

kaspersky

Kaspersky Security Center Cloud Console

～追加費用不要のクラウド管理コンソール～

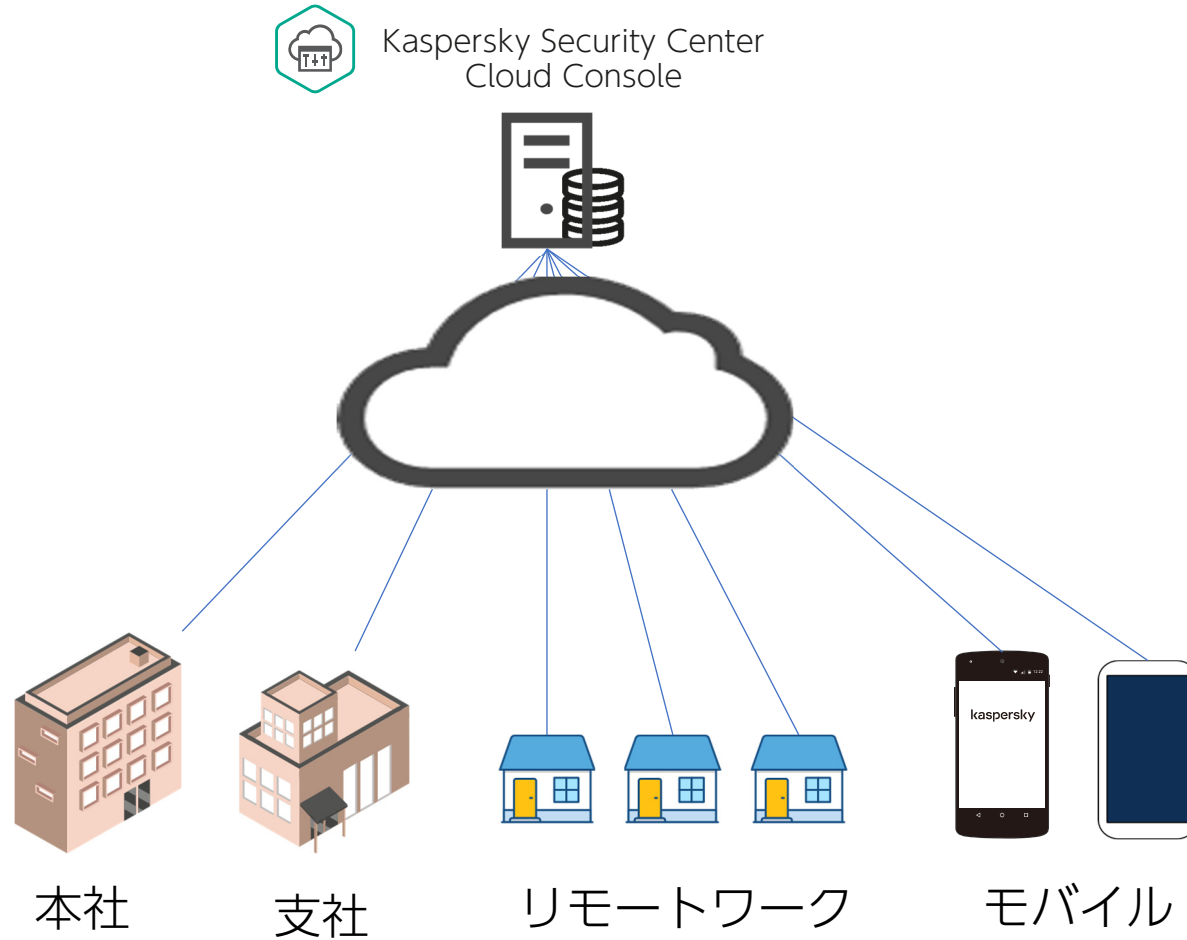
2023年05月23日

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 Security Center Cloud Console (KSC CC) の概要

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。

エンドポイントセキュリティや
EDRの管理機能を提供。

日本語を含めた多言語インターフェース。

管理状態・脅威状況が簡単に把握できるダッシュボード





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)



対応製品ライセンス：

Kaspersky Hybrid Cloud Security、
Kaspersky Hybrid Cloud Security Enterprises

デスクトップライセンス：300以上

サーバーライセンス：50以上

CPUライセンス：20以上

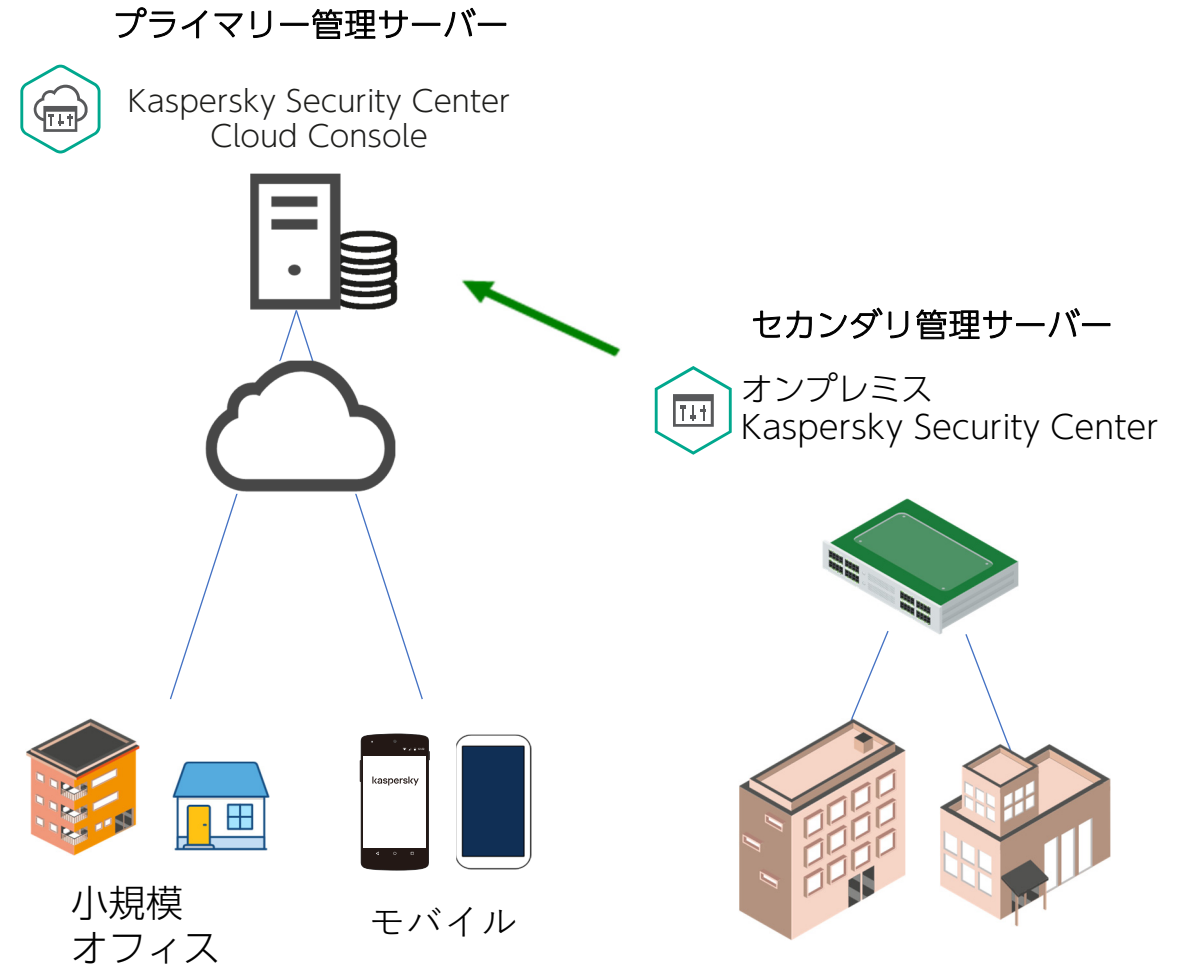
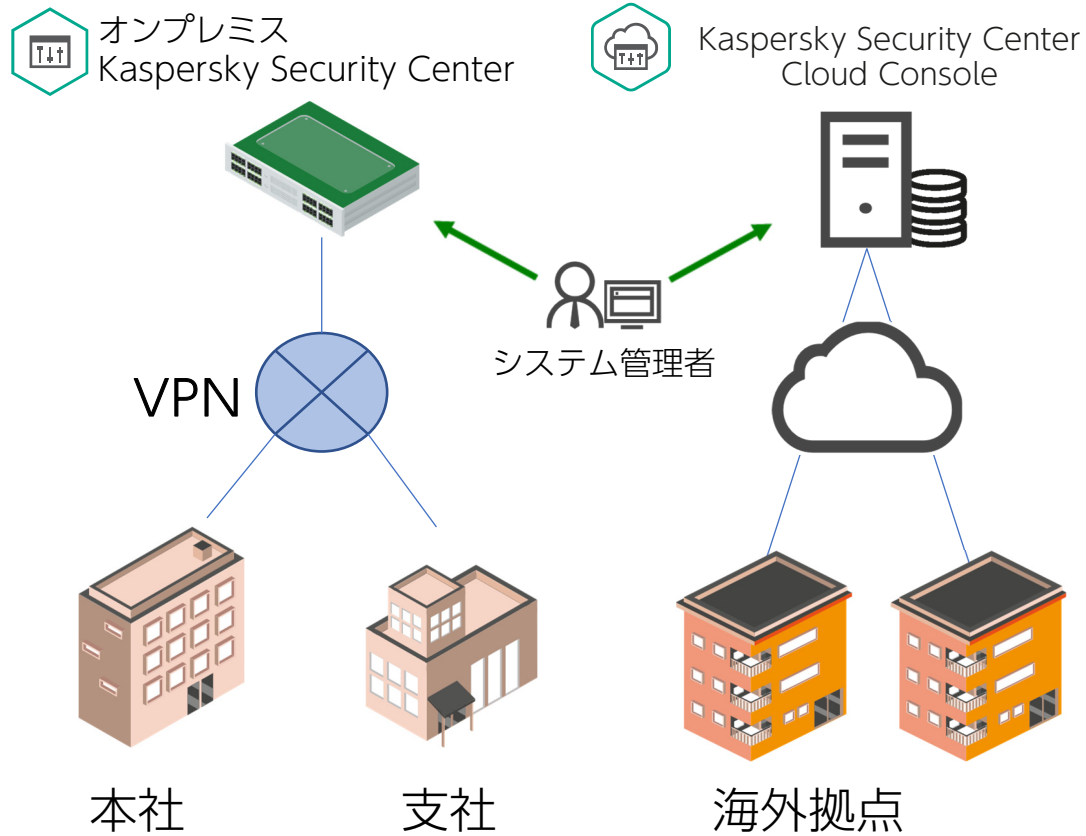
デスクトップ：クライアントOSのみ
サーバー：サーバーOSのみ

Kaspersky Security Center Cloud Consoleでは、Kaspersky Security for Virtualization はサポートしていません。
Kaspersky Endpoint Security for Windows、Kaspersky Endpoint Security for Linuxを使用します。



- 管理可能なアプリケーション(使用可能なライセンスの機能範囲)
 - Kaspersky Endpoint Security for Windows(KES for Win)
 - Kaspersky Security for Windows Server (KSWs)
 - Kaspersky Endpoint Security for Mac
 - Kaspersky Endpoint Security for Linux
 - Kaspersky Endpoint Security for Android
 - Kaspersky Endpoint Security for iOS
 - Kaspersky Embedded Systems Security
- 管理可能なアプリケーション
 - Kaspersky Managed Detection and Response
 - EDR-Optimum機能 (KES for Windowsのコンポーネントとしてインストール)
 - 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)

構成例



オンプレミスKSCとKSC Cloud Consoleの併用。
ライセンスは300以上必要だが、KSC Cloud Consoleへの
接続デバイス数は300以下でも使用可能。

オンプレミスKSCとKSC Cloud Consoleの併用。
レポートの集約など。



Kaspersky Security Center Cloud Consoleの管理

企業に割り当てられる管理単位をワークスペースと呼びます。

The screenshot displays the Kaspersky Security Center Cloud Console interface. On the left, the 'KL Japan' workspace is shown with its registration date (2022/1/28 13:31:00) and a link to 'ワークスペースに移動' (Move to workspace). A blue arrow points from this link to the 'ワークスペース' (Workspaces) menu item in the left-hand navigation sidebar. The main dashboard area shows '監視とレポート / ダッシュボード' (Monitoring and Reports / Dashboard) with various charts and status indicators. On the right, the 'デバイス / 管理対象デバイス' (Devices / Managed Devices) section is visible, containing a table of managed devices.

| 名前 | 可視 | 前回の管理サーバーへの接続 | ネットワークエージェン... | ネットワークエージェン... |
|--|----|---------------------|----------------|----------------|
| Apple iPad [Device ID A07C4A] | 🟢 | 2022/08/30 16:50:40 | 🟢 | 🟢 |
| asus P004 e... J@gmail.com 35L_280755_J000 | 🟢 | 2022/08/31 11:09:25 | 🟢 | 🟢 |
| PC-01 | 🟢 | 2022/08/31 11:03:20 | 🟢 | 🟢 |
| PC-02 | 🟢 | 2022/08/31 11:07:53 | 🟢 | 🟢 |
| PC-03 | 🟢 | 2022/08/31 11:09:52 | 🟢 | 🟢 |
| PC-04 | 🟢 | 2022/08/31 11:08:55 | 🟢 | 🟢 |
| PC-05 | 🟢 | 2022/08/31 11:07:56 | 🟢 | 🟢 |
| PC-06 | 🟢 | 2022/08/31 11:08:46 | 🟢 | 🟢 |
| PC-07 | 🟢 | 2022/08/31 11:07:34 | 🟢 | 🟢 |
| PC-08 | 🟢 | 2022/08/31 11:08:21 | 🟢 | 🟢 |



Kaspersky Security Center Cloud Consoleの管理

複数の管理者が一つのワークスペースを管理することが可能です。

KL Japan

登録日: 2022/1/28 13:31:00 (UTC +9:00)

説明: KL Japan

[アクセス権管理を非表示にする](#)

アクセス権管理 + アクセス権を付与

会社へアクセス可能なアカウントの数 4

| メールアドレス | アクセスレベル |
|---------------------------------------|---|
| <input type="text" value="アカウントを検索"/> | <input type="text" value="アクセスレベルを検索"/> |
| @kaspersky.com | 管理者 |
| Kas001@...com | ユーザー 🗑️ |
| Kas003@...t.com | ユーザー 🗑️ |
| pi@...gmail.com | ユーザー 🗑️ |

Kaspersky Security Center Cloud コンソール
ワークスペースの数: 1

[KL Japan](#) 🗑️

[ワークスペースに移動](#)

ID: 524e...30e1-49fb...8567aC

アクセス権を付与

メールアドレス

アクセスレベル

管理者 ▼

* 「ユーザー」はモバイルへのインストールに使用。

ワンタイムパスワードを用いた多要素認証



ワークスペースへのサインインにはワンタイムパスワードを用いた多要素認証が使用出来ます。

kaspersky 日本語(日本)

Kaspersky Security Center Cloud Console

メールアドレス
i@kaspersky.com

パスワード
.....

[パスワードをお忘れですか?](#) ログイン



kaspersky 日本語(日本)

Kaspersky Security Center Cloud Console

セキュリティコードを入力してください

認証アプリによって生成されたセキュリティコードを入力します。

コード

[SMS のコードを使用する](#)

携帯へのSMS、Microsoft Authenticator、Google Authenticatorなどを利用出来ます。



Kaspersky Security Center Cloud Consoleで管理する 代表的なアプリケーション

詳細は各アプリケーションの資料をご覧ください。



Kaspersky Endpoint Security for Business Select、Advancedでは、以下のアプリケーションが使用出来ます。

- Kaspersky Endpoint Security for Windows(KES for Win)
- Kaspersky Security for Windows Server (KSWS)
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Android
- Kaspersky Endpoint Security for iOS

レポート、通知など、従来のオンプレミスKSCとほぼ同じ機能が使用出来ます。



セキュリティ専門家のいない組織に、適切なセキュリティ対応力を提供。

成功: 削除済み

詳細 | すべての警告イベント

...前回の処理を開く

- C:\Windows\System32\msiexec.exe
- C:\Windows\SysWOW64\msiexec.exe
- C:\Program Files... exe
- プロセスの開始¹⁰
- ファイルのドロップ³⁶
- コード埋め込み⁸
- レジストリ³⁶

推奨事項

- 調査時にコンピューターをネットワークから分離します。
- ネットワーク内の他のコンピューターでのファイルの実行を防止します。
- ネットワーク内の他のコンピューターで検出された脅威を検索します。
- 検出した脅威について詳しくは、[Kaspersky Open Threat Intelligence Portal](#) および [Kaspersky Open Threat Intelligence Portal](#) を参照してください。
- 調査および脅威の処理完了後、コンピューターのネットワーク分離を無効にします。

推奨事項 (Guided Response) をGUI上でガイド。
 インシデントカードによるマルウェア挙動を可視化。
 ファイル生成
 スクリプトの起動
 マルウェアのネットワーク通信
 マルウェアを自動起動させるレジストリの作成

ワンクリック 簡単対応
 端末の論理的切り離しを遠隔から実行。物理的に切り離さないため、
 管理操作は継続可能。
 プログラムの起動禁止、ファイルの隔離。

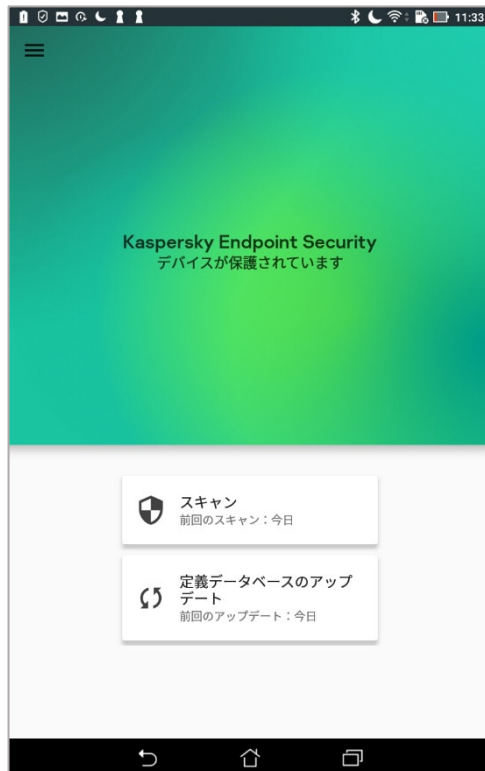
| | | | |
|-----------|--|---|---|
| 警告 | 成功 削除済み | コンピューター | コンピューターをネットワークから分離する コンピューターの分離を解除する |
| 日時 | 2022/09/13 13:55:27 | コンピューター名 | WORKGROUP\PC-01 |
| カテゴリ | PDM:Trojan.Win32.Generic | ネットワークインターフェイス | 192.168.1.18 00-0c-29-71-b0-05 127.0.0.1 00-00-00-00-00-00 |
| オブジェクト名 | C:\Program Files (x86)\... \Agent\... exe | OS | Microsoft Windows 10(10.0.19045) |
| スキャンモード | システムウォッチャーのスキャン時 | グループ名 | Client PCs |
| オブジェクトの種類 | メモリプロセス | ポリシー名 | Kaspersky Endpoint Security for Windows (11.10.0) |
| プロセス | | ログオンセッションID | 00000000.0097b438 |
| 起動/パラメータ | "C:\Program Files (x86)\... \Agent\... exe" | 特権付きユーザー | はい |
| システムPID | 7884 | | |
| 整合性レベル | 整合性 (高) | | |
| ユーザー名 | PC-01\admin | | |
| ファイル | | Kaspersky Threat Intelligence Portal からのデータ | |
| 名前とサイズ | C:\Program Files (x86)\... \Agent\... exe (108.7 KB) | 最終更新日時 | 2022/09/13 13:55:27 |
| MD5 | a724f2750290e0000000000000000000 | ポータルで調べる | |
| SHA256 | 860c0e9a7d751a1e1c0e0e90fd1843b2483ef530a595650b07090900 | ファイル | 不明 (Kaspersky Security Network) |
| 信頼チェックの結果 | ブロック | ユーザー数 | 10人未満の Kaspersky Security Network のユーザーがこのアプリケーションを使用しています。 |
| 作成日 | - | 使用されている地域 | - |
| 編集日 | - | 初回登録日 | 1か月前 |
| ファイル作成者 | - | | |



Kaspersky Endpoint Security for Android

アンチマルウェア、アプリケーション起動コントロール、カメラ、ブルートゥース等の使用制限、パスワードポリシーなどのMDM機能、遠隔ロック、ワイプなどの機能を提供。

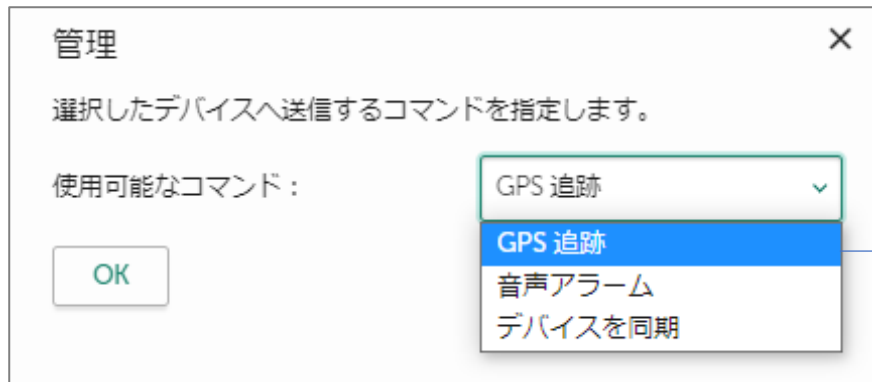
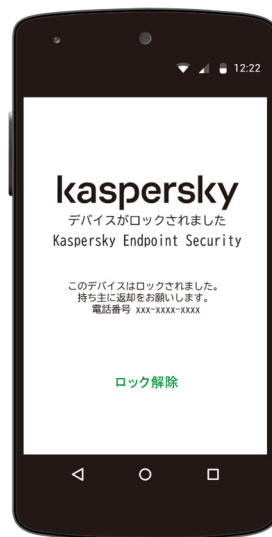
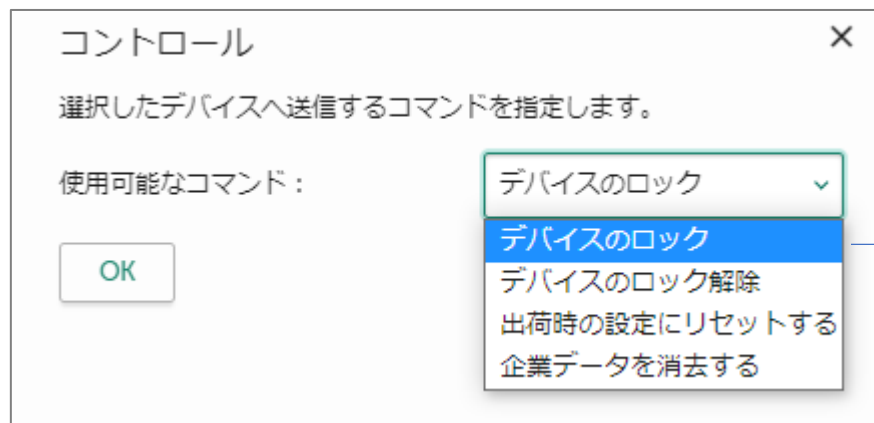
定期同期以外に、Google Firebase Cloud Messaging APIを使用したコマンド即時実行が可能。



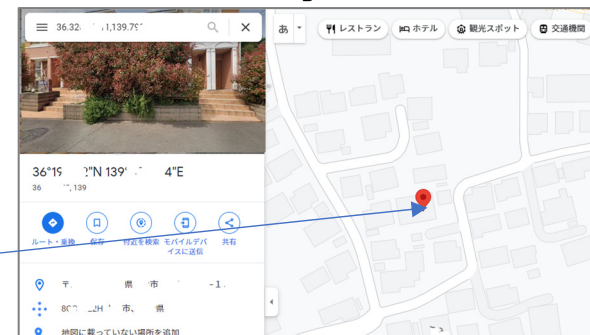
GPS追跡には、Google アナリティクスが有効である必要があります。



Android端末へのロックなどの操作



Google Mapで位置情報を表示



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。



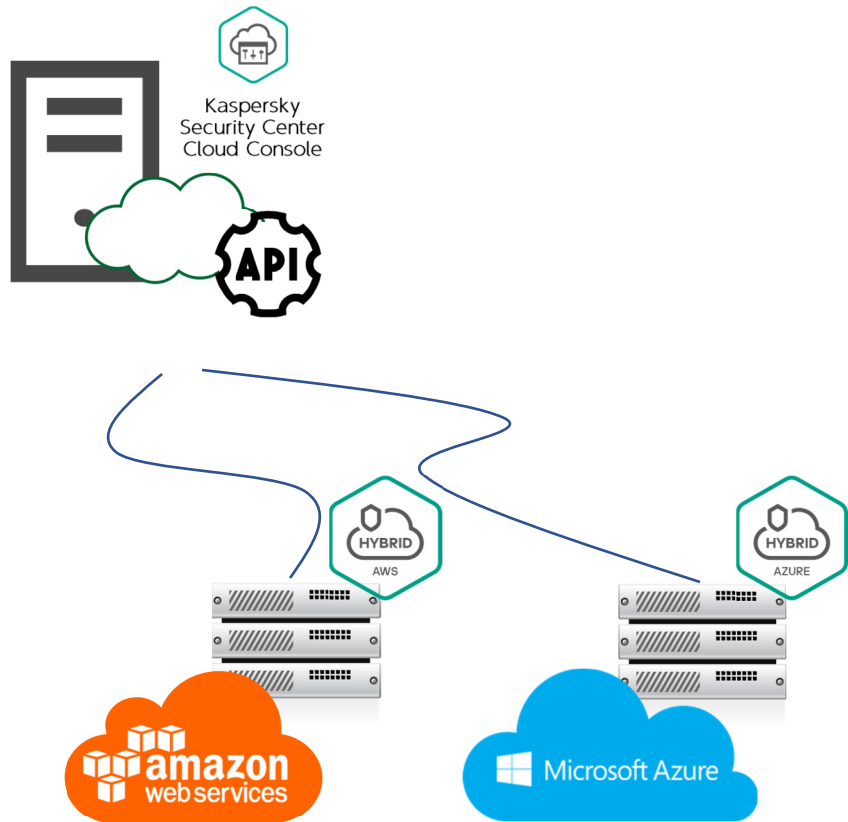
危険サイトであるか
チェック



Kaspersky
Security
Network



KSC CCではiOS/iPAD OS用MDMは提供していません。



- 管理サーバーを自前で持たなくてもクラウドインスタンスを管理可能に。
- AWS APIを使って Amazon EC2 インスタンスを検出。
- Azure API を使って Azure 仮想マシンを検出、ネットワークエージェントを自動インストール。



- KHCSライセンスを適用することにより、ウィザードが走り、設定を支援。Cloud APIの使用を容易にします。

Kaspersky Security Center Cloud Consoleでの Windows 版エンドポイントセキュリティのインストール展開方法



KSC CCを使用して端末を保護・管理するために2つのモジュールをインストールします。

- ① KSC CCと通信するためのネットワークエージェント。 NA
- ② 保護を提供するエンドポイントセキュリティ。 k

方法1

ネットワークエージェントをインストールし終えたのちに、
エンドポイントセキュリティをインストールする。

メリット

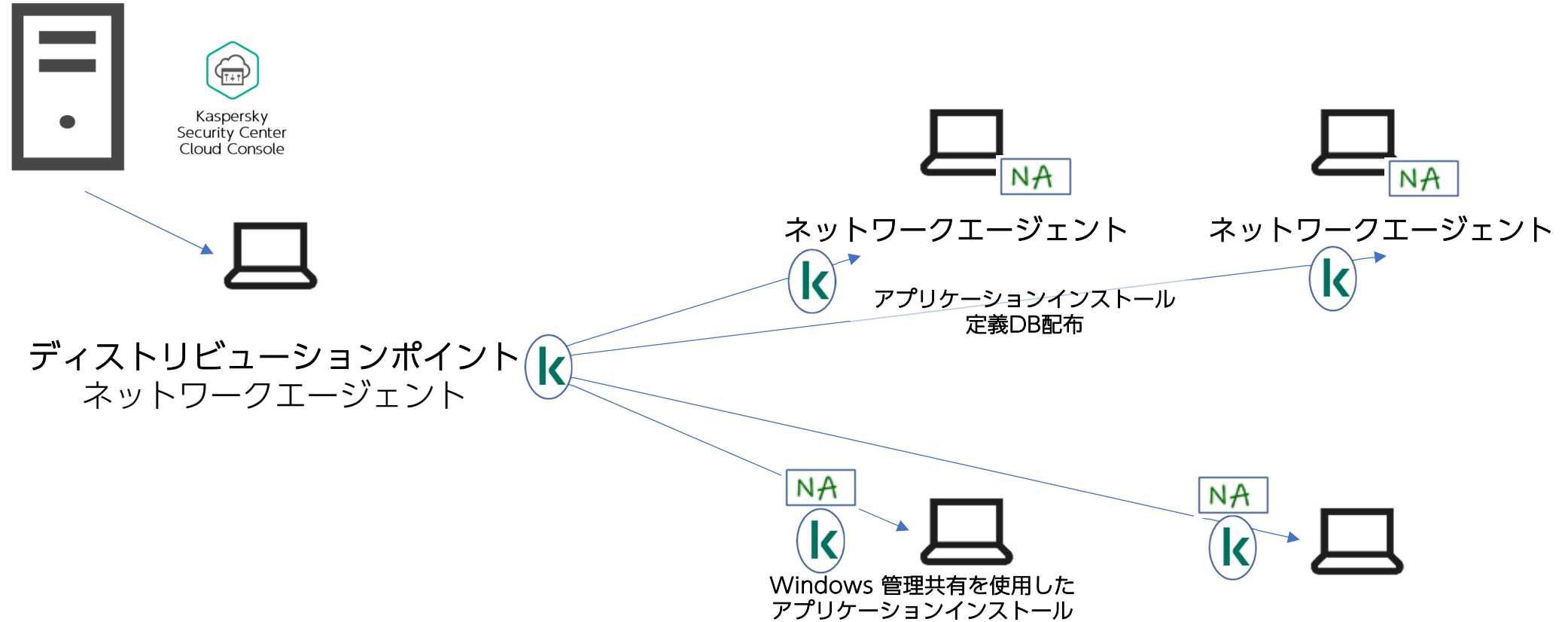
ネットワークエージェントをインストールすると端末の状態が把握でき、
エンドポイントセキュリティのインストールをコントロールしやすい。

方法2

ネットワークエージェント、エンドポイントセキュリティを同時にインストールする。



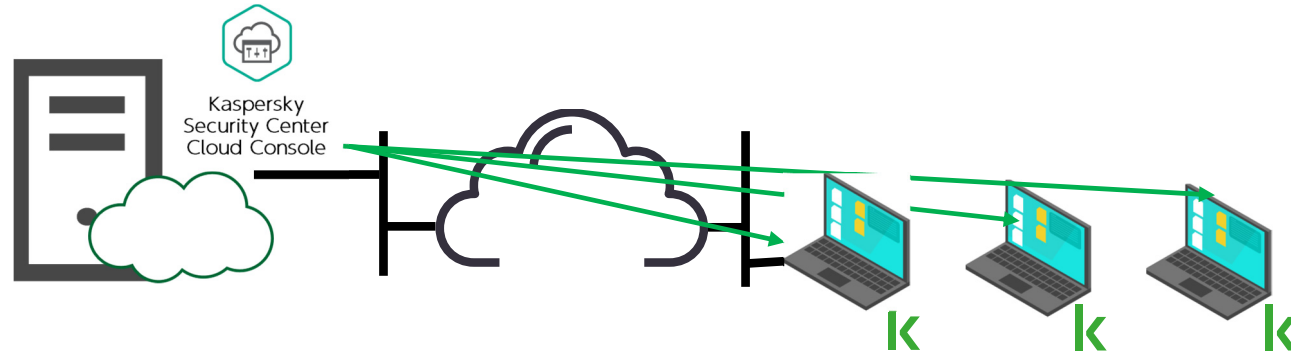
ディストリビューションポイントに指定した端末が、アプリケーションや定義DBの配布機能を持つ。
ネットワークエージェント内に機能があり、KSC CCで指定すれば、ディストリビューションポイントとしてふるまう。



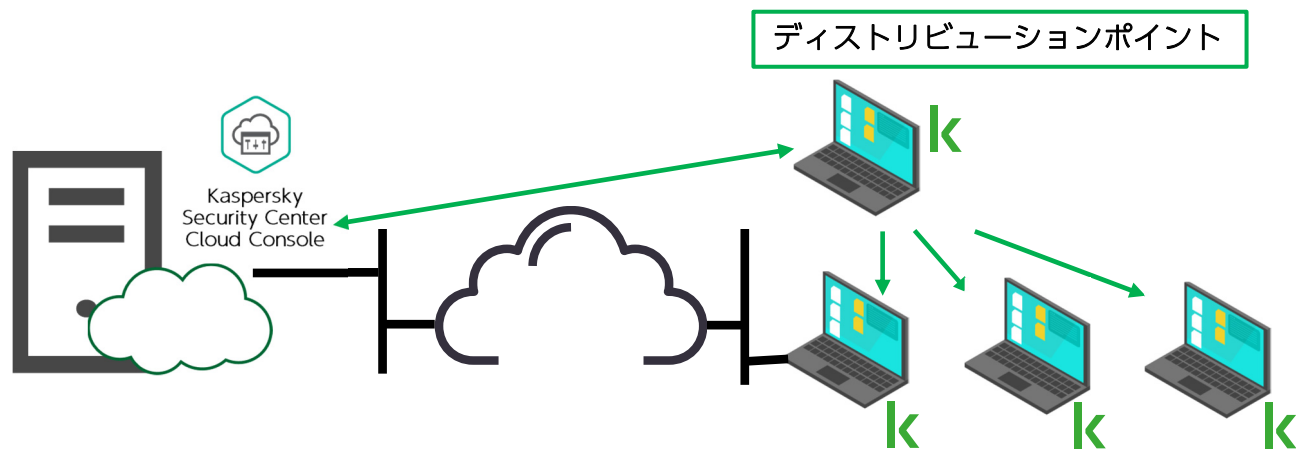
ネットワークエージェントがインストールされていない端末に、
KSC CCからリモートインストールを行うには、Active Directoryが必要。
(ADポーリングを使用)



ディストリビューションポイントを使用することにより、各端末がインターネットにアクセスしインストーラーや定義を直接ダウンロードすることを抑制出来ます。
特に端末数の多い組織では、ディストリビューションポイントの配置をお勧めします。

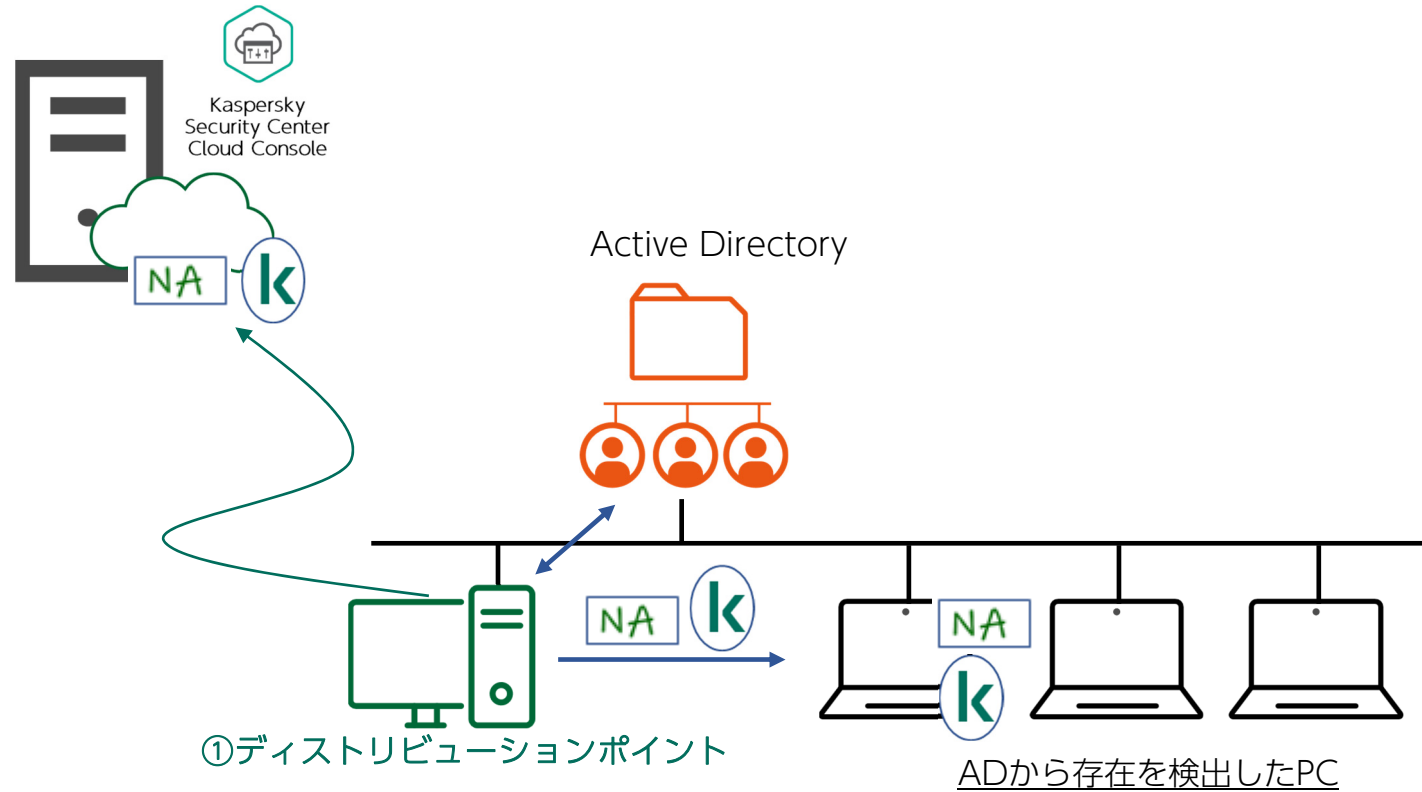


ディストリビューションポイントがない場合



ディストリビューションポイントを設定

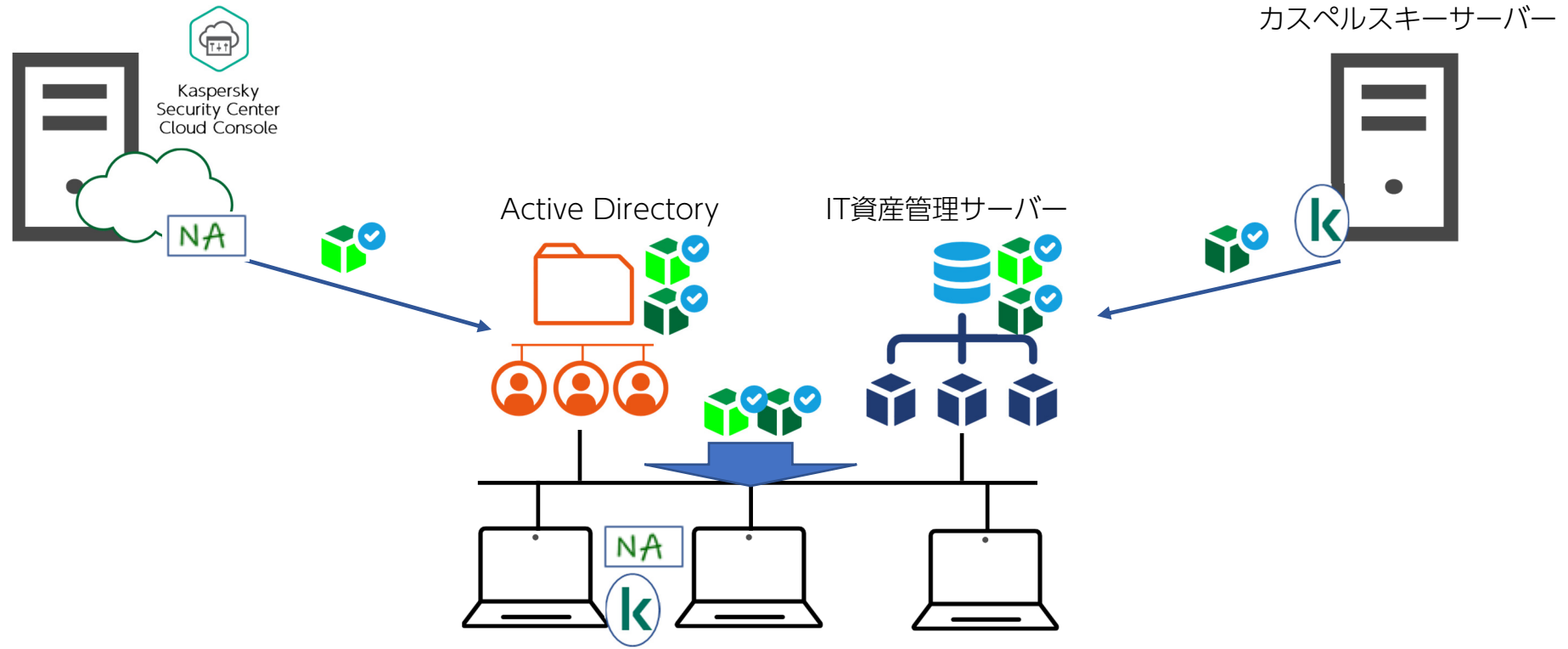
KSC CC クライアントのインストール方法 パターン1



①ネットワークエージェントをインストール、
ディストリビューションポイントに指定

②Active Directoryポーリングを実行し、
組織内のPCを検出。

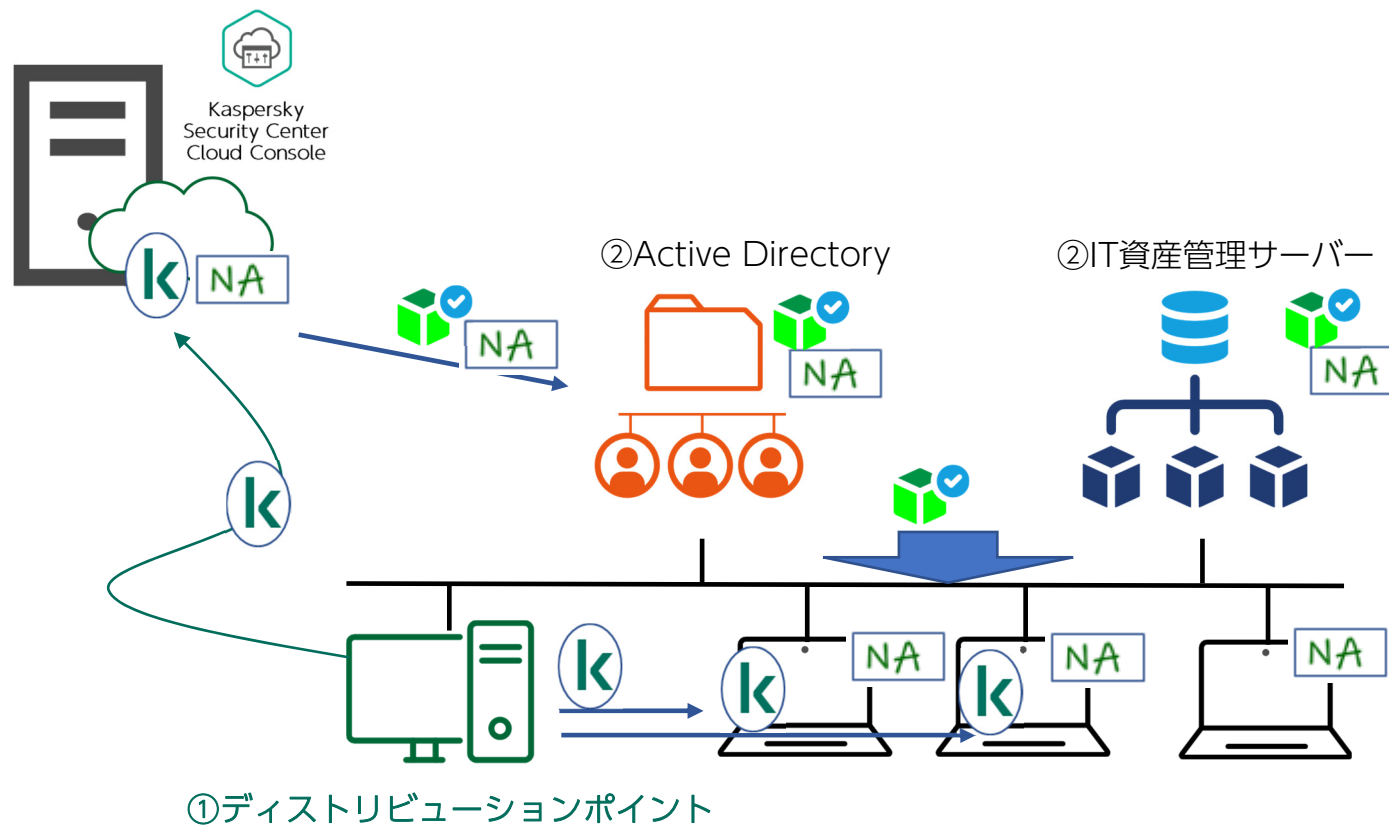
③ディストリビューションポイントを通じて、
組織内のPCにネットワークエージェント、
KESをインストール。
(Windows 管理共有を使用したプッシュインストール)



①ネットワークエージェントインストールパッケージをActive Directory、IT資産管理サーバーにダウンロード。

②カスペルスキーの公開サーバーからエンドポイントセキュリティインストールパッケージをダウンロード。

③Active Directoryのソフトウェア配布機能、IT資産管理サーバーを使用して、インストール。

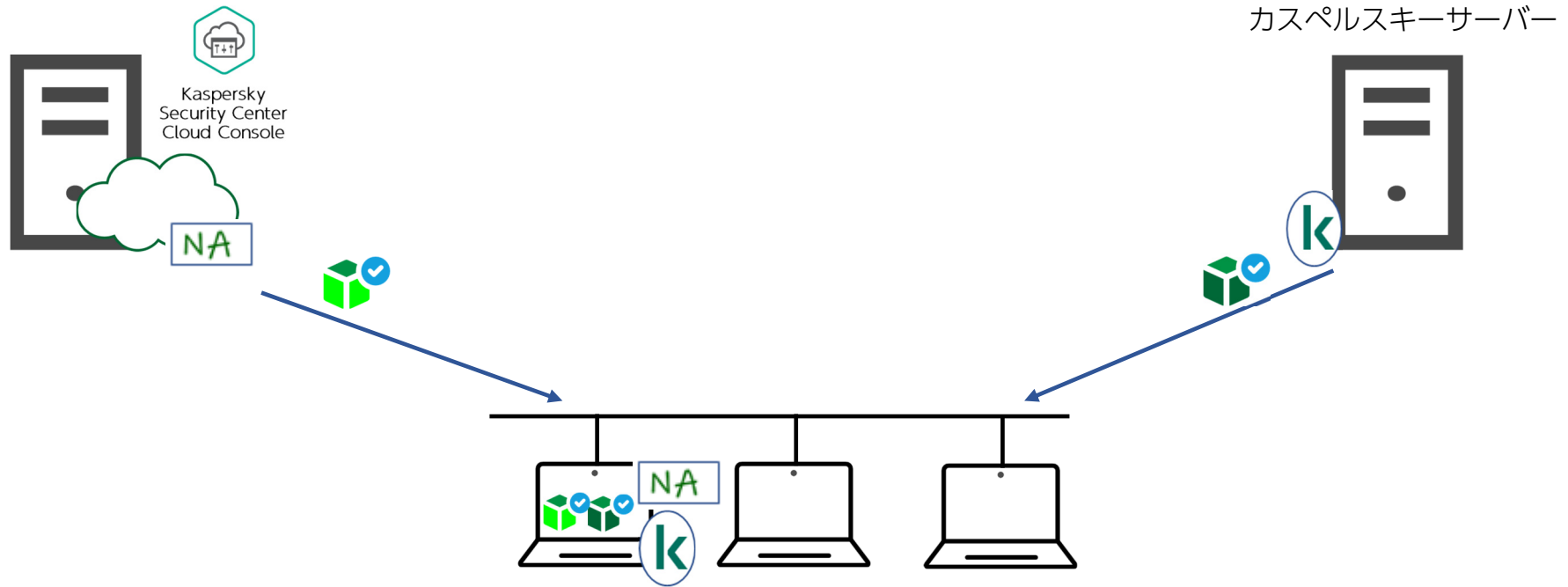


①ネットワークエージェントをインストール、ディストリビューションポイントに指定

②ネットワークエージェントインストールパッケージをActive Directory、IT資産管理サーバーにダウンロード。

③Active Directoryのソフトウェア配布機能、IT資産管理サーバーを使用して、ネットワークエージェントをインストール。

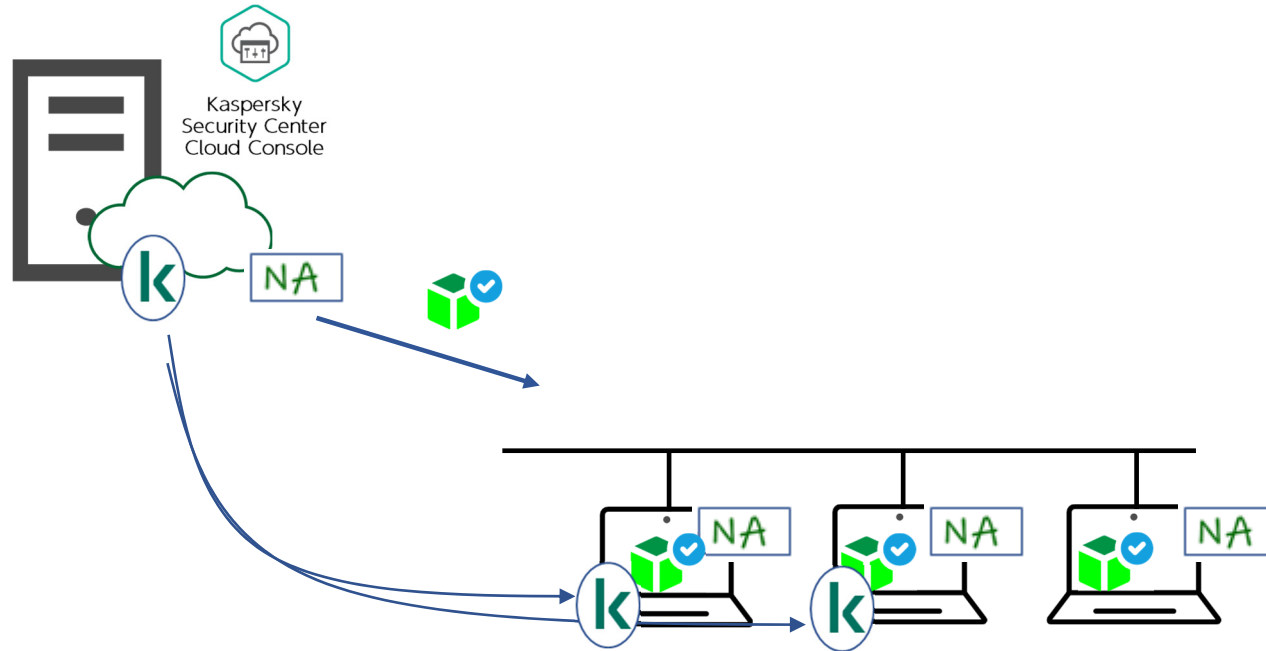
④ディストリビューションポイントを通じて、組織内のPCにKESをインストール。



①ネットワークエージェントインストールパッケージをダウンロード。

②カスペルスキーの公開サーバーからエンドポイントセキュリティインストールパッケージをダウンロード。

③組織内のPCにネットワークエージェント、KESを対話型でインストール。



①ネットワークエージェントを対話型で全端末にインストール。

②ネットワークエージェントを通じて、KESをインストール。

評価申し込み



ワークスペースの作成時に”Trial”を選択出来ますが、
“Trial”から本番環境への移行は出来ません。

評価時のワークスペース削除、ワークスペースの再作成、
ネットワークエージェントのクライアントへの再インストールが発生します。

評価環境から本番環境への移行を考えている場合は、
必ずカスペルスキーの営業までご連絡ください。



事前にアカウントを登録し、ワークスペースを作成

1. アカウントの登録

- 以下のポータルよりアカウントを登録
 - <https://ksc.kaspersky.com/>

2. 会社情報の登録とワークスペースの作成

- 以下のポータルより、1.で作成したアカウントにてサインインして実施
 - <https://ksc.kaspersky.com/>
- アクティベーションコードの登録が必要

kaspersky 日本語(日本)

カスペルスキー製品とサービスへのアクセス用の単一アカウント ログイン

カスペルスキー製品とサービスへのアクセス用の単一アカウントを作成

現在のメールアドレスを入力してください。アカウントを有効化するリンクが記載されたメールがこのメールアドレスに送信されます。

メールアドレス

新しいアカウントの強力なパスワードを作成して入力します。安全性のために、次のパスワード要件を満たす必要があります：

- 8文字以上
- 大文字と小文字
- 番号
- すべての記号が有効

パスワード

パスワード再入力

- パスワードが一致

データは、[プライバシーポリシー](#)に記載された内容に従って処理および送信されること（第三国への送信を含む）を理解しました。[プライバシーポリシー](#)の内容をすべて確認し、理解した上で同意します。

続行するには、[プライバシーポリシー](#)に同意することを確認する必要があります

アカウントを作成

参考 クラウドサービス比較

参考 KES CloudとKSC CC 購入形態の違い



| 購入する製品名称 | 使用出来る環境 | 使用可能なクラウドサービス | クラウドサービス使用時1つのワークスペースで使用出来るライセンス数 |
|--|-------------------------------|---|-----------------------------------|
| KES Cloud KES Cloud Plus KES Cloud Pro | クラウド管理のみ | KES Cloud Kaspersky Business HUB https://cloud.kaspersky.com/ | 10~999 |
| KESB Select KESB Advanced EDR-Optimum | クラウド管理 オンプレミス管理 スタンドアロン | KSC CC Kaspersky Security Center Cloud Console https://ksc.kaspersky.com/ | 300 (100) ~25,000 |

*EDR-Optimum機能は、
スタンドアロンでは使用不可。
管理サーバーが必須。