Kaspersky Vulnerability and Patch Management

～ 脆弱性対策とWindow10 ライフサイクル管理、
ITシステム運用支援ソリューション

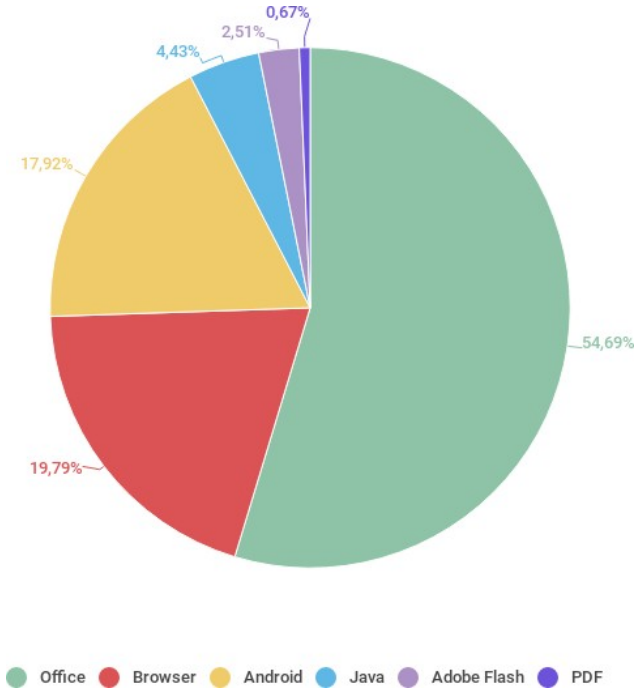
2020年4月
カスペルスキー　セールスエンジニアリング部

kaspersky

2018年総見 脆弱性とエクスプロイト

2018年のMicrosoft Office に対するエクスプロイト攻撃を受けたユーザー数は、2017年に比較すると4倍以上となり、特徴的な意味を持つ結果となった

8月には、Windowsのドライバーファイルであるwin32k.sysの脆弱性を利用した、新しい種類のサイバーアタックを発見した。
これはとても危険な脆弱性で、侵害されたPCをコントロールすることが可能になる。10月には、win32k.sysに、権限昇格を得て、永続的にシステムに存在可能にすることが出来る新たな脆弱性を発見した。

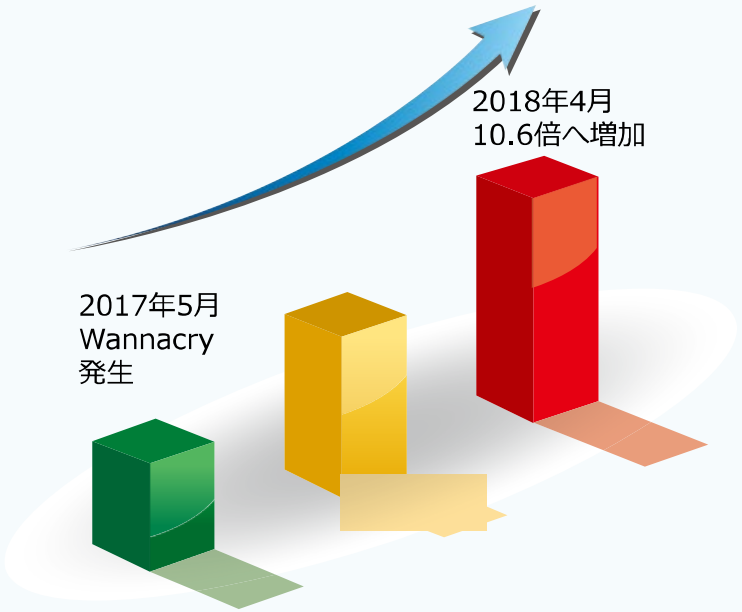


2018年総見 脆弱性とエクスプロイト

EternalBlue と呼ばれるネットワークエクスプロイト攻撃は
10倍となった。

有名になった脆弱性攻撃が下火になることはなく、
攻撃に適した脆弱性は狙われ続け、むしろ増加する。

Eternalblueによる攻撃数の増加



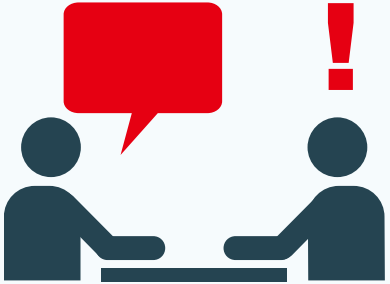
kaspersky

Windows10を取り巻く状況

Windows７の標準サポートが終了し、Windows10への移行が必須となった。

Win10には、年に2回新バージョンがリリースされる半期チャネル（SAC） と
2～3年ごとに新バージョンが登場する長期サービスチャネル（LTSC）の2つがあるが、
Microsoftは企業のクライアントOSとして、Windows10のSACで提供される
Windows 10 ProまたはEnterpriseの利用を推奨している。
例えば、Office 365 Pro Plusは、LTSCをサポートしない方針となった。

LTSCは、 POSシステム、ATMなど**特定用途での使用を想定している。**



Windows10を取り巻く状況

SAC Win10ではモダンライフサイクルポリシーが採用され、サポートライフサイクルが短くなっている。

Windows 10 の バージョン履歴	提供日	Home、Pro、Pro Education、 および Pro for Workstations エディションのサービスの終了	Enterprise および Education のサービスの終了
Windows 10 Version1909	2019 年 11 月 12 日	2021 年 5 月 11 日	2022 年 5 月 10 日
Windows 10 Version 1903	2019 年 5 月 21 日	2020 年 12 月 8 日	2020 年 12 月 8 日
Windows 10 Version 1809	2018 年 11 月 13 日	2020 年 5 月 12 日	2021 年 5 月 11 日
Windows 10 Version 1803	2018 年 4 月 30 日	2019 年 11 月 12 日	2020 年 11 月 10 日
Windows 10 バージョン 1709	2017 年 10 月 17 日	2019 年 4 月 9 日	2020 年 4 月 14 日
Windows 10 バージョン 1703	2017 年 4 月 5 日	2018 年 10 月 9 日	2019 年 10 月 8 日
Windows 10 バージョン 1607	2016 年 8 月 2 日	2018 年 4 月 10 日	2019 年 4 月 9 日

https://support.microsoft.com/ja-jp/help/13853/windows-lifecycle-fact-sheet

kaspersky

Windows10運用の課題

（1）品質更新プログラム Quality Updates (QU)の適用と
サードパーティー製品パッチ適用。

品質更新プログラムは月例パッチとしてリリース。
脆弱性修正のために、適宜適用が必要。

ブラウザー、Acrobat Readerなどのサードパーティー製品の
タイムリーな脆弱性パッチ適用も重要。

（2）機能更新プログラム Feature Update (FU)

機能更新プログラムは半年に一度リリース。
サポート継続のためには最低でも年一回の適用が必要。

適用には検証や配布計画、適用延期などが必要。
サイズが大きいためトラフィックコントロールや、
スケジュール分散などが必要。

kaspersky

Kaspersky Vulnerability and Patch Managementのご紹介

kaspersky

Kaspersky Vulnerability and Patch Managementとは

脆弱性管理とIT資産管理機能を持つセキュリティ製品。
主要な攻撃経路である脆弱性を管理し防御力を高めるソリューションです。

kaspersky

Kaspersky Vulnerability and Patch Management

脆弱性管理のポイント

脆弱性可視化

企業・組織内の
アプリケーション・Windowsの
脆弱性を把握

優先順位付け

脆弱性の危険度、
エクスプロイトの再現性の高さを
クラス分け

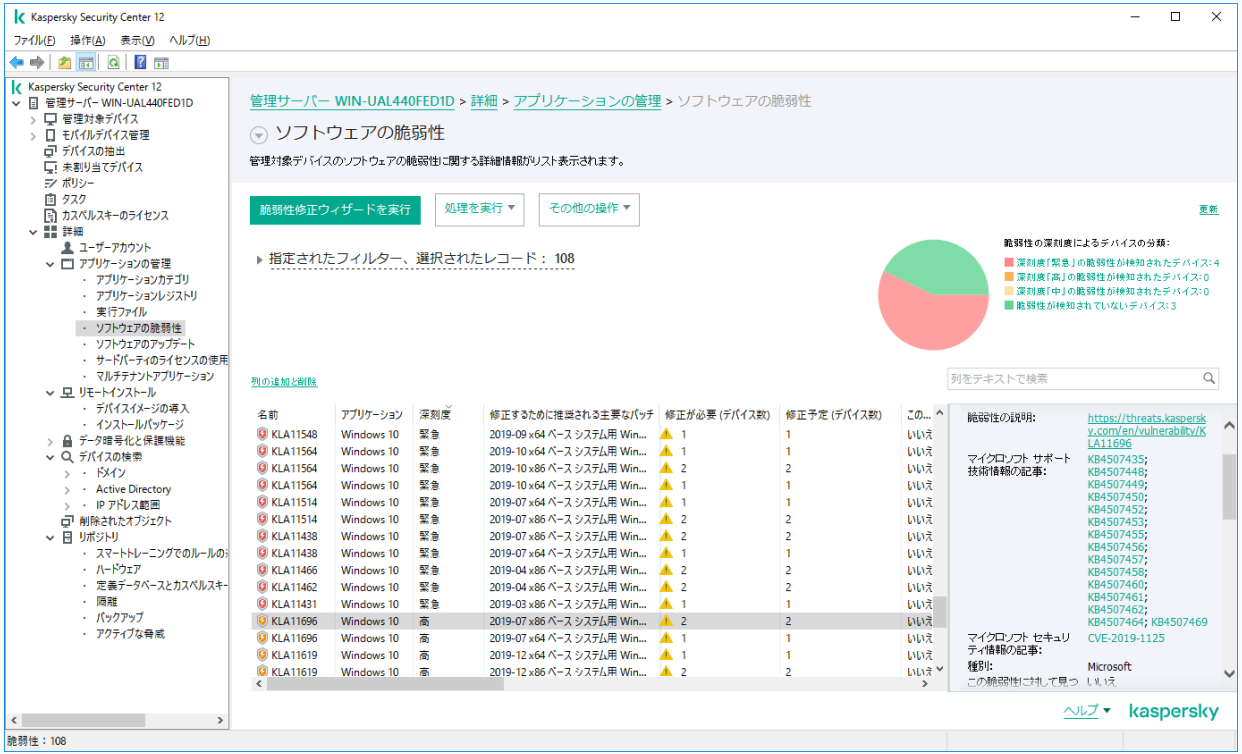
パッチ適用の
コントロール

ルールベースのタスク作成
スケジュール
トラフィックコントロール

kaspersky

Kaspersky Vulnerability and Patch Management

・脆弱性可視化

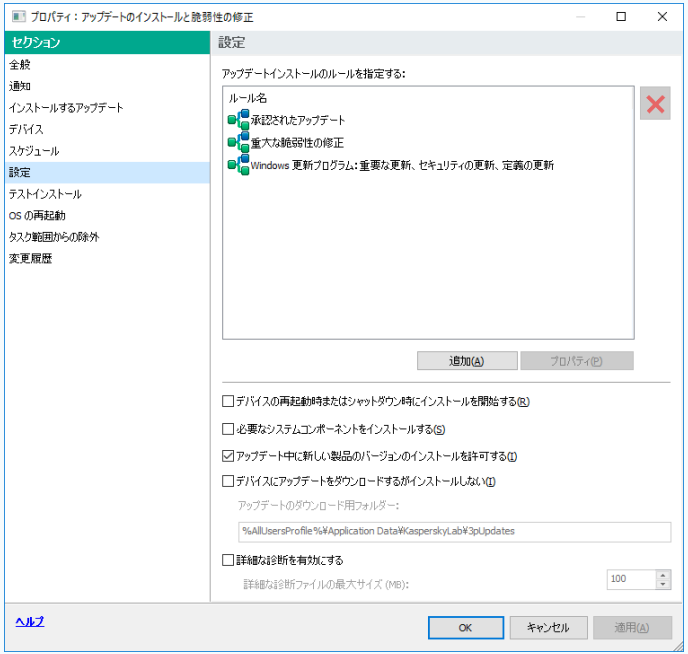


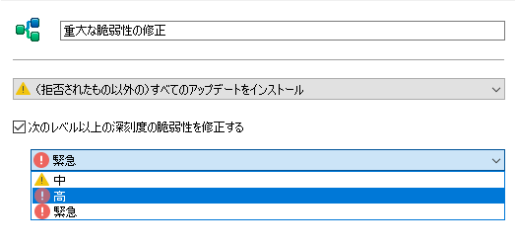
脆弱性スキャンタスクにより
各Windows端末に存在する
脆弱性を可視化

実行ファイルの開始時にも
脆弱性をスキャン

Kaspersky Vulnerability and Patch Management

・優先順位付け





カスペルスキーが深刻度・
緊急度をラベル付け。

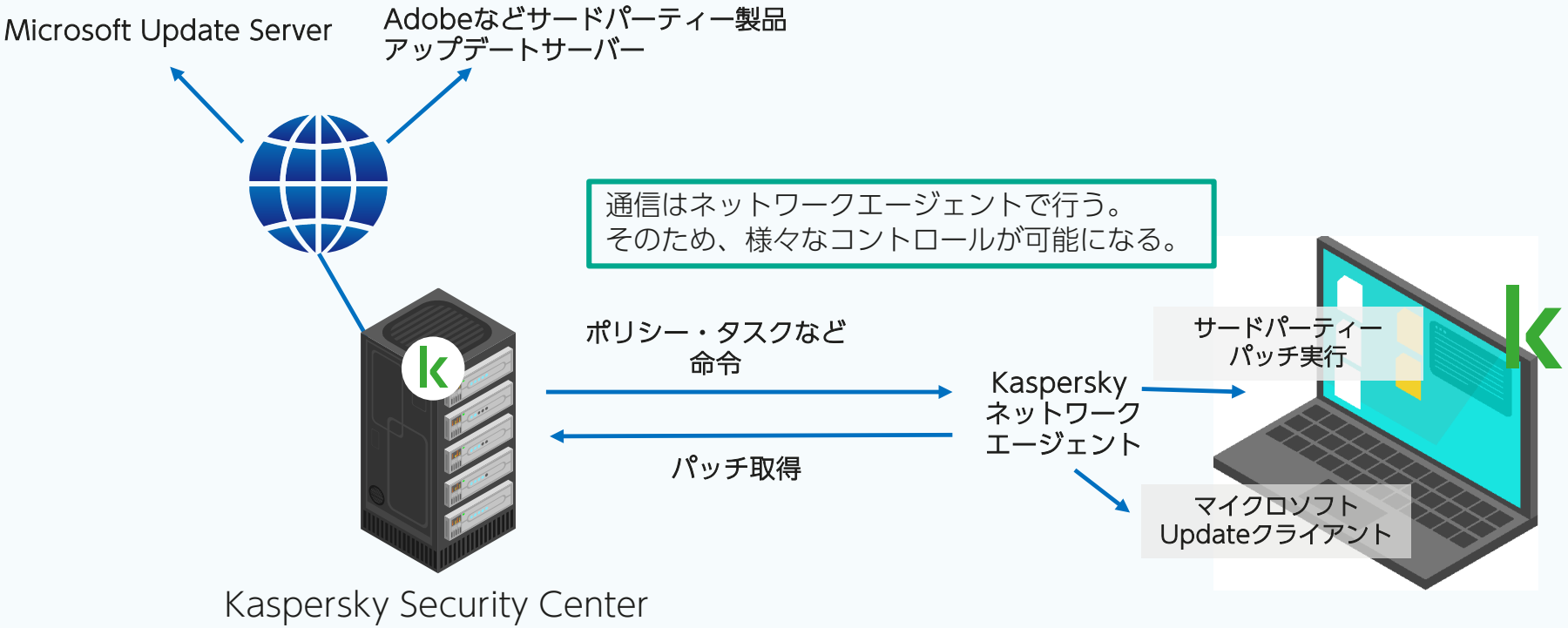
個別のパッチを指定するのではなく、
アプリケーションと深刻度を
組み合わせた、ルールベースでの
パッチ適用タスクを作成。

タスクはスケジュールに従って、
定期的に実行される。

kaspersky

Kaspersky Vulnerability and Patch Management

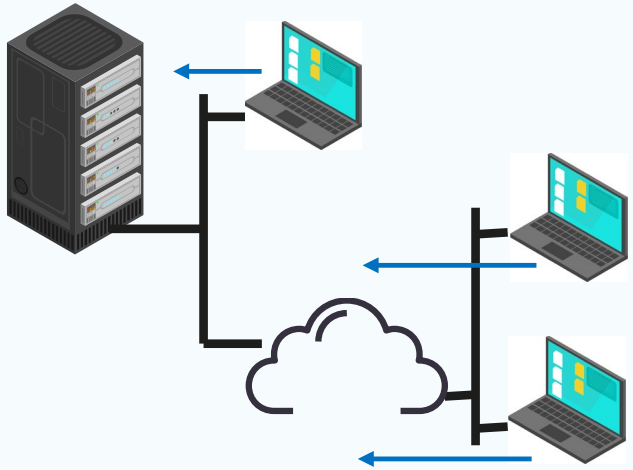
・パッチ配信の仕組み



Kaspersky Vulnerability and Patch Management

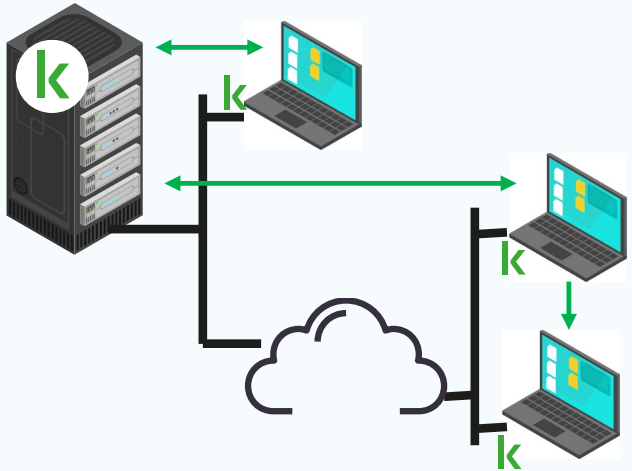
・パッチ適用のコントロール　WSUSとの比較

WSUSの場合



各端末のWindows Updateクライアントから
通信される。
基本的に各端末がWSUSサーバーと直接通信する

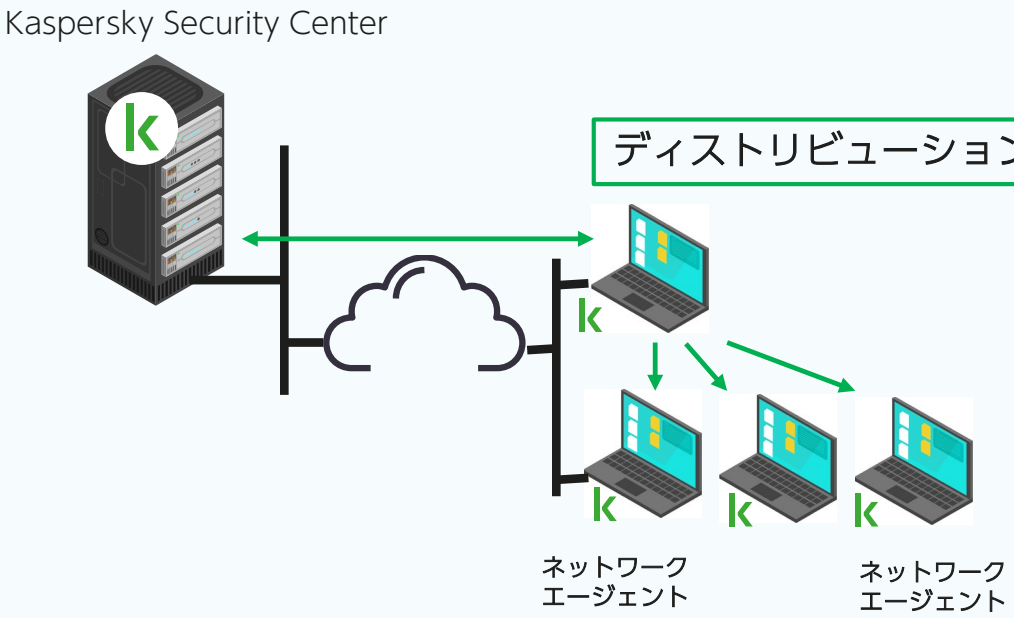
KVPMの場合



各端末のネットワークエージェントがKSCの指示を受けて
スケジュール実行。
拠点での通信は、ディストリビューションポイントを通じて
実行可能。

Kaspersky Vulnerability and Patch Management

・パッチ適用のコントロール

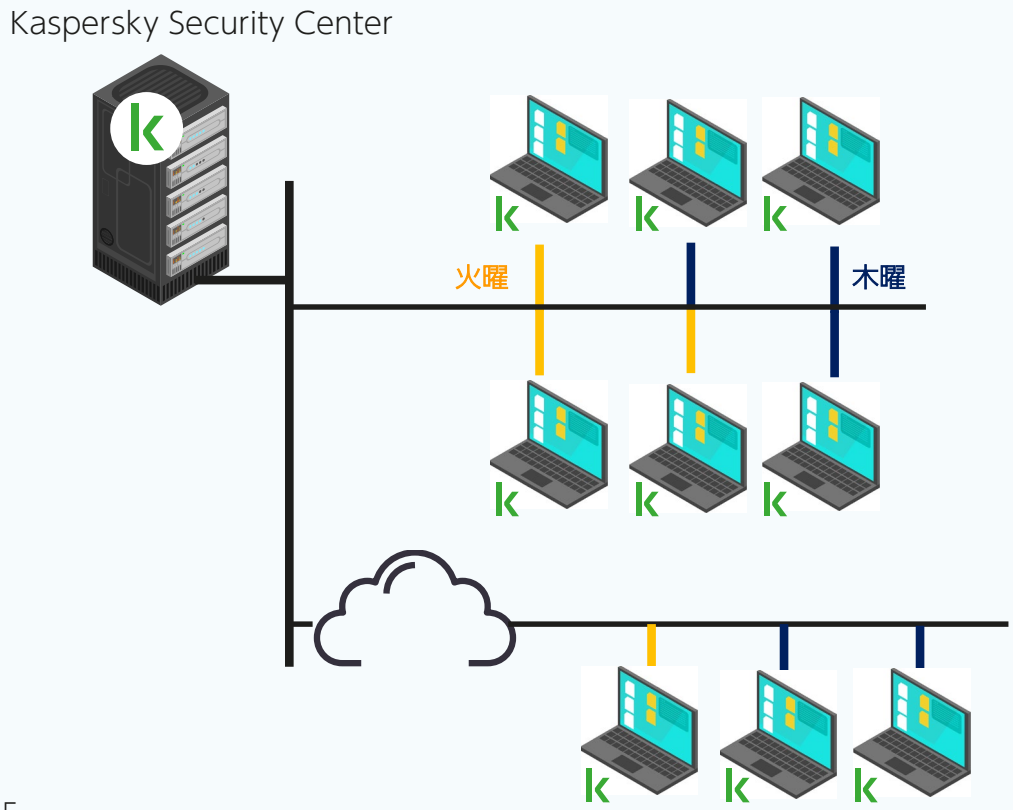


拠点にディストリビューションポイントを設定

拠点の各端末は、ディストリビューションポイントからパッチを取得して適用

Kaspersky Vulnerability and Patch Management

・パッチ適用のコントロール

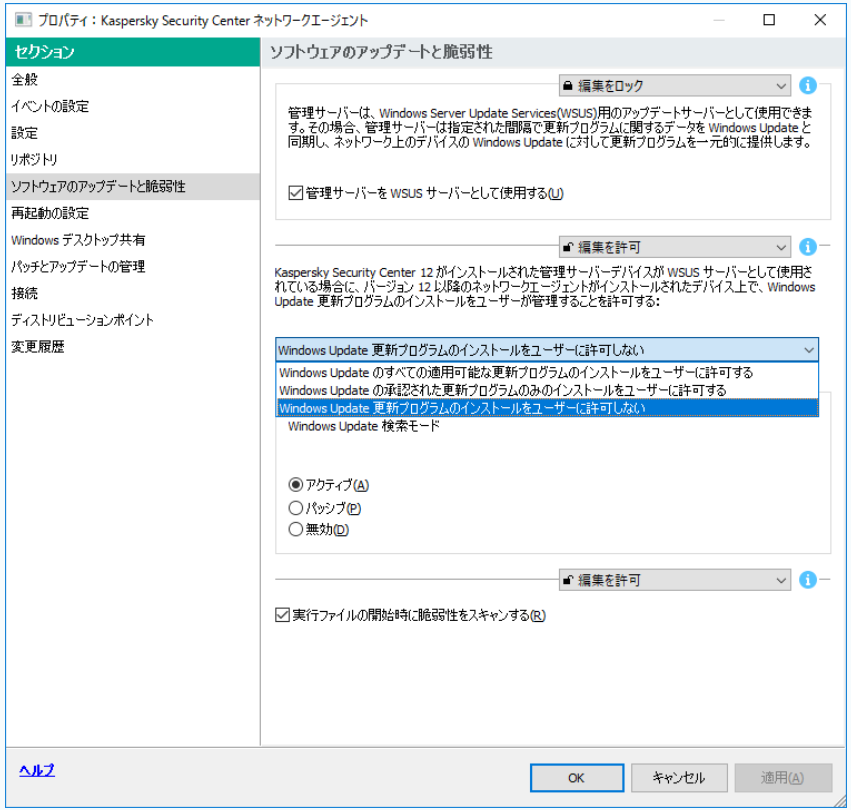


スケジュール分散

ある端末群は火曜日、ある端末群は木曜日といった、スケジュール実行が可能。

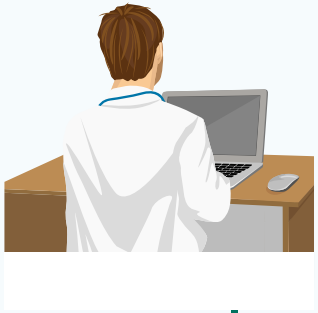
Kaspersky Vulnerability and Patch Management

・パッチ適用のコントロール



各端末のWindows Updateクライアントの
挙動を抑制し、計画的な運用を可能にします。

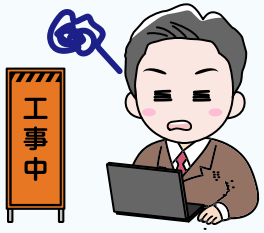
エンドユーザーによるWindows Update実行を
抑止することができます。



Windows10 機能更新プログラム

機能更新プログラム（FU）適用　問題

- 適用のタイミングを遅らせたい。
  年に二度の適用ではなく、一度だけにしたい。
- サイズが大きいので、トラフィックを抑制したい。



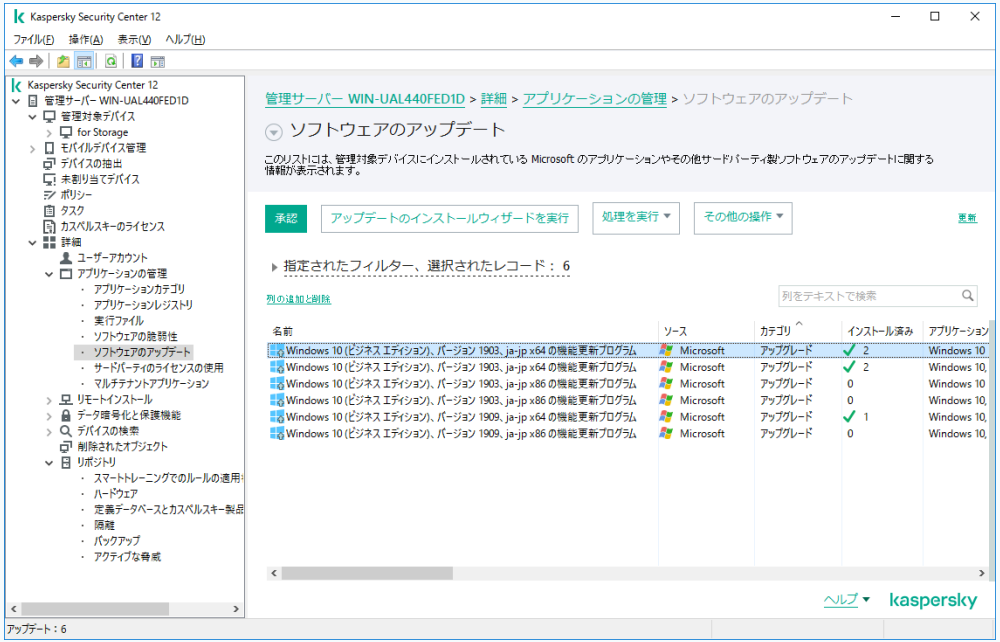
KVPMの機能により、FUの適用を延期。

スケジュール、ディストリビューションポイントにより、
負荷分散、トラフィックコントロールを実現。

kaspersky

Windows10 機能更新プログラム

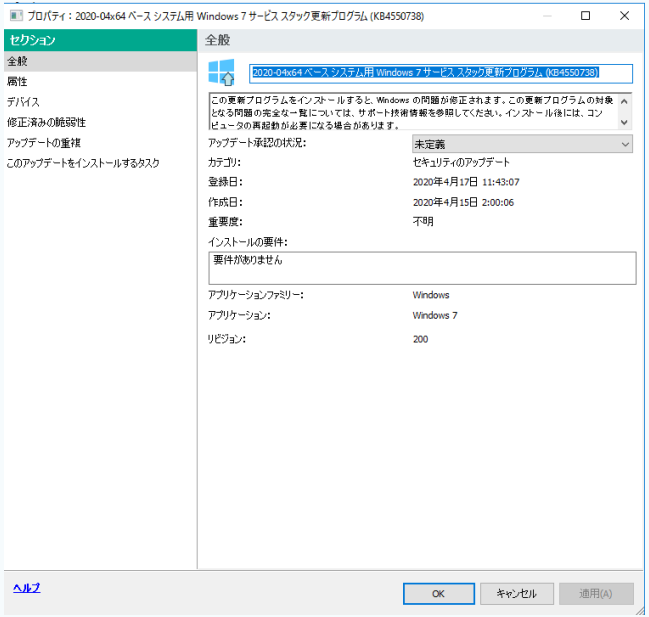
管理サーバーに機能更新プログラムをダウンロード
対象端末も自動で判別

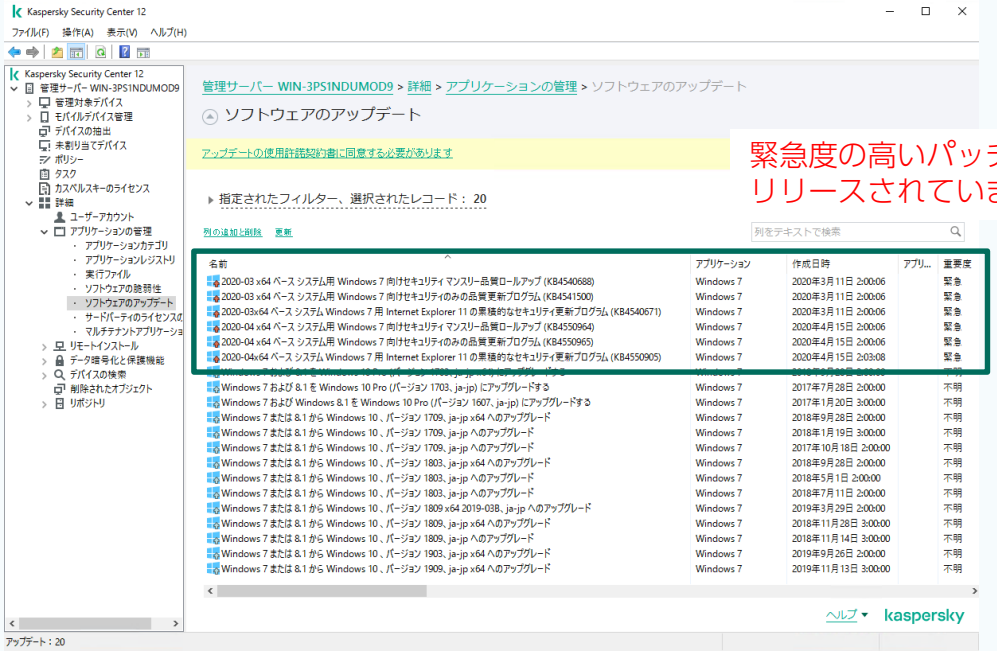


運用例
常時のパッチ適用タスクでは
アップグレードカテゴリーは対象外とし、
機能更新プログラムを適用するタスクを
タイムリーに作成実行する。

Windows 7 の拡張セキュリティ更新プログラム Extended Security Update (ESU)の運用

Windows 7 サポート終了後でも、ESUを購入されたお客様は、
KVPMからパッチ適用することができます。





その他の機能紹介

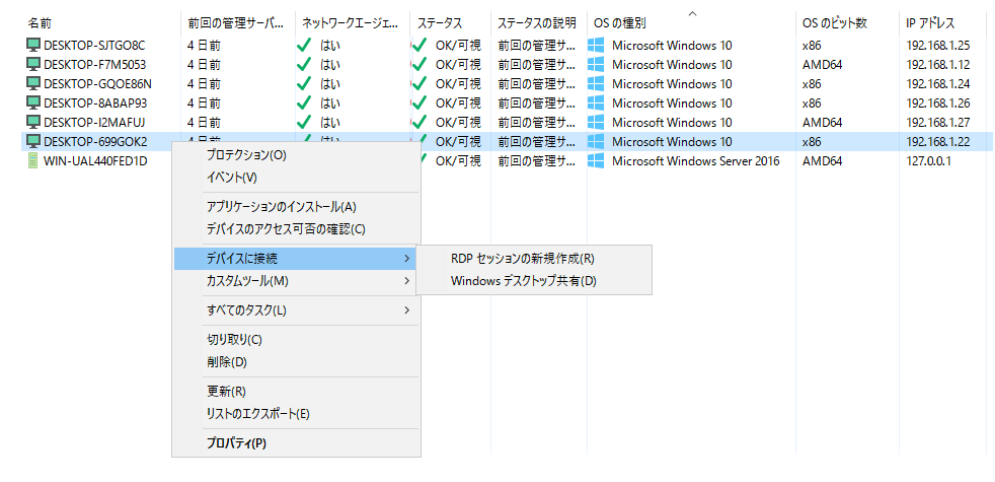
kaspersky

リモートコントロールツール

接続したい端末を右クリックするだけの簡単操作

2種類の接続方法

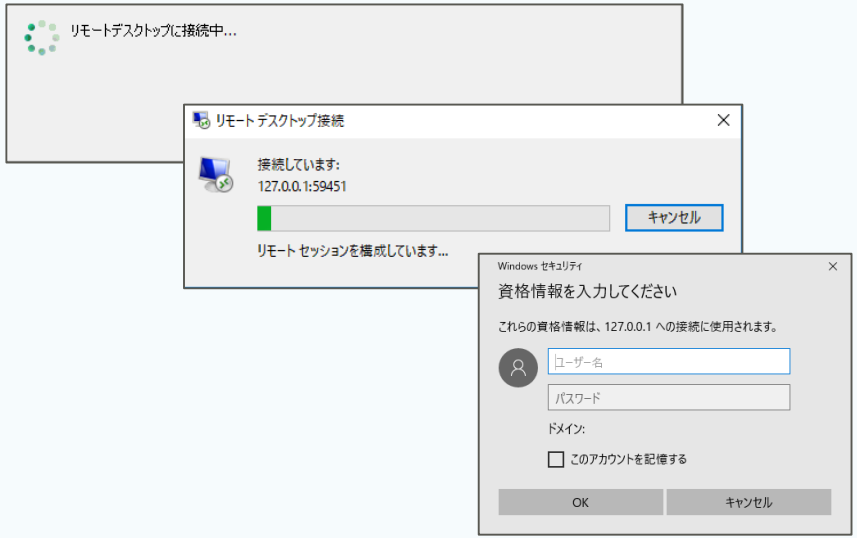
- リモートデスクトップ接続　（エンドユーザーが使用している画面と別の画面で接続。リモートメンテナンス向け）
- Windowsデスクトップ共有　（エンドユーザーが使用している画面を共有。ヘルプデスク向け）



kaspersky

リモートデスクトップ接続

ビューから右クリックし、接続します。
認証情報を入力し、新規セッションを作成。
接続された端末側は画面がロックされます。

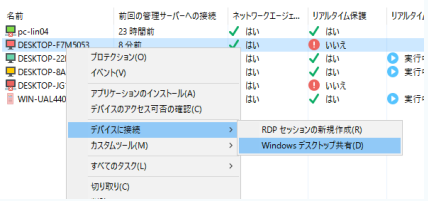


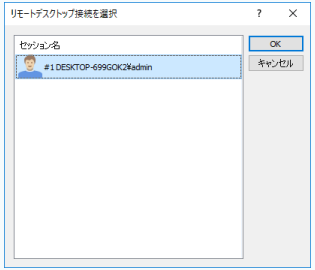
リモート操作

kaspersky

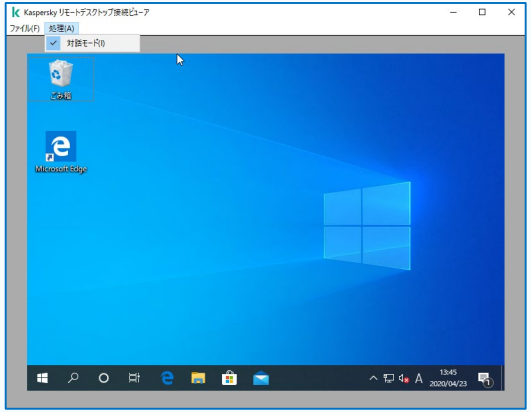
Windowsデスクトップ共有

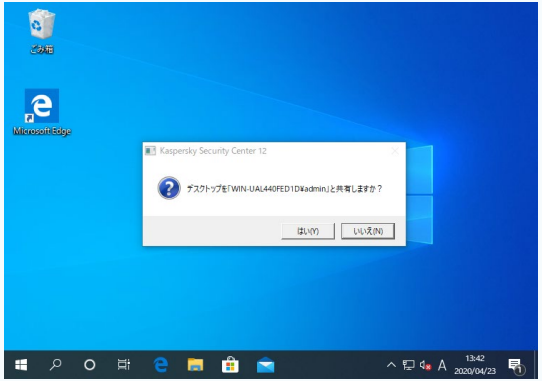
ビューから右クリックし、接続します。
エンドユーザーが使用している画面を共有します。





リモート操作





エンドユーザー側では
接続を許可する

kaspersky

Kaspersky Vulnerability and Patch Managementの購入方法

kaspersky

Kaspersky Vulnerability and Patch Management

（1） Kaspersky Vulnerability and Patch Management 単体で購入

適しているケース

- 他社アンチウィルス製品との併用。
- Linux、Android、MACの台数が多く、SelectからAdvancedへの移行がどうしても割高となってしまう場合。
（ほとんどのケースでAdvancedの購入が安価です。）

（2） Kaspersky Endpoint Security For Business Advancedを購入

適しているケース

- カスペルスキーのエンドポイントセキュリティを利用中か乗換を検討している。
- Advanced の他機能（HD暗号化、アダプティブアノマリーコントロール、Windows Serverでのアプリケーション起動コントロール）を導入したい。

kaspersky