Kaspersky Security Center 14
Kaspersky Endpoint Security 12
ポリシー・タスク設定　実践編

2023/09/20

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 2.0

kaspersky

目次

1. はじめに

1.1. 本資料の目的

本資料では、Kaspersky Endpoint Security for Business におけるポリシー、およびタスクの目的別の設定についてご説明します。

ポリシー、タスク設定の考え方については、別資料「ポリシー・タスクの考え方 KSC/KES 対応版」をご参照ください。

各種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.　デバイスのパフォーマンス改善

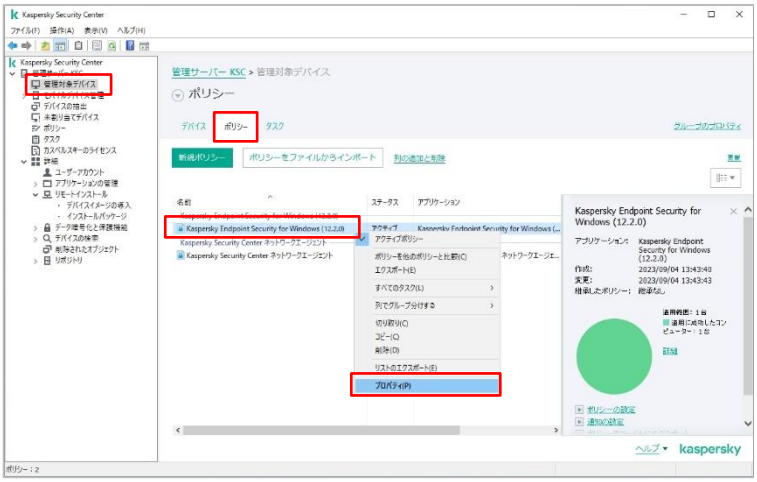
2.1.　スキャン対象形式を調整する

スキャンの対象を減らすことでパフォーマンスが改善されることがあります。
また、実行スケジュールでスキャンの間隔や時間帯を調整する方法（「4.タスクのスケジュール設定」参照）もご検討ください。

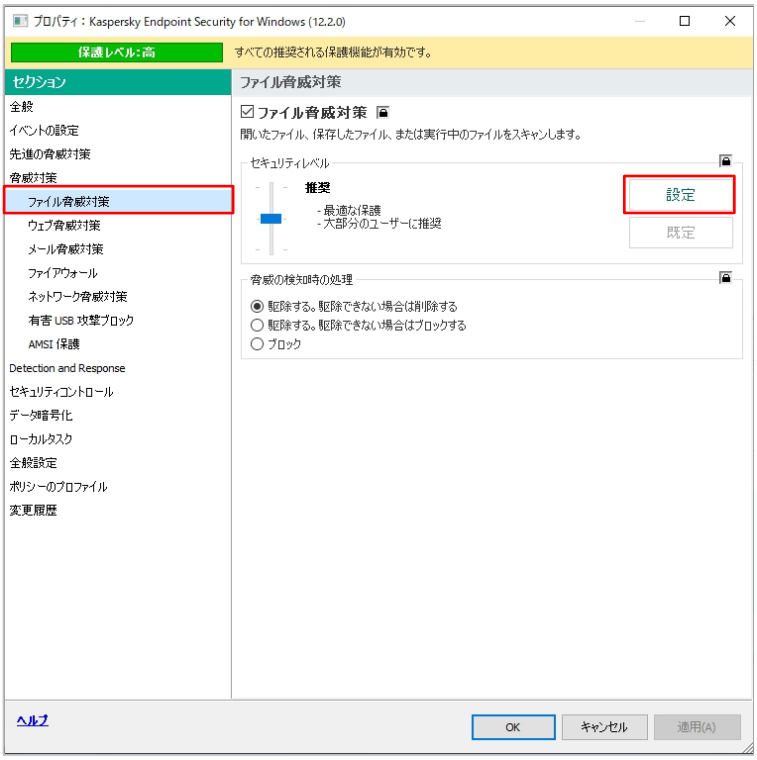
ここでは、スキャンの対象をファイル形式によって調整する方法についてご説明します。
「Kaspersky Endpoint Security（KES）」ではスキャンの対象を以下の 3 種類から選択できます。

・**すべてのファイルをスキャン** - スキャン対象がもっとも多く完了まで時間がかかる可能性がありますが、高いセキュリティを保つことができます。
・**ファイル形式でファイルをスキャン** - ファイルヘッダを精査し感染の可能性のあるファイル形式のみスキャンします。既定ではこの設定が選択されており、セキュリティとパフォーマンスのバランスが取られています。
・**拡張子でファイルをスキャン** - ファイルヘッダは確認せずファイル名の拡張子のみで感染の可能性のあるファイル形式かを判断し、スキャンします。ファイル名の拡張子が変更されていると、感染の可能性があるファイル形式であってもスキャンがスキップされる可能性があります。

(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。

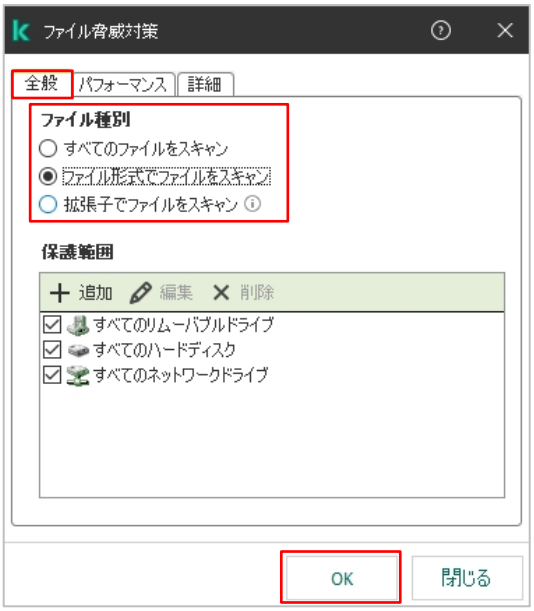


(2) 「脅威対策」-「ファイル脅威対策」セクションを開きます。
右画面にて「セキュリティレベル」欄内の「設定」をクリックします。



(3) 「全般」タブの「ファイル種別」欄で対象を選択します。

設定後、「OK」をクリックして設定を反映させます。



本節は以上です。

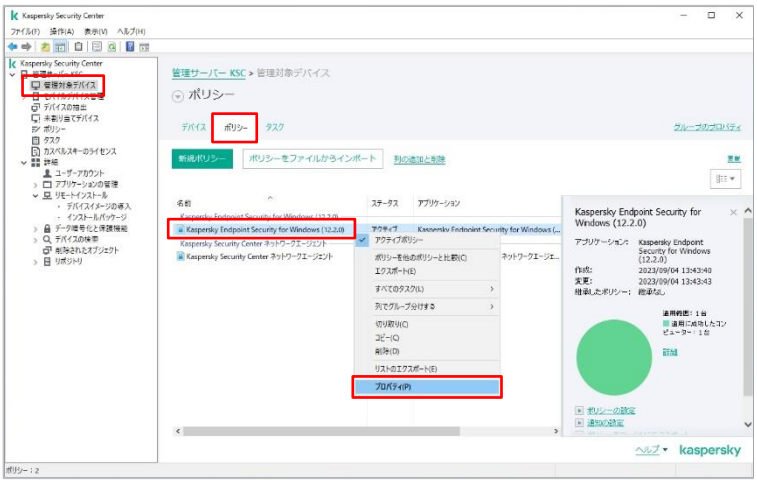
2.2.　新規作成または更新されたファイルのみをスキャン対象にする

スキャンの対象を新規作成または更新されたファイルに限定することで、スキャン対象を減らすことができます。この機能によりスキャンのパフォーマンスを向上させることができます。

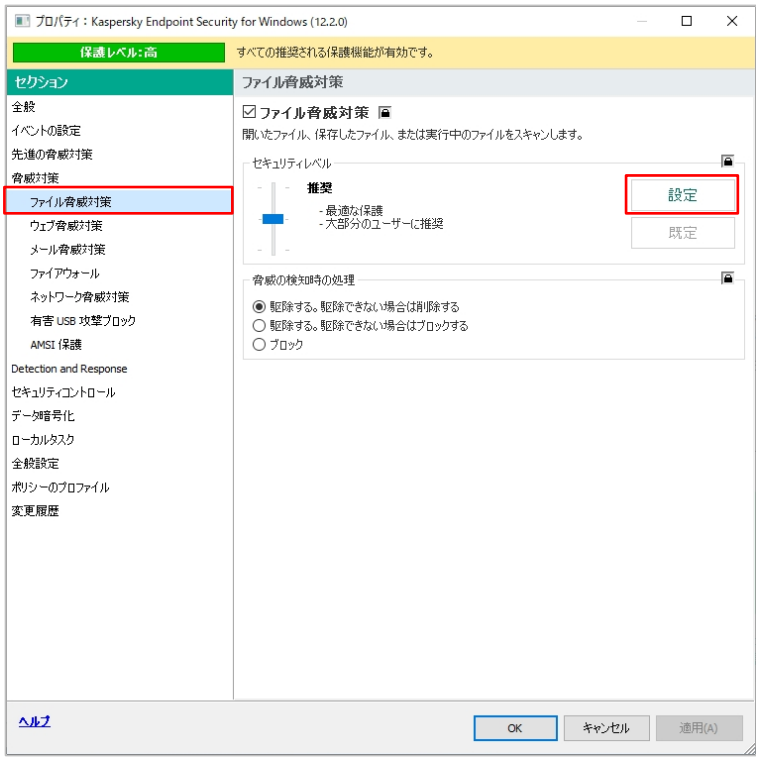
既定では有効になっています。

（本機能が有効な場合、iSwift/iChecker 方式でのスキャンは行われません）

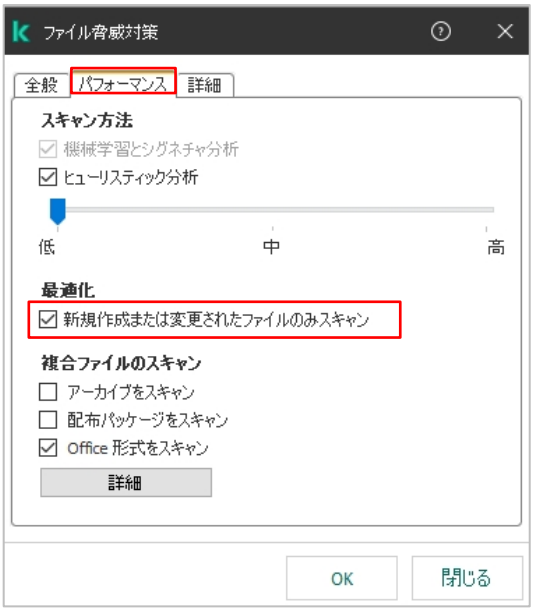
(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



(2) 「脅威対策」-「ファイル脅威対策」セクションを開きます。
右画面にて「セキュリティレベル」欄内の「設定」をクリックします。

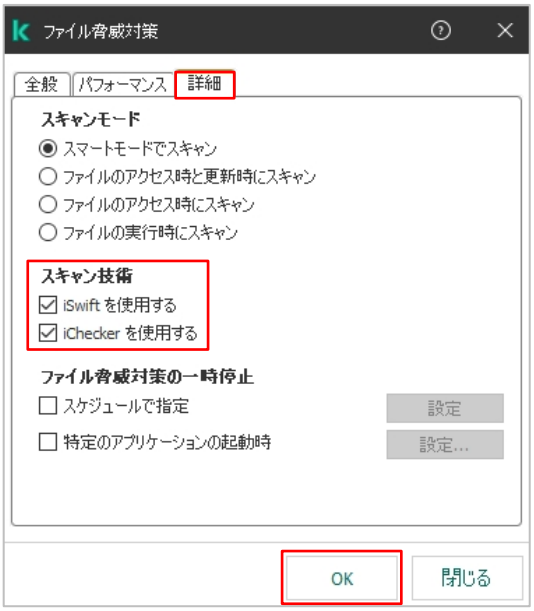


(3) 「パフォーマンス」タブを開き、「新規作成または更新されたファイルのみスキャン」にチェックを入れます。



(4) 「詳細」タブを開き、「スキャン技術」欄でそれぞれの有効/無効を設定します。

設定後、「OK」をクリックして設定を反映させます。

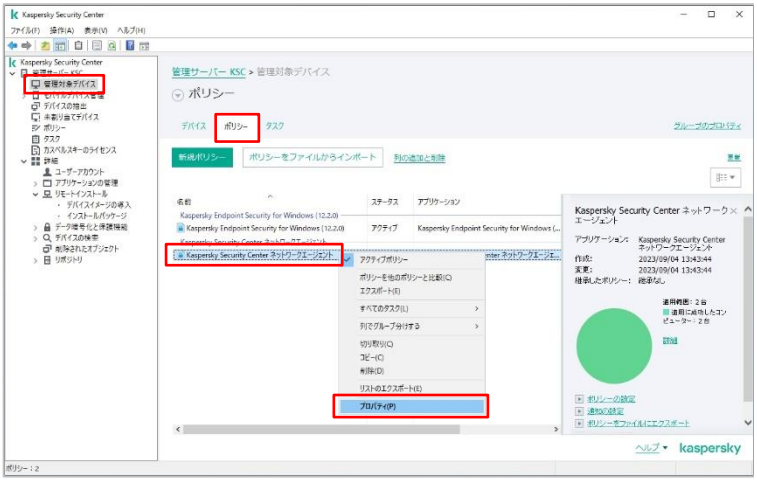


2.3. クライアントと管理サーバーの同期間隔を変更

ネットワークエージェントは、定期的に管理サーバーに接続してデバイスの情報やステータスの送信、ポリシーなど設定に更新があるか確認しています。管理下のクライアント台数などにより、この同期が管理サーバーのパフォーマンスやネットワークトラフィックに影響を及ぼす可能性があります。

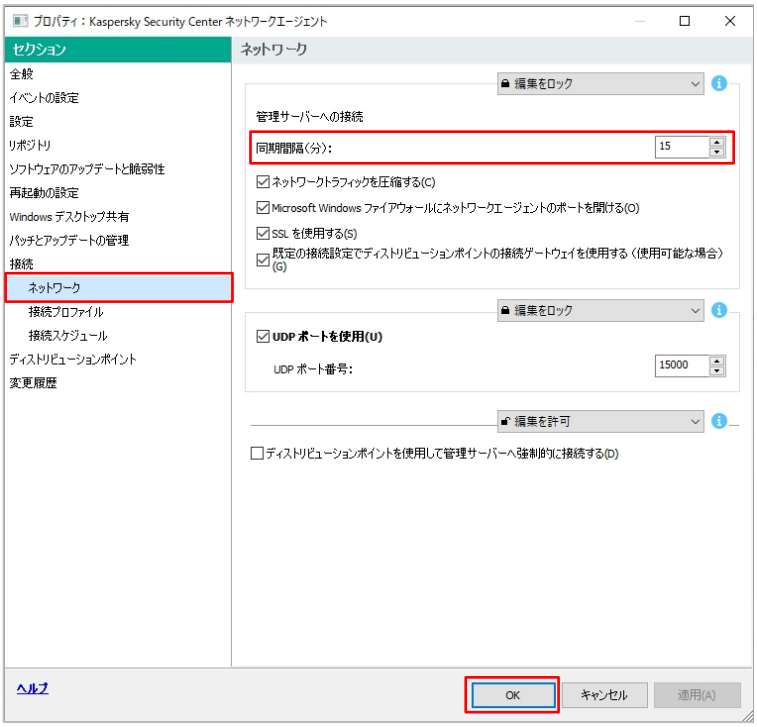
この確認の間隔を延ばすことで、ネットワークと管理サーバーにかかる負荷を抑えることができます。初期設定では 15 分間隔となっています。

(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KSC ネットワークエージェント」のポリシーを右クリックして「プロパティ」を選択します。



(2) 「接続」-「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」の値を設定します。

設定後、「OK」をクリックして設定を反映させます。

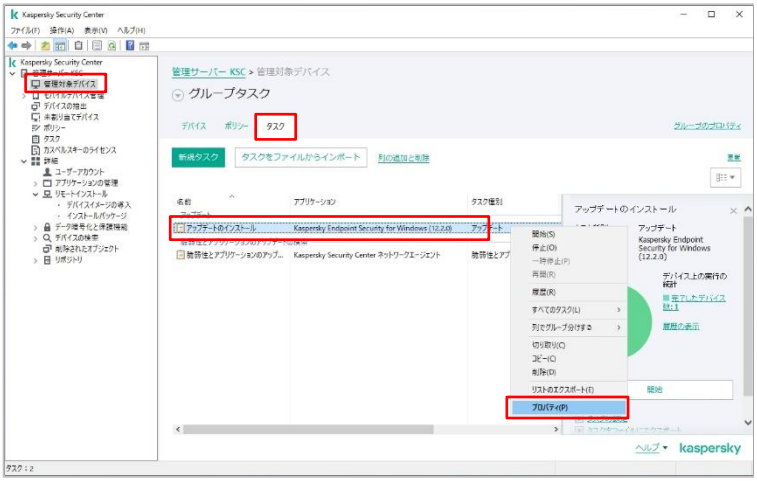


本節は以上です。

2.4. デバイスへの定義データベース配信に伴う管理サーバー負荷を軽減

デバイスへの定義データベースの配信は、既定で管理サーバーから行われます。
同時に実行する台数が多い場合、パフォーマンスに影響を及ぼす可能性があります。
タスクの実行を分散化することで管理サーバーやネットワークの負荷を軽減できる可能性があります。

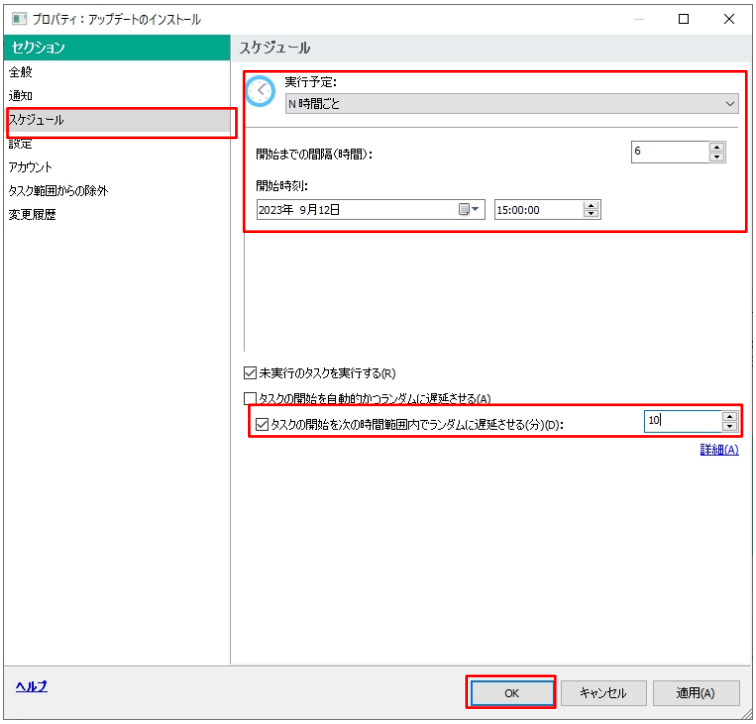
(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



(2) 「スケジュール」セクションを開きます。
「実行予定」を「N 時間ごと」など定期的に実行する設定に変更します。

同じ画面で、「タスクを実行するまでの時間を自動的に設定する」をオフにして、「タスクを次の時間にランダムに実行する」をオンに設定し、時間を入力します。

設定後、「OK」をクリックして設定を反映させます。



- ランダム実行時間、クライアント台数とアップデートのタイミングについて
  - ✧ ランダム実行時間：L 分
  - ✧ クライアントの台数：N 台
  - ✧ アップデートのタイミング： [L / N]分間隔

例：ランダム実行時間：100 分
クライアントの台数：50 台
開始時刻：09:00:00

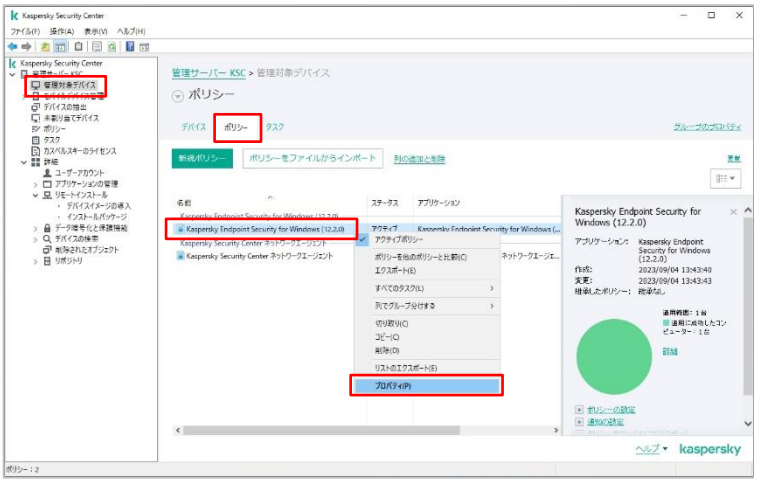
本節は以上です。

3. ネットワーク設定

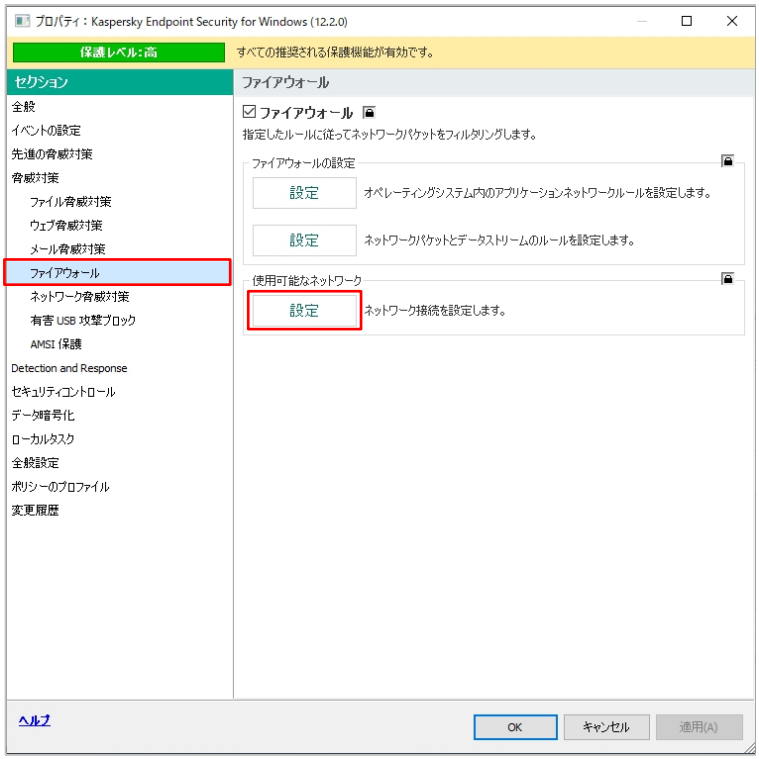
3.1. ファイアウォール設定

使用可能なネットワークを設定するネットワークの動作をファイアウォールで監視するネットワークの設定を行います。

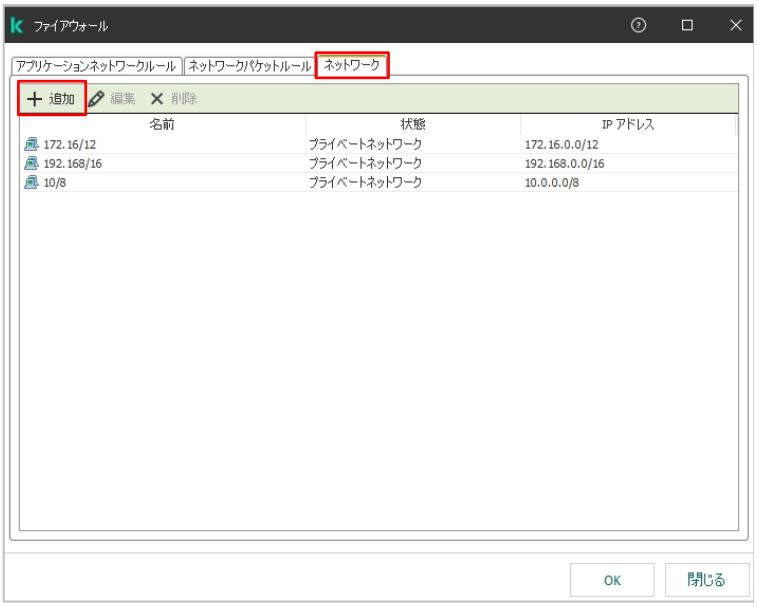
(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



(2) 「脅威対策」-「ファイアウォール」を開きます。
右画面にて「使用可能なネットワーク」の「設定」をクリックします。



(3) 「ファイアウォール」画面が表示されます。
「ネットワーク」タブを開き、「追加」をクリックします。



(4) 「ネットワーク接続」画面が表示されます。
ネットワークの「名前」、「状態」、「IP アドレスの編集」を設定します。

「状態」は、「パブリックネットワーク」、「プライベートネットワーク」、「許可するネットワーク」より選択します。
設定後、「OK」をクリックして設定を反映させます。

パブリックネットワーク、プライベートネットワーク、許可するネットワークについての説明は以下の通りです。

- **パブリックネットワーク**：
  アンチウイルス製品、ファイアウォール、またはフィルターによって保護されないネットワークのステータス（インターネットカフェのネットワークなど）です。このようなネットワークに接続されているコンピューターのユーザーに対して、ファイアウォールはこのコンピューターのファイルやプリンターへのアクセスをブロックします。外部ユーザーは、このコンピューターの共有フォルダーからデータにアクセスすることも、このコンピューターのデスクトップにリモートアクセスすることもできません。ファイアウォールは、各アプリケーションのネットワークの動作を、各アプリケーションに設定されたネットワークルールに従ってフィルタリングします。

- **プライベートネットワーク**：
  そのネットワークからユーザーがこのコンピューターのファイルやプリンターにアクセスすることを信頼するネットワーク（LAN またはホームネットワークなど）に割り当てます。

- **許可するネットワーク**：
  コンピューターが攻撃されない、または不正にアクセスされない安全なネットワークに割り当てます。このステータスのネットワークの場合、ファイアウォールは指定されたネットワーク内のすべてのネットワークの動作を許可します。

本節は以上です。

3.2. 管理サーバーのプロキシサーバー設定

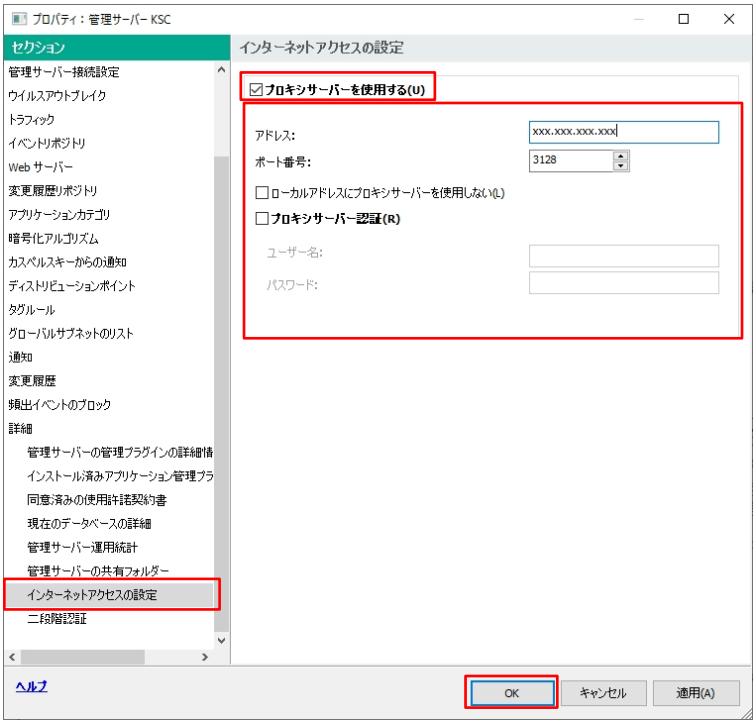
インターネットへの接続がプロキシサーバーを経由する環境である場合、管理サーバーは定義データベース情報をダウンロードするためにプロキシサーバーの設定が必要となります。

管理サーバーのプロキシサーバー設定は以下のように行います。

(1) 管理コンソールにて「管理サーバー」を右クリックし、「プロパティ」を選択します。

(2) 管理サーバーのプロパティが表示されます。「詳細」-「インターネットアクセスの設定」セクションで「プロキシサーバーを使用する」を有効にし、必要な項目を設定します。

設定後、「OK」をクリックして設定を反映させます。

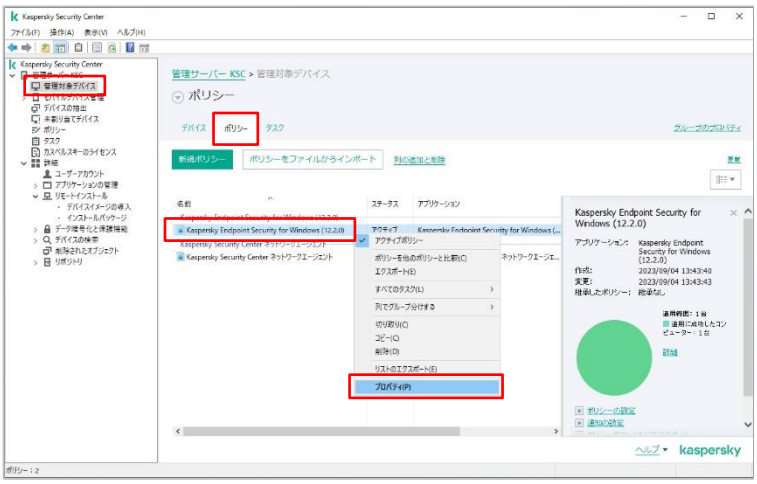


本節は以上です。

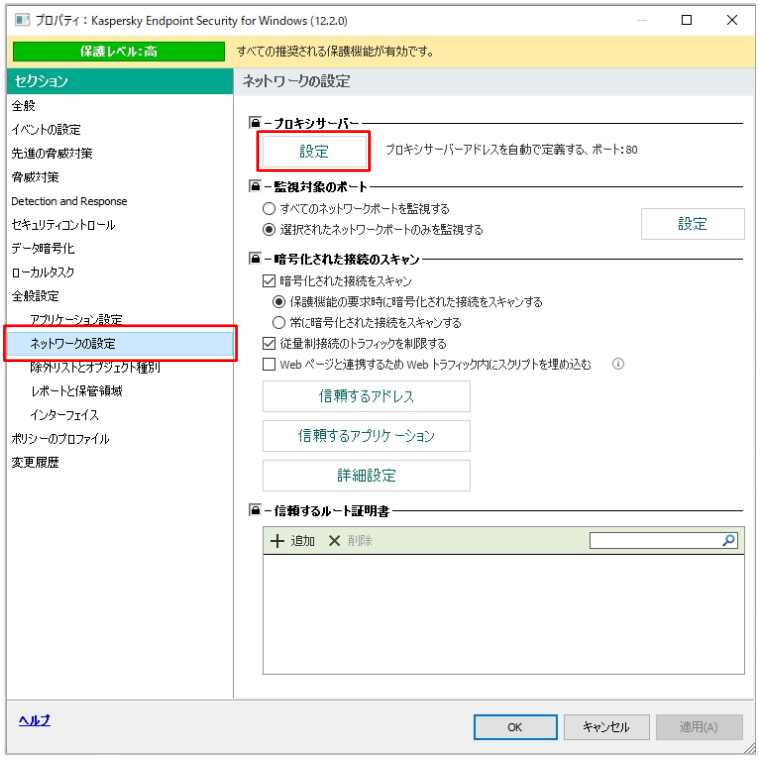
3.3. クライアントデバイスのプロキシサーバー設定

クライアントデバイスのプロキシサーバーの設定は以下のように行います。

(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



(2) 「全般設定」-「ネットワークの設定」セクションを開きます。
「プロキシサーバー設定」の「設定」をクリックします。



(3) 「プロキシサーバー設定」画面が表示されます。
「プロキシサーバーを使用する」を有効にして、必要な項目を設定します。

※「プロキシサーバーを自動的に検出する」に設定した場合はOSの設定に従い動作します。

設定後、「OK」をクリックして設定を反映させます。

本節は以上です。

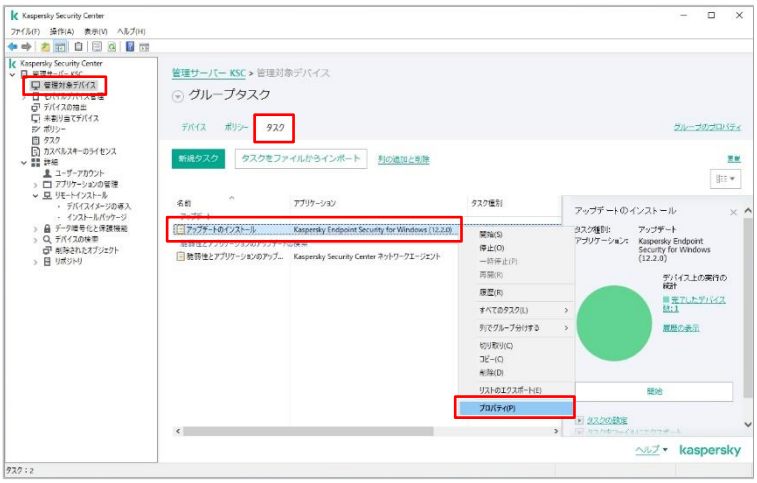
4. タスクのスケジュール設定

4.1. 定義データベースの更新スケジュールを設定する

定義データベースの更新タスクの実行スケジュールを設定します。

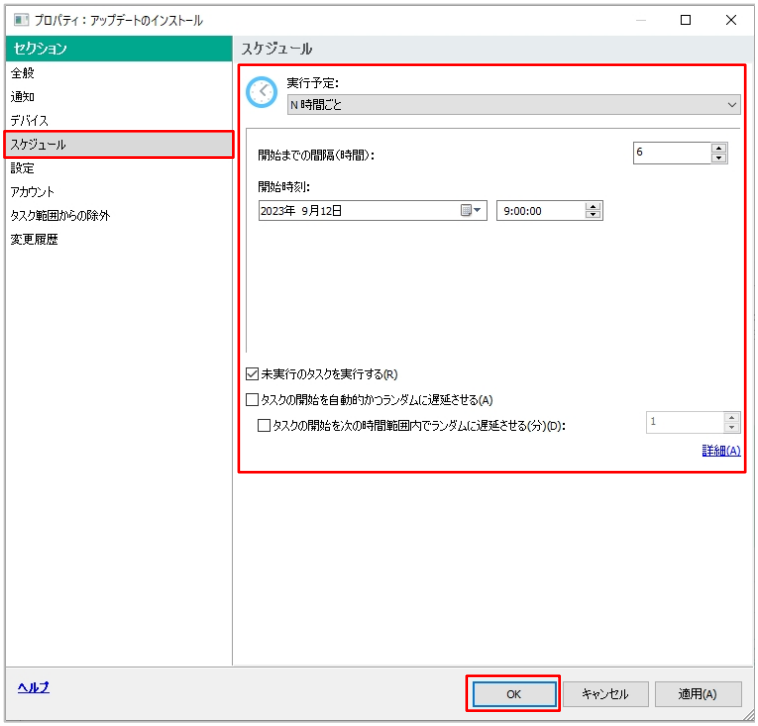
(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「管理対象デバイス」の「タスク」タブを開きます。

「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」を選択します。



(2) 「スケジュール」セクションを開きます。
任意のスケジュールを設定します（スケジュールの設定例は次ページ参照）。

設定後、「OK」をクリックして設定を反映させます。



- 「未実行のタスクを実行する」にチェックを入れておくと、設定したスケジュールの時刻に電源が OFF になっていた端末は、次回起動後にタスクが実行されます。
- 「タスクを実行するまでの時間を自動的に設定する」にチェックを入れておくと、設定スケジュール以降でクライアントがランダムな時間を設定しタスクを開始します。この設定によって管理サーバーの負荷が分散されます。（「2.4.デバイスへの定義データベース配信に伴う管理サーバー負荷を軽減」を参照してください。）

●スケジュール設定例

スケジュール設定	概要	設定例
N 時間ごと	設定した開始日時から「N 時間」間隔でタスクが実行される。	間隔：1 時間ごと 開始時間： 2016 年 1 月 1 日 09:00:00
N 日ごと	設定した開始日時から「N 日」間隔でタスクが実行される。	間隔：1 日ごと 開始時間：09:00:00
N 分ごと	設定した開始日時から「N 分」間隔でタスクが実行される。	間隔：30 分ごと 開始時間：09:00:00
毎週	毎週指定した曜日、時間で 1 回実行される。	毎週：月曜日 開始時間：09:00:00
毎月	毎月指定した日、時間で一回実行される。	毎月：1 日 開始時間：09:00:00
1 回	指定した日時で一回実行される。	実行日：2014/01/01 開始時間：09:00:00
手動	管理コンソールでタスクの「開始」をクリックした際に実行される。	「開始」クリック時
アプリケーション開始時	OS が起動して、KES のサービスが開始されてから 1 回実行されます。	アプリケーション開始時 タスクを実行するまでの時間：15 分
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	管理サーバーに新しい定義 DB がダウンロードされ次第、1 回実行される。 (管理サーバーは 1 時間毎に定義 DB をチェックしている。)	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
ウイルスアウトブレイク検知次第	ウイルスのアウトブレイクが発生したイベントをトリガーに 1 回実施される。	「ウイルスアウトブレイク」ステータスは別途定義される。
他のタスクが完了次第	他のタスクが完了したことをトリガーにして 1 回実施される。	「他のタスク」を指定する。

本節は以上です。

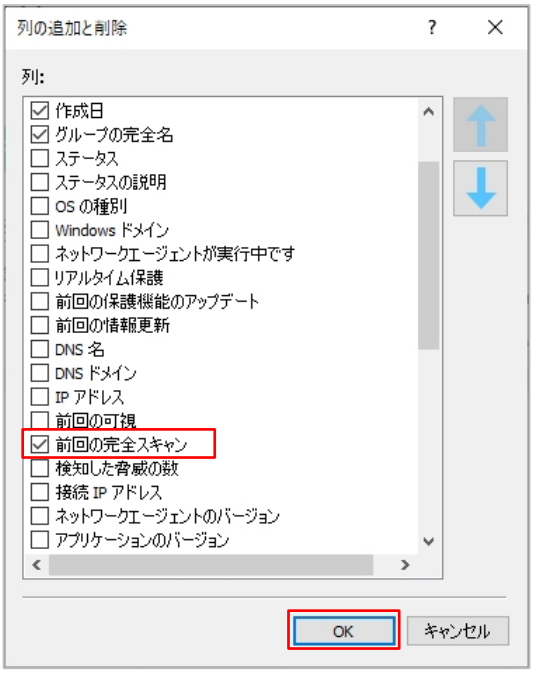
4.2. 各デバイスのスキャン実施完了日時を確認

ウイルススキャンの最終実施時間はグループの「**デバイス**」タブの列情報にて確認することができますが、既定では表示されません。

この列の項目を設定することで、スキャン実施日時などの情報を表示することができます。

(1) 管理コンソールにて「管理対象デバイス」を開きます。
「デバイス」タブを開き、「列の追加と削除」をクリックします。

(2) 「前回の完全スキャン」にチェックを入れます。
設定後、「OK」をクリックして設定を反映させます。



(3) 列の項目に、ウイルススキャンの最終実施時間が追加され、実行時間を確認することができます。

「前回の完全スキャン」列には完全スキャンタスクが最後に完了した時間が記録されます。
記録される条件として、タスク設定のスキャン対象範囲に最低限、次の内容が含まれている必要があります。

【スキャン対象領域】
・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

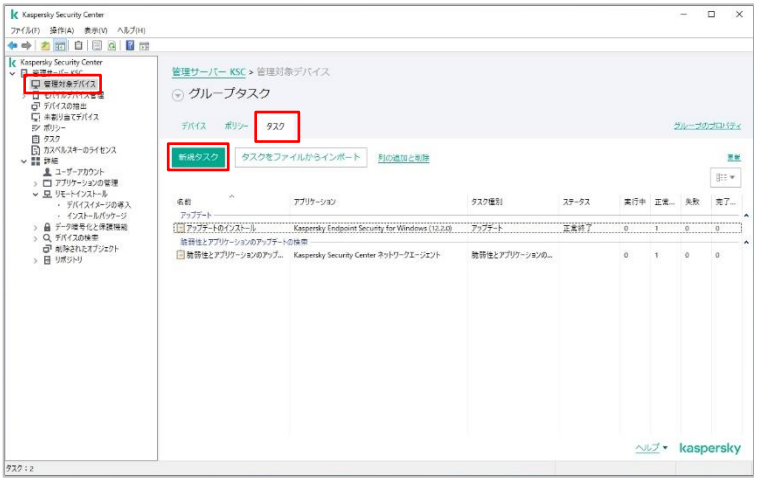
「前回の完全スキャン」が空白の場合、上記フォルダーを含むウイルススキャンが完了していない状態です。
初期設定ではこの状態が 14 日以上続いた場合、もしくは上記フォルダーを範囲に含むウイルススキャン実施から 14 日以上経過した場合、各クライアントは「**緊急**」ステータスに移行します。

本節は以上です。

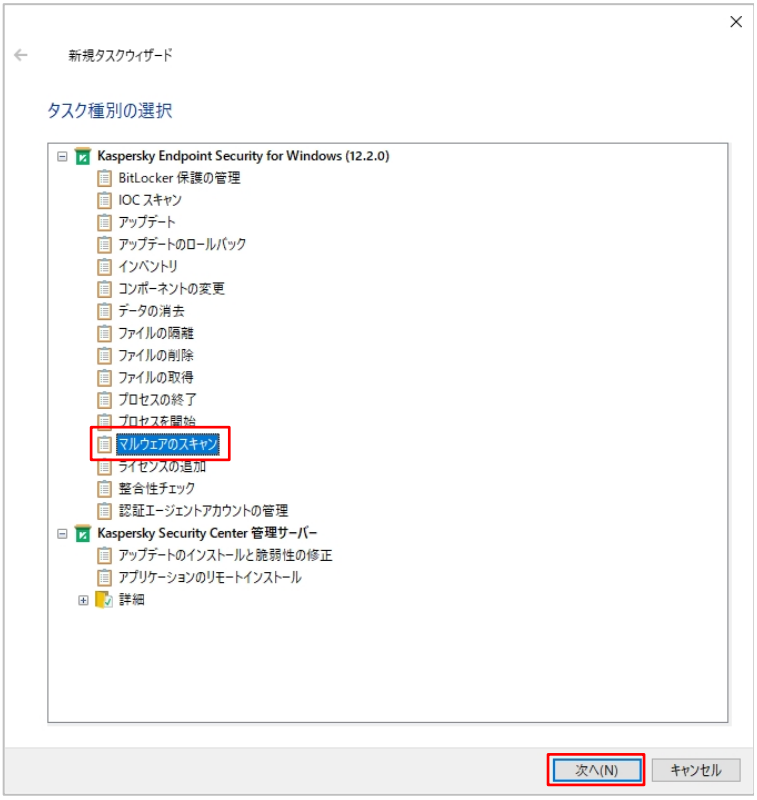
4.3. スキャンタスクの作成

スキャンタスクは既定で作成されません。以下の手順で、完全スキャンや範囲を指定したスキャンタスクを作成することができます。

(1) 管理コンソールにて「管理対象デバイス」を開きます。
「タスク」タブを開き、「タスクの作成」をクリックします。



(2) 「タスク種別の選択」画面が表示されます。
「KES」配下にある「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) 「スキャン範囲」画面が表示されます。

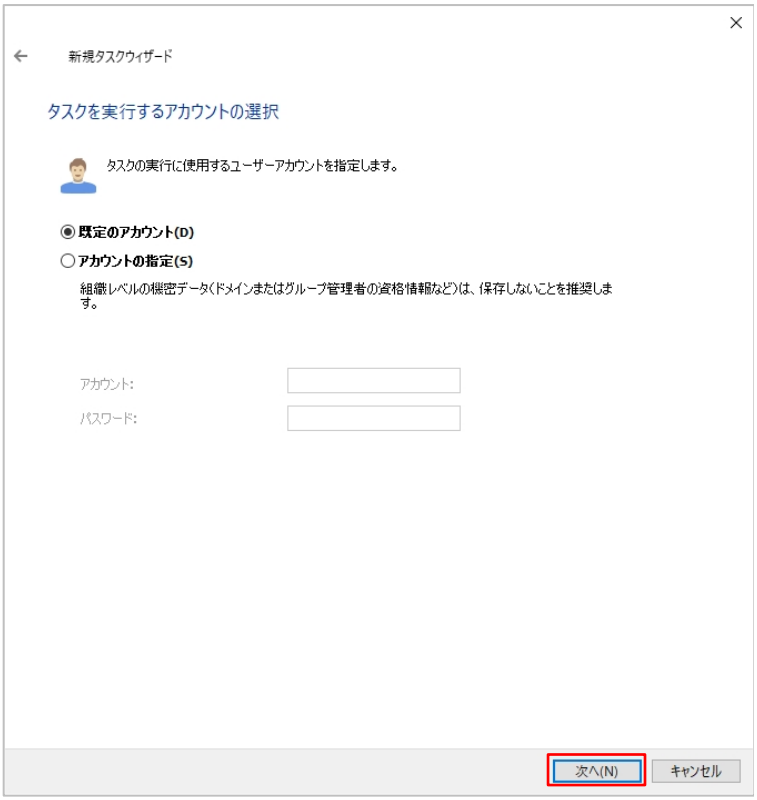
ここでスキャンする範囲を設定します。
既定では、完全スキャンに該当するメモリーや全てのハードディスクなどが範囲として含まれています。

スキャンタスクの完了時間を「前回の完全スキャン」列に表示させる場合、最低限以下の項目のチェックが必要です。

「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」

(4) 「KES の処理」画面が表示されます。
脅威を検出したときの処理を選択し、「次へ」をクリックします。

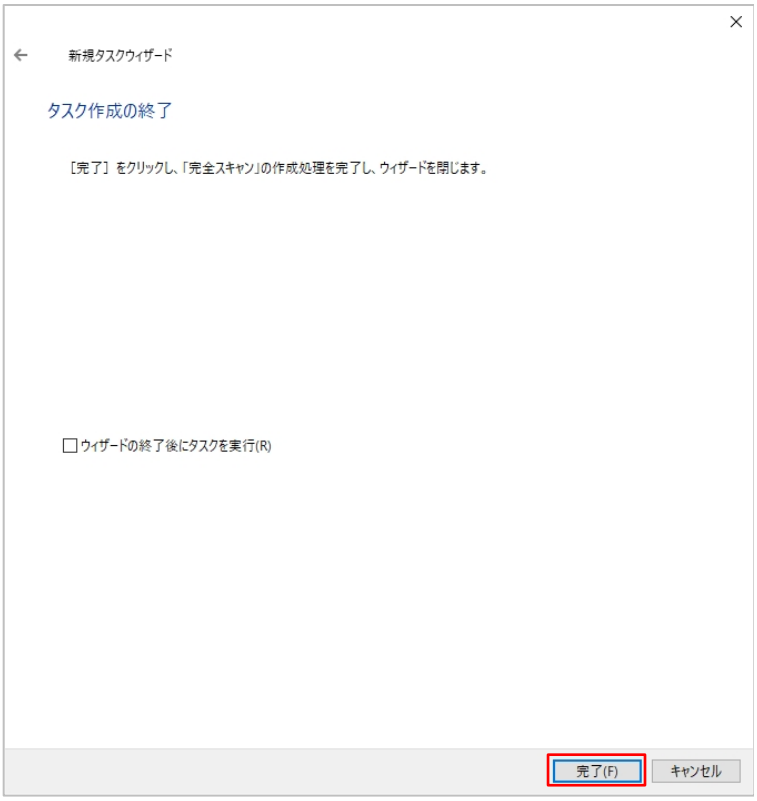
(5)「タスクを実行するアカウントの選択」画面が表示されます。
ここでは既定値のまま、「次へ」をクリックします。



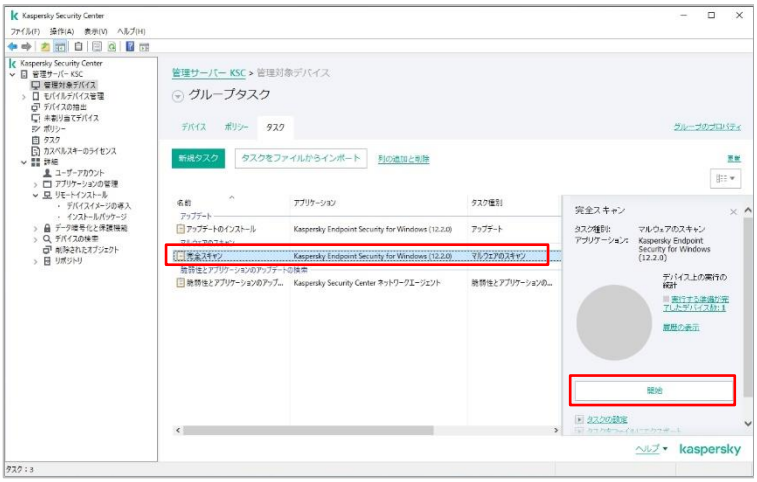
(6)「タスクスケジュールの設定」画面が表示されます。
任意の実行スケジュールを設定します。
ここでは「手動」と設定し、「次へ」をクリックします。

(7) 「タスク名の定義」画面が表示されます。
任意のタスクの名前を入力し、「次へ」をクリックします。

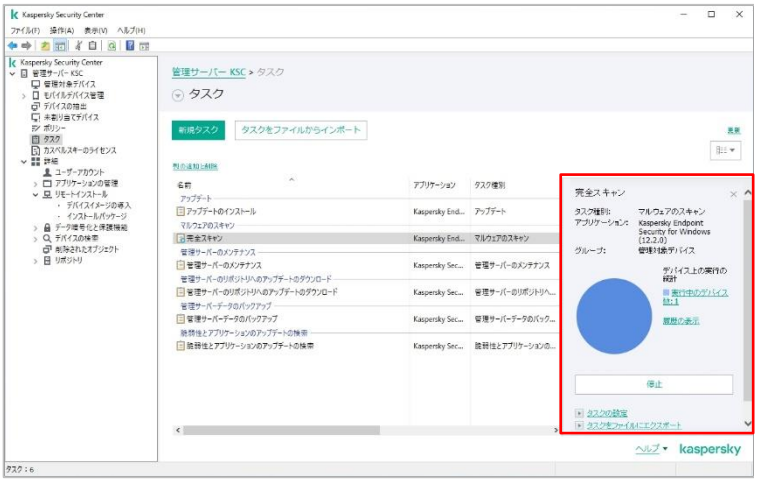
(8) 正常に作成されたことを確認し、「完了」をクリックします。



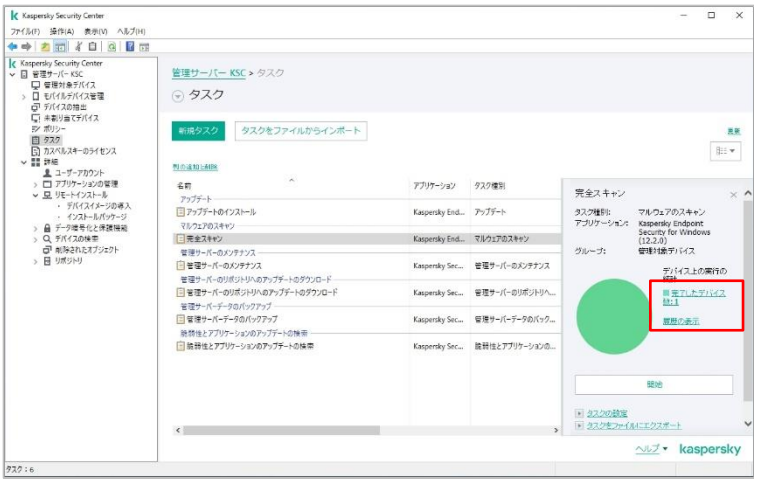
(9) 一覧に作成したタスクが表示されていることを確認します。
開始する場合、作成したスキャンタスクを選択し、「開始」ボタンをクリックします。
（もしくはタスクを右クリックし「開始」を選択します）



(10) タスクの実行状況は詳細画面にて確認することができます。



(11) タスクが完了すると、詳細画面にて「完了したデバイス数」に加算されます。
「履歴の表示」をクリックすると、各デバイス毎のステータスを確認することができます。



(12)　管理コンソールにて「管理対象デバイス」を開きます。

「デバイス」タブを開きます。

「前回の完全スキャン」列に完全スキャンタスクが最後に完了した時間が記録されています。

本章は以上です。

5.　その他

5.1.　デバイス情報の削除方法（ライセンスの解放）

契約期間中にデバイスの故障や交換など、入れ替えなどが発生した場合の設定をします。

KSCの管理下にあるデバイスが破損した、または買い換えの為に利用しなくなったデバイスがある場合、KSCはしばらくの間※1そのデバイスがまだライセンスを利用しているものとしてカウントします。

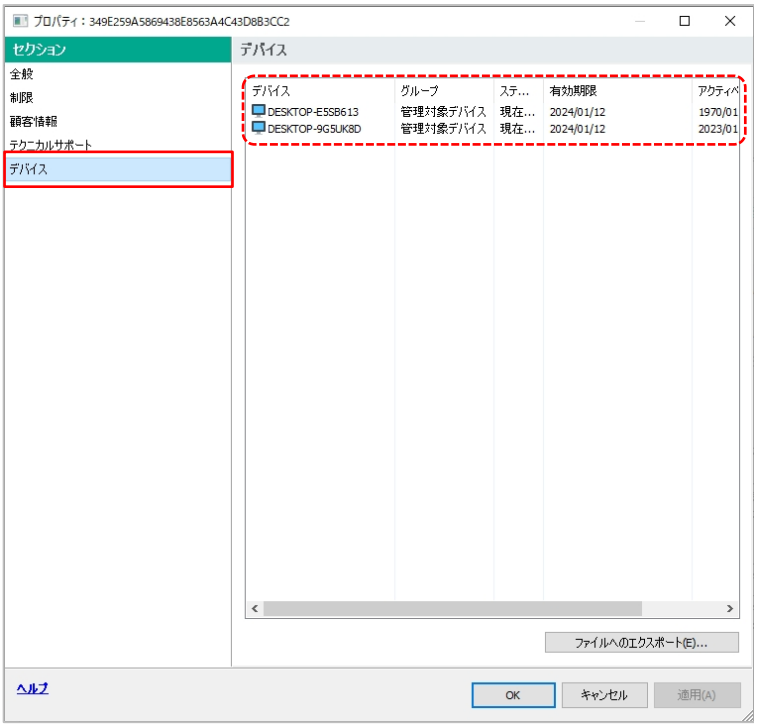
そのため、不要なデバイスが発生した場合は、KSC 上からデバイスを削除してライセンスを開放してから新しく追加するデバイスにKESとNAをインストールします。

[※1]既定では、デバイスから管理サーバーへの接続がない状態で 60 日経過すると管理サーバーの管理下から外れ、ライセンスを開放します。設定箇所は後述します。

現在のライセンスの状態は、左側のコンソールツリーにて「カスペルスキーのライセンス」で確認できます。

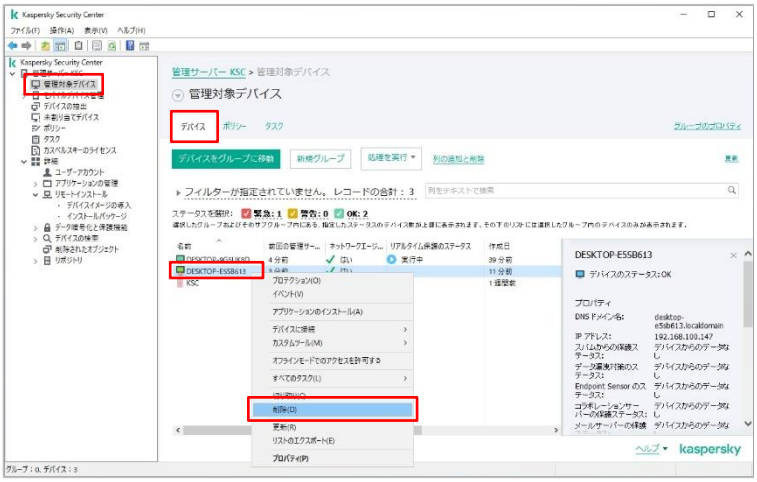
(1) 管理コンソールにて「カスペルスキーのライセンス」を開きます。
右画面にて確認したいライセンスを右クリックし、「プロパティ」を選択します。

(2) ライセンスのプロパティ画面が表示されます。
「デバイス」セクションを開くと、このライセンスが割り当てられているデバイス情報を確認することができます。



続いて、デバイスを KSC の管理から外し、ライセンスを解放するには以下の手順を実施します。

(1) 管理コンソールにてライセンスを解放したいデバイスのグループ（ここでは「管理対象デバイス」）を開きます。
「デバイス」タブを開き、該当のデバイスを右クリックして「削除」を選択します。

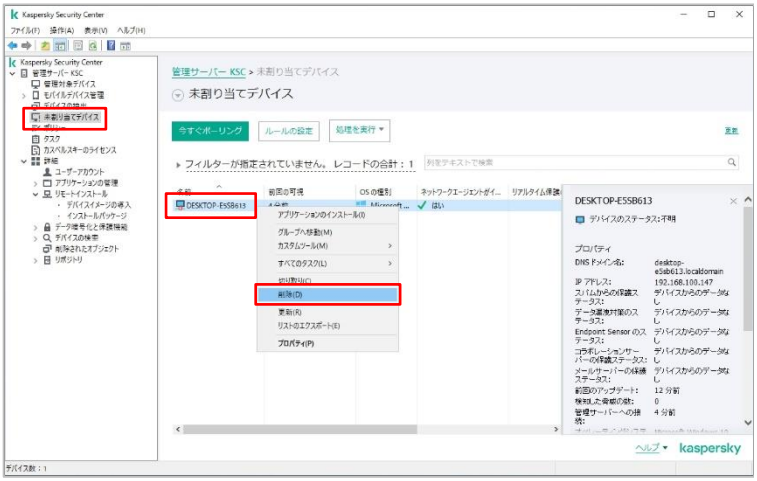


(2) 削除を確認するメッセージが表示されるので、「はい」をクリックします。

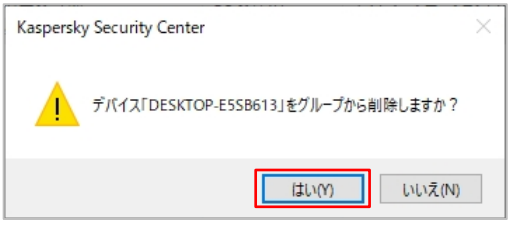
(3) グループから削除するとデバイスは「未割り当てデバイス」に移動します。

※端末の自動振り分け（資料「ポリシータスクの考え方」の「2.3 デバイスの自動振り分け」）を使用している場合、再度グループへ自動的に移動することがあります。
この場合は管理コンソールにて「未割り当てデバイス」の「プロパティ」を開き、該当する割り当てルールのチェックマークを“オフ”にして一時的に振り分けを無効にしてください。

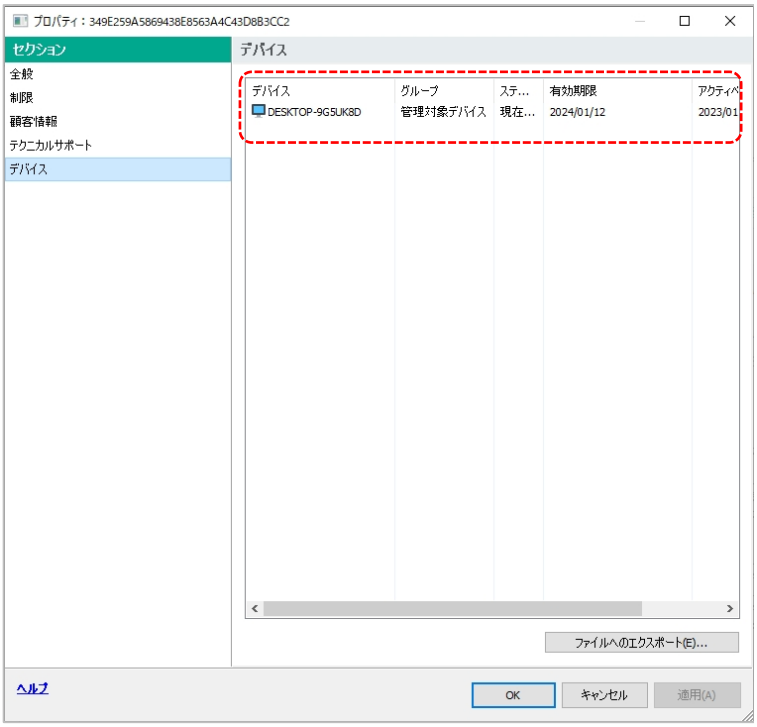
(4) 管理コンソールにて「未割り当てデバイス」を開きます。
該当のデバイスを右クリックして「削除」を選択します。



(5) 削除を確認するメッセージが表示されるので、「はい」をクリックします。
これでこのデバイス情報は KSC 上から完全に削除されます。



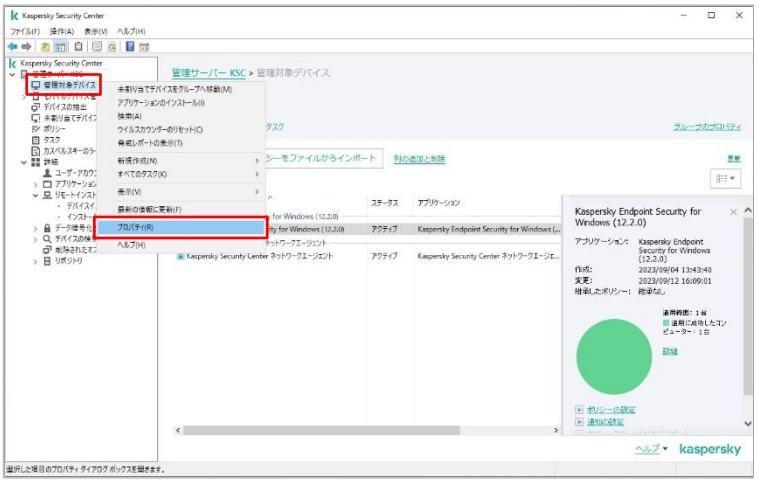
(6) 削除するとライセンスが解放されます。
ライセンスのプロパティの「デバイス」セクションにも対象のデバイスが表示されなくなります。



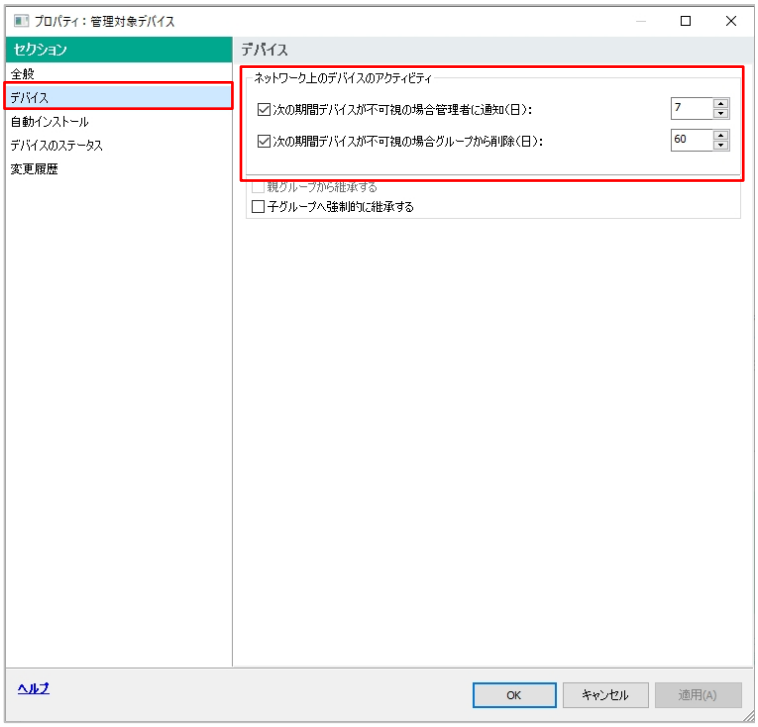
ライセンスが解放されたことを確認し、新しく追加するデバイスに KES と NA をインストールします。

既定では、デバイスから管理サーバーへの接続がない状態で 60 日経過すると、管理サーバーからデバイス情報が自動的に削除され、ライセンスも開放されます。これは管理グループに設定されています。

(1) 管理コンソールにて「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) グループのプロパティ画面が表示されます。
「デバイス」セクションを開きます。
既定では以下のように設定されています。



・次の期間デバイスが不可視の場合管理者に通知：7 日間
　通信がない状態で 7 日間経過すると管理サーバーにイベントが記録されます。

・次の期間デバイスが不可視の場合グループから削除：60 日間
　通信がない状態で 69 日間経過すると、自動的にグループからデバイスが削除されます。

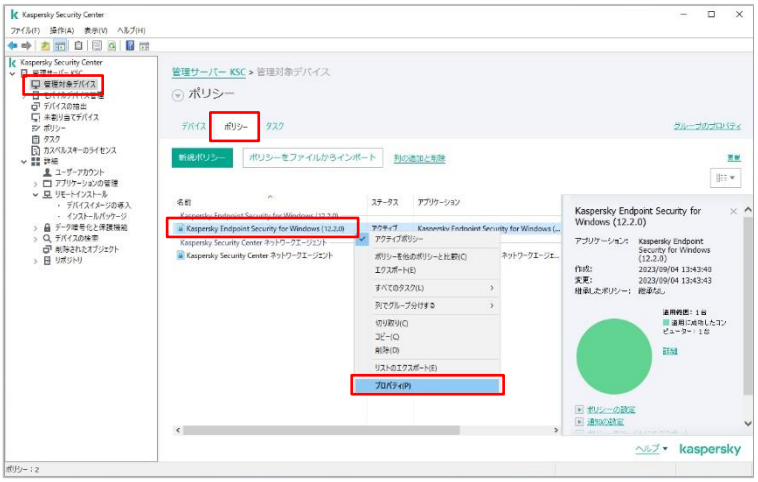
デバイスを自動で削除されないようにする場合は、「次の期間デバイスが不可視の場合グループから削除」のチェックを外し無効化します。

本節は以上です。

5.2. グループタスク開始・停止をユーザーに許可する

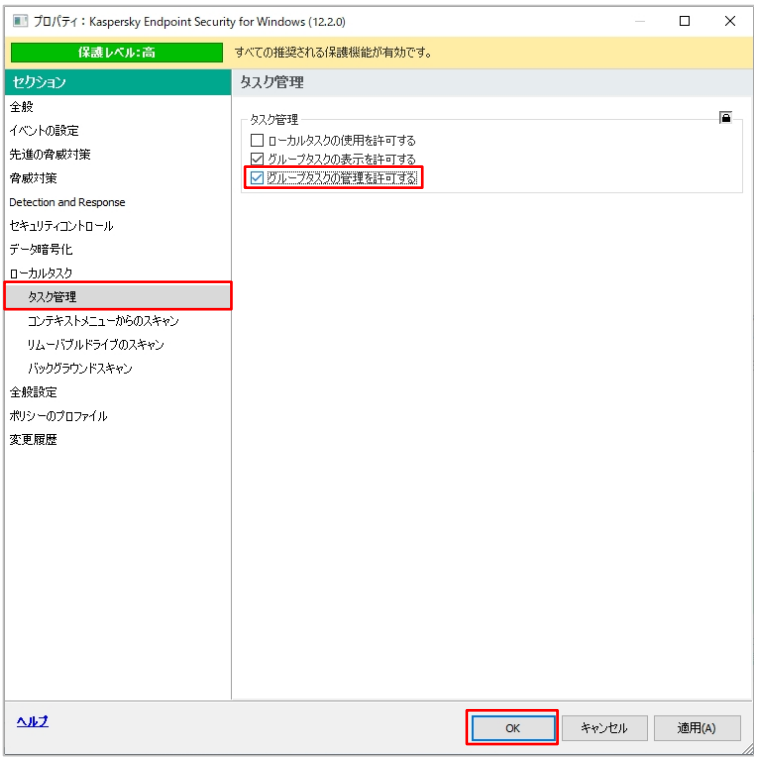
管理サーバー上で作成されたグループタスクは、既定では管理下のデバイスを使用するユーザーが開始・停止することはできません。ユーザーに操作権限を付与するには以下の設定を行います。

(1) 右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



(2) 「ローカルタスク」-「タスク管理」を開きます。
右画面にて「グループタスクの管理を許可する」にチェックを入れます。

設定後、「OK」をクリックして、設定を反映させます。



(3) 「グループタスクの管理を許可する」が無効の場合、ユーザーが KES のコンソールを開いた際に操作するボタンは表示されず、ユーザーはタスクに対し何もすることができません。

設定が有効の場合、タスクに「実行」ボタンが追加され、ユーザーは手動でタスクを開始することができます。
また開始中のタスクを「停止」ボタンにて留めることもできます。

<ユーザーに操作権限がない場合>

<ユーザーに操作権限がある場合>

本節は以上です。

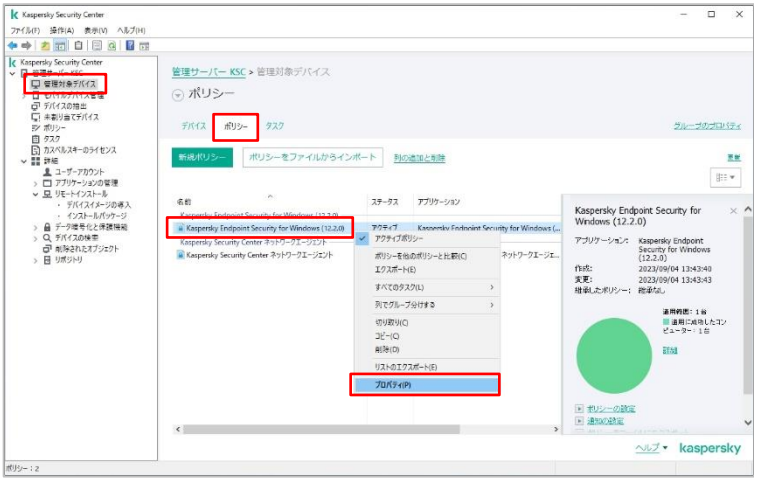
5.3. ローカルタスクの開始・停止をユーザーに許可する

ローカルタスクとは、通常 KES をスタンドアロンで使用する場合に使用するタスクです。

このタスクは管理サーバーの管理下であっても有効化することができ、ユーザーは KES 上で設定や操作することができます。

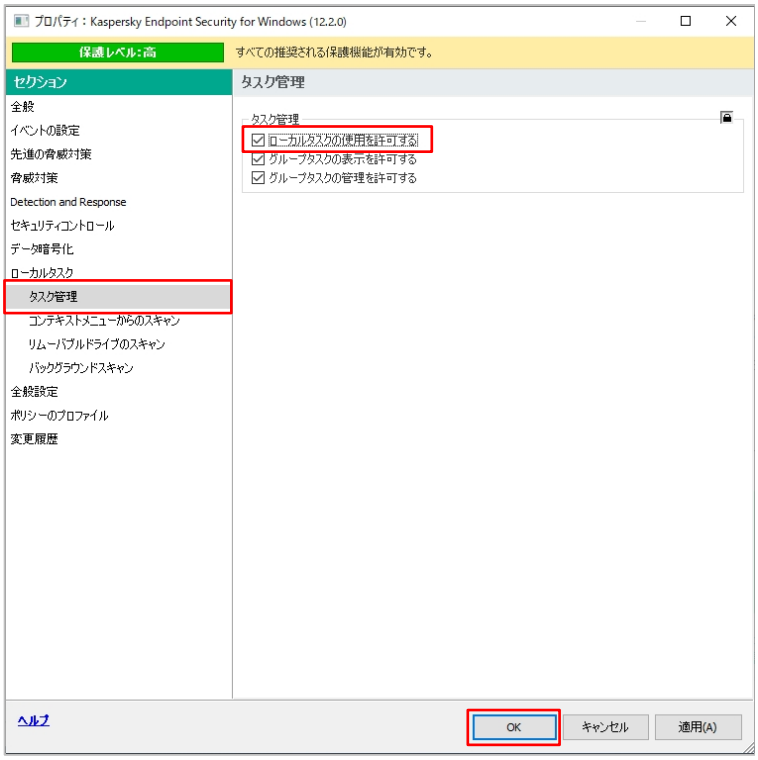
既定ではタスクは表示されておらず、ユーザーが設定・開始・停止することはできません。タスクを表示させ、ユーザーに操作権限を付与するには以下の設定を行います。

(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



(4) 「ローカルタスク」-「タスク管理」を開きます。
右画面にて「ローカルタスクの使用を許可する」にチェックを入れます。

設定後、「OK」をクリックして、設定を反映させます。



(2)「ローカルタスクの使用を許可する」が無効の場合、KES のコンソール上にはグループタスクのみ表示されています。

<ユーザーにローカルタスクの操作権限がない場合>

設定が有効の場合、グループタスクのほか、ローカルタスクも表示されローカルタスクの設定・実行・停止など操作ができるようになります。

※グループタスクとローカルタスクの両方を実行することができるため、スキャンタスクなどの実行が重複し負荷がかからないよう、設定にご注意ください。

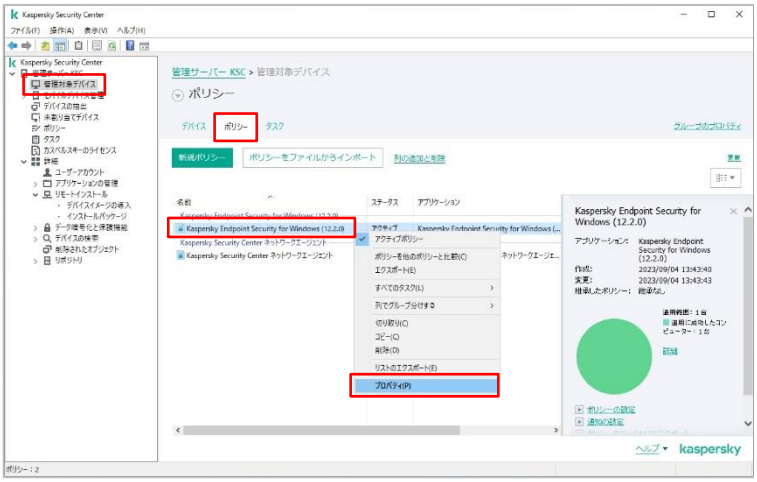
<ユーザーにローカルタスクの操作権限がある場合>

本節は以上です。

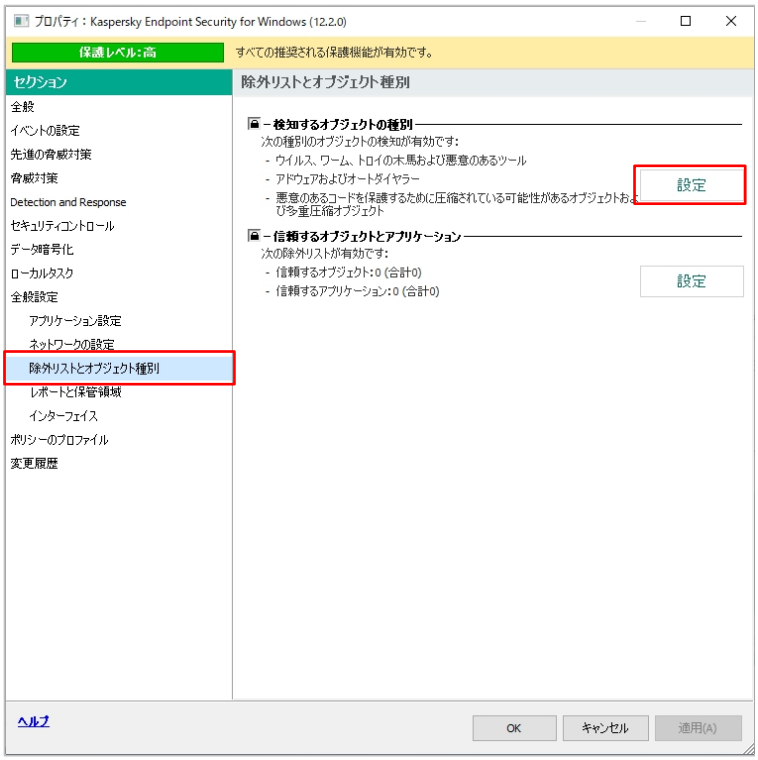
5.4.　グレーウェアを検知対象に含める

リモート接続アプリケーションなどは、それを操作する利用者によって正規なツールにも不正なツールにもなりえます。既定ではこのような**グレーウェア**のファイルを検知しません。検知するように設定するには以下のように設定します。

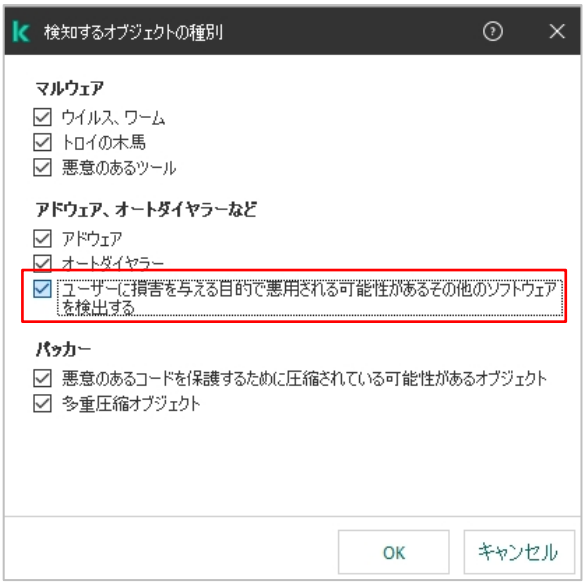
(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



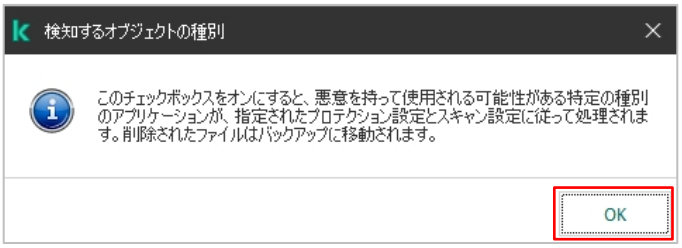
(2) 「全般設定」→「除外リストとオブジェクトの種別」を開きます。
「検知するオブジェクトの種別」の「設定」をクリックします。



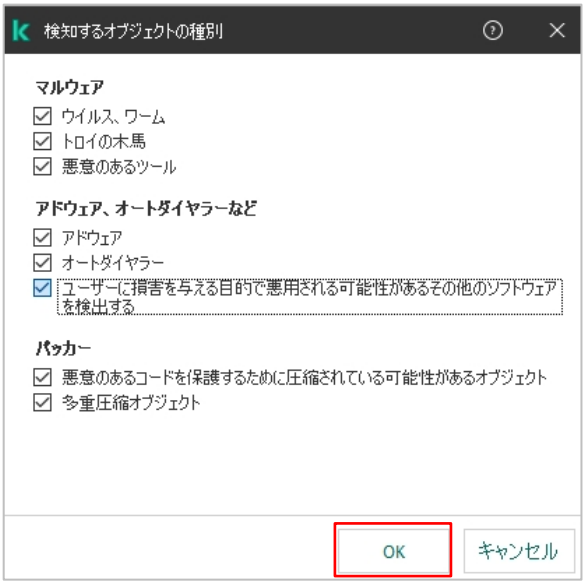
(3) 「アドウェア、オートダイヤラーなど」欄の「コンピューターや個人データに損害を与える目的で犯罪者によって悪用される可能性のあるソフトウェアを検出する」にチェックを入れます。



(4) チェックを入れると確認のメッセージが表示されますので、「OK」をクリックします。



(5) 「OK」をクリックして設定を反映させます。



本節は以上です。

5.5. Windows 共有フォルダーへのアクセスを許可する

KES をインストールしたデバイスは、既定で OS のファイアウォールが無効となり、KES のファイアウォールコンポーネントが有効となります。

KES のファイアウォールでは、以下の条件を満たすデバイス上にある Windows 共有フォルダーへのアクセスは可能です。

(1) プライベートネットワークに所属しているデバイス。（以下の IP アドレスが設定されているデバイス）

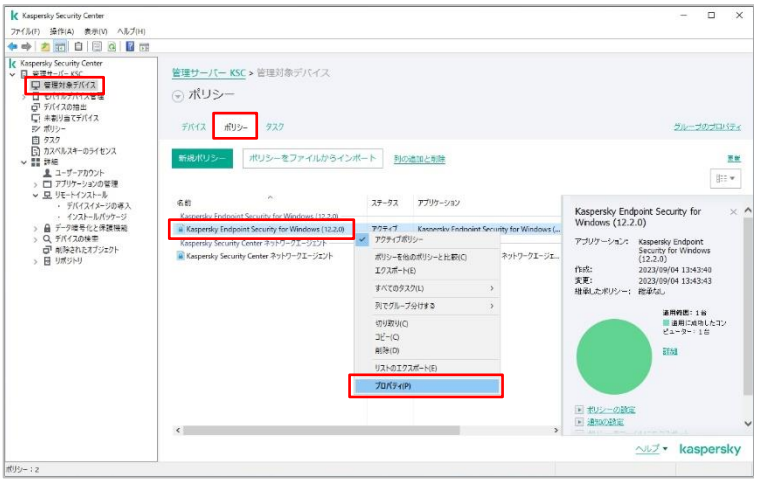
- 172.16.0.0/12
- 192.168.0.0/16
- 10.0.0.0/8

(2) KES のファイアウォールで設定した「許可するネットワーク」に所属している。

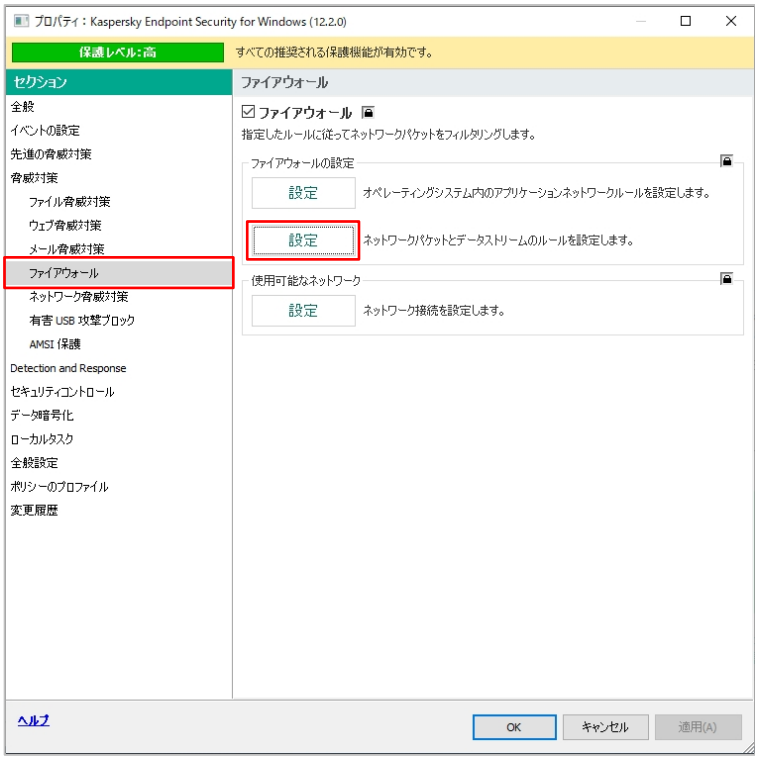
社内で使用しているクライアント PC は、(1)に該当することが多いと考えられます。

上記以外に該当するクライアント PC に対して、共有フォルダーへのアクセスを許可する場合、「3.1 ファイアウォール設定」を参照してネットワーク範囲を「許可するネットワーク(またはプライベートネットワーク)」に追加するか、以下の様にファイアウォールを設定します。

(1) 管理コンソールにて「管理対象デバイス」を開きます。
右画面にて「ポリシー」タブを開き、「KES」のポリシーを右クリックして「プロパティ」を選択します。



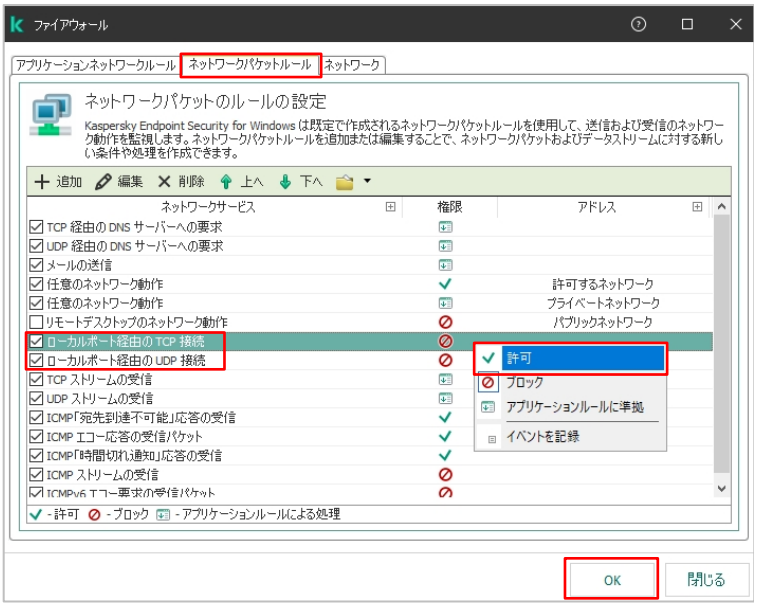
(2) 「脅威対策」-「ファイアウォール」を開きます。
「ファイアウォールルール」内の「ネットワークパケットとデータストリームのルールを設定します。」欄の「設定」をクリックします。



(3) 「ネットワークパケットルール」タブで以下の項目を右クリックして「許可」に設定します。

・ローカルポート経由の TCP 接続
・ローカルポート経由の UDP 接続

設定後、「OK」をクリックして設定を反映させます。



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

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