Kaspersky Endpoint Security for Windows
脆弱性情報とソフトウェアアップデート情報確認ガイド

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 3
1.1. 本書について、前提条件 3
2. 脆弱性情報の確認 4
2.1. フィルター設定 4
2.2. CVE（Common Vulnerabilities and Exposures）番号の検索 6
2.3. 個別の脆弱性情報の確認（Microsoft 製品） 8
2.4. 個別の脆弱性情報の確認（サードパーティー製品） 11
2.5. 管理対象デバイス上での脆弱性情報の確認 14
3. ソフトトウェアアップデート情報の確認 18
3.1. フィルターの設定 18
3.2. 個別のソフトウェアアップデート情報の確認（Microsoft 製品） 19
3.3. 個別のソフトウェアアップデート情報の確認（サードパーティー製品） 23
3.4. デバイス単位でのソフトウェアの脆弱性・アップデート情報の確認 26
4. 脆弱性レポートの表示 28
5. ソフトウェアアップデートレポートの表示 30

1. はじめに

1.1. 本書について

本資料では、Kaspersky Endpoint Security for Windows (以降 KES) にて、管理対象デバイス関する**脆弱性情報**と**ソフトウェアアップデート情報**を確認する方法についてご説明します。

各種情報はレポートとして出力が可能であり、デバイス毎に確認する事も可能です。

- **ソフトウェアの脆弱性：**
  管理対象デバイスで検知された脆弱性情報に基づいた表示です。脆弱性情報は、Kaspersky の脆弱性データベースに基づいています。

- **ソフトウェアのアップデート：**
  管理対象デバイスにインストールされている Microsoft 製品、及び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に基づいています。

1.2. 前提条件

本機能の利用には、本機能を使用する権利のあるライセンスが必要です。
本資料は上記ライセンスが適用されていることを前提とした手順になります。ライセンスの適用方法については、「Kaspersky Endpoint Security for Business 脆弱性診断とパッチ配布設定ガイド」をご参照ください。

本機能を使用する権利のあるライセンス

- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Detection and Response Optimum Bundle
- Kaspersky Endpoint Detection and Response Expert

2.　脆弱性情報の確認

本章では、脆弱性情報の確認手順についてご説明します。

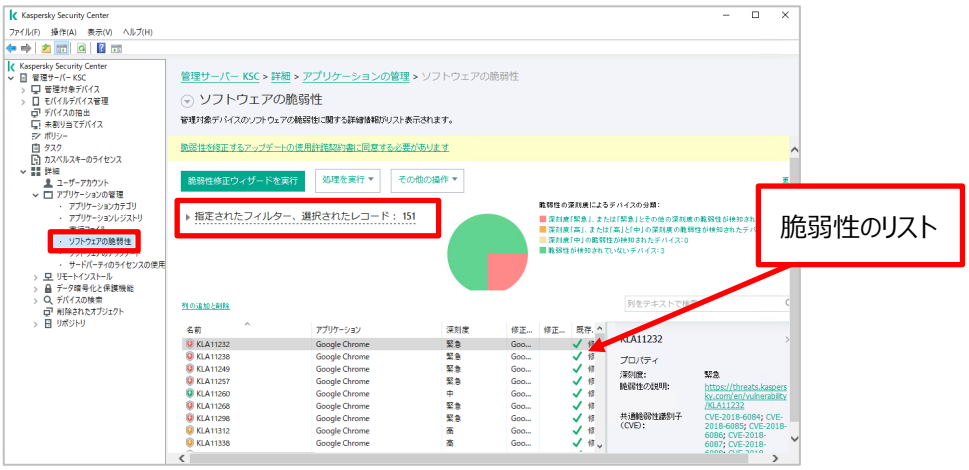
2.1.　フィルター設定

脆弱性情報の表示において、フィルターを設定する手順についてご説明します。

(1) KSC 管理コンソールにて、「詳細」-「アプリケーションの管理」-「ソフトウェアの脆弱性」を開きます。
画面右側に管理対象デバイス全体の脆弱性情報がリストで表示されます。

「指定されたフィルター、選択されたレコード」をクリックすると、画像②の様にフィルタリングの設定が確認できます。
既定では、Microsoft 製品、サードパーティー製品の両方を表示し、修正ファイルを入手可能なアップデートを表示します。フィルター設定項目は、画像②で示したもの以外にも多数存在します。必要応じて設定を実施してください。

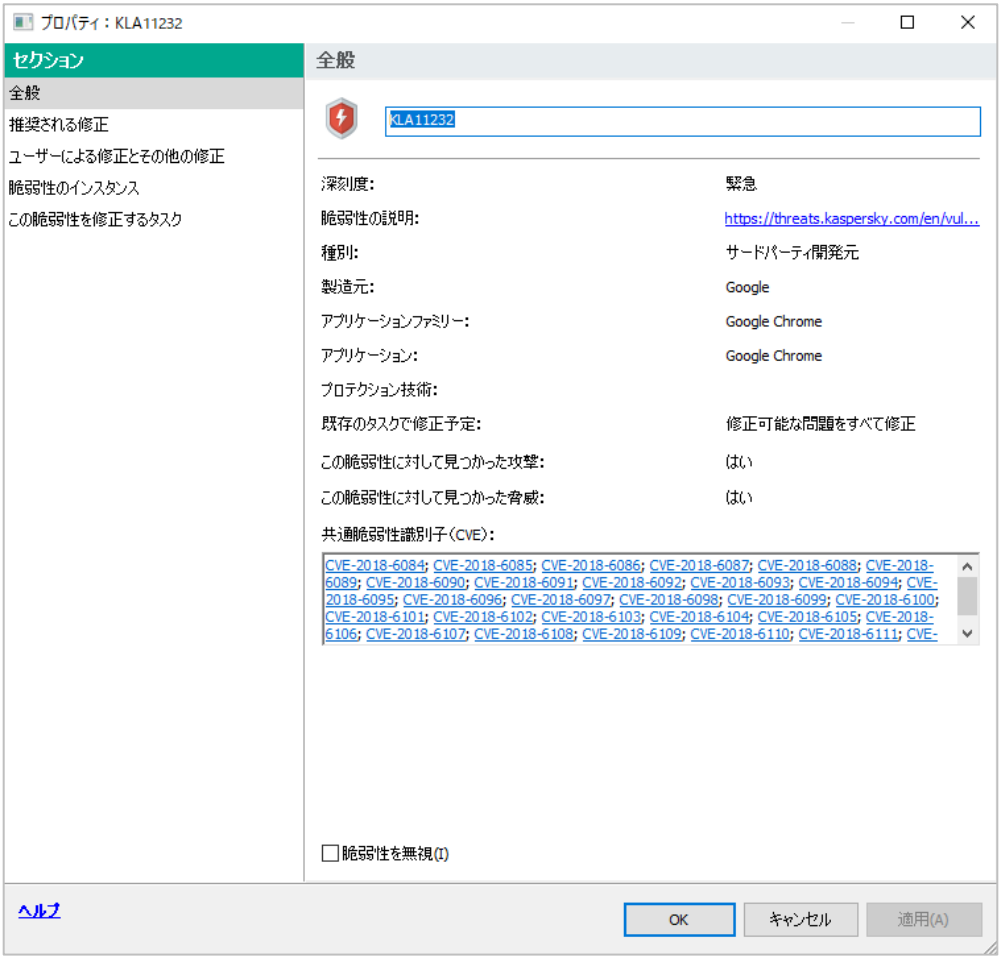
画像①



画像②

(2) フィルター設定にて、「修正が入手可能」を「いいえ」に設定し、「適用する」をクリックする事で、修正が入手できないソフトウェアの情報を確認する事もできます。
バージョンアップ等のみで対応可能なソフトがある場合は確認する事ができます。

(3) 脆弱性情報をダブルクリックしてプロパティを開くことで、詳細の確認も可能です。

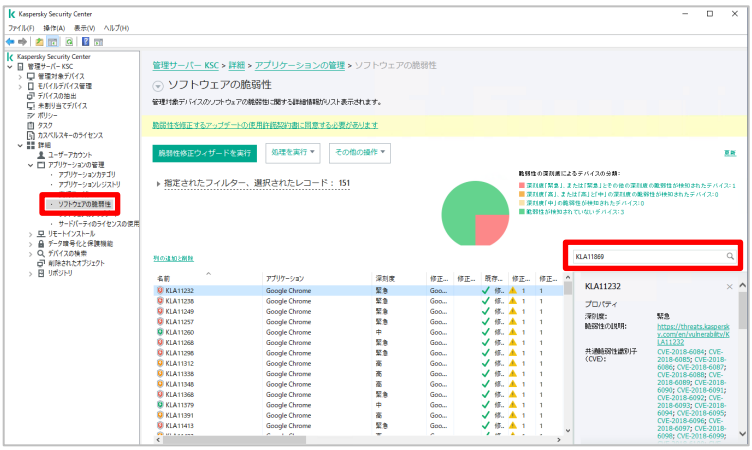


本節は以上です。

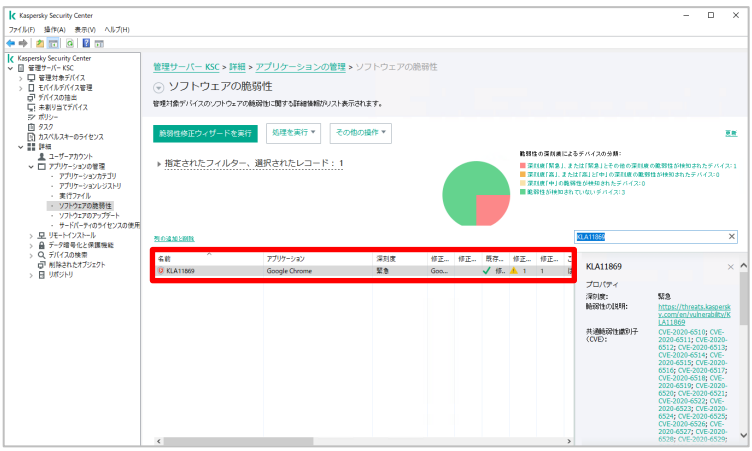
2.2.　CVE（Common Vulnerabilities and Exposures）番号の検索

「ソフトウェアの脆弱性」では、CVE 番号（共通脆弱性識別子）を元に、管理下のデバイスに該当する脆弱性があるかどうか検索することができます。

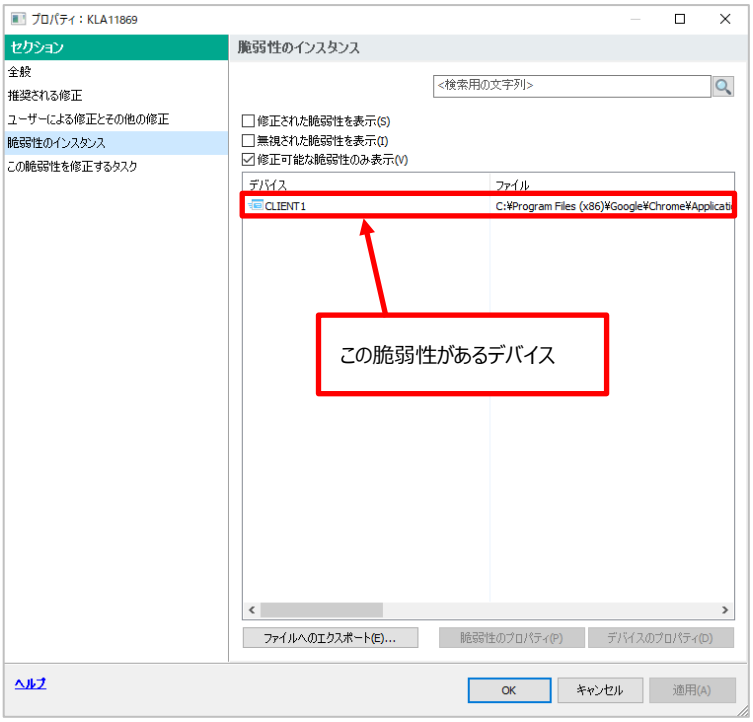
(1) KSC にて「詳細」-「アプリケーションの管理」-「ソフトウェアの脆弱性」を開きます。画面右の入力フィールドに、CVE 番号を入力し、検索を実行します。



(2) CVE 番号に該当する脆弱性を持つデバイスが存在する場合、脆弱性番号が表示されます。



(3) 詳細を確認する場合は、脆弱性番号をダブルクリックしてプロパティを開きます。
（確認項目は後述する「2.3 個別の脆弱性情報の確認」を参照）

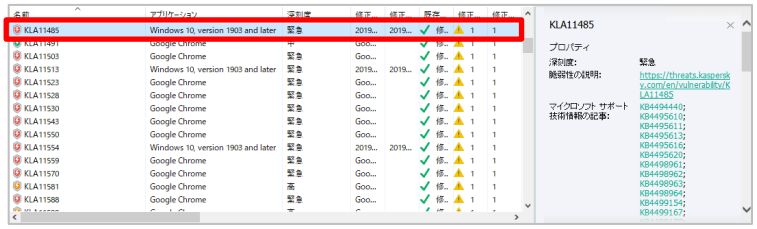


本節は以上です。

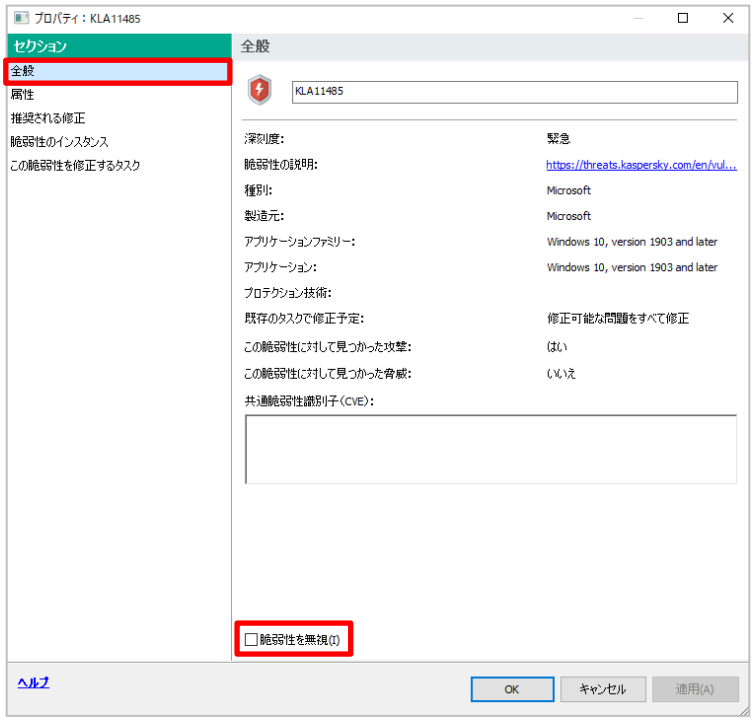
2.3. 個別の脆弱性情報の確認（Microsoft 製品）

個別の脆弱性情報（Microsoft 製品）を確認する手順についてご説明します。

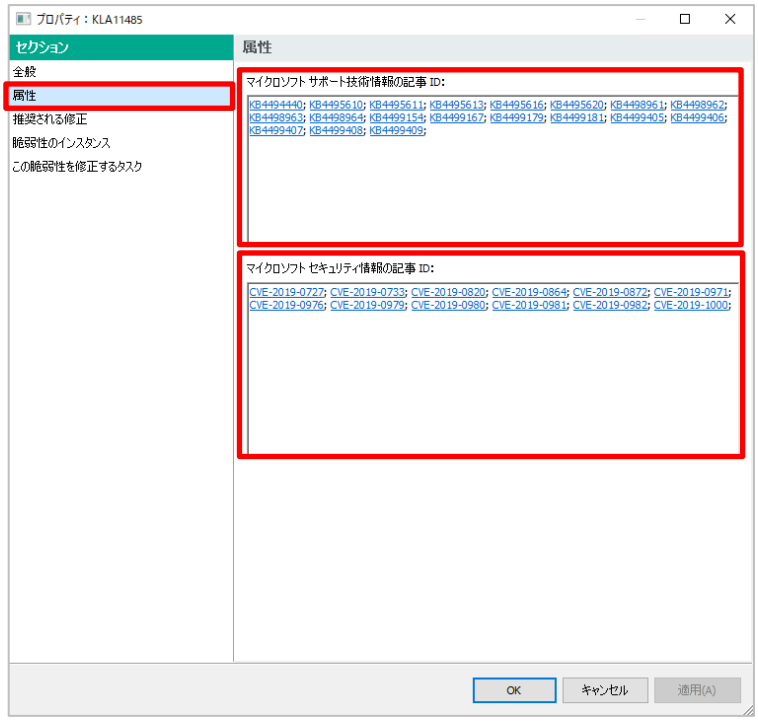
(1) 脆弱性情報の詳細を確認する事ができます。
脆弱性情報をダブルクリックすると詳細を表示することができます。



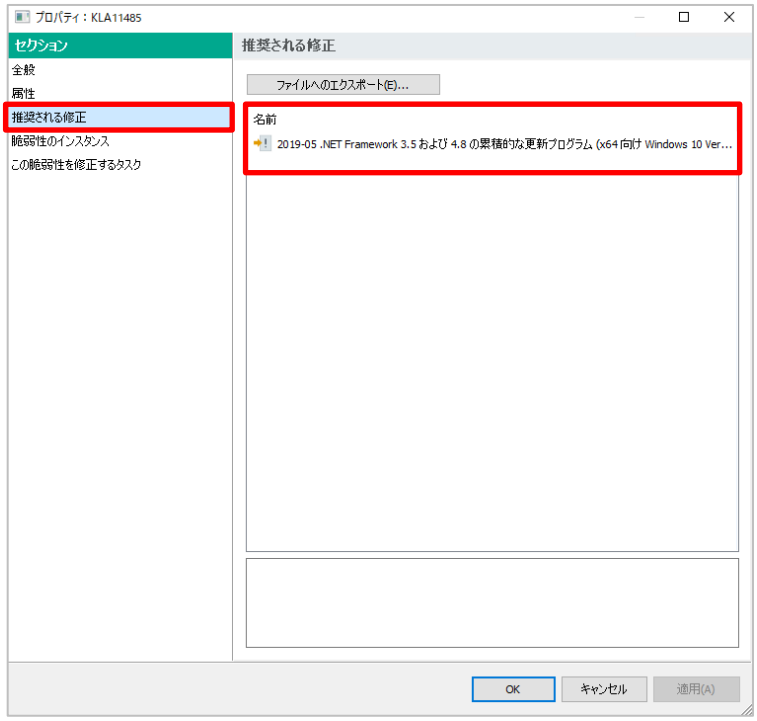
(2) 「全般」セクションを選択します。
脆弱性情報の緊急度や基本的な情報を確認する事ができます。CVE（Common Vulnerabilities and Exposures（共通脆弱性識別子））に基づいた情報を確認できます。
また、「脆弱性を無視」にチェックを入れる事でこの脆弱性をレポートに表示させない設定も可能です。



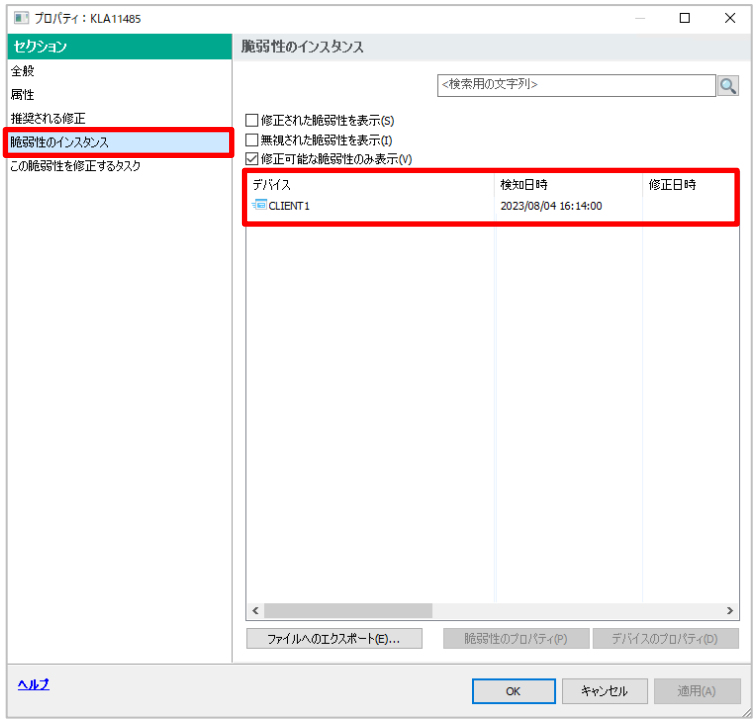
(3) 「属性」セクションを選択します。
マイクロソフト製品の場合、技術情報に基づいた情報とセキュリティ情報に基づいた情報を確認することができます。



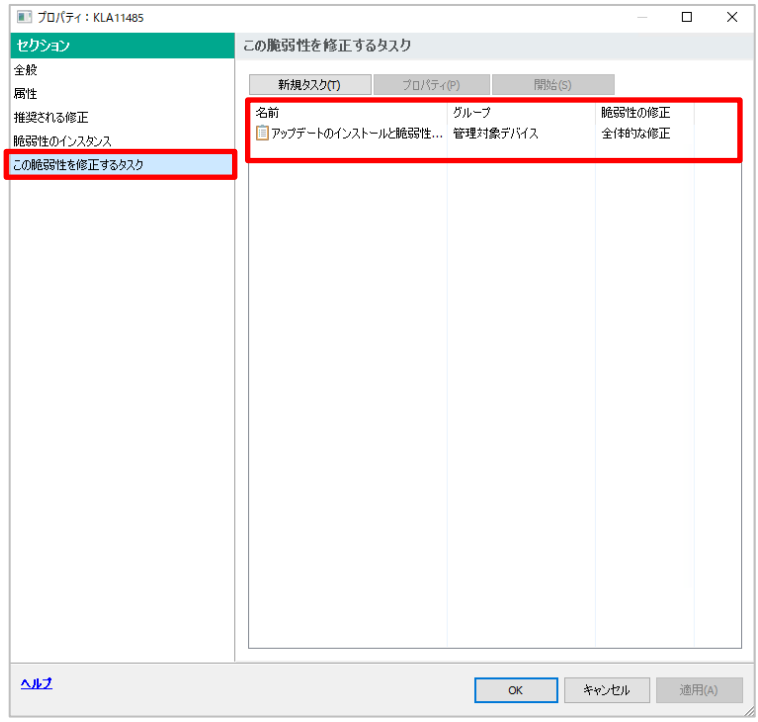
(4) 「推奨される修正」セクションを選択します。
脆弱性の修正に必要な更新プログラムが表示されます。



(5) 「脆弱性のインスタンス」セクションを選択します。
この脆弱性が検知されたデバイスの情報が表示されます。



(6) 「この脆弱性を修正するタスク」セクションを選択します。
この脆弱性を修正するタスクが存在する場合はそのタスクが表示されます。



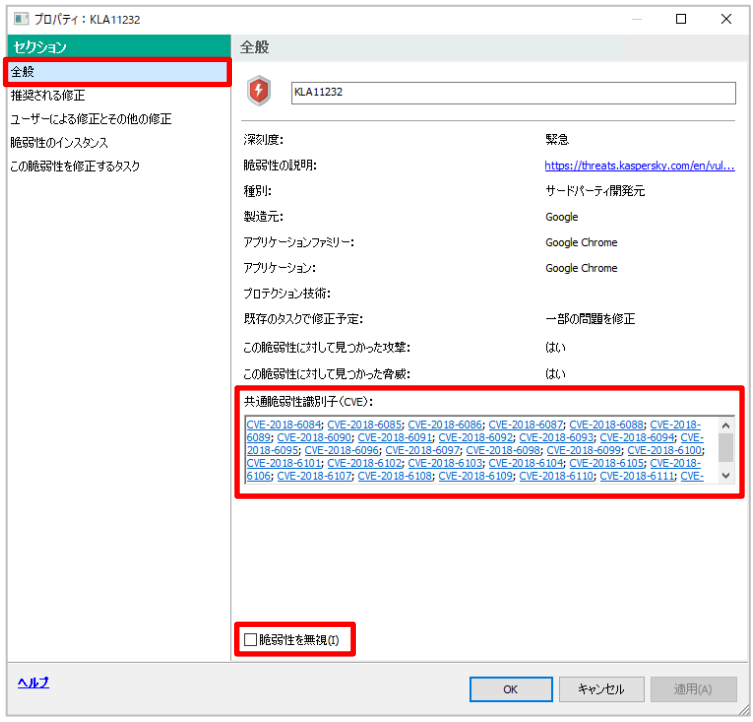
本節は以上です。

2.4.　個別の脆弱性情報の確認（サードパーティー製品）

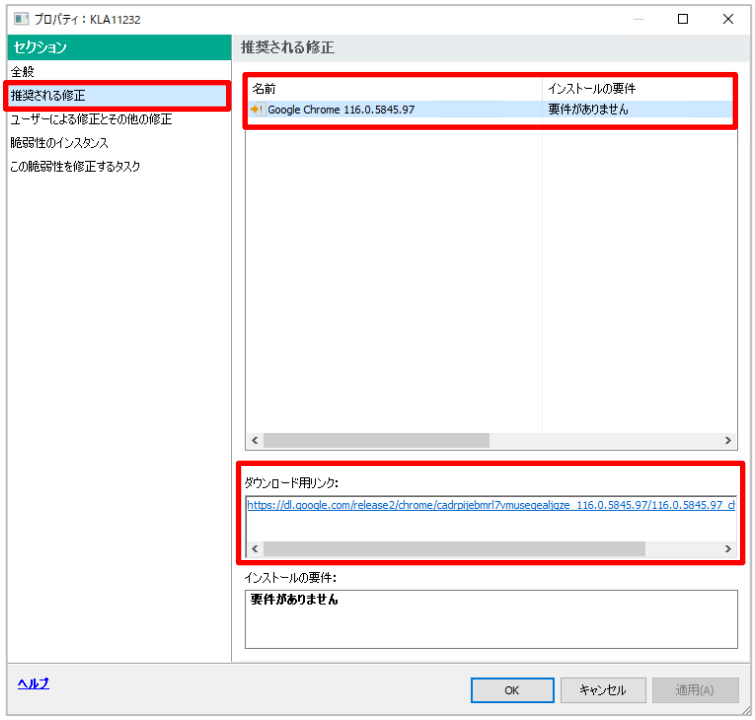
個別の脆弱性情報（サードパーティー製品）を確認する手順についてご説明します。

(1) 脆弱性情報の詳細を個別に確認する事も可能です。「KLA11232」をダブルクリックして表示させた例です。サードパーティー製品の情報です。

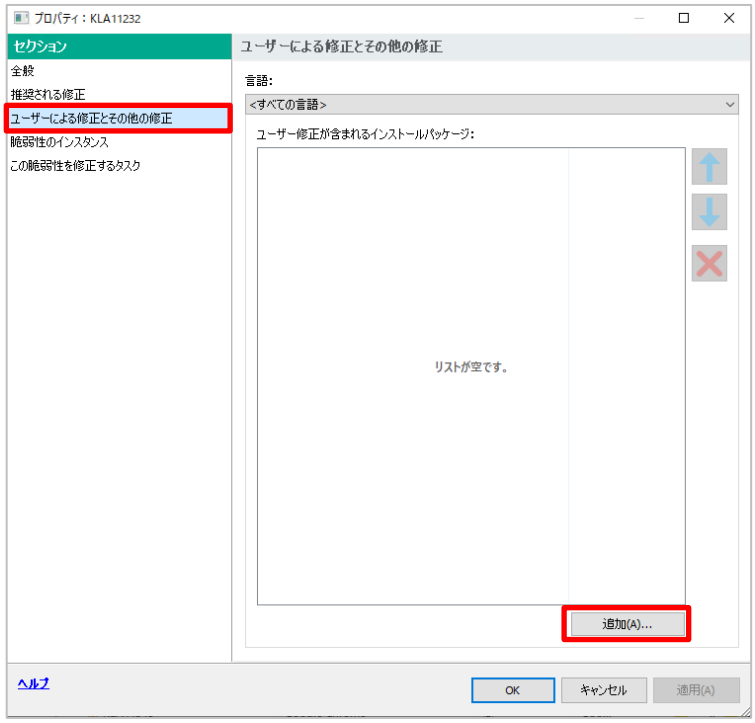
(2) 「全般」セクションを選択します。
脆弱性情報の緊急度や基本的な情報を確認する事ができます。
CVE（Common Vulnerabilities and Exposures（共通脆弱性識別子））に基づいた情報を確認できます。
また、「脆弱性を無視」にチェックを入れる事でこの脆弱性をレポートに表示させない設定も可能です。



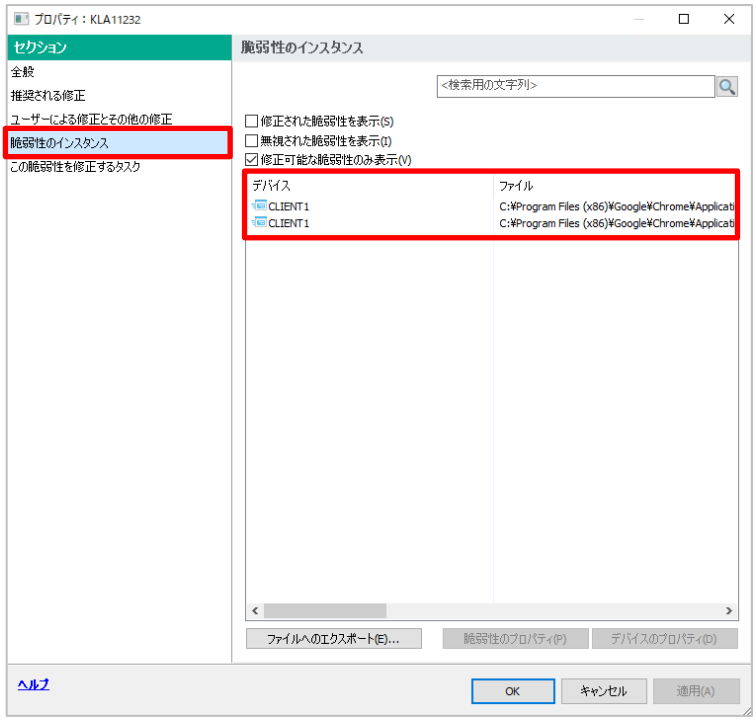
(3) 「推奨される修正」セクションを選択します。
推奨される修正プログラムとダウンロード用 URL が表示されます。



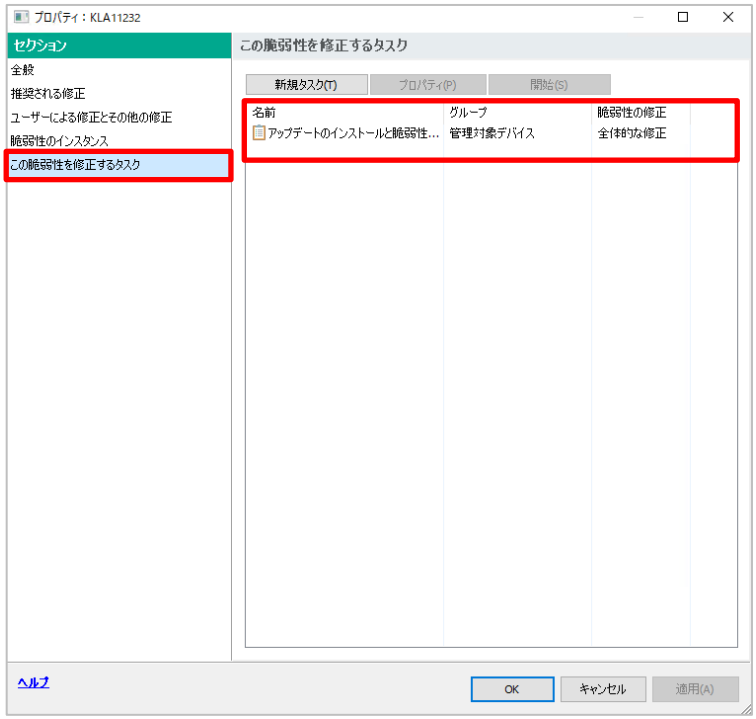
(4) 「ユーザーによる修正とその他の修正」セクションを選択します。
「追加」をクリックすることで、個別にインストールパッケージを追加することができます。



(5) 「脆弱性のインスタンス」セクションを選択します。
脆弱性が検知されたデバイスの情報とインストールパスが表示されます。



(6) 「この脆弱性を修正するタスク」セクションを選択します。
この脆弱性を修正するタスクが存在する場合はそのタスクが表示されます。
また、ここから修正タスクを作成することもできます。



本節は以上です。

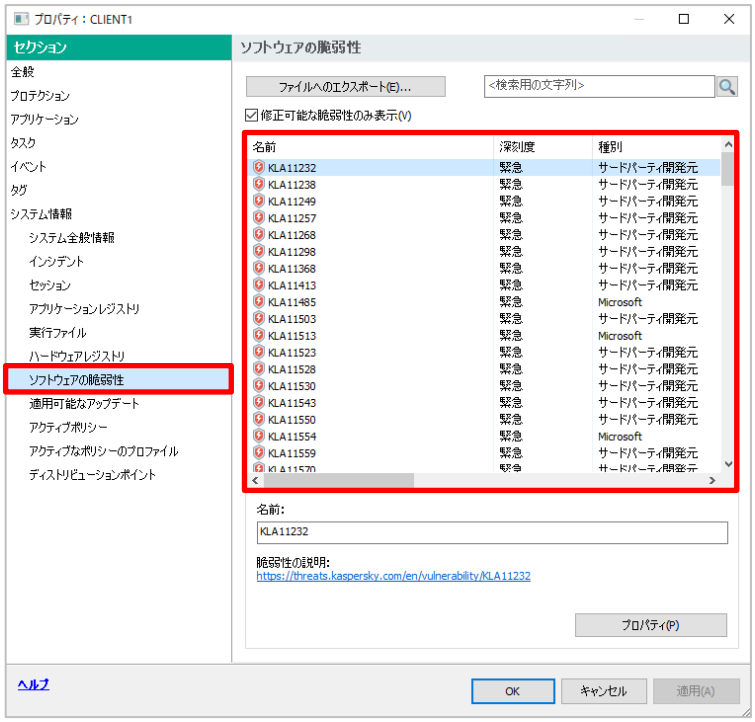
2.5.　管理対象デバイス上での脆弱性情報の確認

管理対象デバイス上での脆弱性の確認する手順をご説明します。

(1) 管理対象デバイスをクリックすると管理下にあるデバイス情報が表示されます。
既定では、脆弱性をトリガーとした緊急度のステータスは確認できない設定となっております。

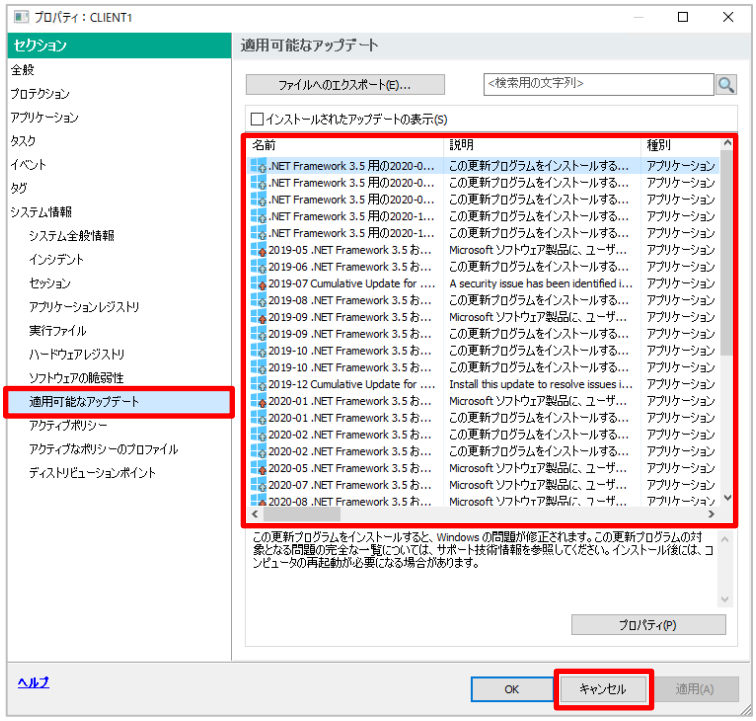
(2) 個別に情報を確認する場合、管理対象デバイスに表示されているデバイスをダブルクリックします。

(3) デバイスのプロパティが表示されます。
「ソフトウェアの脆弱性」セクションでは、このデバイスに関する脆弱性情報を確認できます。



(4) 「適用可能なアップデート」セクションでは、適用可能なパッチ情報を確認できます。

確認後は「キャンセル」をクリックし画面を閉じます。



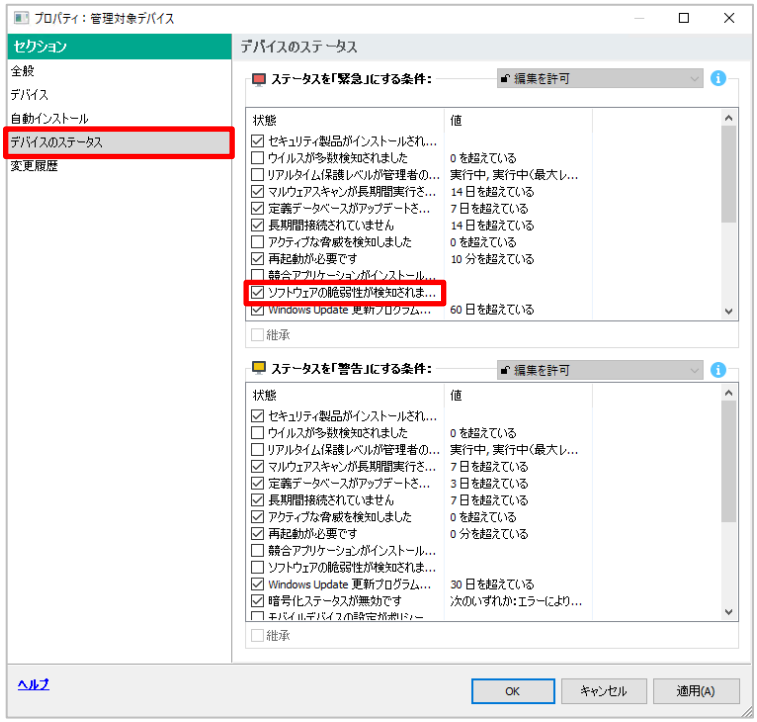
本節は以上です。

脆弱性を持つデバイスのステータスを変更させたい場合は、以降の手順を実施します。

(5) KSC にて「管理対象デバイス」を右クリックし、「プロパティ」を選択します。

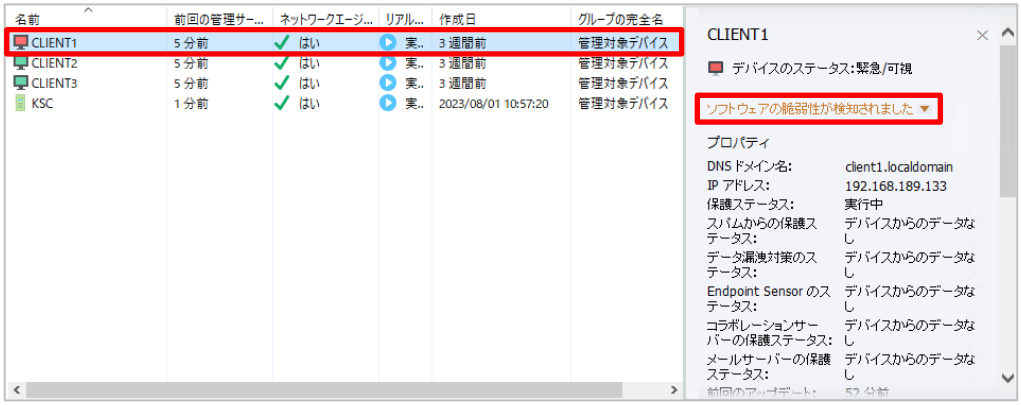
(6) 「デバイスの状態」セクションを選択します。既定では、「緊急」、「警告」共に「ソフトウェアの脆弱性が検知されました。」にチェックが入っていません。

上段の「緊急」項目内にある「ソフトウェアの脆弱性が検知されました」にチェックを入れた後、同項目をダブルクリックします。



(7) 脆弱性の重要度を指定する事ができます。
既定では、「緊急」のみにチェックが入っています。設定後、「OK」をクリックします。
(6)の画面に戻ったら、「OK」をクリックし設定画面を閉じます。

(8) 脆弱性が検知されたデバイスが**「緊急」**ステータスとして表示されます。
画面右側を確認すると「ソフトウェアの脆弱性が検知されました」との表示が確認できます。



本章は以上です。

3.　ソフトウェアアップデート情報の確認

本章では、ソフトウェアアップデート情報の確認手順についてご説明します。

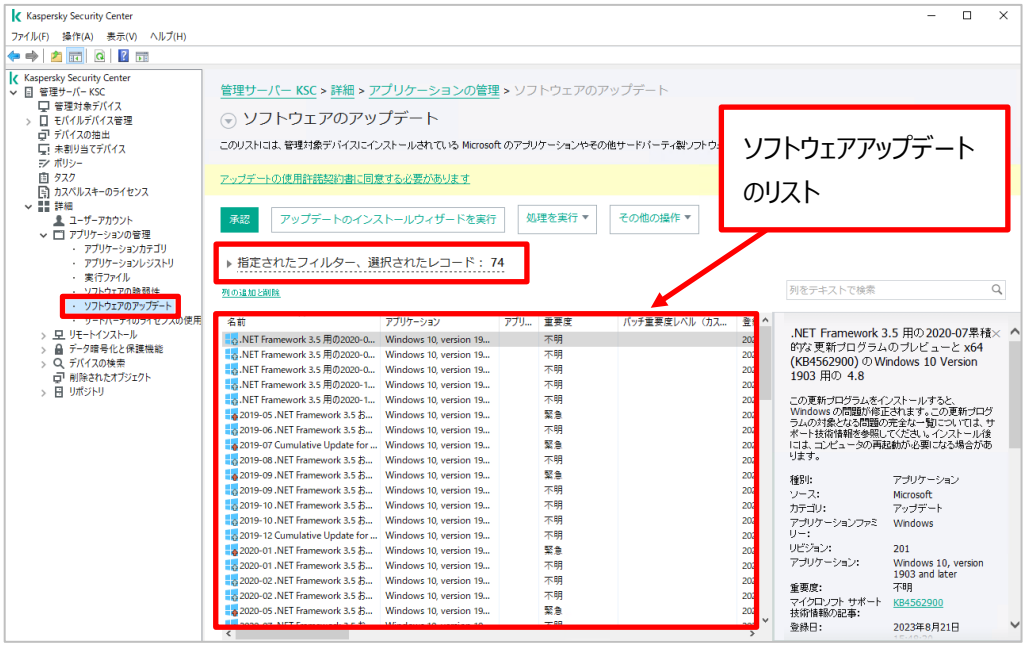
3.1.　フィルターの設定

ソフトウェアアップデート情報の表示方法に関してご説明します。

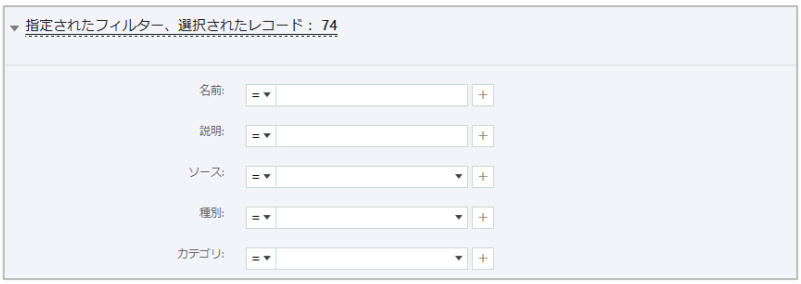
(1) KSC にて、「詳細」-「アプリケーションの管理」-「ソフトウェアのアップデート」を開きます。
画面右側に管理対象デバイス全体のソフトウェアのアップデート情報がリスト表示されます。

「指定されたフィルター」をクリックすると、画像②の様にフィルタリングの設定が確認できます。
既定では、Microsoft 製品、サードパーティー製品、Kaspersky 製品情報を表示し、修正ファイルが入手可能なアップデートを表示します。フィルター設定項目は、画像②で示したもの以外にも多数存在します。必要応じて設定を実施してください。

画像①



画像②

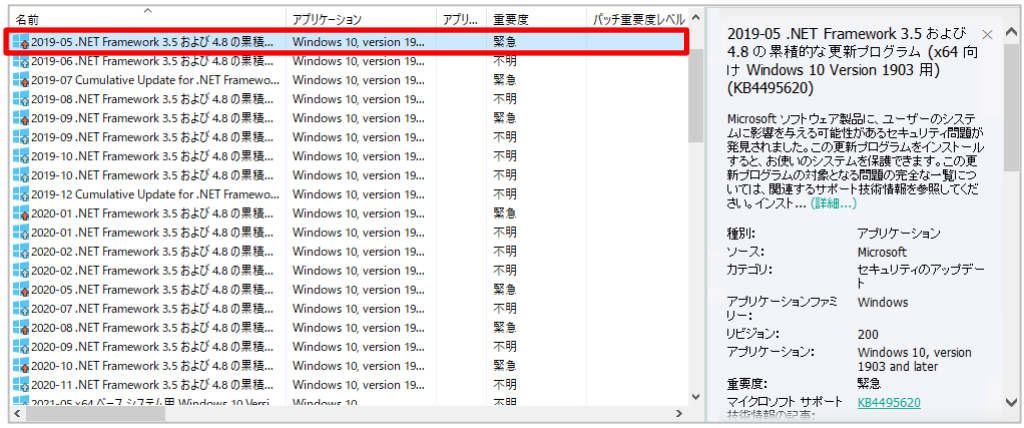


本節は以上です。

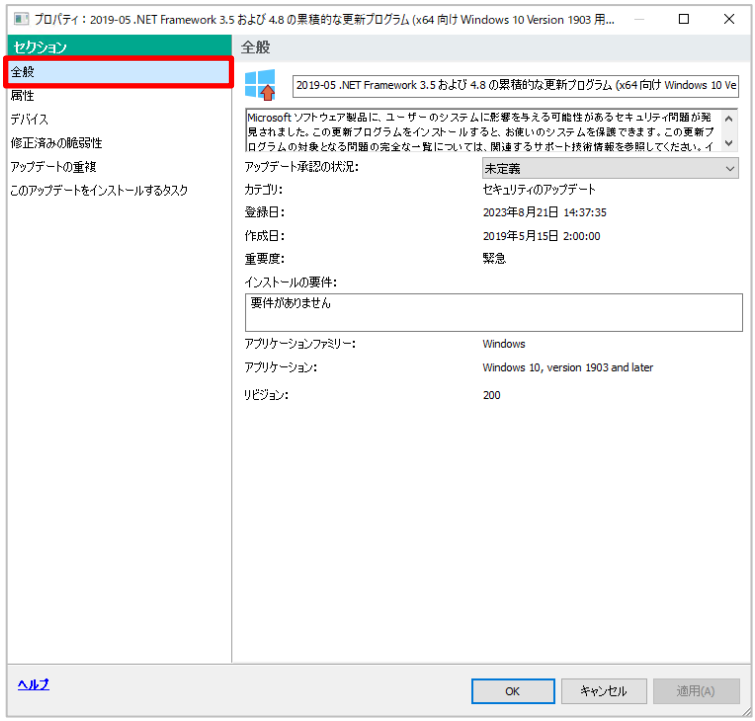
3.2.　個別のソフトウェアアップデート情報の確認（Microsoft 製品）

個別のソフトウェアアップデート情報（Microsoft 製品）の確認する手順についてご説明します。

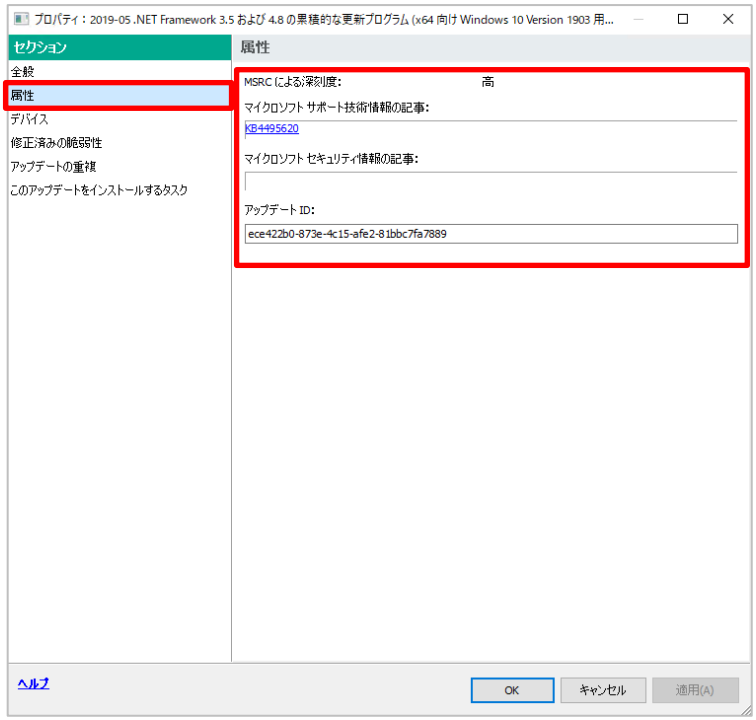
(1) ソフトウェアアップデート情報の詳細を確認することができます。
アップデートの項目をダブルクリック（もしくは右クリックしてプロパティ）を実施すると詳細を確認することができます。



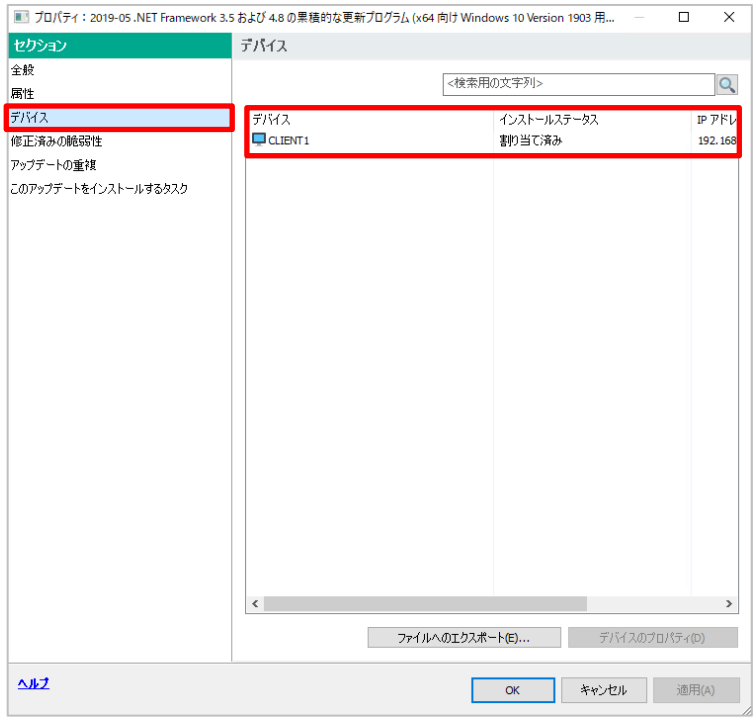
(2) 「全般」セクションを選択します。
プログラムの基本的な情報が表示されます。



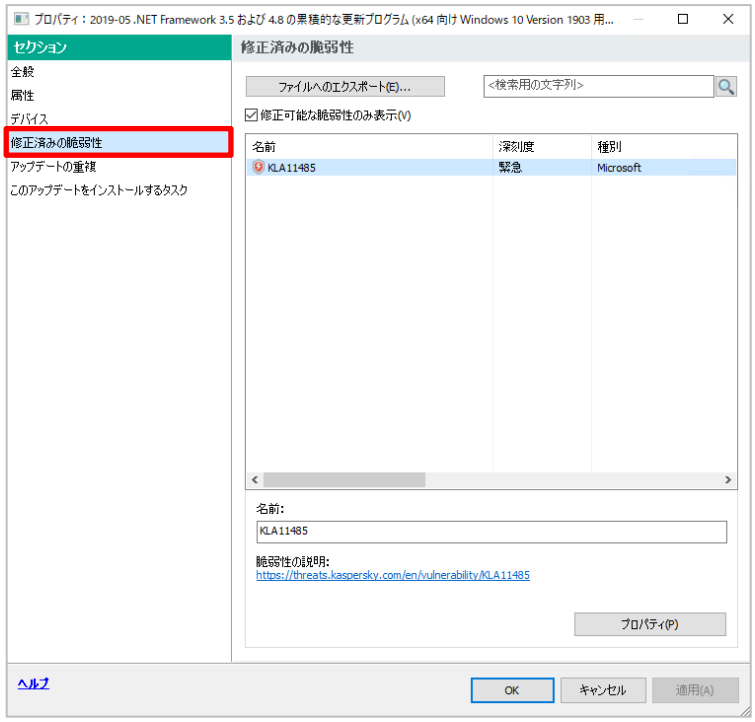
(3) 「属性」セクションを選択します。
マイクロソフト製品の場合、技術情報に基づいた情報とセキュリティ情報に基づいた情報が表示されます。
（本プログラムは修正プログラムなのでセキュリティ情報は表示されません。）



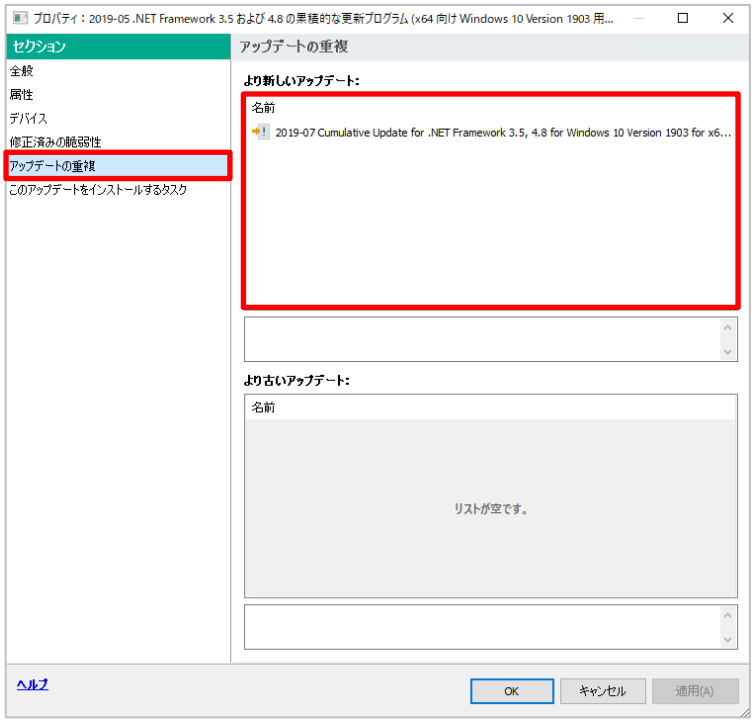
(4) 「デバイス」セクションを選択します。
アップデートの対象となるデバイスの一覧が表示されます。



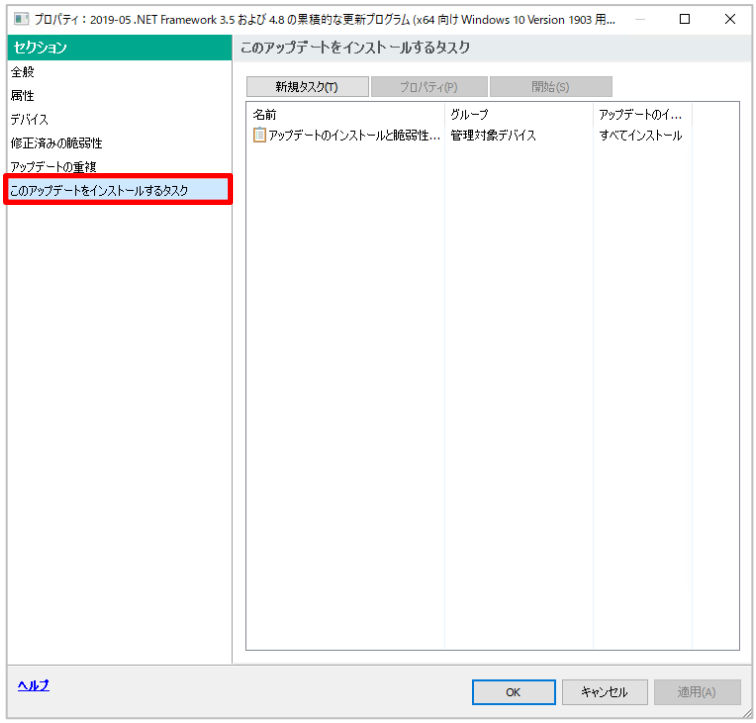
(5)「修正済みの脆弱性」セクションを選択します。
プログラムのインストールにより修正される脆弱性情報が表示されます。（種類によっては脆弱性情報が表示されないものもあります。）



(6)「アップデートの重複」セクションを選択します。
プロパティを開いたアップデートより新しいアップデート、古いアップデートが存在する場合、一覧に表示されます。



(7)「このアップデートを修正するタスク」セクションを選択します。
脆弱性を修正するタスクがある場合はそのタスクが表示されます。また、ここからタスクを作成することもできます。

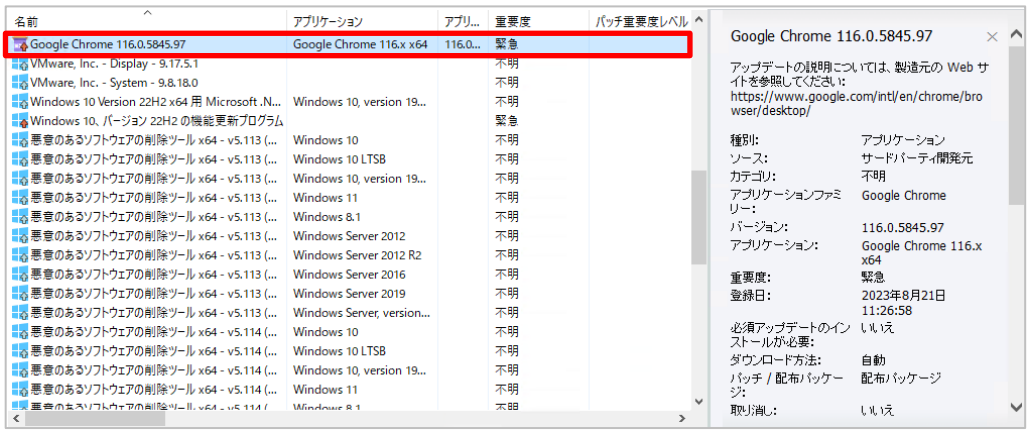


本節は以上です。

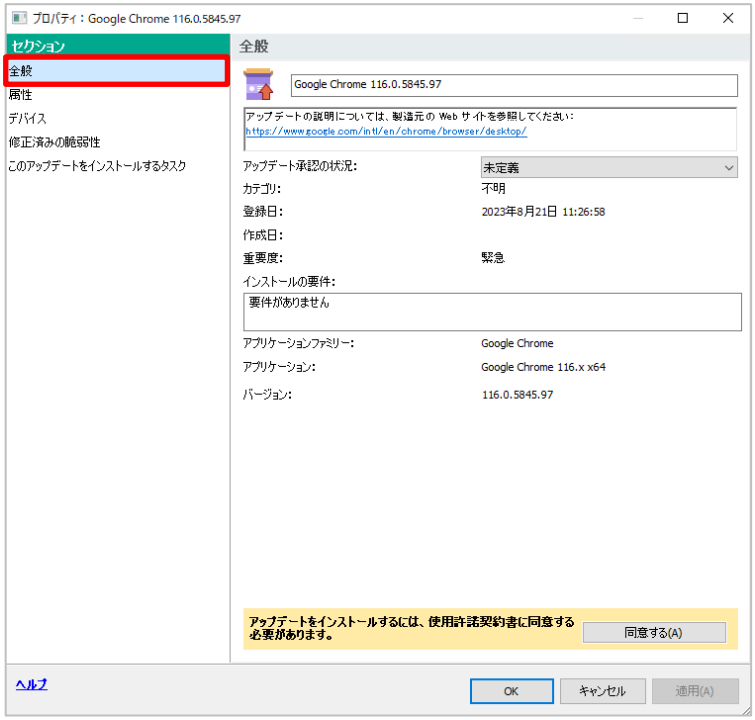
3.3. 個別のソフトウェアアップデート情報の確認（サードパーティー製品）

個別のソフトウェアアップデート情報（サードパーティー製品）の確認する手順についてご説明します。

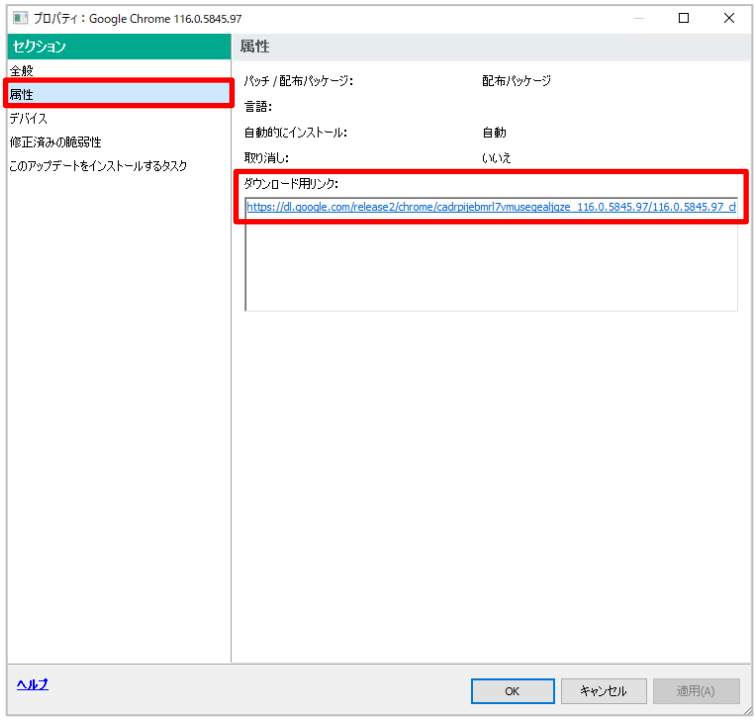
(1) ソフトウェアアップデートのリストより、サードパーティー製アプリケーションをダブルクリックして情報を表示させた例です。



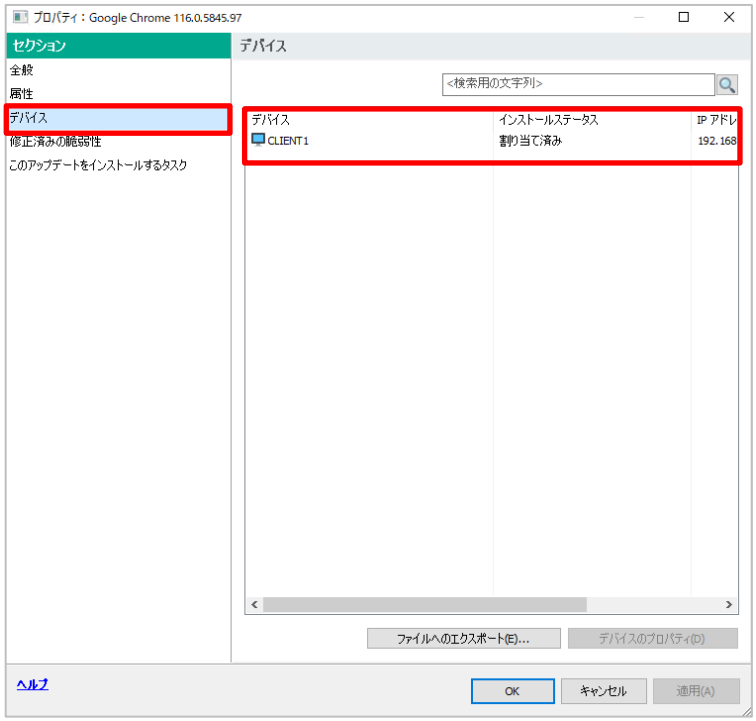
(2) 「全般」セクションを選択します。
プログラムの基本的な情報が表示されます。



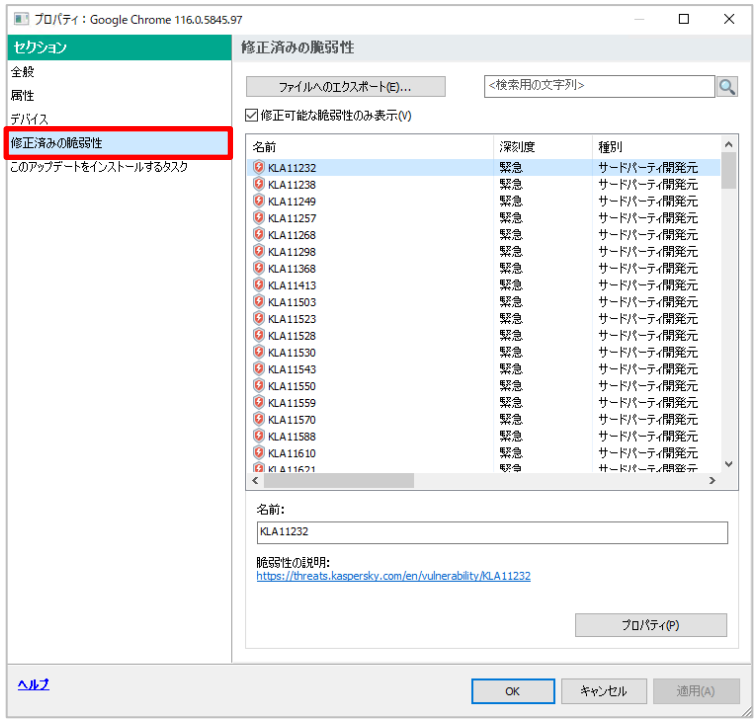
(3) 「属性」セクションを選択します。
パッチやアップデートのダウンロード用 URL を確認することができます。



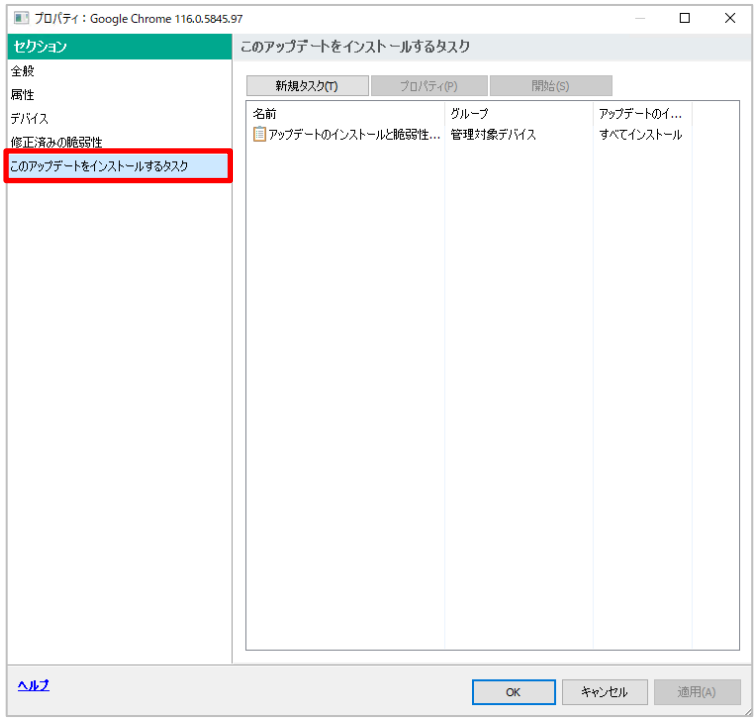
(4) 「デバイス」セクションを選択します。
アップデートの対象となるデバイスの一覧が表示されます。



(5)「修正済みの脆弱性」セクションを選択します。
プログラムのインストールにより修正される脆弱性情報が表示されます。



(6)「このアップデートを修正するタスク」セクションを選択します。
脆弱性を修正するタスクがある場合はそのタスクが表示されます。
また、ここからタスクを作成することもできます。



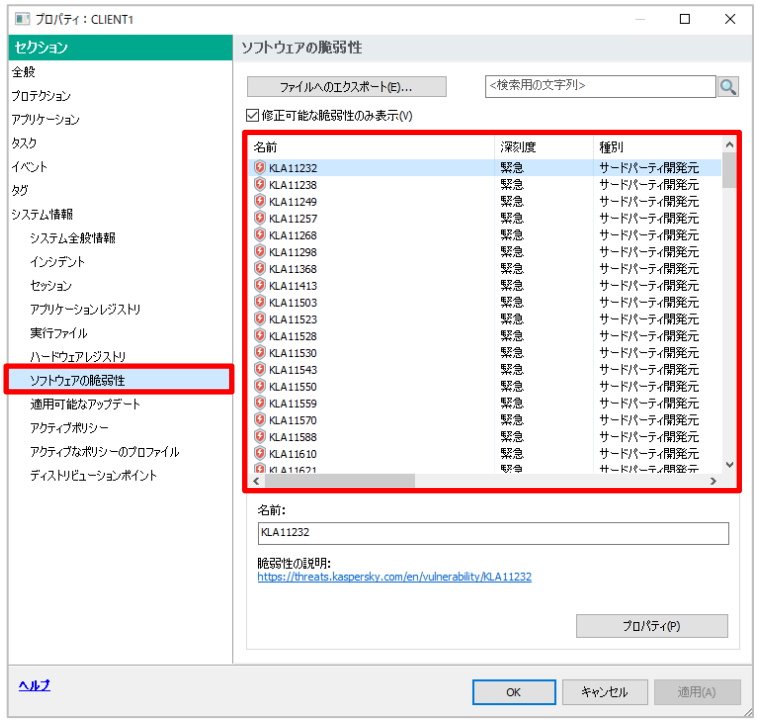
本節は以上です。

3.4. デバイス単位でのソフトウェアの脆弱性・アップデート情報の確認

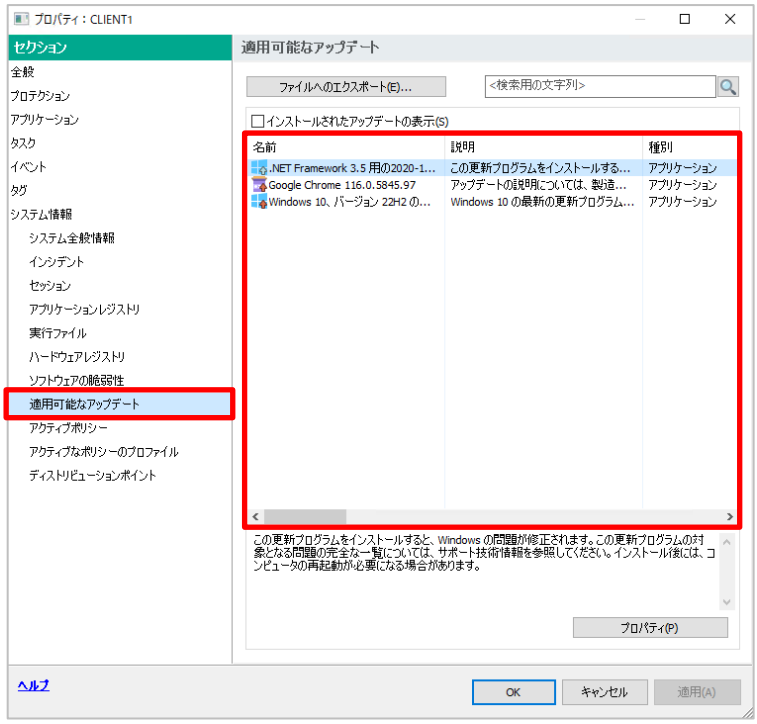
管理対象デバイス毎に、ソフトウェアの脆弱性やアップデート情報を確認する手順についてご説明します。

(1)「管理対象デバイス」をクリックすると、管理下のコンピューター情報が表示されます。
デバイス情報を確認する場合、管理対象デバイスに表示されているデバイス名をダブルクリックします。

(2)「ソフトウェアの脆弱性」セクションを選択します。
このデバイスが持つ脆弱性の一覧を確認することができます。



(3) 「適用可能なアップデート」セクションを選択します。
このデバイスに適用可能なパッチやアップデート情報を確認することができます。



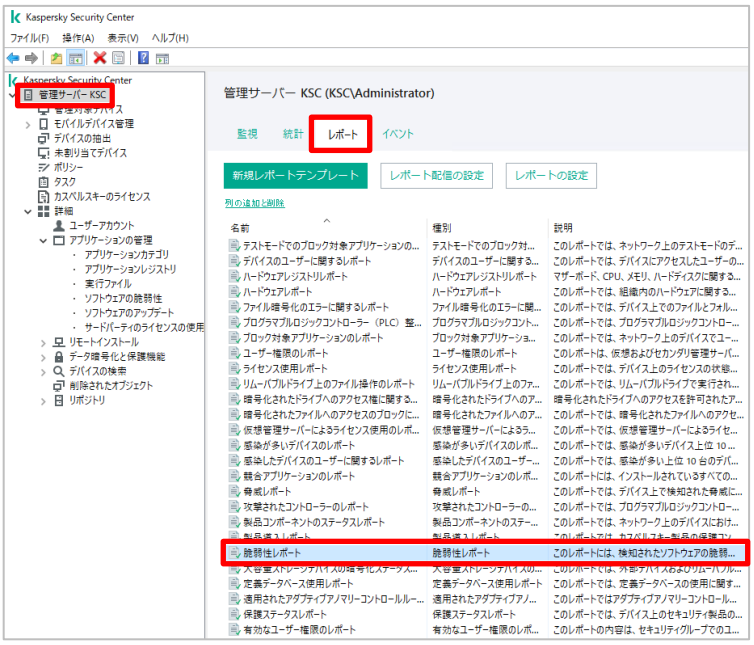
本章は以上です。

4.　脆弱性レポートの表示

本手順は脆弱性レポートの表示方法についての手順です。

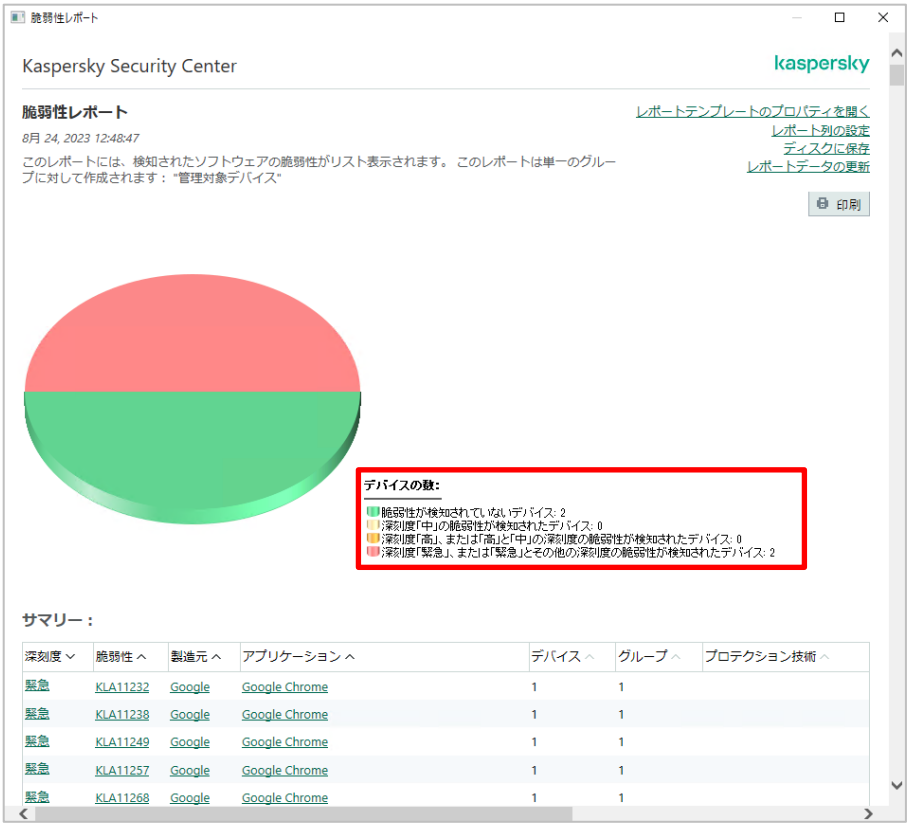
(1) KSC にて「管理サーバー」を選択し、右画面にて「レポート」タブを選択します。

「脆弱性レポート」をダブルクリックするとレポートが自動的に生成されます。



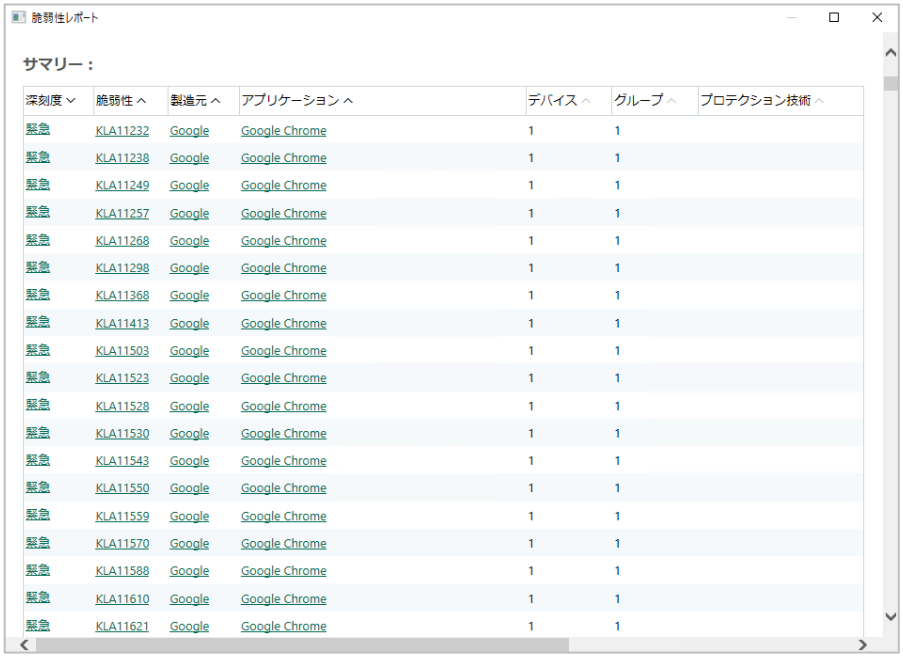
(2) レポートが作成され、画面に表示されます。

画面右下に脆弱性の度合いと対象デバイス数が表示されます。ここでは、「深刻度「緊急」の脆弱性が検知されたデバイス」が 2 台存在する事が確認できます。



(3) レポートは、全体情報だけではなく、アプリケーションや脆弱性の個別情報の確認にも使用可能です。

「重要度」、「脆弱性」、「製造元」、「アプリケーション」をクリックすることで、その選択した項目に沿った別のレポートを生成することも可能です。



深刻度	脆弱性	製造元	アプリケーション	デバイス	グループ	プロテクション技術
緊急	KLA11232	Google	Google Chrome	1	1	
緊急	KLA11238	Google	Google Chrome	1	1	
緊急	KLA11249	Google	Google Chrome	1	1	
緊急	KLA11257	Google	Google Chrome	1	1	
緊急	KLA11268	Google	Google Chrome	1	1	
緊急	KLA11298	Google	Google Chrome	1	1	
緊急	KLA11368	Google	Google Chrome	1	1	
緊急	KLA11413	Google	Google Chrome	1	1	
緊急	KLA11503	Google	Google Chrome	1	1	
緊急	KLA11523	Google	Google Chrome	1	1	
緊急	KLA11528	Google	Google Chrome	1	1	
緊急	KLA11530	Google	Google Chrome	1	1	
緊急	KLA11543	Google	Google Chrome	1	1	
緊急	KLA11550	Google	Google Chrome	1	1	
緊急	KLA11559	Google	Google Chrome	1	1	
緊急	KLA11570	Google	Google Chrome	1	1	
緊急	KLA11588	Google	Google Chrome	1	1	
緊急	KLA11610	Google	Google Chrome	1	1	
緊急	KLA11621	Google	Google Chrome	1	1	

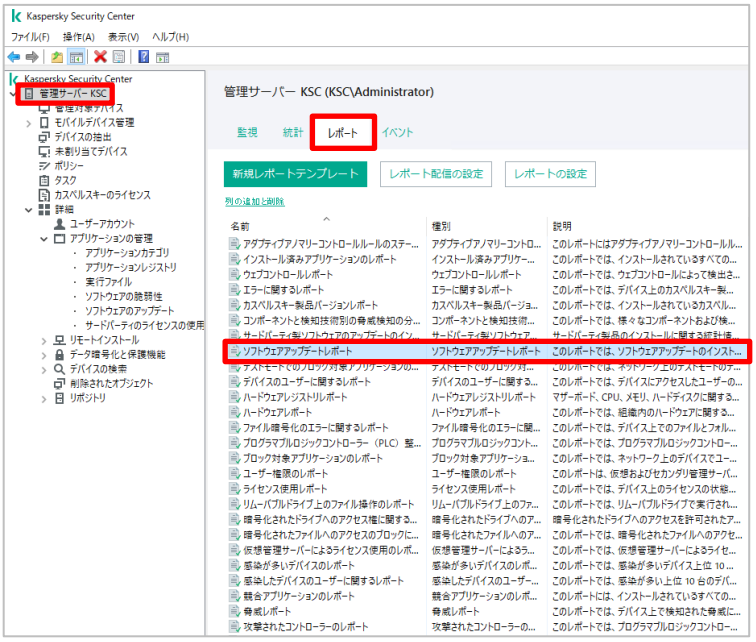
本章は以上です。

5. ソフトウェアアップデートレポートの表示

ソフトウェアアップデートレポートを表示する手順についてご説明します。

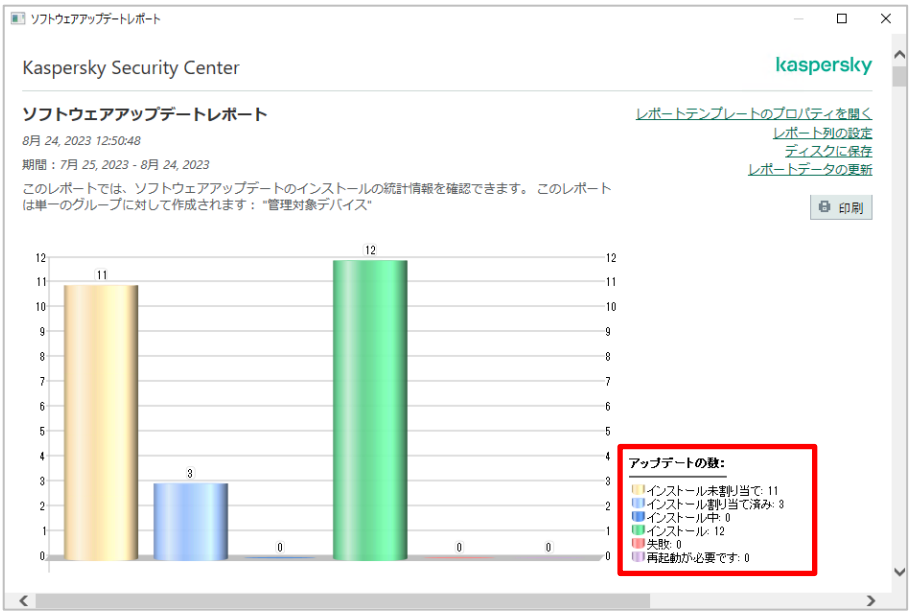
(1) KSC にて「管理サーバー」を選択し、右画面にて「レポート」タブを選択します。

「ソフトウェアアップデートレポート」をダブルクリックするとレポートが自動的に生成されます。



(2) レポートが作成され、画面に表示されます。

「アップデートの数」の項目は、アップデートのステータスを項目別に示しています。ここでは、「インストール未割り当て」が 11 個、割り当て済みが 3 個、インストール済みが 12 個存在します。



(3) レポートは、脆弱性レポートと同様、アプリケーション項目や緊急度の項目が存在します。
「修正が必要な脆弱性の重要度」、「ステータス」、「製造元」などをクリックすることで、その選択した項目に沿った別のレポートを生成することも可能です。

修正が必要な脆弱性の重要度	仮想管理サーバー	ステータス	ソース	製造元	アプリケーションファミリー	インストールされているアプリケーションのメジャーバージョン	インストールされているアプリケーションのバージョン	パッチの名前	時間	登録	詳細 URL
緊急		インストール未割り当て	Windows Update 更新プログラム	該当なし	該当なし	該当なし	該当なし	Windows 10、バージョン 22H2 の機能更新プログラム	8月 22, 2023 19:02:23	8月 9, 2023 16:12:14	該当なし
緊急		割り当て済み	Windows Update 更新プログラム	該当なし	該当なし	該当なし	該当なし	2023-08 Microsoft server operating system version 21H2 x64 ベースシステム用の累積更新プログラム (KB5029250)	8月 21, 2023 16:45:06	8月 9, 2023 14:27:51	該当なし
緊急		割り当て済み	サードパーティの更新プログラム	Google	Google Chrome	Google Chrome 116.x x64	116.0.5845.97	Google Chrome 116.0.5845.97	8月 21, 2023 16:54:25	8月 21, 2023 11:26:58	https://www.google.com/intl/en/chrome/browser/c
緊急		インストール	Windows Update 更新プログラム	該当なし	該当なし	該当なし	該当なし	2023-08 x64 ベース システム用 Windows 10 Version 22H2 の累積更新プログラム (KB5029244)	8月 21, 2023 16:50:37	8月 9, 2023 16:12:39	該当なし

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/