Kaspersky Endpoint Security for Windows
脆弱性診断とパッチ配布設定ガイド

2023/09/05

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. 4.1

kaspersky

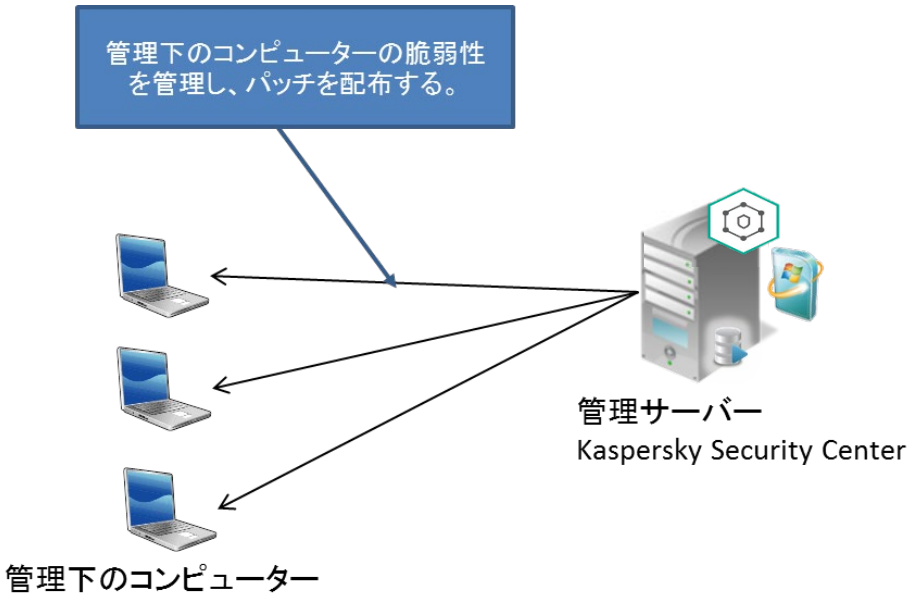
目次

1. はじめに

1.1. 本書について、前提条件

本書では、Kaspersky Endpoint Security for Windows(以降 KES)および Kaspersky Security Center(以降 KSC) による脆弱性診断やパッチ配信機能についてご説明します。
本機能を使用する権利のあるライセンスを KSC に登録する事で、KSC にてパッチの自動配布等の機能が使用可能となります。基本的な操作は全て KSC から行います。
本書を使用する際の前提条件は、以下の通りです。

- **管理サーバーとして KSC が構築されていること。**
- **KSC に Kaspersky Endpoint Security for Business Advanced、Kaspersky Endpoint Detection and Response Optimum Bundle、Kaspersky Endpoint Detection and Response Expert のライセンスが適用されていること。**
- **クライアントコンピューターに KES およびネットワークエージェントがインストールされ、KSC の管理下として登録されていること。**



KSC の構築手順については、「Kaspersky Security Center 14.2 簡単インストールガイド」をご参照ください。資料は以下の URL よりダウンロードが可能です。

https://kasperskylabs.jp/biz/

1.2. 用語説明

本書で使用される製品及び技術について、以下の通りご説明します。

- **Kaspersky Security Center（KSC）：**
  管理サーバーにインストールされた Kaspersky 製品の管理ツールです。
  Kaspersky Endpoint Security 及び ネットワークエージェント がインストールされた PC の管理と、定義データベースの配信を行います。
  「KSC」と略します。

- **Kaspersky Endpoint Security（KES）：**
  実際にウィルス対策を担う製品です。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。
  「KES」と略します。

- **ネットワークエージェント（NA）：**
  KSC とクライアント PC が通信する為に必要となるソフトです。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。
  「NA」と略します。

2. パッチ管理の課題解決及び製品の動作概要

2.1. パッチ管理の課題解決

OS 及びアプリケーションの脆弱性の修正は、マルウェア等を介した第三者からの攻撃手段に使用されてしまう恐れがあるため、セキュリティ保護とデバイス制御と同様に重要な課題です。

しかしながら、脆弱性情報の収集やパッチの適用などの作業は、セキュリティ管理者にとって大きな負担となっております。

定期的な脆弱性の修正はマルウェア等からの脆弱性を利用した攻撃に対する防御にもなります。ソフトウェアの修正は、バグフィックスやパフォーマンス改善にも寄与し、結果的に管理者の負担を軽減します。

KES は、脆弱性診断やパッチ配信機能を有し、脆弱性の修正やソフトウェアのバグフィックスなどのアップデートを実行することができます。

また、パッチ配信機能の自動化や、アップデートの結果をレポート化して把握する事も可能です。

脆弱性診断およびパッチ配信機能にて実現できることをまとめると以下のようになります。

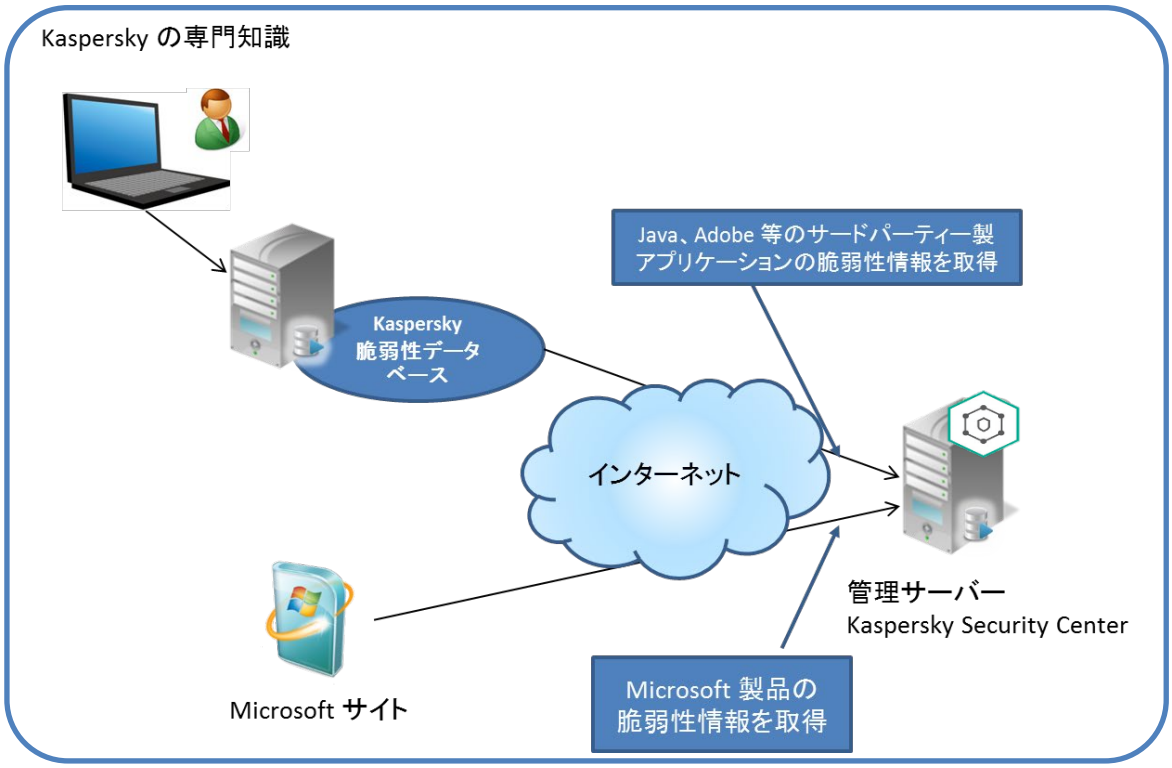
- **管理下にあるデバイスの脆弱性を把握。**
- **OS 及びアプリケーションのアップデートを自動化。**
- **脆弱性の修正を自動化。**
- **レポート機能によりアップデートの結果を把握。**

「セキュリティの向上」、「管理者に対する負担の軽減」につながります。

2.2. 脆弱性情報の取得、及び脆弱性修正の動作概要

KSC は、Windows OS やその他 Microsoft 製品のアップデート情報、脆弱性情報をインターネット上の Microsoft Update サイトから取得します。

また、サードパーティー製アプリケーションのアップデート情報、脆弱性情報をカスペルスキー脆弱性データベースから取得します。動作の概要は以下の通りです。



KSC は、取得した情報を元に管理対象コンピューターに対し、Windows OS や Microsoft 製品の脆弱性を診断し、パッチを配信する事が可能です。

KES では、以下の 2 パターンの方法を設定することができます。

パターン A：KSC を WSUS サーバーとして使用する

パターン B：外部の WSUS サーバーを使用する

いずれのパターンにおいても KSC は、脆弱性情報、アップデート情報を保持します。

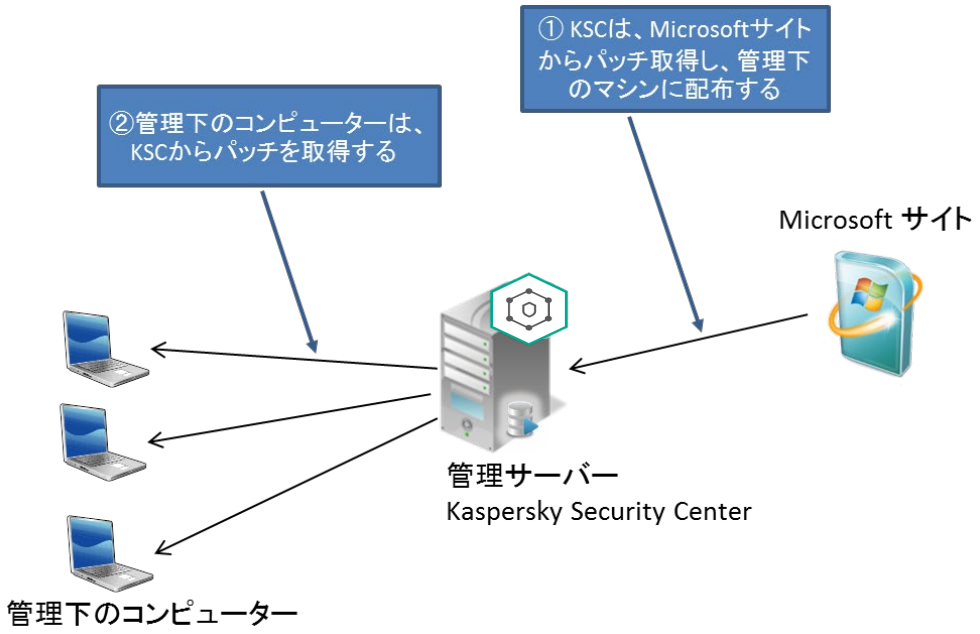
kaspersky

【Microsoft 製品のパッチ管理】

パターン A： KSC を WSUS サーバーとして使用する

KSC が WSUS サーバーとなり、パッチを配信するパターンです。

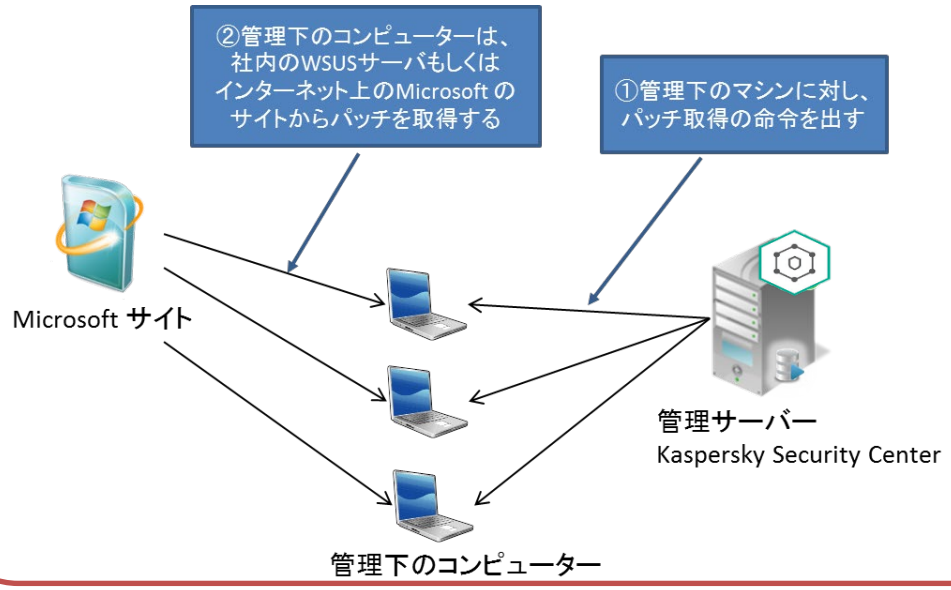
クライアントに対するパッチの更新はすべて KSC がコントロールします。



パターン B：外部の WSUS サーバーを使用する

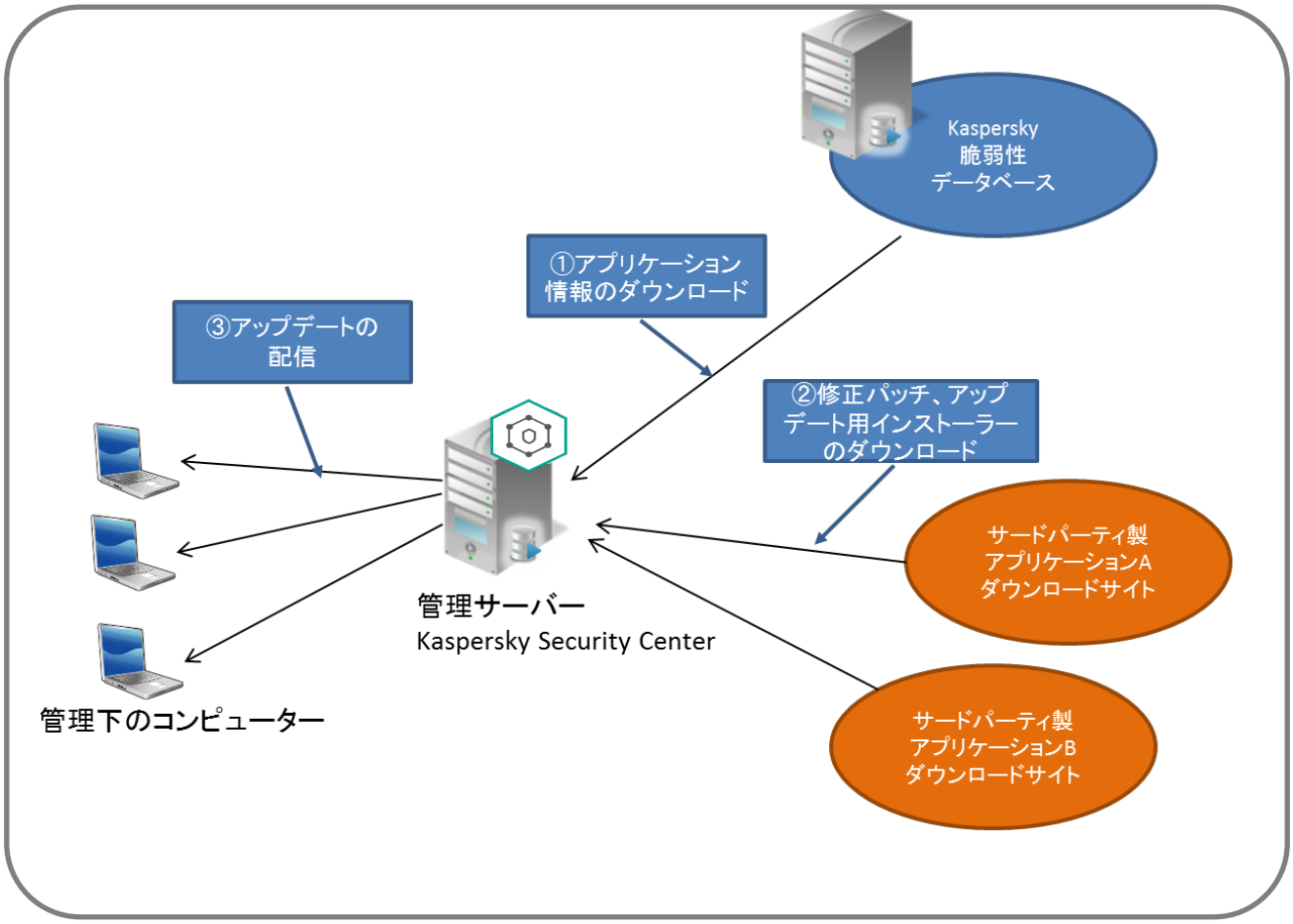
クライアントは、OS の設定や Active Directory グループポリシーの設定に従い、Windows Update にてパッチをダウンロードします。

KSC はクライアントの脆弱性情報を管理し、選択したパッチを WSUS サーバー（もしくはインターネット上の Microsoft アップデートサイト）からインストールする様、指示を出すことができます。



【サードパーティ製アプリケーションのパッチ管理】

同様にサードパーティ製アプリケーションの脆弱性を診断し、アップデートパッチを配信する事が可能です。動作の概要は以下の通りです。



3. 環境構成時の注意点

脆弱性診断とパッチ配布機能を使用する場合の注意点についてご説明します。

①コントロールできる OS は Windows のみ

脆弱性情報の収集やパッチ配信ができるのは「Windows OS のみ」となります。
その他の OS（Mac, Android, Linux など）は本機能を使用できません。

※ KSC 管理サーバーにて Mac OS, Linux などカスペルスキー製品が導入されているデバイスを管理することは可能です。

②脆弱性診断およびパッチ配信用として専用サーバーを用意

脆弱性診断およびパッチ配信機能の利用には多くのリソースを消費するため、Active Directory などのサーバーと同居するのではなく、専用サーバーを用意してください。

③KSC がインターネットへ接続できること

本機能を有効後、KSC はインターネットへ接続し、Windows Update 情報の取得、また修正パッチやサードパーティ製アプリケーションのダウンロードを行います。
そのため、KSC がインターネットへ接続できる構成である必要があります。

④十分なディスク空き容量を用意

使用する KSC 管理サーバー上の **C ドライブ**に十分なディスク空き容量を用意してください。
Windows パッチやサードパーティ製インストーラーを格納する領域として必要となります。
「KSC 管理者ガイド P.30」には "少なくとも 100GB 以上の空き容量が必要" と記載されておりますが、**1TB** 程度の空き容量を用意することを推奨します。

注1) 実際に使用されるディスク領域はクライアントコンピューター数、OS の種類、パッチ、アップデート数などに依存します。

注2) パッチやアプリケーションのインストーラーは KSC 上に残り続け、自動的に削除されません。ディスク容量不足が発生した場合は「Appendix 1.アップデートファイルの削除」を実施してください。

kaspersky

⑤ ネットワーク負荷の考慮

本機能の導入当初など、多くの MS パッチやアップデートがある場合、**配信用データとして数 GB のファイル**が各クライアントへ転送される場合があります。**本機能による運用を開始する前に、各クライアントにて Windows Update を実施いただき、最新の状態にすることをお勧めします。**
また、以下のような環境に該当する場合は、ネットワーク上に大量の配信用データが流れ、業務に影響を及ぼす可能性があります。

- **データセンターに KSC があり、クライアント拠点とは離れた場所にある。**
  ⇒ クライアント拠点にディストリビューションポイントの設置をご検討ください。
- **拠点が全国にあり、KSC とは WAN を介する。**
  ⇒ 拠点毎にディストリビューションポイントの設置をご検討ください。
- **ネットワークの転送速度が遅い。**
  ⇒ ディストリビューションポイントの設置、タスクの分散実行をご検討ください。

⑥ ディストリビューションポイントは専用サーバーを用意

ディストリビューションポイントを使用する場合は専用のサーバーを用意することを推奨します。
また、クライアントへの配信用データが保管されるため、KSC と同等のディスク空き容量を用意することを推奨します。

注1) 「ディストリビューションポイント」の詳細は「ディストリビューションポイント設定ガイド」を参照してください。

注2) ワークステーションも指定可能ですが、OS として同時接続数(20 台)の制限があります。

⑦ タスク実行対象クライアントの分散化

対象端末が多く、また多くのアップデートがある場合は、数台ずつに分けてタスクを実行してください。
「アップデートのインストールと脆弱性の修正」タスクは、タスクの実行対象となるクライント全台に対し同時に開始されるためです。（ランダム実行はできません）

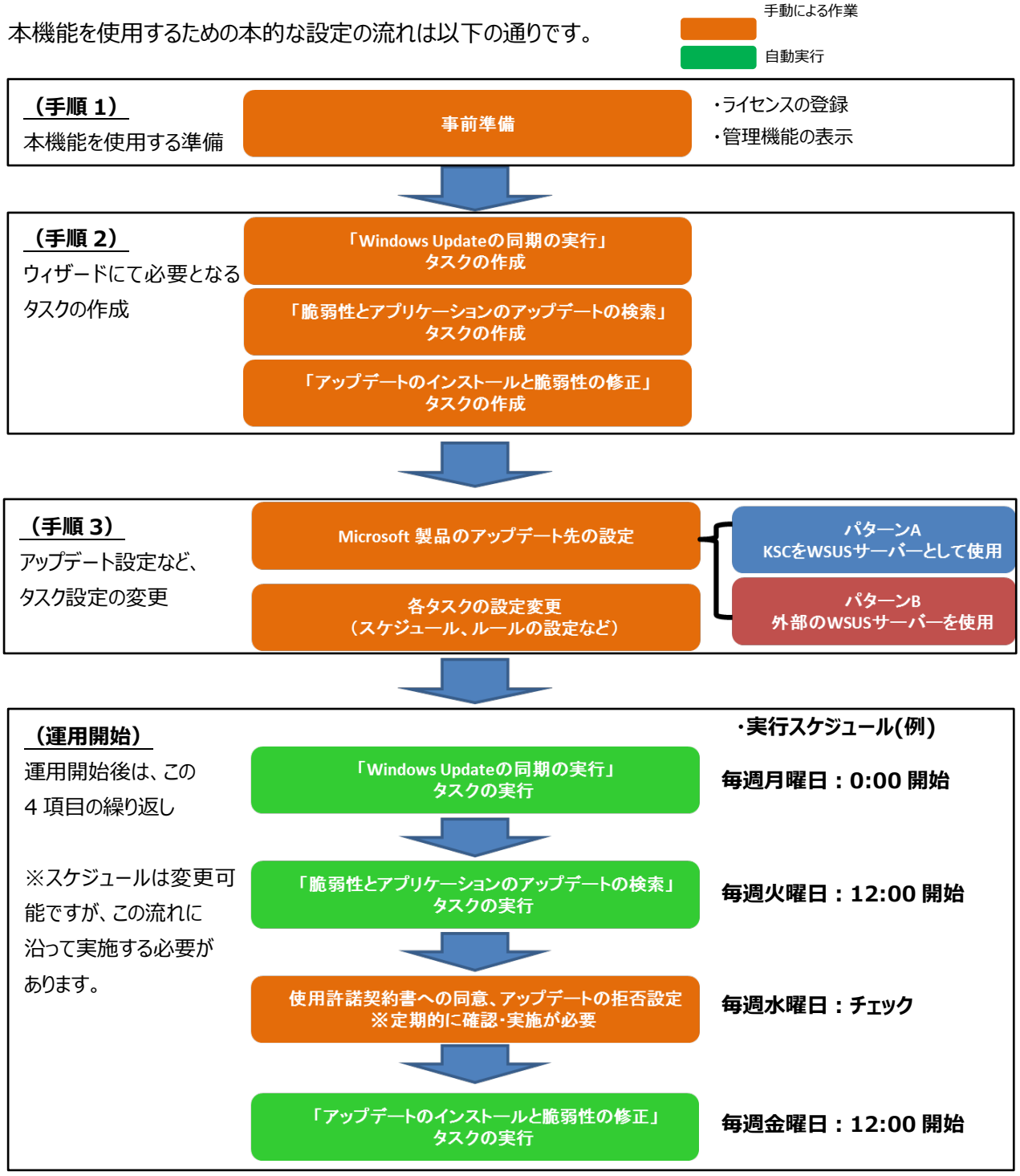
⑧「Windows Update の同期の実行」タスクは必ず修正する

本機能では、Windows Updates のメタデータ情報を取得する「Windows Update の同期の実行」タスクが動作します。既定の設定ではすべての Microsoft 製品の情報をダウンロードするよう設定されており、大量のデータがデータベースに格納されます。
SQL Express を使用している場合、データベースサイズに 10GB の上限があるため、大量のデータが格納され 10GB に達すると KSC が起動できなくなる可能性があります。
アップデート対象の OS や製品、言語を絞ることでこの問題を避けることができます。詳細は後述の手順「5.2.1. 「Windows Update の同期の実行」タスクの設定変更」をご参照ください。

kaspersky

4. 設定の流れ

本機能を使用するための本的な設定の流れは以下の通りです。



※「Windows Update の同期」タスクは初回起動時、時間(数時間)がかかります。
初回起動後、アプリケーショのリストが更新されるため、選択項目を確認し、再度実行してください。

設定の流れについては、次ページ以降でご説明します。

本手順では上記スケジュールにてタスクを実行する手順をご案内します。

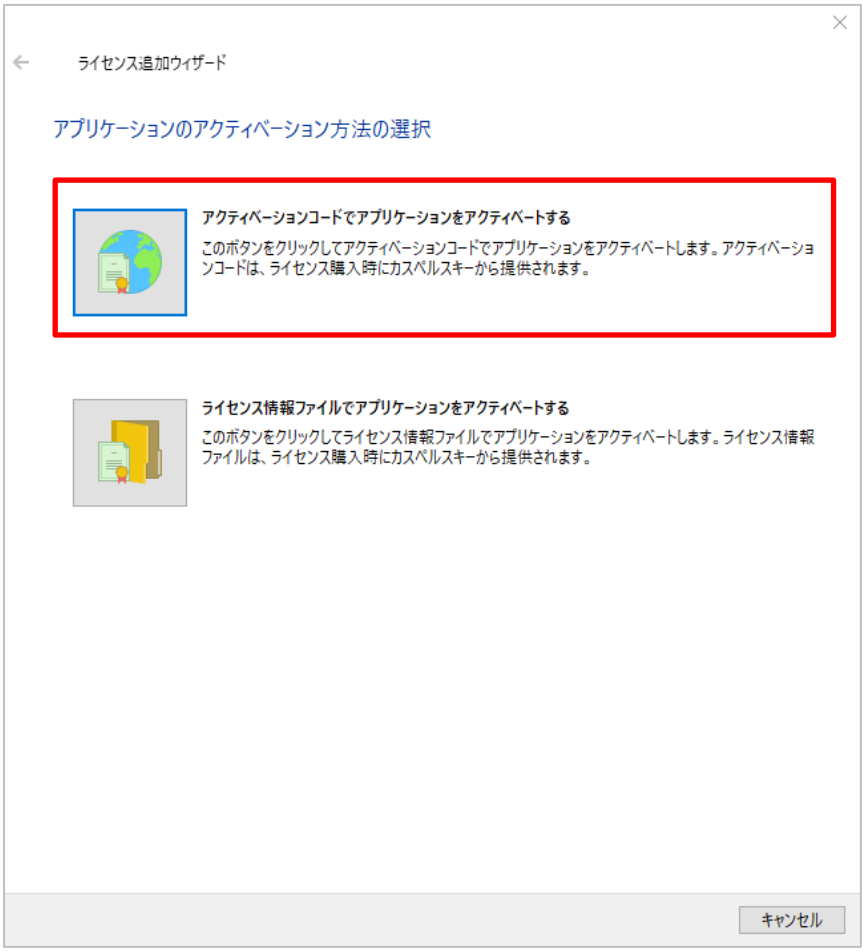
5. 事前準備

5.1. ライセンスの登録

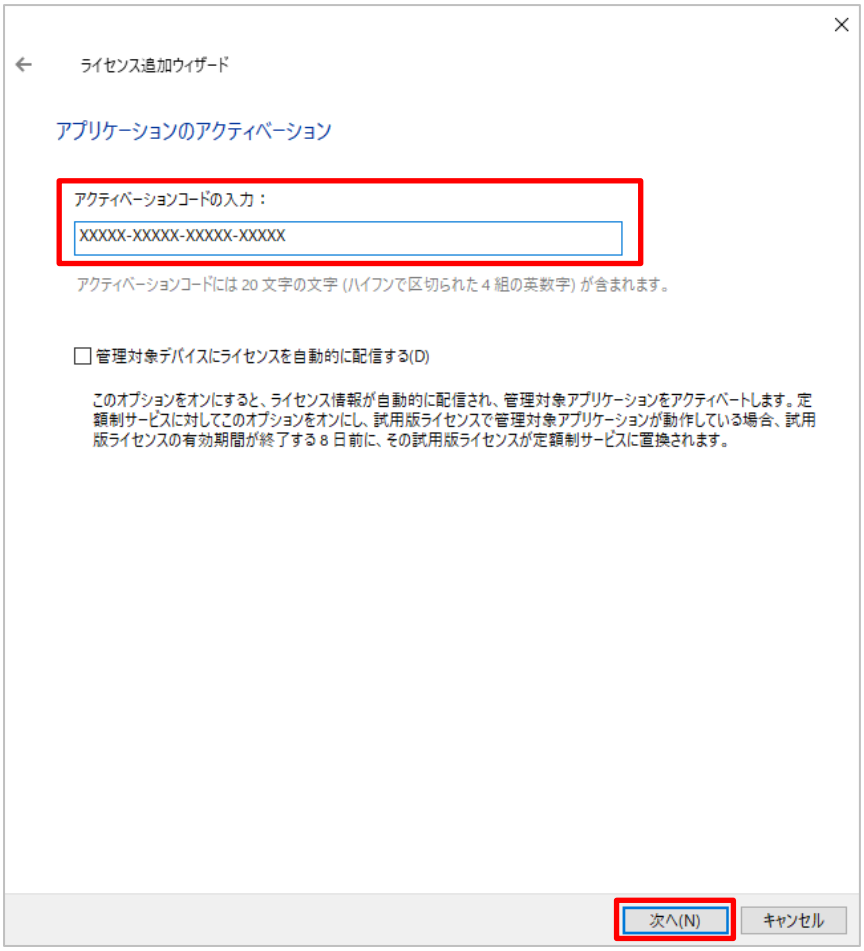
管理サーバー上で 脆弱性診断とパッチ配信機能が使用できるよう、ライセンスの登録を行います。

(1) KSC にて「管理サーバー」-「カスペルスキーのライセンス」を開き、右画面にて「アクティベーションコードまたはライセンス情報ファイルの追加」をクリックします。

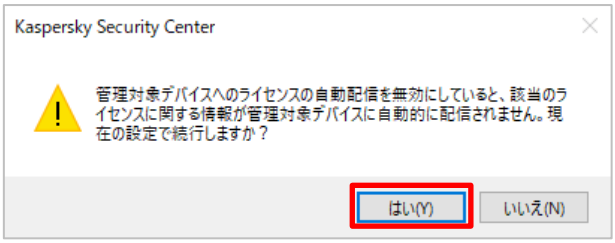
(2) 「ライセンス追加ウィザード」にて「アクティベーションコードでアプリケーションをアクティベートする」をクリックします。



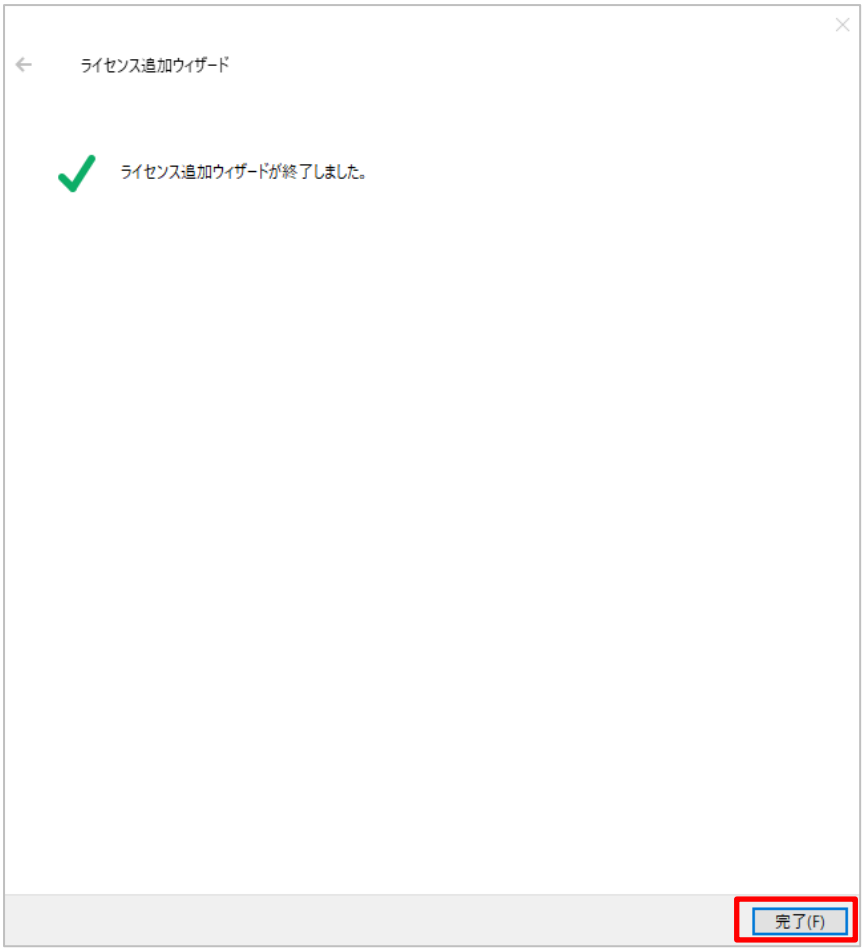
(3) アクティベートコードを入力し、
「次へ」をクリックします。



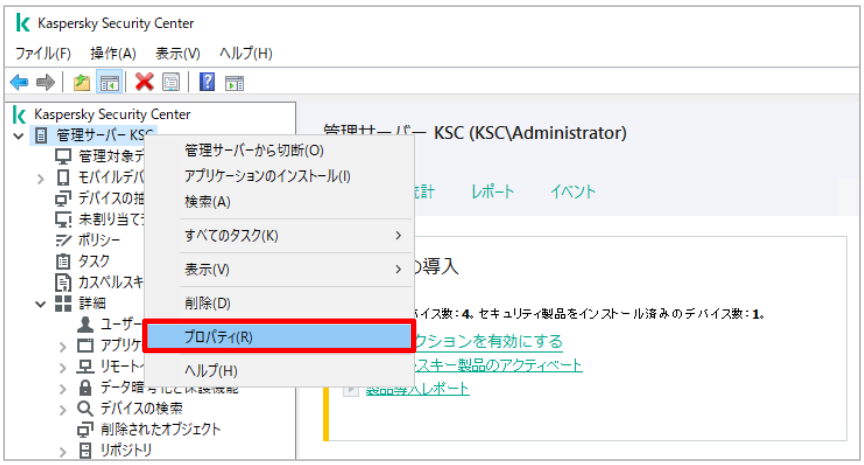
(4) 右のダイアログが表示されたら、
「はい」をクリックします。



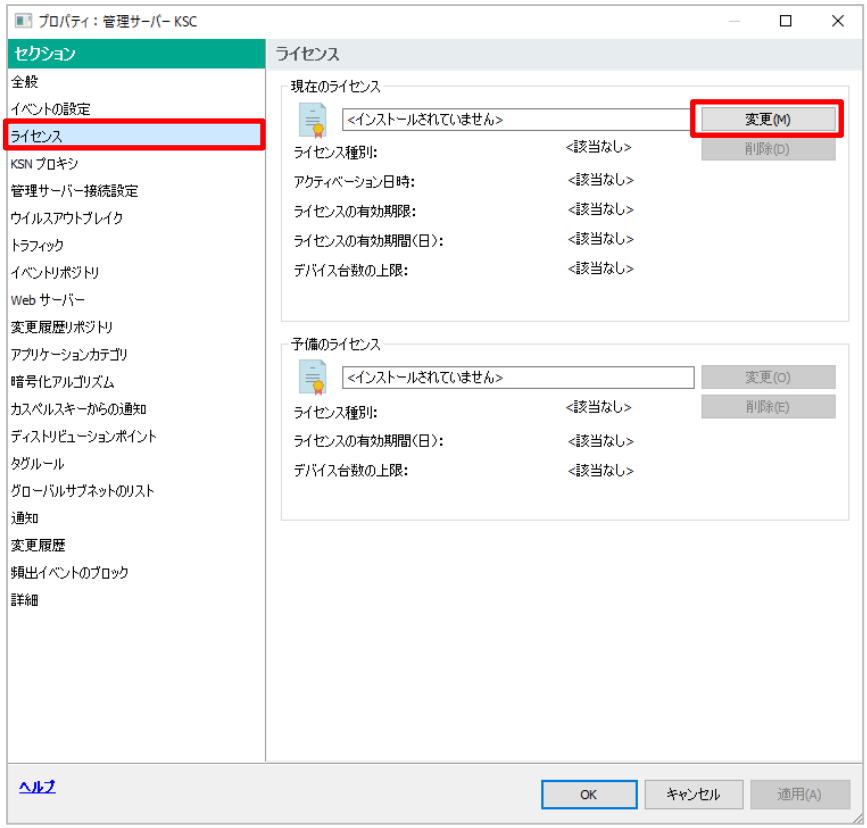
(5) 「ライセンス追加ウィザードを正常に完了しました」と表示されることを確認し「完了」をクリックします。



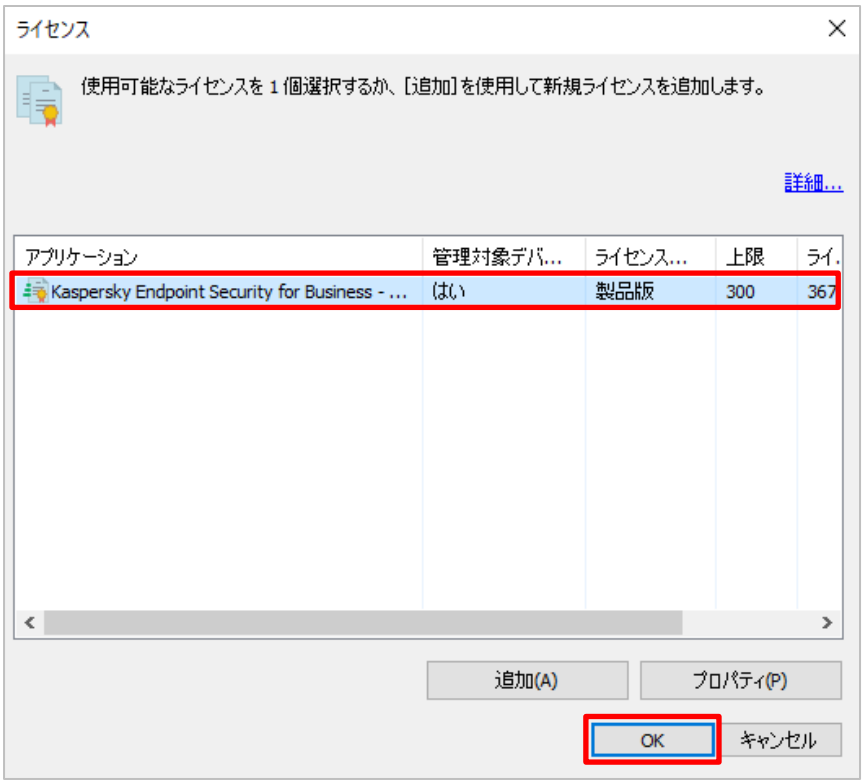
(6) 「管理サーバー」を右クリックし、「プロパティ」をクリックします。



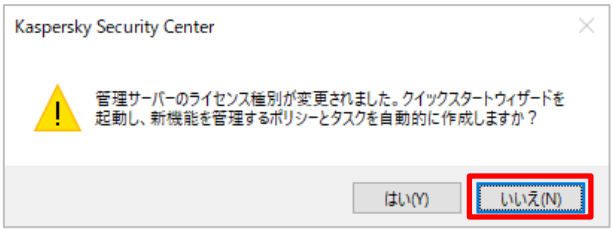
(7) 「ライセンス」セクションを開き、「変更」ボタンをクリックします。



(8) 一覧から”(1)”で追加したライセンスを選択し、「OK」をクリックします。

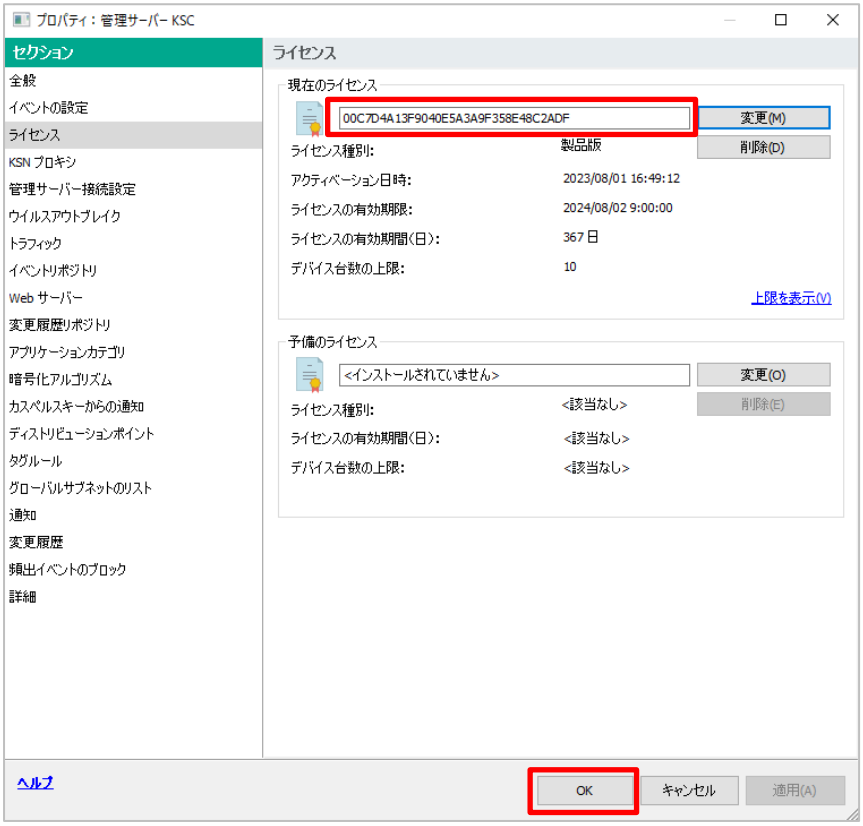


(9) 右のダイアログが表示されるので「いいえ」をクリックして閉じます。



ウィザードは後からでも起動できます。
手順は「**5.「管理サーバークイックスタートウィザード」によるタスクの設定**」をご参照ください。

(10) ライセンスが追加されたことを確認し、「OK」をクリックします。



本節は以上です。
続いて、本機能の操作ができるよう、管理項目を表示する設定を行います。

5.2. ディストリビューションポイント自動割り当て設定の解除

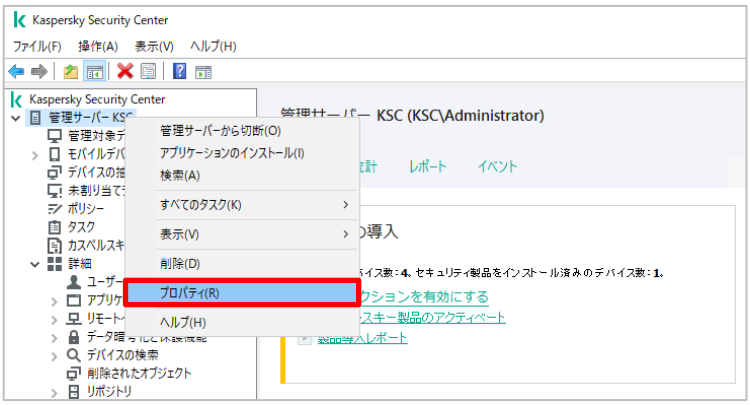
ディストリビューションポイントの自動割り当て設定を解除する手順をご説明します。

「ディストリビューションポイント」とは、定義データベースやインストールパッケージの配信元となり、KSC への接続の集中化を避け、分散する機能になります。

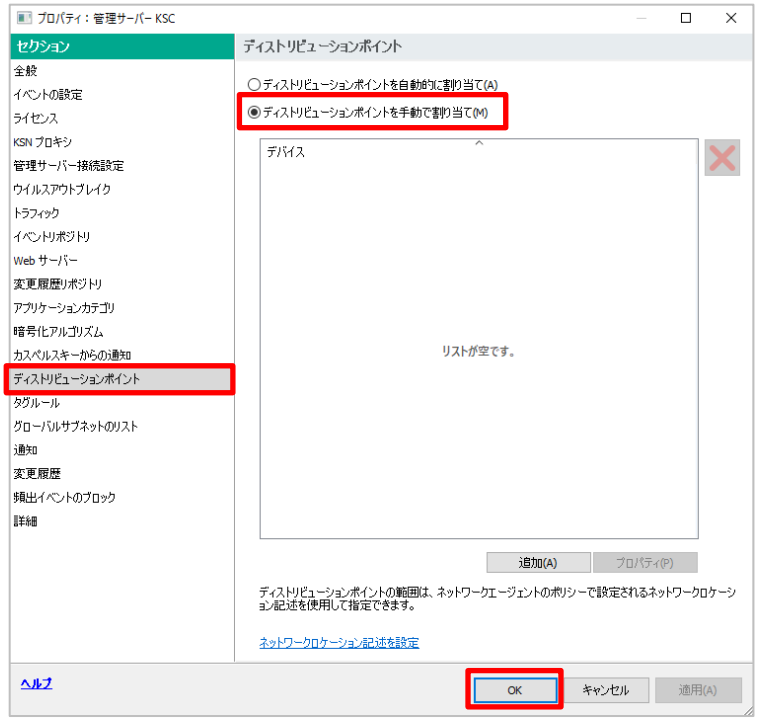
この機能は既定で、管理下の端末を自動的に選定し、ディストリビューションポイントとして指定する設定となっております。普段使用しているクライアントコンピューターが指定される可能性もあり、ディスク使用量の増加や、意図しない通信の発生など、予期せぬ問題が発生する可能性があります。

この問題を避けるため、事前にディストリビューションポイントの自動割り当て設定の解除を推奨しております。以下に手順をご説明します。

(1) KSC 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) 「ディストリビューションポイント」セクションを選択します。
「ディストリビューションポイントを手動で割り当て」を選択し、「OK」をクリックします。



本節は以上です。

「ディストリビューションポイント」の詳細、設定方法につきましては、「ディストリビューションポイント設定ガイド」を参照してください。

5.3. Microsoft 製品用パッチ、サードパーティ製アップデート用ファイルの保管先変更

Microsoft 製品パッチ、サードパーティ製アップデート用ファイルの保存場所を変更する手順をご説明します。

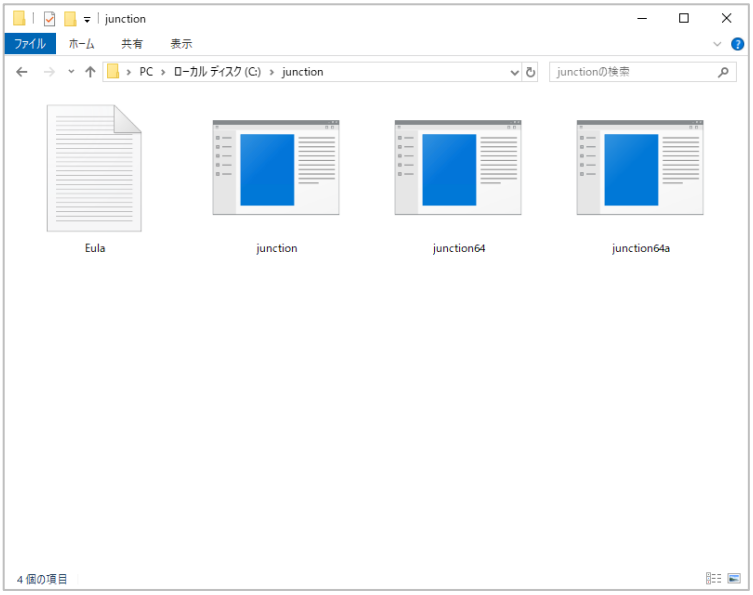
ダウンロードしたパッチやインストーラーは、既定で C ドライブの以下フォルダー配下に格納されます。

・C:¥ProgramData¥KasperskyLab¥adminkit¥

元々C ドライブのディスク容量が少ない場合や、運用開始後にディスク容量が不足した場合、本手順を実行し、保存先を変更してください。

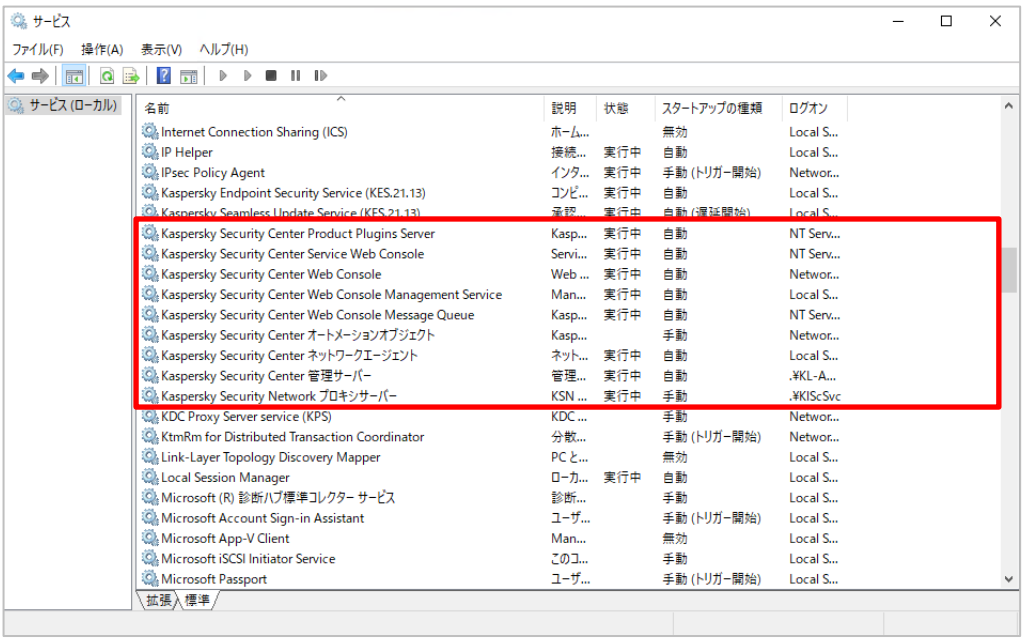
(1) Junction.exe を以下のサイトからダウンロードします。
https://docs.microsoft.com/ja-jp/sysinternals/downloads/junction

(2) ダウンロードしたファイルを KSC 上に解凍します。ここでは、C:¥junction に解凍しています。



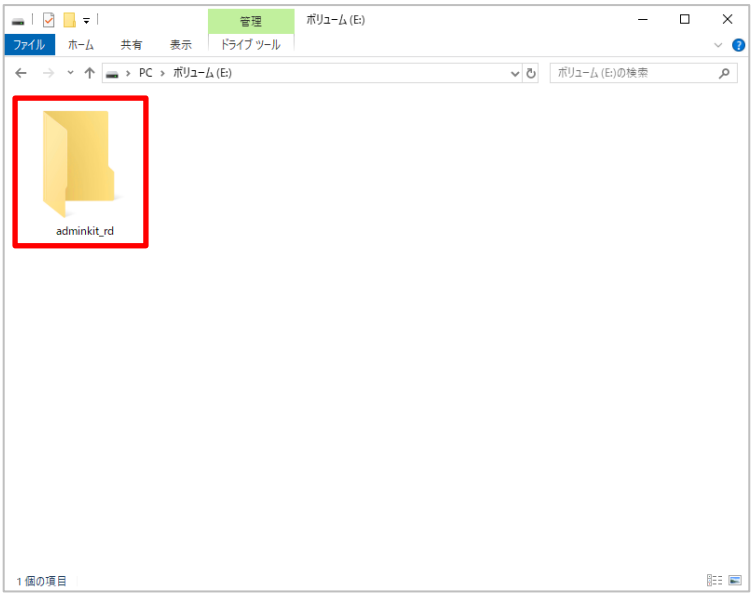
(3) サービスマネージャーを開き、以下サービスをすべて停止します。（インストール方法により存在しないサービスもあります。）

- Kaspersky Security Center Product Plugins Server
- Kaspersky Security Center Service Web Console
- Kaspersky Security Center Web Console
- Kaspersky Security Center Web Console Management Service
- Kaspersky Security Center Web Console Message Queue
- Kaspersky Security Center オートメーションオブジェクト
- Kaspersky Security Center ネットワークエージェント
- Kaspersky Security Center 管理サーバー
- Kaspersky Security Network プロキシサーバー

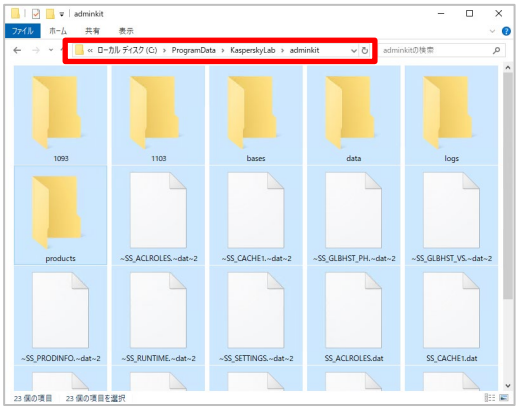


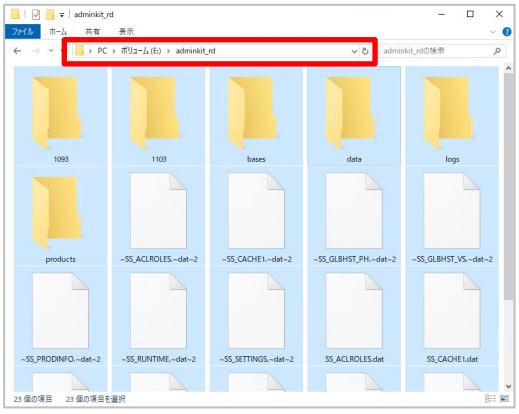
(4) 変更先ドライブにフォルダーを作成します。
本書では、以下フォルダーを変更先とします。

・E:¥adminkit_rd



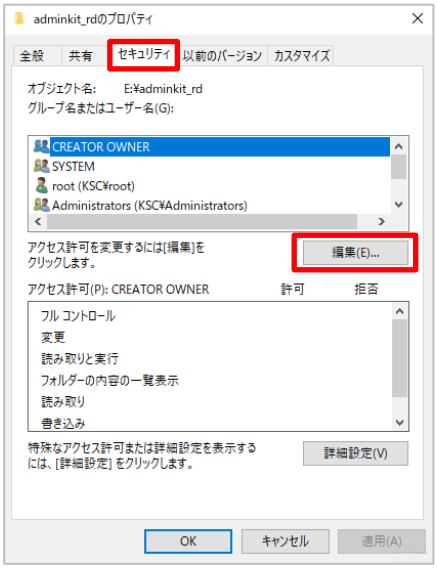
(5) C:¥ProgramData¥KasperskyLab¥adminkit フォルダー内のファイルをすべて
E:¥adminkit_rd フォルダーへコピーします。
（事前にエクスプローラーのフォルダーオプションにて、隠しファイル、フォルダーを表示するよう設定してください）



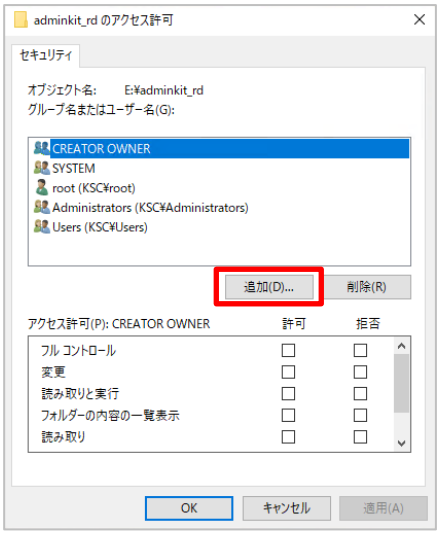


(6) E:¥adminkit_rd のアクセス権を
C:¥ProgramData¥Kaspersky-Lab¥adminkit と同様の
設定とします。

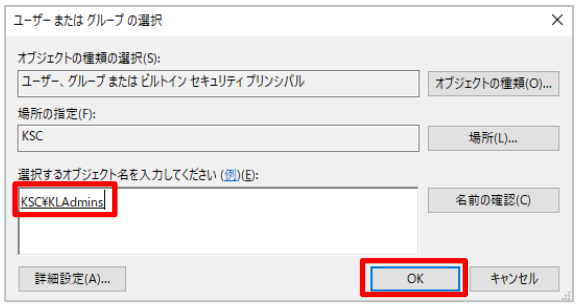
E:¥adminkit_rd フォルダーを右クリックし、「プロパティ」を選択します。そして「セキュリティ」タブをクリックし、「編集」をクリックします。



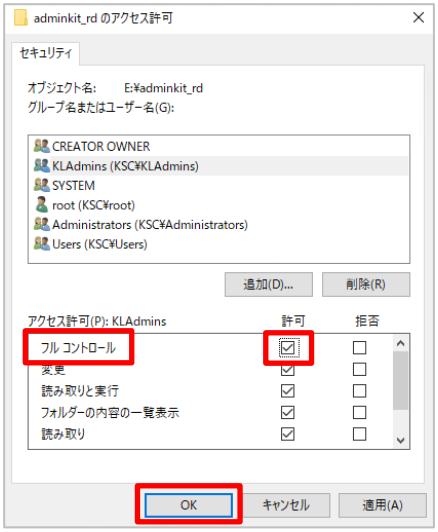
(7)「追加」タブをクリックします。



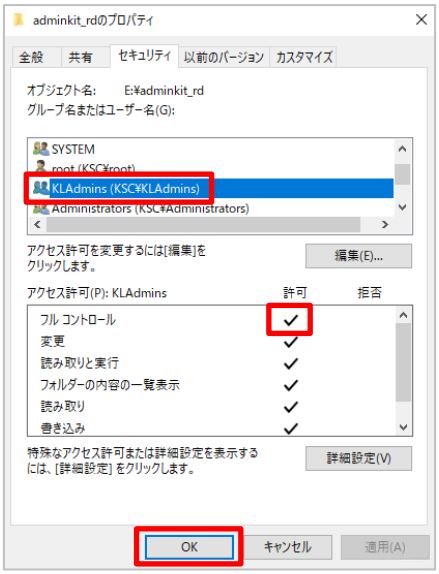
(8)「選択するオブジェクト名を入力してください」欄に「KLAdmins」と入力し、「名前の確認」をクリックして間違いがないことを確認後、「OK」をクリックします。



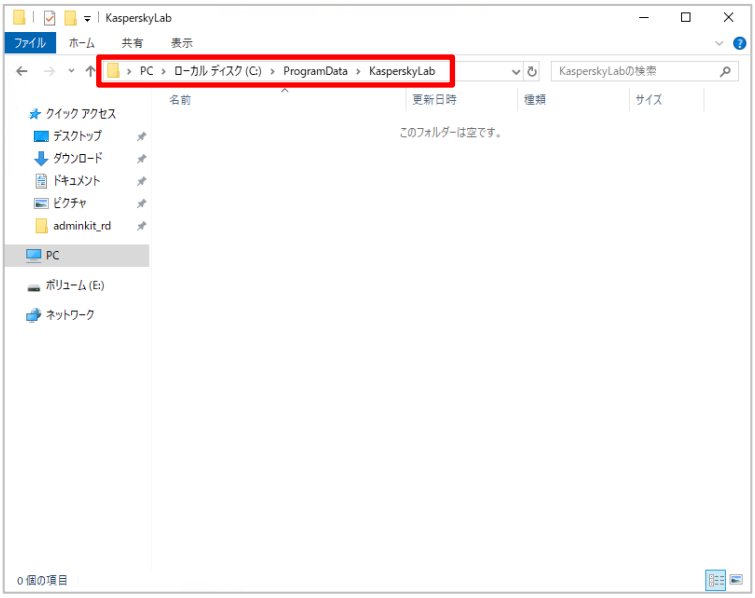
(9)「KLAdmins」が追加されていることを確認します。
「フルコントロール」にチェックを入れ、「OK」をクリックします。



(10)　「KLAdmins」が存在し、「フルコントロール」が「許可」になっていることを確認し、「OK」をクリックします。



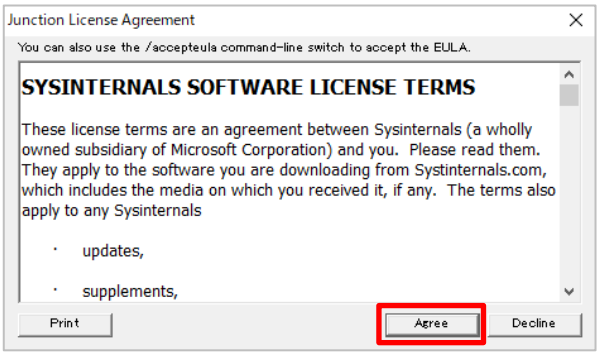
(11)　C:¥ProgramData¥Kaspersky-Lab 配下の adminkit フォルダーを削除します。



(12)　コマンドプロンプトを管理者権限で起動し、以下コマンドを実行します。

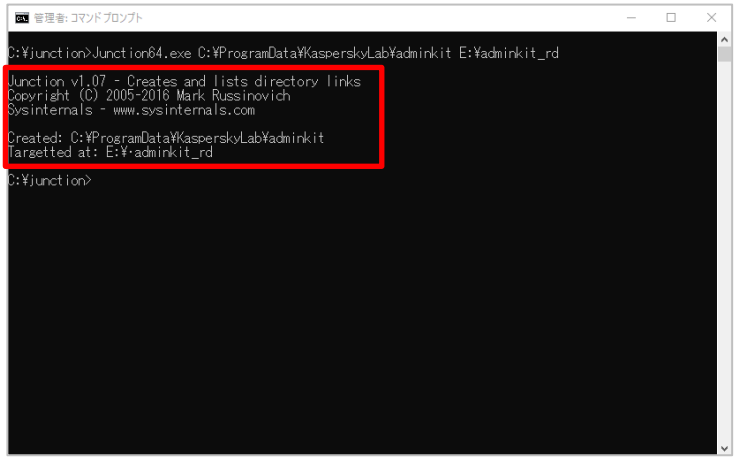
Junction64.exe C:¥ProgramData¥KasperskyLab¥adminkit E:¥adminkit_rd

Junction64.exe の起動が初めての場合、図の様なウィンドウが表示されるので「Agree」をクリックします。

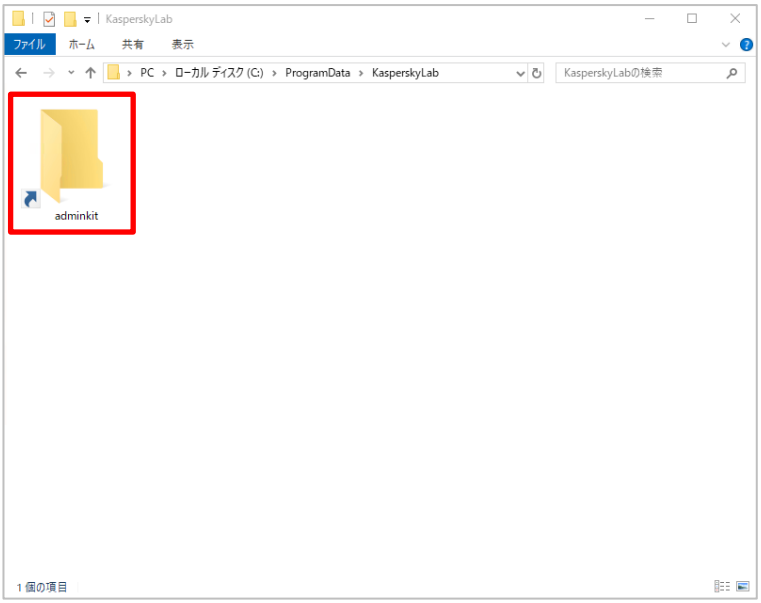


(13)　コマンドが正常に実行されると以下内容が出力されます。

Created: C:¥ProgramData¥KasperskyLab¥adminkit
Targetted at : E:¥adminkit_rd



(14)　C:¥ProgramData¥Kaspersky-Lab¥ 配下に図の様な adminkit フォルダーのショートカットが作成されていることを確認します。



(15)　“(3)”で停止したサービスをすべて起動し（または OS 再起動）、KSC 管理コンソールが正常に起動し、操作可能であることを確認します

本章は以上です。

6. 「管理サーバークイックスタートウィザード」によるタスクの設定

本機能の設定をウィザードで実施する方法をご説明します。
以下手順にてウィザードを実行することで、脆弱性管理に必要となるタスクを作成することができます。

【注意】

✓ **KSC を新規構築する場合**

⇨ **「6.1 管理サーバークイックスタートウィザード」**を参考に、手順を実行してください。

✓ **既に KSC 管理サーバーを運用中の環境に対し、追加で本機能の設定する場合**

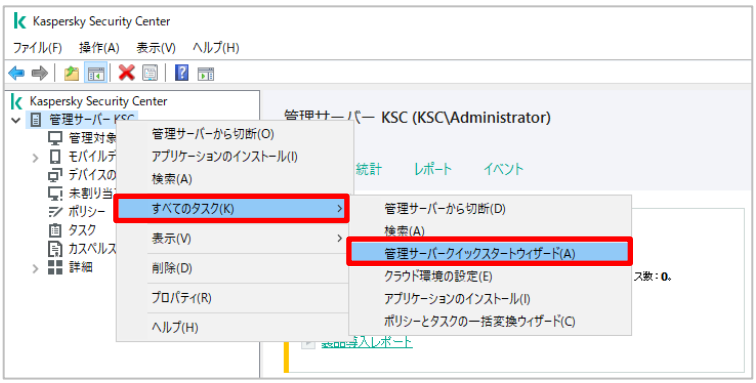
⇨ Appendix に記載されている**「2.「アップデートのインストールと脆弱性の修正」タスクの手動作成、及び詳細」**を参考に、**「手動」**で本機能のタスクを作成してください。

- 2.「アップデートのインストールと脆弱性の修正」タスクの手動作成、及び詳細
- 3.「Windows Update の同期の実行」タスクの手動作成
- 4.「脆弱性とアプリケーションのアップデートの検索」タスクの手動作成

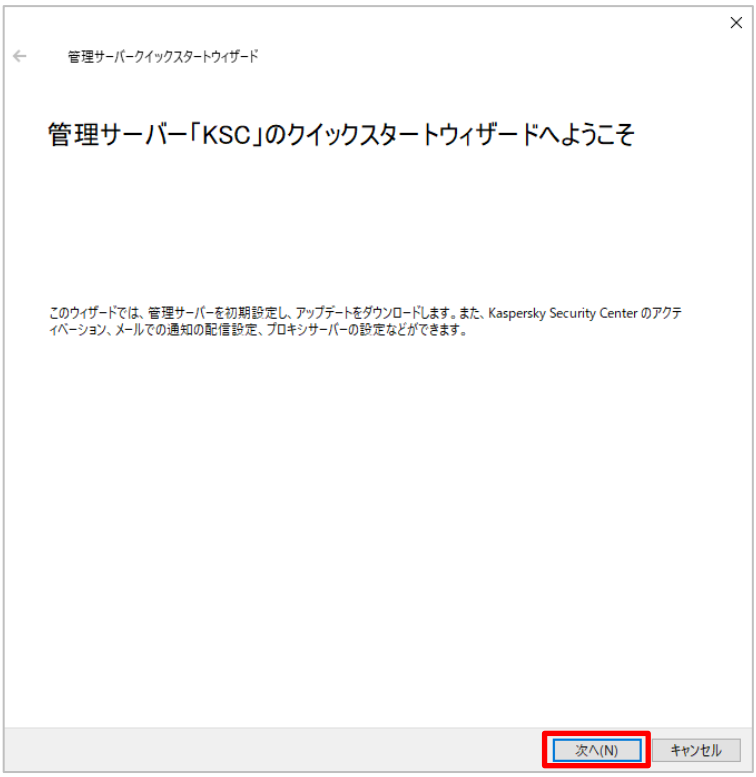
※ウィザードを使用すると、意図せず既存環境の設定を変更してしまう可能性があるため、実施しないようにしてください。

6.1.　クイックスタートウィザードの実行

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



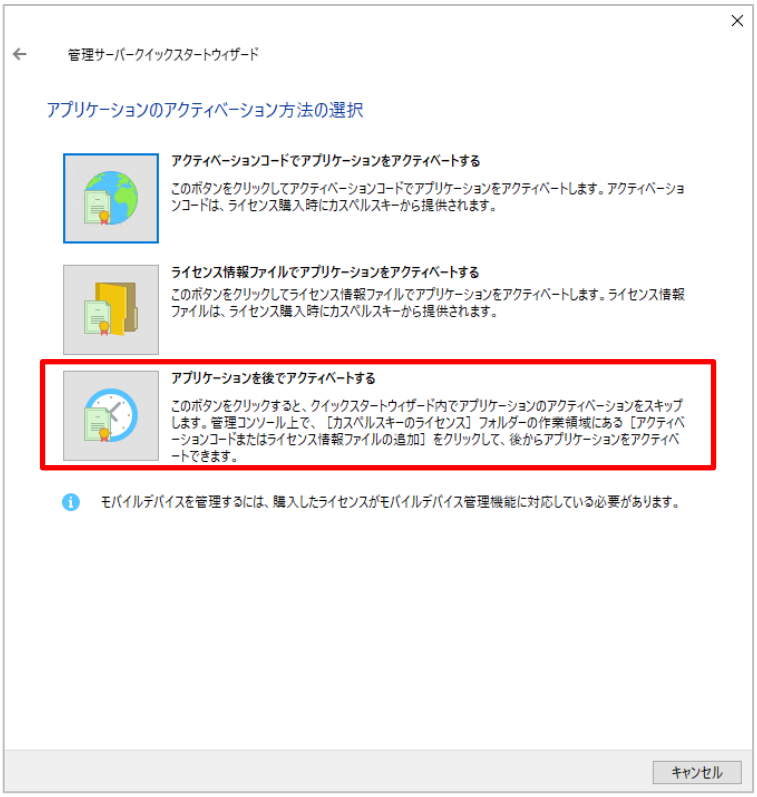
(2)「次へ」をクリックします。



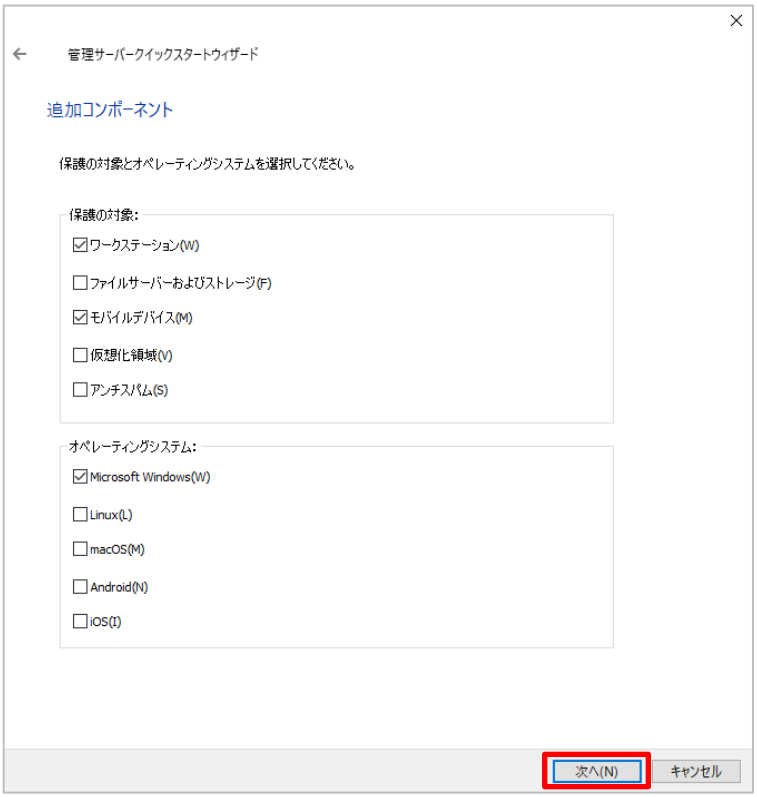
(3) インターネットへのアクセスするためのプロキシサーバー設定を行います。
ここでは既定値のまま「次へ」をクリックします。

※ インターネットへ接続する際にプロキシサーバーを経由する場合、OS 側の設定とは別に、ここで設定が必要です。

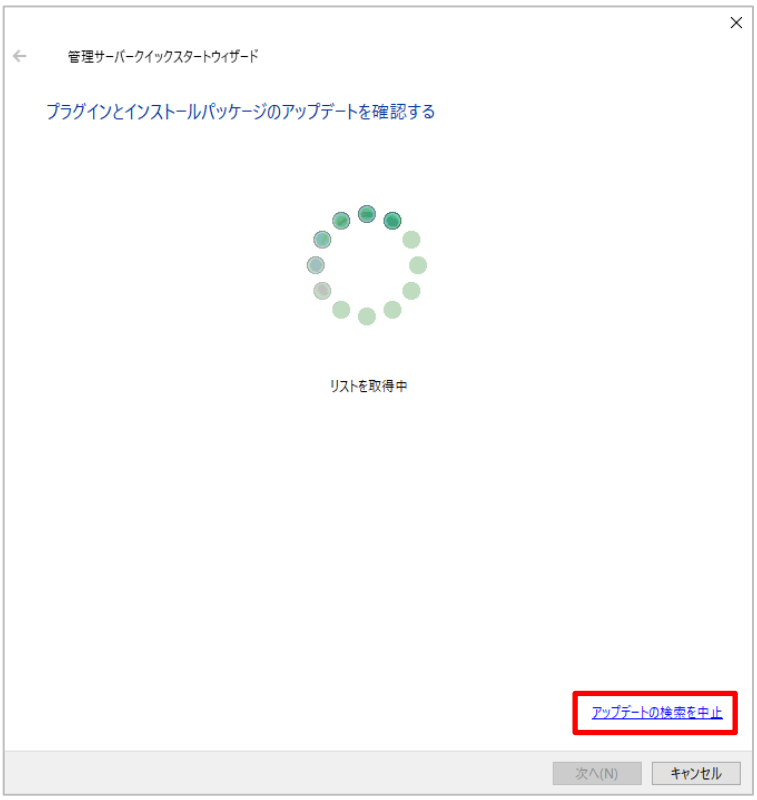
(4) 「アプリケーションを後でアクティベートする」をクリックします。



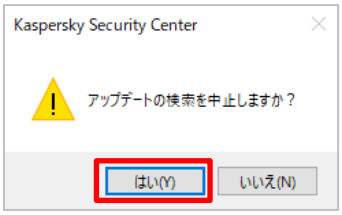
(5) 保護対象のプラットフォームと OS を選択します。
ここでは既定値のまま「次へ」をクリックします。



(6) インターネット経由でリストの取得が行われます。
取得が行われる前に「アップデートの検索の中止」をクリックします。

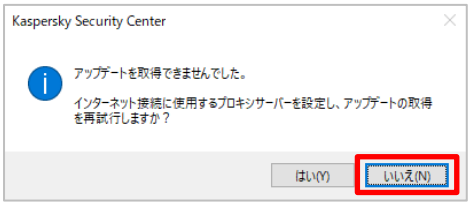


(7) 右記のダイアログが表示されるので「はい」をクリックします。



※ もしこのダイアログが表示される前にリストが表示された場合は、一度ウィザードをキャンセルし、(1)から再開してください。

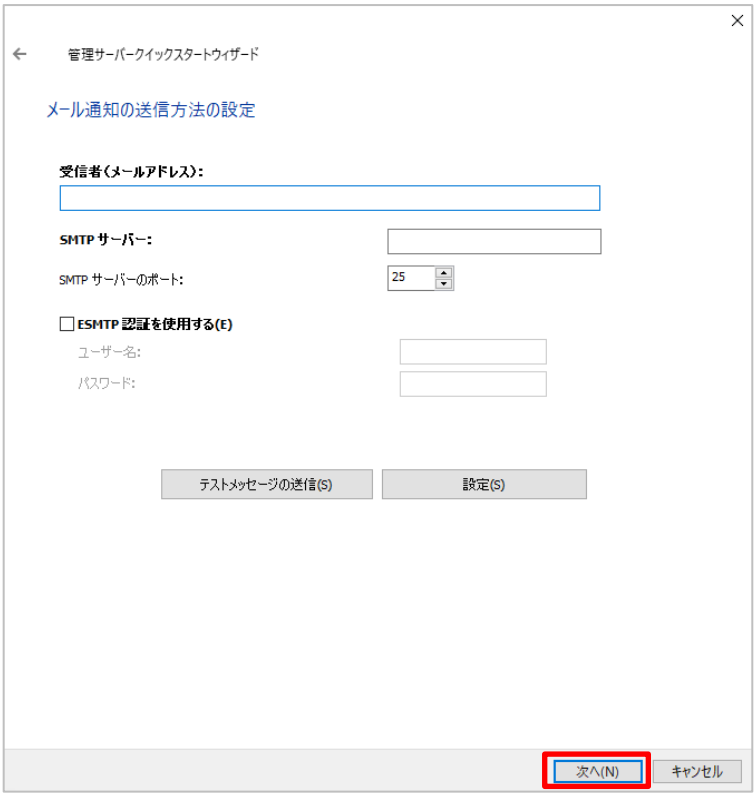
(8) 続いて右記のダイアログが表示されるので、「いいえ」をクリックします。



(9)「Kaspersky Security Network への参加に同意する」にチェックを入れ、「次へ」をクリックします。

※「同意しない」にチェックを付けることも可能です。

(10)　イベント発生時にメール通知する場合、宛先を入力します。
設定しない場合は空白で構いません。「次へ」をクリックします。

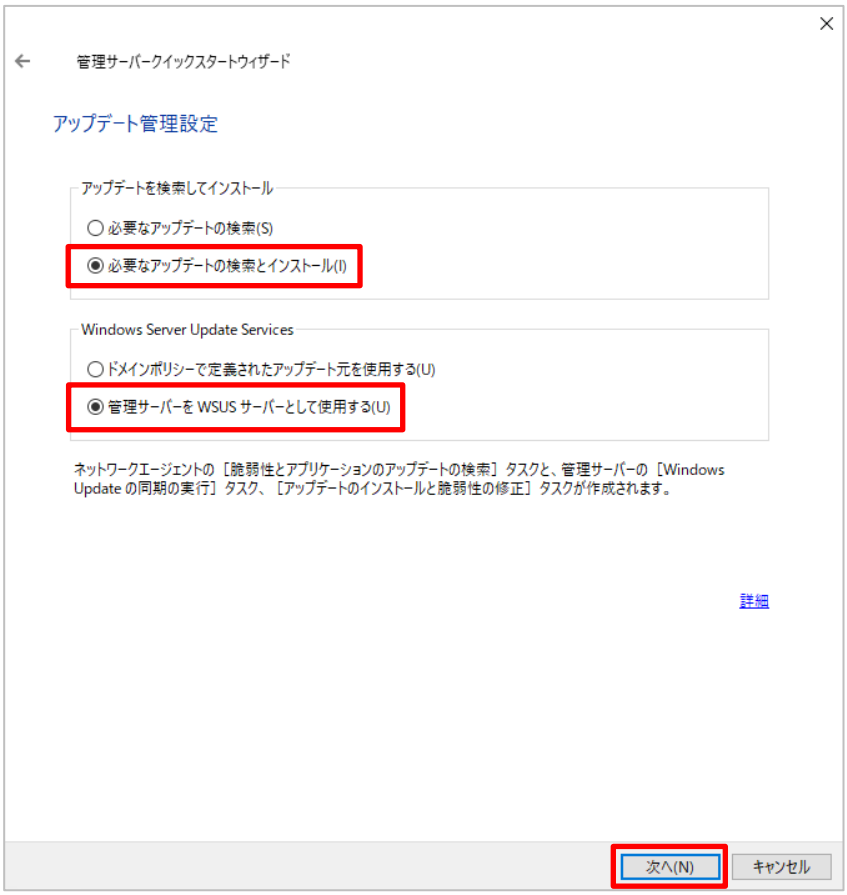


(11)　アップデート管理設定を実施します。

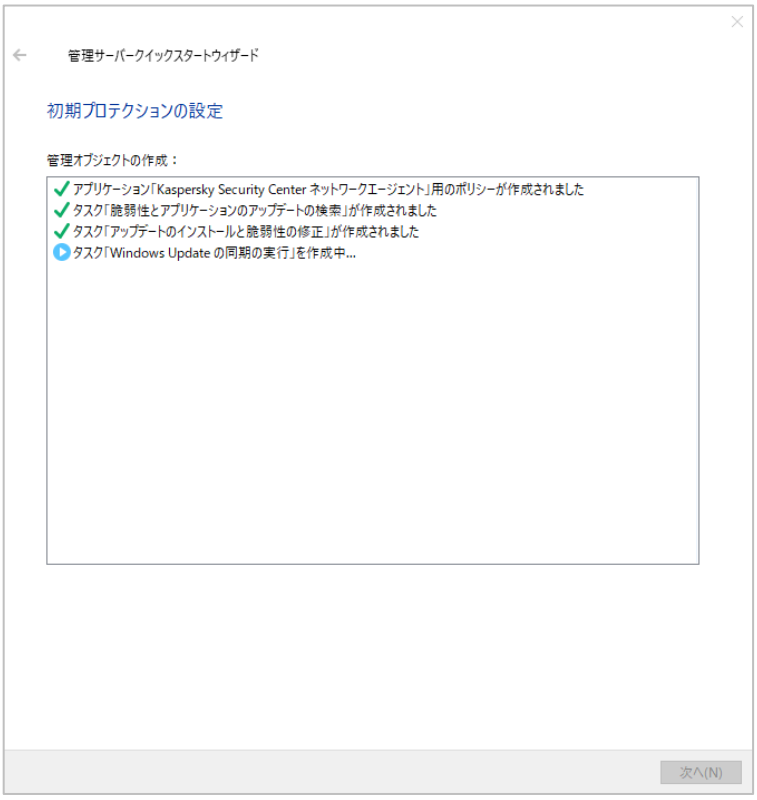
本手順では、すべてのタスクを作成するため、**「必要なアップデートの検索とインストール」「管理サーバーを WSUS サーバーとして使用する」**にチェックを入れ、「次へ」をクリックします。（後から各タスクの作成、設定変更も可能です）

- **「重要なアップデートの検索」**にチェックした場合：
  → 「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。
- **「必要なアップデートの検索とインストール」**にチェックした場合：
  → 「脆弱性とアプリケーションのアップデートの検索」タスクと、「アップデートのインストールと脆弱性の修正」タスクが作成されます

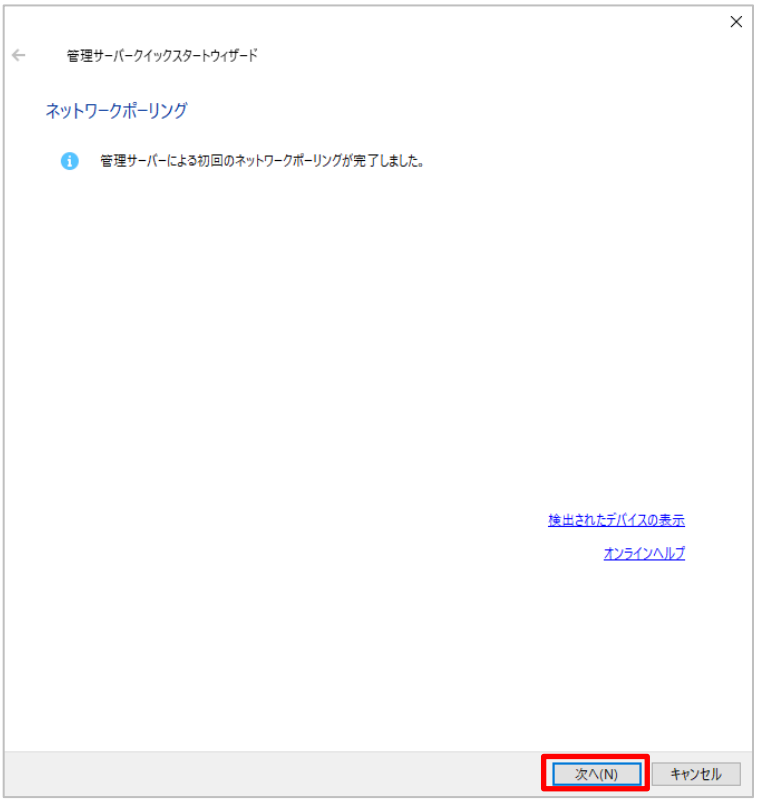
- **「ネットワークから WSUS サーバーを使用する」**にチェックした場合：
  → 外部の WSUS サーバーを使用する設定となります。
- **「管理サーバーを WSUS サーバーとして使用する」**にチェックした場合：
  →「Windows Update の同期の実行」タスクが作成されます。



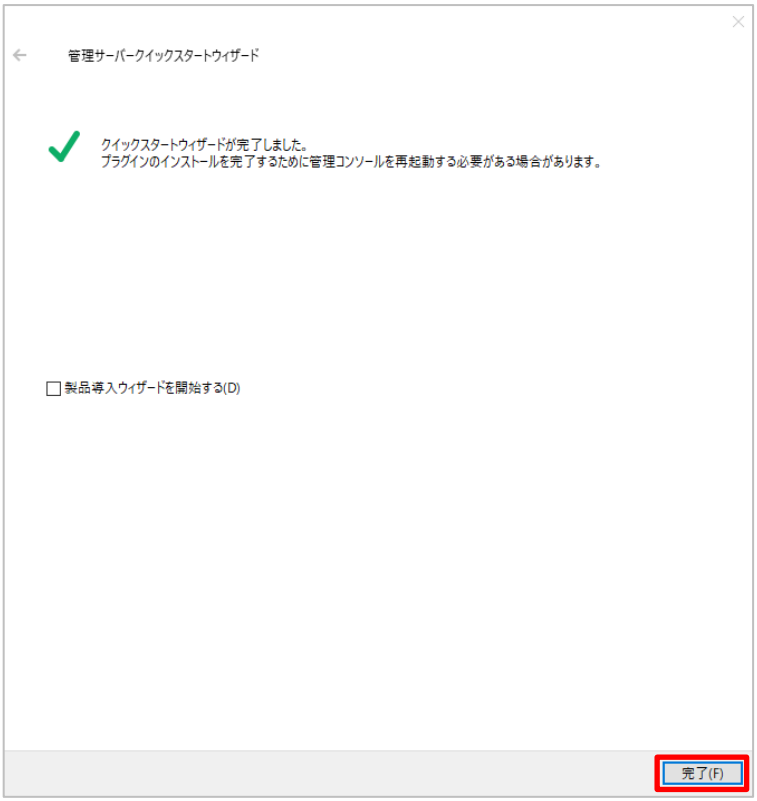
(12)　初期タスクが作成されるので、しばらく待ちます。



(13)　「次へ」をクリックします。



(14)　「完了」をクリックし画面を閉じます。



(15)　KSC 画面左側の「タスク」をクリックし、画面右側に以下タスクが作成されていることを確認します。

・「Windows Update の同期の実行」
・「アップデートのインストールと脆弱性の修正」
・「脆弱性とアプリケーションのアップデートの検索」

本節は以上です。

6.2. 作成したタスクの確認、設定変更

「6.1. クイックスタートウィザードの実行」で作成した各タスクの内容を確認、設定変更を行います。
設定値は「4. 設定の流れ」を元としておりますが、お客様の運用に合わせ設定してください。

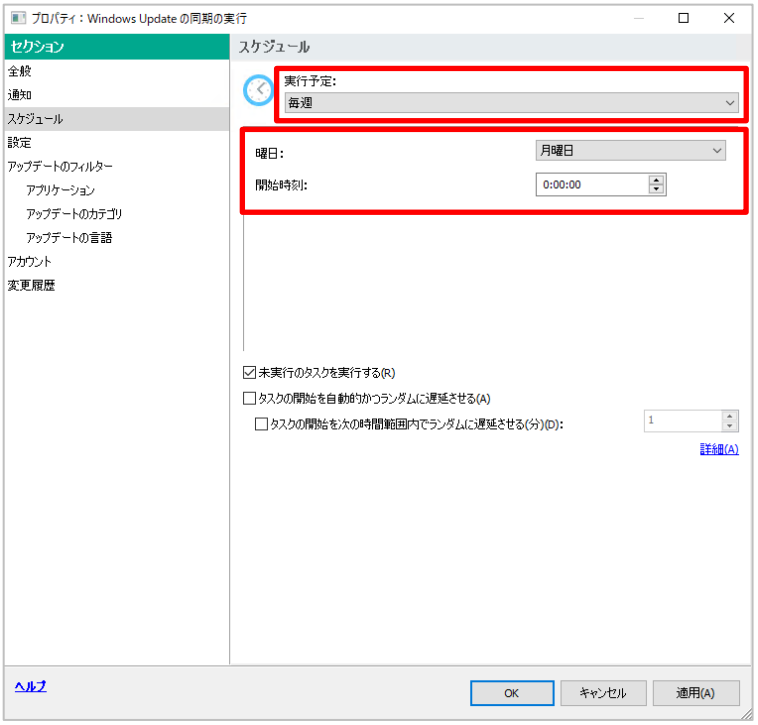
6.2.1.「Windows Update の同期の実行」タスクの設定変更

本タスクを実行する事で、KSC は Windows OS 及び、その他 Microsoft 製品のパッチ情報を保持します。
このタスクでは、パッチやインストーラーそのものはダウンロードせず、**メタデータのみダウンロード**します。

(1) KSC にて「タスク」をクリックし、右側にて「Windows Update の同期の実行」タスクをダブルクリックします。

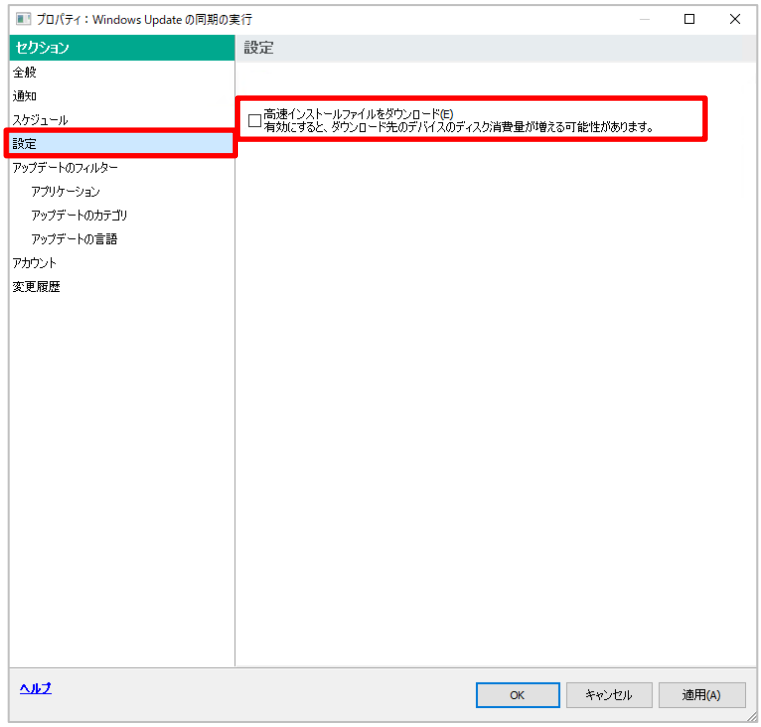
(2)「スケジュール」セクションを選択します。
ここでは、実行予定として以下を設定します。

・実行予定：毎週
・曜日：月曜日
・開始時刻：0:00:00



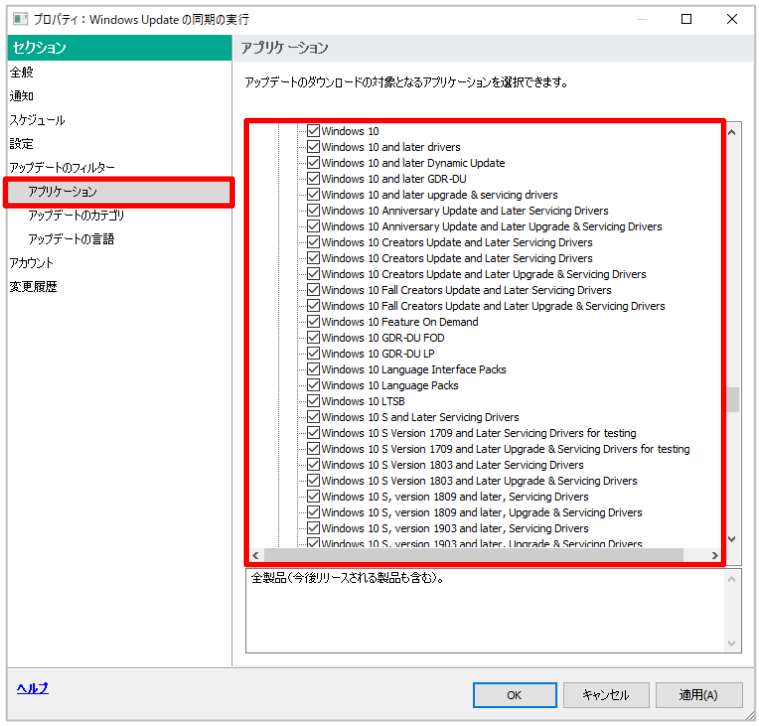
(3) 「設定」セクションを選択します。
「高速インストールファイル」を使用するかどうか設定します。
チェックを入れず、規定値とします。

・「高速インストールファイル」
「高速インストールファイル」は、クライアントに対しバイナリレベルで差分の更新プログラムを提供する機能です。
本設定を有効にした場合、高速インストールファイルがダウンロードされますが、通常の更新プログラムと比較し数倍のファイルサイズとなり、多くのディスクリソースを使用します。
弊社では本機能は初期値である「チェックを外した状態」で運用することをお勧めします。



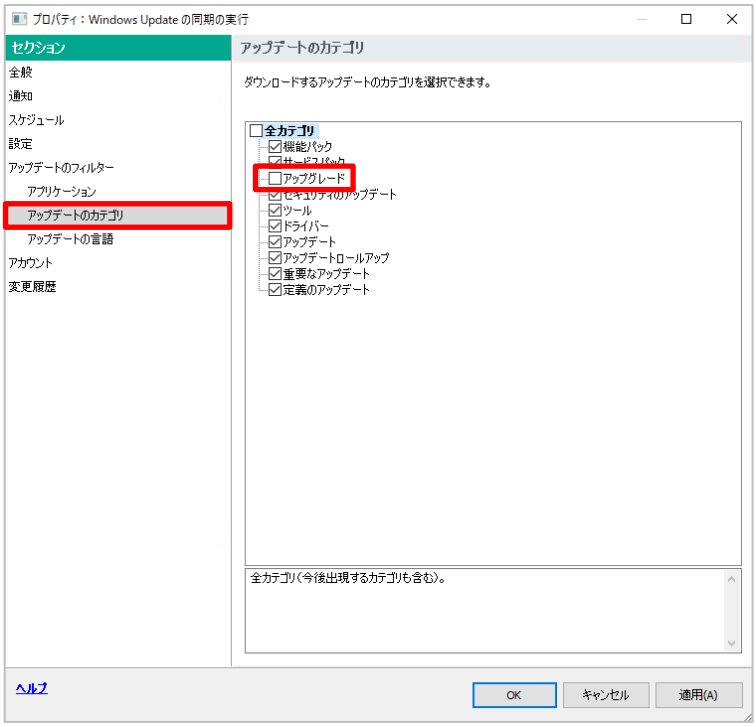
(4) 「アップデートのフィルター」 →
「アプリケーション」セクションを選択します。
既定では「すべての製品」が選択されています。すべての製品を選択した状態ですと不要な製品の情報も取得する事となるため、**必要なアプリケーションのみ選択**します。
（図は Windows10 のみを選択している例です。）

※最新バージョンがリリースされている場合、本タスク実行後にリストの内容も更新されます。
定期的に確認し、チェックのオン、オフを設定してください。

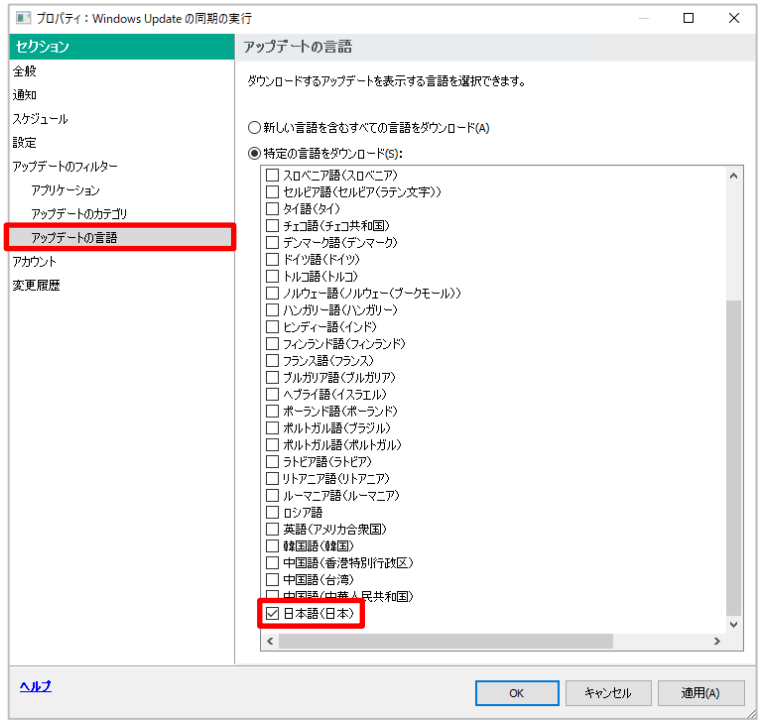


(5) 「アップデートのフィルター」-「アップデートのカテゴリ」セクションを選択します。
既定では「すべてのカテゴリ」が選択されていますが、**「アップグレード」のチェックを外してください。**
必要に応じて、他項目の設定を実施してください。

※ 「アップグレード」は Windows 10 Future Update や OS のアップグレードに関する情報となります。
意図せず Future Update が行われないよう、チェックを外すことを推奨します。
Future Update を適用する場合は、別資料「Future Update 適用ガイド」をご参照ください。



(6) 「アップデートのフィルター」-「アップデートの言語」セクションを選択します。
既定ではすべての言語をダウンロードするよう設定されています。
「特定の言語をダウンロード」にチェックし、「日本語(日本)」にチェックを入れます。



(7) 「OK」をクリックして設定を保存します。

本項は以上です。

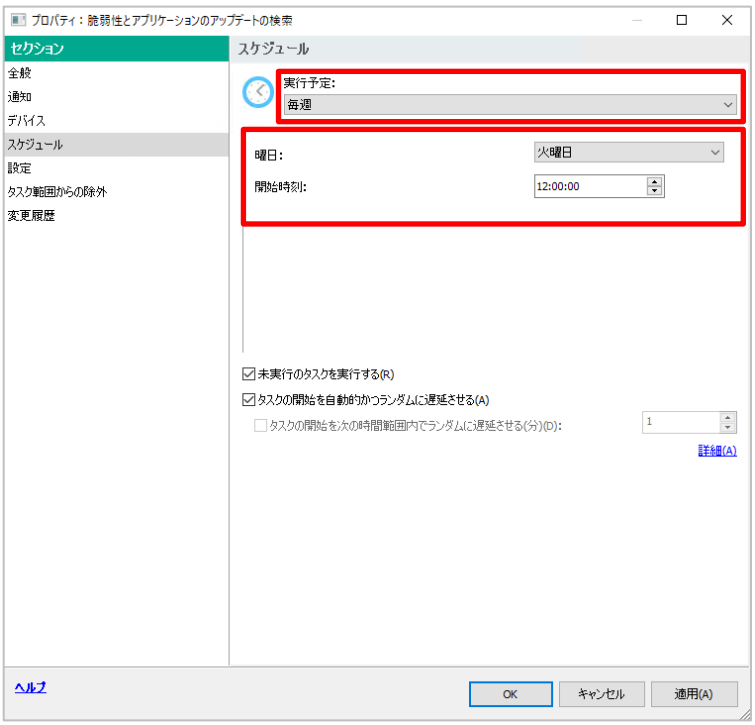
6.2.2.「脆弱性とアプリケーションのアップデートの検索」タスクの設定変更

本タスクを実行する事で、KSC はデバイス上の脆弱性情報やアプリケーションのバージョン情報を収集します。

(1) KSC にて「タスク」を開き、「脆弱性とアプリケーションのアップデートの検索」タスクをダブルクリックします。

(2) 「スケジュール」セクションを選択します。
実行予定として以下を設定します。

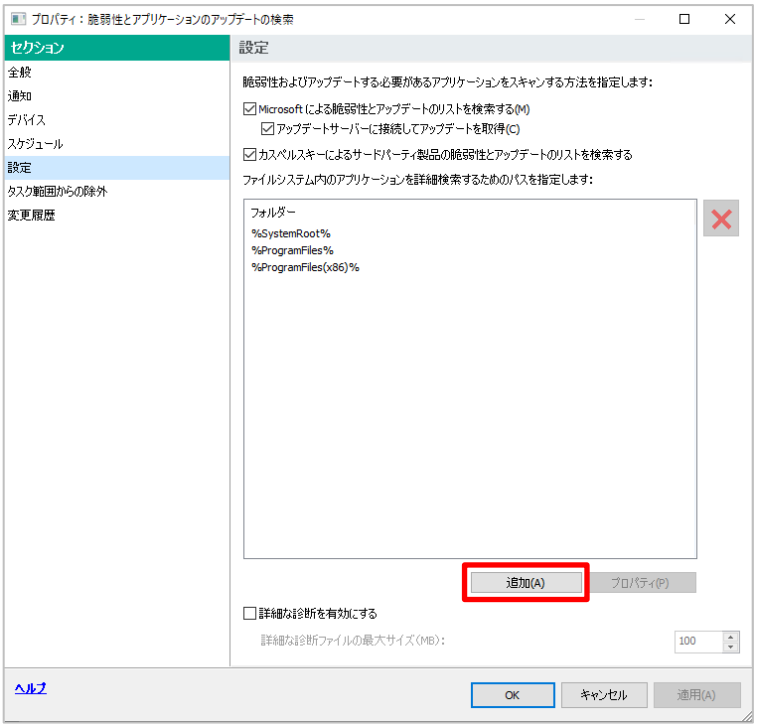
・実行予定：毎週
・曜日：火曜日
・開始時刻：12:00:00



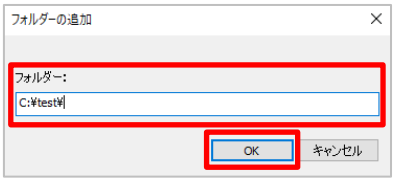
(3) 「設定」セクションを選択します。
既定では以下のフォルダーがスキャンされます。

・%SystemRoot%
・%ProgramFiles%
・%ProgramFiles(x86)%

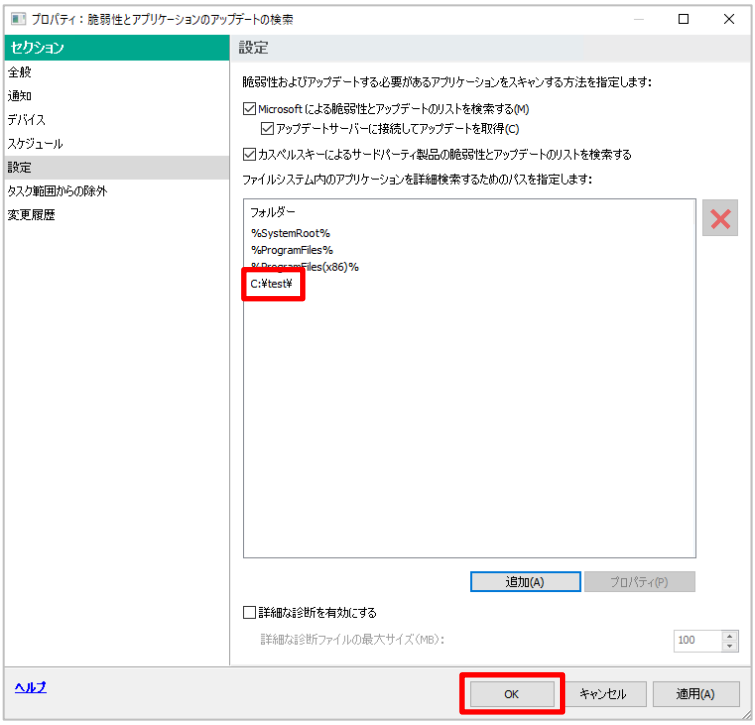
上記フォルダー以外をスキャン対象として追加したい場合、「追加」をクリックします。



(4) スキャンに加えたいフォルダーパスを入力し、「OK」をクリックします。
（図は、「C:¥test」フォルダーを追加する例です。）



(5) 画面右側のフォルダー一覧に「C:¥test」が含まれていることを確認します。



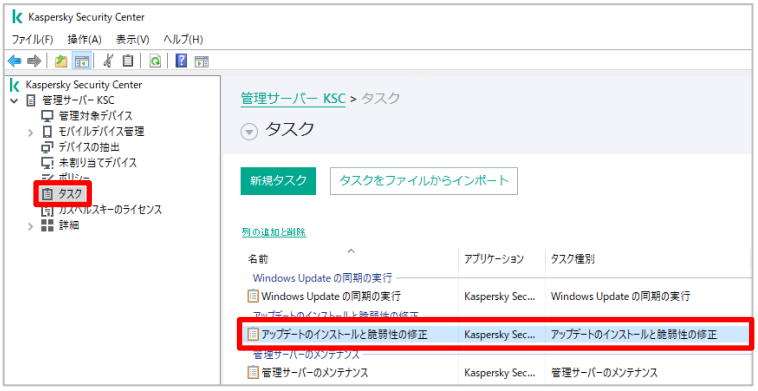
(6) 「OK」をクリックして設定を保存します。

本項は以上です。

6.2.3.「アップデートのインストールと脆弱性の修正」タスクの設定変更

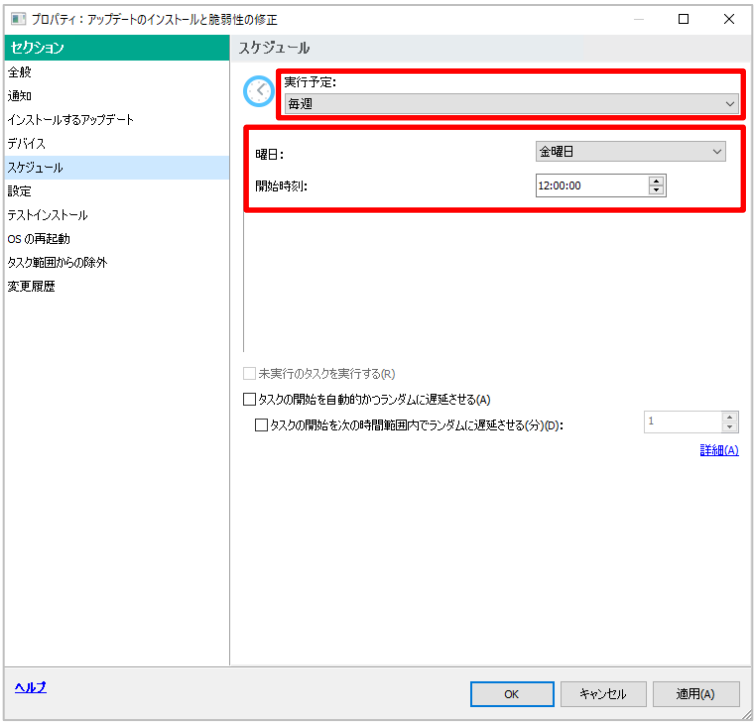
本タスクを実行する事で、Microsoft 製品のパッチ、アプリケーションのアップデートファイルをダウンロードし、デバイスに対し脆弱性の修正、アップデートのインストールを行います。

(1) KSC にて「タスク」を開き、「アップデートのインストールと脆弱性の修正」タスクをダブルクリックします。



(2)「スケジュール」セクションを選択します。
実行予定として以下を設定します。

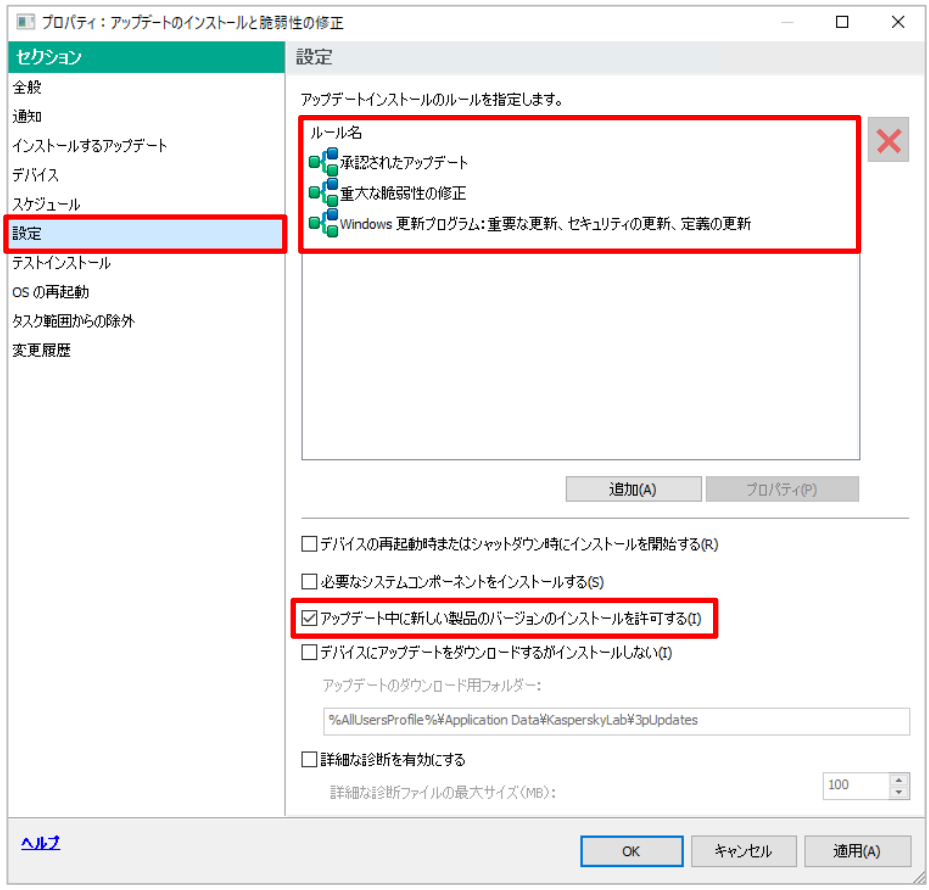
・実行予定：毎週
・曜日：金曜日
・開始時刻：12:00:00



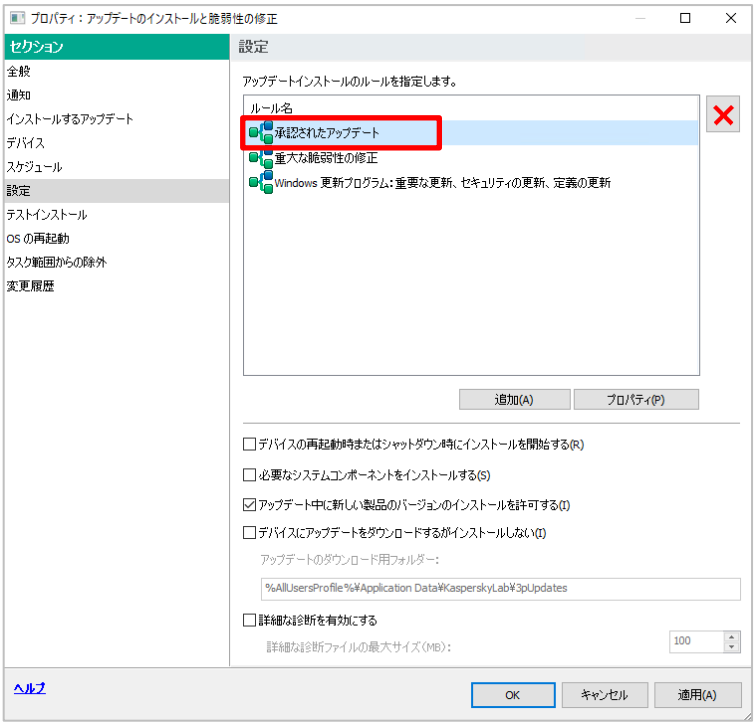
(3) 「設定」セクションをクリックします。3 つのルールが作成されていることを確認できます。

- 承認されたアップデート
  → マイクロソフト製品、サードパーティ製品すべてのアップデートのルールに基づいたルールです。
- 重大な脆弱性の修正
  → サードパーティ製品のアップデートルールです。
- マイクロソフトの更新プログラム：重要な更新、セキュリティの更新、定義の更新
  → Microsoft 製品に関する Windows Update のルールです。

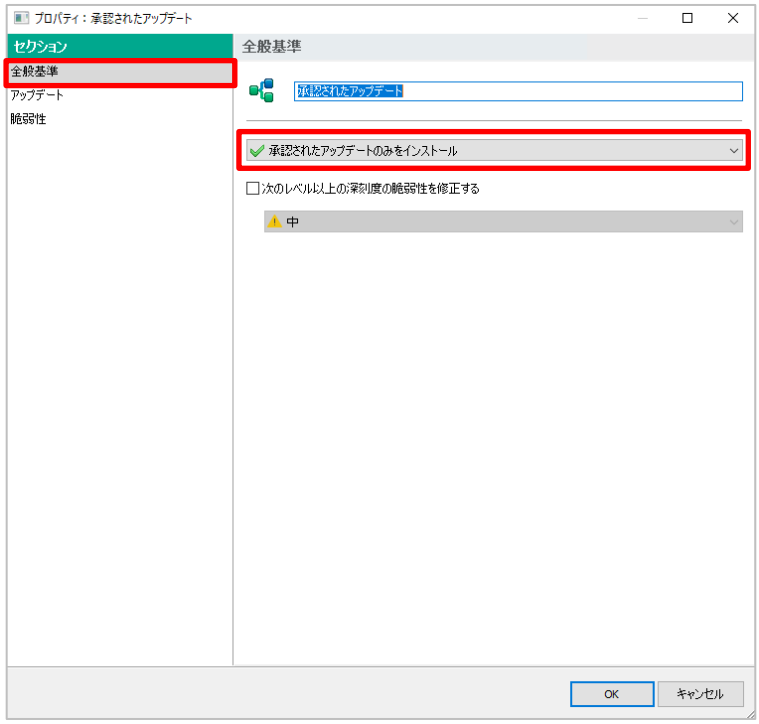
また、「アップデート中に新しい製品のバージョンのインストールを許可する」にチェックが入っています。



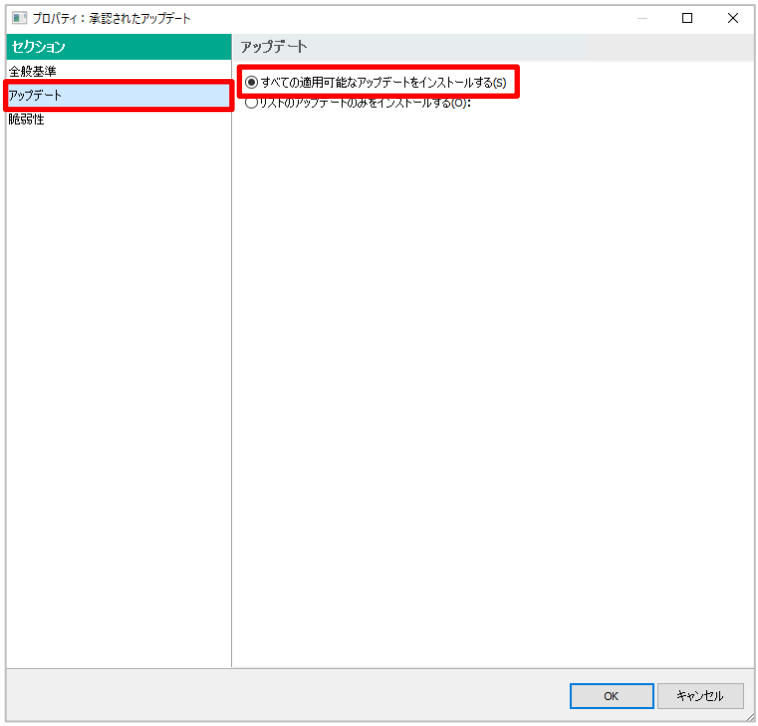
(4)「承認されたアップデート」をダブルクリックします。



(5)「全般基準」セクションを選択します。
「承認されたアップデートのみをインストール」が設定されている事が確認できます。

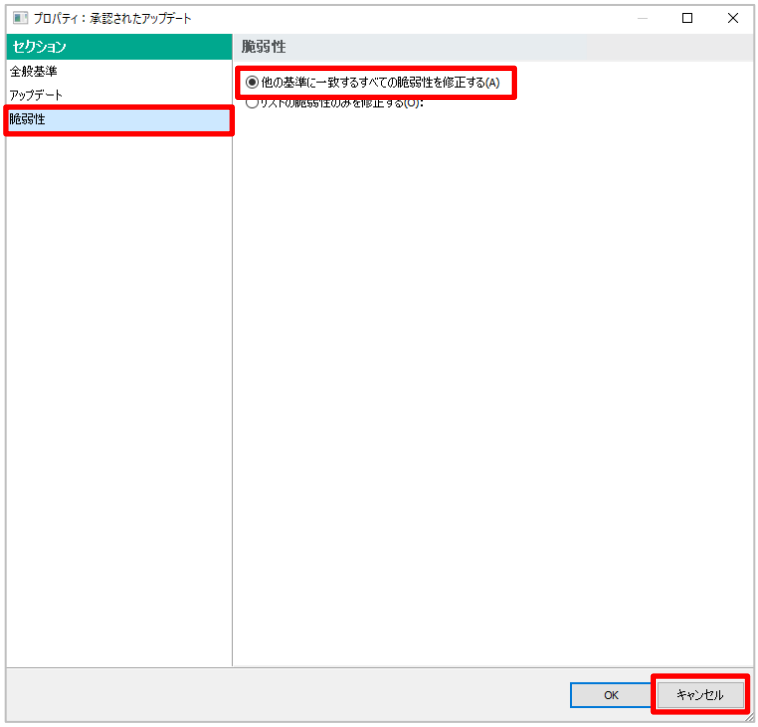


(6) 「アップデート」セクションを選択します。
「すべての適用可能なアップデートをインストールする」が設定されている事が確認できます。

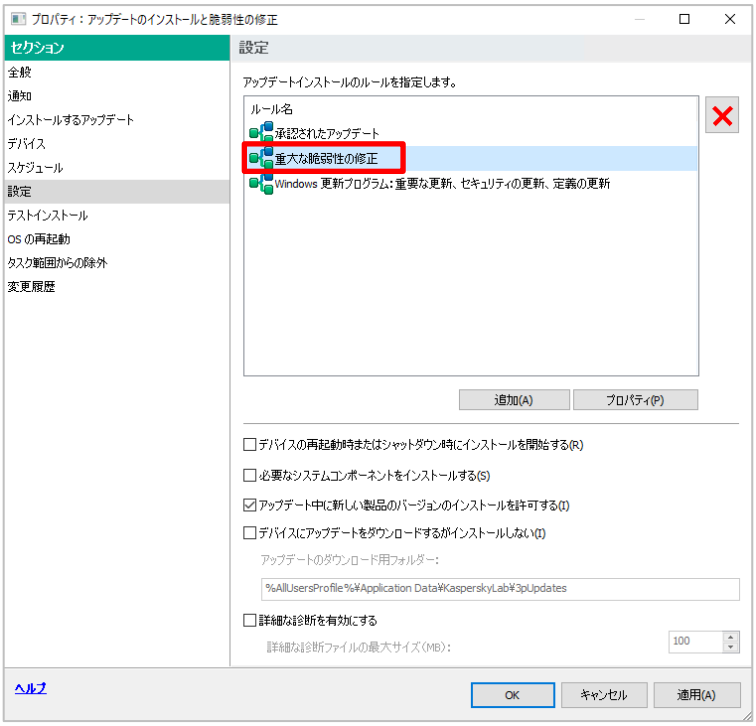


(7) 「脆弱性」セクションを選択します。
「他の基準に一致するすべての脆弱性を修正する」が設定されている事が確認できます。

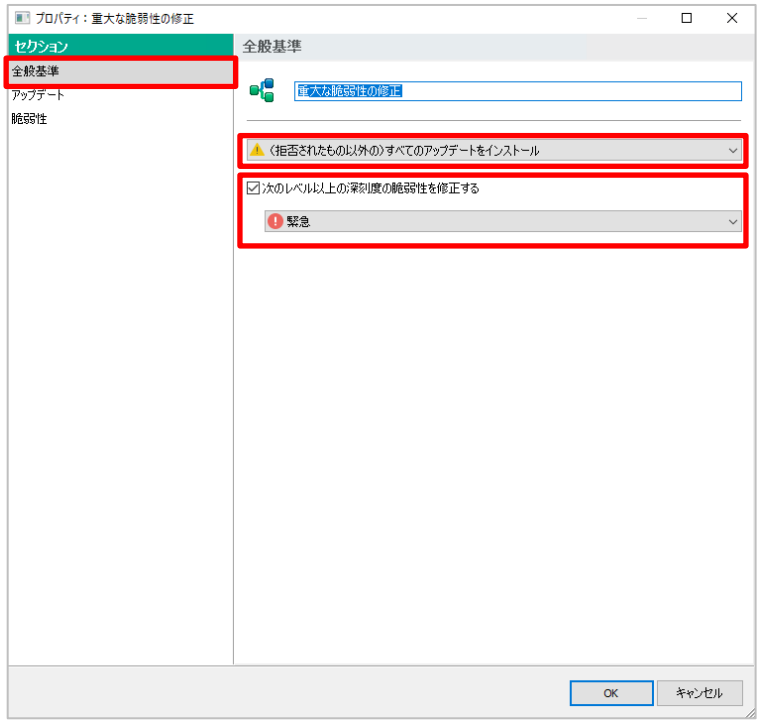
「キャンセル」をクリックし画面を閉じます。



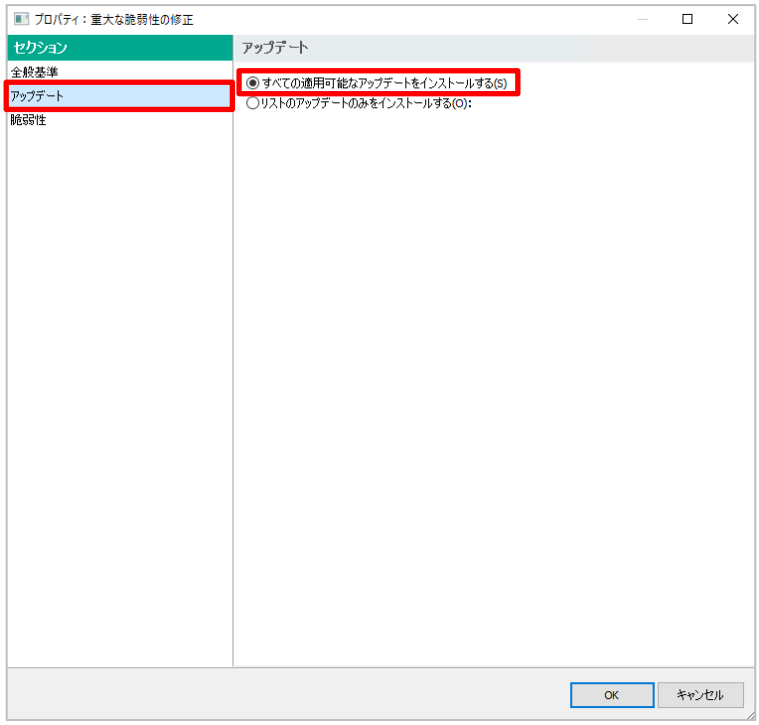
(8)「重大な脆弱性の修正」をダブルクリックします。



(9)「全般基準」セクションを選択します。
カスペルスキー基準の「緊急」以上、かつ拒否されたもの以外すべてのアップデートをインストールする設定となっております。

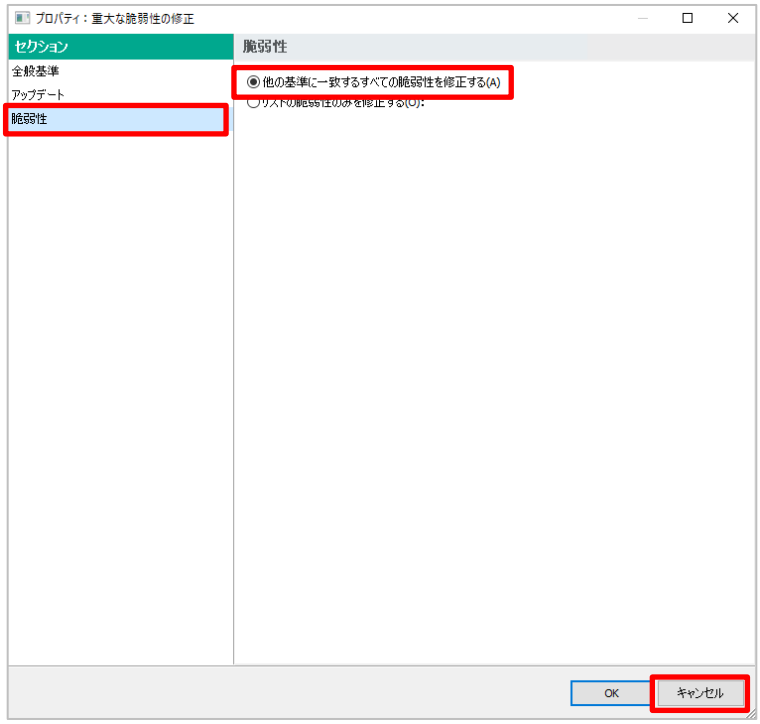


(10)　「アップデート」セクションを選択します。
「すべての適用可能なアップデートをインストールする」設定となっております。

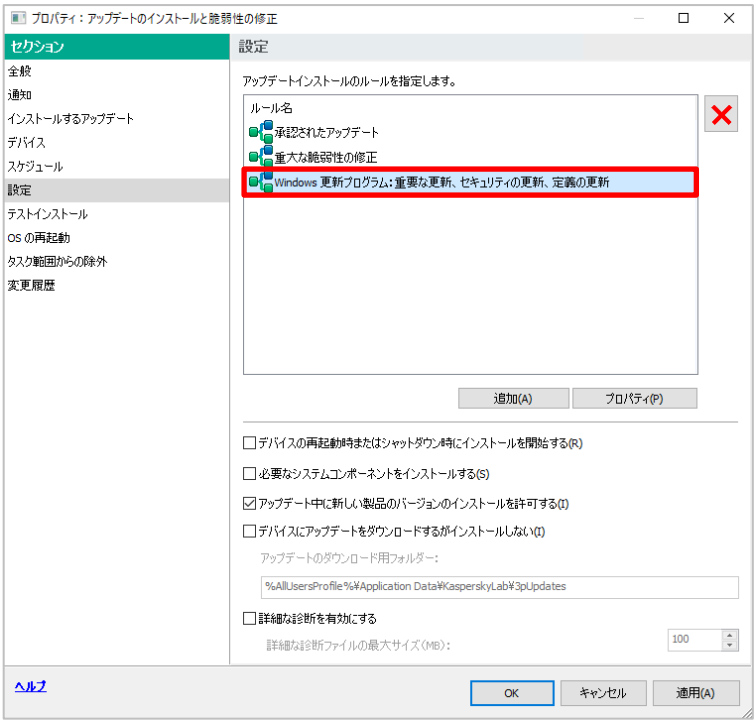


(11)　「脆弱性」セクションを選択します。
「他の基準に一致するすべての脆弱性を修正する」が設定されている事が確認できます。

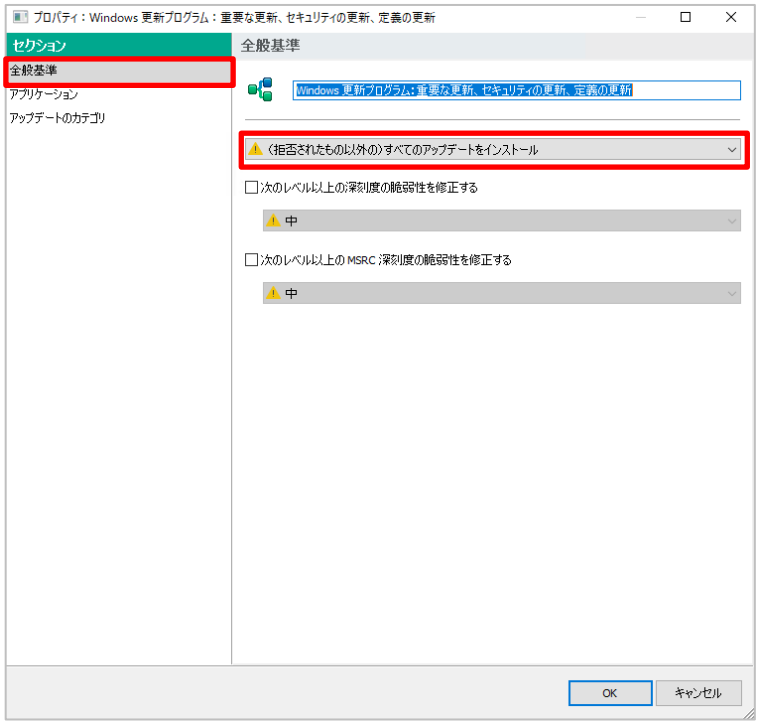
「キャンセル」をクリックし画面を閉じます。



(12)　「windows 更新プログラム：重要な更新、セキュリティの更新、定義の更新」をダブルクリックします。



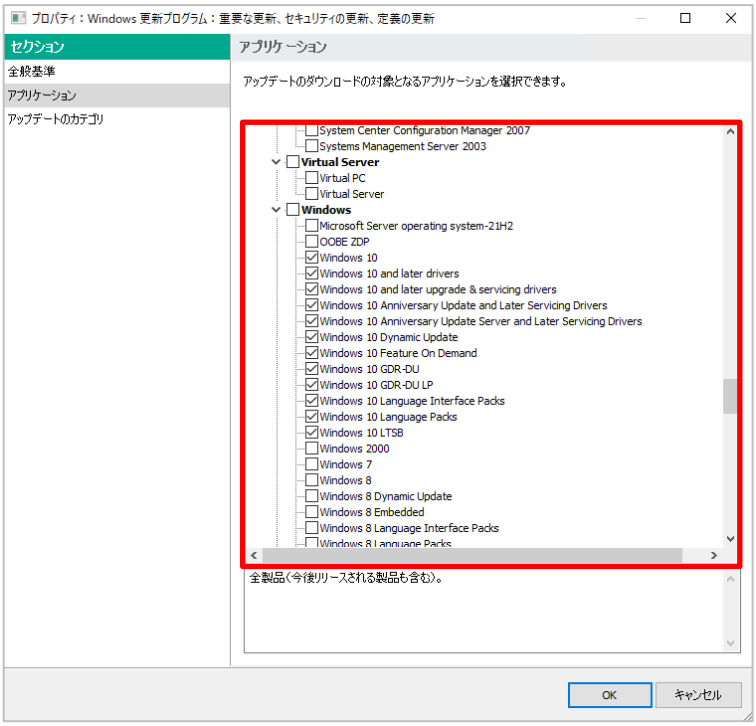
(13)　「全般基準」セクションを選択します。拒否されたもの以外すべてインストールする設定となっております。



(14)　「アプリケーション」セクションを選択します。

既定では「すべての製品」が選択されています。必要なアプリケーションを選択します。

（図は Windows10 のみを選択している例です。）



(15)　「アップデートのカテゴリ」セクションを選択します。

以下の項目のみにチェックが入っています。

・セキュリティのアップデート

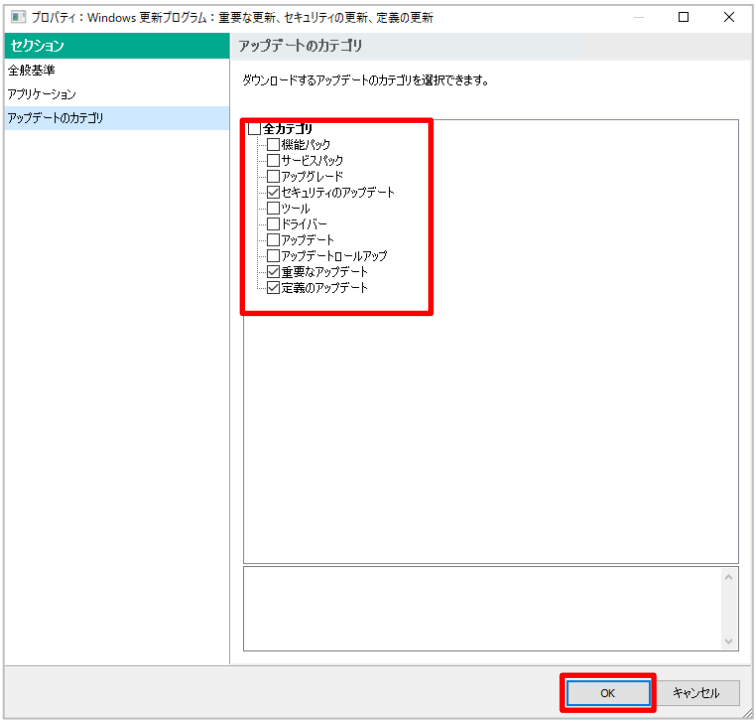
・重要なアップデート

・定義のアップデート

必要に応じて、適用したいアップデート項目にチェックを入れてください。

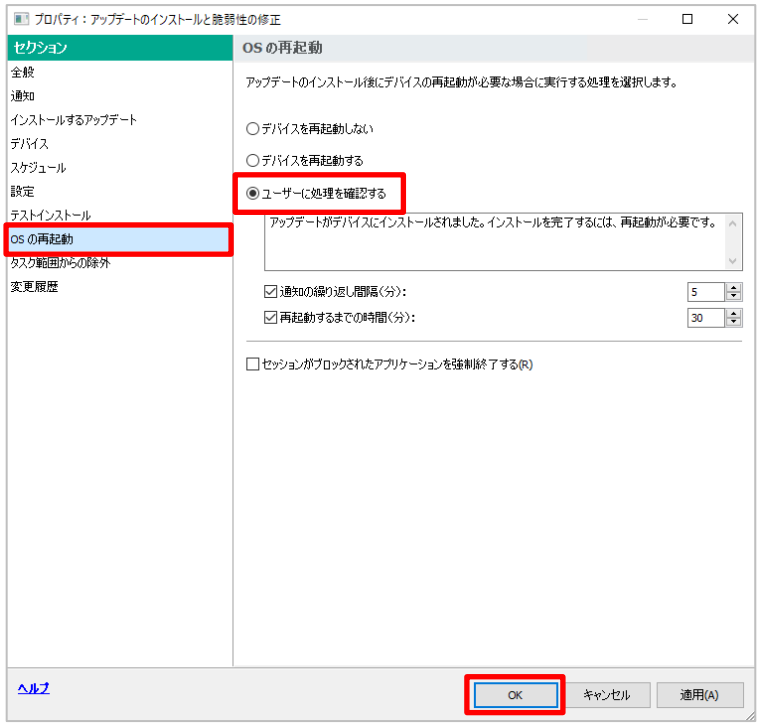
ここでは「すべてのカテゴリ」にチェックを入れています。

「OK」をクリックし画面を閉じます。



(16)　「OS の再起動」セクションを選択します。
「ユーザーに処理を確認する」にチェックが入っています。

「OK」をクリックし画面を閉じます。



(17)　このタスクでは、以下の様な設定となります。

- 毎週金曜日 12:00:00 に実行する。
- 再起動が必要となる場合、30 分間、5 分間隔で OS 再起動を促す。
- 承認されたアップデートはすべてインストールする。
- KL 重要度が「緊急」のアップデートをインストールする。
  サードパーティ製アプリケーションは、「緊急」以上、且つ「拒否」されたもの以外、すべてアップデートする。
- 新しいバージョンへのアップデートを許可する。
- Microsoft 製品はチェックをした Windows 10 のバージョンに関して、すべてのアップデートをインストールする。

本節は以上です。

6.3.　タスクの手動作成

各タスクはウィザードを使用する方法のほか、手動でも作成することができます。

(1) KSC にて「タスク」を開き、「新規タスク」をクリックします。

(2)「Kaspersky Security Center 管理サーバー」を展開し、作成するタスクを選択して「次へ」をクリックします。
画面では「アップデートのインストールと脆弱性の修正」を選択しています。

「Windows Update の同期の実行」タスクは 1 個のみ、他のタスクは複数作成することができます。

(3) 各タスクの設定を行います。
設定内容は、「6.2. 作成したタスクの確認、設定変更」の各タスク設定を参照してください。

本章は以上です。

7. Microsoft 製品のアップデート先の選択

本章では、Microsoft 製品のアップデート先を設定する手順をご説明します。

本設定を行う前に必ず「Windows Update の同期」タスクを一度以上実行し、完了させる必要があります。完了前に設定を実施しても、正しく反映されません。

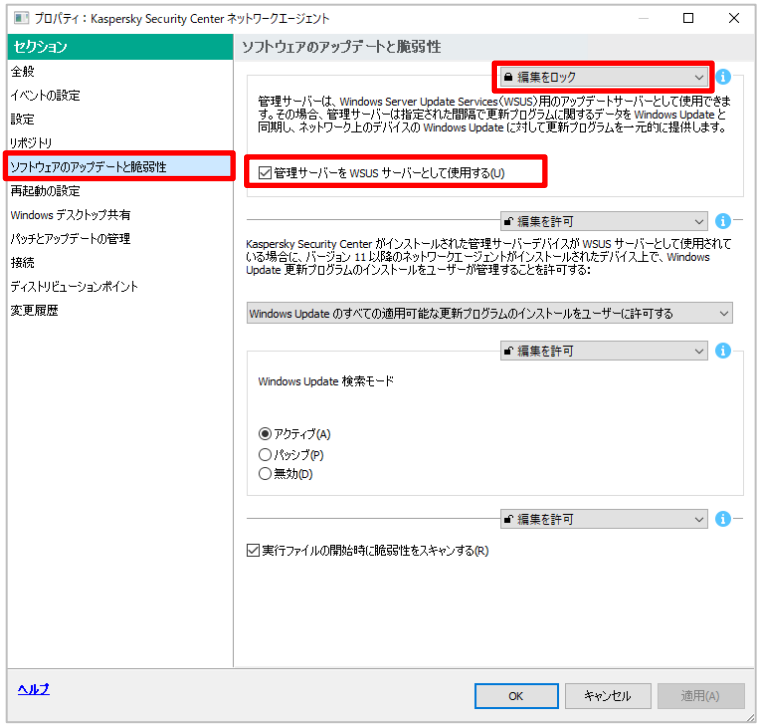
7.1. パターン A：KSC を WSUS サーバーとして使用する

パターン A

本設定を実行する事で、KSC は **WSUS サーバー**となります。KSC 自身が Microsoft 製品のアップデートファイルをダウンロードし、クライアントに配信します。

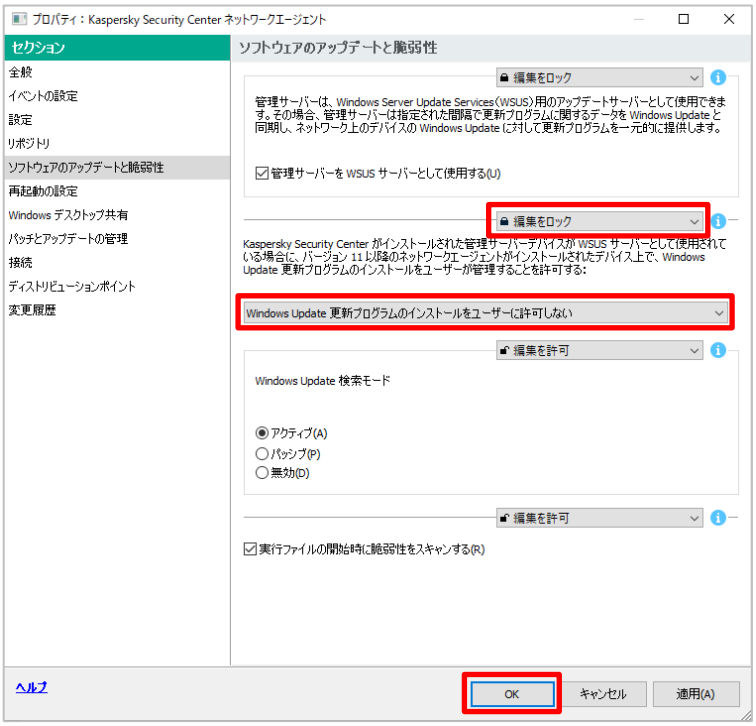
(1) KSC より、「ポリシー」→「Kaspersky Security Center ネットワークエージェント」をダブルクリックします。

(2) 「ソフトウェアのアップデートと脆弱性」セクションを選択します。
画面右側に表示される**「管理サーバーを WSUS サーバーとして使用する」**にチェックを入れます。
また、「編集をロック」に設定します。



(3) リストボックスにて**「Windows Updates 更新プログラムのインストールをユーザーに許可しない」**を選択します。
「編集をロック」に設定し、「OK」をクリックします。

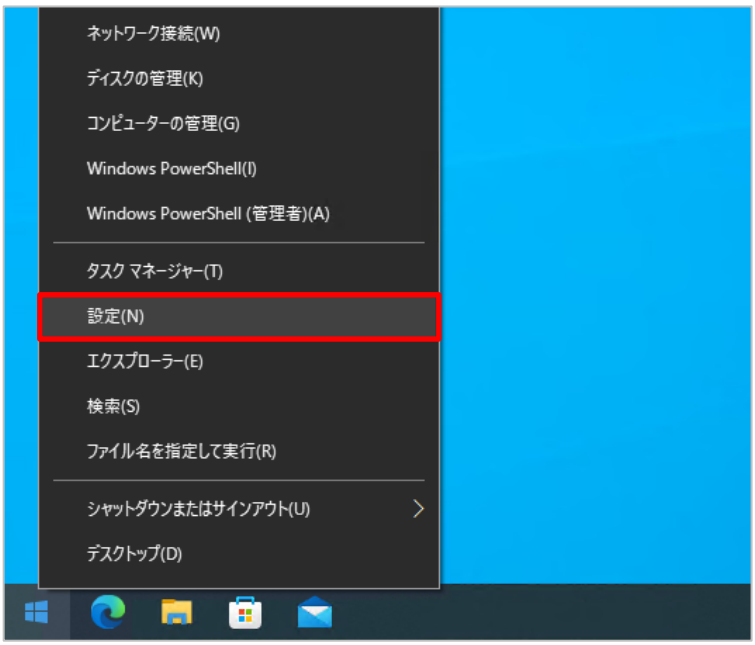
以上で KSC 上での操作は完了です。



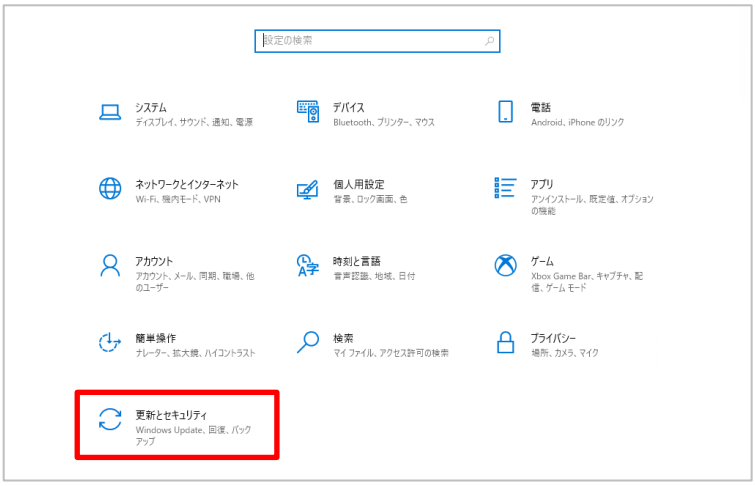
パターン A

【参考】クライアント側での設定状態を確認する場合、管理者権限で管理下のコンピューターにログインします。
（例として Windows 10 を使用します。）

(1) 「スタート」ボタンを→クリックし、「設定」を選択します。



(2) 「更新とセキュリティ」をクリックします。



(3) 「Windows Update」セクションが表示されますので、図のように、「一部の設定は組織によって管理されています」となっていることを確認します。

本節は以上です。

7.2.　パターン B：外部の WSUS サーバーを使用する

パターン B

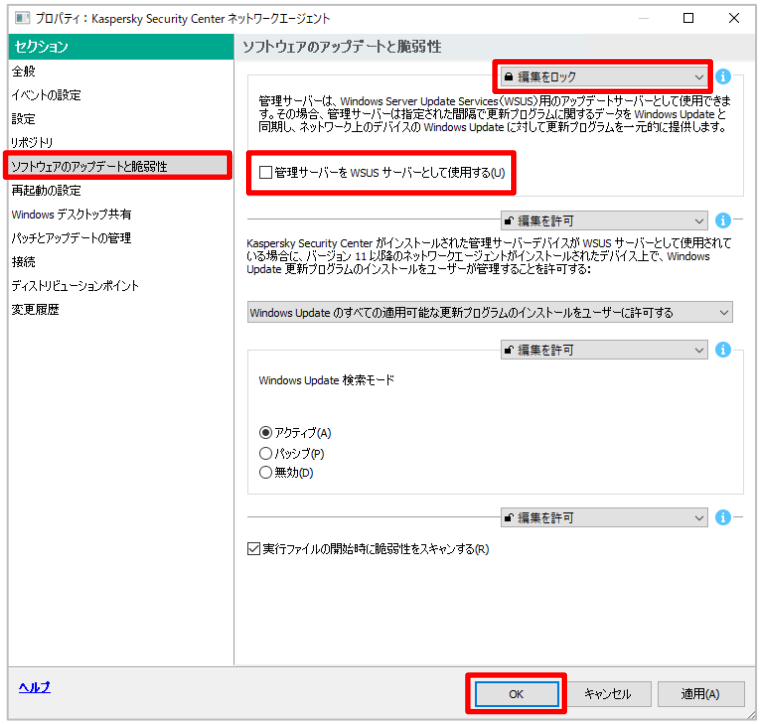
本設定は、外部の WSUS サーバーを使用するパターンです。

Windows 更新プログラムのダウンロード先として、社内に既に存在する WSUS サーバー（若しくはインターネット上の Microsoft アップデートサイト）が使用されます。（既定では本設定となっております。）

(1) KSC にて「ポリシー」を選択し、「Kaspersky Security Center ネットワークエージェント」をダブルクリックします。

(2) 「ソフトウェアのアップデートと脆弱性」セクションを選択します。
画面右側に表示される**「管理サーバーを WSUS サーバーとして使用する」**のチェックを外します。
「編集をロック」に設定し、「OK」をクリックします。

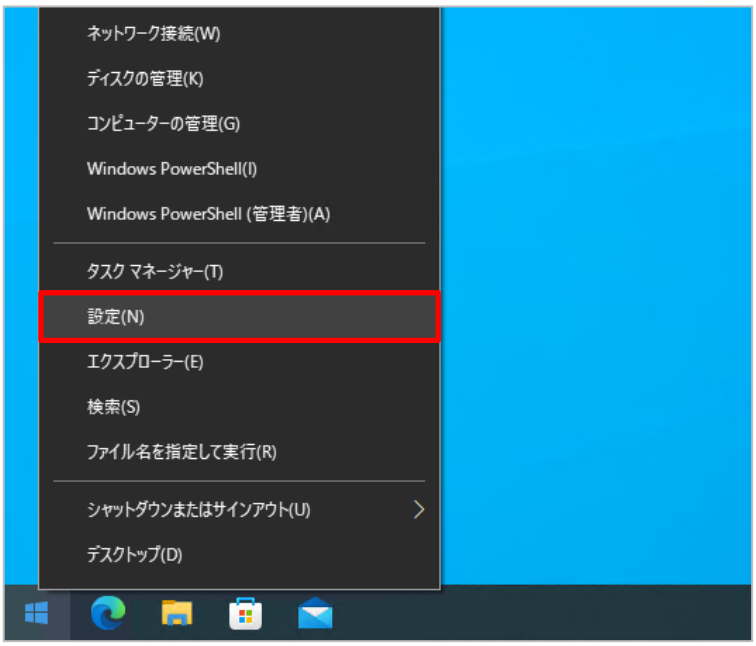
以上で KSC 上での操作は完了です。



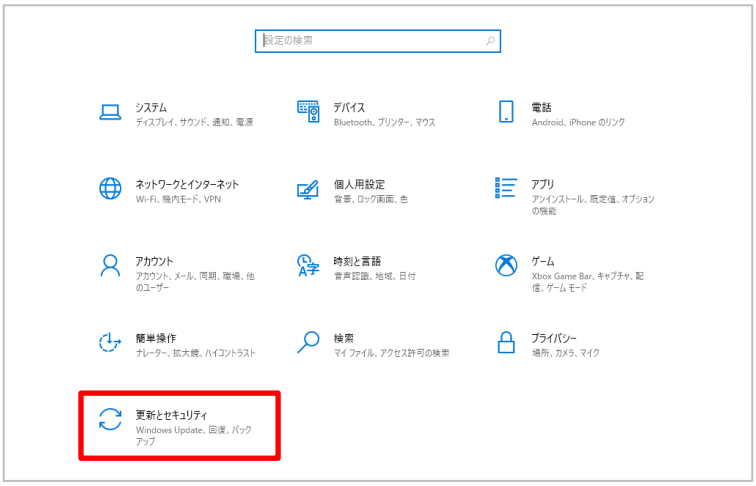
パターン B

【参考】クライアント側での設定状態を確認する場合、管理者権限で管理下のコンピューターにログインします。
（例として Windows 10 を使用します。）

(1) 「スタート」ボタンをクリックし、「設定」を選択します。

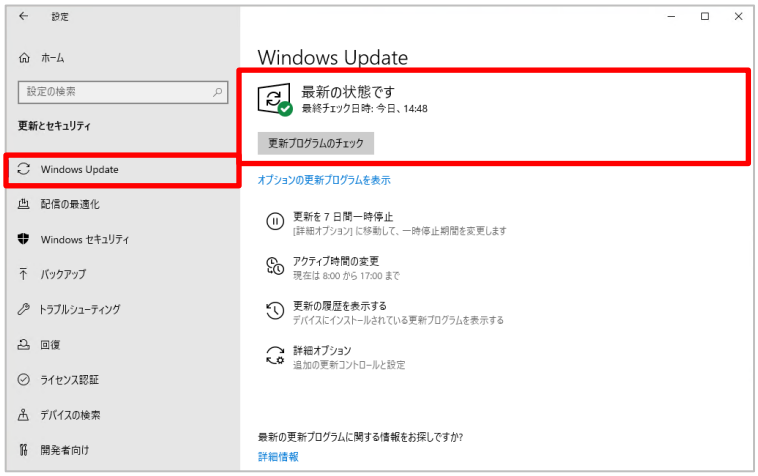


(2) 「更新とセキュリティ」をクリックします。



(3) 「Windows Update」セクションが表示されますので、図のように、「一部の設定は組織によって管理されています」との表記が**存在しないこと**を確認します。

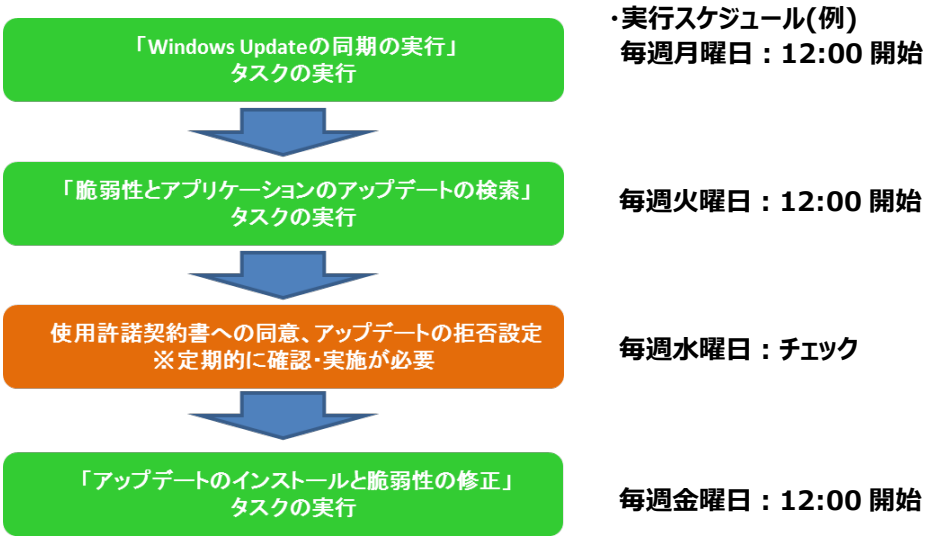
「更新プログラムのチェック」を実行すると、Windows Update サーバーと接続し、更新プログラムのダウンロード、インストールを行います。



本章は以上です。

8. タスクの実行結果確認、及び運用について

本章では、各タスクの実行結果の確認、及び、運用後の作業についてご説明します。
「4. 設定の流れ」でも記載させていただきましたが、運用開始後は以下の流れでタスクが実行されます。

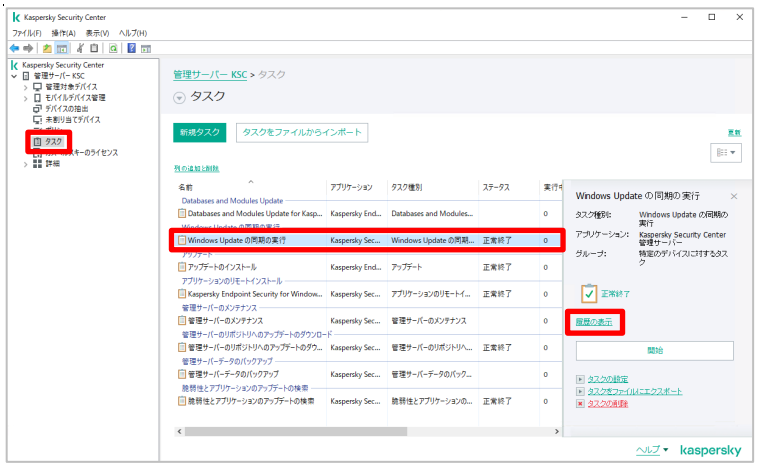


各タスクは設定したスケジュールに従って実行されますが、「使用許諾契約書への同意、アップデートの拒否設定」については、管理者が手動で実施する必要があります。

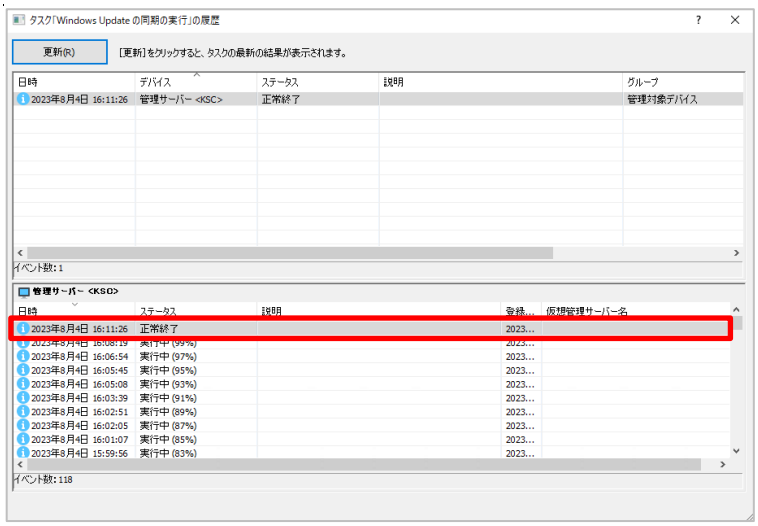
8.1. 「Windows Update の同期の実行」タスクの確認

「Windows Update の同期の実行」タスクの実行結果は、「履歴の表示」にて確認します。

(1) KSC にて「タスク」を選択し、「Windows Update の同期の実行」を選択し、「履歴の表示」をクリックします。



(2) ステータスが「正常終了」となっていることを確認します。



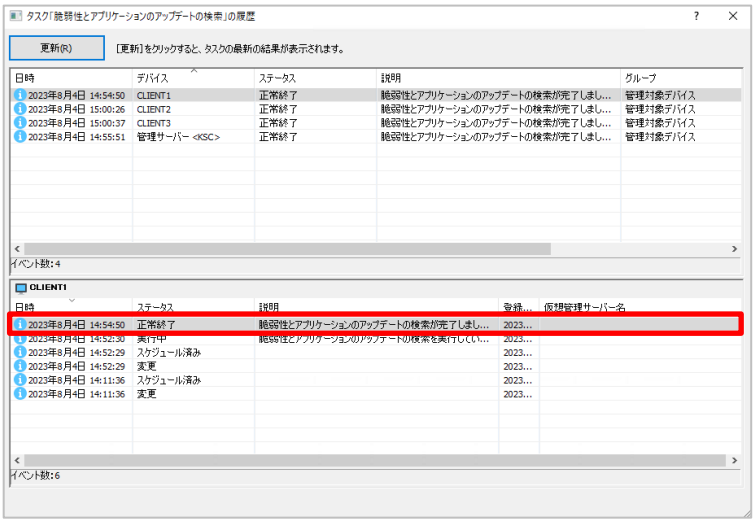
本節は以上です。

8.2. 「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

「脆弱性とアプリケーションのアップデートの検索」タスクの実行結果は、「履歴の表示」にて確認します。

(1) KSC にて「タスク」を選択し、「脆弱性とアプリケーションのアップデートの検索」を選択し、「履歴の表示」をクリックします。

(2) 「ステータス」欄が「正常終了」となっていることを確認します。



本節は以上です。

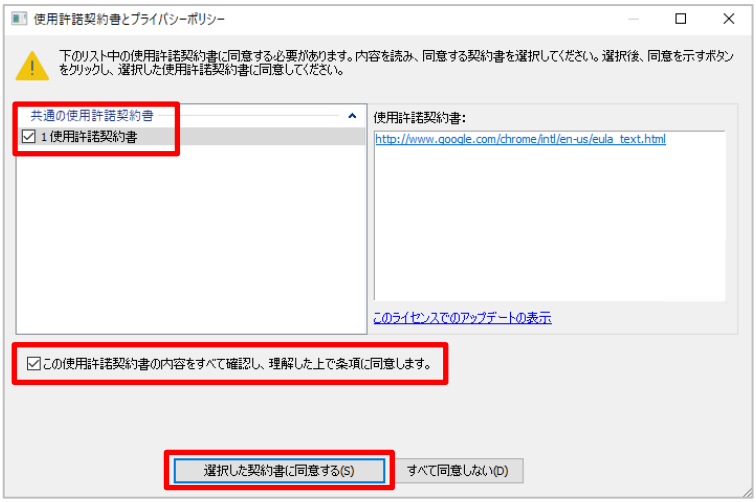
8.3. 使用許諾契約書への同意、及びアップデートの「拒否」設定

「脆弱性とアプリケーションのアップデートの検索」タスクにて検索したアプリケーションについて、使用許諾契約書に同意する手順、及び、インストール対象としたくないアプリケーションを「拒否」する設定をご説明します。

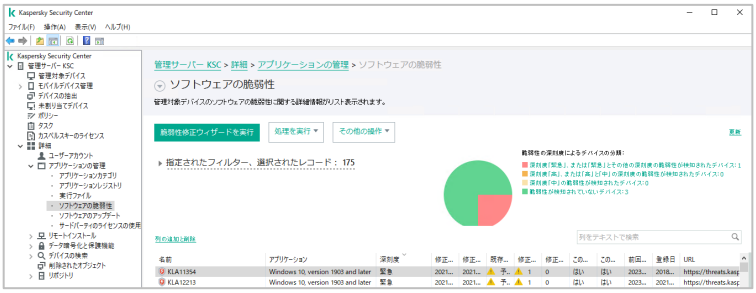
本手順を実施しないとインストールができないパッチもあるため、「脆弱性とアプリケーションのアップデートの検索」タスク実行後にチェックし、実施してください。

(1) KSC にて「詳細」-「アプリケーションの管理」-「ソフトウェアの脆弱性」を選択します。
画面右側に表示される「脆弱性を修正するアップデートの使用許諾契約に同意する必要があります」をクリックします。

(2) 「使用許諾契約書」横のチェックボックスすべてにチェックを入れ、「この使用許諾契約書の内容をすべて確認し、理解したうえで条項に同意します。」にチェックを入れた上で「選択した契約書に同意する」をクリックします。



(3) 使用許諾契約書に関する表示が存在しない事を確認します。

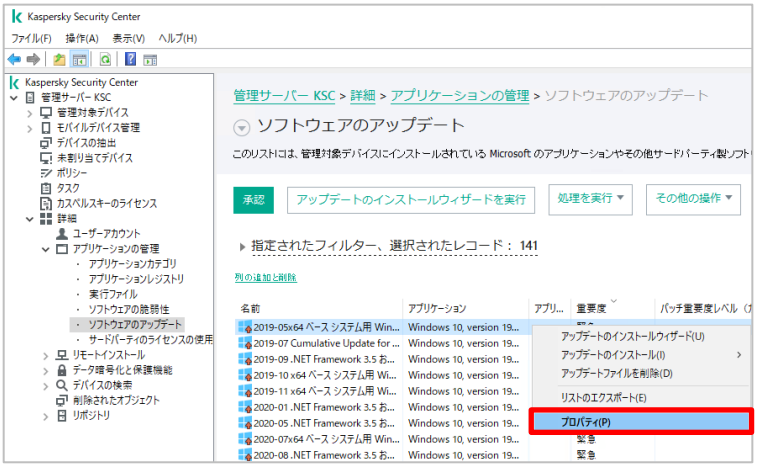


(4) KSC にて「詳細」-「アプリケーションの管理」-「ソフトウェアのアップデート」を選択し、使用許諾の通知がある場合は、同様に同意の処理を行います。

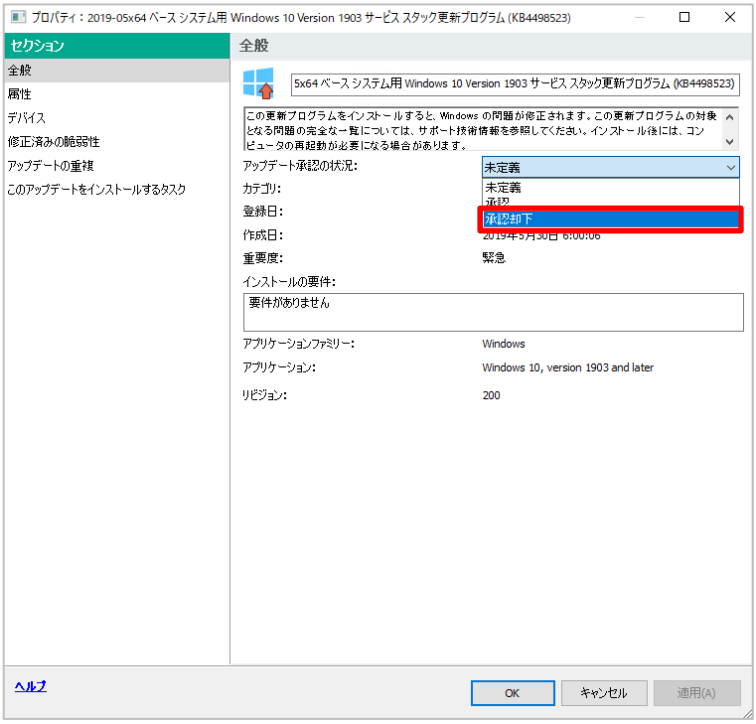
アップデートさせたくないアプリケーションがある場合、「承認却下」と設定することでインストール対象から除外することができます。

その場合、「アップデートのインストールと脆弱性の修正」タスクにて、「承認却下」と設定されているアプリケーションはインストールしないよう設定してください。（既定ではこの設定です）

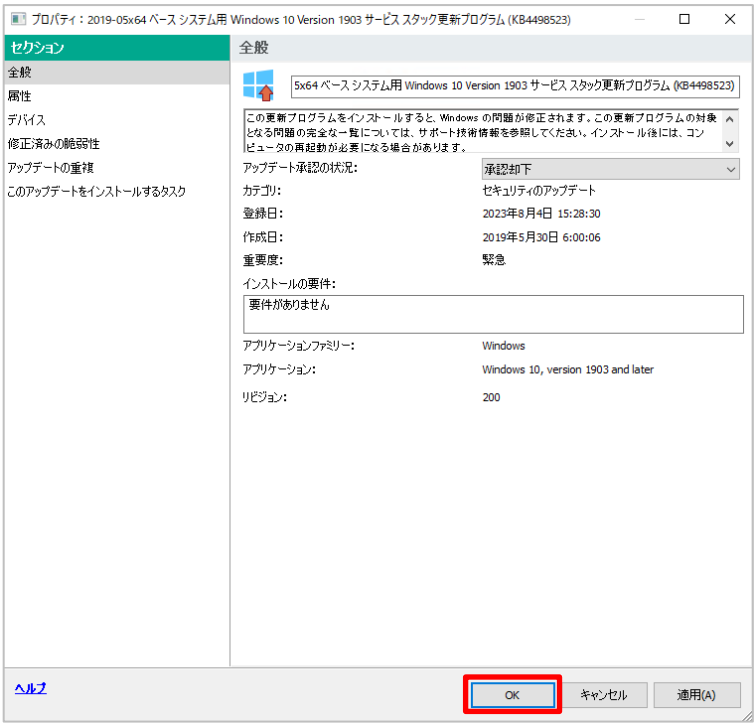
(1) アップデートさせたくないアプリケーション、またはパッチを右クリックし、「プロパティ」を開きます。



(2) 「アップデート承認の状況」にてリストを展開し、「承認却下」を選択します。



(3)「OK」をクリックして設定を保存します。

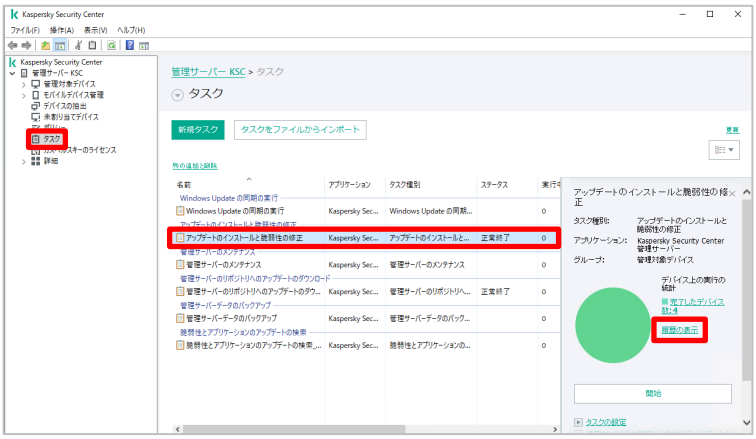


本節は以上です。

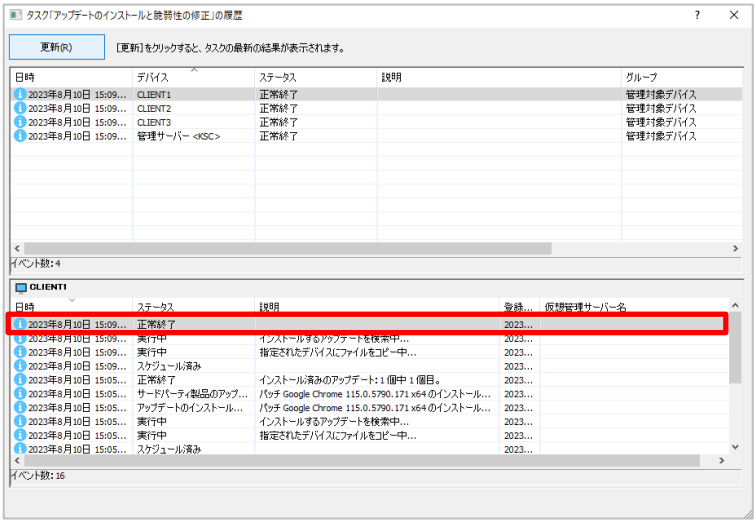
8.4. 「アップデートのインストールと脆弱性の修正」タスクの確認

「アップデートのインストールと脆弱性の修正」タスクの実行結果は、「履歴の表示」にて確認します。

(1) KSC にて「タスク」を選択します。
「アップデートのインストールと脆弱性の修正」を選択し、「履歴の表示」をクリックします。



(2) 「ステータス」欄が「正常終了」となっていることを確認します。



本章は以上です。

1. アップデートファイルの削除

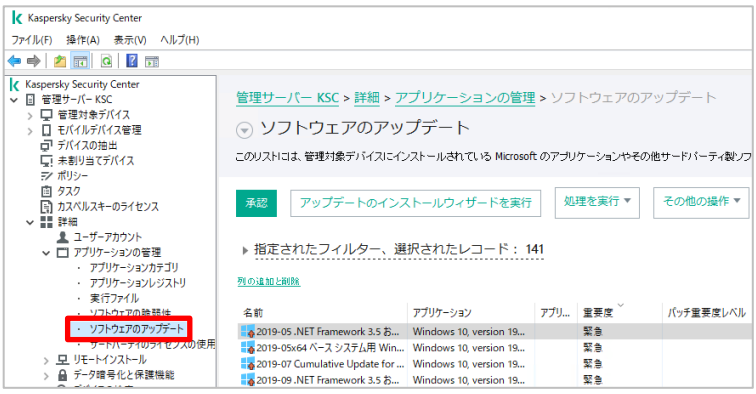
本章では、アップデートファイルの削除についてご説明します。

アップデート用のインストーラーファイルは KSC のフォルダーへダウンロードされ、クライアントへ展開されますが、インストール完了後も KSC 上に残り続け、自動的に削除されることはありません。

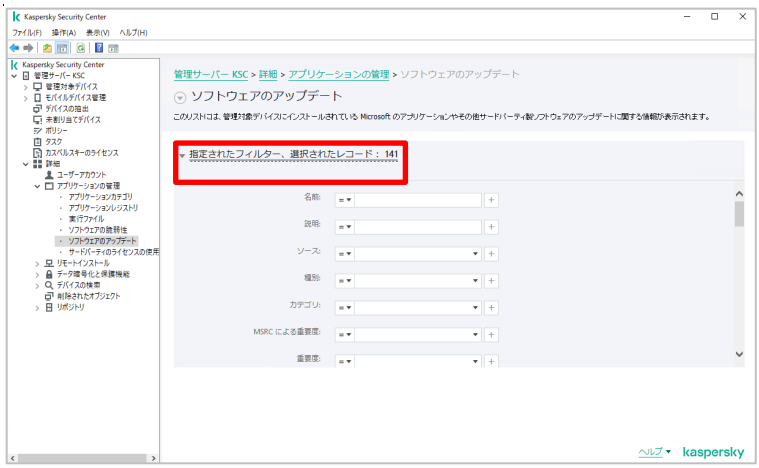
以下の手順を実施することで、アップデート対象のクライアントが存在しないインストーラーファイルを削除することができます。

※ 削除手順を実施してもメタデータは残り続けます。また、削除したインストーラーが再度必要となった場合はもう一度ダウンロードされます。

(1) KSC にて「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」を選択します。



(2) 右画面にて「指定されたフィルター、選択されたレコード」をクリックしてフィルター設定を表示します。

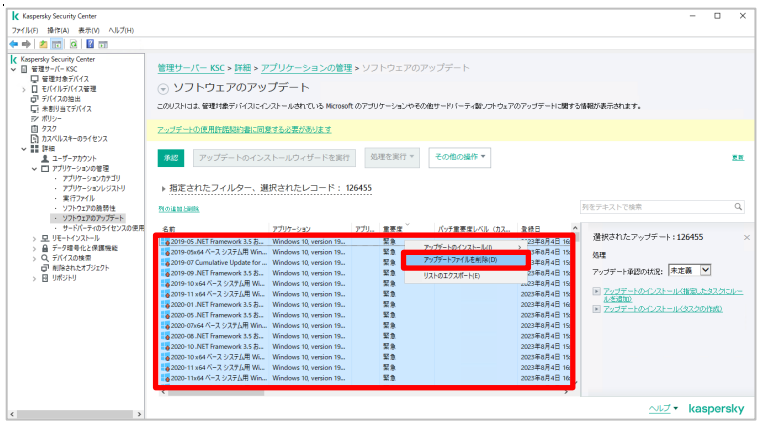


(3) 「デバイス上に未インストール」の条件をクリックし、「＞」から「＝」に変更します。

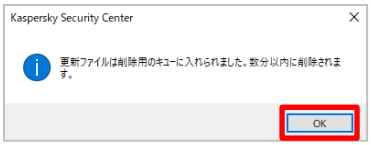
(4) 変更後、右側に「適用する」のと表示されるので、クリックします。アップデートが「0」であるリストが表示されます。

(5) アップデートのリストを全選択し、右クリックして「アップデートファイルを削除」をクリックします。

※ 対象の数により、全選択や右クリック後のメニュー表示に時間がかかる場合があります。



(6) ダイアログが表示されるので、「OK」をクリックして閉じます。
数分後に対象となるファイルは自動的に削除されます。



(7) 実施後、フィルター条件を元の「＞」に戻してください。

本章は以上です。

2. 「アップデートのインストールと脆弱性の修正」タスクの手動作成、及び詳細

本章では、「アップデートのインストールと脆弱性の修正」タスクについて、詳細と手動で作成する際の手順をご説明します。

手動でタスクを設定したい、各タスクの設定項目について詳細を確認したい場合にご参照ください。

タスクには以下 3 種類のルール設定があります。

- **すべてのアップデートのルール**
  - 脆弱性やアップデート情報に基づいたルール設定です。Microsoft 製品、サードパーティ製品を区別しません。

- **Windows Update のルール**
  - Microsoft 製品に関するアップデートルールです。対象とする Microsoft 製品の選択や、「重要な更新」「ドライバ」などアップデートのカテゴリを決定します。

- **サードパーティ製品のアップデートのルール**
  - サードパーティ製品のアップデートルールです。対象とするアプリケーションを決定します。

ルール毎にタスクを作成することもできますが、一つのタスクで 3 つのルールを組み合わせることも可能です。

すべての項目を最新にアップデートする設定も可能ですが、初期アップデートに時間がかかり、適用の順番がバラバラになる（Service Pack を適用する前にパッチを当て、二重にパッチを当ててしまう）などの事態になる可能性が考えられるため、環境や運用に合わせて設定をご検討ください。

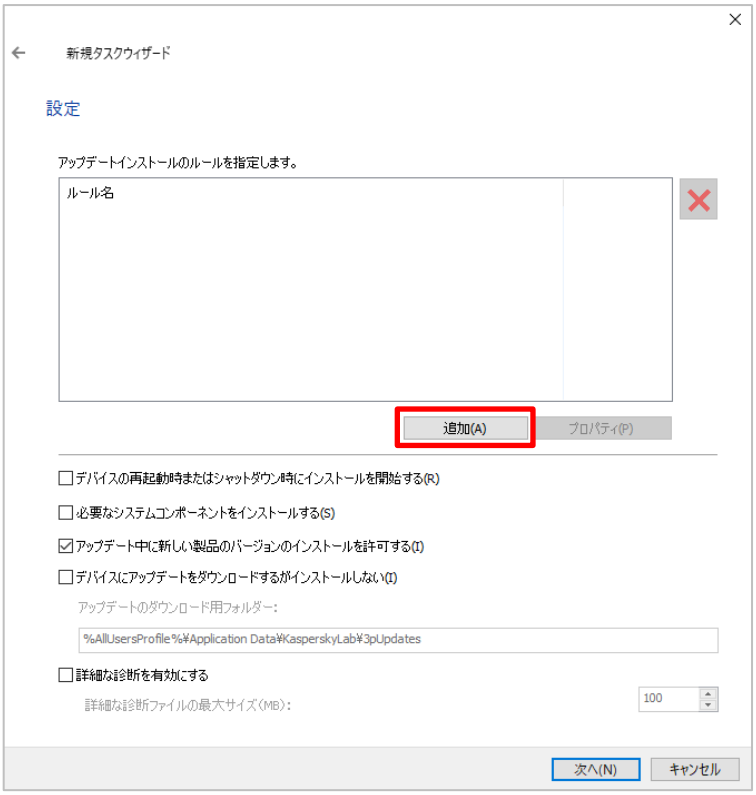
2.1. 全般的な脆弱性パッチ及びアップデートパッチの作成、設定

「すべてのアップデートルール」を作成、設定する際の手順です。

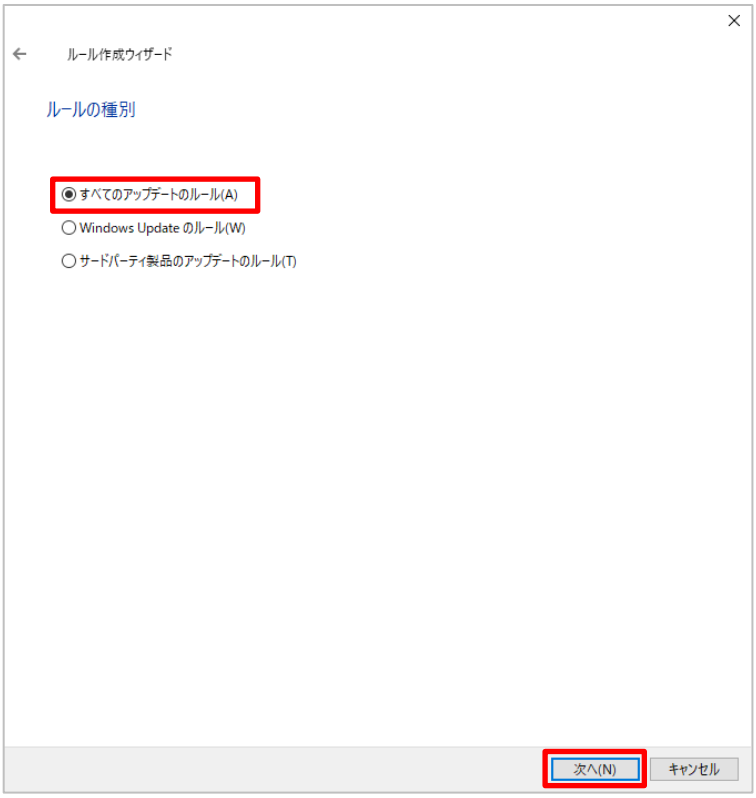
(1) KSC にて「タスク」を選択し、画面右側の「新規タスク」をクリックします。

(2) 新規タスクウィザードが起動します。「Kaspersky Security Center 管理サーバー」→「アップデートのインストールと脆弱性の修正」を選択し、「次へ」をクリックします。

(3)「追加」ボタンをクリックします。

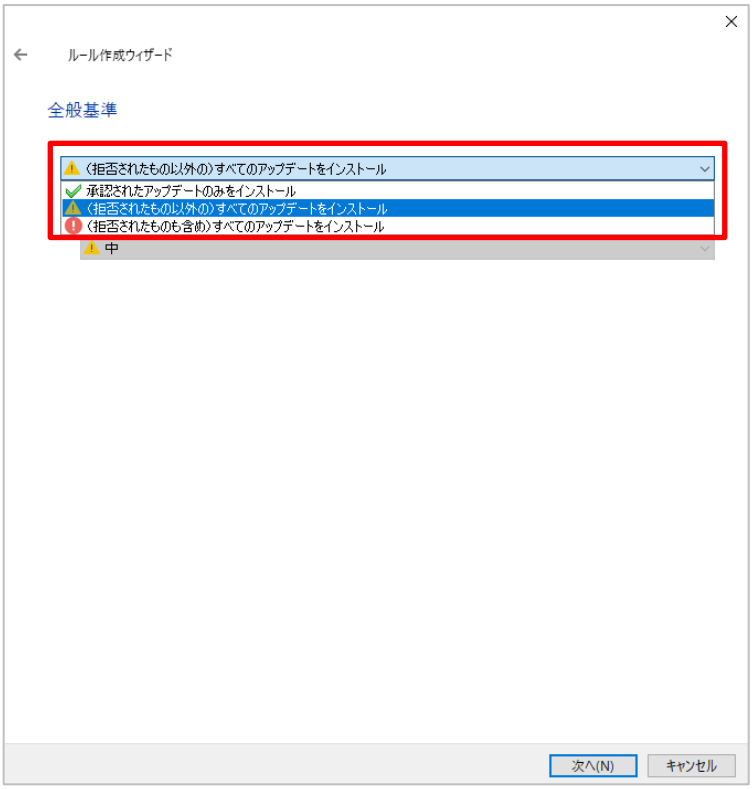


(4)「すべてのアップデートのルール」にチェックを入れ、「次へ」をクリックします。



(5)「全般基準」を設定します。

ここではアップデートの種類と脆弱性の基準を選択します。まず、アップデートの種類を選択します。以下の 3 種類からの選択です。



・承認されたアップデートのみをインストール。

→ 管理者によって手動で「承認」されたアップデートのみをインストールする設定です。

・(拒否されたもの以外の)すべてのアップデートをインストール。

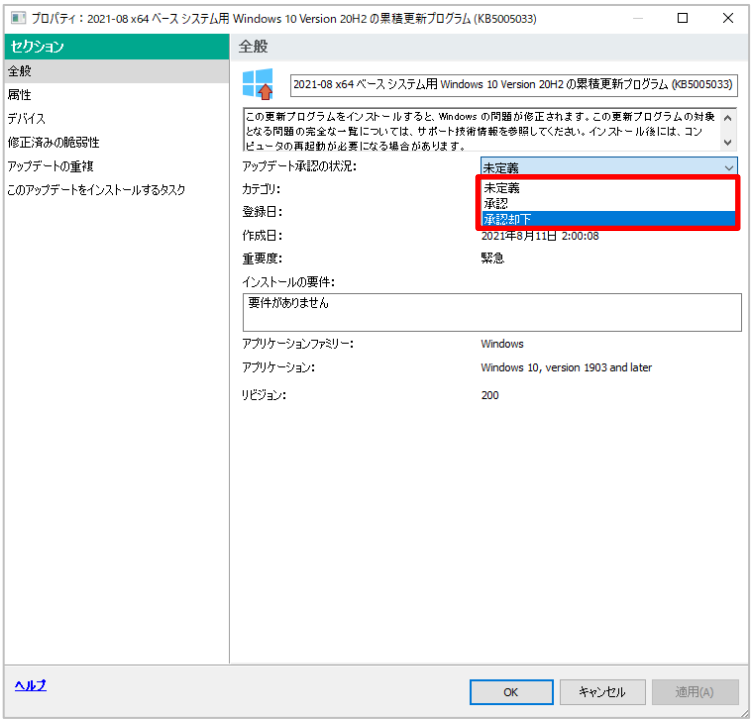
→「拒否」と設定されたもの以外はインストールする設定です。既定の設定です。

・(拒否されたものも含め)すべてのアップデートをインストール。

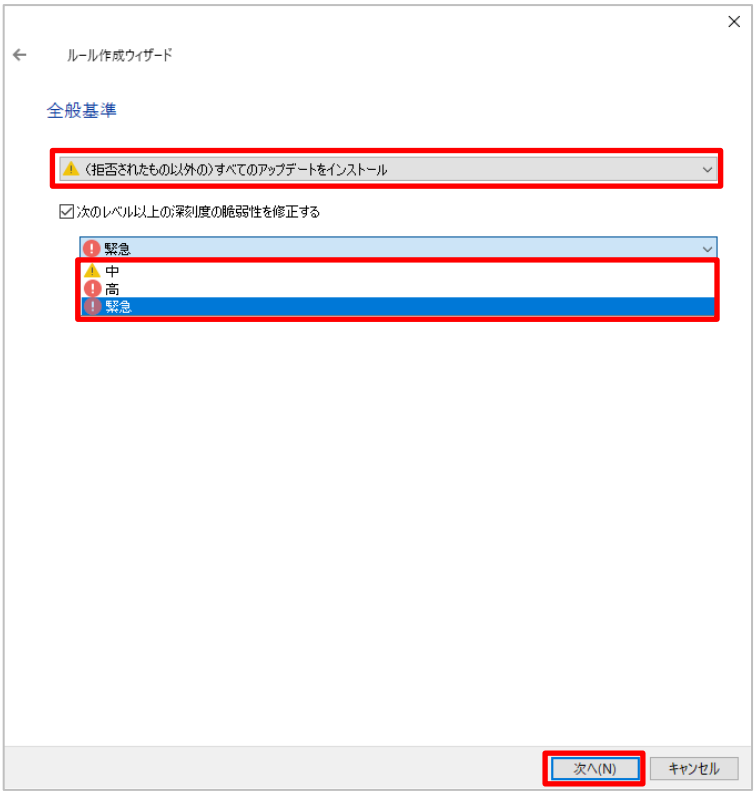
→「拒否」と設定されたものも含め、すべてインストールする設定です。

※「承認」、「拒否」の設定は、各アップデートリストのプロパティにて設定することができます。

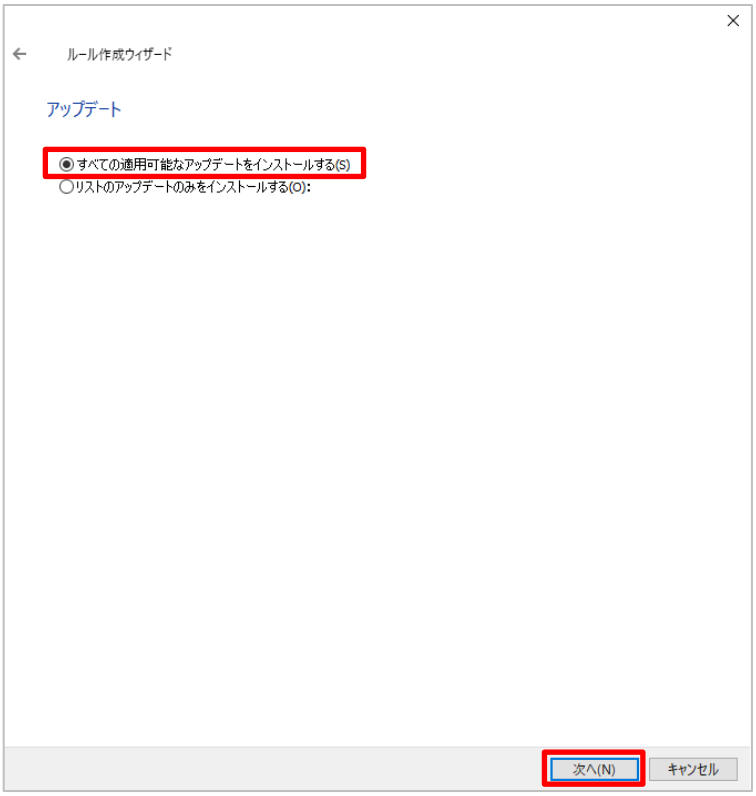
「アップデート承認の状況」のリストボックスから選択します。



(6) 「次のレベル以上の深刻度の脆弱性を修正する」にチェックを入れる事で、カスペルスキーが認定した重要度に基づいた脆弱性の修正を変更する事が可能です。
条件に追加したい場合は、チェックを入れ、中・高・緊急の 3 種類から選択します。

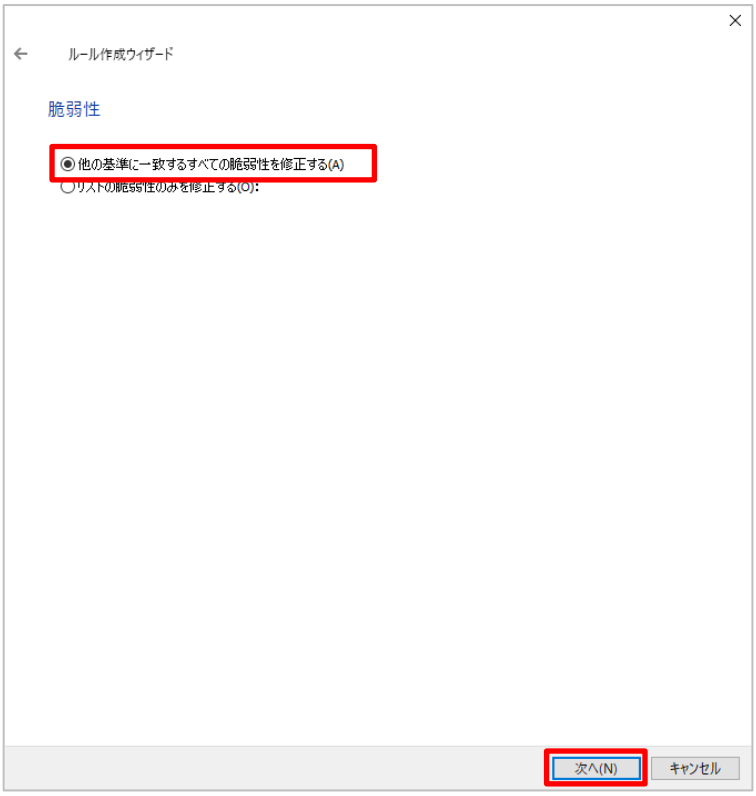


(7) 「アップデート」を設定します。
「すべての適用可能なアップデートをインストールする」にチェックが入っていることを確認し、「次へ」をクリックします。

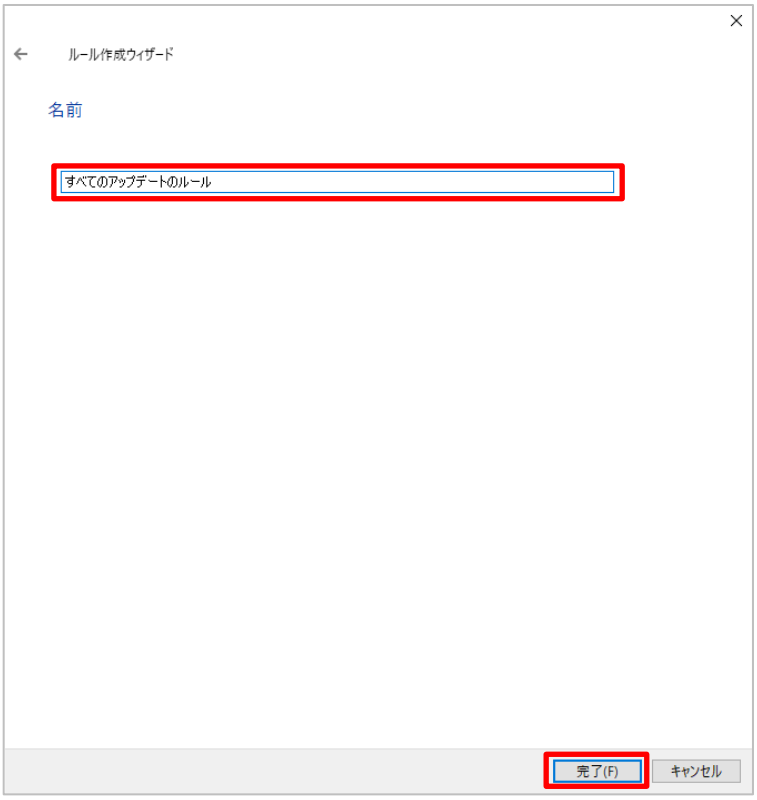


(8) 「脆弱性」を設定します。
「他の基準に一致するすべての脆弱性を修正する」にチェックが入っていることを確認します。

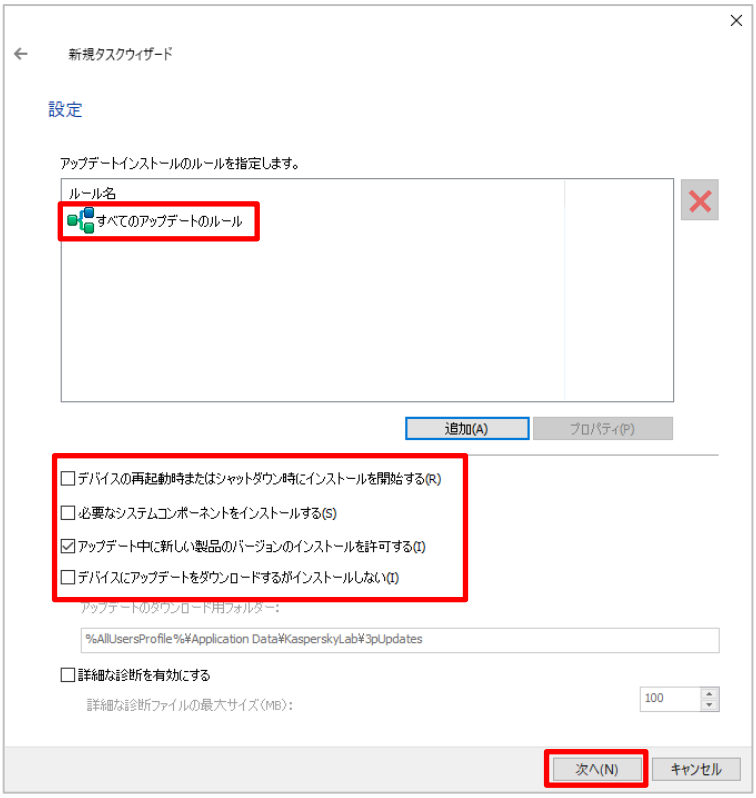
「次へ」をクリックします。



(9) ルール名を設定します。
設定後、「完了」をクリックします。
（ここでは「すべてのアップデートのルール」としています）



(10)　ルールが作成されていることを確認します。
画面下部の 4 つの項目について必要に応じて設定をします。
4 つの項目については、以下(11)で説明します。



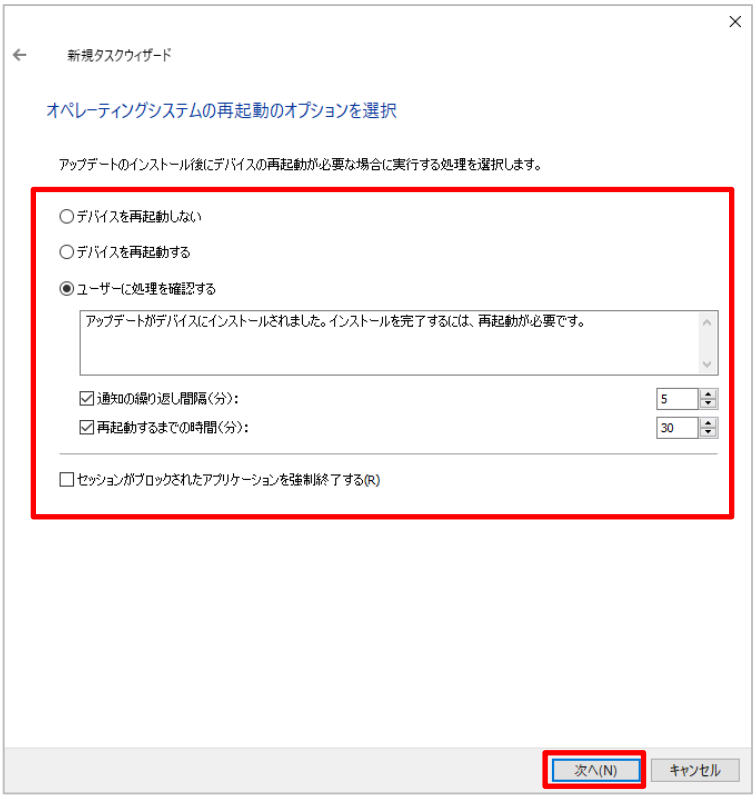
(11)　上記⑩の図に記載されている 4 項目の詳細は以下の通りです。

- **デバイスの再起動時またはシャットダウン時にインストールを開始する**
  タスク実行時では無く、コンピューターの再起動時、またはシャットダウン時にアップデートをインストールする設定です。
- **必要なシステムコンポーネントをインストールする**
  必須のコンポーネントも一緒にインストールする設定です。例えば、Apache をインストールする際、Java が必要となる場合、Java も同時にアップデートされます。
- **アップデート中に新しい製品のバージョンのインストールを許可する（既定で有効）**
  アプリケーションのバージョンを上げる場合にチェックを入れる設定です。
  例えば、「Skype 5.10」がインストールされているコンピューターと「Skype 6.6」がインストールされているコンピューターが存在し、「Skype 6.9」にアップグレードするとします。
  - ➢ このオプションが**「有効」**になっている場合、「Skype6.6」のほか、異なるバージョンである「Skype 5.10」も対象となり、「Skype 6.9」にアップグレードされます。
  - ➢ このオプションが**「無効」**になっている場合、同じバージョン(6.x)である「Skype 6.6」がインストールされたコンピューターのみが「Skype 6.9」にアップグレードされます。
- **デバイスにアップデートをダウンロードするがインストールしない**
  → アップデートファイルをダウンロードしますが、インストールは実際には行わない設定です。

(12)　アップデート後の OS の処理を設定します。以下 3 種類の選択が可能です。

- デバイスを再起動しない
- デバイスを再起動する
- ユーザーに処理を確認する

「デバイスを再起動する」を設定した場合、インストール完了後、60 秒後に強制的に再起動されます。
「ユーザーに処理を確認する」を設定した場合、表示するメッセージの設定や、通知の繰り返し時間、再起動するまでの時間を設定可能です。
また、アプリケーションを強制的に閉じる設定も可能です。
設定後、「次へ」をクリックします。



(13)　タスクを実行するデバイスを選択します。
ここでは「管理グループにタスクを割り当てる」を選択します。

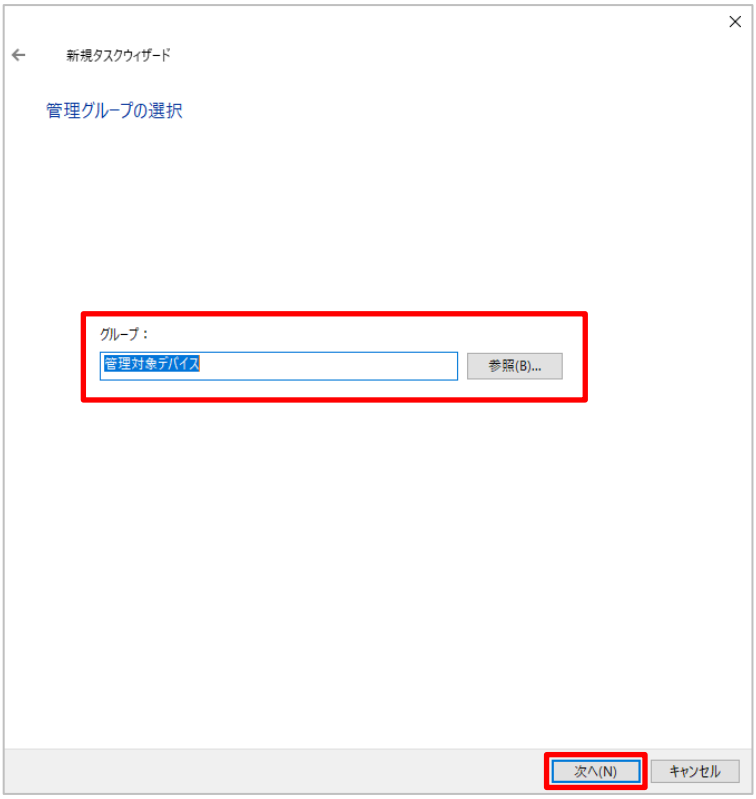
特定のデバイスを指定したい場合は、「ネットワークの管理サーバーによって検出されたデバイスを選択する」を選択し、対象とするデバイスを選択します。

(14)　管理グループを選択します。

グループ分けを細かく設定している場合、「参照」をクリックし選択します。

既定では、「管理対象デバイス」が選択されます。

選択後、「次へ」をクリックします。



(15)　タスクのスケジュールを設定します。

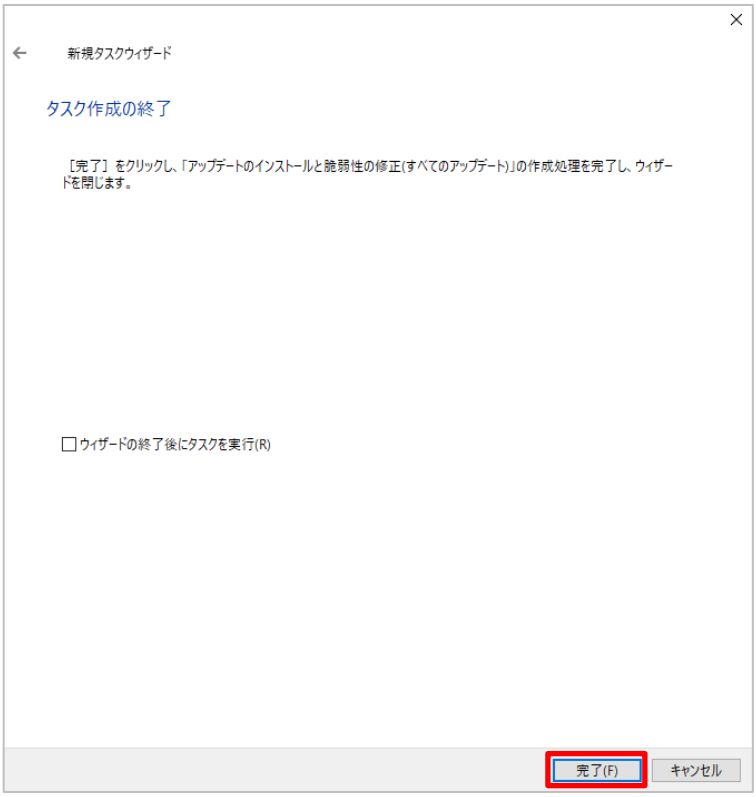
既定では「手動」となっております。

設定後、「次へ」をクリックします。

(16)　タスク名を設定します。
既定では、「アップデートのインストールと脆弱性の修正」となります。

設定後、「次へ」をクリックします。

(17)　タスクの作成が正常に終了したことを確認し、「完了」をクリックします。
タスク作成後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」にチェックを入れます。



本節は以上です。

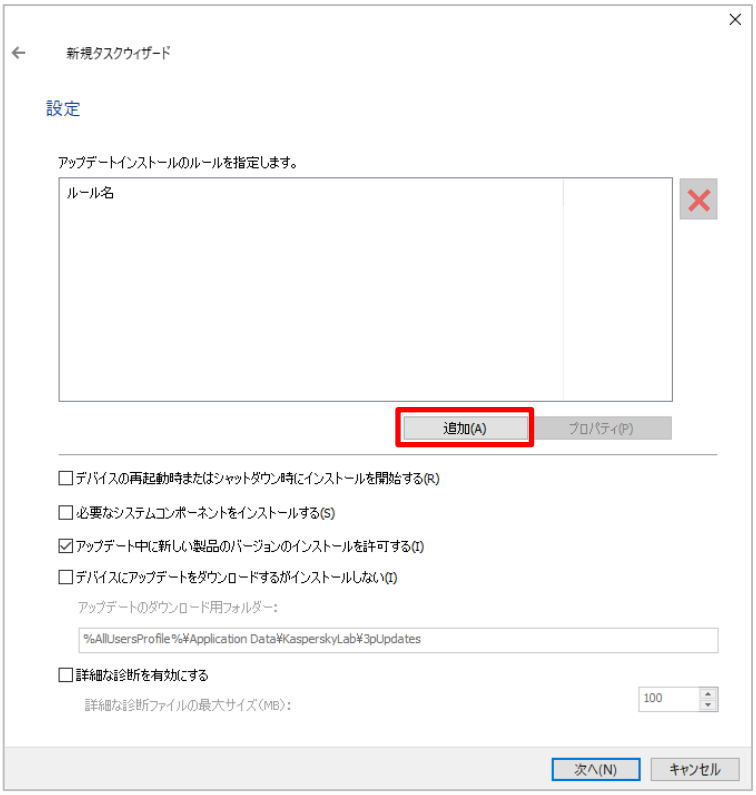
2.2. Microsoft 製品の脆弱性パッチ及びアップデートパッチの作成、設定

「Windows Update のルール」を作成、設定する際の手順です。

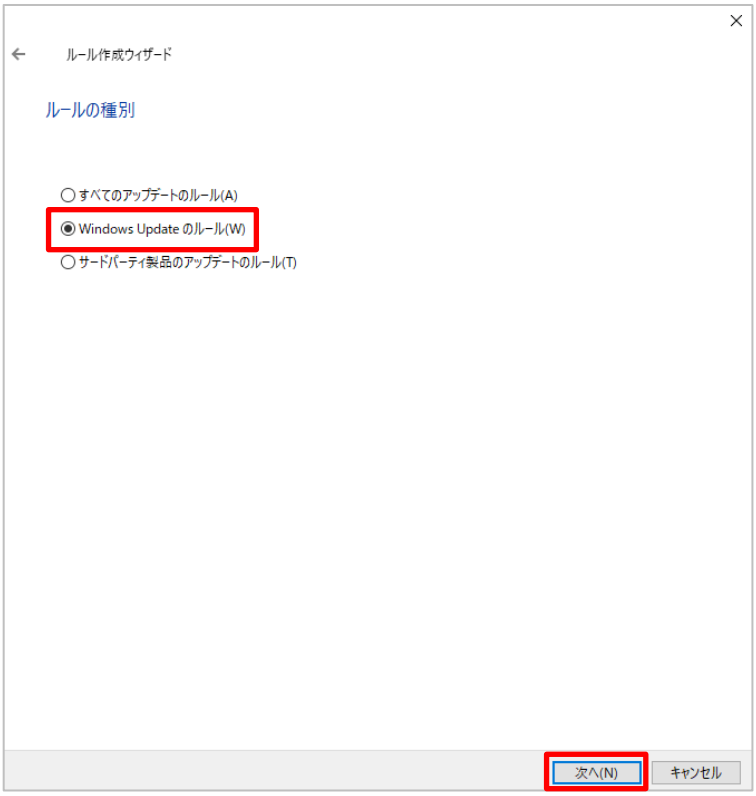
(1) KSC にて「タスク」を選択し、画面右側の「新規タスク」をクリックします。

(2) 新規タスクウィザードが起動します。「Kaspersky Security Center 管理サーバー」→「アップデートのインストールと脆弱性の修正」を選択し、「次へ」をクリックします。

(3)「追加」ボタンをクリックします。



(4)「Windows Update のルール」にチェックを入れ、「次へ」をクリックします。



(5)「全般基準」を開きます。

ここでは全般基準を設定します。

・承認されたアップデートのみをインストール。

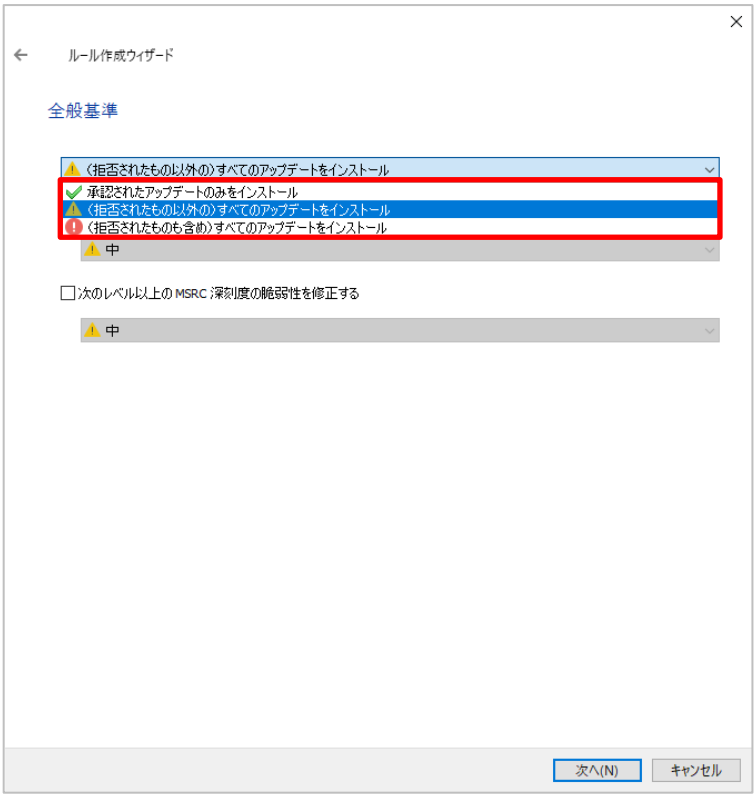
→ 管理者によって手動で「承認」されたアップデートのみをインストールする設定です。

・(拒否されたもの以外の)すべてのアップデートをインストール。

→「拒否」と設定されたもの以外はインストールする設定です。既定の設定です。

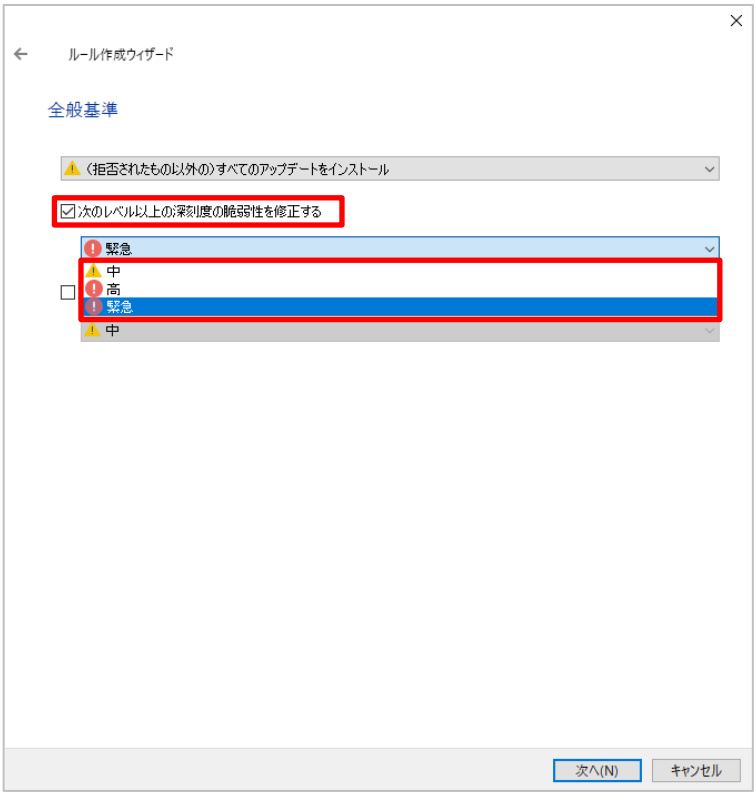
・(拒否されたものも含め)すべてのアップデートをインストール。

→「拒否」と設定されたものも含め、すべてインストールする設定です。



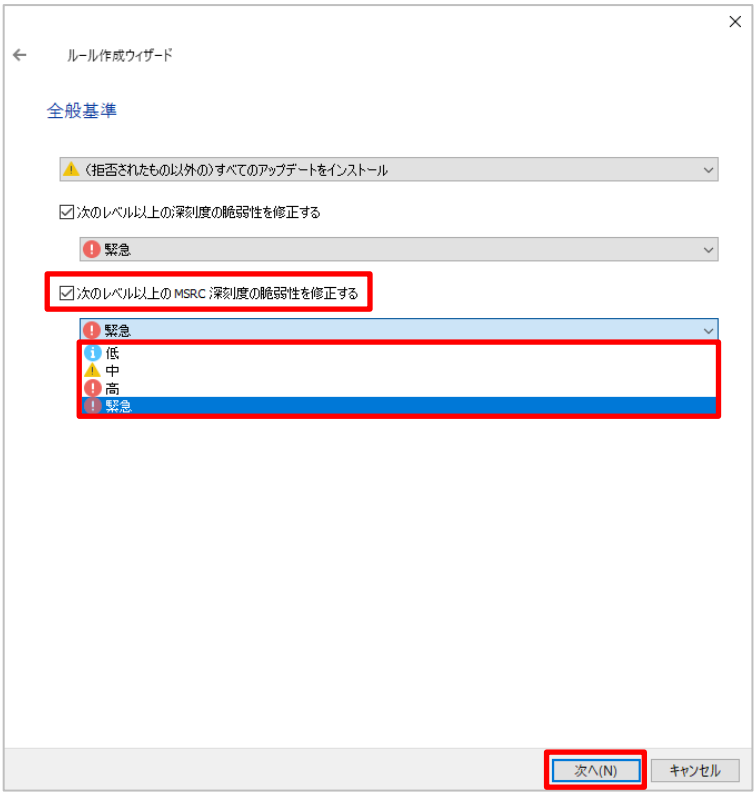
(6) カスペルスキーが認定した重要度に基づいた脆弱性の修正を変更する事が可能です。

条件に追加したい場合は、「次のレベル以上の深刻度の脆弱性を修正する」にチェックを入れて中・高・緊急の 3 種類から選択します。



(7) MSRC（マイクロソフト セキュリティ レスポンス センター）の基準に基づいた脆弱性の修正を設定できます。
条件に追加したい場合は、「次のレベル以上の MSRC 重要度の脆弱性を修正する」にチェックを入れて低・中・高・緊急の４種類から選択します。

設定後、「次へ」をクリックします。

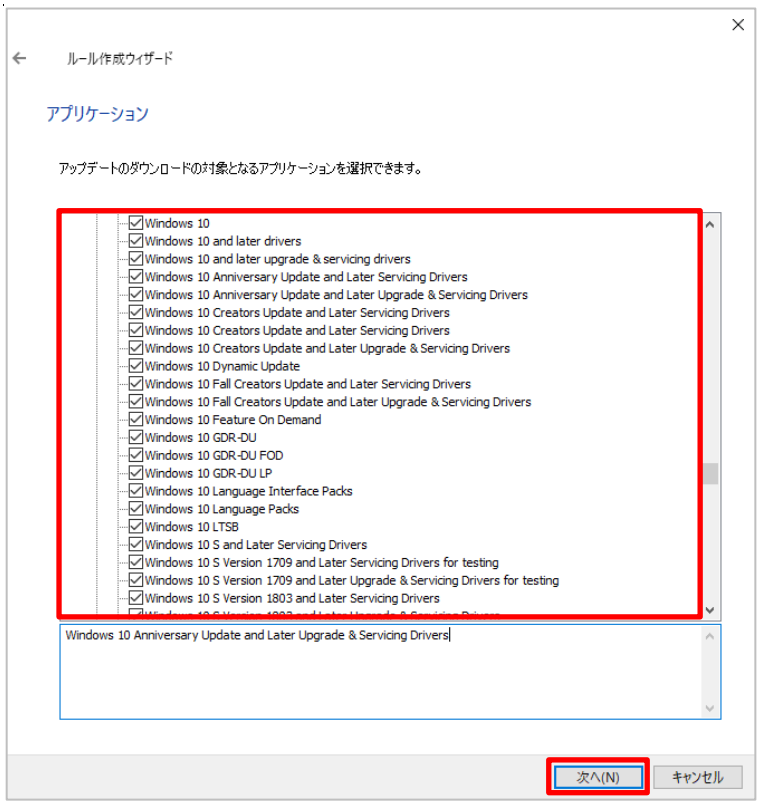


(8) 「アプリケーション」を設定します。
ここではアップデートの対象とする Microsoft 製品を選択します。

既定ではすべてが選択されているので必要なものを選定し設定してください。（図は、Windows10 のみを選択しています。）

設定後、「次へ」をクリックします。

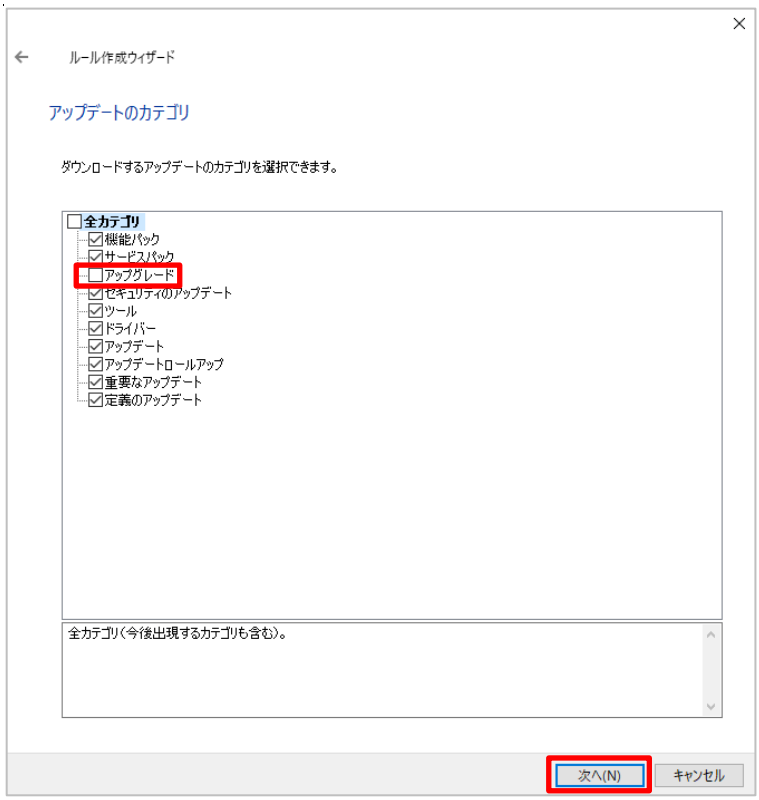
※最新バージョンがリリースされている場合、「Windows Update の同期の実行」タスク終了後にこのリストの内容も更新される場合があります。
定期的に確認し、チェックのオン、オフを設定してください。



(9) 「アップデートカテゴリ」を設定します。
ここではアップデートするカテゴリを選択します。

「アップグレード」のチェックを外し、必要に応じて他カテゴリを選択して、「次へ」をクリックします。

※ 「アップグレード」は Windows 10 Future Update や OS のアップグレードに関する情報となります。
意図せず Future Update が行われないよう、チェックを外すことを推奨します。



(10) この後の手順は、Appendix「2.1. 全般的な脆弱性パッチ及びアップデートパッチの作成、設定」の”(9)”以降と同様となりますので、そちらをご参照ください。

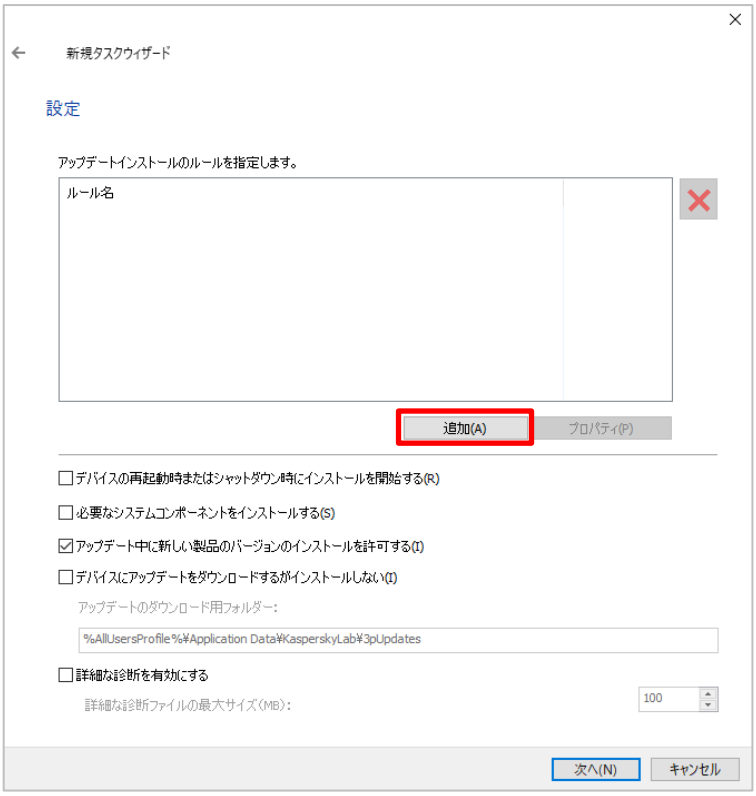
2.3. サードパーティ製品の脆弱性パッチ及びアップデートパッチの作成、設定

「サードパーティ製品のアップデートルール」を設定する際の手順です。

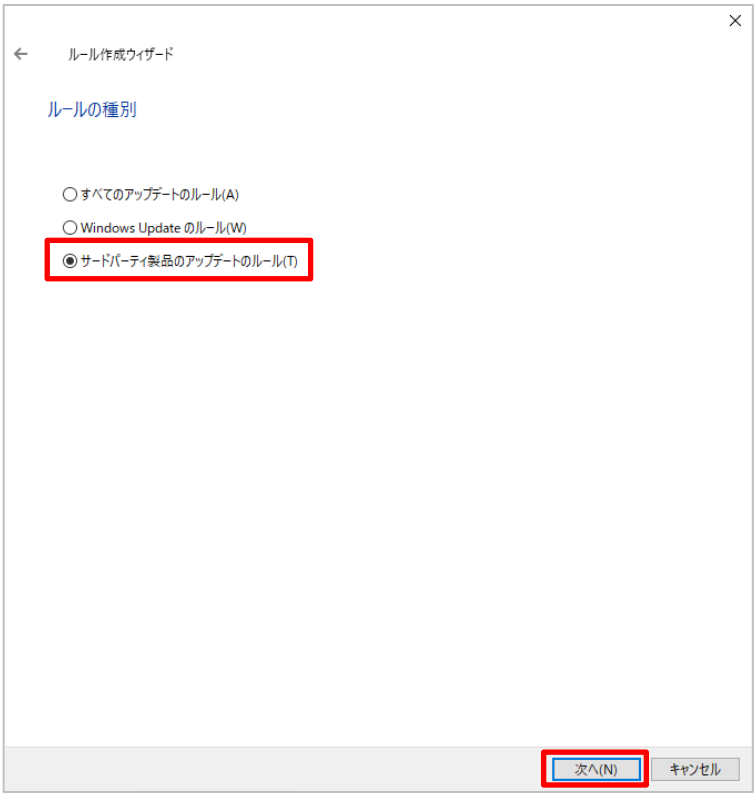
(1) KSC にて「タスク」を選択し、画面右側の「新規タスク」をクリックします。

(2) 新規タスクウィザードが起動します。「Kaspersky Security Center 管理サーバー」→「アップデートのインストールと脆弱性の修正」を選択し、「次へ」をクリックします。

(3) 「追加」ボタンをクリックします。

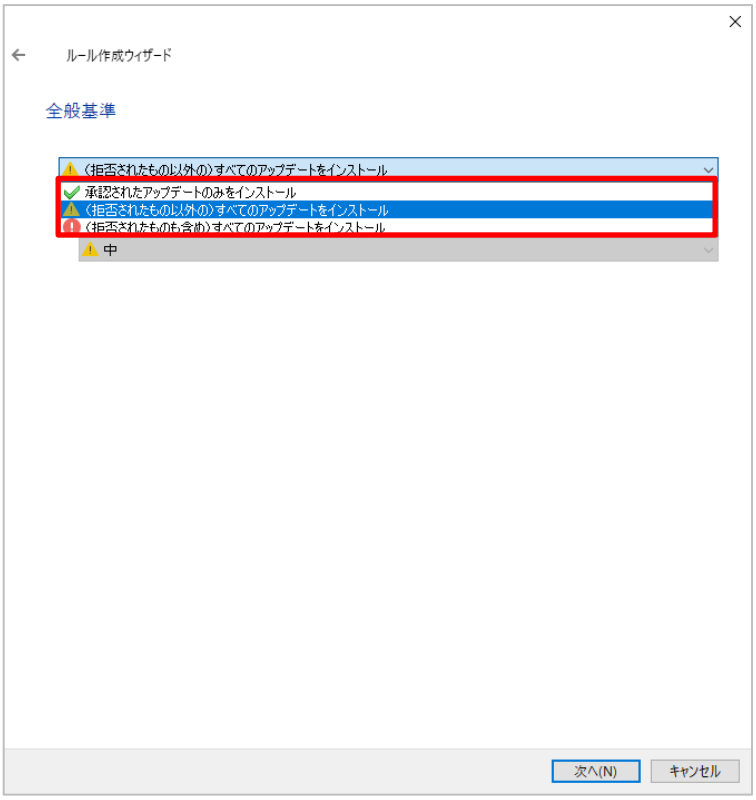


(4) 「サードパーティ製品のアップデートのルール」にチェックを入れ、「次へ」をクリックします。



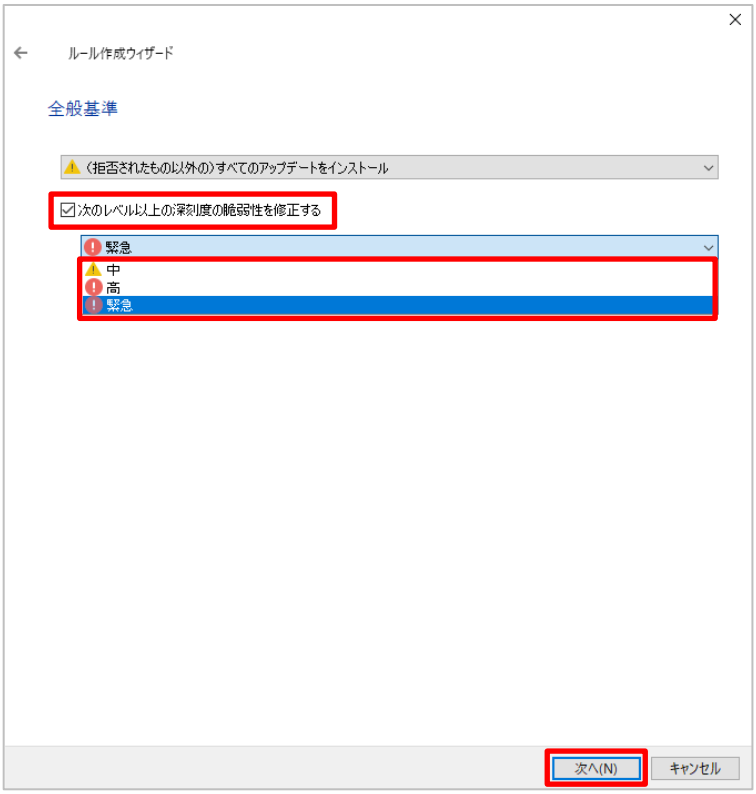
(5)「全般基準」を設定します。

・承認されたアップデートのみをインストール。
→ 管理者によって手動で許可されたアップデートのみをインストールする設定です。
・(拒否されたもの以外の)すべてのアップデートをインストール。
→ 拒否されたもの以外は自動でインストールする設定です。既定の設定です。
・(拒否されたものも含め)すべてのアップデートをインストール。
→ 拒否したものもすべてインストールする設定です。



(6) カスペルスキーが認定した重要度に基づいた脆弱性の修正を変更する事が可能です。
条件に追加したい場合は、「次のレベル以上の深刻度の脆弱性を修正する」にチェックを入れて中・高・緊急の 3 種類から選択します。

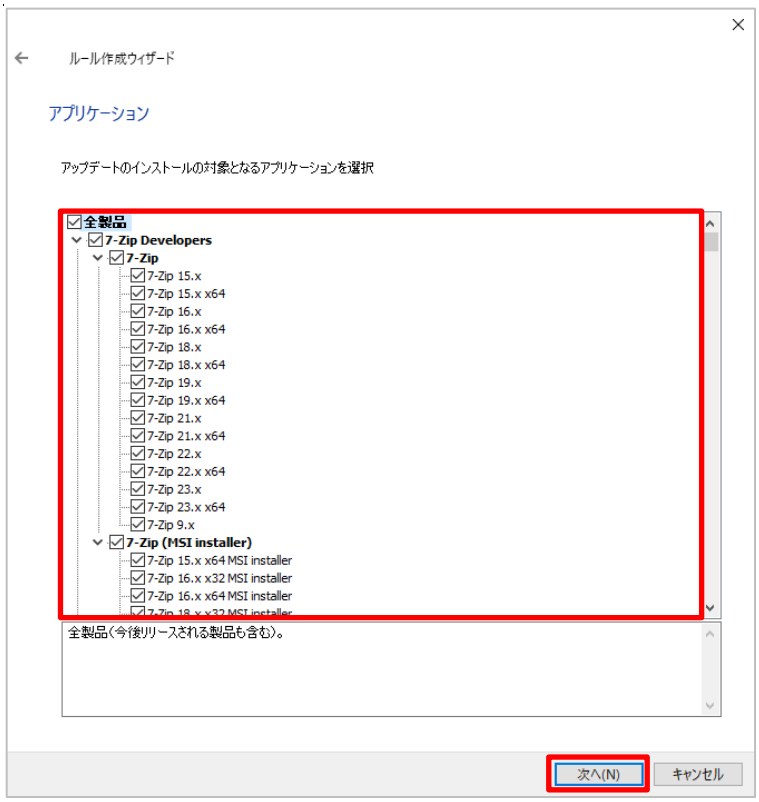
設定後、「次へ」をクリックします。



(7) 「アプリケーション」を開きます。
ここではアップデートの対象とするアプリケーションを選択します。

既定ではすべてが選択されているので必要なものを選定し設定してください。

設定後、「次へ」をクリックします。



(8) この後の手順は、Appendix「2.1. 全般的な脆弱性パッチ及びアップデートパッチの作成、設定」の”(9)”以降と同様となりますので、そちらをご参照ください。

本章は以上です。

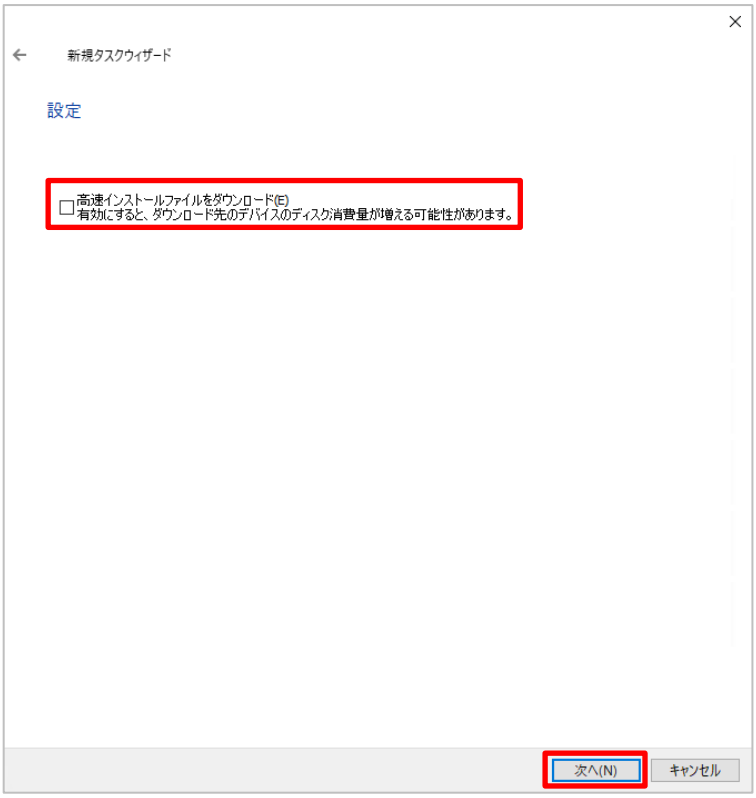
3. 「Windows Update の同期の実行」タスクの手動作成

本章では、「Windows Update の同期の実行」タスクについて、手動で作成する際の手順をご説明します。このタスクは複数作成することはできません。

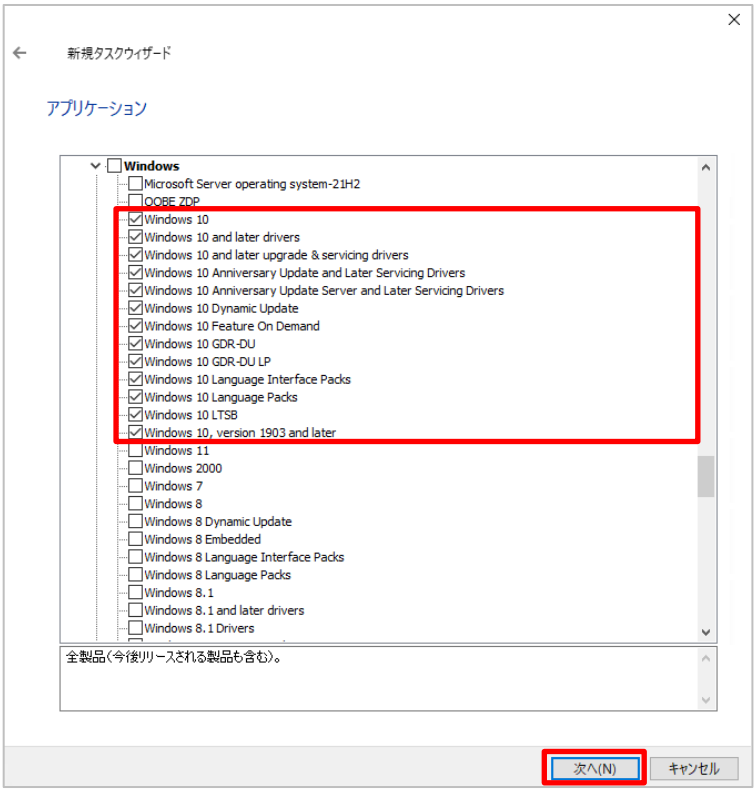
(1) KSC にて「タスク」を選択し、画面右側の「新規タスク」クリックします。

(2) 新規タスクウィザードが起動します。「Kaspersky Security Center 管理サーバー」→「Windows Update の同期の実行」を選択し、「次へ」をクリックします。

(3) 「高速インストールファイルをダウンロード」のチェックは入れず、「次へ」をクリックします。

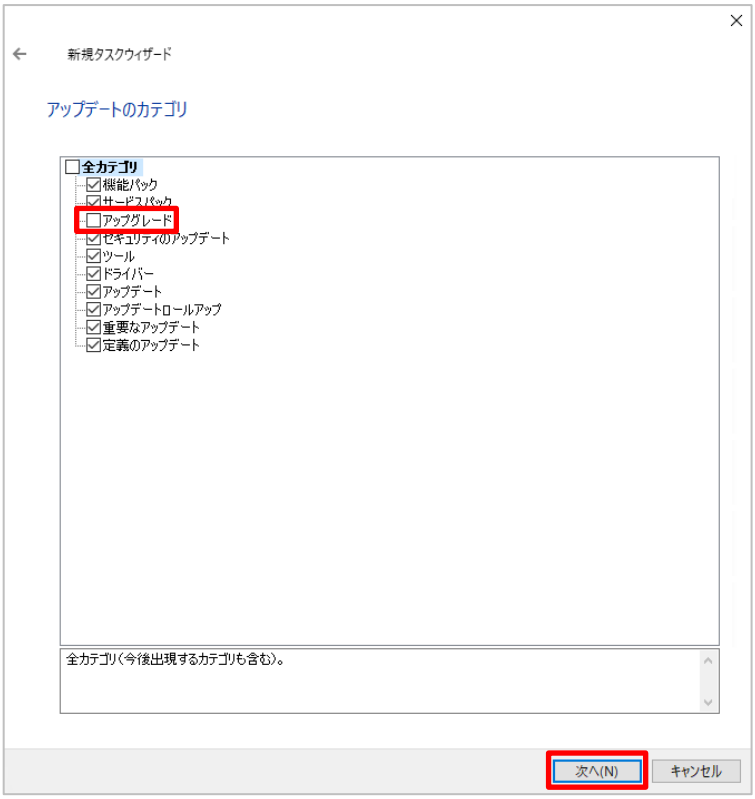


(4) アップデート対象のアプリケーションを選択します。
既定ではすべてが選択されていますが、**必要なアプリケーション・OS のみを選択**してください。
図は、Windows10 のみを選択している例です。

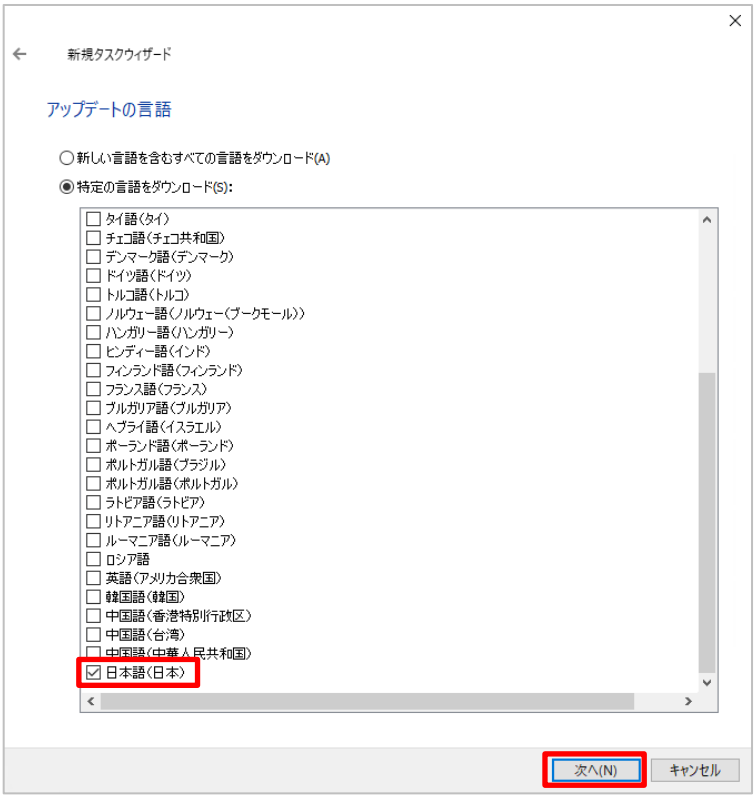


(5) 「アップデートカテゴリ」を設定します。
ここではアップデートするカテゴリを選択します。
既定ではすべてのカテゴリが選択されていますが、**「アップグレード」のチェックを外し**、必要に応じて他カテゴリを選択して、「次へ」をクリックします。

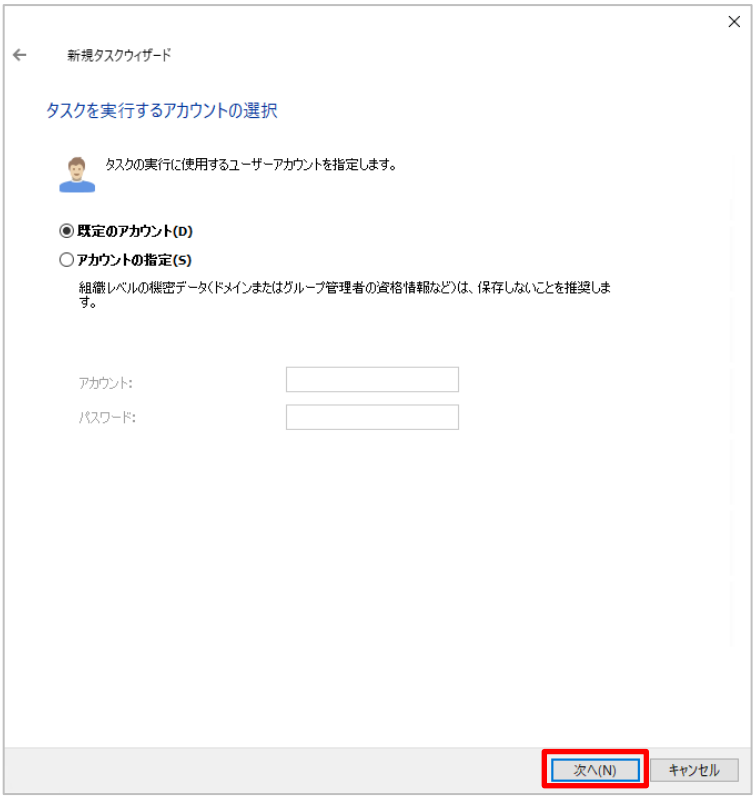
※ 「アップグレード」は Windows 10 Future Update や OS のアップグレードに関する情報となります。
意図せず Future Update が行われないよう、チェックを外すことを推奨します。



(6) 「特定の言語をダウンロード」にチェックし、「日本語」にチェックを入れ、「次へ」をクリックします



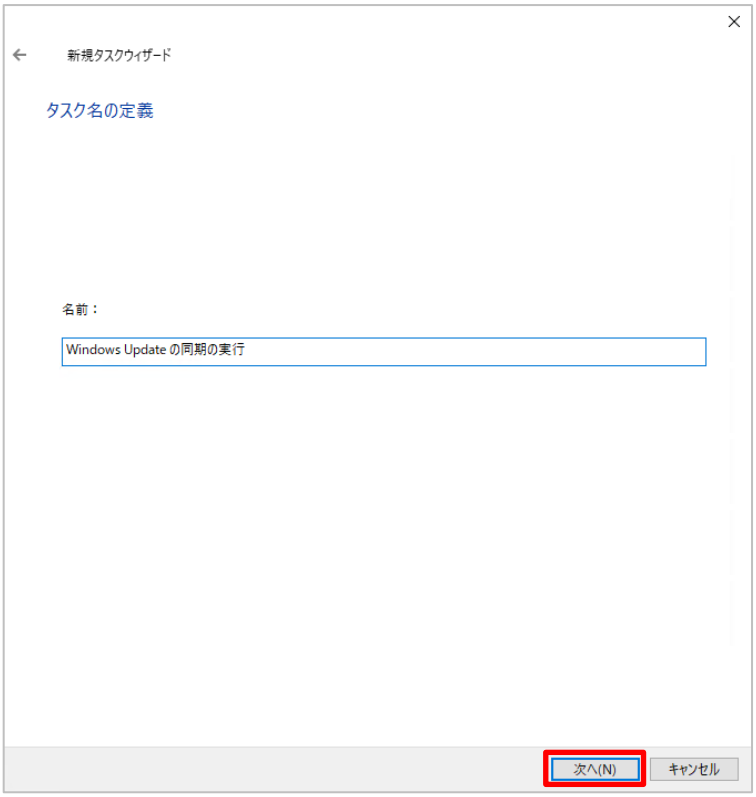
(7) 「次へ」をクリックします。



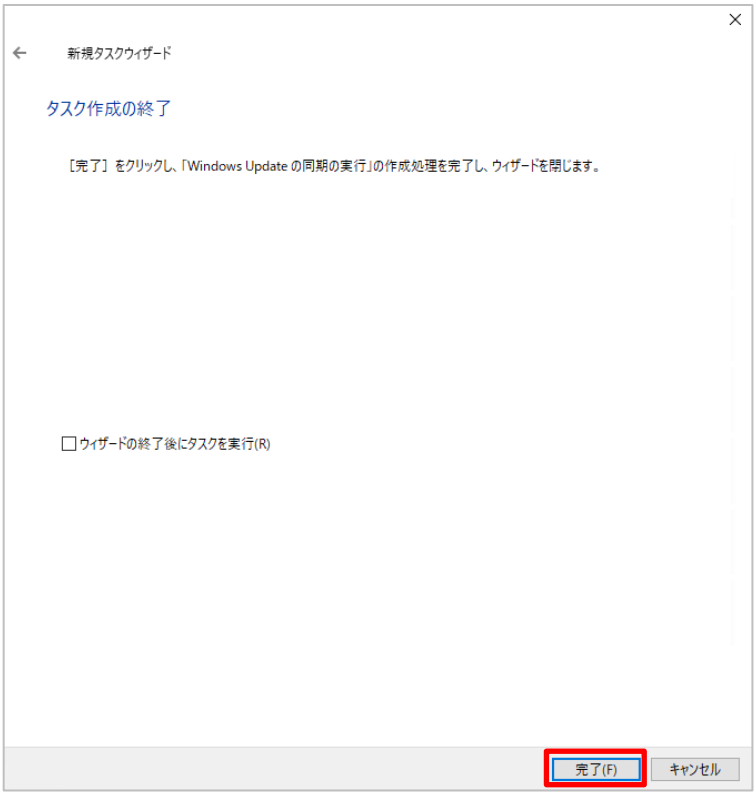
(8) 実行スケジュールとして以下を設定し、
「次へ」をクリックします。

・実行予定：毎週
・曜日：月曜日
・開始時刻：0:00:00

(9)「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。



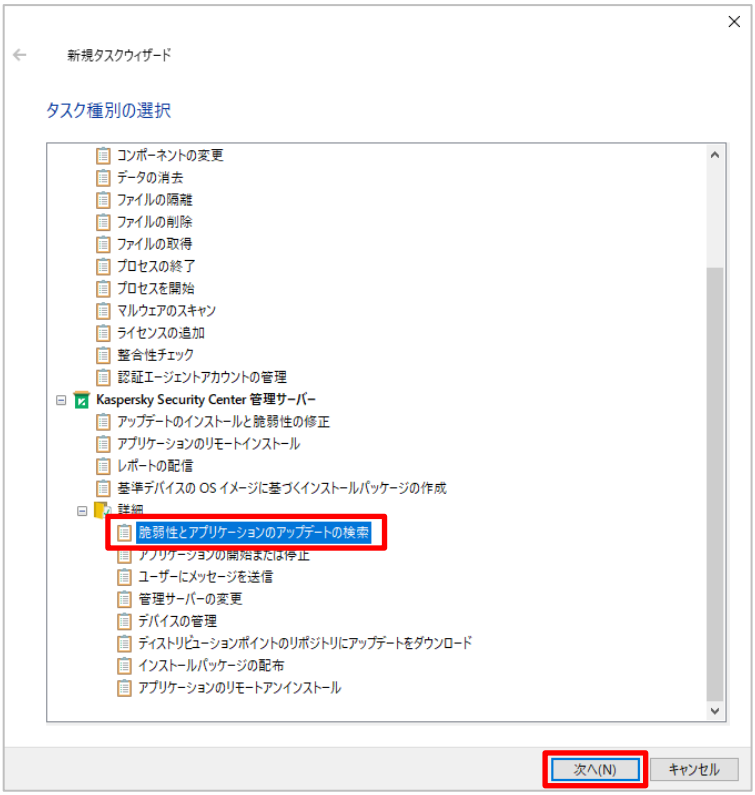
本章は以上です。

4.　「脆弱性とアプリケーションのアップデートの検索」タスクの手動作成

本章では、「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、手動で作成する際の手順をご説明します。

(1) KSC にて「タスク」を選択し、画面右側の「新規タスク」をクリックします。

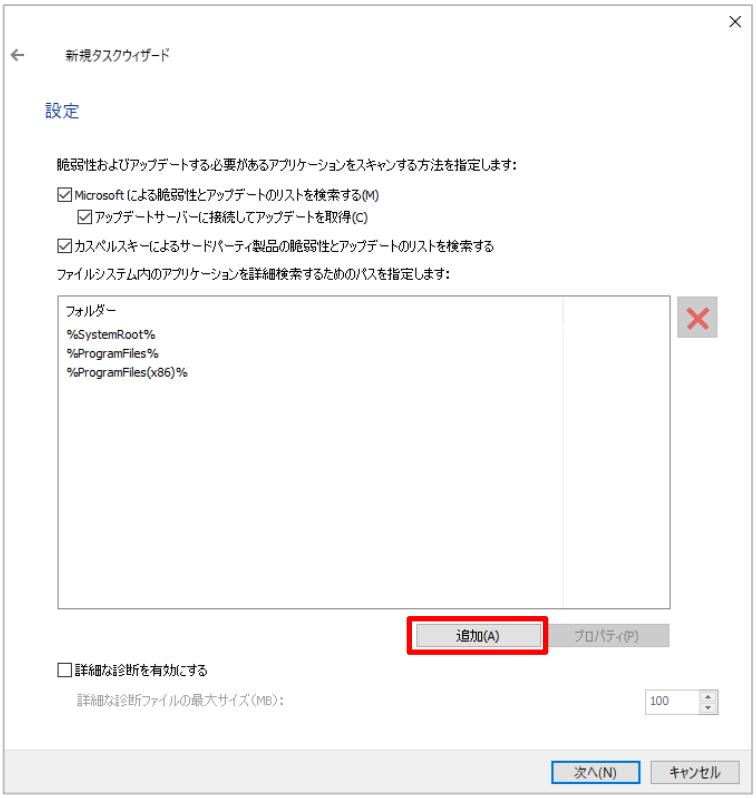
(2) 新規タスクウィザードが起動します。「Kaspersky Security Center 管理サーバー」→「脆弱性とアプリケーションのアップデートの検索」を選択し、「次へ」をクリックします。



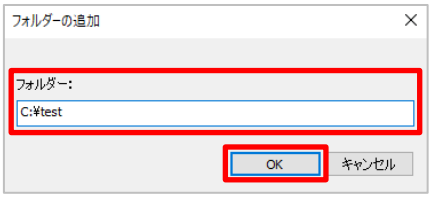
(3) 既定では以下のフォルダーがスキャンされます。

・%SystemRoot%
・%ProgramFiles%
・%ProgramFiles(x86)%

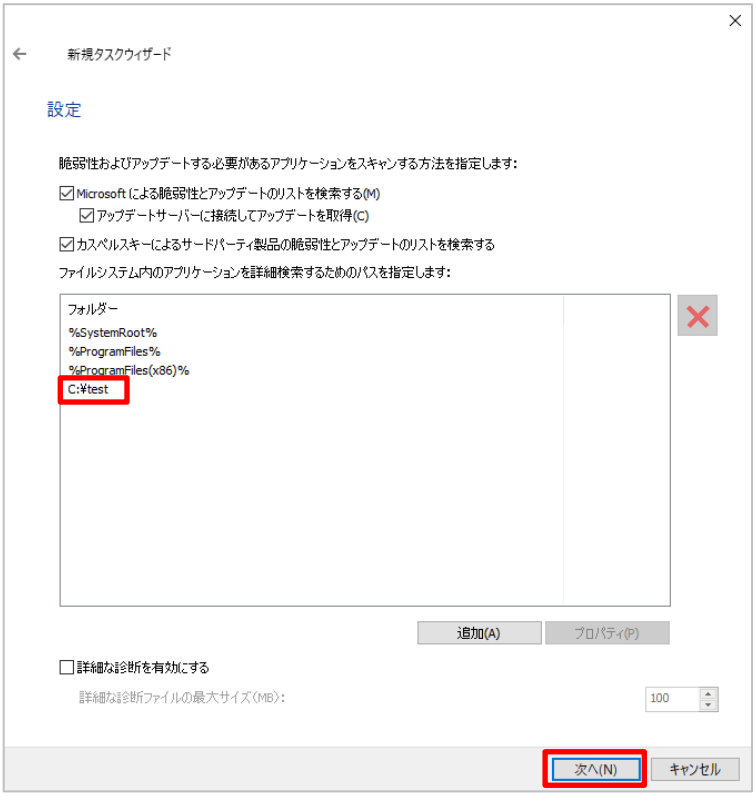
上記フォルダー以外をスキャン対象として追加したい場合、「追加」をクリックします。



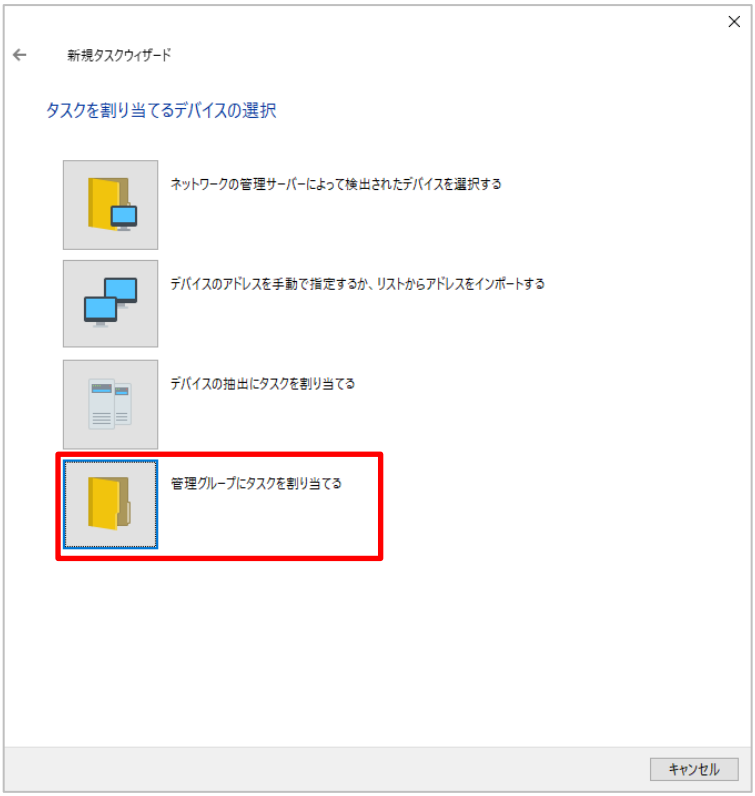
(4) スキャンに加えたいフォルダーパスを入力し、「OK」をクリックします。
（図は、「C:¥test」フォルダーを追加する例です。）



(5) 画面右側のフォルダー一覧に「C:¥test」が含まれていることを確認し、「次へ」をクリックします。



(6) タスクを割り当てるデバイス、グループを選択します。
ここでは、グループに割り当てるので、「管理グループにタスクを割り当てる」をクリックします。

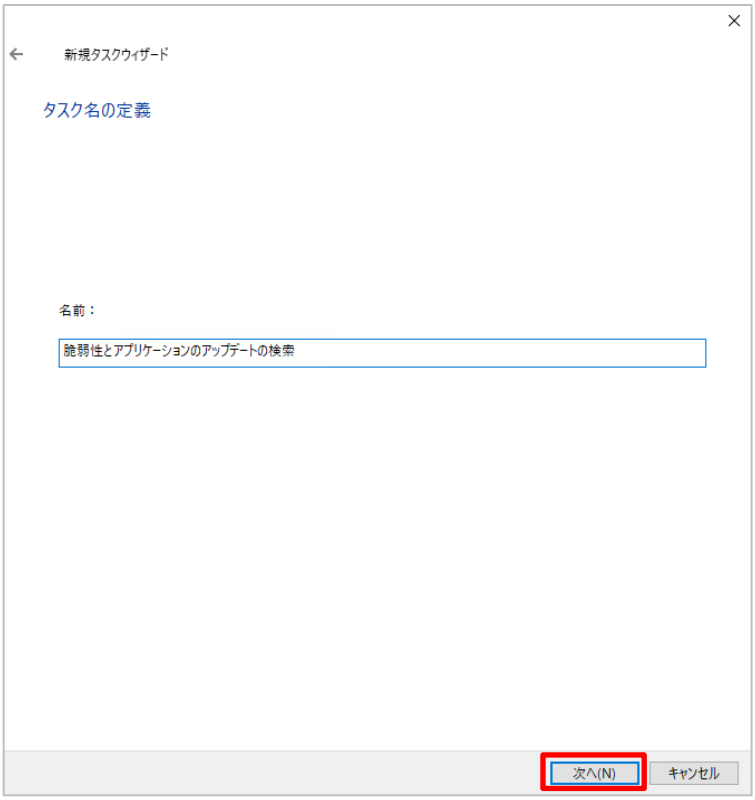


(7) グループを指定します。
ここでは、「管理対象デバイス」グループを選択しています。
「次へ」をクリックします。

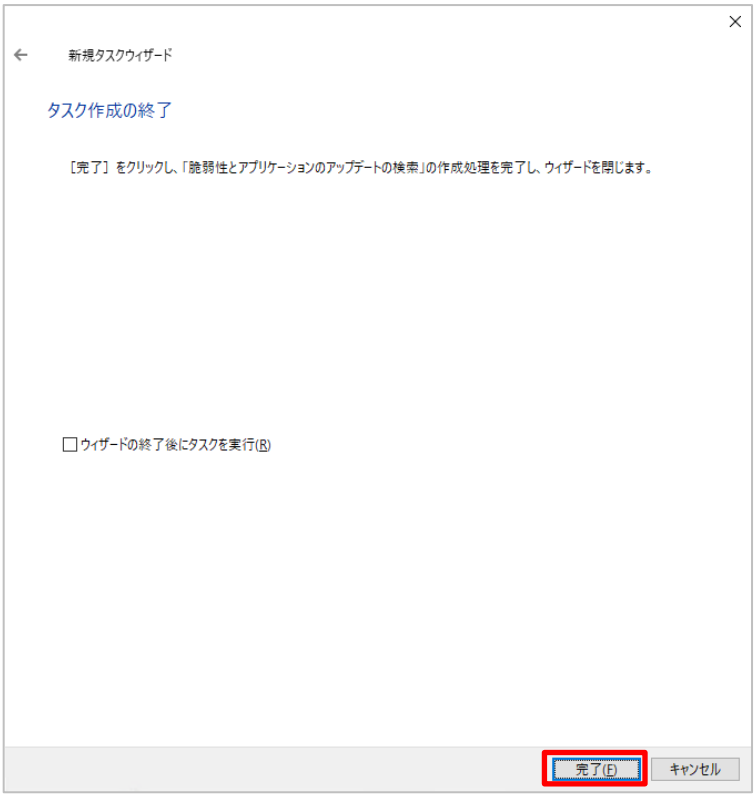
(8) 実行予定として以下を設定し、「次へ」をクリックします。

・実行予定：毎週
・曜日：火曜日
・開始時刻：12:00:00

(9) 「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/