ESET Endpoint Protection シリーズ
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5版
作成：2020年8月3日

キヤノンマーケティングジャパン株式会社

初めに

本資料は、「ESET Endpoint Protectionシリーズ」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 Security Management Center	7.X	ESMC	Windows サーバー用 Linuxサーバー用	クライアント 管理用プログラム ※ESET Remote Administratorの後継
ESET Endpoint Security	7.X	EES	Windows クライアント用	総合セキュリティ プログラム
ESET Endpoint アンチウイルス	7.X	EEA		ウイルス・スパイウェア 対策プログラム
ESET File Security for Microsoft Windows Server	7.X	EFSW	Windows サーバー用	ウイルス・スパイウェア 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 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 対策プログラム
ESET NOD32アンチウイルス for Linux Desktop	4.0	EAVL	Linux デスクトップ用	ウイルス・スパイウェア 対策プログラム
ESET File Security for Linux	4.5	EFSL	Linux サーバー用	ウイルス・スパイウェア 対策プログラム
ESET Endpoint Security for Android	2.X	EESA	Android用	ウイルス・スパイウェア 対策プログラム

※本資料では、適宜上記のプログラム名や略称を使用して説明いたします。

目次

- **ESET Endpoint Protectionシリーズにおけるサーバーの構成要素**
  - ESET Security Management Center
  - 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(～400クライアント)
  - 規模別構成例(～1000クライアント)
  - 規模別構成例(1000～5000クライアント)
  - 規模別構成例(5000～10000クライアント)
  - 規模別構成例(10000～50000クライアント)
  - 規模別構成例(50000～100000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
  - クラウドオプション、または、クラウドオプション Liteの構成
- **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
  - データベースの選定
  - 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 Endpoint Protectionシリーズにおける 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 Security Management Center

ESET Security Management Center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プログラムです。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 Security Management Center（ESMC）

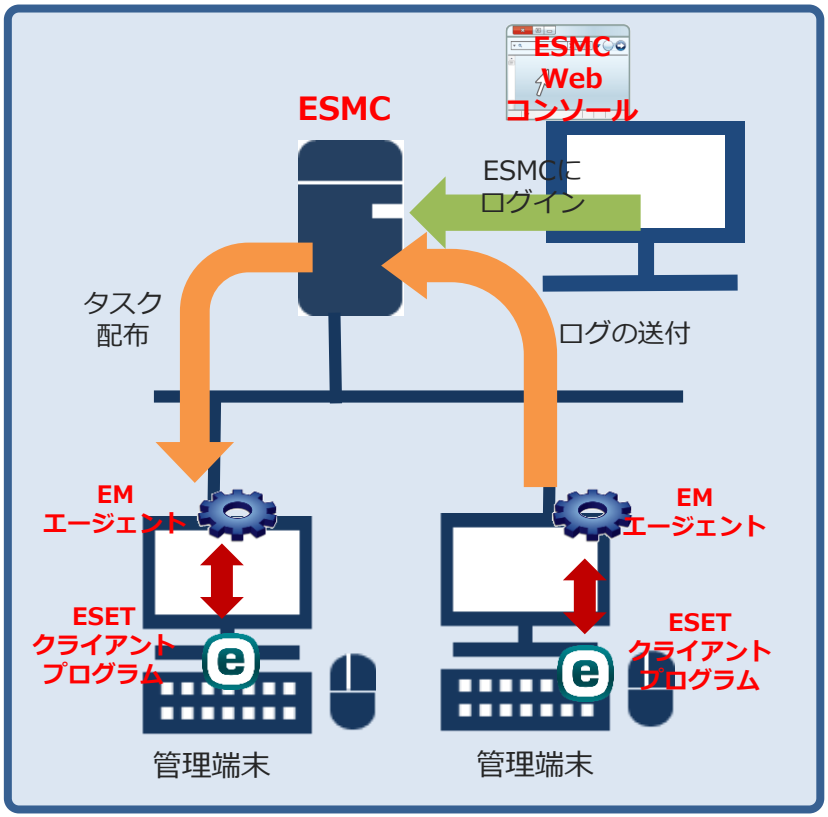
ESMCはクライアントプログラムの情報収集やタスク配布などを行います。クライアントとの通信はエージェントを経由して行います。

ESMC 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、ブラウザーを使用してESMCへアクセスします。ブラウザー経由でクライアント情報の閲覧やESMC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ESMCへデータを送信します。また、ESMC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。

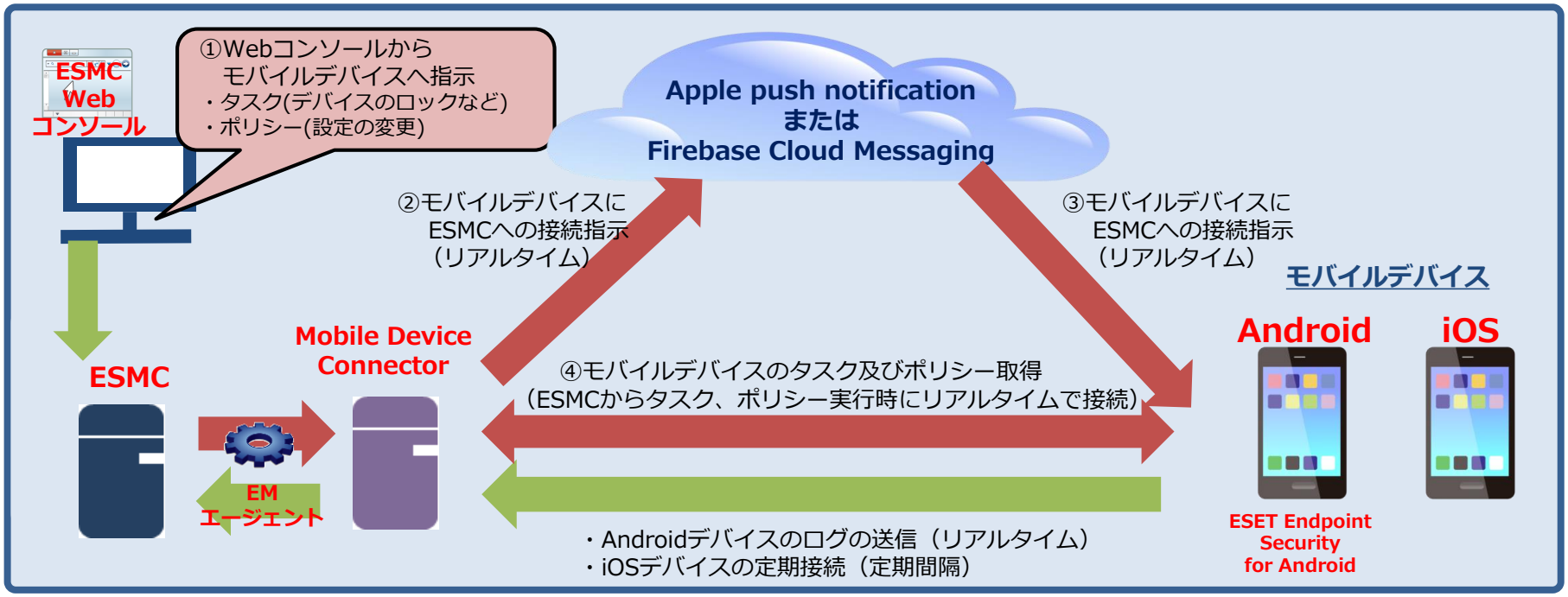


Mobile Device Connector

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

ESMC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ESMCに含めることができます。



ミラーサーバー

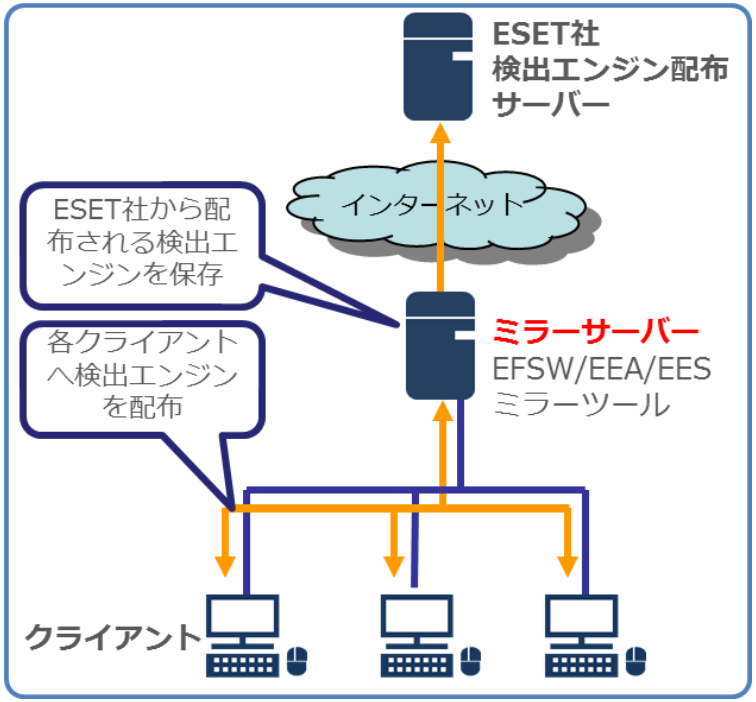
ミラーサーバーとは、ESET社から配布される検出エンジンなどのアップデートファイルを保存し、クライアントに配布する機能をもつサーバーです。
プログラムに搭載されているミラー機能またはミラーツールを使用して、ミラーサーバーを構築することができます。

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。



ESET File Security for Linuxをご利用の場合は、ミラーツールをご利用ください。
Linuxでミラーツールを利用したミラーサーバーの構築手順は下記をご確認ください。
https://eset-support.canon-its.jp/faq/show/4495?site_domain=business

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

規模別構成例

管理するクライアント数に応じて、各規模でのESET Endpoint Protection シリーズ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

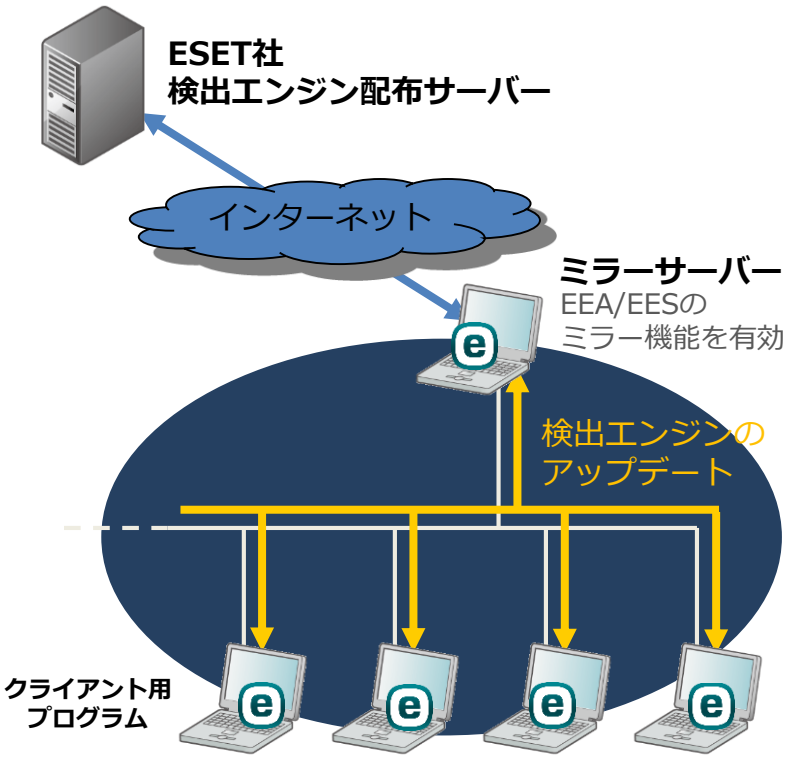
クライアント数	管理サーバーのOS	備考
～100	ー	管理サーバーを利用しない場合の構成
～400	Windows サーバー / Linux	
～1000	Windows サーバー / Linux	
1000～5000	Windows サーバー / Linux	
5000～10000	Windows サーバー / Linux	
10000～50000	Windows サーバー	
50000～100000	Windows サーバー	
オフライン環境の構成		
モバイル管理の構成		Mobile Device Connectorの追加
クラウドオプション、または、クラウドオプション Liteの構成		オンプレミスでミラーサーバー　なし
クラウドオプション、または、クラウドオプション Liteの構成		オンプレミスでミラーサーバー　あり

※10000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。
※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 Endpoint Protectionシリーズは、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。

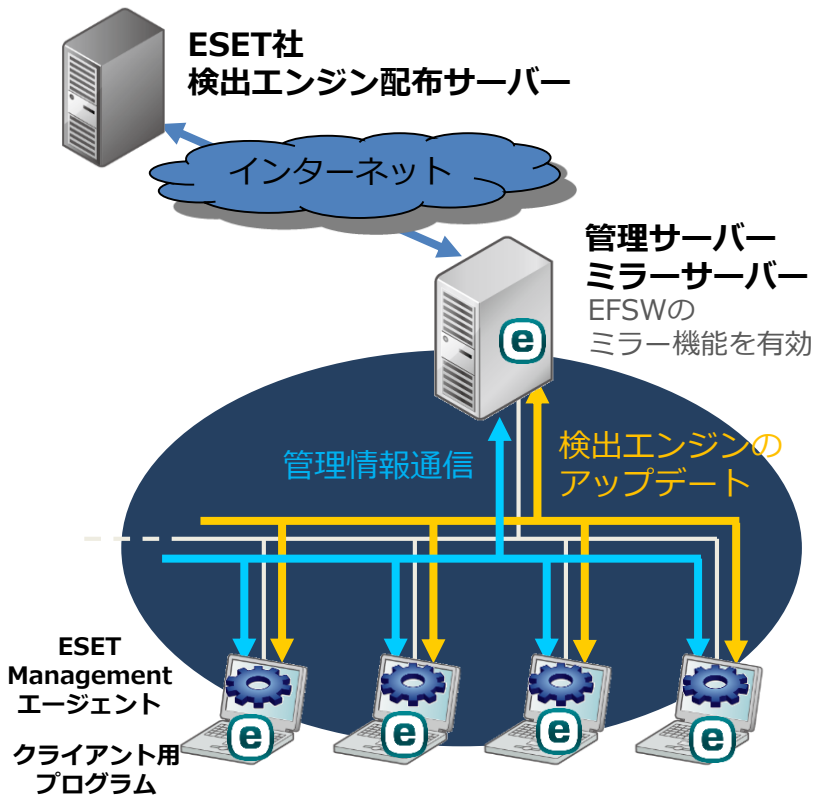
管理サーバーが不要な場合や小規模支店などは本構成例を参考にしてください。



構成	•1台の端末でミラーサーバーを運用 (管理サーバーは利用しない) ※管理サーバーが必要な場合は次ページを参照
ミラーサーバー スペック	•CPU：2コア •メモリ：2GB以上 •HDD：10GB以上 •ネットワークアダプタ：1Gbps
ミラーサーバー 利用プログラム	•ウイルス対策：EEA/EES •ミラー機能：EEA/EES
クライアントの 接続間隔	•ミラー機能への接続間隔：60分

規模別構成例(～400クライアント)

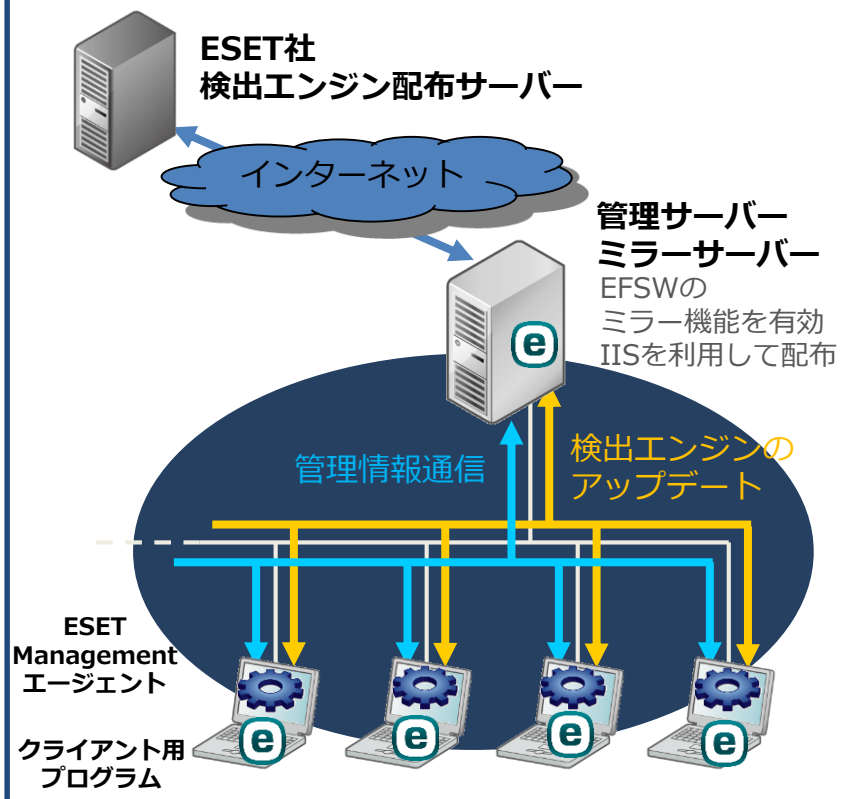
本構成例は、１台のサーバー機で管理サーバーとミラーサーバーを運用します。
クライアント管理と検出エンジンの配布を実施する場合の基本的な構成となります。
規模にかかわらず、管理サーバーは1台で運用することが可能です。



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：2コア •メモリ：4GB以上 •HDD：50GB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：EFSW •ミラー機能：EFSW •管理機能：ESMC •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(～1,000クライアント)

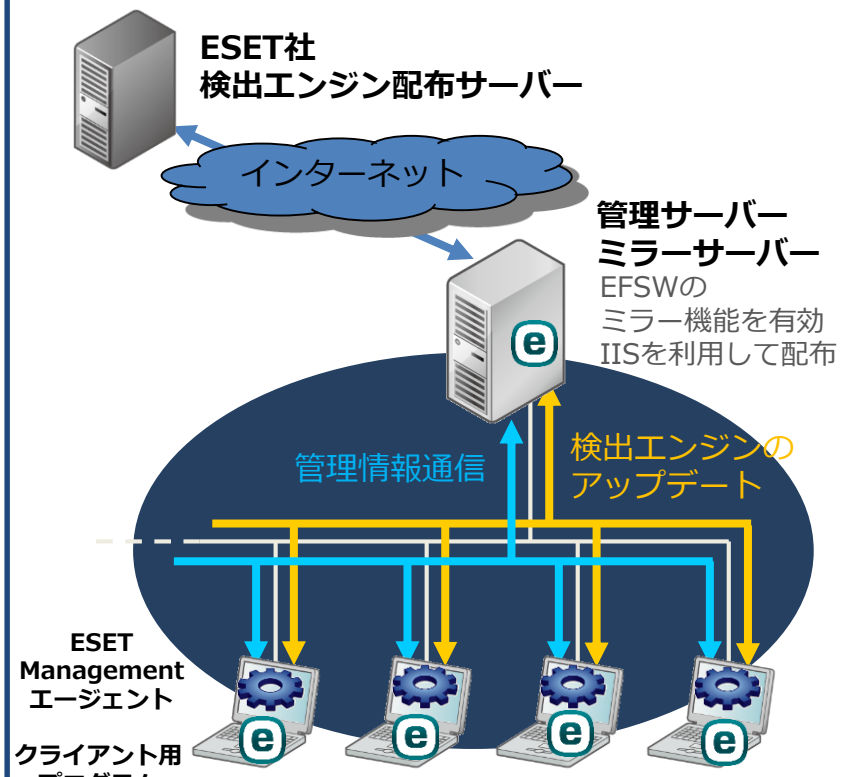
本構成例は、１台のサーバー機で管理サーバーとミラーサーバーを運用します。
検出エンジンを配布する対象のクライアント数が400を超える場合は、IISを利用して配布します。



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：EFSW •ミラー機能：EFSW(IISを利用して配布) •管理機能：ESMC •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(1,000～5,000クライアント)

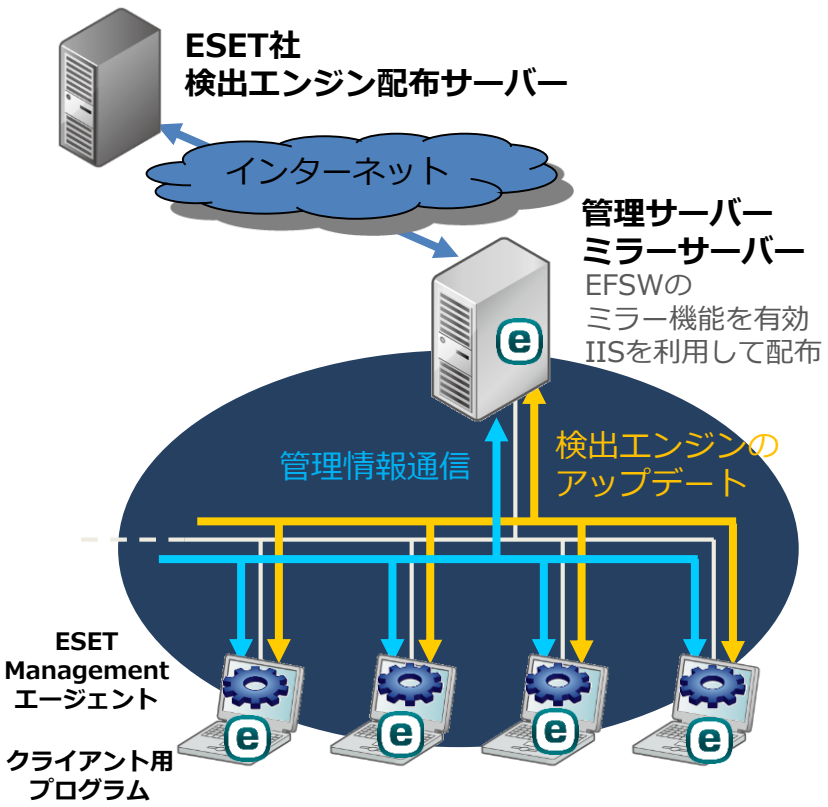
本構成例は、１台のサーバー機で管理サーバーとミラーサーバーを運用します。
なお、規模が大きいため、サーバースペック(CPUコア数やメモリなど)は高める必要があります。



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：4~8コア •メモリ：4~8GB •HDD：150GB •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：EFSW •ミラー機能：EFSW(IISを利用して配布) •管理機能：ESMC •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(5,000～10,000クライアント)

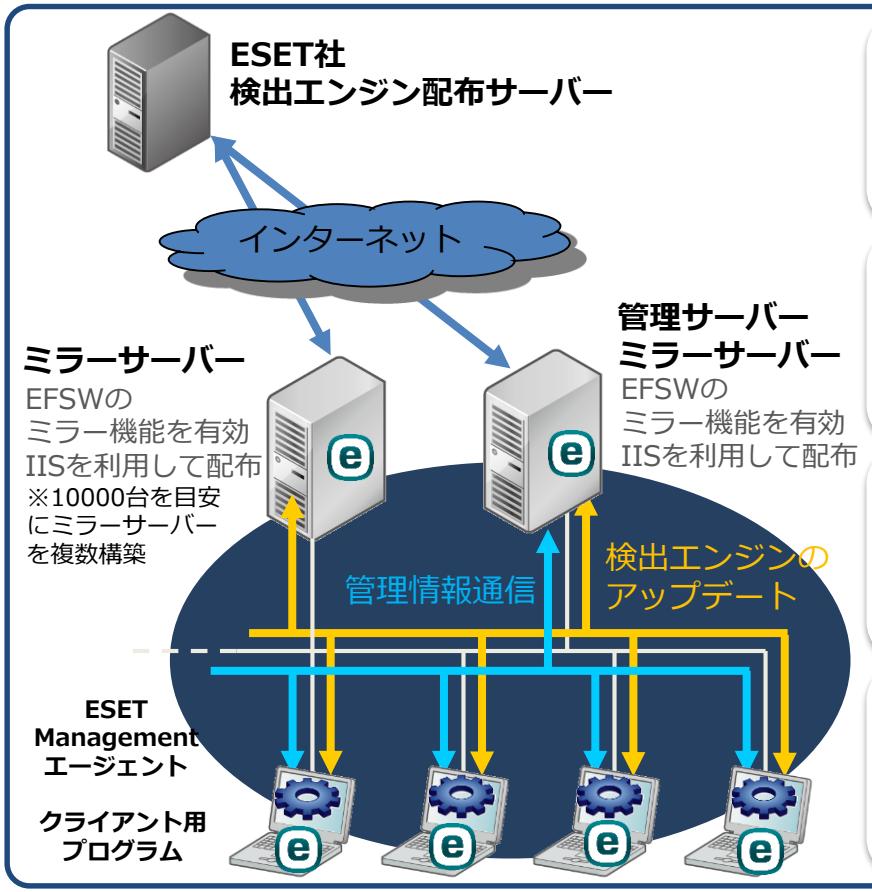
本構成例は、１台のサーバー機で管理サーバーとミラーサーバーを運用します。
多くのクライアントを管理するため、管理サーバーで利用するデータベースも
MS SQL Standardを利用します。また、管理サーバーへの接続間隔も20分程度に
延長し、サーバーやネットワークの負荷を軽減します。



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：8コア •メモリ：8～16GB •HDD：200GB •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：EFSW •ミラー機能：EFSW(IISを利用して配布) •管理機能：ESMC •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：20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)

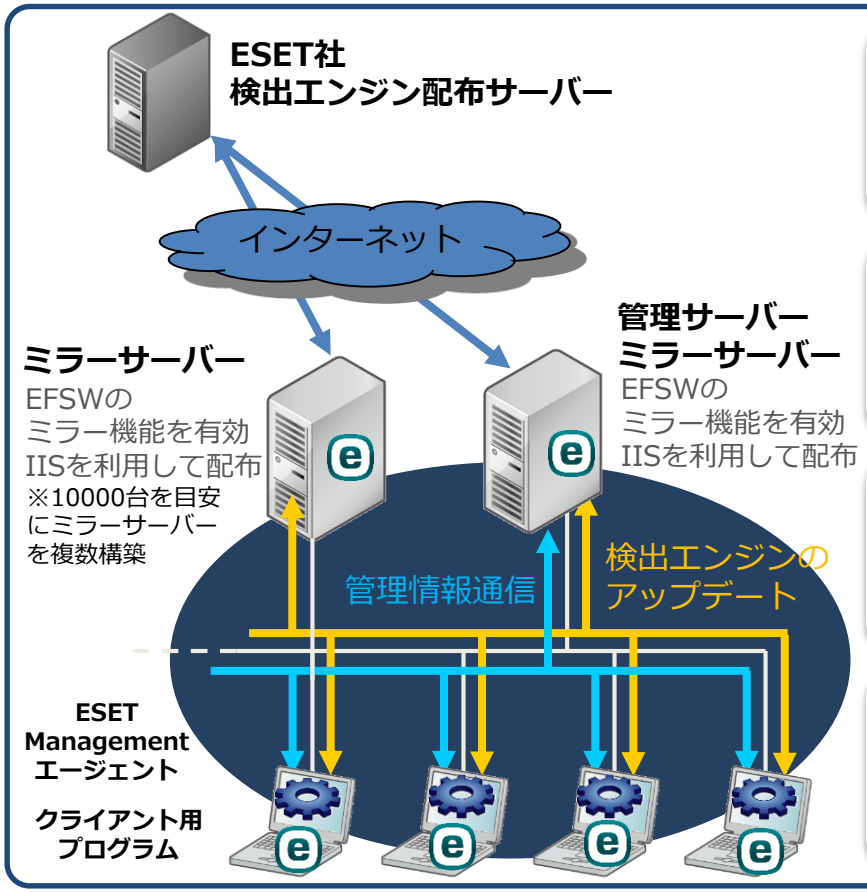
本構成例は、大規模であるため、高スペックのサーバーで管理サーバーとミラーサーバーを運用します。また、10000クライアントを目安にミラーサーバーを複数構築します。



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(5,000～10000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：EFSW •ミラー機能：EFSW(IISを利用して配布) •管理機能：ESMC •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)

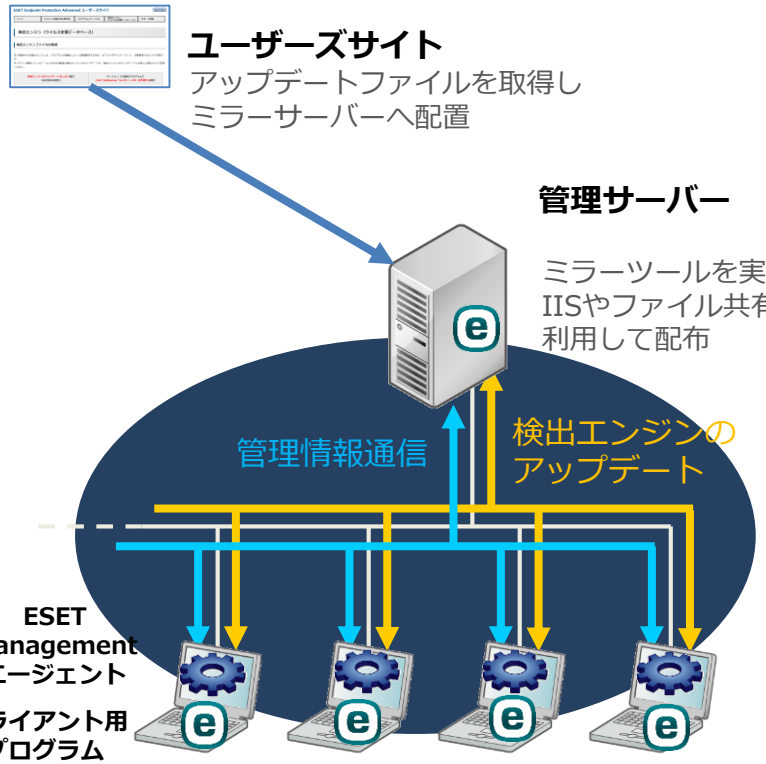
本構成例は、大規模であるため、高スペックのサーバーで管理サーバーとミラーサーバーを運用します。さらに規模が大きくサーバーやネットワーク負荷が高くなる可能性があるため、管理サーバーへの接続間隔の延長や検出エンジンの取得タイミングを分散させます。



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(5000～10000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：16コア以上 •メモリ：32GB以上 •HDD：350GB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：EFSW •ミラー機能：EFSW(IISを利用して配布) •管理機能：ESMC •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：40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

オフライン環境の構成例

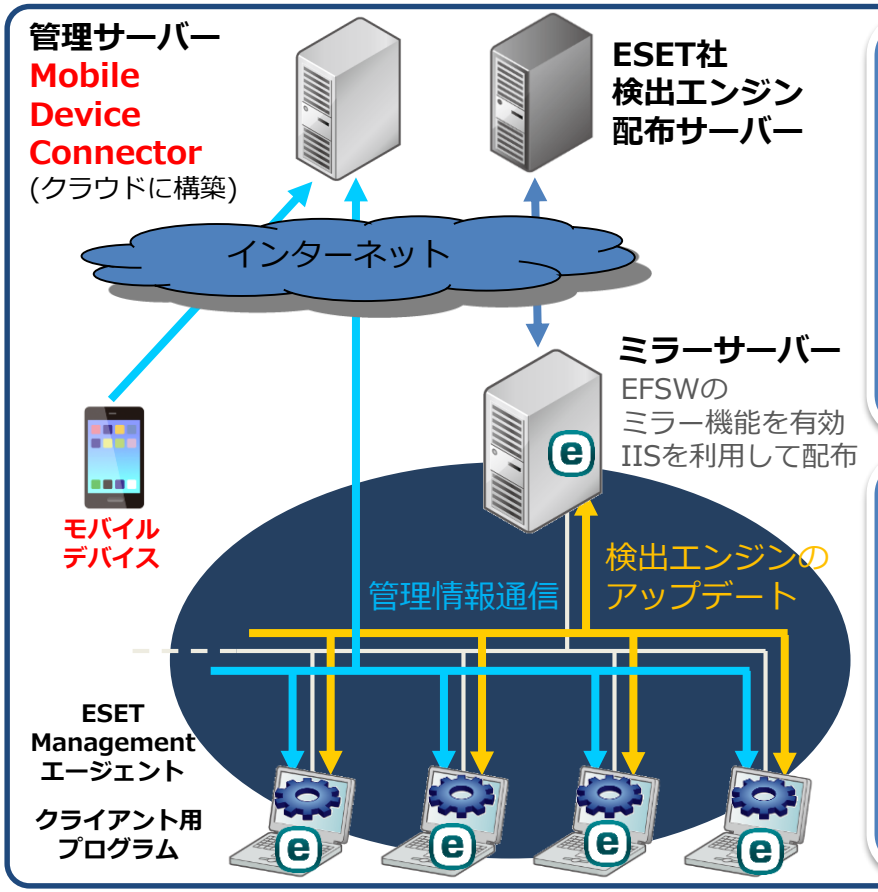
オフライン環境の場合、クライアントに配布するアップデートファイルは、ユーザーズサイトから取得し、サーバーに配置します。配置したアップデートファイルをIISやファイル共有を利用し各クライアントへ配布します。



構成	•各規模の構成例を参考にサーバーを構築 ※アップデートファイルはユーザーズサイトから取得し、IISやファイル共有を利用し各クライアントへ配布
サーバーの利用プログラム	•ウイルス対策：EFSW •ミラー機能：なし ※アップデートファイルはIISやファイル共有を利用して配布 •管理機能：ESMC ※オフライン環境のため「インストーラ」機能は利用不可 •データベース：MS SQL Express(既定) ※5000クライアントを超えた場合はMS SQL Standardを使用

モバイル管理の構成例

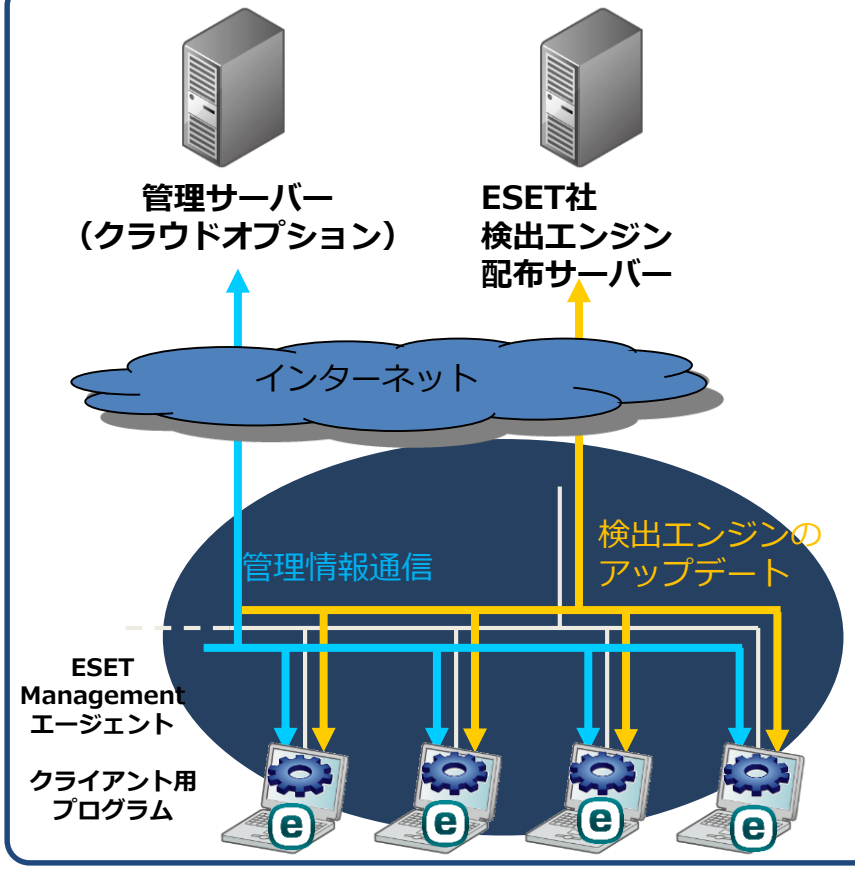
Android向けプログラムやiOSのモバイルデバイスを管理する場合は、各規模の構成例にMobile Device Connectorを追加します。Mobile Device Connectorはモバイルデバイスがアクセス可能な場所に設置します。



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
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

クラウドオプション、またはクラウドオプション Liteの構成例（オンプレミス　ミラーサーバーなし）

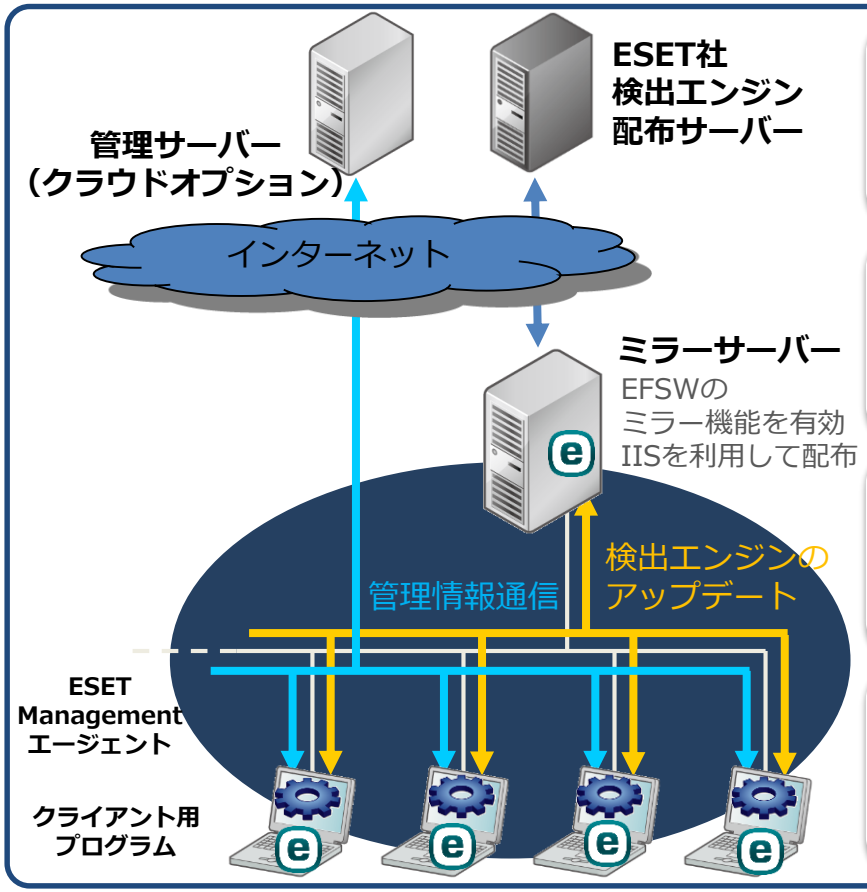
本構成例は、オンプレミスに管理サーバーを構築せずに弊社のクラウドオプション、または、クラウドオプション Liteを利用した構成です。十分なネットワーク帯域を保持している環境を想定しているため、ミラーサーバーは社内に構築せずにインターネット経由で検出エンジンをダウンロードします。



構成	•クラウドオプションの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	•クラウドオプションの為、不要です。 ※弊社にて提供
サーバーの 利用プログラム	•管理機能：ESMC ※弊社にて提供
クライアントの 接続間隔	•管理サーバーへの接続間隔：20分 ※変更不可

クラウドオプション、またはクラウドオプション Liteの構成例（オンプレミス　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弊社のクラウドオプションまたは、クラウドオプション Lite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。



構成	•クラウドオプションの管理サーバーとオンプレミスでミラーサーバーを構築
サーバースペック	•クラウドオプションの為管理サーバは不要 ※弊社にて提供 •ミラーサーバは前ページまでの規模別構成例を参照。
サーバーの利用プログラム	•管理機能：ESMC ※弊社にて提供 •ミラーサーバー：EFSW(IISを利用して配布)
クライアントの接続間隔	•管理サーバーへの接続間隔：20分 ※変更不可 •ミラーサーバーへの接続間隔：60分

参考情報

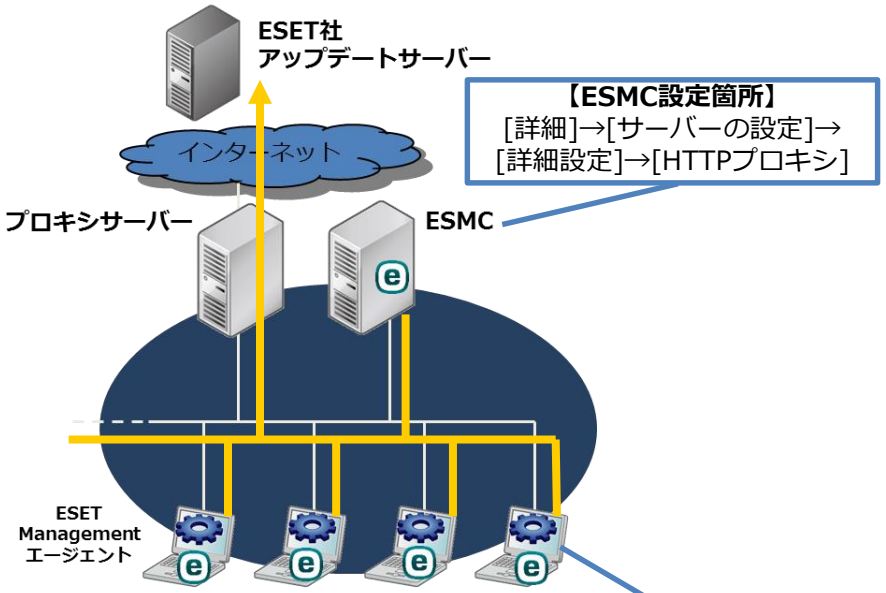
管理サーバーおよびエージェントのアップデートについて

ESET Security Management Center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。

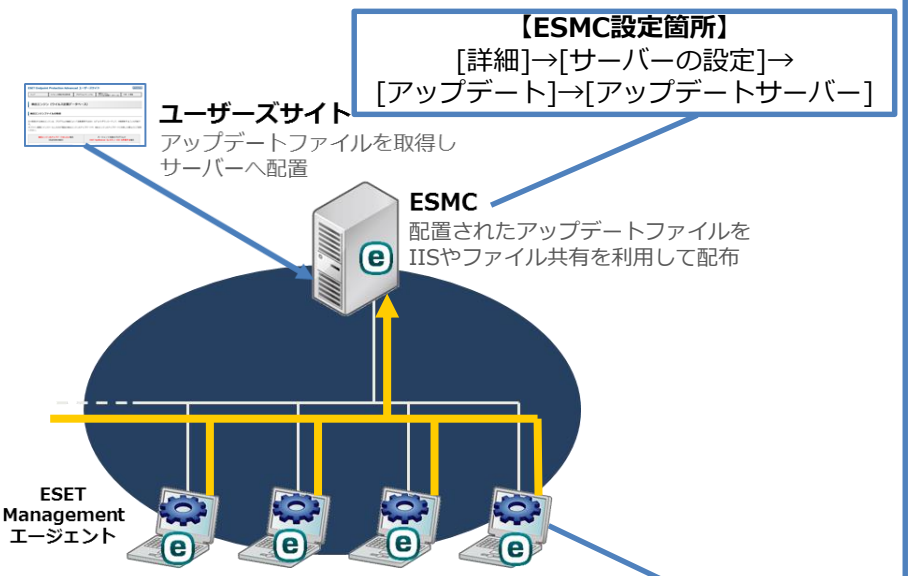
プロキシを経由する環境

ESMC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

ユーザー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、ESMC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。



データベースの選定

ESET Security Management Centerでは以下のデータベースを利用することができます。

プログラム	利用可能なデータベース	データベースの最大サイズ
ESMC(Windows版)	Microsoft SQL Server 2012、2014、2016、2017、2019 Standard Edition	制限なし
	Microsoft SQL Server 2012、2014、2016、2017、2019 Express Edition	10GBまで
ESMC(Linux版)	MySQL 5.6、5.7、8.0	制限なし

※Microsoft SQL Serverについて、エディションの指定はありません。主なエディションを記載しています。

5,000クライアントを管理しており、1クライアントあたり30件のログをデータベースに格納(計150,000件)した場合、データベースにはおよそ２GB のデータが蓄積されます。1日当たりのログの出力数を1000件とした場合、5か月間で２GB のデータが蓄積されます。

管理するクライアント数や1クライアントあたりのログ出力件数、1日あたりのログ出力件数などを試算し、お客様の運用に適切なデータベースを選択してください。

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
1分	16MB
15分	1MB
30分	0.5MB
60分	144KB

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
モジュールアップデート	4KB
オンデマンド検査	4KB
ポリシー配布	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。

クライアント数＊(1日のトラフィック+(アクション実行時のトラフィック＊1日に実行されるアクション発生数))

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 （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。 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 （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。 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 （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。 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： 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