Kaspersky Endpoint Security for Businessのご紹介

V4.0

2023年6月16日

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

Kaspersky Endpoint Security for Business とは

- Kaspersky Endpoint Security for Businessは、
  Windows、Mac、Linux、mobileなどを保護する統合的なセキュリティ製品です。

  製品名（ライセンス名称）
  Kaspersky Endpoint Security for Business

  使用可能なアプリケーション名
  Kaspersky Endpoint Security for Windows
  Kaspersky Endpoint Security for Mac
  Kaspersky Endpoint Security for Linux　など

- Kaspersky Endpoint Security for Business には、
  SelectとAdvancedの2つのライセンスがあり、使用出来る機能が異なります。

Kaspersky Endpoint Security for Business とは

アプリケーションの主な特徴

Kaspersky Endpoint Security for Windows

ふるまい検知、マルウェアによる操作の修復（ロールバックエンジン）、機械学習エンジン、アノマリー検知（異常検知）など先進的かつ高度な防御機能と、デバイスコントロール、アプリケーション起動コントロール、Webコンテンツフィルタリングなどを備えた、統合エンドポイントセキュリティ。

Kaspersky Endpoint Security for Mac

ファイルアンチウイルスだけでなく、Web脅威対策、ネットワーク脅威対策、Webコンテンツフィルタリングなどを備えた、法人向け統合エンドポイントセキュリティ。
管理サーバーによる集中管理が可能。

Kaspersky Endpoint Security for Linux

ファイルアンチウイルスだけでなく、Web脅威対策、ネットワーク脅威対策などを実装。
デバイスコントロール、ファイアウォール管理、ファイル共有に置かれたファイルの暗号化攻撃を防ぐアンチクリプターなども備えた高度なアプリケーションです。

Kaspersky Endpoint Security for Business とは

アプリケーションの主な特徴

Kaspersky Security for Mobile

- Kaspersky Endpoint Security for Android
  Android向けに、アンチウイルス機能、アプリケーションコントロールが可能。

- Kaspersky Endpoint Security for iOS
  iOS/iPadOS向けに、KSNを使用した危険サイトブロック、ジェイルブレイクの検知を提供。

- Mobile Device Management
  Android、 iOS/iPAD OS向けに、MDM機能を提供。

＊＊Kaspersky Endpoint Security for iOSを使用するには、KSC 14 以降WebコンソールかKSC CCが必要です。
＊＊Mobile Device Managementの機能には、KSC14 MMCコンソールでのみサポートされる機能があります。

詳しくはヘルプをご参照ください。
https://support.kaspersky.com/KESMob/10SP4MR3/ja-JP/216976.htm

SelectとAdvanced の比較

使用出来るアプリケーション・機能	Kaspersky Endpoint Security for Business	
	Select	Advanced
Kaspersky Endpoint Security for Windows	●	●
Kaspersky Endpoint Security for Mac	●	●
Kaspersky Endpoint Security for Linux	●	●
Kaspersky Endpoint Security for Android	●	●
Kaspersky Endpoint Security for iOS	●	●
Mobile Device Management	●	●
SIEMサポート	Syslogサポート	SIEM連携
暗号化	―	●
脆弱性管理（KVPM機能相当）	―	●
OS デプロイ	―	●

それぞれのアプリケーションで、Selectで使用出来る機能、Advancedで使用出来る機能の差異もあります。
詳細はそれぞれのアプリケーションの資料でご確認ください。

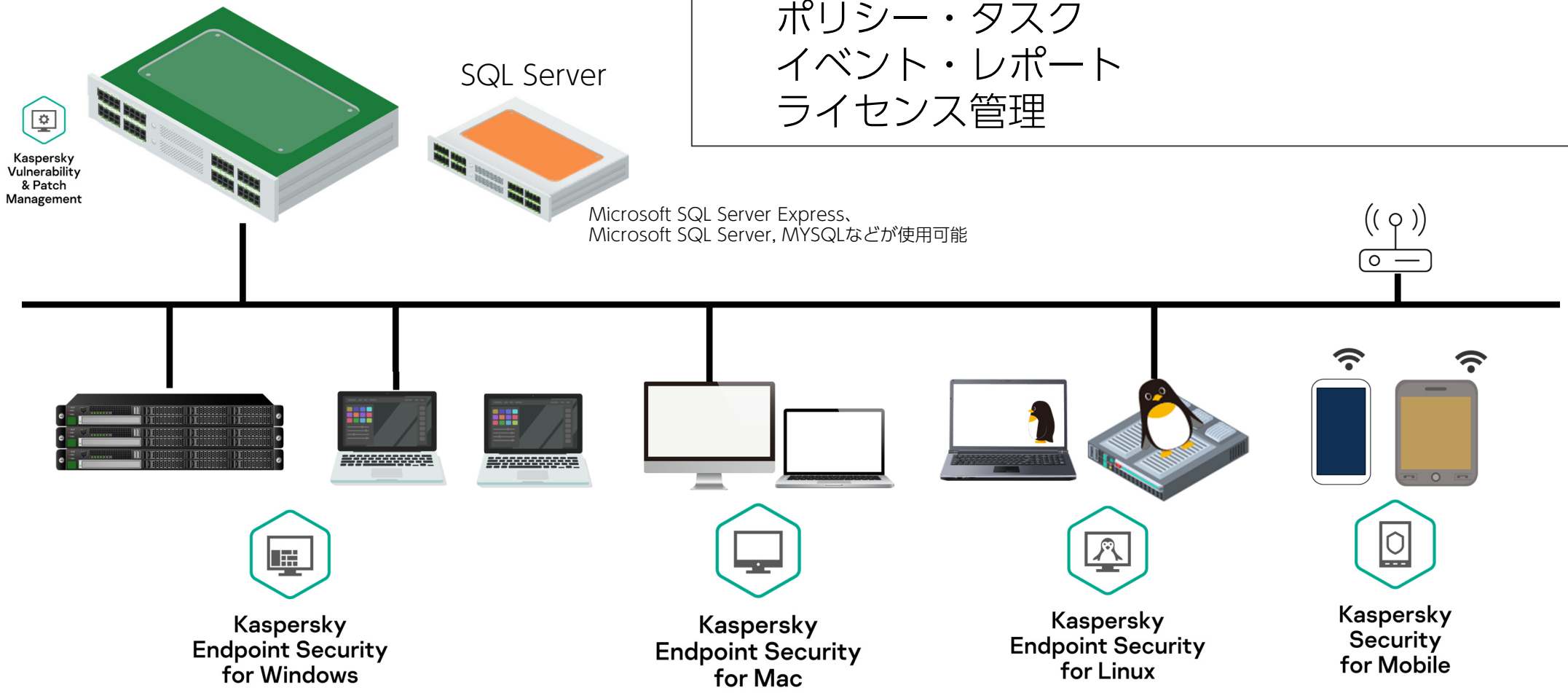
構成について

kaspersky

Kaspersky Endpoint Security for Businessの基本構成

Kaspersky Security Center
(管理サーバー)

Kaspersky Security Centerによる集中管理を提供
様々なアプリケーション、デバイスを管理
- ポリシー・タスク
- イベント・レポート
- ライセンス管理



kaspersky

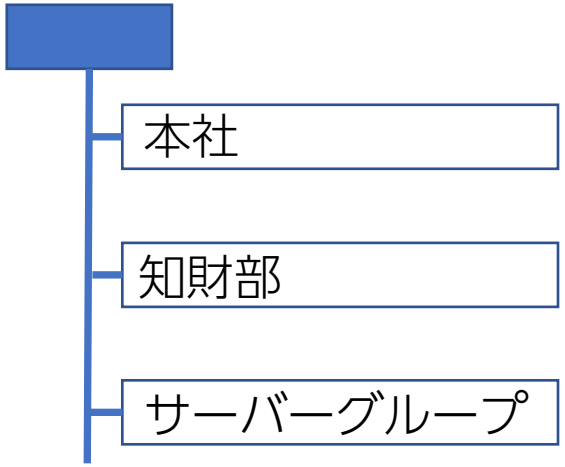
Kaspersky Endpoint Security for Businessの基本構成

Kaspersky Security Center（KSC）
グループ/ポリシー・タスクによる管理

グループを作成することにより、階層化管理が可能。

グループに対し、ポリシー・タスクを適用。

- ✓ ポリシーとは、常時の設定を行うもの。
  リアルタイムスキャンの設定など。
- ✓ タスクとは、一時またはスケジュール実行する処理。
  スケジュールスキャン、定義更新など。

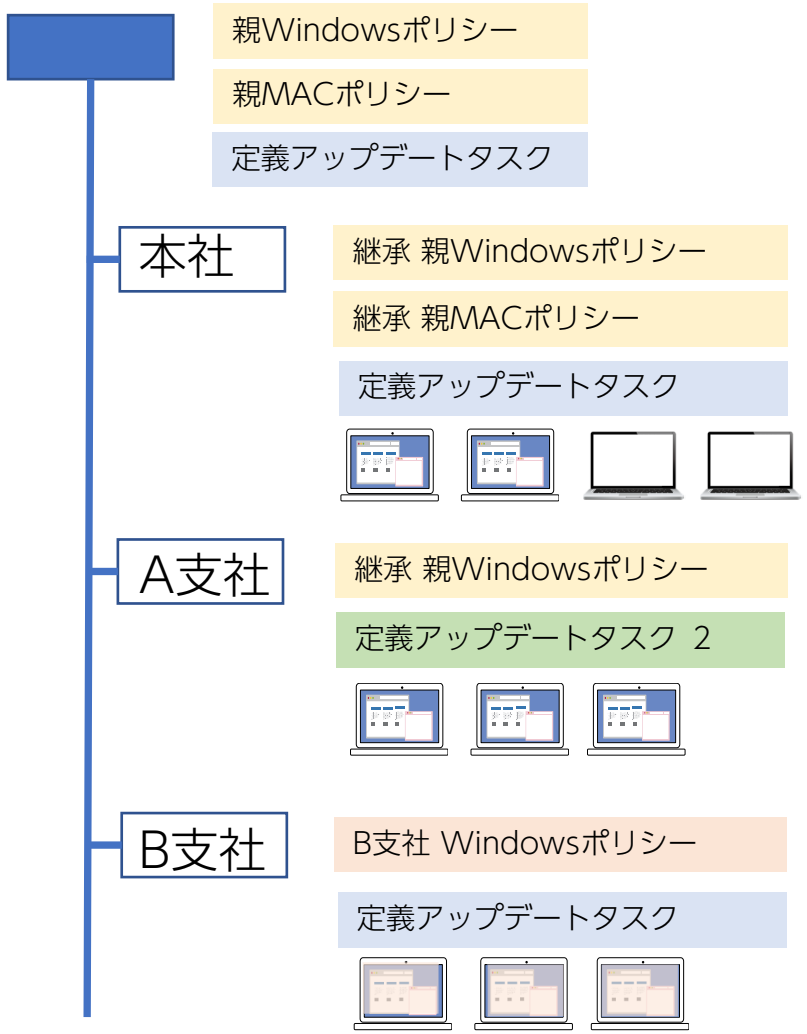


設計例
- 単一グループで運用する
- ロケーションでグループ作成する
- 設定変更したい単位でグループを作成する

Kaspersky Endpoint Security for Businessの基本構成

Kaspersky Security Center（KSC）
グループ/ポリシー・タスクによる管理

例 1



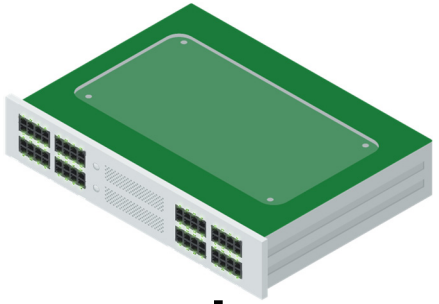
- グループには、Windows、MAC、LINUXなど混在可能。
- グループでポリシーを作成しなければ、上位ポリシーが継承される

- グループでタスクを作成し、上位タスク継承を無効化するとタスクが置き換え出来る。

- グループでポリシーを作成すると、そのポリシーが有効になる。

Kaspersky Security Center がサポートする、その他のアプリケーション

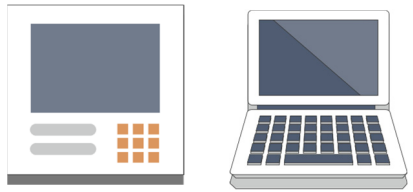
Kaspersky Security Center
(管理サーバー)



Kaspersky Security Centerでは、
Kaspersky Endpoint Security for Business以外の
製品も管理することができます。
＊ 製品詳細は、各製品資料でご確認ください。

Kaspersky Hybrid Cloud Security
Kaspersky Security for Virtualization

Kaspersky Security For Storage



Kaspersky Embedded Systems Security

別途ライセンスが必要です。

Kaspersky Security Center（KSC)

製品に付属する管理サーバー。KSCのライセンス費用は不要。
Windowsプラットフォームをサポート。
小規模から大規模環境までサポート。

プライマリー・セカンダリー構成により、他拠点・大規模構成が可能。
子会社・MSPでの管理に最適な仮想管理サーバー機能。

- 仮想管理サーバーが有効なケース
  - ✓ 管理サーバー用マシンは最小にしたいが、子会社ごとに管理は独立させたい。
  - ✓ 子会社ポリシーに制限をかけたい。
  - ✓ マネージドサービスプロバイダー

構成に柔軟性を持たせる機能を追加費用無しで使用可能。
ディストリビューションポイント
接続ゲートウェイ

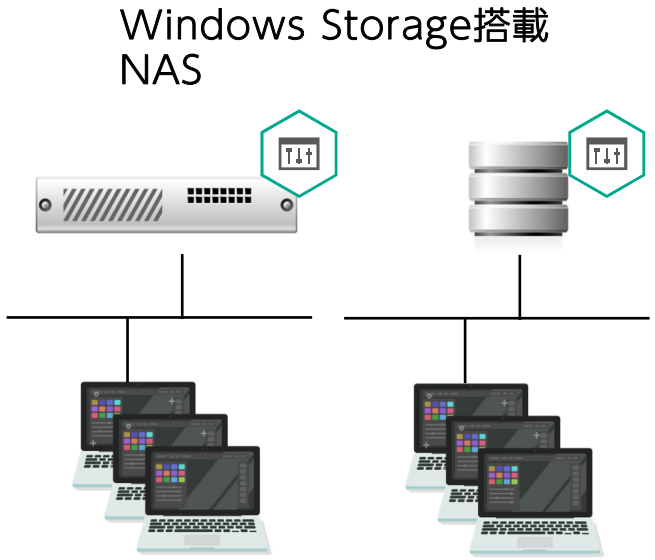
Smallユーザー、SOHOでの構成

① スタンドアロンでの使用も可能

KSC管理時と同一アプリケーションを使用。
法人向け製品のため、細かな設定が可能。

② 小規模環境向けKSCの構築

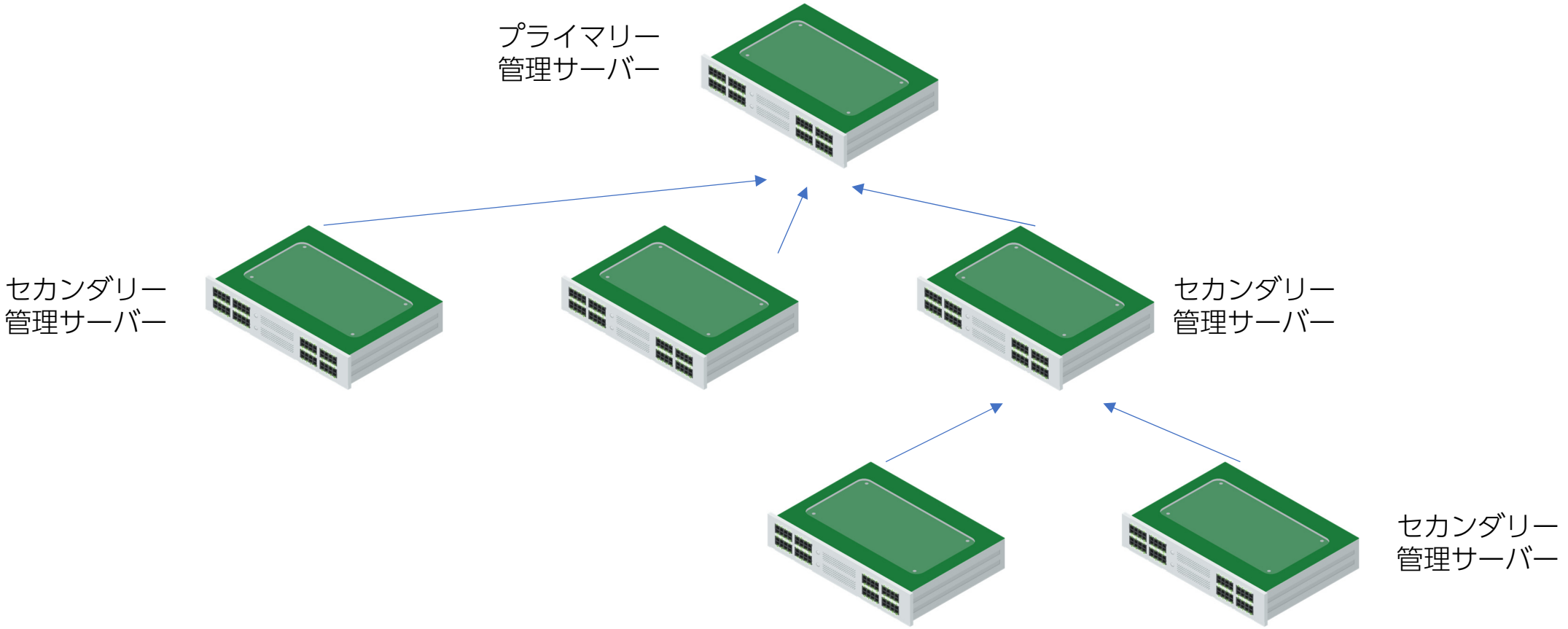
KSCは、Windows Storage Server等も使用可能



Kaspersky Security Center　大規模向け構成

プライマリー・セカンダリー構成

セカンダリーサーバーのレポートを
プライマリーサーバーに集約することが出来ます。



Kaspersky Security Center　仮想管理サーバー

項目01　AAAAA

項目02　FFFFF

項目03　PPPPP

管理サーバー

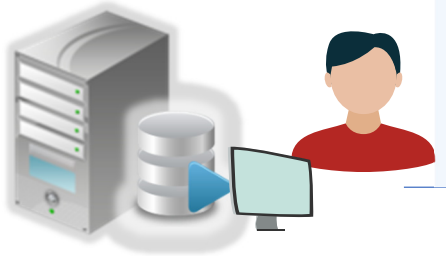
管理サーバーの中に、仮想管理サーバーを作成し、複数の管理サーバー機能を持たせることが出来ます。

仮想管理サーバー（論理）

項目01　AAAAA

項目02　GGGGG

項目03　QQQQQ



項目01　AAAAA

項目02　GGGGG

項目03　SSSSS

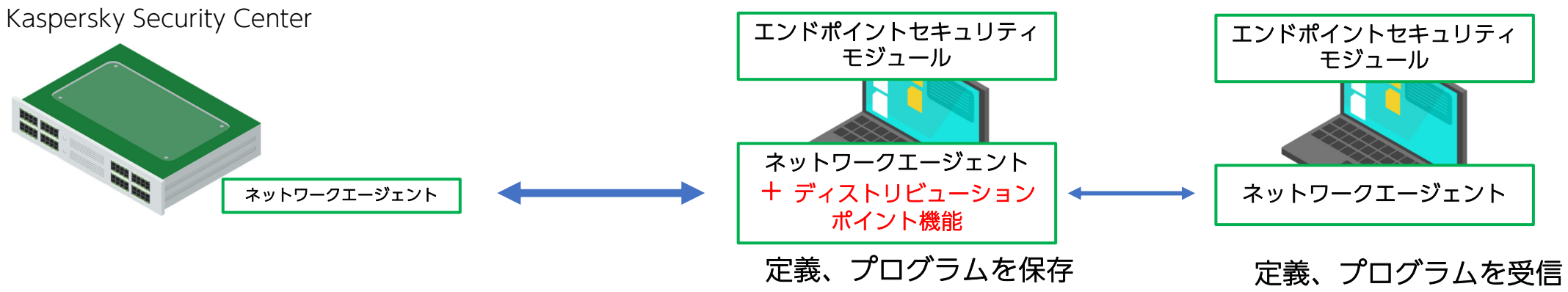
ポリシー設定
親管理サーバーでロックされた項目は、
仮想管理サーバーでは変更できない。
ロックされていない項目は設定可能となる。
統制と柔軟性を両立。

管理者を仮想管理サーバ向けに作成。
仮想管理サーバにはアクセス権を設定、
管理者は割り当てられた仮想管理サーバーにのみ、アクセスできる。

Kaspersky Security Center　ディストリビューションポイント

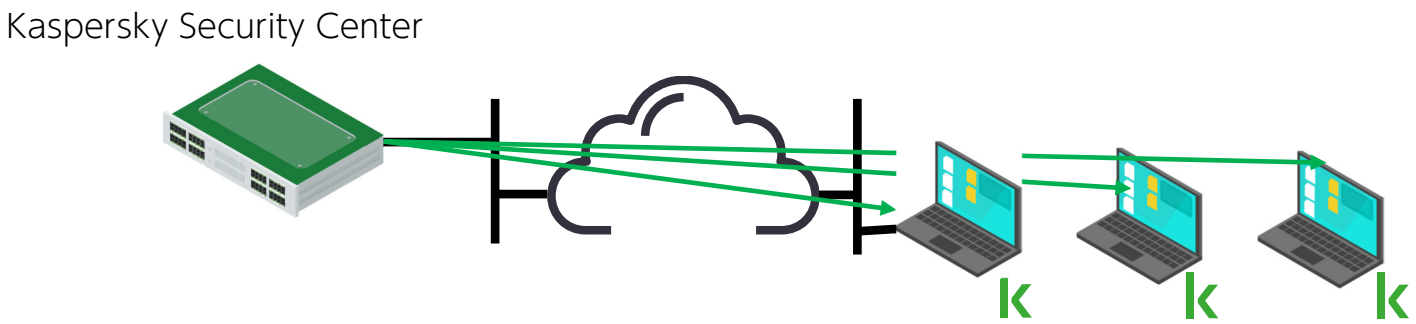
ディストリビューションポイントとは

ディストリビューションポイントは、通信部分にKSCの
代理機能を持たせ、パフォーマンス向上を図る機能です。



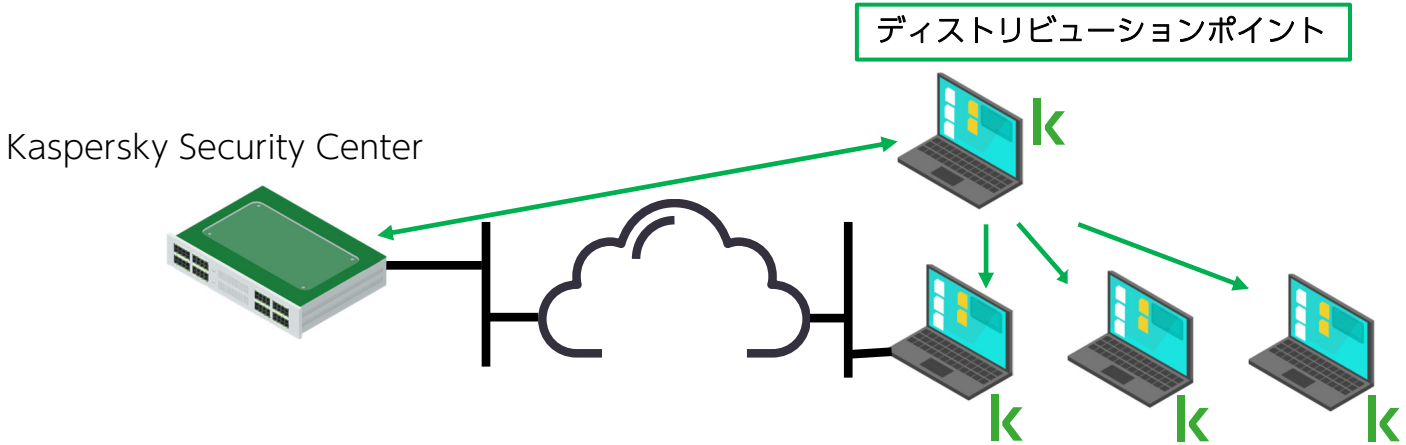
＊＊エンドポイントセキュリティ製品は、
セキュリティ部分と通信部分に分かれています。

Kaspersky Security Center　ディストリビューションポイント



ディストリビューションポイントがない場合

拠点の各端末は、KSCと直接通信を行う。規模によっては、ネットワークトラフィック、KSCの負荷が懸念される。

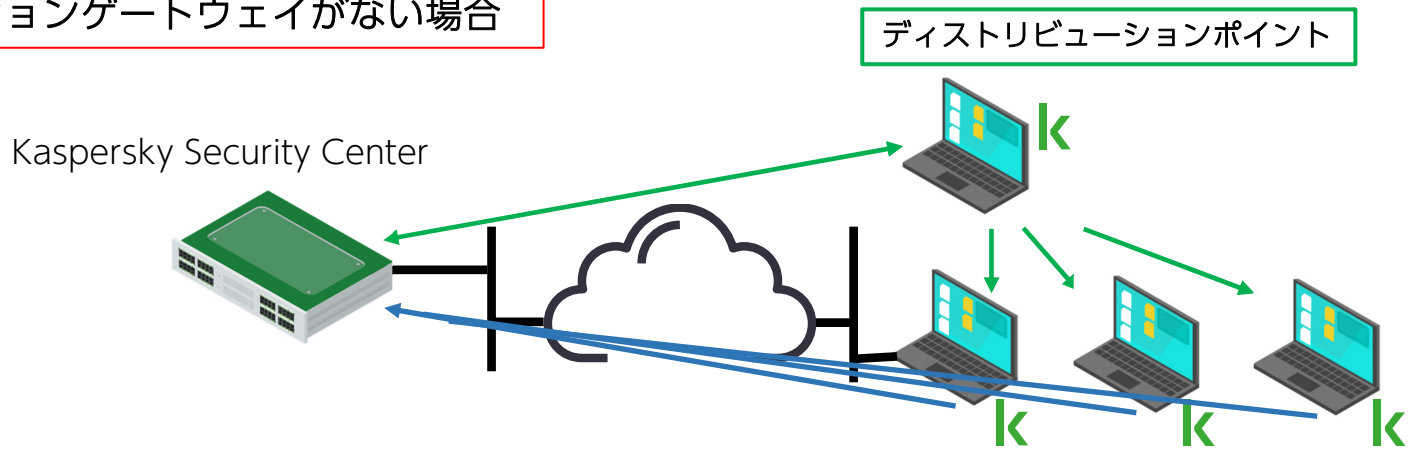


拠点にディストリビューションポイントを設定

拠点の各端末は、ディストリビューションポイントから、定義やインストールプログラム、更新プログラムをダウンロード。
脆弱性管理機能においては、パッチ配信でも使用する。

Kaspersky Security Center　ディストリビューションポイントとコネクションゲートウェイ

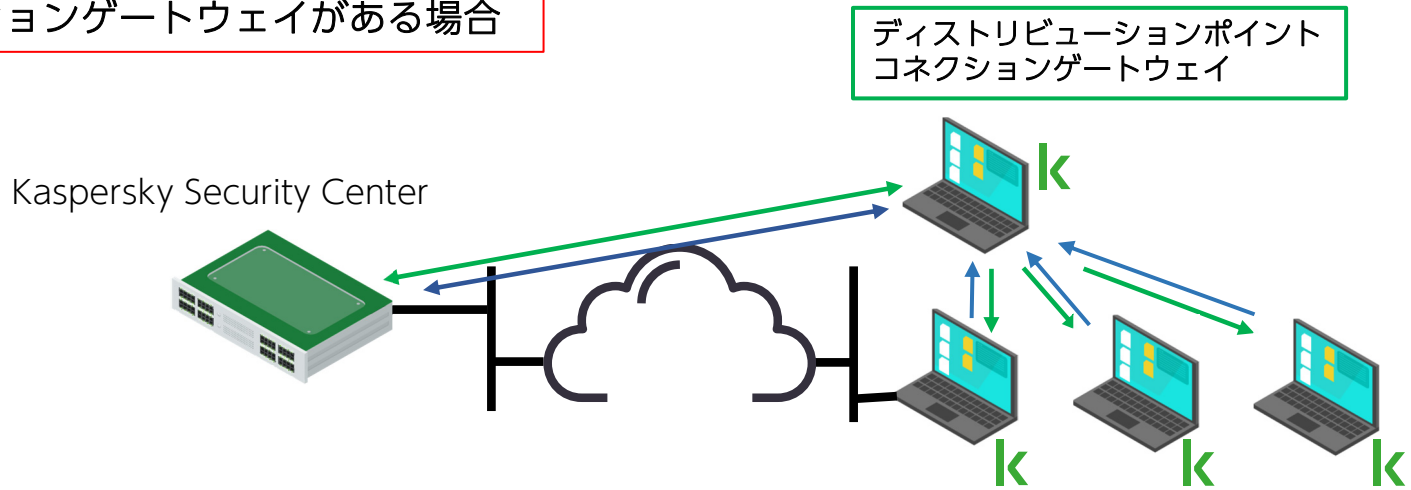
コネクションゲートウェイがない場合



ディストリビューションポイントは、定義、プログラムなど、配信をKSCの代理で行う仕組みです。
（緑矢印 ←）

各クライアントは、KSCとの疎通、ログのアップロードはKSCと直接行います。
（青矢印 ← ）

コネクションゲートウェイがある場合



各クライアントは、KSCとの疎通、ログのアップロードをディストリビューションポイント端末を通じて行います。
（青矢印 ← ）

通じて行います。

Kaspersky Security Center　Windows版 と Linux版の違い

機能	Windows版	Linux版
KSN プロキシ	○	○
管理コンソールの種別	MMCおよびWebコンソール	Webコンソール
Windows、macOS、Linux 管理対象デバイスの保護	○	(Linux および Windows デバイスの保護のみ)
モバイルデバイスの保護	○	×
仮想マシンの保護	○	×
パブリッククラウドインフラストラクチャの保護	○	×
ポリシー、タスク	○	○
サードパーティ製ソフトウェアのアップデートインストールと脆弱性の修正	○	リモートインストールのみ
管理サーバーの WSUS サーバーとしての使用	○	×
クライアントデバイスのデスクトップへのリモート接続	○	×
カスペルスキー製品の自動アップデート	○	×
アダプティブアノマリーコントロールのサポート	○	×
Kaspersky Managed Detection and Response との統合	○	×

詳しくはオンラインヘルプをご確認ください。

Kaspersky Security Center Windows 14.2の強化

使用出来るデータベースが強化されました。
詳しくはシステム要件をご確認ください。

- Microsoft SQL
- PostgreSQL 13.x 64 ビット
- PostgreSQL 14.x 64 ビット
- Amazon RDS と Microsoft Azure のクラウドプラットフォームでサポートされる
  すべての SQL Server

など。

Kaspersky Security Center Windows 14.2 変更点

Windows クライアントOSはKSCの稼働プラットフォームとしてサポートされません。

https://support.kaspersky.com/KSC/14.2/ja-JP/242037.htm

kaspersky

レポート・IT資産管理機能

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）

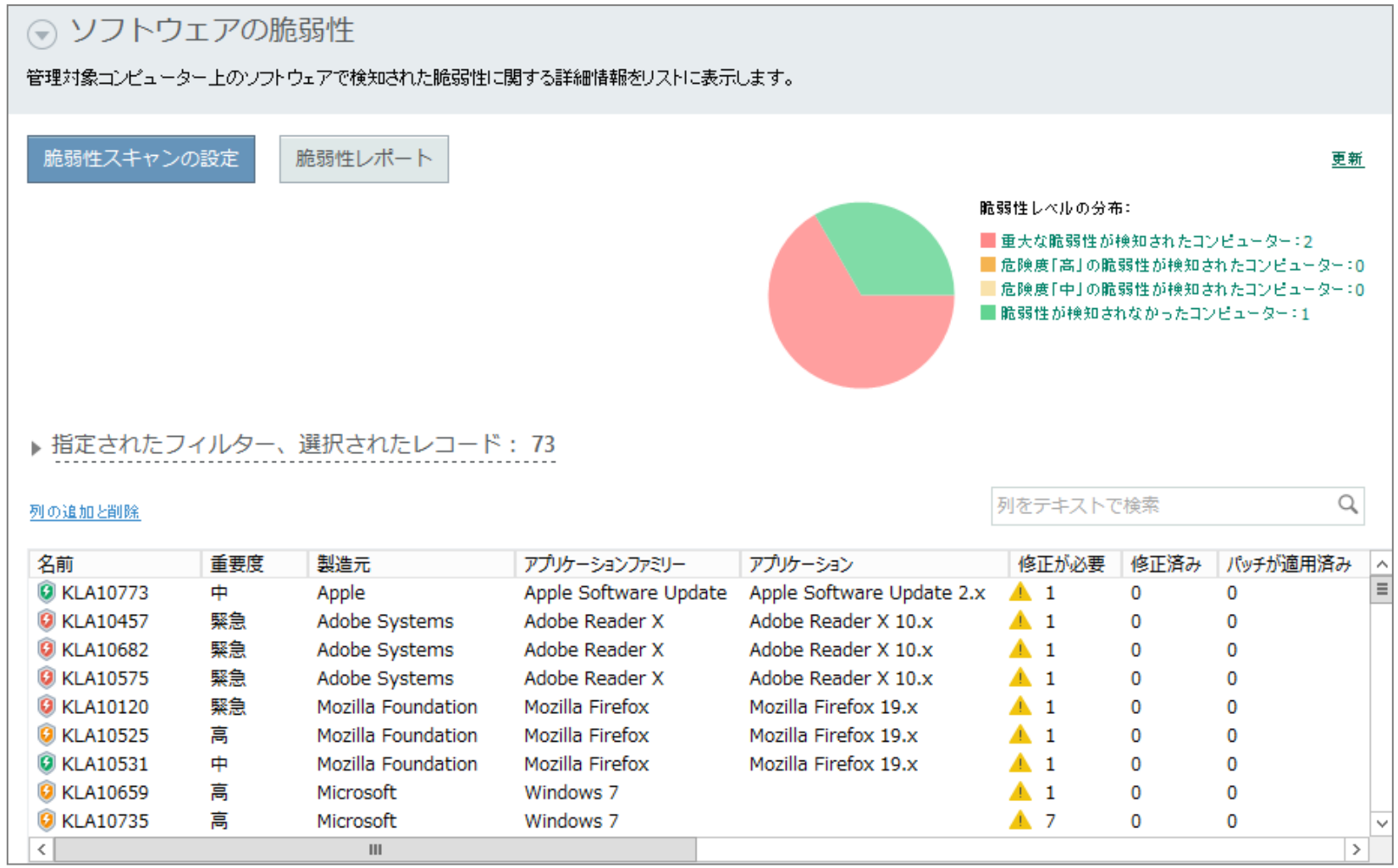
仮想サーバー	グループ名	コンピューター名	マザーボード	CPU	メモリ (MB)	データストレージ	合計 (GB)	合計空き容量 (GB)	ビデオアダプター	ネットワークアダプター	サウンドアダプター	光学ドライブ	モニター	IP アドレス
	管理対象コンピューター	CLIENT215	440BX Desktop Reference Platform	Intel(R) Xeon (R) CPU E5520 @ 2.27GHz	4096	VMware Virtual disk SCSI Disk Device 7/34	34	7	VMware SVGA 3D	Intel(R) PRO/1000 MT Network Connection (00:0C:29:86:91:92)		NECVMWar VMware IDE CDR10 ATA Device	汎用非 PnP モニター	10.251.81.215

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

脆弱性レポート

管理するPCのアプリケーションの脆弱性をレポート



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 Security Center Cloud Console

Kaspersky Security Center Cloud Console（KSC CC）の概要

カスペルスキーがクラウドで提供する管理コンソール。

お客様はKaspersky Endpoint Security for Business等の対象製品を購入。
KSC CCは無償提供。

お客様はWebブラウザでアクセスし、管理を行う。

対応製品ライセンス：
- Kaspersky Endpoint Security for Business Select (KESB Select)
- Kaspersky Endpoint Security for Business Advanced (KESB Advanced)
- Kaspersky EDR-Optimum、Add-on
- Kaspersky Embedded Systems Security(KESS)

300ライセンス以上で使用可能。

サブスクリプションライセンスの場合、100ライセンス以上で使用可能。（KESSを除く）

Kaspersky Security Center Cloud Consoleの概要

- 管理可能なアプリケーション
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server（KESBの機能範囲）
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Android
  - Kaspersky Endpoint Security for iOS

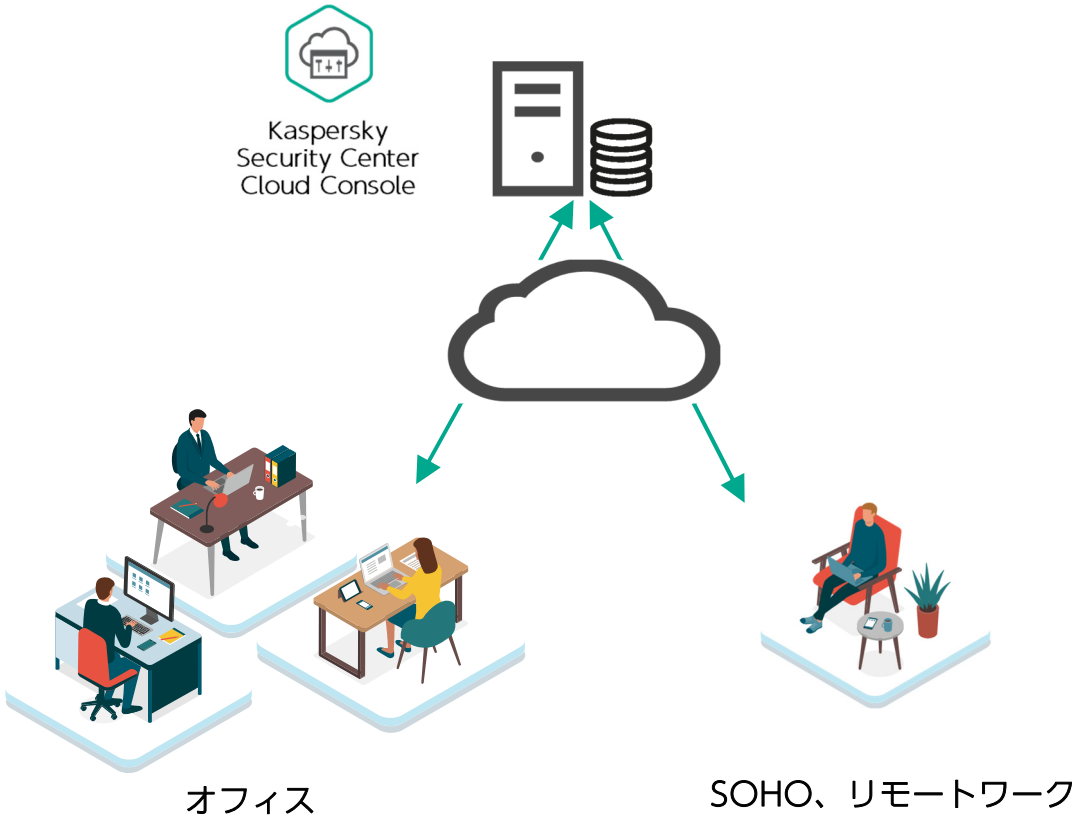
- 管理可能なアプリケーション
  - EDR-Optimum (KES Win, KSWS)
  - Kaspersky Embedded Systems Security
  - Advancedに含まれるVulnerability and Patch Management機能
  - Advancedに含まれる暗号化（bitlockerを使用したフルディスク暗号化）
  - Advancedに含まれるリモート接続機能(NAT環境では使用出来ません)

KESB = Kaspersky Endpoint Security for Business

kaspersky

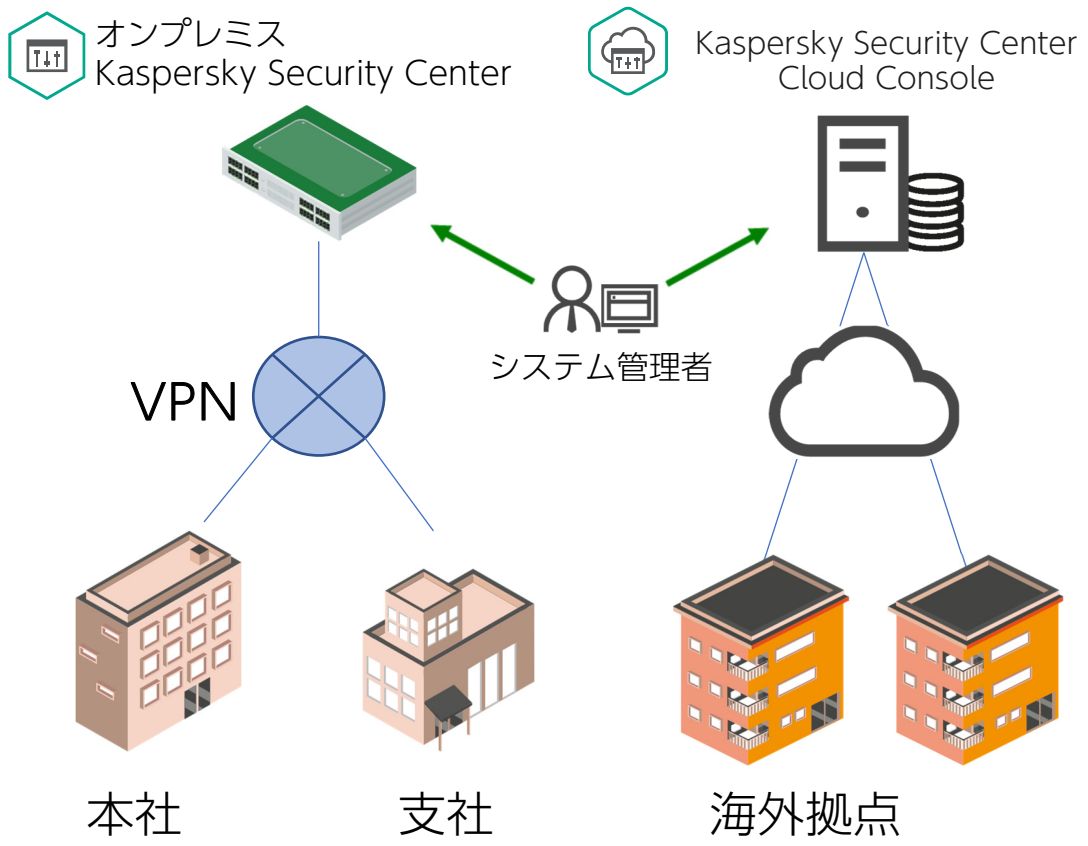
Kaspersky Security Center Cloud Consoleの利点

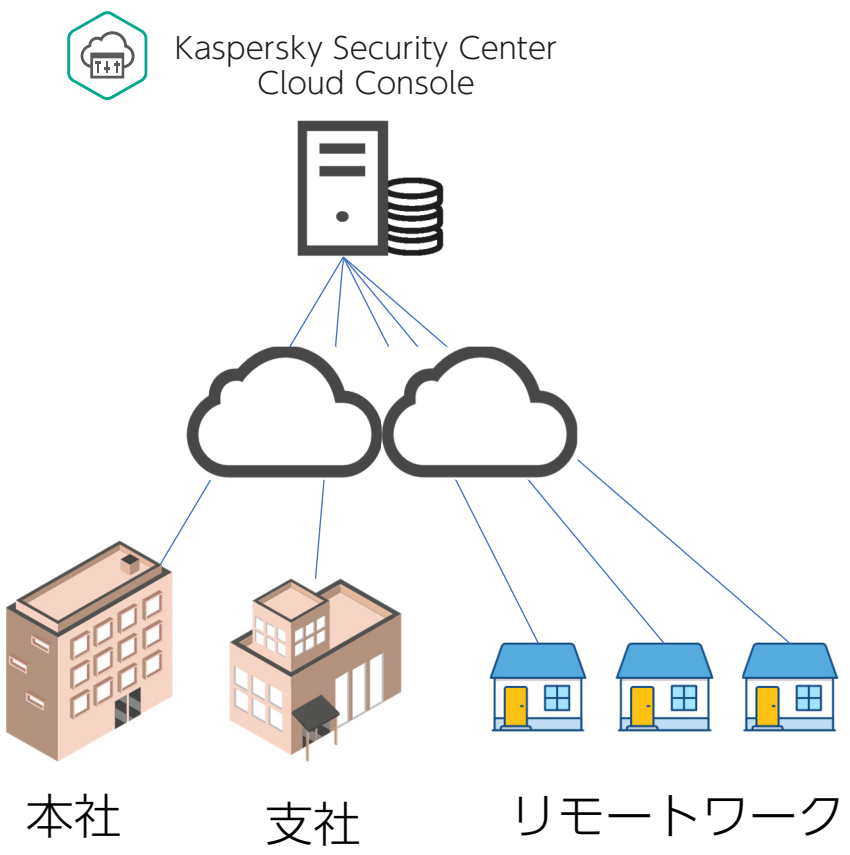
- サーバー機器の調達や構築が不要で、すぐに利用可能
- サーバー機器の監視やメンテナンス作業が発生せず、運用負荷を削減
- クラウドで提供されるため、オフィス外でもセキュリティ管理が可能



ユースケース

利用条件 Kaspersky Endpoint Security for Business 300ライセンス以上を保有





オンプレミスKSCとKSC Cloud Consoleの併用
KSC Cloud Consoleへの接続数は300以下でも使用可能

KSC Cloud Consoleによる移動端末サポート