kaspersky

Kaspersky Endpoint Security for Business（KESB）製品概要

2023年8月

kaspersky

Agenda

カスペルスキー製品の特長

製品体系

kaspersky

カスペルスキー製品の特長

Kaspersky Endpoint Security for Business（KESB）

KESB　ライセンス体系

✓ KESBには、以下2つのライセンスがあります。

KESB Select

基本的なセキュリティ保護機能に加え、コントロール機能にてセキュリティを強化

サーバーOSに対してもセキュリティ対策を実現

KESB Advanced

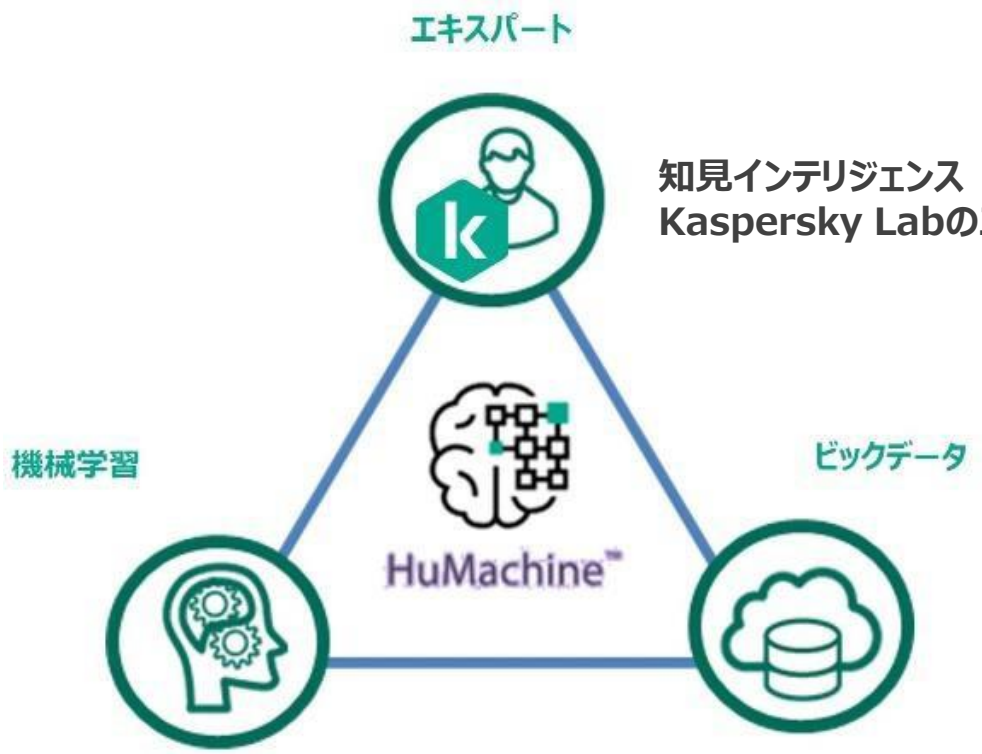
KESB Selectの保護機能に加え、パッチ自動配信、アノマリーコントロール、デスクトップ共有、OSイメージ管理、暗号化など、管理機能を強化

kaspersky

HuMachine（ヒューマシン）とは？

安全

✓ ビッグデータ、機械学習、当社エキスパートアナリストの専門技能という3つの基本要素を融合



知見インテリジェンス
Kaspersky Labのエキスパートによる独自分析

機械学習技術による数学的な
モデルに基づいて脅威を分析

レピュテーションインテリジェンス
クラウドデータ、ふるまい、自動分析

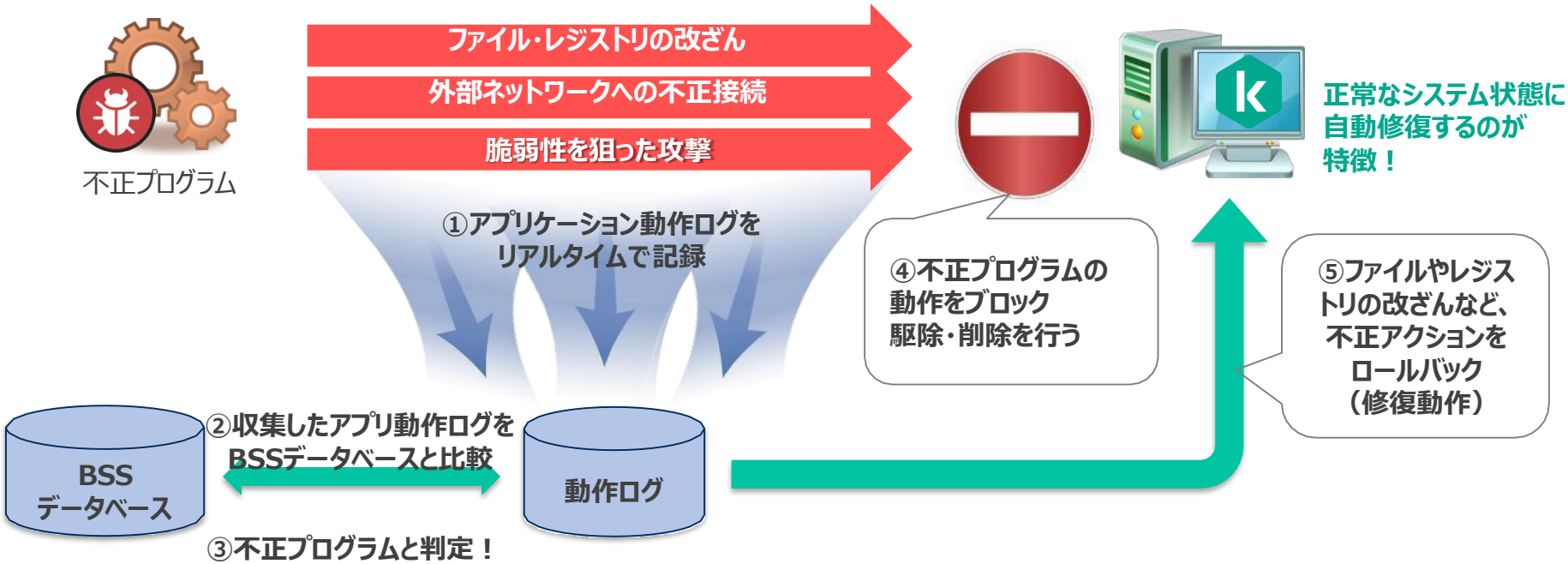
kaspersky

安全

ふるまい検知と修復エンジンによるロールバック

- ✓ カスペルスキーのふるまい検知は、サンドボックス技術だけでなく、実環境上でもマルウェア特有の挙動をとらえて、不正プログラムと判定し、ブロック・隔離・駆除・削除を実行。
- ✓ 防御するまでに変更されてしまったレジストリやシステムファイルを修正（ロールバック）し、正常なシステム状態まで修復。

単にサンドボックスの検知とブロックをするだけの他社製品と大きな違いがあります。

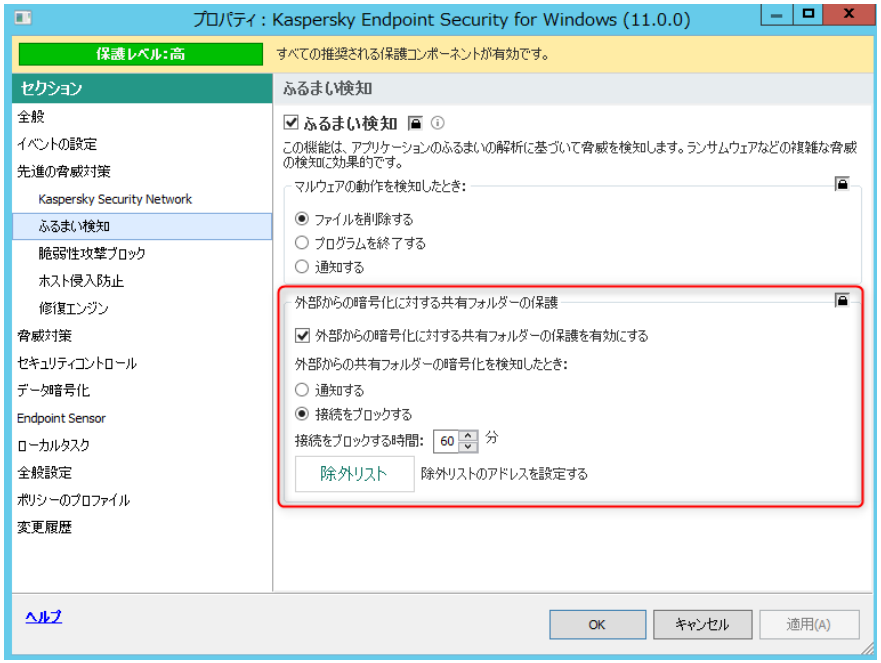


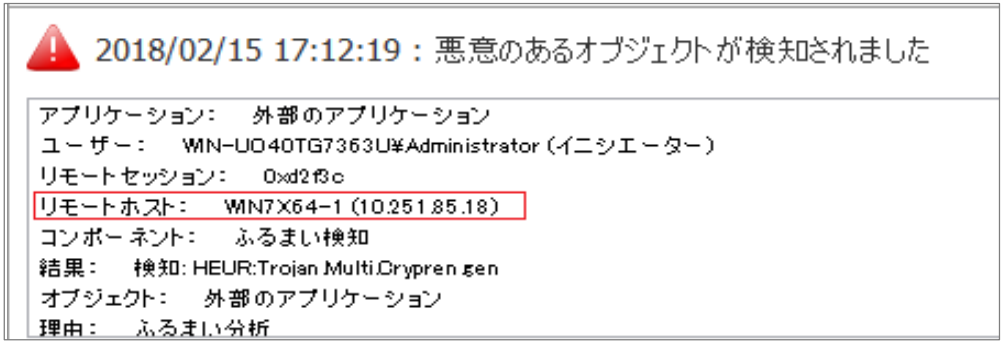
kaspersky

ふるまい検知：共有フォルダへの暗号化攻撃保護

安全

- ✓ 共有フォルダに対して、外部からの悪意のあるファイル操作を監視・ブロック。
  （監視動作：削除、内容変更、サイズ変更、移動）
- ✓ 攻撃を検知したら攻撃元ホストを指定時間ブロック。（時間の指定は1分～30日の間）

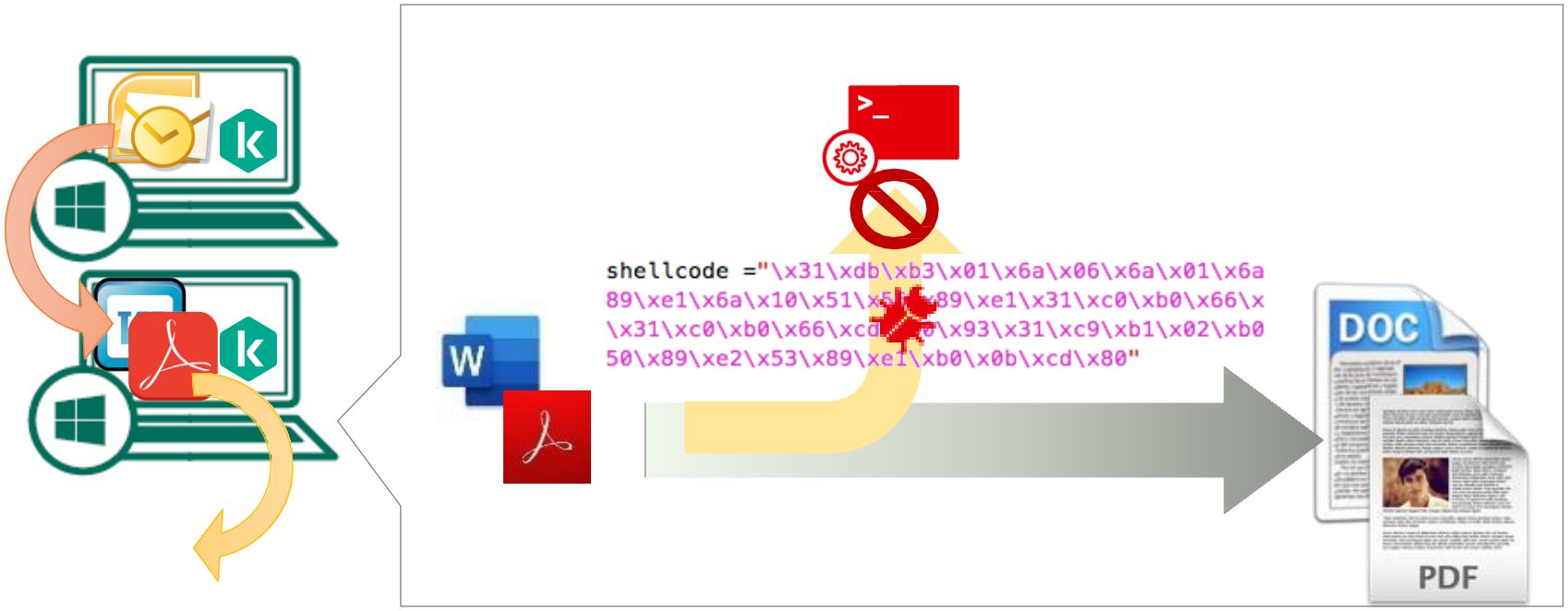




kaspersky

脆弱性攻撃ブロック

- ✓ 脆弱性攻撃ブロックの機能でも、アプリケーションの挙動を監視。
- ✓ 脆弱性を突かれて不正コードが実行されようとした際にブロック。
- ✓ ファイルのシグネチャベースではマルウェアか判断がつかない場合に特に有効。
- ✓ システムプロセスのメモリも保護するため、**ファイルレスマルウェア対策に効果的。**



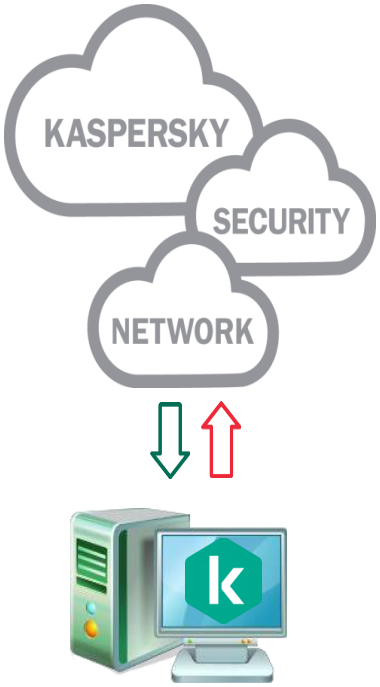
クラウドデータベース
Kaspersky Security Network（KSN）

安全

- ✓ KSNは世界中のユーザーから収集された最新の脅威情報データベース。
- ✓ カスペルスキー製品によって保護された仮想マシンは、この脅威情報データベースを参照することで、ゼロデイ攻撃のような最新の脅威にも対応することが可能。

KSN

KSNは、４億人以上のカルペルスキー製品ユーザーと最新の脅威情報を共有しています。



■ KSNの仕組み

① カスペルスキーが導入されたコンピューターは不審な挙動を見せる脅威に関する情報をリアルタイムでKSNに送信

② カスペルスキーのAI技術（Automatic Analysis System）にて、悪意のある脅威は即座に「緊急検知DB」に追加される

③ ユーザーコンピューターはリアルタイムでKSN上の緊急検知DBやホワイトリスト情報を都度参照し、最新の情報で端末を保護

④ KSNへ登録された脅威情報はカスペルスキーのアナリストが正確に解析・評価し、定義DBへ反映

kaspersky

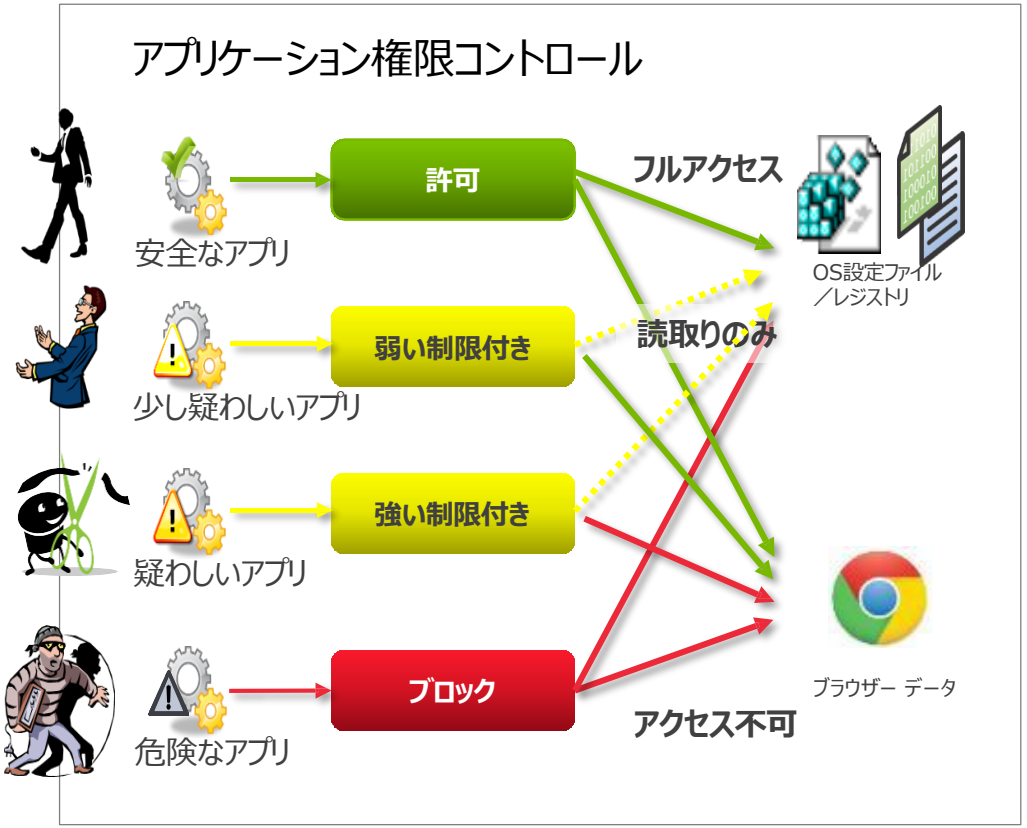
ホスト侵入防止

安全

- ✓ 白黒判定が困難なグレーなプログラムに関しては、完全にブロックするのではなく、他アプリへ影響を与える動作でなければ　実行可能など、細かな自動権限制御を実施。
- ✓ 他社にはないカスペルスキー特有の技術で、**誤検知低減に非常に効果的**。

特長

- ➢ アンチウイルスがアプリケーションの信頼性を評価し、自動で制限付きグループに割り当てられます。例えば、そのアプリ単体で動くこと自体は問題ないが、他プロセスへコードを埋め込むことで悪用される可能性があるアプリと判断した場合などに制限付きグループに割り当てられます。
- ➢ 完全に動作をブロックするわけではないため、セキュリティレベルを維持しつつ、誤検知を低下させることを実現します。他社製品の多くはこうしたグレーアプリを白・黒いずれかで判断してしまうため、誤検知が多くなってしまう製品もあります。

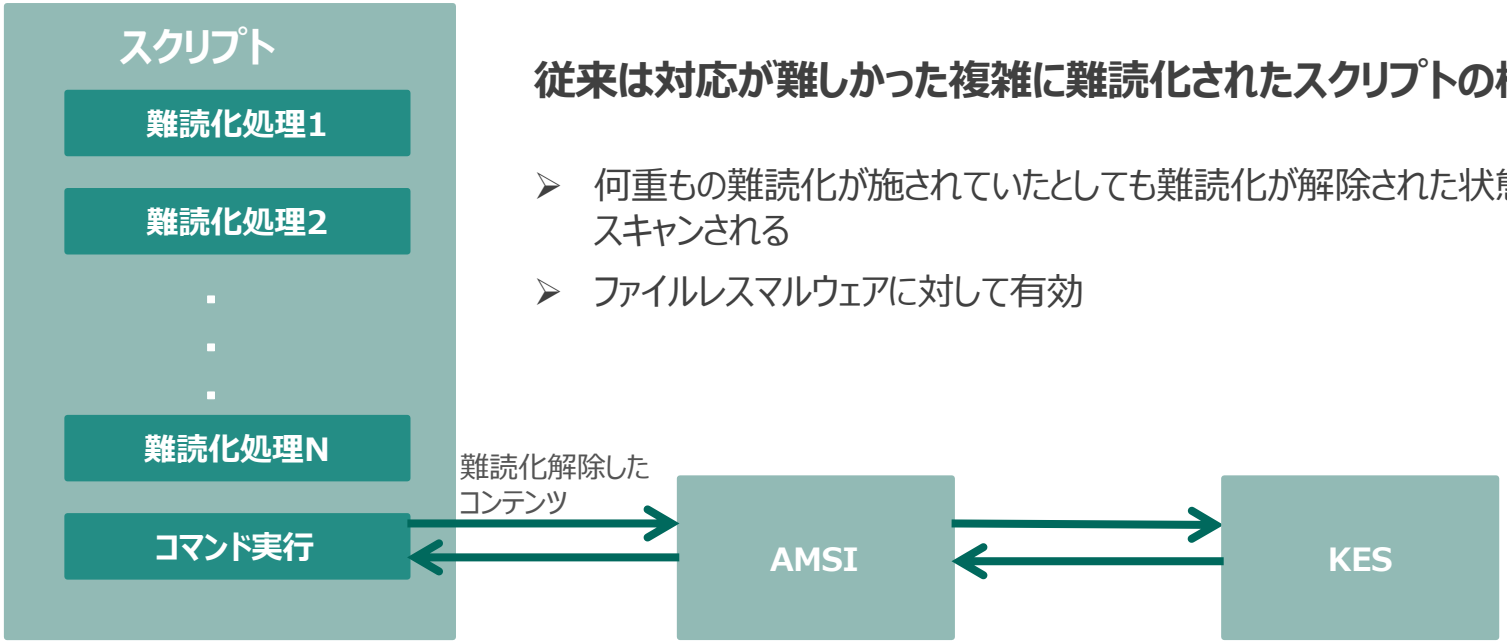


kaspersky

AMSI 保護プロバイダー

安全

- ✓ Antimalware Scan Interface（AMSI）と統合することで、AMSI対応アプリケーションで実行中のプログラムの中からKESにコンテンツを引き渡し、マルウェアでないかどうかをチェックできる
- ✓ Kaspersky独自の機能ではなくWindows10 に搭載されている機能への対応
- ✓ AMSI対応アプリケーション
  - ➢ PowerShell, JavaScript, VBScript等のスクリプトエンジン
  - ➢ Office VBAマクロ
  - ➢ 対応アプリケーションは今後も増える



従来は対応が難しかった複雑に難読化されたスクリプトの検知能力が向上

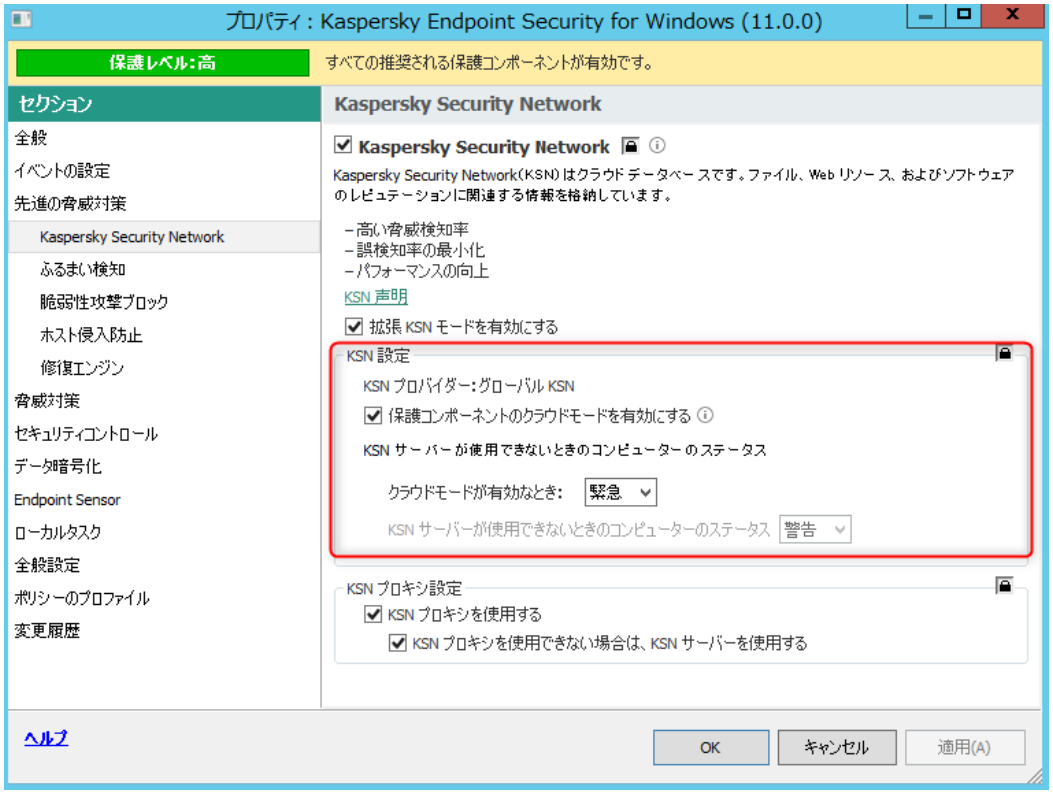
- ➢ 何重もの難読化が施されていたとしても難読化が解除された状態でKESによってスキャンされる
- ➢ ファイルレスマルウェアに対して有効

kaspersky

クラウドモード（ライトウェイトモード）

低負荷

- ✓ 軽量版の定義データベースを使用し、オペレーティングシステムのリソース消費を減少。
  （メモリ使用量 ~**10%減**、ディスク使用量 ~**30%減**）
- ✓ クラウドモード利用時は、KSN*利用が必須。　　*P9参照
- ✓ デメリットは、クラウドモード有効端末がKSNを利用できない場合に保護レベルが低下。



➢ **定義DBダウンロード時の挙動**

KSCはフル版および軽量版の定義DBの両方をダウンロードして保持。
KESはクラウドモード有効・無効の設定に従って、フル版 or 軽量版の定義DBをKSCより取得。

➢ **クラウドモード切替時の挙動**

クラウドモード有効・無効切り替えの設定反映タイミングは次回の定義DB更新時になる。
（理由は、定義DBのロードが必要なため）

➢ **エラー時の挙動**

KSNを利用できない場合：
KSC上でデバイスがKSNに接続できない旨を知らせるステータス表示になる。

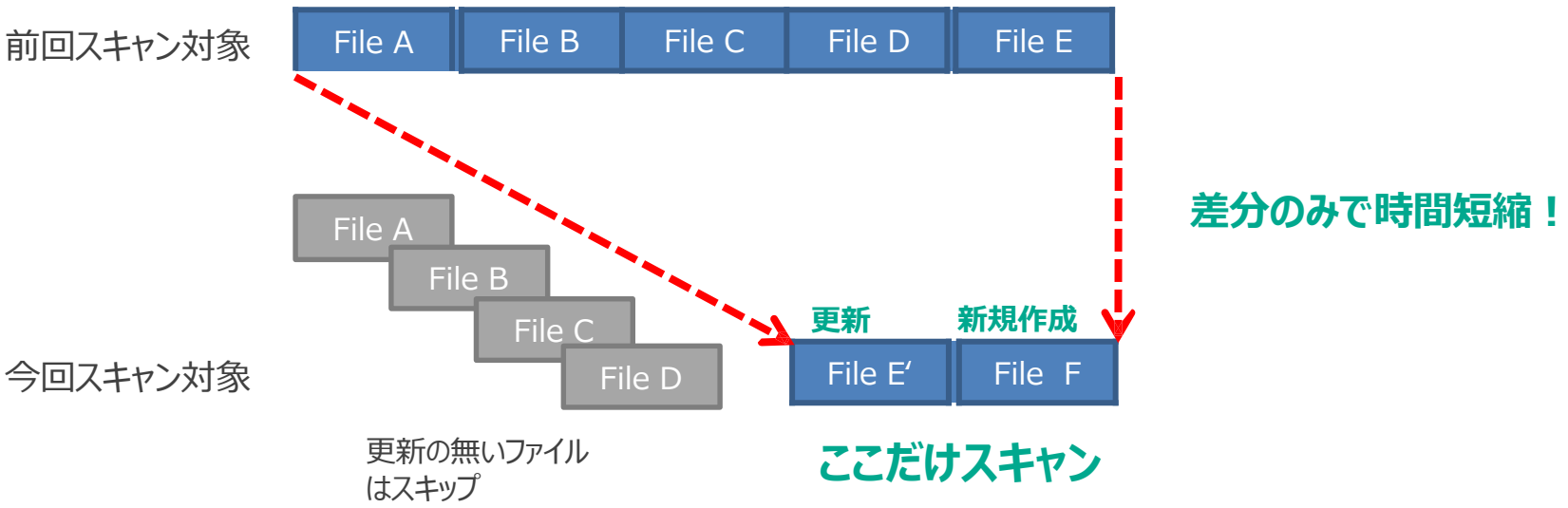
KSNプロキシを利用できない場合：
KSNサーバーを使用。（既定で有効 ）

kaspersky

低負荷　オンデマンドスキャン

低負荷

- ✓ 前回スキャン時と比較し、更新された差分のみスキャン。
- ✓ オンデマンドスキャンの時間短縮を実現します。



あるお客様の導入事例では、1時間以上かかっていたスキャンが、約10分に短縮！

毎日定期スキャンを行うことで差分を少なくし、かつセキュリティも強固に保てます。

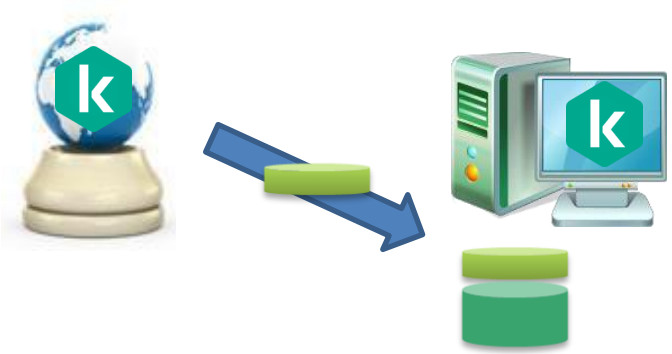
kaspersky

低負荷　定義ファイルの更新

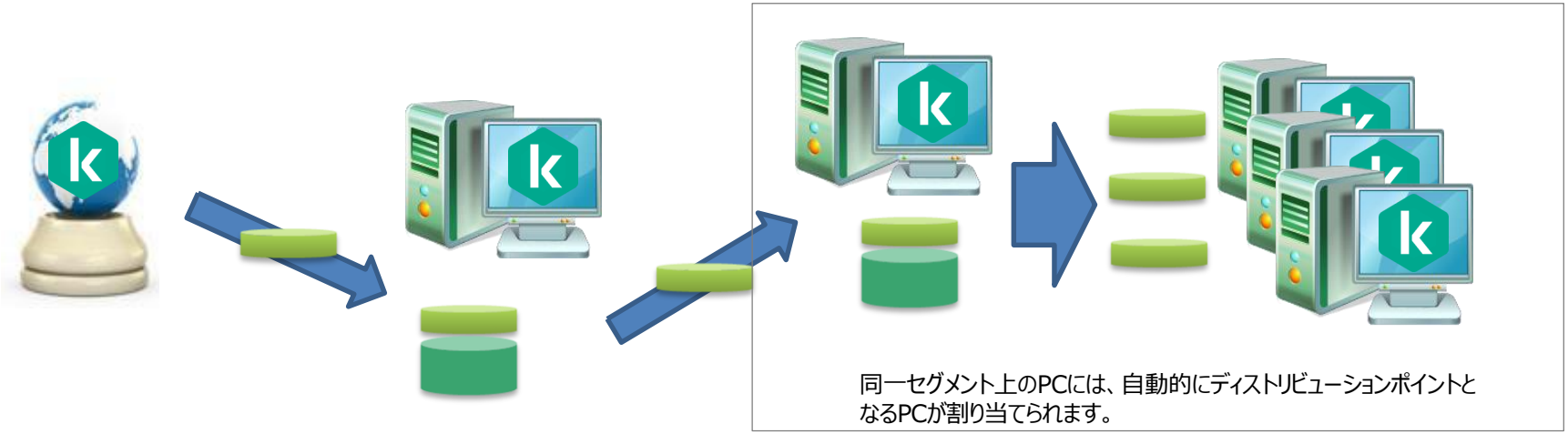
低負荷

- ✓ カスペルスキーでは前回更新した定義ファイルとの**差分で配信！**
- ✓ 最新の脅威からも守り、かつPCの定義ファイル更新負荷も低減します。
  - ➢ 定義ファイル配信回数：**約1時間に1回**
  - ➢ 1回あたりの増加ファイル：**約500KB～数MB**

※いずれも2020年4月時点の平均値。値は時期により変動します。



ディストリビューションポイントを使用することで、
すべてのPCがサーバーにアクセスせず更新が可能です。

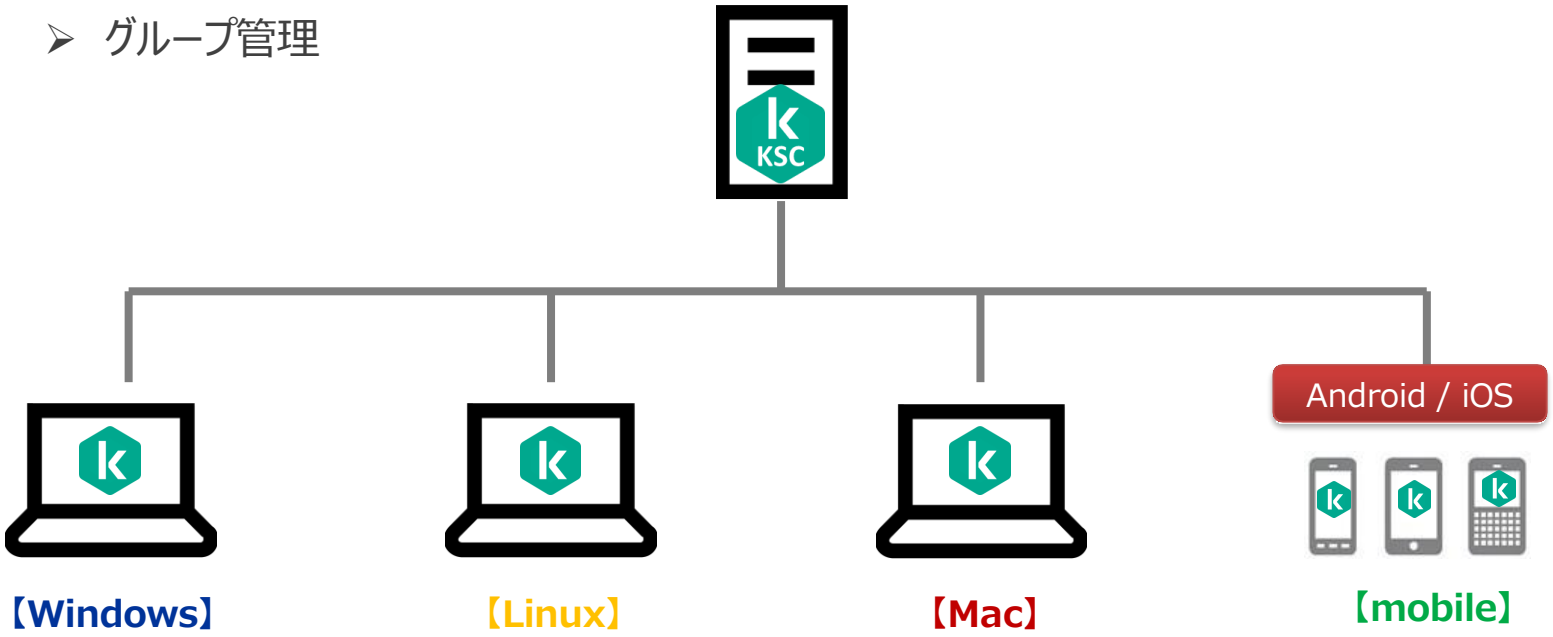


kaspersky

充実した管理ツール

管理

- ✓ Kaspersky Security Center(以降KSC)で集中管理
  - ➢ ポリシー設定の配布
  - ➢ 定義データベースの配布
  - ➢ イベント、レポートの管理
  - ➢ リモートインストール
  - ➢ グループ管理

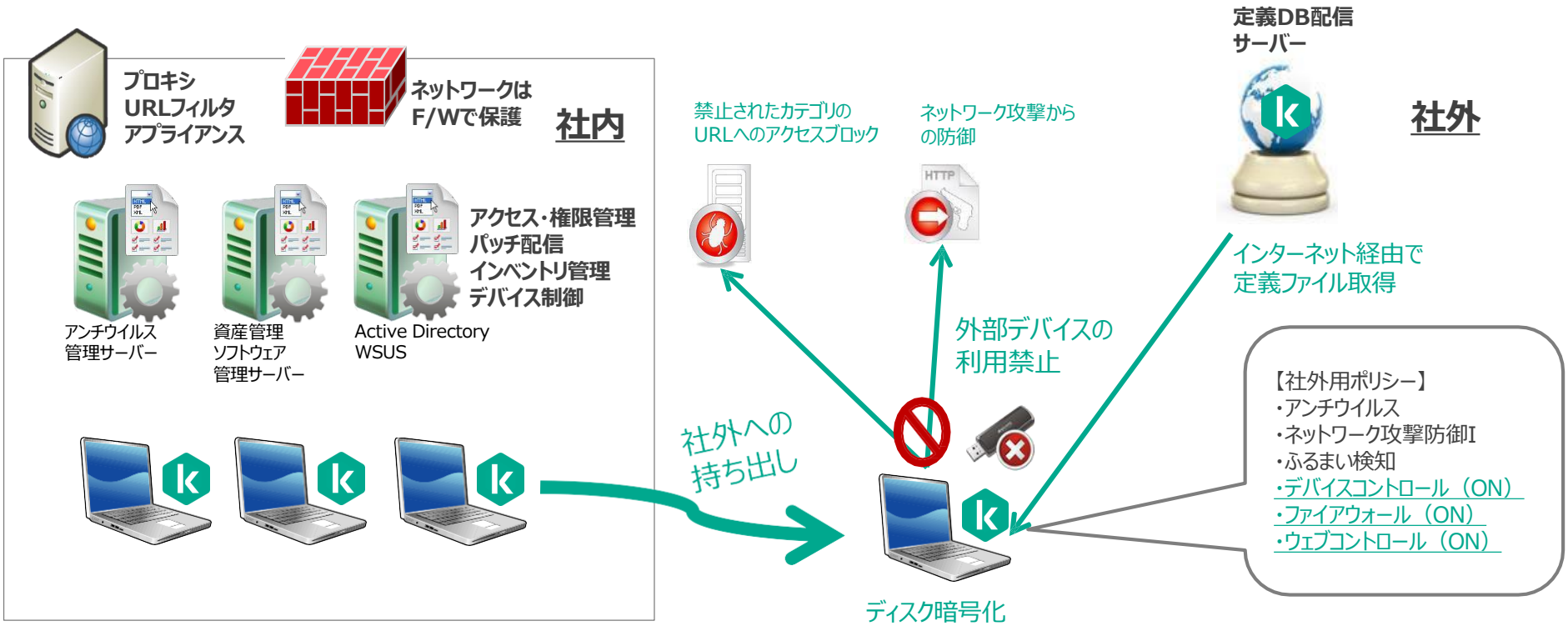


kaspersky

充実した管理ツール

管理

- ✓ KSCの設定により**ポリシーの二重化**が可能。
  - ➢ 社内では：F/W、URLフィルタリング、プロキシで保護。
  - ➢ 社外では：ファイアウォール、ウェブコントロール、デバイスコントロールをON



kaspersky

充実した管理ツール

管理

✓ 簡単な乗換、簡単なインストール作業

- **プッシュインストール**
  競合製品のアンインストール、カスペルスキー製品のインストールをKSCから実施。
  - AD環境ではクライアントの設定変更が不要なので、おすすめです。
  - 競合製品のアンインストールタスク、カスペルスキー製品のインストールタスクを
    まとめて自動実行することが可能。

- **スタンドアロンインストールパッケージ**
  競合製品のアンインストール機能を組み込んだインストールパッケージを作成。
  クライアントで個別で実施。
  - 資産管理ツールがある場合は、資産管理ツールで配布、実行することも可能。
  - WebGUIからインストールパッケージを公開することも可能。

- **イメージ展開**
  OSのイメージに載せてPCに配布可能。(予めセルフディフェンス機能をOFFにしておく必要があります。)
  PCの入れ替え時におすすめの方法。
  ※対象ライセンス KESB Advanced

kaspersky

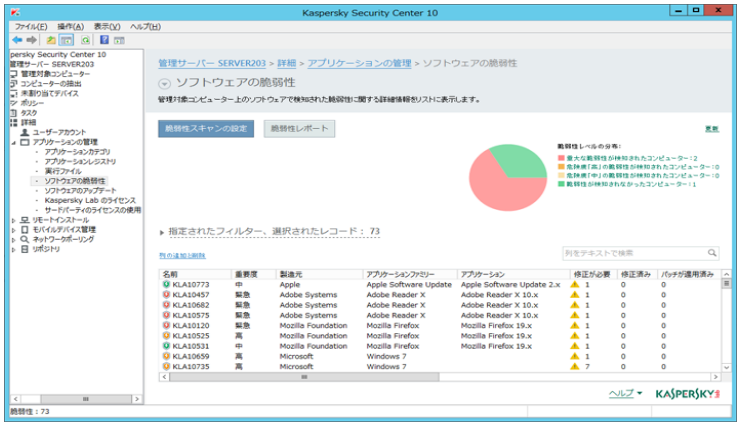
充実した管理ツール

管理

✓ **300Lic以上**ご利用頂けると、オンプレミス型とクラウド型の管理を選択可能　（併用も可能）

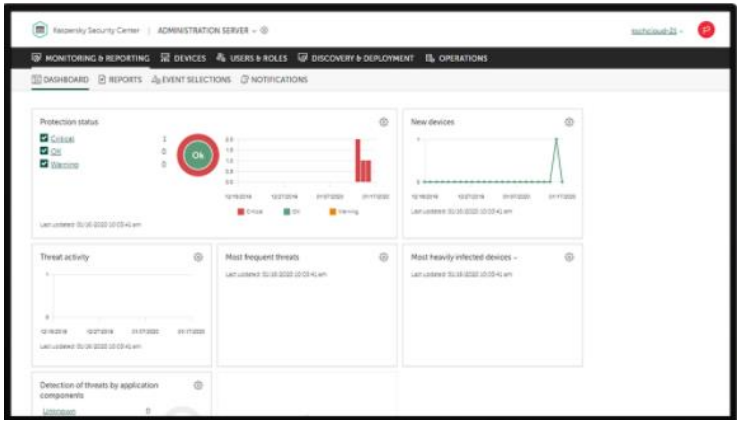
Kaspersky Security Center

・オンプレミス構成（AWSやAzureへの構築も可能）
・専用のアプリケーションをインストール
・MMCとWebのコンソールあり
・オフライン環境対応
・ライセンス数の利用条件無し



Kaspersky Security Center Cloud Console

・クラウドベース
・アカウントの作成とインターネット環境が必要
・ブラウザで利用可能
・300Lic以上から無償でご利用可能



kaspersky

充実した管理ツール （オンプレミス型とクラウド型の違い）

管理

機能	Kasersky Scurity Center	
	オンプレミス	Cloud Console
管理サーバーの配置場所	オンプレミス	Cloud
データベース 配置場所	オンプレミス	Cloud
管理サーバーとデータベースのメンテナンス	お客様による管理	カスペルスキーによる管理
グループ階層管理	○	○ KSC Cloud Consoleはプライマリー管理サーバとしてのみ機能 （ポリシーとタスク管理のみ可能））
オンプレミスからKSC Cloud Consoleへの移行 （管理対象デバイスと関連オブジェクトの移行）	-	○
管理対象デバイスを別の管理サーバーに切り替え	○	ー （ネットワークエージェントの再インストールが必要）
ネットワークポーリング	○	○ （ディストリビューションポイントによる ネットワークポーリングのみ可能）
管理可能な端末台数	100,000	10,000（拡張予定あり）
Windows, macOS, Linux の管理・保護	○	○
モバイルデバイスの管理・保護	○	○
KSVサポート（仮想マシンの保護）	○	×
パブリッククラウド API連携	○	×
イベント通知	○	○（e-mailのみ）
ポリシーによる管理	○	○ （Administration Serverポリシーを除く）
タスクによる管理	○	○
Kaspersky Security Network サポート	○	○
KSN Proxy	○	○ （ディストリビューションポイントが持つKSNプロキシ機能のみ） ※KSC CCでは使用できない
Kaspersky Private Security Network	○	×
ライセンスの集中管理、適用	○	○
仮想管理サーバー機能	○	×
Vulnerability and Patch Management 機能	○	○
暗号化管理	○	×
管理用ユーザーアカウントの作成	○	○
SIEM との統合	○	×
WSUS サーバーとしての利用	○	×
ポリシーとタスクの適用状況監視	○	○

kaspersky

kaspersky

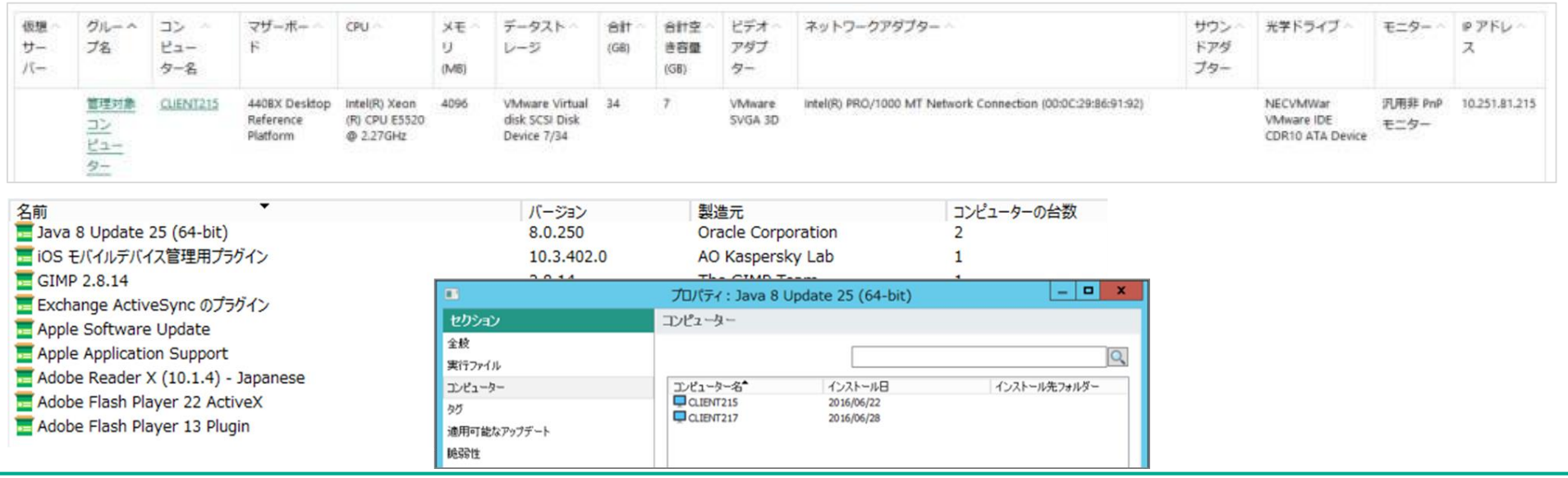
管理・セキュリティコントロール機能

～KESBシリーズの基本機能～

IT資産管理とぜい弱性スキャン

多機能

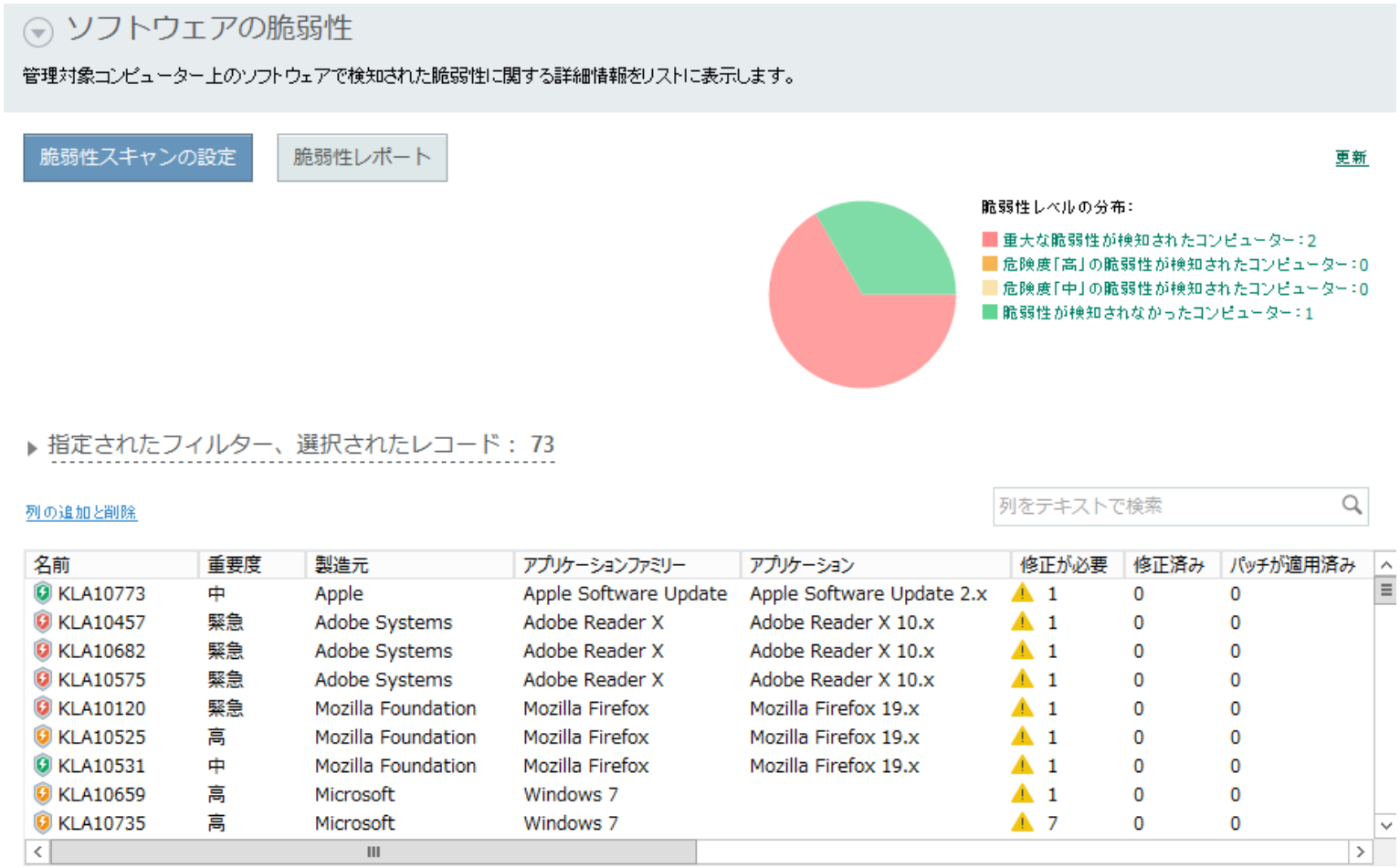
- ✓ インベントリ情報の収集
  - ➢ ハードウェアインベントリ
    （コンピューター名、IPアドレス、マザーボード、CPU、メモリ、データストレージ、ネットワークアダプターなど）
  - ➢ ソフトウェアインベントリ
    （インストールされたアプリケーション情報やコンピュータ内の実行形式、拡張子を持つプログラム）
- ✓ アプリケーションのリモートインストール/削除
  - ➢ カスペルスキー製品だけでなく、サードパーティアプリケーションのインストール/アンインストールが可能



IT資産管理とぜい弱性スキャン

多機能

✓ 脆弱性レポート



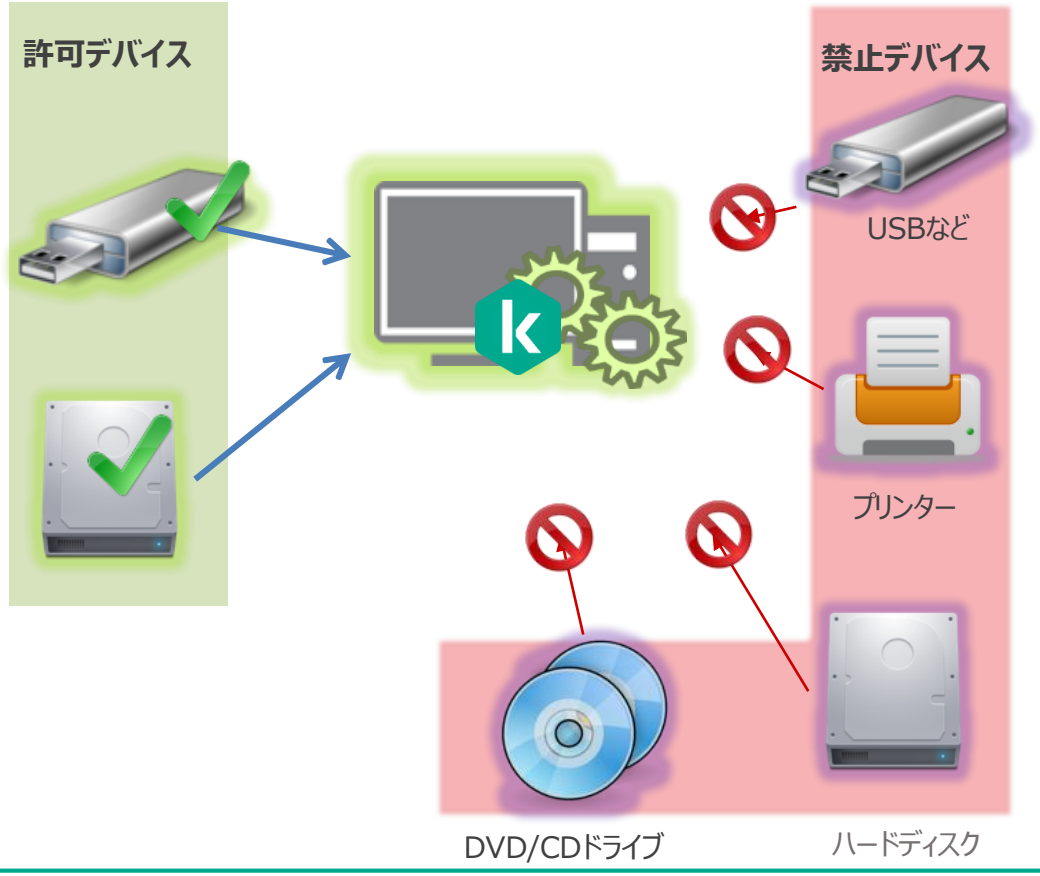
名前	重要度	製造元	アプリケーションファミリー	アプリケーション	修正が必要	修正済み	パッチが適用済み
KLA10773	中	Apple	Apple Software Update	Apple Software Update 2.x	1	0	0
KLA10457	緊急	Adobe Systems	Adobe Reader X	Adobe Reader X 10.x	1	0	0
KLA10682	緊急	Adobe Systems	Adobe Reader X	Adobe Reader X 10.x	1	0	0
KLA10575	緊急	Adobe Systems	Adobe Reader X	Adobe Reader X 10.x	1	0	0
KLA10120	緊急	Mozilla Foundation	Mozilla Firefox	Mozilla Firefox 19.x	1	0	0
KLA10525	高	Mozilla Foundation	Mozilla Firefox	Mozilla Firefox 19.x	1	0	0
KLA10531	中	Mozilla Foundation	Mozilla Firefox	Mozilla Firefox 19.x	1	0	0
KLA10659	高	Microsoft	Windows 7		1	0	0
KLA10735	高	Microsoft	Windows 7		7	0	0

kaspersky

デバイスコントロール

多機能

- ✓ USBメモリや外付けHDDなど、外部デバイスの接続を制御
- ✓ 許可デバイス、シリアルの登録や、Windowsログインユーザー単位の制御など、細かいコントロールが可能



特長

- 外部デバイスの接続を制御
- 書き込み/読み込みの制御も可能
- ログインユーザー毎の制御が可能
- シンクライアントのデバイス制御にも利用可能

ログインユーザー毎のポリシー設定

管理者としてログイン

外部ドライブの読み書きを許可

一般ユーザーとしてログイン

外部ドライブの書き込みを禁止

アプリケーションコントロール

多機能

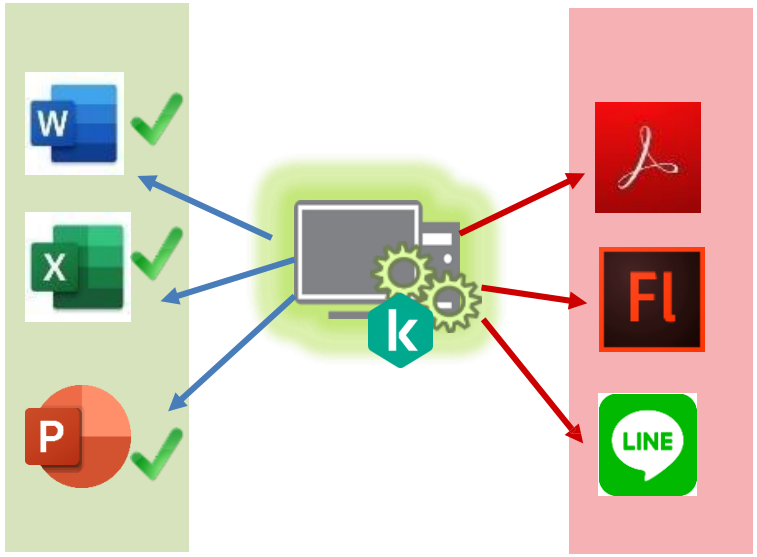
- ✓ 起動可否をアプリケーションごとに制御できる機能
- ✓ ブラックリスト形式・ホワイトリスト形式の両方に対応

[ブラックリスト方式]
起動を禁止するアプリケーションを登録

[ホワイトリスト方式]
起動を許可するアプリケーションのみを登録
デフォルトではOSとOS付随のアプリケーションのみ起動が許可

許可されたアプリ

禁止されたアプリ



ログインユーザー毎の制御が可能

例

管理者：すべてのアプリケーションの起動が可能

一般　：許可されたアプリケーションのみ起動が可能

ウェブコントロール

多機能

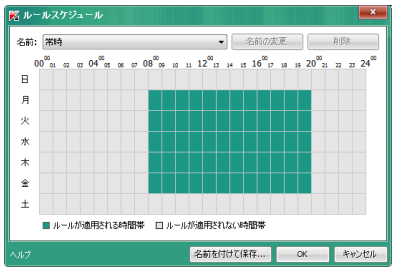
- ✓ ウェブアクセスをコンテンツ毎に制御 (コンテンツフィルタ機能)
- ✓ スケジュール設定、ホワイトリストの登録、ログインユーザー毎の制御も可能

特長

- ➢ ウェブコンテンツによるフィルタリングが可能
- ➢ コンテンツのカテゴリは
  - -アダルトサイト
  - -ギャンブルサイト
  - -SNS
  - -チャット、フォーラム(掲示板)
  - -ウェブメール
  - -クレジットカード決済

など・・・

- ➢ ホワイトリストの登録も可能。
- ➢ ポリシーの適用時間帯を設定することが可能。
  (例：業務時間帯→適用、時間外→非適用)
- ➢ ログインユーザー毎のポリシー設定が可能。



Point!

・ルールの**スケジュール設定**が可能です。
例：業務時間帯→ルール適用
業務時間外→ルール非適用

kaspersky

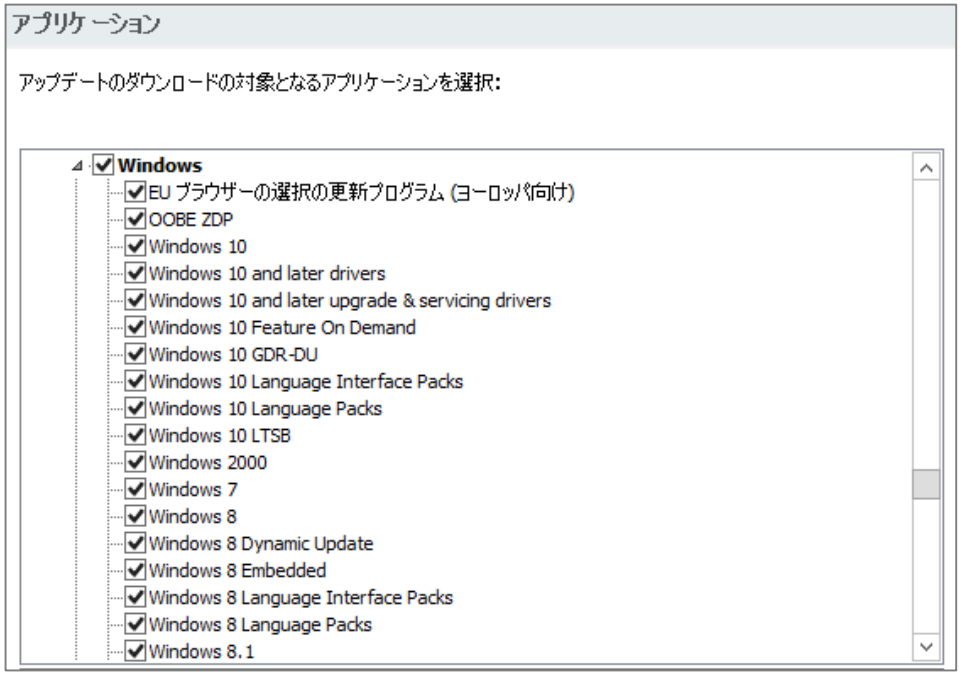
パッチ管理機能・データ暗号化

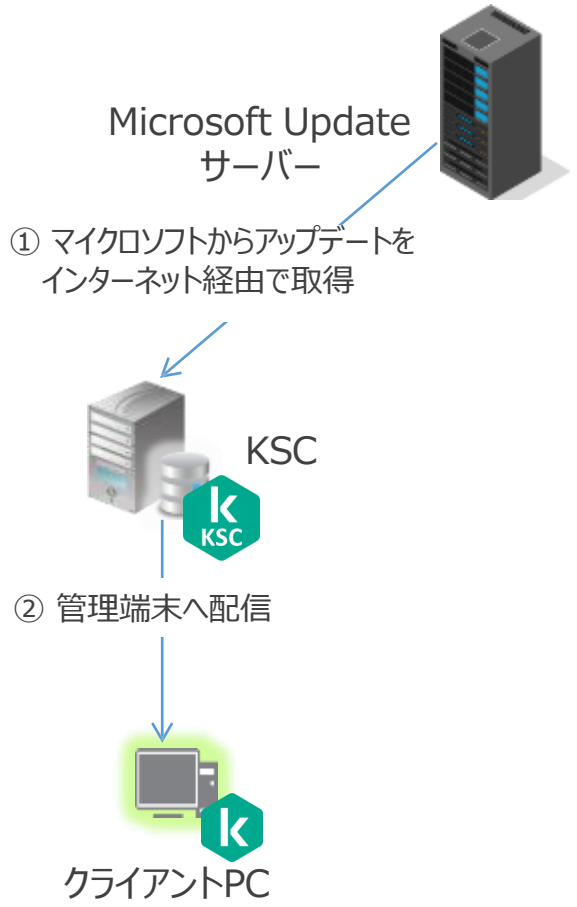
～Advancedで追加される機能～

パッチ配信 – Microsoftのアプリケーション

多機能

✓ KSCからMicrosoft製品のアップデートを配布





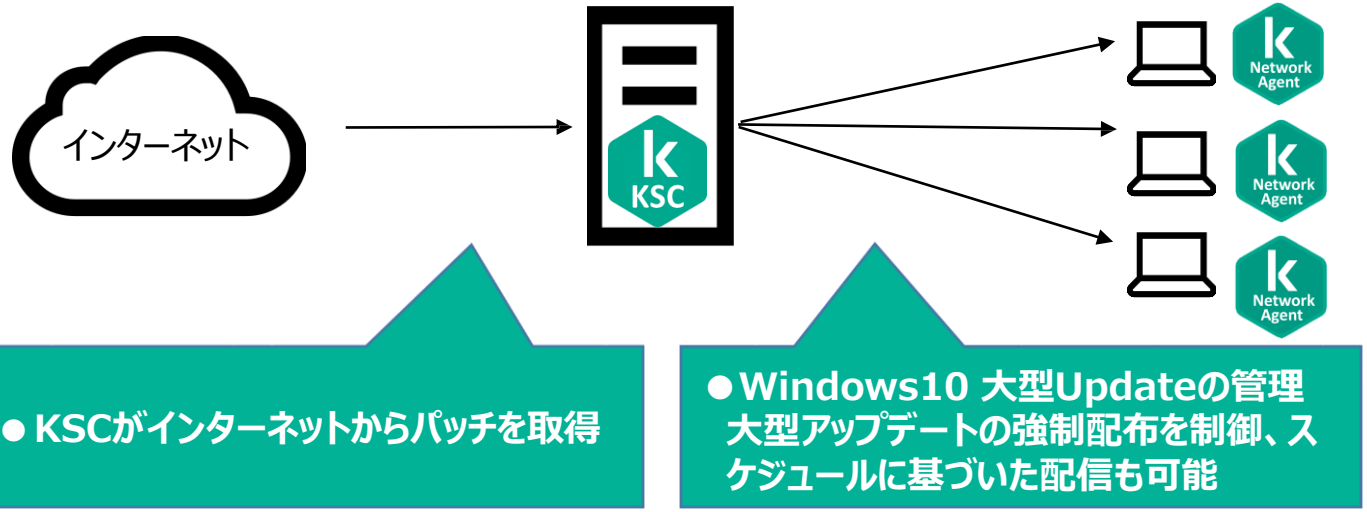
- WSUS 単体ではクライアントへの配信スケジュールを設定できないが KSCの「タスク」機能により可能となります
- ワークグループ環境におけるクライアントのレジストリ設定は不要

kaspersky

パッチ管理（Windows10,11大型アップデート対応）

多機能

✓ 大型アップデート制御のイメージ



お客様状況により様々なパターンに対応

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。
ADの構築、WSUSサーバの構築などが不要なため、簡単にセキュリティ課題を解決可能。

構築済みのWSUSサーバーを使用する
KSCが管理下のコンピューターに対し、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） からパッチを取得する様、指示を出すパターン。配信スケジュールの設定、柔軟なグループ分けによりネットワーク不可の軽減などを補助します。

kaspersky

パッチ配信　– サードパーティのアプリケーション

多機能

✓ 脆弱性が報告されている主要なアプリケーションをカバー

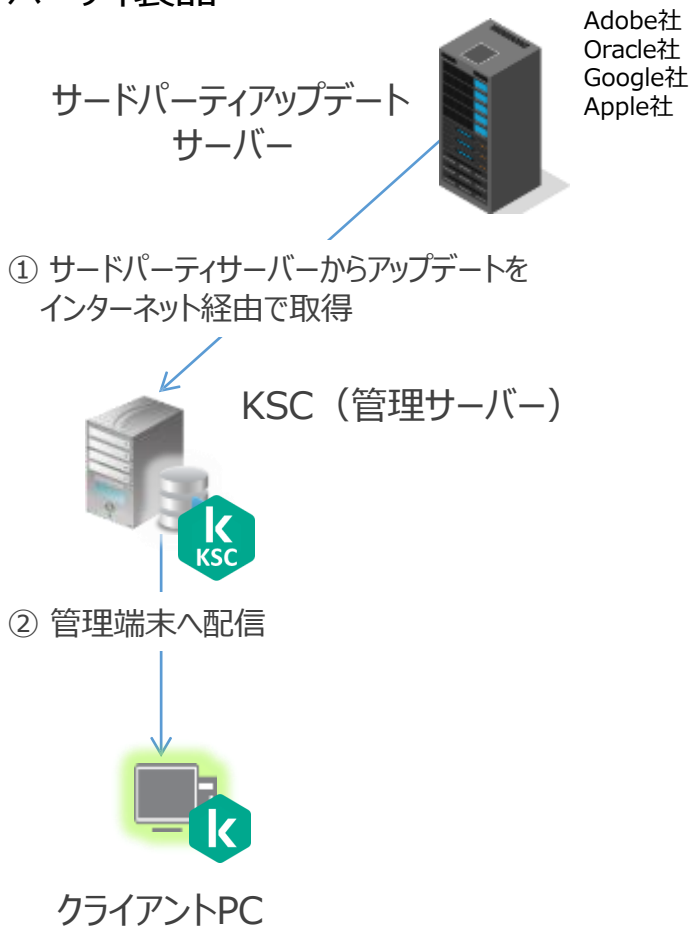
KSCからAdobe社・Oracle社・Google社・Apple社など、サードパーティ製品
80社以上150種類以上のアップデートを配布。

アプリケーション

アップデートのインストールの対象となるアプリケーションを選択

- すべての製品
  - 7-Zip Developers
  - Acro Software Inc
  - Adobe Systems
    - Adobe Acrobat DC Classic
    - Adobe Acrobat DC Continuous
    - Adobe Acrobat Reader DC Classic
    - Adobe Acrobat Reader DC Continuous
    - Adobe Acrobat X
    - Adobe Acrobat XI
    - Adobe AIR
    - Adobe Flash Player ActiveX
    - Adobe Flash Player NPAPI
    - Adobe Flash Player PPAPI
    - Adobe Photoshop CS5
    - Adobe Reader
    - Adobe Reader X
    - Adobe Reader XI
    - Adobe Shockwave Player
    - Adobe Shockwave Player (MSI installation)
  - Google
  - ImgBurn Developers
  - IrfanView
  - LightScribe
  - LogMeIn, Inc.
  - Martin Prikryl
  - Matthew T. Ashland
  - Microsoft
  - Mozilla Foundation
  - Nullsoft
  - OpenOffice.org
  - Opera Software
  - Oracle Corporation
  - PDF Complete Inc
  - pdfforge GbR
  - Piriform
  - Postgresql
  - RealNetworks
  - RealVNC
  - Right Hemisphere Inc.

※ 上記は対応アプリケーションの一部です
リストにないアプリケーションに関しては、別途アプリ提供元WEBサイトなどから
インストールパッケージを取得し、リモートインストール機能でパッチ適用可能。

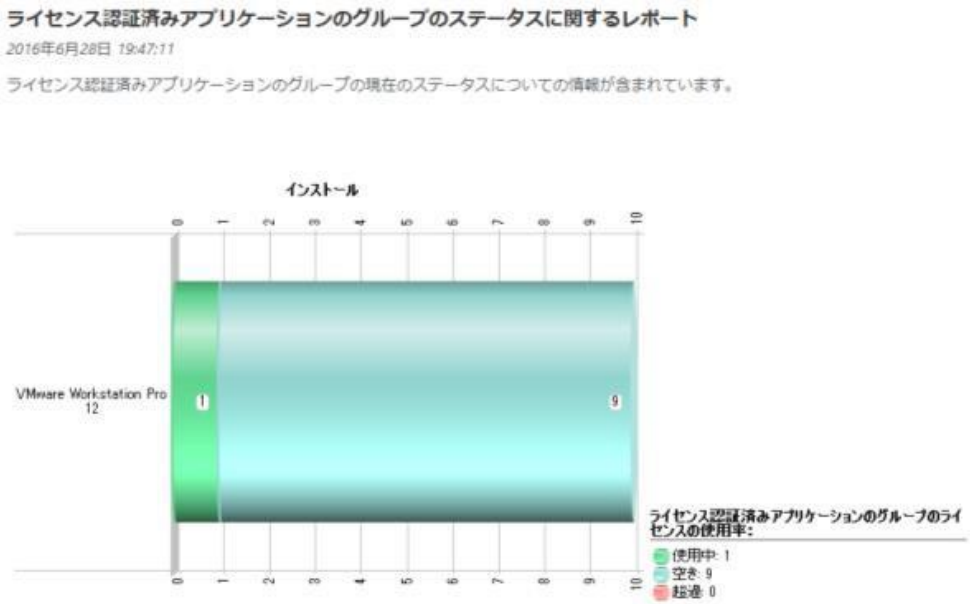


kaspersky

ソフトウェアライセンス管理

多機能

✓ アプリケーションのライセンス管理が可能



サマリー:

名前	種別	上限	インストール	使用率ステータス
VMware Workstation Pro 12	ライセンスの制限を監視する	10	1	使用頻度の低いライセンス

上限を超過しているグループ: 0　上限に到達したグループ: 0　ライセンスの使用頻度が低いグループ: 1

詳細 1 件(1 件中)

名前	種別	アプリケーション	バージョン	製造元	仮想サーバー	グループ名	コンピューター名	IP アドレス	前回の可視	前回の接続
VMware Workstation Pro 12	ライセンスの制限を監視する	VMware Workstation	12.1.0	VMware, Inc.		管理対象コンピューター	SERVER203	127.0.0.1	2016年6月28日 19:46:18	2016年6月28日 19:44:42

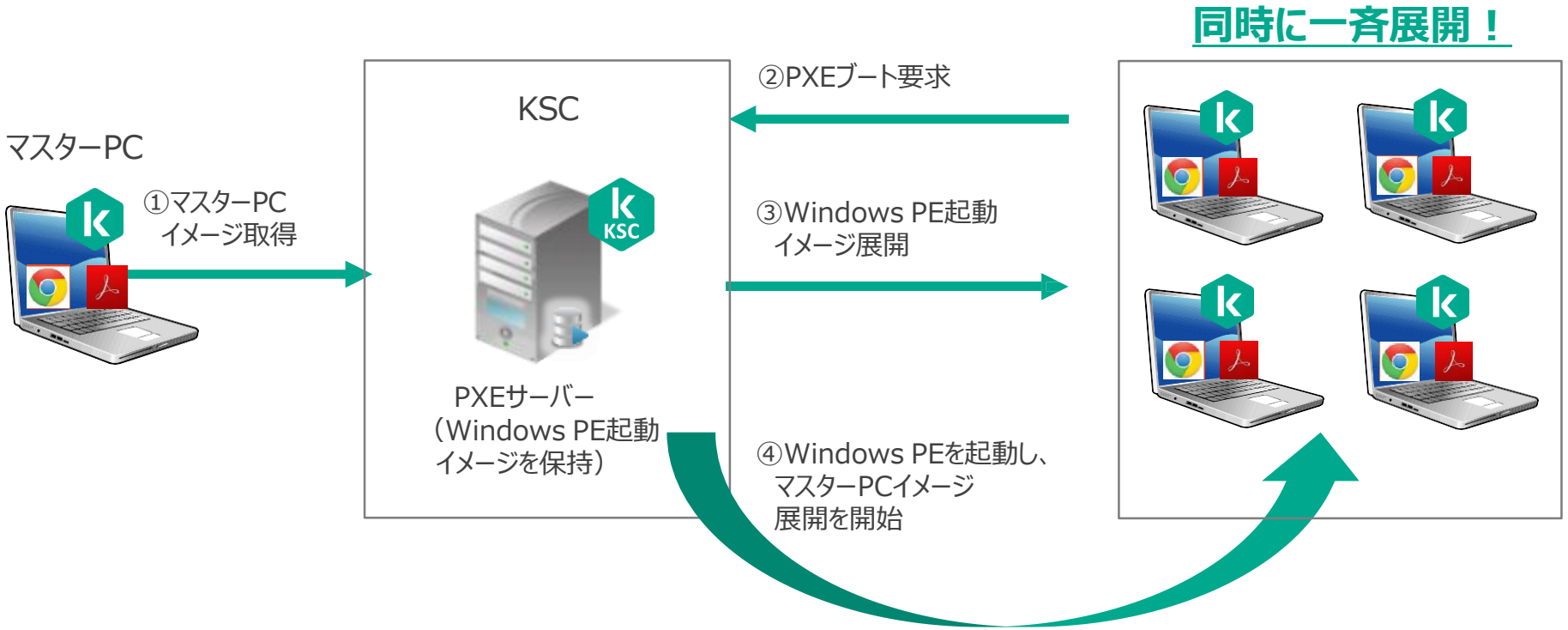
- 管理端末にインストールされているアプリケーション情報をもとに管理
- アプリケーションごとに「使用中」「空き」」「超過ライセンス数」を表示
- 管理対象アプリケーションとライセンス数量を設定し超過がないかチェック
  （超過時のアラートメールも設定可能）

kaspersky

OSイメージ管理

多機能

- ✓ マスターPCのOSイメージを他PCに複製しセットアップする機能
- ✓ 作成したイメージをネットワーク経由で一斉展開が可能



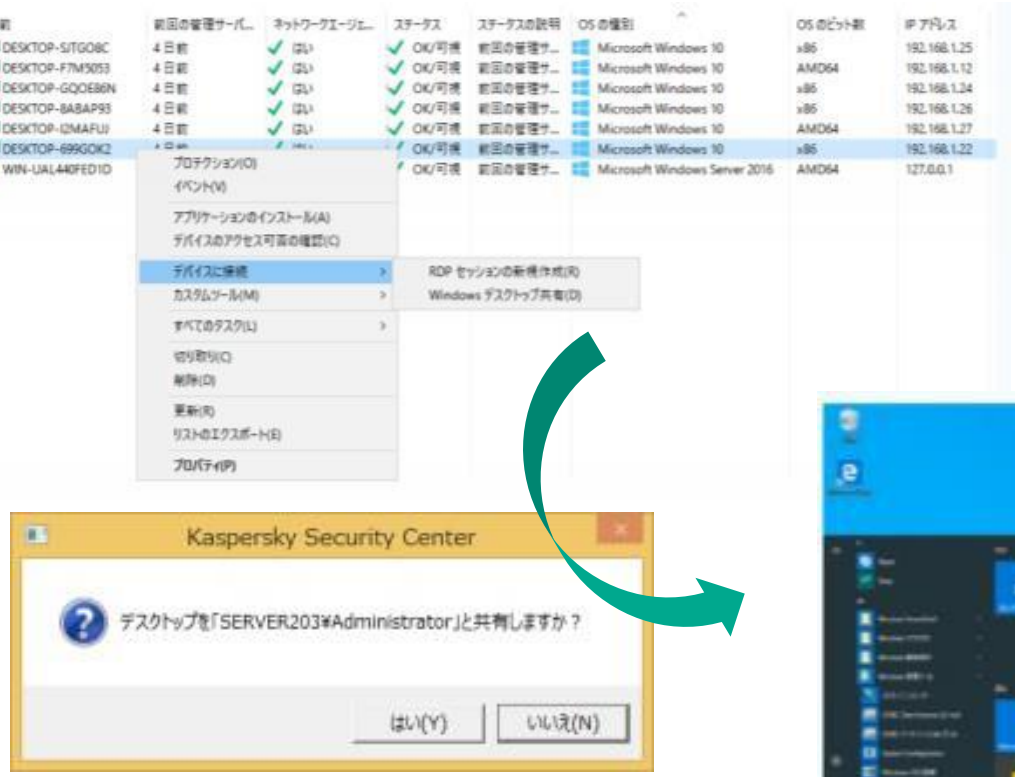
※ Windows PEとは
⇒ CDメディアやネットワークブートが容易に可能な軽量なWindows OSです。
Windows PEをブートさせ、その上でマスターイメージ展開が行われます。

kaspersky

デスクトップ共有

多機能

✓ Kaspersky Security Center 上の端末一覧から、接続する端末を選択



遠隔操作サポート（ヘルプデスク業務）

- Windows標準のRDP（リモートデスクトップ）とは異なり、ログオンユーザーが操作している画面を共有し、操作が可能
- ウイルス感染時など、ユーザーが行った操作をヒアリングしながら、インシデント対応が必要な際などに役立つ機能

kaspersky

データ暗号化

多機能

✓ データ暗号化により重要な情報の漏えいを防止し、ビジネスを守る

➢ Windows　BitLocker、MAC FileVaultの一元管理

- ADの構築無しでパスワードポリシーの設定などの一元管理が可能
- 管理サーバー（KSC）ポリシーによるリモートでの暗号化・複合化の実行
- 管理対象端末の暗号化ステータス監視

➢ ディスク暗号化

- PCの盗難／紛失時でも、ディスクからの情報漏洩を防止
- OSが起動前のプリブート認証で、第三者によるPC起動も防止

➢ ファイル暗号化

- 指定した拡張子やフォルダー単位で暗号化
- アプリケーションの実行ファイルを指定することで、そのアプリケーションが作成するファイルを自動で暗号化

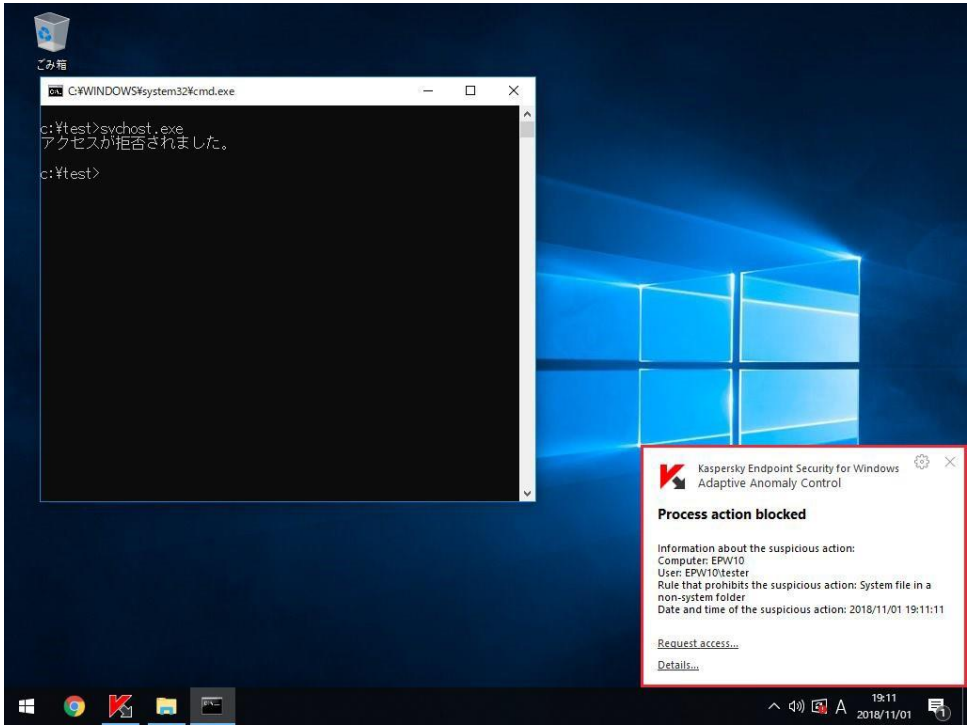
➢ リムーバブルドライブの暗号化（USBメモリーなど）

- ドライブ全体の暗号化、もしくはファイル単位の暗号化のいずれかを有効にして使用
- ポータブルモードを設定すると、暗号化した状態で外部にファイルを持ち出し可能

アダプティブアノマリーコントロール

多機能

✓ エンドポイントにとって一般的でない、潜在的に危険な動作を監視しブロックする機能



システムディレクトリ以外の場所にあるダミーのシステムファイルと同名のファイル（svchost.exe）を起動しようとすると不審な動作としてブロックされる

潜在的に危険な動作の一例

- 難読化されたPowerShellコードの実行
- スクリプトからネィティブAPIのコール
- システムディレクトリ以外に配置されているシステムファイルと同名ファイルの起動
- Officeアプリケーションからスクリプトのキック
- WMI経由でリモートからWindowsツール（mshta.exe, powershell等）の開始

これらをブロックするためのルールが提供される。ルールは定義DBにより更新、最新の悪用テクニックに対応

kaspersky

KESB　ライセンス別　Windowsの機能一覧

機能	Kaspersky Endpoint Security for Business			
	Select		Advanced	
	クライアントOS	サーバーOS	クライアントOS	サーバーOS
Kaspersky Security Network（KSN）	●	●	●	●
ふるまい検知	●	●	●	●
脆弱性攻撃ブロック	●	●	●	●
ホスト侵入防止	●	ー	●	ー
修復エンジン（ロールバック）	●	●	●	●
ファイル脅威対策	●	●	●	●
ウェブ脅威対策	●	ー	●	●
メール脅威対策	●	ー	●	●
ネットワーク脅威対策	●	●	●	●
ファイアウォール	●	●	●	●
有害USB攻撃ブロック	●	●	●	●
暗号化された接続のスキャン	●	●	●	●
アプリケーションコントロール	●	ー	●	●
デバイスコントロール	●	ー	●	●
ウェブコントロール	●	ー	●	●
AMSI 保護プロバイダー	●	●	●	●
アダプティブアノマリーコントロール	ー	ー	●	ー
ディスク全体の暗号化（Bitlocker）	ー	ー	●	●
OSイメージ管理	ー	ー	●	ー
デスクトップ共有	ー	ー	●	ー
リモートデータ消去	●	●	●	●
脆弱性管理（パッチ配信）	ー	ー	●	●

kaspersky

Thank you!

kaspersky.com