ユーザーズガイド
導入・運用編

目次

Chapter 1
ESET ライセンス製品の導入とその際の検討事項
P.7

目次

Chapter 4
ウイルス対策における運用
P.117

Chapter 5
よくある質問
お問い合わせの際に
P.149

■本書について

○本書は、ESETセキュリティ ソフトウェア シリーズ ライセンス製品の共通ガイドとしてまとめています。

○文中に出てくるERAは「ESET Remote Administrator」、ERASは「ESET Remote Administrator Server」、ERACは「ESET Remote Administrator Console」のことです。

○文中に設けているアイコンは、該当するプログラムを示しています。「ESET Endpoint Security」はアイコン、「ESET Endpoint アンチウイルス」はアイコン、「ESET File Security for Microsoft Windows Server」はアイコン、「ESET File Security for Linux」はアイコン、「ESET NOD32アンチウイルス」はアイコン、「ESET Endpoint Security for Android」はアイコン、「ESET Remote Administrator」はアイコン、「ESET Remote Administrator Server」はアイコン、「ESET Remote Administrator Console」はアイコンです。

○文中に出てくるクライアントPCは、Windows端末、Mac端末およびAndroid端末を総称しています。

■お断り

[Chapter 1]
ESET ライセンス製品の導入とその際の検討事項

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で構成されます。本節では、規模に応じたESET ライセンス製品の運用方法について説明します。

1.1.1 運用と構成方法の検討

ESET ライセンス製品の運用方法には、クライアント用プログラムのみの運用と、管理サーバーやミラーサーバーを設置した運用があります。本製品の導入にあたっては、最初にクライアント数を考慮し、管理サーバーやミラーサーバーの必要性などについて検討を行ってください。

1.1.1.1 クライアント管理機能導入の検討

クライアント管理用プログラム「ESET Remote Administrator（ERA）」を利用することで、クライアントPCのウイルス警告、ファイアウォール警告、イベントログなどの情報の取得や各種設定の配布が行えます。ERAの導入は必須ではありませんが、クライアントPC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ERAを導入することをお勧めします。

管理するクライアント数が多い場合など2台以上の管理サーバーを設置する場合は、「複製機能」により各種データを集約することもできます。

なお、ERAの対応OSは、Windowsのみです。ERAを使用する場合は、Windowsが必要になります。

››› POINT

クライアント管理用プログラムの主な機能については、「ESET ライセンス製品 ご利用の手引」をご参照ください。

1.1.1.2 ミラーサーバー機能導入の検討

ミラーサーバーを設置すると、クライアントPCはインターネットへのアクセスを行わずに、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。ミラーサーバーの構築は、ESET Remote AdministratorやESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxで構築できます。

また、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、以下の方法が準備されています。クライアント用にインストールするセキュリティプログラムによって対応する配布方法が異なりますので、ミラーサーバーを構築する場合は、この点に留意して、設置を行ってください。

●アップデートファイルの配布方法とセキュリティプログラムの対応一覧

配布方法＼プログラム		Windows用セキュリティプログラム	Mac OS X用セキュリティプログラム	Linux用セキュリティプログラム
		ESET Endpoint Security ESET Endpoint アンチウイルス ESET File Security for Microsoft Windows Server Windows用プログラムの旧バージョン	ESET NOD32アンチウイルス	ESET File Security for Linux
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メモリーなど	○	×	×

1.1.1.3 利用するクライアント用プログラムの選択

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が提供されます。お客さまは、提供されたクライアント用プログラムの中からOSや用途に応じて自由に利用するセキュリティプログラムを選択できます。

プログラム		概要
Widnows クライアント用プログラム	ESET Endpoint セキュリティ	ウイルス・スパイウェア対策をはじめ、不正侵入対策、迷惑メール対策、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。
	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。
Windows サーバー用プログラム	ESET File Security for Microsoft Windows Server	
Mac OS X用プログラム	ESET NOD32アンチウイルス	
Linux サーバー用プログラム	ESET File Security for Linux	
Android用プログラム	ESET Endpoint セキュリティ for Android	ウイルス・スパイウェア対策をはじめ、迷惑メール対策、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。

▸▸▸ POINT

各プログラムの主な機能については、「ESET ライセンス製品 ご利用の手引」をご参照ください。

1.1.1.4 サーバー動作環境／接続するクライアント数とネットワーク環境の検討

管理サーバーやミラーサーバーを運用する場合、注意しなければならないのがサーバーやネットワークに対する負荷の集中です。管理サーバーは、各クライアントPCの情報を収集するため定期的にクライアントPCとの通信を行います。そのため、クライアントPCの情報取得頻度を上げたり、同じ情報取得頻度でもクライアント数が増加するとそれだけサーバーやネットワークへの負荷が高まります。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るため、ミラーサーバーと兼用している管理サーバーは、管理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。
サーバーのスペックが予想される負荷に耐え得るかどうか、また、負荷を分散させるために2台以上のサーバーを導入するかどうかなどを検討します。

▸▸▸ POINT

ERAを導入したり、ミラーサーバーを設置する場合は、そのサーバーに接続するクライアント数を必ず確認してください。クライアント数が増加するとサーバー負荷が高くなります。運用の目安となるユーザー数と構成例を13ページで紹介していますので、そちらを参考にサーバーのスペックをご検討ください。

1.2 新規導入や他社製品からの乗り換えによる導入の流れ

本節では、他社製のセキュリティプログラムからESET ライセンス製品に乗り換える場合の移行方法について説明します。新規導入の際も、導入の流れは同様です。

1.2.1 導入の流れ

他社製品からの移行を行う場合に重要なのが、移行期間においてセキュリティレベルを低下させることなくスムーズな移行を行うことです。弊社では、スムーズな移行のために以下のステップで作業を行うことを推奨しています。

STEP1 クライアント用プログラムの検討 12 ページ参照

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、変更を行った場合にどのような変化が発生するのかを検討します。

↓

STEP2 サーバー構成の検討 13 ページ参照

管理サーバーやミラーサーバーの必要性を検討し、サーバーの動作環境などを確認します。

↓

STEP3 ネットワーク環境の検討 31 ページ参照

ネットワーク負荷やクライアント PCとサーバー間の通信経路を確認します。

↓

STEP4 移行プランの検討 34 ページ参照

既存ソフトウェアのアンインストール方法やクライアント用プログラムの導入方法を検討し、具体的な移行プランを作成します。

↓

STEP5 移行作業 58 ページ参照

作成した移行プランに従って、作業を行います。

1.3 STEP1 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検討では、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、変更を行った場合にどのような変化が発生するのかを検討します。以下のような点に着目して検討してください。

1.3.1 チェックポイント

1.3.1.1 クライアント用プログラムの選択

ESET ライセンス製品は、製品ごとに複数のクライアント用プログラムが提供されます。提供されるクライアント用プログラムの機能などを検討し、どのセキュリティプログラムを利用するのが適しているかを検討します。

プログラム ＼ 製品		ESET Endpoint Protection Advanced	ESET Endpoint Protection Standard
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	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	○	○
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	○	○
Android用	総合セキュリティプログラム ESET Endpoint Security for Android	○	○

1.3.1.2 動作環境の確認

導入予定のクライアントPC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を確認します。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ご参照ください。

1.3.1.3 既存のセキュリティ製品との違いを確認

現在利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が導入されるので、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。

››› POINT

各プログラムの主な機能については、「ESET ライセンス製品 ご利用の手引」をご参照ください。

1.4 STEP2 サーバー構成の検討

サーバー構成の検討では、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、サーバーの動作環境などを確認します。以下の点に着目して検討してください。

1.4.1 チェックポイント

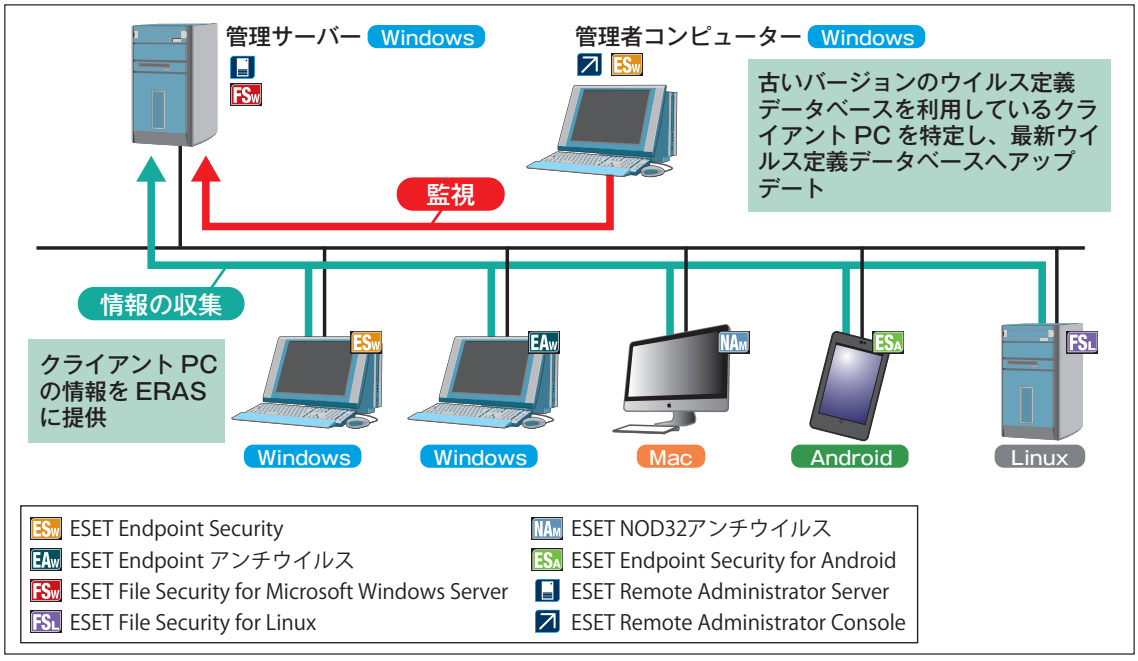
1.4.1.1 管理サーバーの必要性

クライアント管理用のサーバーを導入すると、クライアントPCの状況を集中管理したり、クライアントPCに導入したESET ライセンス製品の動作設定などを配布できます。

管理サーバーの導入

管理サーバーの導入にあたっては、管理サーバーとして運用するコンピューターにESET Remote Administrator Server（ERAS）を、ERASをリモート操作する管理用コンピューターにESET Remote Administrator Console（ERAC）をインストールします。それぞれのインストールは、弊社ユーザーズサイトからダウンロードしたインストーラーを実行することで行います。

なお、ERASおよびERACはWindows用プログラムです。またERAのインストールには、「ライセンスキーファイル（.licファイル）」が必要です。ESET ライセンス製品ご利用の手引を参考に、弊社ユーザーズサイトからライセンスキーファイル（.licファイル）をあらかじめダウンロードしてください。



▸▸▸ POINT

ERASのリモート操作に利用するERACは、複数のコンピューターにインストールできます。また、ERASをインストールしたコンピューターにもインストールできます。

ERA導入時の注意点

ここでは、ERAを導入するときの注意点について説明します。ERAは、ネットワークを利用してクライアントPCの情報を取得したり、ウイルス定義データベースのアップデートを行います。適切な設定を行わないと、情報の取得や操作が正常に行えないのでご注意ください。

■ プロキシサーバー

インターネット接続にプロキシサーバーの経由が必要な環境にミラーサーバーを設置する場合は、ミラーサーバーがプロキシサーバー経由でESET社の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す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」をご参照ください。

なお、ウイルス定義データベース（*.nup）は、プロキシサーバーでキャッシュを行わないように設定してください。プロキシサーバーのキャッシュ仕様によっては、ウイルス定義データベースがもつデジタル署名が不整合を起こし、クライアントPCでのアップデートができなくなります。

■ ファイアウォールソフトの設定

ERASをインストールしたコンピュータ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機能を搭載したプログラムが動作していると、クライアントPCがウイルス定義データベースのアップデートに失敗したり、ERACをインストールした管理用コンピューターからリモート操作が行えない場合があります。

ERACからのリモート操作が行えない場合やクライントPCがウイルス定義データベースのアップデートに失敗する場合は、ファイアウォール機能を搭載したプログラムが動作しているかどうかを確認してください。ファイアウォール機能を搭載したプログラムが動作している場合は、その設定を確認し、ERASがERACとの通信に利用するポートおよびクライアントPCとの通信に利用するポートを開放します。ミラーサーバーの場合も同様に、クライアントPCがアップデートに利用するポートを開放します。ERAS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。

プロトコル	ポート番号	用途
TCP	2221	クライアントPCからミラーサーバーへの接続
	2222	クライアントPCからERASへの接続
	2223	ERACからERASへの接続
	2224	リモートインストール用エージェントからERASへの接続
	2225	ダッシュボードサーバーからERASへの接続
	2846	管理サーバー（ERAS）を複数設置した場合に、下位の管理サーバー（ERAS）から上位の管理サーバー（ERAS）への接続

■ 既存ネットワークに新たにERAを導入する場合の確認事項

ERAはWindows環境で動作するため、「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を購入するケースが発生することがあるのでご注意ください。Windows CALの詳細については、Microsoft社にご確認ください。

››› POINT

ミラーサーバーにおけるウイルス定義データベースの保存先をCALの概念のない、NASやストレージサーバー、Linuxで構築したサーバーに置くことでCALが必要ないケースもあります。

1.4.1.2 ミラーサーバーの必要性

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えます。これによりクライアントはウイルス定義データベースのアップデートの際にインターネット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。

ミラーサーバーの構築は、ESET Remote AdministratorやESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxで構築できます。また、ESET Remote AdministratorやESET Endpoint アンチウイルスでミラーサーバーを構築した場合は、差分アップデート（ナノアップデート）やSSL接続などの機能も利用できます。

プログラム	ESET Remote Administrator	ESET Endpoint アンチウイルス	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	●IISと組み合わせて構築することで、大規模環境でのミラーサーバーとして利用するできる ●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PCのアップデートが可能 ●USB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）	●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PCのアップデートが可能 ●USB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PCのアップデートが可能 ●USB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）	●Linux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PCのアップデートが可能
デメリット	●ウイルス検査機能が搭載されていないため、ウイルス検査機能をもったプログラムと併用する必要がある	●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	●差分アップデートが利用できないため、ベースアップデート時には約30MBの定義ファイル配信が発生する	

※ESET Endpoint SecurityおよびMac OS X用のESET NOD32アンチウイルスは、ミラーサーバー構築機能をサポートしていません。

1.4.1.3 ミラーサーバーの種類の検討

ミラーサーバーを設置してアップデートファイルを配布する方法には、HTTPサーバーを利用した配布や共有フォルダーを利用した配布があります。HTTPサーバーを利用する場合の配布方法およびクライアントPCの台数は以下を目安にご検討ください。

HTTPサーバー	クライアント数
ESET Remote Administrator Server（ERAS）内蔵のHTTPサーバー	400台
ESET Endpoint アンチウイルス内蔵のHTTPサーバー	100台
ESET File Security for Microsoft Windows Server内蔵のHTTPサーバー	100台
ESET File Security for Linux内蔵のHTTPサーバー	1,000台
Microsoft Internet Information Services（IIS）	3,000台
Apache	3,000台

1.4.1.4 データベースの種類の検討

ERASをインストールした管理サーバーでは、クライアントPCで発生したログをデータベースに登録して管理します。ここでは、ERAS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の種類と最大容量

管理サーバーで利用されるデータベースは、登録できる保存容量の違いによって以下のデータベース形式をサポートしています。既定値では、1,000クライアントで3カ月間のログを保存することを目安とした最大保存容量「2GB」のMicrosoft Access形式のデータベースが利用されます。1,000クライアント以上で利用する場合は、「クライアント数」とログの「保存期間」を考慮してデータベースの形式を決定してください。

●利用できるデータベースの形式と最大保存容量

データベースの形式	登録可能な最大容量
Microsoft Access（既定のデータベース形式）	最大2GB
Microsoft SQL Server 2005 ／ 2008 Express Edition	最大4GB
Microsoft SQL Server 2008 R2 Express Edition	最大10GB
Microsoft SQL Server 2005 ／ 2008 Standard Edition	最大値なし

利用データベースの選定の目安

管理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とログの保存期間によって変動します。必要なデータベースの容量は、以下の例を目安に計算します。

●データベース形式選定の目安

ログの容量	1回あたり約2.1KB
クライアント用に作成される1日あたりのログ	6件
ログの保存期間	3カ月（90日）

▸▸▸ POINT

ログの保存期間の既定値は、ウイルスログが6カ月間、その他のログが3カ月間です。

例

クライアント数1,000の環境で、3カ月間ログを保存した場合のデータベース容量

1,000台（クライアント数）×6件（件／日）×2.1KB（1回あたりのログ容量）×90日（保存期間）

＝1134MB

●クライアント数に応じた推奨データベース形式

クライアント数	3カ月間保存した場合の推定容量	利用できるデータベースの形式
1,000	1134MB	Microsoft Access、Microsoft SQL Server 2005/2008 Express Edition
2,000	2268MB	Microsoft SQL Server 2005/2008 Express Edition
3,000	3402MB	Microsoft SQL Server 2005/2008 Express Edition
4,000	4536MB	Microsoft SQL Server 2008 R2 Express Edition
5,000 以上	5670MB	Microsoft SQL Server 2008 R2 Express Edition

CAUTION

ERAとMicrosoft SQL Serverとの接続は、SQL Server認証を推奨します。Windows認証を利用し、かつERASとデータベースサーバーが異なるコンピューターの場合は、ERASのサービスの動作アカウントには、データベースへのアクセス権限があるユーザー（ドメインアドミニストレーターなど）を設定してください。アクセス権がない場合は、インストールに失敗します。

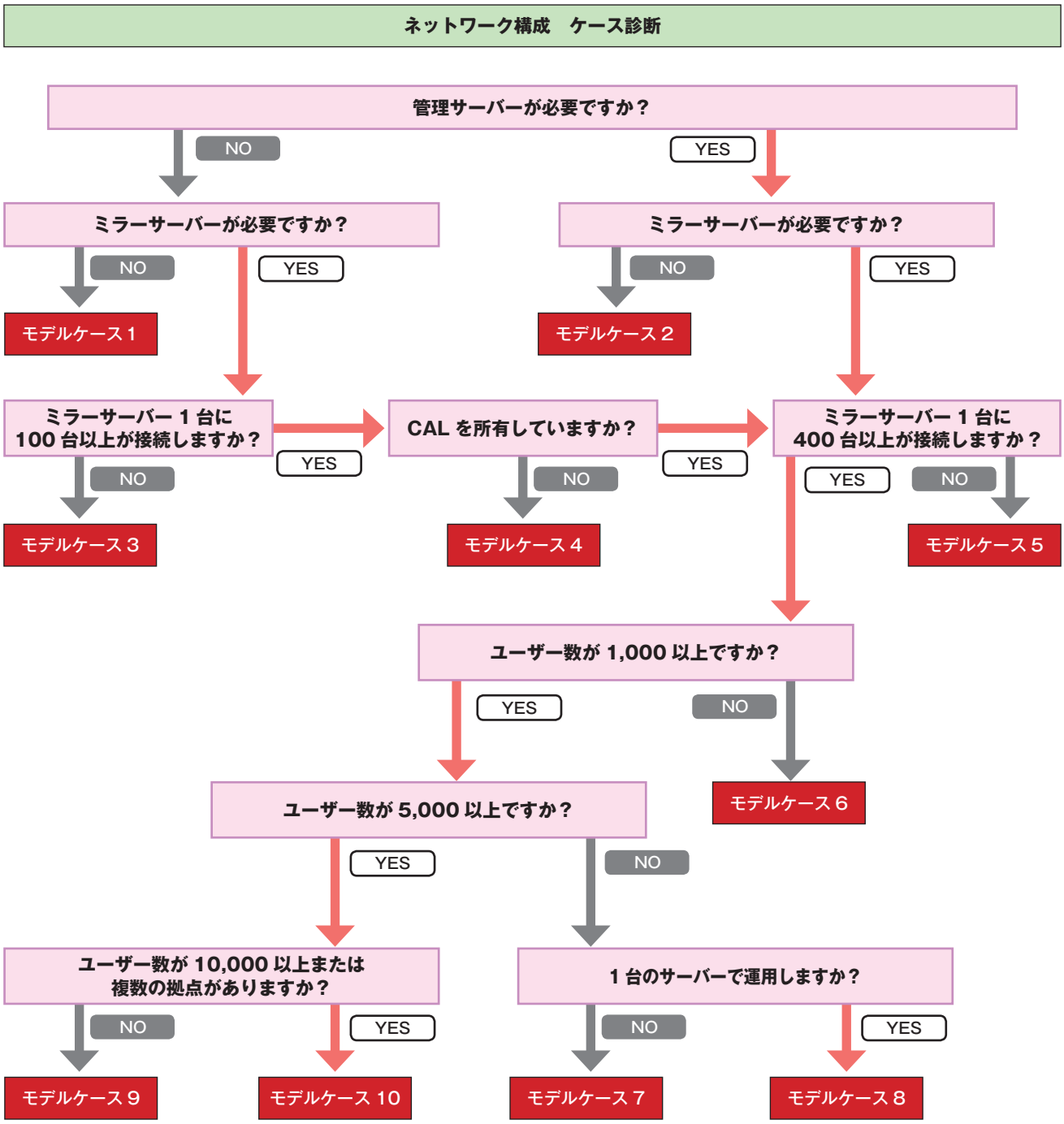
1.4.1.5 動作環境の確認

管理サーバーやミラーサーバーを設置する場合は、サーバーとして利用する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。クライアント管理用プログラムの動作環境については、弊社製品ホームページ上をご参照ください。

1.4.2 サーバー構成のモデルケース

ここでは、サーバー構成のモデルケースと、各ケースのサーバースペック例を紹介します。サーバー構成を検討する際の参考にしてください。

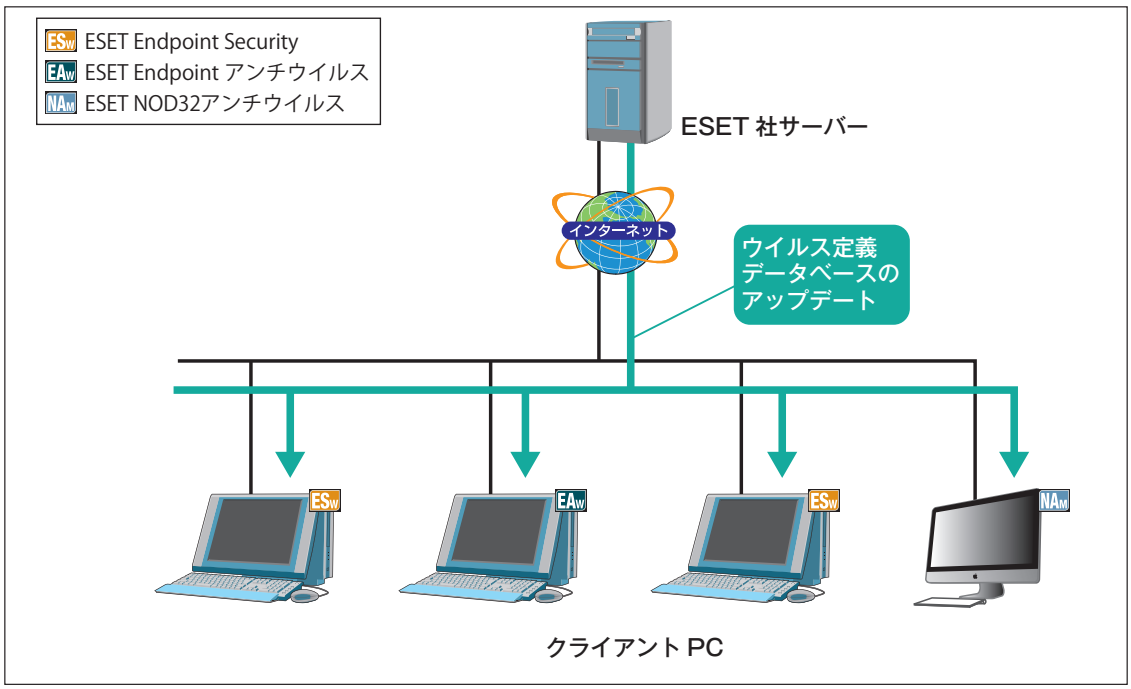
1.4.2.1 診断フロー



1.4.2.2 モデルケース1 クライアント用プログラムのみを利用する場合

クライアント用プログラムのみを用いた運用では、サーバーの設置が不要です。

なお、この構成で利用する場合、各クライアントはインターネットに接続し、ESET社の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ように設定します。



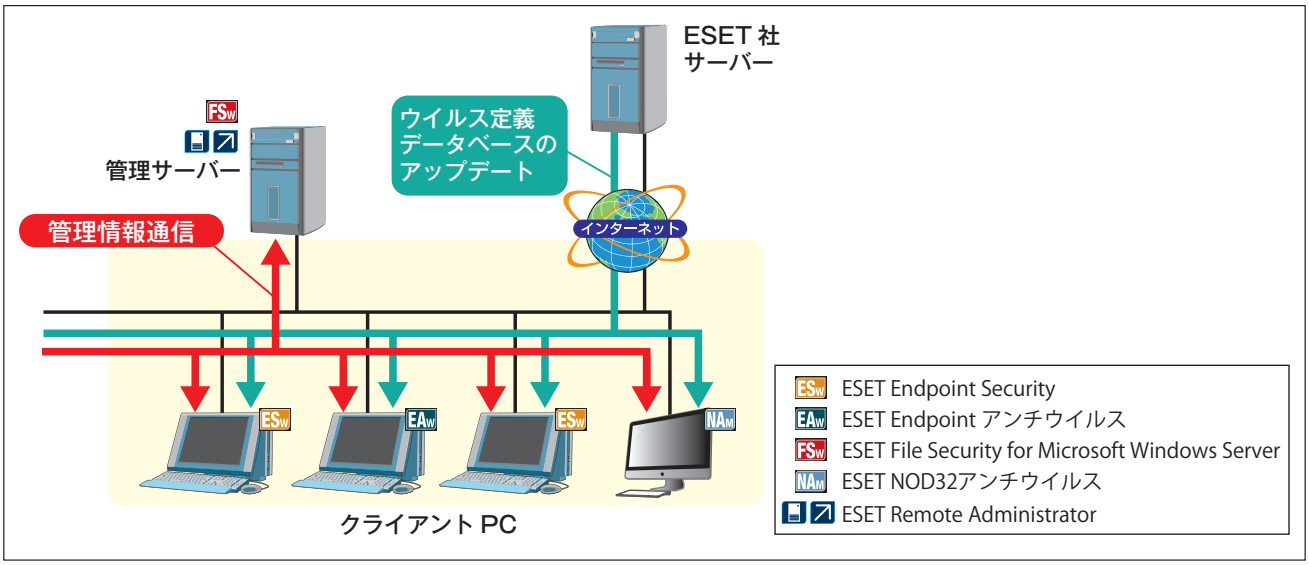
構成

クライアントのみで構成します。サーバーは必要ありません。

1.4.2.3 モデルケース2 管理サーバーを利用する場合（ミラーサーバーなし）

管理サーバーのみを用いた運用の場合は、クライアント管理用プログラム（ERA）を導入し、ERAを利用して各クライアントを管理します。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PC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ご注意ください。



構成

■ クライアント数400台未満

- ●1台のサーバーで管理サーバーを運用
- ●データベースは、既定のMicrosoft Access形式（mdb）を利用

■ クライアント数400台以上

- ●1台のサーバーで管理サーバーを運用
- ●データベースは、Microsoft SQL Server 2005以降を利用

※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

サーバースペック

■ クライアント数400台未満

- ●インテル Pentium4 2.4GHzと同等以上の性能を有したCPU
- ●2GB以上のメモリー
- ●1Gbpsのネットワークアダプター

■ クライアント数400台以上

- ●インテル Core 2 Duo　2.4GHzと同等以上の性能を有したDual Core以上のCPU
- ●4GB以上のメモリー
- ●1Gbpsのネットワークアダプター

クライアントの接続間隔

■ クライアント数400台未満

●管理サーバーへの接続間隔：10分

■ クライアント数400台以上

●管理サーバーへの接続間隔：30分

CAUTION

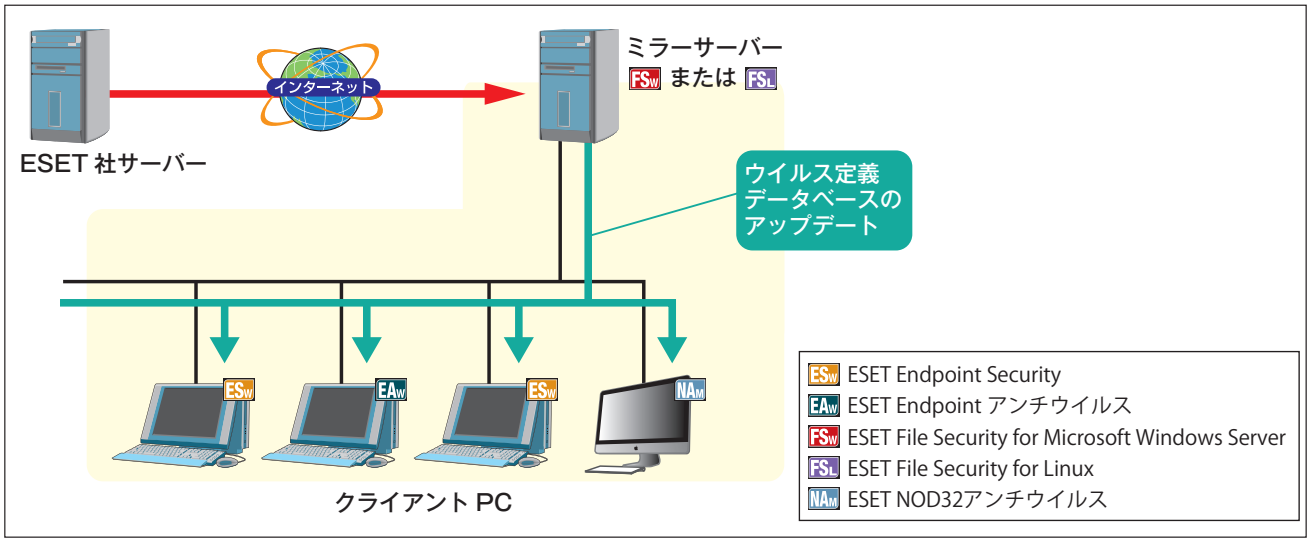
上記は、参考値です。管理可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定などにより異なります。

1.4.2.4 モデルケース3 100ユーザー以下・管理機能なし

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PCに提供するものです。ミラーサーバーを設置することで、各クライアントPC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、インターネット接続にかかわるトラフィックが軽減されるほか、インターネット接続環境にないクライアントPCにもアップデートファイルを容易に配布できます。

ミラーサーバー機能は、クライアント管理用プログラムであるERAと、Windows用のクライアント用プログラムであるESET Endpoint アンチウイルスおよびESET File Security for Microsoft Windows Server、Linuxサーバー用のESET File Security for Linuxに搭載されています。また、ESET Endpoint アンチウイルスは、サーバーOSをサポート対象外としていますので、Windowsサーバーでご利用の場合は、ESET File Security for Microsoft Windows Serverを使用してください。

ESET Endpoint アンチウイルスおよびESET File Security for Microsoft Windows Serverを利用してミラーサーバーを構築する際、クライアントPCの台数は100台以下を推奨しています。



構成

- ●1台のサーバーでミラーサーバーを運用
- ●ESET Endpoint アンチウイルスまたはESET File Security for Microsoft Windows Server、ESET File Security for Linux内蔵の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

サーバースペック

- ●インテル Pentium4 2.4GHzと同等以上の性能を有したCPU
- ●2GB以上のメモリー
- ●1Gbpsのネットワークアダプター

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

CAUTION

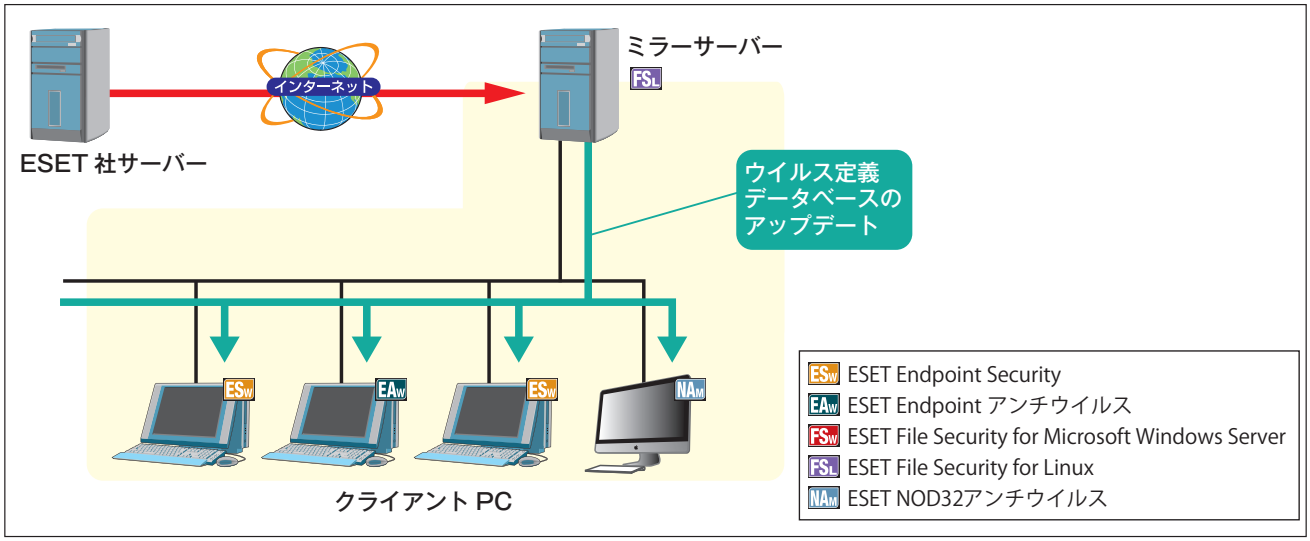
上記は、参考値です。接続可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定などにより異なります。

1.4.2.5　モデルケース4　1,000クライアント以下・管理機能なし

ESET File Security for Linuxをミラーサーバーとして運用します。

アップデートファイルの配布にはESET File Security for Linuxの内部HTTPサーバーである「ESET Mirror http daemon」を利用します。

このモデルケースでは、ミラーサーバーにLinuxを利用しますのでCALが不要となり、コストを軽減することができますが、ESET File Security for Linuxでミラーサーバー機能を利用する場合、差分アップデート機能に対応していないため、ウイルス定義データベースのアップデート時にネットワーク負荷がかかる場合があります。



構成

- ●一台のサーバーでミラーサーバーを運用
- ●ESET File Security for Linuxの内部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

- ●～1,000台

サーバースペック

- ●インテルPentium 4互換プロセッサ2.0GHzと同等以上の性能を有したCPU
- ●2GB以上のメモリー
- ●1Gbpsのネットワークアダプター

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

▸▸▸ POINT

クライアント数が1,000台以上ならApacheを利用してアップデートファイルを配布してください。

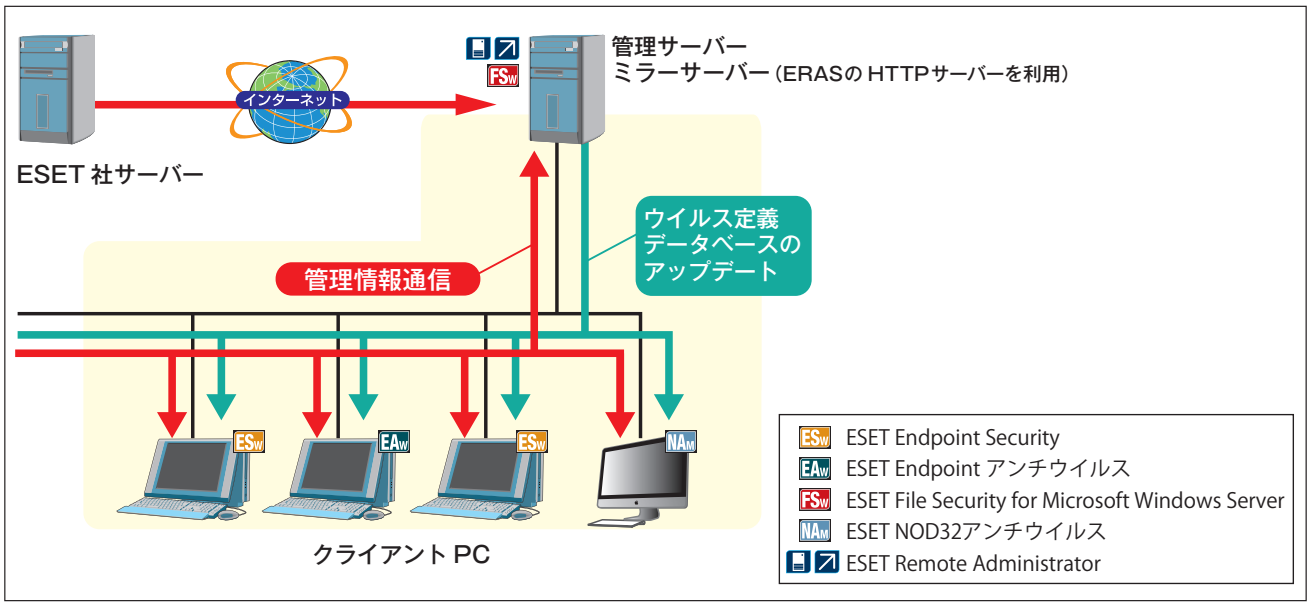
CAUTION

上記は、参考値です。接続可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定によって異なります。

1.4.2.6 モデルケース5 400ユーザー以下

ERAは、管理機能だけでなくミラー機能も搭載しています。そのため、ERAをインストールするだけでサーバーを管理サーバー兼ミラーサーバーとして運用させることが可能です。

2つの機能を1台のサーバーで兼用させる場合、それぞれの機能による負荷が1台のサーバーにかかることになります。サーバーに大きな負荷がかかる場合は、管理サーバーとミラーサーバーを別々に設置すること、さらには各サーバーをそれぞれ2台以上設置することをご検討ください。



構成

- ●1台のサーバーで管理サーバーとミラーサーバーを運用
- ●ESET Remote Administrator Server（ERAS）内蔵の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
- ●データベースは、既定のMicrosoft Access形式（mdb）を利用

クライアント数の目安

- ●～400台

サーバースペック

- ●インテル Pentium4互換のプロセッサ 2.4GHzと同等以上の性能を有したCPU
- ●2GB以上のメモリー
- ●1Gbpsのネットワークアダプター

クライアントの接続間隔

- ●管理サーバーへの接続間隔：10分
- ●ミラーサーバーへの接続間隔：120分

CAUTION

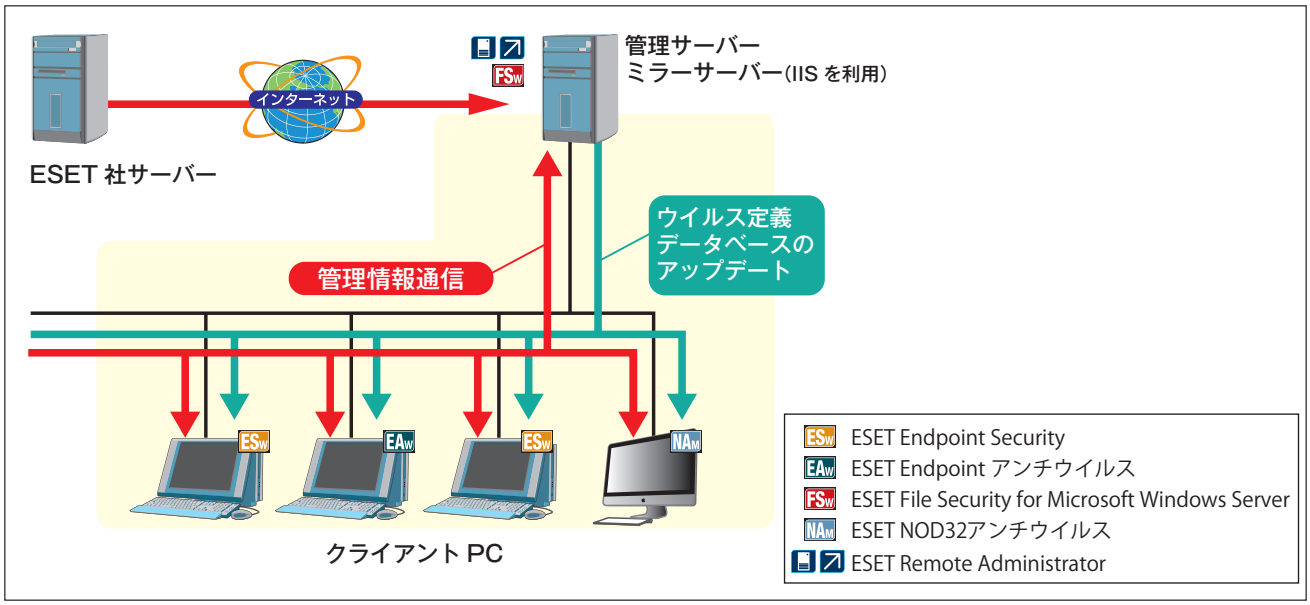
上記は、参考値です。管理可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定により異なります。なおサーバーへの負荷が高い場合には、管理サーバーとミラーサーバーを 別々に設置することをお勧めします。

1.4.2.7　モデルケース6　400～1,000ユーザー程度

1台のサーバーで、管理サーバー兼ミラーサーバーとして運用します。

アップデートファイルの配布には、Microsoft Internet Information Services（IIS）を利用します。このモデルケースにおける接続クライアント数の上限は1,000台です。

このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。



構成

- ●1台のサーバーで管理サーバーとミラーサーバーを運用
- ●Microsoft Internet Information Services（IIS）を利用を利用してアップデートファイルを配布
- ●データベースは、Microsoft SQL Server 2005以降を利用

※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

- ●～1,000台

サーバースペック

- ●インテル Pentium4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- ●4GB以上のメモリー
- ●1Gbpsのネットワークアダプター

クライアントの接続間隔

- ●管理サーバーへの接続間隔：30分
- ●ミラーサーバーへの接続間隔：360分

CAUTION

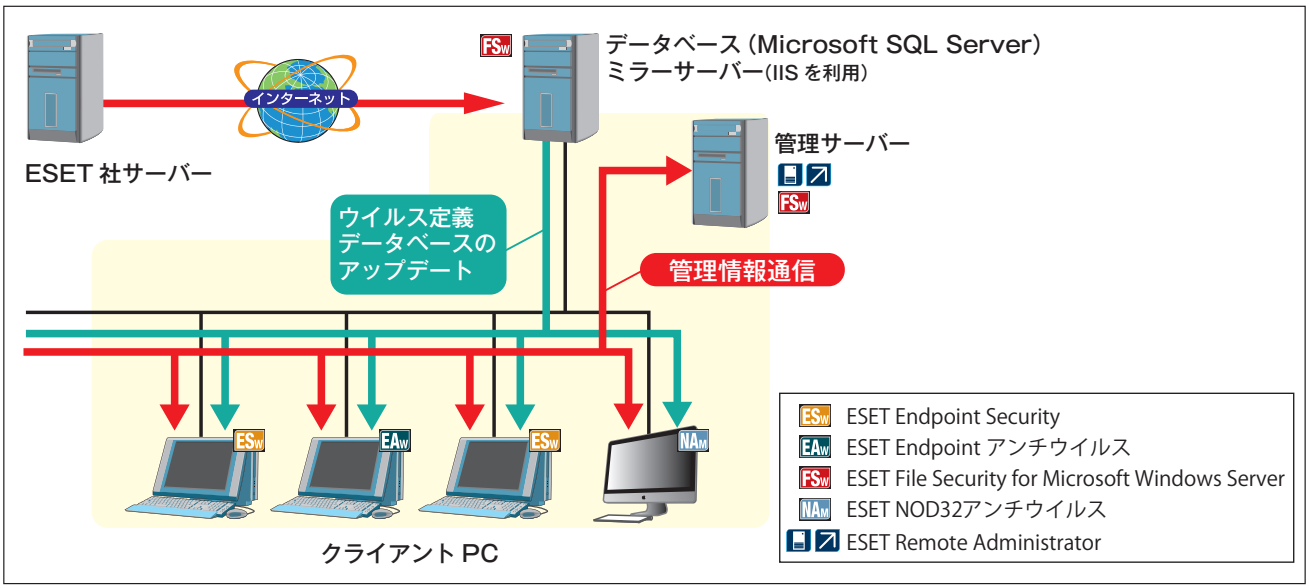
上記は、参考値です。管理可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定により異なります。なおサーバーへの負荷が高い場合には、管理サーバーとミラーサーバーを 別々に設置することをお勧めします。

1.4.2.8 モデルケース7 1,000～5,000ユーザー程度①

管理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) を利用します。このモデルケースにおける管理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、3,000台です。そのため3,000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してください。

このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。また、外部のデータベースを利用することで、管理サーバーとデータベースを分離します。



構成

- ●管理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（管理サーバー 1台／ミラーサーバー 1台以上）
- ●Microsoft Internet Information Services (IIS) を利用してアップデートファイルを配布
  （接続クライアント数が、3,000台を超える場合は、IISのミラーサーバーを複数台設置）
- ●データベースは、Microsoft SQL Server 2005以降を利用
  ※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

- ●～5,000台

サーバースペック

- ●インテル Pentium4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- ●4GB以上のメモリー
- ●1Gbpsのネットワークアダプター

クライアントの接続間隔

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

CAUTION

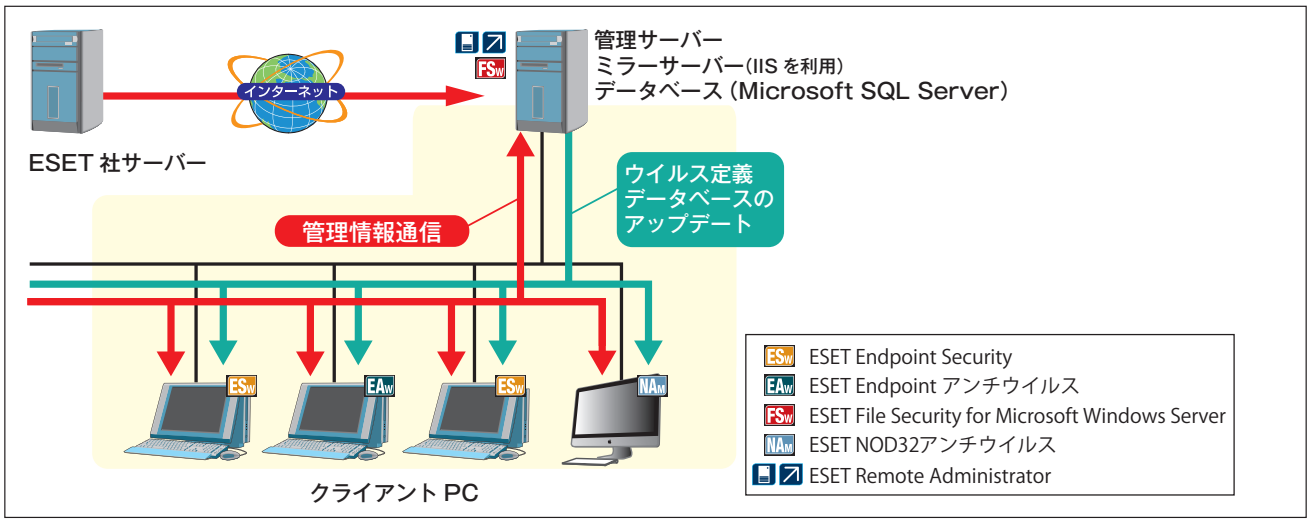
上記は、参考値です。管理可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定により異なります。

1.4.2.9　モデルケース8　1,000～5,000ユーザー程度②

1台のサーバーを管理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を利用します。

アップデートファイルの配布には、Microsoft Internet Information Services（IIS）を利用します。このモデルケースにおける管理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、3,000台です。そのため3,000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してください。

このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。



構成

- 1台のサーバーで管理サーバーとミラーサーバーを運用
  （クライアント数が3,000台以上の場合は別途ミラーサーバーを設置）
- Microsoft Internet Information Services（IIS）を利用してアップデートファイルを配布
  （接続クライアント数が、3,000台を超える場合は、IISのミラーサーバーまたはApacheのミラーサーバーを複数台設置）
- データベースは、Microsoft SQL Server 2005以降を利用
  ※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

- ～5,000台

サーバースペック

- インテル Pentium4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- 4GB以上のメモリー
- 1Gbpsのネットワークアダプター
- RAID 0構成のHDDまたはSSD

クライアントの接続間隔

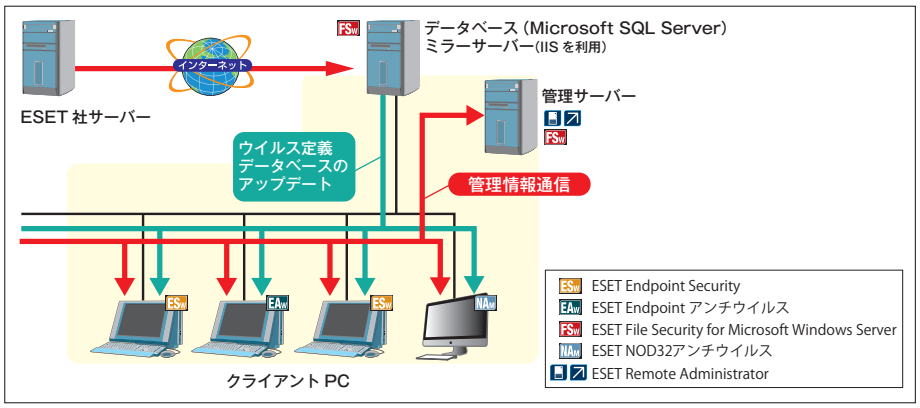
- 管理サーバーへの接続間隔：30分
- ミラーサーバーへの接続間隔：60分

CAUTION

上記は、参考値です。管理可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定により異なります。なおサーバーへの負荷が高い場合には、管理サーバーとミラーサーバーを 別々に設置することをお勧めします。

1.4.2.10 モデルケース9 5,000～10,000ユーザー程度

管理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RAID 0構成のHDDまたはSSDを利用します。アップデートファイルの配布には、Microsoft Internet Information Services (IIS)を利用します。このモデルケースにおける管理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、3,000台です。そのため3,000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してください。
このモデルケースでは、ミラー機能をERAもしくはESET File Security for Microsoft Windows Serverが行います。また、外部のデータベースを利用することで、管理サーバーとデータベースを分離します。



構成

- ●管理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（管理サーバー1台／ミラーサーバー1台以上）
- ●Microsoft Internet Information Services (IIS) を利用してアップデートファイルを配布
  （接続クライアント数が、3,000台を超える場合は、IISのミラーサーバーを複数台設置）
- ●データベースは、Microsoft SQL Server 2005以降を利用
  ※サーバー負荷が高い場合などは、複数台設置することをお勧めします。

クライアント数の目安

- ●～10,000台

管理サーバーのサーバースペック

- ●インテル Pentium 4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- ●2GB以上のメモリー
- ●1Gbpsのネットワークアダプター

ミラーサーバーのスペック

- ●インテル Pentium 4 互換プロセッサ3.0GHzと同等以上の性能を有したCPU
- ●4GB以上のメモリー
- ●1Gbpsのネットワークアダプター
- ●RAID 0構成のHDDまたはSSD

クライアントの接続間隔

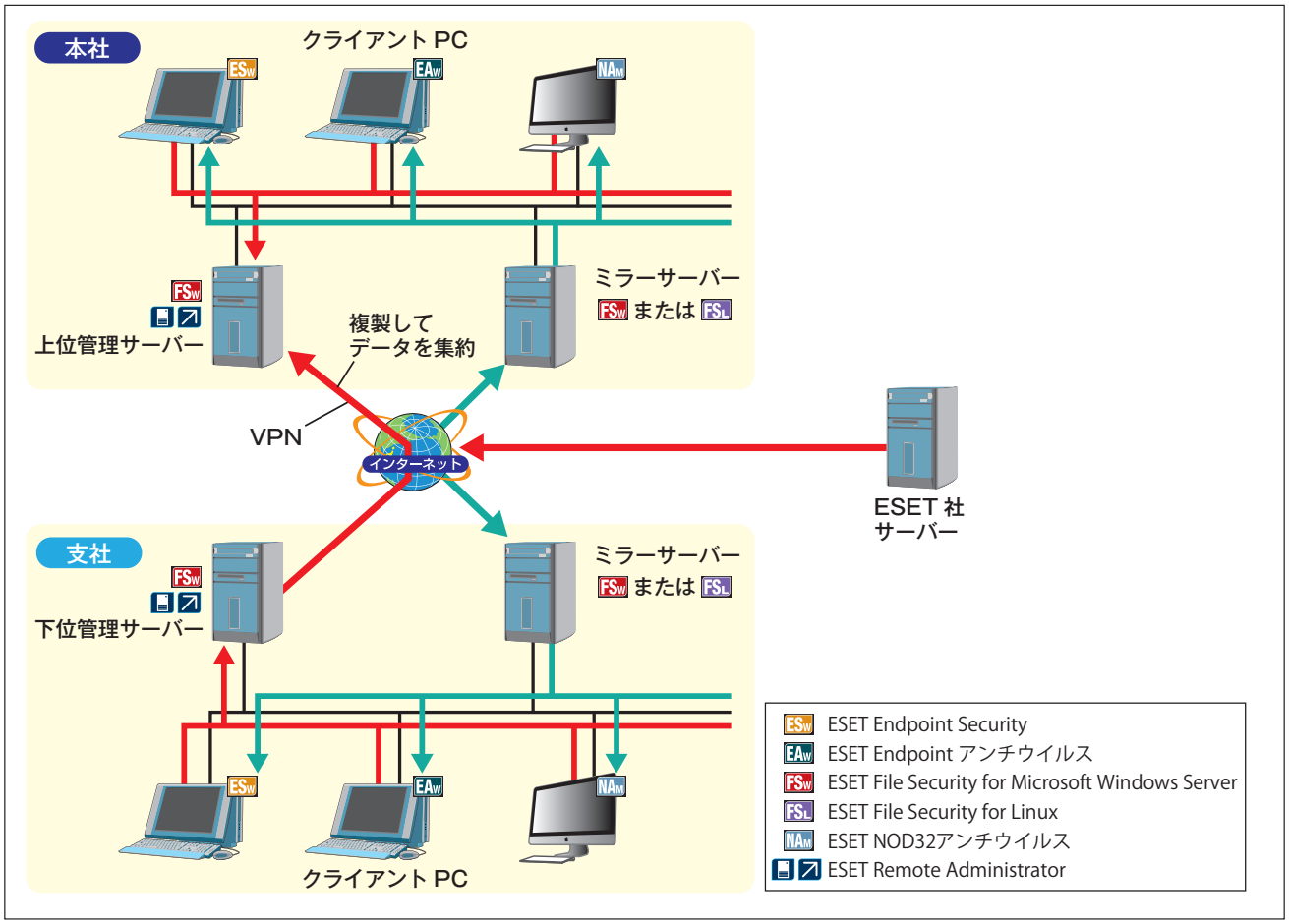
- ●管理サーバーへの接続間隔：30分
- ●ミラーサーバーへの接続間隔：60分

CAUTION

上記は、参考値です。管理可能なクライアントの総数などは、サーバースペックやネットワーク構成、サーバーの設定により異なります。

1.4.2.11　モデルケース10　10,000ユーザー以上複数拠点がある場合

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管理サーバーやミラーサーバーを設置します。このモデルケースでは、下位管理サーバーのデータを複製する機能を利用して、VPNなどを介して本社などに設置された上位管理サーバーへ集約します。



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

サーバースペック

●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のスペックを目安にする

クライアントの接続間隔

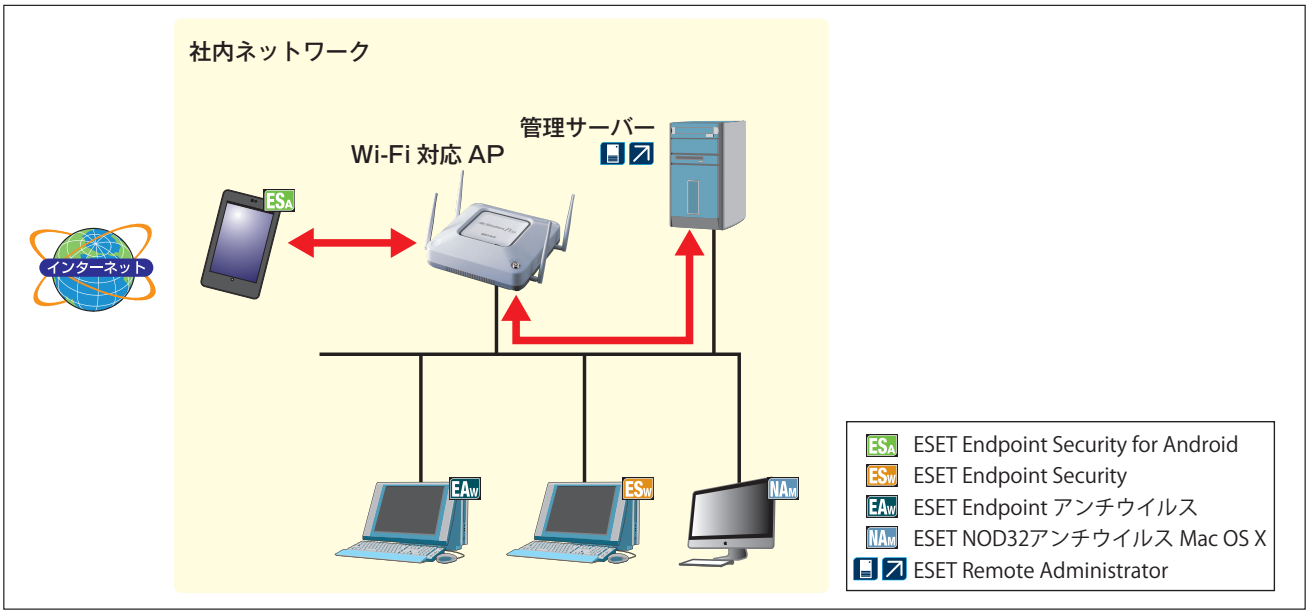
●設置する拠点や部署の規模に応じて、小規模や中規模の構成例を目安にする

1.4.3 Android端末の管理構成

ERAを利用してESET Endpoint Security for Androidを管理する場合、Wi-FiやVPN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。

1.4.3.1 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端末のWi-Fi接続機能を利用し社内ネットワークに接続します。

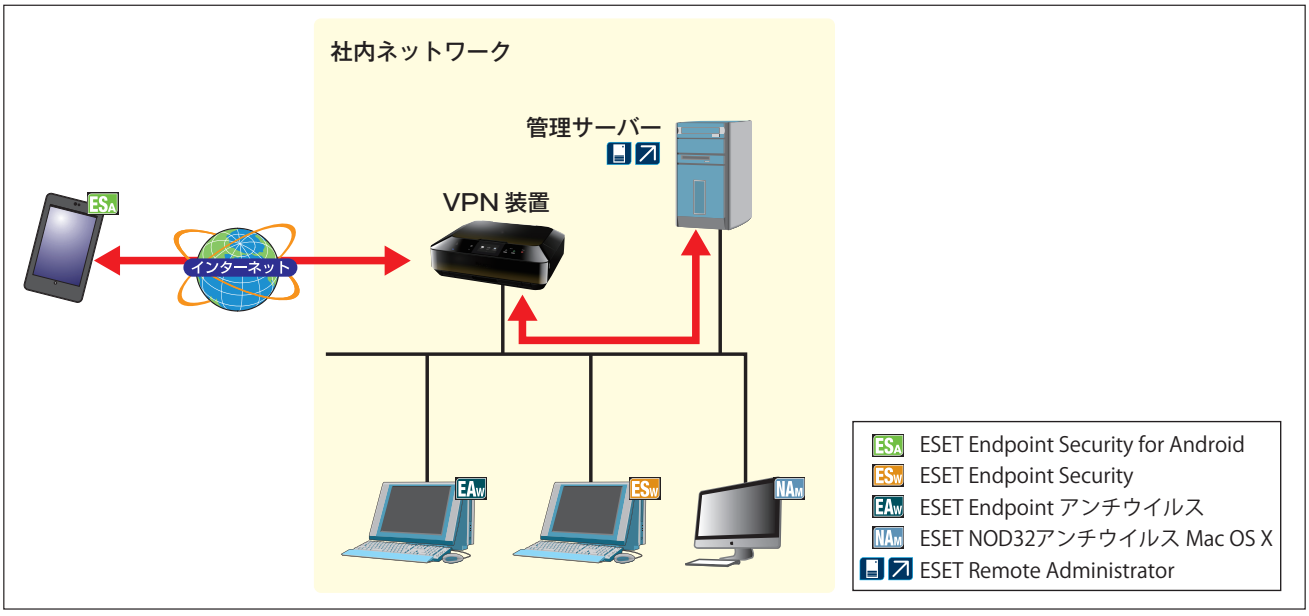


1.4.3.2 VPNを利用してERAに接続

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端末の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。

▸▸▸ POINT

VPN接続の設定については、Android端末と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 STEP3 ネットワーク環境の検討

ネットワーク環境の検討では、ESET ライセンス製品を導入することで発生する社内ネットワークの負荷の影響や、クライアントPCとサーバー間の通信経路を確認します。以下の点に着目して検討してください。

1.5.1 チェックポイント

1.5.1.1 ネットワーク負荷の検討

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、32ページをご参照ください。

1.5.1.2 インターネットへの通信経路の確認

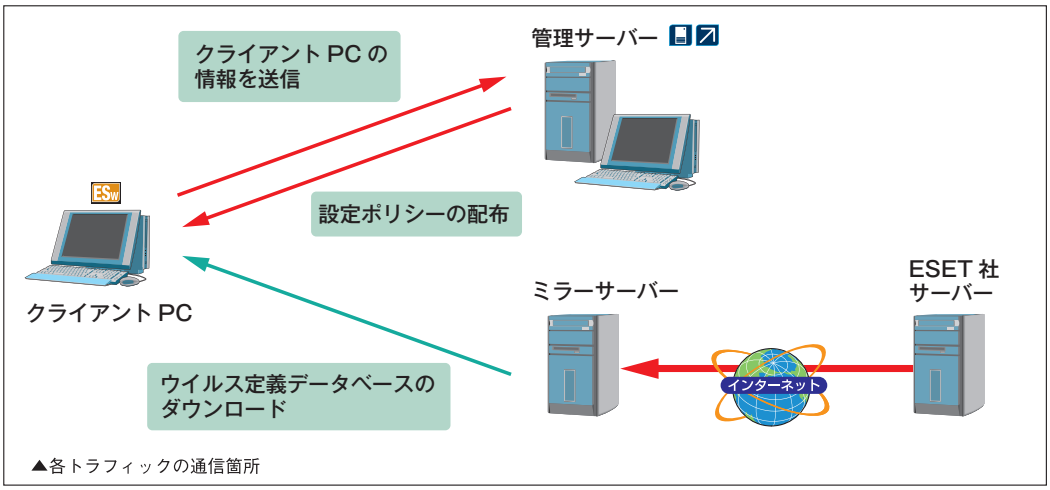
ミラーサーバーは、インターネットを利用してESET社のアップデートサーバーからウイルス定義データベースなどのアップデートファイルの入手を行います。インターネット接続の経路上にプロキシサーバーやファイアウォールが設置されていないかを確認し、ミラーサーバーの通信に影響がないかを確認します。

1.5.1.3 サーバーとクライアントPC間の通信経路の確認

管理サーバーとミラーサーバーは、定期的にクライアントPCとの通信を行います。管理サーバー/ミラーサーバーとクライアントPC間の通信経路を確認し、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

管理サーバーやミラーサーバーを導入すると、各種サーバーとクライアントPCとの間で定期的に通信が行われます。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。



▲各トラフィックの通信箇所

1.5.2.1 ①クライアント管理に伴うトラフィック

クライアントPCと管理サーバー間の通信です。定期的（既定値では10分間隔）にクライアントPCからログなどの情報が送信されます。また、管理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、以下の項目の設定を変更することによって制御することができます。

●ログレベル

管理サーバーがクライアントPCから取得するログの種類を減らすことによって、トラフィックを減少させます。

●定期検査のタイミング

クライアントPCに定期検査を設定している場合、検査を行う日時をグループ分けすることによってスキャンログを分散させます。

通信内容	サイズ	備考
ウイルスログ	数KB	クライアントが検出したウイルス情報です。
ファイアウォールログ （※ESET Endpoint Security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。
スキャンログ	数KB～数100KB	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	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。
モバイルログ	数KB	セキュリティ監査やスパム対策の情報です。
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KB	ESET製品の設定情報になります。
保護機能・保護状態	数KB	ESET製品の保護状態の情報になります。
システム情報	数KB	HW、SW、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。

CAUTION

ウイルスログ、スキャンログ、ファイアウォールログ、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。

1.5.2.2 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

クライアントPCとミラーサーバーなどのアップデートサーバー間の通信です。主にクライアントPC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、以下の項目の設定を変更することによって制御することができます。

●アップデートの間隔

クライアントPC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。ただし、アップデートの間隔を長く設定するほど、ウイルスに対するリスクが増える可能性があります。

●差分アップデート機能

ESET ライセンス製品は、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）を配信する事があります。これをベースアップデートと呼び、通常、年に3､4回の頻度でベースアップデートが実施されます。

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。

CAUTION

※ESET File Security for Microsoft Windows ServerまたはESET File Security for Linuxでミラーサーバーを構築した場合、差分アップデート機能はサポートされません。このため、ESET File Security for Microsoft Windows ServerまたはESET File Security for Linuxで構築したミラーサーバーからウイルス定義データベースのアップデートを実施した場合、ベースアップデート時には最大約40MBのファイルが配信されます。
※1週間程度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は、差分アップデート機能は適用されません。

●ミラーサーバー向けトラフィックの通信仕様

通信内容		サイズ	備考
定義データベース		数KB ～数百KB	ウイルス定義データベースになります。
ベースアップデート①	差分アップデート未適用時	数MB ～約15MB	年に3～4回程度配信される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です。 ※2012年6月2日の実績は約2.2MBとなります。
	差分アップデート適用時	約数KB ～約数百KB	
ベースアップデート②	差分アップデート未適用時	約40MB	年に1回程度配信される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です。 ※2012年3月27日の実績は約40MBとなります。
	差分アップデート適用時	約数KB ～約数百KB	
新モジュール追加		約1MB ～約3MB	不定期に新モジュールが追加される場合があります。 ※2012年3月14日の実績は約2MBとなります。

CAUTION

インストール後の初回アップデート時は、通常時と比較してネットワーク負荷が高くなることが予想されるので、ネットワーク障害が発生しないように考慮する必要があります。

1.6 STEP4 移行プランの検討

移行プランの検討では、既存プログラムの削除方法や導入するクライアント用プログラムの導入方法を検討し、具体的な移行プランを作成します。以下の点に着目して検討を行ってください。

1.6.1 チェックポイント

1.6.1.1 他社製プログラムのアンインストール方法の検討

現在利用している他社製セキュリティプログラムのアンインストール方法を確認します。一般的には、以下の方法でアンインストールできます。

●手動アンインストール
●他社製プログラムの管理サーバーからリモートアンインストール
●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

1.6.1.2 クライアント用プログラム導入方法の検討

クライアント用プログラムのインストール方法を、規模やネットワーク環境に合わせて検討してください。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。Windows用プログラムの場合は36ページ、Mac OS X用プログラムの場合は41ページ、Linux用プログラムの場合は44ページ、Android用プログラムの場合は45ページをご参照ください。

コラム

「コンポーネントの選択」機能について

ESET Endpoint Securityは、インストールするコンポーネント（機能）を選択する「コンポーネントの選択」機能を搭載しています。この機能を利用しクライアントPC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PCの負荷を軽減できるほか、設定ミスなどによる不要なトラブルを防止できます。詳細な手順については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

選択可能なコンポーネント一覧

●電子メールクライアント保護　●迷惑メール対策機能　●ドキュメント保護機能
●プロトコルフィルタ　●ファイアウォール機能　●ミラー機能

※ ESET Endpoint アンチウイルスまたはESET File Security for Microsoft Windows Serverは、インストールするコンポーネントの選択は行えません。
※ コンポーネントの選択は、インストール時には手動で選択できるほか、インストールコマンドの引数に“REMOVE=（機能名）”を付けて実行することもできます。

1.6.1.3 移行プランの作成

具体的な移行プランを作成します。移行期間にセキュリティレベルを低下させることを避け、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推奨しています。以下に弊社で作成したサンプルプランを掲載しておきますので参考にしてください。

●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
1. サーバー機器、ESET ライセンス製品の手配	→			
2. サーバーの構築		→		
3. サーバーの設置		▲		
4. 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）			→	
5. 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）			▲	
6.ESET 製品の本番運用		→	→	→
※既存プログラムと ESET 製品の共存期間		↔	↔	

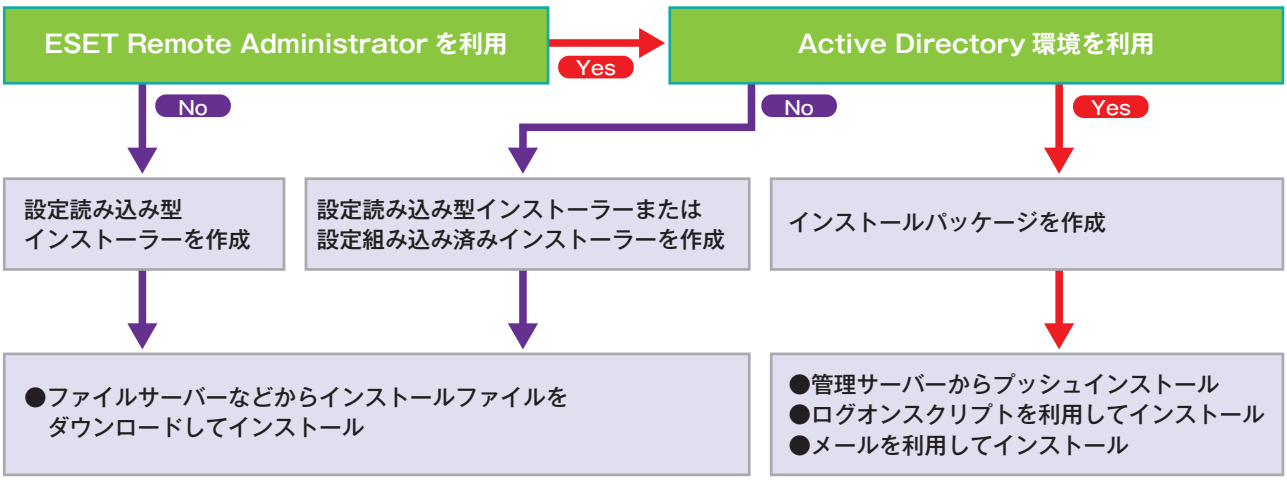
1.6.2 クライアント用プログラム導入方法 ～ Windows編

ESETセキュリティ製品では、クライアント用プログラムのインストールに際して、お客さまの多様な環境に応じるように、いくつかの方法を用意しています。本節では、クライアント用プログラムの各種インストール方法の概要および導入の流れを説明します。

1.6.2.1 診断フロー

Windows用プログラムの導入方法は、クライアントPCの設置環境や導入台数、運用方法などに応じて複数の方法が用意されています。以下の診断フローを参考に環境に合わせた導入方法を検討してください。

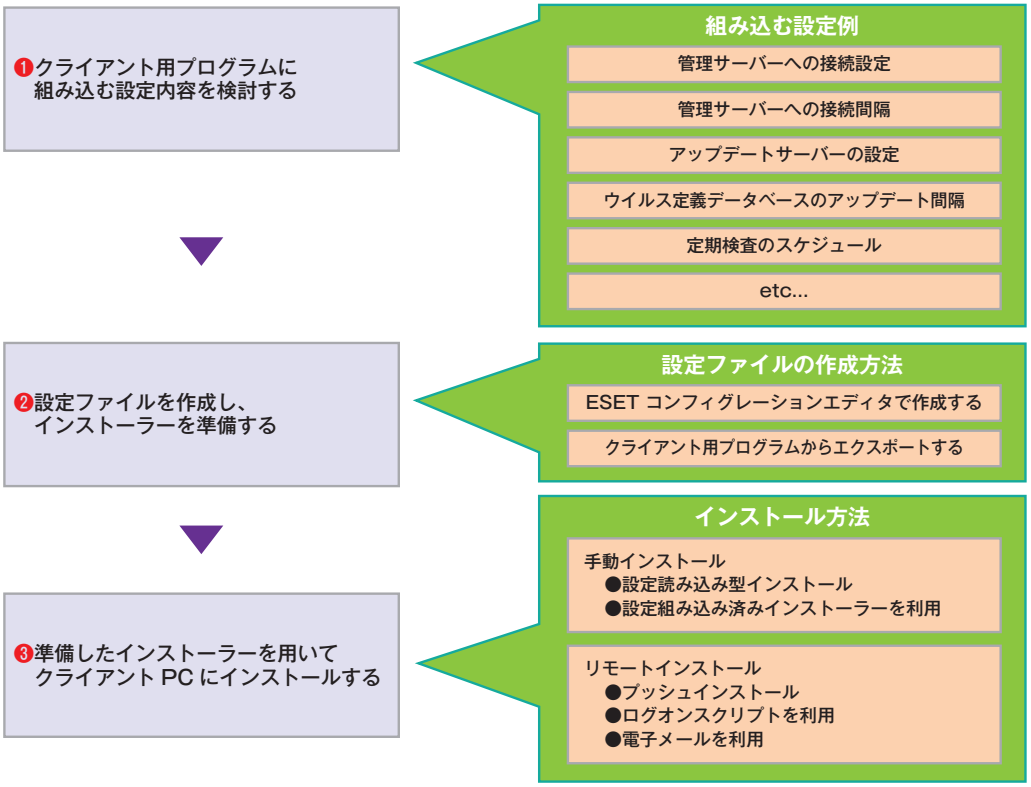
●クライアント展開の診断フロー



1.6.2.2 導入の流れ

設定組み込み済みインストーラーを利用したインストールまたは設定読み込み型インストールを実施する場合は、最初に組み込む設定内容を検討します。次に、設定組み込み済みイントーラーまたは設定ファイルの作成を行い、利用環境に応じたインストール方法でクライアント用プログラムをインストールします。

全クライアント共通の設定でクライアント用プログラムをインストールするときの導入手順



クライアント用プログラム設定のポイント

クライアント用プログラムは、コンピューターの使用環境に応じた設定を施すことによって、より安全かつ効率的な運用が行えます。

設定ファイルの作成

クライアント用プログラムには、サーバーへの接続設定やコンピューターの検査設定など、様々な設定が施されています。そして、これらの設定はファイルとして保存されており、この設定ファイルをカスタマイズすることによって、多数のコンピューターがあるような環境において、効率的な管理・運用が可能なほか、クライアント用プログラムのインストールも容易に行えます。

設定ファイルは、ESET Remote Administrator（ERA）で作成できるほか、クライアント用プログラムでも作成できます。作成方法については、それぞれのユーザーズマニュアルをご参照ください。

インストール方法

クライアント用プログラムのインストールにあたっては、インストールの実施方法がいくつか用意されているので、クライアントPCの設置環境や導入台数、運用方法などに応じて選択してください。以降に、インストーラーの違いによるインストール方法およびリモートによるインストールの方法を記載していますので、参考にしてください。

●手動インストール

インストール方法	必要なファイル	特徴
インストーラー(.msi)を利用	●インストーラー(.msi)	製品パッケージに付属するインストーラーをそのまま利用してインストールを行います。サーバークライアント用プログラムの各種設定は、すべて既定値が利用されるので、管理サーバーやミラーサーバーを設置する場合は、それらへの接続設定など最低限必要となる設定を、各自プログラムインストール後に行う必要があります。
設定読み込み型インストール	●インストーラー(.msi) ●設定ファイル ●バッチファイル	クライアント用プログラムの設定ファイルを事前に作成し、その設定ファイルとインストーラー(.msi)を組み合わせてインストールを行います。設定ファイルの内容をインストール時に適用できるので、インストール後の設定が不要または最小限にすることができます。また、設定ファイルの作成に、クライアント用プログラムからのエクスポートを利用した場合、ESET Remote Administrator(ERA)を利用しなくても、このインストール方法を利用できます。実際のインストールには、インストーラー(.msi)と設定ファイルの他にインストール用のバッチファイルが必要になります。なお、ESET Endpoint Securityをインストールする場合は、インストールコマンドの引数に"REMOVE=機能名"を付けて実行することでインストールするコンポーネントを選択できます。詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。
設定組み込み済みインストーラーを利用	●設定組み込み済みインストーラー ●バッチファイル(サイレントインストールを行う場合)	インストーラー(.msi)に独自の設定を施したインストーラー(設定組み込み済みインストーラー)を作成し、それを利用してインストールを行います。設定ファイルの内容をインストール時に適用できるので、インストール後の設定が不要または最小限にすることができます。設定組み込み済みインストーラーの作成には、ERA を利用する必要があります。なお、インストールウィザードを表示しないサイレントインストールを行うには、インストール用のバッチファイルが必要になります。なお、ESET Endpoint Securityをインストールする場合は、バッチファイルに記載するインストールコマンドの引数に "REMOVE＝（機能名）"を付けて実行することで必要なコンポーネントのみをインストールすることができます。詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

※各インストーラーなどは、リムーバブルメディアや共有フォルダーに保存し、各クライアントPC上にコピーして利用します。

●リモートインストール

インストール方法	必要なファイル	特徴
プッシュインストール	●インストールパッケージ	ERAを利用し、リモートでクライアントPCにログオンしてインストールを行う方法です。1度の操作で複数のクライアントPCに対して操作を実行できるので、インストール効率は高くなります。ただし、この方法でインストールを実施するには、対象クライアントPCの環境に関して各種条件があります。
ログオンスクリプトを利用	●インストールパッケージ	Active Directoryのドメインログオン時にログオンスクリプトを利用して自動インストールを行う方法です。インストールが自動実行されるので、インストール効率は高くなります。ただしこの方法は、Active Directory環境でネットワークを構築している場合にのみ利用できます。
電子メールを利用	●インストールパッケージ	インストールパッケージの一部を電子メールに添付してクライアントPCに送り、ユーザーがそれを実行し、インストールを開始する方法です。インストールパッケージ本体をERAから取得するため、クライアントPCとERAが通信できる必要があります。

※インストールパッケージはERAを利用して作成します。各クライアントPCに適用する内容およびインストール時のオプションを設定することができます。また、ESET Endpoint Securityをインストールする場合は、必要なコンポーネントのみをインストールするインストールパッケージを作成できます。詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

● Active Directory 環境とワークグループ環境のそれぞれで推奨されるインストール方法

インストール方法		Active Directory環境	ワークグループ環境
手動インストール	インストーラー (.msi)を利用	○	○
	設定読み込み型インストール	○	○
	設定組み込み済みインストーラーを利用	○	○
リモートインストール	プッシュインストール	○	△※ 1
	ログオンスクリプトを利用	○	×
	電子メールを利用	○	△※ 2

※1 インストール先のクライアントPCにログオンするためのユーザー名とパスワードが必要。クライアントPCごとにこれらが異なっている場合は、各々に対して入力する必要があります。

※2 あらかじめ指定したユーザー名とパスワードを利用するため、クライアントPCごとの管理者権限をもつユーザー名とパスワードがすべて同一でない限り、お勧めできません。

1.6.2.3　リモートインストール利用時の条件

プッシュインストール、ログオンスクリプトを利用したインストール、電子メールを利用したインストールでは、次の利用条件を満たしている必要があります。インストール作業を実施する前に環境が整っているか必ずご確認ください。なお、リモートインストールの実施の具体的な手順については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

①クライアントPCとERASがLAN経由で通信が可能なこと

②クライアントPCがActive Directory環境のメンバの場合、ドメインアドミニストレーター権限を持ったアカウントが利用可能であること
※Active Directory環境の場合、ドメインアドミニストレーター権限のパスワードが空白ではないこと
※プッシュインストール実行時にアカウント名とパスワードの指定が必要となります。

③クライアントPCがワークグループ環境のメンバの場合、各クライアントPCの管理者権限を持ったアカウントが利用可能であること
※管理者権限を持ったアカウントのパスワードが空白ではないこと
※プッシュインストール実行時にアカウント名とパスワードの指定が必要となります。

④クライアントPCのOSがWindows 2000/XP/Vista/7、Windows Server 2003/2008であること

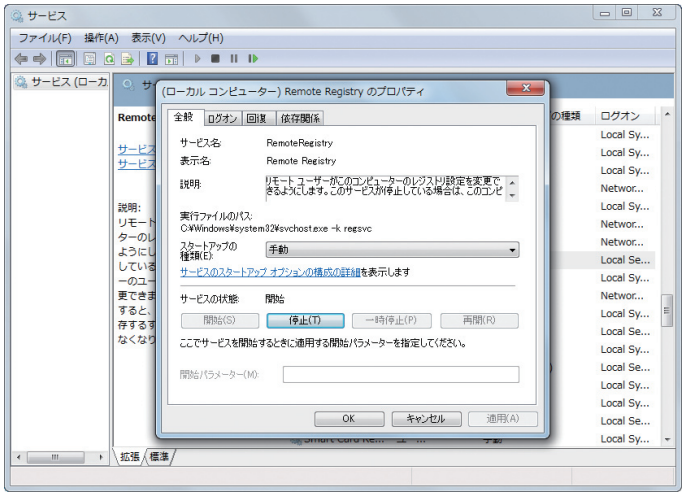
⑤クライアントPC側の通信ポートが通信可能な状態になっていること

●リモートインストール時に利用されるクライアントPCの通信ポート

ポート番号／プロトコル	備考
137/TCP,UDP	NetBios 名前サービス
138/UDP	NetBios データグラムサービス
139/TCP	NetBios セッションサービス
445/TCP,UDP	SMB ダイレクトホスティングサービス

⑥クライアントPCで「Remote Registry」サービスが開始されていること

Remote Registryサービスが開始されているかどうかは、[スタート] メニュー→ [コントロールパネル] → [システムとセキュリティ] → [管理ツール] → [サービス] で確認できます。Remote Registryサービスが開始されていない場合は、[Remote Registry] をダブルクリックし、[全般] タブにある [開始] ボタンをクリックしてください。



⑦クライアントPCの共有フォルダーおよびプリンター共有が有効になっていること

⑧クライアントPCのフォルダーオプションで「簡易ファイルの共有を使用する（推奨）」が無効になっていること

※環境によって設定が異なりますので、必ずご確認ください。

⑨Windows Vista以降のOS（Windows Server 2008）にリモートインストールする場合、ERASは管理者権限を持つアカウントで動作させること

※Active Directory環境の場合は、ドメインアドミニストレーター権限を持ったアカウント、ワークグループ環境の場合は、コンピューターの管理者権限を持ったアカウントで動作させてください。

1.6.3 クライアント用プログラム導入方法 ～ Mac OS X編

ESET NOD32アンチウイルス は、お客さまの多様な環境に応じるように、いくつかのインストール方法を用意しています。ここでは、ESET NOD32アンチウイルスの各種インストール方法の概要および導入の流れを説明します。

1.6.3.1 インストール方法

ESET NOD32アンチウイルスのインストール方法は、以下の通りです。インストールにあたっては、クライアントPCの設置環境や導入台数、運用方法などに応じて選択してください。

●手動インストール

インストール方法	必要なファイル	特徴
付属のインストーラー(.dmg)を利用	インストーラー(.dmg)	製品パッケージに付属するインストーラー(.dmg)をそのまま利用してインストールを行います。カスタムインストールを行うことで、管理サーバーやミラーサーバーへの接続設定などを行えます。
設定組み込み済みインストーラー(.pkg)を利用	設定組み込み済みインストーラー(.pkg)	アップデートサーバーへの接続設定や管理サーバーへの接続設定、権限ユーザーの設定などを行った設定済みパッケージ(.pkg)を利用してインストールを行います。設定組み込み済みインストーラー(.pkg)は、付属のインストーラー(.dmg)を利用して作成します。

●リモートインストール

インストール方法	必要なファイル	特徴
プッシュインストール	インストールパッケージ	ERAを利用し、リモートでクライアントPCにログオンしてインストールを行う方法です。1度の操作で複数のクライアントPCに対して操作を実行できるので、インストール効率は高くなります。ただし、この方法でインストールを実施するには、対象クライアントPCの環境に関して各種条件があります。
Apple Remote Desktopを利用	設定組み込み済みインストーラー(.pkg)	Apple社のリモート管理ソフト「Apple Remote Desktop」などを利用して、リモートインストールを行います。インストールには、付属のインストーラー(.dmg)で作成した設定組み込み済みインストーラー(.pkg)が必要です。アップデートサーバーへの接続設定や管理サーバーへの接続設定、権限ユーザーの設定などを事前に行っておくことができます。

1.6.3.2 手動インストールする場合の導入の流れ

ESET NOD32アンチウイルスを手動でインストールする場合は、以下の流れで行います。他社製のセキュリティプログラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET NOD32アンチウイルスのインストールを実施してください。

STEP1 他社製セキュリティプログラムのアンインストール

他社製のセキュリティプログラムを利用している場合は、そのプログラムのアンインストールを行います。

↓

STEP2 設定組み込み済みインストーラーの作成（必要に応じて）

付属のインストーラー(.dmg)を利用して、アップデートサーバーへの接続設定や管理サーバーへの接続設定、権限ユーザーの設定などを行った設定組み込み済みインストーラー(.pkg)を作成します。

↓

STEP3 イントール作業の実施

STEP2で作成した設定組み込み済みインストーラー(.pkg)や付属のインストーラー(.dmg)を利用して、各クライアントが手動でインストールします。

↓

STEP4 設定ファイルの配布

ERAを利用して各種設定をクライアントPCに配布するか、ESET NOD32アンチウイルスからエクスポートした設定ファイルを利用して、クライアントPCの各種設定を変更します。

1.6.3.3 リモートインストールする場合の導入の流れ

ERAは、SSH経由でESET NOD32アンチウイルスをプッシュインストールできます。プッシュインストールを行う場合は、以下の流れで行います。

STEP1 他社製セキュリティプログラムのアンインストール

他社製のセキュリティプログラムを利用している場合は、そのプログラムのアンインストールを行います。

↓

STEP2 クライアントPCの設定

クライアントPCのリモートログインを有効に設定し、SSH経由で外部のコンピューターからリモート接続できるように設定を変更します。詳しい設定については、OS付属の取り扱い説明書をご参照ください。

↓

STEP3 インストール作業の実施

ERAを利用してクライアントPCにSSH経由のプッシュインストールを実施します。詳細な手順については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

↓

STEP4 設定ファイルの配布

ERAを利用して、各種設定をクライアントPCに配布するか、ESET NOD32アンチウイルスからエクスポートした設定ファイルを利用し、クライアントPCの各種設定を変更します。

CAUTION

ERAからプッシュインストールを行うには、以下の条件を満たしている必要があります。
・クライアントPCは、SSHを経由したリモートログインが行えるように設定されている必要があります。
・ERAがリモートログインに利用するSSHアカウントは、管理者権限のアカウントである必要があります。

▸▸▸ POINT

ESET NOD32アンチウイルスは、Apple社が販売しているMac OS X用のリモート管理ソフト「Apple Remote Desktop」を利用したリモートインストールも行えます。詳細は、ESET NOD32アンチウイルス Mac OS Xのユーザーズマニュアルをご参照ください。

1.6.4 クライアント用プログラムの導入方法～ Linux編

ここでは、ESET File Security for Linuxのインストール方法の概要および導入の流れを説明します。

1.6.4.1 インストール方法

ESET File Security for Linuxのインストール方法は、以下の通りです。

●手動インストール

インストール方法	必要なファイル	特徴
インストーラー(.bin)を利用	インストーラー(.bin)	弊社ユーザーズサイトからダウンロードしたインストーラー(.bin)を利用して、コマンドラインで作業を行います。インストール作業は、root権限(スーパーユーザー)で行う必要があります。また、ソフトウェアの各種設定は、インストール作業完了後にすべて手動で行います。

1.6.4.2 手動インストールする場合の導入の流れ

ESET File Security for Linuxを手動でインストールする場合は、以下の流れで行います。他社製のセキュリティプログラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET File Security for Linuxのインストールを実施してください。

STEP1 他社製セキュリティプログラムのアンインストール

他社製のセキュリティプログラムを利用している場合は、そのプログラムのアンインストールを行います。

↓

STEP2 インストール作業の実施

インストーラー(.bin)を利用して、手動でインストールを行います。

↓

STEP3 各種設定の実施

ESET File Security for Linuxの各種設定を管理している「esets.cfg」ファイルの編集を行って各種設定を行います。

1.6.5　クライアント用プログラムの導入方法～ Android編

ESET Endpoint Security for Androidは、お客さまの多様な環境に応じるように、いくつかのインストール方法を用意しています。ここでは、ESET Endpoint Security for Androidの各種インストール方法の概要および導入の流れを説明します。

1.6.5.1　インストール方法

ESET File Security for Androidのインストール方法は、以下の通りです。インストールの際は、端末の設置環境や導入台数、運用方法などに応じて選択してください。

●手動インストール

インストール方法	必要なファイル	特徴
インストーラー（.apk）を利用	インストーラー（.apk）	弊社ユーザーズサイトからダウンロードしたインストーラー(.apk)を利用して、インストールを行います。ソフトウェアの各種設定は、インストール作業完了後に手動で行います。
設定読み込み型インストール	インストーラー（.apk） 設定ファイル（xml）	設定ファイルを事前にERA付属のESET コンフィグレーションエディターで作成し、その設定ファイルとインストーラー(.apk)を組み合わせてインストールを行います。設定ファイルの内容をインストール時に適用できるので、インストール後の設定を最小限にすることができます。設定ファイルは、「settings.xml」というファイル名で保存する必要があります。また、インストールを行うときは、設定ファイルをAndroid端末の「/mnt/sdcard」フォルダーにコピーしてインストール作業を実施します。
Link Generator を利用	インストーラー（.apk）	設定ファイルをERAで事前に作成し、ESET社が提供するLink Generatorで作成したリンクとインストーラー(.apk)を組み合わせてインストールを行います。インストーラー(.apk)を利用してインストールした後、対象とするAndroid端末に配布したリンクをタップすることで、Android端末が自動的にERAに接続し、設定が反映されるので、インストール後の設定を最小限にすることができます。

1.6.5.2　設定読み込み型インストールする場合の導入の流れ

ESET Endpoint Security for Androidを設定読み込み型インストールする場合を説明します。他社製のセキュリティプログラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET Endpoint Security for Androidのインストールを実施してください。

設定ファイルの作成はERAで行います。ESET コンフィグレーションエディターを起動して、[製品フィルタ] で [ESET Endpoint Security for Android] を選択し、必要な設定を行ってください。設定後、ファイル名を「settings.xml」でセーブし、Android端末の「/mnt/sdcard」フォルダーにコピーしてインストール作業を実施します。

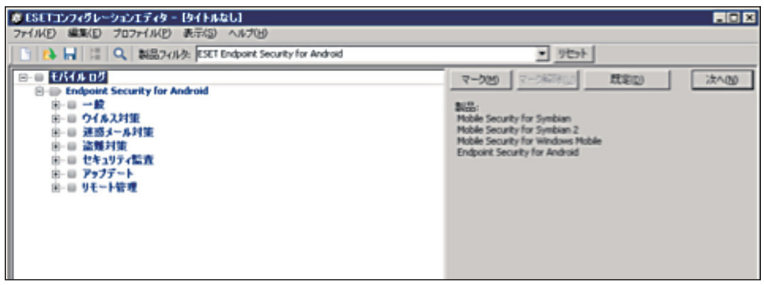
ここから、設定ファイルの作成手順を説明します。

1 [スタート] ボタン＞[すべてのプログラム] ＞ [ESET] ＞ [ESET Remote Administrator Console] ＞ [ESET コンフィグレーションエディタ] をクリックしてESET コンフィグレーションエディターを起動します。

2 

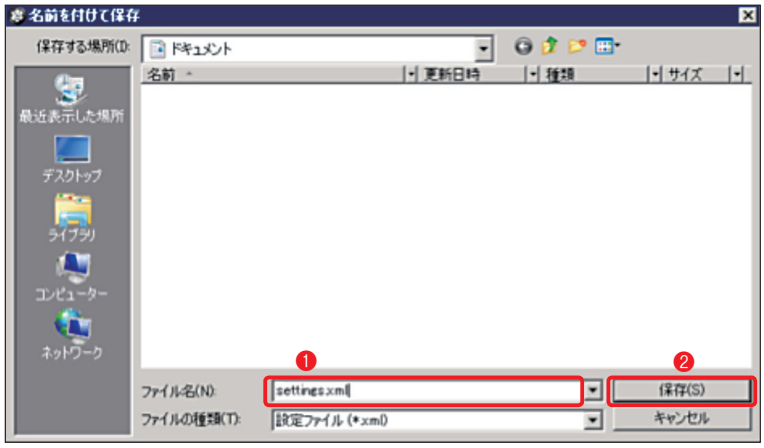
[製品フィルタ] で「ESET Endpoint Security for Android」を選択します。

3



［モバイルログ］＞［Endpoint Security for Android］で必要な設定を行います。

4



［ファイル］＞［名前を付けて保存］をクリックして❶ファイル名に「settings.xml」と入力して❷［保存］をクリックします。

この設定ファイルをAndroid端末の「/mnt/sdcard」フォルダーにコピーしてインストール作業を実施します。

設定読み込み型インストールをする場合は、以下の流れとなります。

STEP1　他社セキュリティプログラムのアンインストール

他社製のセキュリティプログラムを利用している場合は、そのプログラムのアンインストールを行います。

↓

STEP2　設定ファイルの作成

ERA 付属の ESET コンフィグレーションエディターを利用して、アップデートサーバーへの接続設定や管理サーバーへの接続設定などを行った設定ファイルを作成します。設定ファイルは、「settings.xml」というファイル名で保存します。

↓

STEP3　インストール作業の実施

STEP2で作成した設定ファイルをAndroid端末の「/mnt/sdcard」フォルダーにコピーしてインストーラー(.apk)を利用して手動でインストールします。

↓

STEP4　各種設定の実施

ERAを利用して設定できない設定を手動で変更します。

▸▸▸ POINT

設定読み込み型インストールで、ERA付属のESET コンフィグレーションエディターを利用して設定できない項目は、[信頼するSIMカードを定義]、[ESETをデバイス管理者として設定]、[管理者連絡先の定義]です。

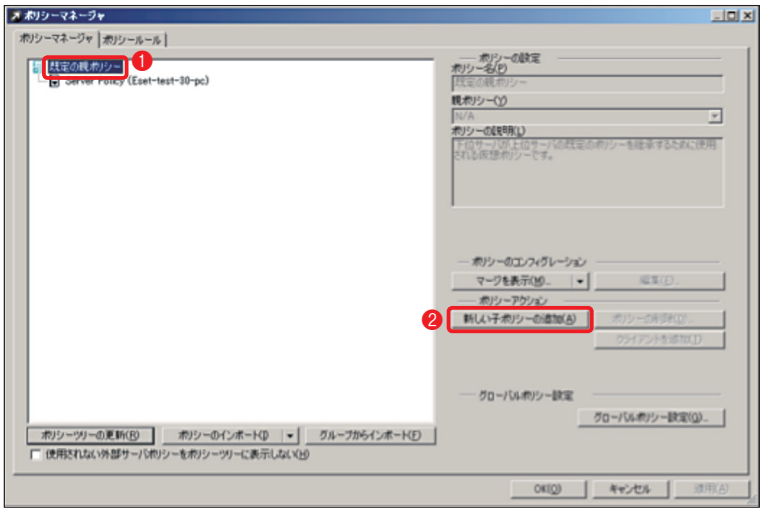
1.6.5.3 Link Generatorを利用してインストールする場合の導入の流れ

Link Generatorとは、ESET社が提供しているコマンドラインプログラムです。Link Generatorを利用すると、ERAへ接続するためのリンクが生成されます。ERAのポリシーマネージャと組み合わせて利用することで、ESET Endpoint Security for Androidをインストール後にリンクをクリックすると同時に設定を反映させることが可能です。
Link Generatorは弊社ユーザーズサイトからダウンロードしてください。
ここでは、Link Generatorを利用してESET Endpoint Security for Androidをインストールする場合を説明します。
他社製のセキュリティプログラムを利用している場合は、必ず、そのプログラムのアンインストールを行い、ESET Endpoint Security for Androidのインストールを実施してください。

ここからLink Generatorを利用したESET Endpoint Security for Androidのインストールから初期設定反映までの設定例を説明します。お客さまのご利用の環境に合わせて設定を変更してください。
ここではポリシーを二つ作成して、ERAに初めて接続したときに割り当てるポリシーと二回目以降にERAに接続したときに割り当てるポリシーの作成方法を説明します。

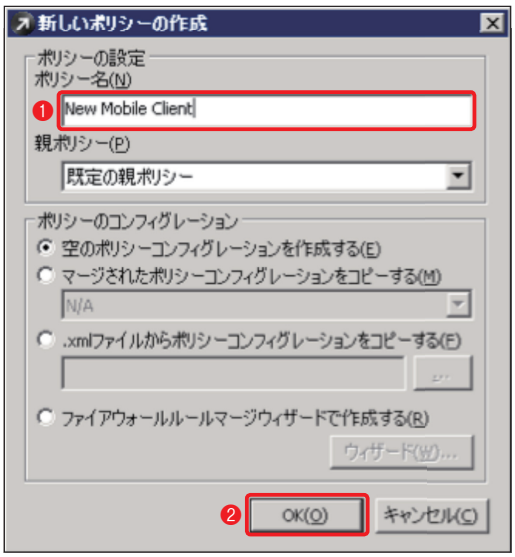
1 ERACを起動して「ツール」→「ポリシーマネージャ」をクリックします。

2



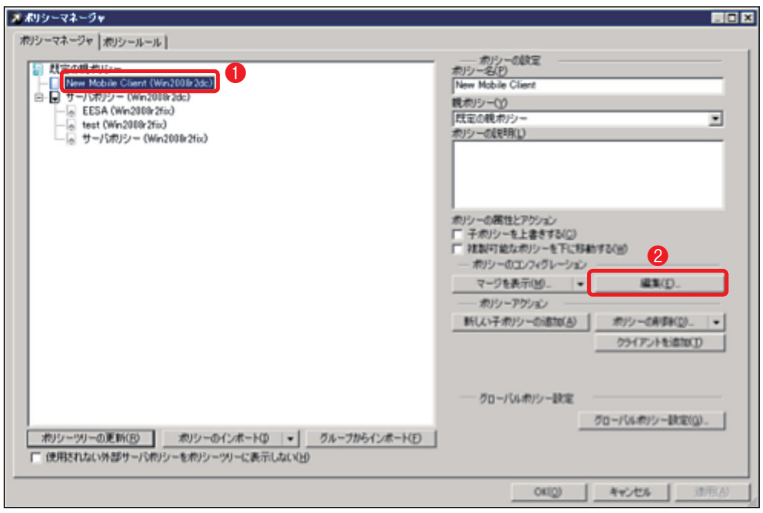
❶「既定の親ポリシー」を選択して❷「新しい子ポリシーの追加」をクリックします。

3



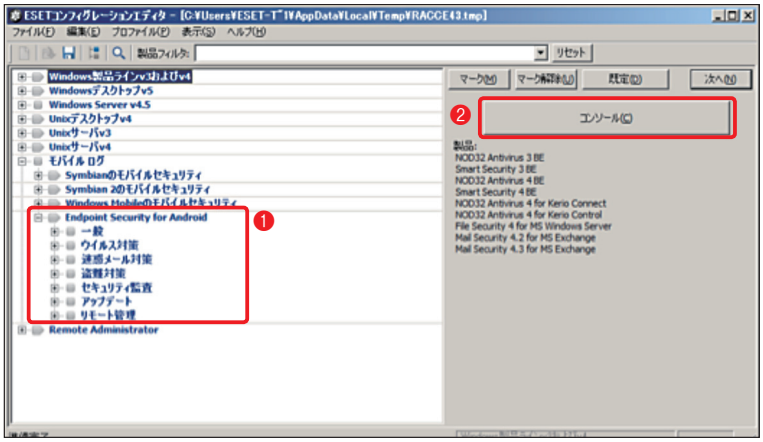
「新しいポリシーを作成」画面で❶任意のポリシー名を入力して❷「OK」をクリックします。

4



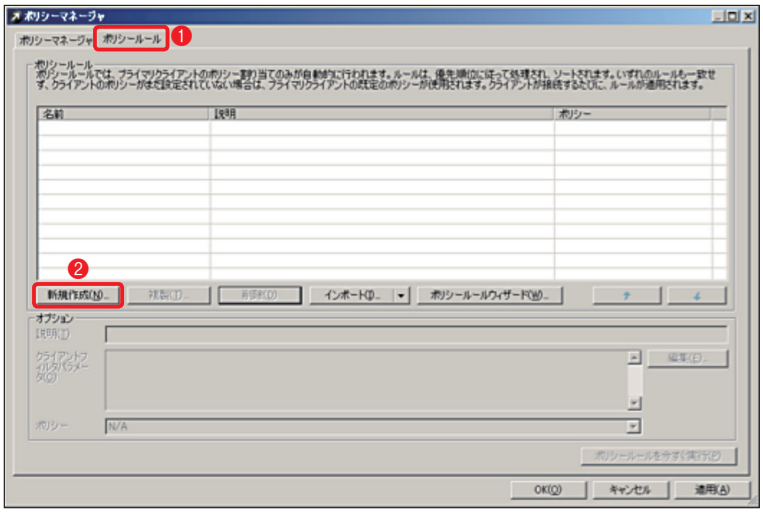
❶手順3で作成したポリシー名を選択して、❷「編集」をクリックします。

5



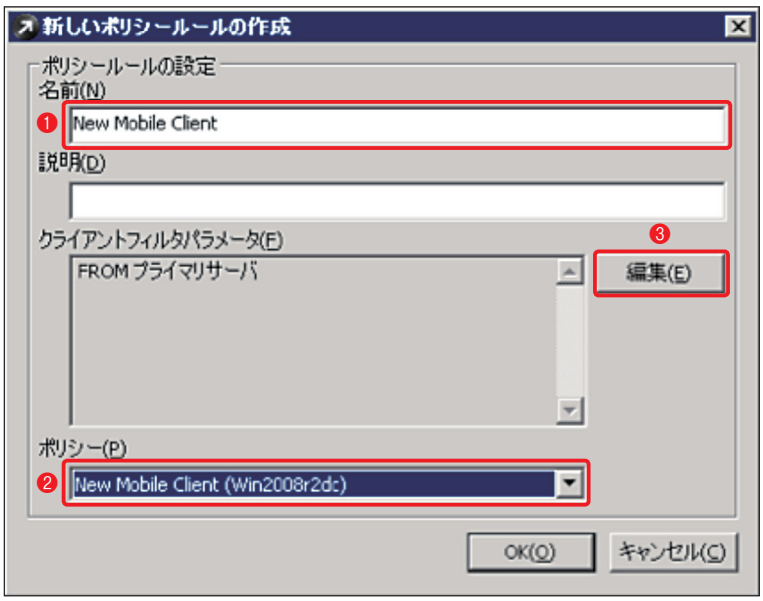
「ESETコンフィグレーションエディタ」の❶「モバイルログ」→「Endpoint Security for Android」の必要な部分の設定値を入力し、設定が終了したら❷コンソールをクリックし、「はい」をクリックします。

6



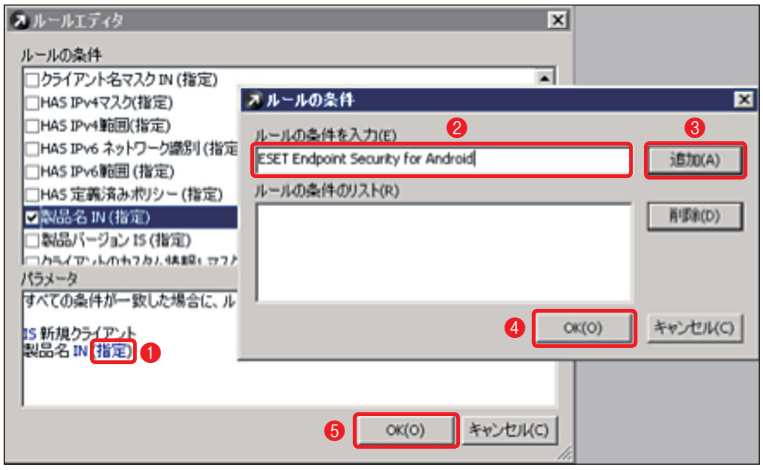
「ポリシーマネージャ」の❶「ポリシールール」タグをクリックし、❷「新規作成」をクリックします。

7



「新しいポリシールールの作成」画面で❶「名前」に任意の名前を入力して❷「ポリシー」で手順3で作成したポリシーを選択して❸「編集」をクリックします。

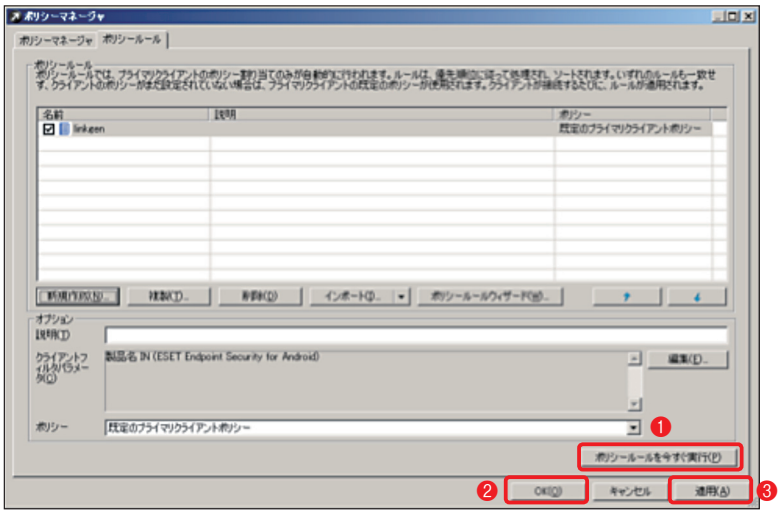
8



「ルールエディタ」画面で［ルールの条件］で［IS 新規クライアント］、［製品名IN（指定）］にチェックを入れ、❶「指定」をクリックします。［ルールの条件］画面が開きますので❷「ESET Endpoint Security for Android」と入力して❸「追加」、❹「OK」、❺「OK」とクリックします。

※［IS 新規クライアント］にチェックを入れるとERAに初めて接続したクライアントにのみポリシーが適用されます。

9



❶「ポリシールールを今すぐ実行」をクリックし確認画面が出てくるので［はい］、［OK］をクリックして、❷「適用」、❸［OK］をクリックします。

10 手順2から9を繰り返します。その際、手順3で別のポリシー名を入力し、手順5で二回目以降に割り当てるポリシーを作成します。二回目以降に割り当てるポリシーに対して、手順8で［製品名IN（指定）］にだけチェックを入れます。

次にLink Generatorの使用方法を説明します。
コマンドプロンプトを起動させ、Link Generatorの実行ファイル「linkGen.exe」のあるフォルダーに移動して以下のコマンドを実行させます。

linkGen.exe ＜ERA の IP アドレス＞ ＜ERA に接続するポート番号＞ ＜TRUE/FALSE ＞ ＜ERA へ接続するためのパスワード＞

＜TRUE/FALSE＞：「TRUE」を入力すると自動的に挿入しているSIMカードが信頼するSIMカードとして登録されます。「FALSE」を入力した場合、信頼するSIMカードに自動的に登録されませんので、手動で信頼するSIMカードを入力してください。
＜ERAへ接続するためのパスワード＞：ERAへとの接続にパスワード認証を有効にしている場合のみ入力してください。

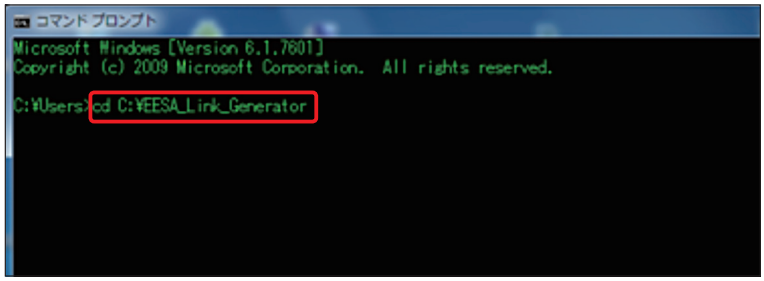
入力例

ERAのIPアドレスが192.168.xxx.xxx、ポート：2222、信頼するSIMカードを挿入してERAにクライアントが接続する時にパスワード認証が「password」の場合の以下のようになります。

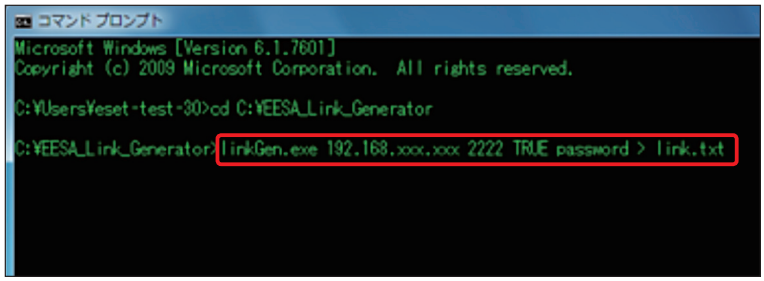
linkGen.exe 192.168.xxx.xxx 2222 TRUE password

以下、Ling GeneratorをCドライブの「EESA_Link_Generator」フォルダー内に置いて、条件は上記の場合の使用方法について説明します。

1 [スタート] ボタン→ [すべてのプログラム] → [アクセサリ] からコマンドプロンプトを起動します。

2 

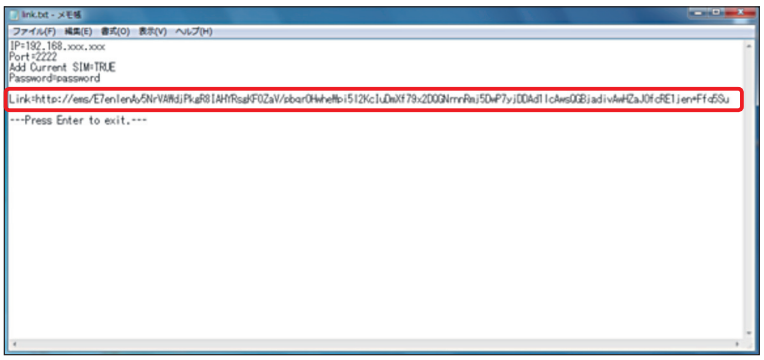
「cd C: ¥EESA_Link_Generator」と入力してEnterキーを押下します。
「EESA_Link_Generator」フォルダーの中にLink Generatorのプログラム「linkGen.exe」があります。

3 

「linkGen.exe 192.168.xxx.xxx 2222 TRUE password ＞ link.txt」と入力してEnterキーを二回押します。

4 「EESA_Link_Generator」フォルダーにlink.txtが作成されます。

5



link.txtを開いて内容を確認します。Linkのhttp://からが今回作成したリンクとなります。
メールでリンクを配布する場合は６へ、Webでリンクを公開する場合は７に進んでください。

作成したリンクの例

```
http://ems/E7enlenAy5NrVAWdjPkgR8lAHYRsgKF0ZaV/pbqrOHwheWpi5l2KcluDmXf79x2DQGNrnnRmj5DwP7yjDDAd1lcAwsQGBjadivAwHZaJOfcRE1jen+Ffq5Su
```

6

メールでリンクを配布する場合は、http://からリンクをすべてコピーし、本文に貼り付けてください。

ESET Endpoint Security for Androidをインストール後、メールで配布されたリンクをタップします。
リンクをタップした後、[アプリケーションを選択] 画面が表示されますので、「ESET Endpoint Security」を選択するとAndroid端末が自動的にERAに接続し、設定が反映されます。
※タップしてから設定の反映までしばらくかかる場合があります。

7 作成したリンクをWebで公開する場合、以下のHTMLタグを公開するHTMLファイルに挿入してください。

```
<a href="ems:< 作成したリンクの http://ems/ 以降の部分 >"> 任意の文字 </a>
```

記述例

```
<a href="ems:E7enlenAy5NrVAWdjPkgR8lAHYRsgKF0ZaV/pbqrOHwheWpi5l2KcluDmXf79x2DQGNrnnRmj5DwP7yjDDAd1lcAwsQGBjadivAwHZaJOfcRE1jen+Ffq5Su"> 設定はこちら </a>
```

上記の記述例の場合、ESET Endpoint Security for Androidをインストール後、Android端末のブラウザーで作成したWebページを開いて、[設定はこちら] をタップするとAndroid端末が自動的にERAへ接続し、設定が反映されます。
※タップしてから設定の反映までしばらくかかる場合があります。

Link Generatorを利用してインストールする場合は、以下の流れとなります。

STEP1　他社セキュリティプログラムのアンインストール

他社製のセキュリティプログラムを利用している場合は、そのプログラムのアンインストールを行います。

↓

STEP2　ポリシーの作成

ERAを利用して、アップデートサーバーへの接続設定や管理サーバーへの接続設定などを行ったポリシーを作成します。

↓

STEP3　リンクの作成

Link Generatorを使用してリンクを作成して、Android端末にリンクを配布します。

↓

STEP4　インストール作業の実施

インストーラー(.apk)を利用して手動でインストールします。

↓

STEP5　設定の反映

STEP3で配布したリンクをタップして設定を反映します。

↓

STEP6　各種設定の実施

ERAを利用して設定できない項目を手動で設定します。

▸▸▸ POINT

Link Generatorを利用して設定できない項目は、[ESETをデバイス管理者として設定]、[管理者連絡先の定義]です。

1.6.6 複数の拠点がある場合のインストール

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、Windows用の設定組み込み済みインストーラーやMac OS X用の設定組み込み済みインストーラーを利用するとともに、ESET Remote Administrator（ERA）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ラーやコンフィグレーションの管理などが容易になります。

1.6.6.1 クライアント展開のポイント

ESET Remote Administrator（ERA）には、クライアントPC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。クライアント用プログラムをインストールしたコンピューターが、ERA（管理サーバー）の管理対象となっていれば、これらの機能を利用して設定の管理を容易に行えます。

グループ機能

グループ機能は、クライアントPCを特定の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」のほか、特定の条件を指定して自動的にグループ分けを行う「パラメータグループ」を作成できます。たとえば、複数の拠点がある場合は、パラメータ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。グループ機能の詳細については70ページをご参照ください。

ポリシー機能

クライアントPCに特定の設定（コンフィグレーション）を強制的に適用できる機能です。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強制的に適用できます。たとえば、パラメータグループを利用するとグループ分けが自動化され、グループごとのポリシー適用を自動化できます。ポリシー機能の詳細については77ページをご参照ください。

1.6.6.2 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利用して、本社と支社間などの複数の拠点にクライアント用プログラムを展開する場合は、以下の流れで行います。ここでは、各拠点ごとに準備されたミラーサーバーに接続する設定をグループ機能とポリシー機能で一元管理する場合を例に流れを説明しています。

事前作業

❶インストーラー(パッケージ)の作成
Windows用プログラムの場合は、ERAを利用して、「リモート管理」設定を組み込んだ「設定組み込み済みインストーラー」を作成します。Mac OS X用プログラムの場合は、付属のインストーラー(.dmg)を利用して、「リモート管理」設定、権限ユーザーの設定などを行った「設定組み込み済みインストーラー(.pkg)」を作成します。

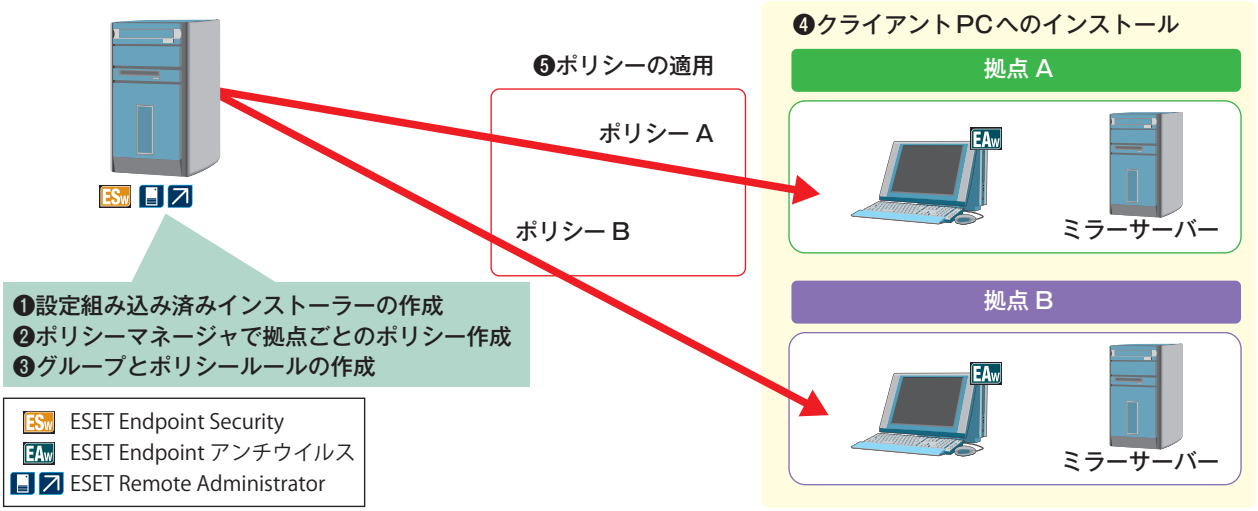
❷ポリシーの作成
ERAに搭載された「ポリシーマネージャ」で各拠点ごとのアップデート先が設定されたポリシーを作成します。

❸グループとポリシールールの作成
IPアドレスなどの情報をもとに各拠点ごとにパラメータグループを作成し、ERAに搭載されたポリシーマネージャで❷で作成したポリシーを割り当てます。

導入と展開

❹クライアントPCへのインストール
❶で作成したインストーラーを利用して、各拠点のクライアントPCにクライアント用プログラムをインストールします。

❺ポリシーの適用
インストール完了後、クライアントPCが管理サーバー(ERA)へ接続したときにポリシーを取得し、各拠点毎のアップデート先設定が自動的に適用されます。



※インストーラーを作成する際に、「リモート管理」の設定を間違えると、ポリシーの配布ができません。また、ERAにアクセスができませんので、タスクでの設定修正はできません。
※クライアントは複数のグループに所属できます。どのポリシーが適用されるかは、ポリシールールで設定された順番により決定されます。

1.6.7 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のポイントと注意点

クライアント用プログラムは、クライアントPCだけでなく管理サーバーにも導入できますが、両者ではポイントとなる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。クライアント用プログラムの設定を検討するときに重要なのが、導入するコンピューターの役割です。クライアントPC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。それぞれの場合で以下のような点に着目して設定を行うことを推奨しています。

クライアントPC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（パラメータ設定の保護）　※Windows用プログラムのみ**
- **権限ユーザー　※Mac OS X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**

リモート管理／アップデート

管理サーバーや、ウイルス定義データベースのアップデートに利用されるミラーサーバーなどを設置する場合は、クライアント用プログラムの各サーバーへの接続に関する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、既定値ではコンピューターの定期的な検査スケジュールは用意されていません。本製品は、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。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。

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用プログラムの設定は、既定値ではユーザーの判断（操作）で変更が可能になっています。この設定は、ユーザーによる自由な設定変更ができないようにパスワード保護をかけ、変更が必要な場合は管理者が行うようにするものです。なお、パスワード保護をかけることにより、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となります。

権限ユーザー

Mac OS X用プログラムは、すべての設定を自由に変更できる権限ユーザーをアカウントごとに選択できます。この機能を使うと、管理者として登録された権限ユーザーのみがクライアント用プログラムの詳細な設定を行えるようになります。

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はスケジュールされたアップデートに対して、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の設定を行えます。2つのアップデートサーバーを設定しておくことで、プライマリの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のアップデートサーバーに切り替えてアップデートを行います。たとえば、プライマリにミラーサーバーを、セカンダリにESET社のアップデートサーバーを設定することで、社内で利用しているコンピューターを社外に持ち出して利用する場合でも常に最新のウイルス定義データベースが適用されます。
なおWindows用プログラムの場合、手動でのアップデート時は、現在設定されたサーバー（プロファイル）のみを利用しますので、手動で切り替える必要があります。

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を検出した場合、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。この処理は、ユーザーが毎回対処方法を選択できるように変更できます。ユーザーが処理方法を選択する場合は、ウイルスなどの脅威を検出した際に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、まずは該当ファイルをウイルス検査の対象から除外してください。次に、隔離された該当ファイルを復元してください。
また、該当ファイルを再び検出しないようにウイルス定義データベースを修正するためには、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）

本製品は、疑わしいファイルを検出した場合に、ESET社へそのファイルの提出を求める場合があります。提出に同意すると、そのファイルをESET社に送信します。

コラム

「設定のポイントと注意点」

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を推奨しています。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。

一部検査機能の無効化

サーバーでは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が推奨されます。

■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

データベースなどの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設定してください。

1.7 STEP5 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。以下に、移行例をご紹介します。

クライアント用プログラム	ESET Endpoint Security
クライアント数	2,000
管理サーバー数	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	バッチファイルを利用
参照モデルケース	モデルケース 6

STEP1　管理サーバー（ERA）とミラーサーバーを構築

↓

STEP2　設定組み込み済みインストーラーを作成

ERAを利用して、ESET Endpoint Securityの設定組み込み済みインストーラーを作成。

↓

STET3　既存ソフトウェアをアンインストール

↓

STEP4　クライアント用プログラムをインストール

作成した設定組み込み済みインストーラーをファイルサーバー（共有フォルダー）に保存し、各クライアントがダウンロードしてクライアント用プログラムをインストール（その際、アップデート先をローカルに指定）。

↓

STEP5　アップデートサーバーの設定を配布

アップデートサーバーをミラーサーバーにする設定を、管理サーバーからクライアントPCに配布。

1.8 バージョンアップによる導入

本節では、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。

1.8.1 バージョンアップ時のポイント

ESET ライセンス製品のバージョンアップは、基本的に上書きインストールが行えますが、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へアップデートする場合に限って、ESET NOD32アンチウイルスのアンインストールが必要です。

	現行環境	バージョンアップ環境	上書きインストール
Windows用プログラム	ESET Remote Administrator V4.0	ESET Remote Administrator V5.0	○
	ESET Smart Security V4.x	ESET Endpoint Security	○
	ESET NOD32アンチウイルス V4.x	ESET Endpoint アンチウイルス	○
		ESET File Security for Windows Server	×
Mac OS X用プログラム	ESET NOD32アンチウイルス V4.0	ESET NOD32アンチウイルス V4.1	○

●上書きインストールが可能な環境

現行環境

管理サーバー	ESET Remote Administrator V4.0
ミラーサーバー	ESET Remote Administrator V4.0
クライアント用プログラム	ESET Smart Security V4.2またはESET NOD32アンチウイルス V4.2

バージョンアップ環境

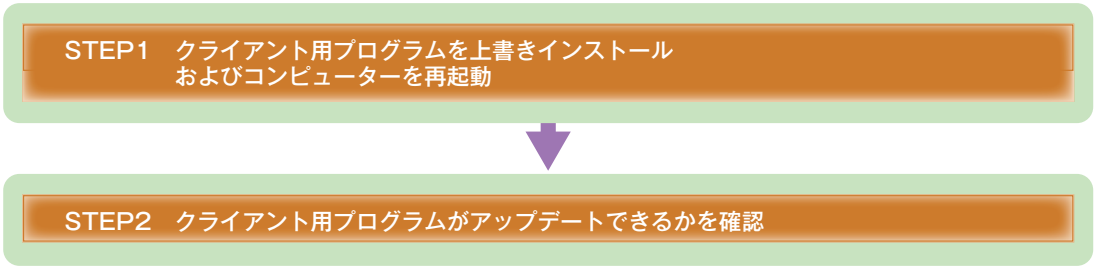
管理サーバー	ESET Remote Administrator V5.0
ミラーサーバー	ESET Remote Administrator V5.0
クライアント用プログラム	ESET Endpoint SecurityまたはESET Endpoint アンチウイルス

1.8.2 ESETセキュリティ ソフトウェア シリーズ ライセンス製品 V4.2からのバージョンアップ

ESETセキュリティ ソフトウェア シリーズ ライセンス製品 V4.2からV.5.0へのバージョンアップの際、既存のESETセキュリティ製品をアンインストールする必要はありません。上書きインストールでバージョンアップすることができます。

1.8.2.1 クライアントPCのみで運用している場合のバージョンアップ手順

クライアントPCのみで運用している場合は、最初に1台だけバージョアップを行い、そのコンピューターの動作確認と設定を行います。次に、バージョンアップ済みのコンピューターの設定ファイルを保存し、それを適用して残りのクライアントPCのバージョアップを行います。



1.8.2.2 管理サーバーとクライアントPCで運用している場合のバージョンアップ手順

管理サーバーとクライアントPCで運用している場合は、最初に管理サーバーのデータベースのバックアップを行います。次に管理サーバー（ERA）の上書きインストールを行い、続いてERACを上書きインストールすれば、管理サーバー側のバージョンアップは完了です。

クライアント用プログラムのバージョンアップは、まず、インストール用に設定組み込み済みインストーラーを作成します。次にこの設定組み込み済みインストーラーを利用して上書きインストールします。

STEP1　管理サーバーのデータベースをバックアップ

●バージョンアップ時に問題が発生した場合に備えてデータベースのバックアップを作成します。

↓

STEP2　管理サーバーにERAを上書きインストールおよびコンピューターを再起動

●ERAのインストールウィザードの途中で「旧製品のデータベースと設定のインポートに関する設定」が行えます。ここで「すべてインポート」を選択すると、インストールに多くの時間を要することがあります。

↓

STEP3　管理者用PCにERACを上書きインストールおよびコンピューターを再起動

↓

STEP4　管理者用PCを利用して管理サーバーに接続

●クライアント用プログラムの設定組み込み済みインストーラーを作成します。

↓

STEP5　クライアント用プログラムを設定組み込み済みインストーラーで上書きインストールおよびコンピューターを再起動

●最初に、数台のクライアントPCを利用して、インストールが正常に行えるかどうかの確認のためにテストを行います。

↓

STEP6　各クライアントPCからアップデート操作を行って、アップデートが行えるかどうかを確認

1.8.2.3 ミラーサーバーとクライアントPCで運用している場合のバージョンアップ手順

ミラーサーバーとクライアントPCで運用している場合は、最初にミラーサーバーのバージョンアップを行い、接続確認を行った後、クライアントPCのバージョンアップを行います。この場合のクライアントPCのバージョンアップは、「クライアントPCのみで運用している場合のバージョンアップ手順」と同じです。

STEP1 ミラーサーバーにERAまたはESET Endpointアンチウイルスを上書きインストールおよびコンピューターを再起動

- ERAでミラーサーバーを構築していた場合は、インストールウィザードの途中で「旧製品のデータベースと設定のインポートに関する設定」が行えます。ここで「すべてインポート」を選択します。
- ESET NOD32アンチウイルスでミラーサーバーを構築していた場合は、ESET Endpoint アンチウイルスをそのまま上書きインストールおよびコンピューターを再起動を行います。

※ ESET NOD32アンチウイルスで構築していたミラーサーバーをESET File Security for Microsoft Windows Serverにアップデートする場合は、ESET NOD32アンチウイルスをアンインストールした後に、ESET File Security for Microsoft Windows Serverのインストールを行います。また、新しくインストールしたESET File Security for Microsoft Windows Serverは、再度設定をやり直す必要があります。

↓

STEP2 ERAをインストールした場合は、管理者用PCにERACを上書きインストールおよびコンピューターを再起動

↓

STEP3 ESET社のアップデートサーバーに接続できるかどうかを確認

- ERAをミラーサーバーに利用している場合は、ERACでミラーサーバーに接続し、アップデートサーバーの接続確認を行います。
- ESET Endpointアンチウイルスを利用している場合は、手動アップデートを行って接続を確認します。
- ESET File Security for Microsoft Windows Serverにアップデートした場合は、再度、ミラーサーバーの設定をやり直します。

↓

STEP4 クライアント用プログラムを上書きインストールおよびコンピューターを再起動

↓

STEP5 クライアント用プログラムがアップデートできるかどうかを確認

1.8.2.4　管理サーバーとミラーサーバーによる運用をしている場合のバージョンアップ手順1 ～管理サーバーとミラーサーバーが同じコンピューターの場合

管理サーバーとミラーサーバーを同一のコンピューターで構築している場合も、最初に管理サーバーのデータベースのバックアップを行います。次に管理サーバー（ERA）の上書きインストールを行い、続いてERACを上書きインストールすれば、管理サーバー、ミラーサーバー共にバージョンアップ完了です。
クライアント用プログラムのバージョンアップは、インストール用の設定組み込み済みインストーラーを作成し、このインストーラーを利用して上書きインストールで行います。

STEP1　管理サーバーのデータベースをバックアップ

- バージョンアップ時に問題が発生した場合に備えて念のためデータベースのバックアップを作成します。

↓

STEP2　管理サーバーにERAを上書きインストールおよびコンピューターを再起動

- ERAのインストールウィザードの途中で「旧製品のデータベースと設定のインポートに関する設定」が行えます。ここで「すべてインポート」を選択すると、インストールに多くの時間を要することがあります。

↓

STEP3　管理者用PCにERACを上書きインストールおよびコンピューターを再起動

↓

STEP4　管理者用PCを利用して管理サーバーに接続

- ERAがアップデートサーバーに接続できるかどうか確認します。
- クライアント用プログラムの設定組み込み済みインストーラーを作成します。

↓

STEP5　クライアント用プログラムを設定組み込み済みインストーラーで上書きインストールおよびコンピューターを再起動

- 最初に、数台のクライアントPCを利用して、インストールが正常に行えるかどうかの確認のためにテストを行います。

↓

STEP6　各クライアントPCからアップデート操作を行って、アップデートが行えるかどうかを確認

1.8.2.5 管理サーバーとミラーサーバーによる運用をしている場合のバージョンアップ手順2 ～管理サーバーとミラーサーバーが異なるコンピューターの場合

管理サーバーとミラーサーバーが異なるコンピューターで構築されている場合は、最初に59ページと同じ手順で管理サーバー側のバージョンアップを行います。

次にミラーサーバーを上書きインストールでバージョンアップし、続いて設定組み込み済みインストーラーを作成して、上書きインストールでクライアントPCのバージョンアップを行います。

STEP1 管理サーバーのデータベースをバックアップ

↓

STEP2 管理サーバーにERAを上書きインストールおよびコンピューターを再起動

- ERAのインストールウィザードの途中で「旧製品のデータベースと設定のインポートに関する設定」が行えます。ここで「すべてインポート」を選択すると、インストールに多くの時間を要することがあります。

↓

STEP3 ミラーサーバーにERAまたはESET Endpointアンチウイルスを上書きインストールおよびコンピューターを再起動

- ERAでミラーサーバーを構築していた場合は、インストールウィザードの途中で「旧製品のデータベースと設定のインポートに関する設定」を行うことができます。ここで「すべてインポート」を選択します。
- ESET NOD32アンチウイルスを利用してミラーサーバーを構築していた場合は、ESET Endpoint アンチウイルスをそのまま上書きインストールします。

※ ESET NOD32アンチウイルスで構築していたミラーサーバーをESET File Security for Microsoft Windows Serverにアップデートする場合は、ESET NOD32アンチウイルスをアンインストールした後に、ESET File Security for Microsoft Windows Serverのインストールを行います。また、新しくインストールしたESET File Security for Microsoft Windows Serverは、再度設定をやり直す必要があります。

↓

STEP4 管理者用PCにERACを上書きインストールおよびコンピューターを再起動

↓

STEP5 ESET社のアップデートサーバーに接続できるかどうかを確認

- ERAをミラーサーバーに利用している場合は、ERACでミラーサーバーに接続し、アップデートサーバーの接続確認を行います。
- ESET Endpointアンチウイルスを利用している場合は、手動アップデートで接続を確認します。
- ESET File Security for Microsoft Windows Serverにアップデートした場合は、再度、ミラーサーバーの設定をやり直します。

↓

STEP6 管理者用PCを使用して管理サーバーに接続し、クライアント用プログラムの設定組み込み済みインストーラーを作成

STEP7 クライアント用プログラムを設定組み込み済みインストーラーで上書きインストールおよびコンピューターを再起動

- 最初に、数台のクライアントPCを利用して、正常にインストールが行われたか確認のためにテストを行います。

STEP8 各クライアントPCからアップデート操作を行い、アップデートが行えるかどうかを確認

[Chapter 2]
クライアントPCの効率的な管理方法

2.1 効率的な管理を行うための機能

ESET Remote Administrator（ERA）には、クライアントPCを効率的に管理し、スムーズな運用を実現するための機能が備えられています。

2.1.1 主な管理機能

ESET Remote Administrator（ERA）には、「ダッシュボード機能」「グループ機能」「タスク機能」「ポリシー機能」「通知機能」などのクライアントPC管理機能を搭載しています。また、ウイルス定義データベースを効率的に配布管理する「ロールバック機能」「ミラー機能」なども搭載しています。

●主な管理機能

機能	概要	参照ページ
ダッシュボード機能	各クライアントPCから収集した各種情報やESET Remote Administrator Server（ERAS）のCPU負荷やデータベースの負荷などのパフォーマンス情報をWebブラウザー経由で閲覧できます。ダッシュボードに表示する情報は、ESET Remote Administrator Console（ERAC）からカスタマイズできます。また、ダッシュボードは暗号化された接続（HTTPS）にも対応しています。	69ページ
グループ機能	クライアントPCを特定のグループに分類して管理するための機能です。グループは、「グループマネージャ」を使うことで作成できます。グループマネージャで作成したグループは、タスクの一括配布やポリシーの一括適用などに利用できます。	70ページ
タスク機能	ERASを利用したリモート操作でクライアントPCに指示（タスク）を出す機能です。クライアントPCの各種設定を変更したり、ウイルス検査の実行指示など様々な指示を出すことができます。タスクは、グループ単位またはクライアントPC単位で実行できます。	73ページ
ポリシー機能	クライアントPCの特定の設定（コンフィグレーション）を継続的に保守し、強制的に適用させる機能です。タスク機能に用意されたクライアントPCの各種設定を行う［コンフィグレーション］タスクと同等の機能も提供します。ポリシー機能は、グループ単位またはクライアントPC単位で実行できます。	77ページ
通知機能	セキュリティ上の問題が発生したときなどに、管理者にメッセージを通知する機能です。	79ページ

●ウイルス定義データベース関連機能

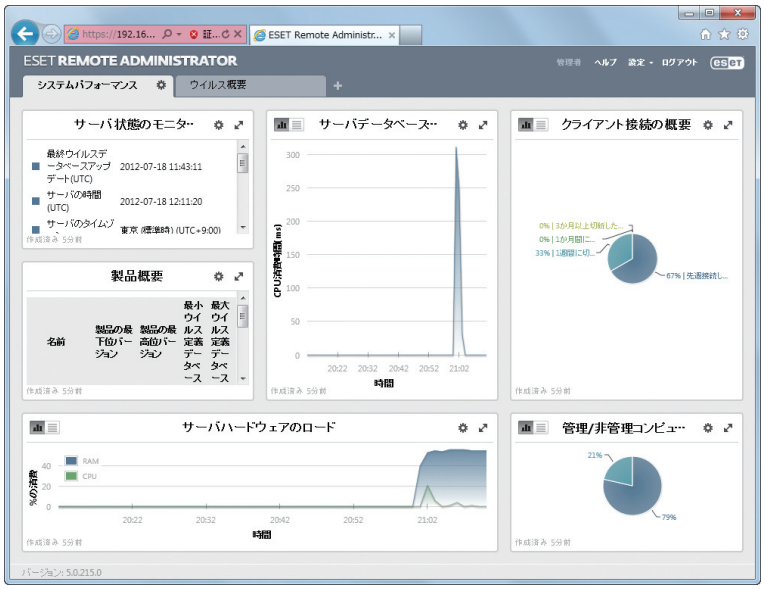
機能	概要	参照ページ
ロールバック機能	クライアントPCに適用したウイルス定義データベースやモジュールを適用前のバージョンに戻す機能です。また、ウイルス定義データベースのアップデートを一定時間無効にすることもできます。	81ページ
ミラー機能	ESET社がインターネット上に設置しているウイルス定義データベースのアップデートサーバーを複製し、これと同等の機能を備えたサーバーを社内に設置できる機能です。この機能を利用すると、社内LANなどのローカルネットワーク内に、ウイルス定義データベースを配布するサーバーを設置できます。	82ページ

2.2 ダッシュボード機能

ESET Remote Administrator（ERA）には、Webブラウザー経由で各クライアントPCから収集した情報やESET Remote Administrator Server（ERAS）のパフォーマンス情報を閲覧する「ダッシュボード」機能が備わっています。ここでは、ダッシュボード機能について説明します。

2.2.1 ダッシュボード機能とは

ダッシュボード機能を利用すると、各クライアントPCから収集したウイルスや迷惑メールに関する情報、ブロックされたWebサイトなどのさまざまな情報やESET Remote Administrator Server（ERAS）のパフォーマンス情報などをWebブラウザー経由で閲覧できます。この機能を利用することで、簡単に各クライアントの状況やERASをインストールしたコンピューターの負荷などを知ることができます。また、ダッシュボードに表示する情報は、ESET Remote Administrator Console（ERAC）から自由にカスタマイズできます。ダッシュボードは、暗号化された接続（HTTPS）にも対応しています。ダッシュボード機能の詳細な使い方は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



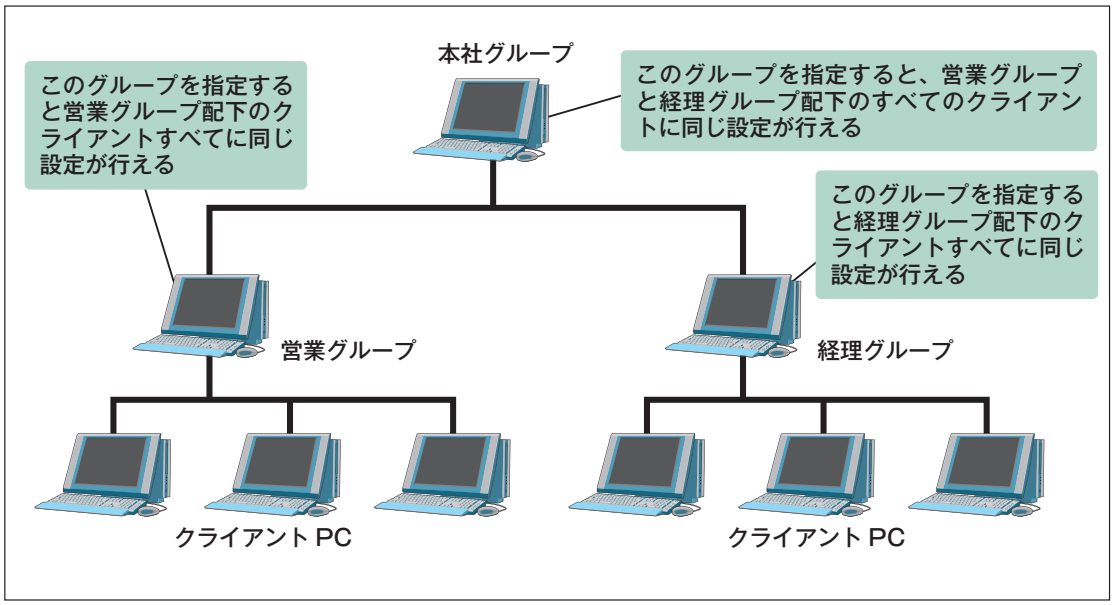
2.3 グループ機能

ESET Remote Administrator Server（ERAS）を利用したクライアントPCの操作は、クライアントPC単位だけでなく、グループ単位で一括して行うことも可能です。このグループを作成する機能を「グループマネージャ」といいます。ここでは、グループ機能について説明します。

2.3.1 グループ機能とは

グループ機能は、クライアントPCを特定のグループに分類して管理する機能です。グループは、グループマネージャによって作成でき、「静的グループ」と「パラメータグループ」に大別されます。また、Active Directoryのグループ情報と同期して利用することもできます。静的グループは、手動でクライアントPCをグループ分けするときに利用する小規模の管理に向いています。パラメータグループは、特定の条件を指定しその条件にあったクライアントPCのみでグループを構成できます。パラメータグループは、条件を指定するだけでグループ分けを自動化できるので、大規模な管理に向いています。

作成したグループは、新規タスクの一括配布やポリシー（セキュリティの設定）の一括適用などに利用できます。



2.3.2　静的グループとパラメータグループ

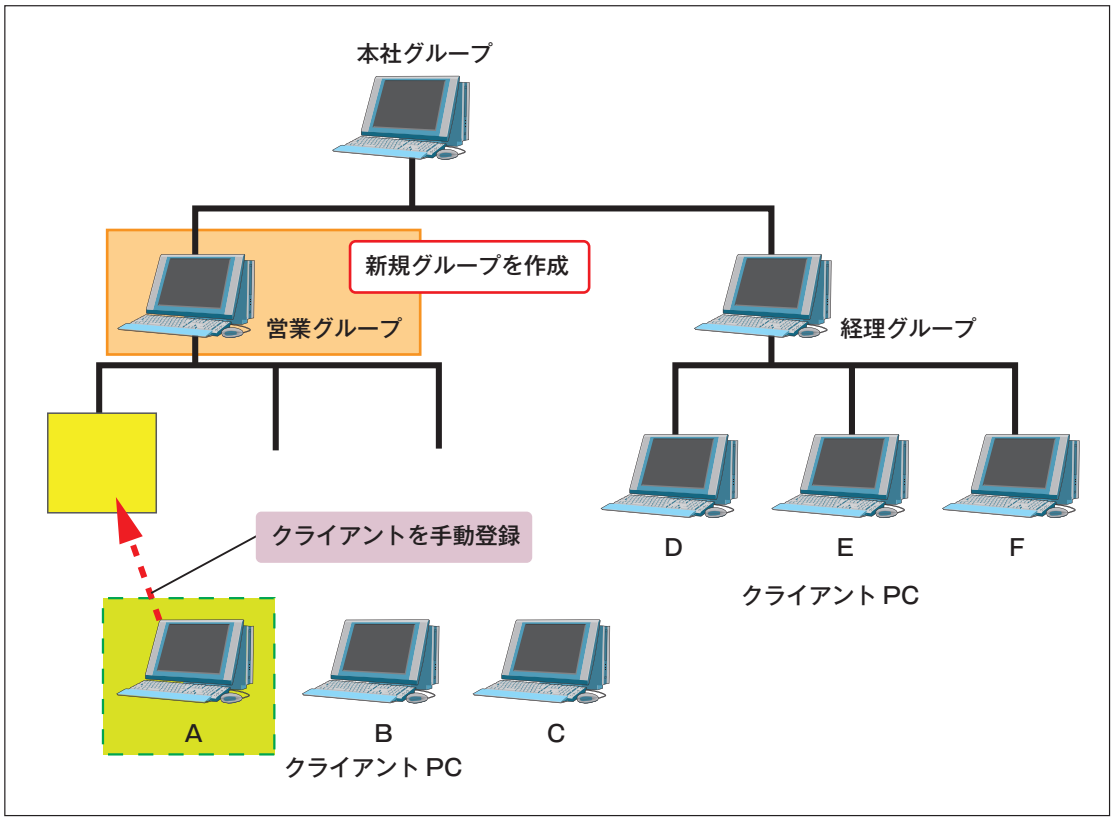
グループは「静的グループ」と「パラメータグループ」に大別でき、それぞれ以下のような特徴があります。

POINT

Active Directoryを利用している場合は、Active Diectoryで利用しているグループとの同期機能も利用できます。この機能の使い方については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

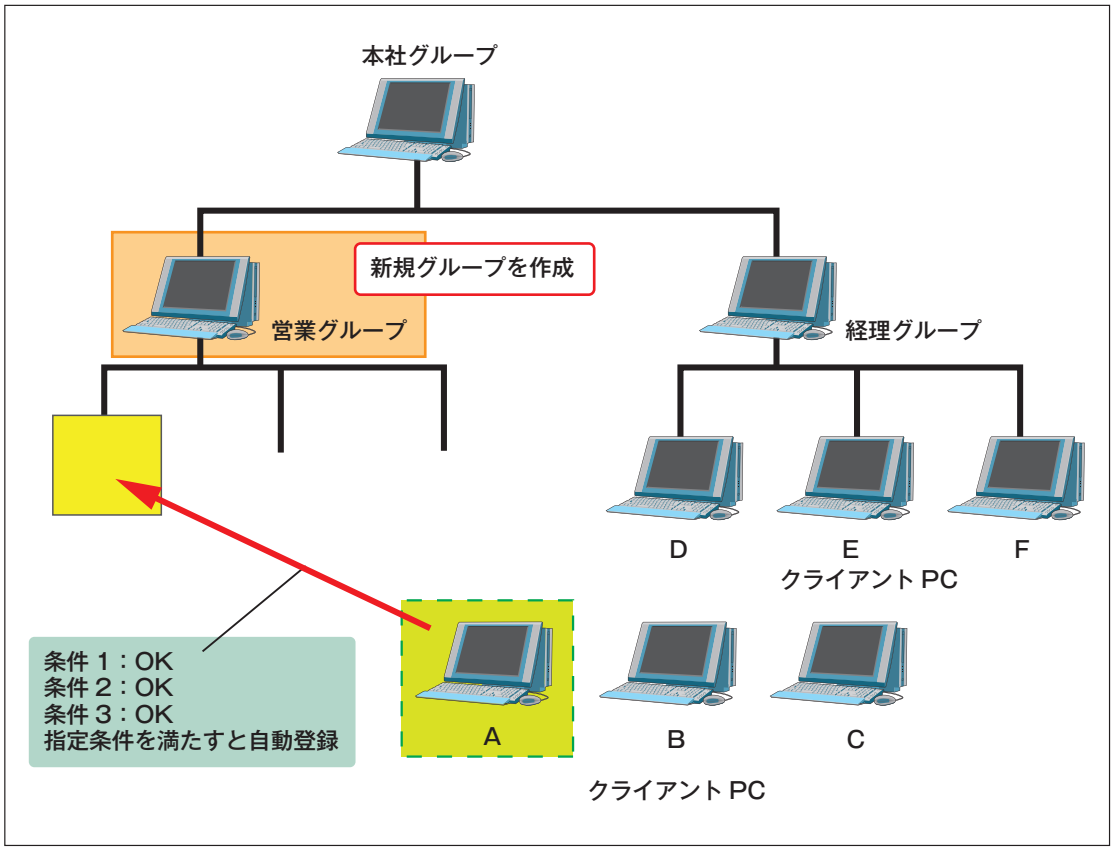
2.3.2.1　静的グループ

静的グループは、クライアントPCを手動でグループ分けするときに利用します。静的グループの作成手順については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



2.3.2.2 パラメータグループ

パラメータグループは、グループに登録する条件を指定し、その条件を満たすクライアントPCを自動的にグループ登録します。パラメータグループの作成手順については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



条件の例

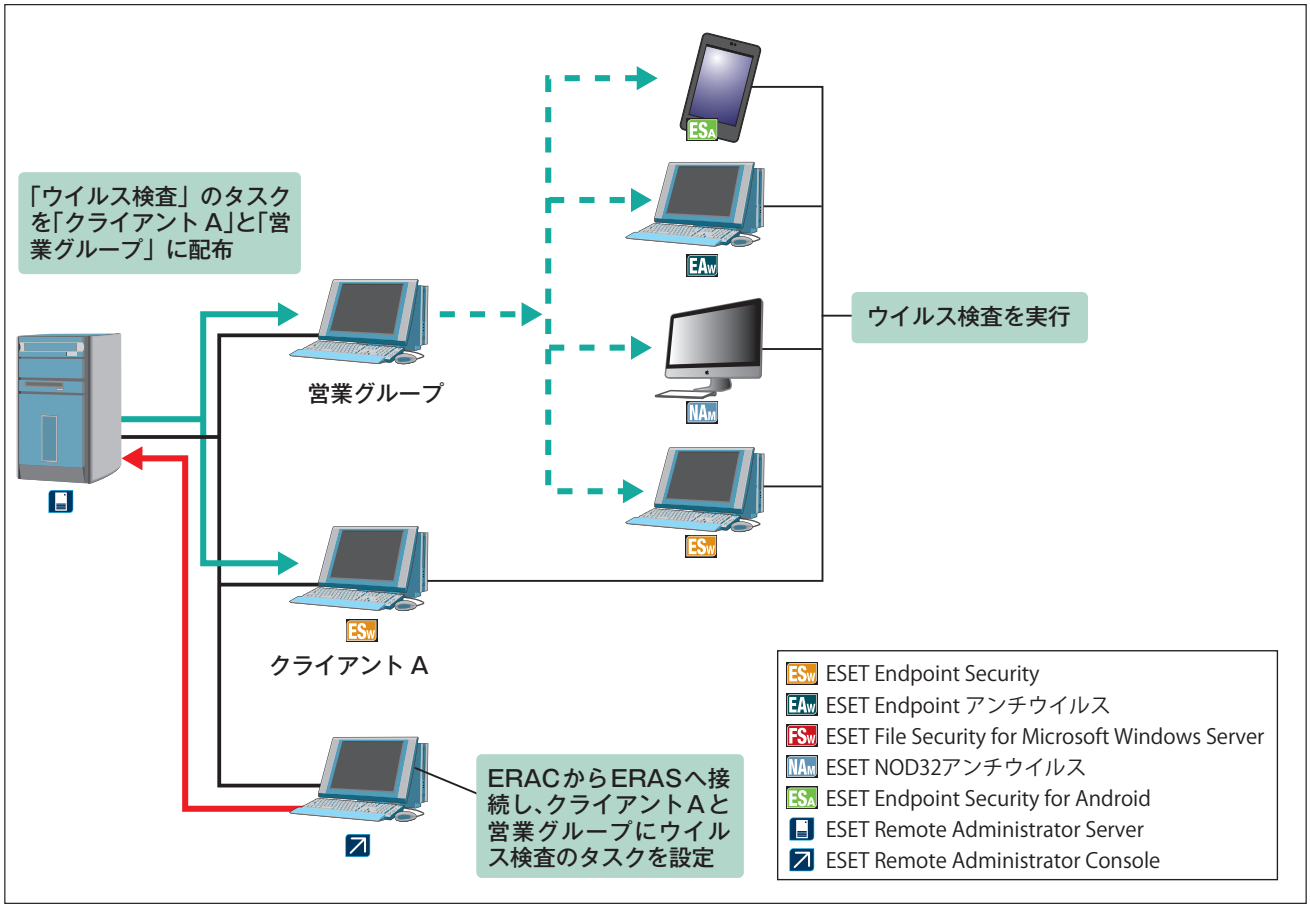
- ●グループ
- ●ドメイン
- ●コンピューター名
- ●IPアドレス
- ●クライアント用プログラムの製品名やバージョン
- ●ウイルス定義データベースのアップデート状況
- ●OS

2.4 タスク機能

タスク機能は、ESET Remote Administrator Sever（ERAS）からクライアントPCの設定などをリモート操作で変更する機能です。ここではタスクの配布について説明します。

2.4.1 タスクとは

タスクとは、リモート操作でクライアントPCに様々な指示（タスク）を送り、実行させる機能です。クライアントPCは定期的にERASに接続して、自身の各種情報を送信します。その際にタスクがあると、クライアントPCはERASからタスクを受信し、それを実行します。



2.4.2 タスクの種類

タスクには、以下の種類があります。タスクはクライアントPC単位だけでなく、グループ単位でも実行できます。また、一部のタスク（オンデマンド検査タスクやウイルス定義データベースのアップデートタスク）は、各クライアントPCのタスク実行時間をランダムに遅らせることができます。

●タスクの種類

種類	概要
コンフィグレーション	クライアントPCの各種設定を変更するときに利用します。たとえば、定期的な検査スケジュールの登録や管理サーバー / アップデートサーバーへの接続設定、ウイルス検出時のアクションの設定などさまざまな設定が行えます。
オンデマンドスキャン	ウイルス発見時の駆除を有効に設定したウイルス検査をクライアントPCに実行させたいときに利用します。このウイルス検査は、ウイルスを発見すると駆除を実行します。また、このタスクは、各クライアントPCのタスク実行時間をランダムに遅らせることができます。
オンデマンドスキャン(駆除無効)	ウイルス発見時の駆除を無効に設定したウイルス検査をクライアントPCに実行させたいときに利用します。このウイルス検査は検査によるログが作成されるだけで、感染ファイルに対するアクションは実行されません。また、このタスクは、各クライアントPCのタスク実行時間をランダムに遅らせることができます。
今すぐアップデート	ウイルス定義データベースのアップデートを強制的に実行したいときに利用します。このタスクを設定したクライアントPCは、強制的にウイルス定義データベースのアップデートが実行されます。また、このタスクは、各クライアントPCのタスク実行時間をランダムに遅らせることができます。これにより、ウイルス定義データベースのアップデートを分散でき、ミラーサーバーやネットワークに負荷を軽減します。
SysInspectorスクリプト	このタスクでは、対象のクライアントPC上でSysInspectorスクリプトを実行します。このスクリプトは、望ましくない可能性があるオブジェクトをシステムから削除したい場合などに利用します。※1
保護機能	クライアントPCの各保護機能(ドキュメント保護、リアルタイム保護、Webアクセス保護など)の有効／無効を切り替えたいときに利用します。設定を無効にする場合は、一定時間経過すると設定値を元に戻す(有効にする)期間が選択できます。※2
スケジュール済みタスクの実行	クライアントPCに登録されているスケジュールタスクを実行したいときに利用します。※2
隔離からの復元/削除	クライアントPCで発見され、隔離中のファイルを復元または削除するときに利用します。誤ってウイルスと判断され隔離されたファイルなどをリモート操作で復元するときなどに利用します。※1
ウイルス定義データベースのロールバック	クライアントPCに適用したウイルス定義データベースやモジュールに不具合が見つかった場合、適用前のバージョンにロールバックしたいときに利用します。また、クライアントPCのウイルス定義データベースのアップデートを一定期間無効にすることもできます。※2
クライアントのアップデートキャッシュのクリア	クライアントPCのアップデートキャッシュを削除したいときに利用します。ウイルス定義データベースのアップデートが成功していない可能性がある場合、クライアントPCのアップデートキャッシュをクリアし、最新のアップデートをダウンロードします。※2
セキュリティ監査ログの作成	Android端末のバッテリレベル、Bluetoothステータス、ディスクの空き領域、デバイスの可視性、ホームネットワーク、および実行中のプロセスなどをチェックしたログを作成したいときに利用します。※3
通知の表示	Android端末に通知(警告メッセージなど)を送信したいときに利用します。※3

※1　ESET Smart Security V4以降またはESET NOD32アンチウイルス V4以降でのみ利用できます。
※2　ESET Endpoint SecurityまたはESET Endpoint アンチウイルスでのみ利用できます。
※3　ESET Endpoint Security for Androidでのみ利用できます。

2.4.3　タスクの設定手順

クライアントPCに対して各種タスクを設定するときは、以下の手順に沿って作業します。選択したタスクの種類によってタスクの設定方法は異なりますが、基本的な手順は以下の通りです。

STEP1　タスクの選択

新規タスクの種類から[コンフィグレーション]を選択します。
●コンフィグレーション
●オンデマンドスキャン(駆除無効)
●オンデマンドスキャン(駆除有効)
●定義データベースのアップデート
●SysInspectorスクリプト
●隔離からの復元/削除

↓

STEP2　タスクの設定

ESET コンフィグレーションエディターを利用してタスクの詳細設定を行います。他のタスクは、画面内のオプションを設定することで詳細設定を行います。

↓

STEP3　タスクを配布するクライアントPCの選択

タスクを配布するクライアントPCは、クライアントPC単位で指定できるだけでなく、グループ単位でも指定可能です。クライアントPCのグループ分けは、グループマネージャを利用して行えます。

↓

STEP4　タスクの配布（実行）

2.4.4 [コンフィグレーション]タスクの設定方法

[コンフィグレーション]タスクの設定は、基本的にESET コンフィグレーションエディターを利用して行いますが、その方法には大きく分けて以下の3種類の方法があります。

2.4.4.1 新規作成

新規設定を作成する方法です。❶[作成]ボタンをクリックするとESET コンフィグレーションエディターが起動するので、これでクライアントPC用の設定を作成します。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

2.4.4.2 作成済みの設定ファイル(.xml)を利用

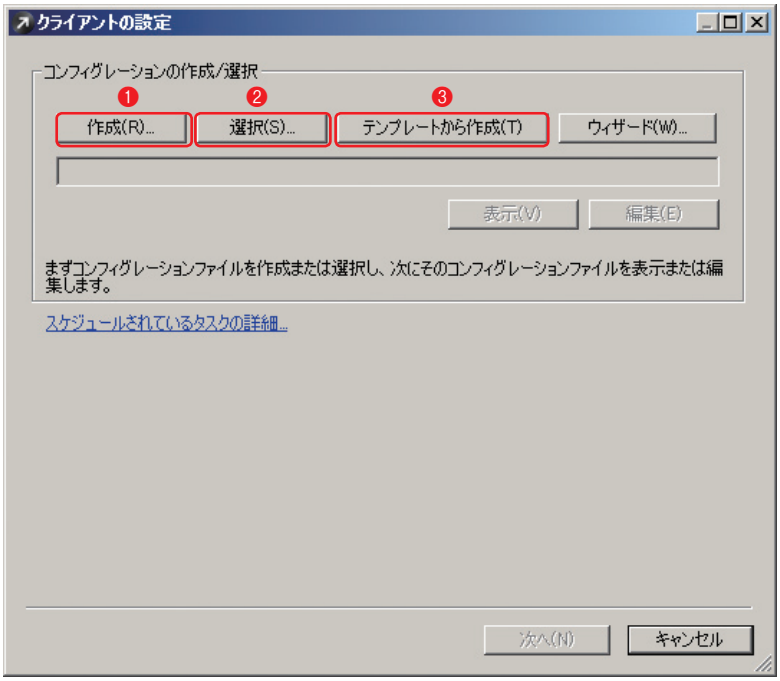
事前にESET コンフィグレーションエディターなどを利用して作成しておいたクライアントPC用の設定ファイル(.xml)を利用する方法です。❷[選択]ボタンをクリックすると、[ファイルを開く]ダイアログが開くので、事前に準備しておいた設定ファイル(.xml)を読み込みます。ファイルを選択した後に、[表示]ボタンをクリックすると設定を確認でき、[編集]ボタンをクリックするとその設定ファイル(.xml)を編集できます。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

2.4.4.3 テンプレートから作成

作成済み設定ファイル(.xml)を利用した方法によく似た方法で、事前に準備しておいたテンプレート用の設定ファイル(.xml)を利用して設定を行います。❸[テンプレートから作成]ボタンをクリックすると[ファイルを開く]ダイアログが開くので、事前に準備しておいたテンプレート設定ファイル(.xml)を読み込みます。ファイルを選択した後に、[表示]ボタンをクリックすると設定を確認でき、[編集]ボタンをクリックするとテンプレート設定ファイル(.xml)を編集できます。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

▸▸▸ POINT

[ウィザード]ボタンをクリックすると、「パーソナルファイアウォールマージウィザード」画面が起動します。この設定により、稼働中のクライアントPCで利用されているファイアウォールルールを読み出して、それを利用して新しいファイアウォールルールを作成できます。



2.5 ポリシー機能

ポリシー機能とは、クライアントPCに対する特定の設定（コンフィグレーション）を継続的に保守し、強制的に適用させる機能です。ここでは、ポリシーについて説明します。

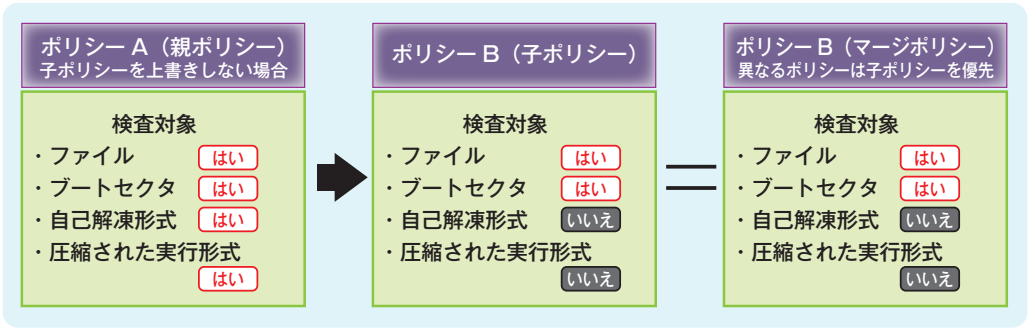
2.5.1 ポリシー機能とは

ポリシーは、タスク機能に用意された［コンフィグレーション］タスクと同等の機能を提供しています。［コンフィグレーション］タスクが1度きりの設定であるのに対し、ポリシー機能では継続的に設定が適用されます。ポリシーの変更を行った場合、その変更点はクライアントPCが自身の各種情報を送信するためにERASへ接続した後、すぐに適用されます。

2.5.2 ポリシーの親子関係

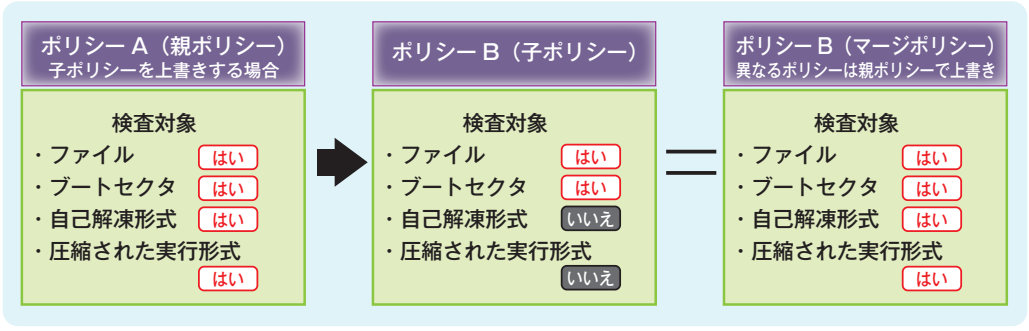
ポリシーでは、「継承」という概念が導入されています。子ポリシーは親ポリシーの設定を継承でき、設定をマージ（統合）できます。通常、親ポリシーと子ポリシーの設定が異なっている場合、子ポリシーの設定が優先されますが、逆に親ポリシーが子ポリシーの設定を上書きし、強制的に親ポリシーの設定を子ポリシーに適用することもできます。

●通常の親子のポリシー



▲通常は、親ポリシーと子ポリシーの設定が異なっている場合、子ポリシーの設定が優先されます。

●親ポリシーを強制的に適用



▲親ポリシーと子ポリシーの設定が異なっている場合に、親ポリシーを強制的に適用することも可能です。

2.5.3 ポリシーを利用した設定適用の流れ

クライアントPCのポリシーを変更することで各種設定を行うときは、以下の流れで作業します。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

STEP 1 ポリシーの作成

ポリシーマネージャを起動し、[ポリシーマネージャ] タブでポリシーを作成

↓

STEP 2 ポリシー内容の作成

作成したポリシーの設定内容を決め、ESET コンフィグレーションエディターで作成

↓

STEP3 ポリシーの適用

[ポリシールールによる適用] は、手動による適用（[ポリシーマネージャからの適用] [クライアントペインからの適用]）より優先されます。

●ポリシールールによる適用

●手動による適用

・ポリシーマネージャからの適用

・クライアントペインからの適用

2.6 通知機能

ERAには、ウイルスが検出された場合などセキュリティ上の問題が発生したとき、管理者などに異常を知らせるための通知機能が搭載されています。通知機能は、［通知マネージャ］を利用することで通知内容の設定や通知の方法、各種警告などをカスタマイズできます。

2.6.1 通知ルール作成の流れ

［通知マネージャ］を利用して電子メールで通知を行うには、あらかじめERASに電子メールの送信設定を行っておく必要があります。また［通知マネージャ］には、［事前定義のルール］が準備されていますが、既定ではすべてのルールが無効に設定されています。通知ルールは、事前定義のルールが利用できるほか、新規ルールの作成や事前定義のルールをカスタマイズして利用することもできます。通知ルールの作成は、以下の手順に沿って作業します。詳細は「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

STEP1 利用する通知ルールを選択する

既存の通知ルールから、適用する通知ルールを選択します。

↓

STEP2 ［トリガの種類］［優先順位］、通知間隔や時間に関する設定を行う

- トリガは通知を行うきっかけになる現象で、［クライアント状態］［サーバ状態］［終了したタスク イベント］［新規クライアントイベント］［新規ログイベント］の 5 種類から選択します。
- ［優先順位］は通知メッセージの優先順位で、最上位の［P1］から最下位の［P5］の中から選択します。優先順位によってルールの機能が影響を受けることはありません。
- 通知間隔や時間に関する設定は、通知ルールの［有効化までの時間］［繰り返す間隔］［スロットル間隔（定期的なチェック間隔）］などを設定します。

※選択した［トリガの種類］によって、行う時間の設定が異なります。

↓

STEP3 ［クライアントフィルタ］を設定する

対象とするクライアント PC の条件を設定します。条件は、複数指定できます。
※選択した［トリガの種類］によっては、この設定は行えません。

↓

STEP4 ［パラメータ］を設定する

通知を行う条件を設定します。
※設定できる内容は、選択した［トリガの条件］によって異なり、この設定を行えない場合もあります。

↓

STEP5 ［アクション］を設定する

作成したルール(条件)を満たしたときの動作の設定を行います。[電子メール][SNMPトラップ][実行(サーバ上)][ファイルにログを保存する(サーバ上)][Syslogにログを保存する][ログ]から選択できます。

STEP6 ［メッセージ］を設定する

通知に利用するメッセージを設定します。メッセージには変数が利用できます。

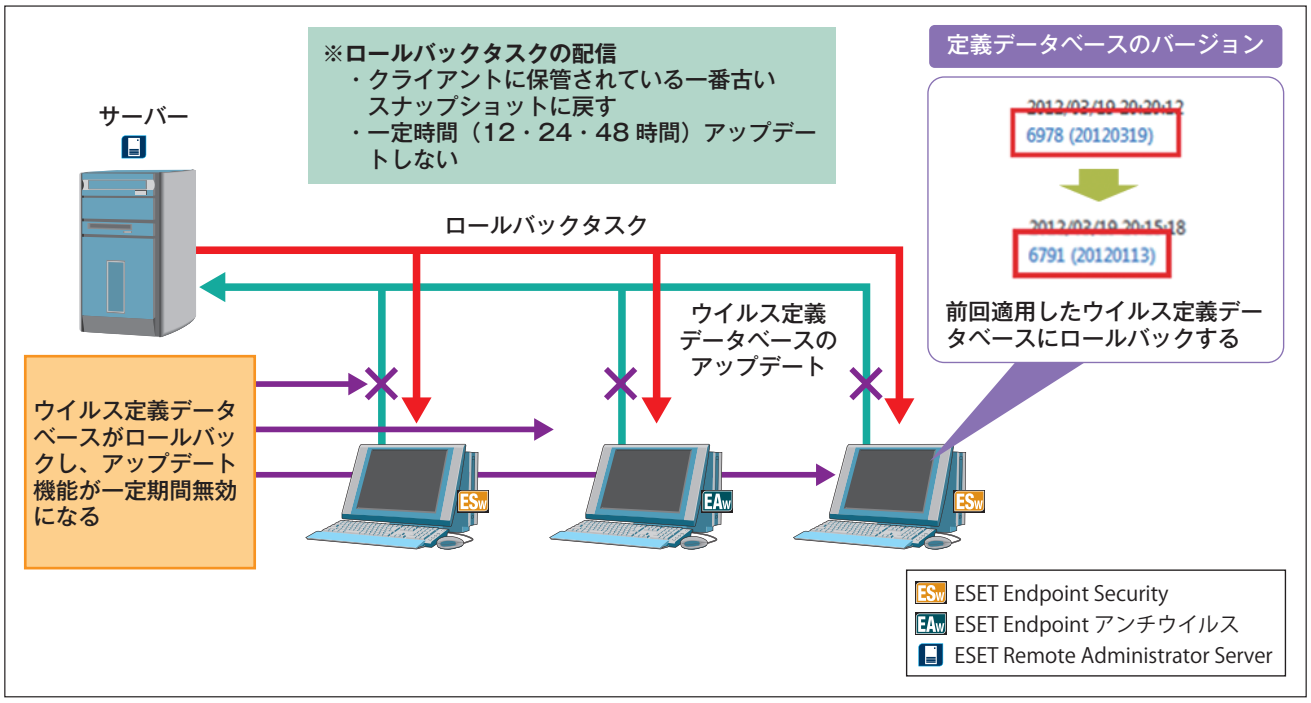
2.7 ロールバック機能

クライアントPCに適用したウイルス定義データベースを適用前のバージョンに戻す機能を「ロールバック」機能と呼びます。ここでは、ロールバック機能について説明します。

2.7.1 ロールバック機能とは

ESET Endpoint SecurityおよびESET Endpoint アンチウイルスには、適用したウイルス定義データベースを適用前のバージョンに戻すロールバック機能が備わっています。この機能によって、ウイルス定義データベースの特定バージョンでウイルスに感染していないプログラムを誤検出した場合、適用前のバージョンに戻すことでその不具合を回避できます。

また、ERASからクライアントPCへのウイルス定義データベースのアップデートを一定期間（12時間、24時間、48時間）無効にすることもできます。一部のWindows システムファイルやアプリケーションで利用されるファイルをウイルスの疑いがあるファイルとして判定したときなどに、ロールバックを行い、ウイルス定義データベースのアップデートを一定期間無効とすることで暫定的な対応とするという運用も行えます。



※ロールバック機能は、ESET Endpoint SecurityおよびESET Endpoint アンチウイルス以降でのみ利用できます。ESET File Security for Microsoft Windows ServerまたはESET NOD32アンチウイルス、ESET File Security for Linux、ESET Endpoint Security for Androidではこの機能をサポートしていません。

2.8 ミラー機能

ESET社はインターネット上でウイルス定義データベースのアップデートサーバーを提供しています。ミラー機能とは、アップデートサーバーを複製したサーバーを社内に設置することで、各クライアントPCがインターネットに接続することなく、ウイルス定義データベースのアップデートを行える機能です。本節では、ミラー機能について説明します。

2.8.1 アップデートファイルの配布とミラー機能

ウイルスなど悪意のある不正なプログラムは、日々新種や亜種が登場しています。これらの脅威からコンピューターを守るには、常に最新のウイルス定義データベースが必要です。アップデートサーバーはそのために設置されています。また、アップデートサーバーは最新のウイルス定義データベースを配布するだけでなく、必要に応じてプログラムコンポーネントのアップデートの配布も行っています。

ミラー機能は、社内LANなどのローカルネットワーク内に、ウイルス定義データベースを配布するサーバーを設置することで実現します。各クライアントPCがローカルネットワーク内のミラーサーバーからアップデートすることにより、インターネット接続にかかわる回線の負荷が軽減されます。また、インターネットへの接続が制限されている環境や、ネットワークへの接続環境がないクライアントにも最新のウイルス定義データベースを提供しやすくなります（次ページ参照）。

ミラーサーバーは、ESET Remote Administrator Server（ERAS）またはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linux のいずれかを利用して構築します。ミラーサーバーは、規模に応じて複数台設置できます。たとえば、各拠点ごとに複数台のミラーサーバーを設置できます。なお、ミラーサーバーの構築にはラインセンスキーファイルの登録が必要です。

CAUTION

ESET Endpoint SecurityおよびMac OS X用プログラムのESET NOD32アンチウイルスは、ミラーサーバーの構築をサポートしていません。

2.8.2 アップデートファイルの配布方法

ミラーサーバーを構築してウイルス定義データベースやプログラムコンポーネントを配布する際には、以下の方法があります。利用環境に応じて、配布方法をご検討ください。なお、Mac OS X用プログラムのESET NOD32アンチウイルスは、HTTP経由によるアップデートのみをサポートします。他のアップデート方法はサポートしていないのでご注意ください。

<table>
<tr><th colspan="2">アップデート方法</th><th>概要</th><th>クライアントPC接続台数の目安※</th></tr>
<tr><td rowspan="6">HTTP経由によるアップデート</td><td>ERAS</td><td rowspan="4">ERASとESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxにはミラーサーバー機能が搭載されており、内蔵のHTTPサーバー機能を利用して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配布できます。この機能を利用すれば、別途Webサーバーを用意することなく、アップデートファイルを各クライアントPCに配布できます。アップデートファイルを提供する方法としては、これが最も簡単です。なお、この方法でアップデートファイルを配布する場合のクライアント数としては、ESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Serverを利用した場合は100台以下、ESET File Security for Linuxを利用した場合は1,000台以下、ERASを利用した場合は400台以下を推奨しています。</td><td>400台</td></tr>
<tr><td>ESET Endpoint アンチウイルス</td><td rowspan="2">100台</td></tr>
<tr><td>ESET File Security for Microsoft Windows Server</td></tr>
<tr><td>ESET File Security for Linux</td><td>1,000台</td></tr>
<tr><td>Microsoft Internet Information Services (IIS)</td><td rowspan="2">ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxがミラーサーバー用に取得した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、IISまたはApacheのWebサーバーで配布する方法です。この方法は、Webサーバーに搭載された帯域制御機能や同時接続制御機能などを利用することでネットワーク負荷を制御できるというメリットがあります。大量のクライアントPCが同時にアップデートを行う可能性がある場合に効果的な方法です。なお、この方法でアップデートファイルを配布する場合のクライアント数としては、3,000台以下を推奨しています。</td><td rowspan="2">3,000台</td></tr>
<tr><td>Apache</td></tr>
<tr><td rowspan="3">共有フォルダーを利用したアップデート</td><td>ERAS</td><td rowspan="4">ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Serverがミラーサーバー用に取得した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共有フォルダーに保存し、各クライアントPCがファイル共有機能を利用してアップデートを行う方法です。</td><td>—</td></tr>
<tr><td>ESET Endpoint アンチウイルス</td><td rowspan="2">—</td></tr>
<tr><td>ESET File Security for Microsoft Windows Server</td></tr>
<tr><td colspan="2">他のPCの共有フォルダーを利用したアップデート</td><td>—</td></tr>
<tr><td colspan="2">リムーバブルメディアを利用したアップデート</td><td>ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxがミラーサーバー用に取得した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USBメモリーやCD-Rなどに保存し、各クライアントPCのアップデートを行う方法です。クライアントPCが既存のネットワークと切り離されている場合や、スタンドアロンで利用されている場合にこの方法を利用します。なお、アップデートファイルは、ユーザーズサイトでも提供しています。</td><td>—</td></tr>
</table>

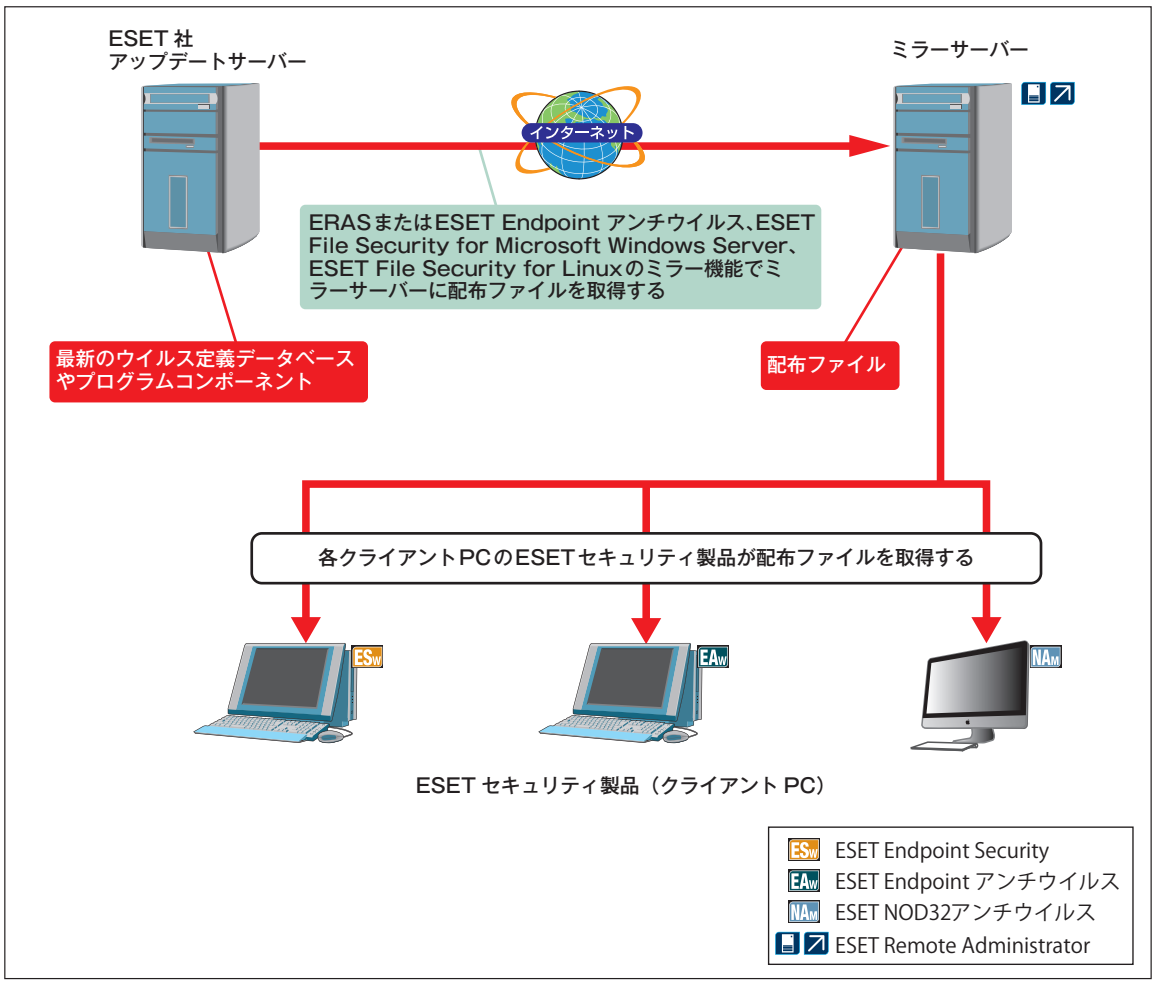
※ ミラーサーバー 1 台あたりのクライアント PC 接続台数です。

2.8.3 ミラーサーバーの構成例

ここではミラーサーバーの構成例として、ミラーサーバーを1台設置する場合と、2台以上設置する場合を紹介します。実際には、ご利用の規模に応じて設置するミラーサーバーの台数をご検討ください。なお、ミラーサーバーの設置にはインターネット接続環境が必要になります。

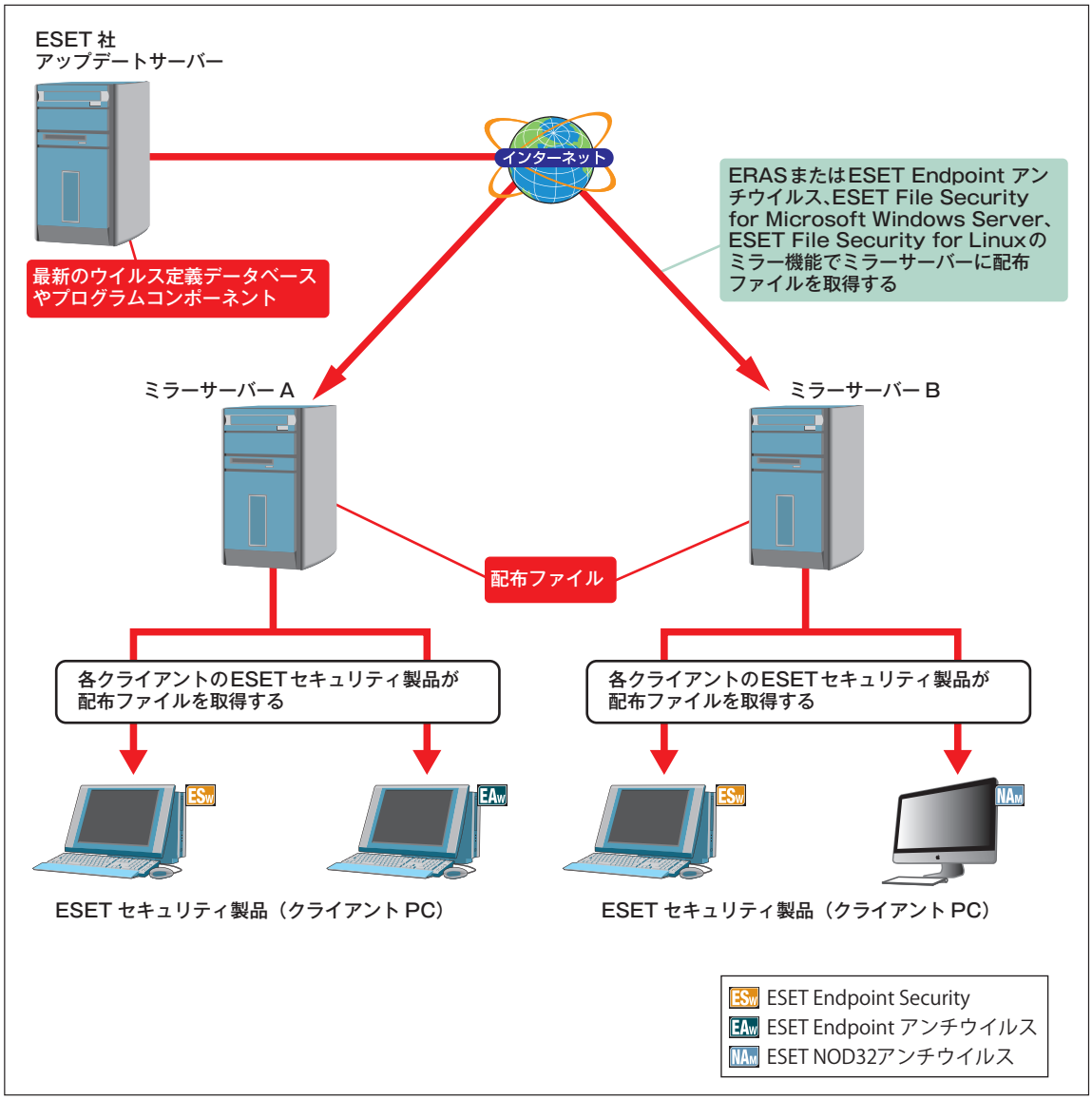
2.8.3.1 ミラーサーバーの構成例1～ミラーサーバーが1台の場合

ミラーサーバーに設定したコンピューターが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取得します。各クライアントPCは、ミラーサーバー上の配布ファイルを取得します。



2.8.3.2　ミラーサーバーの構成例2～ミラーサーバーが2台以上の場合

ミラーサーバーに設定したコンピューターが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取得します。各クライアントPCは利用環境に応じて、アップデート先のミラーサーバーを設定します。



2.8.4 ミラーサーバー構築時の注意点

ミラーサーバーを構築する場合、ネットワーク構成によっては問題が発生する場合があります。ここでは、ミラーサーバー構築時の注意点を説明します。

2.8.4.1 ライセンスキーファイル

ミラーサーバーの構築には、ラインセンスキーの登録が必要です。ライセンスキーファイルは弊社ユーザーズサイトからダウンロードできます。詳しくは、「ESET ライセンス製品 ご利用の手引」をご参照ください。

2.8.4.2 プロキシサーバーが設置されている場合

インターネット接続にプロキシサーバーを利用している場合、ミラーサーバーを構築するERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxにプロキシ設定を行ってください。プロキシ設定の方法ついては、ERASまたはESET Endpoint アンチウイルス、ESET File Security for Microsoft Windows Server、ESET File Security for Linuxのユーザーズマニュアルをご参照ください。
なお、ウイルス定義データベースのファイル(*.nup)は、プロキシサーバーなどで強制キャッシュを行わないように設定してください。プロキシサーバーなど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に不整合を起こす可能性があります。

2.8.4.3 プログラムコンポーネントのダウンロード設定について

ERASのミラーサーバーの既定値では、プログラムコンポーネント(ESET セキュリティ製品のバージョンアッププログラム)のアップデート用ファイルのダウンロードを行いません。ESET Endpoint アンチウイルスおよびESET File Security for Microsoft Windows Server、ESET File Security for Linuxのミラーサーバーは、ダウンロードする前に確認ダイアログが表示されます。また、プログラムコンポーネントをダウンロードし、配布したい場合は、必要なコンポーネントを設定します。
ただし、製品の新しいバージョンが公開されても、必ずしもコンポーネントアップデートが行われるわけではありません。その場合は、アップデート用のプログラムコンポーネントは表示されません。

2.8.4.4 共有フォルダーを利用する場合

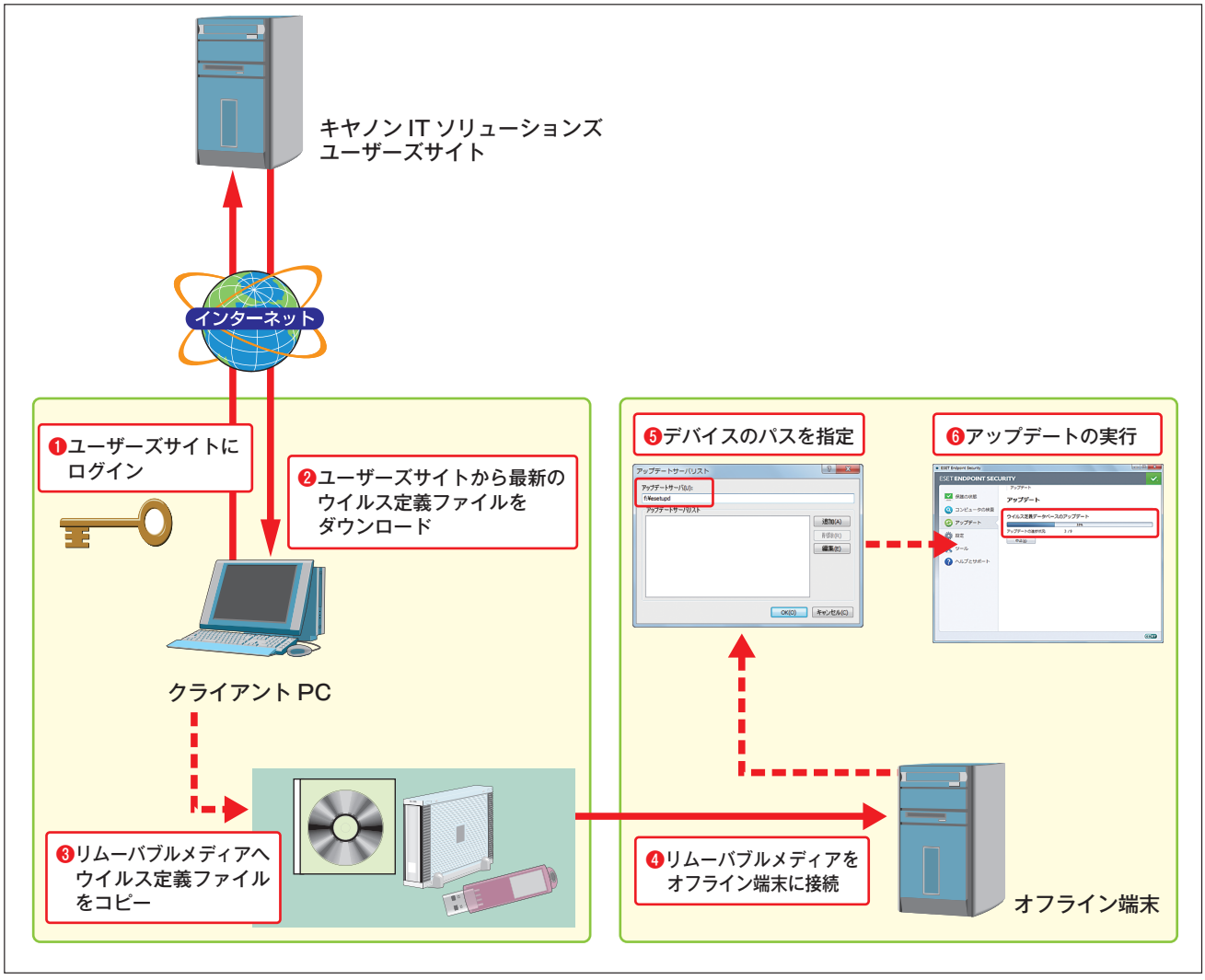
ファイル共有機能を利用してアップデートを行う場合は、共有フォルダーへのアクセス権限を適切に設定してください。アクセス権限の設定が間違っていると、共有フォルダーにアクセスできずアップデートを行えないことがあります。なお、Mac OS X用プログラムのESET NOD32アンチウイルスおよびESET File Security for Linuxは、共有フォルダーからのアップデートをサポートしていません。

2.8.4.5 リムーバブルメディアを利用する場合

Mac OS X用プログラムのESET NOD32アンチウイルスおよびESET File Security for Linuxは、リムーバブルメディアからのアップデートをサポートしていません。

2.8.5　オフライン環境での更新

セキュリティ上の問題などでインターネットやミラーサーバに接続できないオフライン環境のコンピューターは、USBメモリーやCD-Rなどのリムーバブルメディアを利用してアップデートを行います。アップデート用のファイルは弊社ユーザーズサイトから入手する方法と、ミラーサーバーに保存されたファイルを使用する方法があります。弊社ユーザーズサイトから、アップデート用のファイルを取得しUSBメモリーやCD-Rなどのリムーバブルメディアを利用したアップデートは、以下のような流れで行います。



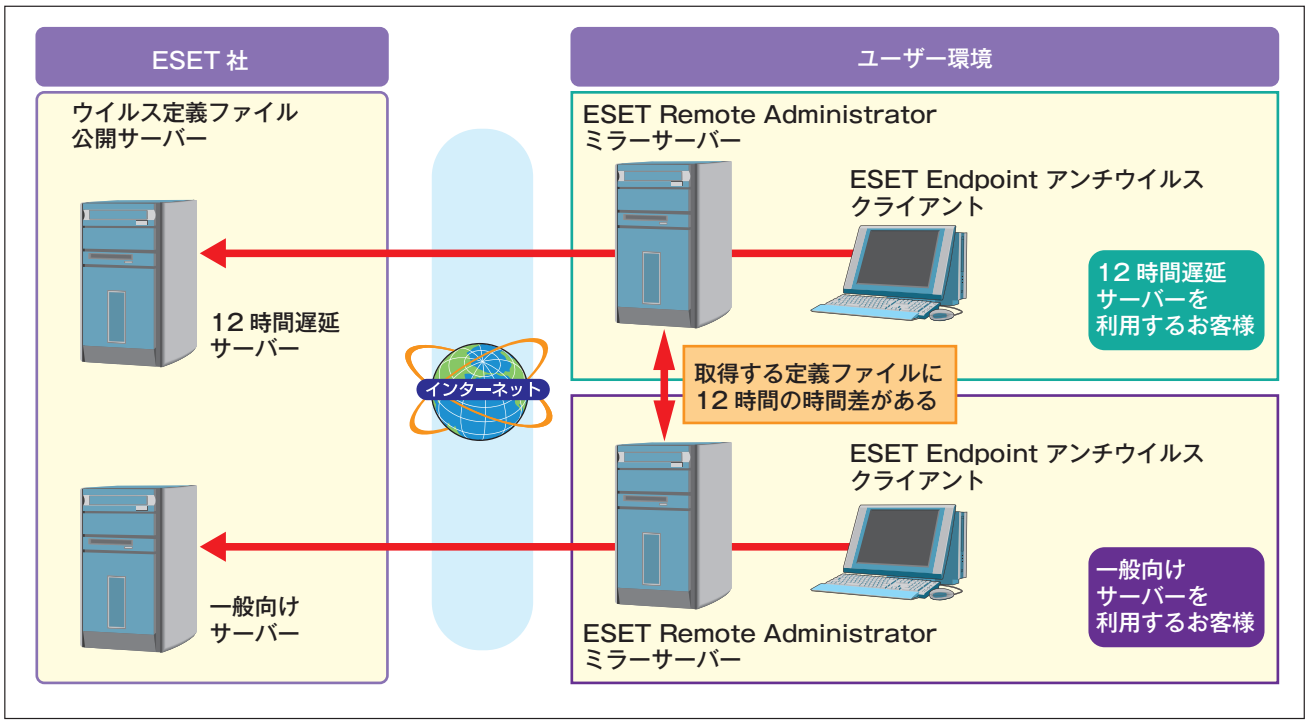
※詳細な手順については、弊社ユーザーズサイトに掲載されている「オフライン更新手順書(http://canon-its.jp/product/eset/users)」を参照ください。また、ミラーサーバーに保存された配布用ファイルを使用する場合はこちらのURL（http://canon-its.jp/supp/eset/est00000031.html）を参照ください。

2.8.6 ウイルス定義データベースの時差配信

ウイルス定義データベースの時差配信を行うことで、ウイルス定義データベースの障害や誤検知などのリスクを軽減できます。ウイルス定義データベースの時差配信は、ESET Remote Administrator（ERA）およびESET Endpoint アンチウイルスに搭載された「遅延アップデート」を利用する方法と多段構成でミラーサーバーを構築する方法があります。

2.8.6.1 遅延アップデートを利用した時差配信

ERAおよびESET Endpoint アンチウイルスには、「遅延アップデート」機能が搭載されています。遅延アップデート機能とは、一般向けに公開されているウイルス定義データベースより一定時間（12時間）遅らせたウイルス定義データベースをESET社のアップデートサーバーから取得する機能です。この機能を利用してミラーサーバーを構築すると、常に一定時間（12時間）遅らせたウイルス定義ファイルを公開できます。この機能により、誤検知などのリスクを軽減できます。遅延アップデートの詳細については、ERAまたはESET Endpoint アンチウイルスのユーザーズマニュアルをご参照ください。

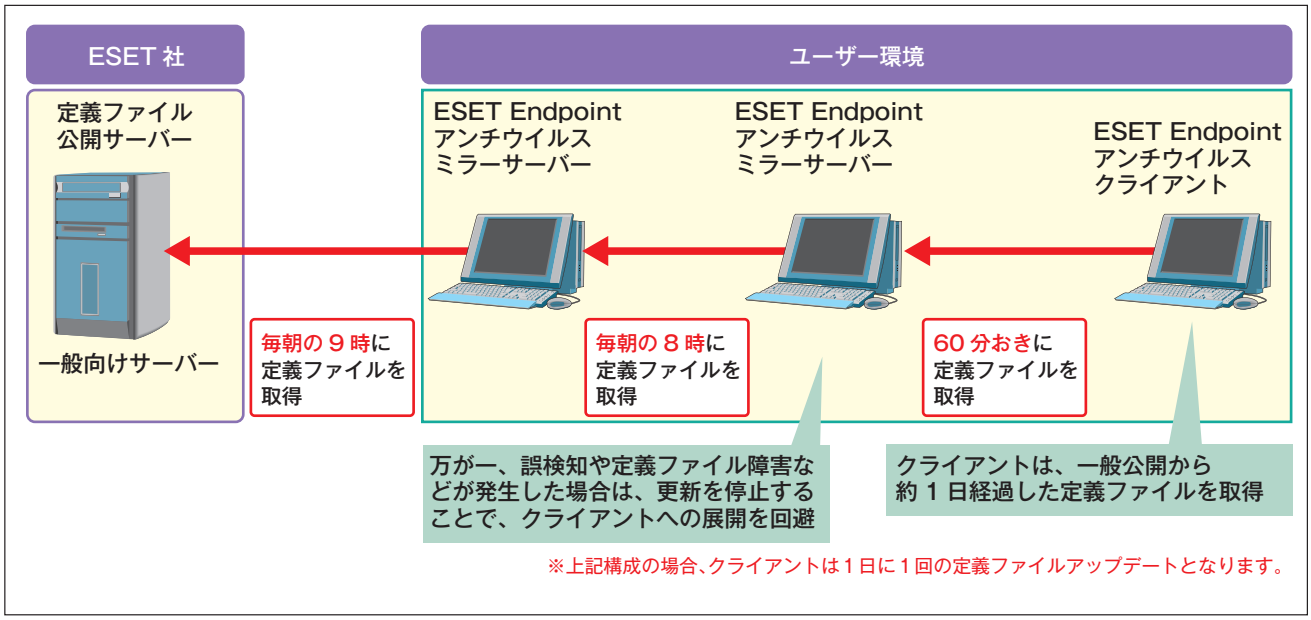


※遅延アップデート機能は、ESET Remote Administrator V5.0およびESET Endpoint アンチウイルスでのみサポートされます。ESET File Security for Microsoft Windows Server、ESET File Security for Linuxはこの機能を搭載していません。

※遅延アップデートを行うと、常に一定時間（12時間）前の古いウイルス定義データベースを利用するためウイルス感染などのリスクが増加しますのでご注意ください。

2.8.6.2　ミラーサーバーの多段構成による時差配信

ミラーサーバーを多段構成で設置し、ウイルス定義データーベースの取得時間をずらすことで、ウイルス定義データーベース配信を任意の時間ずらす構成を組むことができます。ミラーサーバーを多段構成で利用する場合は、以下のような構成でミラーサーバーを構築します。



※ウイルス定義データベースの時差配信を行うと、古いウイルス定義データベースを利用するためウイルス感染などのリスクが増加しますのでご注意ください。

2.9 Android端末の管理

ESET Endpoint Security for AndroidがインストールされたAndroid端末をESET Remote Administrator(ERA)で識別し管理する方法を説明します。

2.9.1 Android端末の識別

Android端末をERAに接続した場合に登録されるクライアント名(コンピュータ名)は、SIMカードを挿入できるAndroid端末の場合は、IMEI(International Mobile Equipment Identity)またはMEID(Mobile Equipment Identifier)となり、SIMカードを挿入できないAndroid端末の場合はWi-Fi MACアドレスとなります。
また、ERAに登録されるMACアドレスはAndroid端末のWi-Fi MACアドレスとなります。
これらはアルファベットと数字で構成されており、複数台のAndroid端末を管理する場合、クライアント名(コンピュータ名)がどのAndroid端末に対応しているかを識別しにくいため、クライアント名を任意の識別しやすい名前に変更することをおすすめします。

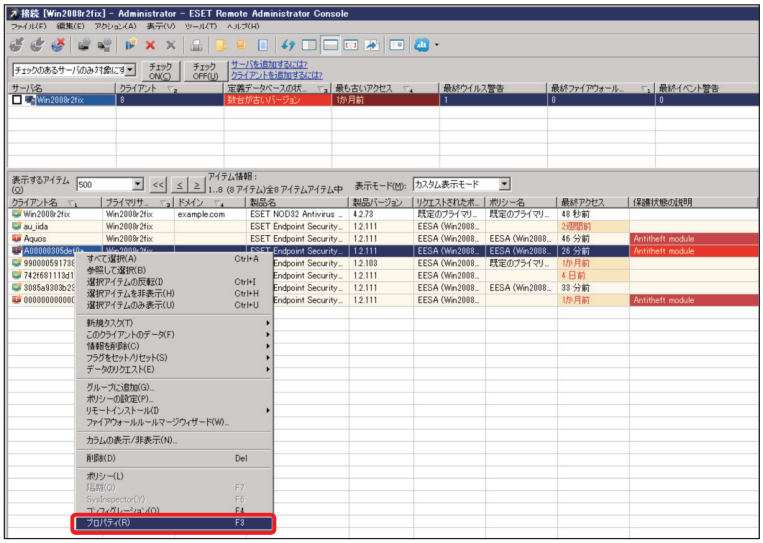
1 事前にAndroid端末のIMEI、MEIDまたはWi-Fi MACアドレスを確認します。

SIMカードを挿入できるAndroid端末:IMEIまたはMEID (ご利用の携帯電話事業者によって変わります)
SIMカードを挿入できないAndroid端末:Wi-Fi MACアドレス

POINT

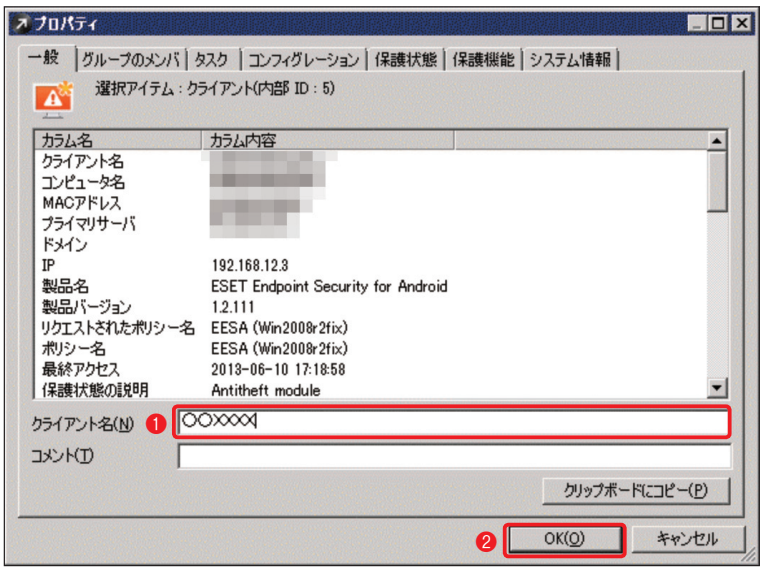
IMEI、MEIDおよびWi-Fi MACアドレスは、Android端末で、[設定]>[端末情報]>[端末の状態]>[IMEI]、[MEID]または[Wi-Fi MACアドレス]で確認できます。端末によっては操作が異なる場合がございます。

2



ERACの[クライアント]タブで、事前に確認したIMEIなどからAndroid端末を特定し、該当のクライアントを選択して、右クリックから[プロパティ]をクリックします。

3



❶ [一般] タブの [クライアント名] に任意の識別しやすいクライアント名を入力し
❷ [OK] をクリックします。

[Chapter 3]
ERA のログ管理

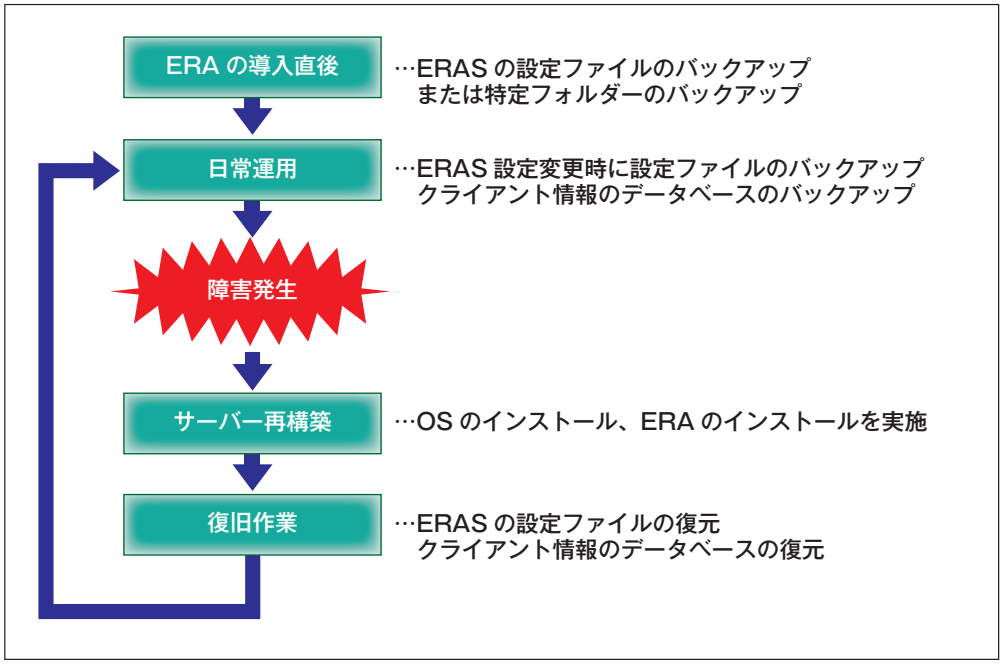
3.1 障害対策のポイント

ESET Remote Administrator（ERA）のバックアップを取得しておくと、管理サーバーに障害が発生した場合の復旧に利用できます。ここでは、サーバーの障害対策について説明します。

3.1.1 バックアップを利用したサーバーの復旧

ERAをインストールした管理サーバーに何らかの障害が発生したときに有効なのが、バックアップを用いたサーバーの復旧です。バックアップがあれば、ERAをインストールした管理用サーバーコンピューターを、他のサーバーコンピューターに復元できます。ERA導入直後にバックアップを作成しておきます。設定変更を行ったときや日常運用でも定期的にバックアップを作成しましょう。

ESET Remote Administrator Server（ERAS）の動作設定やクライアント情報のデータベースのバックアップは、ERASと共にインストールされる「ESET Remote Administrator Maintenance Tool（ERAメンテナンスツール）」を利用することでバックアップを作成できるほか、ERASがインストールされたフォルダーを手動でバックアップすることで行えます。また、ESET Remote Administrator Console（ERAC）の設定情報のバックアップは、ERACがインストールされたフォルダーを手動でバックアップすることで行えます。



▲管理サーバーのバックアップと障害復旧作業の標準的なステップ

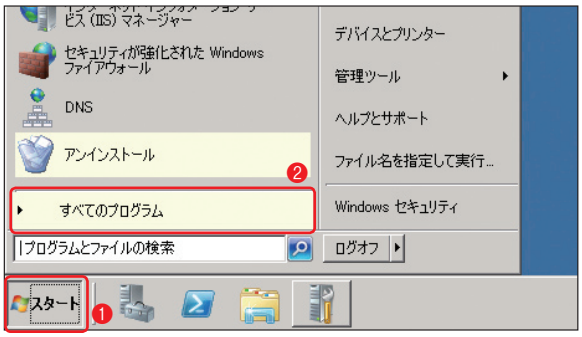
3.2 バックアップの作成

ここでは、ESET Remote Administrator Server（ERAS）の設定ファイルおよびクライアント情報のデータベースをバックアップする方法を説明します。

3.2.1 ERASの設定ファイルのバックアップ作成手順

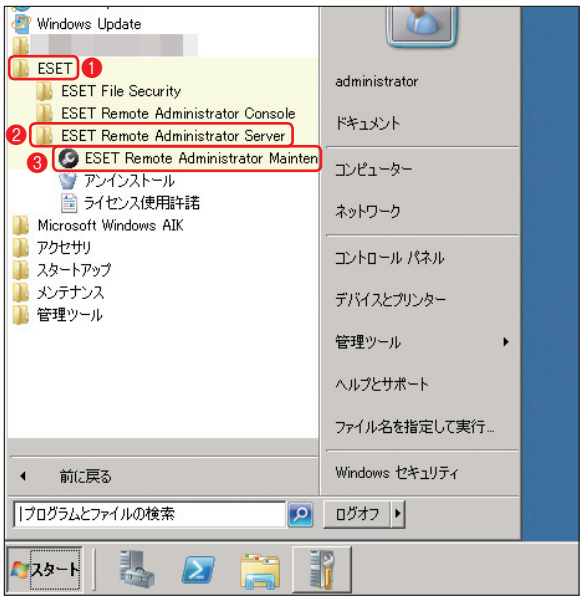
ここでは、ERAメンテナンスツールを利用して、ERASの設定ファイルのバックアップを作成する手順を説明します。ESET Remote Administrator Maintenance Tool（ERAメンテナンスツール）は、ERASをインストールした管理サーバーにインストールされているため、すべての作業を管理サーバーで行います。バックアップ作成の際は、同じコンピューターにESET Remote Administrator Console（ERAC）もインストールして、以下の手順を行ってください。

1



❶管理サーバーの［スタート］ボタンをクリックし、❷［すべてのプログラム］をクリックします。

2

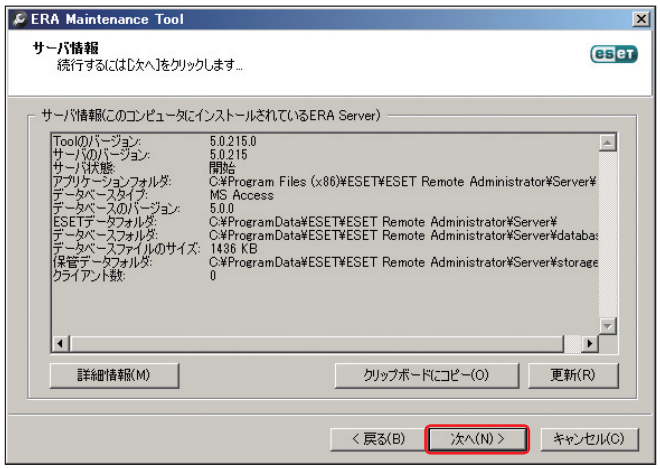


ERAメンテナンスツールを起動します。❶［ESET］、❷［ESET Remote Administrator Server］、❸［ESET Remote Administrator Maintenance Tool］と順にクリックします。

3

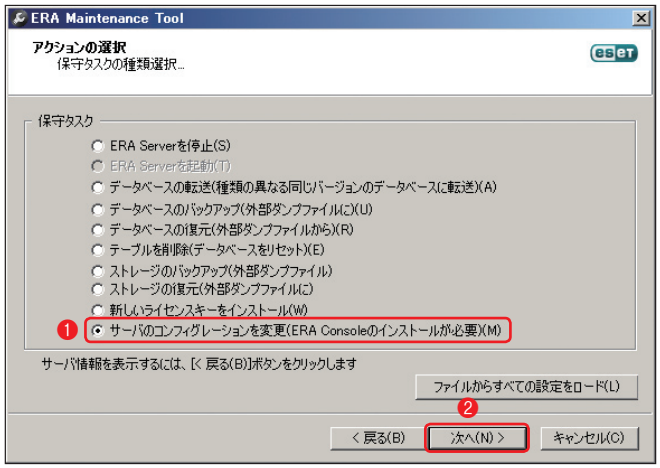
ERAメンテナンスツールが起動します。[次へ] ボタンをクリックします。

4



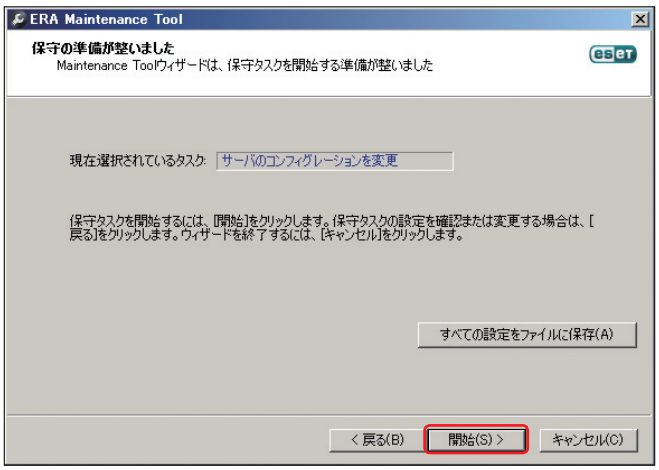
[サーバ情報] ダイアログが表示されます。[次へ] ボタンをクリックします。

5



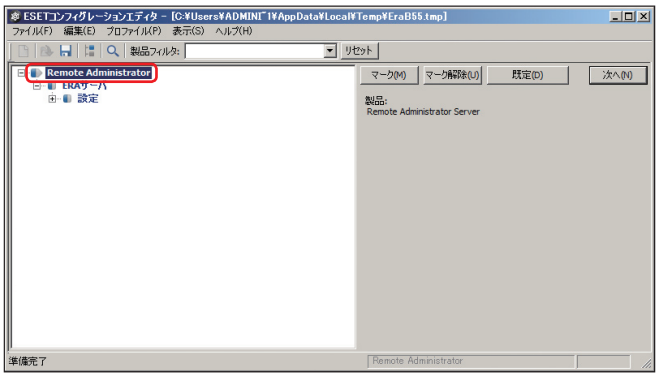
[アクションの選択] ダイアログが表示されます。❶ [サーバのコンフィグレーションを変更] にチェックを入れ、❷ [次へ] ボタンをクリックします。

6



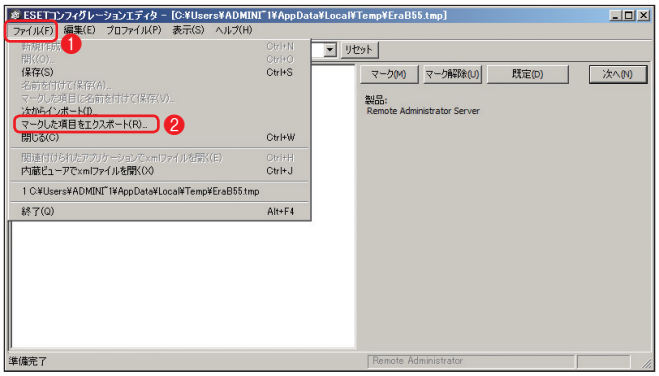
[開始] ボタンをクリックします。

7



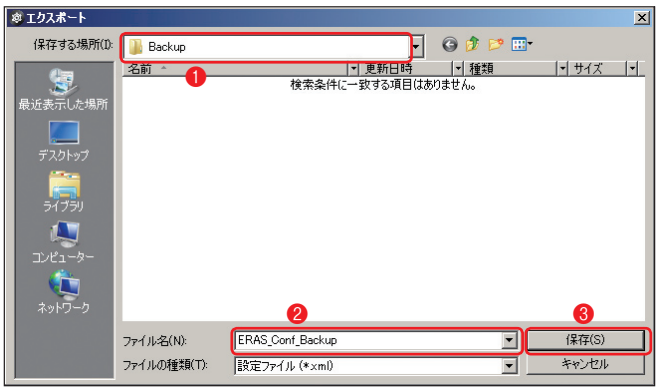
ESET コンフィグレーションエディターが起動します。[Remote Administrator] をクリックします。

8



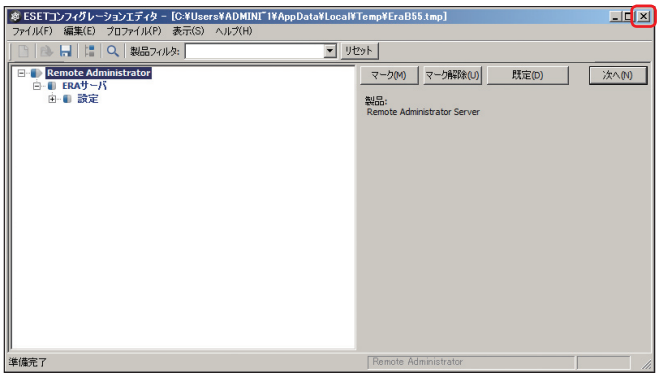
❶ [ファイル] メニュー、❷ [マークした項目をエクスポート] をクリックします。

9



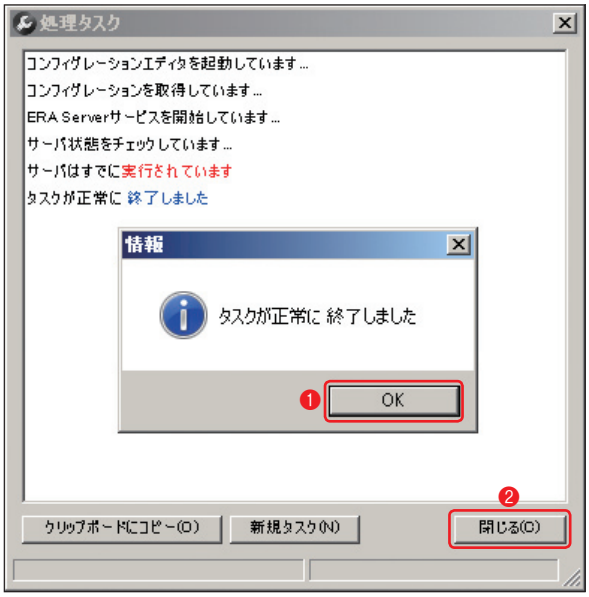
設定ファイルを保存します。❶保存先を選択して、❷ファイル名を入力し、❸ [保存] ボタンをクリックします。

10



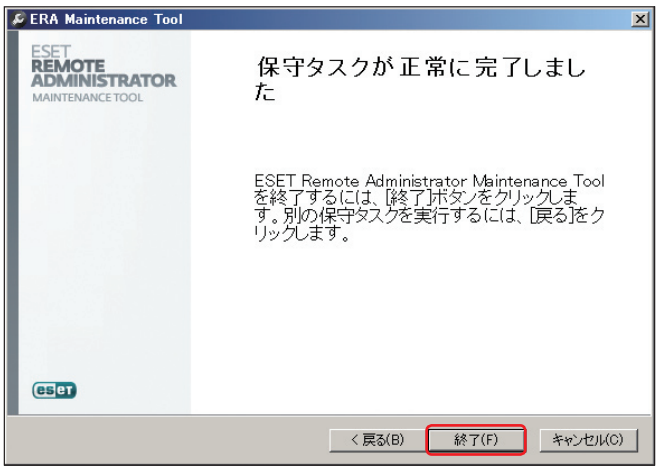
[×] ボタンをクリックして、ESET コンフィグレーションエディターを終了します。

11



ダイアログが表示されます。❶[OK] ボタンをクリックし、[処理タスク] ダイアログの❷ [閉じる] ボタンをクリックします。

12



ERAメンテナンスツールを終了します。[終了] ボタンをクリックします。

POINT

ERASの設定は、ERACを利用することでも保存できます。ERACを利用してERASの設定を保存する場合は、[ツール] メニュー、[サーバオプション] をクリックし、[サーバオプション] ダイアログを開きます。[詳細] タブをクリックし、[詳細設定を編集] ボタンをクリックするとESET コンフィグレーションエディターが開くので、97 ～ 98ページの手順7～9を参考に設定ファイルを保存してください。

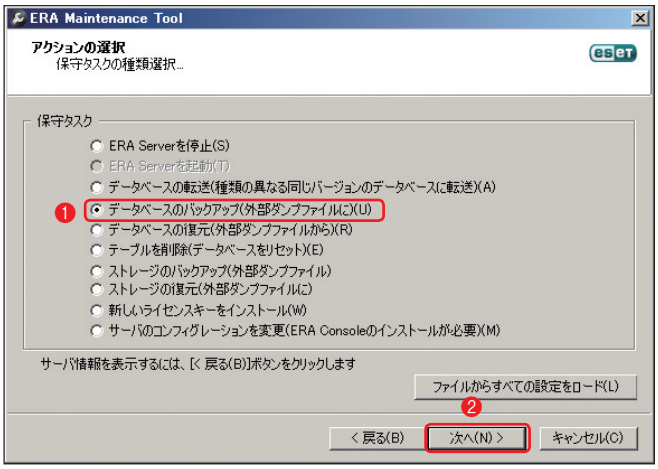
3.2.2 クライアント情報のデータベースのバックアップ作成手順

ここでは、ERAメンテナンスツールを利用してクライアントPCのログのバックアップを作成する手順を説明します。ERAメンテナンスツールはERASをインストールした管理サーバーにインストールされているため、すべての作業を管理サーバーで行います。

CAUTION

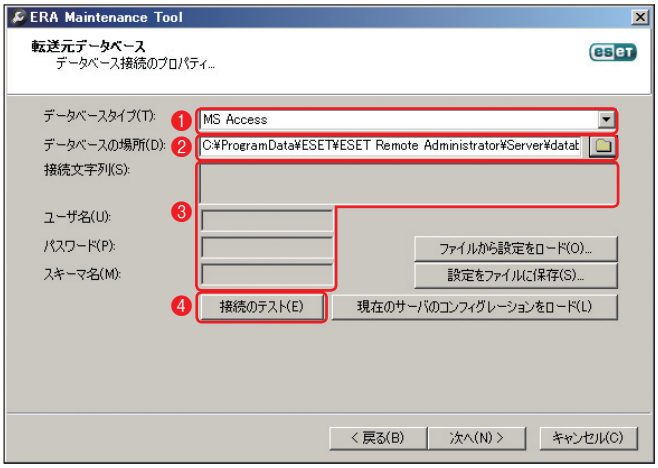
クライアントPCのログのバックアップを作成しているときは、ERASの動作が停止します。

1



95～96ページの手順1～3を参考に、ERAメンテナンスツールを起動し、[アクションの選択] ダイアログを開きます。❶ [データベースのバックアップ] にチェックを入れ、❷ [次へ] ボタンをクリックします。

2

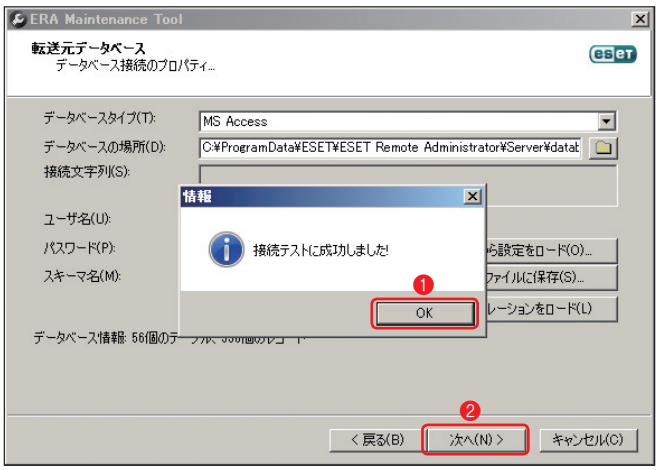


バックアップするデーターベースを設定します。❶ [データベースタイプ] および❷ [データベースの場所] を選択します。❸ [接続文字列] [ユーザ名] [パスワード] [スキーマ名] など接続に必要な情報を設定します。すべての設定を行ったら、❹ [接続のテスト] ボタンをクリックします。

POINT

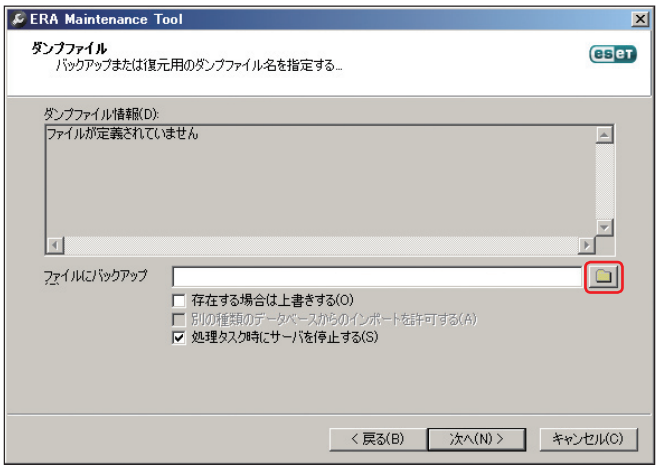
ERASの既定値のデータベースである「Microsoft Access」を利用し、かつデータベースの保存場所を変更していない場合は、この設定を行う必要はありません。また、Microsoft Access以外のデータベースを利用している場合は、[接続文字列] や [ユーザ名] [パスワード] [スキーマ名] などを正確に入力しないとバックアップが行えません。

3



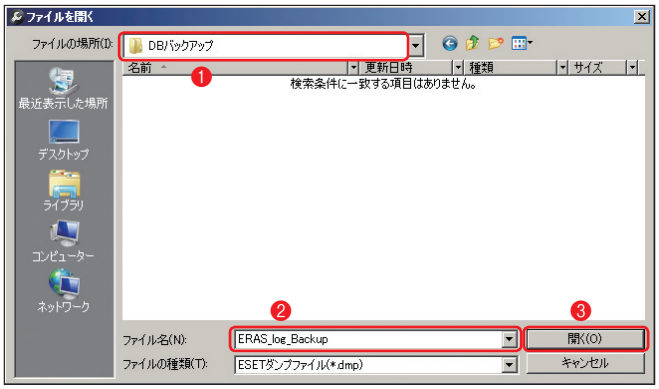
ダイアログが表示されます。❶[OK]ボタンをクリックします。[転送元データベース] ダイアログに戻ります。❷ [次へ] ボタンをクリックします。

4



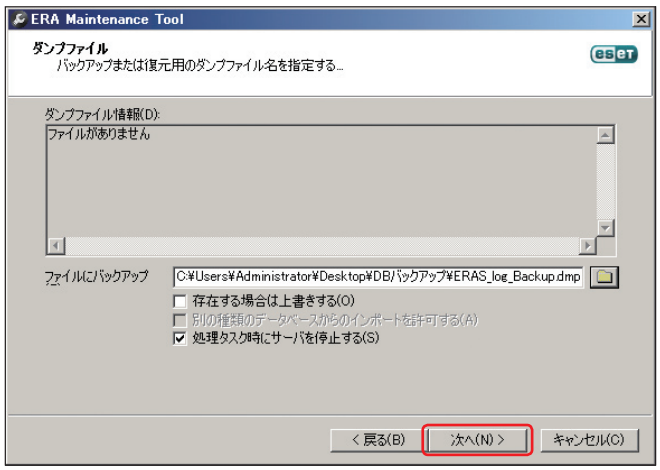
[ダンプファイル]ダイアログが表示されます。[ファイルを参照] ボタンをクリックします。

5



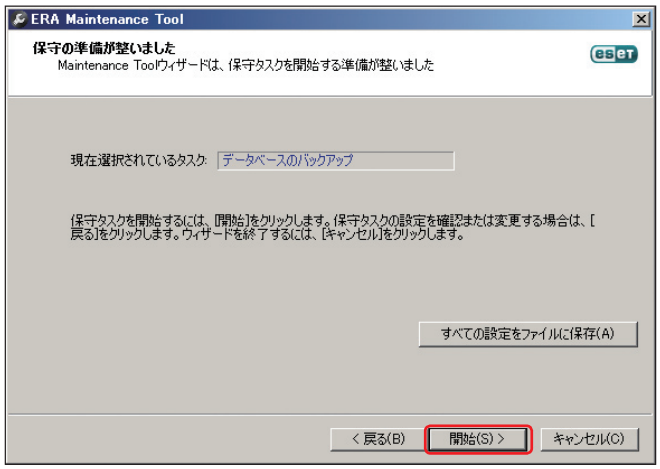
ファイルの保存先を設定します。❶保存先を選択して、❷ファイル名を入力し、❸ [開く] ボタンをクリックします。

6



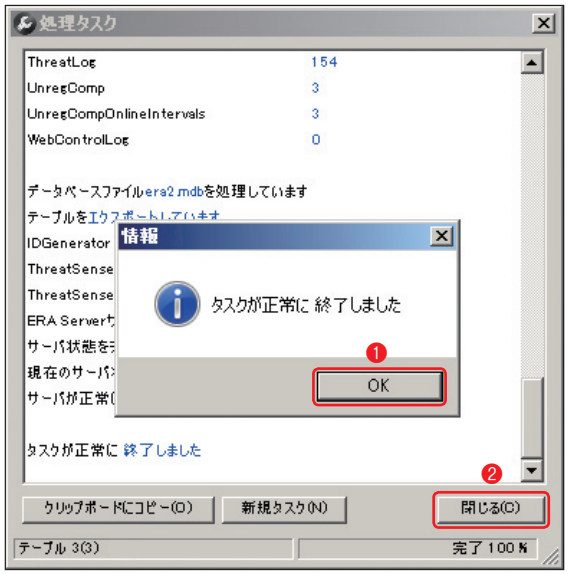
[次へ] ボタンをクリックします。

7



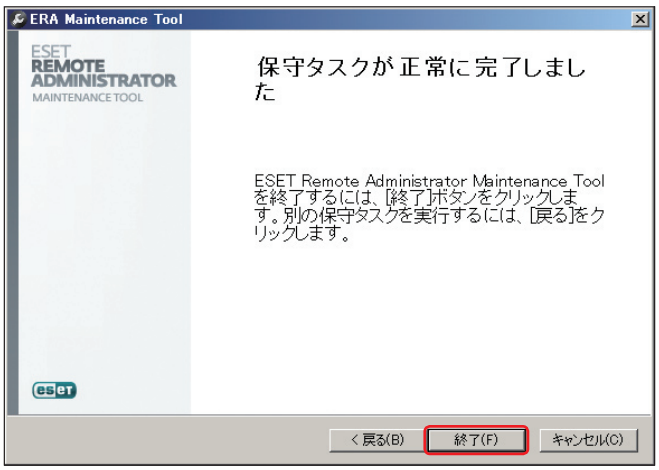
[開始] ボタンをクリックします。

8



バックアップが完了すると、ダイアログが表示されます。❶ [OK] ボタンをクリックし、[処理タスク] ダイアログの❷ [閉じる] ボタンをクリックします。

9



ERAメンテナンスツールを終了します。[終了] ボタンをクリックします。

3.2.3 データフォルダーのバックアップ方法

ERASおよびERACは、特定のデータフォルダーをバックアップすることで各種設定や情報などをバックアップできます。ERASは、インストール時に既定の内蔵DB（Microsoft Access)をデータベースに選択した場合に限って、以下のデータフォルダーをバックアップすることで、取得したクライアント情報、ログなどの全ての情報をバックアップできます。データベースにMicrosoft SQL Server 2005 Express Edition / Standard Editionなどの既定の内蔵DB（Microsoft Access)以外を利用している場合は、以下のフォルダーをバックアップしても取得したクライアント情報、ログなどを記録したデータベースはバックアップされません。既定の内蔵DB以外を利用している場合は、利用しているデータベースのマニュアルなどを参考にデータベースのバックアップを別途行なってください。なお、リストア（復元）は、バックアップしたフォルダーをバックアップ時と同じフォルダーに上書きすることで行えます。

Windows Server 2003の場合

ERAS	C:￥Documents and Settings￥All Users￥Application Data￥ESET￥ESET Remote Administrator￥Server
ERAC	C:￥Documents and Settings￥All Users￥Application Data￥ESET￥ESET Remote Administrator￥Console

Windows Server 2008 ／ 2008 R2の場合

ERAS	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Server
ERAC	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Console

Windows Server 2012 Standardの場合

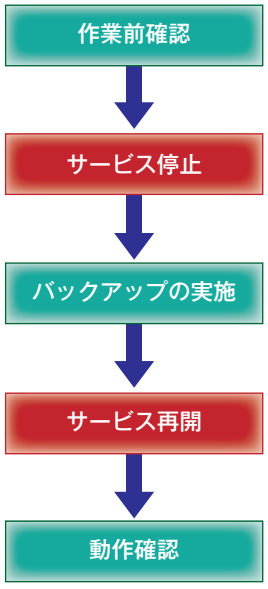
ERAS	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Server
ERAC	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Console

CAUTION

バックアップするERAとリストアするERAのホスト名およびバージョンが同一でないとリストア後に正常に動作しません。サーバー環境を再構築する場合は、必ず同じホスト名とバージョンに設定してください。

3.2.4 データフォルダーのバックアップ方法の流れ

ERASおよびERACのデータフォルダーをバックアップするときは、以下の流れで作業します。ERASのバックアップを行うときは、ERASのサービスを停止する必要がある点にご注意ください。



…❶対象ファイルの保存場所を確認します。

…❷ERAS の動作を停止します。ESET Remote Administrator Maintenance Tool を利用して動作を停止します。

…❸任意の保存先に上記のフォルダー内のファイルを全てバックアップします。

…❹バックアップが終了したら、停止させていた「ESET Remote Administrator Server」の動作を再開します。動作の再開は、ESET Remote Administrator Maintenance Tool を利用します。

…❺ERAC で ERAS に接続して「ESET Remote Administrator Server」の稼働が再開しているかを確認します。

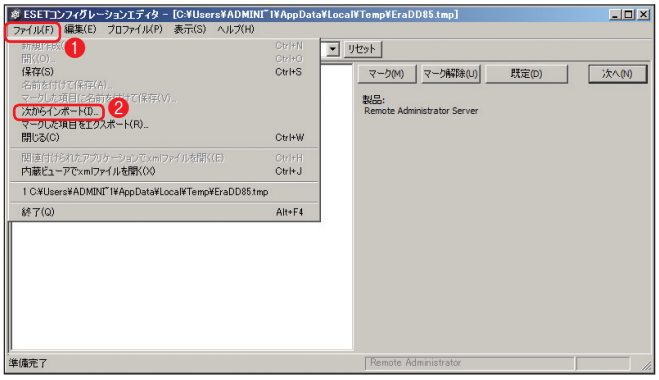
3.3 バックアップファイルの復元

ここでは、バックアップしたERASの設定ファイルおよびクライアント情報のデータベースを復元する方法を説明します。

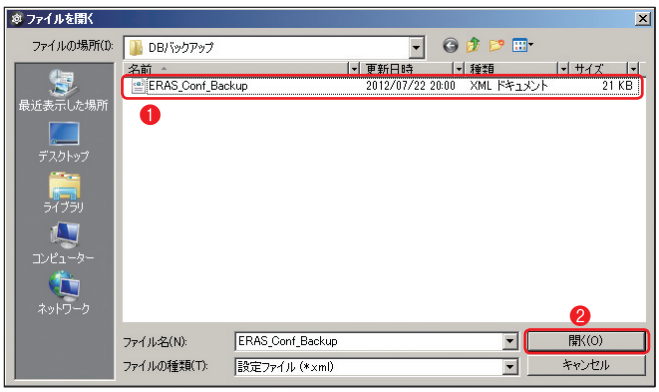
3.3.1 バックアップしたERASの設定ファイルの復元手順

ここでは、バックアップしたERASの設定ファイルを復元する手順を説明します。ERAメンテナンスツールはERASをインストールした管理サーバーにインストールされているため、バックアップの作成時と同様にすべての作業を管理サーバーで行います。

1 95～96ページの手順1～5を参考に、ERAメンテナンスツールを起動し、[サーバーのコンフィグレーションを変更] を選択して手順を進め、ESET コンフィグレーションエディターを起動します。

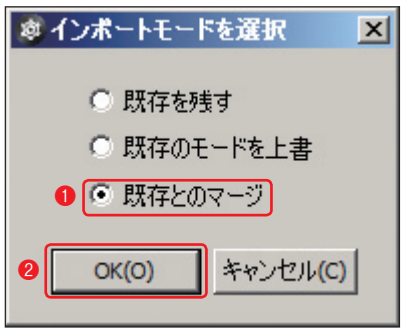
2 

❶ [ファイル] メニュー、❷ [設定ファイルをインポート] をクリックします。

3 

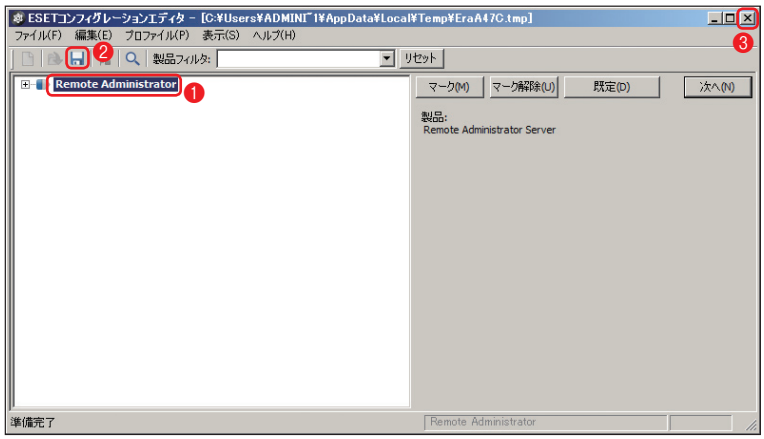
設定ファイルを選択します。❶バックアップしておいた設定ファイルを選択し、❷ [開く] ボタンをクリックします。

4



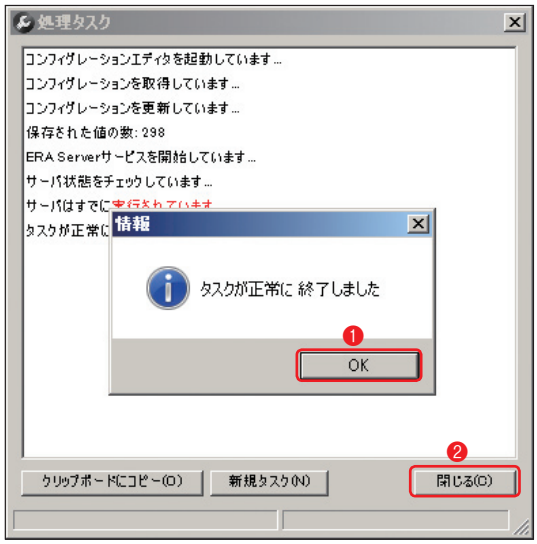
ダイアログが表示されます。❶[既存とのマージ] にチェックが入っていることを確認し、❷[OK] ボタンをクリックします。

5



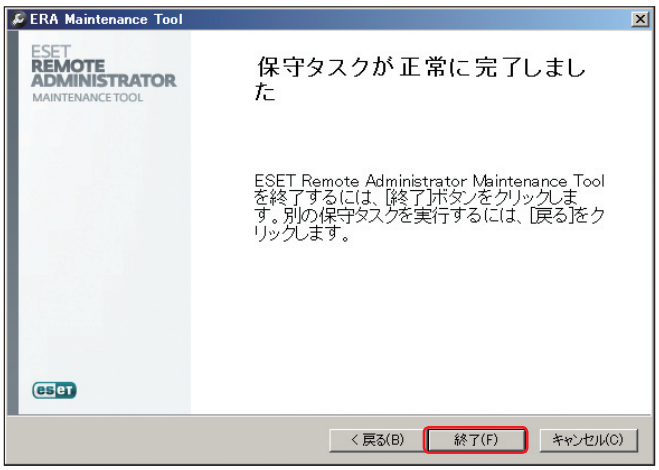
❶[ESET Remote Administrator] をクリックし、❷[保存] ボタンをクリックします。続いて❸[×] ボタンをクリックし、ESET コンフィグレーションエディターを終了します。

6



ダイアログが表示されます。❶[OK] ボタンをクリックし、❷[処理タスク] ダイアログの [閉じる] ボタンをクリックします。

7



ERAメンテナンスツールを終了します。[終了] ボタンをクリックします。

POINT

設定ファイルの復元は、ERACからも行うことができます。ERACを利用してERASの設定を復元する場合は、[ツール] メニュー、[サーバオプション] をクリックし、[サーバオプション] ダイアログを開きます。[詳細] タブをクリックし、[詳細設定を編集] ボタンをクリックするとESET コンフィグレーションエディターが開くので、手順2～5を参考に設定ファイルをインポートします。次に、[コンソール] ボタンをクリックしてダイアログが表示されたら、[はい] ボタンをクリックします。これで設定が復元されます。

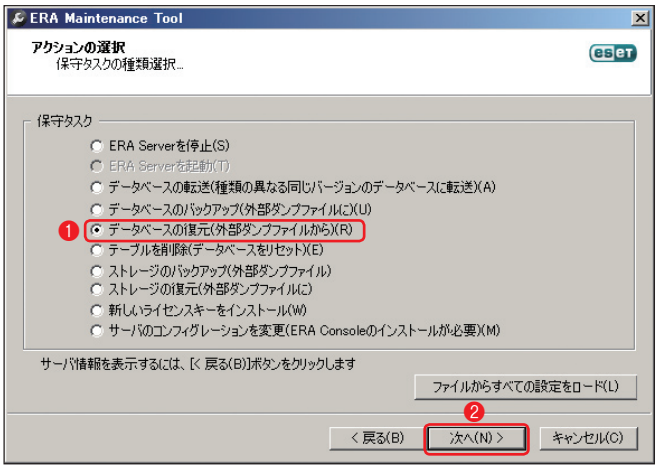
3.3.2 バックアップしたクライアント情報のデータベースの復元手順

ここでは、バックアップしたクライアント情報のデータベースをERASに復元する手順を説明します。復元には、ERAメンテナンスツールを利用します。ERAメンテナンスツールはERASをインストールした管理サーバーにインストールされているため、すべての作業を管理サーバーで行います。

CAUTION

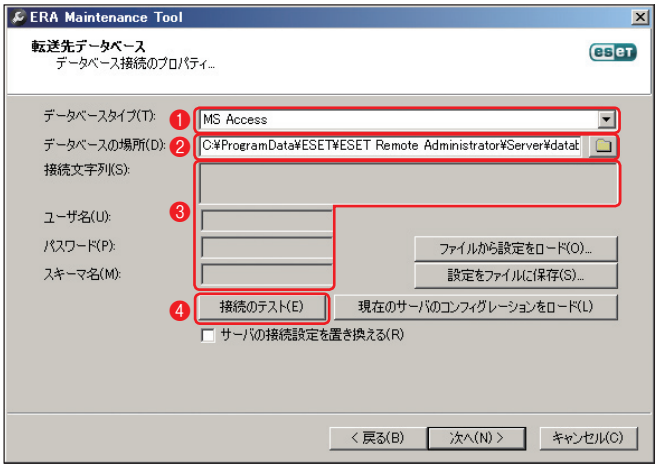
クライアントPCのログを復元しているときは、ERASの動作が停止します。

1



95～96ページの手順1～3を参考に、ERAメンテナンスツールを起動し、[アクションの選択] ダイアログを開きます。❶ [データベースの復元] にチェックを入れ、❷ [次へ] ボタンをクリックします。

2

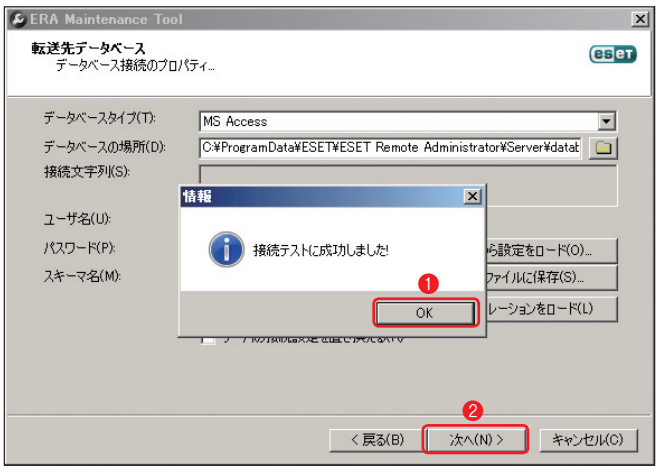


復元先のデーターベースを設定します。❶ [データベースタイプ] および❷ [データベースの場所] を選択します。❸ [接続文字列] [ユーザ名] [パスワード] [スキーマ名] など接続に必要な情報を設定します。すべての設定を行ったら、❹ [接続のテスト] ボタンをクリックします。

▸▸▸ POINT

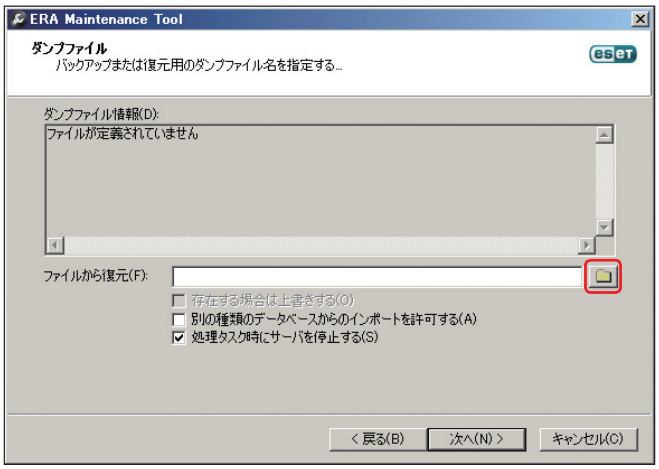
ERASの既定値のデータベースである「Microsoft Access」を利用し、かつデータベースの保存場所を変更していない場合は、この設定を行う必要はありません。また、Microsoft Access以外のデータベースを利用している場合は、[接続文字列] や [ユーザ名] [パスワード] [スキーマ名] などを正確に入力しないとデータベースの復元が行えません。

3



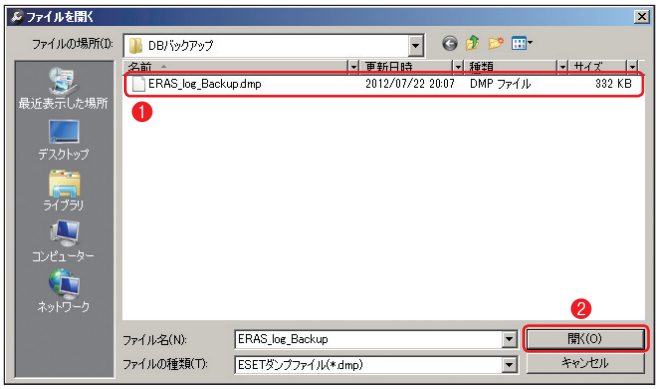
ダイアログが表示されます。❶[OK]ボタンをクリックします。[転送元データベース] ダイアログに戻ります。❷ [次へ] ボタンをクリックします。

4



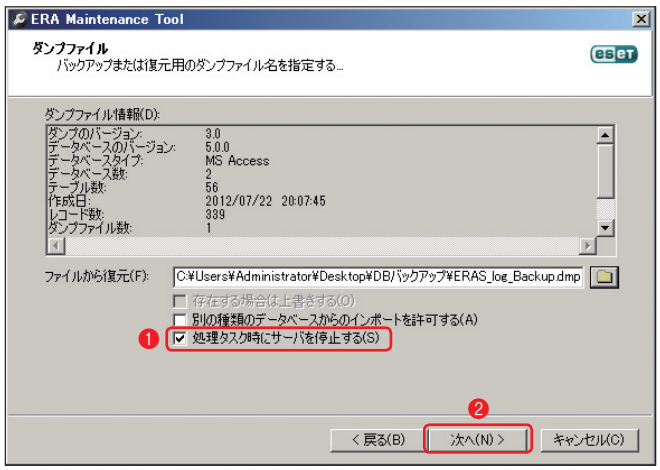
[ダンプファイル]ダイアログが表示されます。[ファイルを参照] ボタンをクリックします。

5



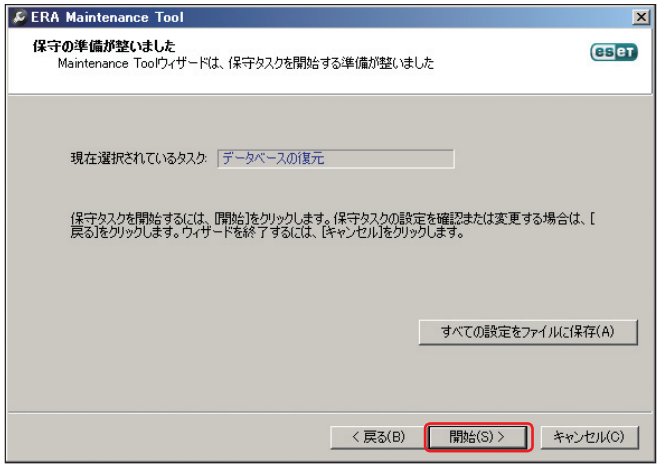
❶バックアップしたデータベースファイルを選択し、❷ [開く] ボタンをクリックします。

6



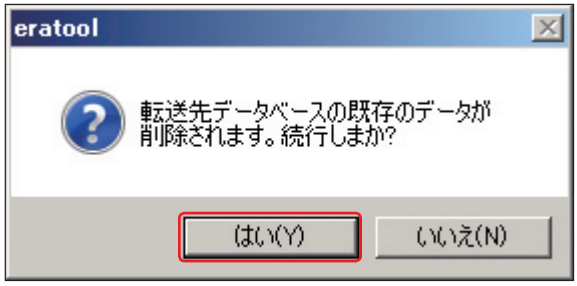
❶ [処理タスク実行時にサーバを停止する] にチェックを入れ、❷ [次へ] ボタンをクリックします。

7



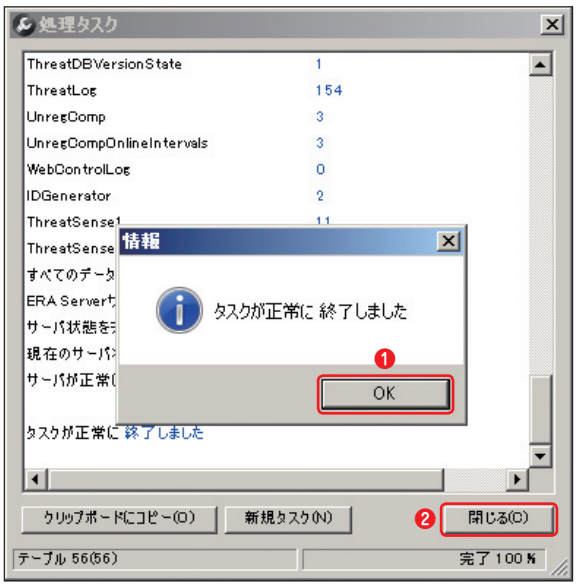
[開始] ボタンをクリックします。

8



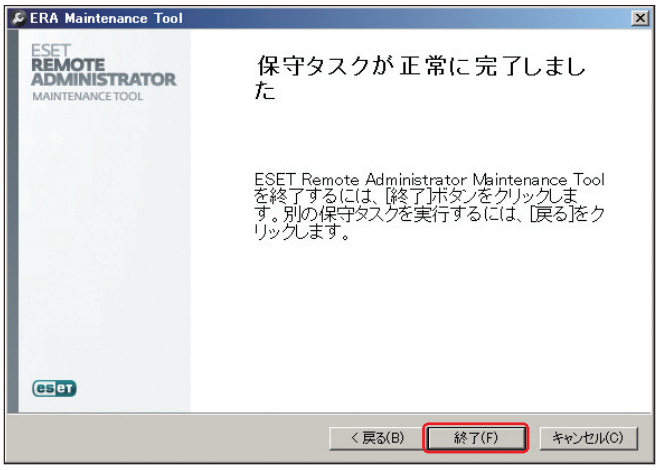
ダイアログが表示されたときは、[はい] ボタンをクリックします。

9



ダイアログが表示されます。❶[OK] ボタンをクリックし、[処理タスク] ダイアログの❷[閉じる] ボタンをクリックします。

10



ERAメンテナンスツールを終了します。[終了] ボタンをクリックします。

3.3.3 データフォルダーのリストア（復元）

ERASおよびERACのデータフォルダーをバックアップしたときは、バックアップしたフォルダーをバックアップ時と同じフォルダーに上書きすることでリストア（復元）できます。また、ERASを既定の内蔵DB（Microsoft Access)をデータベースに利用していた場合は、取得したクライアント情報、ログなどの全ての情報をリストアできます。データベースにMicrosoft SQL Server 2005 Express Edition / Standard Editionなどの既定の内蔵DB（Microsoft Access)以外を利用している場合は、ERASの設定情報など一部の情報のみがリストアされます。

Windows Server 2003 ／ 2003 R2の場合

ERAS	C:￥Documents and Settings￥All Users￥Application Data￥ESET￥ESET Remote Administrator￥Server
ERAC	C:￥Documents and Settings￥All Users￥Application Data￥ESET￥ESET Remote Administrator￥Console

Windows Server 2008 ／ 2008 R2の場合

ERAS	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Server
ERAC	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Console

Windows Server 2012 Standardの場合

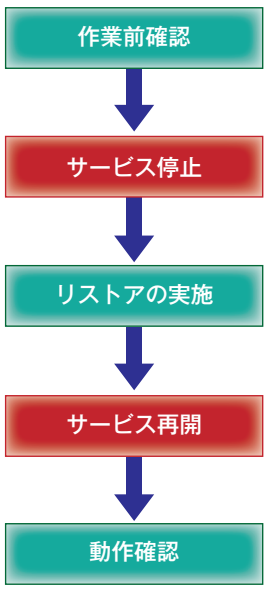
ERAS	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Server
ERAC	C:￥ProgramData￥ESET￥ESET Remote Administrator￥Console

CAUTION

バックアップするERAとリストアするERAのホスト名およびバージョンが同一でないとリストア後に正常に動作しません。サーバー環境を再構築する場合は、必ず同じホスト名とバージョンに設定してください。

3.3.4 データフォルダーのリストア（復元）の流れ

バックアップしておいたERASおよびERACのデータファルダーをリストア（復元）するときは、以下の流れで作業します。なお、ERASのリストアを行うときは、ERASのサービスを停止する必要がある点にご注意ください。



…❶対象ファイルの保存場所を確認します。

…❷ERAS の動作を停止します。ESET Remote Administrator Maintenance Tool を利用して動作を停止します。

…❸バックアップしておいたデータフォルダー内のファイルを、上記のフォルダーに全てコピーします。

…❹リストアが終了したら、停止させていた「ESET Remote Administrator Server」の動作を再開します。動作の再開は、ESET Remote Administrator Maintenance Tool を利用します。

…❺ERAC で ERAS に接続して「ESET Remote Administrator Server」の稼働が再開しているかを確認します。

3.4 ログ管理のポイント

ここでは、ESET Remote Administrator Server（ERAS）で管理されるログについて説明します。ERASで管理しているログは、「ERAサーバーログ」と「クライアントPC情報ログ」に大別されます。

3.4.1 ERAサーバーログ

ERAサーバーログは、ERASの動作に関するログです。管理サーバーに障害が発生したときの原因究明に利用でき、管理者への通知内容をログとして保存することもできます。

3.4.2 クライアントPC情報ログ

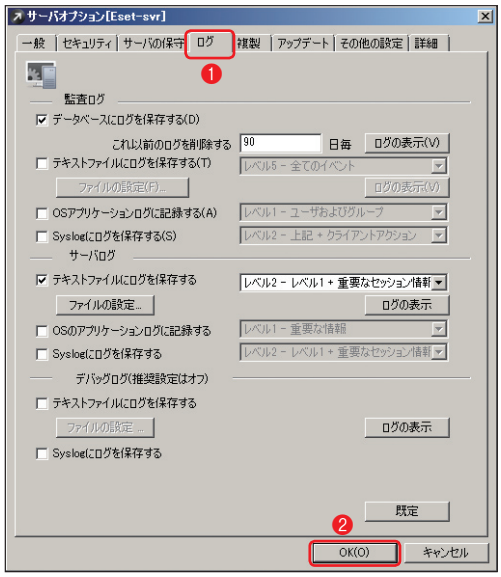
クライアントPC情報ログは、クライアントPCから収集したログです。以下のような種類のログがあり、管理者はERACを利用してその内容を確認できます。

クライアント	クライアントPCの最新情報を確認したいときに利用します。クライアントPCのウイルス定義データベースのバージョンや、警告の有無などを確認できます。
ウイルスログ	クライアントPCで検出されたウイルスを確認したいときに利用します。クライアントPCで検出されたウイルス名やウイルスの検出日時などを確認できます。
ファイアウォールログ	クライアントPCで検出されたファイアウォールの警告が確認できます。ESET Endpoint SecurityおよびESET Smart Securityを利用しているクライアントPCのみ、このログが報告されます。
イベントログ	クライアントPCで発生したシステムイベントを確認できます。
HIPSログ	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のログを確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログを開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。
デバイスコントロールログ	USBストレージやCD／DVDなどのデバイスの制御動作のログを確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログを開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。
Webコントロールログ	Web制御動作のログを確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログを開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。ESET Endpoint Securityを利用しているクライアントPCのみ、このログが報告されます。
迷惑メール対策ログ	迷惑メール対策のログを確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログを開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。ESET Endpoint SecurityおよびESET Smart Securityを利用しているクライアントPCのみ、このログが報告されます。
グレーリストログ	グレーリストのログを確認できます。既定値では、このログは取得されません。取得するには、[サーバオプション]ダイアログを開き、[サーバの保守]タブにある[ログ収集パラメータ]ボタンをクリックして、設定を行う必要があります。なお、このログは、日本語版では確認できません。
検査ログ	クライアントPCで実行されたスキャン結果を確認できます。
モバイルログ	ERASで管理しているAndroid端末の詳細なログが表示されます。
隔離	隔離されたウイルスに関する情報を確認できます。
タスク	ESET Remote Administrator Console（ERAC）を利用してERAS から実行されたタスクの動作結果などの情報を確認できます。

3.4.3 ERAサーバーログの設定変更手順

ここでは、ERAサーバーログの設定を変更する方法を説明します。ERAサーバーログの設定は、ERACを利用してERASにログオンすることで行います。

1 ERACを起動し、ERASにログオンします。[ツール] メニュー、[サーバオプション] をクリックして、[サーバオプション] ダイアログを開きます。

2 

❶ [ログ] タブをクリックします。ERAサーバーログに関する設定を行い、❷ [OK] ボタンをクリックします。設定内容については、以下をご参照ください。

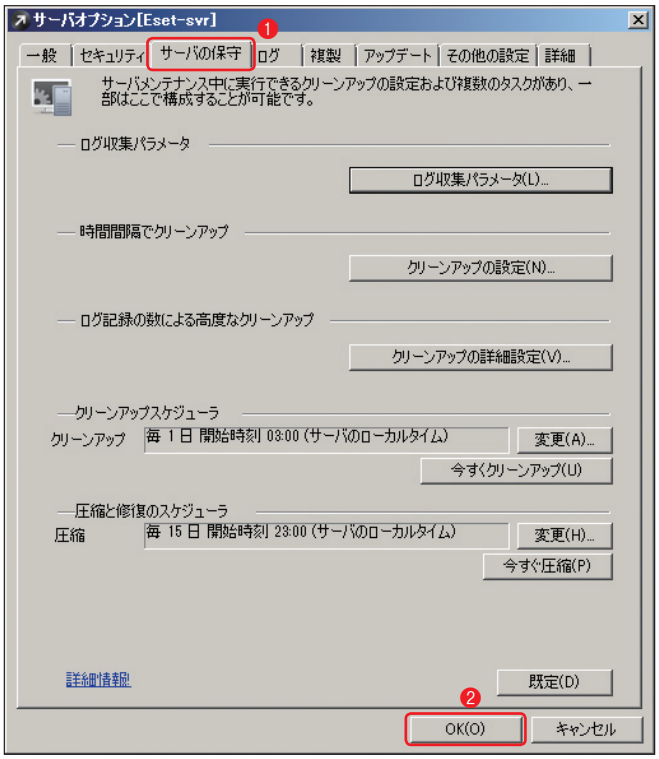
監査ログ	
データベースにログを保存する	チェックを入れると、データベースに監査ログを記録します。監査ログは、すべてのERACユーザーによるコンフィグレーションの変更および実行されたアクションを監視して記録します。
テキストファイルにログを保存する	チェックを入れると、監査ログをテキストファイル形式で保存します。[ファイルの設定] ボタンをクリックすると、作成するログファイルの名称やログをいつ削除するかなどの設定が行えます。このログは、既定値では以下のフォルダーに保存されます。 Windows Server 2003/2003 R2の場合 C: ¥Documents and Settings ¥All Users ¥Application Data ¥ESET ¥ESET Remote Administrator ¥Server ¥logs Windows Server 2008/2008 R2の場合 C: ¥ProgramData ¥ESET ¥ESET Remote Administrator ¥Server ¥logs
OSのアプリケーションログに記録する	チェックを入れると、OS のイベントビューアに監査ログの情報をコピーします。
Syslogにログを保存する	チェックを入れると、Syslogに監査ログ情報を保存し、保存するログレベルを設定できます。ログレベルは、既定値の[レベル2]で利用することを推奨しています。
サーバログ	
テキストファイルにログを保存する	チェックを入れると、ログをテキストファイル形式で保存します。ログレベルは、既定値の[レベル2]で利用することを推奨しています。また、[ファイルの設定] ボタンをクリックすると、作成するログファイルの名称やログをいつ削除するかなどの設定が行えます。このログは、既定値では監査ログと同じフォルダーに保存されます。
OSのアプリケーションログに記録する	チェックを入れると、OS のイベントビューアにサーバーログの情報をコピーします。
Syslogにログを保存する	チェックを入れると、Syslogにサーバーログ情報を保存し、保存するログレベルを設定できます。ログレベルは、既定値の[レベル2]で利用することを推奨しています。
デバックログ	
テキストファイルにログを保存する	チェックを入れると、デバックログをテキストファイル形式で保存します。[ファイルの設定] ボタンをクリックすると、作成するログファイルの名称やログをいつ削除するかなどの設定が行えます。このログは、既定値では監査ログと同じフォルダーに保存されます。また、デバックログの推奨設定はオフです。
Syslogにログを保存する	チェックを入れると、Syslogにデバックログ情報を保存します。また、デバックログの推奨設定はオフです。

3.4.4　クライアントPC情報ログの設定変更手順

ここでは、クライアントPC情報ログの設定を変更する方法を説明します。クライアントPC情報ログの設定は、ERACを利用してERASにログオンすることで行います。

1 ERACを起動し、ERASにログオンします。[ツール] メニュー、[サーバオプション] をクリックして、[サーバオプション] ダイアログを開きます。

2



❶ [サーバの保守] タブをクリックします。クライアントPC情報ログの保存に関する設定を行い、❷ [OK] ボタンをクリックします。設定内容については、以下をご参照ください。

ログ収集パラメータ	サーバーが受信するログのレベルを定義できます。HIPSログやデバイス制御ログ、Web制御ログ、迷惑メール対策ログ、グレーリストログは、既定値では取得されません。この設定を変更したいときは、ここで行います。
クリーンアップの設定	ログを削除するまでの期間を設定できます。設定は、各ログごとに行えます。
クリーンアップの詳細設定	常時保存しておくログの最大件数を設定できます。設定は各ログごとに行え、ここで指定した件数を超えると古いログから順に削除されます。また、クリーンアップの設定も併用すると、先に設定した条件を満たしたほうが優先されます。
圧縮と修復のスケジューラ	データベースの圧縮と修復を行う間隔を設定します。圧縮と修復を行うと、不整合や誤作動がなくなり、データベースとの通信速度が向上します。[変更] ボタンをクリックすると、データベースの圧縮と修復を行う間隔を設定できます。また、[今すぐ圧縮] ボタンをクリックすると、直ちにデータベースの圧縮と修復を開始されます。
クリーンアップスケジューラ	指定された間隔でデータベースのクリーンアップを実行します。[変更] ボタンをクリックすると、クリーンアップを実行する間隔を設定できます。また、[今すぐクリーンアップ] ボタンをクリックすると直ちにクリーンアップが開始されます。

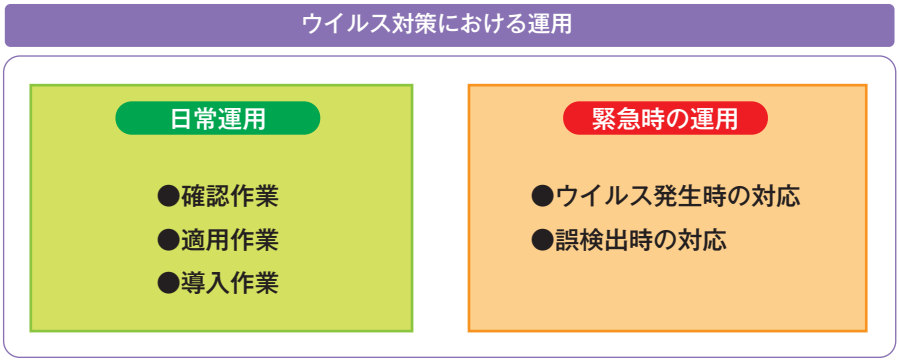
※データベースのクリーンアップおよび圧縮と修復は、スケジューリングしてサーバの負荷が最少のときに実行することをお勧めします。既定では、3カ月または6カ月を経過したエントリとログは削除され、15日ごとにデータベースの圧縮と修復が実行されます。

[Chapter 4]
ウイルス対策における運用

4.1 ウイルス対策のポイント

ここでは、ESET ライセンス製品を利用したウイルス対策の運用方法について説明します。ウイルス対策の運用は、日常の運用フェーズと緊急時の運用フェーズに大別されます。

4.1.1 ウイルス対策における運用



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 PC 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。	119 ページ
ウイルス検出時（緊急時）の対応	クライアント PC 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。	122 ページ
ウイルス誤検出時の対応	Windows や Mac OS X 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。	131 ページ

4.2 日常の運用

ここでは、ESET ライセンス製品導入後の日常の運用について説明します。

4.2.1 日常の運用フェーズ

ESET ライセンス製品導入後の日常の運用は、「確認」「適用」「追加導入」の3つのフェーズがあります。それぞれのフェーズで実施すべき主な事柄は、以下のとおりです。

確認	・ウイルス定義データベースのバージョン確認 ・プログラムのバージョン確認 ・ライセンス期限／クライアント数の確認 ・各種ログの確認 ・ウイルス検出状況の確認 ・設定状況の確認
適用	・最新ウイルス定義データベースへのアップデート オフライン環境でのアップデート／時差配信 ・最新プログラムへのアップグレード ・ポリシーの適用・タスクの適用
導入	・新規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 ・ライセンスの更新

4.2.2 クライアントPCの状態を確認するには

「確認」フェーズでは、ESET Remote Administrator Console（ERAC）を利用してクライアントPCの状態を確認します。クライアントPCの状態は、[クライアント] [ウイルスログ] [ファイアウォールログ] [イベントログ] [HIPSログ] [デバイスコントロールログ] [Webコントロールログ] [迷惑メール対策ログ] [グレーリストログ] [検査ログ] [モバイルログ]などのペインを利用して確認できます。また、各ペインに表示する項目は[ツール]、[コンソールオプション]をクリックして [コンソールオプション] ダイアログを開き、[カラム-表示/非表示] タブで変更できます。

■ [クライアント] ペイン

[クライアント] ペインは、クライアントPCの様々な情報を総合的に確認するときに利用します。確認できる項目は、利用しているESET ライセンス製品の製品名やバージョン、ポリシー名、最終アクセス日時、保護状態の説明、定義データベースのバージョン、最終ウイルス警告、最終ファイアウォール警告、最終イベント警告、最終感染ファイル、最終駆除ファイル、最終検査日時、再起動要求、OS名などがあります。

■ [ウイルスログ] ペイン

[ウイルスログ] ペインでは、クライアント用プログラムによって検出されたウイルスに関する詳細なログを確認できます。

■ [ファイアウォールログ] ペイン

[ファイアウォールログ]ペインでは、ESET Endpoint SecurityおよびESET Smart Securityによって検出されたファイアウォールに関する詳細なログを確認できます。

■ [イベントログ] ペイン

[イベントログ] ペインでは、クライアントPCで発生したイベント（アップデートの成功・失敗などに関する詳細なログを確認できます。

■ [HIPSログ] ペイン

[HIPSログ] ペインでは、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のログを確認できます。既定値では、このログは取得されません。取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリックして、設定を行う必要があります。

■ [デバイスコントロールログ] ペイン

[デバイスコントロールログ] ペインでは、USBストレージやCD／DVDなどのデバイスの制御動作のログを確認できます。既定値では、このログは取得されません。取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリックして、設定を行う必要があります。

■ [Webコントロールログ] ペイン

[Webコントロールログ] ペインでは、Web制御動作のログを確認できます。既定値では、このログは取得されません。取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリックして、設定を行う必要があります。ESET Endpoint Securityを利用しているクライアントPCのみ、このログが報告されます。

■ [迷惑メール対策ログ] ペイン

[迷惑メール対策ログ] ペインでは、迷惑メール対策のログを確認できます。既定値では、このログは取得されません。取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリックして、設定を行う必要があります。ESET Endpoint SecurityおよびESET Smart Securityを利用しているクライアントPCのみ、このログが報告されます。

■ [グレーリストログ] ペイン

[グレーリストログ] ペインでは、グレーリストのログを確認できます。既定値では、このログは取得されません。取得するには、「サーバオプション」ダイアログを開き、「サーバの保守」タブにある「ログ収集パラメータ」ボタンをクリックして、設定を行う必要があります。

■ [検査ログ] ペイン

[検査ログ] ペインでは、クライアントPCで実行された [コンピュータの検査] に関するログを確認できます。

■ [モバイルログ] ペイン

[モバイルログ] ペインでは、ERASで管理しているAndroid端末の詳細なログが表示されます。

4.3 ウイルス検出時(緊急時)の対応

ウイルス感染などの緊急時には、運用フェーズにおける、すみやかな対応が必要になります。ここでは、ウイルスを検出したクライアントPCが発見された場合の対応ステップの例を紹介しますので、運用の際の参考にしてください。

4.3.1 ウイルス検査時の対応の流れ

STEP1 ウイルスの発見および報告

- ウイルスの発見
- 管理者への通知（通知マネージャを利用し電子メールで管理者へ通知）
- ウイルスが検出されたコンピューターの利用者、その他関係者への連絡

▼

STEP2 初動対応の実施

- ウイルスが検出されたコンピューターの利用中止(ネットワークケーブルを外し、該当PCをネットワークから切断する)
- ローカルドライブのウイルス検査の実施
- ウイルスの隔離・駆除・削除の実施
- ウイルスの駆除・削除ができない場合、サポートセンターへのお問い合わせ

▼

STEP3 ウイルスの詳細調査・報告

- ウイルスの特定と感染範囲の把握
- システムへの影響範囲の特定と対応
- 感染経路の特定（原因特定）
- 感染状況の報告

▼

STEP4 防止・抑制策の実施

- OSやアプリケーションのセキュリティパッチ適用／コンピューターの構成変更(設定変更)
- 感染源へのアクセス制御

4.4 ウイルス検出時の対応例

ここでは、ウイルスが検出された場合の実際の対処例を元に具体的な運用例を紹介します。運用の際の参考にしてください。

4.4.1 ウイルスが検出されたときの対処手順

仮定する状況

- クライアントPC複数台でウイルスを検出
- 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
- 感染経路は、ユーザー私物のUSBメモリー

↓

対処

STEP1 ＜管理者への通知＞通知メールでシステム管理者がウイルス検出を確認 124 ページ参照

↓

STEP2 ＜ウイルスの隔離・駆除・削除＞ウイルス駆除後、全クライアントPCのウイルス検査を実施 125 ページ参照

↓

STEP3 ＜報告＞レポートの作成 128 ページ参照

↓

STEP4 ＜防止・抑制策の実施＞USBメモリーの使用禁止または利用できるデバイスを制限ポリシーの適用 130 ページ参照

4.4.2 STEP1 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［通知マネージャ］を利用し、一定数以上のクライアントPC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ことで実現します。この機能を利用すると、緊急性を即座に感知し迅速な対応が行えます。［通知マネージャ］は各種警告をカスタマイズでき、日常の運用事項を登録することで安全な運用が行えます。

［通知マネージャ］を利用し管理者に様々な情報を電子メールで通知するには、［サーバオプション］の［その他の設定］タブ内の［SMTP設定］で、電子メール送信に利用するSMTPサーバーが設定されている必要があります。また、［通知マネージャ］で［通知ルール］を事前に登録しておく必要があります。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」をご参照ください。

1.ERASへの電子メール送信に必要なSMTPサーバーの設定を行う

［サーバオプション］→［その他の設定］→［SMTP 設定］

↓

2.［通知マネージャ］で通知ルールと通知方法を設定

一定数以上のウイルス検出

4.4.3　STEP2 ウイルスの隔離・駆除・削除

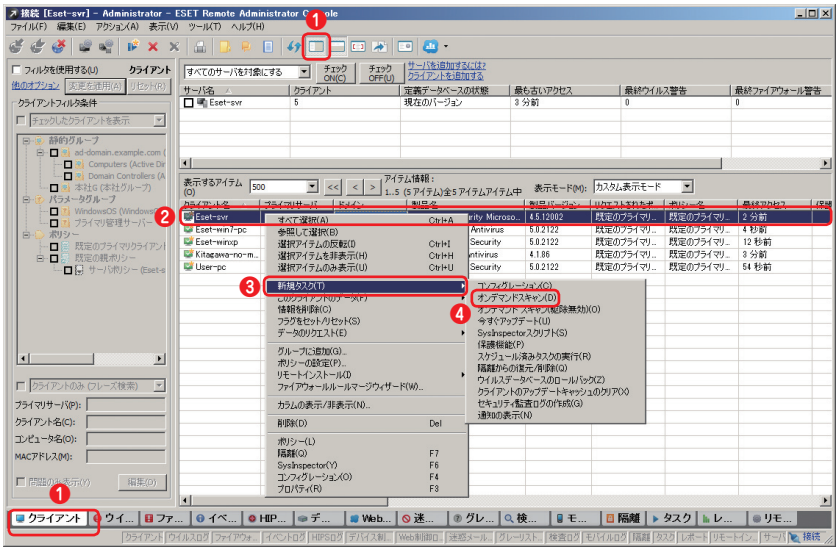
ウイルス検出時は管理者への通知と共に、ウイルスの蔓延を防止することに注力します。ウイルスの蔓延を防ぐために重要なポイントは、ウイルスの隔離・駆除・削除を行った後に再度ウイルス検査を実施し、二重、三重のチェックを行うことです。再度のウイルス検査を実施することによって、別ウイルスによるさらなる蔓延を防止できます。該当ウイルスを検出していないクライアントPCでもウイルス検査を実施し、安全を確認します。
なおウイルス検査を実施する場合は、各クライアントPCのローカルディスク全体を検査対象とします。ウイルス検査の実施は、管理者がERAを利用したリモート操作で一括して行うこともできます。

4.4.3.1　ERAを利用したリモート検査の実施手順

ここでは、ERAを利用してクライアントPCにリモート検査を実施する方法を説明します。

1 ERACを起動し、ERASにログオンします。

2

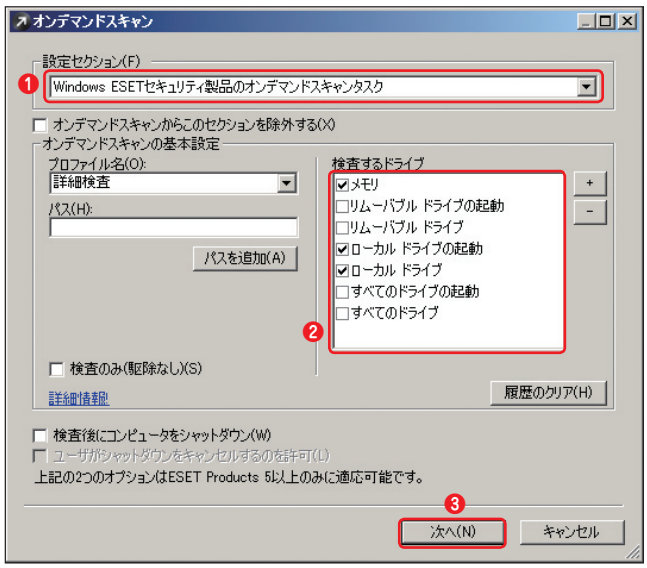


❶[クライアント]タブまたは[[クライアント]ペインを表示]ボタンをクリックし、❷[クライアント]ペインに表示されているクライントPCを右クリックします。❸[新規タスク]→❹[オンデマンドスキャン]をクリックします。

POINT

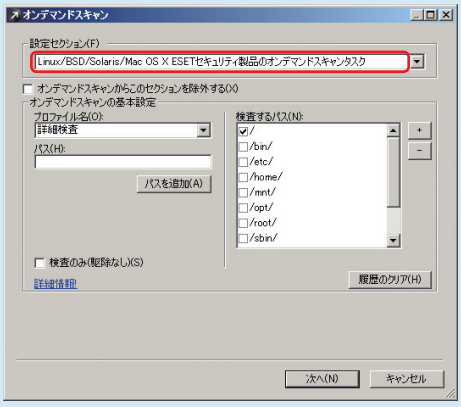
[オンデマンドスキャン]ダイアログは、[アクション]メニューをクリックし、[新規タスク]、[オンデマンドスキャン]を選択することでも開けます。

3



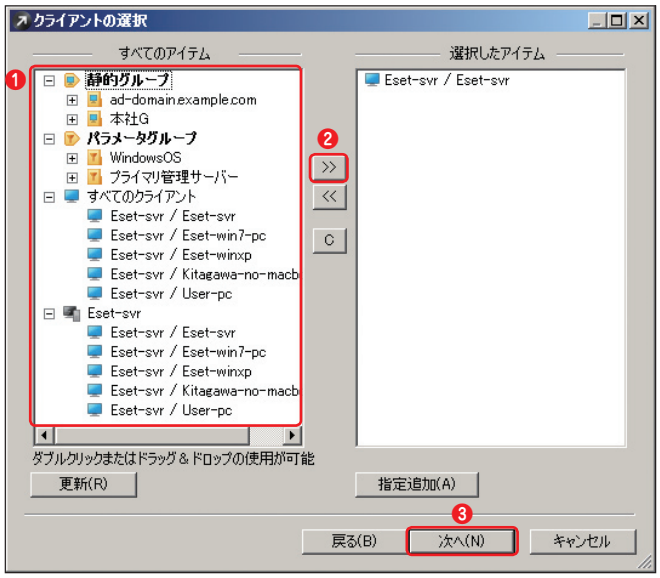
[オンデマンドスキャン] ダイアログが表示されます。Windows端末のウイルス検査を行うときは、設定セクションに❶[Windows ESETセキュリティ製品のオンデマンドスキャンタスク]が選択されていることを確認します。❷ローカルドライブにチェックが入っていることを確認し、❸[次へ]ボタンをクリックします。

POINT



Mac OS XまたはLinuxがインストールされたクライアントPCのウイルス検査を行うときは、設定セクションで[Linux/BSD/Solaris/Mac OS X ESETセキュリティ製品のオンデマンドスキャンタスク]を選択します。また、Android端末のウイルス検査を行うときは、設定セクションで[ESET Mobile Securityのオンデマンドスキャンタスク]を選択します。

4

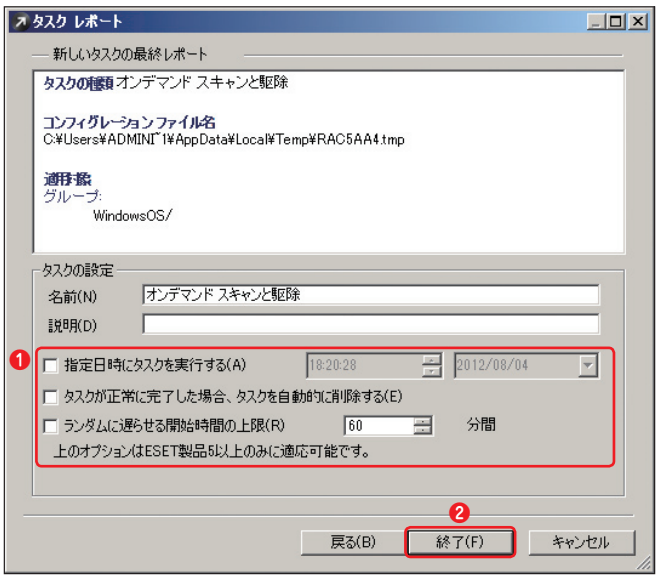


クライアントPCを選択します。❶[すべてのアイテム]リストからオンデマンドスキャンを実施するグループまたはクライアントPCをクリックし、❷[クライアントの追加([>>])]ボタンをクリックします。追加し終えたら、❸[次へ]ボタンをクリックします。

POINT

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PCを登録できます。また、[選択したアイテム]リスト内のグループおよびクライアントPCをクリックし[クライアントの削除([<<])]ボタンをクリックすると、選択を解除できます。[クリア([C])]ボタンをクリックすると、すべての選択を解除できます。

5



❶タスクの実行日時などの設定を行い、❷[終了]ボタンをクリックします。

POINT

[指定日時にタスクを実行する]にチェックを入れ、日時を指定すると、指定した日時にオンデマンドスキャンのタスクが配布されます。また、ESET Endpoint SecurityまたはESET Endpoint アンチウイルスに対してオンデマンドスキャンタスクを配布する場合は、[ランダムに遅らせる開始時間の上限]にチェックを入れ、時間を設定すると、タスクの遅延実行を行えます。

CAUTION

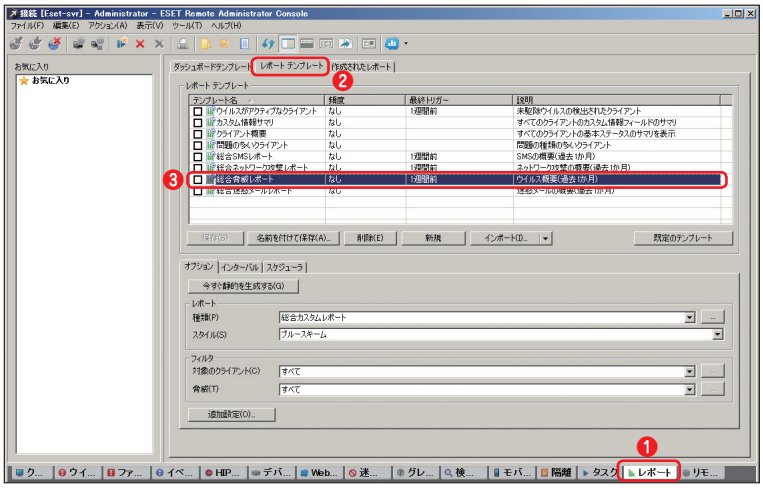
オンデマンドスキャンタスクは、WindowsとMac OS X、Linux、Androidで別々にタスクを配布する必要があります。たとえば、Windowsがインストールされたクライアント PCにMac OS X用のオンデマンドスキャンタスクを配布すると、タスクが実行されずにエラーとなります。オンデマンドスキャンタスクを配布するときは、各OSごとに行ってください。

4.4.4 STEP3 報告～レポートの作成

ウイルス検出時と終息時には、レポートを作成します。ERAは、管理しているクライアントPC情報ログをもとにレポートを作成する機能を搭載してます。この機能を利用すると、ウイルス検出状況の詳細を簡単にレポート化できます。また終息時にも同一フォーマットでレポートを作成することで、ウイスル感染から事態の終息までを視覚化できます。ERASを利用したレポートの作成は以下の手順で行います。

1 ERACを起動し、ERASにログオンします。

2

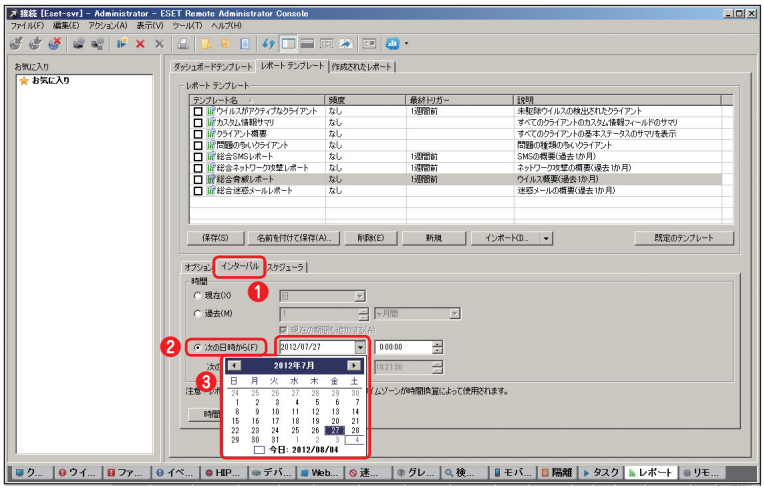


❶[レポート]タブをクリックし、❷[レポートテンプレート]タブをクリックします。❸レポートテンプレートから作成したいレポートをクリックします。

POINT

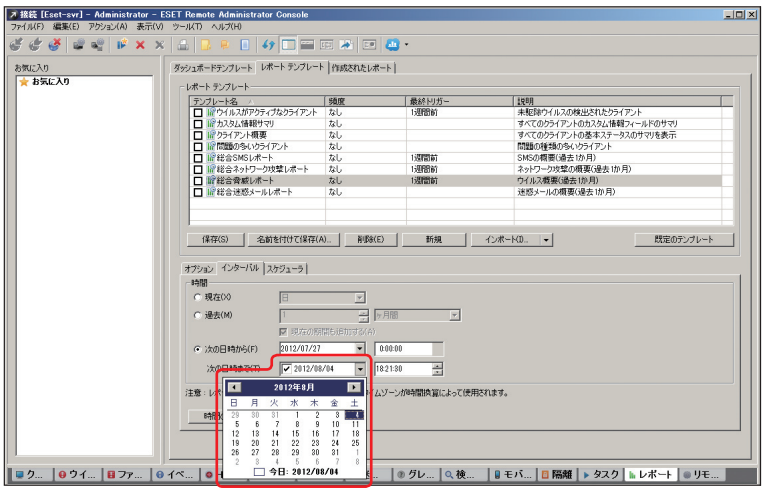
[対象のクライアント]や[脅威]のドロップダウンボタンをクリックすると、選択したクライアントPCやウイルスに絞り込んでレポートを作成できます。また、[追加設定]ボタンをクリックし[レポート詳細設定]ダイアログを開くと、CSV形式でレポートを保存するなどの設定が行えます。

3



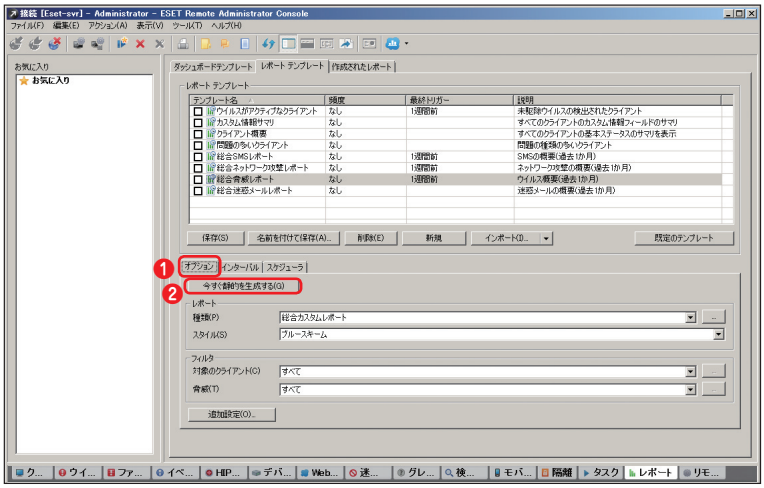
期間を設定します。❶[インターバル]タブをクリックします。❷[次の日時から]にチェックを入れ、❸ドロップダウンボタンをクリックして、ログの取得開始日時を設定します。

4



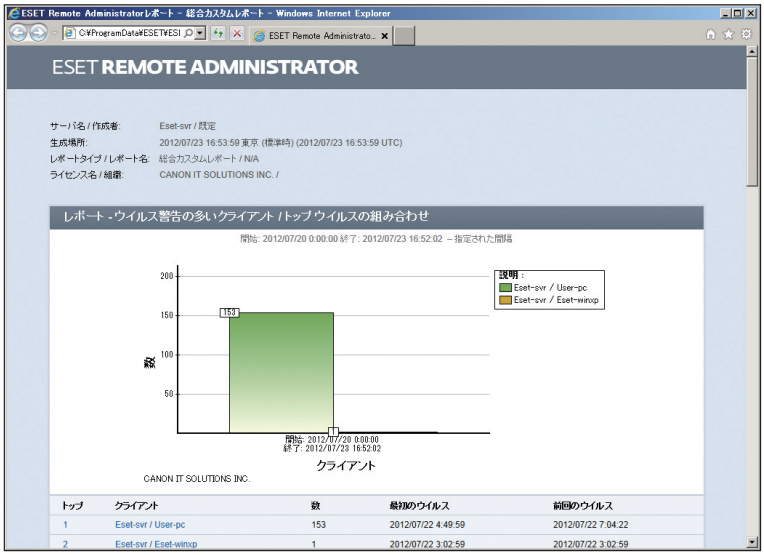
終了日時を設定します。[次の日時まで]のドロップダウンボタンをクリックし、終了日時を設定します。

5



レポートを作成します。❶[オプション]タブをクリックし、❷[今すぐ作成]ボタンをクリックします。

6



レポートが作成されます。レポート作成中は、進捗状況が表示されます。作成し終わるとWebブラウザーが開き、レポートが表示されます。

4.4.5 STEP4 防止・抑止策の適用

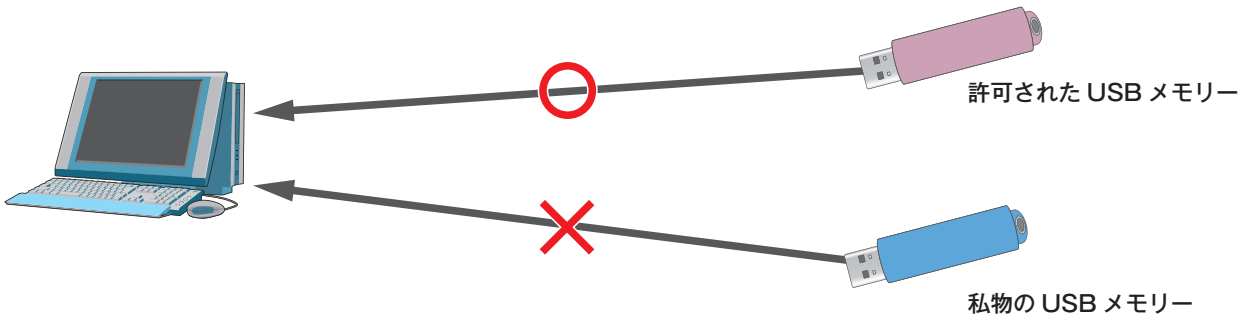
今回の例では、USBメモリー（外部デバイス）経由でウイルスに感染したことが前提となっているので、防止・抑止策として、クライアントPCに対して外部デバイス（USBメモリーやUSB HDD、CD-R、DVD-Rなど）の利用を禁止する設定を行うか利用できるデバイスを制限します。設定は［ポリシーマネージャ］を利用し、全クライアントPCに外部デバイスの使用禁止ルールまたは利用できる機器を制限するルールを一括配布するか、コンフィグレーションタスクで同様の設定を作成しそれを配布します。以下にデバイスを制御する場合の運用例を掲載しておきますので参考にしてください。

運用例1

許可されたデバイスのみ利用可能とする

デバイスコントロール機能を利用すると、各クライアントPCで利用できる外部デバイスを指定でき、特定のUSBデバイスのみ利用可能にしたり、利用不可にすることができます。たとえば、私物のUSBメモリーを利用不可にし、許可されたUSBメモリーのみを利用可能に設定できます。この機能は、ESET Endpoint Security、ESET Endpoint アンチウイルスおよびESET NOD32アンチウイルスで利用できます※。

※ESET NOD32アンチウイルスでは一部機能制限があります。



運用例2

特定のパソコンのみ外部デバイスの利用を許可

外部デバイスの利用可／不可をパソコン単位で制御します。たとえば、特定のパソコンのみUSBデバイスの利用を許可し、その他のPCについてはUSBデバイスの利用を制限することができます。

4.5 ウイルス誤検出時の対応

誤検出とは、WindowsやMac OS X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、アンチウイルスソフトがウイルスと判定してしまうことです。ここでは、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を説明します。

4.5.1 ファイルがウイルスとして検出された場合の対応手順

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
（http://canon-its.jp/product/eset/）
●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
※ERAを利用した、クライアントPC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）

4.5.2 隔離されたファイルの復元手順～クライアントPC編（Windowsの場合）

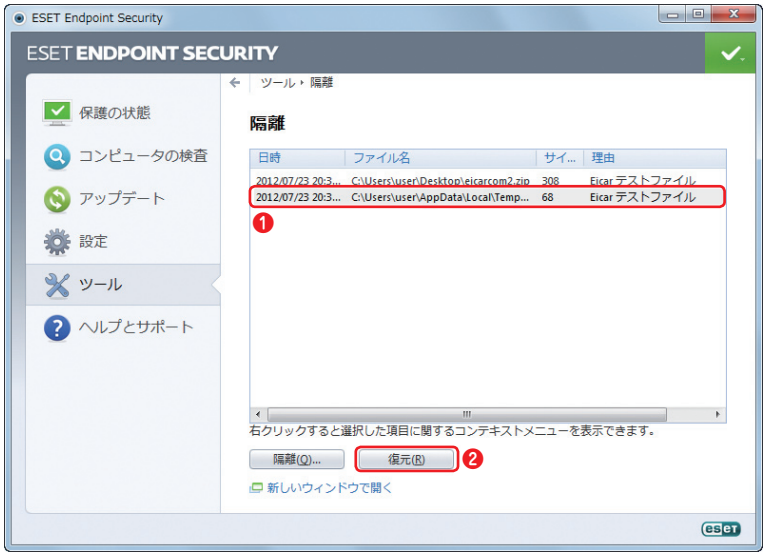
ここでは、ESET Endpoint SecurityまたはESET Endpoint アンチウイルスでウイルスとして検出され隔離されたファイルの復元手順を説明します。

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。

2

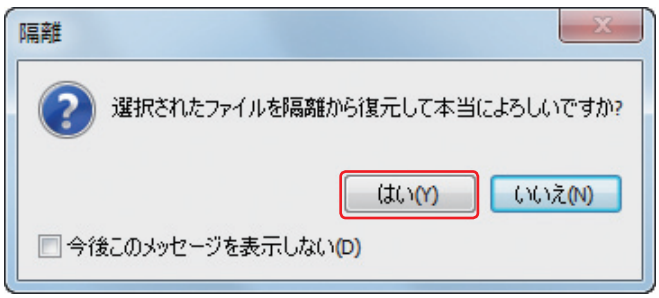
❶ [ツール]、❷ [隔離] をクリックします。

3



❶ [復元] したいファイルをクリックし、
❷ [復元] をクリックします。

4

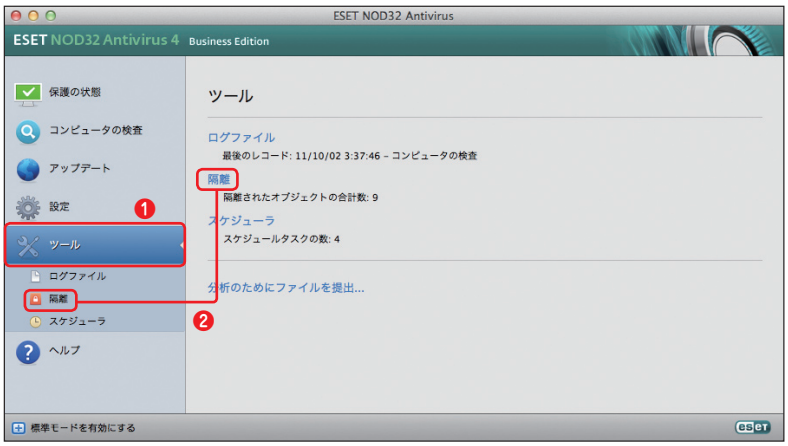


確認ダイアログが表示されます。[はい] ボタンをクリックします。

4.5.3 隔離されたファイルの復元手順～クライアントPC編（Mac OS Xの場合）

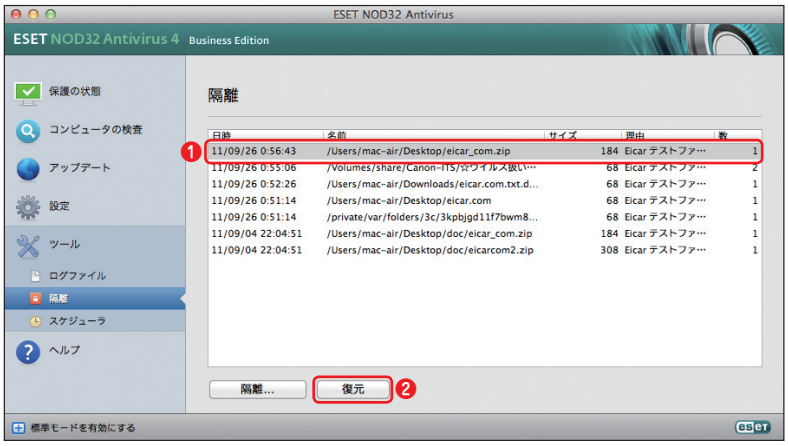
ここでは、ESET NOD32アンチウイルスでウイルスとして検出され、隔離されたファイルの復元手順を説明します。

1



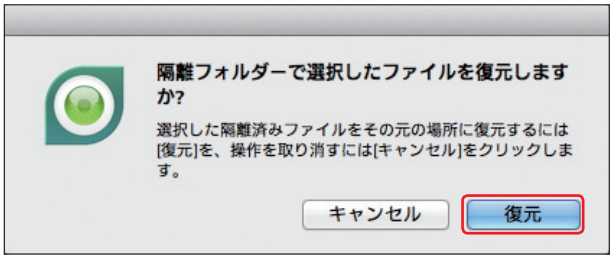
メインウィンドウを開き、詳細モードに切り替えて、❶[ツール] ボタンをクリックし、❷[隔離] ボタン、もしくは [隔離] をクリックします。

2



❶復元したい項目をクリックし、❷[復元] ボタンをクリックします。

3



復元を行います。[復元] ボタンをクリックします。隔離前にファイルが存在したフォルダーに、誤って検出されたファイルが復元されます。

4.5.4 隔離されたファイルの復元手順～クライアントPC編（Linuxの場合）

ここではESET File Security for Linuxでウイルスとして検出されたファイルの復元手順を説明します。

1 コマンドラインで以下のように入力し、隔離されているファイルを一覧表示します。

```
# /opt/eset/esets/sbin/esets_quar -l
```

隔離ファイルの一覧表示例

```
id="5834281359974756716", date="17.01.2013 14:11:12", name="./eicar.com", size="68",
reason="Eicar test file", count="1"
id="5834280538916396591", date="17.01.2013 14:07:41", name="/root/testfile.txt",
size="61", reason="added by user", count="1"
```

2 ファイルを復元します。上記の隔離ファイルの一覧例から「testfile.txt」を「/tmp」ディレクトリに復元する場合は以下のように入力します。

```
# /opt/eset/esets/sbin/esets_quar -r /tmp –object-name=/root/testfile.txt
```

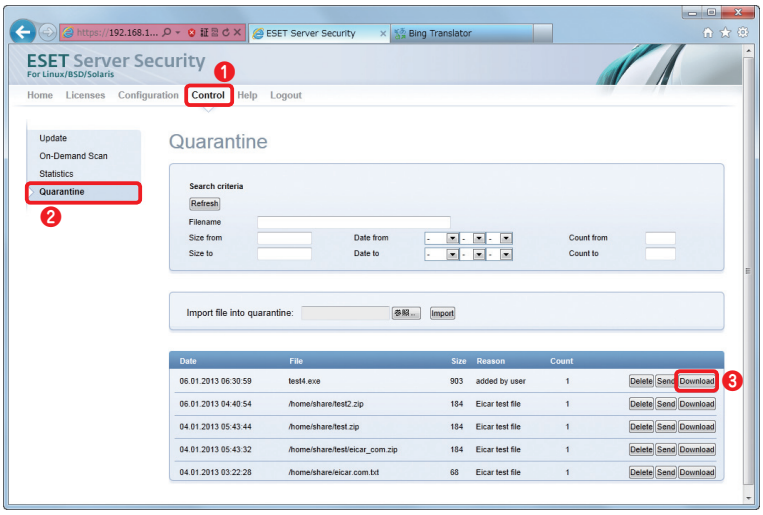
››› POINT

復元された後のファイル名は「5834280538916396591.testfile.txt」のように「ID.元のファイル名」になります。

コラム

隔離されたファイルのダウンロード

隔離されたファイルをダウンロードしたいときは、以下の手順で作業します。



Webブラウザーを開き、Webインターフェースのページを開きます。
❶[Control]をクリックし、
❷[Quarantine]をクリックします。ダウンロードしたいファイルの
❸[Download]ボタンをクリックし、ファイルを保存します。

4.5.5 隔離されたファイルの復元手順～クライアントPC編（Androidの場合）

ここでは、ESET Endpoint Security for Android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。

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

2 

[ウイルス対策] をタップします。

3 

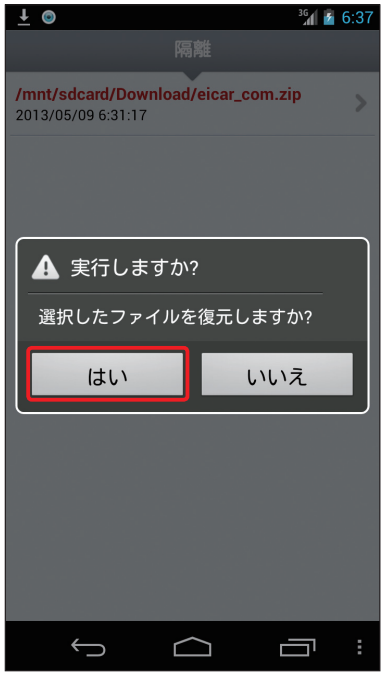
[隔離] をタップします。

4 

復元したいファイルをタップします。

5 

ダイアログが表示されます。[復元] をタップします。

6 

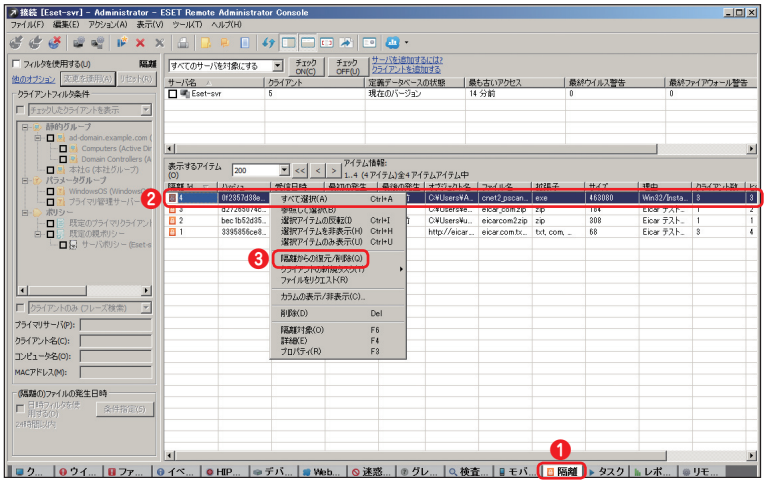
確認画面が表示されます。[はい] をタップします。

4.5.6　隔離されたファイルの復元手順～ ERA編

ここでは、隔離されたファイルの復元をERAを利用してリモート操作で行う手順を説明します。

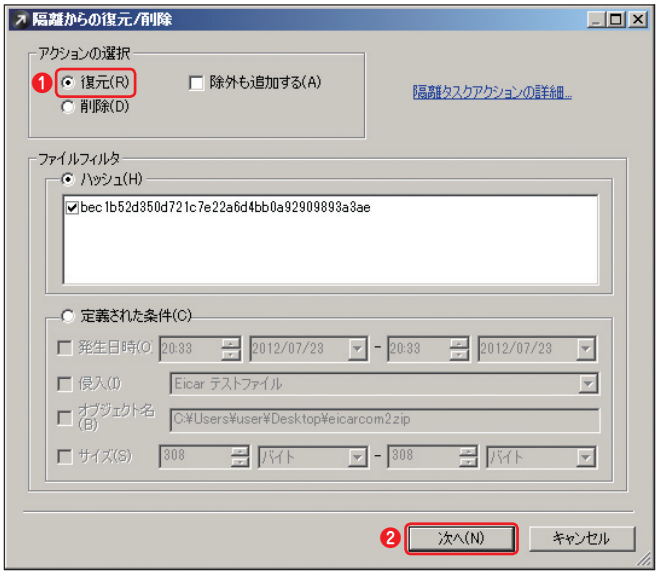
1 ERACを起動し、ERASにログオンします。

2



復元作業を始めます。❶[隔離]タブをクリックし、❷復元したいファイルを右クリックして❸[隔離からの復元/削除]をクリックします。

3

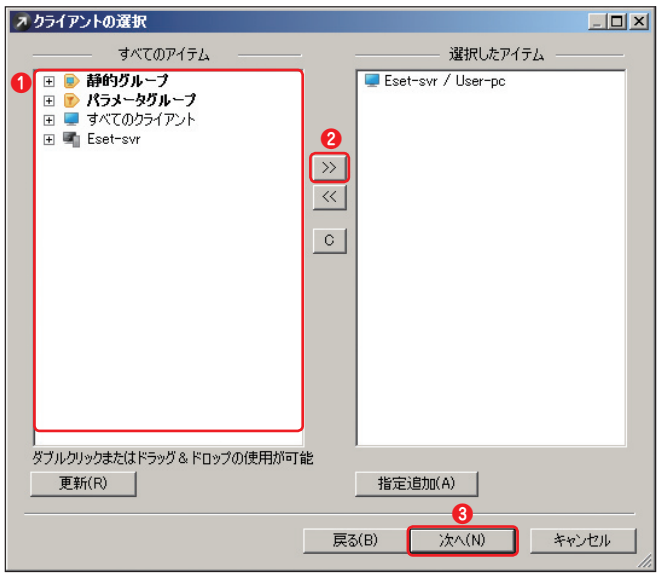


復元を実行します。❶[復元]にチェックを入れ、❷[次へ]ボタンをクリックします。

POINT

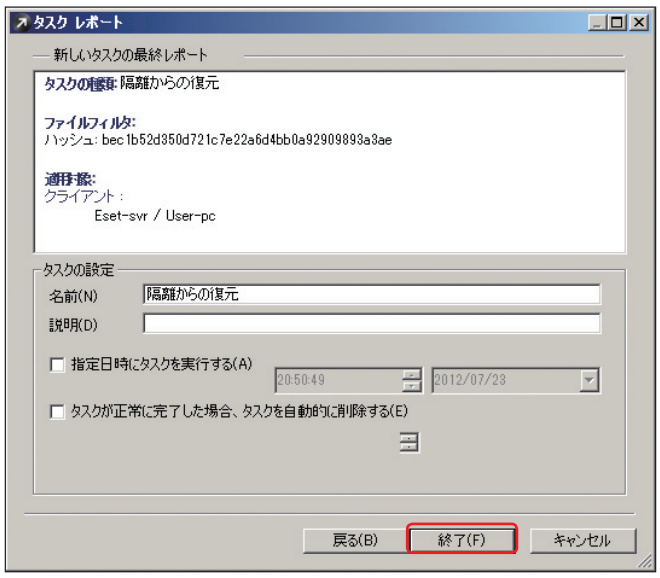
[除外も追加する]は、未知のウイルスとして検出されたファイルのみ有効になります。

4



クライアントを選択します。❶[すべてのアイテム]リストから復元先のグループおよびクライアントPCをクリックし、❷[クライアントの追加([>>])]ボタンをクリックします。追加し終えたら、❸[次へ]ボタンをクリックします。

5



ファイルの復元を開始します。[終了]ボタンをクリックし、復元を開始します。

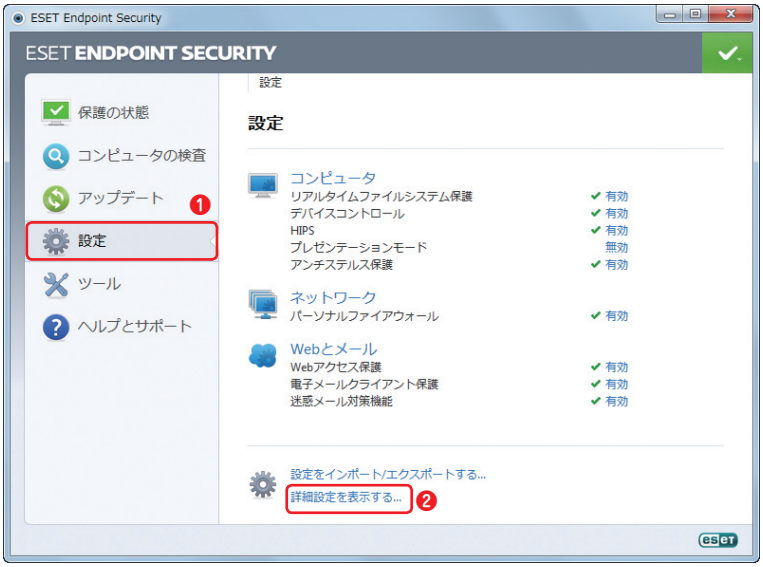
※ESET Endpoint Security for AndroidおよびESET File Security for Linuxの隔離ファイルには対応しておりません。

4.5.7 ウイルスとして検出されたファイルをウイルス検査対象から除外する手順～クライアントPC編（Windows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、設定後は間違って削除や隔離などが行われることはありません。ここでは、ESET Endpoint SecurityまたはESET Endpoint アンチウイルスでファイルの除外設定を行う手順を説明します。

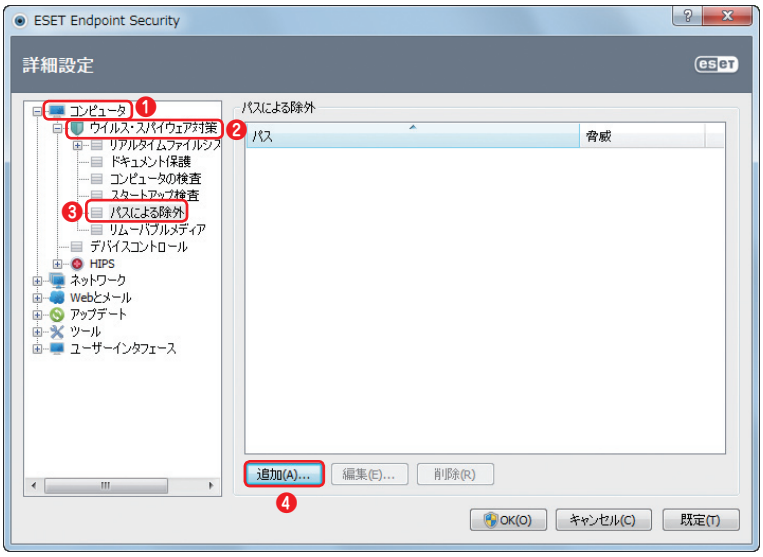
1 ESET Endpoint SecurityまたはESET Endpoint アンチウイルスのメイン画面を開きます。

2



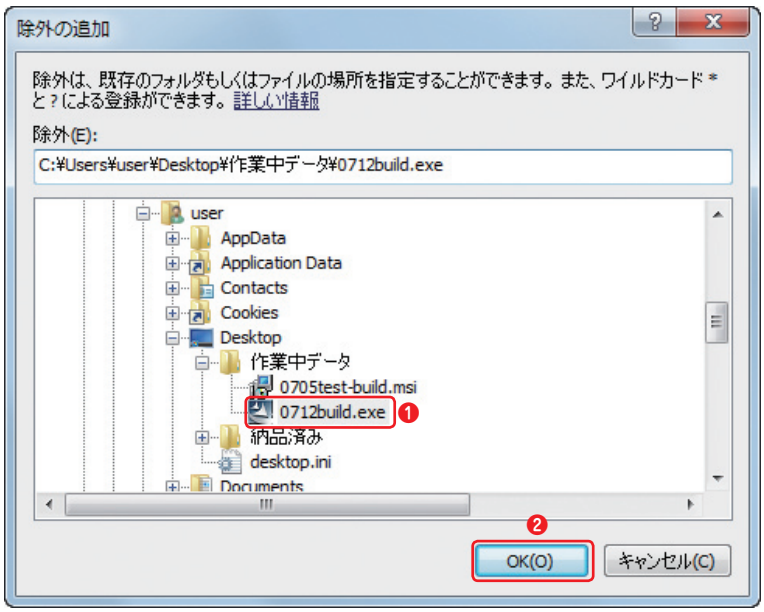
❶［設定］、❷［詳細設定を表示する］をクリックします。

3



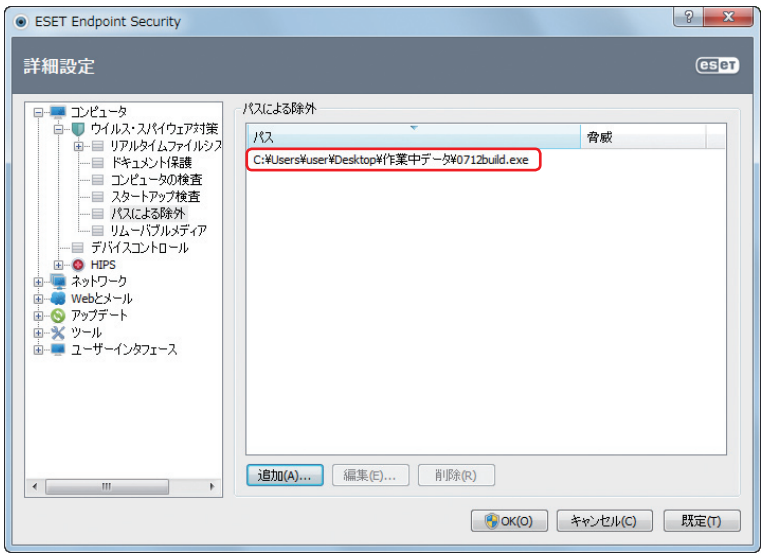
❶［コンピュータ］をダブルクリックし、❷［ウイルス・スパイウェア対策の設定］をダブルクリックします。❸［パスによる除外］をクリックし、❹［追加］ボタンをクリックします。

4



除外するファイルを選択します。❶除外するファイルを選択し、❷[OK] ボタンをクリックします。

5



除外リストにファイルが登録されます。

POINT

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、[OK] ボタンをクリックするか [除外] 欄に除外したいフォルダーのフルパスを入力し、[OK] ボタンをクリックします。拡張子を登録するときは、[除外] 欄に「c:¥test¥*.doc」のような形式で入力します。

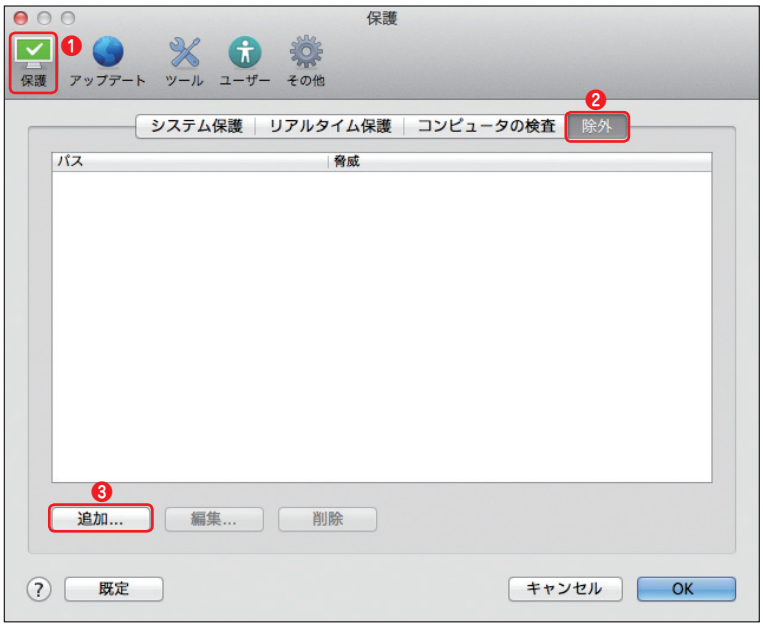
4.5.8 ウイルスとして検出されたファイルを検査対象から除外する手順～クライアントPC編（Mac OS Xの場合）

ここでは、クライアント側でファイルの除外設定を行う手順を説明します。

1

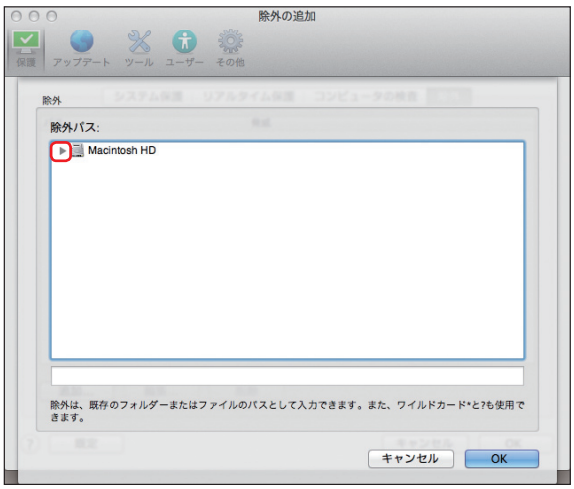
メインウィンドウを開き、詳細モードに切り替えて、❶[設定] ボタンをクリックし、❷[アプリケーションの設定を入力する] をクリックします。

2



❶[保護] ボタンをクリックし、❷[除外] をクリックします。❸[追加] ボタンをクリックします。

3

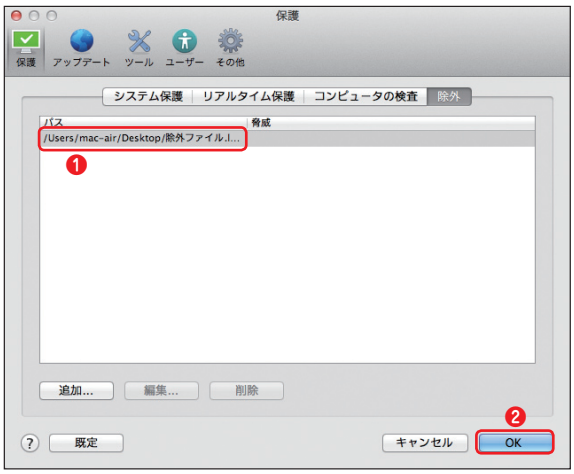


フォルダー一覧を表示します。[▶]をクリックします。

4

除外したいファイルを選択します。❶除外したいファイルをクリックし、❷[OK]ボタンをクリックします。

5



❶選択したファイルが除外ファイルに登録されます。❷[OK]ボタンをクリックします。

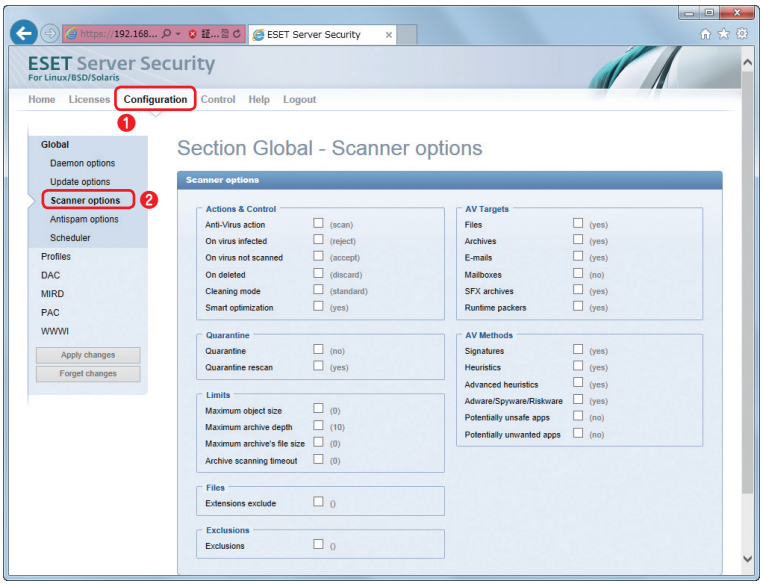
▸▸▸ POINT

除外リストには、フォルダーも登録できます。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、[OK]ボタンをクリックするか[除外]欄に除外したいフォルダーのフルパスを入力し、[OK]ボタンをクリックします。

4.5.9 ウイルスとして検出されたファイルを検査対象から除外する手順（Linuxの場合）

ここでは、ESET File Security for Linuxで指定したファイルを検査から除外する手順を説明します。

1

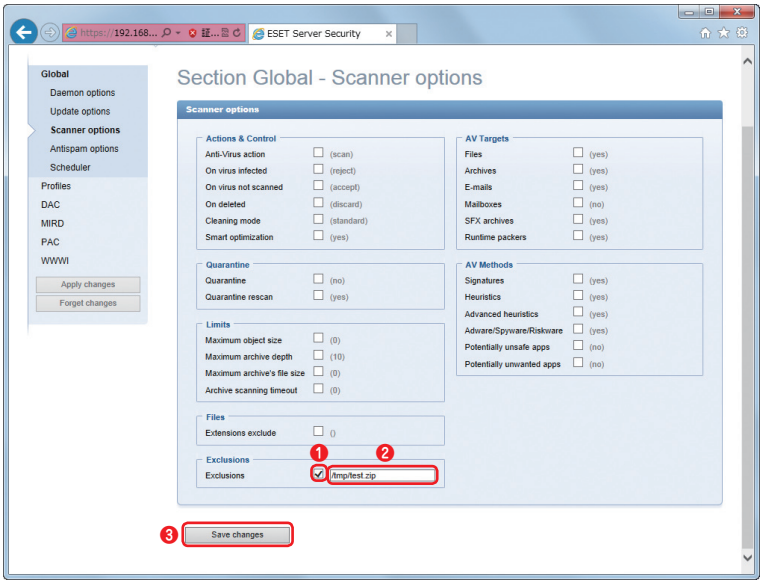


Webブラウザーを開き、Webインターフェースのページを開きます。

❶[Configuration]をクリックし、

❷[Scanner options]をクリックします。

2

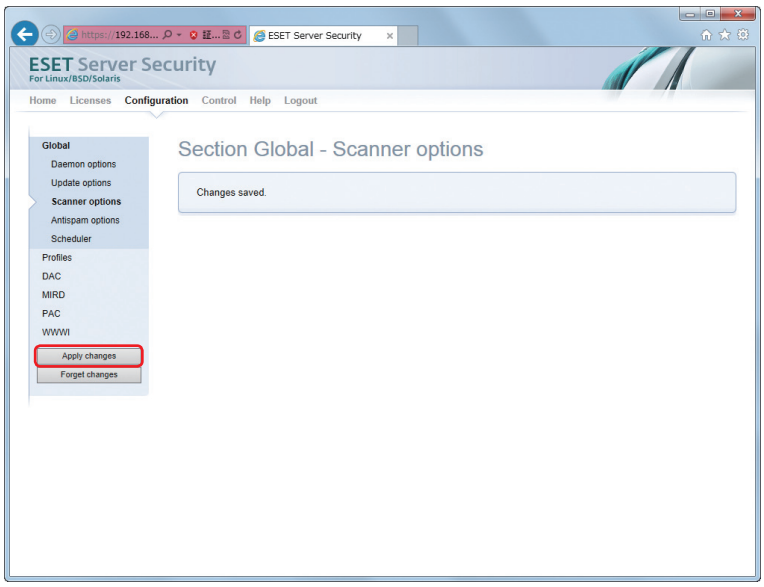


❶[Exclusions]にチェックを入れ、❷除外したいファイルをフルパスで入力します。❸[Save Chages]をクリックします。

POINT

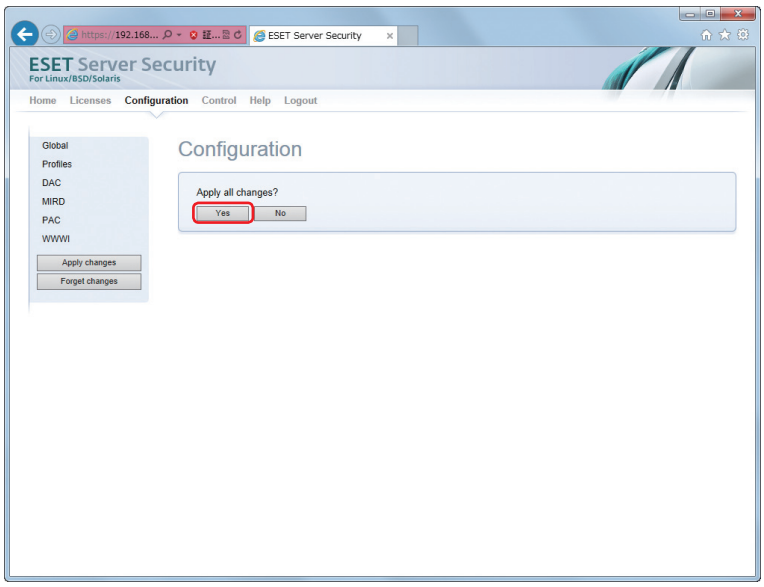
/usr以下のすべてのファイルを除外したい場合は/usr/*.*::、複数指定したい場合は/usr/*.*::/var/*.*::と連続して入力してください。なお、オンデマンドスキャンで検査を除外したいファイルは、検査を実行する時に[Control]→[On Demand Scan]の[Exclunde paths]で設定してください。

3



[Apply changes] をクリックします。

4



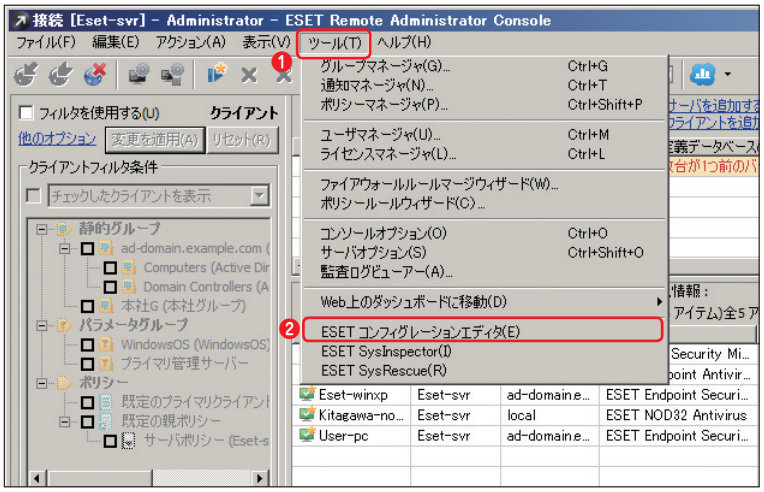
[Yes] をクリックします。

4.5.10 ウイルスとして検出されたファイルを ウイルス検査対象から除外する手順～ ERA編

ここでは、ウイルスとして検出されたファイルの除外設定をERAを用いて行う方法を説明します。ERAを利用する場合はESET コンフィグレーションエディターでファイルの除外設定を作成し、[新規タスク] または [ポリシーマネージャ] を利用して一括配布します。

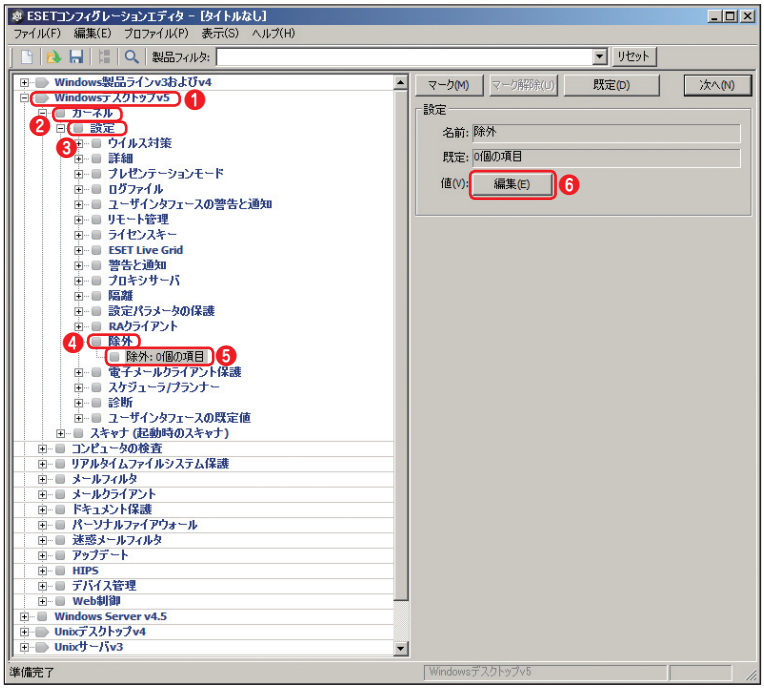
1 ERACを起動し、ERASにログオンします。

2



ESET コンフィグレーションエディターを開きます。❶[ツール] メニュー、❷[ESET コンフィグレーションエディタ] をクリックします。

3

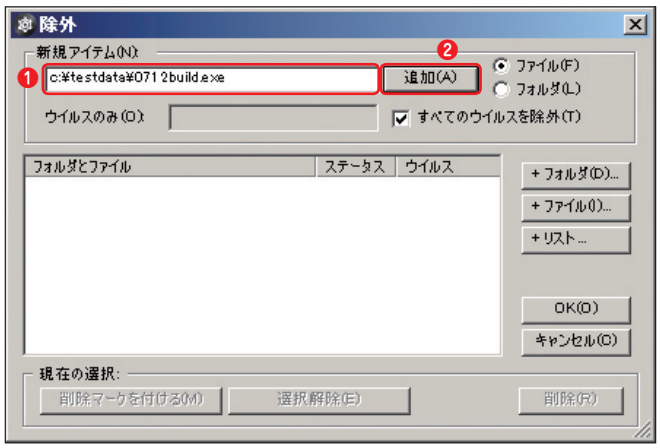


❶設定を行いたいプログラムから❷[カーネル (Mac OS X/Linuxの場合は [ESETデーモン])]、❸[設定]、❹[除外] と順にクリックしていき、最後に❺[除外] をクリックし、❻[編集] ボタンをクリックします。

POINT

Windows用のESET Endpoint SecurityおよびESET Endpoint アンチウイルスの設定を行う場合は、[Windowsデスクトップv5] を選択してください。ESET File Security for Microsoft Windows Serverの設定を行う場合は、[Windows Server V4.5] を選択してください。Mac OS X用のESET NOD32アンチウイルスの設定を行う場合は、[Unixデスクトップv4] を選択してください。ESET File Security for Linuxの設定を行う場合は、[Unixサーバ V4] を選択してください。Windows用のESET Smart SecurityおよびESET NOD32アンチウイルスの設定を行う場合は、[Windows製品ラインv3およびv4] を選択してください。

4

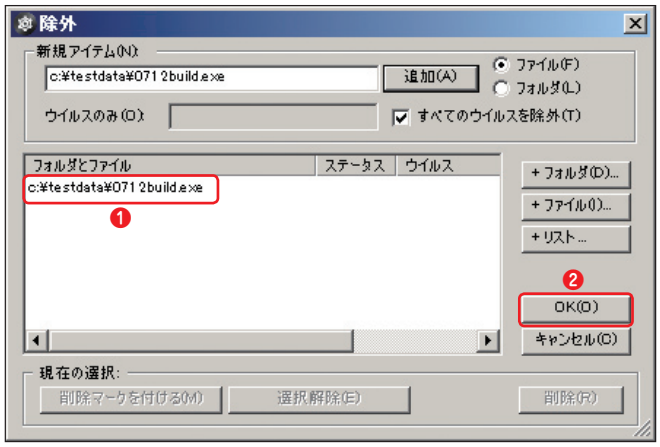


[除外] ダイアログが開きます。❶ [新規アイテム] 欄に除外したいファイルまたはフォルダーをフルパスで直接入力し、❷ [追加] ボタンをクリックします。

POINT

除外リストへの登録は、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、「C:¥testdata¥*.*」のような形式で、フルパスでフォルダー名を入力し、ファイル名を「*.*」とします。また、拡張子で指定する場合は、「c:¥testdata¥*.doc」のような形式で入力します。

5



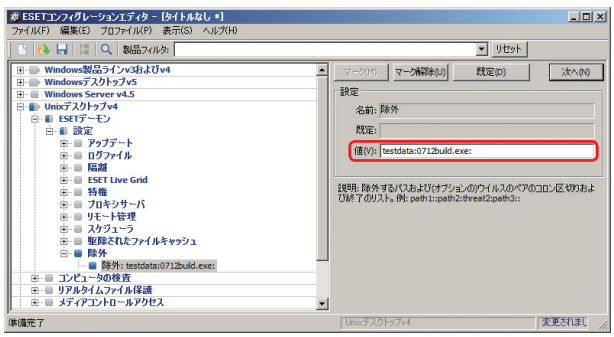
❶入力したファイルが登録されます。❷ [OK] ボタンをクリックします。

CAUTION

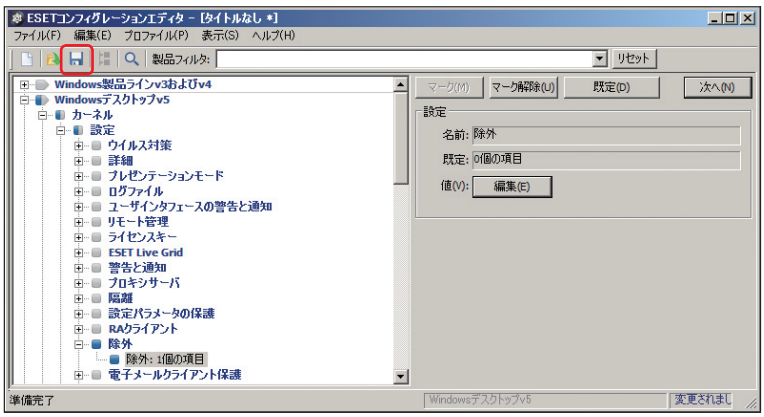
[フォルダ] ボタンや [ファイル] ボタンをクリックすると、ダイアログを利用してファイルやフォルダーの指定が行えますが、このダイアログは、現在操作しているコンピューター内のみを表示します。

コラム

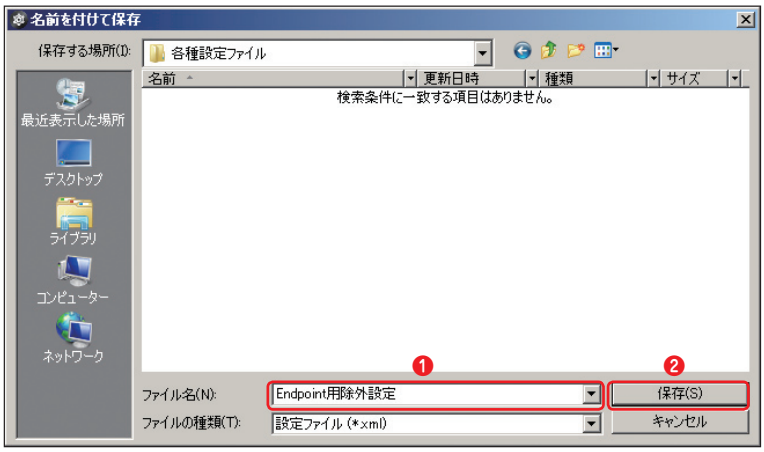
Mac OS Xの除外設定について



Mac OS Xの除外設定を行う場合は、手順4で以下のような画面が表示されます。除外したいファイルを [値] 欄にフォルダーとファイル名の間を「:(コロン)」で区切って入力します。フォルダーのみを登録したいときは、フォルダー名の後に [:(コロン)] を2回入力します。入力が終わったら、手順6に進みます。

6 

[保存] ボタンをクリックします。

7 

設定ファイルを保存します。❶ファイル名を入力し、❷[保存] ボタンをクリックします。

8 [×] ボタンをクリックし、ESET コンフィグレーションエディターを閉じます。

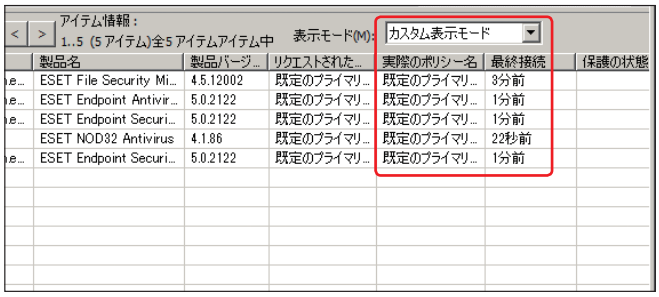
9 保存した設定ファイルを [新規タスク] または [ポリシーマネージャ] を利用して一括配布します。

[FAQ]
よくある質問
お問い合わせの際に

質問事項一覧

01 ERAC上での時間の表示形式を変更するには？

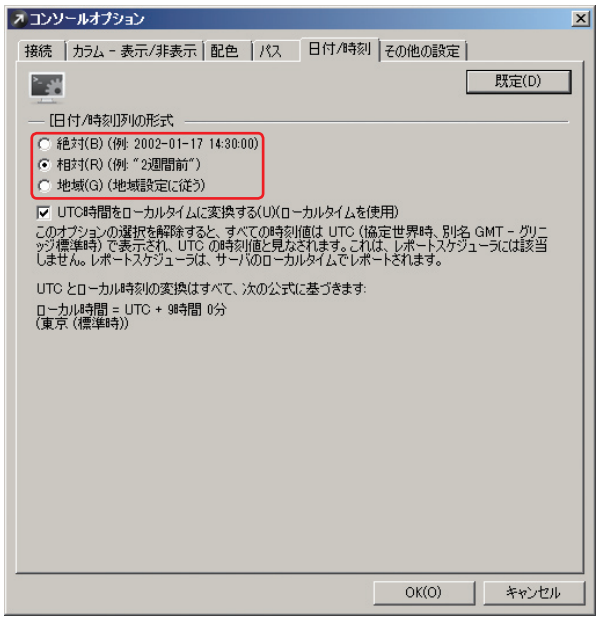
時間の表示形式は、既定では［相対］であり、下図のように現在の時刻との差が表示されます。



ERAC上での時間の表示形式を変更するには、以下の操作を行います。

1 ERACを起動し、ERASへログオンします。

2 ［ツール］メニューから、［コンソールオプション］をクリックします。

3 

［コンソールオプション］ダイアログが表示されますので、［日付/時刻］タブをクリックします。
［絶対］［相対］［地域］から、表示形式を選択します。

02 クライアントPCの設定をERASからリモートで変更するには？

クライアントPCの設定をERASからリモートで変更するには、設定変更の対象となるクライアントPCに対して、［コンフィグレーション］タスクを割り当てます。
※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

03 クライアントPCにアップデートを行わせるには？

クライアントPCにアップデートを行わせるには、対象となるクライアントPCに対して、[今すぐアップデート] タスクを割り当てます。

※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

04 クライアントPCにコンピューターの検査を行わせるには？

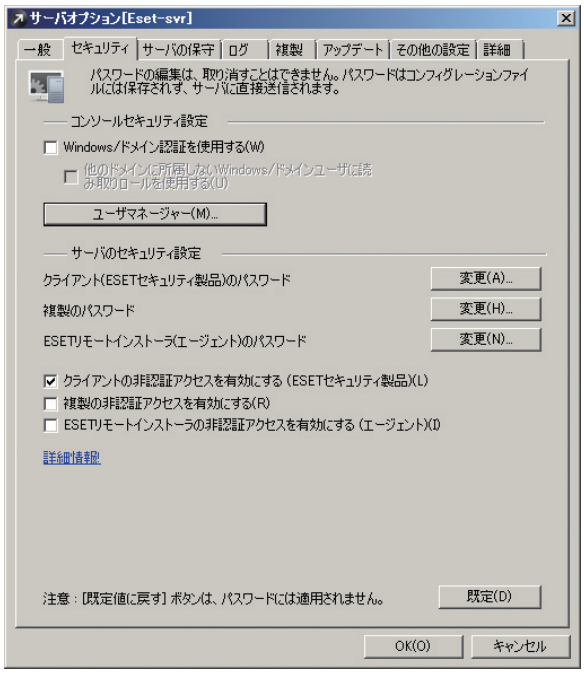
クライアントPCにコンピューターの検査を行わせるには、対象となるクライアントに対して、[オンデマンドスキャン] または [オンデマンドスキャン（駆除無効）] タスクを割り当てます。

※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

05 ERASのパスワードを変更するには？

ERASのパスワードを変更するには、[サーバオプション] ダイアログの [セキュリティ] タブで設定を行います。

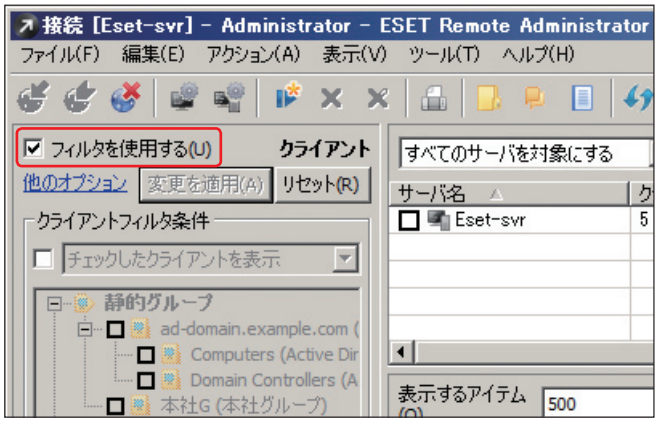
※詳細は、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。



06 表示されるアイテムのフィルタリングを行うには？

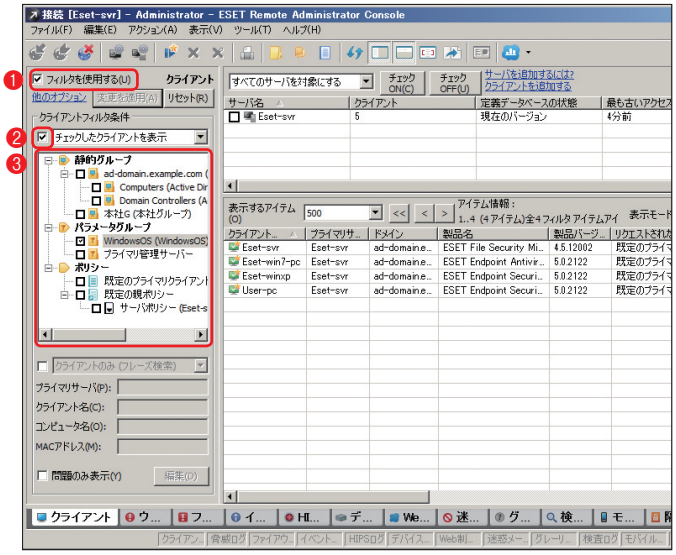
[レポート] ペインと [リモートインストール] ペインを除く、各ペインに表示されるアイテムのフィルタリングを行うには、[フィルタ] 機能を有効にし、フィルタリング条件を指定します。フィルタリングの条件には、[共通フィルタ] と [ペイン固有フィルタ] が準備されています。共通フィルタでは、グループマネージャで作成したグループ単位でフィルタリングできるほか、[プライマリサーバ] や [クライアント] [コンピュータ名] [MACアドレス] などのクライアントの条件を指定したフィルタリングも行えます。

フィルタ機能を有効にする



フィルタ機能を有効にするには、[フィルタを使用する] にチェックを入れます。フィルタ機能を無効にする場合は、チェックを外します。

グループを利用してフィルタリングする



グループを利用してフィルタリングするには、以下の操作を行います

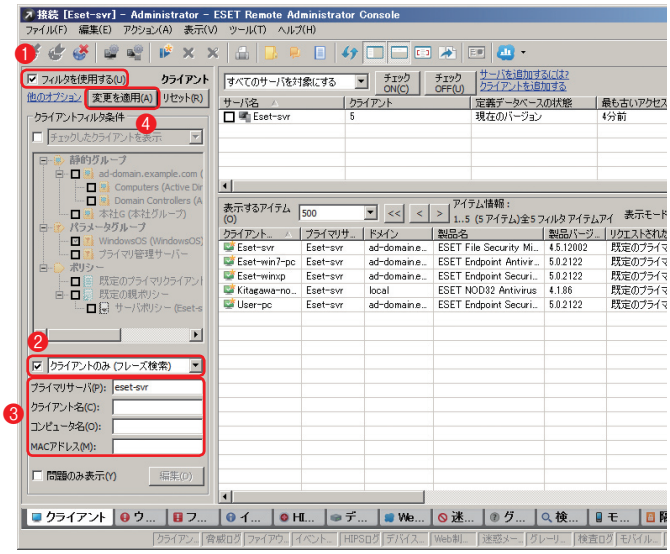
❶ [フィルタを使用する] にチェックを入れ、フィルタ機能を有効にします。

❷チェックボックスにチェックを入れます。

❸表示したいグループにチェックを入れます。条件がすぐに反映され、チェックを入れたグループのみが表示されます。

クライアントを指定した条件でフィルタリングする

クライアントPCを指定条件でフィルタリングするには、以下の操作を行います。



❶ [フィルタを使用する] にチェックを入れ、フィルタ機能有効にします。

❷チェックボックスにチェックを入れ、フィルタリングの方法を設定します。

❸ [プライマリサーバ] [クライアント] [コンピュータ名] [MACアドレス] の各エディットボックスにフィルタリング条件を入力します。複数のエディットボックスに入力した場合、すべての条件にあてはまるアイテムを表示します。

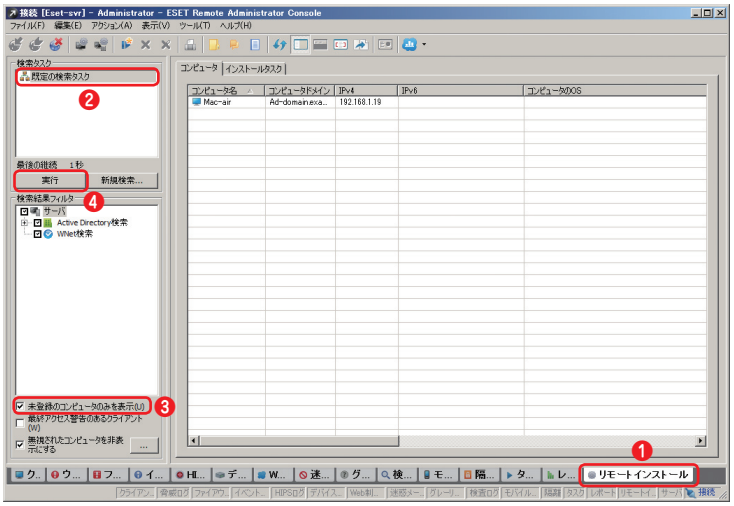
❹ [変更を適用] ボタンをクリックします。

07 ERASで管理されていないコンピューターを検出するには？

ERASに接続していないコンピューターや、ESET セキュリティ製品がインストールされていないコンピューターを検出するには、以下の操作を行います。

1 ERACを起動し、ERASへログオンします。

2



❶ [リモートインストール] タブをクリックします。

❷ [既定の検査タスク] をクリックします。

❸ [未登録のコンピュータのみを表示] にチェックを入れます。

❹ [実行] ボタンをクリックします。

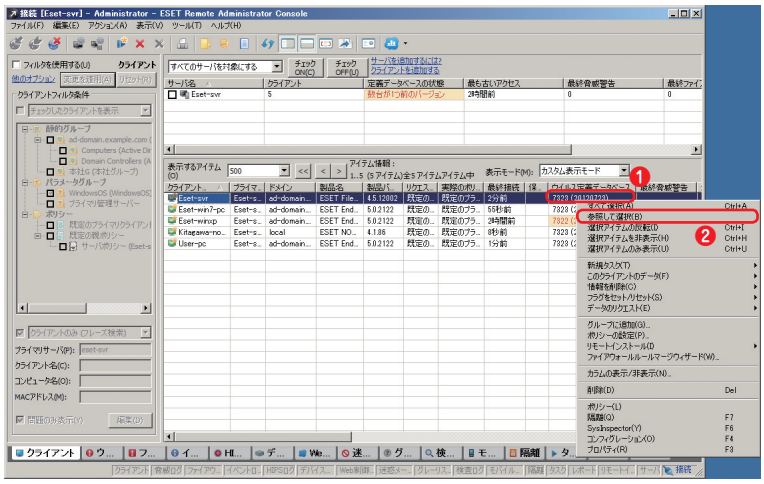
3 登録されていないコンピューターが [リモートインストール] ペインに表示されます。

08 ウイルス定義データベースが最新でないクライアントのみを表示するには？

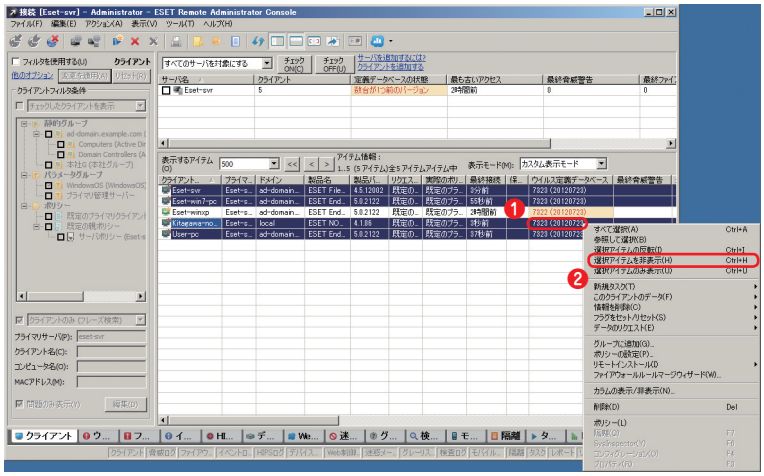
[クライアント] ペインで、ウイルス定義データベースが最新でないクライアントのみを表示するには、以下の操作を行います。

1 ERACを起動し、ERASへログオンします。

2 [クライアント] タブをクリックします。

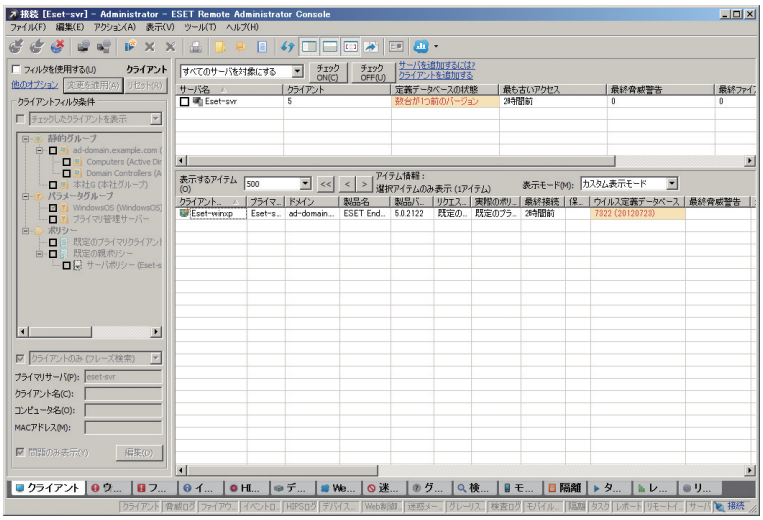
3 

❶最新のウイルス定義データベースを利用しているクライアントの [ウイルス定義データベース] 欄を右クリックして、❷ [参照して選択] をクリックします。

4 

❶再度右クリックして、❷ [選択アイテムを非表示] をクリックします。

5 ダイアログが表示されます。[OK] ボタンをクリックします。

6 

ウイルス定義データベースが最新でないクライアントのみが表示されます。

POINT

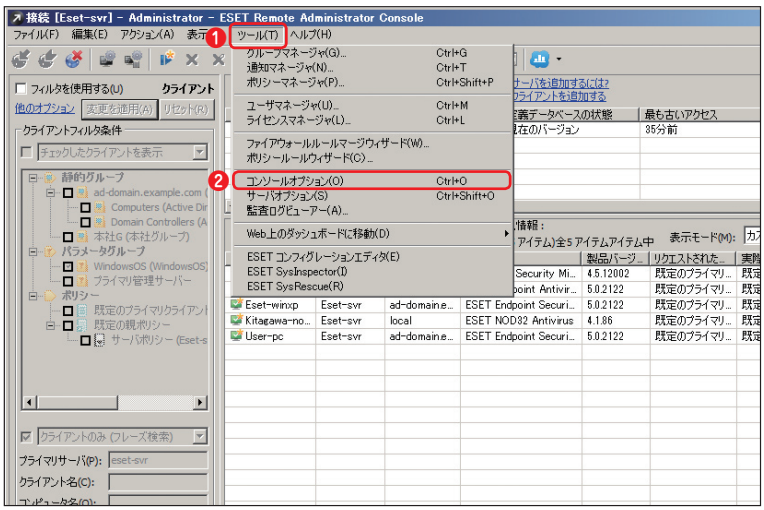
表示をもとに戻すときは、[表示] メニューの[選択アイテムのみ表示] をクリックするか、[更新] ボタンをクリックします。キーボードの[F5] キーを押すことでも表示をもとに戻せます。

09 画面表示の更新を停止するには？

画面表示の更新を停止するには、以下の操作を行います。

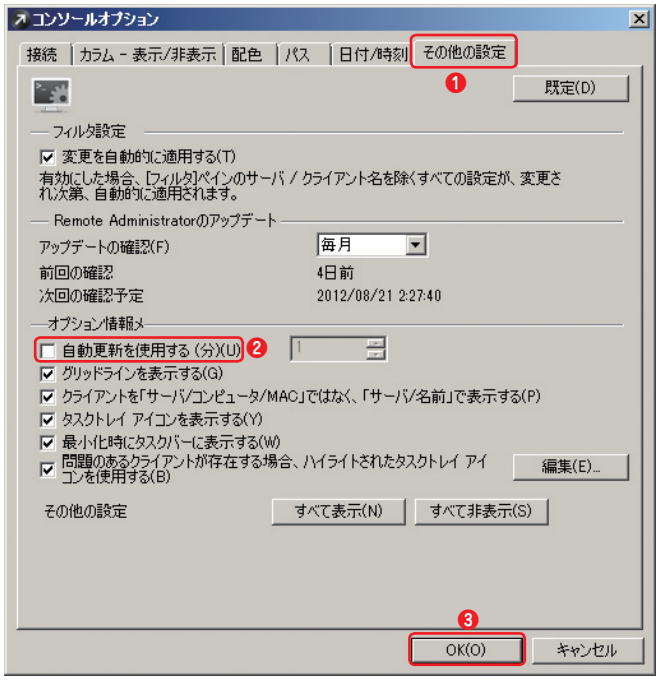
1 ERACを起動し、ERASへログオンします。

2



❶ [ツール] メニューをクリックし、❷ [コンソールオプション] をクリックします。

3



❶ [その他の設定] タブをクリックし、❷ [自動更新を使用する(分)] のチェックを外します。❸ [OK] ボタンをクリックします。

10 コマンドラインオプションについて

Windows用プログラムのインストールパッケージは、作成の際にさまざまなコマンドラインオプションを指定できます。詳細については、「ESET Remote Administrator ユーザーズマニュアル」をご参照ください。

11 複製が正常にできないのですが？

複製がうまくいかない場合、以下の項目をご確認ください。

- 下位サーバーは上位サーバーが指定したポート番号（既定値は「2846」）へ接続できる必要があります。
- 上位サーバーが下位サーバーを指定する際は、「IPアドレス」ではなく「コンピューター名」によって指定する必要があります。
- 管理情報の複製は、下位サーバーが上位サーバーへ接続した際に実行されます。複製が行われるまでに時間がかかることがあります。
- 上位サーバーから下位サーバー配下のクライアントPCへタスクを発行した場合、下位サーバーが上位サーバーへ接続した時点で実際のタスクが発行されます。このため、クライアントPCがタスクを受け取るまでに時間がかかることがあります。

12 [リモートインストール] ペインで検出されないコンピューターがあるのですが？

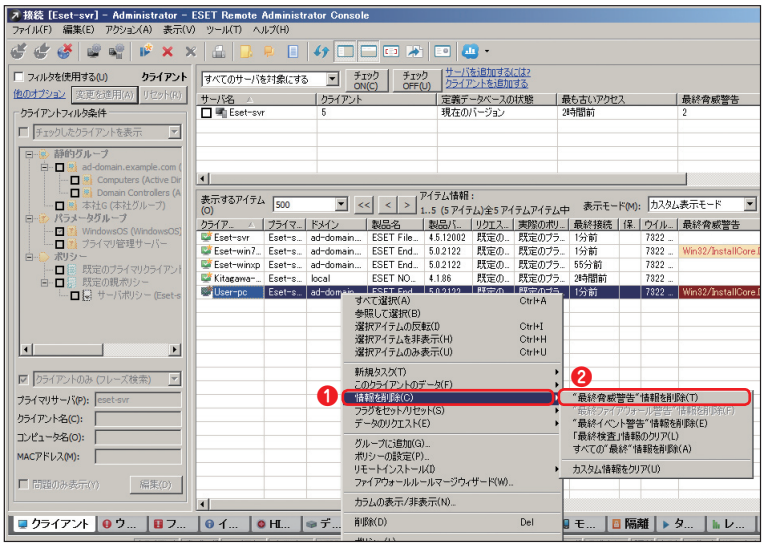
検出には、NetBIOSを利用します。[リモートインストール] ペインで検出することができるコンピューターには、Windowsがファイル共有時に利用する [Microsoftネットワーク用ファイルとプリンター共有] や [Microsoftネットワーク用クライアント] などの機能がインストールされている必要があります。

13 [最終ウイルス警告]に表示されている警告が消えないのですが？

[最終ウイルス警告]には、クライアントPCが最後に検出したウイルスの名称が表示されますが、クライアントPC側でウイルスの駆除、または削除を行っても[最終ウイルス警告]に表示されている警告は消えません。[最終ウイルス警告]に表示されている警告を消すには、以下の操作を行います。

1 [最終ウイルス警告]欄に表示されている文字を消したいクライアントPCを右クリックします。

2



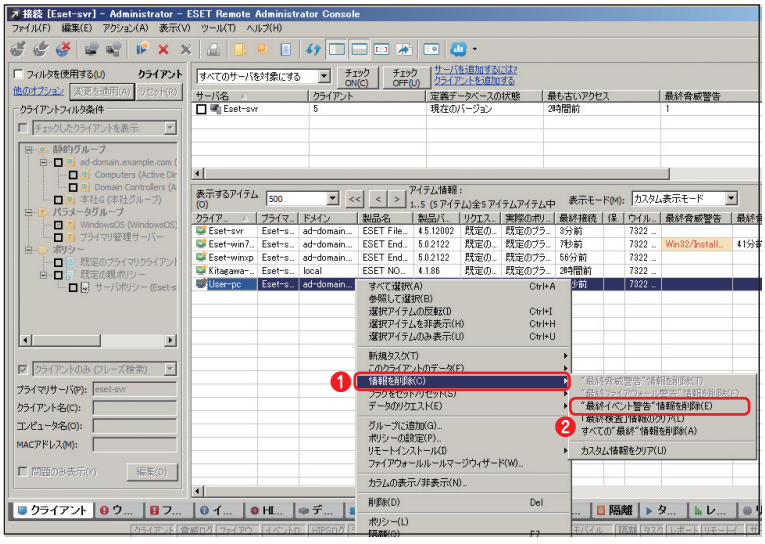
表示されるコンテキストメニューから❶[情報を削除]をクリックし、❷["最終脅威警告"情報を削除]をクリックします。

14 [最終イベント警告]に表示されている警告が消えないのですが？

[最終イベント警告]に表示されている警告を消すには、以下の操作を行います。

1 [最終イベント警告]に表示されている文字を消したいクライアントPCを右クリックします。

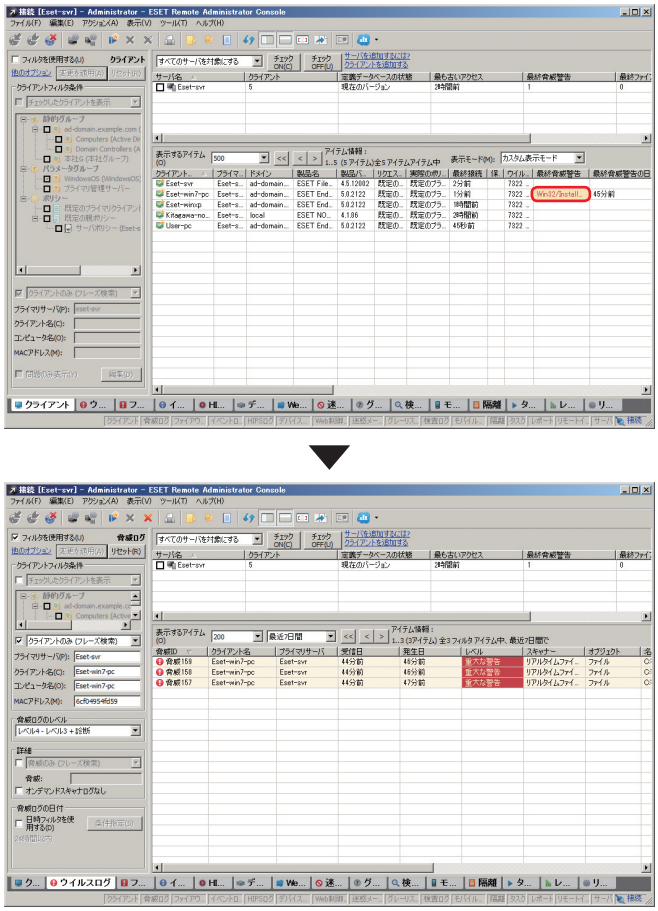
2



表示されるコンテキストメニューから❶[情報を削除]をクリックし、❷["最終イベント警告"情報を削除]を選択します。

15 簡単にフィルタを利用する方法は？

[クライアント] ペインに表示される [最終ウイルス警告] [最終ファイアウォール警告] [最終イベント警告] などのカラムは、フィルタに利用できます。この機能を利用すると、特定のクライアントPCの指定カラムに関連するログ情報のみを表示することができます。たとえば、特定のクライアントPCの [最終ウイルス警告] に関するログ情報のみを表示したいときは、そのクライアントPCの [最終ウイルス警告] カラムをダブルクリックします。



フィルタリングして表示したいクライアントPCのカラム欄（ここでは、[Eset-win7-pc] の [最終ウイルス警告]）をクリックすると、[ウイルスログ] ペインに、選択したクライアントPCのログ情報のみが表示されます。

16 タスクがなかなか配布されないのですが？

クライアントに対して発行したタスクは、クライアントがERASへ接続した際にクライアントへ配布されます。クライアントがERASへ接続するまで、タスクは配布されません。

17 ERASとERACは同一のコンピューターにインストールする必要がありますか？

必要ありません。ERASとERACは、異なるコンピューターにインストールしても運用できます。ただし、ERASをインストールしたコンピューターでERAメンテナンスツールを利用する際には、ERASとERACは同一のコンピューターにインストール必要があります。

18 初めてERASへの接続時に入力するパスワードは何ですか？

既定の状態では、ERASにはパスワードが設定されていませんので、[パスワード] ダイアログには何も入力せずに [OK] ボタンをクリックしてください。

19 ERAS、ERACはインストール台数に制限がありますか？

ERAS、ERAC共に特に制限は設けておりませんので、必要な台数分インストールしてください。

20 ERASを導入する際に利用するポート番号は？

ERASを導入した環境で利用されるポートは、以下の通りです。

プロトコル	ポート番号	用途
TCP	2221	クライアント PC がミラーサーバーへ接続するときに参照
	2222	クライアント PC が ERAS へ接続するときに参照
	2223	ERAC が ERAS へ接続するときに参照
	2224	クライアント PC が ERAS へ接続するときに参照
	2225	ダッシュボートサーバー
	2846	管理サーバー（ERAS）を複数設置した場合に、下位の管理サーバー（ERAS）から上位の管理サーバー（ERAS）へ接続するときに参照

また、プッシュインストール時には、ERASから、インストール対象となるクライアントPCの以下のポートに対して通信できる必要があります。

プロトコル	ポート番号
TCP,UDP	137
UDP	138
TCP	139
TCP,UDP	445

21 ウイルス定義データベースをUSB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メモリーやCD-Rを利用して、クライアントPCに配布する方法は、以下の2通りがあります。それぞれ以下の手順で作業します。なお、この方法でウイルス定義データベースのアップデートが行えるのは、Windows用のセキュリティプログラムのみです。ESET NOD32アンチウイルス Mac OS X用およびESET File Security for Linux、ESET Endpoint Security for Androidは、この方法でのウイルス定義データベースのアップデートに対応していません。

●ユーザーズサイトからダウンロードしたファイルを利用
●ミラーサーバーに保存されたファイルを利用

ユーザーズサイトからダウンロードしたファイルを利用

弊社ユーザーズサイトにて、ウイルス定義データベースをダウンロードし、ダウンロードしたファイルをUSBメモリーやCD-Rに書き込んで利用します。ダウンロード方法、およびファイルの利用手順については、ユーザーズサイトの「オフライン更新手順書」をご参照ください。

CAUTION
弊社ユーザーズサイトへログインするには、有効な「シリアル番号」および「ユーザー名」が必要です。

ミラーサーバーに保存されたファイルを利用

ミラーサーバーに保存されたファイルを利用する場合は、ミラーサーバーを構築し、最新のウイルス定義データベースをダウンロードする必要があります。ミラーサーバーは、ESET Remote Administrator（ERA）またはESET File Security for Microsoft Windows ServerおよびESET Endpoint アンチウイルス、ESET File Security for Linuxで構築できます。ミラーサーバーの構築手順については、各プログラムのユーザーズマニュアルをご参照ください。

1.ウイルス定義データベースのアップデートを行います。ウイルス定義データベースのアップデート方法については、各プログラムのユーザーズマニュアルをご参照ください。

2.ウイルス定義データベースが保存されたフォルダーをUSBメモリーやCD-Rなどに書き込みます。既定値では、以下フォルダーにウイルス定義データベースが保存されています。

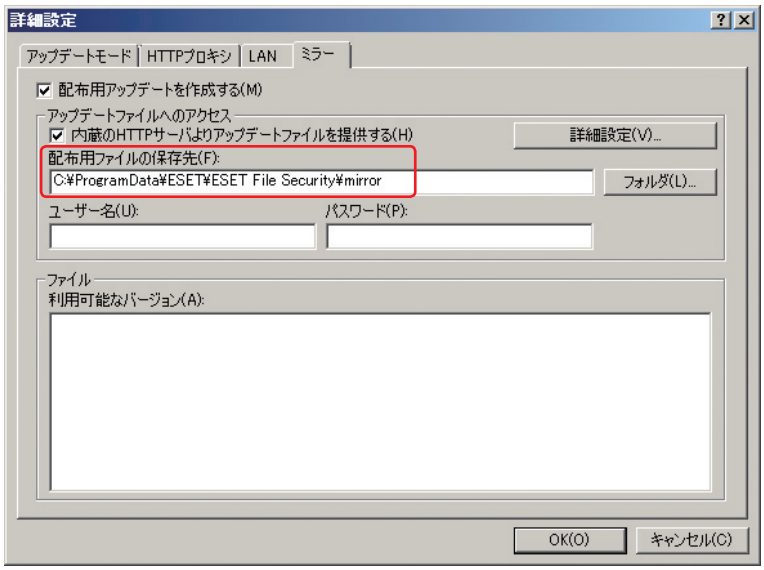
●ERAの場合
Windows Server 2003/2003 R2の場合
C:¥Documents and Settings¥All Users¥Application Data¥ESET¥ESET Remote Administrator¥Server¥Mirror

Windows Server 2008/2008 R2の場合
C:¥ProgramData¥ESET¥ESET Remote Administrator¥Server¥mirror

Windows Server 2012 Standardの場合
C:￥ProgramData￥ESET￥ESET Remote Administrator￥Server￥mirror

●ESET File Security for Microsoft Windows ServerおよびESET Endpoint アンチウイルスの場合
ミラーサーバー構築時に指定した［配布用ファイルの保存先］フォルダーをUSBメモリーやCD-Rに書き込みます。

●ESET File Security for Linuxの場合
/var/opt/eset/esets/lib/mirror



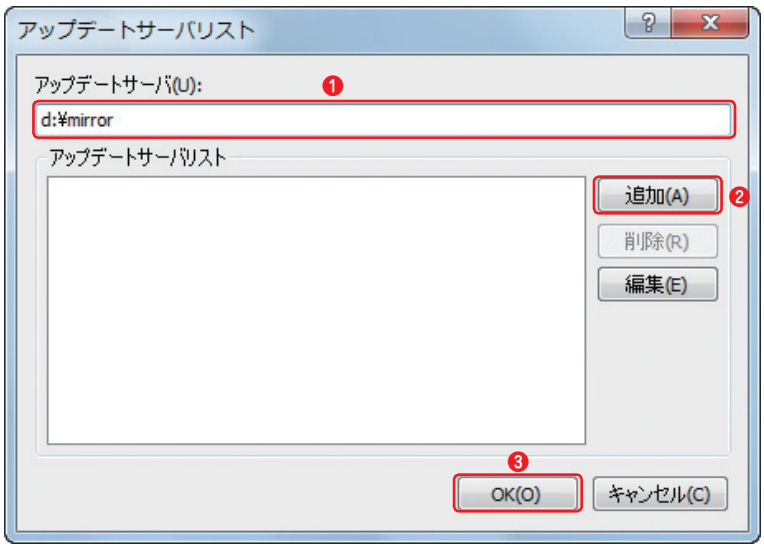
画面はESET File Security for Microsoft Windows Serverの場合。ESET Endpoint アンチウイルスも同じ画面で［配布用ファイルの保存先］フォルダーを確認できます。

クライアントPCの設定

1 Windows用プログラムのユーザーズマニュアルを参考に基本画面を開き、詳細設定画面または設定画面を開きます。

2 ［アップデートサーバ］の設定を行います。Windows用プログラムのユーザーズマニュアルを参考に設定画面を開き、「編集」ボタンをクリックします。

3 ［アップデートサーバ］に、❶USBメモリーやCD-Rの「mirror」フォルダのパス（例：D:￥mirror）を入力し、❷「追加」ボタンをクリックします。❸「OK」ボタンをクリックします。



4 [アップデートサーバ] ドロップダウンメニューより、手順3で設定したフォルダパスを選択し、「OK」ボタンをクリックします。

5 アップデートを実行します。

22 プログラムコンポーネントのミラーを作成するには？

ミラーサーバーにプログラムコンポーネントを保存する場合の設定は、ERASおよびESET Endpoint SecurityまたはESET Endpoint アンチウイルスのユーザーズマニュアルをご参照ください。ただし、製品の新しいバージョンが公開されても、必ずしもコンポーネントアップデートが行われるわけではありません。その場合は、アップデート用のプログラムコンポーネントは表示されません。また、この機能はWindows用プログラムのみで利用できます。

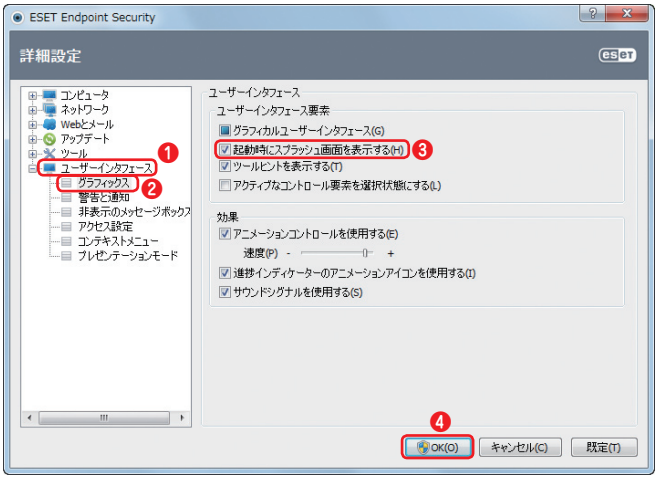
23 セキュリティプログラムの起動時に表示されるスプラッシュ画面を非表示にするには？

セキュリティプログラムの起動時に表示されるスプラッシュ画面を非表示にしたいときは、以下の手順で設定を行います。

Windows用プログラムの設定を直接変更する場合

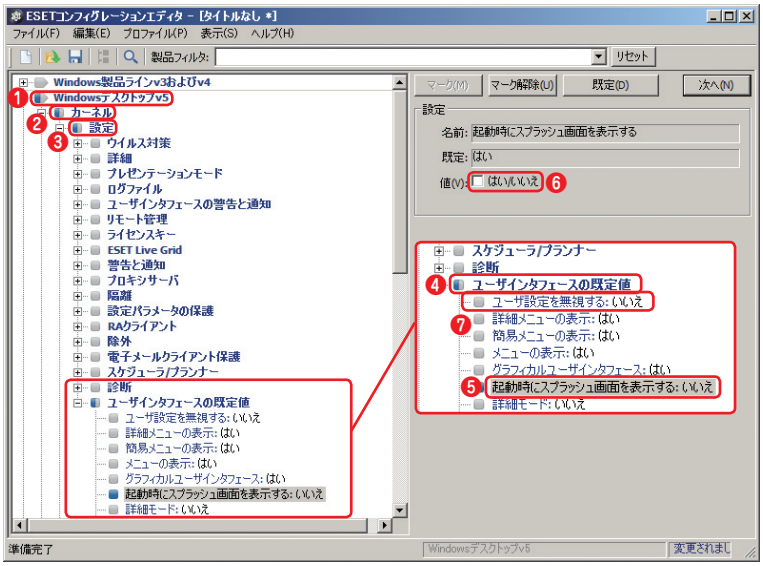
1 ESET Endpoint SecurityまたはESET Endpoint アンチウイルスのメイン画面を開きます。
[設定] をクリックし、[詳細設定を表示する] をクリックします。

2



❶ [ユーザーインタフェース] をダブルクリックし、❷ [グラフィックス] をクリックします。❸ [起動時にスプラッシュ画面を表示する] のチェックを外します。❹ [OK] ボタンをクリックします。

ESET コンフィグレーションエディターを利用する場合



ESET コンフィグレーションエディターを利用する場合は、左ペインのツリーで❶設定を行いたいクライアント用プログラム（ここでは［Windowsデスクトップv5］）をクリックし、❷［カーネル］→❸［設定］→❹［ユーザインタフェースの既定値］とクリックして開き、❺［起動時にスプラッシュ画面を表示する］で❻［値］のチェックを外し、❼［ユーザーの設定を無視する］も同様に［値］のチェックを外します。

▸▸▸ POINT

Windows用のESET Endpoint SecurityおよびESET Endpoint アンチウイルスの設定を行う場合は、「Windowsデスクトップv5」を選択して上記の手順で作業します。ESET File Security for Microsoft Windows Serverの設定を行う場合は、「Windows Server V4.5」を選択し、［File Security 4.5 for MS Windows Server］→［一般設定］→［ユーザインターフェース］→［ユーザインターフェースの既定値］とダブルクリックして設定を行います。また、Windows用のESET Smart SecurityおよびESET NOD32アンチウイルスの設定を行う場合は、「Windows製品ラインv3およびv4」を選択して設定を行います。なお、Mac OS X用プログラムは、ESET コンフィグレーションエディターで起動時に表示されるスプラッシュ画面の非表示を設定することはできません。

Mac OS X用プログラムの設定を直接変更する場合

1

メインウィンドウを開き、詳細モードへ切り替えてから、❶[設定]ボタンをクリックし、❷[アプリケーションの設定を入力する]をクリックします。

2

❶[ユーザー]ボタンをクリックし、❷[インタフェース]をクリックします。❸[起動時にスプラッシュウィンドウを表示する]のチェックを外し、❹[OK]ボタンをクリックします。

24 Mac OS Xでの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併せて検査の対象とすると、検査の対象数が多くなり、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外して検査を行ってください。

お問い合わせの際に

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。	169 ページ
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、PC 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。	172 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。	179 ページ
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。	190 ページ

●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。	173 ページ
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。	175 ページ
プロセス情報の取得	コンピューター上で動作中のドライバやアプリケーション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などを確認するために取得します。	177 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。	181 ページ
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。	191 ページ

CAUTION

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。

環境設定ファイル（SysInspector）の情報（*.zip）の取得方法

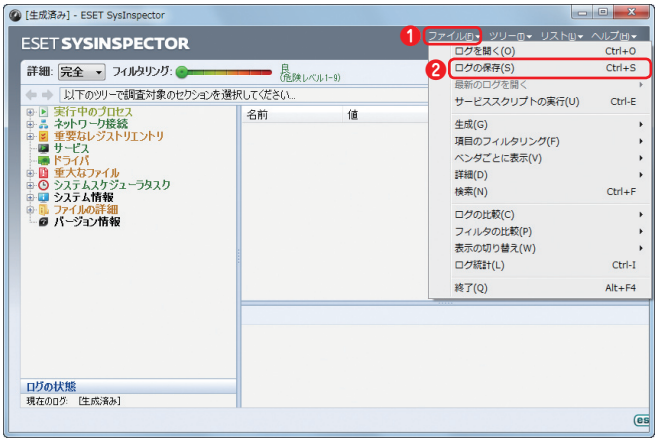
SysInspectorの情報は、情報を取得したいコンピューターを直接操作して取得する方法とESET Remote Administrator Console（ERAC）を利用してリモート操作で取得する方法があります。

コンピューターを直接操作して取得する

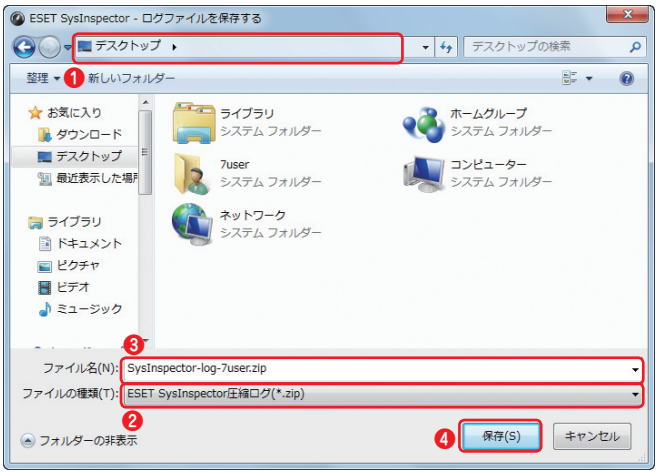
1 [スタート]ボタンから、[すべてのプログラム]（もしくは[プログラム]）、[ESET]、[ESET Endpoint Security]（または[ESET Endpoint Antivirus]）とクリックし、最後に[ESET SysInspector]をクリックします。Windows Vista/7をご利用の場合は、[ユーザーアカウント制御]ダイアログが起動します。Windows Vistaをご利用の場合は[続行]ボタン、Windows 7をご利用の場合は[はい]ボタンをクリックします。

CAUTION

SysInspectorの起動には数分かかる場合があります。

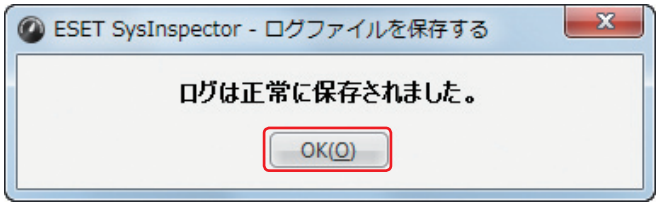
2 

❶[ファイル]をクリックし、❷[ログの保存]をクリックします。

3 

保存先とファイル名を入力します。❶保存先を選択し、❷[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、❸[ファイル名]を入力します。❹[保存]ボタンをクリックします。

4 ダイアログが表示されます



保存されたことを知らせるダイアログが表示されるので、[OK] ボタンをクリックします。

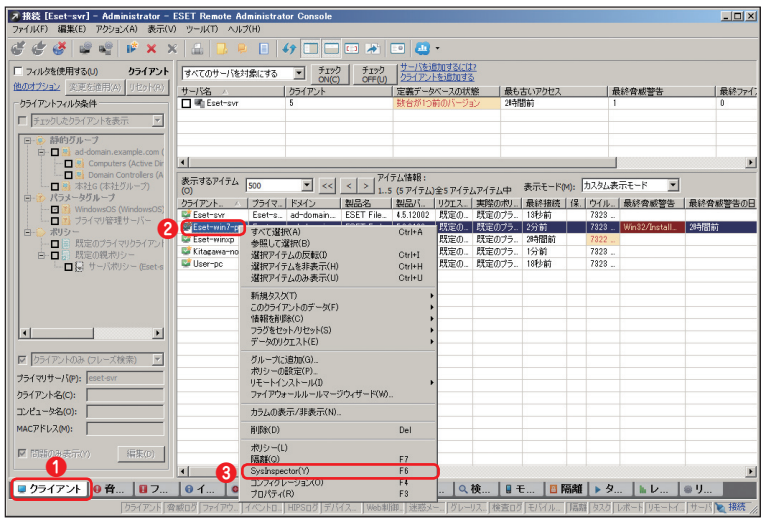
5 SysInspectorを終了します

[閉じる] ボタンをクリックして、ESET SysInspectorを終了します。

ERACのリモート操作で取得する

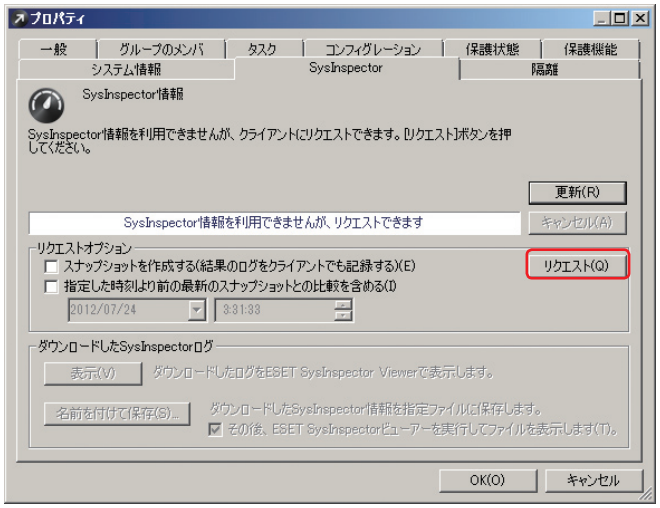
1 [スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[ESET]、[ESET Remote Administrator Console] とクリックし、最後に [ESET Remote Administrator Console] をクリックします。

2



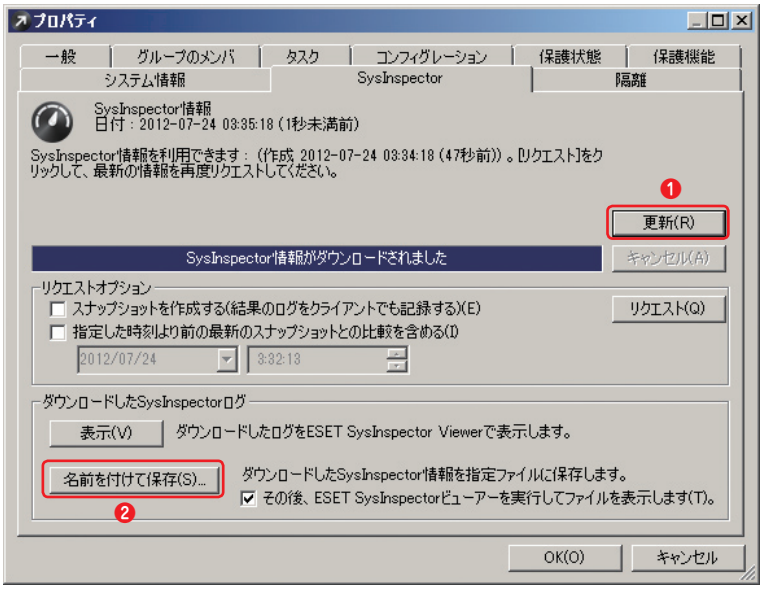
❶ [クライアント] ペインをクリックし、❷ SysInspectorの情報を取得したいコンピューターを右クリックします。❸ [SysInspector] をクリックします。

3



[リクエスト] ボタンをクリックします。

4

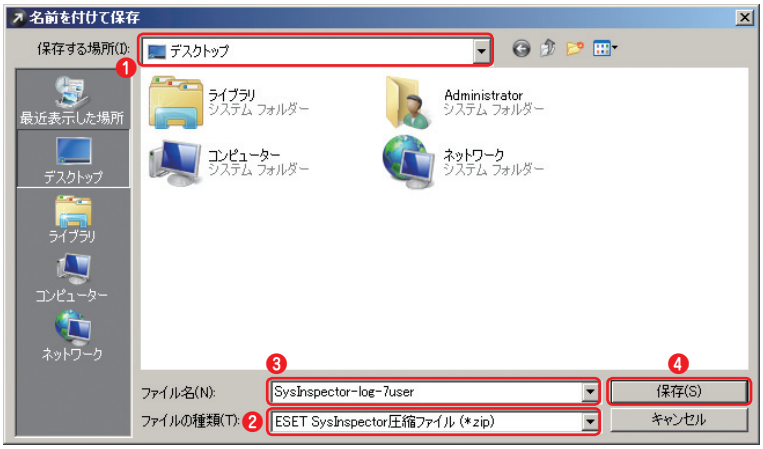


SysInspectorの情報は、対象コンピューターがリクエスト処理実行後、管理サーバー（ERAS）に接続したときにERASへ送信されます。情報が送信されたら、❶[更新]ボタンをクリックしてください。SysInspectorの情報がダウンロードされます。❷[名前をつけて保存]ボタンをクリックします。

▸▸▸ POINT

[ESET SysInspector ビューアーを起動し、ファイルを表示する]にチェックを入れて保存すると、保存終了後にESET SysInspector Viewerが起動し、取得した情報の閲覧が行えます。

5



❶保存先を選択し、❷[ファイルの種類]が[ESET SysInspector圧縮ファイル(*.zip)]であることを確認して、❸[ファイル名]を入力します。❹[保存]ボタンをクリックします。

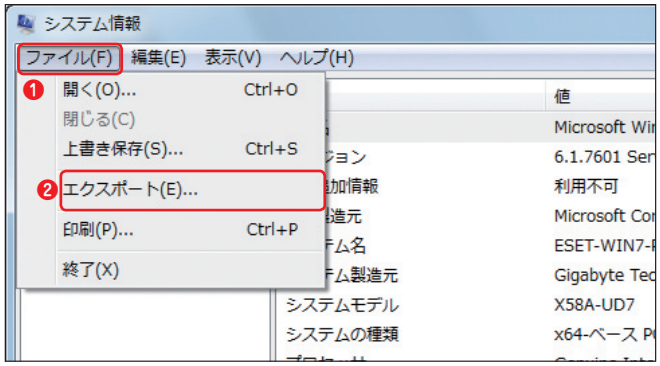
Windowsのシステム情報（*.txt）の取得方法

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］を利用して取得します。Windows XP以降のすべてのWindows OSで同じ手順で取得できます。

1 ［システム情報］を起動します

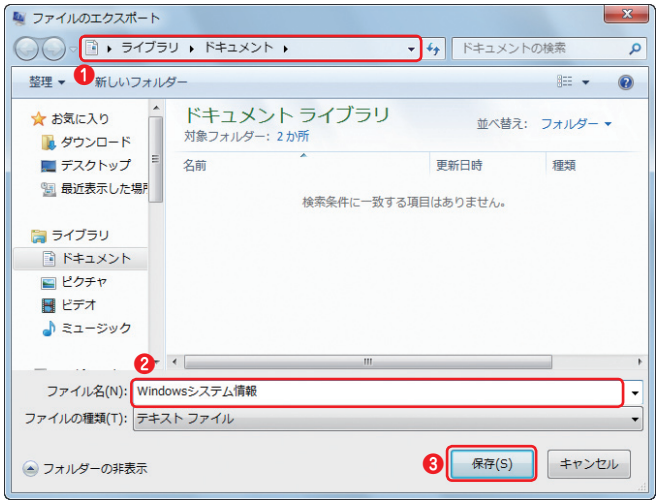
［スタート］ボタンから、［すべてのプログラム］（もしくはプログラム）、［アクセサリ］、［システムツール］とクリックし、最後に［システム情報］をクリックします。

2 システム情報を保存します



❶［ファイル］をクリックし、❷［エクスポート］をクリックします。

3 保存先とファイル名を入力します



❶保存先を選択し、❷［ファイル名］を入力します。❸［保存］ボタンをクリックします。システム情報の保存が行われます。保存中は、進捗状況画面が表示されます。

Mac OS Xのシステム情報の取得方法

ご利用のMac端末のシステム情報の取得は、以下の手順で行います。ここでは、Mac OS X Lion v10.7のシステム情報の取得手順を説明します。

1 アップルメニューをクリックします

❶[アップルメニュー]をクリックし、❷[この Mac について]をクリックします。

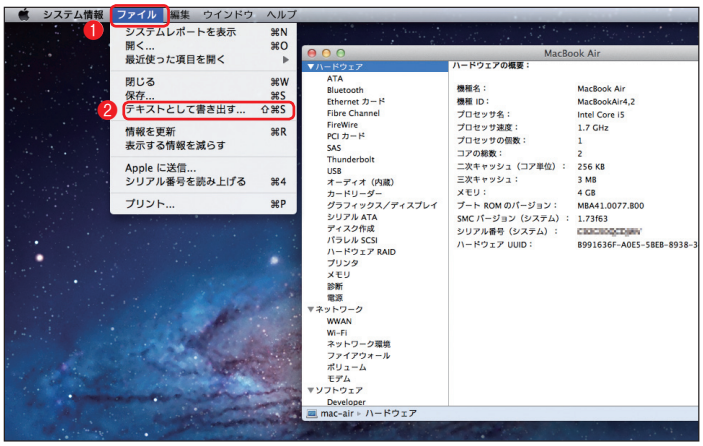
2 画面が表示されます

[詳しい情報]ボタンをクリックします。

3 画面が切り替わります

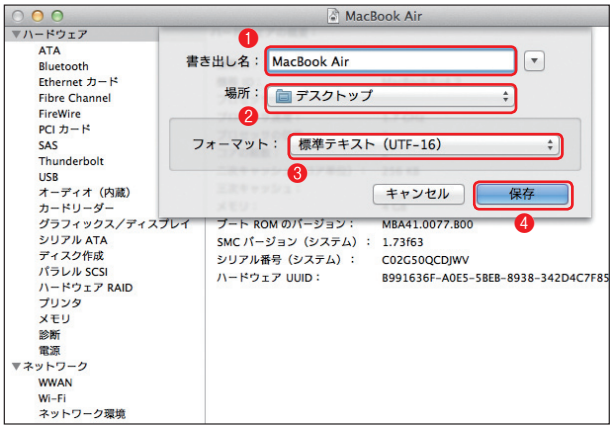
[システムレポート]ボタンをクリックします。

4 システムレポートが表示されます



❶メニューバーの［ファイル］をクリックし、❷［テキストとして書き出す］をクリックします。

5 ファイルを保存します



❶ファイル名を入力し、❷［場所］のプルダウンメニューから保存場所を選択し、❸［フォーマット］のプルダウンメニューから［標準テキスト（UTF-16）を選択し、❹［保存］ボタンをクリックします。

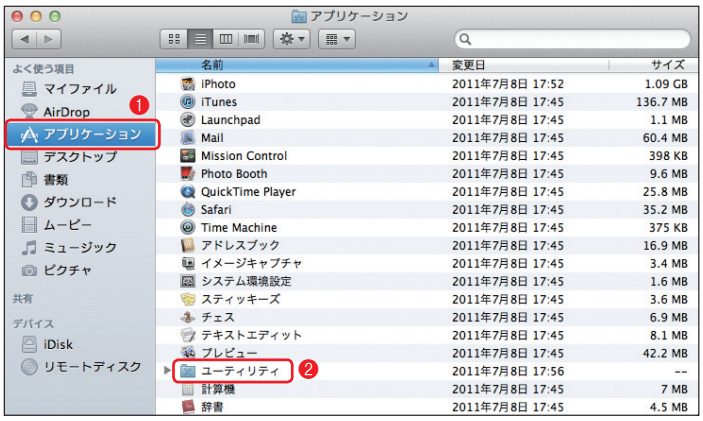
6 ファイルが保存されます

システムレポートが保存されます。

Mac OS Xのコンソールメッセージの取得方法

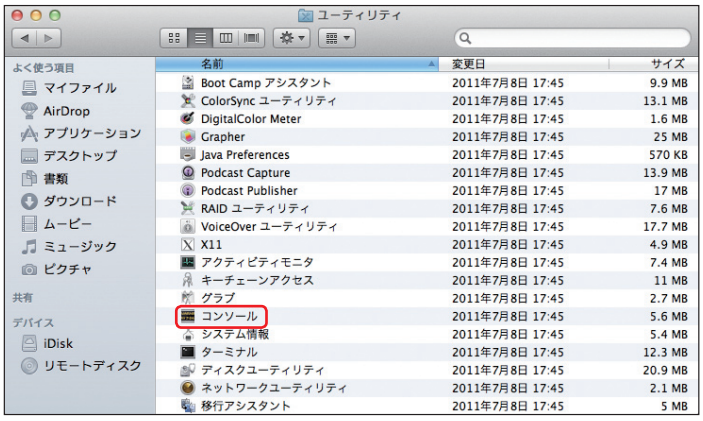
ご利用のMac端末のコンソールメッセージの取得は、以下の手順で行います。

1 Finderを起動します



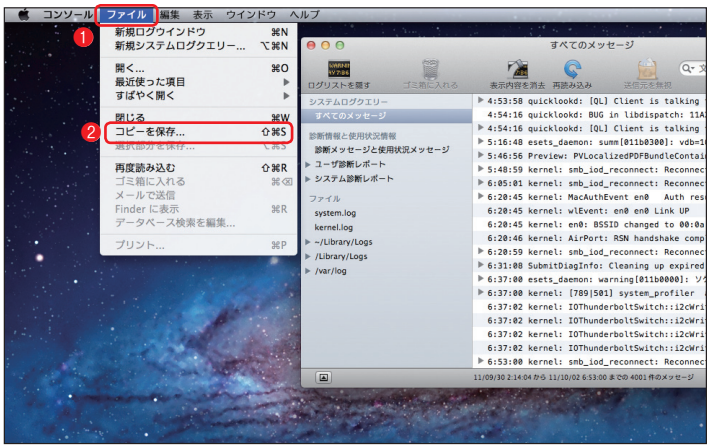
Finderを開き、❶[アプリケーション]をクリックして、❷[ユーティリティ]フォルダーをダブルクリックします。

2 コンソールを起動します



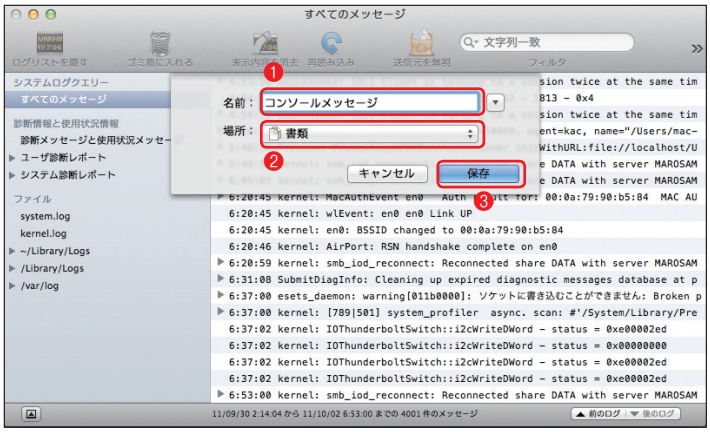
[コンソール]アイコンをダブルクリックします。

3 ファイルの保存を始めます



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

4 ファイルを保存します

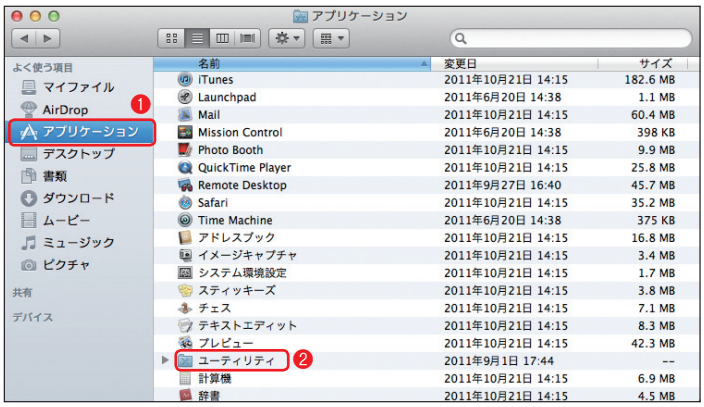


❶ファイル名を入力し、❷[場所] のプルダウンメニューから保存場所を選択します。❸[保存] ボタンをクリックします。

Mac OS Xのプロセス情報の取得方法

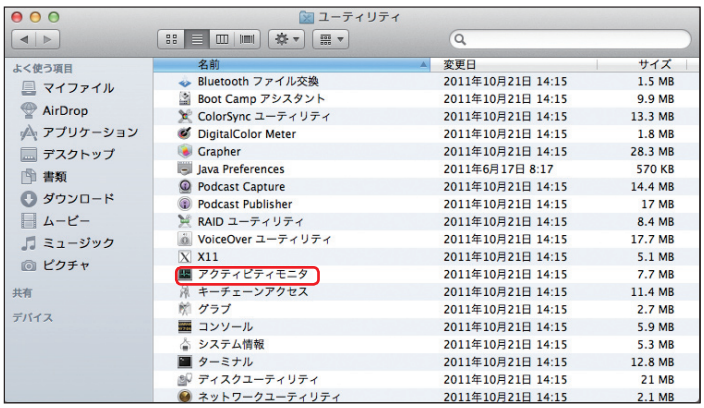
ご利用のMac端末のプロセス情報の取得は、以下の手順で行います。

1 Finderを起動します



Finderを開き、❶[アプリケーション]をクリックして、❷[ユーティリティ]フォルダーをダブルクリックします。

2 アクティビティモニタを起動します



[アクティビティモニタ]アイコンをダブルクリックします。

3 ファイルの保存を始めます

アクティビティモニタが起動します。❶メニューバーの[ファイル]をクリックし、❷[保存]をクリックします。

4 保存を実行します

❶ファイル名を入力し、❷[場所]のプルダウンメニューから保存場所を選択します。❸[標準テキスト]にチェックを入れ、❹[保存]ボタンをクリックします。

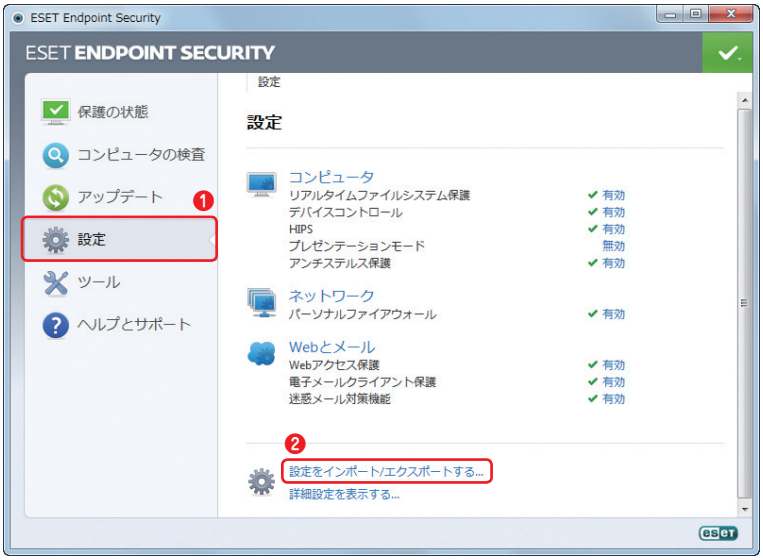
ESET製品の設定ファイル(.xml)の取得方法

ESET製品の設定ファイル(.xml)には、クライアント用プログラムの設定ファイルとESET Remote Administrator(ERA)の設定ファイルがあります。WindowsおよびMac OS Xの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することで取得できます。ERAの設定ファイルは、ESET Remote Administrator Maintenance Tool(ERAメンテナンスツール)を利用して取得します。また、ESET File Security for Linux およびESET Endpoint Security for AndroidはERAを利用して設定ファイルを取得します。

クライアント用プログラムの設定ファイル(.xml)の取得方法(Windowsの場合)

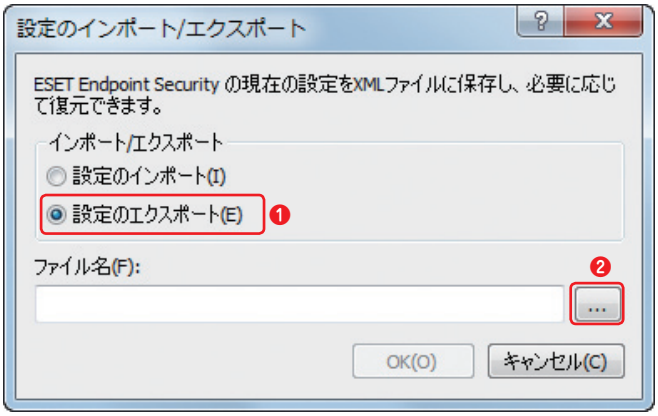
1 ESET Endpoint SecurityまたはESET Endpoint アンチウイルスのメイン画面を開きます。

2



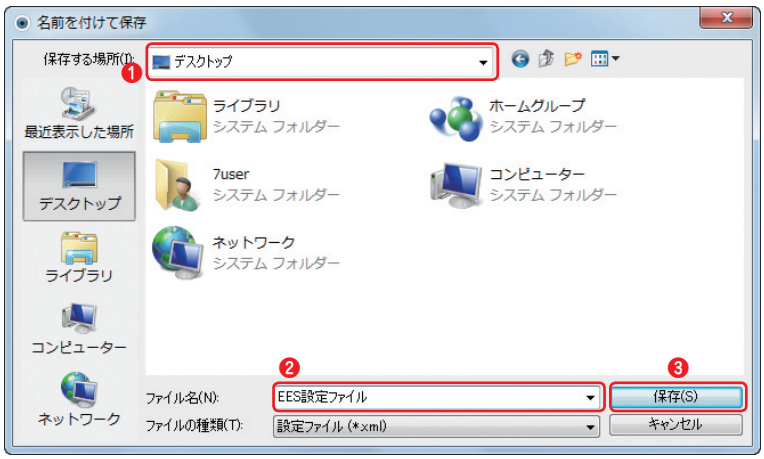
❶[設定]をクリックし、❷[設定をインポートおよびエクスポートする]をクリックします。

3



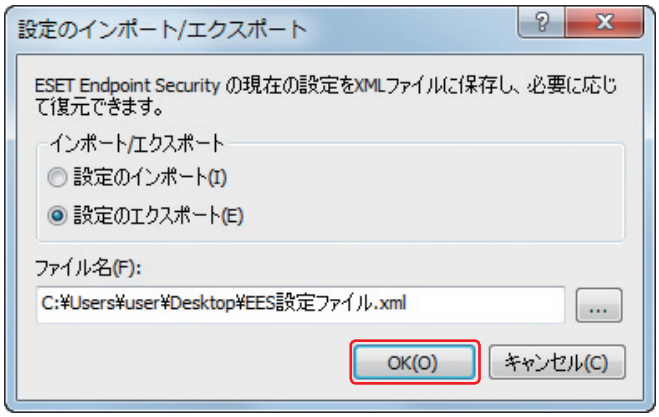
❶[設定のエクスポート]にチェックを入れ、❷[...]ボタンをクリックします。

4



❶保存先を選択し、❷[ファイル名] を入力します。❸[保存] ボタンをクリックします。

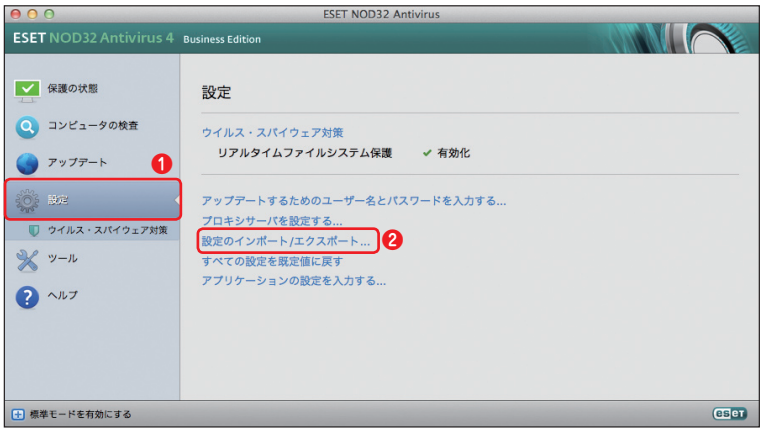
5



設定ファイルを保存します。[OK] ボタンをクリックします。

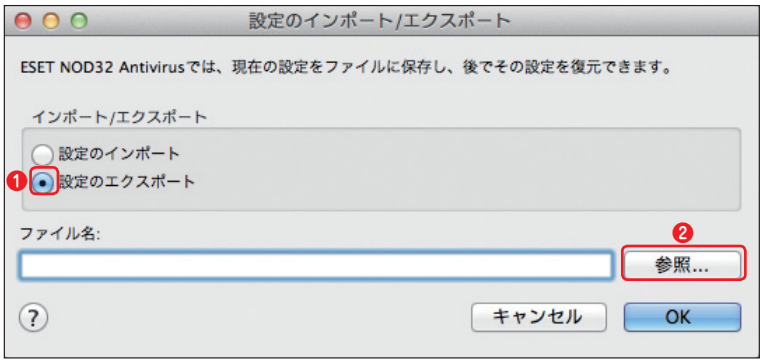
クライアント用プログラムの設定ファイル（.xml）の取得方法（Mac OS Xの場合）

1 メインウィンドウを開きます



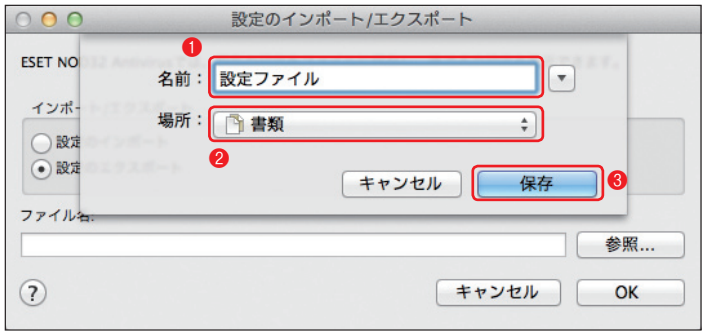
メインウィンドウを開き、詳細モードに切り替えてから、❶ [設定] ボタンをクリックして、❷ [設定のインポート/エクスポート] をクリックします。

2 設定ファイルの保存を開始します



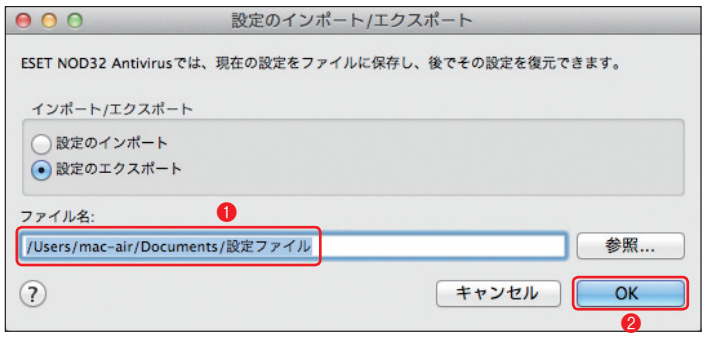
❶ [設定のエクスポート] をクリックし、❷ [参照] ボタンをクリックします。

3 保存先などを設定します



❶ファイル名を入力し、❷保存先を［場所］のプルダウンメニューから選択します。❸［保存］ボタンをクリックします。

4 設定ファイルを保存します

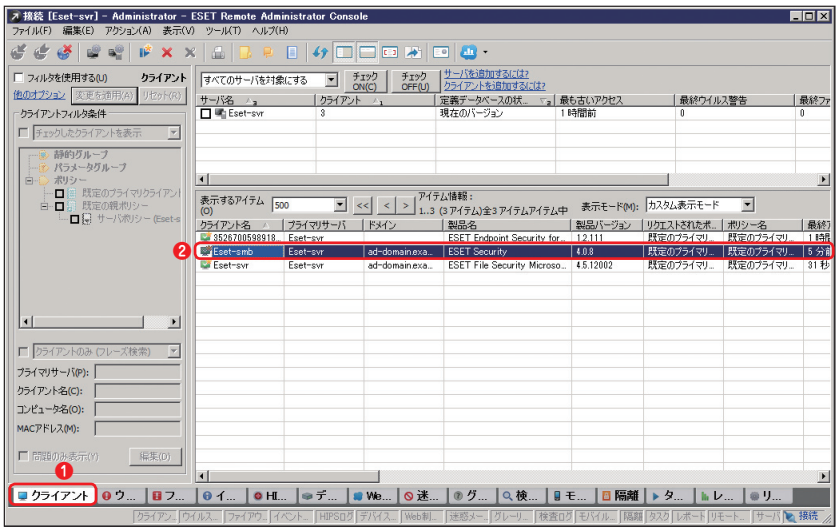


❶保存するファイルがフルパスで表示されます。❷［OK］ボタンをクリックすると、設定ファイルが保存されます。

クライアント用プログラムの設定ファイル（.xml）の取得方法（Linuxの場合）

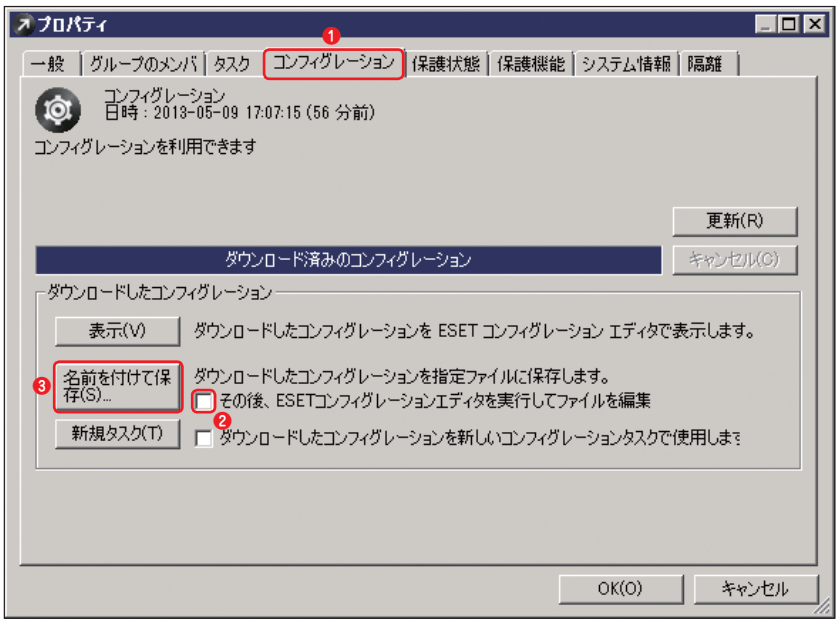
1 [スタート] ボタンから、[すべてのプログラム]（もしくはプログラム）、[ESET]、[ESET Remote Administrator Console] とクリックし、最後に [ESET Remote Administrator Console] をクリックします。

2



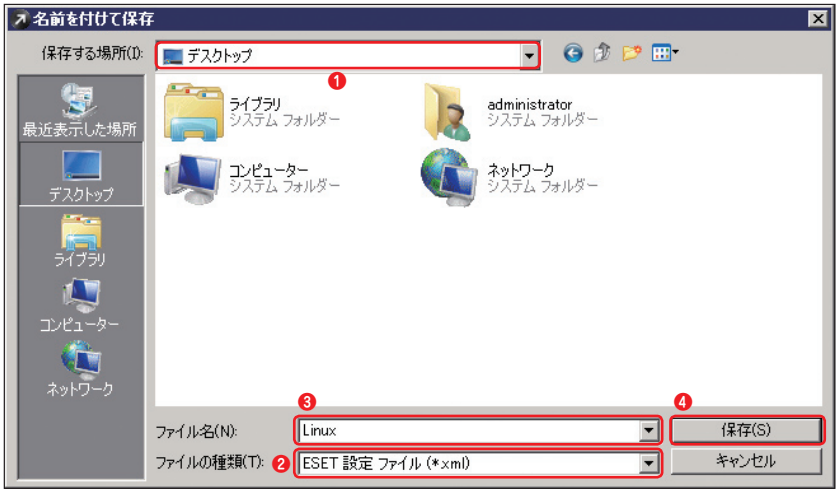
❶ [クライアント] ペインをクリックし、❷設定ファイルを取得したいコンピューターをダブルクリックします。

3



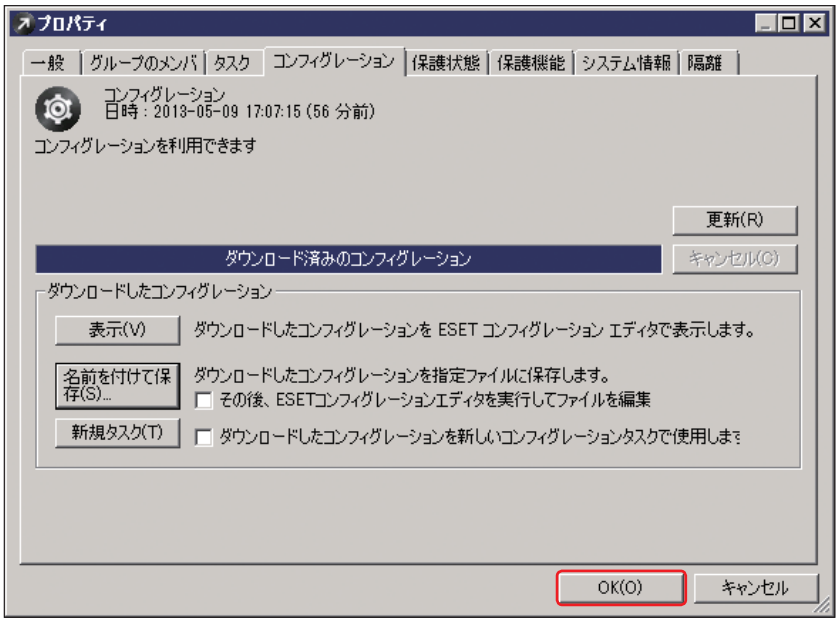
❶ [コンフィグレーション] をクリックし、❷ [その後、ESETコンフィグレーションエディタを実行してファイルを編集] のチェックを外します。❸ [名前を付けて保存] をクリックします。

4



❶保存先を選択し、❷[ファイルの種類] が [ESET 設定ファイル (*.xml)] であることを確認して、❸[ファイル名] を入力します。
❹[保存] をクリックします。

5

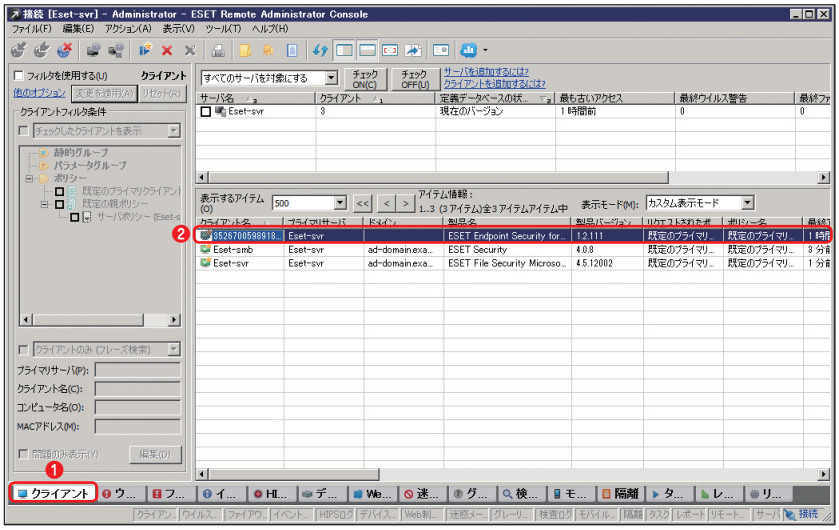


[OK] をクリックして、プロパティ画面を閉じます。

クライアント用プログラムの設定ファイル（.xml）の取得方法（Androidの場合）

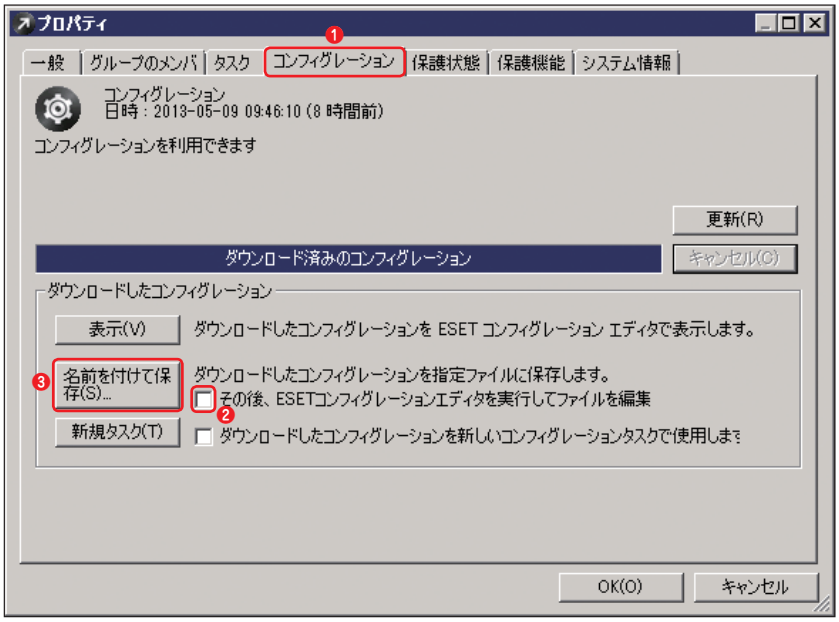
1 [スタート] ボタンから、[すべてのプログラム]（もしくはプログラム）、[ESET]、[ESET Remote Administrator Console] とクリックし、最後に [ESET Remote Administrator Console] をクリックします。

2



❶[クライアント] ペインをクリックし、❷設定ファイルを取得したいコンピューターをダブルクリックします。

3

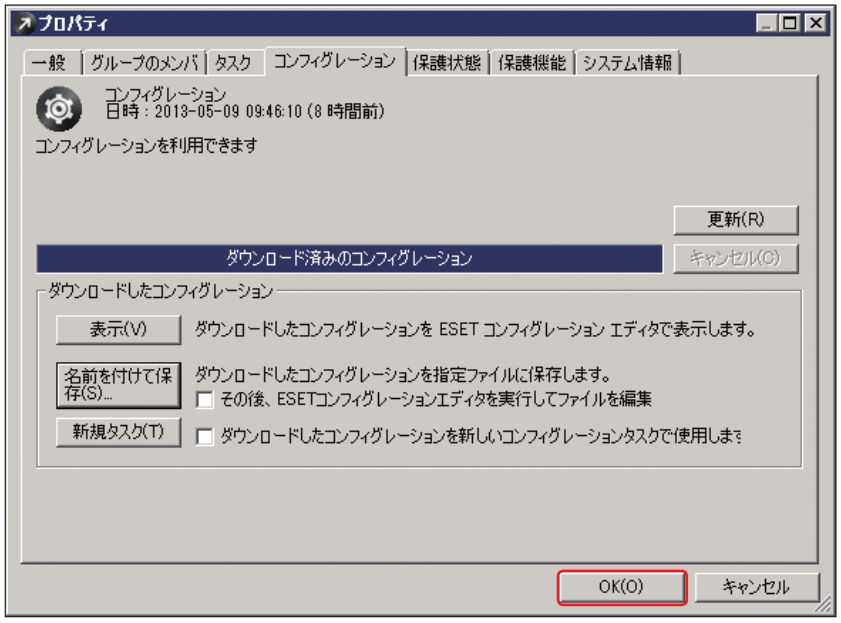


❶[コンフィグレーション] をクリックし、❷[その後、ESETコンフィグレーションエディタを実行してファイルを編集] のチェックを外します。❸[名前を付けて保存] をクリックします。

4

❶保存先を選択し、❷[ファイルの種類] が [ESET 設定ファイル (*.xml)] であることを確認して、❸[ファイル名] を入力します。
❹[保存] をクリックします。

5



[OK] をクリックして、プロパティ画面を閉じます。

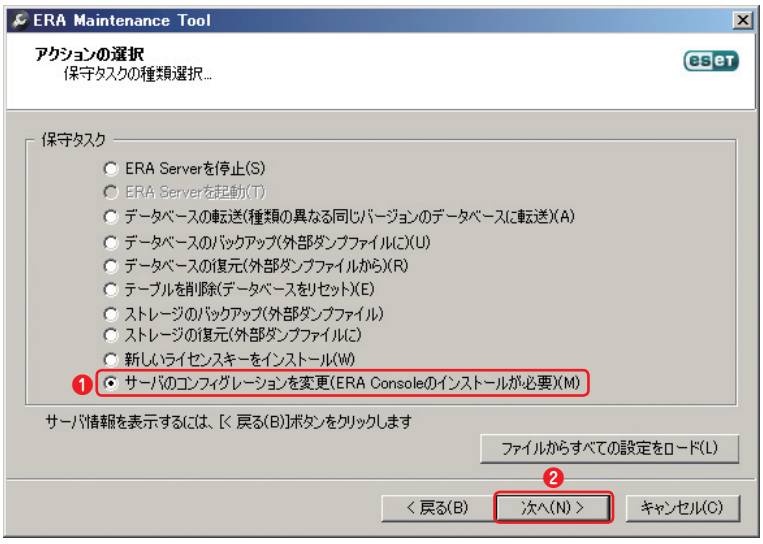
ERASの設定ファイルの取得方法

1 [スタート] ボタンから、[すべてのプログラム] (もしくはプログラム)、[ESET]、[ESET Remote Administrator Server]、[ESET Remote Administrator Maintenance Tool]とクリックします。

2 ERAメンテナンスツールが起動したら、[次へ] ボタンをクリックします。

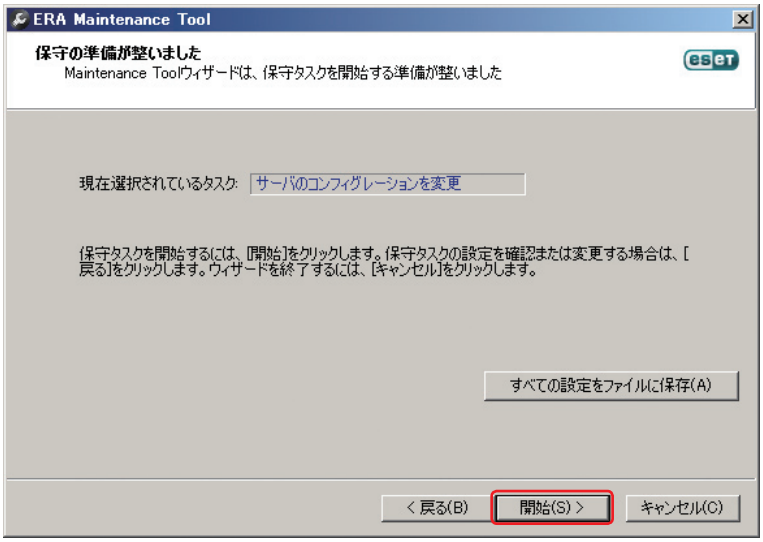
3 [サーバ情報] が表示されます。[次へ] ボタンをクリックします。

4



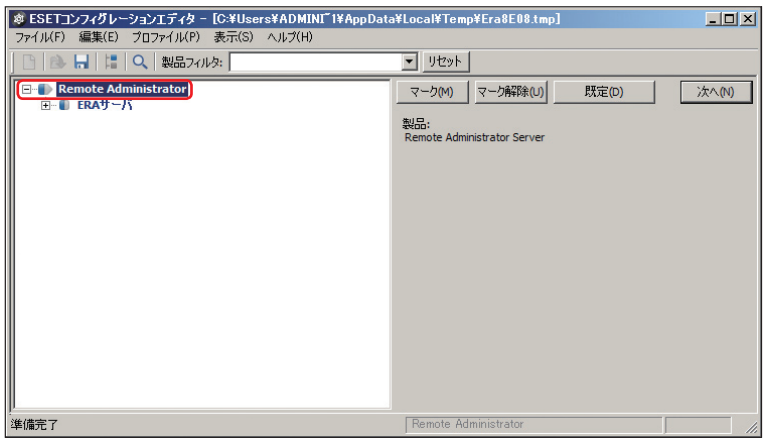
[アクションの選択] ダイアログが表示されます。❶[サーバのコンフィグレーションを変更] にチェックを入れ、❷[次へ] ボタンをクリックします。

5



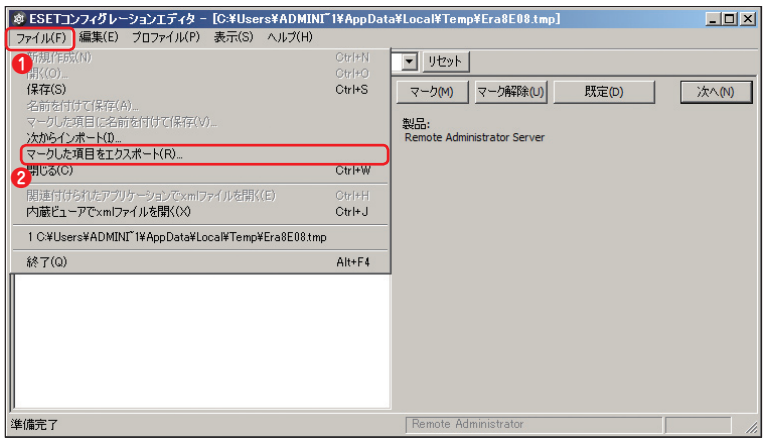
[開始] ボタンをクリックします。

6



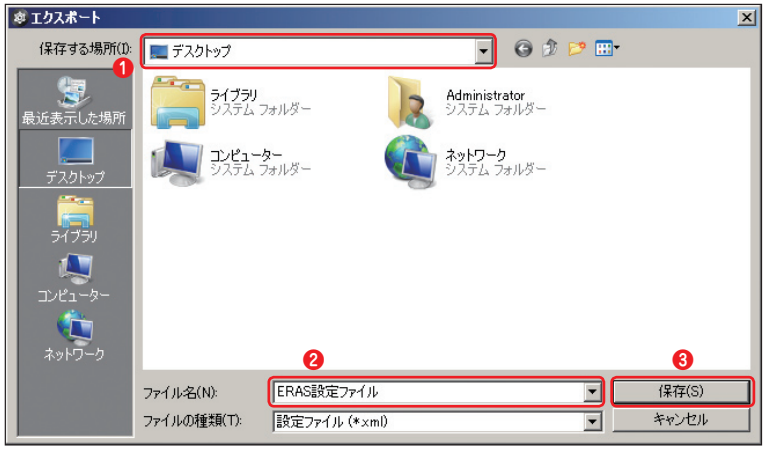
ESET コンフィグレーションエディターが起動します。
[Remote Administrator] をクリックします。

7



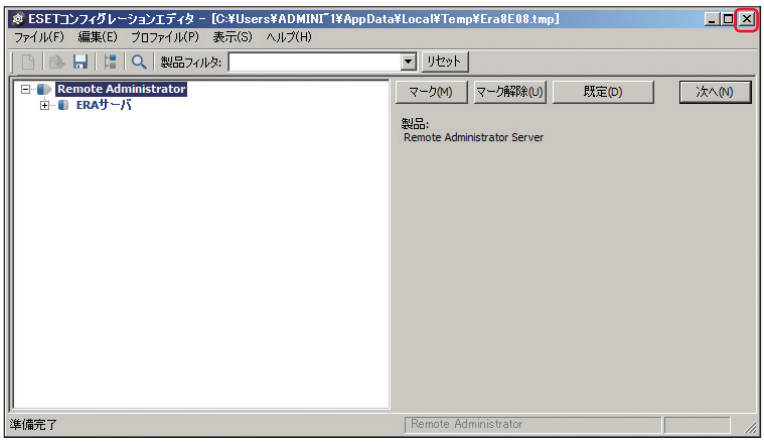
設定のエクスポートを行います。❶[ファイル] メニューをクリックし、❷[マークした項目をエクスポート] をクリックします。

8



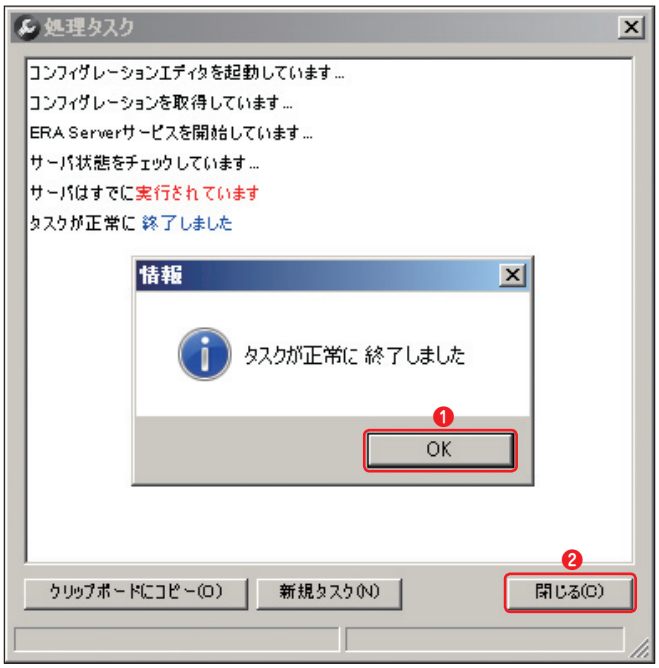
保存先とファイル名を入力します。❶保存先を選択し、❷[ファイル名] を入力します。❸[保存] ボタンをクリックします。

9



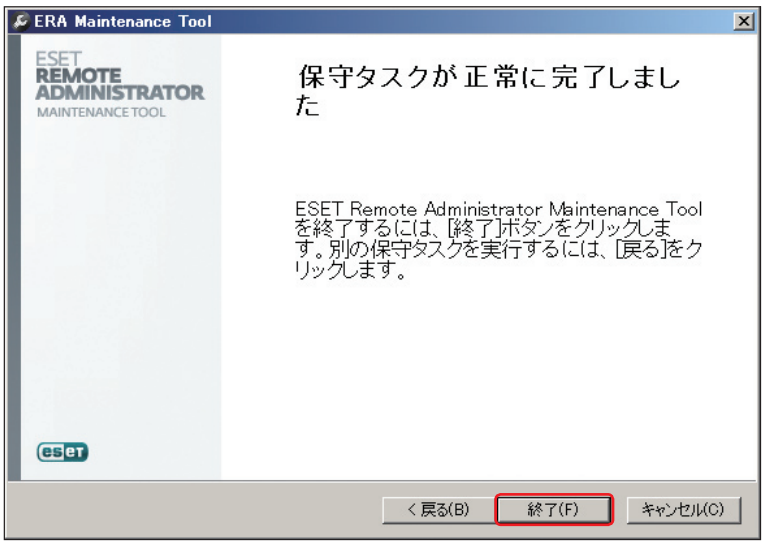
ESET コンフィグレーションエディターを終了します。[×] ボタンをクリックします。

10



ダイアログが表示されます。❶[OK]ボタンをクリックし、❷ [処理タスク] ダイアログの [閉じる] ボタンをクリックします。

11



ERAメンテナンスツールを終了します。[終了] ボタンをクリックします。

スクリーンショットの作成方法

Windowsの場合

弊社では、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。ここでは、Windows端末における一般的なスクリーンショットの作成方法を紹介します。

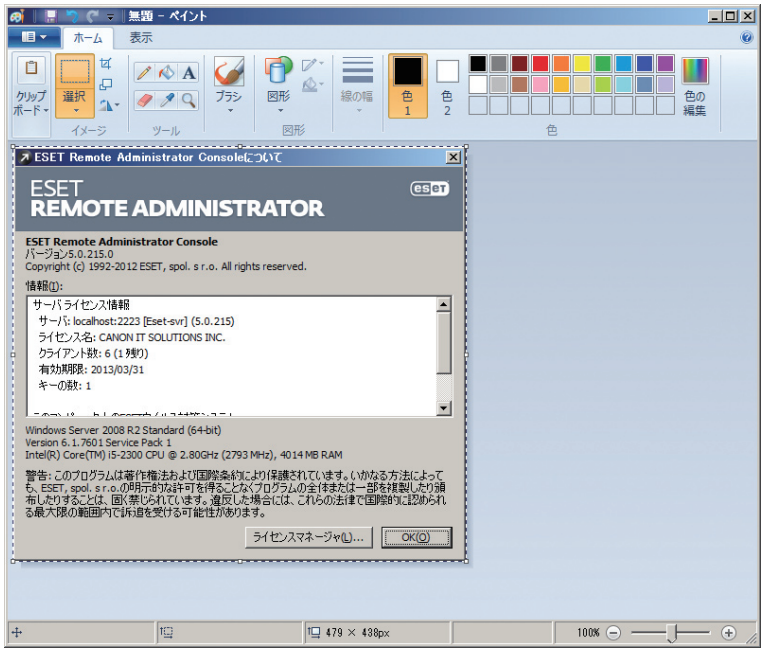
1 スクリーンショットを取ります

スクリーンショットを作成したい画面を表示します。フルスクリーンでスクリーンショットを作成したいときは[PrintScreen]キーを押します。アクティブウィンドウ(作業対象のウィンドウ)のスクリーンショットを作成したいときは、[Alt]キーを押しながら[PrintScreen]キーを押します。

2 [ペイント]を起動します

[スタート]ボタンから、[すべてのプログラム](もしくはプログラム)、[アクセサリ]とクリックし、最後に[ペイント]をクリックします。

3 [ペイント]にペーストします



[ペイント]に、[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。

4 スクリーンショットを保存します

[ファイル]メニュー、[名前を付けて保存]とクリックします。[名前を付けて保存]ダイアログが表示されたら、保存先を選択し、ファイル名を入力してJPEG形式で[保存]ボタンをクリックします。

Mac OS Xの場合

ご利用のMac端末のスクリーンショットの取得は、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。