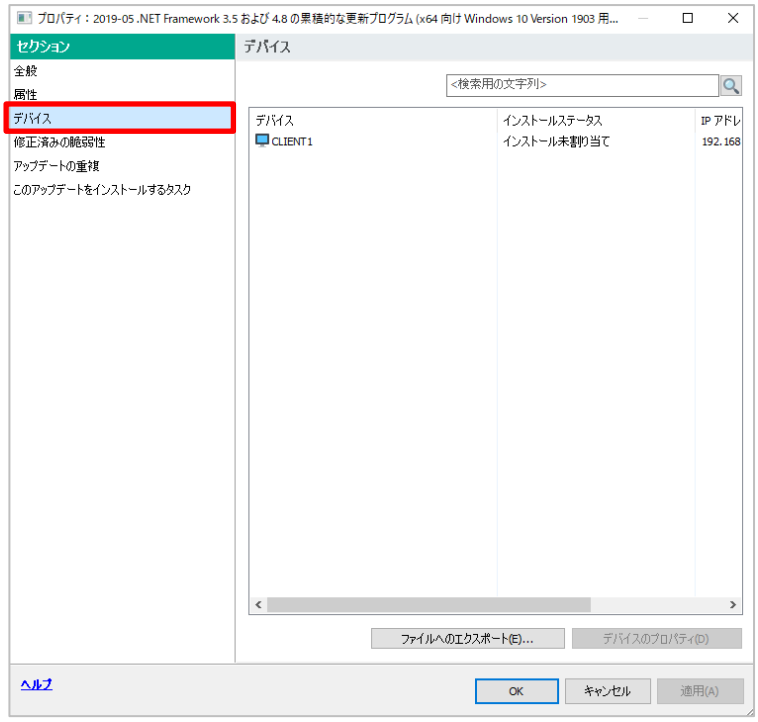
(3) 「全般」セクションでは、アップデートの製造元やバージョン情報などを確認することができます。



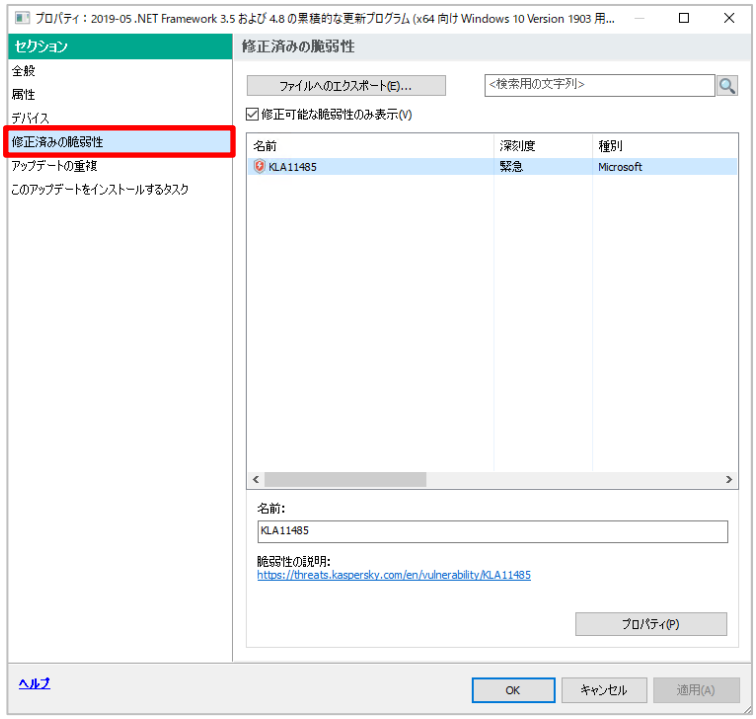
(4) 「属性」セクションでは、パッケージ情報やダウンロード元 URL、マイクロソフト製品であればサポート技術情報（KB 番号）などを確認することができます。



(5) 「デバイス」セクションでは、このアップデートが適用可能であるデバイス情報を確認することができます。



(6) 「修正済みの脆弱性」セクションでは、このアップデートを適用することで修正される脆弱性情報を確認することができます。



本章は以上です。

6. Kaspersky Lab ライセンスの確認

ライセンスは、「ライセンス情報ファイル」と「アクティベーションコード」の形式でご提供しております。
KSC にライセンスを登録することで、管理下のデバイスに適用するライセンスを一元管理することができます。

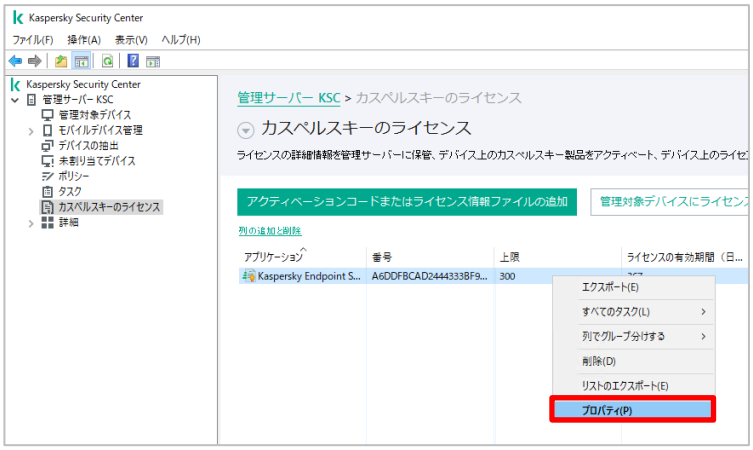
ライセンスの登録方法につきましては、ライセンスに同梱されている**「カスペルスキー製品ライセンス更新手順.pdf」**をご参照ください。

6.1. ライセンス情報の確認

登録されているライセンスのプロパティにて、有効期限や適用台数、適用されているデバイス等を確認することができます。

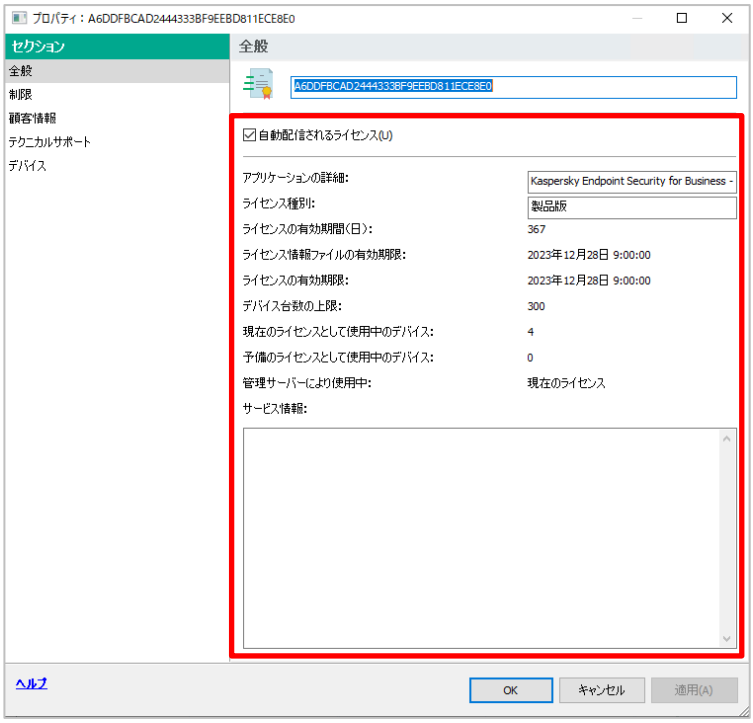
(1) 「詳細」-「アプリケーションの管理」-「Kaspersky Lab のライセンス」を開きます。

(2) ライセンスを右クリックし、「プロパティ」を選択します。



(3)「全般」セクションを開きます。

以下情報を確認することができます。



- **・自動配信されるライセンス**

  管理下のデバイスに対し、自動的にライセンスが登録されます。

- **・アプリケーションの詳細**

  ライセンスの名称を確認できます。

- **・ライセンス種別**

  ライセンスの種類を確認できます。

- **・ライセンスの有効期間(日)**

  有効期限までの残り日数が表示されます。

- **・ライセンス情報ファイルの有効期限**

  ライセンスの有効期限が表示されます。

- **・ライセンスの有効期限**

  ライセンスの有効期限が表示されます。

- **・上限**

  ライセンスが適用できる最大数が表示されます。

- **・現在のライセンスとして使用中のデバイス**

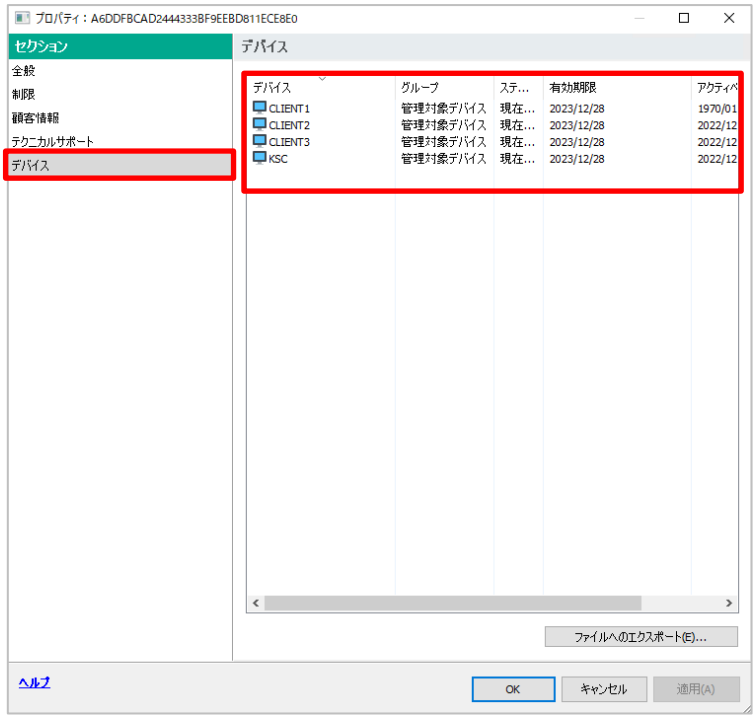
  現在ライセンスが適用されているデバイス数が表示されます。

- **・予備のライセンスとして使用中のライセンス**

  現在予備のライセンスとして登録されているデバイス数が表示されます。

(4) 「デバイス」セクションを開きます。

現在ライセンスが割り当てられているデバイスを確認することができます。



本節は以上です。

6.2.　デバイスの削除（ライセンスの解放）

KSC 上からデバイス情報の削除を実施することで、クライアントに適用されていたライセンス情報を解放することができます。

【こんなときに実施】

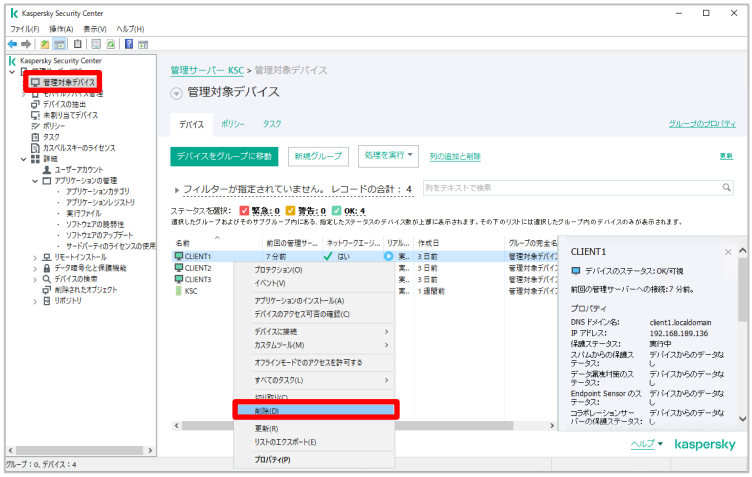
・クライアントデバイスが破損し、別の端末へ入れ替える必要が発生した。

・ライセンス不足が発生し、一時的に特定デバイスに付与されているライセンスを解放したい。

6.2.1. デバイスの手動削除

KSC からデバイスを手動で削除する場合、以下の手順を実施します。

(1) 「管理対象デバイス」を開き、削除対象のデバイスが存在するグループを開きます。「デバイス」タブにて該当デバイス名を右クリックし、「削除」を選択して削除を実行します。



(2) 「未割り当てデバイス」を開きます。“(1)”で削除を実施したクライアントが存在する場合は、ここでも指定して削除を実施します。

表示されていない場合、画面右にある**「更新」**をクリックして最新の表示状態にして確認してください。

「6.1. ライセンス情報の確認」の手順を実施し、デバイスの一覧に削除したデバイスが表示されていないこと、ライセンスの適用数が減少していることを確認してください。

本項は以上です。

6.2.2. デバイスの自動削除

KSC の管理下にあるデバイスは一定期間接続が無い場合、自動的にグループから削除され、ライセンスも解放されます。

そのため、長期間電源が入っていないデバイスや、外出等で KSC と長期間接続されていないデバイスは、自動的に KSC 上から削除されます。

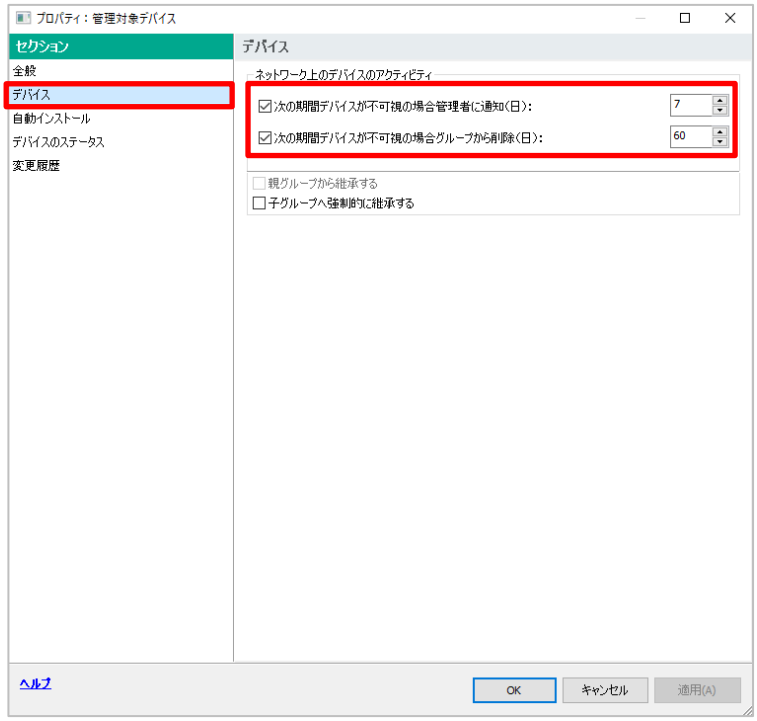
設定はグループのプロパティで確認ができます。

(1) 「管理対象デバイス」を右クリックし、「プロパティ」を選択します。

(2) 「管理対象デバイス」グループのプロパティを開き、「デバイス」セクションを開きます。

既定では、60 日接続が無いクライアントはグループ上から削除されます。

自動削除を実施したくない場合は「次の期間デバイスが不可視の場合グループから削除」のチェックを外してください。



本章は以上です。

7. ウイルス検知時の処理、対応

7.1. マルウェア検知時の処理について

管理下のデバイスにおいて、スキャンやアンチウイルス機能にてマルウェアが検知された際、オブジェクトに対し自動的に処理が行われ、処理内容により以下の各リポジトリに格納されます。

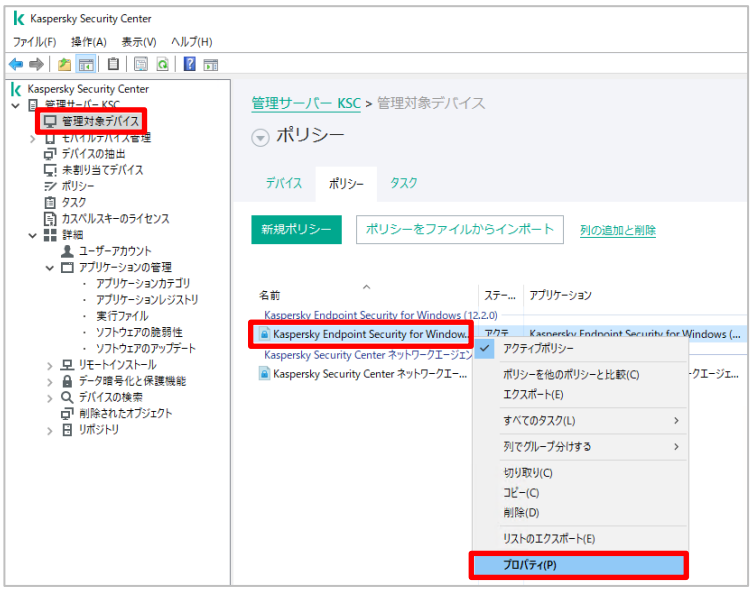
隔離	ウイルスなどの脅威、またはその亜種に感染している可能性があると判断されたオブジェクトは、動作をブロックして元のフォルダーから削除し、「隔離」処理が行われます。 ステータスは「感染の可能性あり」となります。 オブジェクトは特別な領域に安全な形で保存され、検知情報のみが KSC へ通知されます。
バックアップ	マルウェアが検知された場合、動作をブロックしてオブジェクトを元のフォルダーから削除し、バックアップコピーを作成します。 既定では、オブジェクトに対しマルウェアの部分の駆除を試み、駆除ができない場合はオブジェクトの削除処理を試みます。 駆除、または削除処理が成功した場合は、ステータスに「駆除」または「削除」と結果が表示されます。 バックアップコピーは特別な領域に安全な形で保存され、検知情報のみが KSC へ通知されます。
アクティブな脅威	検知はしたものの、以下の理由により隔離、駆除、または削除処理ができないオブジェクトは「未処理ファイル」となります。 ➢ 対象となるオブジェクトが CD-ROM や DVD 内のファイル ➢ 書き込み権限のないデバイス上にあるファイル ➢ メーラーなど、他プロセスの影響により処理ができない ➢ スキャンタスクの設定にて、「脅威検知時の処理」の設定が「通知する」となっていて、通知時にユーザーが「スキップ」処理を選択した場合 検知情報が KSC へ通知されます。

7.1.1. 「隔離」と「バックアップ」の保存領域

「隔離」と「バックアップ」のデータが保存される領域には、既定で**「30 日間」**オブジェクトが保管され、このしきい値を超えた場合、古いものから順に削除されます。

この設定は、KES のポリシーにて確認、変更することができます。

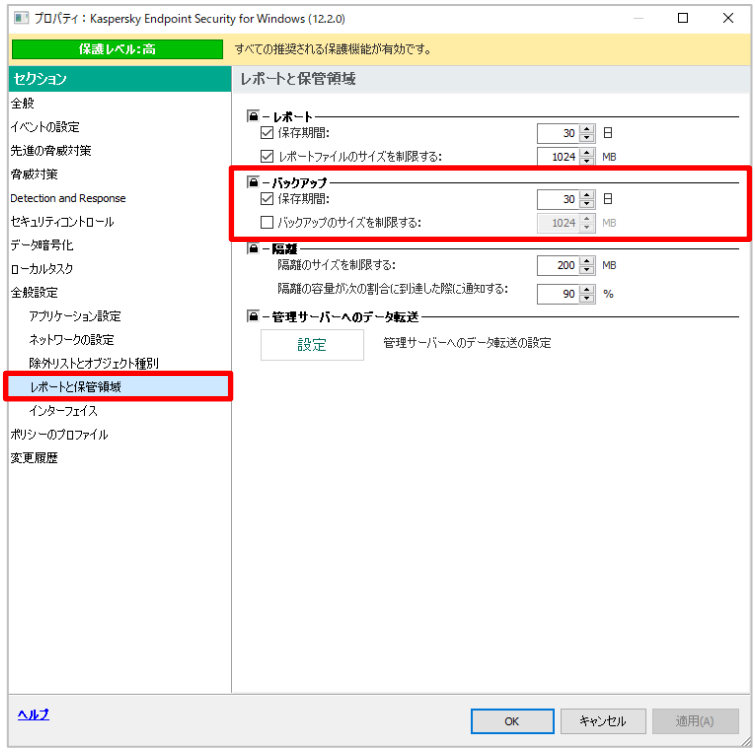
(1) 「管理対象デバイス」を開き、右画面にて「ポリシー」タブを開きます。
KES のポリシーを右クリックし、「プロパティ」を開きます。



(2) 「全般設定」-「レポートと保管領域」セクションを開きます。

・保存期間：30 日
「隔離」「バックアップ」領域に保存する日数を設定できます。

・保存サイズ：オフ（既定:100MB）
「隔離」「バックアップ」領域に保存できる最大サイズを設定できます。
この設定を有効にした場合、期間かサイズどちらかのしきい値に達した場合古いものから削除されます。



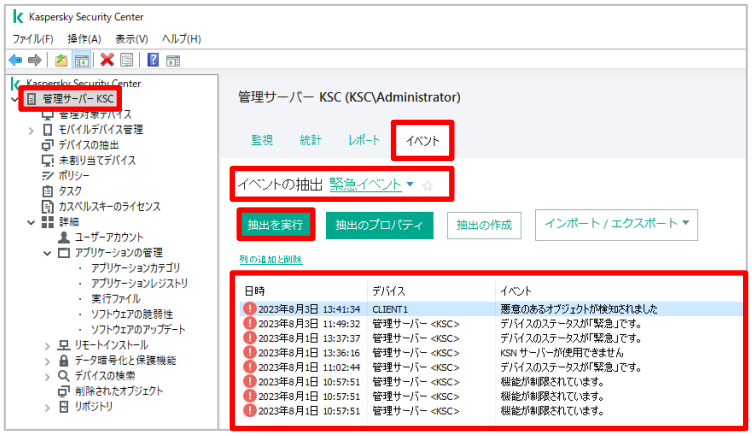
本節は以上です。

7.2. マルウェア検知時のイベントについて

管理下のデバイスにてマルウェアの検知が発生した場合、KSC 上にイベントが通知されます。

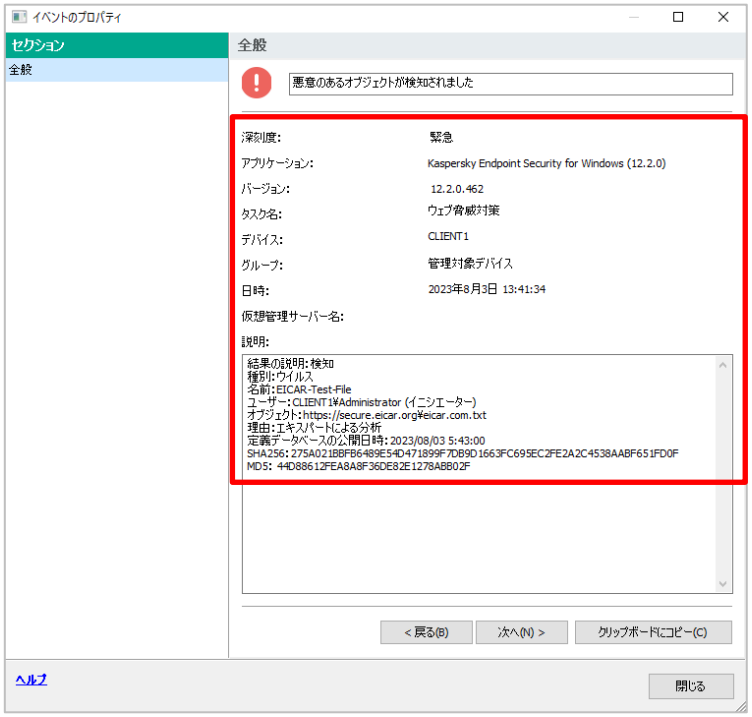
(1) 「管理サーバー」を選択し、「イベント」タブを開きます。

「イベントの抽出」にて「緊急イベント」を指定し、「抽出を実行」をクリックすることで、緊急イベントのみを表示することができます。



(2) イベントをクリックすると、検知の詳細を確認することができます。

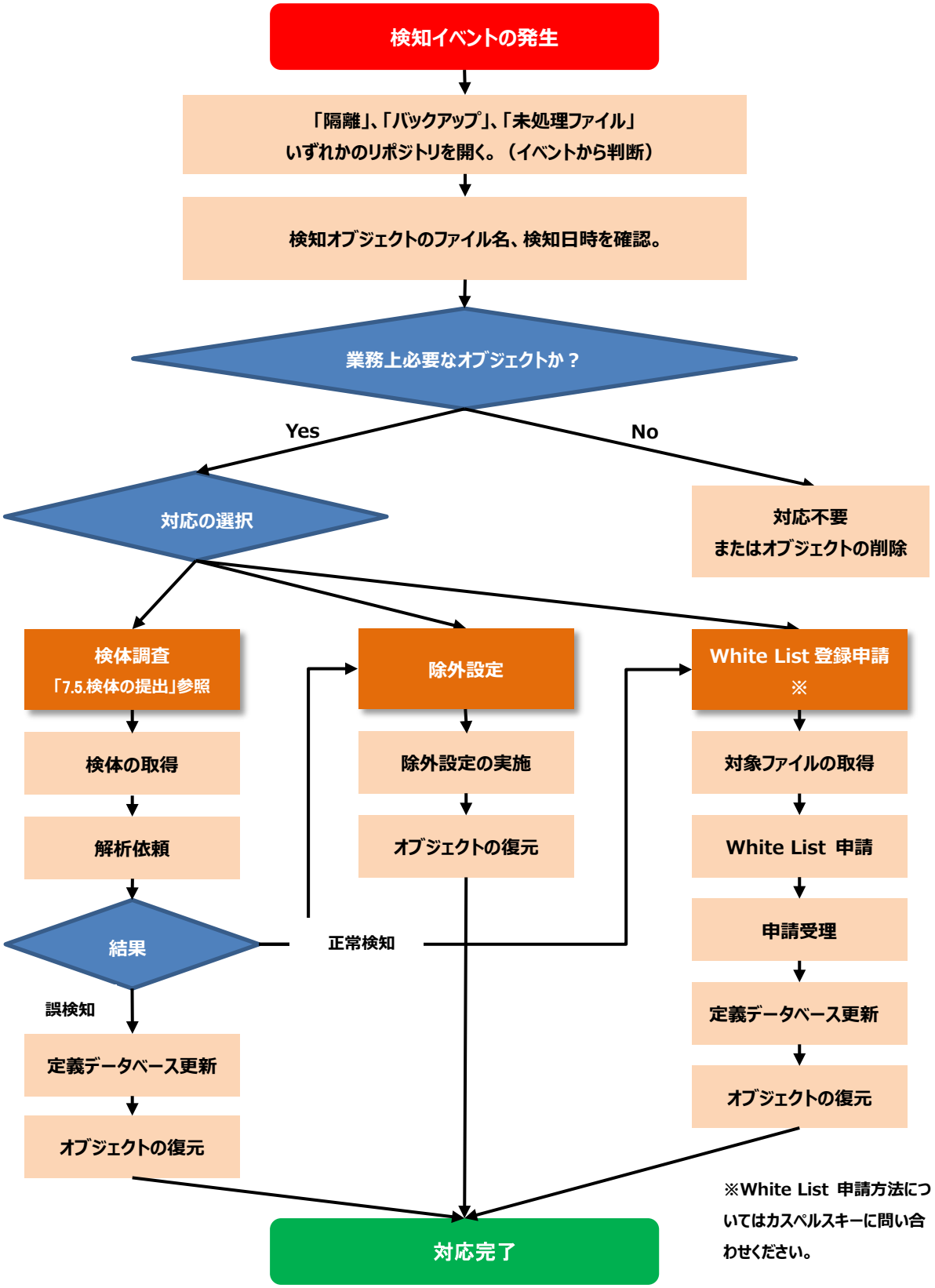
- **アプリケーション**
  デバイスのアプリケーション名が表示されます。
- **バージョン**
  アプリケーションのバージョン情報を確認できます。
- **タスク名**
  検知した保護コンポーネントの名前が表示されます。
  (ファイル脅威対策、ウェブ脅威対策 など)
- **デバイス**
  検知したデバイスのホスト名が表示されます。
- **グループ**
  デバイスが格納されているグループ名が表示されます。
- **日時**
  マルウェアの検知日時が表示されます。
- **説明**
  検知名、オブジェクトのパス、定義 DB の日時など詳細が表示されます。



本節は以上です。

7.3. マルウェア検知時の対応について

管理下のデバイスにてマルウェアの検知が発生した場合、以下のフローを参考に対応を実施してください。



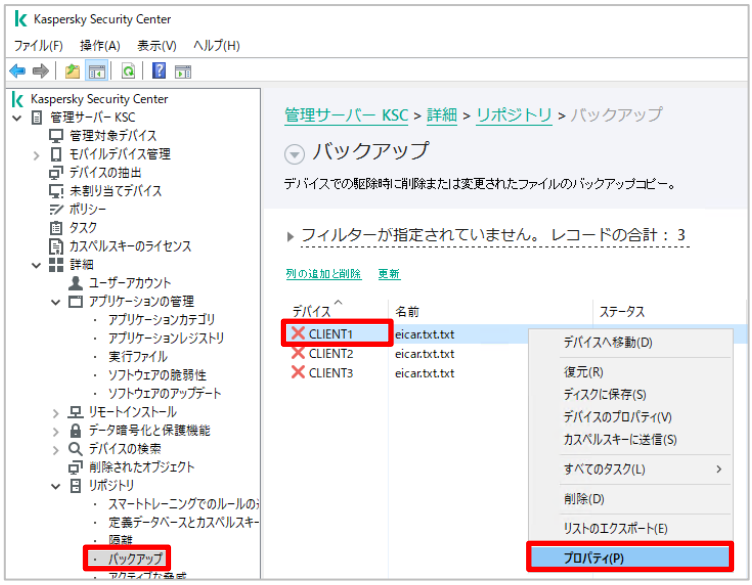
7.4. 「バックアップ」「アクティブな脅威」リポジトリの確認

処理されたオブジェクトの情報は、KSC にて確認することができます。

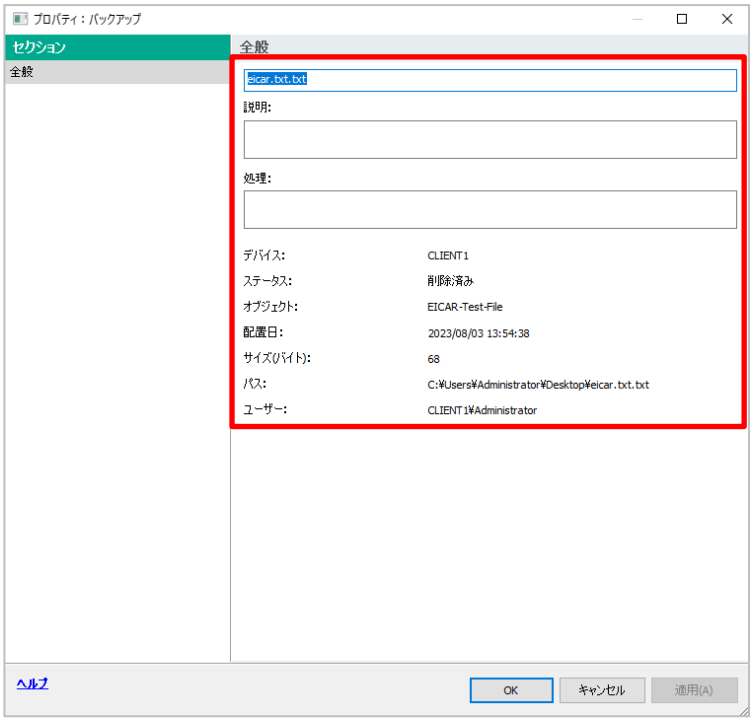
(1) KSC にて「詳細」-「リポジトリ」を開きます。

「バックアップ」、「アクティブな脅威」を開くことで、それぞれ処理されたオブジェクトの情報を確認することができます。

(2) 例として、「バックアップ」を開き、オブジェクトを選択して右クリックしてプロパティを開きます。



(3) 右記のように検知されたオブジェクトに関する詳細情報を確認することができます。



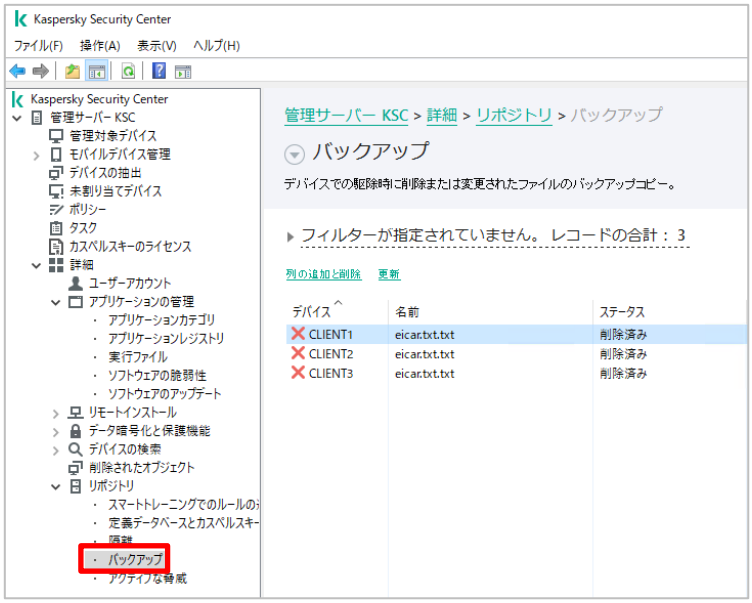
本節は以上です。

7.4.1. 「バックアップ」リポジトリに対する処理

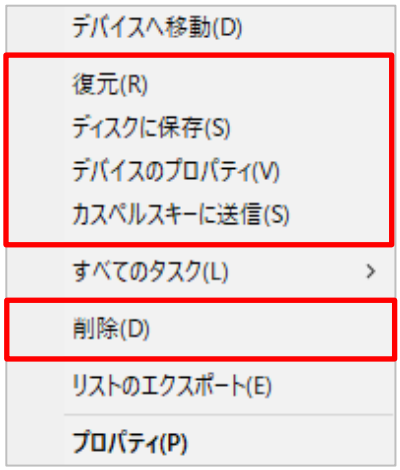
駆除または削除処理が行われ、バックアップコピー処理がされたオブジェクトに対する処理方法をご説明します。

(1) 「詳細」-「リポジトリ」-「バックアップ」を開きます。

管理下のデバイスにて検知し、バックアップコピーが行われたオブジェクトの一覧が表示されます。



(2) オブジェクトを右クリックすると、右記のコンテキストメニューが表示されます。



- **復元※**
  クライアントデバイス上にオブジェクトを復元します。
- **ディスクに保存※**
  KSC 上にオブジェクト本体を保存します。
- **デバイスのプロパティ**
  検知したデバイスのプロパティ画面を表示します。
- **カスペルスキーに送信※**
  KSC 上に安全な形でオブジェクトを保存します。(保存のみで送信はされません)
- **削除※**
  デバイス上にあるオブジェクトの「バックアップコピー」を削除します。

※この処理を実施する場合は、デバイスの起動および KSC との接続が必要です。

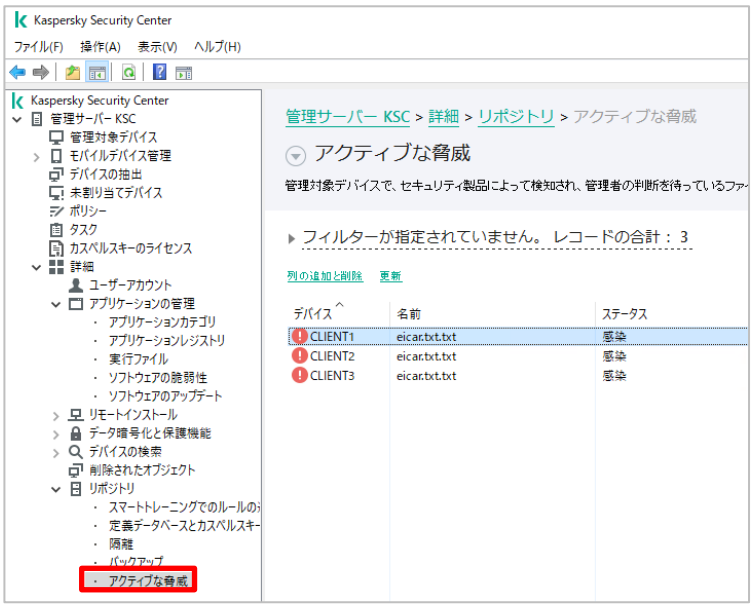
本項は以上です。

7.4.2. 「アクティブな脅威」リポジトリに対する処理

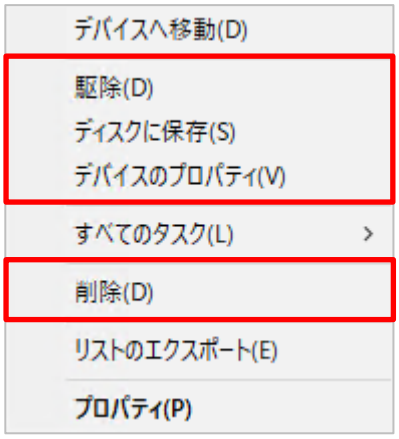
検知したものの駆除または削除処理ができず、「アクティブな脅威」状態のオブジェクトに対する処理方法についてご説明します。

(1) 「詳細」-「リポジトリ」-「アクティブな脅威」を開きます。

管理下のデバイスにて検知したものの、未処理となっているオブジェクトの一覧が表示されます。



(2) オブジェクトを右クリックすると、右記のコンテキストメニューが表示されます。



- **駆除※**
  オブジェクトの駆除を試みます。（失敗する場合もあります）
- **ディスクに保存※**
  KSC 上にオブジェクトを保存します。
- **デバイスのプロパティ**
  検知したデバイスのプロパティ画面を表示します。
- **削除※**
  デバイス上にあるオブジェクトの削除を試みます。（失敗する場合もあります）

※この処理を実施する場合は、デバイスの起動および KSC との接続が必要です。

本節は以上です。

7.5. 検体の提出

カスペルスキーサポートでは、検体の調査を承っております。

弊社アナリストにより、オブジェクトにマルウェアが含まれているかどうか解析を行います。 解析結果により定義データベースの修正を行う場合もあります。

※ ウイルスの仕組み、処理や感染ルートなど、詳細についてはサポートでは承っておりません。

【検体提出時の注意点】

- KSC 上で収集したオブジェクト、ファイル自体、URL など、解析できる形式をご用意ください。
- カスペルスキーサポートへご提供いただく場合は、**"パスワード付きの zip 形式"** にてご提供ください。
- 圧縮時のパスワードは「 **infected** 」を設定してください。（別のパスワードを設定した場合はパスワードをご連絡ください）
- カスペルスキーサポートへ検体を提出する際は、カンパニーアカウントをご使用ください。
  https://companyaccount.kaspersky.com

  [カンパニーアカウントとは]
  https://support.kaspersky.co.jp/faq/companyaccount_help

  カンパニーアカウントの使用方法、検知提出の方法などは、カスペルスキーサポートへお問い合わせください。
  [サポートセンターのご案内（法人向け製品）]
  https://support.kaspersky.co.jp/b2b/JP

kaspersky

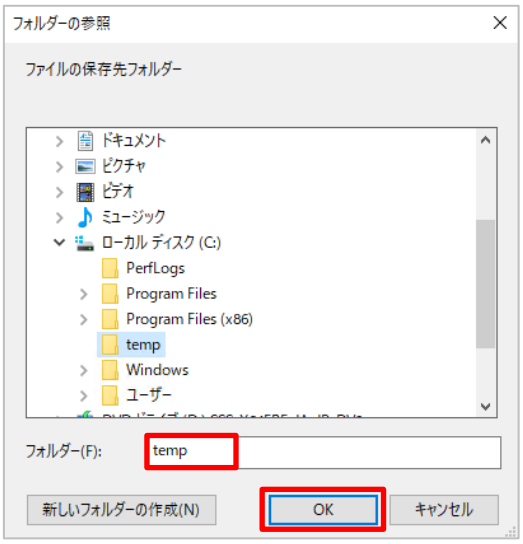
検知したファイルを管理サーバー上から収集する場合は以下の手順を実施します。

(1) 管理サーバーにて「バックアップ」内にあるファイルを右クリックし、「カスペルスキーに送信」を選択します。

※この時、管理サーバーはクライントから実体を収集するため、管理下のデバイスが起動中であり、且つ KSC と通信可能な状態である必要があります。

(2) ファイルの保存先を指定し「OK」をクリックします。
ここでは C:¥temp を指定しています。

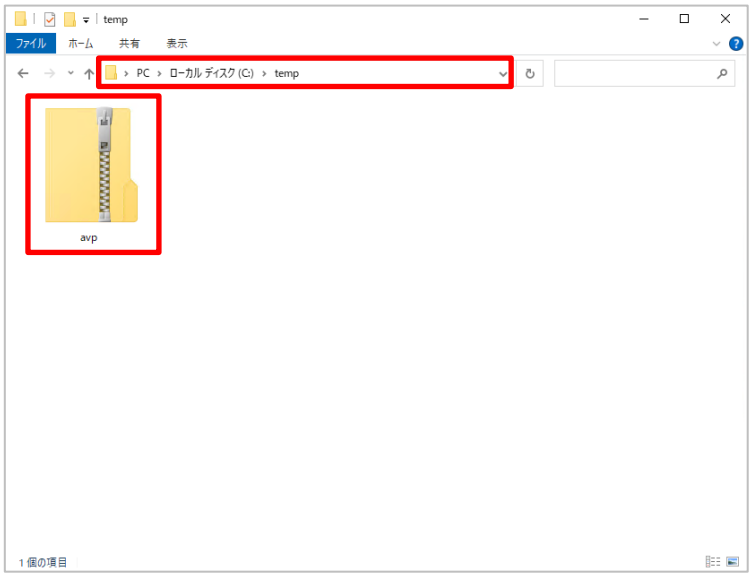
「OK」を実行後、ブラウザーが起動しますが閉じてください。



(3) C:¥temp フォルダー配下に「**avp.zip**」という名前のファイルが作成されます。

実際のファイルとは異なる、安全な形式で作成されております。

このファイルをパスワード付きで圧縮し、カスペルスキーサポート宛にご提供ください。



本章は以上です。

8. ライフサイクルの確認

カスペルスキーにて提供しているアプリケーションにはライフサイクルがあります。
サポート終了（EOL）となったアプリケーションについては、定義データベースの配信は終了し、サポートも受け付けることはできません。

ライフサイクルは以下サイトにてご案内しております。
[製品サポートライフサイクル]
https://support.kaspersky.co.jp/corporate/lifecycle
※内容は予告なく変更する場合がありますので定期的にご確認ください。

ご使用いただいているアプリケーションについて確認し、最新バージョンへの移行を計画いただきますよう、お願いいたします。

9.　便利な機能、効果的な設定

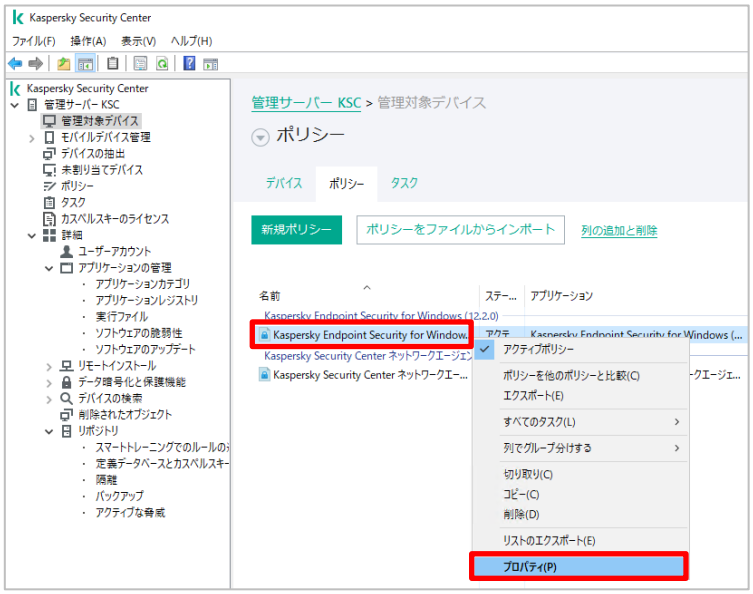
本章では、必須ではないものの、運用を行う上で便利な機能や、効果的な設定についてご説明します。

9.1.　ポップアップ通知

管理下のデバイスにてウイルス検知など特定のイベントが発生した場合、画面にポップアップ通知を表示させることができます。

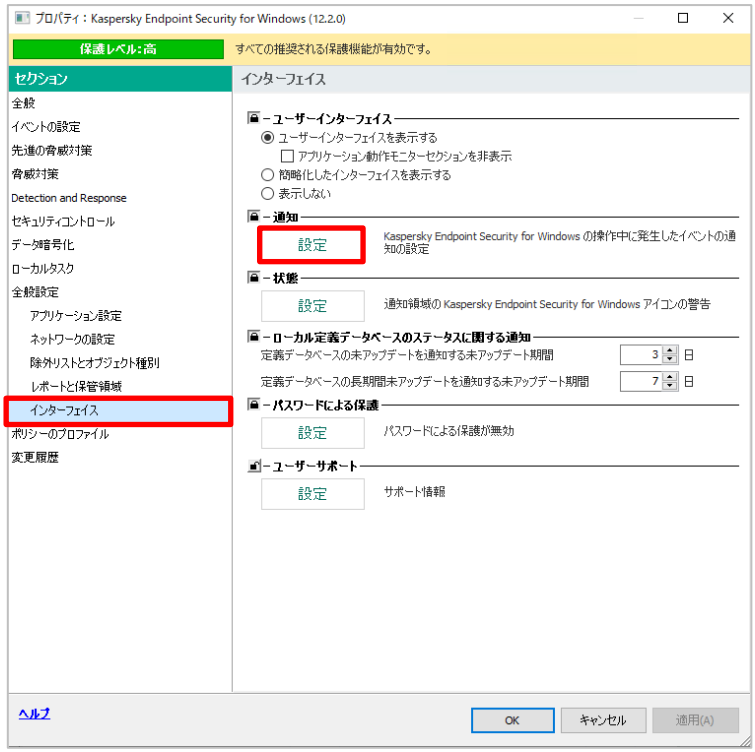
本章では、ファイルアンチウイルス機能にてウイルスを検知した際、ポップアップ通知を表示する設定についてご説明します。

(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) 「全般設定」-「インターフェイス」セクションを開きます。

「通知」項目にある「設定」ボタンをクリックします。



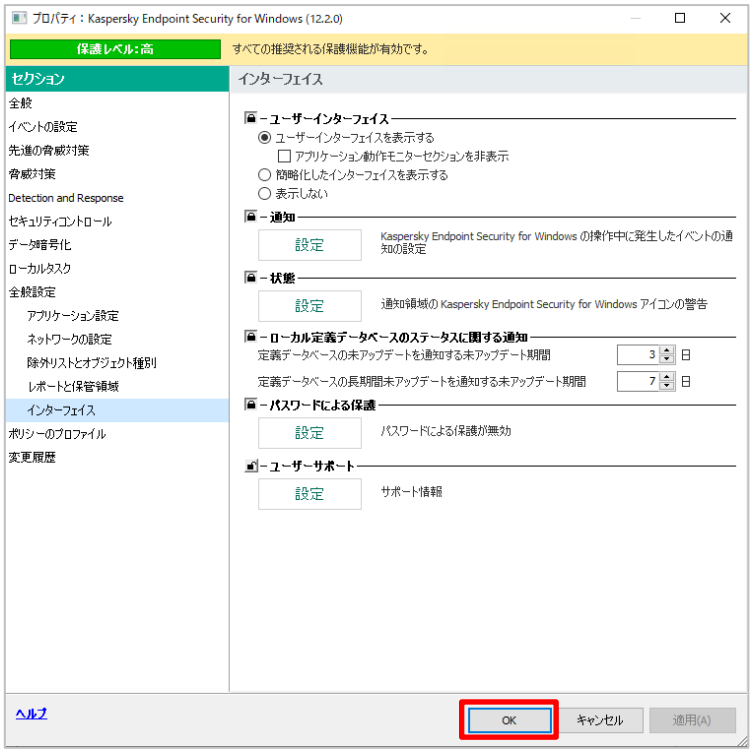
(3) 「ファイル脅威対策」を選択します。

右画面にて、「悪意のあるオブジェクトが検知されました」項目の「画面に通知」にチェックを入れます。

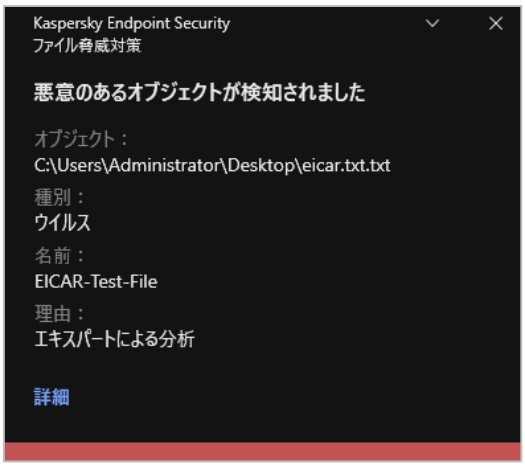
「OK」をクリックし、設定を保存します。

(4) 「OK」をクリックし、ポリシー設定を保存します。

設定は以上になります。



(5) クライアントにてファイル脅威対策コンポーネントがウイルスを検知すると、デスクトップ上に右記のようなポップアップメッセージが表示されます。



本節は以上です。

9.2. モバイルモードの設定

KSC では「モバイルモード」という機能があります。

「モバイルモード」とは、ノートパソコンなど社外で使用する機会があるクライアントコンピューターに対し、社外持ち出し用のポリシー、タスクへ自動的に切り替えることができる機能です。

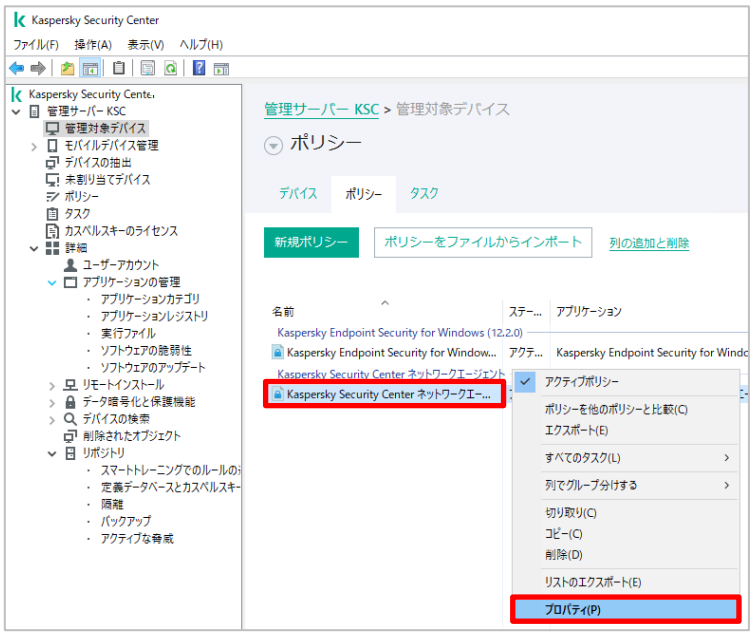
この機能を有効化することで、社内使用時は定義データベースを KSC からダウンロードし、外出時はインターネット上からダウンロードするよう自動的に切り替えることができます。

モバイルモードの詳細につきましては、以下にサイトある**「モバイルモード」**をご参照ください。

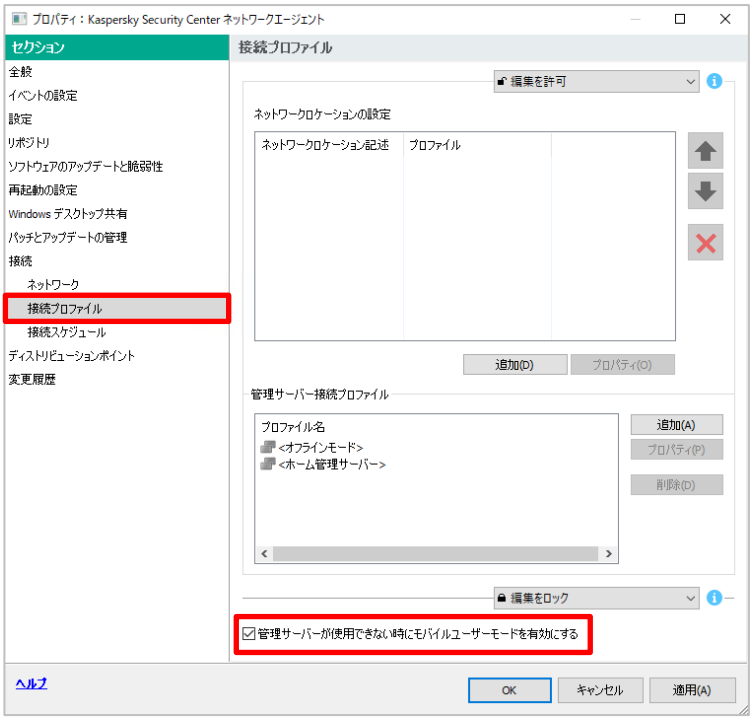
法人のお客様向けダウンロード資料（https://kasperskylabs.jp/biz/）

ここでは、外出時に定義データベースをインターネットからダウンロードするよう、自動的に切り替えるための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。
「Kaspersky Security Center ネットワークエージェント」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にて、「ネットワーク」-「接続」-「接続プロファイル」セクションを開き、「管理サーバーが使用できない時にモバイルユーザーモードを有効にする」にチェックを入れ「OK」をクリックしてプロパティ画面を閉じます。



ポリシーの設定は以上です。

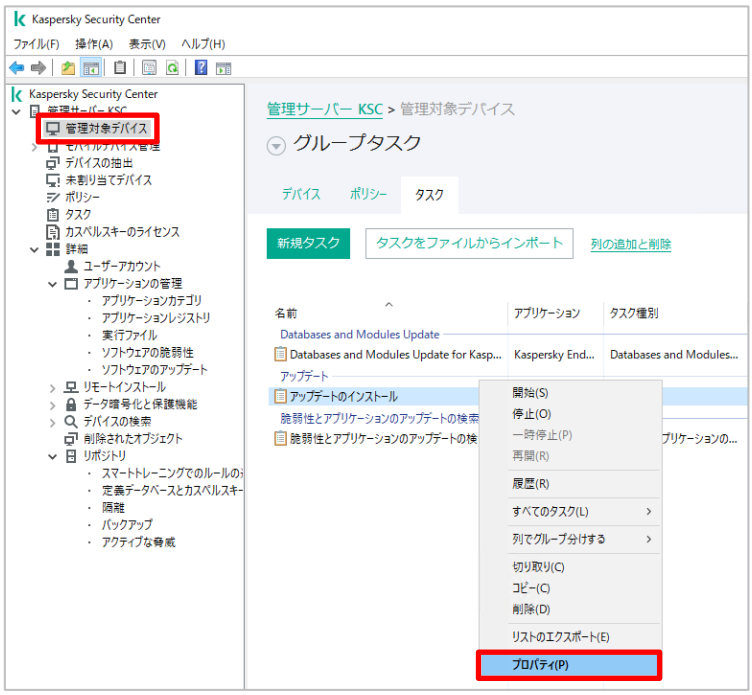
ポリシーがクライアントへ適用されると、モバイルモードへの切り替えが有効となります。

なお、定義データベースのアップデートタスクは既定の設定で使用でき、変更する必要はありません。

ここでは、KSC にて既定で作成される KES 用の定義データベースアップデートタスクである「アップデートのインストール」タスクを使用して設定値をご説明します。

(1)「管理対象デバイス」を開き、「タスク」タブを開き、「アップデートのインストール」タスクを右クリックし、「プロパティ」を開きます。

個別にアップデートタスクを作成している場合は、そのタスクの「プロパティ」を開きます。

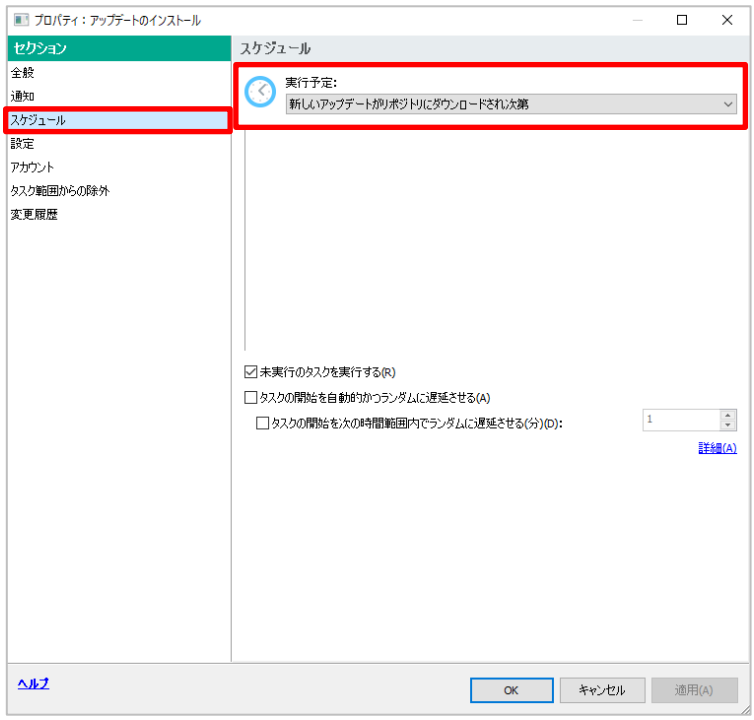


(2)「スケジュール」セクションを開きます。

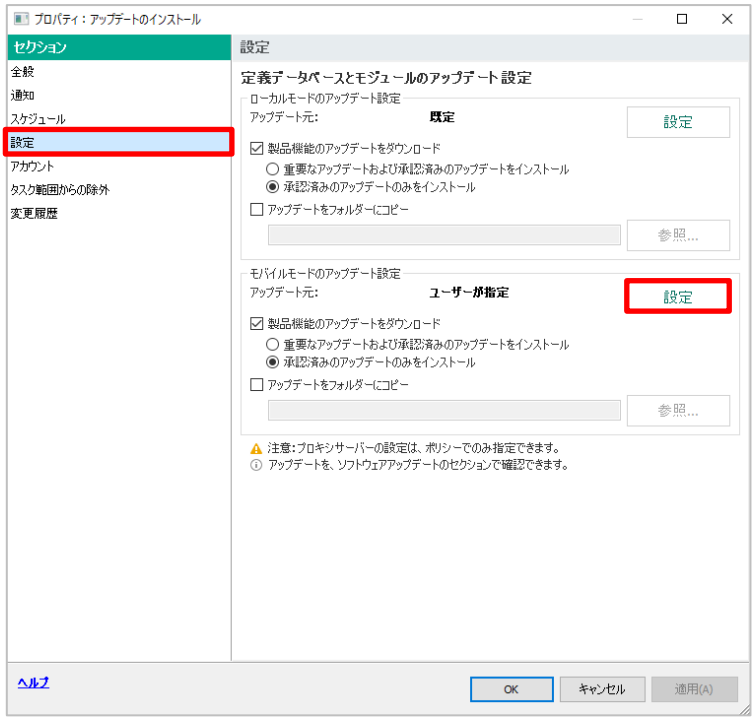
既定の実行予定は**「新しいアップデートがリポジトリにダウンロードされ次第」**となっており、KSC 上で定義データベースが更新された場合に実行されます。

「モバイルモード」に切り替わった場合は、**「2 時間毎に 1 回」**の間隔でタスクが実行されます。

他のスケジュールを設定していた場合は、そのスケジュールに従って実行されます。



(3)「オプション」セクションを開きます。
「モバイルモードのアップデート設定」の「設定」ボタンをクリックします。



(4)モバイルモードに切り替わった際のアップデート先が設定されています。

既定では**「カスペルスキーのアップデートサーバー」**が指定されており、インターネット上のサーバーからダウンロードする設定となっております。

設定を確認後、「閉じる」をクリックして閉じます。

本節は以上です。

9.3.　デバイスの抽出

KSC の「管理対象デバイス」配下に、拠点や部署ごとに複数のグループを作成し、デバイスを管理することができます。

「デバイスの抽出」機能を使用することで、管理下のデバイスに対し、特定の条件に該当するデバイスを抽出することができます。また、この抽出したデバイスに対してタスクを割り当てることができます。

【こんなときに実施】

・「定義データベースがアップデートされていない」条件に該当するデバイスを抽出する。

→ 該当したデバイスに対し、定義データベースのアップデートタスクを実行する。

・KES のバージョン xxxxx のデバイスを抽出する。

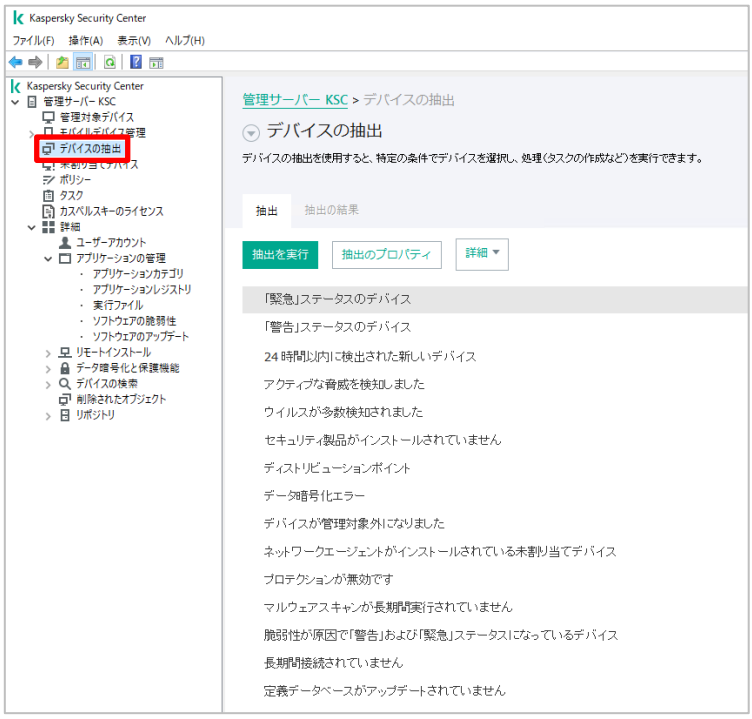
→ 該当したデバイスに対し、KES のバージョンアップタスクを実行する。

9.3.1. 「デバイスの抽出」の表示

「デバイスの抽出」を開くには以下の手順を実施します。

(1) KSC にて「デバイスの抽出」を選択します。

既定で作成されている抽出条件があります。



(2) 既定で右記の抽出条件が作成されております。
抽出条件を選択し、「抽出を実行」をクリックすると、デバイスの抽出が実行されます。

(3) 抽出結果を確認する場合、「抽出の結果 “抽出条件名”」をクリックすることで抽出条件に一致したデバイス一覧を確認することができます。

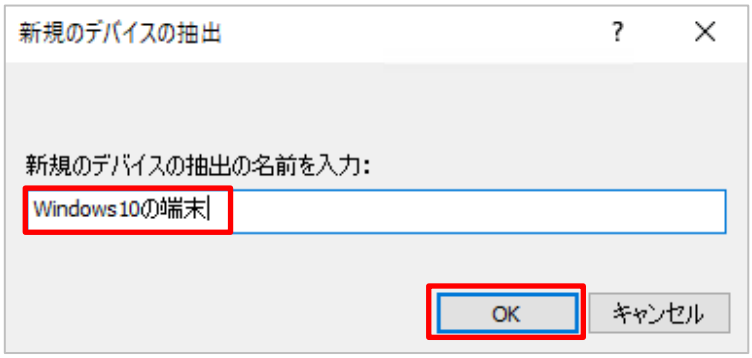
本項は以上です。

9.3.2. 新規抽出条件の作成

「デバイスの抽出」にて新規の抽出条件を作成するには、以下の手順を実施します。

(1) 「デバイスの抽出」を右クリックし、「新規作成」-「新規の抽出」を選択します。

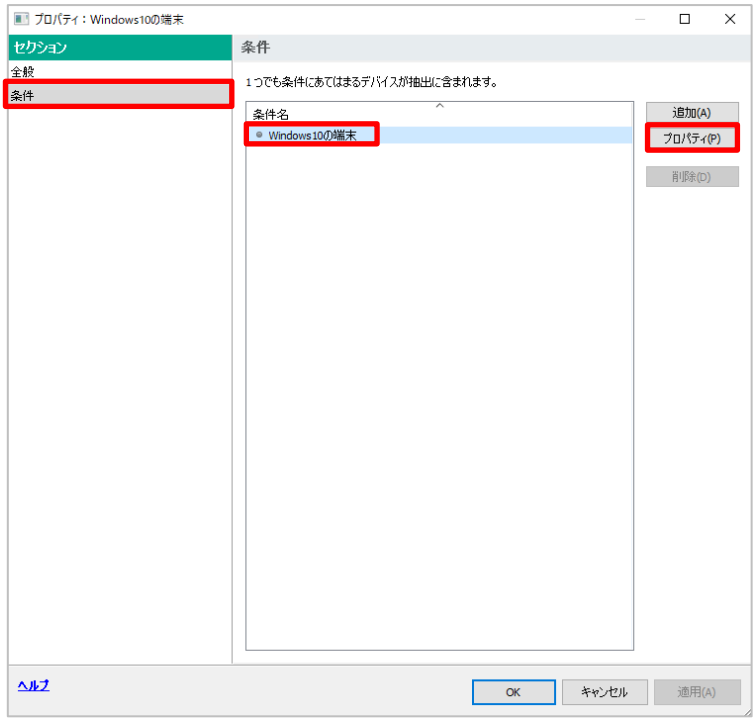
(2) 任意の名前を入力し、「OK」をクリックします。
ここでは「Window10 の端末」としています。



(3) 抽出が作成されたことを確認します。
条件を設定する場合は、作成した抽出条件（ここでは「Windows10 の端末」）が選択されている状態で「抽出のプロパティ」をクリックします。

(4) 「条件」セクションを開きます。
条件名を選択し、「プロパティ」をクリックします。

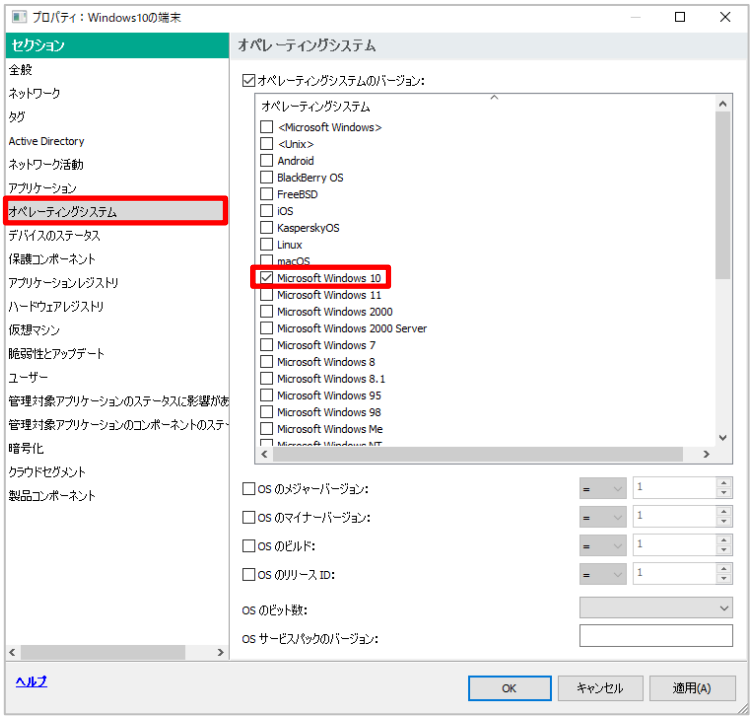
なお、「追加」ボタンをクリックすることで別の条件（OR 条件）を追加することができます。



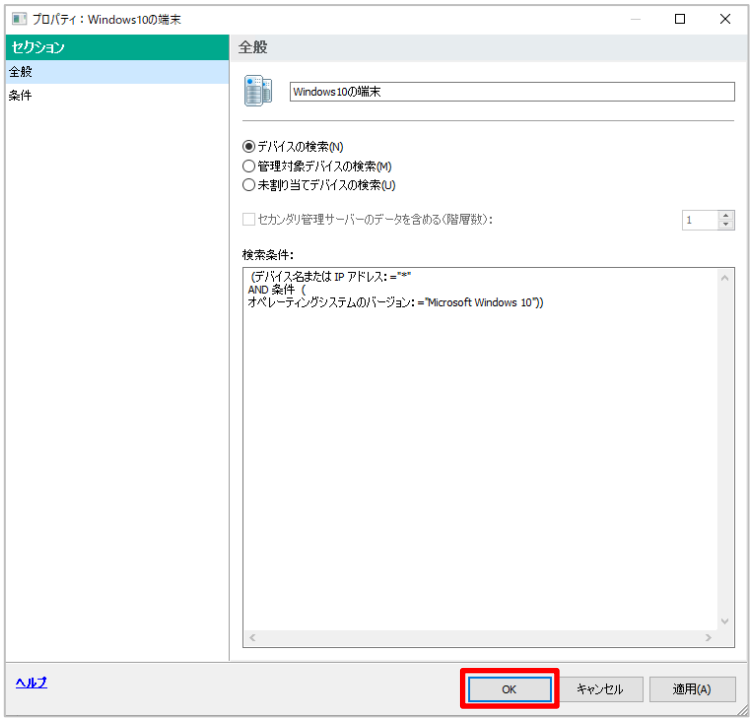
(5) 条件を設定する画面が表示されます。
各セクションを開いて抽出条件を設定したら「OK」をクリックし、設定を保存します。

ここでは、Windows10 の OS を抽出するため「オペレーティングシステム」セクションにて「Microsoft Windows 10」にチェックを入れています。

※ このプロパティ内で設定した内容は AND 条件となります。



(6)「OK」をクリックし、設定を保存します。



本節は以上です。

9.4. ネットワークエージェントの管理サーバーアドレス変更

ネットワークエージェントに設定されている管理サーバー（KSC）の宛先は変更することができます。
ここでは、デバイス側で KSC の宛先を変更する手順についてご説明します。

【こんな時に実施】

・インストール時に設定した宛先に誤りがあったため変更したい。
・KSC の宛先は間違いないが、同期に失敗する。
→ KSC とネットワークエージェントで保持している証明書に差異がある可能性があります。
KSC の宛先を再度設定することで、証明書を再取得します。

※ この手順を実行するには管理者権限が必要になります。

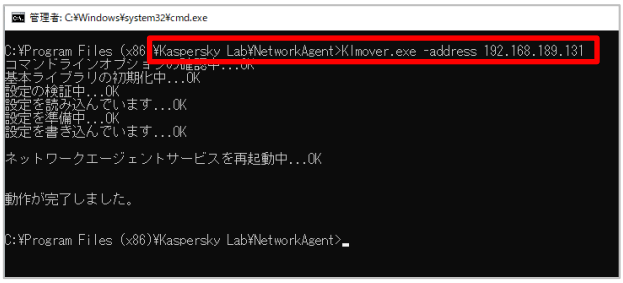
(1) コマンドプロンプトを起動し、ネットワークエージェントのインストールパスへ移動します。
既定では以下パスになります。

・32bit
C:¥Program Files¥Kaspersky Lab¥NetworkAgent
・64bit
C:¥Program Files (x86)¥Kaspersky Lab¥NetworkAgent

(2) 以下のコマンドを入力して実行します。

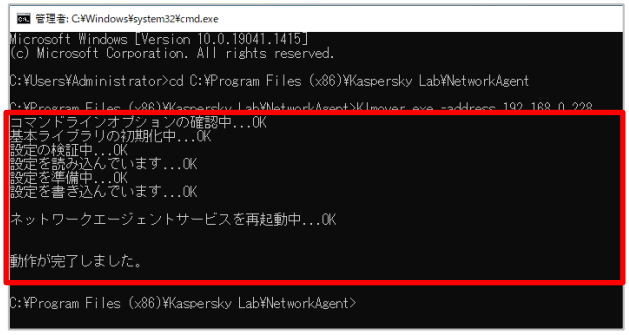
Klmover.exe△-address△KSC のアドレス

△はスペースです。
KSC のアドレスはホスト名、または IP アドレスを指定します。



(3) 宛先の設定が変更され、ネットワークエージェントのサービスが再起動します。

「4.6.3 デバイスから KSC への接続状態を確認」を実行し、KSC との疎通ができるかどうかご確認ください。



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

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