



# ESET PROTECTソリューション 規模別構成例

キヤノンマーケティングジャパン株式会社

第9版

作成：2021年10月11日

**Canon**

キヤノンマーケティングジャパン株式会社

# はじめに

※本資料では、適宜下記のプログラム名や略称を使用して説明いたします。  
※オンプレミス型セキュリティ管理ツールのバージョンによって管理できるクライアント用プログラムに  
差異があります。詳細は以下サポートページをご参照ください。  
[https://eset-support.canon-its.jp/faq/show/143?site\\_domain=business](https://eset-support.canon-its.jp/faq/show/143?site_domain=business)



本資料は、「ESET PROTECTソリューション」で新たに提供を開始した各プログラムをもとに、規模別の構成例をまとめた資料です。以下のプログラムおよびバージョンをもとに構成例をまとめています。

| プログラム名   | バージョン | 略称   | 種別                          | 備考                     |
|--|-------|------|-----------------------------|------------------------|
| ESET PROTECT<br>※ESET Security Management Centerの後継  | 8.X   | EP   | Windows サーバー用<br>Linuxサーバー用 | オンプレミス型<br>セキュリティ管理ツール |
| ESET PROTECT Cloud   | 2.4   | EPC  | ESET社のクラウドにて提供              | クラウド型<br>セキュリティ管理ツール   |
| ESET Endpoint Security   | 8.X   | EES  | Windows クライアント用             | 総合セキュリティ<br>プログラム      |
| ESET Endpoint アンチウイルス  | 8.X   | EEA  |                             | ウイルス・スパイウェア<br>対策プログラム |
| ESET Server Security for Microsoft Windows Server<br>※ESET File Security for Microsoft Windows Serverの後継 | 8.X   | ESSW | Windows サーバー用               | ウイルス・スパイウェア<br>対策プログラム |
| ESET Endpoint Security for OS X  | 6.X   | EESM | Mac クライアント用                 | 総合セキュリティ<br>プログラム      |
| ESET Endpoint アンチウイルス for OS X   | 6.X   | EEAM |                             | ウイルス・スパイウェア<br>対策プログラム |
| ESET Endpoint アンチウイルス for Linux  | 8.X   | EEAL | Linuxデスクトップ用                | ウイルス・スパイウェア<br>対策プログラム |
| ESET Server Security for Linux<br>※ESET File Security for Linuxの後継                                       | 8.X   | ESSL | Linux サーバー用                 | ウイルス・スパイウェア<br>対策プログラム |
| ESET Endpoint Security for Android   | 2.X   | EESA | Android用                    | 総合セキュリティ<br>プログラム      |

※ESET PROTECTソリューションではクライアントOSおよびサーバーOSの端末に導入するプログラムとしてWindows、Mac、Linux、Android OS向けのプログラムをご使用いただけます。各プログラムの機能紹介は別資料をご用意しています。

※Windows、Windows Server、Microsoft Edge および Internet Explorerは、米国 Microsoft Corporation の米国、日本およびその他の国における商標登録または商標です。macOS、OS X および iPhoneは、米国およびその他の国で登録されているApple Inc. の商標です。



## • ESET PROTECTソリューションにおけるサーバーの構成要素

- ESET PROTECT
- ESET PROTECT Cloud
- Mobile Device Connector
- ミラーサーバー

## • 規模別構成例

- 規模別構成例
- 規模別構成例(～100クライアント)
- 規模別構成例(～1,000クライアント)
- 規模別構成例(1,000～5,000クライアント)
- 規模別構成例(5,000～10,000クライアント)
- 規模別構成例(10,000～50,000クライアント)
- 規模別構成例(50,000～100,000クライアント)
- オフライン環境の構成例
- モバイル管理の構成例
- ESET PROTECT Cloudの構成(オンプレミスでミラーサーバー なし)
- ESET PROTECT Cloudの構成(オンプレミスでミラーサーバー あり)

## • 参考情報

- 管理サーバーおよびエージェントのアップデートについて
- トラフィック量の計算(管理サーバー)
- トラフィック量の計算(ミラーサーバー)



# ESET PROTECTソリューションにおける サーバーの構成要素

**Canon**

キヤノンマーケティングジャパン株式会社



ESET PROTECTはESET Endpoint SecurityやESET Endpoint アンチウイルスなどを、ネットワーク経由で統合管理するツールです。Windows、Mac OS X、Linux向けプログラムを管理する管理サーバーとして動作します。

## ESET PROTECT (EP)

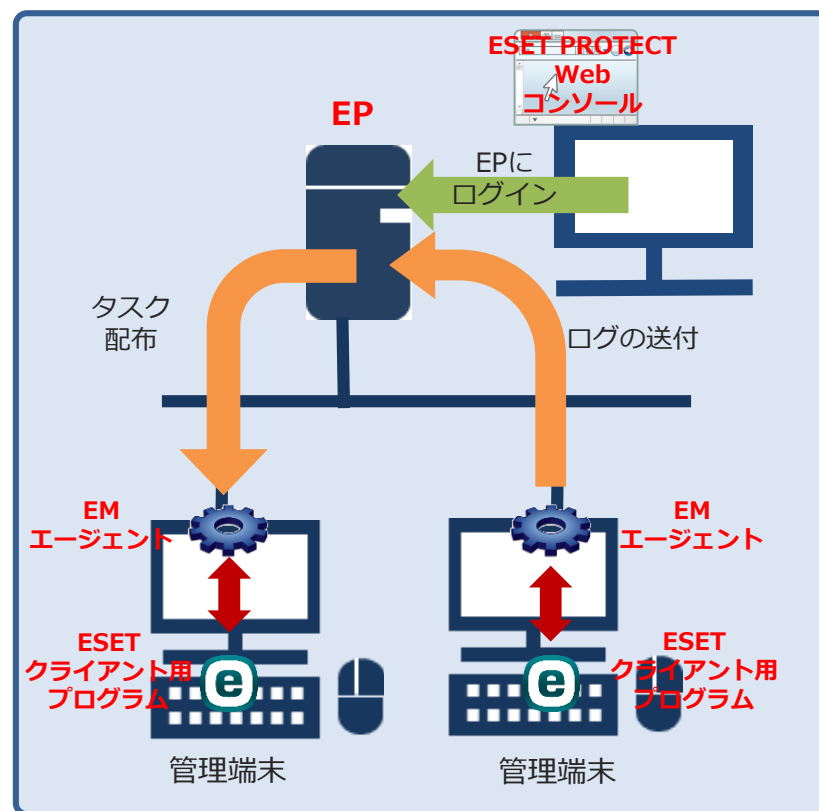
EPはクライアントプログラムの情報収集やタスク配布などを行います。クライアントとの通信はエージェントを経由して行います。

## ESET PROTECT Webコンソール

WebコンソールはWebベースのインターフェースであり、ブラウザを使用してEPへアクセスします。ブラウザ経由でクライアント情報の閲覧やEPの設定変更などを行うことができます。

## ESET Managementエージェント (EMエージェント)

エージェントは、クライアントから情報を収集し一定の間隔毎でEPへデータを送信します。また、EPからのタスク配布などはエージェントへ送信されたのち、エージェントがクライアントへ送信します。





ESET PROTECT Cloudは、ESET社のクラウド環境に構築された、ESET Endpoint SecurityやESET Endpoint アンチウイルスなどを、ネットワーク経由で統合管理するツールです。Windows、Mac OS X、Linux向けプログラムを管理する管理サーバーとして動作します。

## ESET PROTECT Cloud (EPC)

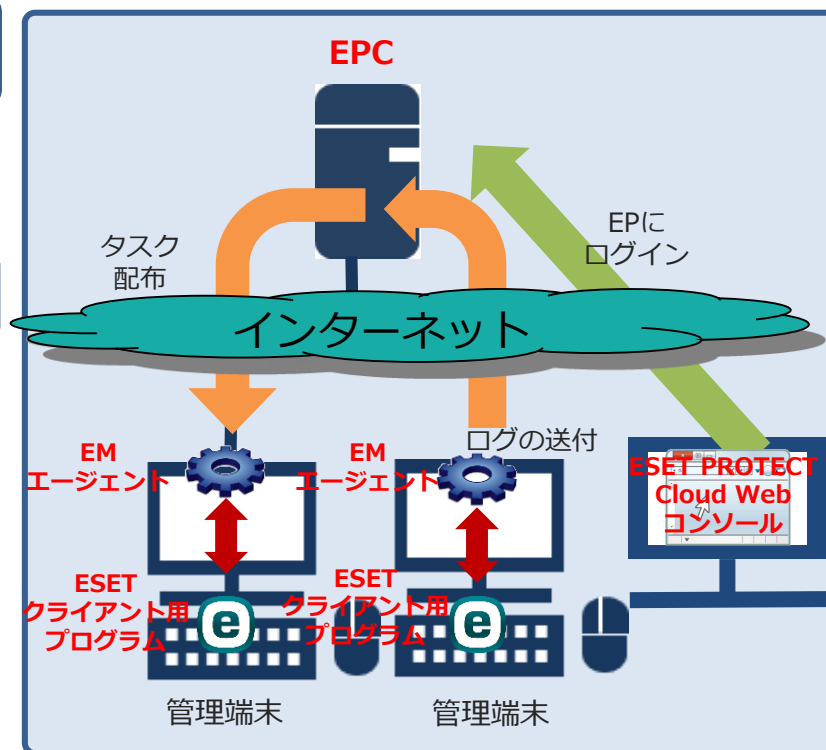
EPCはクライアントプログラムの情報収集やタスク配布などを行います。クライアントとの通信はエージェントを経由して行います。

## ESET PROTECT Cloud Webコンソール

WebコンソールはWebベースのインターフェースであり、ブラウザを使用してEPCへアクセスします。ブラウザ経由でクライアント情報の閲覧やタスクの実行などを行うことができます。

## ESET Managementエージェント (EMエージェント)

エージェントは、クライアントから情報を収集し一定の間隔毎でEPCへデータを送信します。また、EPCからのタスク配布などはエージェントへ送信されたのち、エージェントがクライアントへ送信します。

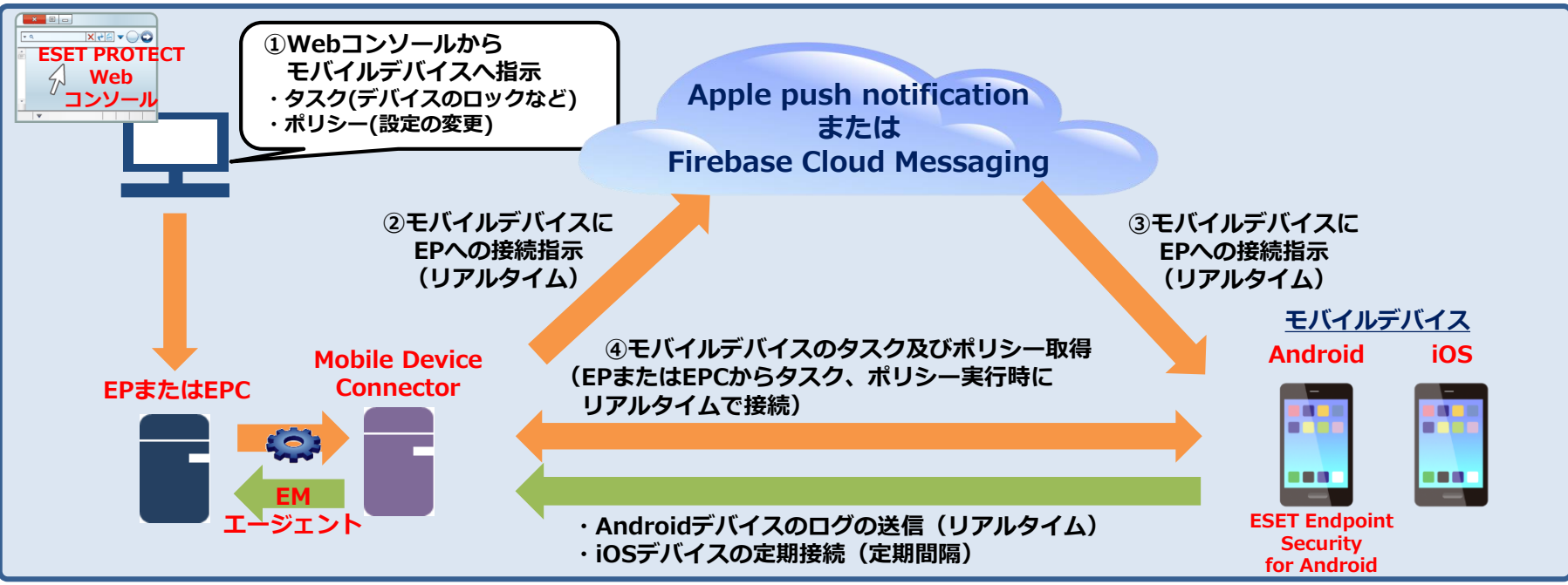




Mobile Device ConnectorはAndroid向けプログラムやiOSのモバイルデバイスを管理する際に必要となります。Mobile Device Connectorはモバイルデバイスの登録およびモバイルデバイスとの通信を行います。

## Mobile Device Connector

EPでAndroid端末やiOSのモバイルデバイスを管理するために必要なコンポーネントとなります。モバイルデバイスの登録および、モバイルデバイスとの通信を行う際に使用します。なお本機能はEPに含めることができます。EPCをご利用の場合は本コンポーネントが含まれた状態で利用を開始できます。





ミラーサーバーとは、ESET社から配布される検出エンジンなどのアップデートファイルをミラーリングし、クライアントに配布するサーバーです。

プログラムのミラー機能、またはミラーツールを使用してミラーサーバーの構築が可能となります。クライアントPCを利用して構築することも可能です。

### ! ミラーサーバーの効果

POINT  
1

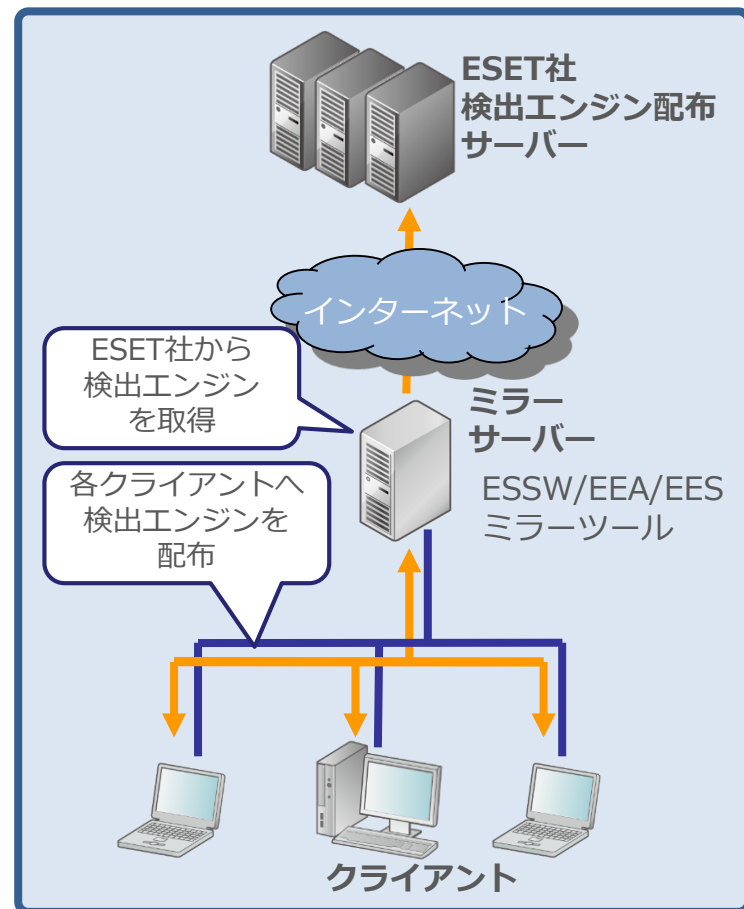
アップデートに伴う各クライアントからのインターネットアクセスをなくし、ネットワーク負荷を軽減する。

POINT  
2

インターネットへ直接アクセスできない環境でも定期的にアップデートが可能になる。

POINT  
3

ミラーサーバーに保存された検出エンジンのデータベースを使用して、ネットワークに接続されていないクライアントをアップデートすることができる。







# 規模別構成例

**Canon**

キヤノンマーケティングジャパン株式会社



管理するクライアント数に応じて、各規模でのESET PROTECTソリューションの構成例と各サーバーのスペックの目安を紹介します。

### 規模別構成例

| クライアント数               | 管理サーバーのOS            | 備考                         |
|-----------------------|----------------------|----------------------------|
| ～100                  | —                    | 管理サーバーを利用しない場合の構成          |
| ～1,000                | Windows サーバー / Linux |                            |
| 1,000～5,000           | Windows サーバー / Linux |                            |
| 5,000～10,000          | Windows サーバー / Linux |                            |
| 10,000～50,000         | Windows サーバー         |                            |
| 50,000～100,000        | Windows サーバー         |                            |
| オフライン環境の構成            |                      |                            |
| モバイル管理の構成             |                      | Mobile Device Connectorの追加 |
| ESET PROTECT Cloudの構成 |                      | オンプレミスでミラーサーバー なし          |
| ESET PROTECT Cloudの構成 |                      | オンプレミスでミラーサーバー あり          |

※10,000クライアントまでは、管理サーバーのOSとしてLinuxをご利用いただけます。

※ESET PROTECT Cloudの最大管理可能端末数は25,000です。

※本資料でご案内しているCPUのクロック数は2.10GHzを想定しています。

※本資料では、Windows サーバーでの構成例を記載しておりますが、Linuxをご利用の場合でも、構成例に違いはございません。

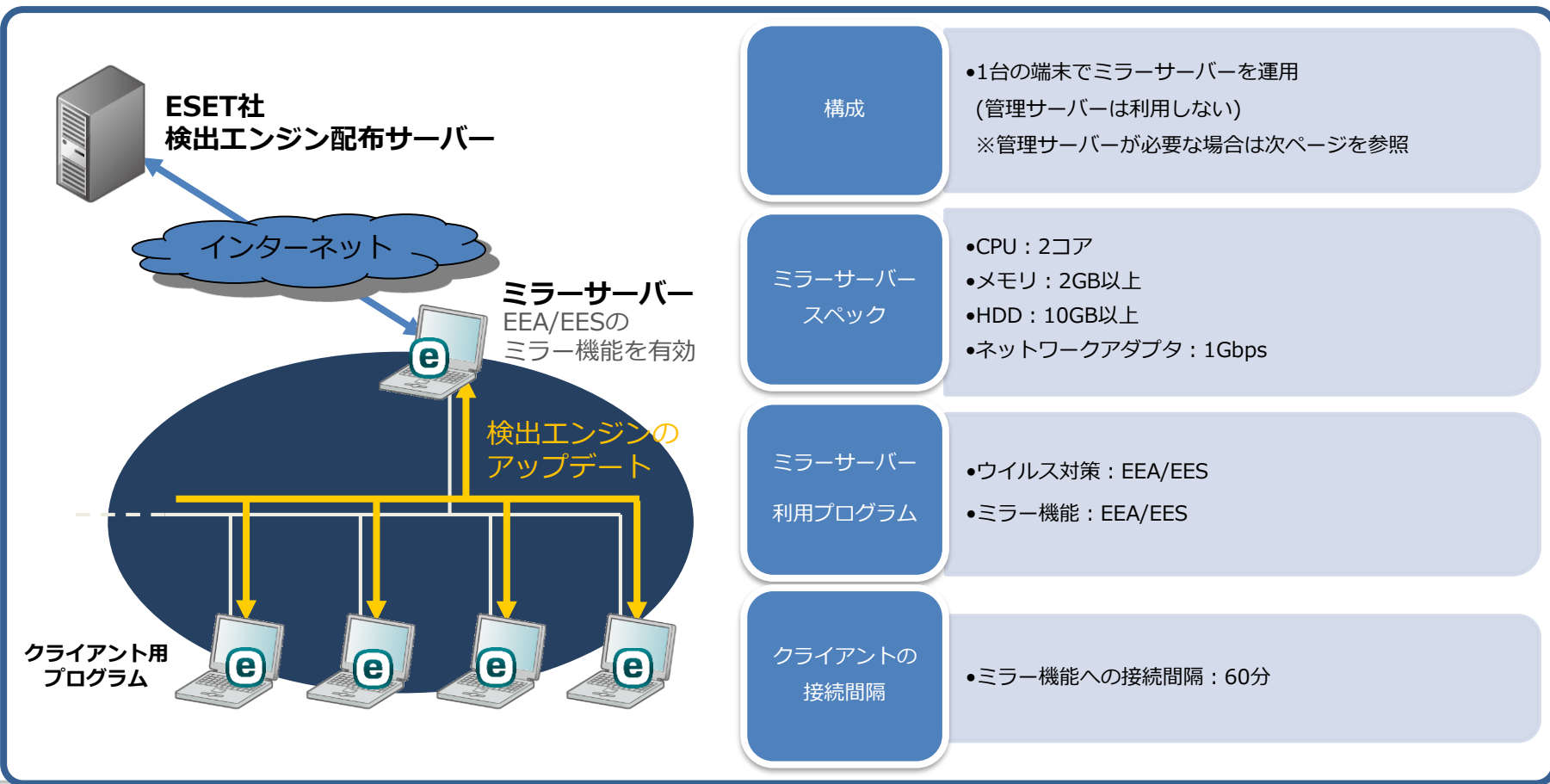
※Linuxをミラーサーバーとしてご利用になる場合は、ミラーツールをご利用ください。

# 規模別構成例(～100クライアント)



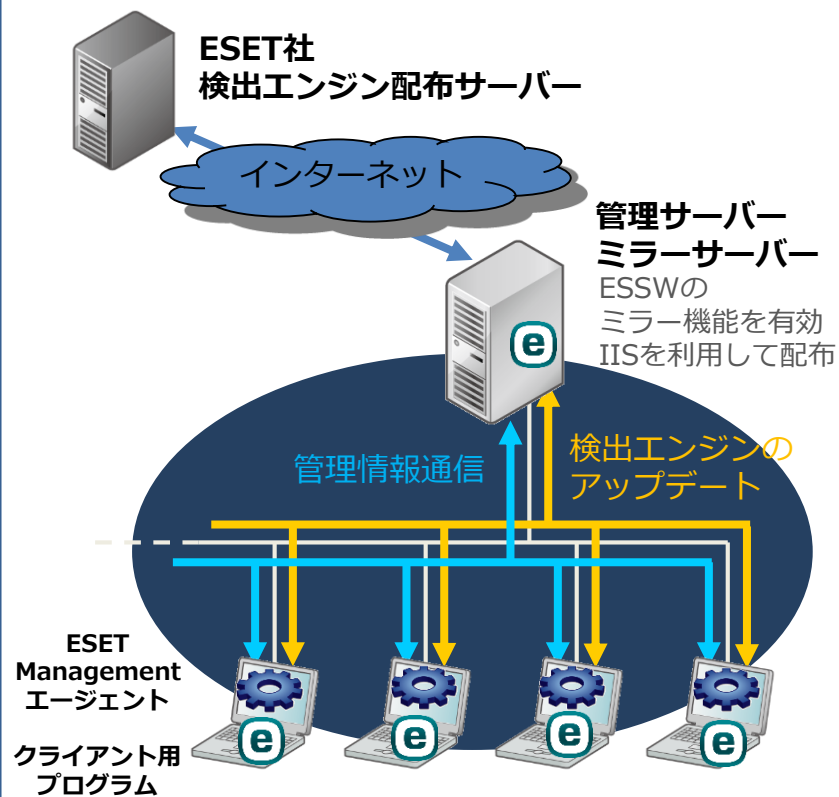
ESET PROTECTソリューションは、管理サーバーを利用せずにクライアントだけを運用することができます。

管理サーバーが不要な場合や小規模支店などは本構成例を参考にしてください。



## 規模別構成例(～1,000クライアント)

本構成例は、1台のサーバー機で管理サーバーとミラーサーバーを運用します。検出エンジンを配布する対象のクライアント数が400を超える場合は、IISを利用して配布します。



### 構成

- 1台のサーバー機で管理サーバーとミラーサーバーを運用

### サーバー スペック

- CPU : 4コア
- メモリ : 4GB
- HDD : 100GB
- ネットワークアダプタ : 1Gbps

### サーバーの 利用プログラム

- ウイルス対策 : ESSW
- ミラー機能 : ESSW(IISを利用して配布)
- 管理機能 : EP
- データベース : MS SQL Express(既定)

### クライアントの 接続間隔

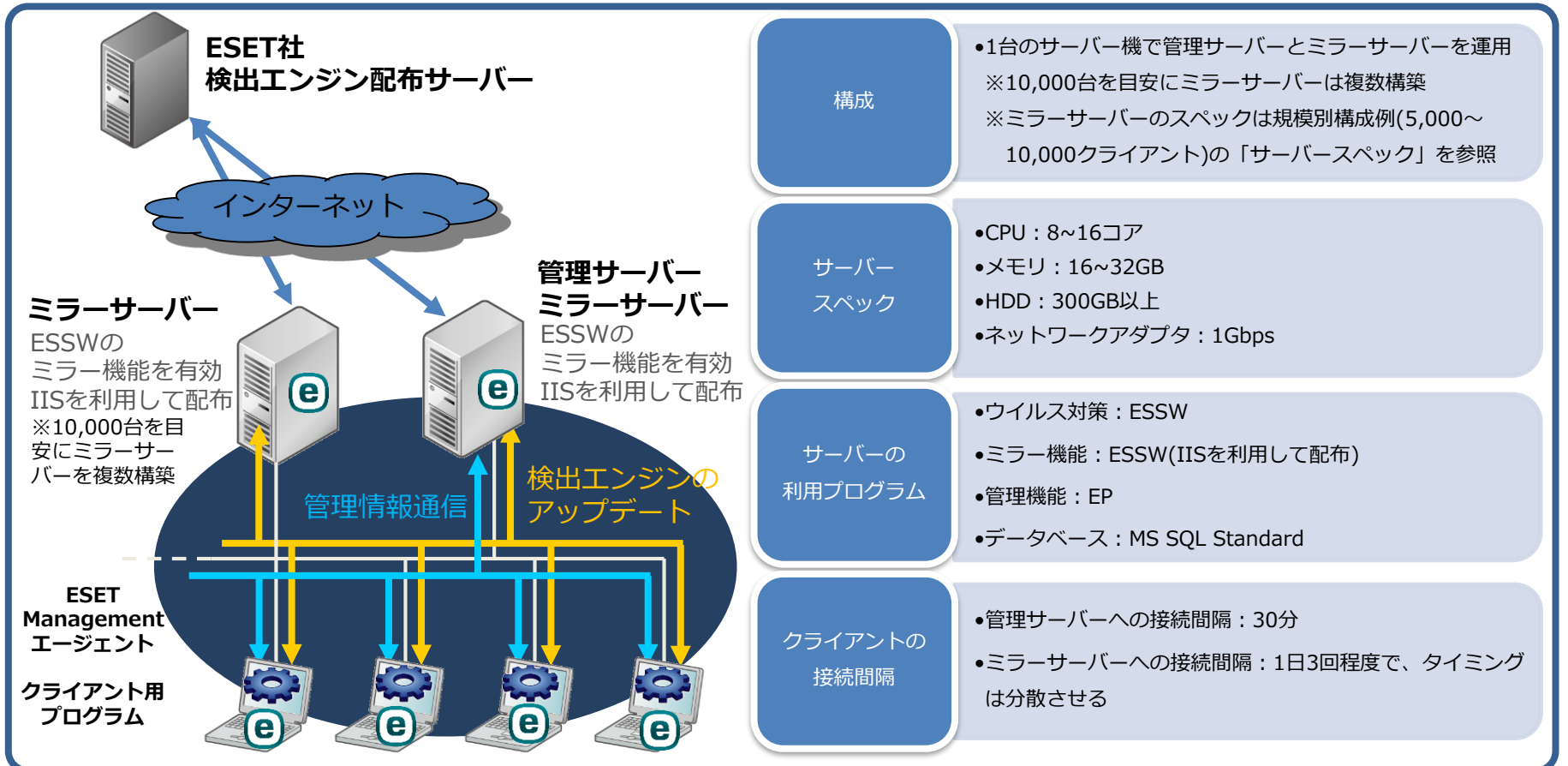
- 管理サーバーへの接続間隔 : 10分
- ミラーサーバーへの接続間隔 : 60分





# 規模別構成例(10,000~50,000クライアント)

本構成例は、大規模であるため、高スペックのサーバーで管理サーバーとミラーサーバーを運用します。また、10,000クライアントを目安にミラーサーバーを複数構築します。



## 構成

- 1台のサーバー機で管理サーバーとミラーサーバーを運用  
※10,000台を目安にミラーサーバーは複数構築  
※ミラーサーバーのスペックは規模別構成例(5,000~10,000クライアント)の「サーバースペック」を参照

## サーバー スペック

- CPU : 8~16コア
- メモリ : 16~32GB
- HDD : 300GB以上
- ネットワークアダプタ : 1Gbps

## サーバーの 利用プログラム

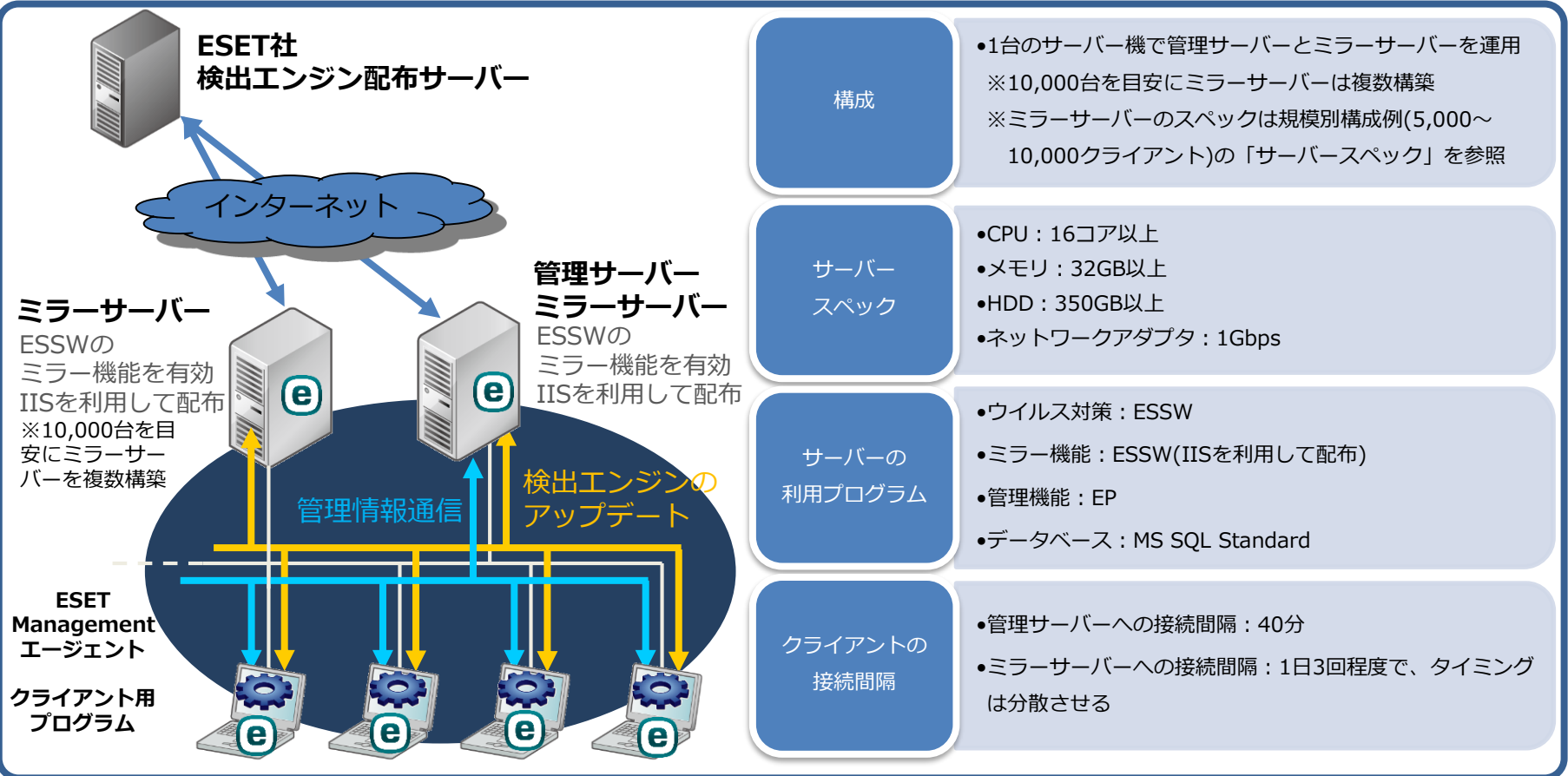
- ウイルス対策 : ESSW
- ミラー機能 : ESSW(IISを利用して配布)
- 管理機能 : EP
- データベース : MS SQL Standard

## クライアントの 接続間隔

- 管理サーバーへの接続間隔 : 30分
- ミラーサーバーへの接続間隔 : 1日3回程度で、タイミングは分散させる

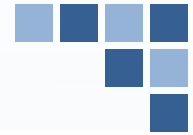
# 規模別構成例(50,000~100,000クライアント)

本構成例は、大規模であるため、高スペックのサーバーで管理サーバーとミラーサーバーを運用します。さらに規模が大きくなりサーバーやネットワーク負荷が高くなる可能性があるため、管理サーバーへの接続間隔の延長や検出エンジンの取得タイミングを分散させます。



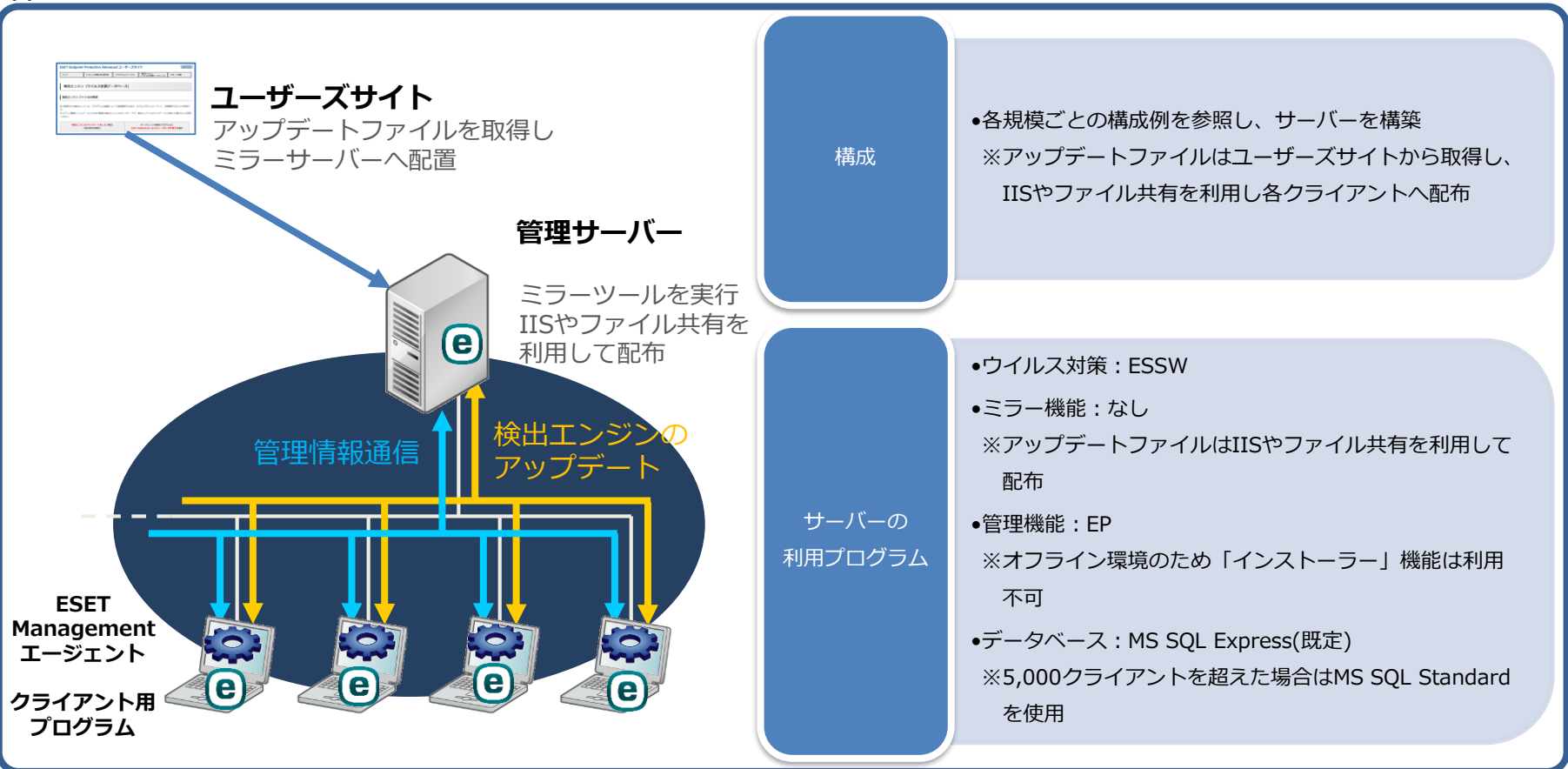


# オフライン環境の構成例



オフライン環境の場合、クライアントに配布するアップデートファイルは、ユーザーズサイトから取得し、サーバーに配置します。

配置したアップデートファイルをIISやファイル共有を利用し各クライアントへ配布します。

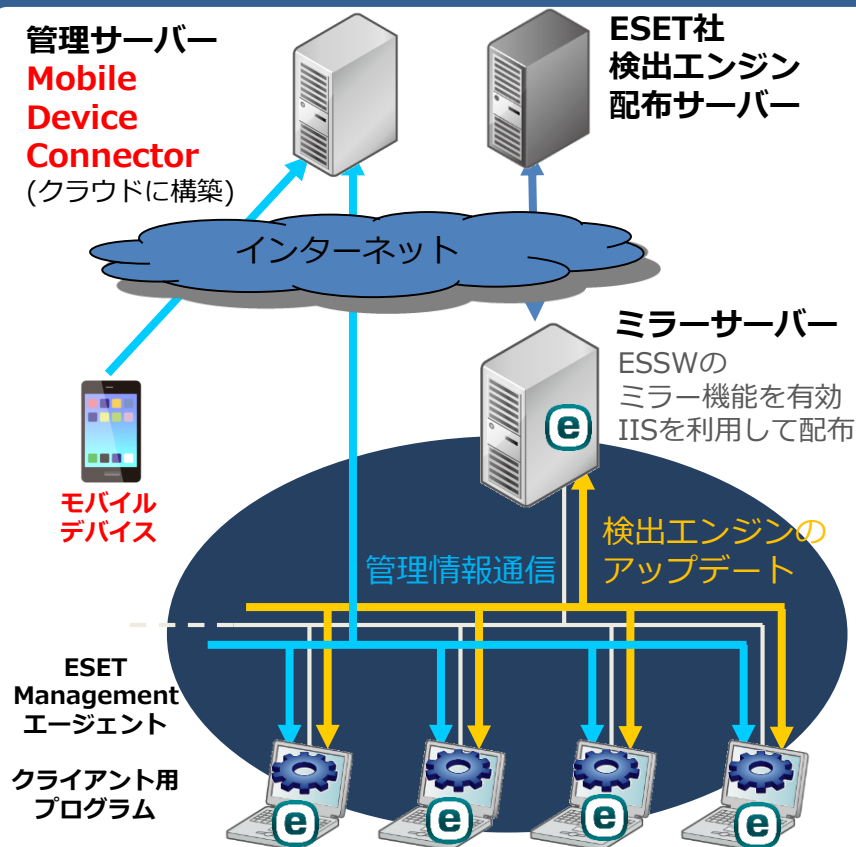


# モバイル管理の構成例

Endpoint Antivirus



Android向けプログラムやiOSのモバイルデバイスを管理する場合は、各規模の構成例にMobile Device Connectorを追加します。Mobile Device Connectorはモバイルデバイスがアクセス可能な場所に設置します。ESET PROTECT Cloudをご利用の場合は、Mobile Device Connectorが含まれた状態で利用を開始できます。



## 構成

- 各規模の構成例にMobile Device Connectorを追加
- ※モバイルデバイスがアクセス可能な場所に設置
- ※本構成のように管理サーバーと同居することも可能
- ※EPCを利用の場合は構築不要

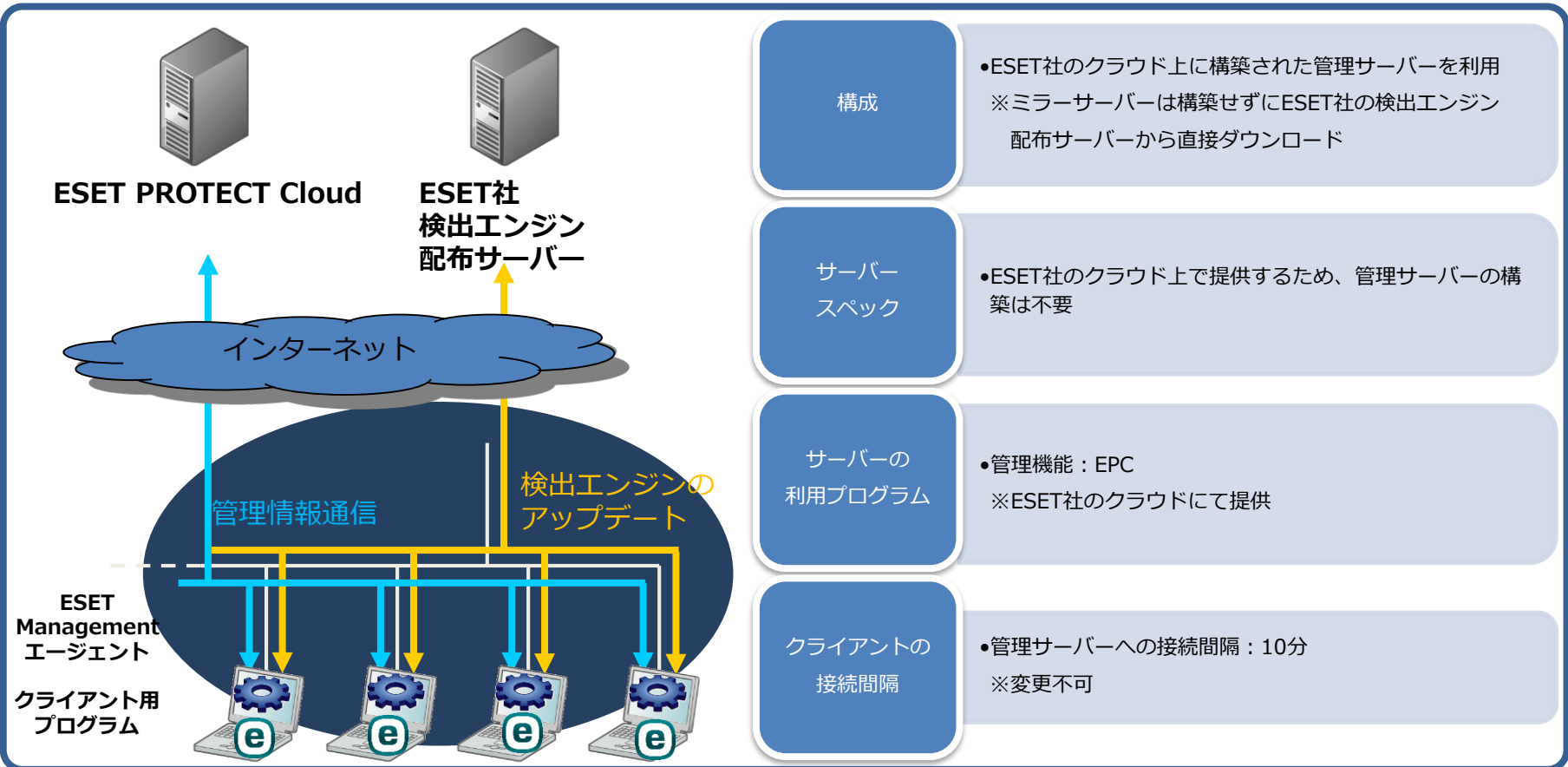
## Mobile Device Connector スペック

- CPU : 4コア以上
- メモリ : 4GB以上
- HDD : 100GB以上
- ※管理サーバーと同居する場合は、本スペックとの合計値を使用

# ESET PROTECT Cloudの構成例 (オンプレミスでミラーサーバー なし)



本構成例は、オンプレミスに管理サーバーを構築せずに、ESET PROTECT Cloudを利用した構成です。十分なネットワーク帯域を保持している環境を想定しているため、ミラーサーバーは社内に構築せずにインターネット経由で検出エンジンをダウンロードします。



## 構成

- ESET社のクラウド上に構築された管理サーバーを利用  
※ミラーサーバーは構築せずにESET社の検出エンジン配布サーバーから直接ダウンロード

## サーバー スペック

- ESET社のクラウド上で提供するため、管理サーバーの構築は不要

## サーバーの 利用プログラム

- 管理機能：EPC  
※ESET社のクラウドにて提供

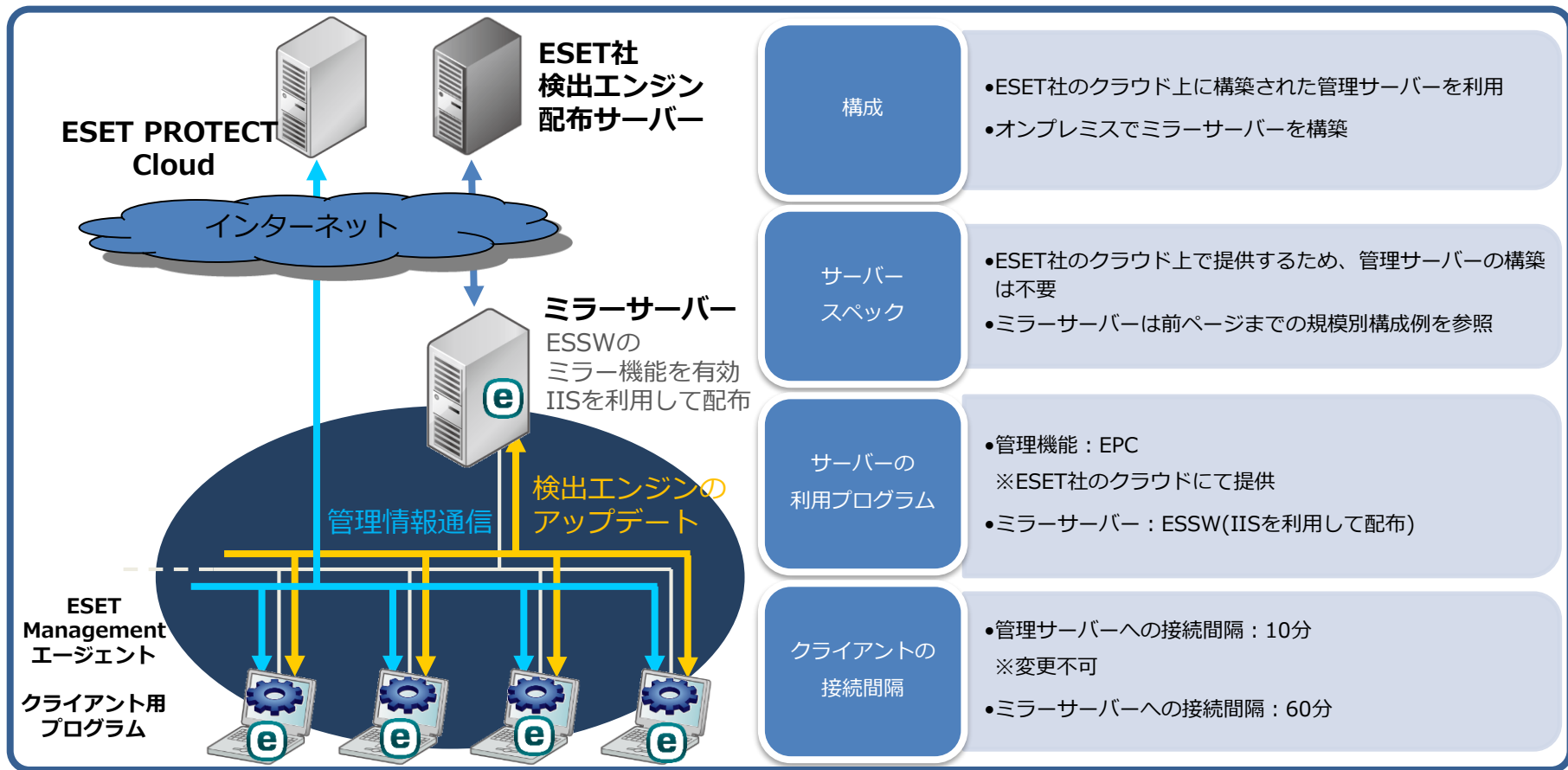
## クライアントの 接続間隔

- 管理サーバーへの接続間隔：10分  
※変更不可

# ESET PROTECT Cloudの構成例 (オンプレミスでミラーサーバー あり)



本構成例は、オンプレミスに管理サーバーを構築せずにESET PROTECT Cloudを利用した構成です。大規模の環境を想定しているため、ミラーサーバーをオンプレミスで構築し、アップデートに伴うネットワーク負荷を軽減します。





## 参考情報

**Canon**

キヤノンマーケティングジャパン株式会社

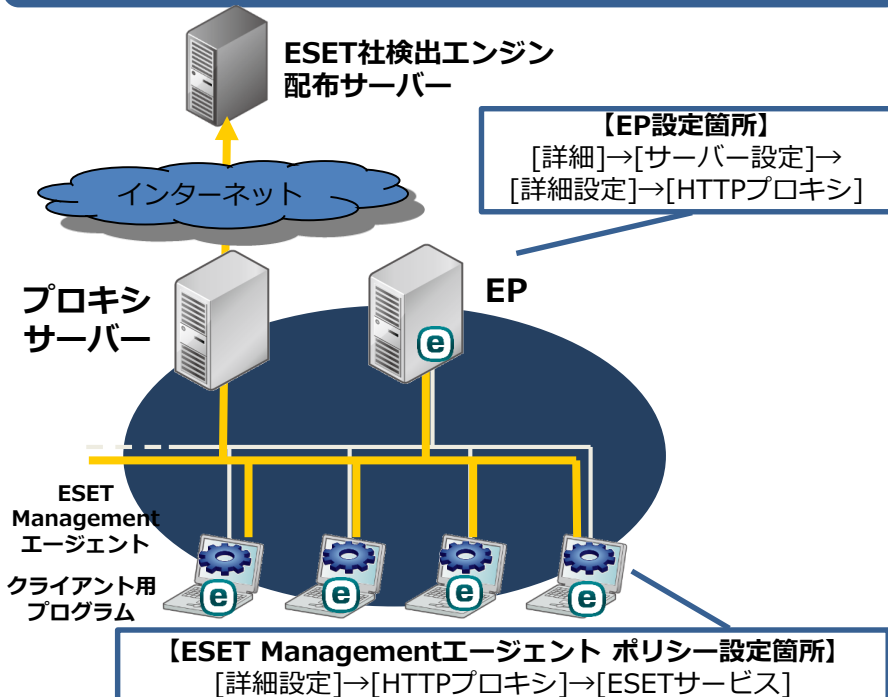
# 管理サーバーおよびエージェントのアップデートについて

ESET PROTECTおよび各クライアントにインストールされているESET Managementエージェントも定期的にアップデートを行います。

既定では、インターネットからアップデートファイルを取得しますが、ネットワーク環境に合わせて設定変更が必要な場合があります。

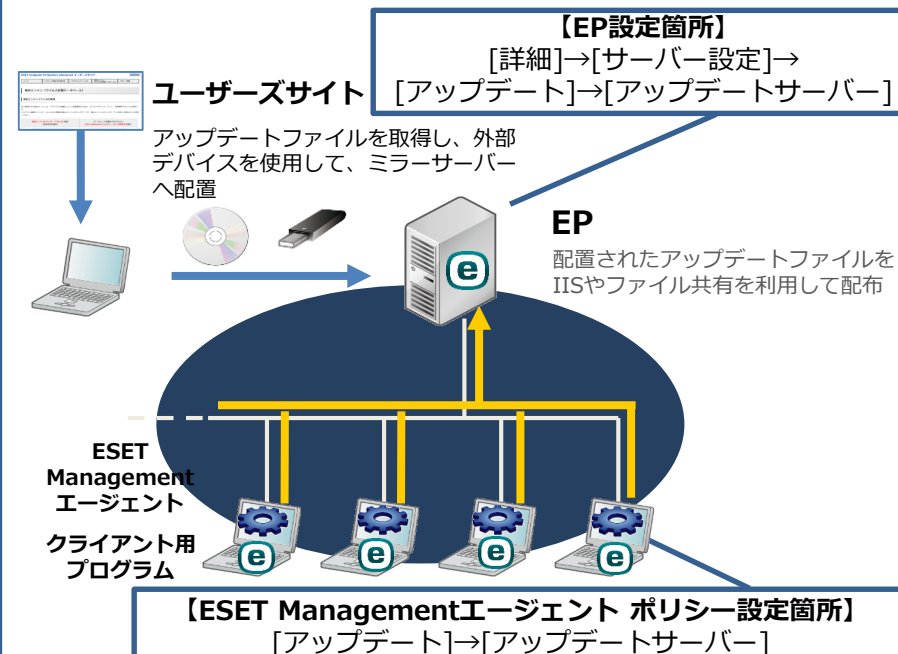
## プロキシを経由する環境

EPおよびESET Managementエージェントの両方でプロキシサーバーの設定を入力する必要があります。



## オフライン環境

ユーザズサイトから取得したアップデートファイルを利用するため、EPおよびESET Managementエージェントの両方でアップデート先を変更する必要があります。



## トラフィック量の計算(管理サーバー)

管理サーバーとクライアントのネットワークトラフィックは、管理サーバーへの接続間隔やクライアントによって実行されるアクションによって異なります。主なトラフィックは以下の通りです。

| 管理サーバーへの接続間隔 | 1日のトラフィックの合計値 |
|--------------|---------------|
| 1分           | 16MB          |
| 15分          | 1MB           |
| 30分          | 0.5MB         |
| 60分          | 144KB         |
| 1日           | 12KB          |

| 実行されるアクション                     | アクション実行時のトラフィック |
|--------------------------------|-----------------|
| クライアントタスク:<br>オンデマンド検査         | 4KB             |
| クライアントタスク:<br>モジュールアップデート      | 4KB             |
| クライアントタスク:<br>SysInspectorログ要求 | 300KB           |
| ポリシー:ウイルス対策 - 最大のセキュリティ        | 26KB            |

管理サーバー運用時の1日トラフィックを試算するには以下の式を利用します。

$$\text{クライアント数} \times (\text{1日のトラフィックの合計値} + (\text{アクション実行時のトラフィック} \times \text{実行回数}))$$

1,000クライアントを管理しており、管理サーバーの接続間隔を15分、管理している全クライアントにモジュールアップデート、オンデマンド検査、ポリシー配布を各3回行われるとした場合、1日のトラフィック量は約1GBとなります。

# トラフィック量の計算(ミラーサーバー)



ミラーサーバーとクライアントのネットワークトラフィックは、以下の通りです。

| 種別         | サイズ                         | 備考  |
|------------|-----------------------------|---|
| 検出エンジン     | 約数KB～約数百KB<br>(約10KB～約2MB)  | 日々配布される、ウイルスの特徴を収録しているファイルです。<br>1日に4～5回程度配布されます。   |
| ベースアップデート① | 約数KB～約数百KB<br>(約数MB～約15MB)  | 検出エンジン効率化のためのパッキングされたファイルになります。<br>年に3回～4回程度配布されます。 |
| ベースアップデート② | 約数KB～約10MB<br>(約十数MB～約40MB) | 検出エンジン効率化のためのパッキングされたファイルになります。<br>年に1回程度配布されます。    |
| 新モジュール追加   | 約1MB～約5MB                   | 不定期に新モジュールが追加される場合があります。                            |

以下の条件のどちらか1つ以上に該当する場合は、大きめのファイルサイズ(赤字記載)となります。

条件1： ESET File Security for Linux、ESET Mail Security for Linux、ESET Web Security for Linuxで構築したミラーサーバーから検出エンジンをアップデートしている場合

条件2： クライアント用プログラム側にて検出エンジンのアップデートを約4日間（20世代）以上間隔をあけて実施する場合

※詳細については以下のURLをご確認ください。

【検出エンジン（ウイルス定義データベース）のサイズと更新頻度について】

[https://eset-support.canon-its.jp/faq/show/154?site\\_domain=business](https://eset-support.canon-its.jp/faq/show/154?site_domain=business)

※ベースアップデート時は、検出エンジンのダウンロードエラーや、ネットワークトラフィックの増加などの問題が一時的に発生する場合があります。これらの問題は、一般的には時間の経過とともに解決します。

ベースアップデートについての詳細は以下をご参照ください。

【ベースアップデートの実施について】

[https://eset-support.canon-its.jp/faq/show/228?site\\_domain=business](https://eset-support.canon-its.jp/faq/show/228?site_domain=business)