ユーザーズガイド
導入・運用編（V6 用）

■お断り

○ 本マニュアルは、作成時のソフトウェアおよびハードウェアの情報に基づき作成されています。ソフトウェアのバージョンアップなどにより、記載内容とソフトウェアに記載されている機能が異なる場合があります。また、本マニュアルの内容は、改訂などにより予告なく変更することがあります。

○ ESET、NOD32、ThreatSense、ESET Endpoint Protection、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ESET Remote Administrator は、ESET, spol. s r.o. の商標です。

○ Microsoft、Windows、Windows Vista、Windows Server、Active Directory、Internet Information Services (IIS) は、米国 Microsoft Corporation の米国、日本およびその他の国における登録商標または商標です。

○ Mac、Mac OS、OS X 、Time Machine 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。

改定日　2018/4/30

目　次

Chapter 1 ESET ライセンス製品の導入と検討事項

1.1 ESET ライセンス製品の運用と構成

ESET ライセンス製品は、クライアント用プログラムとクライアント管理用プログラム「ESET Remote Administrator」で構成されています。本資料では、Windows および Mac OS X のクライアント用プログラム（V6）と、管理用プログラム（V6）を使用した際の運用と構成について説明します。
OS が Windows および Mac OS X 以外のクライアント用プログラムと、V5 以前の運用と構成については V5 用の『ユーザーズガイド 導入・運用編』を参照してください。
なお、Linux のクライアント用プログラムは、最新バージョンが V4 となります。Android 用のプログラムは、最新バージョンが V2 となります。管理用プログラム（V6）を使用して管理が可能なため、本資料で説明します。

1.1.1 運用と構成の検討

ESET ライセンス製品には、次の 2 つの運用方法があります。
- クライアント用プログラムのみで運用
- クライアント管理用プログラム「ESET Remote Administrator」を設置してクライアント用プログラムを運用

ESET ライセンス製品のクライアント用プログラムおよびクライアント管理用プログラム「ESET Remote Administrator」は、次のように構成されています。

■クライアント用プログラム

ESET ライセンス製品は、ライセンス形態ごとに複数のクライアント用プログラムを提供しています。
現在、V6 のクライアント用プログラムとしては、次のプログラムを提供しています。

V6 クライアント用プログラムの種類

プログラム		概要
Android クライアント用プログラム	ESET Endpoint Security for Android ※1	ウイルス・スパイウェア対策をはじめ、盗難対策などの機能を搭載した総合セキュリティプログラム。
Windows クライアント用プログラム	ESET Endpoint Security	ウイルス・スパイウェア対策をはじめ、不正侵入対策※2、迷惑メール対策※3、フィッシング対策などの機能を搭載した総合セキュリティプログラム。
Mac OS X クライアント用プログラム	ESET Endpoint Security for OS X	
Windows クライアント用プログラム	ESET Endpoint アンチウイルス	ウイルス・スパイウェア対策などの機能を搭載したセキュリティプログラム。
Mac OS X クライアント用プログラム	ESET Endpoint アンチウイルス for OS X	
Linux クライアント用プログラム	ESET NOD32 アンチウイルス for Linux Desktop ※4	

プログラム		概要
Windows サーバー用プログラム	ESET File Security for Microsoft Windows Server	ウイルス・スパイウェア対策などの機能を搭載したセキュリティプログラム。
Linux サーバー用プログラム	ESET File Security for Linux※4	

※ 1 最新バージョンは V2 となります。
※ 2 ESET Endpoint Security for OS X の不正侵入対策機能はパーソナルファイアウォールのみです。
※ 3 ESET Endpoint Security for OS X には搭載されていません。
※ 4 最新バージョンは V4 となります。

ワンポイント
各クライアント用プログラムの機能については、『ESET ライセンス製品 ご利用の手引』を参照してください。

■ ESET Remote Administrator

クライアント管理用プログラム「ESET Remote Administrator」を導入すると、クライアントコンピューターからウイルス警告、ファイアウォール警告、イベントログなどの情報を取得したり、クライアントコンピューターに対して設定を配布したりすることができます。
ESET Remote Administrator の導入は必須ではありませんが、クライアントコンピューターのセキュリティ管理を一元化できるので、クライアント数が多い場合は ESET Remote Administrator を導入することをお勧めします。

ESET Remote Administrator は、次の 3 つのソフトウェアで構成されています。
- ESET Remote Administrator Server（以下、ERA サーバー）
- ESET Remote Administrator Web Console（以下、ERA Web コンソール）
- ESET Remote Administrator Agent（以下、ERA エージェント）

下記は必要に応じてインストールしてください。
- ESET Remote Administrator Proxy（以下、ERA プロキシ）
- Rouge Detection Sensor（以下、RD Sensor）
- ミラーサーバー
- Mobile Device Connector

ワンポイント
ESET Remote Administrator の機能については『ESET ライセンス製品 ご利用の手引』を参照してください。

■ ERA Web コンソール

ERA Web コンソールは Web ベースのユーザーインターフェースで、クライアント用プログラムを管理できます。管理しているクライアントの情報確認や、タスクの作成、管理対象外のコンピューターへリモートで ESET セキュリティ製品のインストールなどを行えます。ERA Web コンソールはブラウザーを使用してアクセスします。

■ ERA エージェント

ERA エージェントは ERA サーバーとクライアント間の通信を行うサービスです。クライアント用プログラムは ERA サーバーと直接通信をせずに、ERA エージェント経由で通信を行います。
ERA エージェントがインストールされ、ERA サーバーと通信ができるクライアントコンピューターは管理されている状態として表示されます。クライアント用プログラムのインストールの有無に関わらず、ERA エージェントをコンピューターにインストールすることができます。
ERA エージェントは Windows 用のプログラムの場合、社内の Active Directory の GPO を利用して展開することができます。また、ERA サーバーに接続していない場合でも、ERA エージェントはクライアントコンピューターとのイベントに対応することができます。

■ ERA プロキシ

ERA プロキシは ERA サーバーの軽量バージョンで、クライアントにインストールされている ERA エージェントと接続して、データをコンパイルして ERA サーバーへデータを送信することができます。これにより、ネットワークやデータベース処理のパフォーマンスを劣化させることなく、対応できるクライアント数を増やすことができます。

■ RD Sensor

RD Sensor は、ネットワーク内のコンピューターを検索するツールです。検出されたコンピューターは、定義済みレポートで報告され、ERA サーバーのコンピューターリストに自動的に追加されます。

■ミラーサーバー

ミラーサーバーを設置すると、クライアントコンピューターはインターネットへアクセスせずに、LAN 内に設置されたミラーサーバーからウイルス定義データベースなどのアップデートファイルを取得できます。ミラーサーバーは、Windows 用の ESET Endpoint アンチウイルス、ESET Endpoint Security、ESET File Security for Microsoft Windows Server、ESET File Security for Linux で構築できます。
ミラーサーバーからのアップデートファイルの配布方法には、次の方法が用意されています。クライアントコンピューターにインストールするセキュリティプログラムによって配布方法が異なるので、配布方法に合わせてミラーサーバーを設置する必要があります。

アップデートファイル配布方法

HTTP 経由によるアップデート	製品内蔵の HTTP サーバー機能を利用
	Microsoft Internet Information Service（IIS）を利用
共有フォルダーを利用したアップデート	製品をインストールしたコンピューターの共有フォルダーを利用
	他のコンピューターの共有フォルダーを利用
リムーバブルメディアを利用したアップデート	CD-R や DVD-R、USB フラッシュメモリーなど

なお、V6 では新たに提供されたミラーツールにより、ウイルス定義データベースなどのアップデートファイルを ESET アップデートサーバーからダウンロードし、ローカルに保存することができるようになりました。本ツールによりミラーサーバーを構築しなくても配布用のアップデートファイルをダウンロードすることができます。本ツールで作成したアップデートファイルは上記アップデートファイル配布方法で配布が可能です。
ミラーツールは Windows と Linux 上で動作させることができます。ミラーツールの詳細については『ESET Remote Administrator ユーザーズマニュアル』の「8.2　ミラーツール」をご参照ください。

! 重　要

ESET Endpoint アンチウイルス /ESET Endpoint Security V6.6 をミラーサーバー経由でアップデートする場合は、V6.6 に対応したミラーツールを使用するか、ESET Endpoint アンチウイルス /ESET Endpoint Security V6.6 でミラーサーバーを作成する必要があります。

■ Mobile Device Connector

Mobile Device Connector は、Android 用のクライアント用プログラム「ESET Endpoint Security for Android」と iOS デバイスを管理するアプリケーションです。ERA サーバーで Android および iOS の管理を行う場合、Mobile Device Connector をインストールしたサーバーが必要です。Mobile Device Connector のインストール方法については、『SET Remote Administrator ユーザーズマニュアル』の「3 インストール」をご参照ください。

■サーバー／ネットワーク負荷の検討

ERA サーバーやミラーサーバーを運用する場合、サーバーやネットワークに対する負荷の集中について検討する必要があります。

ERA サーバーは、クライアントコンピューターの情報を収集するために定期的に通信を行います。このため、情報収集頻度を上げたり、同じ頻度でもクライアント数が増加すると、サーバーやネットワークへの負荷が大きくなります。

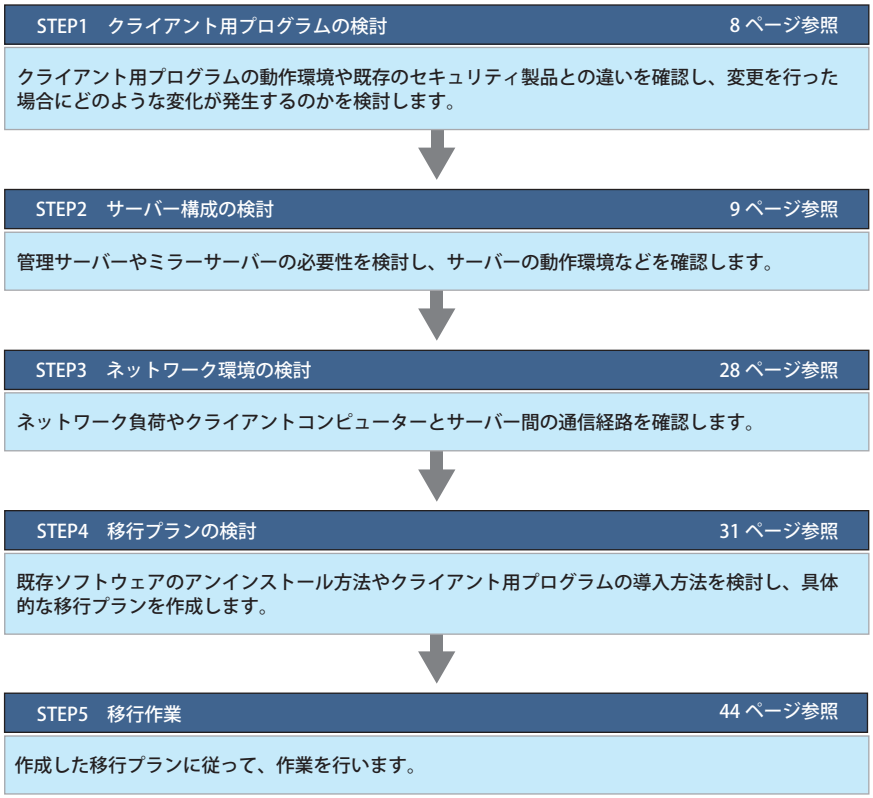
また、ウイルス定義データベースは頻繁にアップデートされます。このため、ミラーサーバーと兼用しているERAサーバーでは、ERA サーバー機能のみで運用している場合よりも負荷が高くなります。

予想される負荷に耐え得るサーバーのスペックを検討します。また、負荷を分散させるために複数のサーバーを導入することを検討します。

1.2　移行・導入作業の流れ

他社製セキュリティプログラムから ESET 製品に移行する場合、移行作業中にセキュリティレベルを低下させることなくスムーズに移行することが大切です。
スムーズに移行するために、次の流れで作業することをお勧めします。新規導入の場合も作業の流れは同様です。

移行・導入作業の流れ



1.3 STEP-1 クライアント用プログラムの検討

クライアント用プログラムの動作環境や既存のセキュリティ製品との違いを確認し、移行するとどのような変化が発生するのかを検討します。
次のようなポイントに着目して検討してください。

■クライアント用プログラムの種類

ESET ライセンス製品には、複数のクライアント用プログラムが含まれています。機能などを検討して、どのセキュリティプログラムが利用目的に適しているかを検討してライセンス製品を選択します。

ライセンス製品とクライアント用プログラム

プログラム ＼ 製品		ESET Endpoint Protection Advanced ライセンス※1			ESET Endpoint Protection Standard ライセンス※2		
		企業向け	官公庁向け	教育機関向け	企業向け	官公庁向け	教育機関向け
Android 用	総合セキュリティプログラム ESET Endpoint Security for Android	○			○		
Windows 用	総合セキュリティプログラム ESET Endpoint Security	○			—		
	ウイルス・スパイウェア対策プログラム ESET Endpoint アンチウイルス	○			○		
Mac OS X 用	総合セキュリティプログラム ESET Endpoint Security for OS X	○			—		
	ウイルス・スパイウェア対策プログラム ESET Endpoint アンチウイルス for OS X	○			○		
Linux クライアント用	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	○			○		
Windows サーバー用	ウイルス・スパイウェア対策プログラム ESET File Security for Microsoft Windows Server	○			○		
Linux サーバー用	ウイルス・スパイウェア対策プログラム ESET File Security for Linux	○			○		

※1 ESET Endpoint Protection Advanced キャンパスライセンスを含む。
※2 ESET Endpoint Protection Standard キャンパスライセンス、および、ESET Endpoint Protection Standard スクールパックを含む。

■動作環境の確認

クライアントコンピューターが、各セキュリティプログラムの動作環境を満たしているかどうか確認します。
クライアント用プログラムの動作環境については、各セキュリティプログラムのユーザーズマニュアルを参照してください。

■既存のセキュリティ製品との相違

現在運用しているセキュリティ製品との違いを把握して、ESET ライセンス製品を導入することによって発生する変化を検討します。たとえば、ESET Endpoint Security を導入すると、ファイアウォール機能により、これまで行えていたアプリケーションとの通信が遮断される可能性があります。このため、ESET Endpoint Security を導入する場合は、ファイアウォールルールの変更などを検討する必要があります。

ワンポイント

各プログラムの機能については『ESET ライセンス製品 ご利用の手引』を参照してください。

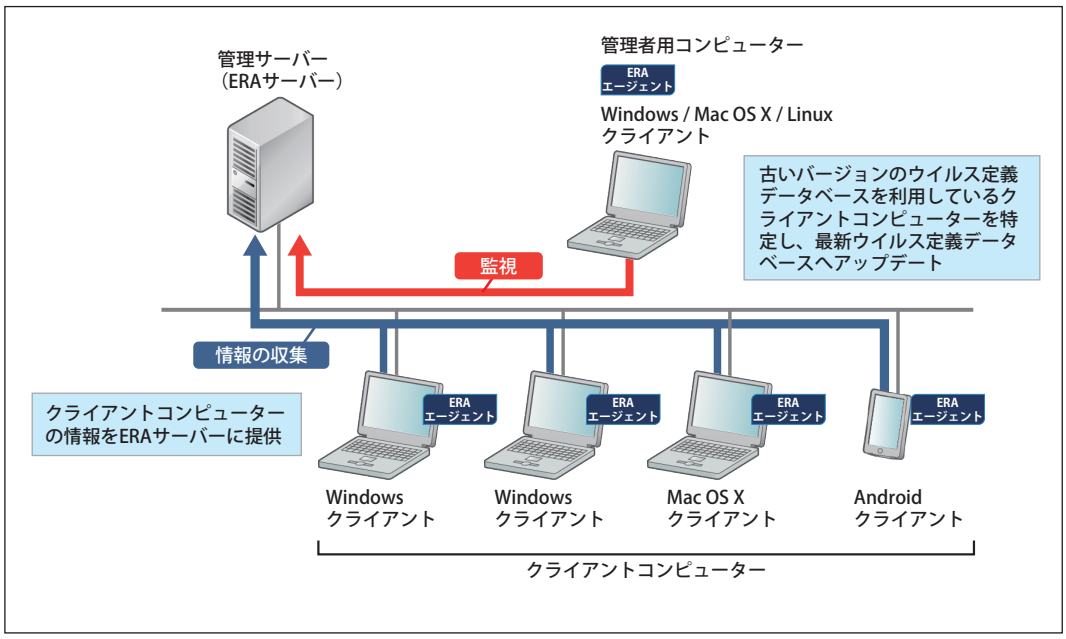
1.4 STEP-2 サーバー構成の検討

クライアント管理機能やミラーサーバーの必要性を検討し、ERA サーバーの動作環境などを確認します。
次のようなポイントに着目して検討してください。

1.4.1 ERA サーバーの検討

ERA サーバーを導入すると、クライアントコンピューターの状況を集中管理したり、クライアントコンピューターにリモートからウイルス定義データベースのアップデートの実行や、クライアント用プログラムの設定を配布したりできます。

ERA サーバーの機能



■ ERA サーバー導入の留意点

ERA サーバーを導入する際は、次のポイントに留意してください。

●プロキシサーバーの設定とキャッシュ

プロキシサーバーが設置されたネットワーク環境に ERA サーバーを設置する場合、ERA サーバーがプロキシサーバーを経由して ESET 社サーバーからウイルス定義データベースなどのアップデートファイルを取得できるように設定する必要があります。設定手順については、『ESET Remote Administrator ユーザーズマニュアル』を参照してください。
この時、ウイルス定義データベース（*.nup）がプロキシサーバーでキャッシュされないように設定する必要があります。プロキシサーバーのキャッシュの仕様によっては、ウイルス定義データベースのデジタル署名が不整合を起こし、クライアントコンピューターでのアップデートに障害が発生する場合があります。

●ファイアウォールの設定

ERA サーバーやミラーサーバーに設定したコンピューターでファイアウォールが動作していると、ウイルス定義データベースのアップデートや管理用コンピューターからのリモート操作が行えない場合があります。
ファイアウォールが動作している場合は、ERA サーバーが管理用コンピューターとの通信に利用するポートやクライアントコンピューターとの通信に利用するポートを開放するように設定を変更します。ミラーサーバーでも、同様にポート設定を変更します。
ERA サーバーやミラーサーバーでは、既定値として以下の通信ポートを利用します。

サーバーが使用するポート

ESET Remote Administrator とそのコンポーネントがインストールされるときに使用されるすべてのネットワーク通信ポートの一覧です。その他の通信は、ネイティブオペレーティングシステムプロセス経由で実行されます（TCP/IP 上の NetBIOS など）。

- **ERA サーバー**

プロトコル	ERA サーバーがリッスンするポート	説明
TCP	2222	ERA エージェントと ERA サーバー間の通信
TCP	2223	ERA Web コンソールと ERA サーバー間の通信（支援型インストールで使用）

- **ERA Web コンソール**

プロトコル	ERA Web コンソールがリッスンするポート	説明
TCP	443	HTTP SSL Web コンソール呼び出し

- **ERA プロキシ**

プロトコル	ERA プロキシがリッスンするポート	説明
TCP	2222	ERA エージェントと ERA プロキシ間の通信

- **HTTP プロキシ**

プロトコル	HTTP プロキシがリッスンするポート	説明
TCP	3128	HTTP プロキシ（更新キャッシュ）

- **ERA エージェント**

プロトコル	ERA エージェントがリッスンするポート	説明
UDP	1237	ウェイクアップコール

- **ERA エージェント（リモート展開用）**

Windows OS のクライアントコンピューターに ERA エージェントをリモート展開する時に使用します。

プロトコル	ERA サーバーから見て ターゲットとなるポート	説明
TCP	139	管理共有の使用
TCP	445	リモートインストール中に TCP/IP を使用して共有リソースに直接アクセス（TCP139 の代替）
UDP	137	リモートインストール中の名前解決
UDP	138	リモートインストール中の参照

- **Mobile Device Connector**

Android および iOS を ERA サーバーで管理する時に使用します。

プロトコル	Mobile Device Connector がリッスンするポート	説明
TCP	9980	モバイルデバイスの登録
TCP	9981	モバイルデバイスとの通信

プロトコル	Mobile Device Connector の内部通信で 使用するポート	説明
TCP	9977	Mobile Device Connector と ERA エージェント間の内部通信
TCP	9978	Mobile Device Connector と ERA エージェント間の内部通信

プロトコル	ERA サーバーへの通信で使用するポート	説明
TCP	2222	Mobile Device Connector から ERA サーバーへの通信

プロトコル	Apple Push Notification サービスへの通信で使用するポート	説明
TCP	5223	インターネット（Apple Push Notification サービス）への通信
TCP	2195	Mobile Device Connector からインターネット（Apple Push Notification サービス）への通信
TCP	2196	Mobile Device Connector からインターネット（Apple Push Notification サービスのフィードバックサービス）への通信
TCP	443	デバイスがポート 5223 でインターネット（Apple Push Notification サービス）に到達できない場合の代替ポート

プロトコル	Google Cloud Messaging への通信で使用するポート	説明
TCP	5228	インターネット（Google Cloud Messaging）への通信
TCP	5229	インターネット（Google Cloud Messaging）への通信
TCP	5230	インターネット（Google Cloud Messaging）への通信

ワンポイント

定義済みポート 2222、2223 が別のアプリケーションによって既に使用されている場合は、別のポートに変更してください。

！重　要

- 上記のポートが他のアプリケーションによって使用されていないことを確認してください。
- ネットワーク内のファイアウォールで、上記のポート経由の通信が許可されていることを確認してください。

● Windows Server Client Access License（CAL）

ERA サーバーを Windows 環境で使用する場合、「Windows Server Client Access License（CAL）」の確認が必要です。新規のコンピューターを導入するときなど、追加で CAL の購入が必要になることがあります。
Windows CAL の詳細については、Microsoft 社にご確認ください。

ワンポイント

ミラーサーバーでのウイルス定義データベースの保存先を NAS やストレージサーバー、または Linux サーバーに設定することで、CAL の追加購入が不要になるケースもあります。

1.4.2 ミラーサーバーの検討

ミラーサーバーを設置すると、ウイルス定義データベースなどのアップデートをミラーサーバー経由で行うことができます。これにより、クライアントコンピューターはアップデートの際にインターネットへの接続が不要になるので、インターネット回線への負荷が軽減されます。

ミラーサーバーは次のプログラムで構築できます。

- ESET Endpoint アンチウイルス
- ESET Endpoint Security
- ESET File Security for Microsoft Windows Server
- ESET File Security for Linux

ミラーサーバーのメリット／デメリット

プログラム	ESET Endpoint アンチウイルス／ESET Endpoint Security	ESET File Security for Microsoft Windows Server ／ ESET File Security for Linux
差分アップデート機能	○	○
ミラーサーバーの SSL 対応	○	○
メリット	• クライアント OS で利用できるため、小規模環境でミラーを構築できる • インターネット側のネットワーク負荷の軽減 • インターネットへ直接アクセスできないクライアントコンピューターのアップデートが可能 • USB フラッシュメモリーや CD-R を経由した、オフラインによるアップデートが可能（Windows 用プログラムのみ対応）	• Windows Server または Linux サーバーでミラーサーバーを構築する場合に利用 • インターネット側のネットワーク負荷の軽減 • インターネットへ直接アクセスできないクライアントコンピューターのアップデートが可能 • USB フラッシュメモリーや CD-R を経由した、オフラインによるアップデートが可能（Windows 用プログラムのみ対応）
デメリット	サーバー OS で利用できないため、大規模環境では利用できない	製品内蔵の HTTP サーバーのため、配布できるクライアントコンピューター数の目安は 1000 台となります。より多くのクライアントコンピューターに配布する場合には、IIS や Apache と連携する必要があります。

! 重 要

ESET Endpoint アンチウイルス /ESET Endpoint Security V6.6 をミラーサーバー経由でアップデートする場合は、V6.6 に対応したミラーツールを使用するか、ESET Endpoint アンチウイルス /ESET Endpoint Security V6.6 でミラーサーバーを作成する必要があります。

■ミラーサーバーの種類

ミラーサーバーでアップデートファイルを配布する場合、HTTP サーバーを利用する方法と共有フォルダーを利用する方法の 2 種類があります。

HTTP サーバーを利用した配布方法とクライアントコンピューター数の目安

HTTP サーバー	クライアント数
ESET Endpoint アンチウイルス／ ESET Endpoint Security 内蔵の HTTP サーバー	100 台
ESET File Security for Microsoft Windows Server 内蔵の HTTP サーバー	1,000 台
ESET File Security for Linux 内蔵の HTTP サーバー	1,000 台
Microsoft Internet Information Services（IIS）	5,000 台
Apache	5,000 台

■データベースの種類

ERA サーバーは、クライアントコンピューターで発生したログをデータベースに記録します。
ERA サーバーで利用するデータベースについて説明します。

●利用できるデータベースと最大容量

利用できるデータベースと最大容量については、以下弊社ホームページを参照してください。
https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html#anc08

クライアント数を考慮して、下記のデータベースから選択します。

利用可能なデータベースと最大保存容量（2017 年 4 月時点）

データベースの形式		登録可能な最大容量
MySQL		最大 4TB（ext3 ファイルシステム使用の場合）
Microsoft SQL Server 2008	Express Edition	最大 4GB
	R2 Express Edition（既定）	最大 10GB
	Standard Edition	最大値なし
Microsoft SQL Server 2012 Microsoft SQL Server 2014 Microsoft SQL Server 2016 ※1	Express	最大 10GB
	Express with Tools ※2	最大 10GB
	Express with Advanced Services	最大 10GB
	Web	最大 524PB
	Standard	最大 524PB
	Business Intelligence ※2	最大 524PB
	Enterprise	最大 524PB

※ 1 Microsoft SQL Server 2016 は ERA 6.5 以上で対応しています。
※ 2 Microsoft SQL Server 2016 にはありません。

●データベース選定の目安

ERA サーバーに保存されるクライアントログの容量は、管理するクライアント数によって変動します。

容量の目安

ディスクのデータベースサイズ　2GB（5,000 クライアントそれぞれがデータベースに 30 件のログを格納）

■動作環境の確認

ERA サーバーやミラーサーバーを設置する場合、サーバー用のコンピューターが推奨される動作環境を満たしているかどうかを確認します。

ESET Remote Administrator の動作環境については、弊社製品ホームページを参照してください。

https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html#anc08

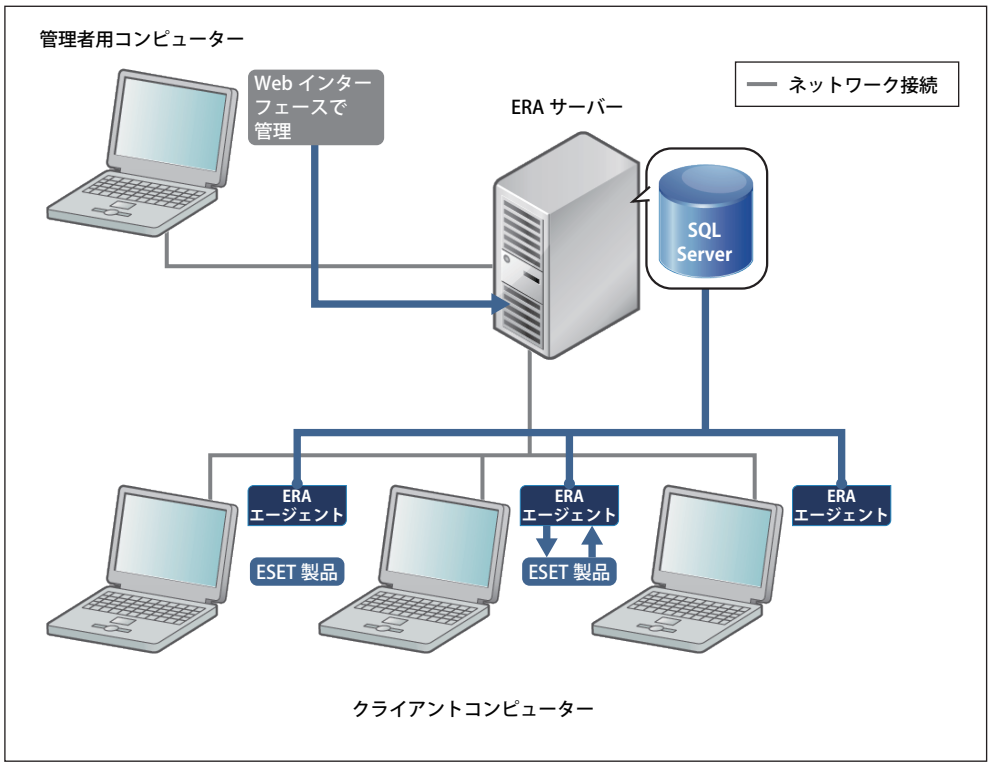
1.4.3　代表的なサーバー構成

ESET Remote Administrator を使用したサーバー環境は、規模や運用形態により次のようなケースが考えられます。

- 小規模ネットワーク（1 台のサーバー）
- 中規模ネットワーク（プロキシを利用したリモートオフィス）
- 大規模ネットワーク（ERA コンポーネントの利用）

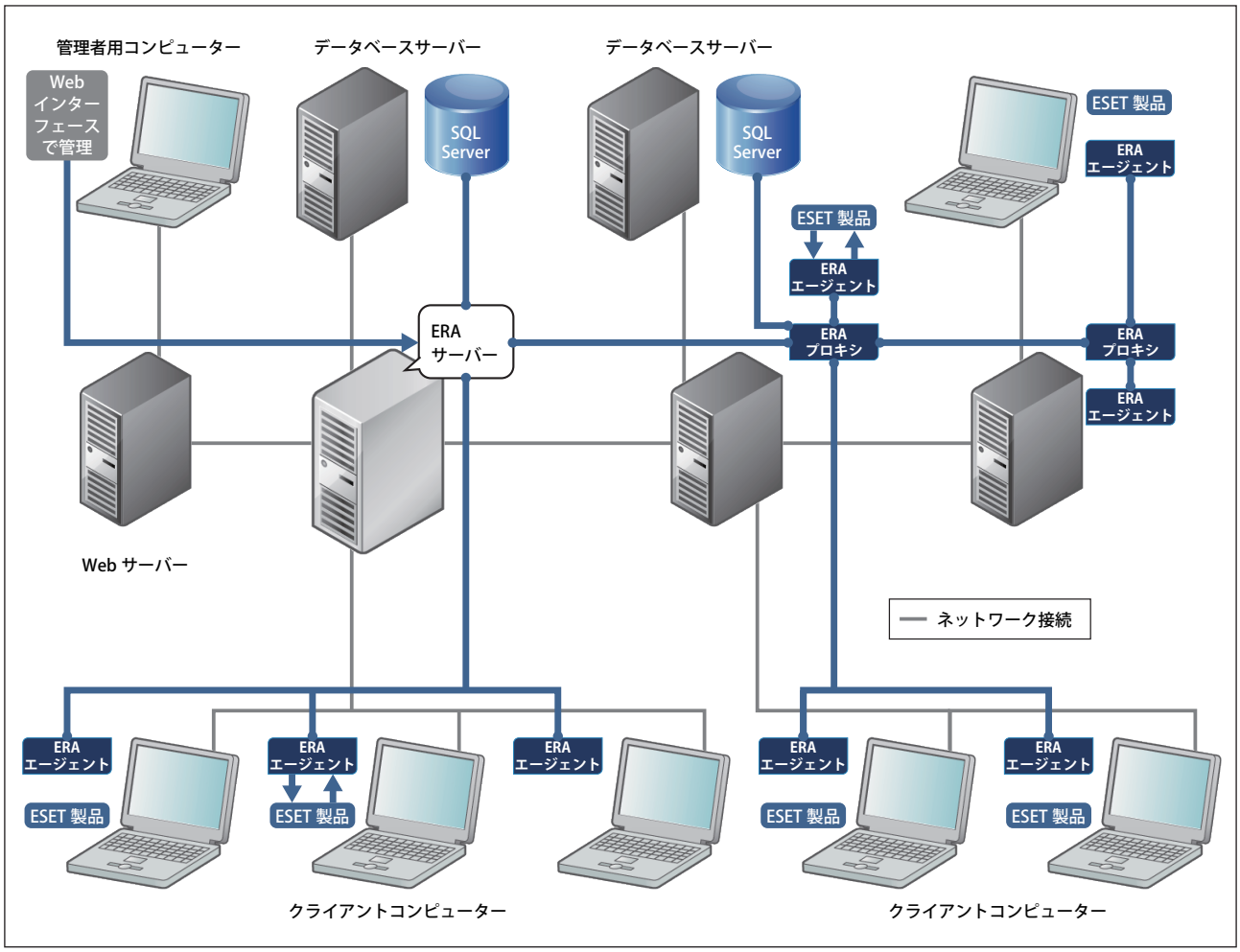
■小規模ネットワーク（1 台のサーバー）

小規模ネットワーク（1000 クライアント以下）を管理するには、ERA サーバーとすべてのコンポーネント（ERA Web コンソール、データベースなど）を 1 台のサーバーにインストールすることをお勧めします。管理対象のクライアントは、ERA エージェント経由で直接 ERA サーバーに接続を行います。管理者は、ネットワーク上の任意のコンピューターから Web ブラウザーで ERA Web コンソールに接続、もしくは ERA サーバーから直接 ERA Web コンソールを実行することができます。



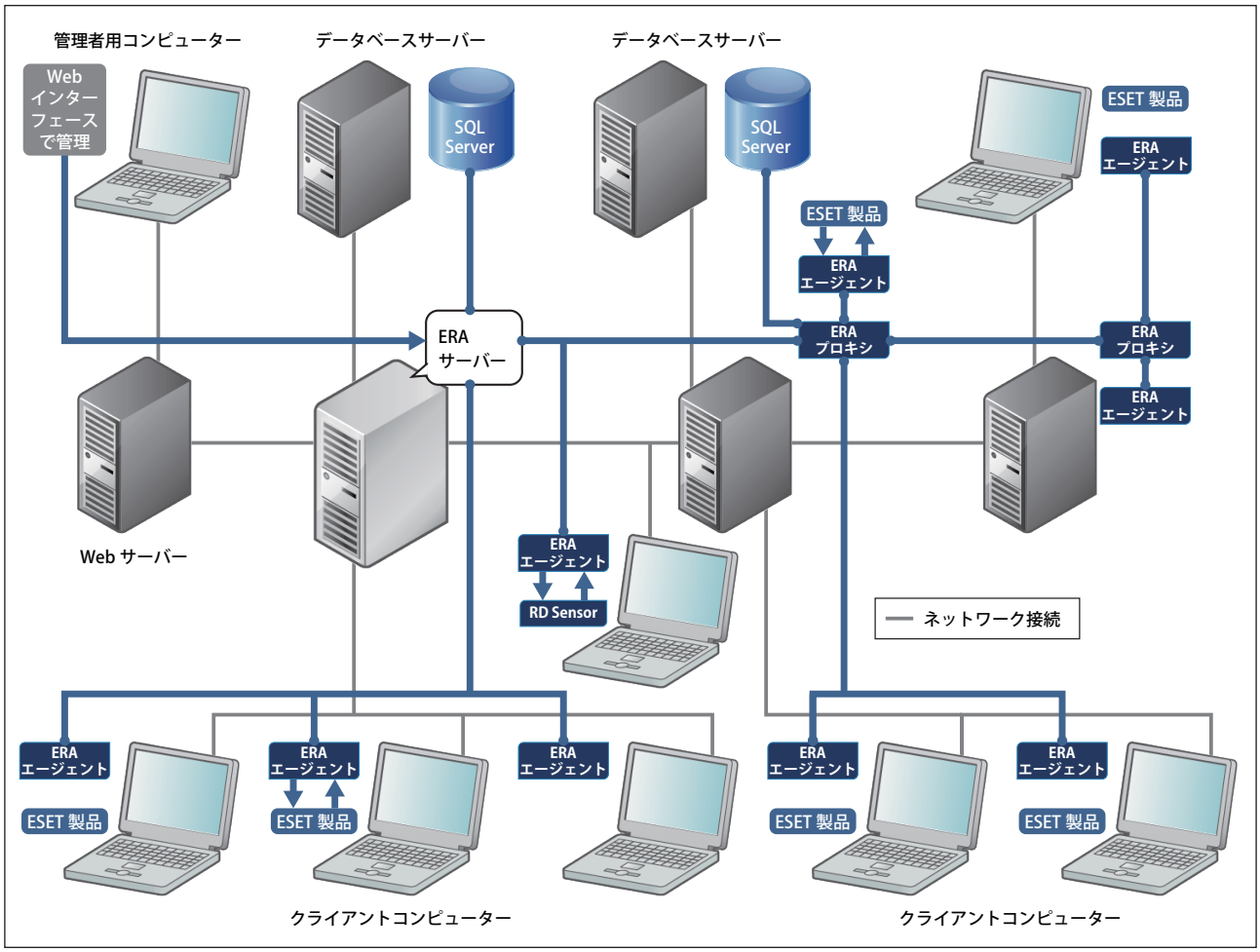
■中規模ネットワーク（プロキシを利用したリモートオフィス）

中規模のネットワーク環境（10,000 クライアント程度）では、ERA プロキシを利用することをお勧めします。同じローカルネットワーク上の ERA エージェントを ERA プロキシで集約し、上位の ERA プロキシまたは ERA サーバーへ接続します。ERA プロキシを使用するには、ERA プロキシがインストールされているホストコンピューターに ERA エージェントがインストールされ、ネットワークの上位レベルの ERA サーバーもしくは ERA プロキシへの接続が必要です。



■大規模ネットワーク（ERA コンポーネントの利用）

大規模のネットワーク環境（10,000 クライアント以上）では、ERA コンポーネントを使用し、RD Sensor と ERA プロキシを利用することをお勧めします。RD Sensor は、ネットワーク内のコンピューターを検出することができます。ERA プロキシでは、ERA エージェントを ERA プロキシに接続させることにより、パフォーマンス上重要な、ERA サーバーの負荷を分散させます。ERA プロキシを利用しても、ERA エージェントを直接 ERA サーバーに接続することも可能です。SQL データベースは、フェールオーバークラスタにも実装され通信の冗長化を実現します。



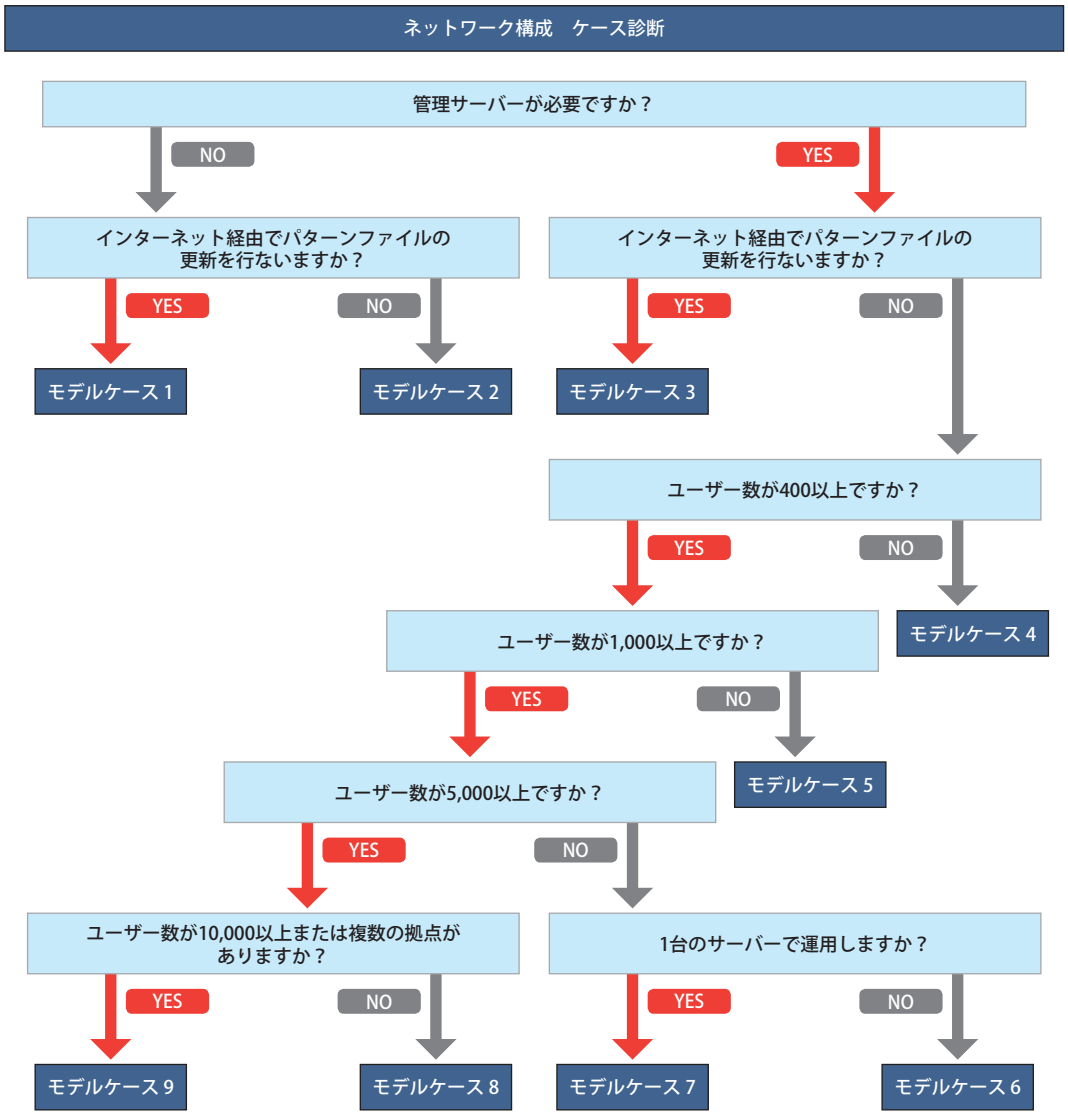
1.4.4 サーバー構成のモデルケース

サーバーを構成する場合のモデルケースをご紹介します。下図の「ネットワーク構成診断」でお使いの環境を確かめ、適合するモデルケースを選択してください。

!重 要

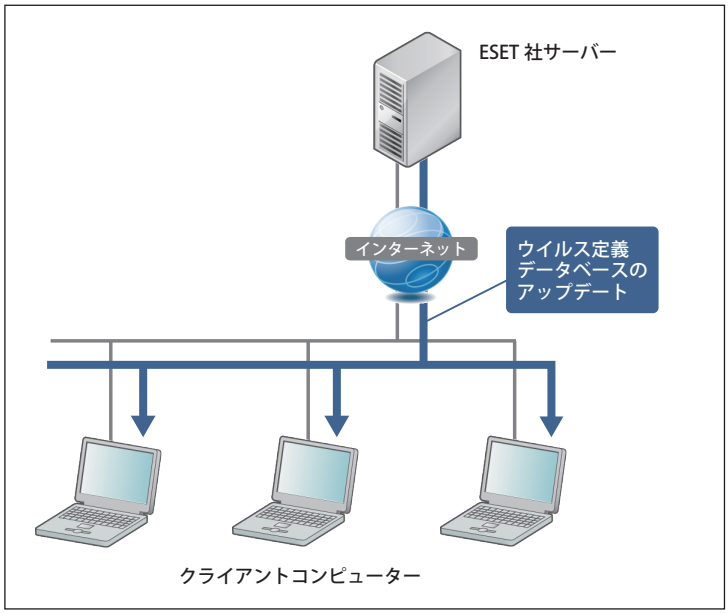
モデルケースで説明する数値は参考値です。管理可能なクライアント数などは、ご利用環境のサーバースペックやネットワーク構成、サーバーの設定などにより異なります。

ネットワーク構成診断



■モデルケース 1「クライアント用プログラムだけで運用」

クライアント用プログラムのみで運用する場合は、サーバーは不要です。
各クライアントはインターネットに接続して、ESET 社サーバーから最新のウイルス定義データベースなどのアップデートファイルを取得する必要があります。



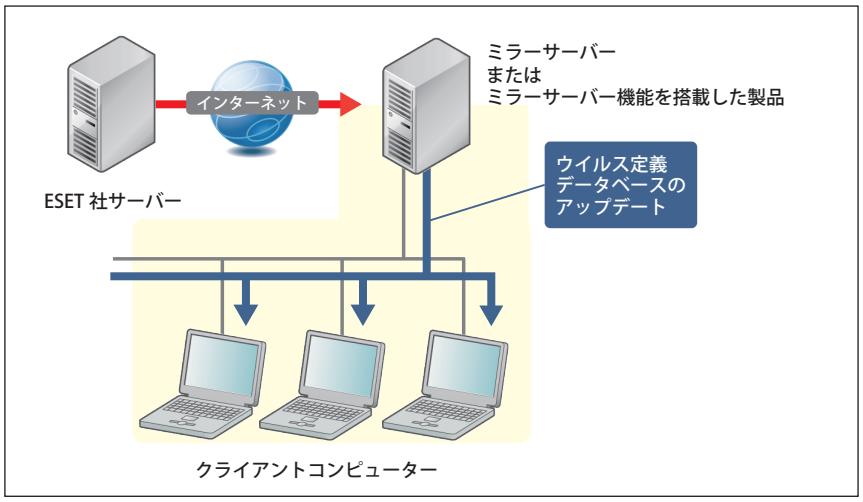
■モデルケース 2「ミラーサーバーを使用（ERA サーバーなし・100 クライアント未満）」

ミラーサーバーは、ウイルス定義データベースなどのアップデートファイルを社内 LAN 経由でクライアントコンピューターに提供します。各クライアントコンピューターは、アップデートのためのインターネット接続が不要になります。これにより、トラフィックを低減させ、インターネット接続環境にないクライアントコンピューターにもアップデートファイルを配布できます。

ミラーサーバー機能は、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linux に搭載されています。

ESET Endpoint Security、ESET Endpoint アンチウイルスは、サーバー OS では使用できないので、Windows サーバーで利用する場合は、ESET File Security for Microsoft Windows Server を使用してください。

ESET Endpoint Security、ESET Endpoint アンチウイルスを利用してミラーサーバーを構築する場合は、クライアントコンピューター 100 台以下を推奨しています。



構成

- ミラーサーバー 1 台
- HTTP サーバー機能を利用してアップデートファイルを配布

クライアント数の目安

- 100 台

サーバー仕様

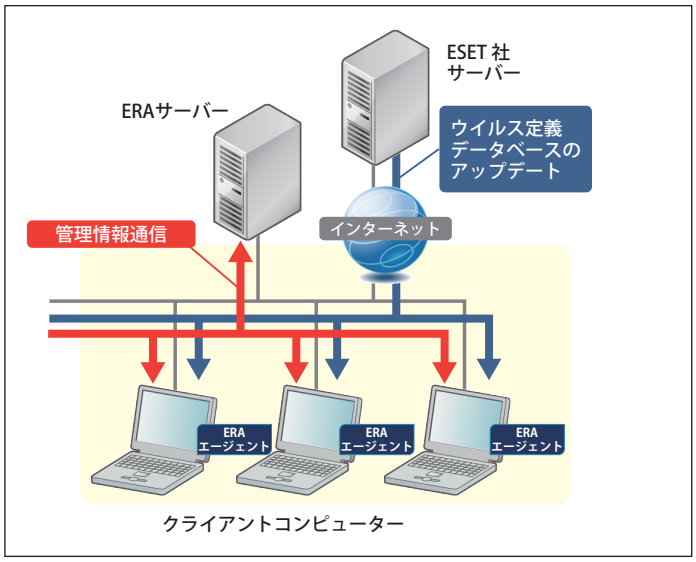
- CPU：インテル互換プロセッサ デュアルコア 2.0GHz と同等以上
- メモリー：2GB 以上
- ネットワークアダプター：1Gbps

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

■モデルケース 3「ERA サーバーを使用（ミラーサーバーなし・400 クライアント未満）」

ERA サーバーのみを使用する運用では、ESET Remote Administrator を導入して各クライアントコンピューターを管理します。各クライアントコンピューターには ERA エージェントをインストールします。
ウイルス定義データベースなどのアップデートファイルは、各クライアントコンピューターが直接 ESET 社のサーバーから取得します。
このモデルケースでは、クライアント数が 400 台程度でサーバー要件が変わる点に注意してください。



構成

- ERA サーバー 1 台で運用
- データベース：Microsoft SQL Server 2008 R2 Express で運用

クライアント数の目安

- 400 台以下

サーバー仕様

- CPU：インテル互換プロセッサ デュアルコア 2.0GHz と同等以上
- メモリー：2GB 以上
- ネットワークアダプター：1Gbps

クライアントの接続間隔

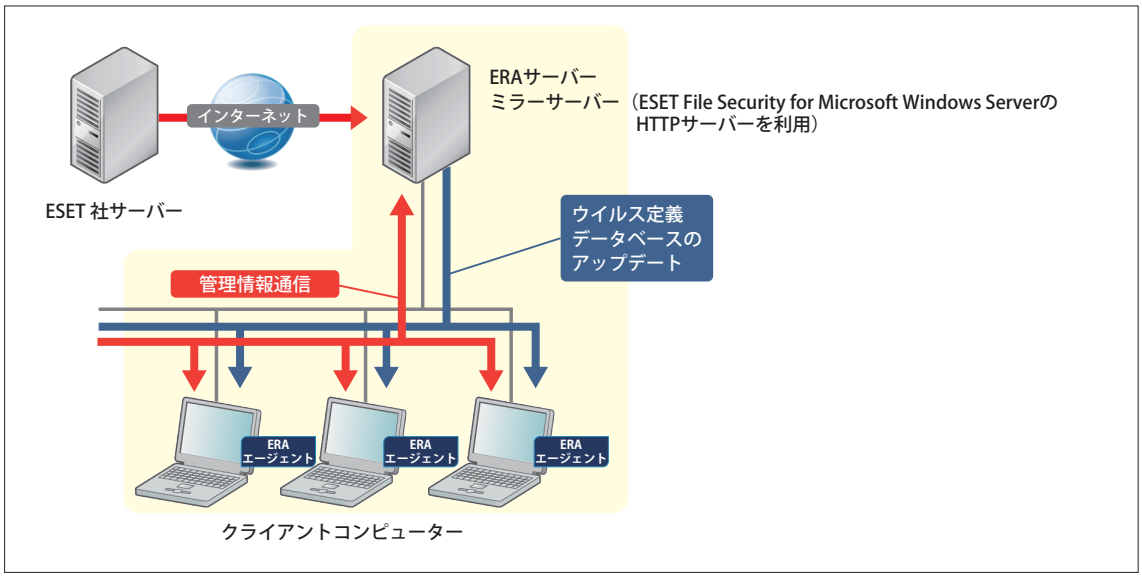
- ERA サーバーへの接続間隔：10 分

■モデルケース 4「ERA サーバーとミラーサーバーを兼用（400 クライアント未満）」

ESET Remote Administrator と ESET File Security for Microsoft Windows Server をインストールします。ESET File Security for Microsoft Windows Server のミラーサーバー機能を使い、1 台のサーバーで ERA サーバーとミラーサーバーを運用します。

ワンポイント

1 台のサーバーマシンで兼用する場合、負荷が大きくなる場合があります。その場合は、ERA サーバーとミラーサーバーを別々に設置したり、各サーバーをそれぞれ 2 台以上設置したりすることを検討してください。



構成

- ERA サーバー・ミラーサーバーを 1 台のマシンで運用
- ESET File Security for Microsoft Windows Server のミラーサーバー機能を使用
- データベース：Microsoft SQL Server 2008 R2 Express で運用

クライアント数の目安

- 400 台以下

サーバー仕様

- CPU：インテル互換プロセッサ デュアルコア 2.0GHz と同等以上
- メモリー：2GB 以上
- ネットワークアダプター：1Gbps

クライアントの接続間隔

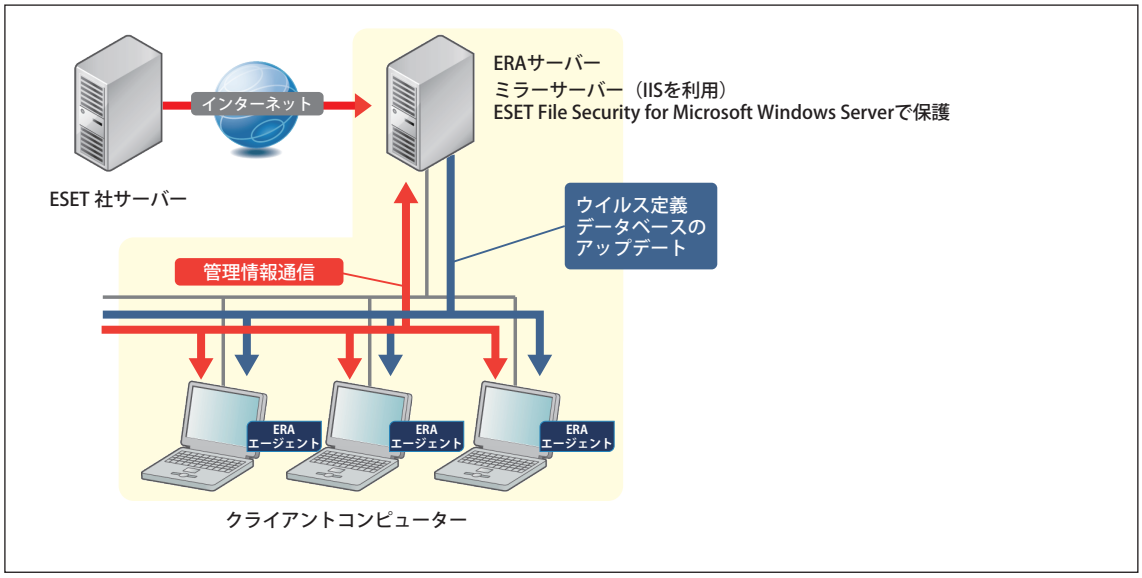
- ERA サーバーへの接続間隔：10 分
- ミラーサーバーへの接続間隔：60 分

■モデルケース 5「ERA サーバーとミラーサーバーを兼用（400 ～ 1,000 クライアント）」

ESET Remote Administrator と ESET File Security for Microsoft Windows Server をインストールします。
アップデートファイルの配布には、Microsoft Internet Information Services（IIS）を使用し、1 台のサーバーで ERA サーバーとミラーサーバーを運用します。

ワンポイント

1 台のサーバーマシンで兼用する場合、負荷が大きくなる場合があります。その場合は、ERA サーバーとミラーサーバーを別々に設置したり、各サーバーをそれぞれ 2 台以上設置したりすることを検討してください。



構成

- ERA サーバー・ミラーサーバーを 1 台のマシンで運用
- ミラーサーバーは Microsoft Internet Information Services（IIS）でアップデートファイルを配布
- データベース：Microsoft SQL Server 2008 R2 Express で運用

クライアント数の目安

- 1,000 台以下

サーバー仕様

- CPU：インテル互換プロセッサ デュアルコア 2.0GHz と同等以上
- メモリー：4GB 以上
- ネットワークアダプター：1Gbps

クライアントの接続間隔

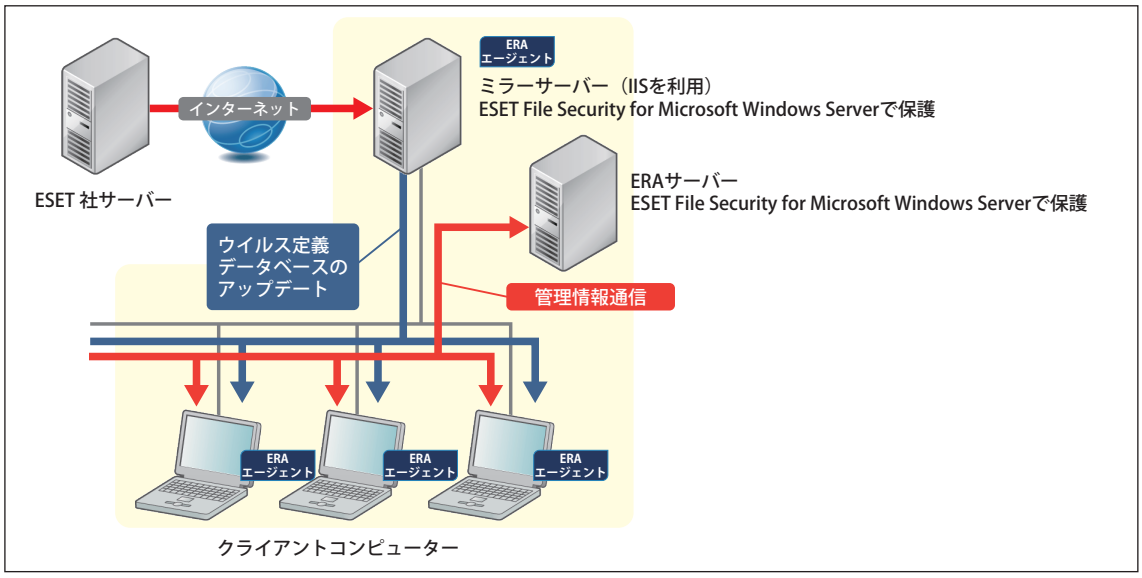
- ERA サーバーへの接続間隔：30 分
- ミラーサーバーへの接続間隔：60 分

■モデルケース 6「ERA サーバーとミラーサーバーを個別に運用（1,000 ～ 5,000 クライアント）」

ERA サーバーとミラーサーバーを別々のコンピューターで運用します。
アップデートファイルの配布には、Microsoft Internet Information Services（IIS）を使用します。
このケースでの ERA サーバーの接続クライアント数の上限は 5,000 台です。また、アップデートファイルの配布に利用するIISのミラーサーバーの接続クライアント数は5,000台です。そのため5,000台以上のクライアントが接続する場合は、IIS のミラーサーバーを複数台設置する必要があります。

ワンポイント

負荷が高い場合は、サーバーを複数台設置します。



構成

- ERA サーバー 1 台／ミラーサーバー 1 台以上
- ミラーサーバーは Microsoft Internet Information Services（IIS）でアップデートファイルを配布
  （接続クライアント数が 5,000 台を超える場合は、IIS のミラーサーバーを複数台設置）
- データベース：Microsoft SQL Server 2008 R2 Express で運用

クライアント数の目安

- 5,000 台以下

サーバー仕様

- CPU：インテル互換プロセッサ デュアルコア 3.0GHz と同等以上
- メモリー：4GB 以上
- ネットワークアダプター：1Gbps

クライアントの接続間隔

- ERA 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：60 分

■モデルケース 7「ERA サーバーとミラーサーバーを兼用（1,000 ～ 5,000 クライアント）」

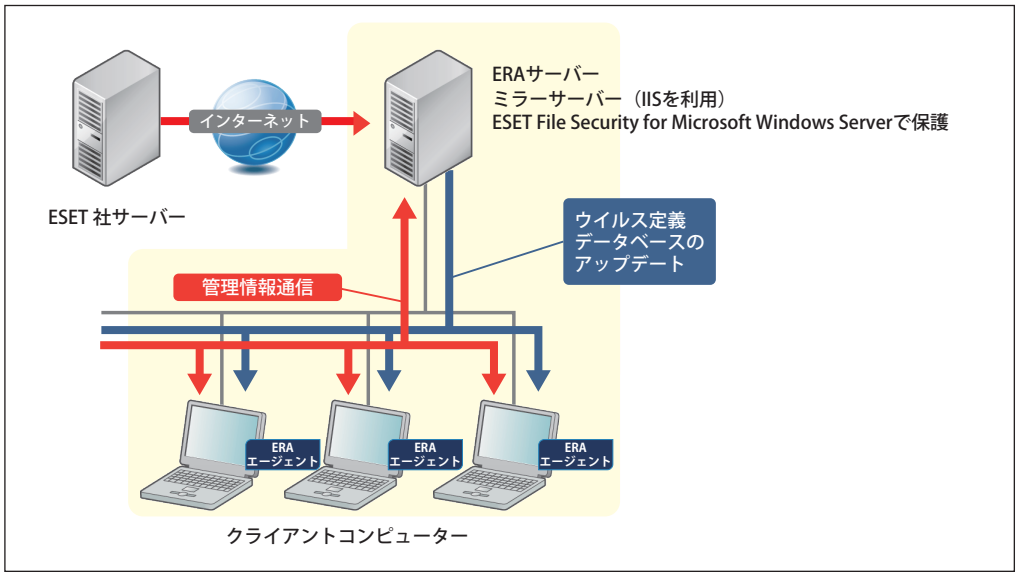
1 台のサーバーを ERA サーバー兼ミラーサーバーとして運用しますが、ストレージに RAID 0 構成の HDD または SSD を使用します。

アップデートファイルの配布には、Microsoft Internet Information Services（IIS）を使用します。

このケースでの ERA サーバーの接続クライアント数の上限は 5,000 台です。また、アップデートファイルの配布に利用するミラーサーバーの接続クライアント数は 5,000 台です。そのため 5,000 台以上のクライアントが接続する場合は、ミラーサーバーを複数台設置する必要があります。

ワンポイント

負荷が高い場合は、サーバーを複数台設置します。



構成

- ERA サーバーとミラーサーバーを兼用
- ミラーサーバーは IIS で運用
  （接続クライアント数が 5,000 台を超える場合は、IIS のミラーサーバーを複数台設置）
- データベース：Microsoft SQL Server 2008 R2 Express で運用

クライアント数の目安

- 5,000 台以下

サーバー仕様

- CPU：インテル互換プロセッサ デュアルコア 3.0GHz と同等以上
- メモリー：4GB 以上
- ネットワークアダプター：1Gbps
- RAID 0 構成の HDD または SSD

クライアントの接続間隔

- ERA 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：60 分

■モデルケース 8「ERA サーバーとミラーサーバーを個別に運用（5,000 ～ 10,000 クライアント）」

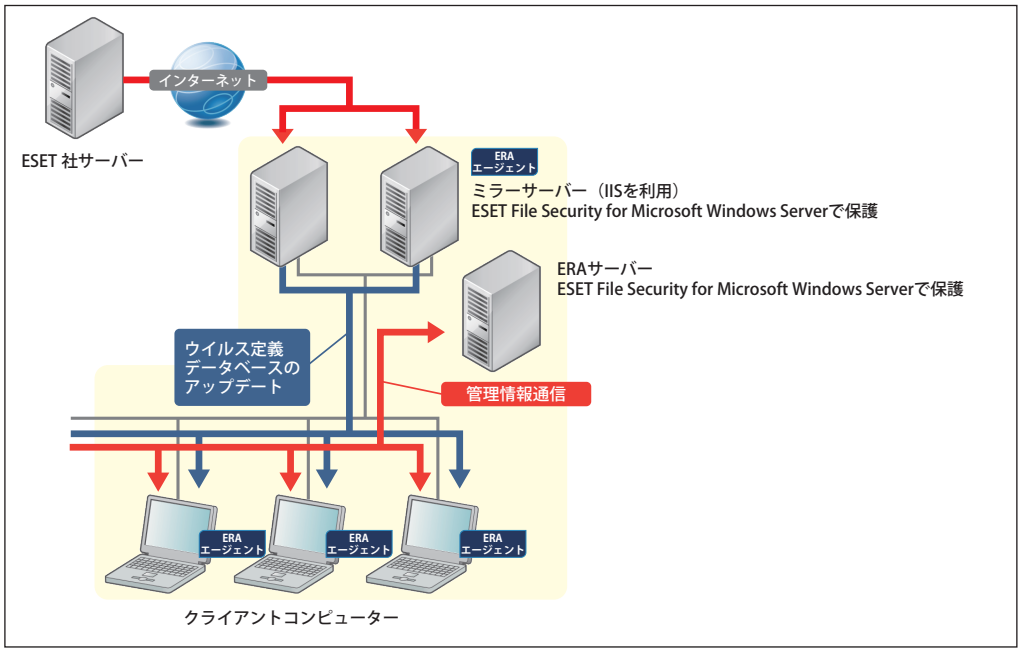
ERA サーバーとミラーサーバーを別々のコンピューターで運用します。また、ミラーサーバーは、ストレージに RAID0 構成の HDD または SSD を使用します。

アップデートファイルの配布には、Microsoft Internet Information Services（IIS）を使用します。

このケースでの ERA サーバーの接続クライアント数の上限は 10,000 台です。また、アップデートファイルの配布に利用する IIS のミラーサーバーの接続クライアント数は 5,000 台です。そのため 5,000 台以上のクライアントが接続する場合は、IIS のミラーサーバーを複数台設置する必要があります。

ワンポイント

負荷が高い場合は、サーバーを複数台設置します。



構成

- ERA サーバー 1 台とミラーサーバー 1 ～ 2 台で運用
  （接続クライアント数が 5,000 台を超える場合は、ミラーサーバーを複数台設置）
- データベース：Microsoft SQL Server 2008 R2 Express で運用

クライアント数の目安

- 10,000 台以下

サーバー仕様

ERA サーバー

- CPU：インテル互換プロセッサ デュアルコア 3.0GHz と同等以上
- メモリー：8GB 以上
- ネットワークアダプター：1Gbps
- RAID 0 構成の HDD または SSD

ミラーサーバー

- CPU：インテル互換プロセッサ デュアルコア 3.0GHz と同等以上
- メモリー：4GB 以上
- ネットワークアダプター：1Gbps

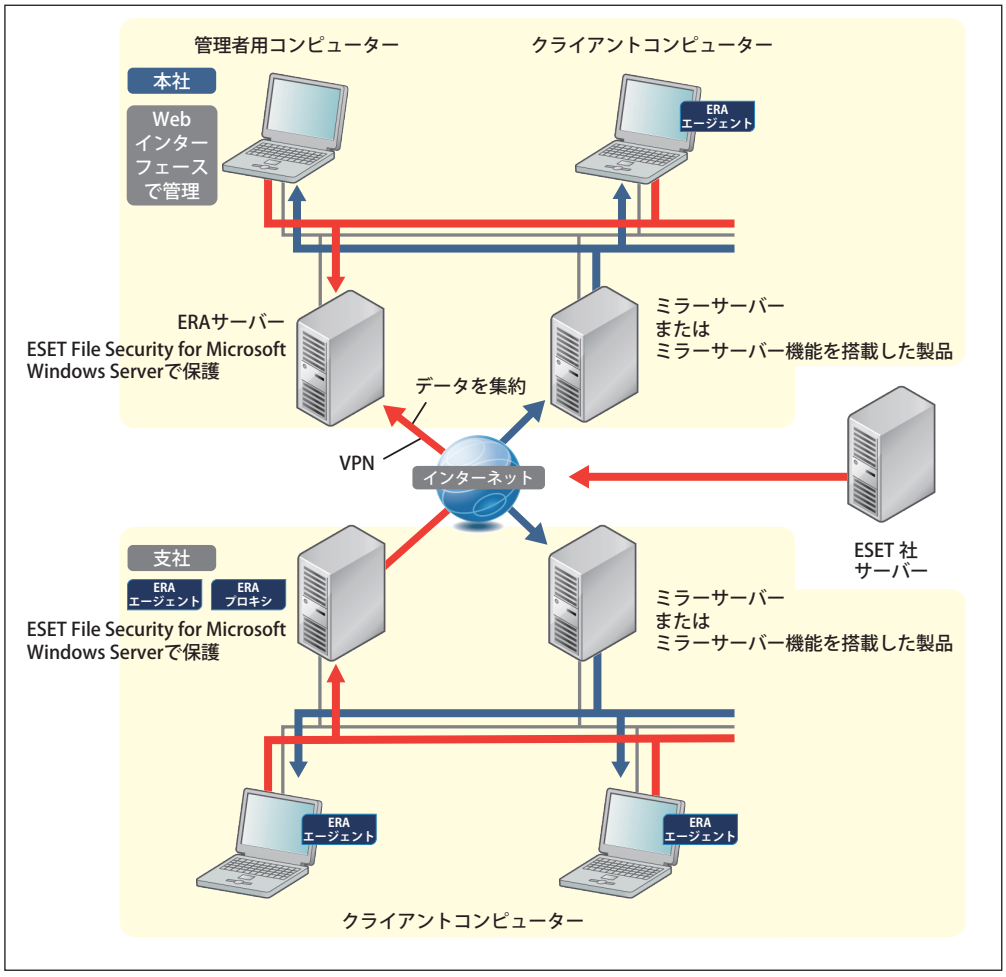
クライアントの接続間隔

- ERA 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：60 分

■モデルケース 9「複数拠点で ERA サーバーとミラーサーバーを運用（10,000 クライアント以上）」

複数の拠点がある場合は、前ページまでの構成例を目安に、各拠点または部署ごとに ERA プロキシやミラーサーバーを設置し、本社などに ERA サーバーを設置します。

このケースでは、支社に設置した ERA プロキシから、VPN などを介して ERA サーバーにデータを集約しています。



構成

- 設置する拠点や部署の規模に応じて、小規模や中規模の構成例を目安にする

サーバー仕様

- 設置する拠点や部署の規模に応じて、小規模や中規模の構成例を目安にする

クライアントの接続間隔

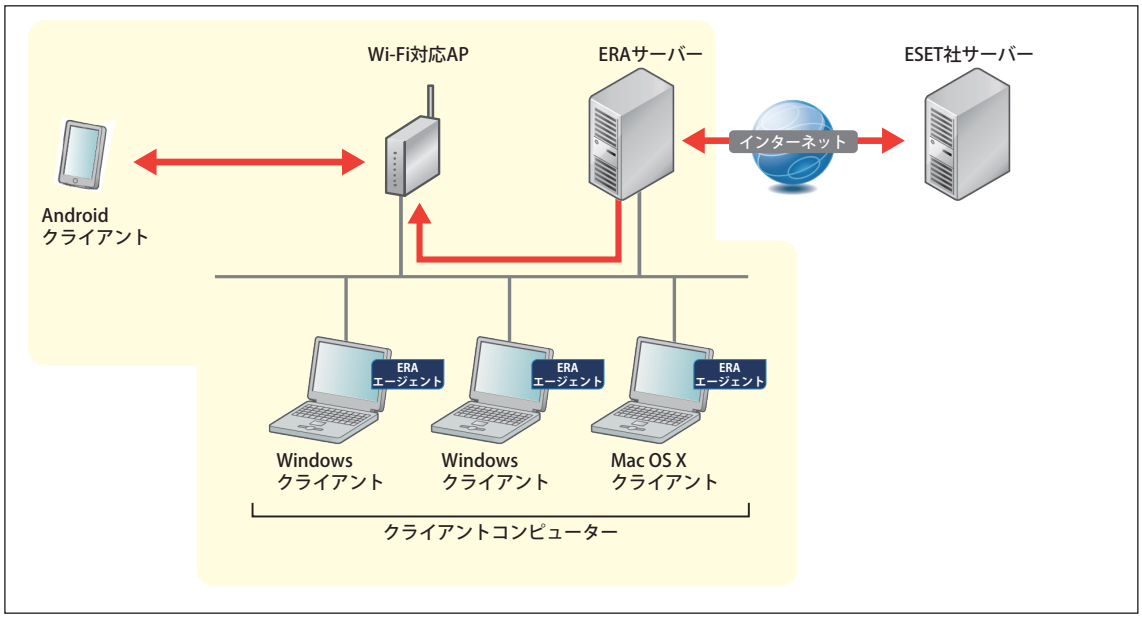
- 設置する拠点や部署の規模に応じて、小規模や中規模の構成例を目安にする

1.4.5 Android デバイスの管理構成

ERA を利用して ESET Endpoint Security for Android を管理する場合、モバイルデバイスコネクターのインストールが必要です。また、Android デバイスは、Wi-Fi や VPN などを利用して ERA に接続する方法があります。なお ESET Endpoint Security for Android の主な機能は ERA で管理しなくても利用可能です。

● Wi-Fi を利用して ERA に接続

Wi-Fi を利用して ESET Endpoint Security for Android を ERA に接続します。この構成では Wi-Fi に対応した無線 LAN アクセスポイント機器などを社内に設置し、Android デバイスの Wi-Fi 接続機能を利用し社内ネットワークに接続します。

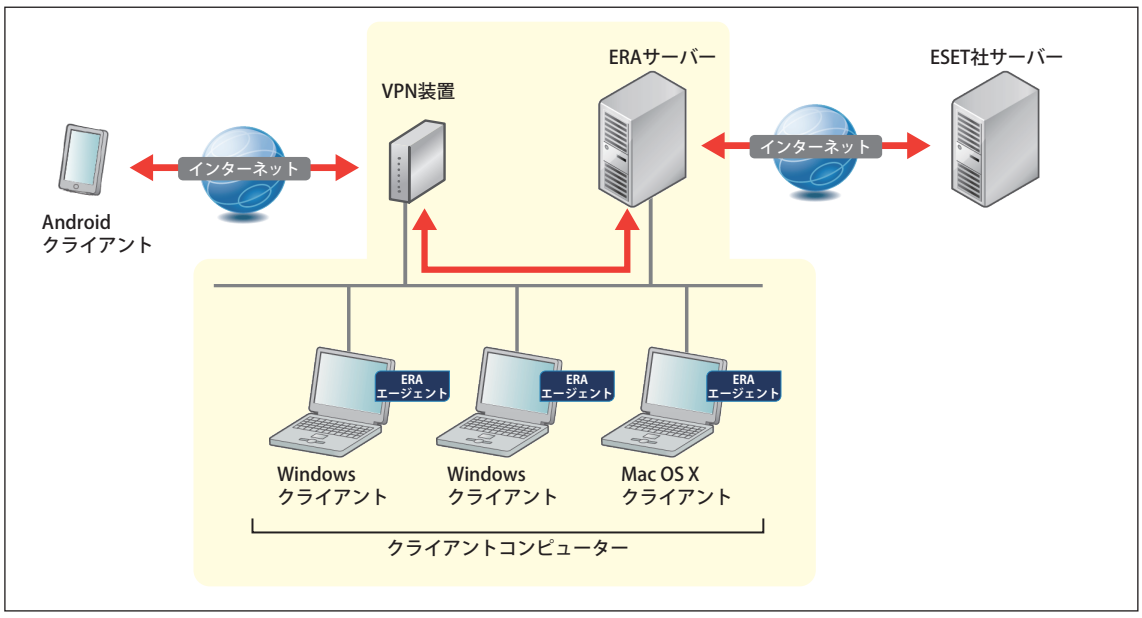


● VPN を利用して ERA に接続

VPN を利用して ESET Endpoint for Android を ERA に接続します。この構成では VPN 装置を設置し、Android デバイスの VPN 接続機能を利用してインターネット (社外) から社内に設置した ERA へセキュアに接続できます。

ワンポイント

VPN 接続の設定については、Android デバイスと VPN 装置のマニュアルなどを参照し設定してください。



1.5 STEP-3 ネットワーク環境の検討

1.5.1 ネットワーク環境のチェックポイント

ESET ライセンス製品を導入することで発生するネットワーク環境への影響を、次の点を中心に検討してください。

●ネットワークの負荷

ESET ライセンス製品を導入することで発生する通信トラフィックが、他業務などのネットワーク環境に影響を与えないかを検討します。
ESET ライセンス製品の導入によって発生する通信トラフィックについては「1.5.2 トラフィックの制御」を参照してください。

●インターネットの通信経路

ミラーサーバーは、インターネットを通じて ESET 社のアップデートサーバーからウイルス定義データベースなどのアップデートファイルを入手します。インターネット接続の経路上にあるプロキシサーバーやファイアウォールを確認して、ミラーサーバーの通信に影響がないかを確認します。

●サーバーとクライアントコンピューター間の通信経路

ERA サーバーとミラーサーバーは、定期的にクライアントコンピューターと通信します。ERA サーバー・ミラーサーバーとクライアントコンピューター間の通信経路を確認して、ファイアウォールなどで通信が遮断される可能性がある場合は設定の変更を検討します。

1.5.2 トラフィックの制御

ERA サーバーやミラーサーバーを導入すると、サーバーとクライアントコンピューターとの間で定期的に通信が発生します。
ESET ライセンス製品導入で発生する通信トラフィックは、クライアント管理に伴うトラフィックとウイルス定義データベースのアップデートに伴うミラーサーバー向けのトラフィックに大別されます。

■クライアント管理に伴うトラフィック

ERA エージェントと ERA サーバー間の通信です。定期的（既定値では 1 分間隔）にクライアントコンピューターからログなどの管理情報が送信されます。また、ERA サーバーからは設定ポリシーの配布などが行われます。
クライアント管理に伴うトラフィックは、次の項目の設定を変更して制御します。

クライアント管理トラフィックを減少させる設定項目

通信間隔	ERA エージェントが ERA サーバーと接続する間隔を増やすことによって、トラフィックを減少させます。
定期検査タイミング	クライアントコンピューターの定期検査をする場合、検査を実行する日時をグループ分けすることでスキャンログを分散させます。

発生する通信トラフィック例

通信内容	サイズ	備考
検出された脅威ログ	数 KB	クライアントが検出したウイルス情報です。
パーソナルファイアウォールログ（※ ESET Endpoint Security および ESET Endpoint Security for OS X のみ）	数 KB	ARP・DNS などを利用した侵入検出の通信情報です。この情報は、環境によっては、1 台で 1 日に数十件発生することもあります。
イベントログ	数 KB	ウイルス定義データベースアップデートの成功・失敗などのイベントです。 環境によっては、1 台で 1 日に数十件発生することもあります。
コンピュータの検査ログ	数 KB	スキャン対象の設定により、ログの容量が変動します。
隔離ログ	数 KB	クライアントがウイルスを隔離したログです。ウイルスの蔓延状況によりログの容量が変動します。
HIPS ログ（※ ESET Endpoint Security および ESET Endpoint アンチウイルスのみ）	数 KB	マルウェアやコンピューターのセキュリティに悪影響を与えようとする望ましくない活動からシステムを保護する HIPS のログです。既定値では、このログは取得されません。
デバイスコントロールログ	数 KB	USB ストレージや CD ／ DVD などのデバイスの制御動作のログです。既定値では、このログは取得されません。
Web コントロールログ	数 KB	Web コントロール動作のログです。既定値では、このログは取得されません。
ESET Live Grid	数 KB ～	ヒューリスティック機能により検出したウイルス情報を ESET 社に送付します。データ量は、検知したウイルスファイルと同等のサイズになります。
コンフィグレーション	数 10KB	ESET 製品の設定情報になります。
システム情報	数 KB	ハードウェア、ソフトウェア、ウイルス定義データベースのバージョンなどの情報です。

ワンポイント

検出された脅威ログ、コンピュータの検査ログ、ファイアウォールログ（※ ESET Endpoint Security および ESET Endpoint Security for OS X のみ）、イベントログが大量に発生した場合、サーバーやネットワークに大きな負荷がかかります。大規模な環境では、ログの保存期間の設定などによるサーバー負荷の減少を検討する必要があります。

■アップデートに伴うトラフィック

クライアントコンピューターとミラーサーバーなどアップデートを実行するサーバー間の通信です。主にクライアントコンピューターのウイルス定義データベースのアップデート時に発生します。
ウイルス定義データベースのアップデートに伴うトラフィックは、次の項目の設定変更で制御します。

アップデートトラフィックを減少させる設定項目

アップデートの間隔	クライアントコンピューターをグループ分けし、グループごとにアップデートの時間を変えることで、アップデートサーバーへのトラフィックを分散します。 ※アップデート間隔を長くすると、ウイルスに対するリスクが増えます。
差分アップデート機能	ウイルス定義データベースのコンパイルのためにパッキングされたファイル（パッキングファイル）を配信することがあります。これはベースアップデートと呼ばれ、年に 3、4 回の頻度で実施されます。 差分アップデートは、ウイルス定義データベースのコンパイルに必要な情報のみを配信することで、ベースアップデート時でも通常のアップデートとほぼ同等サイズのアップデートファイルの配信を行う機能です。これによってベースアップデート時のネットワーク負荷を減らすことができます。

ミラーサーバー向けのトラフィック通信仕様（2016 年 3 月時点）

種別	サイズ	備考
ウイルス定義データベース	約 10KB ～約 2MB （約数 KB ～約数百 KB）	日々配信される、差分更新用のファイルになります。 1 日に 3 回程度配信されます。
ベースアップデート①	約数 MB ～約 15MB （約数 KB ～約数百 KB）	ウイルス定義データベース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 回程度配信されます。
ベースアップデート②	約 10 数 MB ～約 40MB （約数 KB ～約 10MB）	ウイルス定義データベース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 回程度配信されます。
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。

差分アップデート機能が適用されている場合は、（）内に記載されたサイズとなります。なお、1 週間程度（33 世代以上）ウイルス定義データベースをアップデートしていない場合、差分アップデート機能は適用されません。

1.6 STEP-4 移行プランの検討

1.6.1 移行プランのチェックポイント

移行に関して次の点を中心にチェックしてください。

■他社製プログラムのアンインストール方法

一般的に、プログラムは次の方法でアンインストールします。

- 手動アンインストール
- 開発元から提供されている削除ツールを利用してアンインストール

■クライアント用プログラムの導入方法

クライアント用プログラムのインストール方法には、大きく「手動インストール」と「リモートインストール」の 2 種類があります。

インストール方法は、規模やネットワーク環境に合わせて検討する必要があります。

詳細は「1.6.3 クライアント用プログラム導入方法＜ Windows ＞」、「1.6.4 クライアント用プログラム導入方法 ＜ Mac OS X ＞」を参照してください。

●コンポーネント選択機能について

クライアント用プログラムでは、インストールするコンポーネント（機能）を選択することができます。

クライアントコンピューターに不要な機能をインストールしないことで、クライアントコンピューターの負荷を軽減できるほか、設定ミスなどによるトラブルを防止できます。詳細は各ユーザーズマニュアルを参照してください。

● ERA エージェントのインストール

ESET Remote Administrator で管理する場合は、クライアントコンピューターに ERA エージェントをインストールします。

1.6.2 移行プランの作成

移行期間のセキュリティレベル低下を防止してスムーズに移行するために、新規サーバーで ESET 製品環境を構築し、十分な検証を行った上で他社製品から順次移行することをお勧めします。

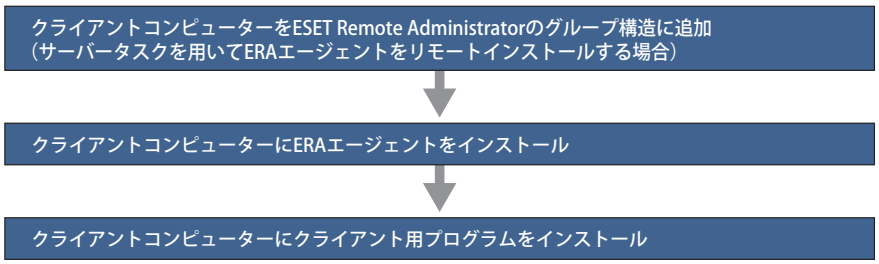
以下のサンプルプランを参考に、移行プランを作成してください。

サンプルプラン

項目	1 カ月目	2 カ月目	3 カ月目	4 カ月目
サーバー機器、ESET ライセンス製品の手配	→			
サーバーの構築		→		
サーバーの設置		▲		
クライアントの展開 （既存プログラムの削除と ESET 製品のインストール）		→	→	
既存プログラムのライセンス終了 （既存プログラム用サーバーの撤去）			▲	
ESET 製品の本番運用		→	→	→
既存プログラムと ESET 製品の共存期間		↔	↔	

1.6.3 クライアント用プログラム導入方法< Windows >

Windows 版のクライアント用プログラム導入の流れを説明します。
クライアント用プログラムの導入方法には、様々な方法があります。ERA サーバーを使用しない場合は、ファイルサーバーからクライアント用プログラムのインストーラーをダウンロードし、手動でインストールを行います。ERA サーバーを使用する場合は、次の手順で、クライアントコンピューターを ESET Remote Administrator で管理し、各コンピューターにクライアント用プログラムをインストールします。



最初に、クライアントコンピューターを ESET Remote Administrator で管理できるように、各クライアントコンピューターに ERA エージェントをインストールします。
ERA エージェントは、ESET Remote Administrator とクライアントコンピューターの通信を行うソフトウェアです。
最後に、ERA エージェントを通じて各クライアントコンピューターにクライアント用プログラムをインストールします。

■ ERA グループ構造へのクライアントコンピューターの追加

サーバータスクを用いて ERA エージェントをリモートインストールする場合は、ESET Remote Administrator で管理するクライアントコンピューターを、ERA グループ構造に登録します。
登録には次の 3 つの方法があります。

- Active Directory 同期
- コンピューター名や IP アドレスを手動入力
- RD Sensor を使用して登録

● Active Directory 同期

ERA Web コンソールで、「静的グループの同期」サーバータスクを作成して実行します。

●コンピューター名や IP アドレスを手動入力

ERA Web コンソールの［コンピュータ］メニューの［新規追加］で、追加するクライアントコンピューターの名前や IP アドレスを入力します。

● RD Sensor を使用して登録

Rogue Detection Sensor（RD Sensor）は、ネットワーク上のコンピューターを検出するツールです。
検出されたコンピューターは、コンピューターレポートに一覧表示されます。
未登録のコンピューター名をクリックして ESET Remote Administrator に追加します。

■ ERA エージェントのインストール

クライアントコンピューターに、ERA エージェントをインストールします。
ERA エージェントのインストールには、次の 3 つの方法があります。

- GPO（Group Policy Object）と SCCM（Microsoft System Center Configuration Manager）を使用してリモートインストール
- サーバータスクを使用してリモートインストール
- ローカルインストール

● GPO と SCCM を使用してリモートインストール

弊社ユーザーズサイトから「ESET エージェント」ファイルをダウンロードして、GPO と SCCM を使ってクライアントコンピューターにリモートインストールします。

●サーバータスクを使用してリモートインストール

ERA Web コンソールの［管理］メニューで［サーバータスク］を選択して［エージェント展開］を実行します。

●ローカルインストール

クライアントコンピューター上でインストール作業をします。
ローカルインストールには、次の方法があります。

オールインワンインストーラー

ERA エージェントと ESET 製品を 1 つのインストーラーに組み込んだオールインワンインストーラーを、ユーザーに配布してクライアントコンピューター上でインストールします。
ESET 製品の設定や ERA エージェントの設定を組み込め、アクティベーション情報も含めることができます。
オールインワンインストーラーは ESET Remote Administrator V6.5 以降で作成することができます。

エージェントライブインストーラー

エージェントライブインストーラーを、メールや USB メディアを使ってユーザーに配布してクライアントコンピューター上でインストールを実行します。
エージェントライブインストーラーは ESET Remote Administrator で作成することができます。証明書情報を付加することができるため、クライアント側で手動の設定を行うことなく、ERA エージェントをインストールすることができます。

サーバー支援インストール／オフラインインストール

弊社ユーザーズサイトから「ERA エージェント」ファイルをダウンロードします。インストーラーを実行して「サーバー支援インストール」または「オフラインインストール」を選択します。
オフラインインストールでは「ピア証明書」と「認証局」を指定する必要があります。

■クライアントコンピューターにクライアント用プログラムをインストール

ERA エージェントをインストールしたクライアントコンピューターに、クライアント用プログラムをインストールします。クライアント用プログラムのインストールには次の 2 つの方法があります。

- クライアントタスクを使用してリモートインストール
- ローカルインストール

●クライアントタスクを使用してリモートインストール

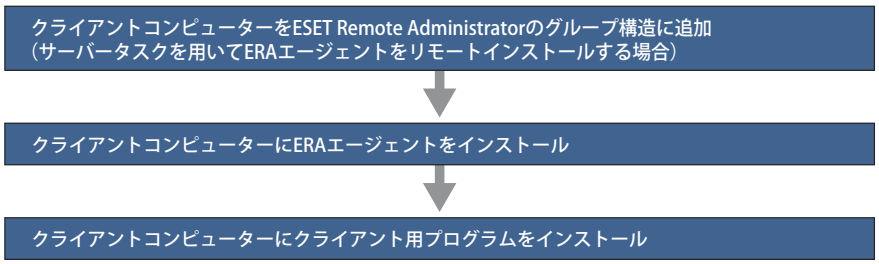
ERA Web コンソールの「管理」メニューで [クライアントタスク] を選択して、「ソフトウェアインストール」を実行します。

●ローカルインストール

リモートインストールで問題が発生した場合などは、クライアントコンピューター上でインストール作業をします。
それぞれのインストール方法の詳細な手順は、『ESET Remote Administrator ユーザーズマニュアル』および、各クライアント用プログラムのユーザーズマニュアルを参照してください。

1.6.4 クライアント用プログラム導入方法 < Mac OS X >

Mac OS X 版のクライアント用プログラム導入の流れを説明します。
クライアント用プログラムの導入方法には、様々な方法があります。ERA サーバーを使用しない場合は、ファイルサーバーからクライアント用プログラムのインストーラーをダウンロードし、手動でインストールを行います。ERA サーバーを使用する場合は、次の手順で、クライアントコンピューターを ESET Remote Administrator で管理し、各コンピューターにクライアント用プログラムをインストールします。



最初に、クライアントコンピューターを ESET Remote Administrator で管理できるように、各クライアントコンピューターに ERA エージェントをインストールします。
ERA エージェントは、ESET Remote Administrator とクライアントコンピューターの通信を行うソフトウェアです。
最後に、ERA エージェントを通じて各クライアントコンピューターにクライアント用プログラムをインストールします。

■ ERA グループ構造へのクライアントコンピューターの追加

サーバータスクを用いて ERA エージェントをリモートインストールする場合は、ESET Remote Administrator で管理するクライアントコンピューターを、ERA グループ構造に登録します。
登録には次の 2 つの方法があります。

- コンピューター名や IP アドレスを手動入力
- RD Sensor を使用して登録

●コンピューター名や IP アドレスを手動入力

ERA Web コンソールの［コンピュータ］メニューの［新規追加］で、追加するクライアントコンピューターの名前や IP アドレスを入力します。

● RD Sensor を使用して登録

Rogue Detection Sensor（RD Sensor）は、ネットワーク上のコンピューターを検出するツールです。
検出されたコンピューターは、コンピューターレポートに一覧表示されます。
未登録のコンピューター名をクリックして ESET Remote Administrator に追加します。

■ ERA エージェントのインストール

クライアントコンピューターに、ERA エージェントをインストールします。
ERA エージェントのインストールには、次の 3 つの方法があります。

- サーバータスクを使用してリモートインストール
- ローカルインストール

●サーバータスクを使用してリモートインストール

ERA Web コンソールの［管理］メニューで［サーバータスク］を選択して［エージェント展開］を実行します。

●ローカルインストール

クライアントコンピューター上でインストール作業をします。
ローカルインストールには、次の方法があります。

エージェントライブインストーラー

エージェントライブインストーラーを、メールや USB メディアを使ってユーザーに配布してクライアントコンピューター上でインストールを実行します。
エージェントライブインストーラーは ESET Remote Administrator で作成することができます。証明書情報を付加することができるため、クライアント側で手動の設定を行うことなく、ERA エージェントをインストールすることができます。

オフラインインストール

弊社ユーザーズサイトから「ERA エージェント」ファイルをダウンロードします。
オフラインインストールでは「ピア証明書」と「認証局」を指定する必要があります。

■クライアントコンピューターにクライアント用プログラムをインストール

ERA エージェントをインストールしたクライアントコンピューターに、クライアント用プログラムをインストールします。クライアント用プログラムのインストールには次の 2 つの方法があります。

- クライアントタスクを使用してリモートインストール
- ローカルインストール

●クライアントタスクを使用してリモートインストール

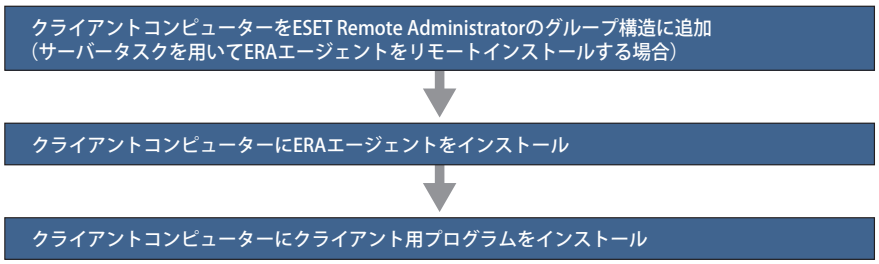
ERA Web コンソールの「管理」メニューで [クライアントタスク] を選択して、「ソフトウェアインストール」を実行します。

●ローカルインストール

リモートインストールで問題が発生した場合などは、クライアントコンピューター上でインストール作業をします。
それぞれのインストール方法の詳細な手順は、『ESET Remote Administrator ユーザーズマニュアル』および、各クライアント用プログラムのユーザーズマニュアルを参照してください。

1.6.5 クライアント用プログラム導入方法 < Linux >

Linux 版のクライアント用プログラム導入の流れを説明します。
クライアント用プログラムの導入方法には、様々な方法があります。ERA サーバーを使用しない場合は、ファイルサーバーからクライアント用プログラムのインストーラーをダウンロードし、手動でインストールを行います。ERA サーバーを使用する場合は、次の手順で、クライアントコンピューターを ESET Remote Administrator で管理し、各コンピューターにクライアント用プログラムをインストールします。



最初に、クライアントコンピューターを ESET Remote Administrator で管理できるように、各クライアントコンピューターに ERA エージェントをインストールします。
ERA エージェントは、ESET Remote Administrator とクライアントコンピューターの通信を行うソフトウェアです。
最後に、ERA エージェントを通じて各クライアントコンピューターにクライアント用プログラムをインストールします。

■ ERA グループ構造へのクライアントコンピューターの追加

サーバータスクを用いて ERA エージェントをリモートインストールする場合は、ESET Remote Administrator で管理するクライアントコンピューターを、ERA グループ構造に登録します。
登録には次の 2 つの方法があります。

- コンピューター名や IP アドレスを手動入力
- RD Sensor を使用して登録

●コンピューター名や IP アドレスを手動入力

ERA Web コンソールの［コンピュータ］メニューの［新規追加］で、追加するクライアントコンピューターの名前や IP アドレスを入力します。

● RD Sensor を使用して登録

Rogue Detection Sensor（RD Sensor）は、ネットワーク上のコンピューターを検出するツールです。
検出されたコンピューターは、コンピューターレポートに一覧表示されます。
未登録のコンピューター名をクリックして ESET Remote Administrator に追加します。

■ ERA エージェントのインストール

クライアントコンピューターに、ERA エージェントをインストールします。
ERA エージェントのインストールには、次の 3 つの方法があります。

- サーバータスクを使用してリモートインストール
- ローカルインストール

●サーバータスクを使用してリモートインストール

ERA Web コンソールの［管理］メニューで［サーバータスク］を選択して［エージェント展開］を実行します。

●ローカルインストール

クライアントコンピューター上でインストール作業をします。
ローカルインストールには、次の方法があります。

エージェントライブインストーラー

エージェントライブインストーラーを、メールや USB メディアを使ってユーザーに配布してクライアントコンピューター上でインストールを実行します。
エージェントライブインストーラーは ESET Remote Administrator で作成することができます。証明書情報を付加することができるため、クライアント側で手動の設定を行うことなく、ERA エージェントをインストールすることができます。

サーバー支援インストール／オフラインインストール

弊社ユーザーズサイトから「ERA エージェント」ファイルをダウンロードします。インストーラーを実行して「サーバー支援インストール」または「オフラインインストール」を選択します。
オフラインインストールでは「ピア証明書」と「認証局」を指定する必要があります。

■クライアントコンピューターにクライアント用プログラムをインストール

ERA エージェントをインストールしたクライアントコンピューターに、クライアント用プログラムをインストールします。クライアント用プログラムのインストールには次の 2 つの方法があります。

- クライアントタスクを使用してリモートインストール
- ローカルインストール

●クライアントタスクを使用してリモートインストール

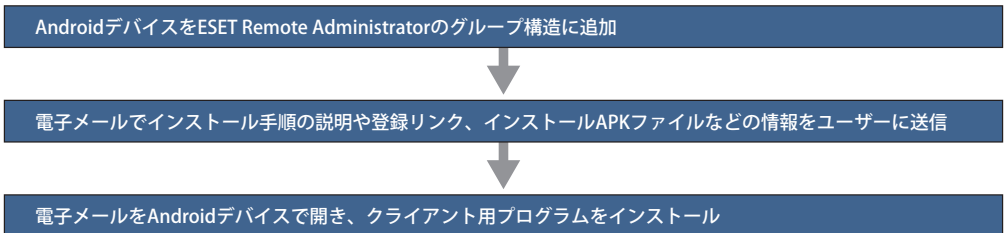
ERA Web コンソールの「管理」メニューで [クライアントタスク] を選択して、「ソフトウェアインストール」を実行します。

●ローカルインストール

リモートインストールで問題が発生した場合などは、クライアントコンピューター上でインストール作業をします。
それぞれのインストール方法の詳細な手順は、『ESET Remote Administrator ユーザーズマニュアル』および、各クライアント用プログラムのユーザーズマニュアルを参照してください。

1.6.6 クライアント用プログラム導入方法＜ Android ＞

Android 版のクライアント用プログラム導入の流れを説明します。クライアント用プログラムの導入方法には、様々な方法があります。ERA サーバーを使用しない場合は、Google Play Store やユーザースサイトからクライアント用プログラムのインストーラー（APK ファイル）をダウンロードし、手動でインストールを行います。ERA サーバーを使用する場合は、次の手順で、クライアントコンピューターを ESET Remote Administrator で管理し、各 Android デバイスでクライアント用プログラムをインストールします。



■ ERA グループ構造への Android デバイスの追加

ESET Remote Administrator で管理する Android デバイスを、ERA グループ構造に登録します。Android デバイスの登録には、ERA サーバーにモバイルデバイスコネクター（Mobile Device Connector）をインストールしておく必要があります。

● Android デバイスの登録（モバイルデバイス登録）

ERA Web コンソールの［クライアントタスク］メニューの［モバイル］セクション内にある［デバイス登録］で登録を行います。ESET Remote Administrator 6.3 をご利用の場合は、［デバイス登録］の［新規追加］で、追加する Android デバイスの IMEI 番号や Wi-Fi MAC アドレス、メールアドレスなどを入力します。タスク名や説明は、任意で入力します。IMEI 番号や Wi-Fi MAC アドレスは事前に調べておきます。

ワンポイント

Android デバイスの識別は、IMEI 番号や Wi-Fi MAC アドレスが利用されます。通常、SIM カードを挿入できる Android デバイスは IMEI 番号を識別情報として登録してください。また、SIM カードを挿入できない Android デバイスは、Wi-Fi MAC アドレスを登録してください。
ESET Remote Administrator 6.5 をご利用の場合は、Android デバイスの登録の際に事前に IMEI 番号や Wi-Fi MAC アドレスを入力する必要はありません。
ESET Remote Administrator 6.5 をご利用の場合は、登録する Android デバイス毎に異なる接続リンクが発行され、登録の際に設定した電子メールアドレス宛に接続リンクが送信されます。

■ Android デバイスにクライアント用プログラムをインストール

ERA サーバーからの登録リンクを利用して ESET Endpoint Security for Android のインストールを行うには次の要件を確認してください。

- ERA サーバーと ERA Web コンソールがサーバーコンピューターにインストールされている
- ERA サーバーにモバイルデバイスコネクター（Mobile Device Connector）がインストールされている
- サーバーコンピューターがネットワークから通信可能
- モバイルデバイス登録が行われている

●イントールの方法

ESET Endpoint Security for Android のインストールは、次の 2 つの方法で実行できます。

- 電子メールを利用したインストール
- ローカルインストール

●電子メールを利用したインストール

ESET Endpoint Security for Android の電子メールを利用したインストールは、次の 2 つの方法で実行できます。

ERA サーバーからの登録リンクを利用

管理者は ERA サーバーより、登録リンク、インストール手順の簡単な説明を電子メールでエンドユーザーに送信します（または、ERA に表示された登録リンクに Android デバイスのブラウザより直接アクセスします）。リンクをタップすると、ユーザーは Android デバイスの既定のインターネットブラウザに移動します。ESET Endpoint Security for Android が登録され、ERA サーバーに移動します。ESET Endpoint Security for Android がデバイスにインストールされていない場合、自動的に Google Play Store に移動するため、ESET Endpoint Security for Android をダウンロードします。その後、標準インストールが実行されます。

●ローカルインストール

ERA サーバーによる管理を必要としない場合、管理者は ESET Endpoint Security for Android をローカルでセットアップして管理できます。各種設定は手動で行い、設定をファイルにエクスポートできます。また、エクスポートした設定ファイルは、ESET Endpoint Security for Android をインストールした任意の Android デバイスにインポートして利用できます。すべてのアプリケーション設定は管理者パスワードによって保護されます。
ローカルインストールを行うときは、ユーザーズサイトまたは Google Play Store からインストール APK ファイルをダウンロードしてインストールを行います。

ユーザーズサイトからダウンロード

ユーザーズサイトより ESET Endpoint Security for Android をダウンロードします。不明なソースまたは提供元不明のアプリのインストールが許可されていることを確認してください。

Google Play Store からダウンロード

以下のリンクを使用すると、プログラムをダウンロードできます。また、Android デバイスで Google Play Store アプリケーションを開き、ESET Endpoint Security (または ESET) を検索します。

https://play.google.com/store/apps/details?id=com.eset.endpoint

1.6.7 オフライン環境に導入する

インターネット接続が行えないオフライン環境のコンピューターにクライアント用プログラムをインストールするときは、クライアント用プログラムのインストールを行った後に「オフラインライセンスファイル」を利用して製品のアクティベーションを行います。アクティベーションに利用するオフラインライセンスファイルは、ELA（ESET License Administrator）で発行できます。また、オフラインライセンスは ESET Remote Administrator で管理でき、手動または ESET Remote Administrator を利用してファイルを利用してアクティベーションを行えます。

■オフラインライセンスファイルの発行

インターネット接続が行えないコンピューターのアクティベーションを行うには、最初に ELA（ESET License Administrator）を利用してオフラインライセンスファイルの発行を行います。続いて、オフラインライセンスファイルを利用してクライアント用プログラムのアクティベーションを実施します。ELA（ESET License Administrator）は、ユーザーズサイトより接続することができます。オフラインライセンスファイルのダウンロード手順は以下のサポートページの Q&A を参照してください。

Q&A の URL : http://eset-support.canon-its.jp/faq/show/4327?site_domain=business

■ ESET Remote Administrator で管理する

ELA（ESET License Administrator）で発行したオフラインライセンスファイルを ESET Remote Administrator で管理したいときは、ESET Remote Administrator にダウンロードしたオフラインライセンスファイルの登録を行います。オフラインライセンスファイルの登録は、ERA Web コンソールを開き、［管理］→［ライセンス管理］→［ライセンスの追加］とクリックして「ライセンスの追加」画面を開き、［オフラインライセンスファイル］をクリックすることで行えます。

また、オフラインライセンスファイルの登録を行うと、ESET Remote Administrator の「ライセンス管理」画面に登録されたオフラインライセンスの総数が表示されます。

■オフラインライセンスファイルを利用した手動アクティベーション

オフラインライセンスファイルを利用して手動でアクティベーションを行うときは、ダウンロードしたオフラインライセンスファイルを、アクティベーションを行うコンピューターで読み出せるようにしておきます。続いて、クライアント用プログラムのメイン画面を開き、［ヘルプ］→［製品のアクティベーション］とクリックしてライセンス画面を開き、［オフラインライセンス］をクリックしてアクティベーションを行います。オフラインライセンスファイルを利用した手動アクティベーションは、Windows 用および Mac OS X 用、Linux 用のクライアント用プログラムともに共通の手順で行えます。

1.6.8 複数拠点がある場合の導入方法

本社と支社など複数の拠点がある場合は、それぞれの環境に応じたクライアント用プログラムのインストール方法を検討します。クライアント用プログラムを展開する際、ESET Remote Administrator のポリシー機能やグループ機能を利用するとインストールや設定管理が容易になります。

■クライアント展開のポイント

ESET Remote Administrator には、クライアントコンピューターを効率的に管理し、スムーズな運用を行うために「グループ機能」や「ポリシー機能」が搭載されています。これらの機能を利用して ERA サーバーから各クライアントコンピューターの設定を管理することができます。

●グループ機能

グループ機能は、クライアントコンピューターをグループに分類して管理する機能です。グループは、手動で作成する「静的グループ」と、条件を指定して自動的にグループ分けを行う「動的グループ」を作成できます。たとえば、複数の拠点がある場合は、動的グループを利用することで、グループ分けを自動化できます。

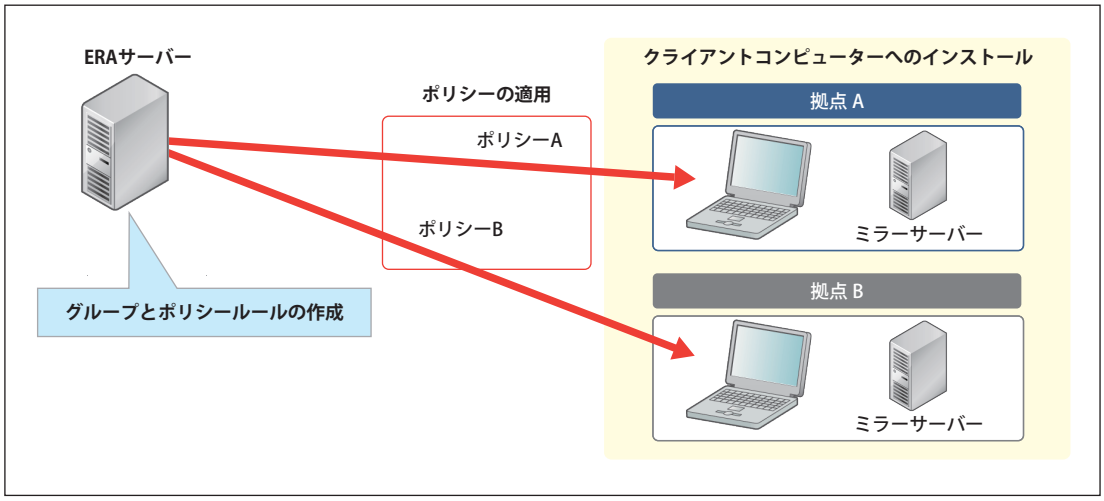
●ポリシー機能

クライアントコンピューターに、強制的に設定を適用する機能です。この機能を利用すると、グループ機能で作成した特定のグループに対して同じ設定を適用できます。動的グループを使用すれば、グループ分けとポリシーの適用を自動化することができます。

■ポリシー機能とグループ機能を利用した展開の流れ

ポリシー機能とグループ機能を使って本社と支社間など、複数の拠点にクライアント用プログラムを展開します。
グループ機能を使ってポリシーを適用するには、ERA Web コンソールで次の操作をします。

1. 新しいポリシーを作成します。
2. グループおよびクライアントコンピューターにポリシーを割り当てます。



1.6.9 クライアント用プログラムとサーバー用プログラムの設定

クライアント用プログラムは、クライアントコンピューターだけでなく ERA サーバーにも導入できます。それぞれで設定項目が異なります。ここでは、それぞれの利用環境に合わせた運用を行うための設定のポイントを説明します。

■サーバーとクライアントコンピューターの設定のポイント

クライアント用プログラムの設定で重要なのが、導入するコンピューターの役割です。クライアントコンピューターではコンピューターの安全の維持が最優先ですが、サーバーに導入する場合は、安全性だけでなく、サーバー負荷をできるだけ減らすような工夫も重要です。以下の点に着目して設定を行うことをお勧めします。

クライアントコンピューターの設定のポイントと注意点
●リモート管理 ●アップデート ●定期検査 ●設定変更のパスワードロック（パラメーター設定の保護） ※Windows用プログラムのみ ●アップデートの冗長化 ●ウイルス検出時のアクション（リアルタイムファイルシステム保護の場合 ●検査対象からの除外 ●ThreatSense.Net早期警告システム

サーバーの設定のポイントと注意点
●一部検査機能の無効化 ●データベースなどのアプリケーションの検査除外 ●コンポーネントアップデート時のOS再起動の無効化

■設定と動作

●リモート管理・アップデート

ERA サーバーやミラーサーバーを設置する場合は、クライアント用プログラムの各サーバーへの接続設定を既定値から変更する必要があります。

●定期検査

クライアント用プログラムは、定期検査のスケジュールを自由に設定できるだけでなく、検査対象とするデータなども設定できます。既定値では定期的な検査スケジュールは設定されていません。コンピューターの安全を維持するためにも、1 週間に 1 回の頻度を目安に定期的な検査を実施するように設定することをお勧めします。

●パラメーター設定の保護

ユーザーが設定変更できないようにパスワード保護をかけ、必要な場合は管理者が変更するように設定することができます。
パスワード保護をかけると、クライアント用プログラムのアンインストールにもパスワード入力が必要になります。
また、V6 以降のクライアント用プログラムでは ERA からポリシーとして割り当てられたパラメーター設定はユーザーが設定変更できなくなります。

●アップデートの冗長化

コンピューターの安全を確保するには、ウイルス定義データベースの迅速なアップデートが欠かせません。クライアント用プログラムでは、2 つのアップデートプロファイルとスケジューラーを利用することで、プライマリとセカンダリの 2 つのアップデートサーバーを設定することができます。プライマリアップデートサーバーが利用できないときに自動的にセカンダリアップデートサーバーに切り替えてアップデートを実行します。
たとえば、プライマリサーバーにミラーサーバーを指定し、セカンダリサーバーに ESET 社のアップデートサーバーを設定することで、クライアントコンピューターを社外で使用する場合でも常に最新のウイルス定義データベースを適用することができます。
手動アップデート時は、現在設定されているプロファイルに設定されたサーバーのみが利用されます。

●ウイルス検出時のアクション（リアルタイムファイルシステム保護）

ウイルスなどの脅威が検出された場合、既定値ではクライアント用プログラムが自動で駆除または削除を行うように設定されています。ユーザーが毎回対処方法を選択できるようにも変更できます。この場合、ウイルスなどの脅威が検出されると、処理方法を選択する画面が表示されます。

●検査対象からの除外

独自開発されたアプリケーションなどが、ウイルスや疑わしいファイルとして検出される場合があります。安全であると確信できるプログラムがウイルスとして検出された場合、該当ファイルをウイルス検査の対象から除外します。次に、隔離されたファイルを復元します。

ワンポイント

該当ファイルが再び検出されないようにウイルス定義データベースを修正したい場合は、サポートセンターまでお問い合わせください。

● ESET Live Grid（ThreatSense.Net 早期警告システム）

疑わしいファイルが検出された場合、ESET 社への情報提供を促す画面が表示されることがあります。提出に同意すると、そのファイルは ESET 社に送信されます。

■サーバー安定運用のポイント

常に安定した動作を求められるサーバーにクライアント用プログラムを導入する場合は、サーバーの負荷が増加しないようにするなどの工夫を行うことが必要です。

サーバーに導入する場合は、以下のような点を参考にチューニングを行ってください。

●不要な検査の無効化

不要な検査を行わないように設定することで、サーバーの負荷を軽減できます。たとえば、ドキュメントの閲覧や電子メールの閲覧、Web の閲覧などを行わないサーバーでは、これらの検査を行わないように設定することをお勧めします。

無効化する検査の例

- Microsoft Office ドキュメントの検査
- 電子メールのウイルス検査
- Web 閲覧時のウイルス検査

●不要なアプリケーションの検査除外

データベースのウイルス検査を行うと、コンピューターの CPU 使用率が高くなる可能性があります。そのような場合は、データベースなどをウイルス検査対象から除外してください。

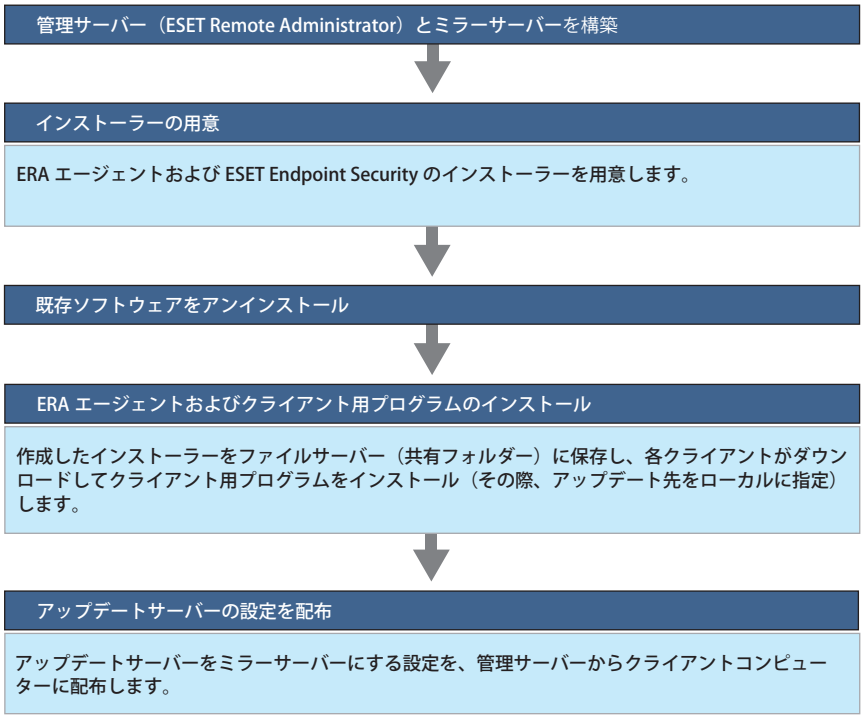
●コンポーネントアップデート時の OS 再起動の無効化

本製品では、プログラムコンポーネントアップデートと呼ばれる、コンピューターの再起動をともなうバージョンアップが行われる場合があります。常時稼働が前提となっているサーバーでは、プログラムのバージョンアップなどによる再起動ができない場合があります。このような環境では、プログラムコンポーネントアップデートが行われた際、OS を自動的に再起動しないように設定します。

1.7 STEP-5 移行作業

作成した移行プランに沿って移行作業を行います。
次が移行の例です。

クライアント用プログラム	ESET Endpoint Security
クライアント数	2,000
ERA サーバー数	1
ミラーサーバー数	1
ミラーの種類	IIS
既存プログラムの削除方法	開発元が提供している削除ツールを利用してアンインストール
参照モデルケース	「■モデルケース 6「ERA サーバーとミラーサーバーを個別に運用（1,000 ～ 5,000 クライアント）」」参照



1.8　バージョンアップによる導入

ESET ライセンス製品の旧バージョンからバージョンアップを行う場合の方法や注意点について説明します。

- **クライアント用プログラムのバージョンアップについて**

Windows 用クライアントプログラムおよび Mac OS X 用クライアントプログラムは、V6 への上書きインストールが可能です。バージョンアップするクライアント用プログラムにユーザ名とパスワードが入力されている場合、自動でアクティベーションが行われます。ユーザ名とパスワードが入力されていない場合、製品認証キーを入力する必要があります。なお、アクティベーションを行うにはインターネット接続が必須となります。
Windows サーバー OS 上にインストールした旧バージョンの ESET NOD32 アンチウイルスから、ESET File Security for Microsoft Windows Server にプログラムを変更する際には、ESET NOD32 アンチウイルスを一旦、アンインストールしてから、インストールする必要があります。
また、Android クライアント用プログラムを V1 から V2 に変更する際には V1 をアンインストールしてからインストールする必要があります。

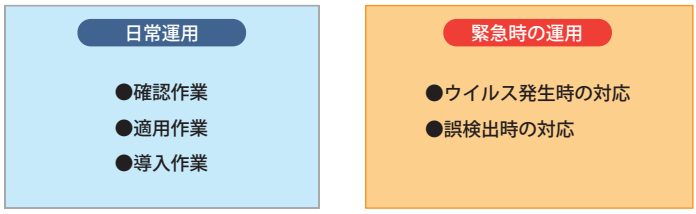
- **管理用プログラムのバージョンアップについて**

V5 から V6 への上書きインストールは行えません。
V6 の管理用サーバーを構築する際には、あらかじめ V5 の管理用サーバーで使用していた各種設定を確認して、V6 の管理用サーバーに設定を実施してください。

Chapter 2 ウイルス対策の運用

2.1　ウイルス対策の運用フェーズ

ウイルス対策には、日常的な運用と緊急時の運用の 2 つのフェーズがあります。



運用フェーズ	概要	参照ページ
日常の運用	ESET ライセンス製品導入後、日頃からクライアントコンピューターの各種ログやウイルス定義データベースのバージョンなどを確認します。	P50 参照
ウイルス検出時（緊急時）の対応	クライアントコンピューターがウイルスに感染した場合、報告から初動対応、詳細調査、防止・抑止策の実施などを行います。	P52 参照
ウイルス誤検出時の対応	Windows や Mac OS X、Linux、Android のシステムファイルやアプリケーションで利用される問題のないファイルを誤ってウイルスと判定する場合があります。その際、隔離ファイルの復元や除外設定などを行います。	P58 参照

! 重　要

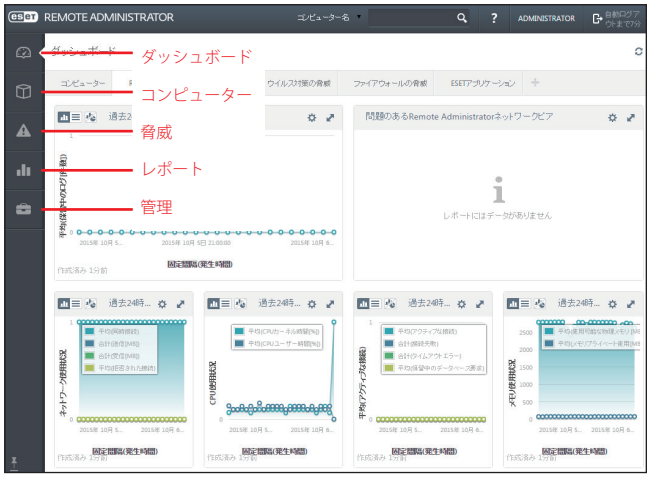
ご利用の製品のバージョンにより、画面の表示が異なります。詳細については、、各製品のマニュアルを参照してください。

2.2 日常の運用

2.2.1 日常運用の実施項目

日常運用の「確認」フェーズでは、ERA Web コンソールからクライアントコンピューターの状態を確認します。
ERA Web コンソールには、次のメニューが用意されています。

- ダッシュボード
- コンピューター
- 脅威
- レポート
- 管理



●ダッシュボード

ダッシュボードには、日常よくチェックする項目を選んで表示しておくことができます。
ダッシュボードを見るだけで、クライアントコンピューターの現在の状況を確認することができます。
ダッシュボードに表示する項目や表示する位置や順番は変更することができます。
初期設定では、「コンピューター」「Remote Administrator サーバー」「ウイルス対策の脅威」「ファイアウォールの脅威」「ESET アプリケーション」が表示されています。

●コンピューター

ESET Remote Administrator で管理しているクライアントコンピューターの状態をチェックしたり、ポリシーを適用したりすることができます。
［詳細］をクリックするとクライアントコンピューターのモデル名や OS のバージョンのほか、ウイルス定義データベースの状況や脅威の有無などが確認できます。

●脅威

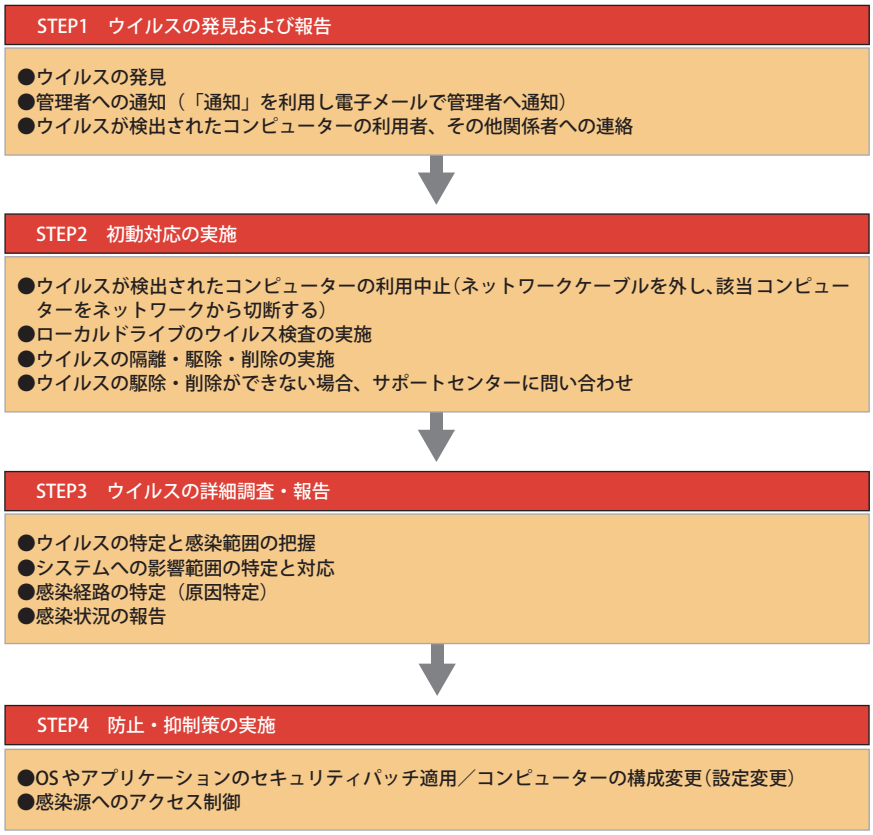
脅威の有無や解決やアクションなどを確認できます。

●レポート

分野ごとに詳細なレポートを生成、編集することができます。
ネットワーク、管理、脅威など 9 分野のレポートが用意されています。
生成したレポートはテキスト形式でエクスポートすることもできます。

2.3 緊急時の運用の流れ

ウイルス感染などの緊急時には、すみやかな対応が必要になります。
クライアントコンピューターからウイルスが検出された場合、次の流れで対応します。



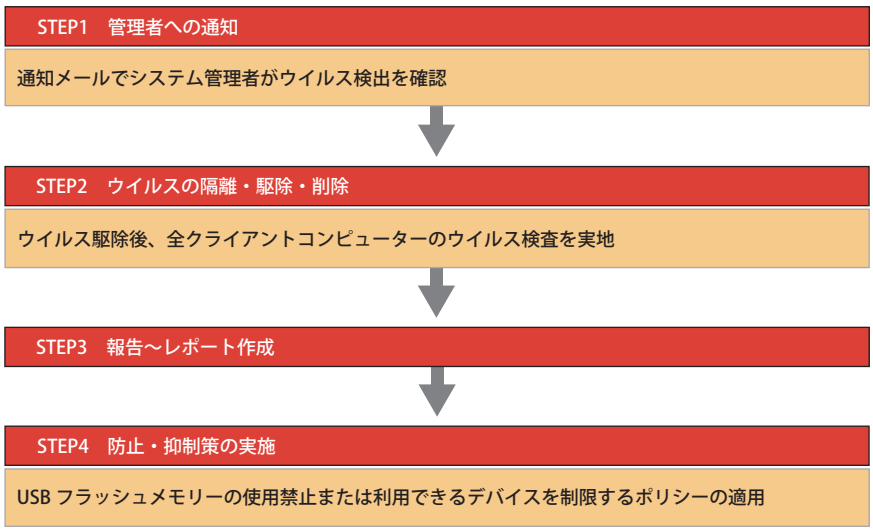
2.4 ウイルス検出時の対応例

2.4.1 対応手順

次の状況でウイルスが検出されたケースについて説明します。

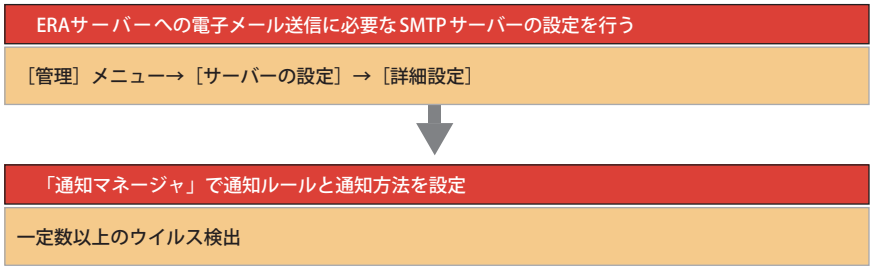
- 複数のクライアントコンピューターでウイルスを検出
- 最新のウイルス定義データベースでウイルスの駆除が可能
- 上層部へウイルスの発生状況の報告が必要
- ユーザーの私物 USB フラッシュメモリーから感染

対応手順



2.4.2 STEP-1 管理者への通知

ウイルスが発見された場合、まず管理者に通知します。
管理者への通知は「通知」を利用します。一定数以上のクライアントコンピューターでウイルスが検出された場合に、電子メールで管理者に通知する設定をします。
各種の警告通知はカスタマイズできるので、日常の運用事項を登録しておくことで安全な運用が実現します。
「通知」で管理者に情報を電子メール通知する場合は、「[管理] メニュー」の「サーバーの設定」内の「SMTP サーバー」で、電子メール送信に利用する SMTP サーバーを設定しておきます。
また、「通知」で「通知ルール」を事前に登録しておきます。
通知機能の詳細については『ESET Remote Administrator ユーザーズマニュアル』を参照してください。



2.4.3 STEP-2 ウイルスの隔離・駆除・削除

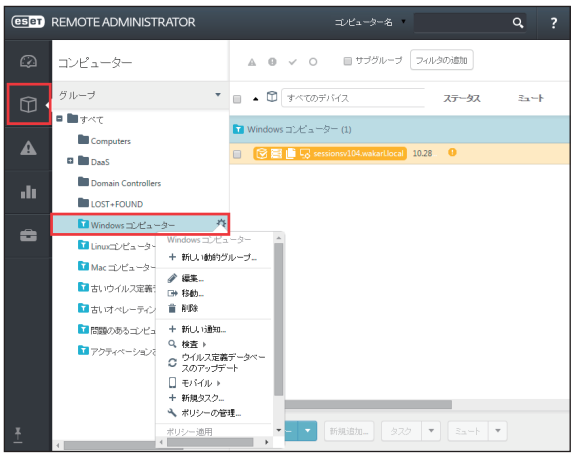
ウイルスの蔓延を防ぐために重要なポイントは、ウイルスの隔離・駆除・削除を実行した後に、再度ウイルス検査を実施して二重三重のチェックを行うことです。再度のウイルス検査を実施することによって、別ウイルスによるさらなる蔓延を防止できます。該当ウイルスを検出していないクライアントコンピューターでもウイルス検査を実施し、安全を確認します。

ウイルス検査を実施する場合は、クライアントコンピューターのローカルディスク全体を検査対象とします。ウイルス検査の実施は、管理者が ESET Remote Administrator からリモート操作で一括して行うこともできます。

■ ESET Remote Administrator によるリモート検査

操作手順

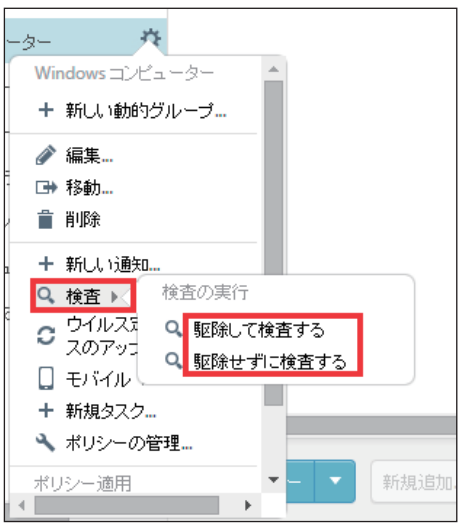
1. ERA Web コンソールにログオンします。
2. [コンピューター] メニューをクリックして、リモート検査を実行するクライアントコンピューター（またはグループ）名横の ⚙ をクリックするか、名前を右クリックします。



ワンポイント

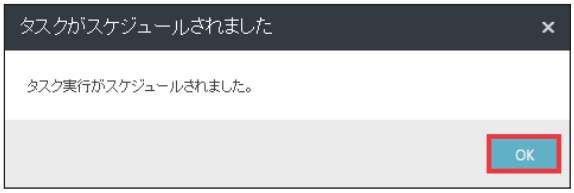
グループを選択すると、そのグループ内すべてのクライアントコンピューターが登録されます。

3. サブメニューで［検査］をクリックして［駆除して検査する］または［駆除せずに検査する］をクリックします。



続く

4 [OK] をクリックします。



2.4.4 STEP-3 報告～レポート作成

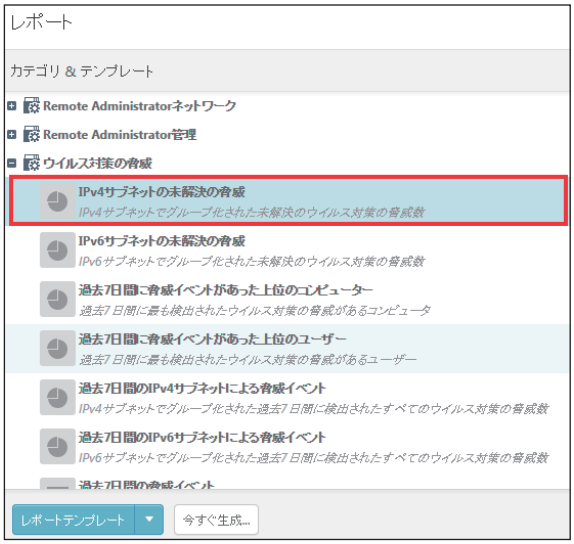
ウイルス検出時と終息時には、レポートを作成します。
クライアントコンピューターのログをもとにレポートを作成することができます。この機能を使うと、ウイルス検出状況の詳細を簡単にレポート化できます。
また、終息時にも同じフォーマットでレポートを作成することで、ウイルス感染から事態の終息までを視覚化できます。

操作手順

1 ERA Web コンソールにログオンします。

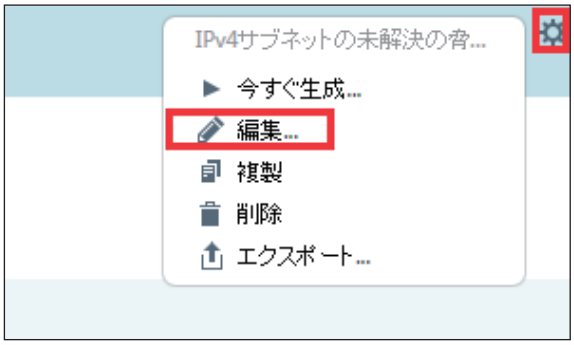
2 [レポート] メニュー>[ウイルス対策の脅威] をクリックします。

3 作成するレポートをクリックします。



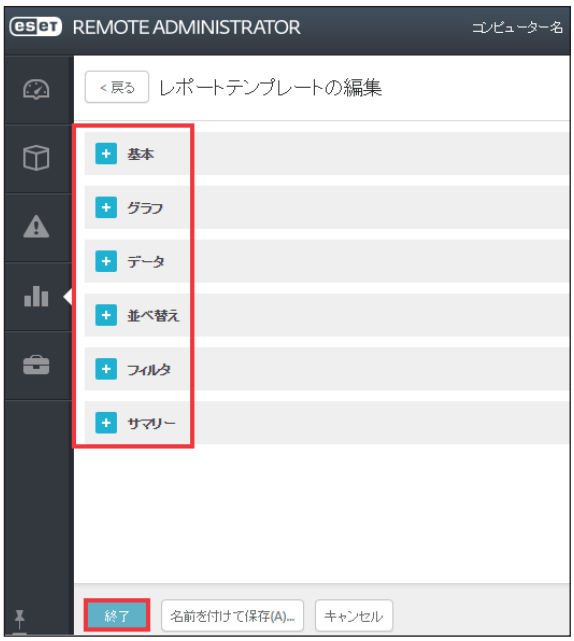
続く

4 レポート名横の ⚙ をクリックして、サブメニューで［編集］をクリックします。



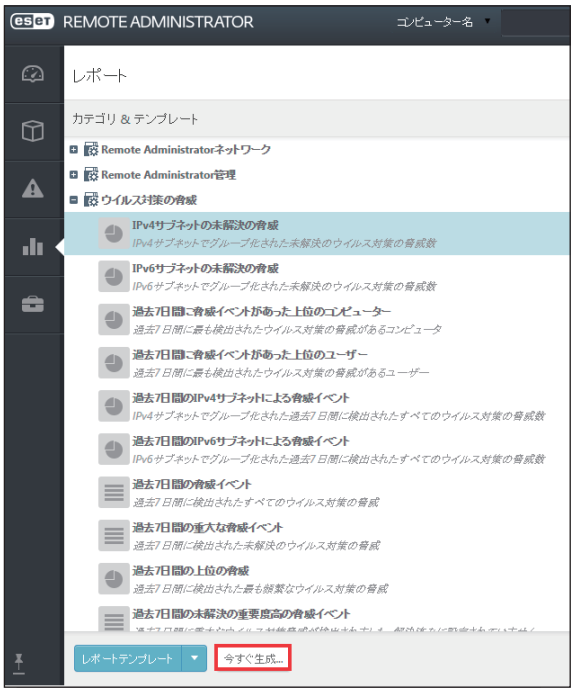
5 レポートの設定をして［終了］をクリックします。

各カテゴリーの［+］をクリックすると、カテゴリーの内容が表示されます。



続く

6 [今すぐ生成] をクリックします。



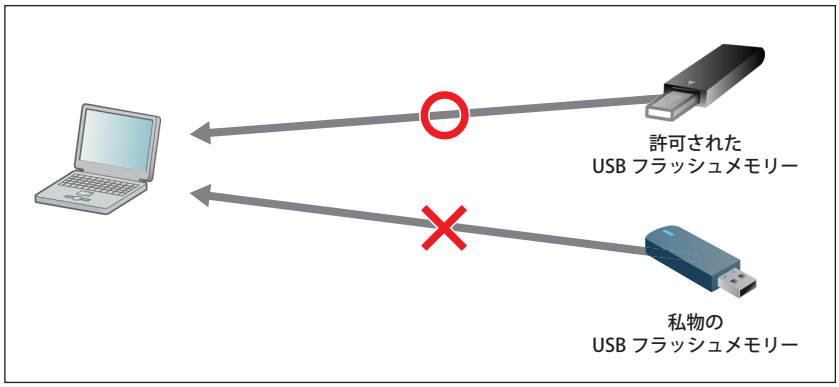
レポートが生成されます。
[保存] をクリックするとレポートを保存することができます。

2.4.5 STEP-4 防止策・抑止策の適用

今回のウイルス検出時の対応例では、USB フラッシュメモリー（外部デバイス）経由でウイルスに感染しました。今後、同様のことが起こらないようにするために、クライアントコンピューターに対して外部デバイス（USB フラッシュメモリー、USB HDD、CD-R、DVD-R など）の利用を禁止するか、利用できるデバイスを制限します。
これは「ポリシーマネージャ」を使って設定します。クライアントコンピューターに外部デバイスの使用禁止ルールまたは利用可能機器を制限するルールを一括配布するか、コンフィグレーションタスクで同様の設定を作成して配布します。
次は、デバイスを制御する場合の運用例です。

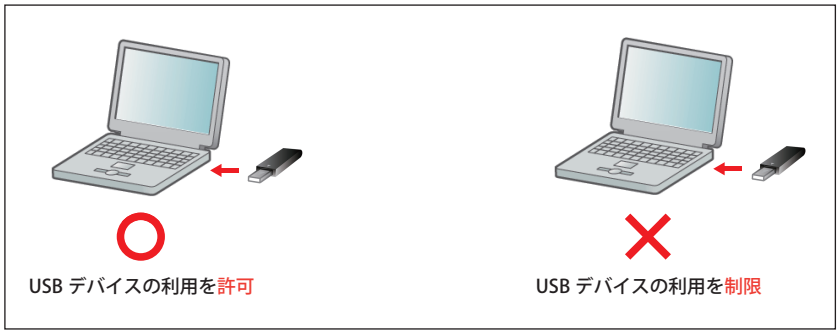
運用例 1 許可されたデバイスのみ利用可能

デバイスコントロール機能を利用すると、クライアントコンピューターで利用できる外部デバイスを指定できます。特定の USB デバイスのみ利用可能にしたり、利用不可に設定することができます。
たとえば、私物の USB フラッシュメモリーを利用不可にし、許可された USB フラッシュメモリーのみを利用可能にすることができます。
この機能は、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET Endpoint Security for OS X、ESET Endpoint アンチウイルス for OS X、ESET File Security for Microsoft Windows Server で設定できます。
※ ESET File Security for Microsoft Windows Server は V6 より使用できます。



運用例 2 特定のクライアントコンピューターにのみ外部デバイスの利用を許可

外部デバイスの利用可／不可をコンピューター単位で制御します。
たとえば、特定のコンピューターのみ USB デバイスの利用を許可し、その他のコンピューターについては利用を制限することができます。



2.5　ウイルス誤検出時の対応

クライアント用プログラムが問題のないファイルをウイルスとして検出してしまった場合の対処法について説明します。

2.5.1　誤検出時の対応手順

誤検出の判定

●弊社 HP にて、該当ファイルの検出情報があるかを確認（https://eset-info.canon-its.jp/info/virusinfo/）
●サポートセンターに誤検出判定問い合わせ、および対応方法を確認

↓

復旧作業の実施

●誤検出であれば、隔離された該当ファイルを復旧

↓

防止策の実施

●クライアント用プログラムでの対象ファイル／フォルダーの除外設定（推奨）
　※フォルダー、拡張子、アプリケーション単位での除外設定
　※ ESET Remote Administrator を利用した、クライアントコンピューターへの一括設定
●最新のウイルス定義データベースへのアップデート（推奨）
● ESET セキュリティ製品の検査機能の設定変更（上記対応ができない場合）

2.5.2　隔離されたファイルの復元 ＜ Windows 版クライアントコンピューターの場合＞

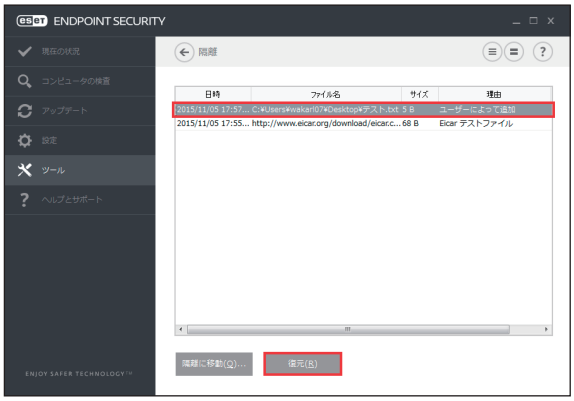
ESET Endpoint Security または ESET Endpoint アンチウイルスでウイルスとして検出され隔離されたファイルの復元手順を説明します。

操作手順

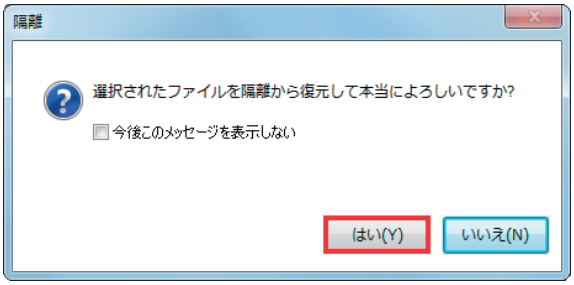
1. クライアント用プログラムのメイン画面を開きます。
2. ［ツール］＞［隔離］をクリックします。

続く

3 復元するファイルを選択して［復元］をクリックします。



4 確認画面で［はい］ボタンをクリックします。



2.5.3 隔離されたファイルの復元 ＜Mac OS X 版クライアントコンピューターの場合＞

ESET Endpoint Security for OS X または ESET Endpoint アンチウイルス for OS X でウイルスとして検出され、隔離されたファイルの復元手順を説明します。

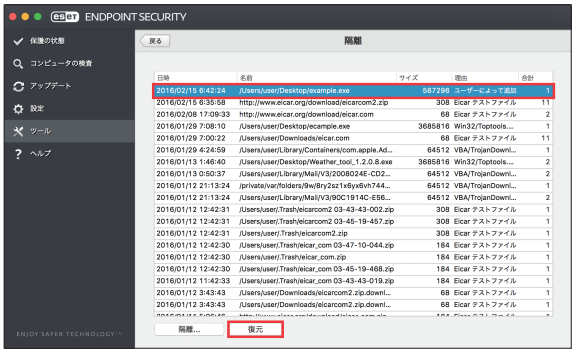
操作手順

1 クライアント用プログラムのメイン画面を開きます。

2 ［ツール］＞［隔離］をクリックします。

続く

3 復元するファイルを選択して［復元］をクリックします。



4 確認画面で［復元］ボタンをクリックします。

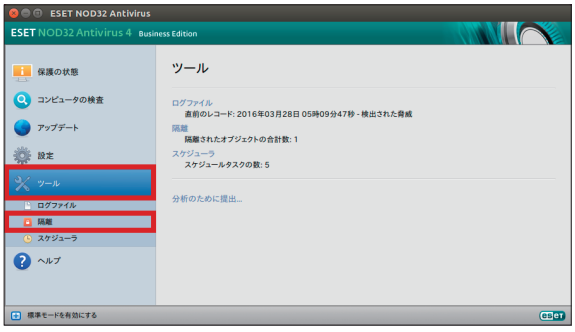
2.5.4 隔離されたファイルの復元 ＜Linux 版 クライアントコンピューターの場合＞

ESET NOD32 アンチウイルス for Linux Desktop でウイルスとして検出され、隔離されたファイルの復元手順を説明します。

操作手順

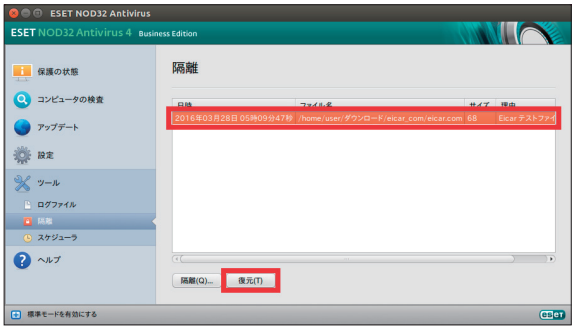
1 クライアント用プログラムのメイン画面を開きます。

2 ［ツール］＞［隔離］をクリックします。



続く

3 復元するファイルを選択して［復元］をクリックします。



4 確認画面で［はい］をクリックします。

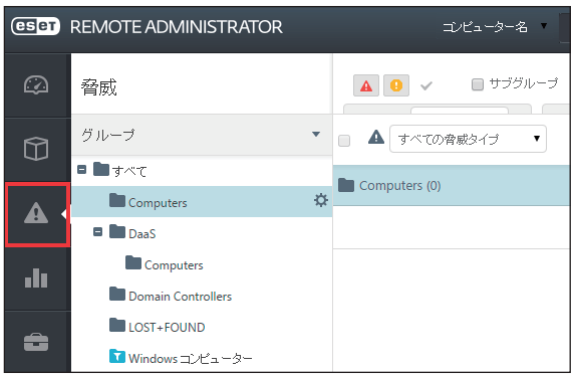
2.5.5 隔離されたファイルの復元 < ERA サーバーの場合>

ERA サーバーからリモート操作で、クライアントコンピューターの隔離されたファイルを復元します。

操作手順

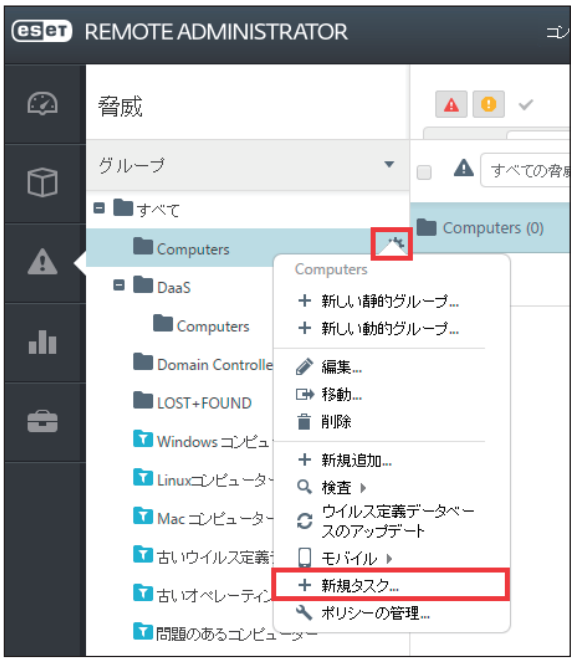
1 ERA Web コンソールにログオンします。

2 ［脅威］メニューをクリックします。



続く

3 対象となるコンピューターまたはグループをクリックして、横にある⚙をクリックしてサブメニューから［新規タスク］を選択します。



4 タスクの名前を入力して、「タスク分類」で［ESET セキュリティ製品］、「タスク」で［隔離管理］を選択します。

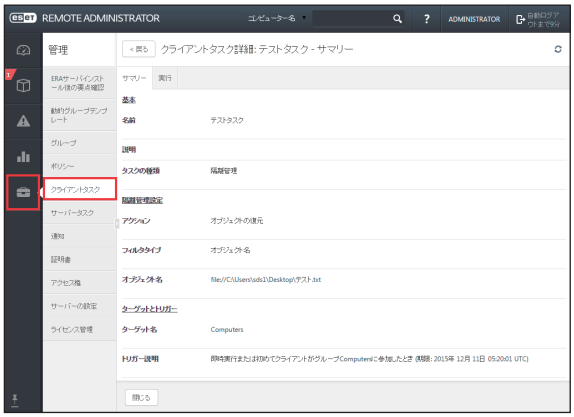
続く

5 「設定」の［+］をクリックして、「アクション」で［オブジェクトの復元］、「ファイルタイプ」で［オブジェクト名］、「オブジェクト名」で復元するオブジェクトを設定します。

最後に［終了］をクリックします。

6 タスクが実行されます。

タスクの確認は［管理］メニュー>［クライアントタスク］で該当のタスクをクリックしてサブメニューから［詳細］を選択します。タスクの情報や実行状況を確認できます。



2.5.6 ファイルをウイルス検査対象から除外 < Windows 版クライアントコンピューターの場合>

ウイルスとして検出されたファイルを、ウイルス検査の対象から除外します。除外設定を行ったファイルはウイルス検査の対象から外されるので、間違って削除や隔離などが行われることはありません。

ESET Endpoint Security または ESET Endpoint アンチウイルスでの除外設定について説明します。

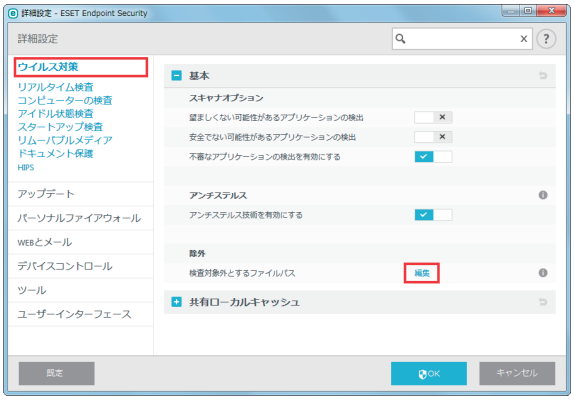
操作手順

1 ESET Endpoint Security または ESET Endpoint アンチウイルスのメイン画面を開きます。

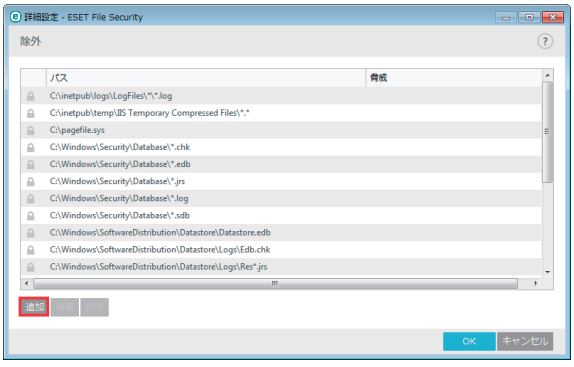
続く

2 ［設定］＞［詳細設定］をクリックします。

3 ［ウイルス対策］をクリックします。続いて、「除外」＞「検査対象外とするファイルパス」の［編集］をクリックします。

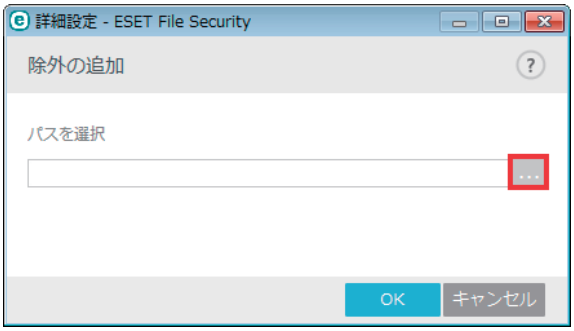


4 「除外」画面で［追加］をクリックします。

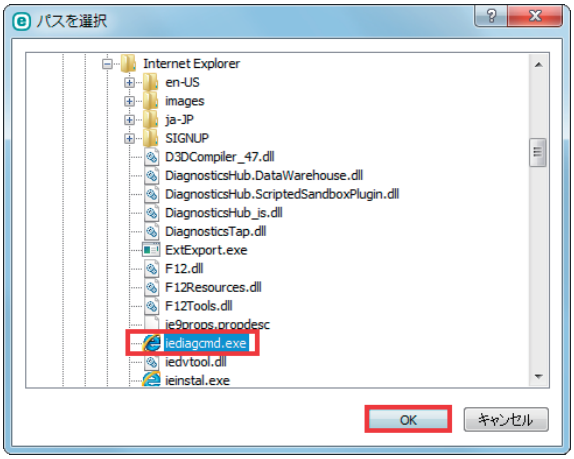


続く

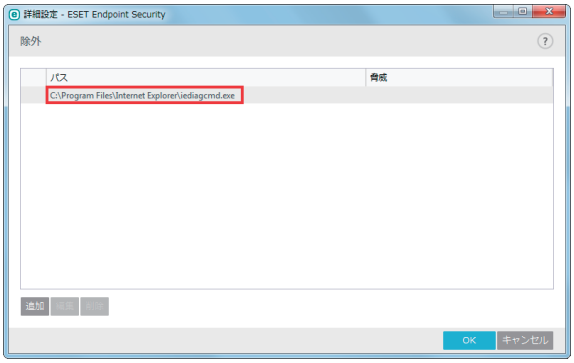
5 「除外の追加」画面で［…］をクリックします。



6 除外するファイルを選択して［OK］ボタンをクリックします。



選択したファイルが除外リストに登録されます。



ワンポイント

除外リストには、フォルダーやファイルの拡張子も登録できます。フォルダーを除外するときは、手順 5 でフォルダーを選択して［OK］ボタンをクリックします。または、［除外］欄に除外するフォルダーのフルパスを入力して［OK］ボタンをクリックします。
拡張子で除外する場合は、［除外］欄に「c:¥test¥*.doc」の形式で拡張子を指定します。

2.5.7　ファイルをウイルス検査対象から除外 ＜Mac OS X 版クライアントコンピューターの場合＞

ウイルスとして検出されたファイルを、ウイルス検査の対象から除外します。除外設定を行ったファイルはウイルス検査の対象から外されるので、間違って削除や隔離などが行われることはありません。
ESET Endpoint Security for OS X または ESET Endpoint アンチウイルス for OS X での除外設定について説明します。

操作手順

1. ESET Endpoint Security for OS X または ESET Endpoint アンチウイルス for OS X のメイン画面を開きます。
2. ［設定］＞［詳細設定を表示する］をクリックします。

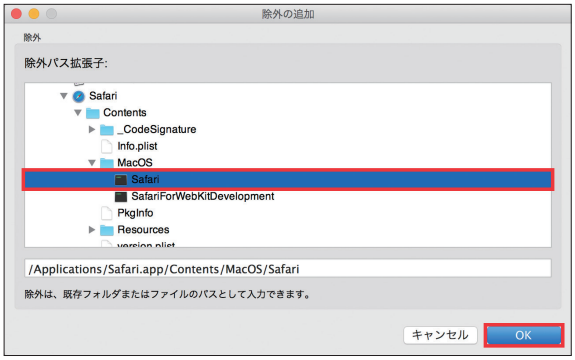
3. ［一般］をクリックします。

4. 除外の［設定］をクリックします。

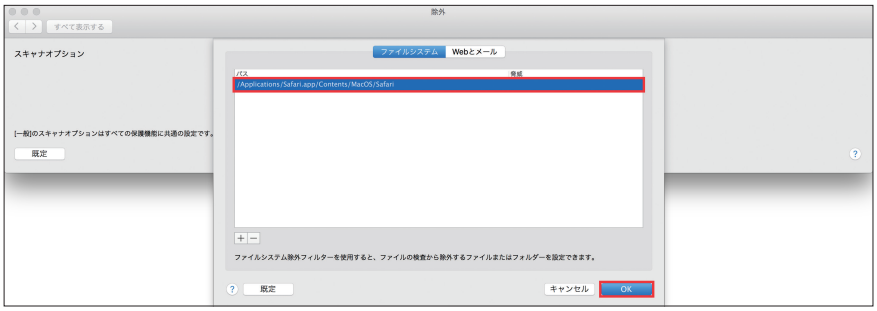
続く

5 ［+］をクリックします。

6 除外するファイルを選択して［OK］ボタンをクリックします。



7 選択したファイルが除外リストに登録されます。［OK］ボタンをクリックします。



ワンポイント

除外リストには、フォルダーやファイルの拡張子も登録できます。フォルダーを除外するときは、手順 6 でフォルダーを選択して［OK］ボタンをクリックします。または、フォルダーツリー下のフォルダーの入力欄に除外するフォルダーのフルパスを入力して［OK］ボタンをクリックします。拡張子で除外する場合は、入力欄に「/tmp/est/*.doc」の形式で拡張子を指定します。

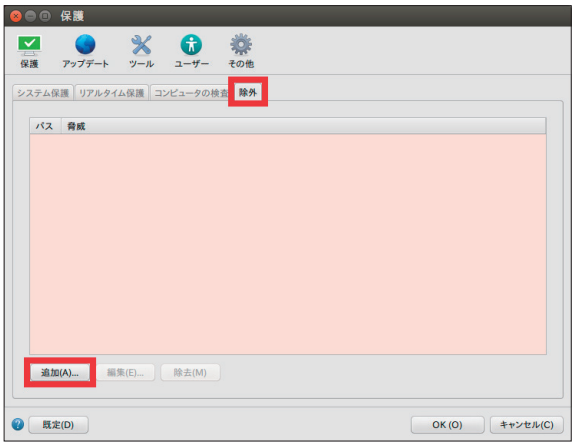
2.5.8 ファイルをウイルス検査対象から除外 <Linux 版クライアントコンピューターの場合>

ウイルスとして検出されたファイルを、ウイルス検査の対象から除外します。除外設定を行ったファイルはウイルス検査の対象から外されるので、間違って削除や隔離などが行われることはありません。ESET NOD32 アンチウイルス for Linux Desktop での除外設定について説明します。

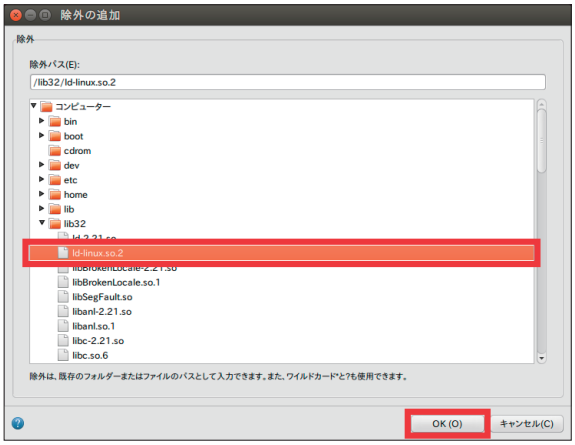
操作手順

1. クライアント用プログラムのメイン画面を開きます。
2. [設定] > [詳細設定を表示する] をクリックします。

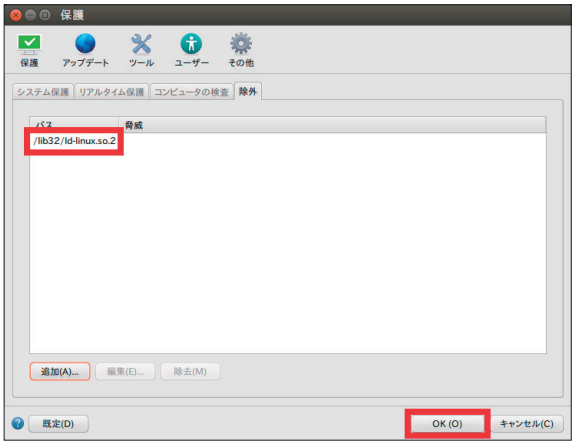
3. [除外] をクリックし、[追加] ボタンをクリックします。



4. 除外するファイルを選択して [OK] ボタンをクリックします。



5 選択したファイルが除外リストに登録されます。［OK］ボタンをクリックします。



ワンポイント

除外リストには、フォルダーやファイルの拡張子も登録できます。フォルダーを除外するときは、手順 4 でフォルダーを選択して［OK］ボタンをクリックするか、「除外パス」の入力欄に除外するフォルダーのフルパスを入力して［OK］ボタンをクリックします。拡張子で除外する場合は、入力欄に「/tmp/est/*.doc」の形式で拡張子を指定します。

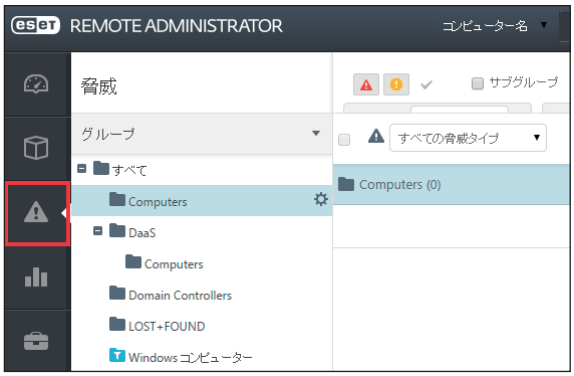
2.5.9 ファイルをウイルス検査対象から除外 ＜ERA サーバーの場合＞

ERA サーバー（ESET Remote Administrator）で、ウイルスとして検出されたファイルの除外設定をします。

操作手順

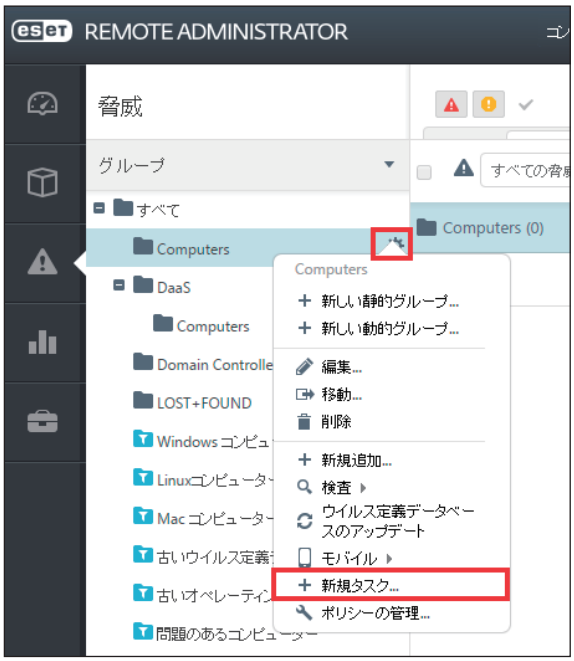
1 ERA Web コンソールにログオンします。

2 ［脅威］メニューをクリックします。



続く

3 対象となるグループをクリックして、横にある ⚙ をクリックしてサブメニューから［新規タスク］を選択します。



4 タスクの名前を入力して、「タスク分類」で［ESET セキュリティ製品］、「タスク」で［隔離管理］を選択します。

［ターゲット］でコンピューター名を選択すると、特定のコンピューターを対象にすることもできます。

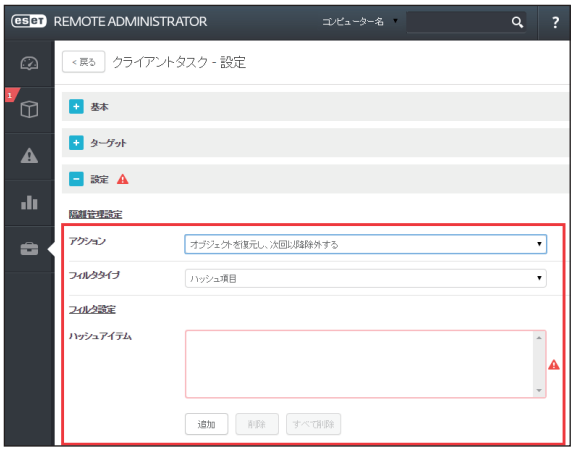
続く

5 「設定」の［＋］をクリックして、「アクション」で［オブジェクトを復元し、次回以降除外する］を選択します。

「フィルタタイプ」で条件を選択し、「フィルタ設定」でフィルター条件を設定します。

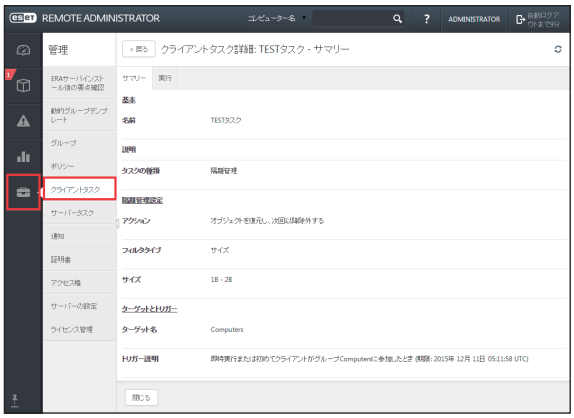
ハッシュ項目	ハッシュアイテムへのハッシュ項目の追加は、既存の隔離情報からだけ追加できます。
発生	オブジェクトが隔離された時間範囲を指定します。
サイズ	隔離オブジェクトのサイズ範囲（バイト単位）で指定します。
ウイルス名	隔離項目リストからウイルスを選択します。
オブジェクト名	隔離項目リストからオブジェクトを選択します。

最後に［終了］をクリックします。



6 タスクが実行されます。

タスクの確認は［管理］メニュー>［クライアントタスク］で該当のタスクをクリックしてサブメニューから［詳細］を選択します。タスクの情報や実行の状況を確認できます。



! 重 要

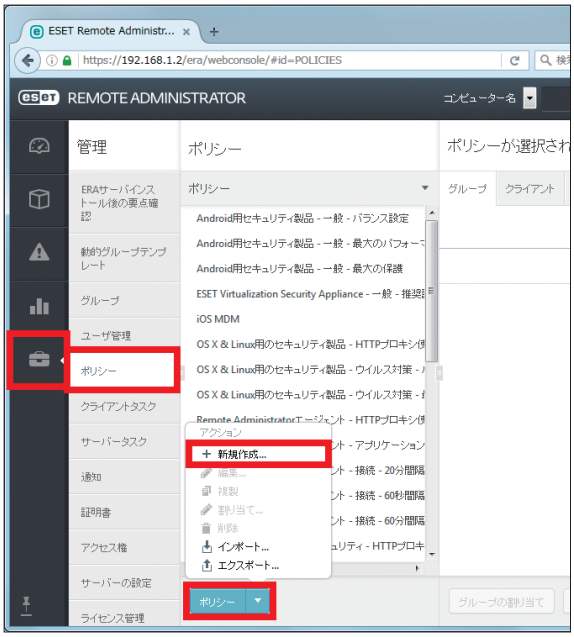
このアクションはヒューリスティック機能で検出された未知のウイルスの場合にのみ有効です。

2.5.10 ファイルをウイルス検査対象から除外 < Android デバイスの場合>

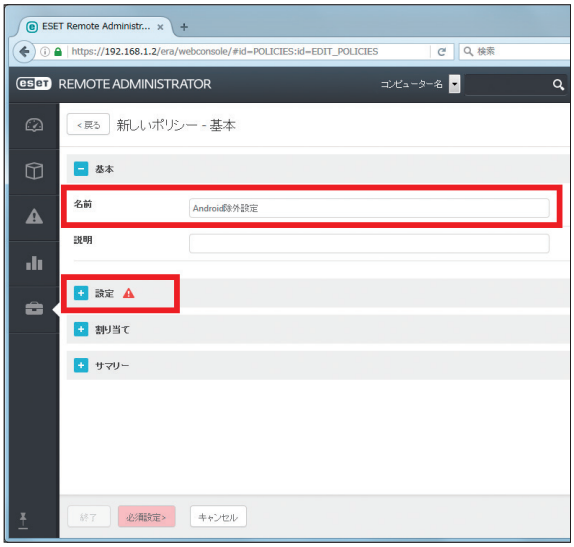
ウイルスとして検出されたファイルを、ウイルス検査の対象から除外します。除外設定を行ったファイルはウイルス検査の対象から外されるので、間違って削除や隔離などが行われることはありません。ESET Endpoint Security for Android では、ERA サーバー（ESET Remote Administrator）で、ウイルスとして検出されたファイルの除外設定のポリシーを作成します。

操作手順

1. ERA Web コンソールにログオンします。
2. ［管理］>［ポリシー］タブ>［ポリシー］>［新規作成］とクリックします。

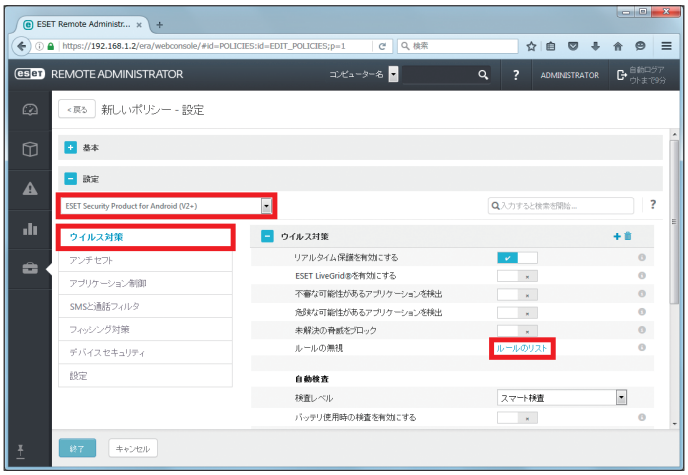


3. 必要に応じて作成するポリシーの名前を入力し、説明を入力します。［設定］をクリックします。



続く

4 ドロップダウンリストから［ESET Security Product for Android（V2+）］を選択します。［ウイルス対策］をクリックし、［ルールのリスト］をクリックします。



5 「ルールの追加」画面が表示されます。［追加］をクリックします。

6 カテゴリを選択し、［ファイル名］または［パッケージ名］を入力します。脅威名を入力し、［追加］をクリックします。

ワンポイント

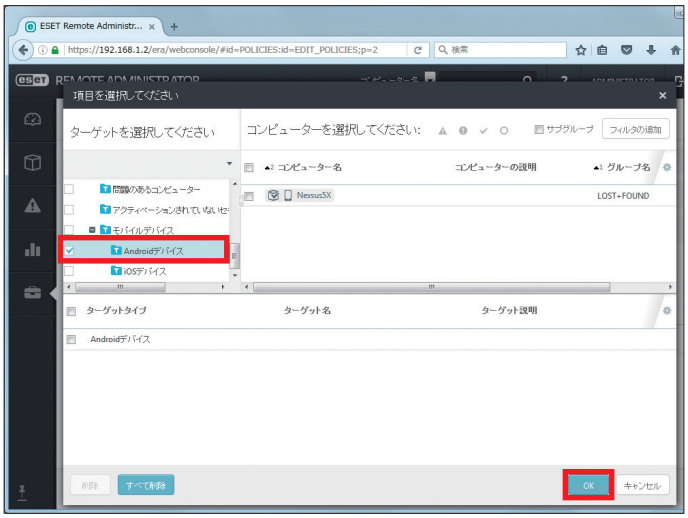
カテゴリは、［ファイル名］または［アプリケーション名］の中から選択できます。また、［ファイル名］を選択した場合は、「ファイル名」と「脅威名」を入力します。［アプリケーション］を選択した場合は、「パッケージ名」と「脅威名」を入力します。

続く

7 ルールが追加されます。［保存］をクリックします。

8 ［割り当て］＞［割り当て ...］とクリックします。

9 作成するポリシーを割り当てる Android デバイスを選択し、［OK］をクリックします。

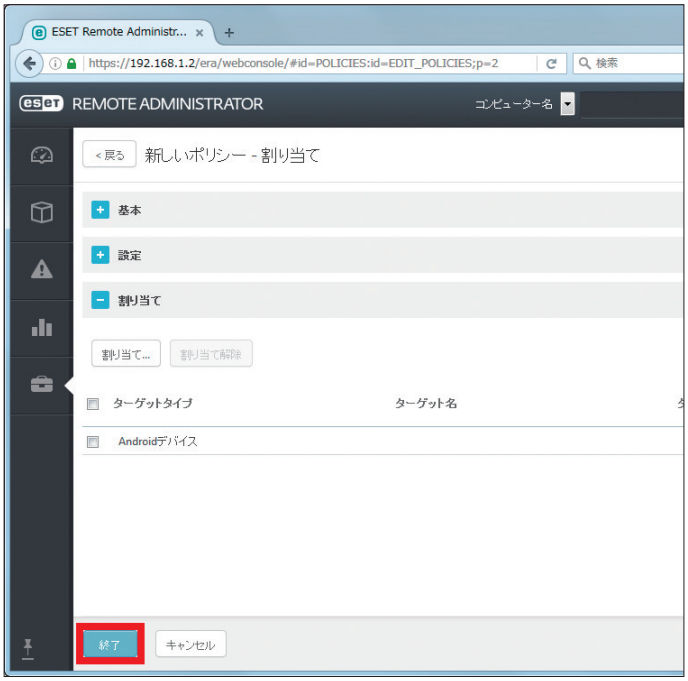


ワンポイント

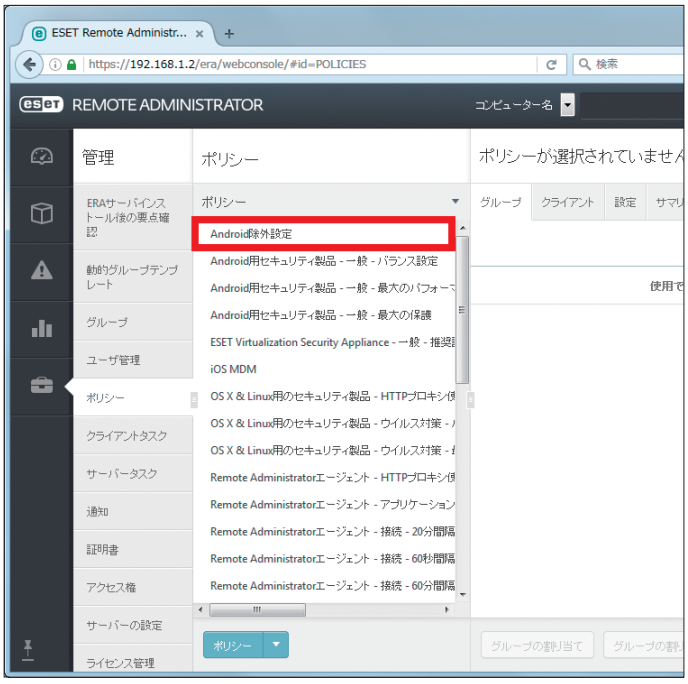
すべての Android デバイスに対して作成中のルールを適用するときは、「Android デバイス」のチェックをオンにします。

続く

⑩ [終了] をクリックします。



⑪ 作成したルールが登録されます。



Chapter 3 FAQ〈よくある質問／お問い合わせの際に〉

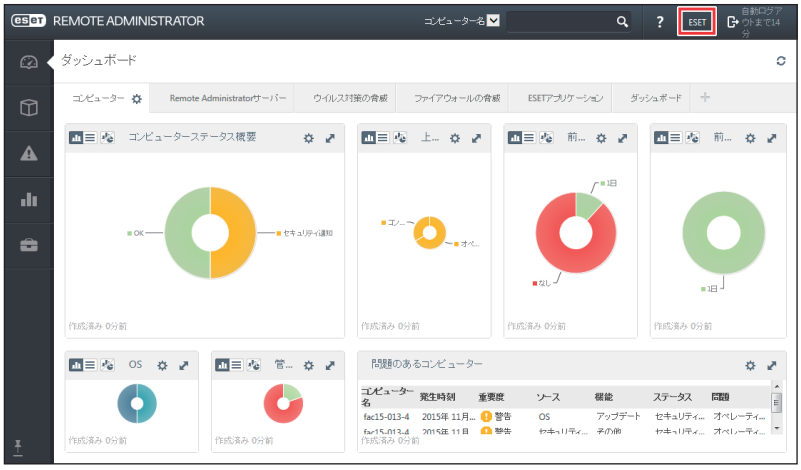
3.1 よくある質問一覧

Q1 ERA Web コンソール上での時間表示を変更するには？

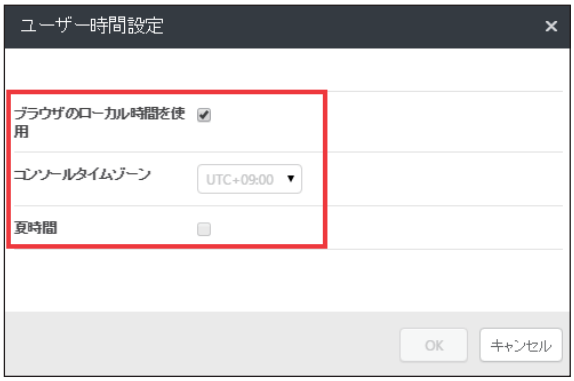
ERA Web コンソールで使用するタイムゾーンなど時間表示の設定を変更することができます。

操作手順

1. ERA Web コンソールにログオンします。
2. ユーザー名をクリックします。



3. 「ユーザー時間設定」画面で使用するタイムゾーンなどを設定します。



Q2 クライアントコンピューターの設定を ERA サーバーからリモートで変更するには？

クライアントコンピューターの設定を ERA サーバーからリモートで変更するには、設定を変更するクライアントコンピューターに対してポリシーを設定して割り当てます。

ワンポイント

詳細は『ESET Remote Administrator ユーザーズマニュアル』の「6.4　ポリシー」を参照してください。

Q3　クライアントコンピューターにアップデートを実行させるには？

クライアントコンピューターにアップデートを実行させるには、ERA サーバーからクライアントコンピューターに対して「ウイルス定義データベース更新」タスクを割り当てます。

ワンポイント

詳細は『ESET Remote Administrator ユーザーズマニュアル』の「6.5　クライアントタスク」を参照してください。

Q4　クライアントコンピューターにコンピューターの検査を実行させるには？

クライアントコンピューターにコンピューターの検査を実行させるには、ERA サーバーからクライアントコンピューターに対して「オンデマンド検査」タスクを割り当てます。

ワンポイント

詳細は『ESET Remote Administrator ユーザーズマニュアル』の「6.5　クライアントタスク」を参照してください。

Q5　ERA サーバーのパスワードを変更するには？

ERA サーバーのパスワードは、［管理］＞［アクセス権］＞［ユーザー］＞<変更するユーザー名>をクリックして、［編集］を選択して変更します。

ワンポイント

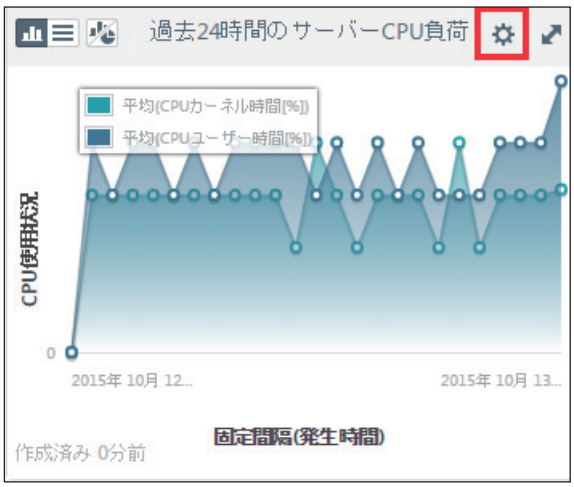
詳細は『ESET Remote Administrator ユーザーズマニュアル』の「6.9　アクセス権」を参照してください。

Q6　表示されるアイテムのフィルタリングを行うには？

ダッシュボードのアイテムに表示されるデータをフィルタリングすることができます。

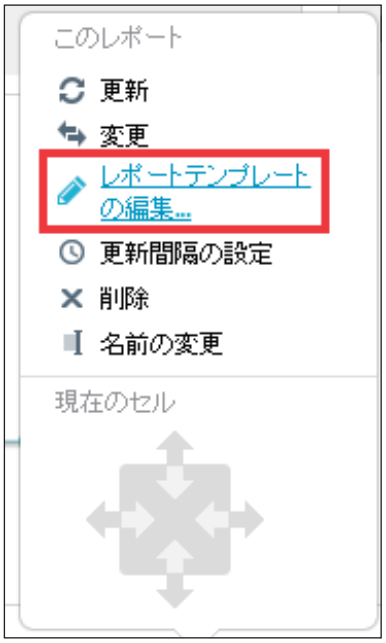
操作手順

1 ダッシュボードのタイトルバーに表示される  をクリックします。

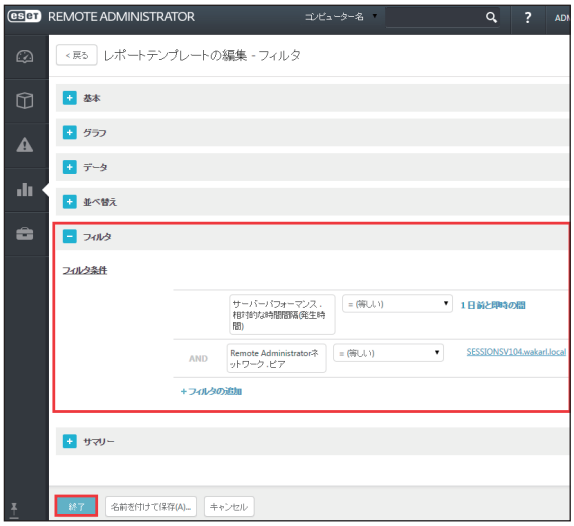


続く

❷［レポートテンプレートの編集］をクリックします。



❸「フィルタ」の［+］をクリックしてフィルタリング条件を指定して［終了］をクリックします。



Q7 RD Sensor が一部のコンピューターを検出しないのですが？

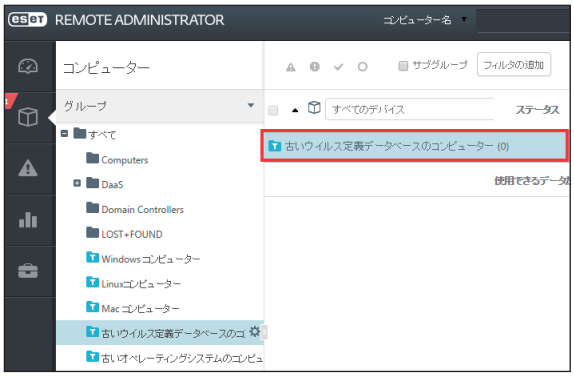
RD Sensor はネットワーク上の通信をリスニングしてコンピューターを検出します。従って、コンピューターが通信していない場合、RD Sensor では検出されません。
DNS 設定をチェックし、DNS ルックアップの問題が通信を妨げていないことを確認してください。

Q8 ウイルス定義データベースが最新でないクライアントコンピューターを表示するには？

ウイルス定義データベースが最新でないクライアントコンピューターを表示することができます。

操作手順

1. ERA Web コンソールにログオンします。
2. ［コンピューター］メニューをクリックします。
3. ［古いウイルス定義データベースのコンピューター］をクリックします。

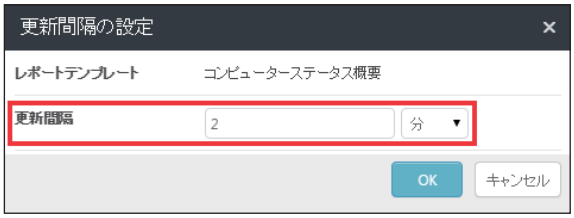


Q9 画面表示の更新間隔を変更するには？

次の操作で画面表示の更新間隔を変更します。

操作手順

1. ERA Web コンソールにログオンします。
2. 「ダッシュボード」画面で、更新間隔を変更するアイテムのタイトルバーにある ⚙ をクリックして［更新間隔の設定］をクリックします。
3. 「更新間隔の設定」画面で設定する秒数を指定します。



Q10 コマンドラインオプションとは？

Windows 用プログラムのインストールパッケージでは、作成の際に様々なコマンドラインオプションを使用できます。詳細は『ESET Remote Administrator ユーザーズマニュアル』の「4.2.3.2　コマンド入力からの製品インストール」を参照してください。

Q11 「コンピューター」メニューで検出されないコンピューターがあります

コンピューターの検出は、NetBIOS を利用して実行されます。
「コンピューター」メニューで検出するコンピューターに、Windows がファイル共有時に利用する「Microsoft ネットワーク用ファイルとプリンター共有」や「Microsoft ネットワーク用クライアント」などの機能がインストールされていることを確認してください。

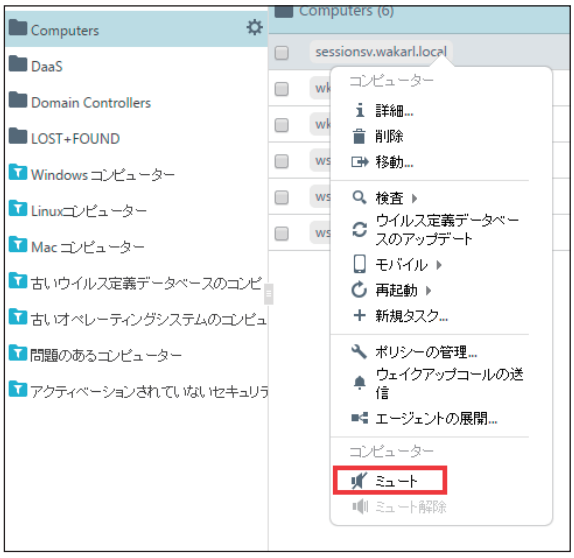
Q12 クライアントコンピューターからの報告を停止するには？

ミュート機能を使用すると、ERA エージェントはクライアントコンピューターの情報報告を停止します。
ミュート中の ERA エージェントは、情報の収集だけを行います。
ミュート解除を選択すると ERA エージェントは通信を回復します。

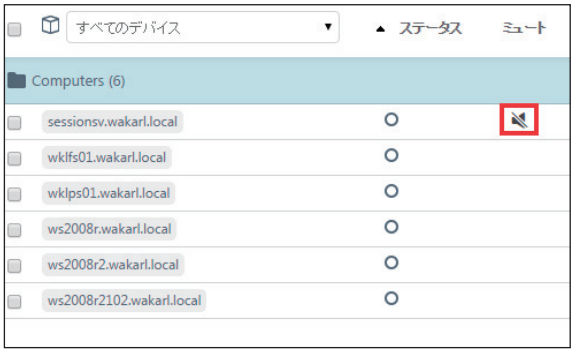
次の操作で ERA エージェントをミュートします。

操作手順

1. ERA Web コンソールにログオンします。
2. 「コンピューター」メニューで、ミュートを設定するコンピューター名をクリックします。
3. ［ミュート］をクリックします。



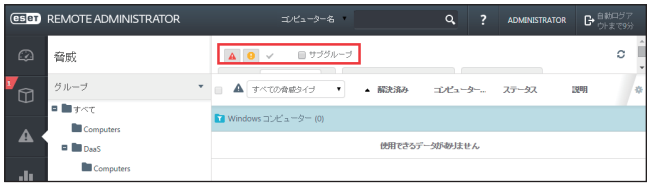
ミュート欄に消音アイコンが表示されます。

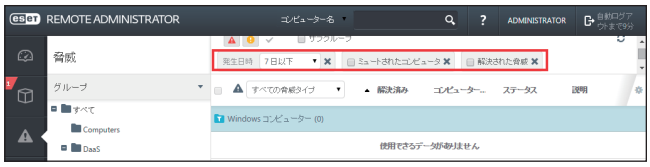


ミュートを解除する場合は、コンピューター名をクリックして［ミュート解除］をクリックします。

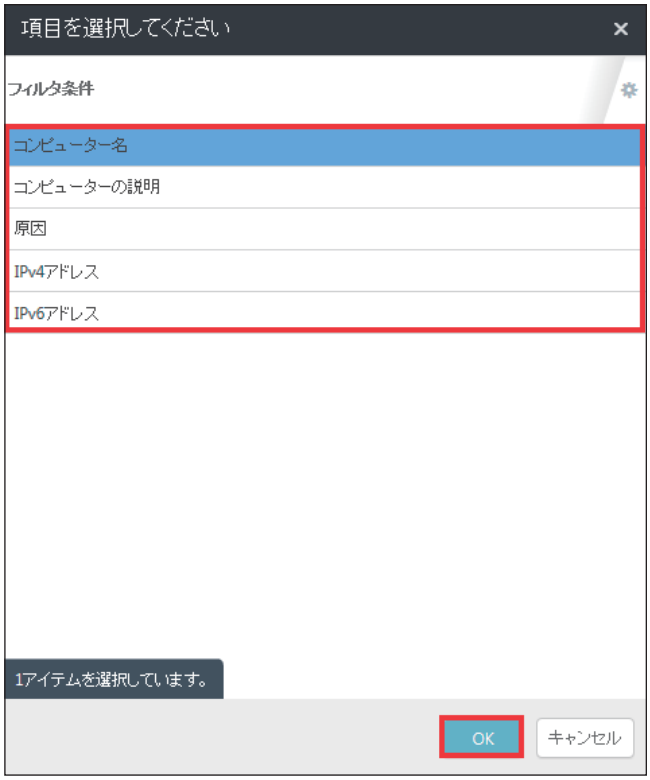
Q13 発生した脅威をフィルタリングするには？

「脅威」メニューで発生した脅威をフィルタリングすることができます。
画面上部のフィルター領域で適用するフィルターを選択したり設定したりします。
既定では、「エラー」「警告」「サブグループ」「発生日時」「ミュートされたコンピュータ」「解決された脅威」などのフィルターが設定されています。
フィルターをチェックしたり値を設定するとフィルタリングが実行されます。





［フィルタの追加］をクリックすると、他のフィルターを追加することができます。
追加するフィルター条件を選択して［OK］をクリックします。
選択したフィルターがフィルター領域に表示されて使用できるようになります。



Q14 タスクがなかなか配布されません

クライアントコンピューターに発行したタスクは、クライアントコンピューターが ERA サーバーに接続した際に配布されます。
クライアントコンピューターが ERA サーバーに接続するまで、タスクは配布されません。
ウェイクアップコール機能を使用すると、すぐにタスクが実行されます。

Q15 初めて ERA サーバーに接続する時のパスワードは何ですか？

ESET Remote Administrator インストール時にパスワードを設定しています。
パスワードがご不明の場合は管理者にお問い合わせください。

Q16 ERA サーバー、ERA Web コンソールはインストール台数に制限がありますか？

制限はありません。必要な台数分インストールすることができます。

Q17 ERA サーバーで使用するポート番号は？

「1.4.1　ERA サーバーの検討」の「●ファイアウォールの設定」で「サーバーが使用するポート」の表を参照してください。

Q18 ウイルス定義データベースを USB フラッシュメモリーや CD-R で配布するには？

ウイルス定義データベースを USB フラッシュメモリーや CD-R を使ってクライアントコンピューターに配布するには、以下の 2 通りの方法があります。
①ユーザーズサイトからダウンロードしたファイルを使用
②ミラーサーバーに保存されたファイルを使用

！重　要

USB フラッシュメモリーや CD-R によるアップデートができるのは、Windows 用のセキュリティプログラムのみです。ESET File Security for Linux は対応していません。

■ユーザーズサイトからダウンロードしたファイルを使用

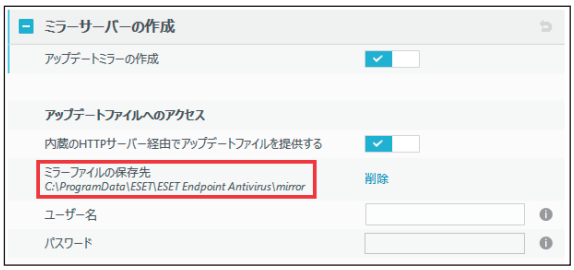
弊社ユーザーズサイトからダウンロードしたウイルス定義データベースファイルを、USB フラッシュメモリーや CD-R に書き込んで使用します。ダウンロード方法と利用手順は、ユーザーズサイトにある『オフライン更新手順書』を参照してください。

■ミラーサーバーに保存されたファイルを使用

ミラーサーバーに保存されたファイルを USB フラッシュメモリーや CD-R に書き込んで使用します。
ミラーサーバーの構築手順は、各プログラムのユーザーズマニュアルを参照してください。

操作手順

1. ウイルス定義データベースをアップデートします。
   ウイルス定義データベースのアップデート方法は、各プログラムのユーザーズマニュアルを参照してください。
2. ウイルス定義データベースが保存されているフォルダーを USB フラッシュメモリーや CD-R などに書き込みます。
   既定値では、ミラーサーバー構築時に指定した「ミラーファイルの保存先」フォルダーに保存されます。



■クライアントコンピューター側の設定

操作手順

1. クライアント用プログラムのメイン画面を開き、［設定］＞［詳細設定］を選択して「詳細設定」画面を開きます。
2. ［アップデート］をクリックします。
3. ［マイプロファイル］＞［基本］をクリックします。

続く

4 ［自動選択］をオフにして［アップデートサーバー］にアップデートファイルのある場所を入力します。
ミラーサーバーの場合は「https:// <コンピューター名または IP アドレス> :2221」、ローカルのフォルダーなどの場合は「D:¥mirror」のように指定します。

Q19 起動時に表示されるスプラッシュ画面を非表示にするには？

次の手順でスプラッシュ画面を非表示にできます。

操作手順

1 クライアント用プログラムのメイン画面を開き、［設定］＞［詳細設定］をクリックします。

2 ［ユーザーインターフェース］をクリックし、［ユーザーインターフェース要素］で［起動時にスプラッシュ画面を表示する］をオフにします。

3 ［OK］ボタンをクリックします。

Q20 Mac OS X でコンピューターの検査に時間がかかる

起動ディスク以外にマウントされているディスクなどを検査の対象にすると、検査対象数が多くなり、検査に時間がかかります。検査時間を短縮したい場合は、「カスタム」検査の検査対象から「/Volumes」下のネットワークドライブ、Time Machine のバックアップ先などを除外して検査を行ってください。

Q21 オフライン環境で使用するには？

V6 のクライアント用プログラムを使用する際には、アクティベーション（認証）作業が必要となります。アクティベーションにはインターネット接続が必要となります。
インターネット接続が行えないオフライン環境のコンピューターにクライアント用プログラムをインストールするときは、クライアント用プログラムのインストールを行った後に「オフラインライセンスファイル」を利用して製品のアクティベーションを行うことが可能です。
詳細は「1.6.7　オフライン環境に導入する」をご参照ください。

3.2 お問い合わせ用ファイルの取得

弊社では、お客さまからのお問い合わせの際、サポート対応を迅速にするために以下のファイルなどの取得をお願いすることがあります。

■取得をお願いする情報の例＜ Windows の場合＞

取得情報	含まれている情報	取得する目的	参照ページ
環境設定ファイル（ESET SysInspector）	端末にインストールされているアプリケーションや、読み込まれているドライバーの情報、レジストリ情報などが含まれています。	不具合が発生するアプリケーションの有無などを確認するために取得します。また、レジストリ情報からウイルスの有無などを確認するために取得します。	P87 参照
Windows のシステム情報	端末にインストールされているアプリケーションやサービスの情報、コンピューター機器の情報などが含まれています。	ネットワークドライバーの詳細なバージョンや、Windows のエラー報告などを確認するために取得します。	P89 参照
ESET 製品の設定ファイル	端末にインストールされている ESET 製品の設定内容が含まれています。	不具合の原因となる誤った設定の有無などを確認するために取得します。	P93 参照
スクリーンショット	ディスプレイ上に表示されている、画面のみの情報です。	実際に表示されたエラー画面などを確認するために取得します。	P99 参照

■取得をお願いする情報の例＜ Mac OS X の場合＞

取得情報	含まれている情報	取得する目的	参照ページ
システム情報の取得	端末にインストールされているアプリケーションやハードウェア、ネットワーク環境などの情報が含まれています。	不具合が発生するアプリケーションの有無の確認や動作環境に問題がないかを確認するために取得します。	P90 参照
コンソールメッセージ	コンピューターで実行された各種タスクやアプリケーションの動作ログが含まれています。	アプリケーション実行時などに発生したエラー情報などを確認するために取得します。	P91 参照
ESET 製品の設定ファイル	端末にインストールされている、ESET 製品の設定内容が含まれています。	不具合の原因となる誤った設定の有無などを確認するために取得します。	P94 参照
スクリーンショット	ディスプレイ上に表示されている、画面のみの情報です。	実際に表示されたエラー画面などを確認するために取得します。	P99 参照

■取得をお願いする情報の例（Android デバイスの場合）

取得情報	含まれている情報	取得する目的	参照ページ
ESET 製品の設定ファイル	端末にインストールされている、ESET 製品の設定内容が含まれています。	不具合の原因となる誤った設定の有無などを確認するために取得します。	P95 参照

！重　要

取得する情報には、ユーザー名、パスワードなどの個人情報が含まれている場合があります。お取り扱いには十分ご注意ください。

3.2.1　環境設定ファイル（ESET SysInspector）の取得方法

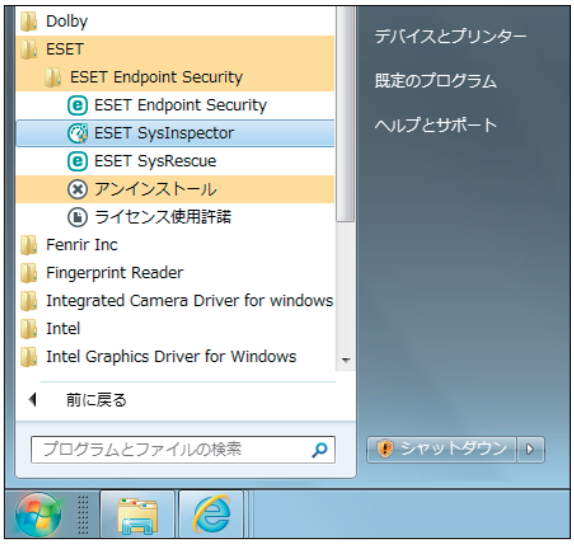
ESET SysInspector 情報を取得するには次の 2 つの方法があります。
①情報を取得するクライアントコンピューターを直接操作して取得する方法
② ERA Web コンソールからリモート操作で取得する方法

■コンピューターを直接操作して取得する

操作手順

1 Windows で［スタート］＞［すべてのプログラム］（または［プログラム］）＞［ESET］＞［ESET Endpoint Security］（または［ESET Endpoint Antivirus］）＞［ESET SysInspector］をクリックします。

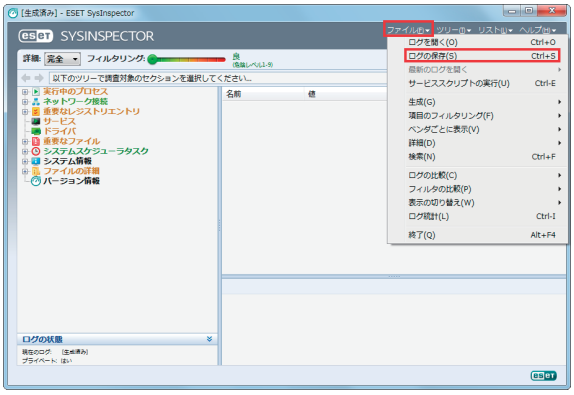
Windows Vista/7 の場合は「ユーザーアカウント制御」画面が起動します。
Windows Vista の場合は［続行］ボタン、Windows 7 の場合は［はい］ボタンをクリックします。



ワンポイント

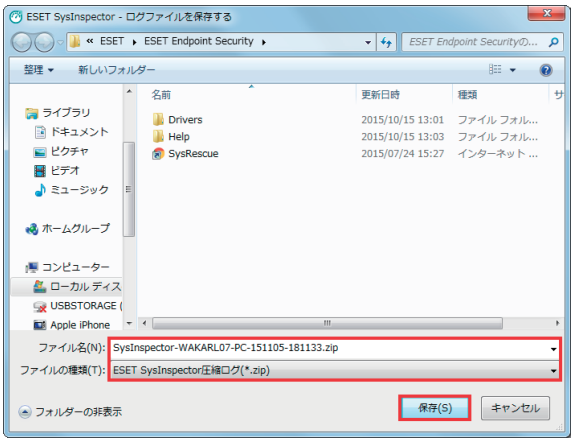
ESET SysInspector の起動には数分かかる場合があります。

2 ［ファイル］＞［ログの保存］をクリックします。

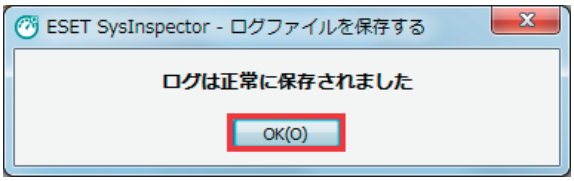


続く

3 保存先を選択し、「ファイルの種類」が「ESET SysInspector 圧縮ログ（*.zip）」であることを確認してから、ファイル名を入力して［保存］ボタンをクリックします。



4 ［OK］ボタンをクリックします。

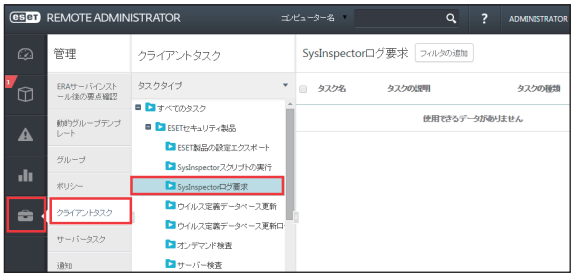


■ ERA Web コンソールからリモート操作で取得

操作手順

1 ERA Web コンソールにログオンします。

2 ［管理］メニュー>［クライアントタスク］>［SysInspector ログ要求］をクリックします。



3 ［新規作成］をクリックします。

4 ［ターゲット］で対象となるコンピューターを設定します。
必要に応じてその他の設定をします。

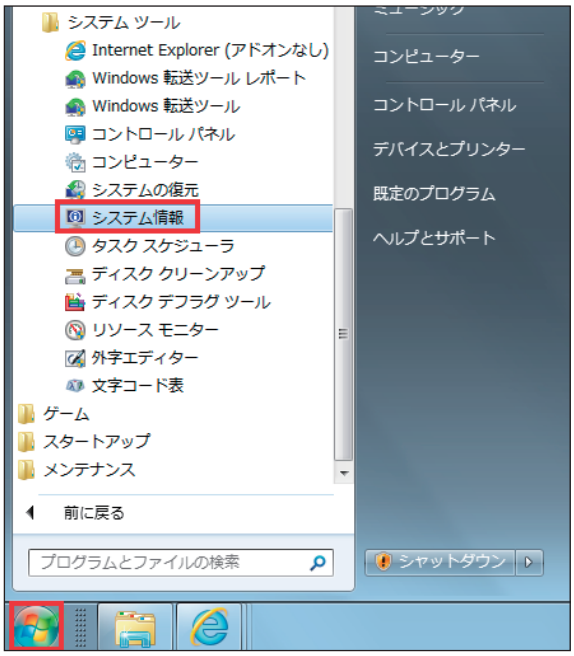
5 ［終了］をクリックします。

3.2.2　Windows システム情報の取得方法

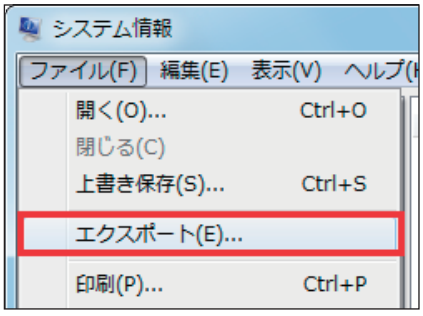
Windows のシステム情報は、Windows に標準インストールされている「システム情報」を使って取得します。
Windows XP 以降のすべての Windows OS で同じ手順で取得できます。

操作手順

1. Windows の［スタート］＞［すべてのプログラム］（またはプログラム）＞［アクセサリ］＞［システムツール］＞［システム情報］をクリックします。

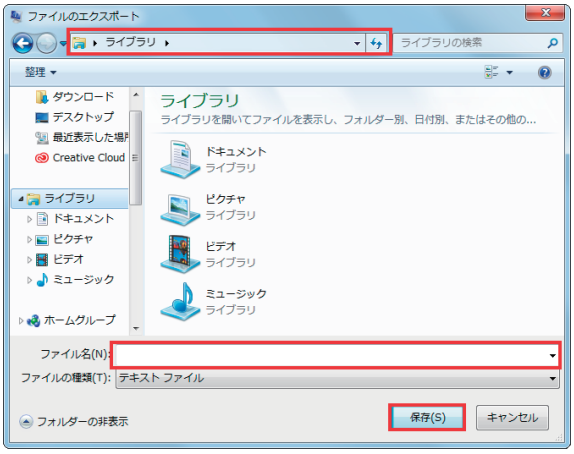


2. ［ファイル］＞［エクスポート］をクリックします。



続く

3 保存先を選択し、「ファイル名」を入力して［保存］ボタンをクリックします。
システム情報が保存されます。

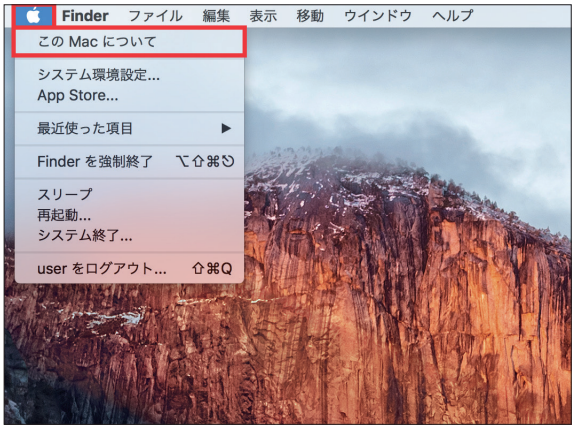


3.2.3　Mac OS X のシステム情報の取得方法

Mac OS X のシステム情報の取得は、「この Mac について」画面から取得できます。ここでは、Mac OS X El Capitan v10.11 を例にシステム情報の取得手順を説明します。

操作手順

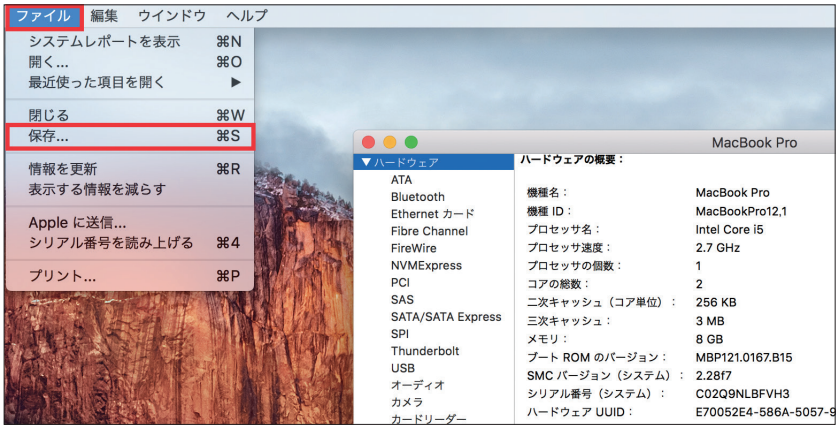
1 ［アップルメニュー］＞［この Mac について］をクリックします。



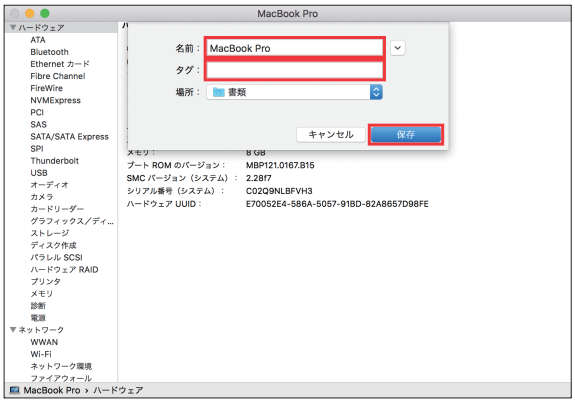
2 ［システムレポート］をクリックします。

続く

3 メニューバーの［ファイル］＞［保存］をクリックします。



4 ファイル名を入力して、保存先フォルダーを選択し、［保存］ボタンをクリックします。



3.2.4　Mac OS X のコンソールメッセージの取得方法

Mac OS X のコンソールメッセージの取得は、以下の手順で行います。

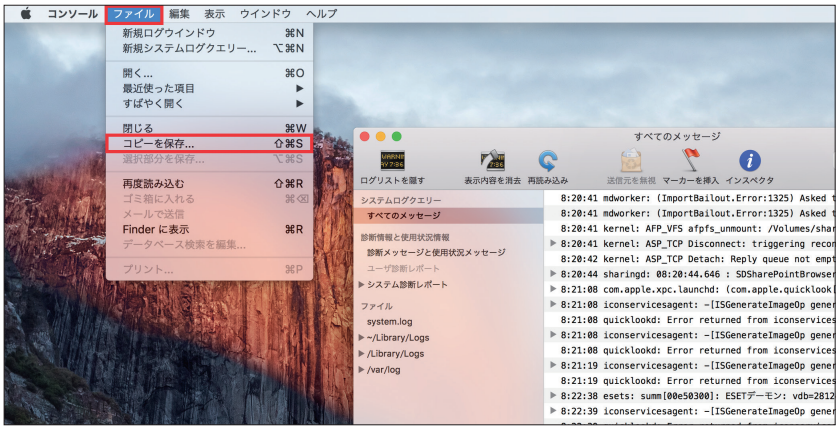
操作手順

1 Finder を開き、［アプリケーション］＞［ユーティリティ］フォルダーを開きます。

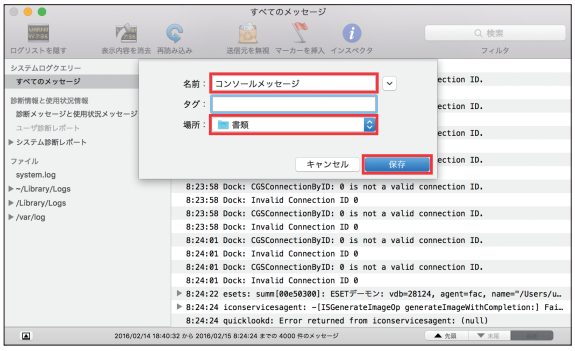
続く

② ［コンソール］アイコンをダブルクリックします。

③ コンソールが起動します。メニューバーの［ファイル］＞［コピーを保存］をクリックします。



④ ファイル名を入力し、保存先を設定して、［保存］ボタンをクリックします。



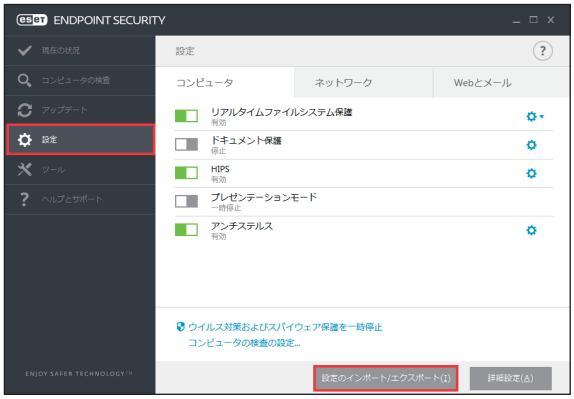
3.2.5　ESET 製品の設定ファイルの取得方法

ESET 製品の設定ファイル（拡張子 xml）には、クライアント用プログラムの設定ファイルとクライアント管理用プログラム（ESET Remote Administrator）の設定ファイルがあります。クライアント用プログラムの設定ファイルは、クライアント用プログラムを直接操作して取得します。

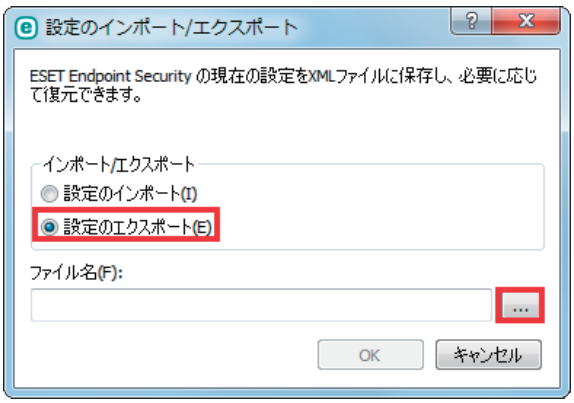
■ Windows の場合

操作手順

1. クライアント用プログラムのメイン画面を開きます。
2. ［設定］＞［設定のインポート / エクスポート］をクリックします。

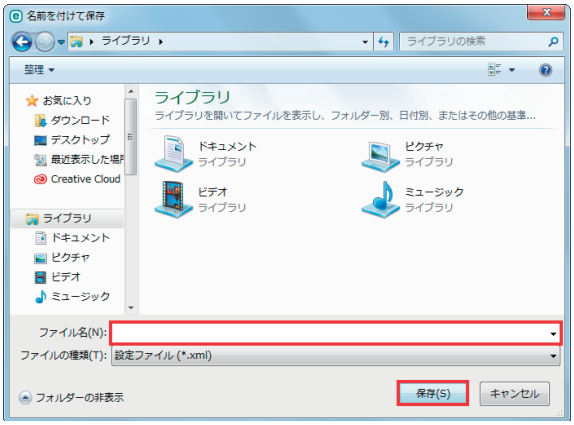


3. 「設定のエクスポート」をチェックして［...］ボタンをクリックします。

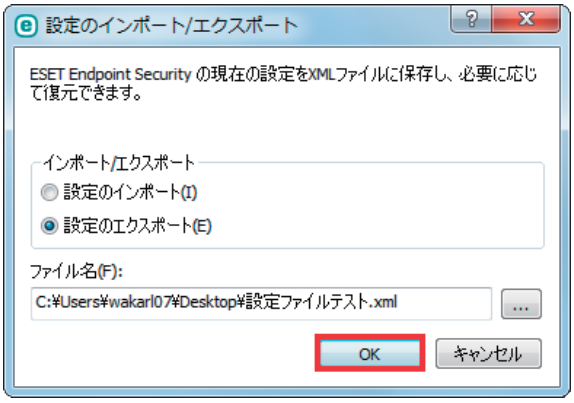


続く

4 保存先を選択して「ファイル名」を入力し、［保存］ボタンをクリックします。



5 ［OK］ボタンをクリックして設定ファイルを保存します。



■ Mac OS X の場合

操作手順

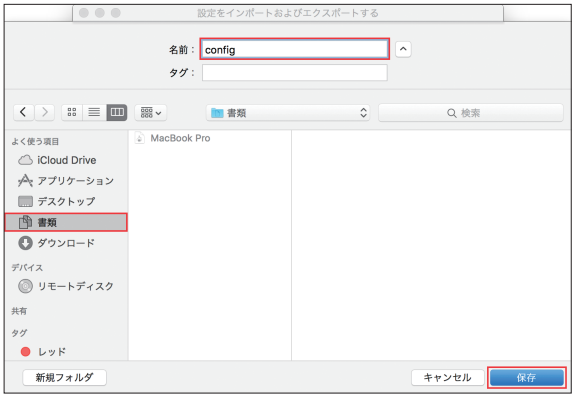
1 ESET Endpoint Security for OS X またはESET Endpoint アンチウイルス for OS X のメイン画面を開きます。

2 ［設定］＞［設定のインポート / エクスポート］をクリックします。

続く

3 ［設定のエクスポート］をチェックして、［参照］ボタンをクリックします。

4 ファイル名を入力し、保存先を選択して、［保存］ボタンをクリックします。



5 保存するファイルがフルパスで表示されます。［OK］ボタンをクリックすると、設定ファイルが保存されます。

■ Android の場合

操作手順

1 ESET Endpoint Security for Android のメイン画面を開きます。

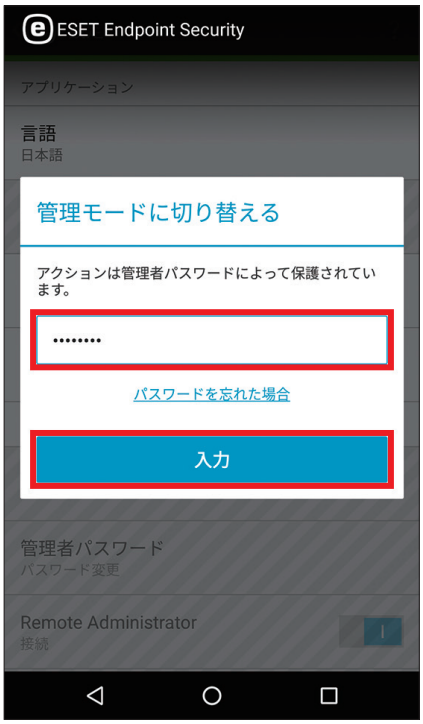
続く

2 ⋮をタップし、［設定］をタップします。

3 ［設定のインポート／エクスポート］をタップします。

続く

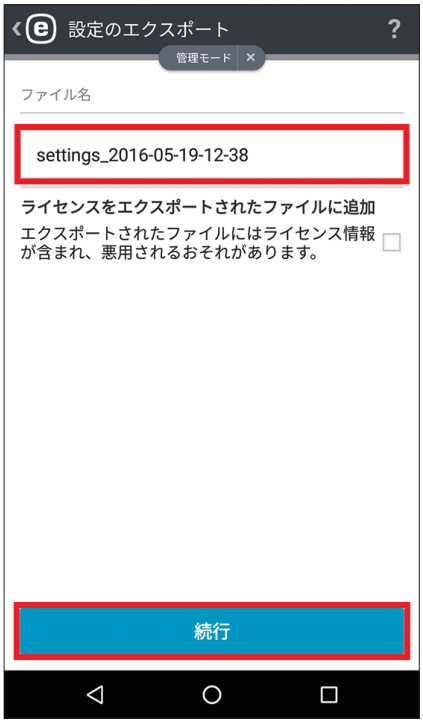
4 「管理モードに切り替える」画面が表示されたときは管理者のパスワードを入力し、[入力] ボタンをタップします。



5 [設定のエクスポート] をタップします。

続く

6 ファイル名を必要に応じて変更し、［続行］ボタンをタップします。



ワンポイント

［ライセンスをエクスポートされたファイルに追加］をタップしてオンにすると、エクスポートする設定ファイル内にライセンス情報を含めることができます。

7 設定ファイルの共有方法をタップし、画面の指示に従って設定ファイルを保存します。

［NFC サービス］をタップすると、NFC を利用して別の Android デバイスに設定ファイルを送信できます。［ドライブ］をタップすると、Google ドライブに設定ファイルを保存できます。［Gmail］をタップすると、設定ファイルを電子メールに添付して送信できます。

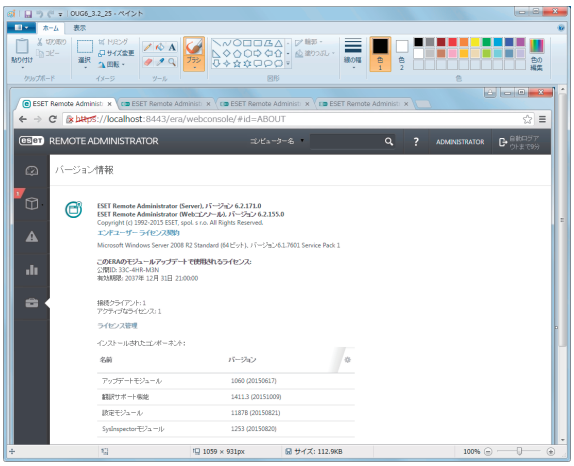
3.2.6　スクリーンショットの作成方法

お問い合わせをいただいた際に、スクリーンショットの提出をお願いする場合があります。
一般的なスクリーンショット作成方法について説明します。

■ Windows の場合

操作手順

1. スクリーンショットを作成する画面を表示します。
2. 次のキーを押します。
   フルスクリーンでスクリーンショットを作成する場合→【PrintScreen】キー
   アクティブウインドウ（作業対象の画面）のスクリーンショットを作成する場合→【Alt】キーを押しながら【PrintScreen】キー
3. ［スタート］＞［すべてのプログラム］（またはプログラム）＞［アクセサリ］＞［ペイント］をクリックします。
4. 【Ctrl】キーを押しながら【V】キーを押して、スクリーンショットをペーストします。



5. ［ファイル］＞［名前を付けて保存］とクリックし、保存先とファイル名を指定して JPEG 形式で［保存］ボタンをクリックします。

■ Mac OS X の場合

Mac OS X でスクリーンショットを取得するときは、以下の手順で行います。

フルスクリーンでスクリーンショットを取得する場合

【shift】キーと【command】キーを押しながら、【3】キーを押します。デスクトップ上にファイルが作成されます。

選択したウィンドウのスクリーンショットを取得する場合

【shift】キーと【command】キーを押しながら、【4】キーを押し、続いて【スペース】キーを押します。マウスポインターがカメラアイコンに変わるので、スクリーンショットを取得したいウィンドウ上で、クリックします。デスクトップ上にファイルが作成されます。