Kaspersky Security Center 14
Kaspersky Endpoint Security 12
ポリシー・タスクの考え方

2023/9/20

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 3
1.1. 本資料の目的 3
1.2. 導入から運用開始までの流れ 4
1.3. 前提 5
1.4. 本資料の使用方法 6
2. グループ 7
2.1. グループの作成手順 8
2.2. デバイスの移動 10
2.3. デバイスの自動振り分け 12
2.4. ディストリビューションポイント 15
3. ポリシー 16
3.1. ポリシー表示 17
3.2. ロック機能 20
3.3. 保護レベル確認 22
3.4. グループポリシー 26
3.5. ポリシーの新規作成 27
3.6. ポリシーのステータス 34
3.7. ポリシーの強制的な継承 35
3.7.1. 親グループのポリシーで「設定を子ポリシーへ強制的に継承させる」をオフにする 36
3.7.2. サブグループのポリシーで「上位ポリシーから設定を継承する」をオフにする 38
3.8. モバイルユーザーポリシー 40
4. タスク 41
4.1. タスクの表示 42
4.2. グループタスク 45
4.3. グループタスクの新規作成 46
4.4. タスクの強制的な継承 51
4.5. タスク範囲からの除外 52
4.6. 特定のコンピューターに対するタスク 56

1. はじめに

1.1. 本資料の目的

Kaspersky Endpoint Security for Business は、デバイスやファイルサーバー、モバイルデバイスなどセキュリティを幅広く効率的に一元管理するためのシステムです。

各デバイス（Endpoint）は Kaspersky Endpoint Security（以下 KES）によって保護され、全体を Kaspersky Security Center（以下 KSC)で管理します。

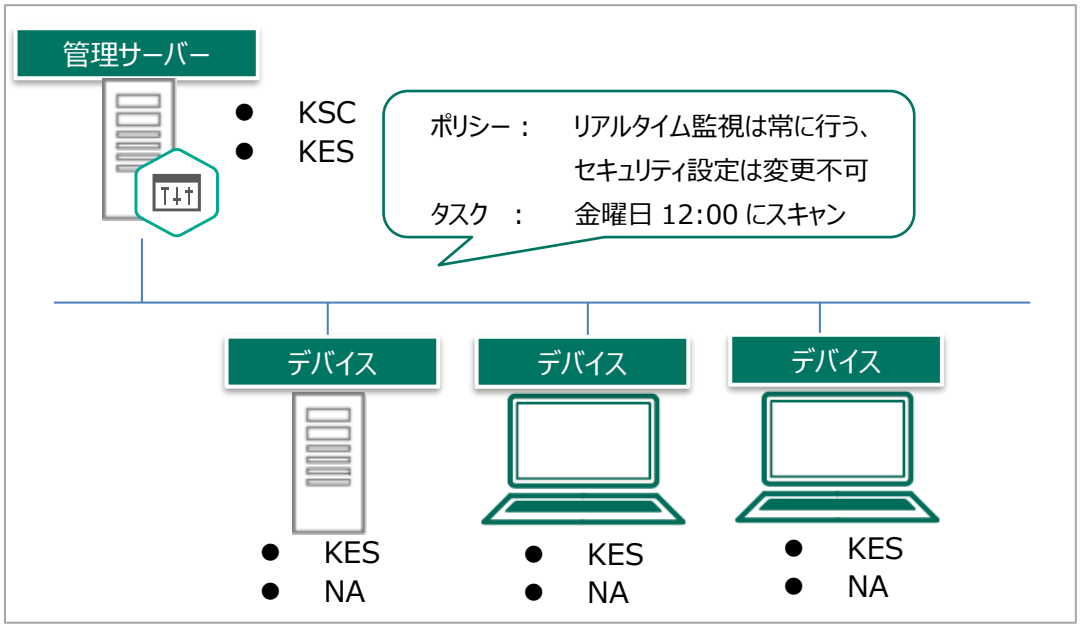
KES と KSC の間はネットワークエージェント（以下 NA）で通信します。

デバイスの管理は「**ポリシー**」と「**タスク**」の組み合わせで行います。

「**ポリシー**」とは、KES の各種機能をどのように適用させるかのルールで、普段デバイスをどのように保護するかを決定します。

「**タスク**」では、アップデートやスキャンなど、手動やスケジュールに沿って定期的に実行する必要のある作業を設定します。

ポリシーは常時動いている設定、タスクはスケジュール（または手動）で実行する設定とお考えください。



この「ポリシー」と「タスク」を適切に設定することで、ネットワーク環境やデバイス性能に応じた、より効率的な運用が可能となります。

本資料では、Kaspersky Endpoint Security for Business におけるポリシー、およびタスクを設定する際の基本的な考え方と、目的別の設定方法をご説明します。

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

→ **「KSC 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

→ **本資料および「ポリシータスク設定 実践編」を参照し、各種設定を実施してください。**

STEP 4.

運用開始前に必要な設定の実施

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

STEP 5.

運用開始

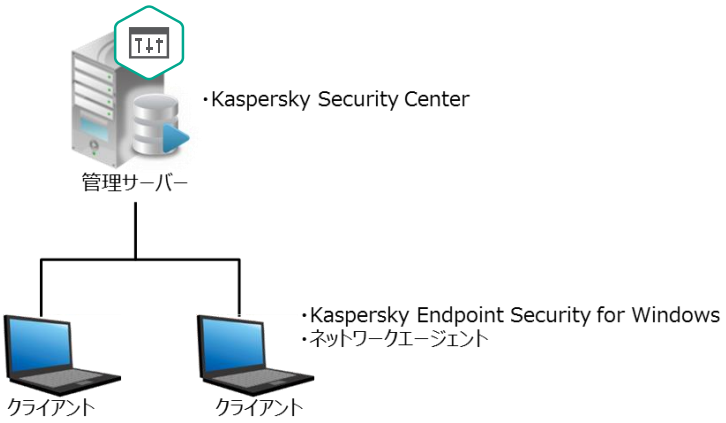
→ **「Kaspersky 運用ガイド」**を参照し、各手順に従い運用してください。

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. 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 とネットワークエージェントが導入されている。
- ✓ 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 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。
  (本資料で使用するのはバージョン 14 です)

- **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コンピューターにインストールされます。
  (本資料で使用するのはバージョン 12 です)

- **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。
  管理下のコンピューター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）

1.4.　本資料の使用方法

本資料は、製品インストール後に基本的な設定を行うために必要な情報について記載しております。
以下のように、運用目的に合わせ該当する説明項目をご参照ください。

拠点や部署ごとに管理グループを作成し、グループ毎にデバイスを管理したい。
⇒「**2. グループ**」を参照

管理下にあるデバイスのアプリケーション設定を一元管理したい。
⇒「**3. ポリシー**」を参照

スキャンやアップデートなどスケジュールを設定して実行したい。
⇒「**4.タスク**」を参照

本資料に記載した以外にも、多くの設定項目がございます。実現したいことがある場合や、設定項目がわからない場合は、カスペルスキーまでお問い合わせください。

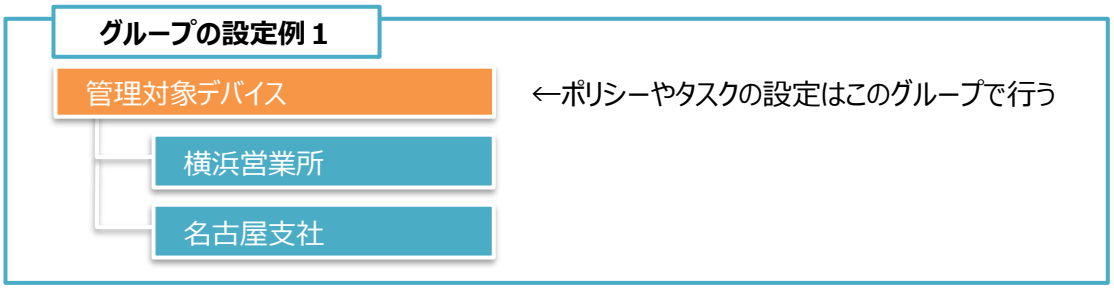
2. グループ

タスクとポリシーは、基本的に「**グループ**」の単位で設定します。

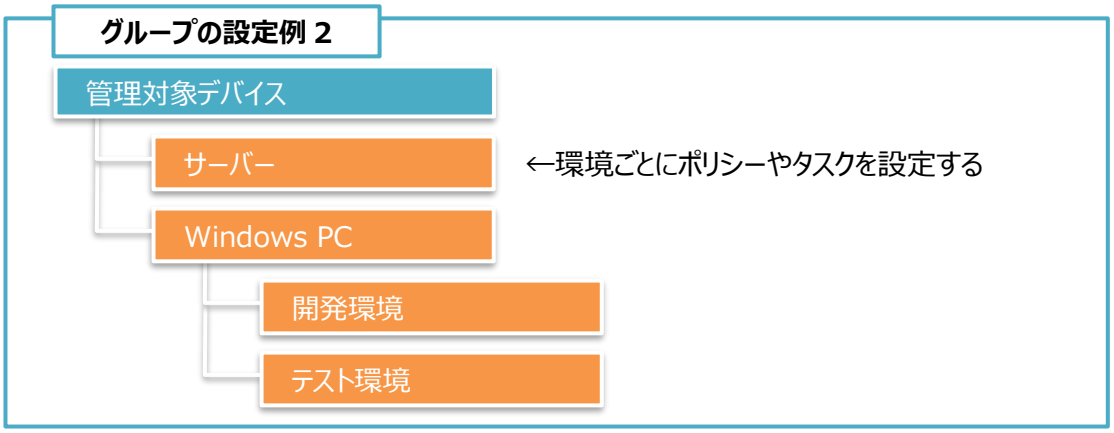
グループを作成し、そのグループにデバイス（エンドポイント）を割り当てることで、グループに属するデバイスをまとめて管理できます。各デバイスが所属できるのはいずれか 1 つのグループで、複数のグループに所属することはできません。

既定では「**管理対象デバイス**」グループのみが作成されています。これは、KES で管理するすべてのデバイスが所属するグループです。部門別、あるいは目的別などの新しいグループを作る際は、この「管理対象デバイス」のサブグループとして作成します。また、サブグループの下にさらにサブグループを作成することも可能です。

原則として、サブグループには親グループのポリシーやタスクの設定が引き継がれます。これを「**継承**」と言います。したがって、「管理対象デバイス」で設定したポリシーやタスクはサブグループに継承されます。
ドメインは異なるが運用は同じという場合、親グループで設定すると全体で統一された管理を行うことができます。



グループごとに設定することで、OS の種類やデバイスの用途ごとに管理を変えることもできます。



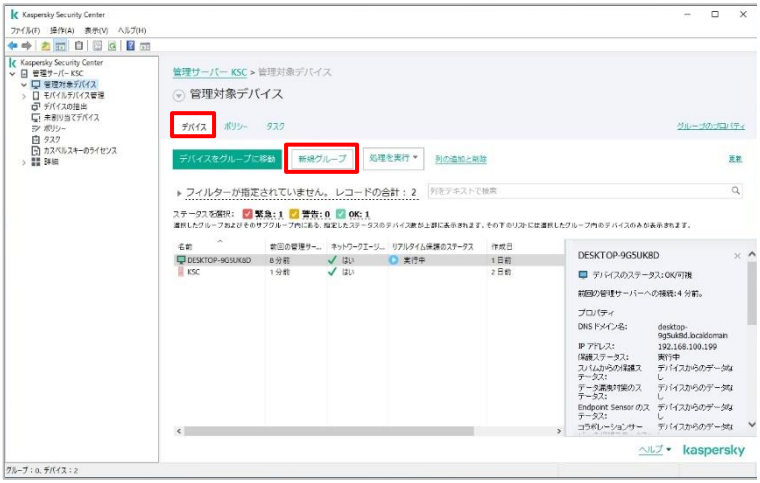
なお、臨時で普段と異なる処理を行いたい場合は「特定のコンピューターに対するタスク」で設定します。特定のコンピューターに対するタスクの場合、他のグループに所属しているデバイスでもまとめてタスクを実行させることができます（⇒「4.6. 特定のコンピューターに対するタスク」）。

2.1.　グループの作成手順

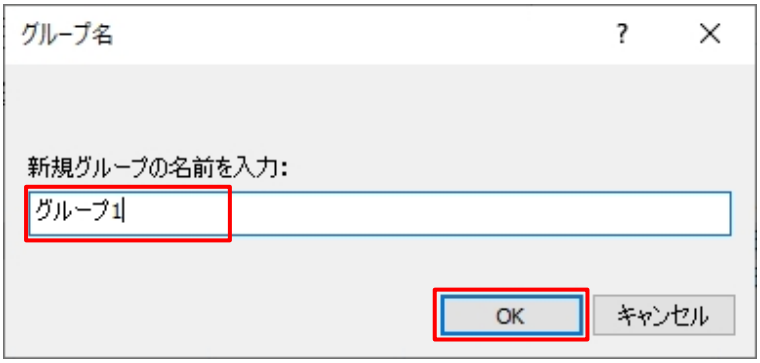
グループは以下の手順で作成します。

(1) KSC の管理コンソールを開きます。
左画面にて親となるグループを選択します。まだグループが存在しない場合は「管理対象デバイス」を選択します。

(2) 右画面にて「デバイス」タブを選び、「新規グループ」をクリックします。



(3) 「グループ名」画面が開きます。
グループ名を入力し「OK」をクリックします。



(4)「管理対象デバイス」配下に作成したグループが追加されたことを確認します。

本節は以上です。

2.2.　デバイスの移動

グループ作成後、グループに所属させるデバイスを移動する方法をご説明します。

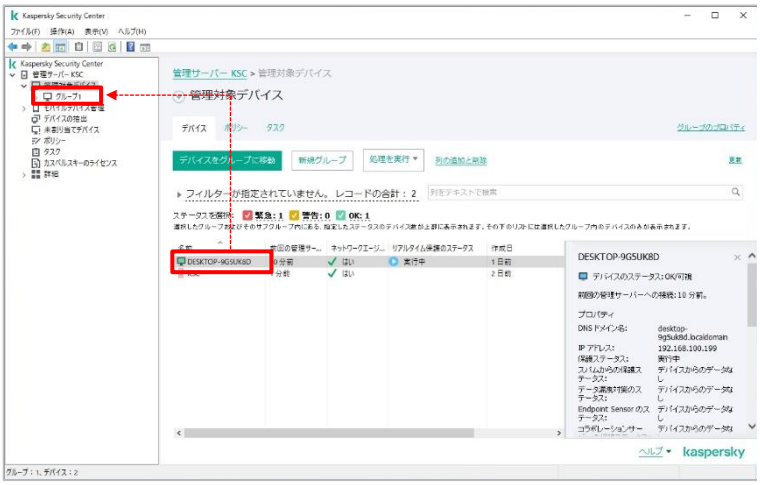
ここでは、デバイスを「管理対象デバイス」から「グループ 1」へ移動します。

(1) 左画面にて移動元のグループ（今回は「管理対象デバイス」）を選択します。

(2) 右画面にて「デバイス」タブを開きます。

(3) 一覧から移動させるデバイスを選択し、移動先のグループ（今回は「グループ 1」）までドラッグ＆ドロップします。

※Ctrl もしくは Shift キーを押しながら選ぶことで複数デバイスを選択できます。



(4) 「グループ 1」を開き、デバイスが移動されていることを確認します。

※また「デバイスをグループに移動」ボタンを使用することでもウィザードにてデバイスを移動することが可能です。

本節は以上です。

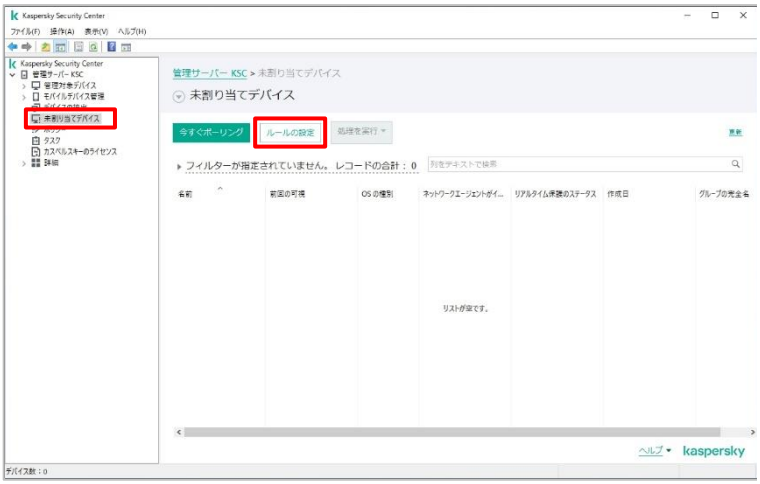
2.3. デバイスの自動振り分け

「未割り当てデバイス」のプロパティを利用することで、グループに割り当て済のデバイスも含めたすべてのデバイスを条件に応じてグループに自動振り分けすることが可能です。

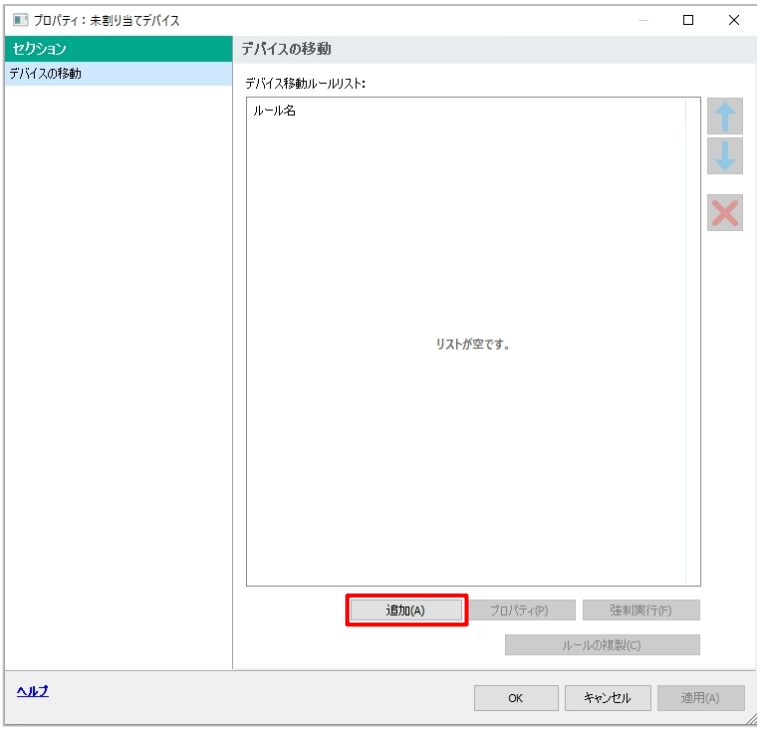
自動振り分けには、デバイス名、OS の種類やバージョン、ドメイン名、IP アドレスの範囲、Active Directory グループ等を指定できます。この設定により、デバイスが追加されたら自動で部門ごとのグループに振り分ける、自動で OS ごとのグループに振り分ける、といった運用ができます。

ここでは、“Windows10 のデバイスを「Windows10」というグループに振り分ける”ルールを設定します。

(1) 左画面にて「未割り当てデバイス」を選択します。
右画面にて「ルールの設定」をクリックします。

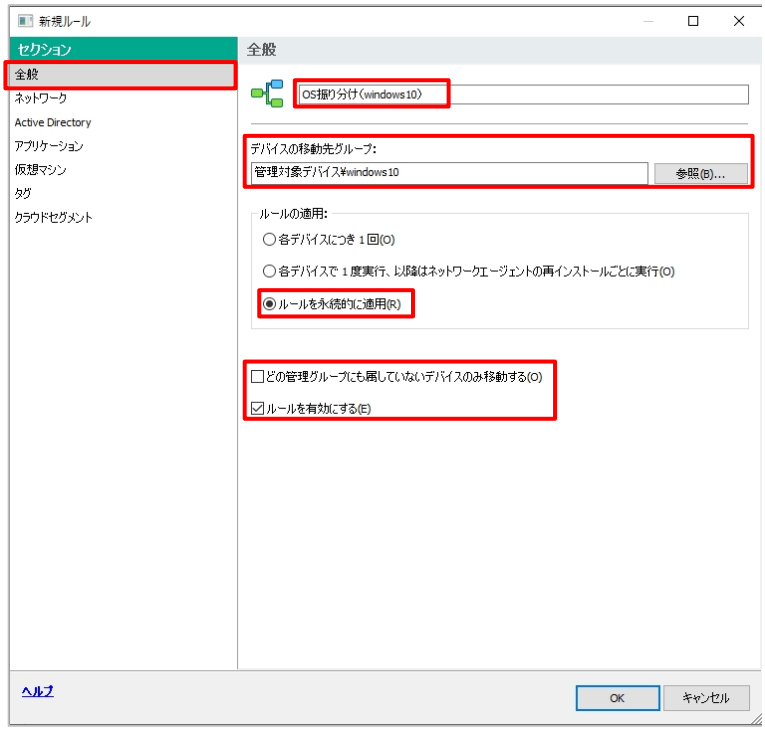


(2) 未割り当てデバイスのプロパティ画面が開きます。
「デバイスの移動」セクションで「追加」をクリックします。



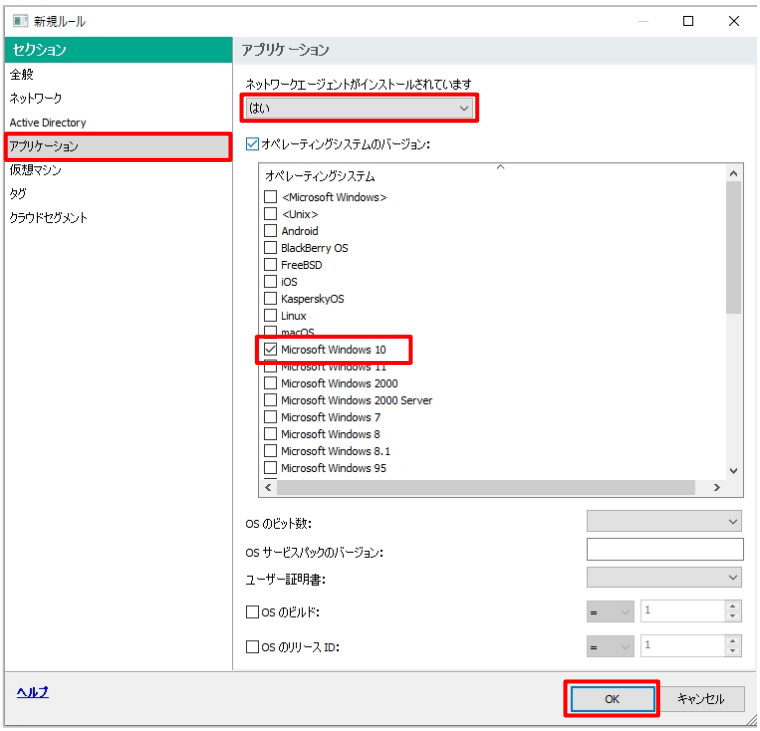
(3) 「新規ルール」画面が開きます。
「全般」セクションにて以下の通り設定します。

- 振り分けルールの名前
- 「デバイスの移動先グループ」：「参照」をクリックし、移動先のグループを選択
- 「ルールの適用」：「ルールを永続的に適用」
- 「どのグループにも属していないデバイスのみ移動する」のチェックを外す
- 「ルールを有効にする」にチェックを入れる



(4) 「アプリケーション」セクションにて以下のように設定し、「OK」をクリックします。

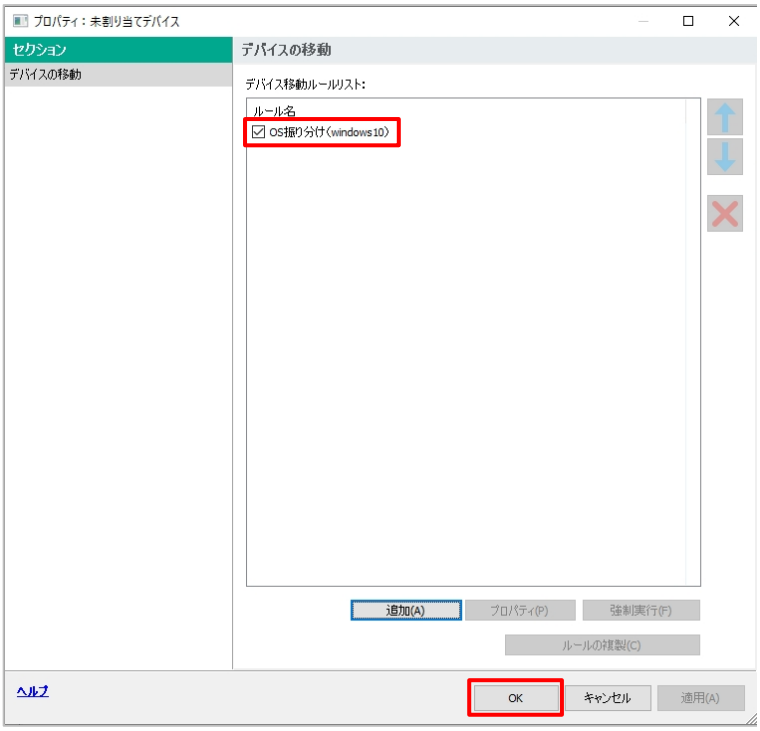
- 「ネットワークエージェントがインストール済み」：はい
- オペレーティングシステムのバージョン：「Microsoft Windows 10」にチェックを入れる
-



(5) プロパティに新しいルールが追加されたのを確認し、「OK」をクリックします。

これで、管理下にある Windows 10 が動作しているデバイスは「Windows10」グループに自動的に振り分けられるようになります。

ルールは複数作成することができます。上から順番に適用され該当したルールに従いグループへ移動します。



本節は以上です。

2.4. ディストリビューションポイント

管理下にある任意のデバイスを「**ディストリビューションポイント**」として役割を割り当てることができます。

ディストリビューションポイントは、管理サーバーから定義データベース情報やインストーラーを受け取り、他のデバイスに提供します。

ディストリビューションポイントを設けることで、管理サーバーへのトラフィックの集中やネットワークの負荷を下げることができます。

設定手順や詳細は、以下サイトの「**ディストリビューションポイント設定ガイド**」をご参照ください。

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

本章は以上です。

3. ポリシー

Kaspersky Endpoint Security for Business では、アプリケーションごとに「**ポリシー**」を設定して運用します。
ポリシーを設定することで、KSC の管理下にあるデバイスの設定を一元管理することができます。

ポリシーはアプリケーション毎に作成する必要があります。（KES for Windows, KES for Linux など）
一つのアプリケーションに適用することができるポリシーは一つのみであり、複数のポリシーを有効にして適用することはできません。

ポリシーは最上位グループである「管理対象デバイス」に作成されたものが下位のグループにも継承されて適用されます。また、グループ毎にポリシーを作成することができ、グループ毎に設定を変更することもできます。

ポリシーの設定例として、アプリケーション「Kaspersky Endpoint Security（KES）」の「社内 PC 用ポリシー」を作成した場合、以下の様な設定が可能です。

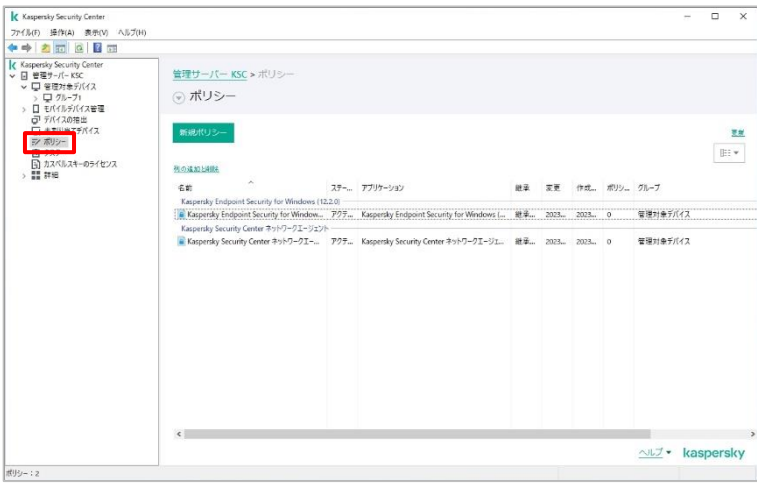
- ファイル・メール・Web の脅威対策を有効にする
- CD/DVD ドライブの使用は可能だが、USB メモリの使用は禁止する
- フォルダー「C:¥test¥」配下のファイルは検知対象外とする。

今後、社内 PC 運用の方針が変わった場合や設定変更する必要がある場合、「社内 PC 用ポリシー」の設定を変更することで、社内 PC 用ポリシーが適用されているすべてのデバイスに対し設定が適用されます。

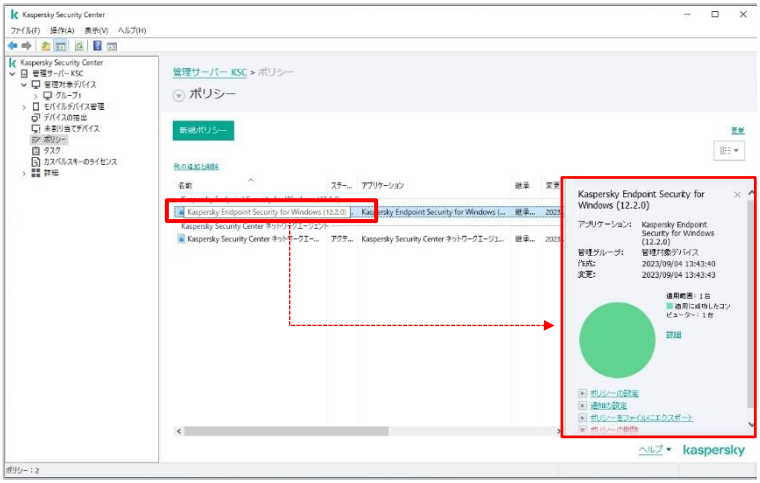
KSC をインストールし「初期設定ウィザード」を実行すると、「管理対象デバイス」グループ用に KES およびネットワークエージェントのポリシーが自動作成されます。

3.1. ポリシー表示

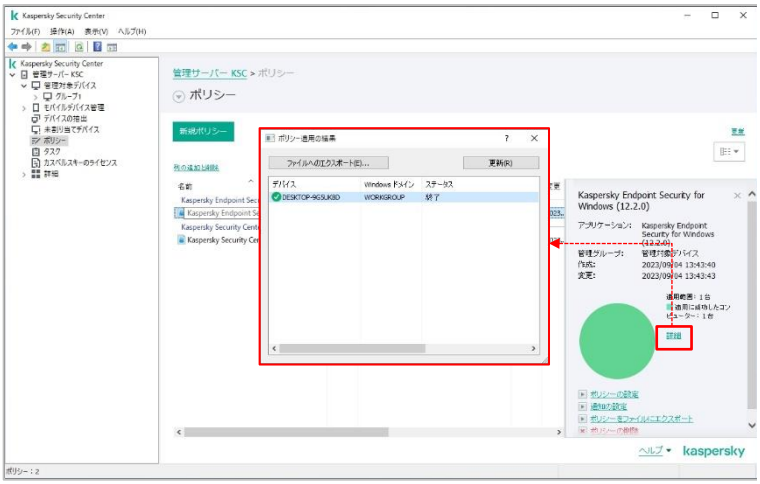
(1) KSC の管理コンソールを開きます。
「ポリシー」を選択すると、右画面に現在定義されているポリシーの一覧が表示されます。



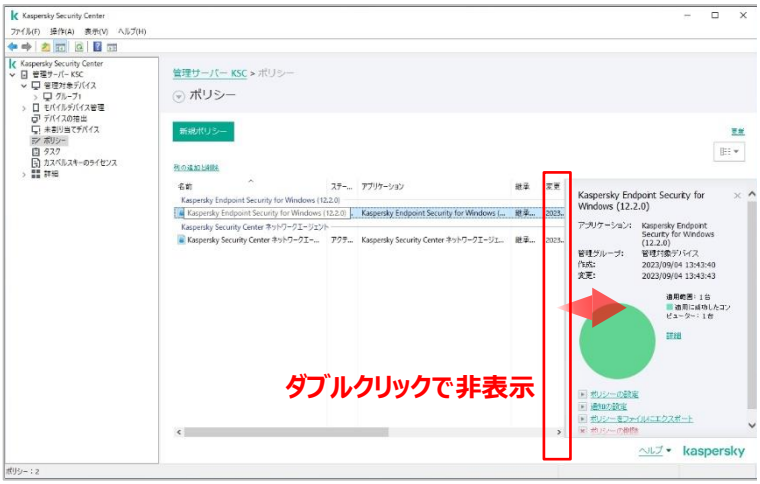
(2) ポリシーを選択すると詳細画面が表示されます。
そのポリシーが適用されているデバイスの台数や、適用の状況が表示されます。



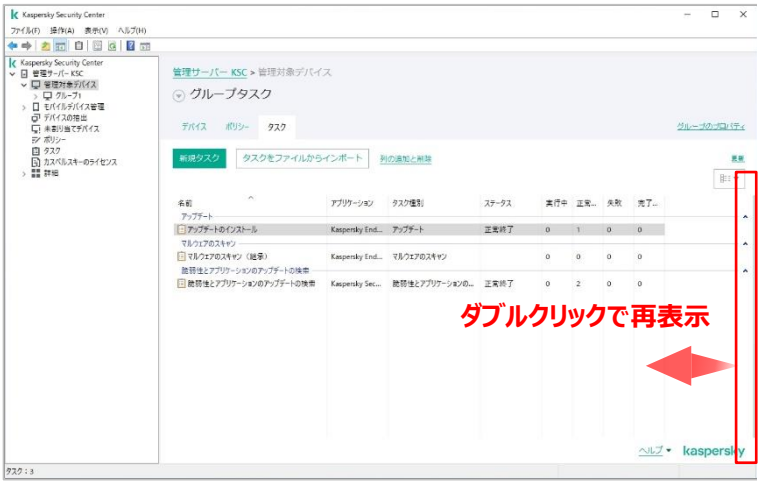
(3) ここで、「詳細」をクリックすると、そのポリシーがどのデバイスに適用されているかを確認することができます。
（ステータスに「終了」と表示されていればポリシーが適用されています）



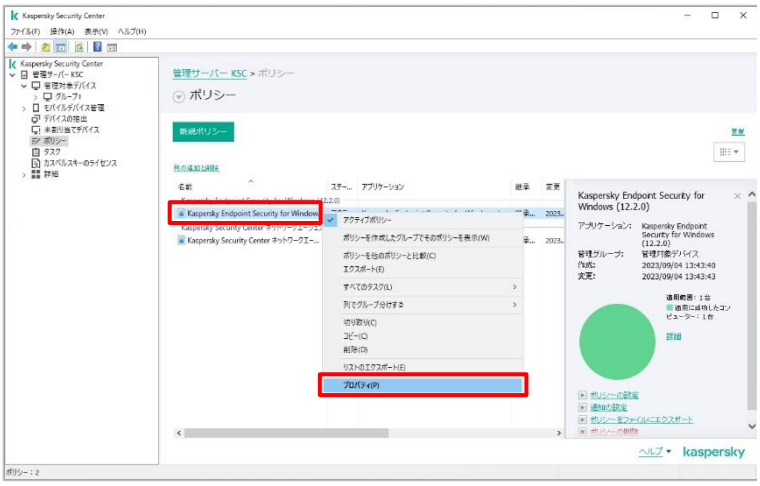
(4) 詳細画面の境界線付近をダブルクリックすると画面が閉じます。



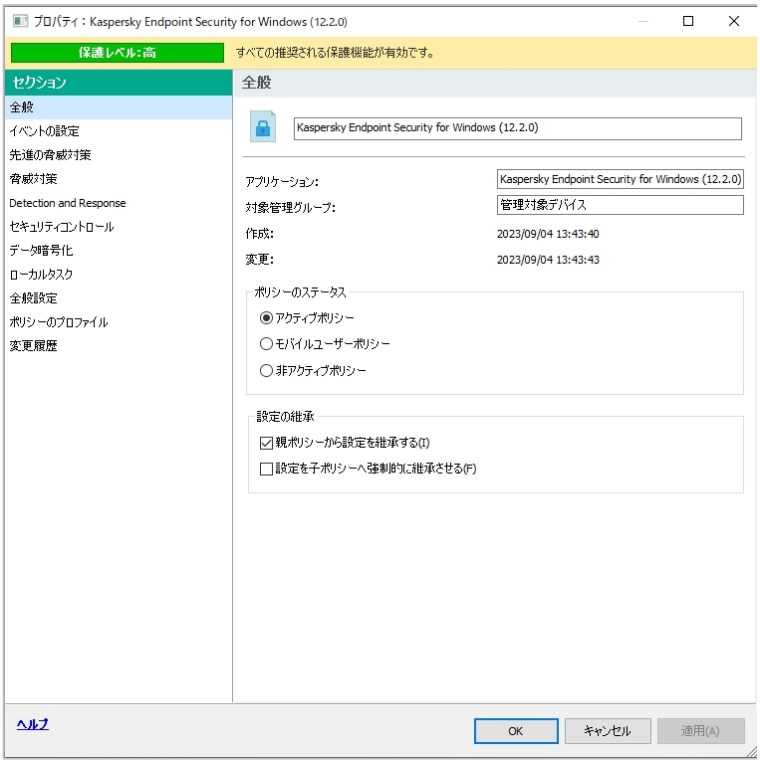
(5) 閉じた状態のとき、右端をダブルクリックすると詳細表示が戻ります。



(6) ポリシーを右クリックして「プロパティ」を選択、またはダブルクリックすることでプロパティが表示されます。



(7) プロパティ画面ではポリシーの設定内容を変更することが可能です。



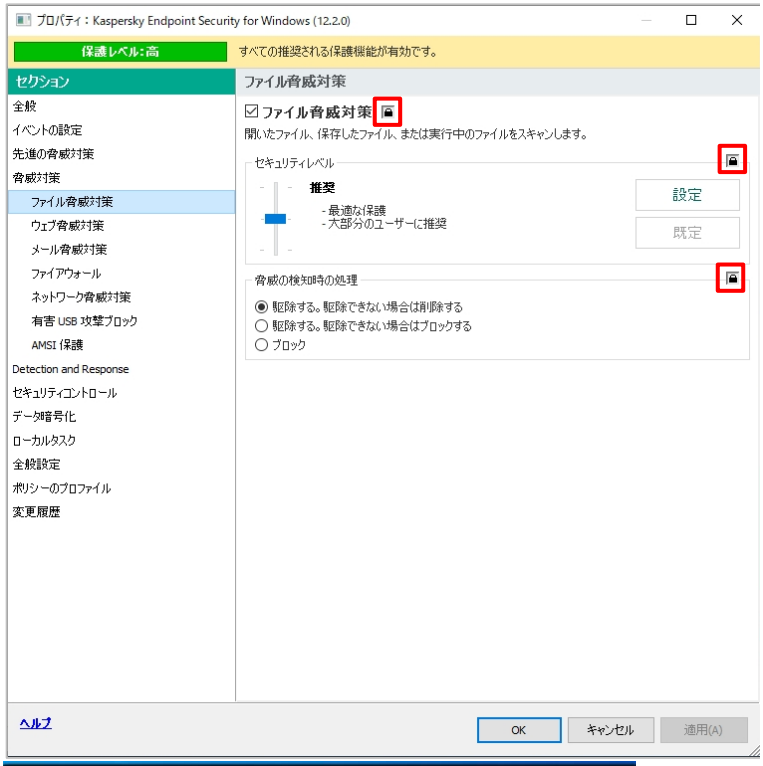
本節は以上です。

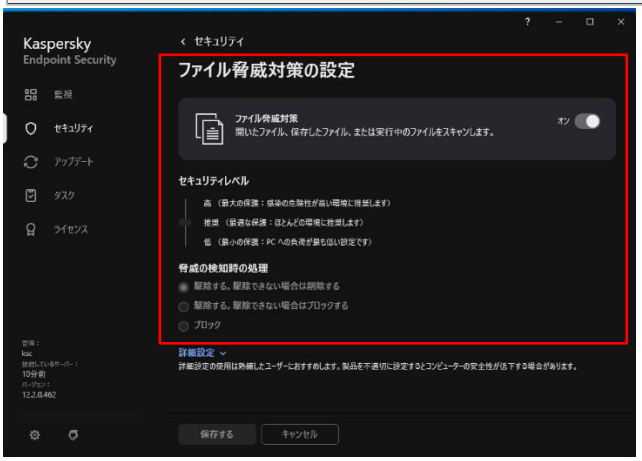
3.2. ロック機能

ポリシーの各項目には鍵マークがついています。ロック状態（ ）の場合、このポリシーが適用されているデバイスは設定を変更することができません。既定ではすべての設定がロックの状態となっています。

(1) デバイス側でのポリシー設定を制限する場合、鍵マークをクリックして閉じた状態（ ）に変更し、設定をロックします。

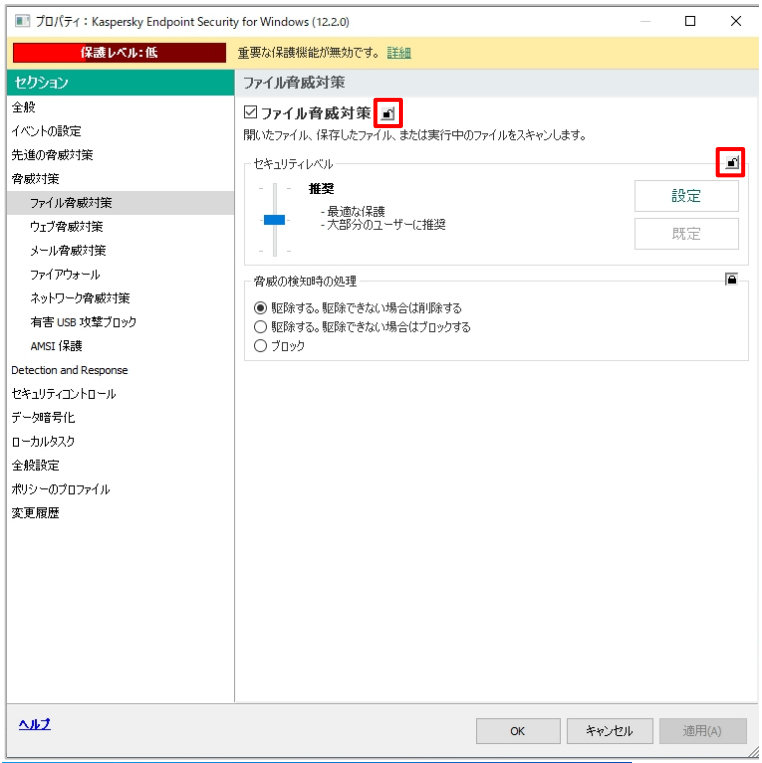
ロックを設定することで、デバイス側では該当の設定はグレーアウトされ変更することはできません。

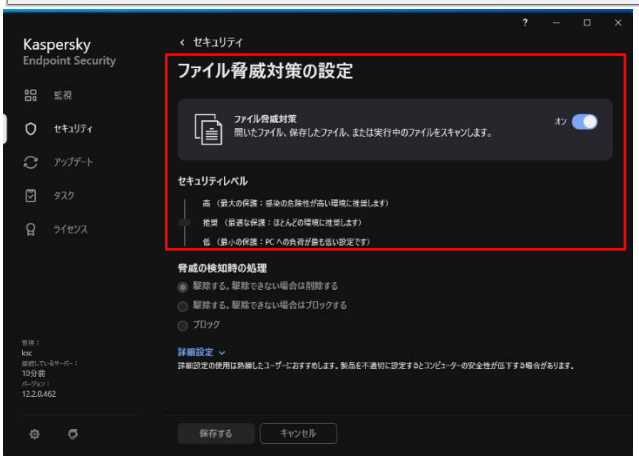




(2) デバイス側でポリシー設定を変更できるようにする場合、鍵マークをクリックして開いた状態( )に変更し、ロックを解除します。

ロックを解除することで、デバイス側では設定のグレーアウトが解除され、設定変更が可能となります。





本節は以上です。

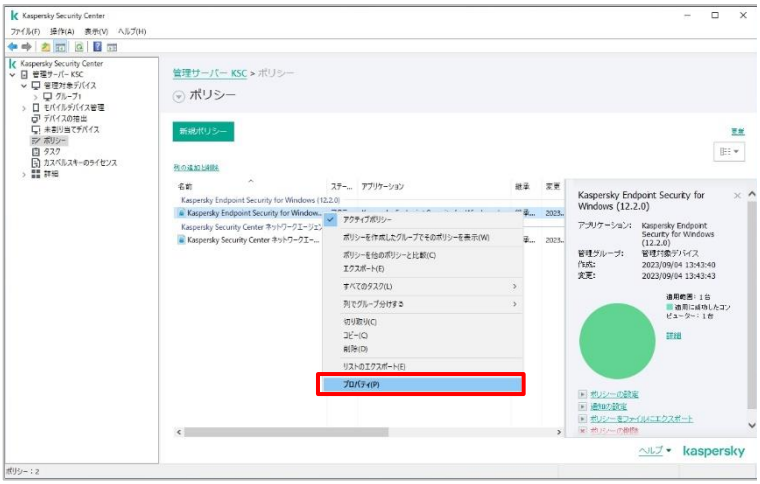
3.3.　保護レベル確認

KES のポリシーにてファイル脅威対策などの機能を無効にすると保護レベルが下がります。各保護レベルの説明は、それぞれ以下の通りです。

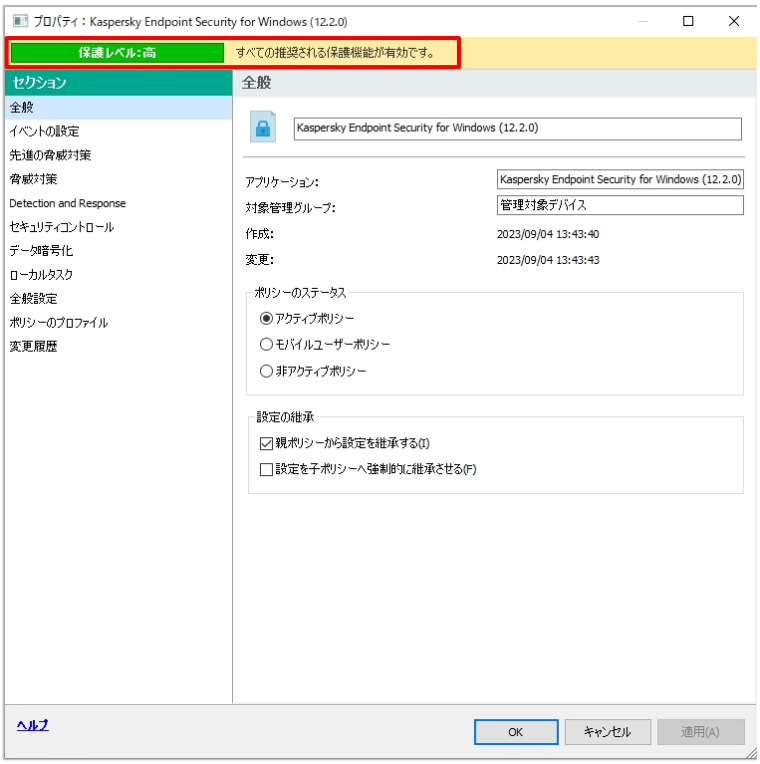
保護レベル：高　→　（ファイアウォール等を除いた）すべての主要なセキュリティ機能が有効となっている
保護レベル：中　→　メール脅威対策やウェブ脅威対策等の機能が 1 つ無効となっている
保護レベル：低　→　ファイル脅威対策、ふるまい検知等の重要な機能が無効となっている

トラブル時の切り分けを行う場合を除いて、基本的には保護レベルが「高」の状態になるよう設定してください。保護レベルの確認手順は以下の通りとなります。

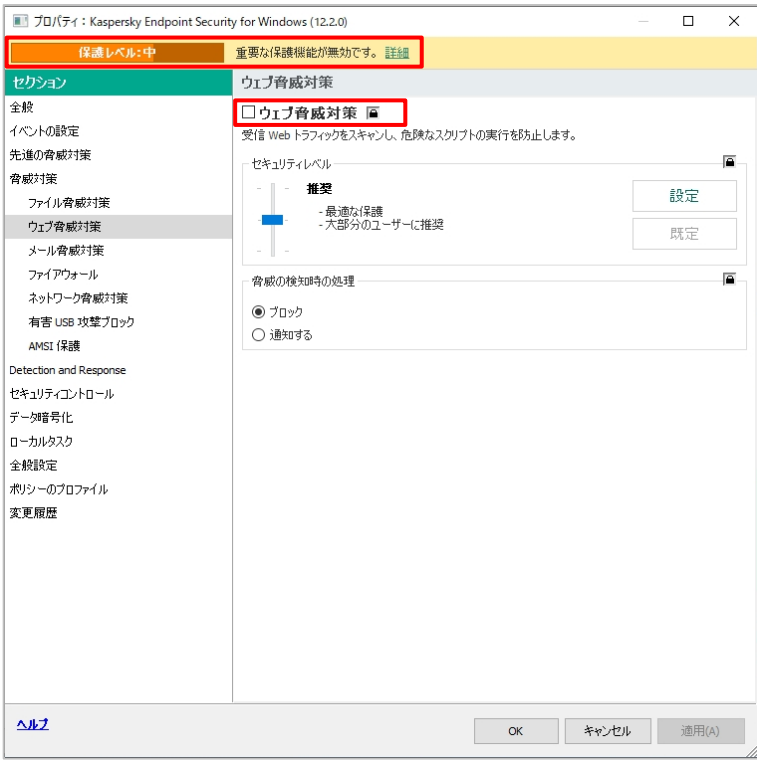
(1) 「ポリシー」にて「KES」のポリシーのプロパティを開きます。



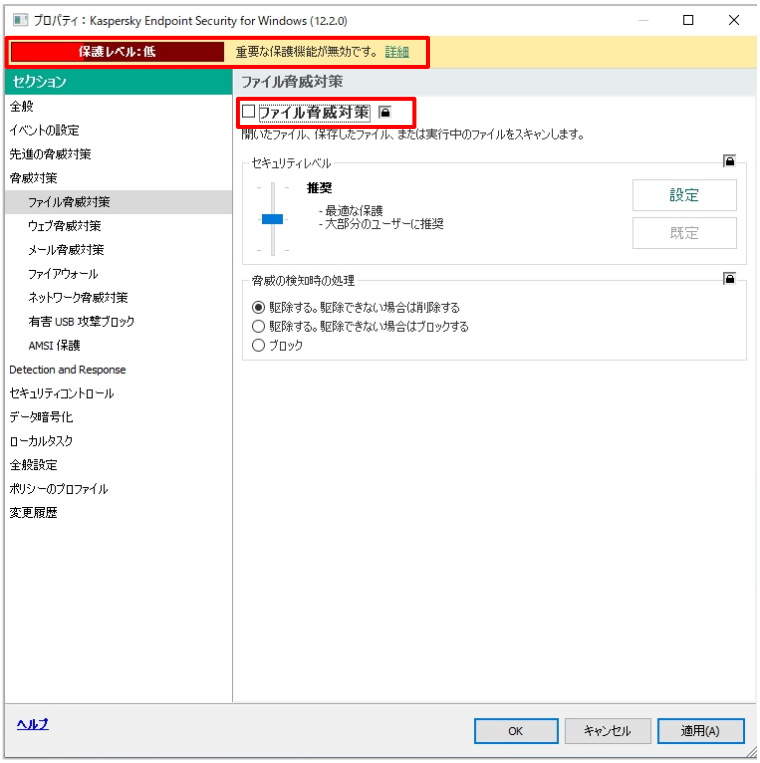
(2) 既定値では、「保護レベル：高」となっています。



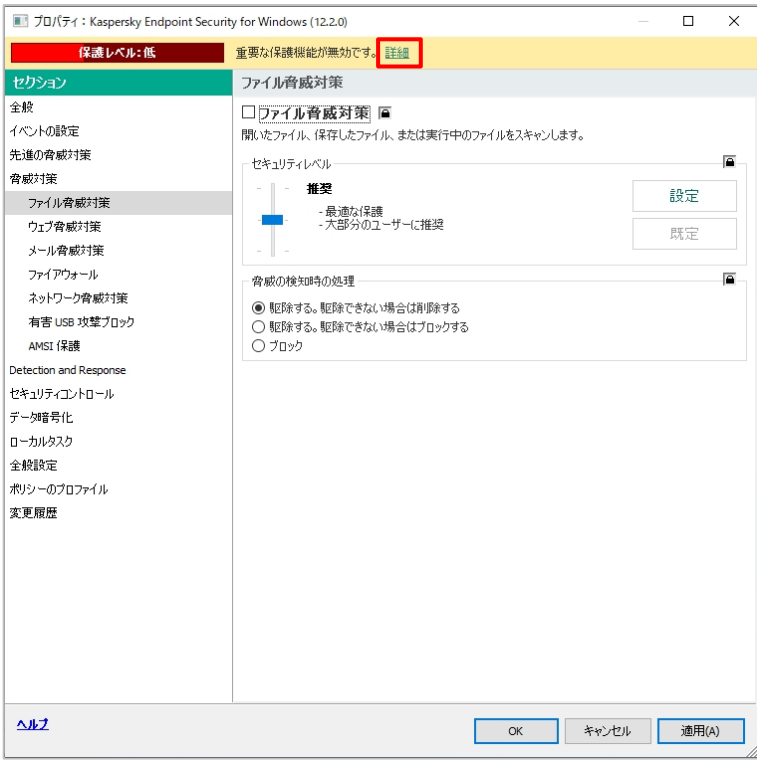
(3)「ウェブ脅威対策」を無効にすると「保護レベル：中」となります。



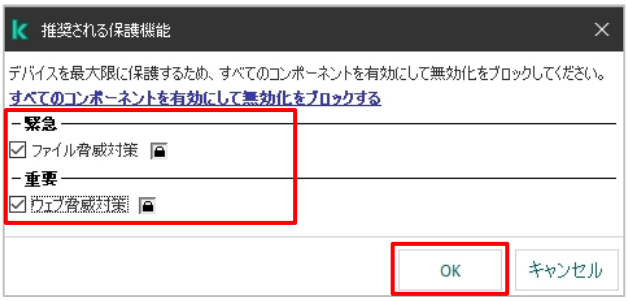
(4)「ファイル脅威対策」を無効にすると「保護レベル：低」となります。



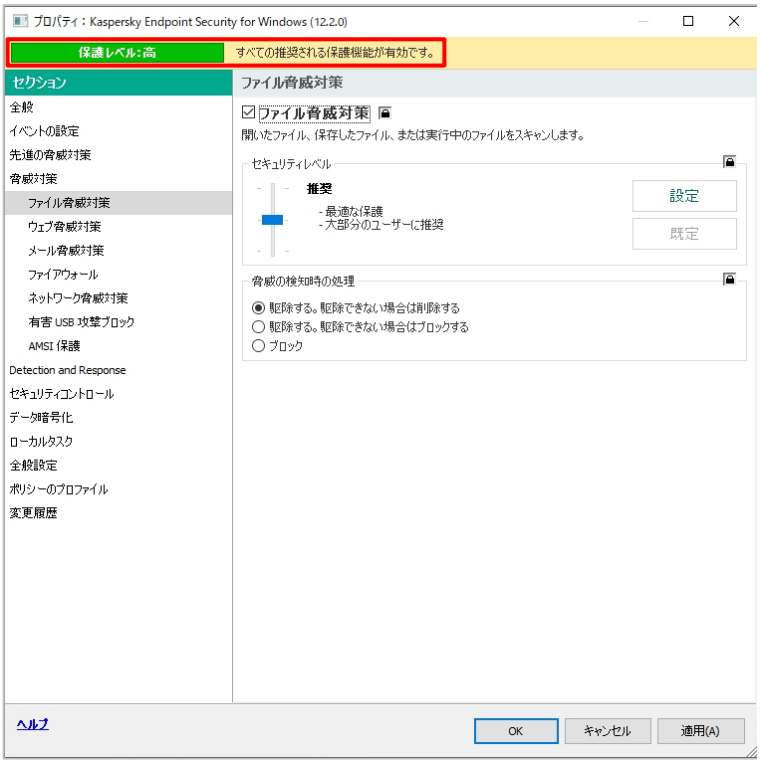
(5) 「詳細」をクリックすると、無効になっている重要な保護機能が確認できます。



(6) 表示された保護機能にそれぞれにチェックを入れ、「OK」をクリックします。



(7) 設定後、保護機能が有効となり、「保護レベル：高」となります。

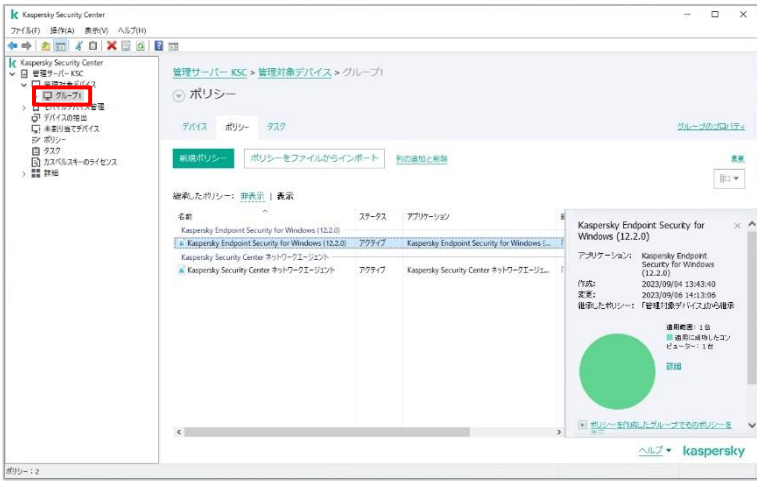


本節は以上です。

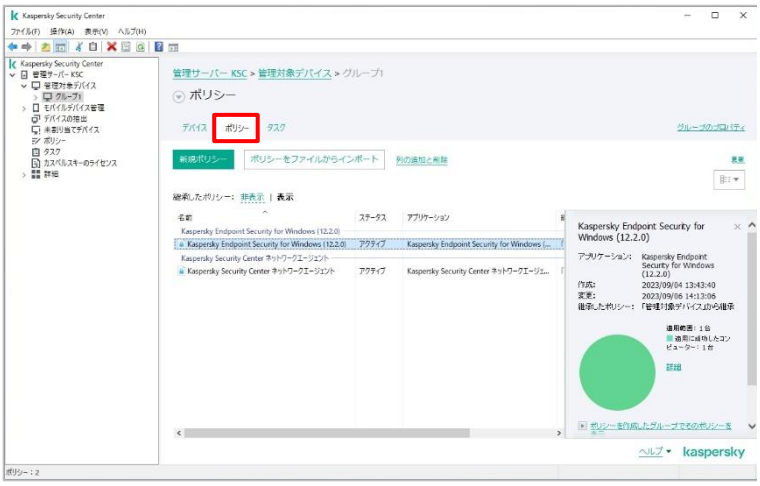
3.4. グループポリシー

ポリシーはグループごとに適用されます。グループの「ポリシー」タブで、各グループに適用されているポリシーを確認することができます。

(1) 左画面にて対象のグループを選択します。



(2) 「ポリシー」タブをクリックします。
既定では継承された親グループのポリシーも全て表示されます。



(3) 親グループのポリシーを表示したくない場合は、ポリシータブで「継承したポリシー：非表示」を選択します。

本節は以上です。

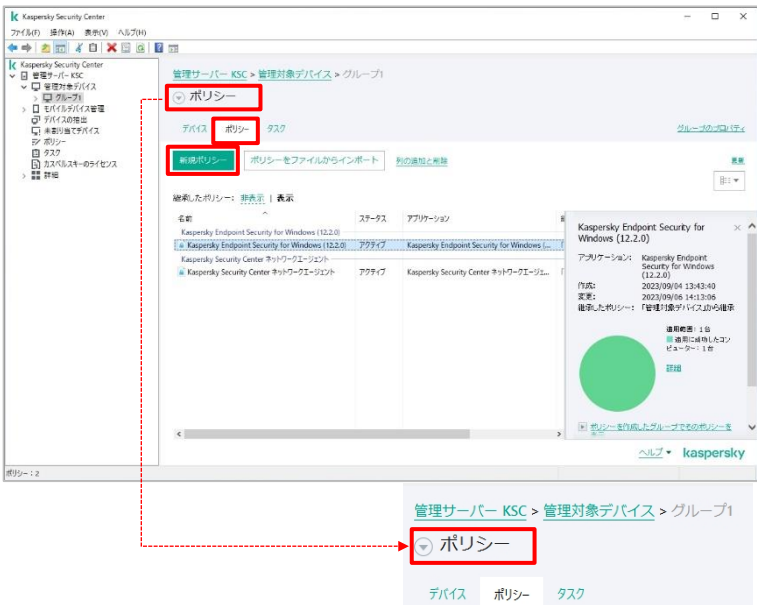
3.5. ポリシーの新規作成

ポリシーは以下の手順で作成します。

(1) ポリシーを作成するグループを選択します。

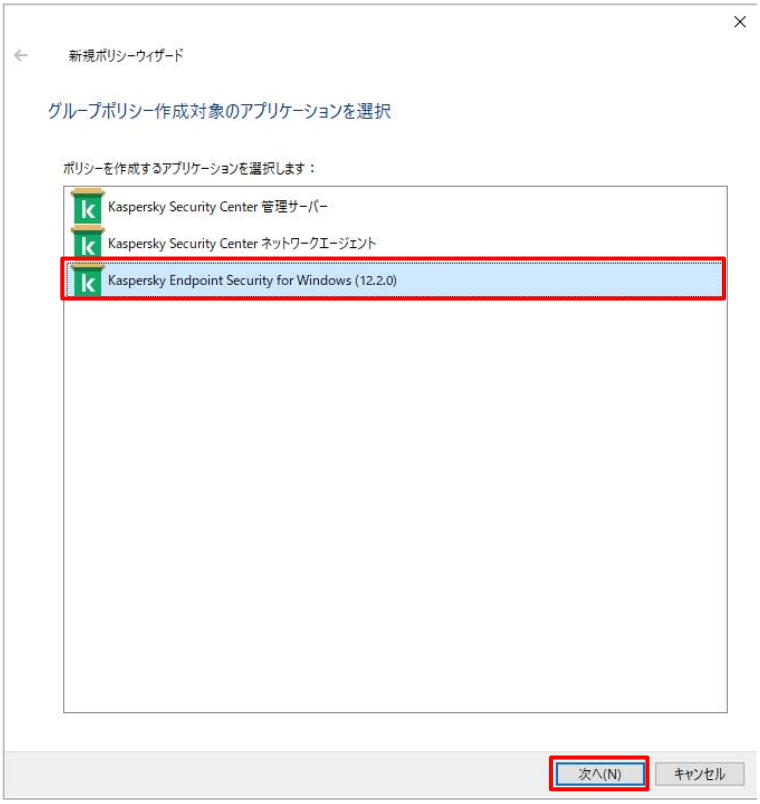
右画面にて「ポリシー」タブを開き、「新規ポリシー」をクリックします。

※「新規ポリシー」ボタンが表示されていない場合は「▲」をクリックしてください。

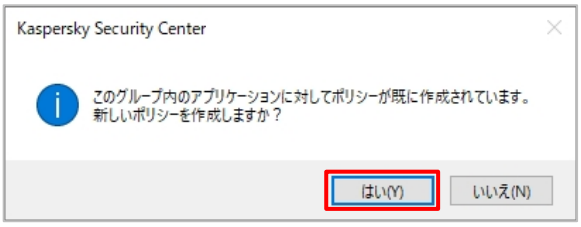


(2) 新規ポリシーウィザードが開きます。
ポリシーを作成するアプリケーションを選択し「次へ」をクリックします。

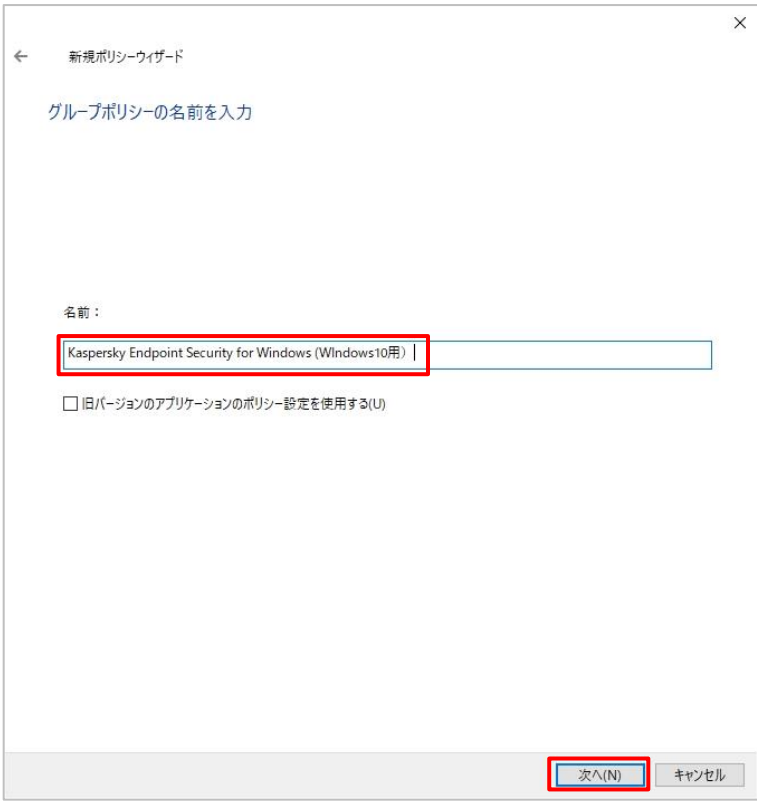
ここでは KES を選択しています。



(3) ※グループに同じアプリケーション用のアクティブポリシーがある場合、右のような確認メッセージが表示されるので「はい」をクリックします。

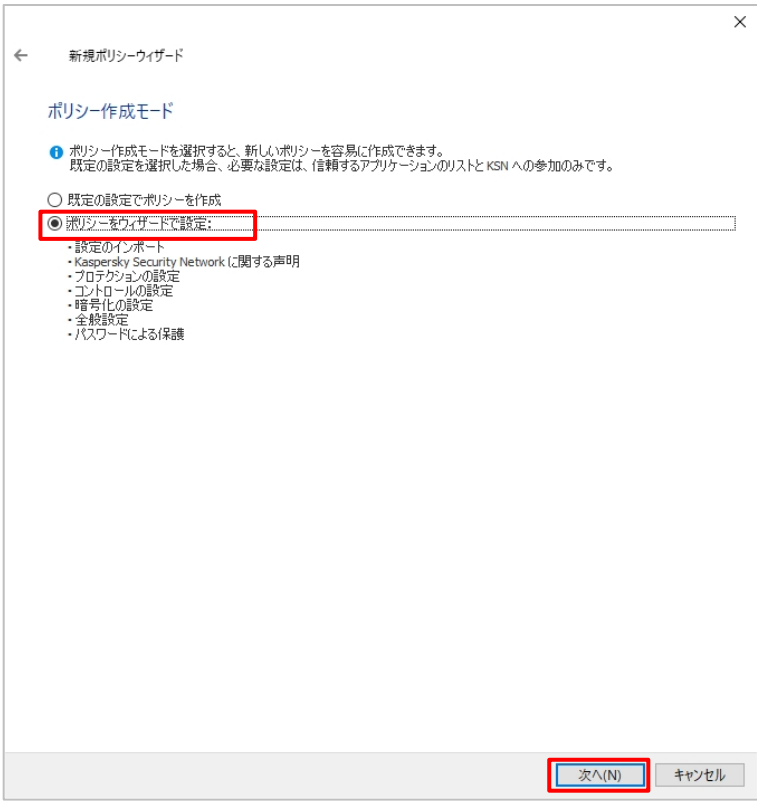


(4) ポリシーの名前を設定します。
任意の名前を入力し、「次へ」をクリックします。
※旧バージョンの設定を利用したい場合は「旧バージョンのアプリケーションのポリシー設定を使用する」のチェックマークを有効にします。
画面に参照ボタンが表示されるので、コピー元のポリシーを選択してください。



(5) ポリシー作成モードを選択します。
ここでは各ポリシー項目を確認するため「ポリシーをウィザードで設定」を選択し、「次へ」をクリックします。
既定の設定値で作成する場合は「既定の設定でポリシーを作成」を選択してください。

ここからの画面はアプリケーションによって異なります。以下は KES for Windows の場合の画面です。



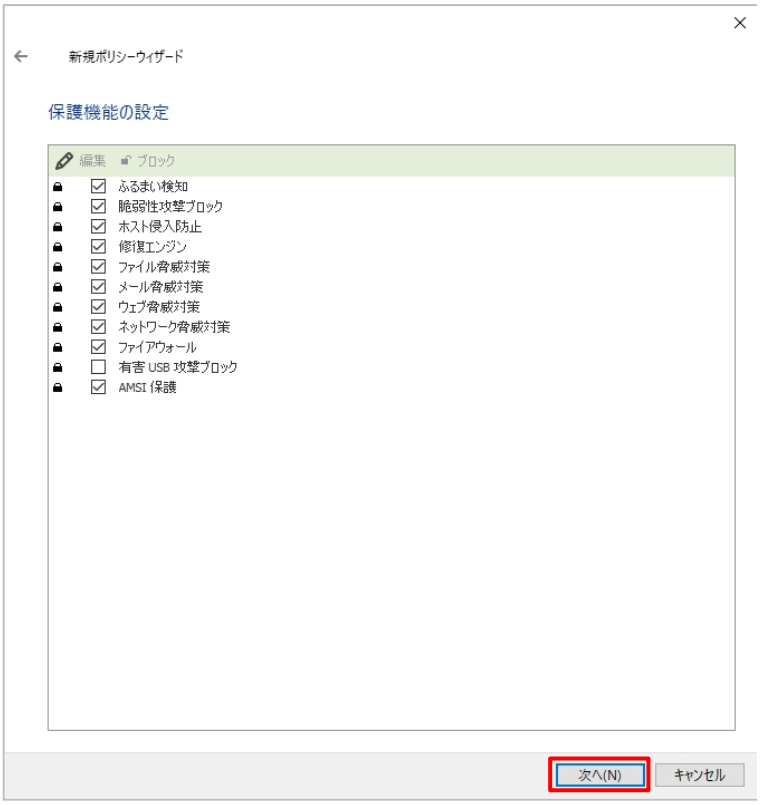
(6) 設定のインポート画面が表示されます。
KES の構成ファイルから設定をインポートする場合は「設定」をクリックしファイルを指定します。
インポートしない場合はそのまま「次へ」をクリックします。

(7) 「Kaspersky Security Network への参加」画面が開きます。
ここでは「Kaspersky Security Network の使用に同意する」を選択して「次へ」をクリックします。

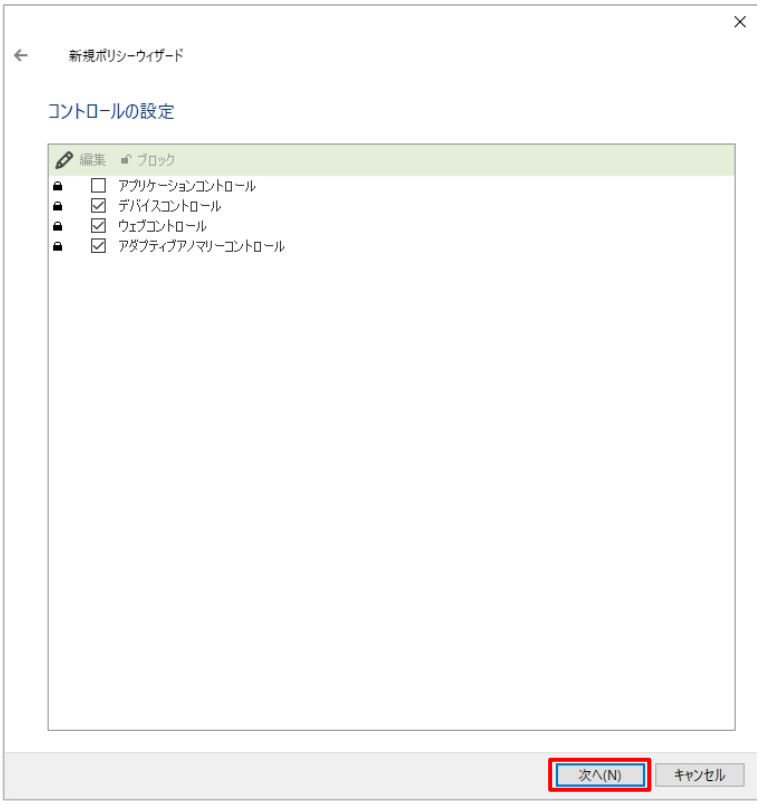
KSN(Kaspersky Security Network)はファイルの不審な活動情報を収集し、匿名化した上で分析しクラウド上にデータベース化します。ファイルが悪質なふるまいを見せている場合は、すぐに緊急検知システム（UDS）データベースに追加され、全ユーザーが参照できるようになります。

(8) 「保護機能の設定」画面が開きます。
ここでは既定値のまま「次へ」をクリックします。

※サブグループ用のポリシーを作成している場合、既定では「親ポリシーから設定を継承する」が有効になっているため、ここで編集をしても設定は親ポリシーから継承されるため、ここの設定は反映されません。
ポリシー作成後、「親ポリシーから設定を継承する」をオフに設定してから変更する必要があります。
ポリシーの継承については 手順「3.7. ポリシーの強制的な継承」を参照してください。

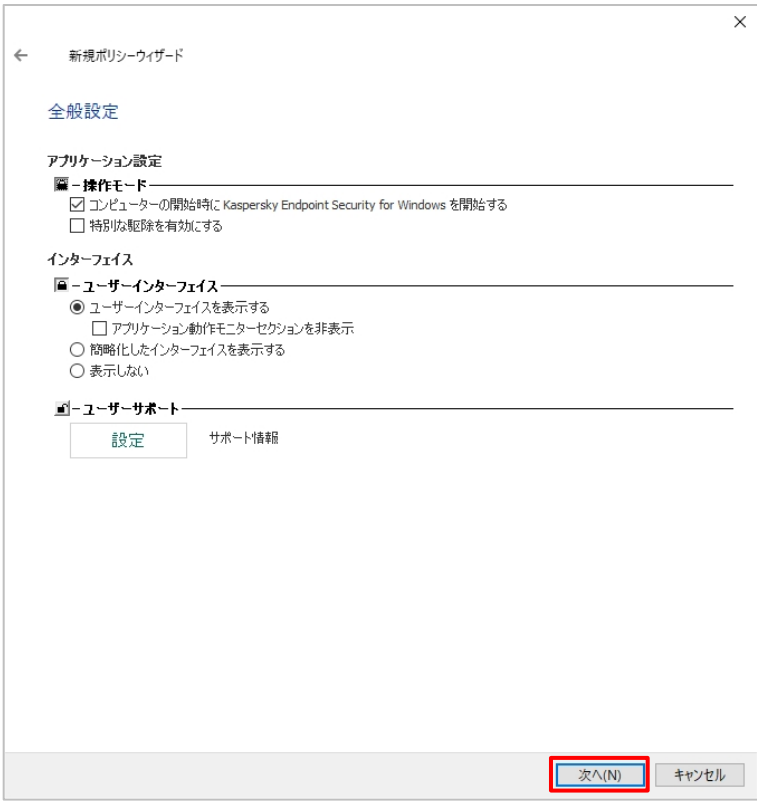


(9) 「コントロールの設定」画面が開きます。
ここでは既定値のまま「次へ」をクリックします。

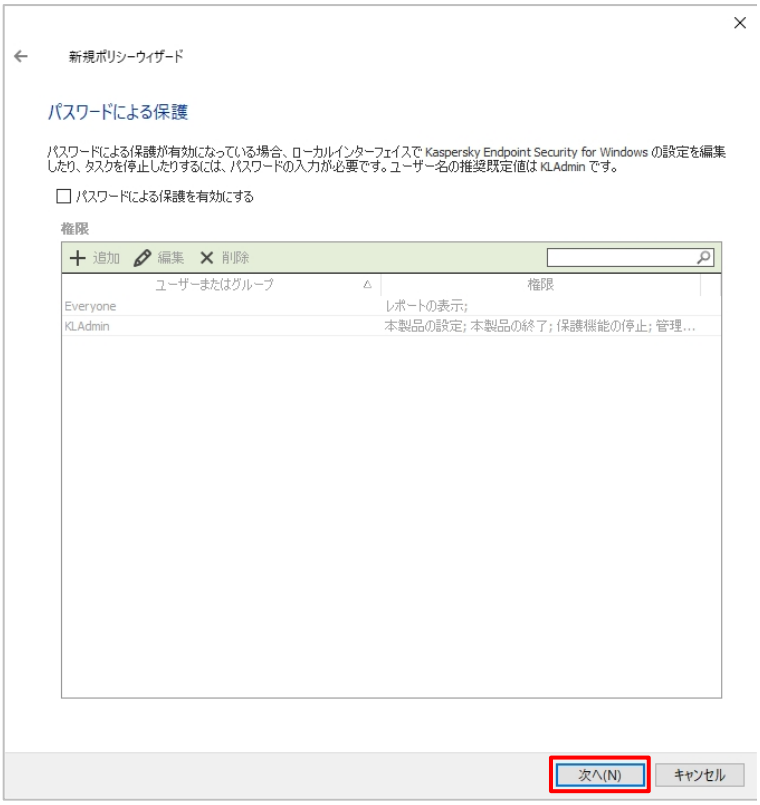


(10)　「暗号化の設定」画面が開きます。
ここでは既定値のまま「次へ」をクリックします。

(11)　「全般設定」の画面が開きます。
個々では既定値のまま「次へ」をクリックします。



(12)　「パスワードによる保護」の画面が開きます。
ここでは既定値のまま「次へ」をクリックします。

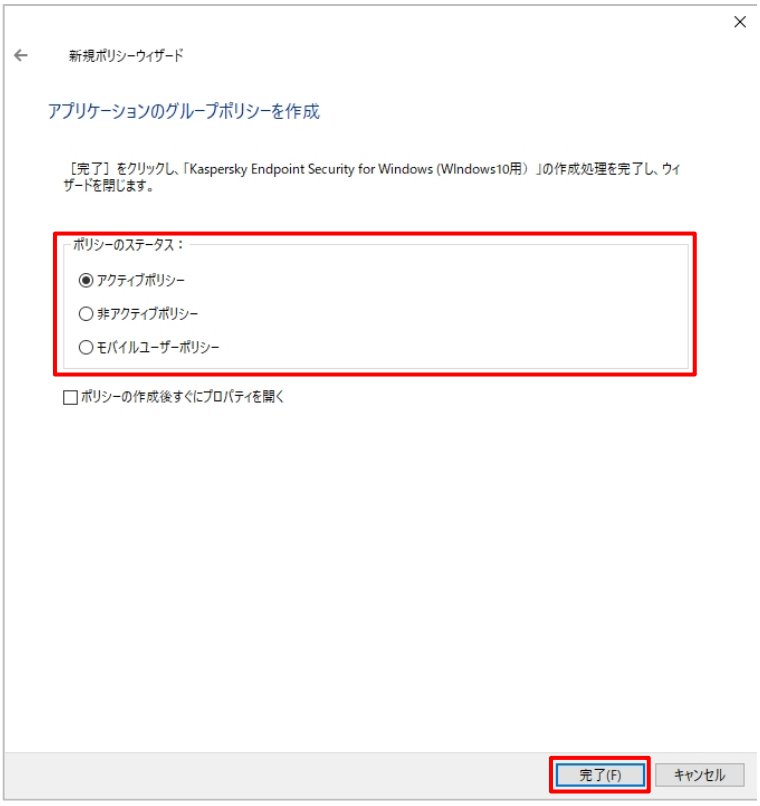


(13)　「アプリケーションのグループポリシーを作成」の画面が開きます。
ここでは「アクティブポリシー」を選択し、「完了」をクリックします。

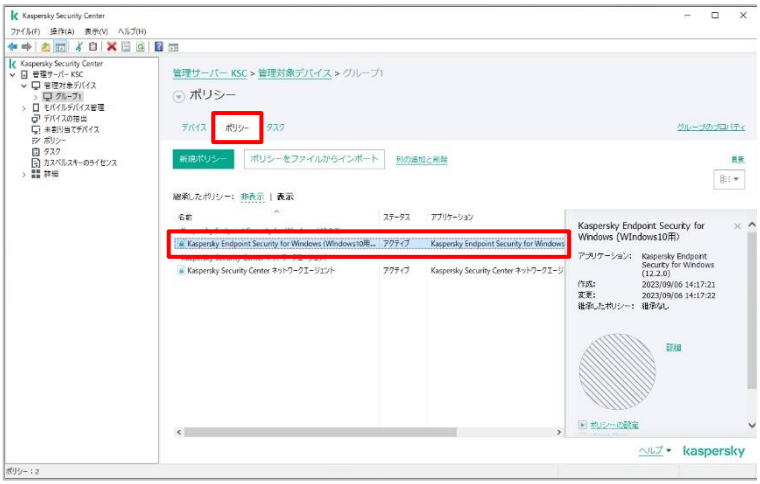
既に「アクティブ」ステータスのポリシーが存在する場合、「アクティブポリシー」を選択するとこのポリシーがアクティブへ切り替わりデバイスへ適用されます。

このポリシーはテスト用で作成するものであり、「アクティブ」ステータスのポリシーを切り替えたくない場合、「非アクティブポリシー」を選択してください。

「ポリシーのステータス」については、「3.6. ポリシーのステータス」を参照してください。



(14)　作成されたポリシーが「ポリシー」タブに表示されます。
「ポリシー」タブでポリシーをダブルクリックするとプロパティ画面が開き、細かい設定を確認・変更できます。



本節は以上です。

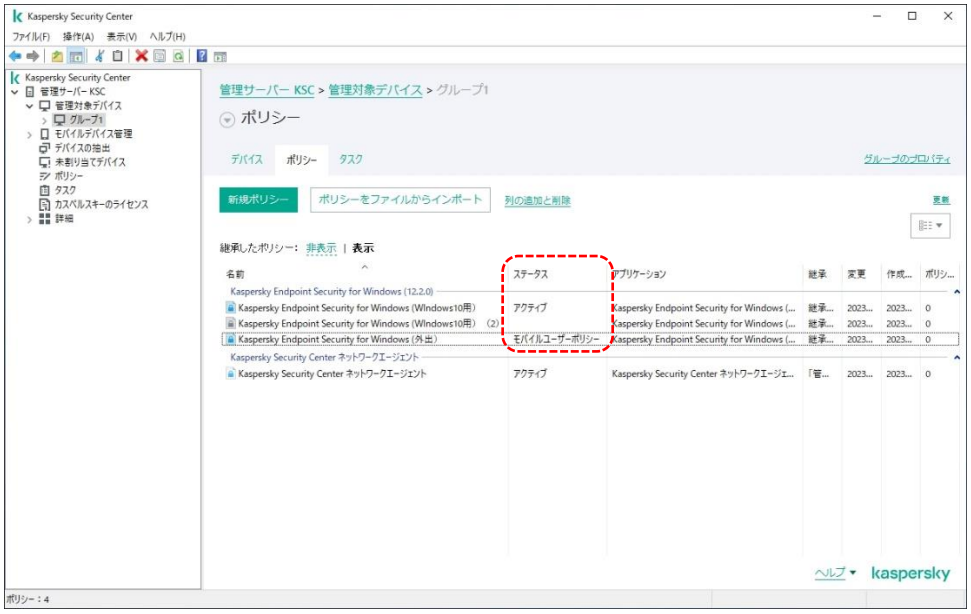
3.6. ポリシーのステータス

ポリシーはグループごとに適用されます。グループの「ポリシー」タブで、各グループに適用されているポリシーを確認することができます。

それぞれのグループに適用されるポリシーは、各アプリケーションにつき一つです。どのポリシーが適用されているかは「**ステータス**」で確認できます。

ステータス	内容
アクティブポリシー	デバイスに適用されているポリシー
モバイルユーザーポリシー	デバイスが KSC と通信できなくなった際に適用されるポリシー （社外に出た場合などに適用される） ※KES for Windows、KES for Mac のみ
非アクティブポリシー	デバイスに適用されないポリシー (テストやバックアップとして保存しておきたい場合などに使用する)

ポリシーの一覧画面では、ステータス欄に「アクティブ」あるいは「モバイルユーザーポリシー」と表示されます。非アクティブポリシーは空欄となります。



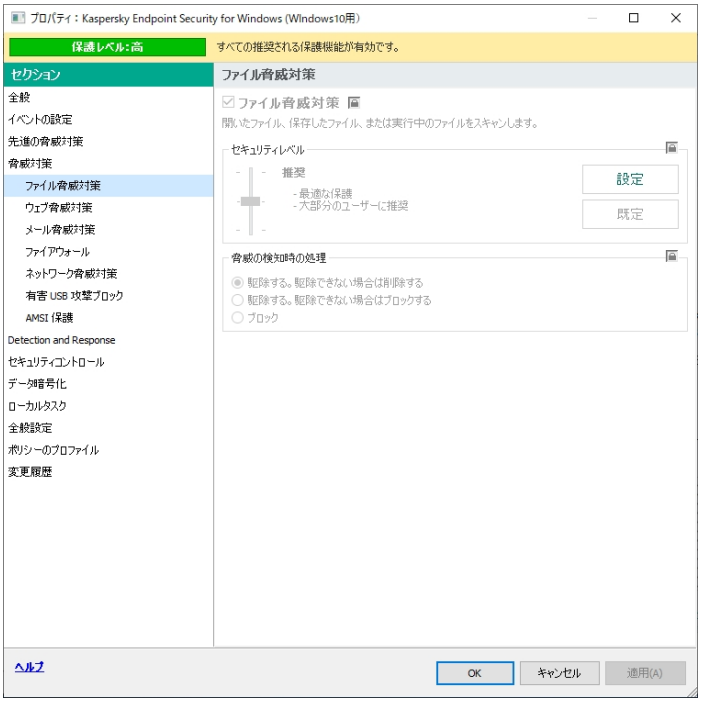
本節は以上です。

3.7. ポリシーの強制的な継承

親グループのポリシーは、親グループに属するサブグループ（子グループ）へ継承されます。
したがって、「管理対象デバイス」の「ポリシー」で設定したポリシーはすべてのグループに**強制的に継承されます。**

サブグループでポリシーを別途作成した場合でも、親グループのポリシーが優先されるため、サブグループのポリシーを定義したい場合は親グループのポリシーを継承しないように設定する必要があります。

<画面例：親グループのポリシーを継承しているため設定は変更できない>



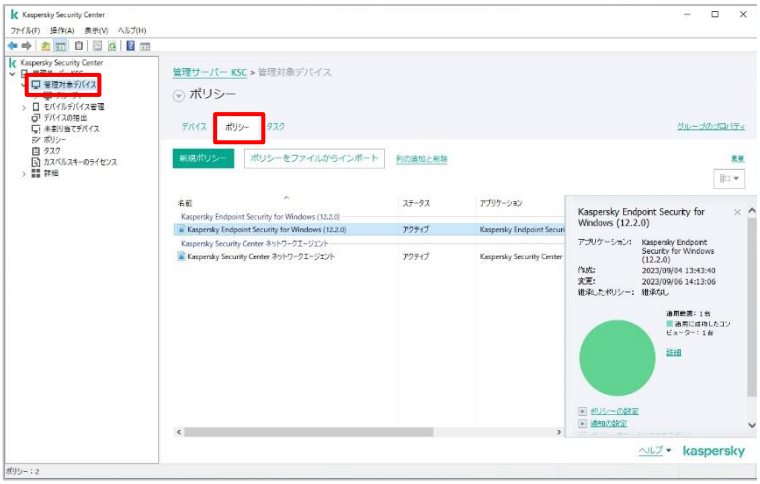
親グループのポリシーを継承させないようにするには、親ポリシー側で以下のように設定します。

- 親グループのポリシー：「**設定を子ポリシーへ強制的に継承させる**」をオフにする（※デフォルトはオフ）
- サブグループのポリシー：「**親ポリシーから設定を継承する**」をオフにする

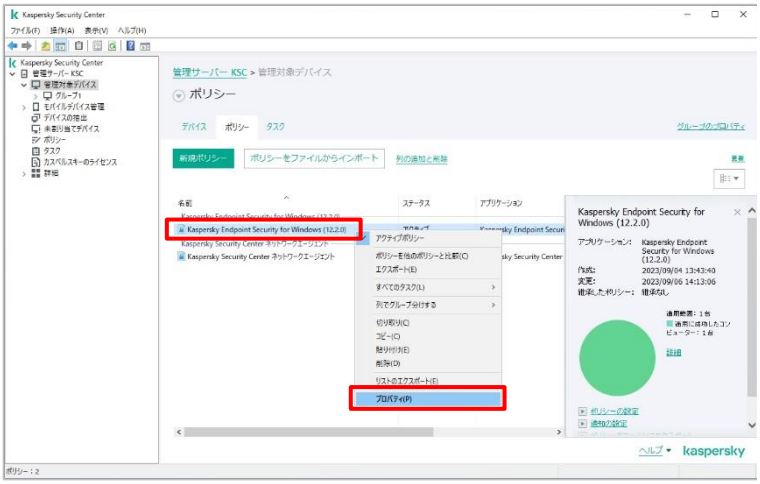
なお、サブグループのポリシーがまだ作成されていない場合は、「ポリシー」タブの「新規ポリシー」でポリシーを作成した上で、この手順に従い「親ポリシーから設定を継承する」をオフにしてください。

3.7.1. 親グループのポリシーで「設定を子ポリシーへ強制的に継承させる」をオフにする

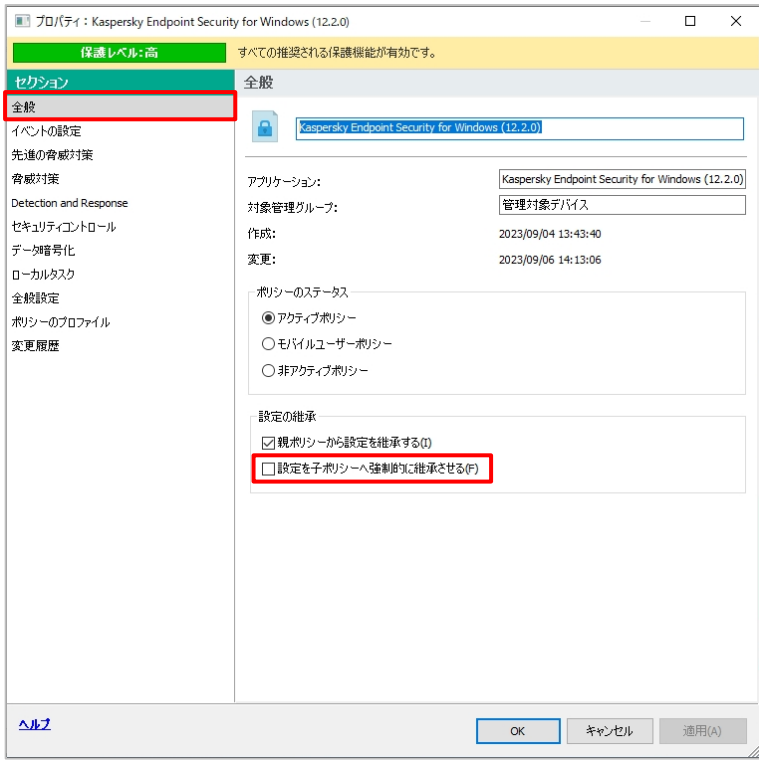
(1) 親グループ（ここでは「管理対象デバイス」グループ）の「ポリシー」タブを表示します。



(2) ポリシー（ここでは KES 用のポリシー）を右クリックして「プロパティ」を選択、またはダブルクリックしてプロパティ画面を開きます。



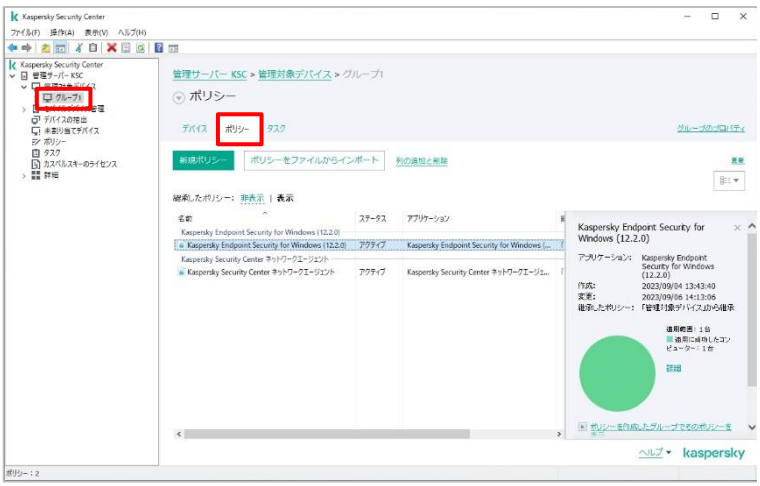
(3) 「全般」セクションを開き、「設定の継承」にて「設定を子ポリシーへ強制的に継承させる」をオフにします。
なお、既定では「オフ」に設定されています。



本項は以上です。

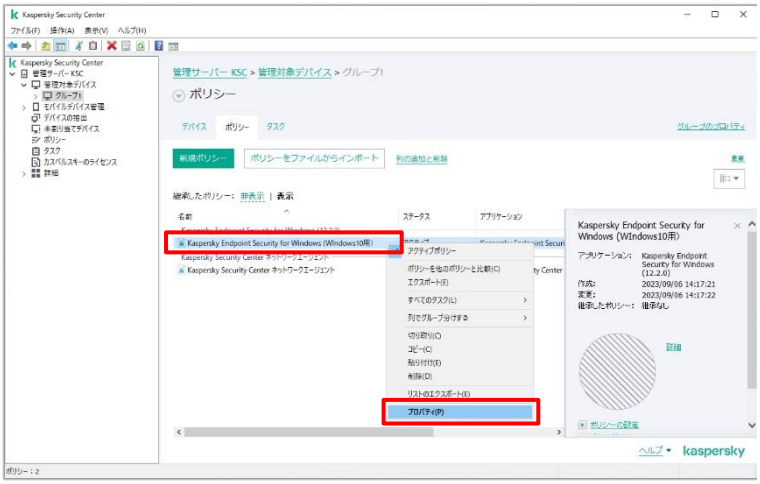
3.7.2. サブグループのポリシーで「上位ポリシーから設定を継承する」をオフにする

(1) サブグループの「ポリシー」タブを表示します。（ここでは「グループ 1」グループ）

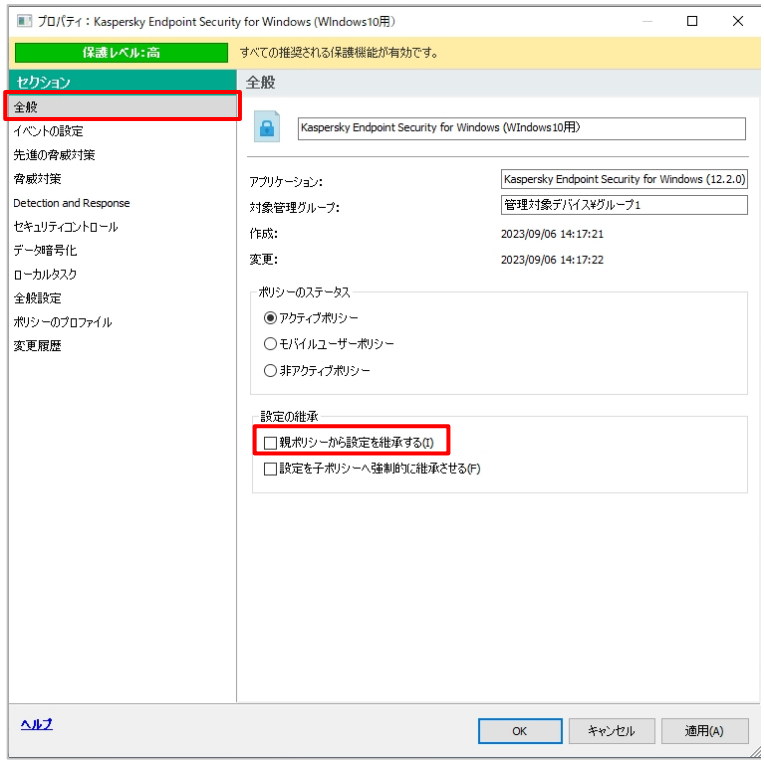


(2) ポリシー（ここでは KES 用のポリシー）を右クリックして「プロパティ」を選択、またはダブルクリックしてプロパティ画面を開きます。

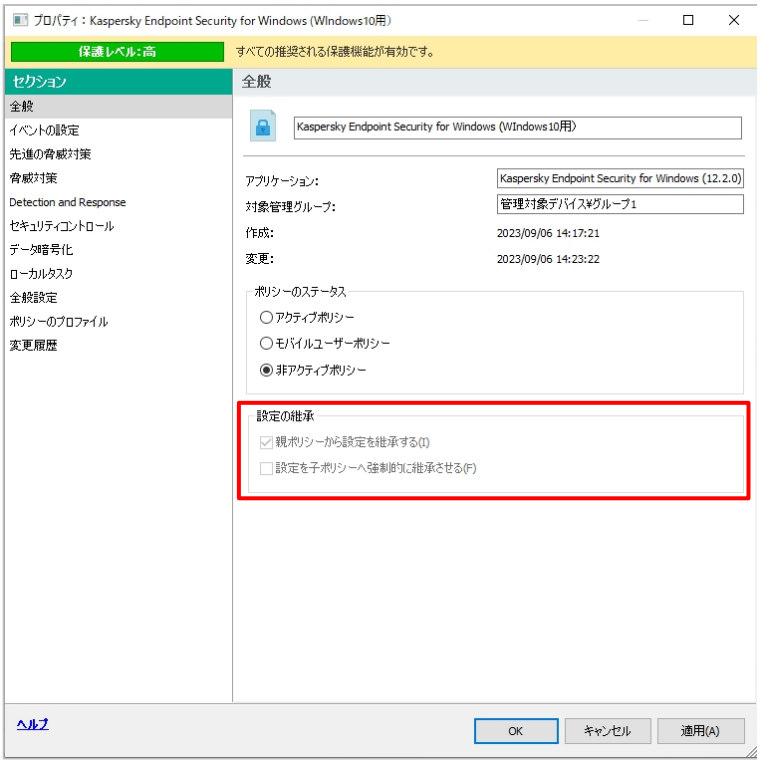
事前にこのグループにて該当のポリシーが作成されている必要があります。継承されたポリシーでは設定を変更することはできません。
（作成手順は「3.5 ポリシーの新規作成」を参照してください）



(3) 「全般」セクションを開き、「設定の継承」にて「親ポリシーから設定を継承する」をオフにします。



(4) 親グループのポリシーで「設定を子ポリシーへ強制的に継承させる」がオンになっている場合、サブグループのポリシーでは「設定の継承」を変更できません。



本項は以上です。

3.8. モバイルユーザーポリシー

KES for Windows では、持ち出し PC のポリシーを社内と社外とで切り替えることで、社外持ち出し時の PC のセキュリティレベルを変更することができます。社外持ち出し時用のポリシーを「**モバイルユーザーポリシー**」と言います。

設定手順や詳細は、以下サイトの「**モバイルモード設定**」をご参照ください。

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

本章は以上です。

4. タスク

「**タスク**」機能を使うと、管理サーバー（KSC）やデバイス（KES）、あるいはサーバーとデバイス間の通信を行うネットワークエージェントに対し、決められた処理をまとめて実行させることができます。

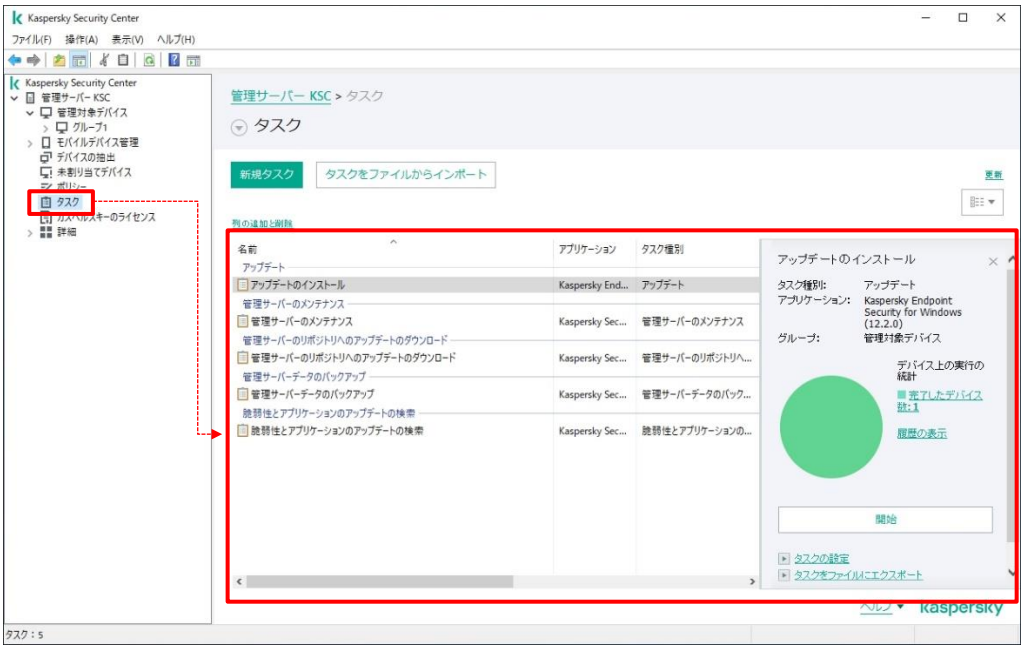
各タスクをどのデバイスで実行するかは、グループごとに設定する「**グループタスク**」と、デバイスを自由に選択する「**特定のコンピューターに関するタスク**」の 2 通りで設定できます。

KSC をインストールし「初期設定ウィザード」を実行すると、「管理対象デバイス」のグループタスクとして、以下のタスクが自動で生成されます。

タスク名	概要	スケジュール（デフォルト値）
アップデートのインストール（KES）	定義 DB のダウンロード・更新	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
脆弱性とアプリケーションのアップデートの検索（ネットワークエージェント）	インストールされているアプリケーションのぜい弱性の検索	毎週火曜日 19:00:00

4.1. タスクの表示

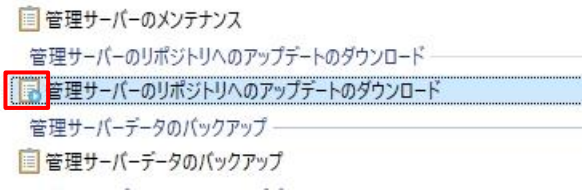
左画面にて「タスク」を選択すると、右画面に現在定義されているタスクが一覧表示されます。



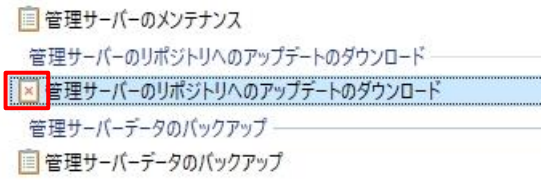
ヒント：タスクのリストで右クリック→「列でグループ分けする」で、アプリケーションやグループで分類して表示できます。

タスクの先頭のアイコンで、タスクの状況が確認できます。

<進行中のタスク>

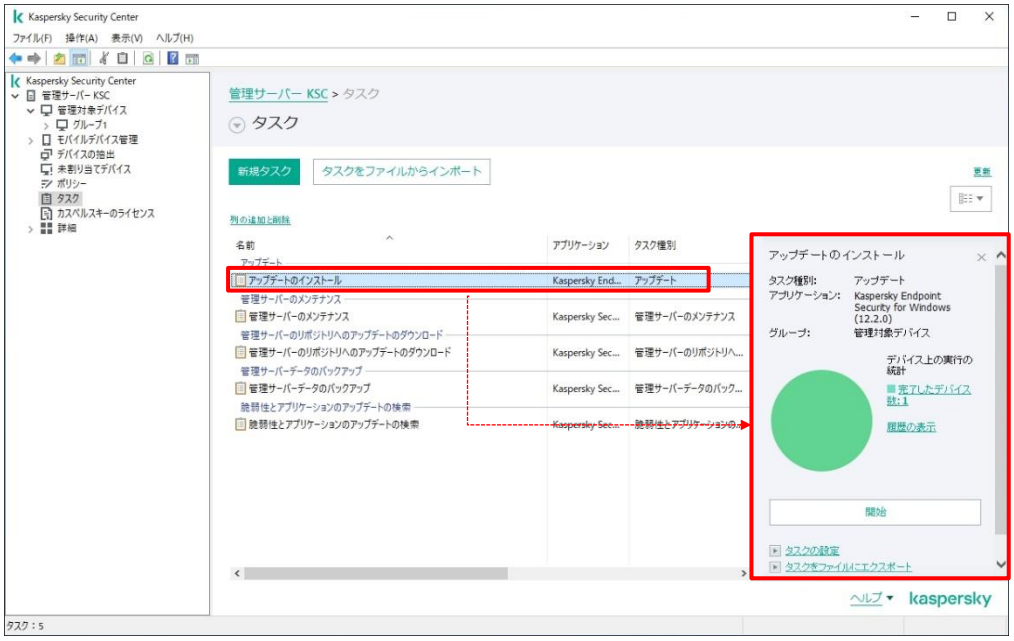


<エラーが発生したタスク>

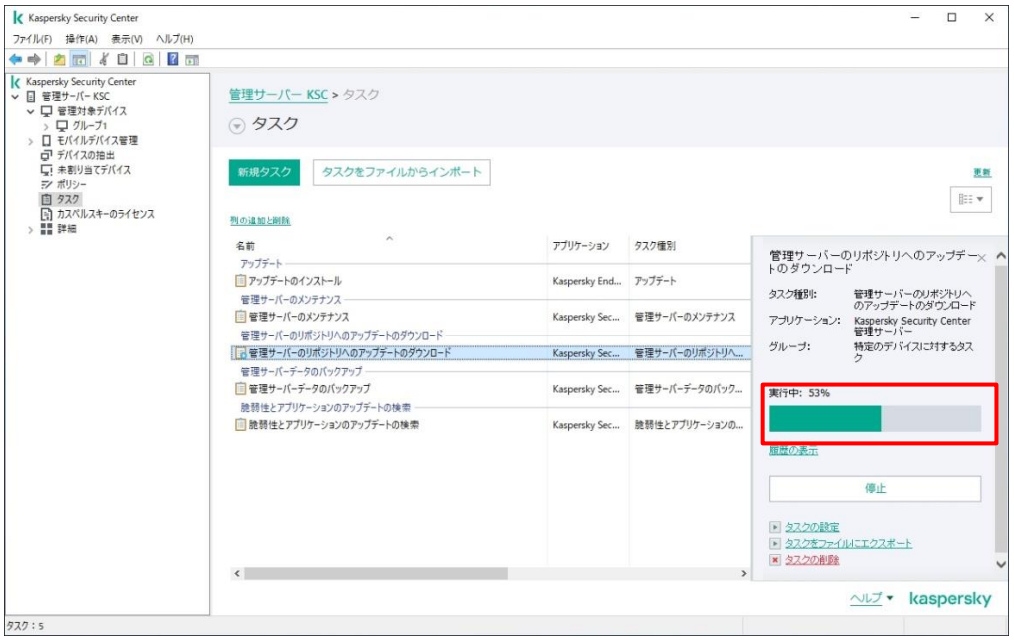


個々のタスクをクリックすると、詳細画面にてタスクが最後に実行された際のステータスを確認することができます。詳細を確認したい場合は「履歴の表示」をクリックします。

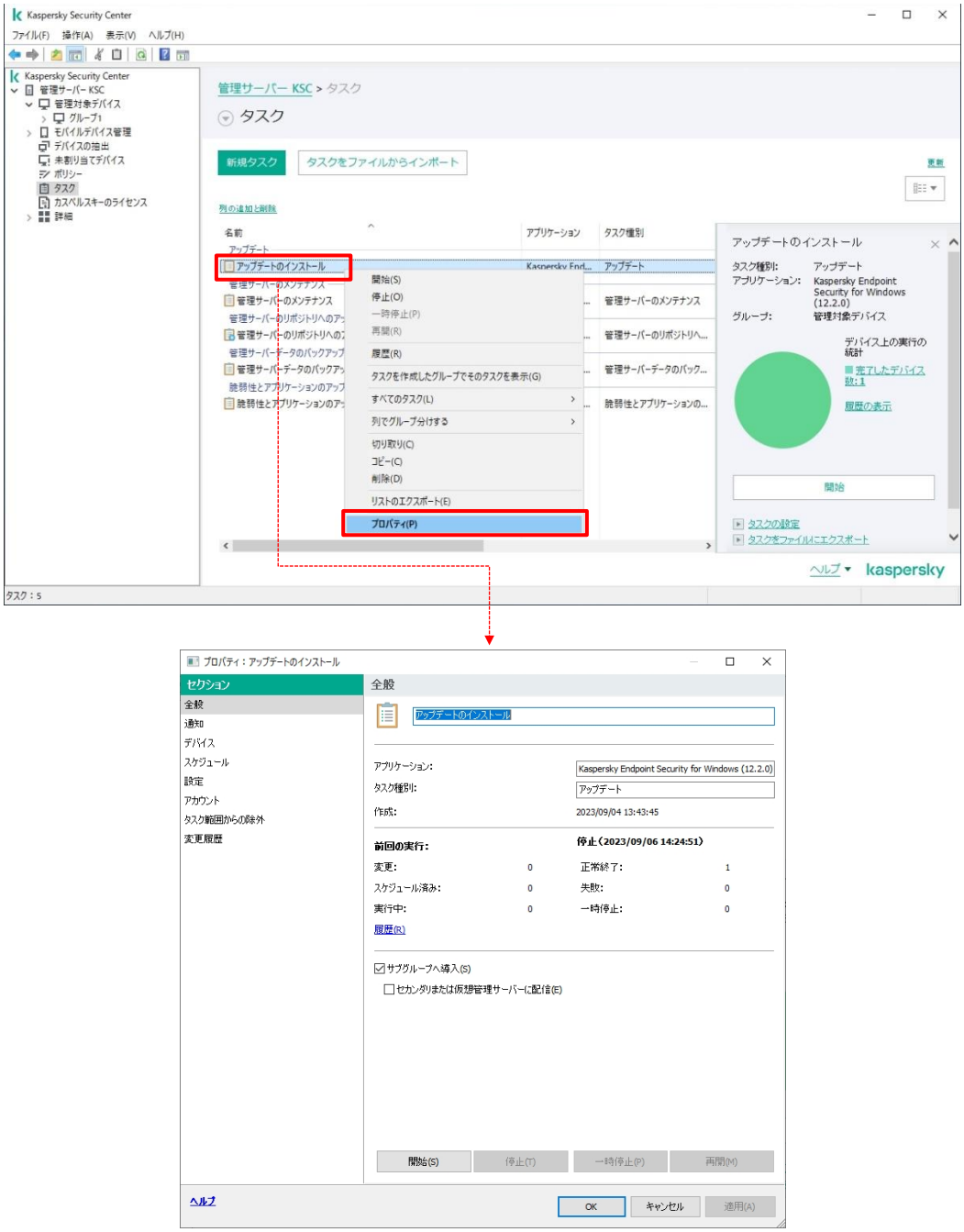
また、「開始」をクリックして、タスクを今すぐ実行することもできます。



<実行中の場合の表示例>



タスクを右クリックして「プロパティ」を選択、またはダブルクリックするとプロパティ画面が表示され、設定の詳細を確認することができます。また、プロパティ画面で設定内容を変更することも可能です。



タスクを変更すると、「ネットワークエージェント」を通じて各デバイス（KES がインストールされたデバイス）に設定情報が配布され、タスク内のスケジュールが設定されます。

デバイスに登録されたタスクはそれぞれのデバイス上の時刻に沿って実行されるため、外出中など KSC と通信ができない状態であってもタスクは実行されます。

本節は以上です。

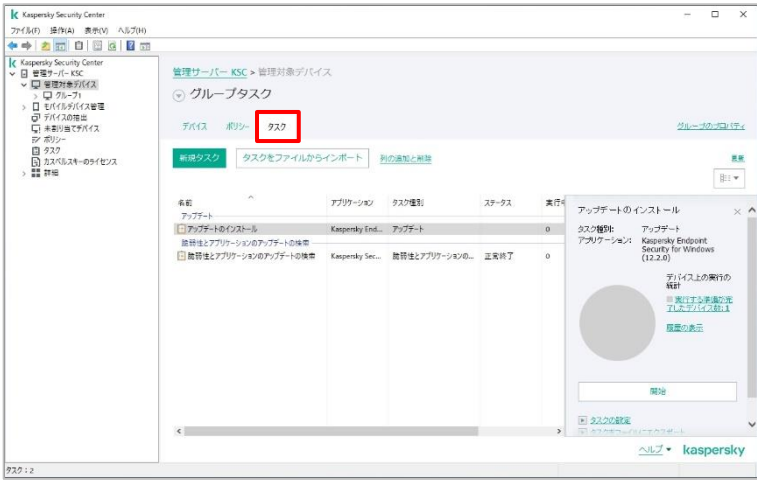
4.2. グループタスク

グループごとに実施するタスクは、グループの「タスク」タブで確認できます。

(1)左画面にて「グループ」を選択します。

(2)「タスク」タブをクリックします。

※「管理サーバー」→「タスク」の画面では、「グループ」欄でグループを確認できます。



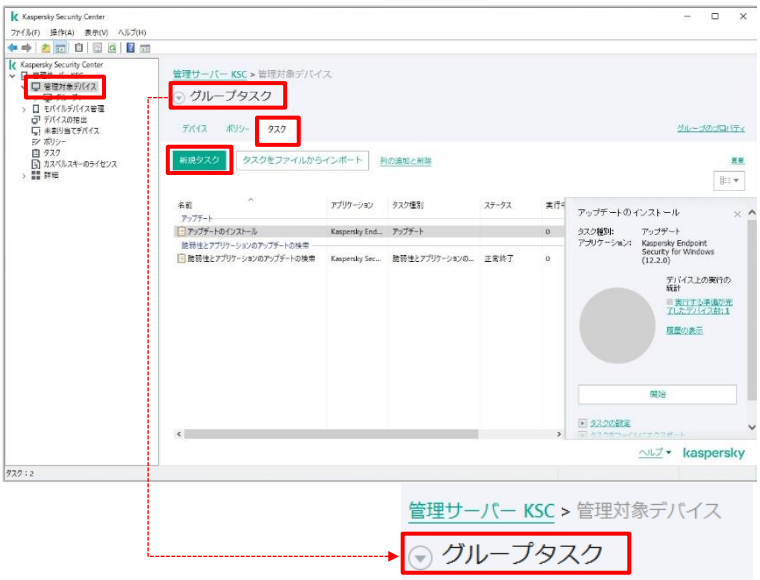
本節は以上です。

4.3. グループタスクの新規作成

グループタスクは、以下の手順で作成します。

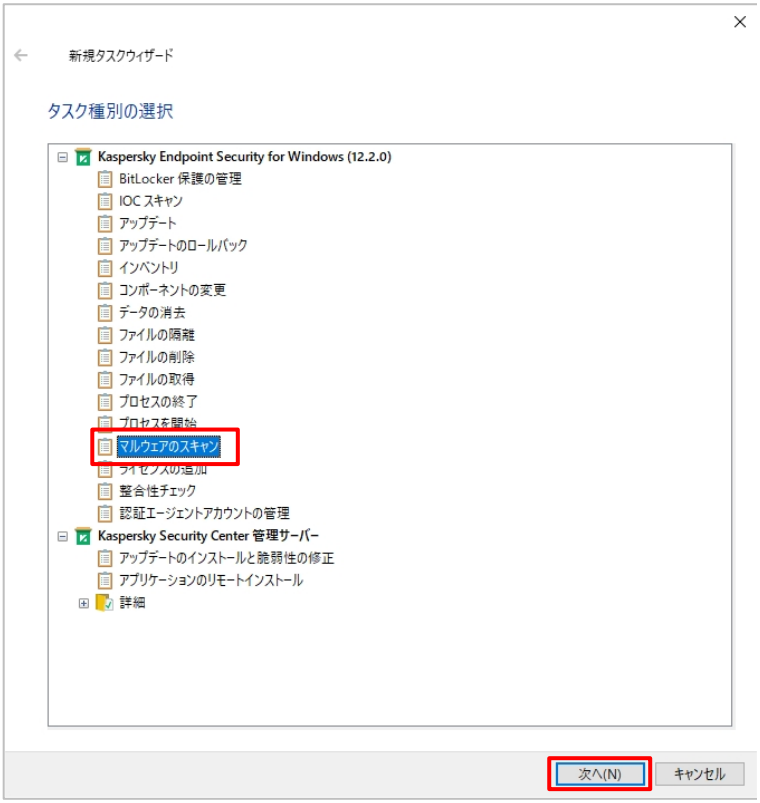
(1) 左画面にて「グループ」を選択し、「タスク」タブを開いて「新規タスク」をクリックします。

※「新規タスク」ボタンが表示されていない場合は「▲」をクリックしてください。



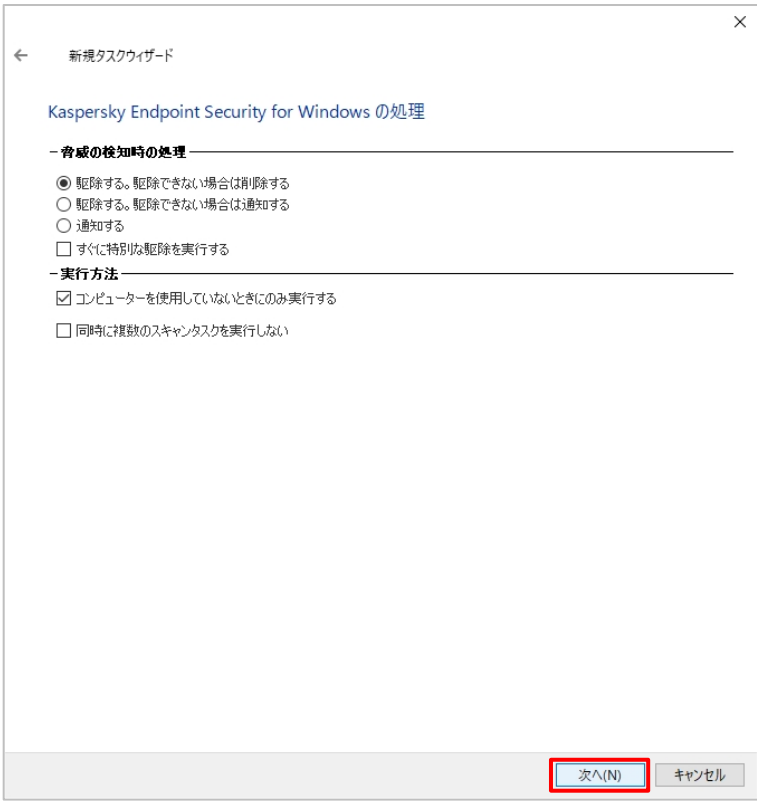
(2)「タスク種別の選択」画面が表示されます。
タスクの種別を選択し、「次へ」をクリックします。

※ここからの画面はタスクの種別によって異なります。以降は KES の「マルウェアのスキャン」を選択した際の画面です。

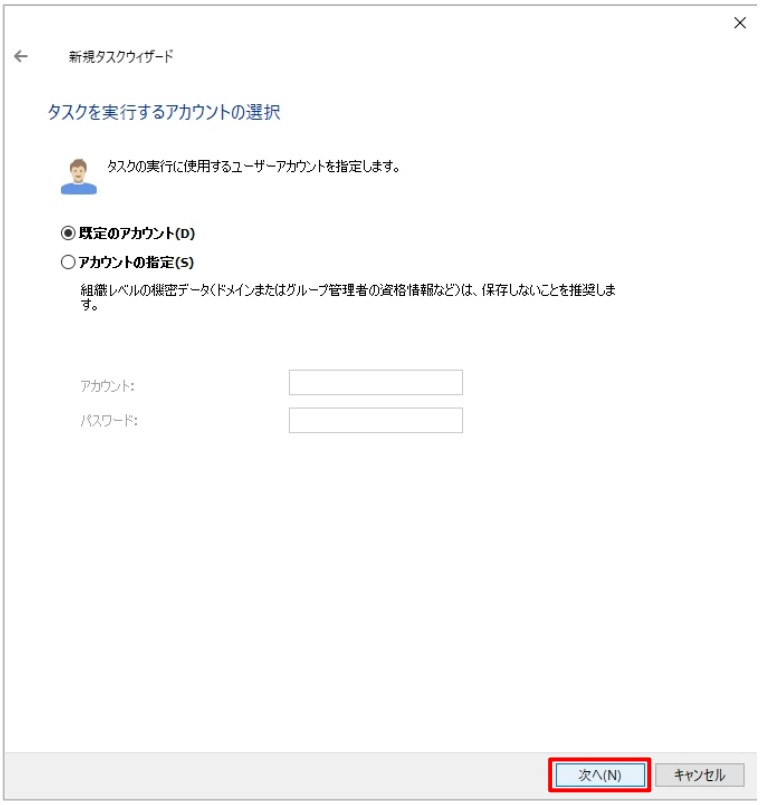


(3)「スキャン範囲」画面が表示されます。
ここでは既定値のまま、「次へ」をクリックします。

(4)「KES の処理」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



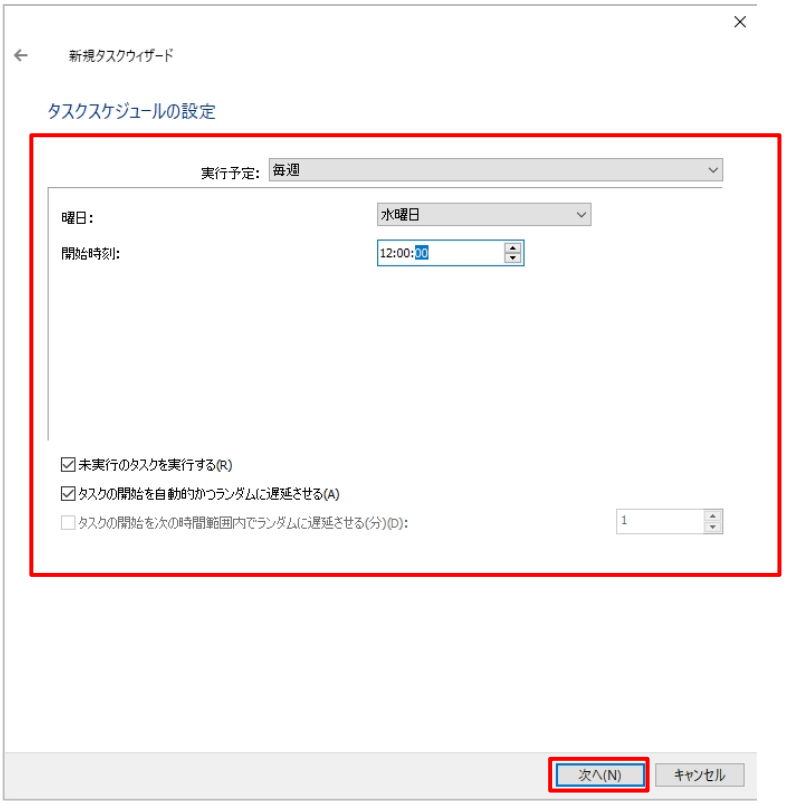
(5)「タスクを実行するアカウントの選択」画面が表示されます。
ここでは既定値のまま、「次へ」をクリックします。



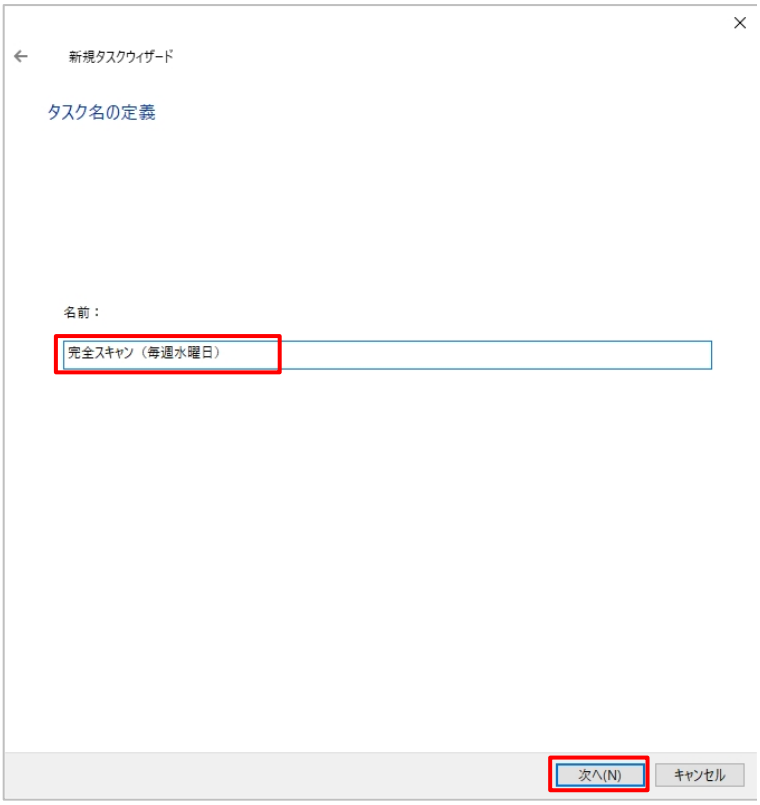
(6)「タスクスケジュールの設定」画面が表示されます。
タスクを実行するスケジュールを設定し、「次へ」をクリックします。

このタスクを ＫＳＣ上から管理者が任意のタイミングで実行したい場合「実行予定」を「手動」に設定してください。
スケジュールに沿って定期的に実行したい場合は「実行予定」を手動以外に変更し、実行スケジュールを設定します。

ここでは毎週水曜日 12:00 にスキャンが実行されるよう設定しています。

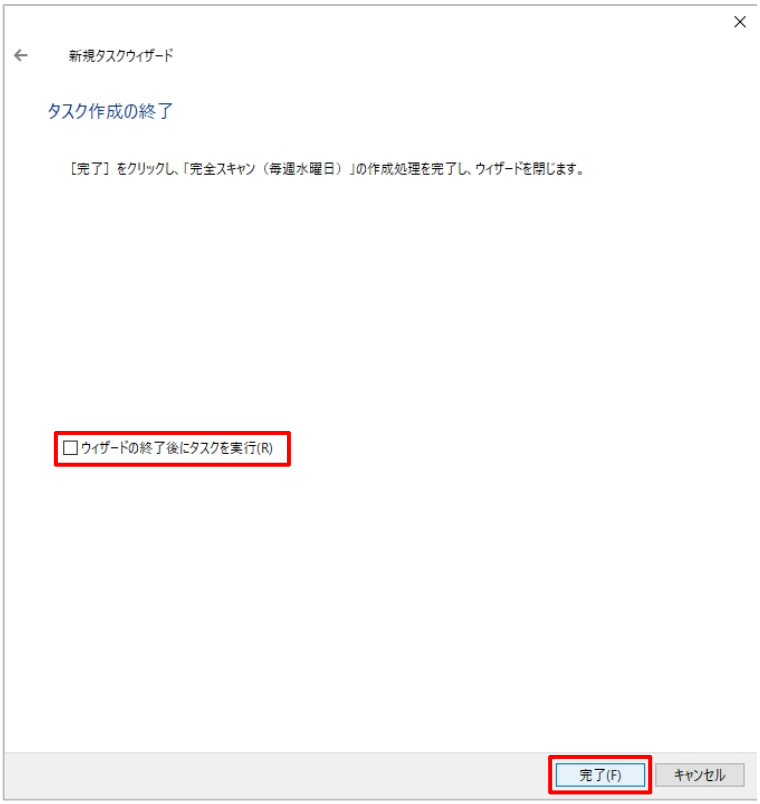


(7)「タスク名の定義」画面が表示されます。
タスクの名前を入力し、「次へ」をクリックします。

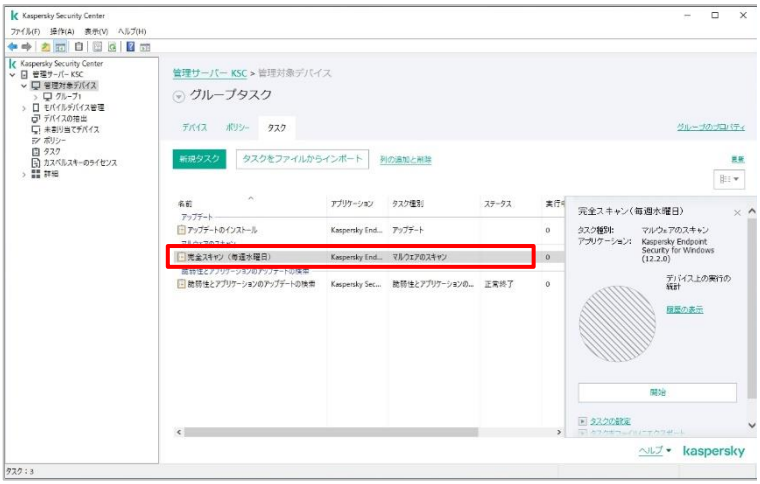


(8) 正常に作成されたことを確認し、「完了」をクリックします。

作成したタスクをすぐに実行したい場合は「ウィザード完了後にタスクを実行する」にチェックマークを入れます。



(9)　作成されたタスクが「タスク」タブに表示されます。
設定を確認・変更する場合はタスクのプロパティを開きます。



本節は以上です。

4.4. タスクの強制的な継承

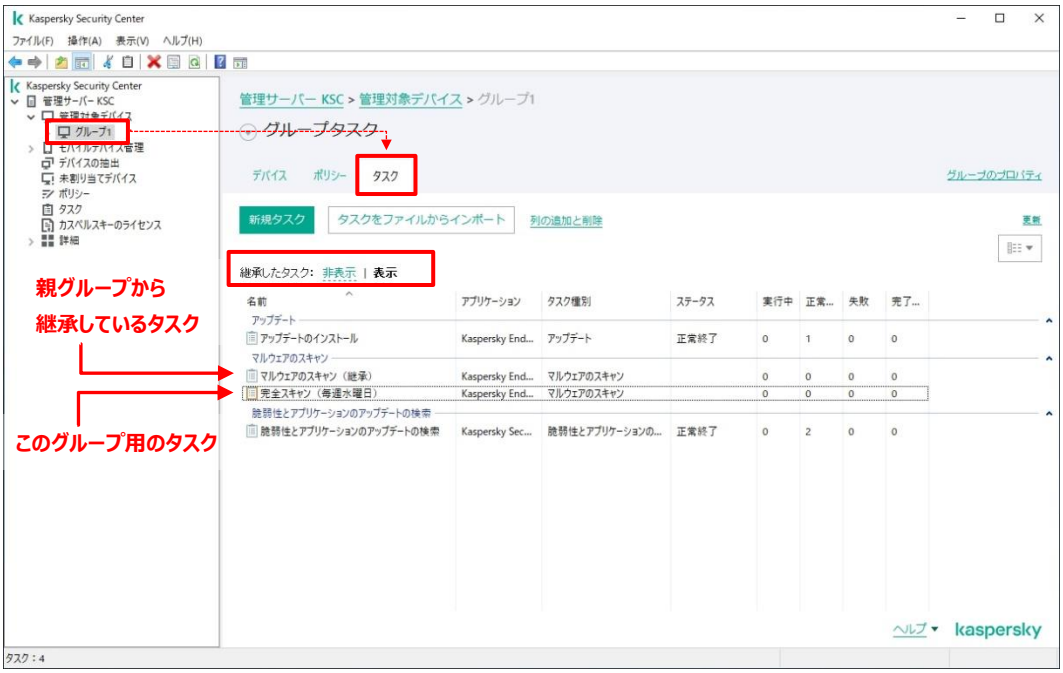
グループごとに実施されるタスクを「**グループタスク**」といいます。

親グループのタスクは、サブグループへ継承されます。既定では「管理対象デバイス」の「タスク」で設定されているタスクがすべてのサブグループに**強制的に継承されます。**

グループの「タスク」タブにて、「継承したタスク：表示」にしていると継承しているタスクが表示されます。継承しているタスクかどうかはアイコンの色で区別することができます。

「継承したタスク：非表示」とすると、このグループ用に作成したタスクのみ表示されます。

＜継承したタスクを表示（…継承したタスク …このグループ用に作成したタスク）＞



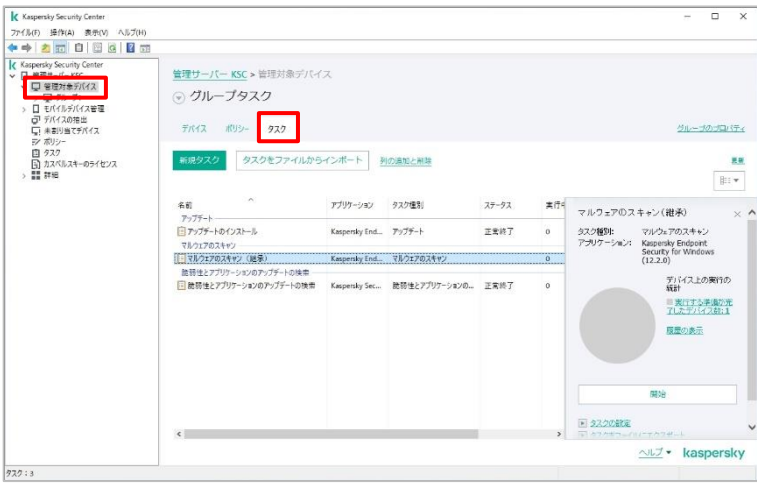
＜継承したタスク：非表示＞

本節は以上です。

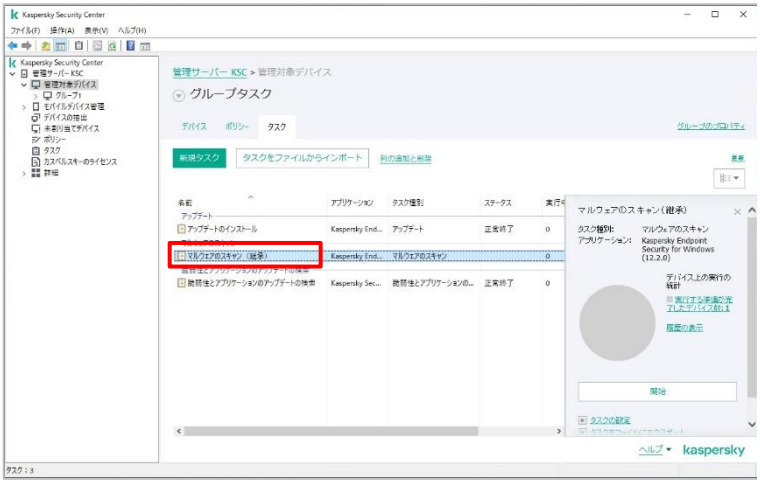
4.5. タスク範囲からの除外

タスクを継承させたくないグループがある場合、次のように「タスク範囲からの除外」を設定します。

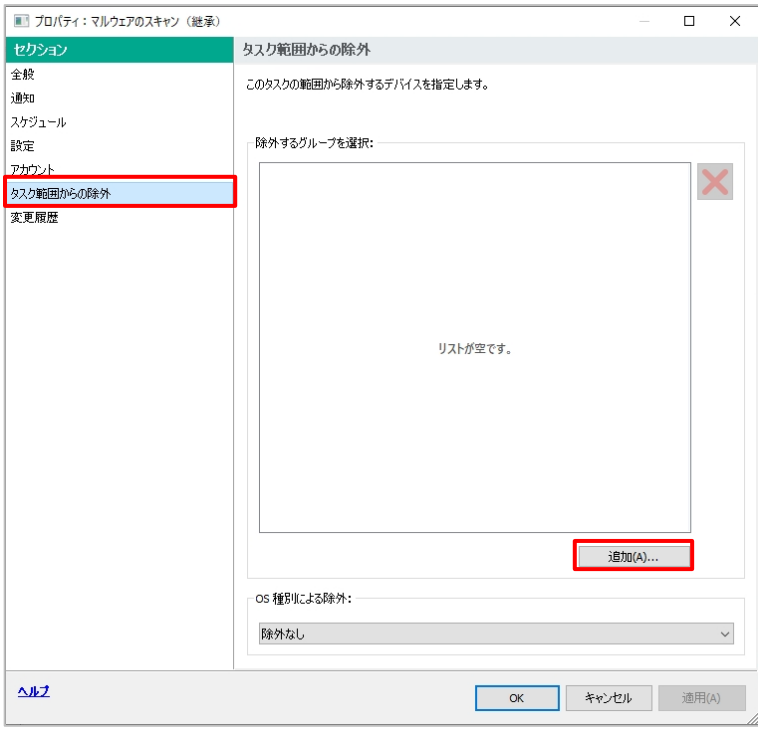
(1) 左画面にて「グループ」を選択し、「タスク」タブを開きます。



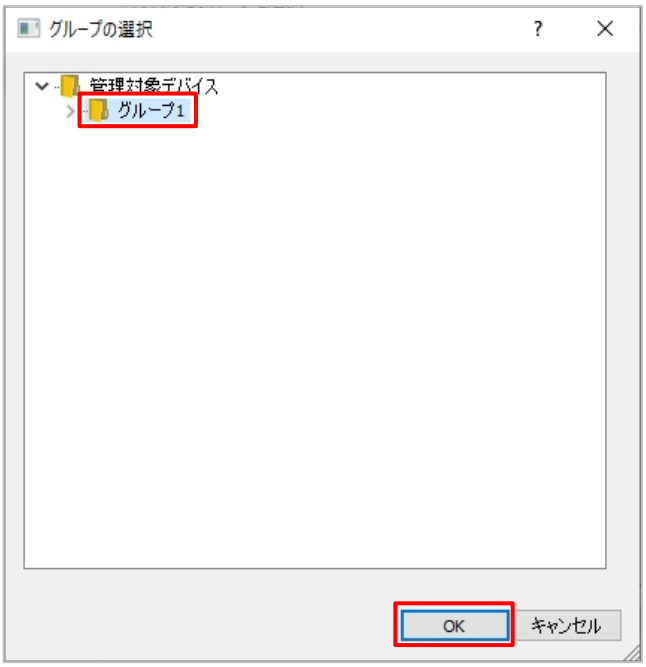
(2) 設定対象となるタスクを右クリックして「プロパティ」を選択、またはダブルクリックしてプロパティ画面を開きます。



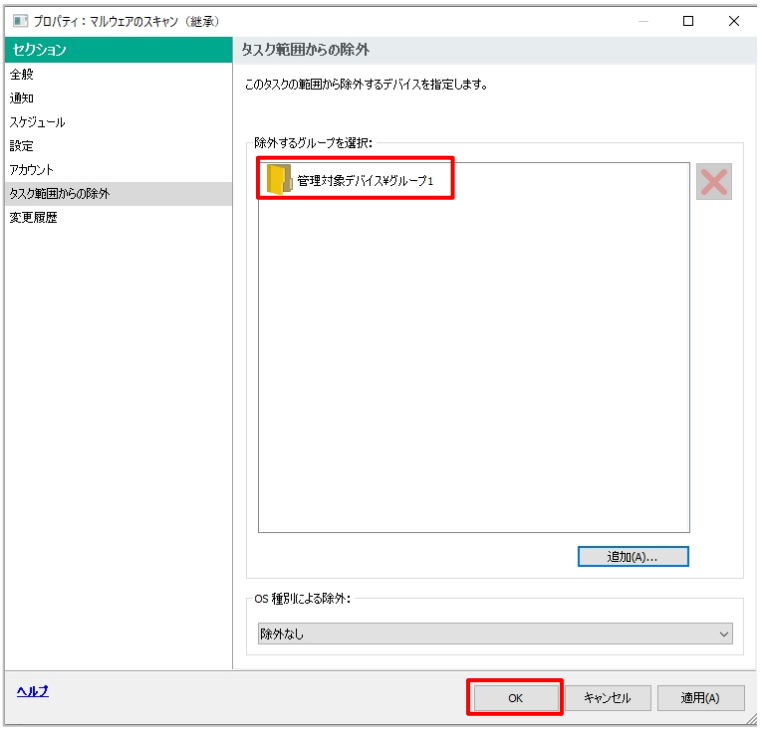
(3) 「タスク範囲からの除外」セクションにて「追加」ボタンをクリックします。



(4) このタスクの実行対象から除外したいグループを選択し、「OK」をクリックします。



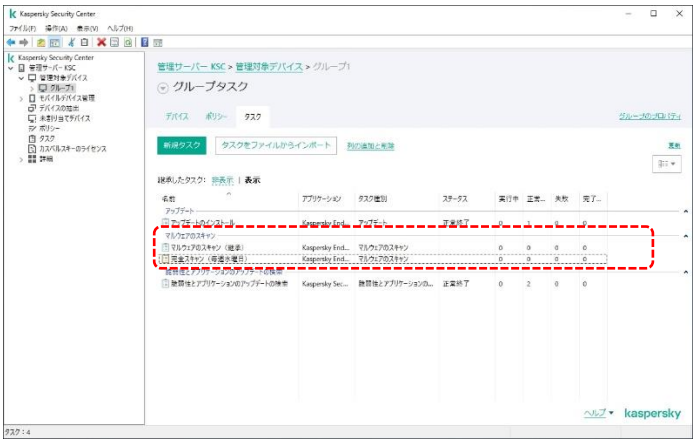
(5) (4)で選択したグループが追加されたことを確認し、「OK」をクリックします。



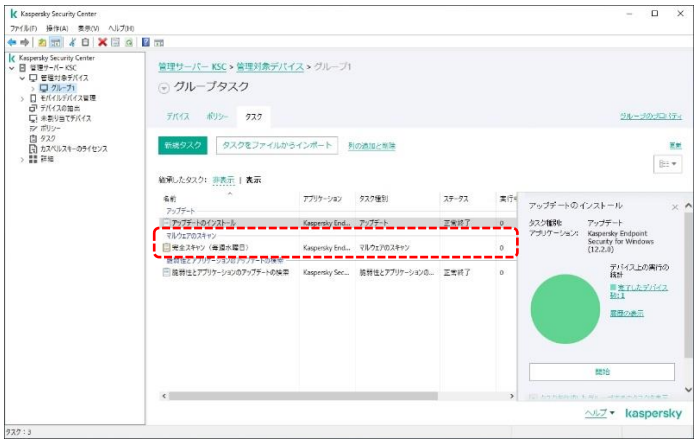
(6) これで、タスク「マルウェアのスキャン（継承）」タスクから「グループ 1」グループが除外されました。

継承から除外されているかどうかは、グループの「タスク」タブでも確認できます。

<除外前>



<除外後>



本節は以上です。

4.6. 特定のコンピューターに対するタスク

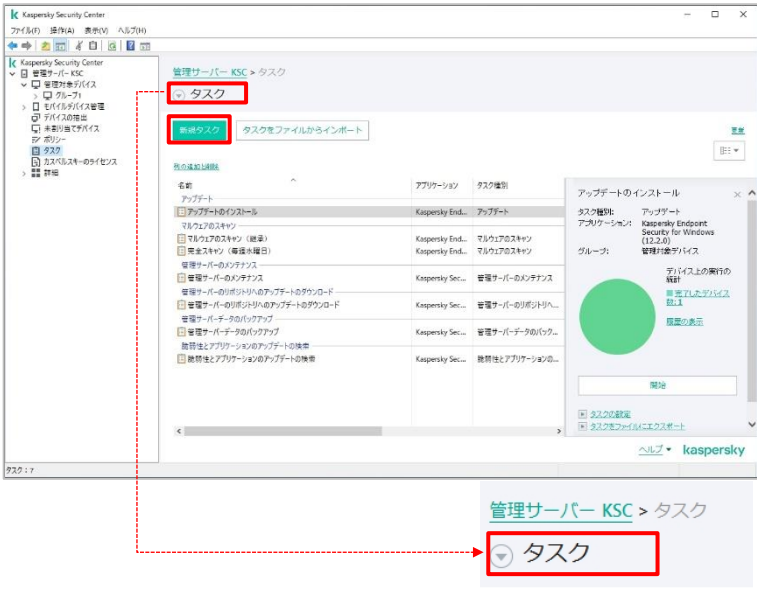
普段使用しているグループとは別に、特定のデバイスでタスクを実行したい場合は「**特定のコンピューターに対するタスク**」としてタスクを作成します。

長期間スキャンされていないデバイスや IP アドレス、対象デバイスを手動で選択などの条件設定が可能です。

特定のコンピューターに対するタスクは、以下の手順で作成します。

(1) 左画面にて「タスク」を選択し、右画面にて「新規タスク」をクリックします。

※「新規タスク」ボタンが表示されていない場合は「▲」をクリックしてください。

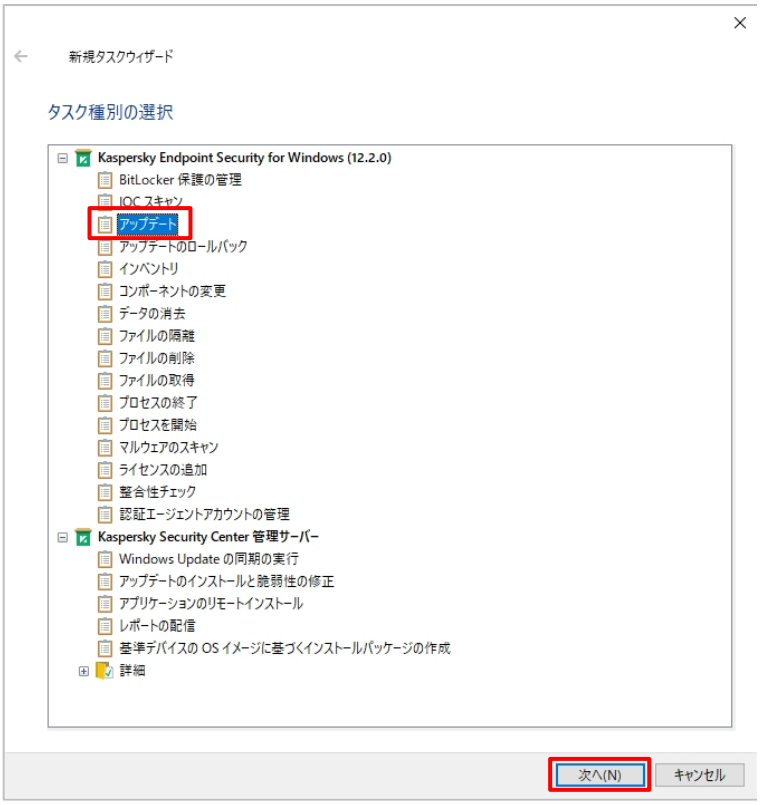


(2) 「タスク種別の選択」画面が表示されます。

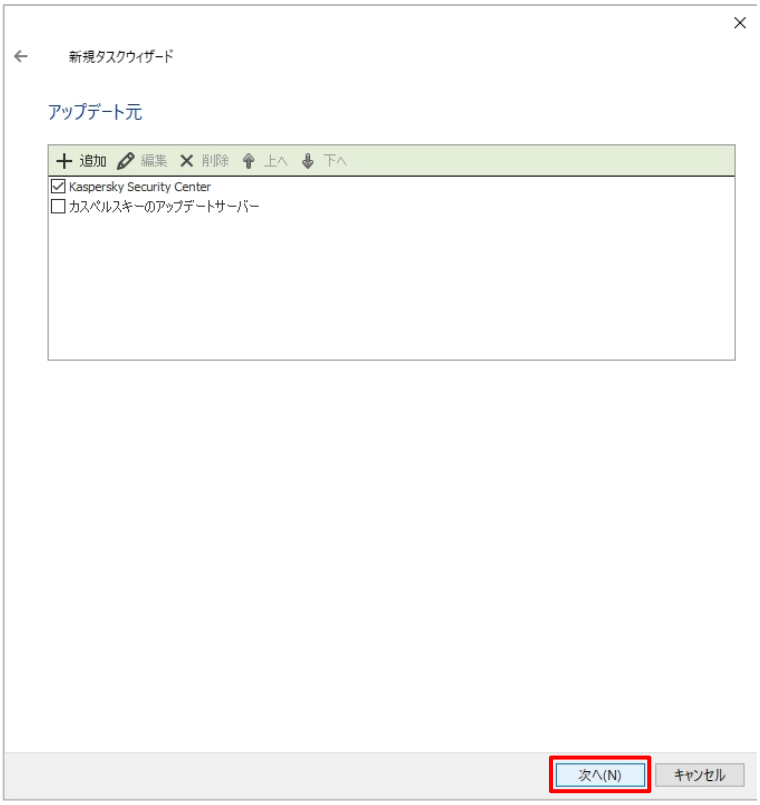
タスクの種別を選択し、「次へ」をクリックします。

ここでは「アップデート」を選択します。

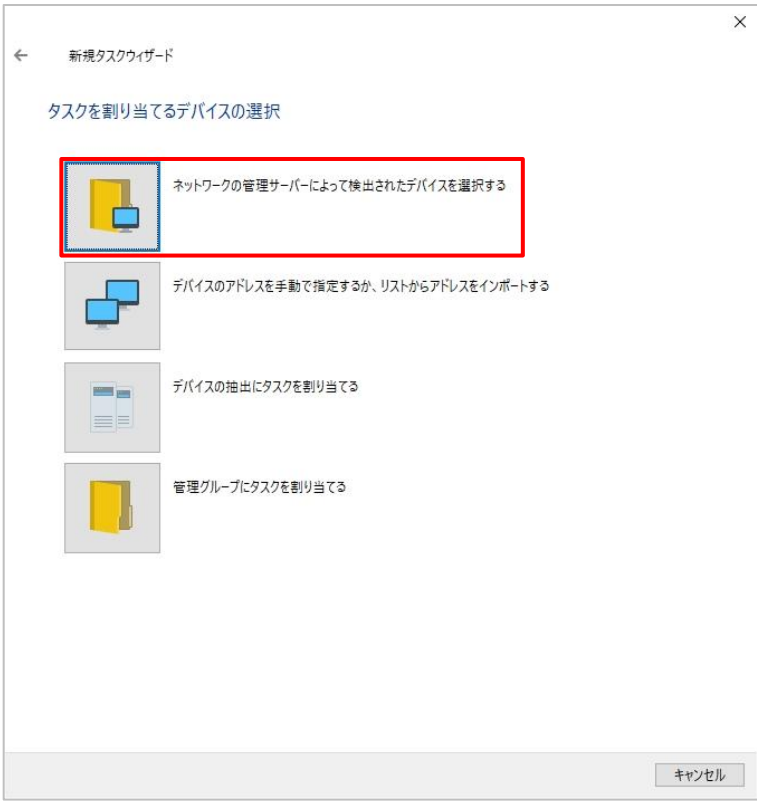
※以降の画面は選択したタスクの種別によって異なります。



(3) 「アップデート元」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。

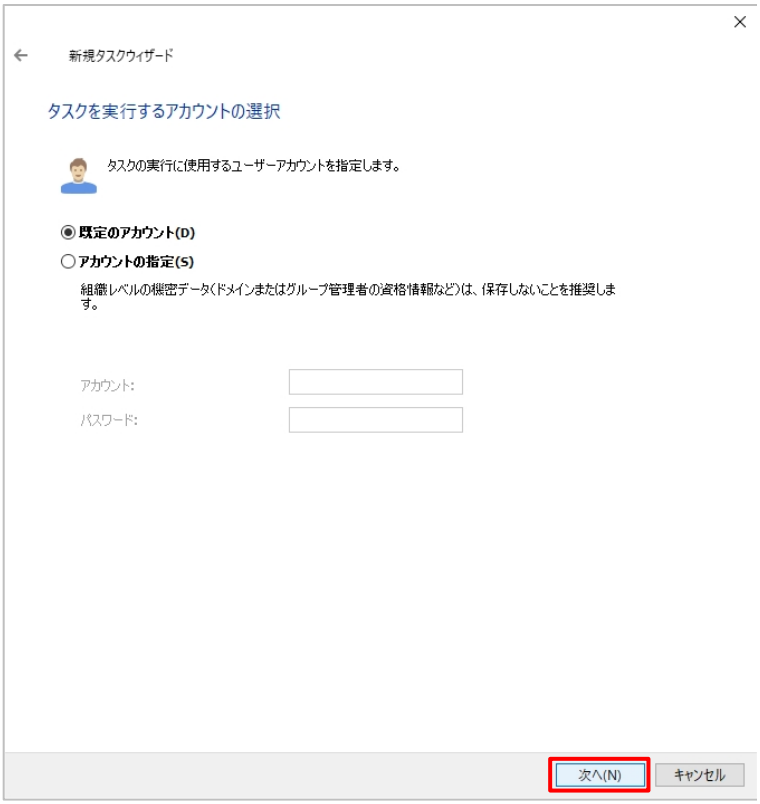


(4) 「タスクを割り当てるデバイスの選択」画面が表示されます。
タスクを実行するデバイスをどのように決めるか選択します。
ここでは、個々のデバイスを選択することができる「ネットワークの管理サーバーによって検出されたコンピューターを選択する」を選択します。



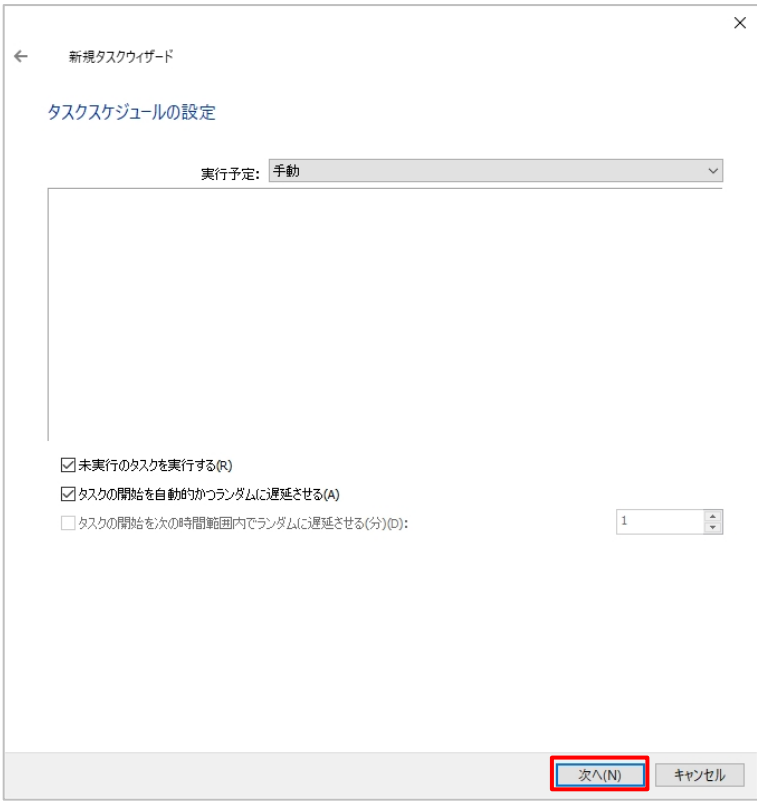
(5) 「デバイスの選択」画面が表示されます。
タスクを実行したいデバイスを選択して「次へ」をクリックします。

(6) 「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。



(7) 「タスクスケジュールの設定」画面が表示されます。
スケジュールを設定し、「次へ」をクリックします。

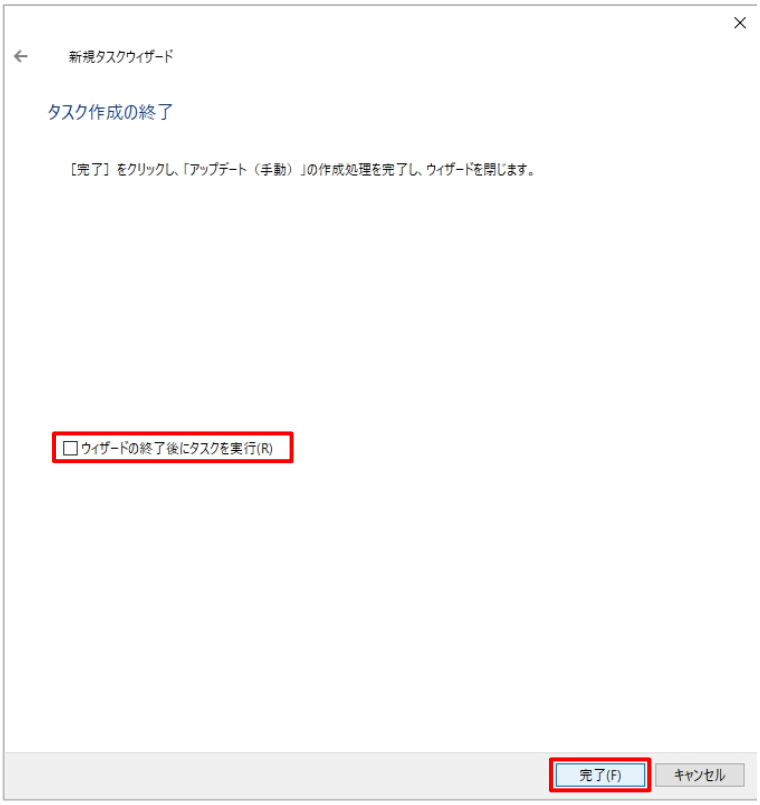
このタスクを ＫＳＣ上から管理者が任意のタイミングで実行したい場合「実行予定」を「手動」に設定してください。
スケジュールに沿って定期的に実行したい場合は「実行予定」を手動以外に変更し、実行スケジュールを設定します。



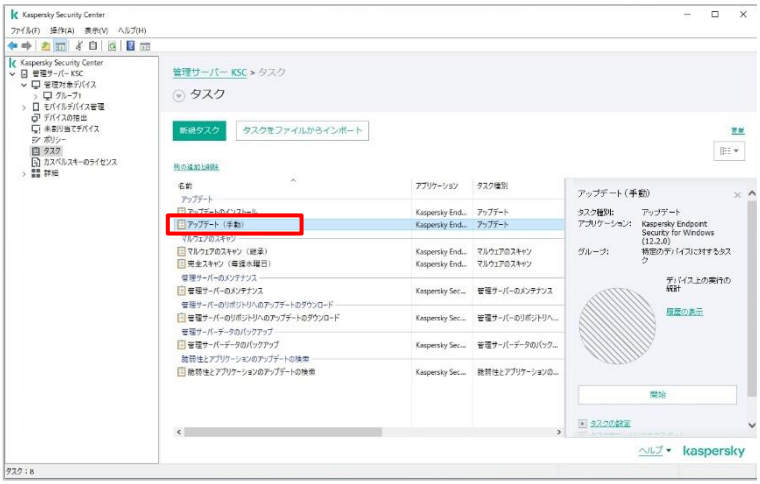
(8) 「タスク名の定義」画面が表示されます。
タスクの名前を入力し、「次へ」をクリックします。

(9) 正常に作成されたことを確認し、「完了」をクリックします。

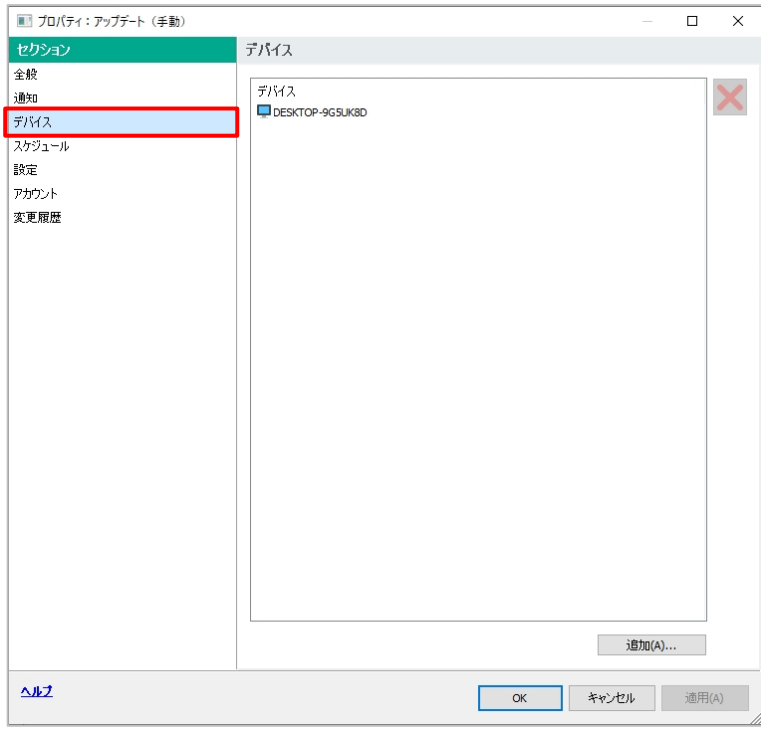
タスクをすぐに実行したい場合は「ウィザード完了後にタスクを実行する」にチェックマークを入れます。



(10) 作成されたタスクがリストに表示されます。（リストを再表示すると、グループ欄に「特定のコンピューターに対するタスク」と表示されます。）



(11)　タスクのプロパティ画面にて設定を確認・変更できます。
対象のデバイスを追加・削除したい場合は「デバイス」セクションで変更します。



本章は以上です。

kaspersky

株式会社カスペルスキー

〒101-0021 東京都千代田区外神田 3-12-8 住友不動産秋葉原ビル 7F

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