ESET PROTECTソリューション
規模別構成例

第6版

2025年1月9日

キヤノンマーケティングジャパン株式会社

もくじ

1.はじめに（本資料について）

1.はじめに（本資料について）

- 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。
- 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でご用意しています。
- 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。
- 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

1.はじめに（本資料について）

- 本資料では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。
- 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。

プログラム名	バージョン	略称	種別	備考
ESET PROTECT on-prem	12.X	EP on-prem	Windows サーバー用 Linuxサーバー用	オンプレミス型セキュリティ管理ツール
ESET PROTECT	-（最新バージョンを提供）	EP	ESET社のクラウドにて提供	クラウド型セキュリティ管理ツール
ESET Endpoint Security	12.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	12.X	EEA		ウイルス・スパイウェア対策プログラム
ESET Server Security for Microsoft Windows Server（旧：ESET File Security for Microsoft Windows Server)	11.X	ESSW	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 macOS	8.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 Linux	11.X	EEAL	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 Server Security for Linux（旧：ESET File Security for Linux)	11.X	ESSL	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	5.X	EESA	Android用	総合セキュリティプログラム

※ Macクライアント用プログラムはV8より、ESET Endpoint Security for OS X とESET Endpoint アンチウイルス for OS X の表記による区別はなくなり、ESET Endpoint Security for macOS の表記に統一されました。ただし、表記は ESET Endpoint Security for macOS であっても機能はこれまでのESET Endpoint Security for OS X と ESET Endpoint アンチウイルス for OS X のように保有ライセンス種別により区別されます。

2.ESET PROTECTソリューションにおけるサーバーの構成要素

2-1.ESET PROTECT on-prem

ESET PROTECT on-prem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オンプレミス型のツールです。Windows、Mac、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 on-prem（EP on-prem）

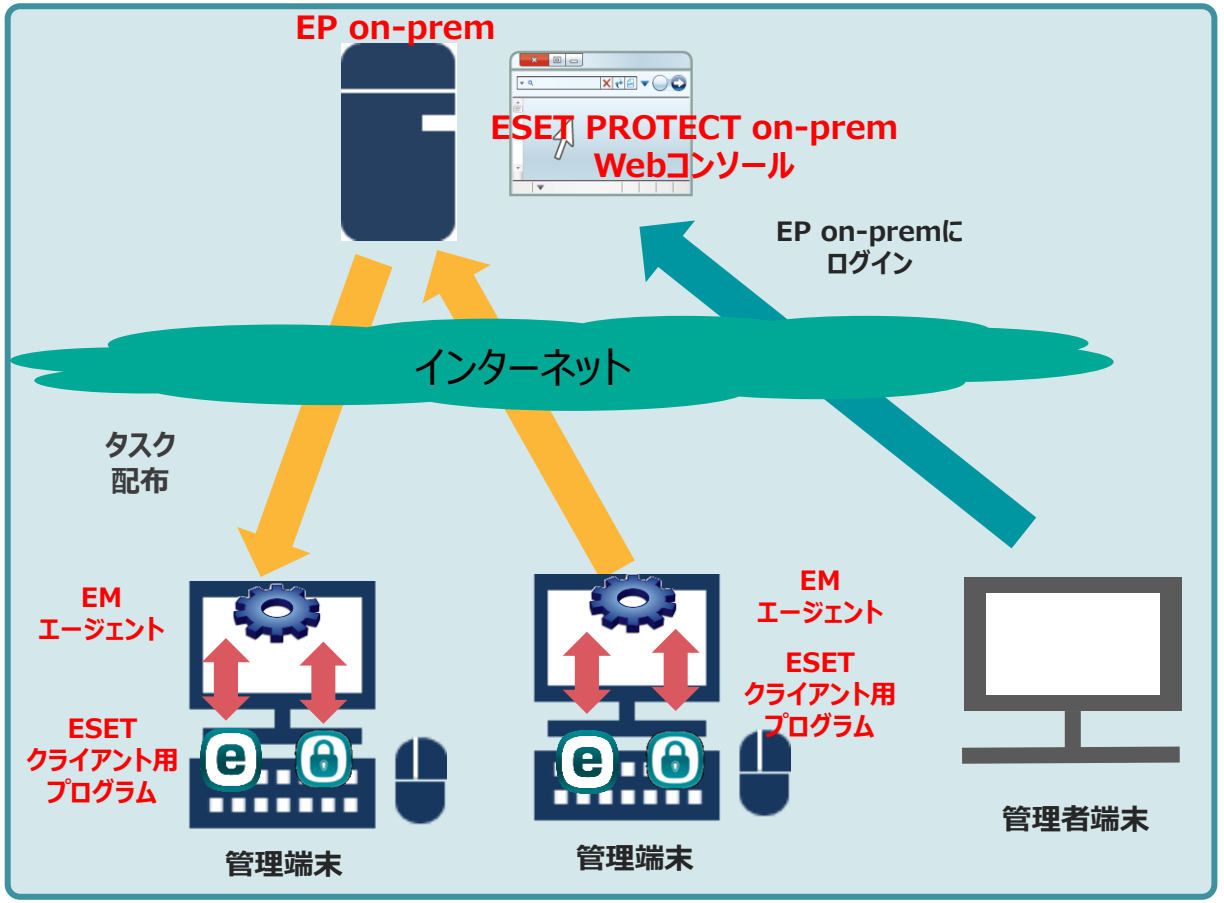
EP on-premはクライアントプログラムの情報収集やタスク配布などを行います。クライアントとの通信はエージェントを経由して行います。

ESET PROTECT on-prem 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EP on-prem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EP on-premへデータを送信します。また、EP on-prem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。
※EP on-premとEMエージェント間の通信には認証プロキシはご利用いただけません。



2-2.ESET PROTECT

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、ESET社のクラウド環境に構築されたクラウド型のツールです。Windows、Mac、Linux、Android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

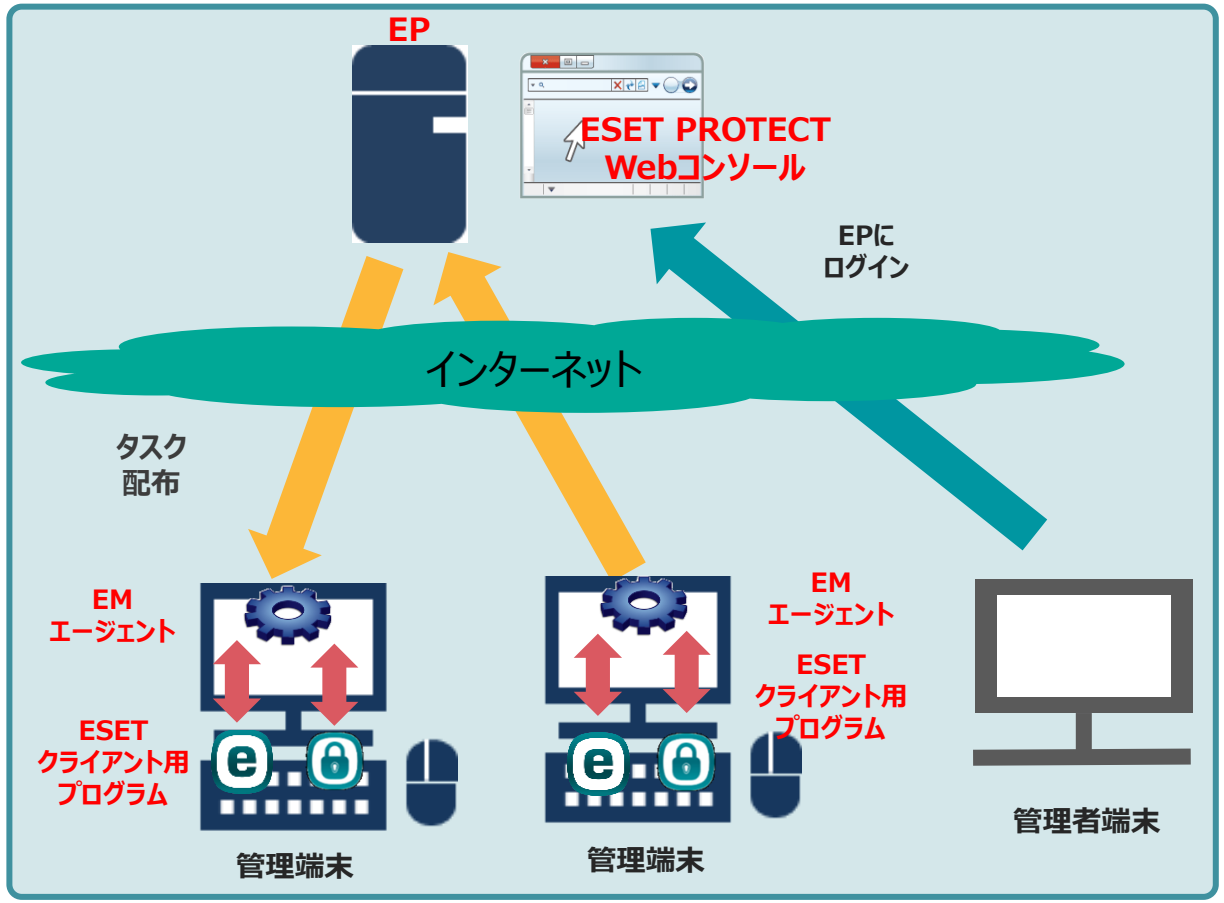
WebコンソールはWebベースのインターフェースであり、ブラウザーを使用してEPへアクセスします。ブラウザー経由でクライアント情報の閲覧やタスクの実行などを行うことができます。

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10分間隔で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。

※エージェントは自動バージョンアップに対応しています。

※EPとEMエージェント間の通信には認証プロキシはご利用いただけません。



2-3.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。

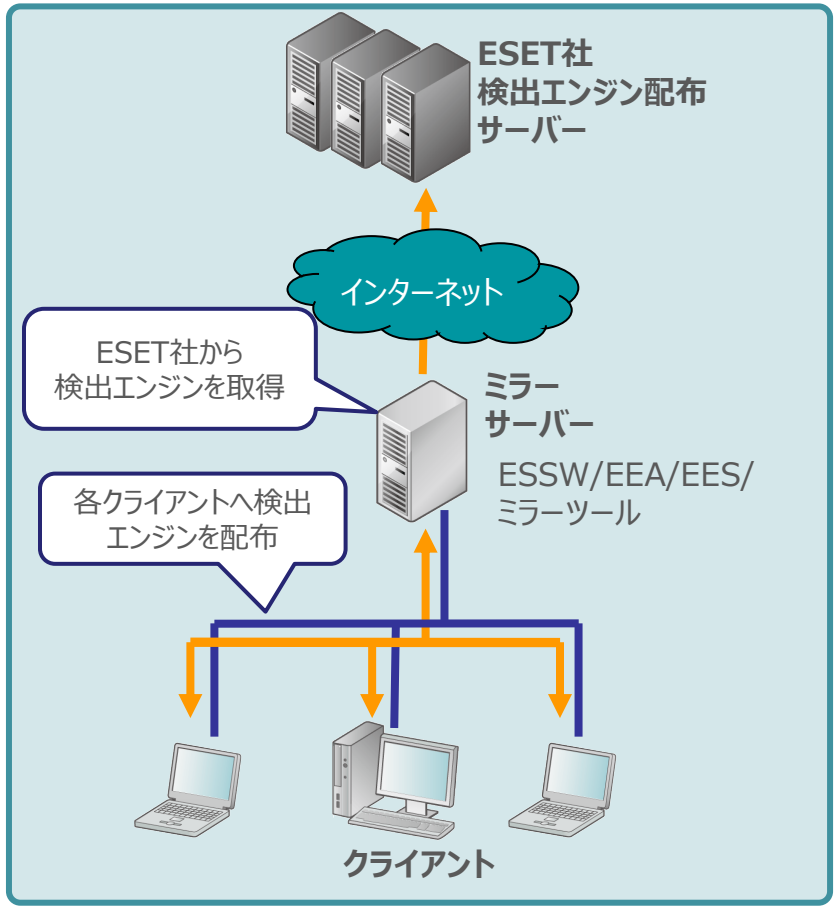
プログラムのミラー機能、またはミラーツールを使用してミラーサーバーの構築が可能となります。クライアントPCを利用して構築することも可能です。

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。



3.規模別構成例

3-1.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 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。

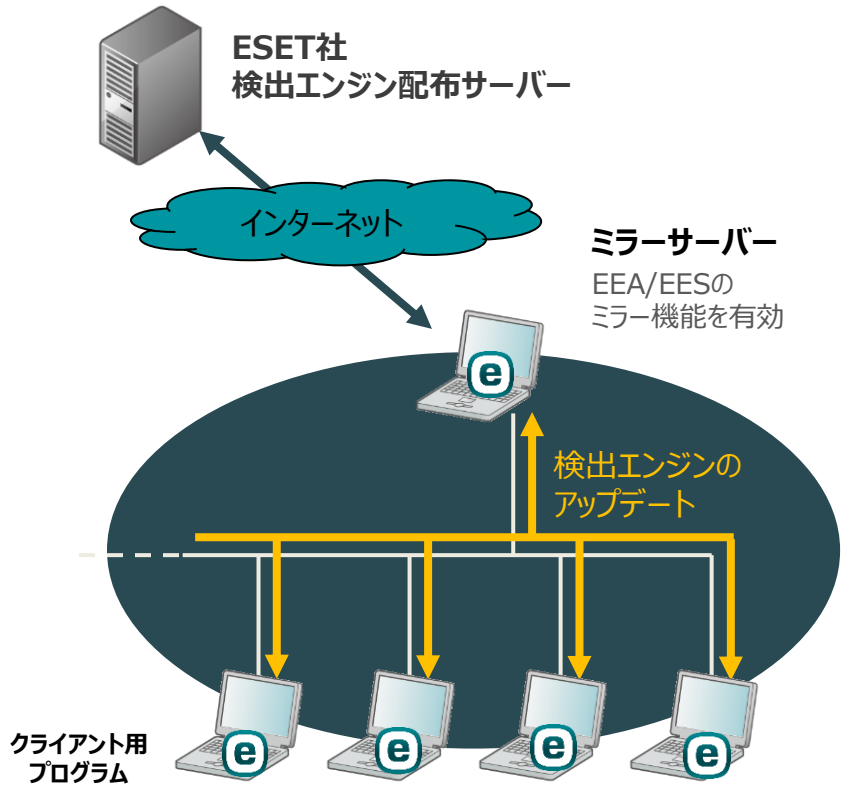
規模別構成例

クライアント数	セキュリティ管理ツールのOS	備考
～100	ー	セキュリティ管理ツール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		
ESET PROTECT の構成		オンプレミスでミラーサーバー　なし
ESET PROTECT 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の最大管理可能端末数は50,000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。
※ミラーサーバーに検出エンジンを配布できる台数はご利用のCAL(クライアントアクセスライセンス)やライセンスによって影響を受ける場合もありますので、事前にご確認ください。
※各プログラムの動作OSは右記をご参照ください。https://eset-support.canon-its.jp/faq/show/4926?site_domain=business
セキュリティ管理ツールで利用するポート番号は右記をご参照ください。 https://eset-support.canon-its.jp/faq/show/94?site_domain=business
セキュリティ管理ツールでサポートしているデータベースは右記をご参照ください。https://eset-support.canon-its.jp/faq/show/91?site_domain=business

3-2.規模別構成例(～100クライアント)

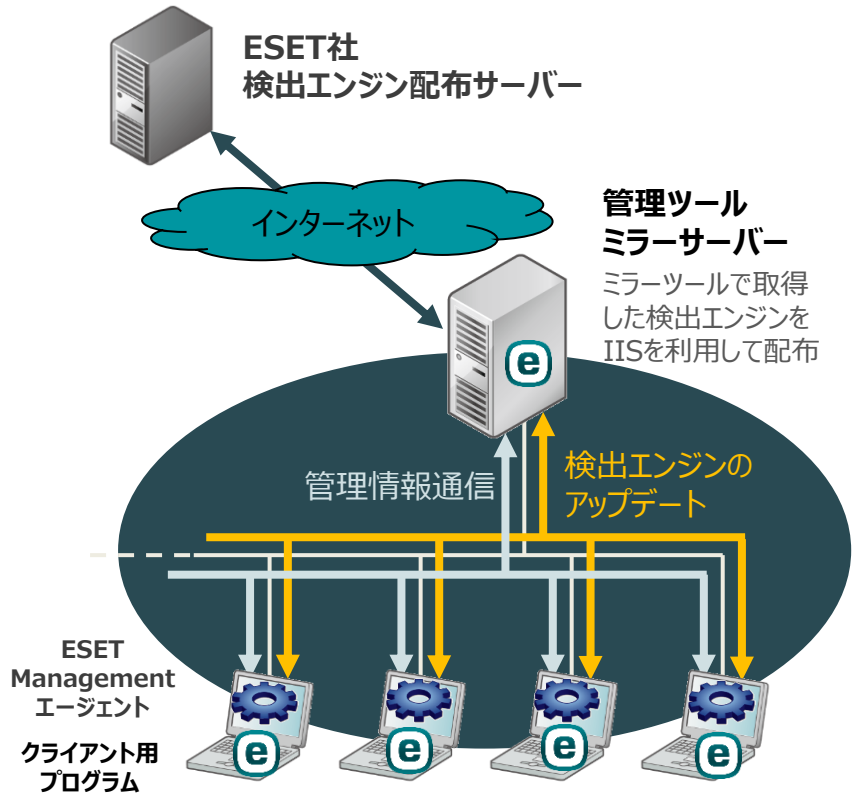
ESET PROTECTソリューションは、セキュリティ管理ツールを利用せずにクライアントだけを運用することができます。
セキュリティ管理ツールが不要な場合や小規模支店などは本構成例を参考にしてください。



構成	• 1台の端末でミラーサーバーを運用 (セキュリティ管理ツールは利用しない) ※セキュリティ管理ツール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：100GB以上 • ネットワークアダプタ：1Gbps
ミラーサーバーの 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	• ミラーサーバーへの接続間隔：60分

3-3.規模別構成例(～1,000クライアント)

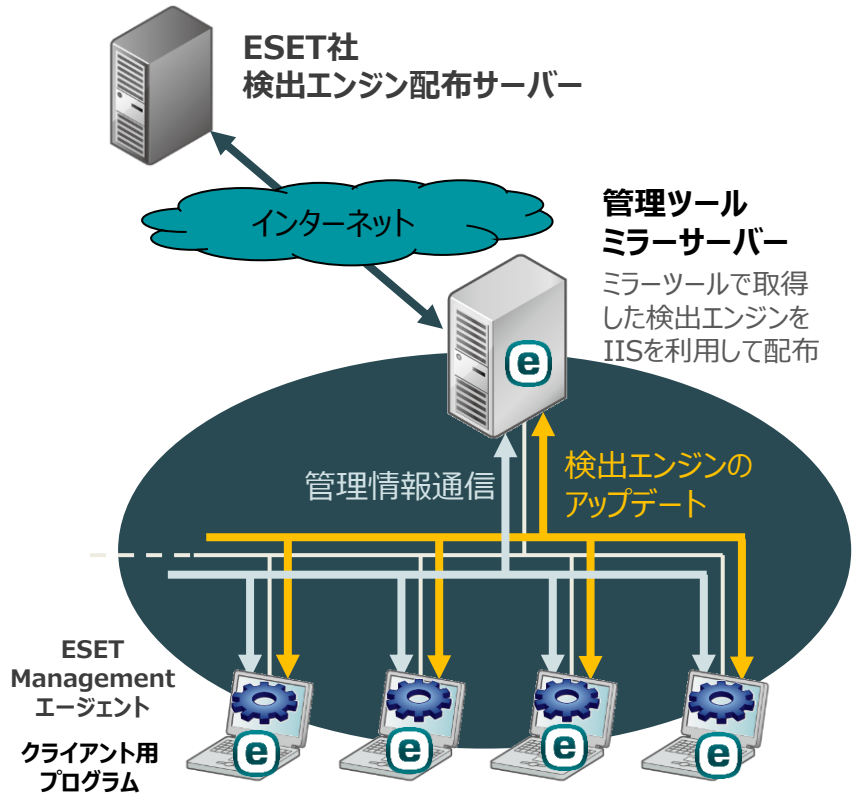
本構成例は、１台のサーバー機でセキュリティ管理ツールとミラーサーバーを運用します。
ミラーサーバーでは、ミラーツールを使用して取得した検出エンジンをIISを利用して配布します。



構成	• 1台のサーバー機でセキュリティ管理ツール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以上 • HDD：100GB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：ミラーツール(IISを利用して配布) • 管理機能：EP on-prem • データベース：MS SQL Express(既定)
クライアントの接続間隔	• セキュリティ管理ツールへの接続間隔：10分 • ミラーサーバーへの接続間隔：60分

3-4.規模別構成例(1,000～5,000クライアント)

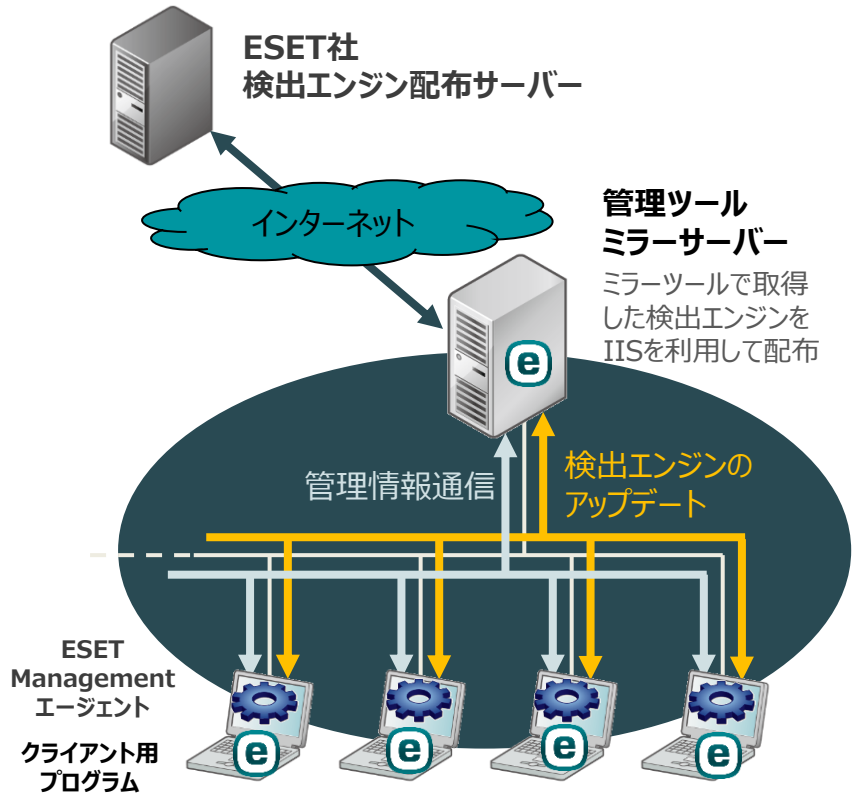
本構成例は、1 台のサーバー機でセキュリティ管理ツールとミラーサーバーを運用します。
なお、規模が大きいため、サーバースペック(CPUコア数やメモリなど)は高める必要があります。



構成	• 1台のサーバー機でセキュリティ管理ツール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： 4~8 GB以上 • HDD：100GB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：ミラーツール(IISを利用して配布) • 管理機能：EP on-prem • データベース：MS SQL Express(既定)
クライアントの接続間隔	• セキュリティ管理ツールへの接続間隔：10分 • ミラーサーバーへの接続間隔：60分

3-5.規模別構成例(5,000～10,000クライアント)

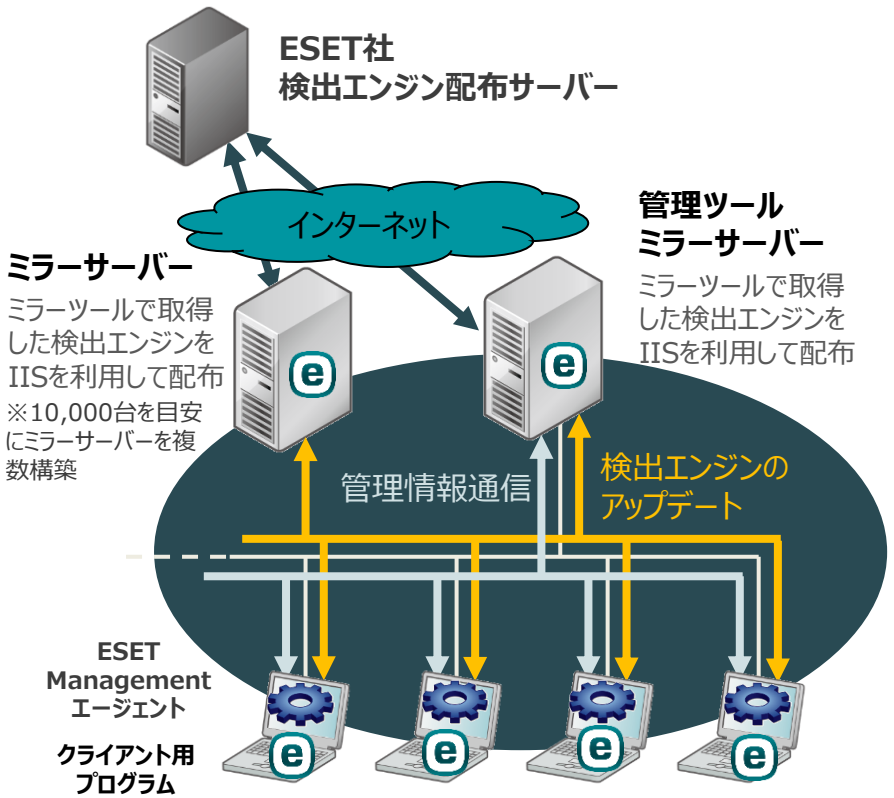
本構成例は、１台のサーバー機でセキュリティ管理ツールとミラーサーバーを運用します。
多くのクライアントを管理するため、セキュリティ管理ツールで利用するデータベースもMS SQL Standardを利用します。
また、セキュリティ管理ツールへの接続間隔も20分程度に延長し、サーバーやネットワークの負荷を軽減します。



構成	• 1台のサーバー機でセキュリティ管理ツール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：8~16 GB以上 • HDD：100GB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：ミラーツール(IISを利用して配布) • 管理機能：EP on-prem • データベース：MS SQL Standard
クライアントの接続間隔	• セキュリティ管理ツールへの接続間隔：20分 • ミラーサーバーへの接続間隔：60分

3-6.規模別構成例(10,000～50,000クライアント)

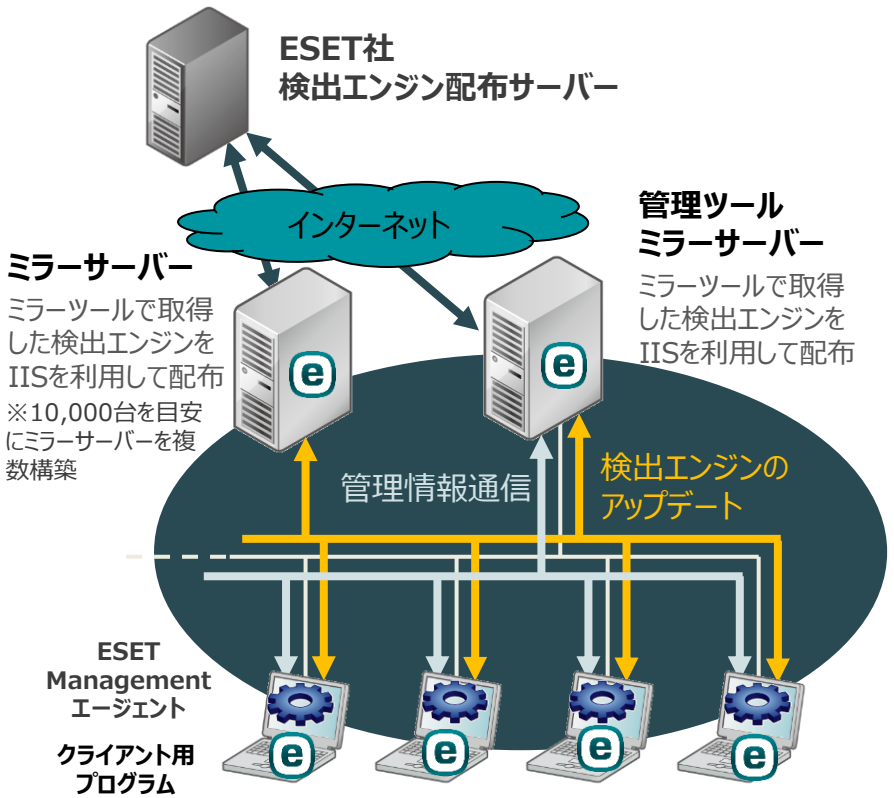
本構成例は、大規模であるため、高スペックのサーバーでセキュリティ管理ツールとミラーサーバーを運用します。
また、10,000クライアントを目安にミラーサーバーを複数構築します。



構成	• 1台のサーバー機でセキュリティ管理ツール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以上 • HDD：100GB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：ミラーツール(IISを利用して配布) • 管理機能：EP on-prem • データベース：MS SQL Standard
クライアントの接続間隔	• セキュリティ管理ツールへの接続間隔：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

3-7.規模別構成例(50,000～100,000クライアント)

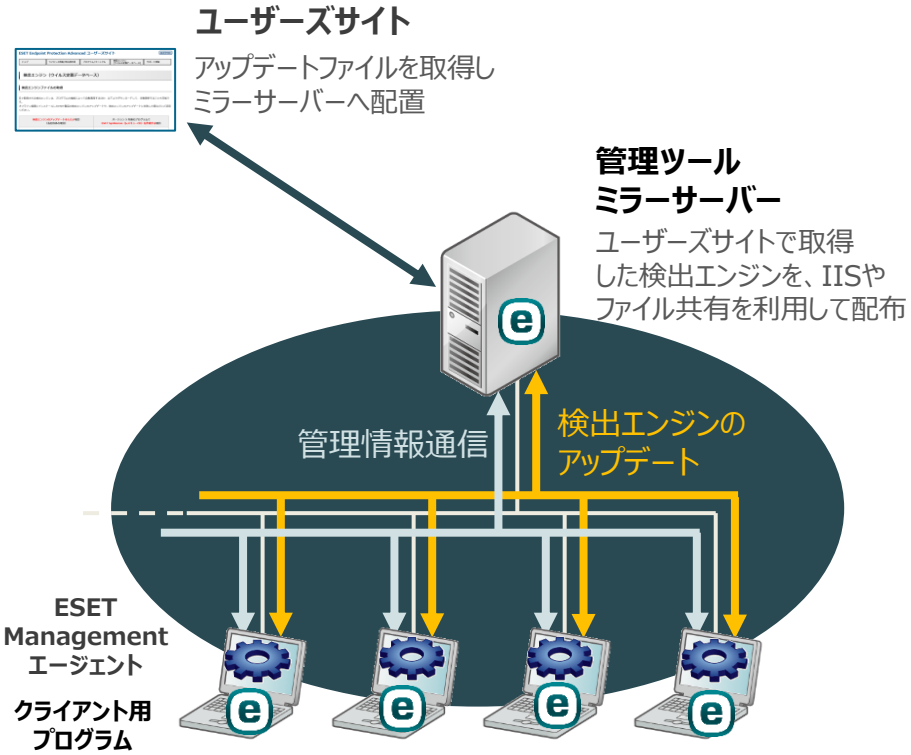
本構成例は、大規模であるため、高スペックのサーバーでセキュリティ管理ツールとミラーサーバーを運用します。さらに規模が大きくサーバーやネットワーク負荷が高くなる可能性があるため、セキュリティ管理ツールへの接続間隔の延長や検出エンジンの取得タイミングを分散させます。



構成	• 1台のサーバー機でセキュリティ管理ツール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：16コア以上 • メモリ：32GB以上 • HDD：100GB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：ミラーツール(IISを利用して配布) • 管理機能：EP on-prem • データベース：MS SQL Standard
クライアントの接続間隔	• セキュリティ管理ツールへの接続間隔：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

3-8.オフライン環境の構成例

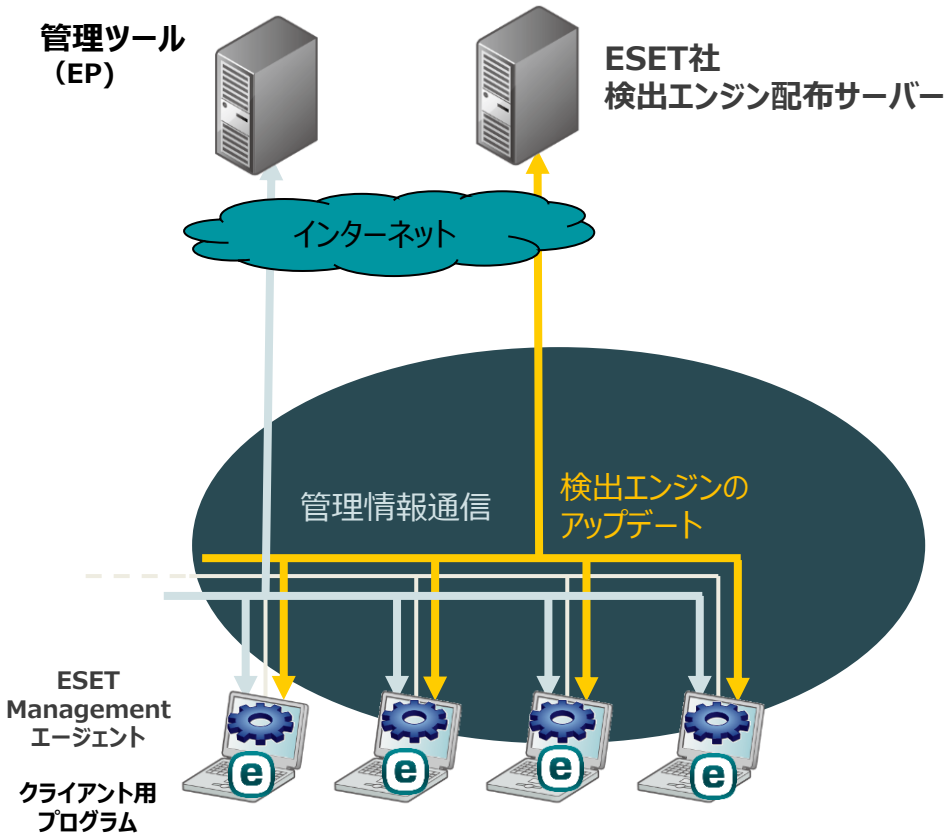
オフライン環境の場合、クライアントに配布するアップデートファイルは、ユーザーズサイトから取得し、サーバーに配置します。
配置したアップデートファイルをIISやファイル共有を利用し各クライアントへ配布します。



構成	• 各規模ごとの構成例を参照し、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：ESSW • 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：EP on-prem ※オフライン環境のため「インストーラー」機能は利用不可 • データベース：MS SQL Express(既定) ※5,000クライアントを超えた場合はMS SQL Standardを使用

3-9. ESET PROTECT の構成例　（オンプレミスでミラーサーバーなし）

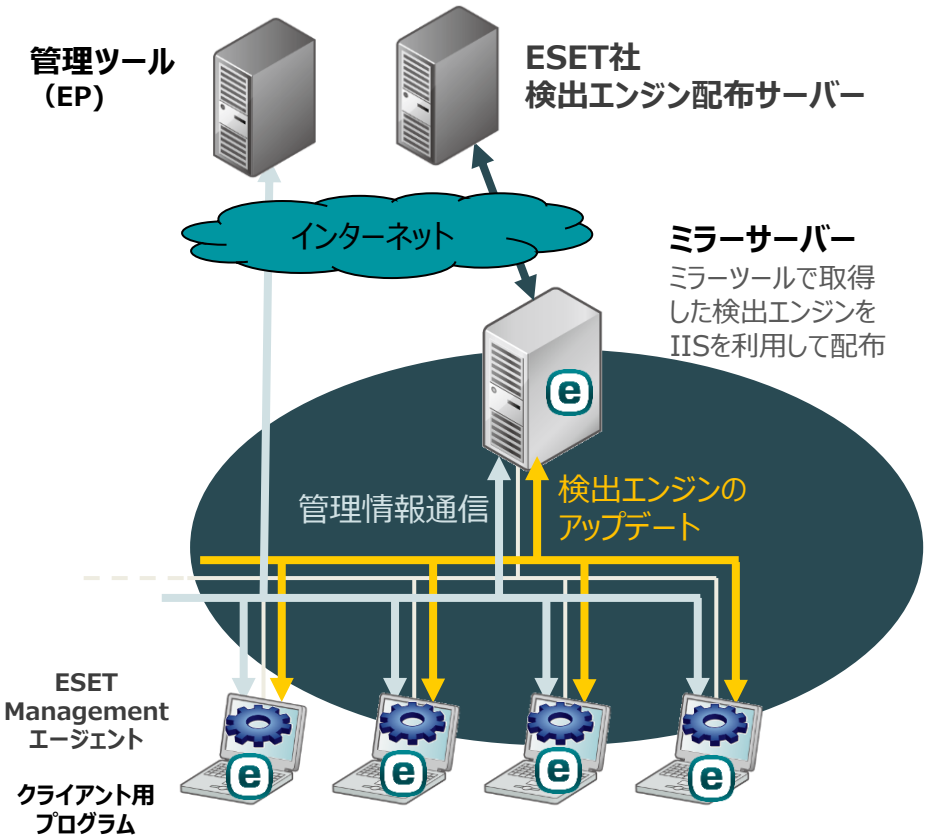
本構成例は、クラウド型セキュリティ管理ツールESET PROTECT を利用した構成です。
十分なネットワーク帯域を保持している環境を想定しているため、ミラーサーバーは構築せずにインターネット経由で、検出エンジンをダウンロードします。



構成	• ESET社のクラウド上に構築されたセキュリティ管理ツールを利用 ※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、セキュリティ管理ツールの構築は不要
サーバーの利用プログラム	• 管理機能：EP ※ESET社のクラウドにて提供
クライアントの接続間隔	• セキュリティ管理ツールへの接続間隔：10分 ※変更不可

3-10. ESET PROTECT 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、クラウド型セキュリティ管理ツールESET PROTECT 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	• ESET社のクラウド上に構築されたセキュリティ管理ツールを利用 • 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	• ESET社のクラウド上で提供するため、セキュリティ管理ツールの構築は不要 • ミラーサーバー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：EP ※ESET社のクラウドにて提供 • ミラーサーバー：ミラーツール(IISを利用して配布)
クライアントの接続間隔	• セキュリティ管理ツールへの接続間隔：10分 ※変更不可 • ミラーサーバーへの接続間隔：60分

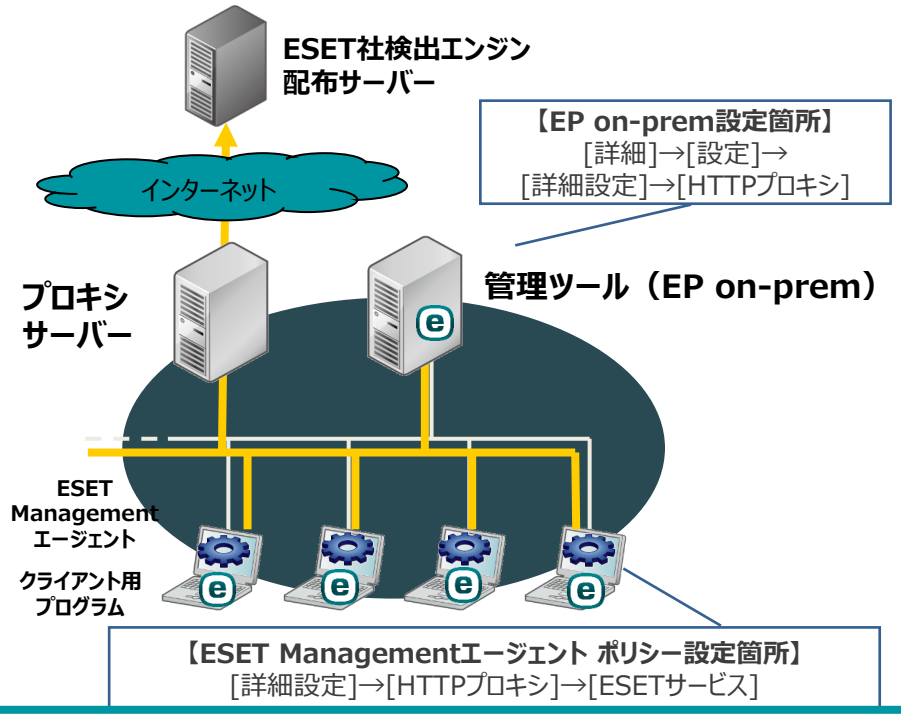
4.参考情報

4-1.セキュリティ管理ツールおよびエージェントのアップデートについて

ESET PROTECT on-prem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。

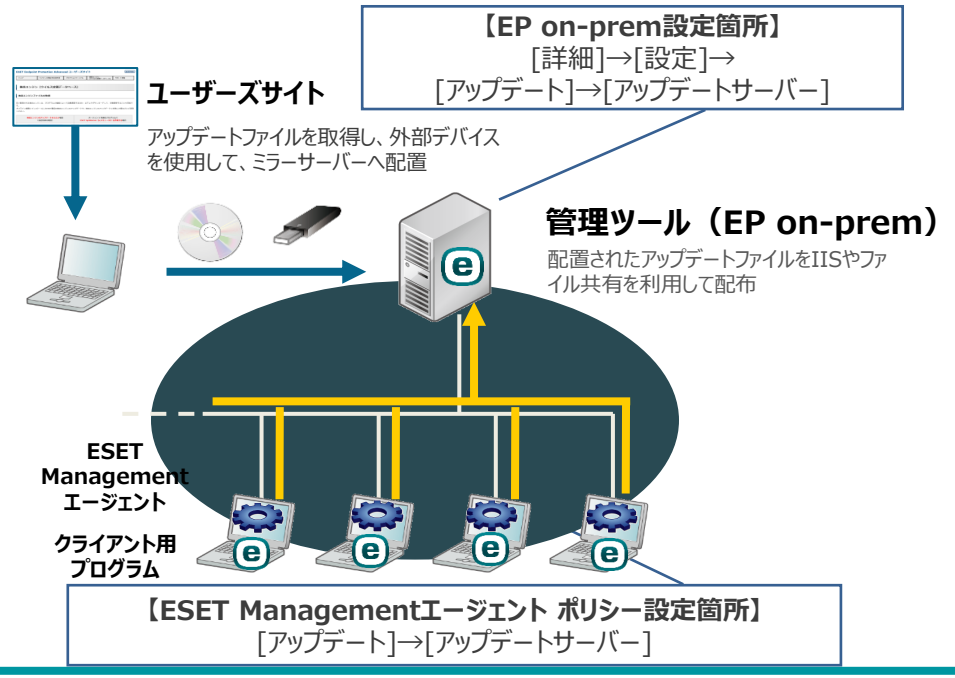
プロキシを経由する環境

プロキシサーバーの設定を入力する必要があります。
※EPをご利用の場合は、ESET Management エージェントへの設定のみ必要です。



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、EP on-prem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。



4-2.トラフィック量の計算(セキュリティ管理ツール)

セキュリティ管理ツールとクライアントのネットワークトラフィックは、セキュリティ管理ツール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。

管理ツールへの接続間隔	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: オンデマンド検査	4KB
クライアントタスク: モジュールアップデート	4KB
クライアントタスク: 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

セキュリティ管理ツール運用時の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日のトラフィックの合計値+(アクション実行時のトラフィック×実行回数))

1,000クライアントを管理しており、セキュリティ管理ツールの接続間隔を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。

4-3.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、一部のデータベースが最適化やパッキングされたファイルです。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、全てのデータベースが最適化やパッキングされたファイルです。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
※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