ESET Remote Administrator
ユーザーズマニュアル

目次

Chapter 11
ESET SysRescue
P.211

■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。

■お断り

改訂日：9/30/2017

[Chapter 1]
はじめに

1.1 インストール概要

ESET Remote Administrator（ERA）は、ワークステーションやサーバーなどで構成したネットワーク接続環境にあるESET製品を集中管理するアプリケーションです。

ESET Remote Administrator自体は、セキュリティ対策機能を提供しません。クライアント環境のセキュリティ対策にはESET Endpoint アンチウイルスやESET Endpoint Securityなどをインストールしておく必要があります。

1.2 新しい機能

ESET Remote Administratorバージョン5.0

新機能

●管理者向けのダッシュボードーWebブラウザを利用したレポートの参照
●リモートインストールー新規設計
●保護機能ークライアント保護機能の一括管理
●スケジュールタスクの実行ークライアントのスケジュールタスクを素早くトリガするタスク
●ユーザマネージャーERAC利用者の管理
●HIPSタブークライアントからのHIPS関連の情報
●Webコントロールタブークライアントからのウェブ制御関連のイベントに関する情報
●デバイスコントロールタブークライアントからのデバイス制御関連のイベントに関する情報
●新しい検索タスクと設計
●ダッシュボードのためのレポートー新しいレポート、新しい設計、サポート
●移行するデータも含め、古いERAバージョン（4.x、3.x）に上書きでインストールできます。

1.3 プログラムのアーキテクチャー

ESET Remote Administratorは2つの独立したコンポーネントであるERA Server(ERAS)とERA Console(ERAC)で構成されています。ERA ServerとERA Consoleをネットワーク上で何台でも実行できます。ただし、インストールしたERAで管理できるクライアントの総数には制限があります。

ERA Server (ERAS)

ERAのサーバーコンポーネントは、Windows Server 2003、Windows Server 2008、およびWindows Server 2012でサービスとして実行できます。このサービスの主なタスクは、クライアントからの情報の収集とクライアントへのさまざまなリクエストの送信です。このようなリクエストにはコンフィグレーションタスクやリモートインストールリクエストなどがあり、ERA Console (ERAC) で生成されます。ERASは、ERACとクライアントコンピュータの接続ポイントです。すべての情報がここで処理、保守、または変更され、クライアントまたはERACに転送されます。

ERA Console (ERAC)

ERACはERAのクライアントコンポーネントで、通常はワークステーションにインストールされ、管理者は個々のクライアント上のESETソリューションをリモートで制御するために使用します。ERACは通常、次のディレクトリーにあります。

%ProgramFiles%¥ESET¥ESET Remote Administrator¥Console

ERACをインストールする際、ERASの名前の入力が必要になることがあります。起動時に、コンソールは自動的にそのサーバーに接続します。ERASの名前の入力は、インストール後に設定することもできます。

[Chapter 2]
ERA Server および ERA Console のインストール

2.1 要件

ERASはサービスとして機能するので、Microsoft Windows NTベースのオペレーティングシステムが必要です。ERASをインストールしたコンピュータは常時オンラインになっていて、コンピュータネットワークを介して以下からアクセスできるようになっている必要があります。

●クライアント（通常はワークステーション）
●ERA Consoleをインストールした PC
●他のERAS（複製した場合）

▸▸▸ NOTE

ESET Remote Administrator5は、データ移行など、以前のバージョンへの上書きインストールをサポートします。

2.1.1 パフォーマンス要件

サーバーのパフォーマンスは、次のパラメータによって変化します。

1.使用するデータベース

●既定では、MS Accessデータベースがサーバーと共にインストールされます。少数のクライアントを扱う場合は、このソリューションをお勧めします。ただし、データベースのサイズは2GBに制限されています。そのため、サーバーでクリーンアップを有効にし、[ツール] -> [サーバオプション] -> [サーバの保守] を選択して、古いデータを削除する間隔を定義する必要があります。

●他のデータベース（Microsoft SQL Server）を使用する場合は別途インストールが必要ですが、処理のパフォーマンスが向上します。技術的な推奨事項に従って、各データベースエンジンに適したハードウェアを使用することが重要です。

●通常は、外部データベース（例えば、別の物理マシンにインストールしたもの）を使用した方が、処理のパフォーマンスが高くなります。

2.クライアントの接続間隔の設定

●ESET Endpoint Security/ESET Endpoint アンチウイルス V5.0以降では、クライアントの接続間隔は既定で10分に設定されています。クライアントのステータスがデフォルトの間隔よりいくぶん頻繁にアップデートされる必要がある場合、この設定を変更することができます。クライアントの接続間隔を短くすると、サーバーのパフォーマンスに影響が生じます。

3.接続ごとにクライアントから報告されるイベントの平均数

●クライアントからサーバーに送信された情報は、特定のイベント（ウイルスログ、イベントログ、スキャンログ、設定の変更など）に分類されます。このパラメーターを直接変更することはできませんが、これに関連する他の設定を変更した場合、それに伴ってこの数が変わることがあります。例えば、詳細なサーバー設定では（[ツール] > [サーバオプション] > [サーバの保守]）、サーバーによって受け入れ可能なログの最大量を設定できます（この設定には、直接接続しているクライアントと複製されたクライアントが含まれます）。

4.ハードウェア要件

■小規模（ERA Serverに接続するクライアントが1,000未満）の場合：

●プロセッサータイプ-Pentium IV互換プロセッサー、2.0GHz以上
●RAM-2GByte
●ネットワーク-1Gbit

■中規模（ERA Serverに接続するクライアントが1,000～4,000）の場合：以下のように、インストールを2台のコンピュータに分割することをお勧めします。

ERA Server：
●プロセッサータイプ－Pentium IV互換プロセッサー、2.0GHz以上
●RAM－2GByte
●ネットワーク－1Gbit

データベースサーバー:
●プロセッサータイプ－Pentium IV互換プロセッサー、2.0GHz以上
●RAM－2GByte
●ネットワーク－1Gbit

または、以下のように1台のコンピュータにERA Serverとデータベースの両方をインストールすることができます。

●プロセッサータイプ－Pentium IV互換プロセッサー、マルチコア、3.0GHz以上
●RAM－4GByte
●ネットワーク－1Gbit
●HDD-Raid 0またはSSDハードドライブあるいは両方

NOTE

この場合（ERA Serverとデータベースの両方を1台のコンピュータにインストール）、MS Accessデータベースは、2GBのサイズ制限があるため定期的なデータベースのクリーンアップが必要になります。また、MS SQL Express 2005のデータベースのサイズ制限はわずか4GBであることにも留意してください。

■大規模（ERA Serverに接続するクライアントが4,000～10,000）の場合：以下のように、インストールを2台のコンピュータに分割して、MS SQL Serverを使用することをお勧めします。

ERA Server:
●プロセッサータイプ－Pentium IV互換プロセッサー、マルチコア、3.0GHz以上
●RAM－4GByte
●ネットワーク－1Gbit

データベースサーバー:
●プロセッサータイプ－Pentium IV互換プロセッサー、マルチコア、3.0GHz以上
●RAM－4GByte
●ネットワーク－1Gbit
●HDD-Raid 0またはSSDディスクあるいは両方

■非常に大規模（ERA Server上のクライアントが10,000～20,000）の場合以下のように、インストールを2台のコンピュータに分割して、MS SQL Serverを使用することをお勧めします。

ERA Server:
●プロセッサータイプ－Pentium IV互換プロセッサー、マルチコア、3.0GHz以上
●RAM－8GByte
●ネットワーク－1Gbit
●HDD-Raid 0またはSSDディスクあるいは両方

データベースサーバー:
●プロセッサータイプ－Pentium IV互換プロセッサー、マルチコア、3.0GHz以上
●RAM－4GByte
●ネットワーク－1Gbit
●HDD-Raid 0またはSSDディスクあるいは両方

NOTE

上記のハードウェア構成は、ERAを実行するための最小要件を表しています。パフォーマンスをさらに向上させるには、もっと優れた構成を使用することをお勧めします。扱うクライアントの数を考慮して、サーバーのオペレーティングシステムのハードウェアに関する最小推奨事項に従うことを強くお勧めします。使用されるデータベースのタイプおよびその制限について詳しくは、ERA Serverによってサポートされるデータベースを参照してください。

2.1.2 使用するポート

次の表は、ERASが使用するネットワーク通信の一覧です。プロセスEHttpSrv.exeはTCPポート2221上でリスンし、プロセスera.exeはTCPポート2222、2223、2224、および2846上でリスンします。その他の通信として、オペレーティングシステムのネイティブプロセス（"NetBIOS over TCP/IP"など）を使用します。
以下はERAが標準で利用するネットワークポートです。

プロトコル	ポート	説明
TCP	2221（ERAS がリスンするポート）	ERAS に統合されているミラー機能で使用する既定のポート（HTTP バージョン）
TCP	2222（ERAS がリスンするポート）	クライアントと ERAS との通信
TCP	2223（ERAS がリスンするポート）	ERAC と ERAS との通信

必要に応じて以下のネットワークポートを利用します。

プロトコル	ポート	説明
TCP	2224（ERAS がリスンするポート）	リモートインストールでの einstaller.exe エージェントと ERAS との通信
TCP	2225（ERAS がリスンするポート）	ESET ダッシュボード HTTP サーバーと ERAS 間の通信
TCP	2846（ERAS がリスンするポート）	ERAS の複製
TCP	139 (ERAS から見てターゲットとなるポート)	共有 admin$ を使用した、ERAS からクライアントへの einstaller.exe エージェントのコピー
UDP	137 (ERAS から見てターゲットとなるポート)	リモートインストール時の " 名前解決 "
UDP	138 (ERAS から見てターゲットとなるポート)	リモートインストール時の " 参照 "
TCP	445 (ERAS から見てターゲットとなるポート)	リモートインストール時の TCP/IP を使用した共有リソースへの直接アクセス (TCP ポート 139 の代わりに使用)

事前定義したポート2221、2222、2223、2224、2225、および、2846がすでに他のアプリケーションで使用されている場合は、別のポートに変更してもかまいません。

ERAで使用する既定のポートを変更するには、[ツール] > [サーバオプション] …をクリックします。ポート2221を変更する場合は、[アップデート] タブを選択してHTTPサーバーのポートの値を変更します。ポート2222、2223、2224、2225、および、2846を [その他の設定] タブの [ポート] セクションで変更できます。.

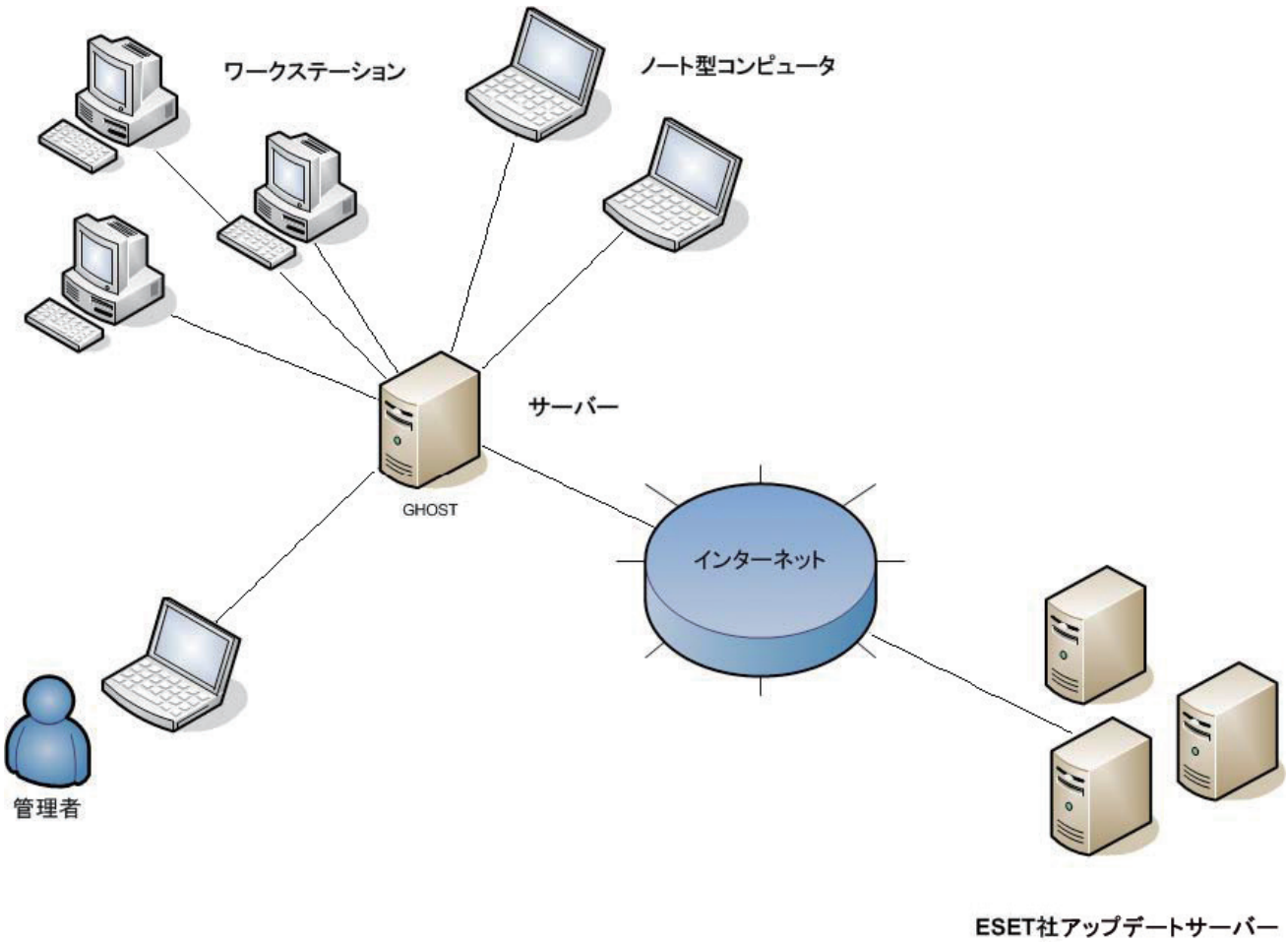
事前定義されたポート2222、2223、2224、および、2846は、詳細インストールモード（ERAS）で変更することもできます。

2.2 インストールの基本ガイド

企業のネットワークは通常、1つのローカルエリアネットワーク（LAN）で構成されます。ミラーサーバーは、ERASまたはESET Endpoint アンチウイルス Business Editionで作成できます。

2.2.1 環境の概要（ネットワーク構造）

すべてのクライアントがMicrosoft Windows 2000/XP/Vista/7を実行しているワークステーションおよびノートパソコンで、1つのドメインの中でネットワーク化されているとします。GHOSTというサーバーは常時稼働でオンラインになっており、Professional EditionまたはServer EditionのWindowsワークステーションです（Active Directoryサーバーでなくてもかまいません）。さらに、ネットワーク構造は次のようになります。



2.2.2 インストール前の手順

インストールの前に、弊社ユーザーズサイトからインストーラーをダウンロードします。

2.2.3 インストール

2.2.3.1 ERA Serverのインストール

GHOSTというサーバーにERASをインストールします（「環境の概要」で取り上げている例を参照してください）。最初に、インストールしたいコンポーネントを選択します。[ESET Remote Administratorサーバ] と [ESET HTTPダッシュボードサーバ] の2オプションがあります。

既定では、両方のコンポーネントがインストールされますが、異なるコンピュータに2つのコンポーネントを分けてインストールすることも選択できます（例えば、公開されているコンピュータにESET HTTPダッシュボードサーバーをインストールするのと同時に、ローカルなイントラネットからのみアクセス可能なコンピュータにERASをインストールできます）。または、ESET HTTPダッシュボードサーバーを使用しないことを選択することもできます。

NOTE

サーバーオペレーティングシステムを実行するマシンにERASをインストールすることをお勧めします。

NOTE

ダッシュボードサーバーとミラーサーバーの両方が、（自動的にインストールされる）同一のHTTPサーバーを使用します。インストール時にダッシュボードサーバーを選択解除しても、後で「ESETコンフィグレーションエディタ」で有効にすることができます（[ERAC] > [ツール] > [サーバオプション] > [詳細] > [ダッシュボード] > [ローカルダッシュボードの使用]）。

希望のコンポーネントを選択した後、[標準] または [詳細] インストールモードのいずれかを選択します。

- [標準] モードを選択すると、ライセンスで定義されている期間中ERASの動作を許可するライセンスキー（拡張子.licまたは.zipのファイル）を挿入するよう指示があります。次に、アップデートパラメーター（ユーザー名、パスワードおよびアップデートサーバー）を設定するよう指示があります。[後でアップデートパラメーターを設定する] の隣にあるチェックボックスを選択し、[次へ] をクリックすることによって、後でアップデートパラメーターを入力することもできます。

- [詳細] インストールモードを選択すると、追加のインストールパラメーターを設定することができます。これらのパラメーターは、後からERAC経由で変更できますが、多くの場合、変更は不要です。唯一の例外はサーバー名です。サーバー名は、DNS名と一致しているか、オペレーティングシステムの%COMPUTERNAME%値またはコンピュータに割り当てられているIPアドレスと一致している必要があります。これは、リモートインストールを実行する上で最も不可欠な情報です。インストール時に名前を指定しない場合、大部分のケースで十分なシステム変数%COMPUTERNAME%の値をインストーラーが自動的に提供します。ERAS情報が保存されるデータベースを選択することも重要です。詳細については、「ERA Serverでサポートされるデータベースの種類」を参照してください。

重要

Microsoft Windowsのセキュリティポリシーは、ローカルシステムアカウントの権限を制限します。この結果、関連するネットワーク操作を実行できないことがあります。ローカルシステムアカウントの下でERAサービスを実行すると、プッシュインストール時に問題が発生することがあります(例えば、ドメインからワークグループにリモートにインストールするときなど)。Windows Vista、Windows Server 2008、またはWindows 7を使用する場合、十分なネットのアクセス権限を付与したアカウントでERAサービスを実行することをお勧めします。ERAを実行するユーザーアカウントは[詳細]インストールモードで指定できます。

NOTE

ERA ServerではUnicodeが完全にサポートされていますが、サーバーが文字をANSIに変換する場合があります(電子メール、コンピュータ名など)。そのような状況では、[Unicode対応でないプログラムの言語]の設定を使用しなければなりません。ERAの日本語版を使用していない(つまり、英語版を使用している)場合でも、この設定をサーバー環境に合うように変更することをお勧めします。[コントロールパネル]>[地域と言語]の管理タブで、この設定を行えます。

既定では、ERASのプログラムコンポーネントは次のディレクトリーにインストールされます。

%ProgramFiles%¥ESET¥ESET Remote Administrator¥Server

ログ、インストールパッケージ、コンフィグレーションなど、その他のデータコンポーネントは、次のディレクトリーに保存されます。

%ALLUSERSPROFILE%¥Application Data ¥ESET¥ESET Remote Administrator¥Server

ERASはインストール後に自動的に起動します。ERASサービスのアクティビティは次の場所に記録されます。

%ALLUSERSPROFILE%¥Application Data¥ESET¥ESET Remote Administrator¥Server¥logs¥era.log

コマンドラインインストール
ERASは、次のコマンドラインパラメーターを使用してインストールできます。

/q-サイレントインストール。ユーザーがインストール操作に介入することはできません。ダイアログウィンドウは表示されません。

/qb-ユーザーが介入することはできませんが、インストールプロセスが進捗状況バーに表示されます。

例:era_server_nt3JPN.msi /qb

コマンドラインインストールのパラメーターおよびコンフィグレーションは、管理者の.xmlコンフィグレーションファイルである"cfg.xml"で補完することができます。このファイルは、ERA.のmsiインストールファイルと同じフォルダーに格納しておく必要があります。コンフィグレーションファイルはESET Configuration Editorで作成できます。このファイルでは、ERAのさまざまな設定が可能です。詳細については、ESET Configuration Editorのセクションを参照してください。

2.2.3.2 ERA Consoleのインストール

管理者のPC/ノートパソコンにESET Remote Administrator Consoleをインストールします。詳細インストールモードの最後に、ERA Serverが起動時に自動的に接続するERACの名前（またはIPアドレス）を入力します。ここで示す例では、GHOSTというラベルを付けます。

インストール後、ERACを起動して、ERASに接続されていることを確認します。既定では、ERA Serverに接続するためのパスワードは必須ではありません（パスワードのテキストフィールドが空白です）が、設定することを強くお勧めします。ERA Serverに接続するためのパスワードを作成するには、[ファイル] -> [パスワード変更] をクリックし、[変更] ボタンをクリックして [コンソールのパスワード] を変更します。

NOTE

管理者は、ESET Remote Administrator Consoleにアクセスして、ユーザーアカウントおよびパスワードを指定することができます。管理者はアクセスのレベルを指定することもできます。詳細については、ユーザマネージャーを参照してください。ユーザマネージャーで定義されたアカウントでERASにアクセスしたいコンピュータにERACをインストールする必要があります。

2.2.3.3 ミラー

ERASのミラー機能を有効にすることでLAN上に定義データベースのアップデートサーバーを構築することができます。ミラーを有効にすると、各クライアントのインターネット接続を使用した定義データベースのアップデート作業をミラーに移行することができ、インターネット接続のトラフィックを下げることができます。

次の手順を実行します。

1) [ファイル] -> [接続] をクリックして、ERA ConsoleをERA Serverに接続します。
2) ERA Consoleで、[ツール] -> [サーバオプション] をクリックして... [アップデート] タブをクリックします。
3) [アップデートサーバ] ドロップダウンメニューから [自動的に選択] を選択し、[アップデートの間隔] は60分のままにしておきます。[アップデート用ユーザ名] (EAV-***) を指定し、[パスワードの設定] をクリックして、ユーザー名とともに受け取ったパスワードを入力するか貼り付けます。
4) [アップデートミラーを作成] オプションを選択します。ミラーリングされたファイルへのパスおよびHTTPサーバーポート（2221）は既定のままにしておきます。[認証] は [なし] のままにしておきます。
5) [詳細] タブをクリックし、[詳細設定を編集] をクリックします。詳細な設定ツリーで、[ERA Server] -> [設定] -> [ミラー] -> [選択したプログラムコンポーネントのためにミラーを作成する] に移動します。右側で [編集] をクリックし、ダウンロードするプログラムコンポーネントを選択します。ネットワークで使用するすべての言語バージョンのコンポーネントを選択する必要があります。
6) [アップデート] タブで [今すぐアップデート] をクリックして、ミラーを作成します。

ミラーの設定オプションの詳細については、「ミラーの有効化および設定方法」を参照してください。

2.2.3.4 ERA Serverでサポートされるデータベースの種類

既定では、このプログラムではMicrosoft Access (Jetデータベースエンジン) 形式を使用します。ERAS 5.3では次のデータベースがサポートされます。

●Microsoft Access (既定)
●Microsoft SQL Server (2005以降のバージョン)

データベースの種類は、ERASの詳細インストールモードで選択できます。インストール後は、ERAから直接、データベースの種類を変更することはできません。変更するにはERA Maintenance Toolを使用します。

▸▸▸ NOTE

●SQL Server Express 2005では、データベースのサイズは4GBに制限されています。
●Microsoft Accessデータベースには2GBに制限されています。

基本要件

文字セット

文字セットにはUNICODEを使用することが重要です (UTF-8の使用をお勧めします)。特に、クライアントで固有のロケールを使用している場合や、ERA自体が日本語版で動作している場合に重要となります。複製を行う予定がなく、すべてのクライアントが同じサーバーに接続する場合は、インストールするERAのロケールの文字セットを使用できます。

MARS (複数のアクティブな結果セット)

MS SQLデータベースを使用する場合、円滑な操作のために、MARSをサポートするODBCドライバーが必要です。MARSをサポートするOBDCドライバーを使用しないと、サーバーの動作効率が低下し、次のエラーメッセージがサーバーログに記録されます。

Database connection problem.It is strongly recommended to use odbc driver that supports multiple active result sets (MARS).The server will continue to run but the database communication may be slower.See the documentation or contact ESET support for more information.

MS SQLデータベース以外で問題が発生した場合は、次のメッセージがサーバーログに記録され、サーバーが停止します。

Database connection problem.Updating the odbc driver may help.You can also contact ESET support for more information.

MARSをサポートしないドライバー:
-SQLSRV32.DLL (2000.85.1117.00)
-SQLSRV32.DLL (6.0.6001.18000) -Windows VistaおよびWindows Server 2008に付属しています。

MARSをサポートするネイティブドライバー:
-SQLNCLI.DLL (2005.90.1399.00)

データベース接続の設定

新しいデータベースを作成したら、次の2つの方法のどちらかでデータベースの接続パラメーターを指定する必要があります。

1.DSN（データソース名）を使用する方法

DSNを手動で開くには、ODBC

データソースアドミニストレーターを開きます。

（[スタート] -> [ファイル名を指定して実行] をクリックし、odbcad32.exeと入力します。）

DSN接続の例：

DSN=ERASqlServer

重要

ERAを正しく機能させるために、システムDSNを使用することを推奨します。

重要

64bitオペレーティングシステムでは、odbcad32.exeを%SystemRoot%¥SysWOW64¥フォルダから実行しなければなりません。

MS SQLでWindows/ドメイン認証を使用している環境にインストールするには、接続文字列の入力時にDSN形式を使用していることを確認してください。

2.直接的な方法（完全な接続文字列を使用）

必要なパラメータ（ドライバ、サーバー、およびデータベース名）をすべて指定する必要があります。

MS SQL Serverの完全な接続文字列の例は次のとおりです。

Driver={SQL Server}; Server=ホスト名 ;

Database=ESETRADB

Driver={SQL Server Native Client 10.0};

Server=ホスト名 ;

Trusted_Connection=yes;

Database=ESETRADB;

MARS_Connection=yes

[接続のテスト] をクリックしてデータベースサーバーへの接続を確認します。

▸▸▸ NOTE

Windows/ドメイン認証の代わりに、データベースサーバー認証を使用することをお勧めします。

2.2.3.5 以前のバージョンへの上書きインストール

ESET Remote Administrator 5は、データ移行など、以前のバージョンへの上書きインストールをサポートします。ERA 5.3の直接インストールがサポートされているのは、バージョン5.0と5.1のみです。

NOTE

再インストール処理中はERA Serverが停止し、すべての接続が中断されるため、クライアアントが接続していないときにのみ再インストールしてください。データベースの転送は、再インストールの前後で実行可能です(詳しくは、データベースの転送を参照してください)。

● [ERA Serverのインストール]:

1.インストールファイルをサーバーにダウンロードします。インストーラファイルをダブルクリックしてインストールを開始します。

2.標準または詳細インストールを選択します。ERA Serverのクリーンインストールと似ています。

● [標準インストール]:

ライセンスキーファイル(*.lic)、ユーザー名およびパスワードを求められます。以下のように2つの移行モードがあります。[コンフィグレーションモードのみのインポート] 新規データベース内に空のテーブルを作成します。[完全インポートモード] データベースからすべてのデータをインポートします。[現在のデータベースのバックアップ作成](デフォルト)を選択すると、データベースに変更が加えられる前にバックアップが作成されます。データベース保守のために [古いレコードに対するデフォルト自動クリーンアップの起動] オプションを選択することができます。

● [詳細インストール]:

ライセンスキーファイル(*.lic)、ERA Serverのサービスを実行するのに使用されるアカウント、通信に使用されるポート、ユーザー名およびパスワード、SMTPサービス設定(オプション)、ログ設定およびデータベース移行設定の入力を指示されます(上記の標準インストールで説明しています)。

NOTE

インストーラが現在のデータベース内の既存データを見つけた場合、プロンプトが表示されます。既存のテーブルの内容を上書きするには、[上書き] を選択します(警告:テーブルの内容が削除され、構造も上書きされます)。[無視] をクリックすると、テーブルはそのまま残ります。[無視] をクリックすると、テーブルが破損している場合や現在のバージョンと互換性がない場合などは、データベース不整合のエラーが発生する場合があります。

現在のデータベースを手動で解析したい場合は、[キャンセル] をクリックして、ERASのインストールを中止します。

● [ERA Consoleのインストール]:

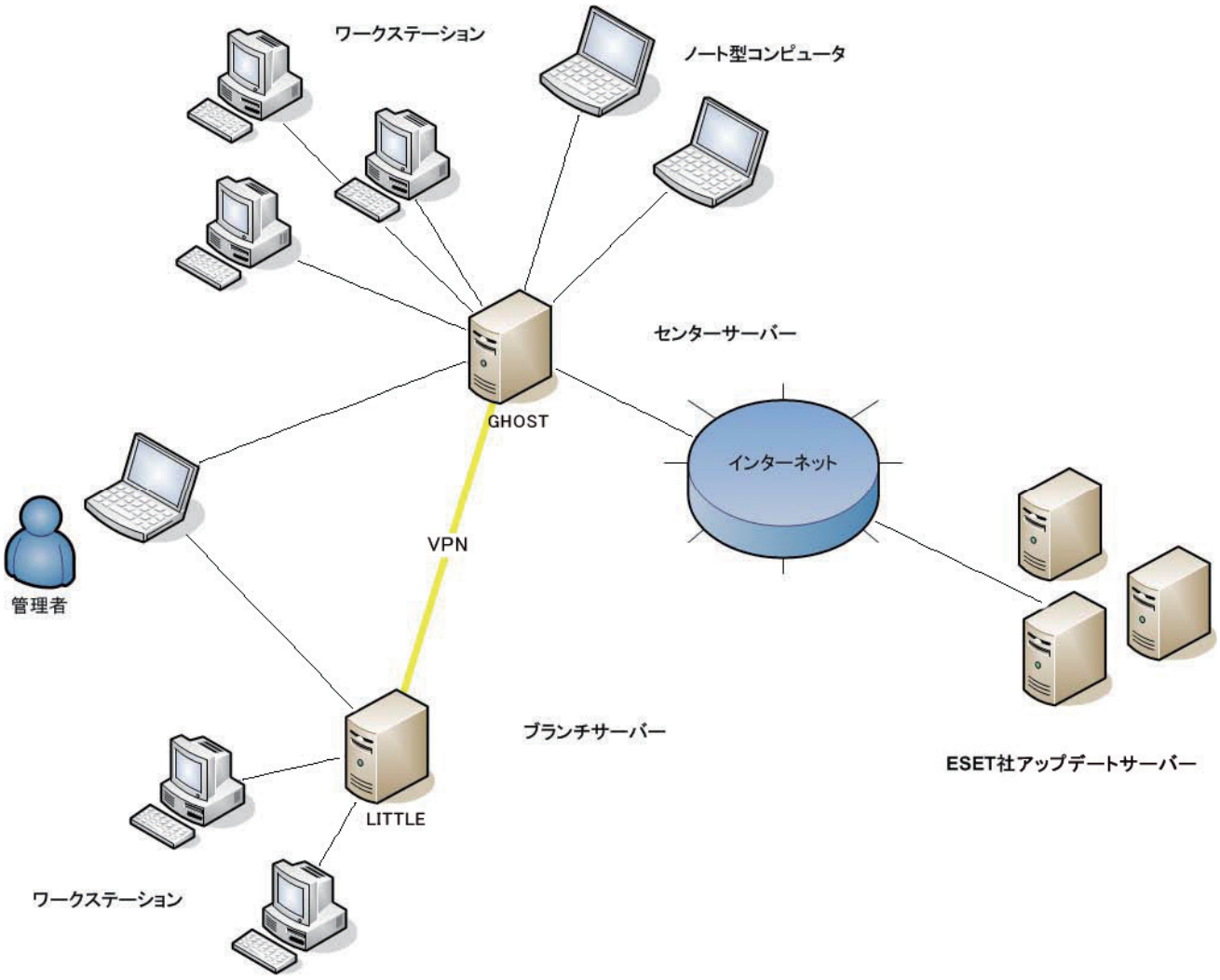
1.インストールファイルをサーバーにダウンロードします。インストールファイルをダブルクリックしてインストールを開始します。

2.ERA Consoleのインストールで説明しているとおりに手順を進めてください。

2.3 シナリオ-大規模ネットワーク環境でのインストール

2.3.1 環境の概要（ネットワーク構造）

次の図は、前のネットワーク構造に1つの支社、複数のクライアント、およびLITTLEという1つのサーバーが追加されたものです。本社と支社との間に低速のVPNチャネルがあるとします。このシナリオでは、サーバーLITTLEにミラーサーバーを構築することを推奨します。また、より使いやすい環境を構築し、転送するデータの量を最小限に抑えるために、LITTLEにもう1つのERA Serverを構築することを推奨します。

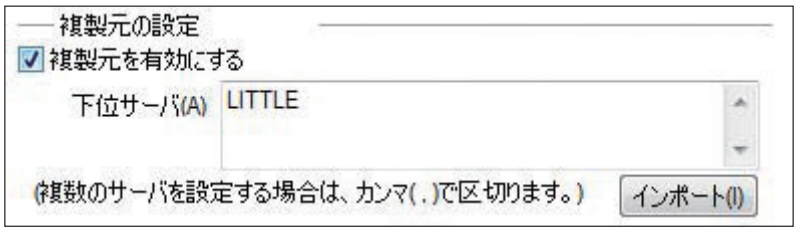


2.3.2 インストール

2.3.2.1 本社でのインストール

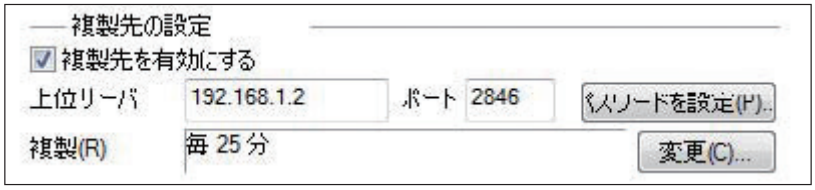
ERAS、ERAC、およびクライアントワークステーションのインストールは、前のシナリオとよく似ています。マスタERAS（GHOST）の設定のみが異なります。[ツール] -> [サーバオプション] -> [複製] で、[複製元を有効にする] チェックボックスをオンにし、[下位サーバ] にセカンダリサーバーの名前を入力します。ここでは、下位サーバーの名前はLITTLEです。

上位サーバーで複製のパスワードが設定されている場合は（[ツール] -> [サーバオプション] -> [保護] -> [複製のパスワード]）、下位サーバーからの認証にそのパスワードを使用する必要があります。



2.3.2.2 支社：ERA Serverのインストール

この直前の例と同様に、2番目のERASとERACをインストールします。ここでは、上位のERASを定義します。上位のERASのIPアドレス、つまりサーバーGHOSTのIPアドレスを使用することをお勧めします。



2.3.2.3 支社：HTTPミラーサーバーのインストール

ここでも、前のシナリオで取り上げたミラーサーバーのインストール設定を使用できます。ユーザー名とパスワードを定義する部分のみが異なります。

「環境の概要」の図のように、支社のアップデートは、ESETのアップデートサーバーからではなく、本社のサーバー（GHOST）からダウンロードします。アップデート元は次のURLアドレスで定義します。

http://ghost:2221（またはhttp://<ghostのIPアドレス>:2221）

既定ではミラーサーバーの認証は不要です。そのため、ユーザー名やパスワードを指定する必要はありません。

ERASでのミラーの設定の詳細については、「ミラーサーバー」を参照してください。

2.3.2.4 支社：クライアントへのリモートインストール

ここでも前のモデルを使用できますが、このインストールは、支社のERAS（この例ではLITTLE）に直接接続されているERACですべての操作を実行する場合に適しています。これによって、低速のVPNチャネルを介してインストールパッケージを転送する必要がなくなります。

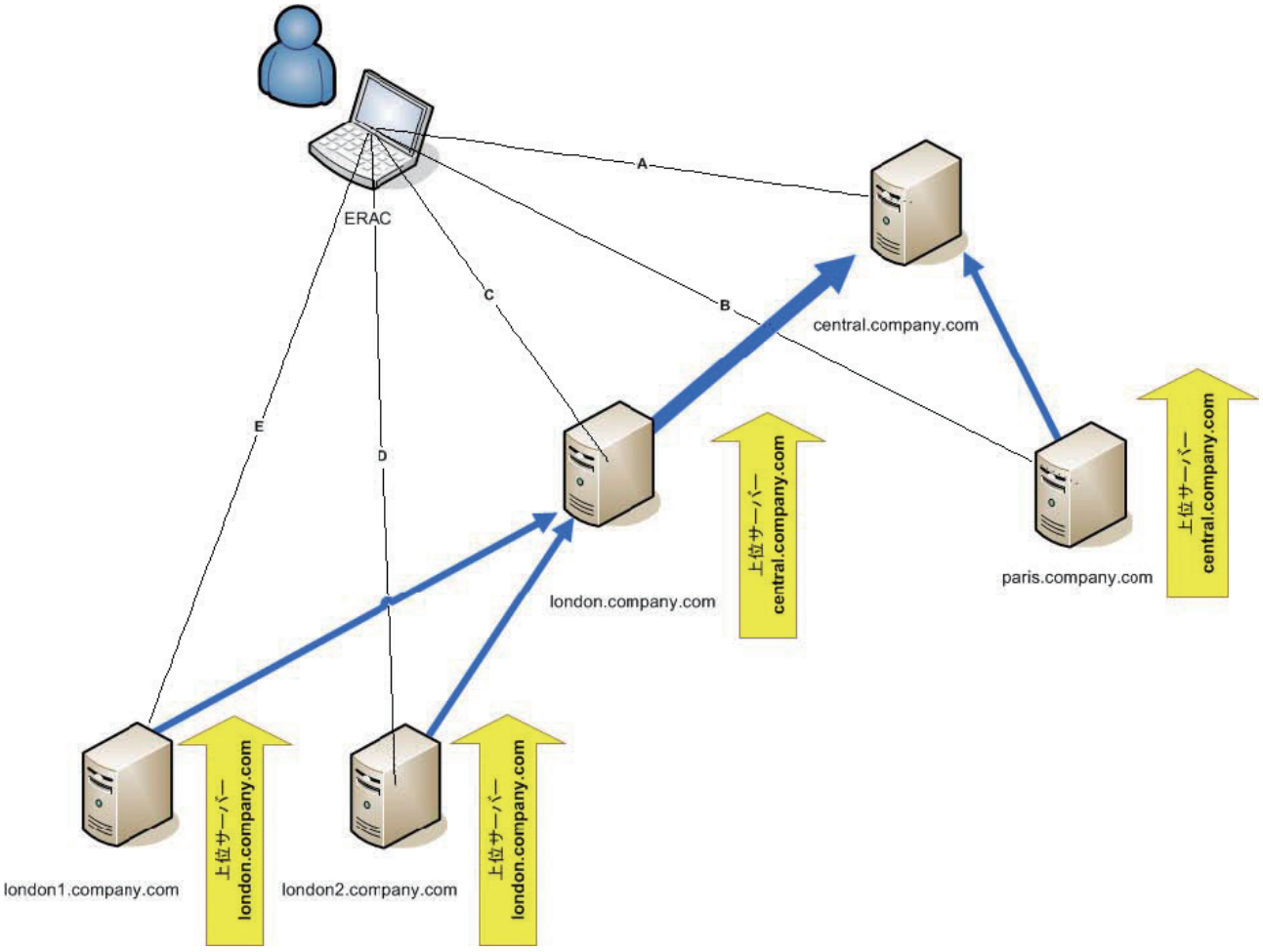
2.3.3 大規模ネットワーク環境に関するその他の要件

大規模ネットワークでは、複数のERA Serverをインストールすることで、アクセスに都合の良いサーバーからクライアントコンピュータのリモートインストールを実行できます。また、ERASには複製機能が用意されており、(「本社でのインストール」および「支社：ERA Serverのインストール」を参照してください) 複製機能を使用すると、下位のERASに接続するクライアント情報を親ERAS (上位サーバー) に転送できます。複製を設定するには、ERACを使用します。

複製機能は、複数の支社やリモートオフィスがある企業にとって非常に便利です。モデル展開シナリオは次のとおりです。各オフィスにERASをインストールし、それぞれに中央のERASとの複製機能を設定します。この設定は、低速であることが多いVPNを介して接続するプライベートネットワークで特に効果が得られます。管理者は、中央のERASに接続すればすべてのクライアントを管理できます。(下図のAで示された通信)。個々の部門へのアクセスにまでVPNを使用する必要がないため (通信B、C、D、およびE)、低速の通信チャネルを経由しなくて済むようになります。

管理者は、事前に設定した間隔で自動的に上位サーバーに転送する情報や、上位サーバーの管理者からリクエストがあったときに送信する情報を「複製」の設定で定義できます。複製によってERAがさらに使いやすくなると同時に、ネットワークトラフィックが最小限に抑えられます。

複製を利用することで管理範囲を分別するといった副次効果も得られます。コンソールでERAS london2.company.comにアクセスする管理者 (通信E) が制御できるのは、london2.company.comに接続しているクライアントのみです。central.company.comにアクセスする管理者 (A) は、本社と個々の部門や支社に存在するすべてのクライアントを制御できます。



[Chapter 3]
ERA Console の操作

3.1 ERA Serverへの接続

ERACの機能の大半は、ERASに接続しないと使用できません。接続前に、名前またはIPアドレスでサーバーを定義します。

ERACを開いて [ファイル] -> [接続の編集] (または [ツール] -> [コンソールオプション]) をクリックし、[接続] タブをクリックします。

[追加/削除] ボタンをクリックして、新しいERA Serverを追加するか、現在リストアップされているサーバーを変更します。[現在の接続状態] ドロップダウンメニューで目的のサーバーを選択します。次に、[接続] ボタンをクリックします。

NOTE

ERAC IPv6プロトコルへの完全サポートアドレスは [ipv6address]:portの形式で、例えば [::1]:2223

このウィンドウの他のオプションは次のとおりです。

- コンソールのスタートアップ時に選択したサーバーへ接続する-オプションが選択されている場合、コンソールの起動時には自動的にERASと接続します。
- コンソールのスタートアップ時に、接続に失敗した場合、メッセージを表示する通信エラーが発生した場合、警告が表示されます。

次の2種類の認証を使用できます。

ERA Server
ユーザーの認証にはERASの資格情報が使用されます。既定では、ERASに接続するためのパスワードは設定されておりませんが、設定することを強くお勧めします。ERASに接続するためのパスワードを設定するには、次の手順を実行します。

[ファイル] -> [パスワード変更] (または [ツール] -> [サーバオプション] -> [一般]) をクリックし、[コンソールのパスワード] の右側にある [変更] ボタンをクリックします。

パスワードの入力時には、[パスワードを記憶] チェックボックスをオンにすることができます。このオプションを使用する場合、セキュリティ上の危険があることに注意してください。記憶済みのパスワードをすべて削除するには、[ファイル] -> [パスワードのクリア] をクリックします。

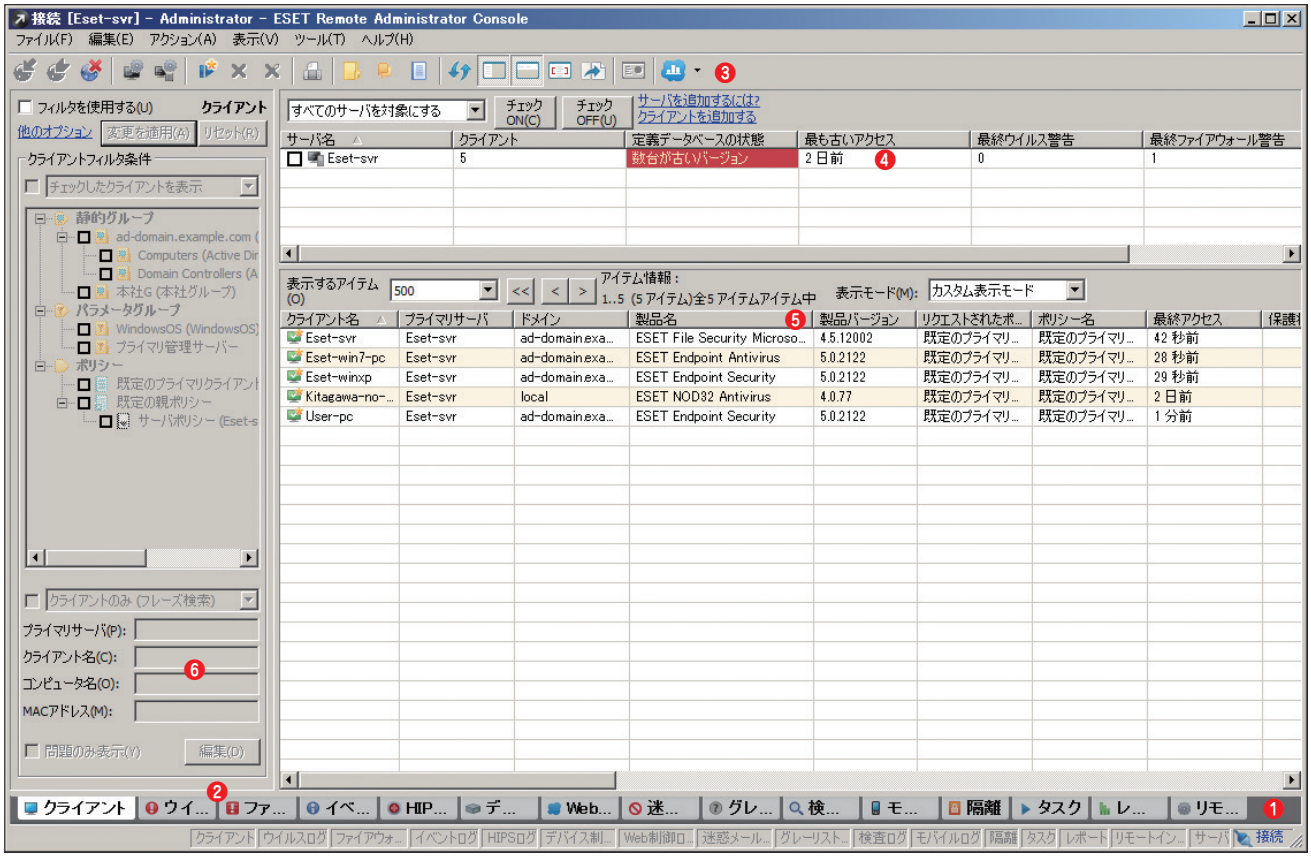
[アクセス権限] ドロップダウンメニューからアクセスタイプ ([Administrator] または [Read-Only]) を選択し、パス

ワードを入力して [OK] をクリックします。コンソールサーバー認証用のユーザーアカウントを設定または変更する場合は、ユーザマネージャツールを使ってください。

Windows/ドメイン
ユーザーの認証にはWindows/ドメインのユーザー資格情報が使用されます。Windows/ドメイン認証が適切に機能するためには、十分な権限が付与されたWindows/ドメインアカウントでERASをインストールしておく必要があります。また、[ツール] -> [サーバオプション] -> [詳細] タブ-> [詳細設定を編集] -> [ESET Remote Administrator] -> [ERA Server] -> [設定] -> [セキュリティ] を選択して、この認証機能を有効にする必要もあります。

[Windows/ドメイン認証を使用する] −Windows/ドメイン認証の有効と無効を切り替えます。
[Administratorグループ] −Windows/ドメイン認証を使用できるグループを定義できます。
[Read-Onlyグループ] −読み取り専用アクセス権の付与されたグループを定義できます。
通信が確立されると、プログラムのヘッダが [接続先: (サーバー名)] に変わります。
また、[ファイル] -> [接続] をクリックしてERASに接続することもできます。

3.2 ERA Console-メインウィンドウ



ステータスバー❶には、ERACとERASとの間の現在の通信の状態が表示されます❶。ERASから取得した必要なデータは、定期的に更新されます（既定では1分ごとの更新です。[ツール] > [コンソールオプション] > [その他の設定] > [自動更新を使用する（分）] を参照してください。更新の進捗状況もステータスバーに表示されます。

NOTE

表示されているデータを更新するには、F5キーを押します。

情報は、重要度順に複数のタブに分かれています❷。タブに表示されるほとんどの情報は、接続されているクライアントに関連するものです。ほとんどの場合、属性❺をクリックしてデータを昇順または降順でソートできます。また、ドラッグアンドドロップ操作でデータを並べ替えることもできます。複数のデータ行を処理する場合は、[表示するアイテム数] ドロップダウンメニューとページ移動ボタンを使用して、データ行を制限できます。目的に応じて属性を表示するには、[表示モード] を選択します（詳細については、「情報のフィルタリング」を参照してください）。タブから特定の情報を印刷する必要がある場合、詳細はページ設定を参照してください。

サーバーセクション❹は、ERA Serverを複製する場合に重要です。このセクションには、ERASが接続されているコンソールに関する概要情報のほか、子の階層、つまり"下位"のERA Serverに関する情報も表示されます。セクション❹にあるサーバーのドロップダウンメニューは、セクション❺に表示される情報の範囲に影響します。

すべてのサーバを対象にする	すべての ERA Server からの情報を表示します - セクション❺。
チェックのあるサーバのみを対象にする	選択された ERA Server からの情報を表示します - セクション❺。
チェックのあるサーバを除外する	選択された ERA Server からの情報を除外します。

セクション4のカラム:

サーバ名	サーバー名が表示されます。
クライアント	選択された ERAS のデータベースに接続またはその中にあるクライアントの総数。
定義データベースの状態	選択された ERAS のクライアント中のウィルス定義データベースの状態。
最も古いアクセス	サーバーへの最大未接続時間が表示されます。
最終ウイルス警告	ウイルス警告の総数（セクション❺の［前回のウイルス警告］を参照してください。
最終ファイアウォール警告	ファイアウォール警告の総数が表示されます。
最終イベント警告	現在のイベントの総数（セクション❺の属性最終イベントを参照)。

現在サーバーから切断されている場合は、サーバーセクション❹を右クリックし、[選択中のサーバに接続] を選択すると、選択したERASに接続できます。複製が有効な場合、サーバーセクション❹にはさらに多くの情報が表示されます。

ERACの重要な機能には、メインメニューまたはERACのツールバー❸からアクセスできます。

最後のセクションは [コンピュータのフィルタ設定] ❻です
ー情報のフィルタリングというタイトルの章を参照してください。

▸▸▸ NOTE

コンテキストメニューを使用して、クライアントおよびフィルタ情報を管理することを強くお勧めします。それがタスク実行、グループおよびポリシー管理ならびにデータのフィルタなどを行う最も迅速な方法です。

3.2.1 ［ページ設定］

［ページ設定］ウィンドウで、ERA Consoleの各種タブの内容を印刷するためのパラメータを設定します。

WYSIWYG	表示されているとおりにタブを印刷します。
印刷	グレースケールでタブを印刷します。白と黒のみの色が使用されます。
アイコンを印刷する	クライアント名の横に表示されているアイコンも印刷します。
ヘッダを印刷する	［ヘッダ］で定義されている文字列を左上隅に挿入します。既定のヘッダを使用するか、［ヘッダ］フィールドに独自のヘッダを書き込みます。
ロゴを印刷する	［ロゴのパス］で定義されている文字列を右上隅に挿入します。既定では、ESET のロゴが印刷されます。このオプションの横の［...］ボタンをクリックするか、ハードドライブからロゴを選択して独自のロゴをアップロードできます。
ページ数	印刷ページの最下部にページ番号を挿入します。
プレビュー	クリックすると、印刷ページのプレビューが表示されます。

3.3 情報のフィルタリング

ERACには、クライアントやイベントを簡単に管理できるさまざまなツールや機能が用意されています。表示される情報を管理しやすいように分類する必要がある場合は、高度なフィルタリングシステムの使用をおすすめします。特に、膨大な数のクライアントが存在するシステムでは効果的です。ERACに用意されているさまざまなツールを使用すると、接続されているクライアントに関する情報の効率的なソートやフィルタリングが可能です。

管理者は、フィルタを使用して、特定のサーバーまたはクライアントワークステーションに関連する情報のみを表示することができます。フィルタのオプションを表示するには、ERACのメニューで [表示] -> [フィルタペインの表示/非表示] をクリックします。

表示モード
[クライアント] タブでは、コンソールの右端にある [表示] ドロップダウンメニューを使用して、表示するカラムの数を調整できます。[全画面表示モード] ではすべてのカラムが表示され、[最小表示モード] では最も重要なカラムのみが表示されます。これらのモードは事前に定義されており、変更することはできません。表示をカスタマイズするには、[カスタム表示モード] を選択してください。[ツール] -> [コンソールオプション] …-> [カラム-表示/非表示] タブで設定できます。

3.3.1 フィルタ

フィルタリングを有効にするには、左上にあるフィルタの使用を選択してください。フィルタ条件を変更すると、表示されるデータが自動的に更新されます。ただし、[ツール] -> [コンソールオプション] -> [その他の設定] タブで、自動的な更新を設定していない場合は更新されません。

クライアントフィルタ条件でフィルタの条件を定義します。クライアントは、複数のグループおよびポリシーに属することができます。静的グループまたはパラメータグループにクライアントを割り当てることは、フィルタリングのためだけでなく、報告などのアクティビティにも大いに役立ちます。グループ管理の詳細については、グループマネージャ」を参照してください。グループ化はフィルタリングだけでなく、グループ毎にポリシーを割り当てる時にも有用です。ポリシーの作成と管理の詳細については、ポリシーをご参照してください。

最初のフィルタ条件はフィルタリング結果の表示条件です。使用可能なオプションは次の4つです。

チェックしたクライアントを表示	選択されたグループ / ポリシーやクライアントパネルで表示されます。
チェックしたクライアントを非表示	選択されていないクライアントとグループなしのクライアントはクライアントパネルで表示されます。一つのクライアントが複数のグループに属し、その中の一つのグループにチェックされていると、クライアントは表示されません。
チェックしたクライアントを非表示、重複メンバーを無視する	選択されていないグループ / ポリシー内のクライアント及びグループの所属なしのクライアントが表示されます。一つのクライアントが複数のグループに属し、その中の一つのグループがチェックされていても、クライアントは表示されます。
クライアントをどのグループにも表示しない	どのグループやポリシーにも属さないクライアントのみが表示されます。 **注意：**リストの上位にあるグループをチェックすると、そのサブグループもすべてチェックされます。

フィルタセクションの下部で、次のパラメータを別途指定できます。

クライアントのみ(フレーズ検査)	出力には、入力した文字列と名前が完全に一致するクライアントのみが得られます。
クライアントのみ(ワイルドカードを許可)	出力には、指定した文字列で名前が始まるクライアントのみが得られます。
クライアントを除外(フレーズ検査)	出力には、指定した文字列で名前を含むクライアントのみが得られます。
クライアントを除外(ワイルドカードを許可)	これらのオプションは前の３つと反対の結果を得ます。

プライマリサーバー、クライアント名、コンピュータ名及びMACアドレスの各フィールドでは、上述のドロップダウンメニューに定義された基準に基づいてそれぞれの文字列全体を受け取ります。これらのどのフィールドに入力した場合でもデータベースクエリが実行され、入力したフィールドに基づいて結果がフィルタリングされます。この場合の論理演算子はANDです。文字列全体、またはワイルドカード(?,*)のいずれかを使えます。

最後のオプションは問題に基づくフィルタリングであり、出力には、指定した種類の問題が発生したクライアントのみが得られます。問題の選択を表示するには問題のみ表示を選択し、編集…をクリックしてください。表示される問題を選択し、クライアントのリストのOKをクリックしてください。

フィルタリング構成に加えた変更はすべて、変更の適用をクリックした後で適用されます。既定の設定に戻すには、[リセット] をクリックします。フィルタの設定を変更する後で新しい出力を自動的に生成するには、ツール>コンソールオプション...>他の設定...変更を自動的に適用するを選択してください。

▸▸▸ NOTE

最後のセクションのフィルタ基準は現在実行中のタブによって変化します。基準はログを効果的にソートするためにカスタマイズされます。

また、表示したいアイテムに時間間隔を選択することによって、タブ内のデータを並べ替えることができます。

3.3.2 コンテキストメニュー

マウスの右ボタンを使用してコンテキストメニューを起動し、カラムへの出力内容を調整します。コンテキストメニューには次のようなオプションがあります。

すべて選択	すべてのエントリを選択します。
参照して選択	任意の属性を右クリックし、それと同じ属性を持つその他すべてのワークステーションまたはサーバーを自動的に選択（強調表示）することができます。... の文字列は、現在のタブの値に自動的に置き換えられます。
選択アイテムの反転	エントリの選択を反転します。
選択アイテムを非表示	エントリの選択を隠します。
選択アイテムのみ表示	リストに未選択されたエントリを隠します。 **注意：**オプションは現在実行中のウィンドウによって変化します。
カラムの表示/隠し	コンソールオプションを開きます＞カラム - 表示 / 非表示選択したペインで使用できるウィンドウを定義できます。

オプション [非表示アイテムを選択] と [選択アイテムのみ表示] は、前のフィルタ方法を使用後にさらに構成が必要な場合に有効です。コンテキストメニューで設定したフィルタをすべて無効にするには、[表示] -> [選択アイテムを隠す] をクリックするか、ERACのツールバーにあるアイコンをクリックします。F5キーを押して表示される情報を更新し、フィルタを無効にすることもできます。

例

●ウイルス警告の出ているクライアントのみ表示するには:

[クライアント] タブで、[最終ウイルス警告] という文字列が表示されている空のペインを右クリックし、コンテキストメニューの ['...'で選択] をクリックします。次に再度、コンテキストメニューの [非表示アイテムを選択] をクリックします。

●クライアント「Joseph」と「Charles」のウイルス警告を表示するには:

[ウイルスログ] タブをクリックし、[クライアント] カラムで値が「Joseph」である属性を右クリックします。コンテキストメニューの ['Joseph'で選択] をクリックします。次に、Ctrlキーを押しながら右クリックし、['Charles'で選択] をクリックします。最後に、右クリックしてコンテキストメニューの [選択アイテムのみ表示] をクリックし、Ctrlキーを放します。

Ctrlキーは複数エントリの選択と選択解除、Shiftキーは連続したエントリの選択と選択解除に使用できます。

▸▸▸ NOTE

特定の（強調表示した）クライアントのタスクを新規作成しやすくするために、フィルタリングを使用することもできます。効果的なフィルタリングの方法は数多く用意されているので、いろいろな組み合わせをお試しください。

3.3.3　日時フィルタ

[日時フィルタ]は、ERACの各タブに表示されます。[DATETIME間隔]を指定して、選択した期間のデータを簡単にソートできます。

過去X時間/日/週/月/年	指定期間を選択します。これは現在のタブにあるアイテムを制限し、この期間内のアイテムのみが表示されます。たとえば、[過去 10 日] を選択すると、過去 10 日間のすべてのアイテムが表示されます。
過去X	ドロップダウンメニューから、表示するアイテムとして事前定義されている期間を選択します。
次の日時以前/次の日時以降	[次の日時以前] または [次の日時以降] の横にあるチェックボックスを選択して日時を指定します。この日時以前またはこの日時以降のすべてのアイテムが表示されます。
期間指定	開始日時と終了日時を選択します。この期間のアイテムが表示されます。

▸▸▸ NOTE

タブに表示するデータとして期間を指定したすべてのログについて、[日時フィルタ]を使用することができます。関連性によってデータをソートするために、タブには詳細レベルを設定するオプションもあります(必要に応じて使用)。[日時フィルタ]は、[表示するアイテム]フィルタをかけたデータを表示します。これらのフィルタは独立ではありません。つまり、[日時フィルタ]はフィルタ済みのデータのみにフィルタを適用します。

3.4 ERA Consoleのタブ

3.4.1 タブとクライアントについての一般的な説明

タブに表示されるほとんどの情報は、接続されているクライアントに関連するものです。ERASに接続されている各クライアントは、次の属性で識別されます。

コンピュータ名（クライアント名/ホスト名）＋MACアドレス＋プライマリサーバー

特定のネットワーク操作（コンピュータ名の変更など）に関連するERASの動作は、ERASの詳細な設定で定義します。これによって、[クライアント] タブでエントリの重複を避けることができます。たとえば、ネットワーク内のいずれかのコンピュータの名前を変更しても、MACアドレスを変更しなければ、[クライアント] タブで新しいエントリが作成されることはありません。

初めてERASに接続するクライアントについては、[新規クライアント] カラムに [はい] という値が表示されます。また、クライアントのアイコンの右上隅に小さい星のシンボルが表示されます。管理者はこの機能を使用して、新しく接続されたコンピュータを簡単に検出できます。この属性は、管理者の操作手順に応じて意味が異なる場合があります。

クライアントを設定し、特定のグループに移動した場合は、そのクライアントを右クリックし、[フラグをセット/リセット] -> ["新規"フラグのリセット] を選択して、"新規"ステータスを無効にすることができます。クライアントのアイコンが次の図のようなものに変わり、[新規クライアント] カラムの値が [いいえ] に切り替わります。

NOTE

コメント属性は、3つのタブすべてで必要に応じて入力できます。管理者は、ここに説明（"オフィス番号129"など）を挿入できます。

ERASでは、時間の値を相対モード（"2日前"）、絶対モード（20.5.2009）、またはシステムモード（地域の設定）で表示できます。

ほとんどの場合、属性をクリックしてデータを昇順または降順で並べ替えられます。また、ドラッグアンドドロップ操作でデータを並べ替えることもできます。

[表示するアイテム]オプションを使用して、タブに表示したいデータを並べ替えます。表示するログ数を設定して（デフォルト値はすべてのログで200です）、ログが表示される期間（デフォルトでは最近の7日間）を入力します。大規模なネットワークでは、表示する期間を制限することをお勧めします。表示する期間を長めに設定すると、データベースに非常に大きな負荷が掛り、パフォーマンスが低下する可能性があります。

▸▸▸ NOTE

すべてのログで [日時フィルタ] を使用して、タブにデータが表示される期間を指定することができます。関連性によってデータをソートするために、(該当する場合) タブでの詳細レベルを設定するオプションもあります。[データフィルタ] は、[表示するアイテム] フィルタを通してフィルタされたデータを表示します。-これらのファイルには依存性があります。

特定の値をダブルクリックすると、他のタブが有効になり、さらに詳しい情報が表示されます。たとえば、[前回のウイルス警告] カラムの値をダブルクリックすると、[ウイルスログ] タブに移動し、指定したクライアントに関連するウイルスログエントリが表示されます。ダブルクリックした値に関連する情報が多すぎてタブビューに表示しきれない場合は、該当するクライアントに関する詳細情報を表示するダイアログウィンドウが開きます。

3.4.2 複製および個々のタブに表示される情報

上位サーバーとして機能するERASにERACが接続されていれば、下位サーバーのクライアントが自動的に表示されます。複製する情報の種類は、下位サーバーの[ツール]->[サーバオプション]->[複製]->[複製先の設定]で設定できます。

このシナリオでは、次の情報が表示されない場合があります。

●詳細な警告ログ([ウイルスログ]タブ)
●詳細なオンデマンドスキャナログ([スキャンログ]タブ)
●現在のクライアントに関する.xml形式の詳細設定([クライアント]タブ、[コンフィグレーション]カラム、[保護状態]、[保護機能]、[システム情報])

ESET SysInspectorプログラムで収集された情報も表示されない場合があります。ESET SysInspectorは、4.x以降のESET製品と統合されています。

プログラムのダイアログウィンドウに情報が見つからない場合は、[リクエスト]ボタン([アクション]->[プロパティ]->[コンフィグレーション]にあります)をクリックします。このボタンをクリックすると、表示されていない情報が下位のERASからダウンロードされます。複製は必ず下位のERASによって開始されるので、表示されていない情報は、事前に設定された複製の時間間隔で配信されます。

上位サーバーでは、サーバーが受け取るログのレベルを設定できます([ツール]->[サーバオプション]->[詳細]->[詳細設定を編集]->[ESET Remote Administrator]->[ERA Server]->[設定]->[サーバの保守]->[受け取るログの種類])。

NOTE

このオプションは、複製したクライアントだけではなく、サーバーに接続されているすべてのクライアントに適用されます。

3.4.3 [クライアント]タブ

このタブには、個々のクライアントについての一般的な情報が表示されます。

属性	説明
クライアント	クライアントの名前（クライアントの［プロパティ］ダイアログの［一般］タブで変更できます）
コンピュータ名	ワークステーション / サーバーの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERAS の名前
ドメイン	クライアントの所属先のドメイン / グループ（ERAS で作成されたものではない）の名前
IP	IPv4 または IPv6 アドレス
製品名	ESET セキュリティ製品の名前
製品バージョン	ESET セキュリティ製品のバージョン番号
リクエストされたポリシー名	リクエストされたポリシー名
ポリシー名	クライアントに割り当てられているポリシーの名前
最終アクセス	クライアントが ERAS に前回接続した時刻（複製で得られたデータを除き、クライアントから収集したすべてのデータはこのタイムスタンプを持っています）
保護状態の説明	クライアントにインストールされている ESET セキュリティ製品の現在の状態
ウイルス定義データベース	ウイルス定義データベースのバージョン
最終ウイルス警告	前回のウイルス発生事件
最終ウイルス警告の日付	前回ウイルス警告が発生したときの日時
最終ファイアウォール警告	ESET Endpoint Security パーソナルファイアウォールで前回検出されたイベント（警告レベル以上のイベントが表示されます）
最終イベント警告	前回のエラーメッセージ
最終ファイル検査	前回のオンデマンド検査で検査されたファイルの数
最終感染ファイル	前回のオンデマンド検査で感染が確認されたファイルの数
最終駆除ファイル	前回のオンデマンド検査で駆除（または削除）されたファイルの数
最終検査日時	前回のオンデマンド検査の日時
ロールバック	ロールバックを行なっているかどうかを表示します
ロールバックアクティブ期限	ロールバックの有効期限
再起動要求	再起動が必要かどうか（プログラムのアップグレード後など）
再起動要求日	最初の再起動が要求された日時
最後に開始した製品	クライアントプログラムを前回起動した日時
製品のインストール日	ESET セキュリティ製品をクライアントにインストールした日付
ローミングユーザ	この属性を持つクライアントは、ERAS に接続するたびに、" 今すぐ更新 " を実行します（ノートパソコンに推奨）。このアップデートは、クライアントのウイルス定義データベースが最新でない場合にのみ実行されます。
新規クライアント	新しく接続したコンピュータ（タブとクライアントの一般情報を参照してください）
OS 名	クライアントのオペレーティングシステムの名前
OS プラットフォーム	オペレーティングシステムのプラットフォーム（Windows/Mac など）
ハードウェアプラットフォーム	32bit かそれとも 64bit かを表示します
コンフィグレーション	クライアントの現在の .xml コンフィグレーション（コンフィグレーションが作成された日時を含む）
保護の状態	一般的な状態の説明（[コンフィグレーション］属性に類似）
保護機能	プログラムコンポーネントの一般的な状態の説明（[コンフィグレーション］属性に類似）
システム情報	クライアントが ERAS に送信したシステム情報（システム情報が送信された時刻を含む）
SysInspector	ESET SysInspector ツールを含むバージョンを持つクライアントは、この補足アプリケーションからログを送信できます。
カスタム情報 1, 2, 3	管理者の指定によって表示されるカスタム情報（このオプションを設定するには、ERAC で［ツール］-＞［サーバオプション］-＞［詳細］タブ -＞［詳細設定を編集］-＞［ESET Remote Administrator］-＞［ERA Server］-＞［設定］-＞［その他の設定］-＞［クライアントのカスタム情報］を選択します）。
コメント	クライアントを説明する短いコメント（管理者が入力）

▸▸▸ NOTE

値の中には、情報提供のみを目的とするものもありますが、管理者がコンソールで確認した時点では最新の内容ではない可能性もあります。例えば、午前7時に発生した更新エラーに関する情報は必ずしも午前8時に更新が完了していなかったというわけではありません。最後のウイルスの警告と最後のイベントの警告はこのような値に入りません。この情報が古いことを管理者が知っている場合は、その値を右クリックし、[情報を削除]-＞["前回のウイルス警告"情報の削除] または ["最終イベント警告"情報を削除] をクリックすると削除できます。前回のウイルス発生事件または前回のシステムイベントについての情報が削除されます。

クライアントタブにおいて、ダブルクリックされたクライアントは追加オプションを表示します。

一般	クライアントタブに表示される類似情報を含みます。これを利用して「クライアント名」変更することができます。この名前でクライアントが ERA に表示でき、さらに、オプションのコメントを追加します。
グループのメンバー	このタブはクライアントが属しているグループを記載しています。詳細については、「情報のフィルタリング」を参照してください。
タスク	指定したクライアントに関係するタスクを表示します。詳細については、「タスク」を参照してください。
コンフィグレーション	現在のクライアントの構成を閲覧したり、xml ファイルへのエクスポートを可能にします。このマニュアルの後半で、.xml ファイルを使用して、新規または変更された .xml 形式のコンフィグレーションファイル用の設定テンプレートを作成する方法を説明します。詳細については、「タスク」を参照してください。
保護状態	これはすべての ESET プログラムに関する概況一覧です。説明の中には対話的なものもあり、それらに対してはその場で対話操作が可能です。この機能は、特定の保護問題を解決するために新しいタスクを手動で定義する必要がないという点で便利です。
保護機能	ESET のすべてのセキュリティ機能（スパム対策、パーソナルファイアウォールなど）のコンポーネントの状態
システム情報	インストールされたプログラムに関する詳細情報、プログラムコンポーネントのバージョンなど。
SysInspector	起動プロセスおよびバックグラウンドで実行されているプロセスに関する詳細情報。
隔離	隔離されたファイルのリストを含みます。隔離されているファイルは、クライアントから要求してローカルディスクに保存できます。

3.4.3.1 重複したクライアントの統合

重複したクライアントの統合は、MACアドレスが異なる同じ名称のコンピュータを1つに統合する機能です。たとえば、ERA Serverによって管理しているコンピュータのネットワークアダプターを変更するとMACアドレスが変更されるため、ERA Consoleの[クライアント]タブに同じ名称のコンピュータが2台表示されます。この場合、ERA Consoleの[クライアント]タブから古いコンピュータを削除できるほか、コンピュータ名が重複したクライアントを1つに統合できます。

2台のコンピュータを統合するには、ERA Consoleの[クライアント]タブに移動し、2台のコンピュータを選択して、右クリックし、コンテキストメニューで[重複クライアントのマージ]をクリックします。[重複クライアントのマージ]ウィンドウが表示されるので、保持したいクライアントを選択し、[クライアントのマージ]ボタンをクリックします。保持するクライアントを間違って選択してしまった場合(長期間ERA Serverに接続していなかったクライアントなど)、選択が間違っていることを示す警告が表示されることがあります。

CAUTION

2台のコンピュータを統合すると、ログは保持されるコンピュータと関連付けられますが、コンピュータを削除すると、タスク、検査、グループ/ポリシーの割り当ては削除されます。

3.4.3.2 ネットワークアクション

ERA Serverで管理されるクライアントごとにネットワークアクションを実行できます。クライアントに対して実行できるネットワークアクションには、[Ping]、[Wake On LAN]、[共有]、[シャットダウン/再起動]、[メッセージ]、[RDP]、または [カスタム...]があります。

ネットワークアクションを実行するときは、ERA Consoleの[クライアント]タブでアクションを実行したいクライアントを右クリックし、[ネットワークアクション]を選択して、実行したいアクションをクリックします。

実行するすべてのネットワークアクション(Pingを除く)は、ダイアログウィンドウの進行状況バーによってアクションの状態を通知します。以下の表に、使用可能なネットワークアクション、(ERA Serverで別の手段で実装されていない限り)これらが実行する Windowsの汎用コマンド、および一部の前提条件のリストを示します。ネットワークアクションは、ここで提示する前提条件をすべて満たさなくても実行できる場合や、これら以外の前提条件を満たさないと実行できない場合があります。このリストは、「動作しない場合に試してみるのに役立つ情報」として扱ってください。

コマンドは、ERAコンソールが実行中のコンピュータで実行されます。このため、コンソールコンピュータでcmd.exeを使用してコマンドを実行すると、まったく同じ動作となり、何が間違っているかを判断するために使用できます。ERA Consoleでの [ツール] > [コンソールオプション] > [その他の設定]で設定する「ネットワークアクションを実行時にIPアドレスの代わりにホスト名を使用する」に基づき、<computer>は対象のコンピュータのホスト名またはIPアドレスで置き換えられます。

ドメイン環境で、一部のコマンドはより有効に機能します。(対象のコンピュータで管理者権限がある)ドメインユーザーとしてログインした場合、資格情報を追加する必要はありません。

ネットワークアクション	コマンド	前提条件
ping	–	・ファイアウォールで有効にした ICMP
Wake On LAN	–	・選択したコンピュータのネットワークカードは、標準のマジックパケット形式に対応している必要があります ・Wake On LAN は、選択したコンピュータの BIOS に設定されており、これらのネットワークカードに設定されている必要があります ・ダイアログウィンドウ自体での詳細
共有	explorer.exe ¥¥<computer>	・対象のコンピュータで有効にした共有 ・共有でのファイアウォールの例外
シャットダウン / 再起動	shutdown /s /t <timeout> /c "<reason_comment>" /f /m <computer> ・再起動を選択する場合、/s の代わりに /r があります ・「理由コメント」が空の場合、/c "<reason_comment>" はありません ・「アプリケーションの強制終了」がチェックされていない場合、/f はありません ・「シャットダウンアクションの中止」がチェックされている場合、常に shutdown /a /m <computer> のみです	・リモートレジストリサービスが有効 ・Windows Management Instrumentation サービスが有効 ・Windows Management Instrumentation (WMI) のファイアウォール例外 ・コンソールコンピュータでの現在の Windows ユーザーは、対象のコンピュータで管理者権限があることが必要です (これはドメイン環境を想定しています) ・ローカルコンピュータで管理者アカウントの下でそれを実行中 ・資格情報の追加 : 1. Windows の資格情報マネージャを検索する 2. [Windows 資格情報の追加] をクリックする 3. 対象のコンピュータで、その対象のコンピュータの名前 (または IP アドレス)、ユーザー名、パスワードを入力する
メッセージ	msg.exe /SERVER:<computer> * "a"	・レジストリ変更 :HKLM¥SYSTEM¥CurrentControlSet¥Control¥Terminal Server 名前 (N):AllowRemoteRPC タイプ :REG_DWORD 値 :1 ・ローカルコンピュータで管理者アカウントの下でそれを実行中 ・資格情報の追加 : 1. Windows の資格情報マネージャを検索する 2. [Windows 資格情報の追加] をクリックする 3. 対象のコンピュータで、その対象のコンピュータの名前 (または IP アドレス)、ユーザー名、パスワードを入力する
RDP	mstsc.exe /v <computer>	
custom - cmd.exe に対して有効なカスタムコマンドを実行できます		

3.4.4 [ウイルスログ] タブ

このタブには、発生した個別のウイルスについての詳細情報が表示されます。

属性	説明
ウイルス ID	データベースにある対応するエントリの ID
クライアント名	ウイルス警告を報告したクライアントの名前
コンピュータ名	ワークステーション / サーバーの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERAS の名前
受信日	ERAS によってイベントがログに記録された日時
発生日	イベントが発生した日時
レベル	警告レベル
スキャナ	ウイルスを検出したセキュリティ機能の名前
オブジェクト	オブジェクトの種類
名前	通常は、ウイルスが存在するフォルダ
ウイルス	検出された悪意のあるコードの名前
アクション	指定したセキュリティ機能で実行されたアクション
ユーザ	事件発生時に識別されたユーザーの名前
情報	検出されたウイルスについての情報

3.4.5 [ファイアウォールログ] タブ

このタブには、クライアントのファイアウォールアクティビティに関連する情報が表示されます。

属性	説明
ファイヤーウォール ID	データベースにある対応するエントリの ID
クライアント	イベントを報告しているクライアントの名前
コンピュータ名	ワークステーション / サーバーの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERAS の名前
受信日時	ERAS によってイベントがログに記録された日時
発生日時	イベントが発生した日時
レベル	警告レベル
イベント	イベントの説明
ソース	ソースの IP アドレス
ターゲット	対象の IP アドレス
プロトコル	関係するプロトコル
ルール	関係するファイアウォール ルール
アプリケーション	関係するアプリケーション
ユーザ	事件発生時に識別されたユーザーの名前

3.4.6 [イベントログ]タブ

このタブはすべてのシステム関連イベントのリストを表示します(ESETセキュリティ製品プログラムのコンポーネントに基づいて)。

属性	説明
イベント ID	データベースにある対応するエントリの ID
クライアント	イベントを報告しているクライアントの名前
コンピュータ名	ワークステーション / サーバーの名前(ホスト名)
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERAS の名前
受信日時	ERAS によってイベントがログに記録された日時
発生日時	イベントが発生した日時
レベル	警告レベル
プラグイン	イベントを報告しているプログラムコンポーネントの名前
イベント	イベントの説明
ユーザ	イベントに関連付けられたユーザーの名前

3.4.7 [HIPSログ]タブ

このタブはすべてのHIPS関連活動を示しています。

属性	説明
HIPS ID	データベースにある対応するエントリの ID
クライアント名	HIPS メッセージを報告しているクライアントの名前
コンピュータ名	HIPS メッセージを報告しているコンピュータの名前
MAC アドレス	HIPS メッセージを報告しているコンピュータの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERA Server の名前
受信日	ERAS によってイベントがログに記録された日時
発生日	イベントが発生した日時
レベル	イベントの緊急レベル
アプリケーション	HIPS ログに生成された応用の名前。これは応用の実行可能への UNC パスの形式を有します。
オペレーション	ターゲットアプリケーションに影響を与える活動
ターゲット	HIPS ログに生成された応用ファイル。そのインストールフォルダの応用にあるファイルへのパスの形式
アクション / ルール	現在のアクティブモード / ルールに基づいて、HIPS によって取られたアクション

NOTE

既定では、HIPS動作のログは無効になっています。このログの有効化、あるいは設定の変更には、ツール>サーバのオプション>サーバのメンテナンス>ログ収集パラメータに進んでください。

3.4.8 [デバイスコントロールログ] タブ

このタブはデバイスの制御動作の詳細ログを示しています。

属性	説明
デバイスコントロール ID	データベースに対応するエントリの ID
クライアント名	イベントを報告しているクライアントの名前
コンピュータ名	コンピュータの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERA Server の名前
受信日	ERAS によってイベントがログに記録された日時
発生日	イベントが発生した日時
レベル	警告レベル
ユーザ	イベントに関連付けられたユーザーの名前
グループ	動作を報告したクライアントをグループ化します
デバイスクラス	移動できるデバイスのタイプ（USB ストレージ、DVD...）
デバイス	移動できるデバイスの呼名とシリアル番号（可能な場合）
イベント	デバイス制御の機能によって報告されたイベント。
アクション	指定したセキュリティ機能で実行されたアクション

NOTE

既定では、デバイスコントロール動作のログは無効になっています。このログの有効化、あるいは設定の変更には、ツール>サーバのオプション>サーバのメンテナンス>ログ収集パラメータに進んでください。

3.4.9 [Web コントロールログ] タブ

このタブはWebの制御動作の詳細ログを示しています。

属性	説明
Web コントロール ID	データベースにある対応するエントリの ID
クライアント名	イベントを報告しているクライアントの名前
コンピュータ名	コンピュータの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERAS の名前
受信日	ERAS によってイベントがログに記録された日時
発生日	イベントが発生した日時
レベル	警告レベル
ユーザ	イベントに関連付けられたユーザーの名前
グループ	動作を報告したクライアントをグループ化します
URL	閉鎖されたウェブページの URL
URL マスク	閉鎖されたウェブページの URL マスク
URL カテゴリ	閉鎖されたウェブページの URL カテゴリ
アクション	指定したセキュリティ機能で実行されたアクション

NOTE

既定では、Webコントロール動作のログは無効になっています。このログの有効化、あるいは設定の変更には、ツール>サーバのオプション>サーバのメンテナンス>ログ収集パラメータに進んでください。

3.4.10 [迷惑メール対策ログ] タブ

このタブはすべての迷惑メール対策関連活動を示しています。

属性	説明
迷惑メール対策 ID	データベースにある対応するエントリの ID
クライアント名	スパムメッセージを報告しているクライアントの名前
コンピュータ名	コンピュータの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERA Server の名前
受信日	ERAS によってイベントがログに記録された日時
発生日	イベントが発生した日時
受信期間	イベントを受信した期間
送信者	スパムとしてマークされたメッセージ送信者の電子メールアドレス
受信者	スパムとしてマークされたメッセージの受信者
件名	スパムとしてマークされたメッセージの件名
メッセージ送信元	メッセージの送信元
スコア	スパム評価の値（スパムメッセージと判定するメッセージの確率）
理由	メッセージがスパムとしてマークされた理由
アクション	このメッセージに取られたアクション

NOTE

既定では、迷惑メール対策動作のログは無効になっています。このログの有効化、あるいは設定の変更には、ツール>サーバのオプション>サーバのメンテナンス>ログ収集パラメータに進んでください。

3.4.11 [グレーリストログ] タブ

このタブはグレーリスト関連活動を示しています。

属性	説明
グレーリスト ID	データベースにある対応するエントリの ID
クライアント名	イベントを報告しているクライアントの名前
コンピュータ名	コンピュータの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERAS の名前
受信日	ERAS によってイベントがログに記録された日時
発生日	イベントが発生した日時
HELO ドメイン	受信サーバーに向かって自身を識別するために、送信サーバーで使用されるドメイン名
IP アドレス	送信者の IP アドレス
送信者	送信者の電子メールアドレス
受信者	受信者の電子メールアドレス
アクション	指定したセキュリティ機能で実行されたアクション
残り時間	メッセージが拒否され、検証され、配信される前に残った時間

NOTE

既定では、グレーリスト動作のログは無効になっています。また、この項目はサポート対象外です。このログの有効化、あるいは設定の変更には,ツール>サーバのオプション>サーバのメンテナンス>ログ収集パラメータに進んでください。

3.4.12 [検査ログ] タブ

このタブには、オンデマンドで始まったコンピュータの検査のうち、リモートで実行しているもの、クライアントコンピュータでローカルに実行しているもの、またはスケジュールタスクとして実行しているものが一覧表示されます。

属性	説明
スキャン ID	データベースにある対応するエントリの ID
クライアント名	検査が実行されたクライアントの名前
コンピュータ名	ワークステーション / サーバーの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERA Server の名前
受信日	ERAS によって検査イベントがログに記録された日時
発生日	クライアントで検査が発生した日時
検査対象	検査済みのファイル、フォルダ、およびデバイス
検査済み	チェックされたファイルの数
感染	感染したファイルの数
駆除済み	駆除（または削除）されたオブジェクトの数
状態	検査の状態
ユーザ	事件発生時に識別されたユーザーの名前
タイプ	ユーザーの種類
スキャナー	スキャナの種類
詳細	クライアントログの提出ステータス

3.4.13 [モバイルログ] タブ

このタブには、ERA Serverに接続したモバイルデバイスの詳細なログが表示されます。

属性	説明
モバイル ID	モバイルデバイスのネットワーク ID
クライアント	アクションが実行されたクライアントの名前
コンピュータ名	ワークステーション / サーバーの名前（ホスト名）
MAC アドレス	ネットワークアダプタの MAC アドレス
プライマリサーバ	クライアントの通信相手である ERA Server の名前
受信日時	ERAS によってイベントがログに記録された日時
発生日時	クライアントでイベントが発生した日時
レベル	警告レベル
ログタイプ	ログの種類（セキュリティ監査ログ、SMS 迷惑メール対策ログなど）
イベント	イベントの説明
オブジェクトタイプ	イベントが関連するオブジェクト（SMS、ファイルなど）
オブジェクト名	イベントが関連する具体的なオブジェクト（SMS 送信者の電話番号、ファイルへのパスなど）
アクション	イベント中に実行されたアクション（または発生したエラー）

3.4.14 [隔離]タブ

このタブには、ネットワークにあるすべての隔離エントリがまとめられています。

属性	説明
隔離 ID	発生順に割り当てられた隔離済みオブジェクトの ID 番号
ハッシュ	ファイルのハッシュコード
受信日時	ERAS によって検査イベントがログに記録された日時
最初の発生	隔離されたアイテムが最初に発生してから経過した時間
最後の発生	隔離されたアイテムが最後に発生してから経過した時間
オブジェクト名	通常は、ウイルスが存在するフォルダ
ファイル名	隔離されたファイルの名前
拡張子	隔離されたファイルの拡張子の種類
サイズ	隔離されたファイルのサイズ
理由	隔離の理由 - 通常は脅威の種類の説明
クライアント数	オブジェクトを隔離しているクライアントの数
ヒット	オブジェクトが隔離された回数
ファイル	オブジェクトをサーバーにダウンロードするように要求されたかどうかを示します

››› NOTE

[オブジェクト名]、[ファイル名]、および[拡張子]の各フィールドには、最初の3つのオブジェクトのみが表示されます。詳細情報を確認するには、F3キーを押すか、選択したアイテムをダブルクリックして、プロパティウィンドウを開きます。

隔離ファイルの集中管理によって、クライアントにローカルで保存されている隔離ファイルの概要を把握でき、必要に応じてそのファイルをリクエストできます。リクエストしたファイルは、暗号化された安全な形式でERA Serverにコピーされます。隔離ファイルの取り扱い手順については、「隔離からの復元/削除」を参照してください。

››› NOTE

隔離ファイルを集中管理するには、EAV/ESSバージョン4.2以降をクライアントにインストールする必要があります。

3.4.15 [タスク]タブ

このタブの意味については、タスクで説明しています。使用可能な属性は次のとおりです。

属性	説明
タスク ID	データベースにある対応するエントリの ID
状態	タスクの状態（有効 = 適用中、終了 = タスクがクライアントに配信されました）
タイプ	タスクの種類
名前	タスク名
説明	タスクの説明
配信日	タスクの実行日時
受信日	ERAS によってイベントがログに記録された日時
詳細	タスクログの提出ステータス
コメント	クライアントを説明する短いコメント（管理者が入力）
作成者	タスクを作成した作成者名
プライマリサーバ	プライマリサーバー名
作成日	タスクの作成日

3.4.16 [レポート]タブ

レポートタブを使用すると、統計情報をグラフや表にまとめることができます。このグラフや表は、グラフおよびグラフィカル出力を提供するERAのツールを使用することによって、コンマ区切り値の形式（.csv）にして、後で保存および処理できます。既定のERAでは出力結果がHTML形式で保存されます。ウイルスに関連するレポートのほとんどは、ウイルスログから生成されます。

1.ダッシュボードテンプレート

Webダッシュボードレポートのためのテンプレート。ダッシュボードはレポートのセットで、Webブラウザを使って、オンラインで利用できます。ダッシュボードのレイアウトは、各管理者が完全にカスタマイズできます。テンプレートをダブルクリックして、ダッシュボードで使用されるレポートのプレビューを表示します。

2.レポートテンプレート

静的レポート用テンプレート。[コンソール] ウィンドウ上部のレポートテンプレートセクションには、作成済みテンプレートの名前が表示されています。テンプレート名の横には、日時/間隔に関する情報、および現在のテンプレートに従ってレポートがいつ生成されるかが表示されます。新しいテンプレートの作成、または既存の定義済みテンプレートの編集ができます（以下に示されたように）：

クライアント概要	すべてのクライアントの保護の状態を示しています。
ウイルス検出後の駆除処理が行われないクライアント	ウイルスがアクティブなクライアント（スキャン中に駆除されていないウイルス）をアクティブなウイルスに関する情報とともに表示します。
総合ネットワーク攻撃レポート	ネットワーク攻撃のアクティビティに関する包括的な報告書を示します。
総合SMSレポート	SMS 迷惑メールアクティビティに関する包括的な報告書。
総合迷惑メールレポート	電子メール迷惑メールアクティビティに関する包括的な報告書。
総合ウイルスレポート	見つかった脅威に関する包括的な報告書。
カスタム情報サマリ	ユーザー定義情報を含む包括的な報告書を示します（最初に定義する必要があります）。
問題の多いクライアント	問題の最大数を持つクライアントを示します（以上のレポートに基づいて）。

既定のテンプレートをクリックして、元の状態に定義済みのテンプレートをリセットします（このアクションは、カスタム作成したテンプレートに影響しません）。

●オプション

今すぐ生成をクリックすると（必ずオプションタブを選択しておきます）、スケジュールに関係なくレポートをいつでも生成できます。

●レポート

種類	定義済みのテンプレート
スタイル	このドロップダウンメニューで、レポートの色やレイアウトを変更することができます。

●フィルタ

対象のクライアント	レポートに含める、または含めないクライアントを指定できます。対象のクライアントの横にあるドロップダウンメニューからレポートに含めるクライアント、サーバー、グループを指定、またはレポートに含めないクライアント、サーバー、グループを指定すると、追加 / 削除ダイアログが開き、レポートに含める対象を設定できます。
脅威	すべての脅威、選択された脅威だけまたは選択された脅威を除外表示する場合に、指定します。ドロップダウンメニューから選択されたウイルスのみ、または選択されたウイルスを除外を選択し、[...] ボタンをクリックして、レポートに含める / 含めない対象のウイルスを選択します。

その他の詳細は、詳細設定をクリックして設定できます。これらの設定は通常、見出しのデータまたは使用される図の種類のデータに適用されます。ただし、選択した属性のステータスに基づいてデータをフィルタしたり、使用するレポート形式（.html、.csv）を選択したりすることもできます。

●インターバル

現在	選択した期間に発生したイベントのみがレポートに記載されます。たとえば、間隔を［現在の週］に設定して水曜日にレポートを作成すると、日曜日、月曜日、火曜日、および水曜日のイベントが記載されます。
過去	選択した過去の期間に発生したイベントのみがレポートに記載されます（たとえば、８月の全日、日曜日～土曜日の全日）。現在の期間も追加するオプションを選択すると、最後に完了した期間から作成時点までのイベントがレポートに記載されます。

例

先週（日曜日～土曜日）のイベントを記載したレポートを作成するとします。そして、このレポートを今週の水曜日に生成するとします。[間隔]タブで[過去]と[1週間]を選択します。[現在の期間も追加する]の選択は解除します。スケジューラタブで頻度を週毎に設定し、水曜日を選択します。その他の設定は、管理者が自由に設定できます。

次の日時から次の日時まで	この設定を使用して、レポートの生成対象期間を定義します。

●スケジューラー

頻度	選択した期間または間隔で、レポートを自動生成するように定義および設定できます。

レポートのスケジュールを指定したら、保存先の設定をクリックして、レポートの保存先を指定します。レポートは、既定でERASに保存されますが、選択したアドレスへの電子メールによる送信やフォルダへのエクスポートも可能です。組織のイントラネット上にある共有フォルダにレポートを送信して、他の社員が参照できるようにする場合は、フォルダにエクスポートするオプションが便利です。フォルダのパスにおいて変数（%）が使えます。変数は大文字小文字の区別はありません。これらの変数は、生成されたレポートにカスタム情報を追加します。もしフォルダのパスに「¥」で節目をつけたら、レポートはこのフォルダに直接書き込まれ、データが上書きされるようになります。サポートされるオプションは次のとおりです。

変数	説明
%INTERVAL%	レポートが生成される間隔
%DATE%	現在の日付、("YYYY-MM-DD")
%TIME%	現在の時間（"HH-MM-SS"）
%DATETIME%	現在の日付と時間（"YYYY-MM-DD HH-MM-SS"）
%TIMESTAMP%	現在の日付と時間、UNIX 時間、8 桁の 16 進数
%RND4%	ランダム値、4 桁の 16 進数、（推奨しません）
%DDay%	現在の日付、詳細形式（"YYYYMMDD"）
%DTIME%	現在の時間、詳細形式（"HHMMSS"）
%YEAR%, %MONTH%, %DAY%, %HOUR %, %MINUTE%, %SECOND%	現在の日付 / 時間
%COUNTER %	5 桁の 10 進法カウンター、1 で始まります
%COUNTER 1%, %COUNTER 2%, %COUNTER 3%, %COUNTER 4%, %COUNTER 5%	1/2/3/4/5- 桁の 10 進法カウンター、1 で始まります。
%CCOUNTER %	5 桁の 10 進法の仮定的なカウンター（第一の反復が消去され、第一の反復が「00002」です）
%CCOUNTER 1%, %CCOUNTER 2%, %CCOUNTER 3%, %CCOUNTER 4%, %CCOUNTER 5%	1/2/3/4/5- 桁の 10 進法カウンター
%UCOUNTER %	5 桁の 10 進法のアンダースコアカウンター（第一の反復が消去され、第一の反が「_00002」です）
%UCOUNTER 1%, %UCOUNTER 2%, %UCOUNTER 3%, %UCOUNTER 4%, %UCOUNTER 5%	1/2/3/4/5- 進法のアンダースコアカウンター。
%%	単独の % 記号

例えばパスの指定に次の形式で入力すると:C:¥Reports¥%INTERVAL%_%COUNTER%"、フォルダ名は次のように生成されます。C:¥Reports¥Day 2012-02-02_00001; C:¥Reports¥Day 2012-02-02_00002など。

生成したレポートを電子メールで送信するには、[ツール] -> [サーバオプション] -> [その他の設定] で、SMTPサーバーおよび送信者のアドレス情報を入力する必要があります。

3.作成されたレポート

これまでに生成されたレポートは、作成されたレポートタブで参照できます。他のオプションについては、個別（または複数）のレポートを選択し、（右クリックして）コンテキストメニューを使用してください。レポート名、レポートが生成された日付、テンプレート名とレポートの保存場所でレポートを分類できます。開くをクリックするか、リストにあるレポートをダブルクリックします。リストにあるレポートをダブルクリックし、下部にあるプレビューを表示します（このオプションを選択すると）。

[お気に入り]リストにあるテンプレートを使用して、いつでも新しいレポートを直ちに生成できます。テンプレートを[お気に入り] に移動するには、レポートを右クリックして、コンテキストメニューのお気に入りに追加を選択します。

3.4.16.1 ダッシュボード

[ダッシュボード] は、システムの状態の包括的な概要を提供する新しいデータで自動的に更新されるレポート群です。ERACへのアクセスおよびログインが可能な各ユーザーには、完全にカスタマイズ可能な個別のダッシュボードセットが提供されます。これらの設定はサーバーに直接保存されるため、ユーザーは任意のブラウザから同じダッシュボードにアクセスできます。

ダッシュボード機能は、デフォルトではERA HTTPサーバーのポート 443を介した通信を使用します。ポートおよび証明書（HTTPS）の変更は、サーバオプションの詳細設定で行います。[ダッシュボード] および [ダッシュボード] 接続オプションにも、ツールバーのERACメインプログラムウィンドウからアクセスすることができます（青い雲のアイコン）。

NOTE

管理者は、ダッシュボード内のレポートを正しく表示させるために、前もって各レポート用にテンプレートを準備する必要があります。

NOTE

デフォルトでは、[ダッシュボード] は、自己署名の証明書でhttpsプロトコルを使用して開始されます。これによって、以下の警告メッセージがWebブラウザに表示されることがあります。このWebサイトによって提供されるセキュリティ証明書は、信頼できる証明機関によって発行されたものではありません。HTTP使用時にはユーザー名およびパスワードはプレーンテキストで送信されることに注意してください。これは、Windows/Domainログイン使用時には特に注意が必要です(安全ではありません)。

ASN	個別ファイルにおける ASN.1 DER でエンコードされた証明書およびキー。
PEM	個別ファイル内の Base64 でエンコードされた追加ヘッダ、証明書およびキー付き ASN
PFX	単一コンテナファイルでの証明書およびプライベートキー

フォーマットが異なる証明書およびキーを使用することはできません。ERACのメインプログラムウィンドウで [ダッシュボード] (ブルークラウドアイコン) をクリックし、続いて [設定] ...をクリックすることによって、プロトコルをhttpに変更できます。または、ESETコンフィグレーションエディタ ([ツール] > [サーバ] > [オプション] > [詳細] > [詳細設定の編集] ...> [リモート管理者] > [ERAサーバ] > [設定] > [ダッシュボード] > [ローカル証明書キー] / [ローカル証明書]) を使用して自分自身の証明書を定義することができます。

NOTE

ダッシュボードもIPv6プロトコルをサポートします。例えば、http://[::1]:8080

既定で用意されている [ダッシュボード] 用の定義済みテンプレートのセットを使用するか、カスタムテンプレートを作成することができます。

既存のレポートテンプレートをインポートまたはエクスポートするには、[インポート...] または [エクスポート...] をクリックします。インポート時の名前の競合 (既存のテンプレートとインポートしたテンプレートの名前が同じ状態) は、インポートしたテンプレートの名前の後ろにランダムな文字列を割り当てることによって解決します。

定義したレポートの設定をテンプレートに保存するには、[保存] または [名前を付けて保存...] をクリックします。テンプレートを新規作成するには、[名前を付けて保存...] をクリックして、テンプレートに名前をつけます。[既定のテンプレート] をクリックすると、定義済みテンプレートが元の状態にリセットされます (この操作はカスタム作成されたテンプレートには影響を与えません)。

●オプション

レポートのプレビュー	このボタンをクリックすると、ダッシュボードが作成され、プレビューが表示されます。

●レポート

タイプ	定義済みテンプレートに基づいたレポートのタイプ。カスタムテンプレートの作成に使用された定義済みテンプレートに対して変更することができます。

●フィルタ

対象のクライアント	レポートに含める、または含めないクライアントを指定できます。対象のクライアントの横にあるドロップダウンメニューからレポートに含めるクライアント、サーバー、グループを指定、またはレポートに含めないクライアント、サーバー、グループを指定すると、追加 / 削除ダイアログが開き、レポートに含める対象を設定できます。
脅威	すべての脅威、選択された脅威だけまたは選択された脅威を除外表示する場合に、指定します。ドロップダウンメニューから選択されたウイルスのみ、または選択されたウイルスを除外を選択し、[...] ボタンをクリックして、レポートに含める / 含めない対象のウイルスを選択します。

その他の詳細は、[詳細設定...] をクリックして設定できます。これらの設定は通常、見出しのデータまたは使用される図の種類のデータに適用されます。但し、選択された属性のステータスに従って、データをフィルタすることもできます。さらに、どのレポートフォーマット (.html,.csv) を使用するかを選択することができます。

●インターバル

[時点] - [最後] [X] [分/時間/日/週/月/年] レポート内のデータはこの時点以降のものになります。時点はインシデントがERAに報告された時点がベースになります。

●更新

[ブラウザの更新間隔] -Webサーバーから受信される新規データの更新間隔を選択します。

[サーバの更新間隔] -データがWebサーバーに送信される時間間隔を選択します。

ダッシュボードのWebサーバーリスト

メインメニューのダッシュボードアイコンの横にある矢印をクリックして、[ダッシュボードのWebサーバ] の接続オプションを設定します。

ダッシュボードのWebサーバ	使用可能なすべてのダッシュボード Web サーバーの一覧。
削除	このボタンをクリックすると、選択したダッシュボードの Web サーバーが一覧から削除されます。
既定として保存	選択したダッシュボードの Web サーバーを既定のダッシュボード Web サーバーに設定します。これは、ダッシュボードアイコンの横にある矢印のクリック後、ドロップダウンメニューで使用することでき、ダッシュボードアイコン自体をクリックした後に開きます。
プロトコル	http か自己署名証明書を用いる https かを選択できます。
ホスト名またはIPアドレス	選択したダッシュボード Web サーバーのホスト名または IP アドレスを表示します。また、ホスト名または IP アドレスを新規入力したり、[追加 / 保存] をクリックしてダッシュボード Web サーバーを一覧に追加 / 保存することもできます。
コメント	選択したダッシュボードの Web サーバーについて必要に応じて入力するコメント / 説明。 **注意：**ダッシュボードでは IPv6 プロトコルもサポートされます（http:// [::1] :8080 など）。

3.4.16.2 レポートシナリオの例

クライアントのネットワークセキュリティを最高のレベルで維持するには、ネットワークのセキュリティ状態の概要を適切に把握しておく必要があります。脅威、アップデート、クライアントの製品バージョンなどに関する詳細を網羅したレポートを簡単に作成できます (詳細については、「レポート」を参照してください)。通常は、週ごとのレポートで必要な情報をすべて確認できます。ただし、脅威が検出された場合のように、特別な警戒が必要となる状況が発生することがあります。

ここでは、例として隔離というパラメータグループを作成します。このグループには、前回のオンデマンドスキャンでウィルスが検出され、駆除したコンピュータのみが属します。この条件を設定するには、[最終スキャンでウイルス検出有り] の隣のチェックボックスを選択します。このパラメータグループを作成する手順については、「パラメータグループ」を参照してください。

NOTE

隔離グループを作成する際、[スティッキー] オプションが無効になっていることを確認してください。これによって確実に、コンピュータが動的に割り当てられ、条件に一致しなくなると削除されます。

隔離コンピュータレポートを作成します。このパラメータグループのレポートを作成する手順については、「レポート」を参照してください。

この例に固有の設定は次のとおりです。

● [オプション] のセクション設定:

種類	詳細な隔離レポート
スタイル	ブルースキーム
対象のクライアント	選択したグループのみ
ウイルス	n/a

● [インターバル] のワイルドカード設定:

現在	毎日

● [スケジューラ] のワイルドカード設定:

頻度	日毎
毎	1 日

Hint

レポートデータベースへの結果の保存や、レポートのコピーを保存するフォルダの設定などが可能です。また、レポートを電子メールで送信することもできます。これらの設定はすべて、[保存先の設定] クリックすると表示されます。

作成されたレポートは、[レポート] セクションの [一般レポート] ワイルドカードで確認できます。

まとめ:ここでは、前回のオンデマンドスキャンで脅威が報告されたコンピュータを含む隔離パラメータグループを作成しました。次に、隔離グループに属するコンピュータを日時で報告する自動レポートを作成しました。これにより、クライアントネットワークの状態を適切に把握し、脅威となる可能性のある状況を制御できます。

Hint

前回のスキャンログの詳細を確認する場合は、レポートの種類として [詳細なスキャンログレポート] を使用します。

3.4.17 ［リモートインストール］タブ

このタブには、クライアントへのESET Endpoint SecurityまたはESET Endpoint アンチウイルスのリモートインストールをさまざまな方法で行うためのオプションが用意されています。詳細については、「リモートインストール」を参照してください。

1.コンピュータを検索するには、デフォルト検索タスクの使用や新しいタスクの作成ができます。新しい検索タスクを作成するには、新しい検索...をクリックし、ネットワーク検索タスクウィザードを起動してください。検索タスクを実行するには、［実行］をクリックしてください。

2.検索の結果は検索の結果フィルタ以下のセクッションのツールを使って、フィルターされます。結果のフィルタリングは実際の検索タスクに影響を与えません。

未登録のコンピュータのみを表示する	現在のサーバーデータベースにリストされていないコンピュータを表示します。
最終アクセス警告のあるクライアント	現在のサーバーデータベースに登録されており、最終接続警告を受けたコンピュータが表示されます。
無視されたコンピュータを非表示にする	既定ではこのオプションはアクティブです。管理者の作成したリストに従ってコンピュータが非表示になります。

3.コンピュータセクションにおいて、現在検索タスクの検索結果は表示されます。ここから、コンテキストメニューを使って、インストールパッケージを管理したり、リモートプッシュインストールを実行したりすることができます。

コンピュータタブのコンテキストメニュー（右クリック）は次のオプションを提供します。

パッケージ管理	インストールパッケージエディタを実行します。詳細については、「リモートインストール」を参照してください。
Windowsクライアントをアップグレード	アップグレードタスクを実行します。このオプションは、古いバージョンの ESS/EAV がインストールされているクライアントに新しいバージョンを上書きインストールする場合に使用します。
Windowsプッシュインストールの診断	リモートインストール時に必要なサービス等がクライアント側で有効かどうかをチェックします。詳細については、「リモートインストールの診断」を参照してください。
Windowsプッシュインストール	Windows リモートプッシュインストールを実行します。
Linux/Macプッシュインストール	Linux のプッシュインストールを実行します。現時点ではこの機能はサポートされていません。
無視リスト	選択したコンピュータを無視リストに登録します。無視リストに登録されたコンピュータは、［無視されたコンピュータを非表示にする］にチェックを入れると非表示になります。
フォルダまたはログオンスクリプトへエクスポート	ログオン / 電子メールリモートインストールをご参照してください。
電子メールで送信	ログオン / 電子メールリモートインストールをご参照してください。
電子メールおよびログオンスクリプトインストールのための既定のログオンを設定する	既定ログオンウィンドウを開き、対象のコンピュータの管理者アカウントのユーザー名とパスワードを指定できます。
プロパティ	クライアントプロパティウィンドウを開き、クライアントについての重要な情報をすべて参照できます。

コンテキストメニューの他のオプションについては、「コンテキストメニュー」を参照してください。

3.4.17.1 ネットワーク検索タスクウィザード

検索タスクはネットワーク上のコンピュータを検索するために使用されるパラメータのセットです。作成した検索タスクは、サーバーに直接保存されているので、すべての管理者が利用できます。

ネットワーク検索タスクでは定期的に実行される定義済みのデフォルトの検索タスクや、ネットワーク全体を検索することができます。このタスクからの検索結果は、サーバー上に格納されます。タスクは編集することが可能です。タスクは一度開始するとそれが完了するまで停止させることはできません。

カスタムタスクパラメータは、サーバーに格納されています。タスク検索結果は、それらを実行したコンソールのみに送信されます。これらの検索タスクは、手動でのみ始められます。

1.まず、ネットワークタスクのタイプを選択します:

ネットワーク検査テンプレート	再利用を安濃にするため名前を設定します。パラメータのセットを使用して新しい検索タスクを作成します。検索結果は保存されていないため、新たな検索を実行すると、現在利用可能なネットワーク上のクライアントコンピュータのリストは更新されるようになります。
一時的なネットワーク検査タスク	このタスクは保存されません。一時的な検索タスクを作成します。

2.次は、ネットワークを検索するために使用される方法を選択します（複数の検索方法を選択できます）:

アクティブディレクトリ	このオプションは、Active Directory のブランチを選択してコンピュータを検索できます。検索の結果に無効なコンピュータを含めることもできます。
Windows Networking（Wnet）	Windows ネットワークにあるすべてのコンピュータを検索します。
シェル	Windowsネットワークにあるすべてのコンピュータを検索します。(ネットワークまはたマイネットワーク)。
IPアドレス	検索中に使われる IP 範囲 /IP マスクを選択した、カスタム IP アドレスリストを定義できます。コンピュータ指定のポートにアクセスすることによって、検索されます。PING を使うことも出来ます。
カスタムコンピュータのリスト	検索対象としてコンピュータのカスタムリスト（テキスト形式）をインポートします。

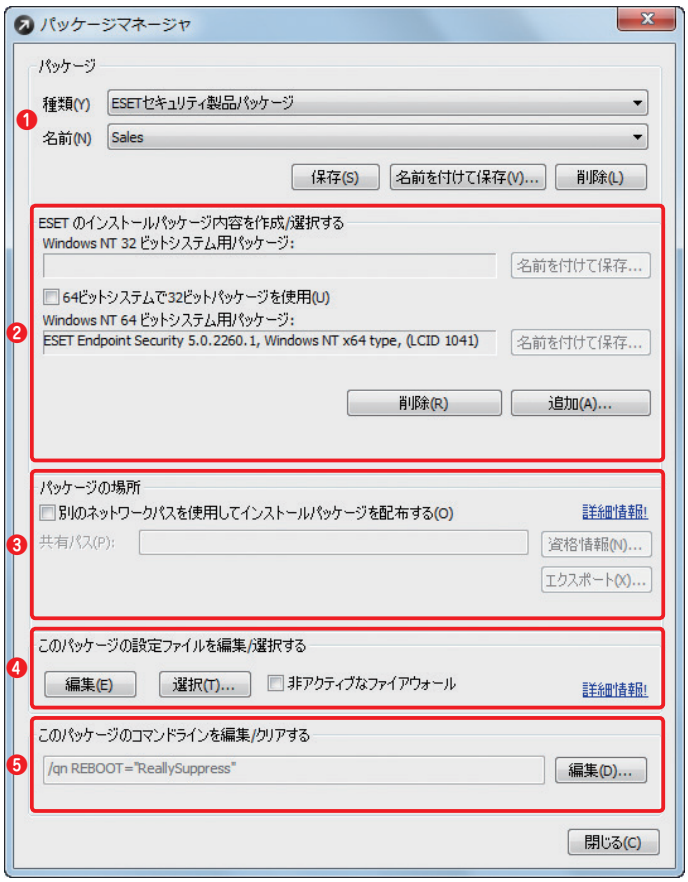
完了をクリックして、新規検索タスクを保存します。すぐにタスクを終了し、起動するには、[終了] & [起動] をクリックします。このタスクを実行するには、リモートインストールタブにある [起動] をクリックします。

▸▸▸ NOTE

サービスがローカルシステムアカウントで実行されている場合は、シェルとWnet検索ではコンピュータを検索できません。local systemアカウントはこのような検索を行う権限を持っていないためです。この問題を解決するには、ユーザーを変えるか、違った方法を導入します。

3.4.17.2 パッケージマネージャ

ERACを通してインストールパッケージを編集するには、[リモートインストール] タブをクリックして、[コンピュータ] タブをクリックします。[パッケージマネージャ] をクリックして、[パッケージマネージャ] ウィンドウを開きます。

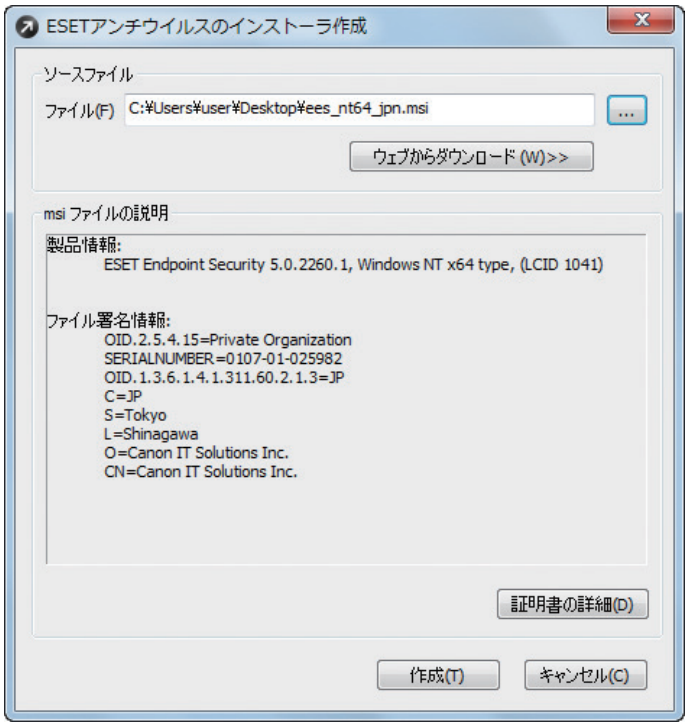


セクション❶の [種類] ドロップダウンメニューで、ERAの追加機能にアクセスできます。ESETセキュリティ製品は、リモートインストールできるだけでなく、[Windows用ESETセキュリティ製品およびNOD32バージョン2のアンインストール] オプションを使用して、リモートでアンインストールすることもできます。カスタムパッケージを選択することにより、外部アプリケーションもリモートインストールできます。サードパーティのセキュリティ製品のアンインストールツールやスタンドアロンの駆除ツールなど、さまざまなスクリプトや実行ファイルをクライアントマシンで実行する場合に、この機能が特に効果的です。使用するカスタムコマンドラインパラメータは [パッケージエントリファイル] で指定できます。詳細については、「ERAを使用したサードパーティ製品のインストール」を参照してください。

各パッケージには、ESETリモートインストーラエージェントが自動的に割り当てられます。これにより、シームレスなインストール、および対象のワークステーションとERASとの間の通信が可能になります。ESETリモートインストーラエージェントは、名前がeinstaller.exeであり、ERASの名前および所属先パッケージの名前と種類の情報が収録されています。エージェントの詳細については、後述のセクションで説明しています。

●ESETクライアントソリューションのインストールファイル❷

[ESETのインストールパッケージ内容を作成／選択する] セクションの [追加] をクリックすると、[ESETアンチウイルスのインストーラ作成] ウィンドウが開きます。[...] ボタンをクリックしてインストールパッケージを選択します。



NOTE

[64ビットのシステムで32ビットのパッケージを使用]のチェックボックスは、ESET Remote Administratorサーバーまたはコンソールをインストールする場合にのみ利用してください。ESETセキュリティ製品(ESET Endpoint SecurityまたはESET Endpointアンチウイルスなど)をインストールする場合にこのチェックボックスをオンにすると、インストールに失敗します。

[ESETのインストールパッケージ内容を作成/選択する]❷で、管理者はスタンドアロンのインストールパッケージを作成できます。このパッケージには、既に存在していて保存済みのインストールパッケージで事前定義されているコンフィグレーションを使用できます([名前を付けて保存...]ボタンを使用)。そのインストールパッケージは、プログラムのインストール先となるクライアントワークステーションで実行できます。ユーザーがそのパッケージを実行するだけで製品がインストールされます。インストール中に元のERASに接続されることはありません。

NOTE

.msiインストールファイルに設定を追加すると、そのファイルのデジタル署名は有効ではなくなります。

重要

Microsoft Windows Vista以降では、サイレントリモートインストールを実行することを強くお勧めします(使用するパラメータは/qnと/qb)。サイレントリモートインストールを使用しないと、UACが原因でタイムアウトが発生し、リモートインストールが失敗する可能性があります。

●パッケージの保管場所❸

インストールパッケージは、ERASの動作する次のディレクトリに保存されます。

%ALLUSERSPROFILE%¥Application Data¥ESET¥ESET Remote Administrator¥Server¥packages

[別のネットワークパスを使用してインストールパッケージを配布する]のチェックボックスをオンすると、別のパス(例えば共有フォルダーなど)を選択できます。

●ESETクライアントソリューション用XML構成ファイル❹

インストールパッケージを新たに作成する場合、ERA Serverに接続するためのプライマリサーバーのパスワードは空欄

に設定されています。ERA Serverに接続するためにパスワードを設定するときは、[編集] をクリックしてこのパッケージの.xmlコンフィグレーションを編集してください。パスワードは、それぞれの製品の [リモート管理] ブランチで設定できます。

また、既定では、ESET Endpoint Securityのファイアウォールをオフにしておくために、[非アクティブファイアウォール] のオプションがオンに設定されています。これは、ERA Serverの特定クライアントへの次回接続の試みを妨げないようにするためです。構成タスクをクライアントに送信することで、後からファイアウォールの設定をオンに戻すことができます。ファイアウォールの設定は、構成タスクの [Windowsデスクトップv5] > [パーソナルファイアウォール] > [設定] > [ファイアウォールシステム統合] で行えます。ここで [すべての機能が有効] の値を選択することで、ファイアウォールをオンにできます。

重要

非アクティブなファイアウォールのオプションをオンまたはオフに切り替えると、2つの設定プロパティが実際に変更されます。1つは ESET Configuration Editorで表示可能であり、もう1つは.xml構成ファイルでのみ表示可能です。こららの2つの設定プロパティのどちらかが設定されない（1つは設定され、もう1つは設定されない）場合、または1 ～ 10の範囲の値が設定されていない場合（例：[値] フィールドで [アプリケーションプロトコルの検査のみ] のオプションを選択する場合）、[ファイアウォールの非アクティブ化] チェックボックスは青色で完全に塗りつぶされます。

重要

ERAサーバー用に構成したパスワード（[ツール] > [サーバーオプション] > [セキュリティ] > [クライアント（ESETセキュリティ製品）のパスワード] で構成可能）を設定している場合、そのパスワードはパッケージを作成する際に自動的に使用されます。これにより、クライアントマシンはそのパスワードを使用してERAサーバーに接続できるようになります。ERAサーバーのパスワードを後から変更すると、ERAサーバーで [クライアントの非認証アクセスを有効にする（ESETセキュリティ製品）] オプションを有効にしていたとしても、管理されたクライアントはサーバーに接続できなくなります。この場合、管理されたクライアントに対して構成タスクを開始する必要があります。

●パッケージに割り当てられたコマンドラインパラメータ5

インストールプロセスに影響を与える可能性のあるパラメータがいくつかあります。これらのパラメータは、ワークステーションで管理者が作業を行う直接インストールでも、リモートインストールでも使用できます。リモートインストールの場合は、インストールパッケージの設定プロセスでこれらのパラメータを選択し、そこで選択したパラメータは対象のクライアントに自動的に適用されます。ESET Endpoint SecurityおよびESET Endpoint アンチウイルスの追加パラメータは、.msiインストールパッケージの名前に続いて入力できます（例：eea_nt64_JPN.msi /qn）。これらのパラメータを以下に示します。

/qn	サイレントインストールモード - ダイアログウィンドウは表示されません。	
/qb!	ユーザーが介入することはできませんが、インストールプロセスの進行が進捗状況バーに % で示されます。	
REBOOT="ReallySuppress"	プログラムのインストール後に再起動しません。	
REBOOT="Force"	インストール後に自動的に再起動します。	
REMOVE=...	選択されたコンポーネントのインストールを無効にします。	
	Emon	電子メールクライアントの保護
	Antispam	アンチスパム保護
	Dmon	書類保護
	ProtocolScan	プロトコルフィルタリング
	Firewall	パーソナルファイアウォール
	eHttpServer	アップデートミラーサーバー
	eDevmon	デバイス制御
	MSNap	Microsoft NAP
	eParental	Web コントロール
REBOOTPROMPT=""	インストール後に、再起動するかどうかの確認を求めるダイアログウィンドウが表示されます（/qn との併用はできません）。	

ADMINCFG="path_to_xml_file"	インストール時に、.xml 形式で指定したファイルで定義したパラメータが ESET セキュリティ製品に適用されます。このパラメータは、リモートインストールには不要です。インストールパッケージには、.xml 形式による独自のコンフィグレーションが収録されていて、これが自動的に適用されます。
PASSWORD=""	このパラメータを ESS/EAV 設定がパスワードで保護されている場合に追加する必要があります。
/SILENTMODE	サイレントインストールモード - ダイアログウィンドウは表示されません。
/FORCEOLD	新しいバージョンがインストール済みの場合に、古いバージョンを上書きインストールします。
/CFG ="path_to_xml_file"	インストール時に、.xml 形式で指定したファイルで定義したパラメータが ESET クライアントソリューションに適用されます。このパラメータは、リモートインストールには不要です。インストールパッケージには、.xml 形式による独自のコンフィグレーションが収録されており、これが自動的に適用されます。
/REBOOT	インストール後に自動的に再起動します。
/SHOWRESTART	インストール後に、再起動するかどうかの確認を求めるダイアログウィンドウが表示されます。このパラメータは、SILENTMODE パラメータと組み合わせた場合にのみ使用できます。

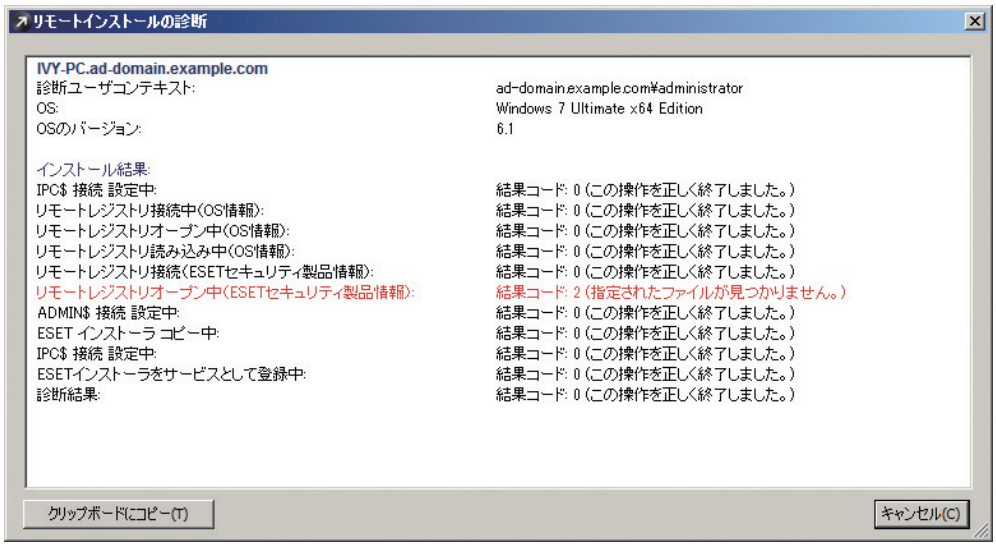
重要

UACがクライアント・ソリューション上で有効になる場合、Windows 7/2008に設定されたデフォルトUACセキュリティは、任意のプログラムを実行する前にユーザーの確認を必要とします。ユーザーの確認作業を避けたいときは、以下のコマンドを使ってインストールを実行してください。

C:¥Windows¥System32¥msiExec.exe -i path_to_the_msi_file /qb!ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress"

C:¥Windows¥System32¥msiExec.exe -iは、Windowsインストーラのコンポーネントとインストールパラメータです。path_to_the_msi_file /qb!ADMINCFG="path_tp_the_xml_file" REBOOT="ReallySupress" は、インストールファイルのパスとユーザーの確認作業を避けるためのパラメータと設定ファイルです。

3.4.17.3 リモートインストールの診断



●IPC$接続の設定:

管理者はすべてのクライアントコンピュータ上においてローカル管理者権限を持つ必要があります。

共有リソースはクライアント上にインストールされ、有効にされなければなりません。

ネットワークファイアウォールは共有リソースを有効にしなければなりません(ポート445と135-139)。

Windows管理者のパスワードを空白にしてはいけません。

"ファイルのシンプル共有の使用"のオプションはワークグループとドメインの混在環境でアクティブにすることはできません。

サーバーサービスがクライアントのマシンにおいて実行されていることを確認してください。

●リモートレジストリの接続(OS情報):

リモートレジストリサービスはクライアント上に有効にされ、起動されなければなりません。

●リモートレジストリ開始（OS情報）：
上記＋管理者はクライアントの登録に完全な許可コントロールを持つ必要があります。

●リモートレジストリ読み込み（OS情報）：
管理者はクライアントの登録に完全な読み込み管理許可を持つ必要があります。上記の動作が成功すれば、本動作も。

●リモートレジストリの接続（ESETセキュリティ製品情報）：
HKEY_LOCAL_MACHINE/SOFTWARE/ESET（またはHKEY_LOCAL_MACHINE/SOFTWAREのブランチ）に対して管理者は完全なコントロール許可を持ったなければなりません。

●リモートレジストリの開始（ESETセキュリティ製品情報）：
リモートレジストリサービスはクライアントのコンピュータ上で実行されていることを確認してください。

●ADMIN$接続の設定:
管理共有ADMIN$は有効にされなければなりません。

●ESETインストーラのコピー:
ポート2222、2223、および2224はサーバーで開かれ、ネットワークファイアウォール上に許可されなければなりません。

●IPC$接続の設定:
この操作はget infoの診断で成功に完成した場合、ここで成功に完成する必要があります。

●サービスとしてのESETインストーラの登録:
einstaller.exeをターゲットコンピュータ上で実行することに十分な権限を持つことを確認してください。

NOTE

診断中にエラーが発生した場合は、この情報に基づいてトラブル対策を開始することができます。インストールする前のRequirementsとエラーコードを分析する頻繁に遇われたエラーコードを参照してください。

3.4.17.4 インストール履歴

[リモートインストール] タブの [インストール履歴] タブには、タスクとその属性のリストがあります。[インストール履歴] タブには、進行中のタスク、実行待ちのタスク、完了したタスクが表示されます。ここでは、表示されるアイテムの数を変更できるほか、リストにあるタスクを右クリックして管理と保守の各種オプションを使用できます。[表示するアイテム数] プルダウンメニューを使用してページあたりの表示アイテム数を選択でき、隣接するナビゲーションボタンを使用してページを切り替えられます。

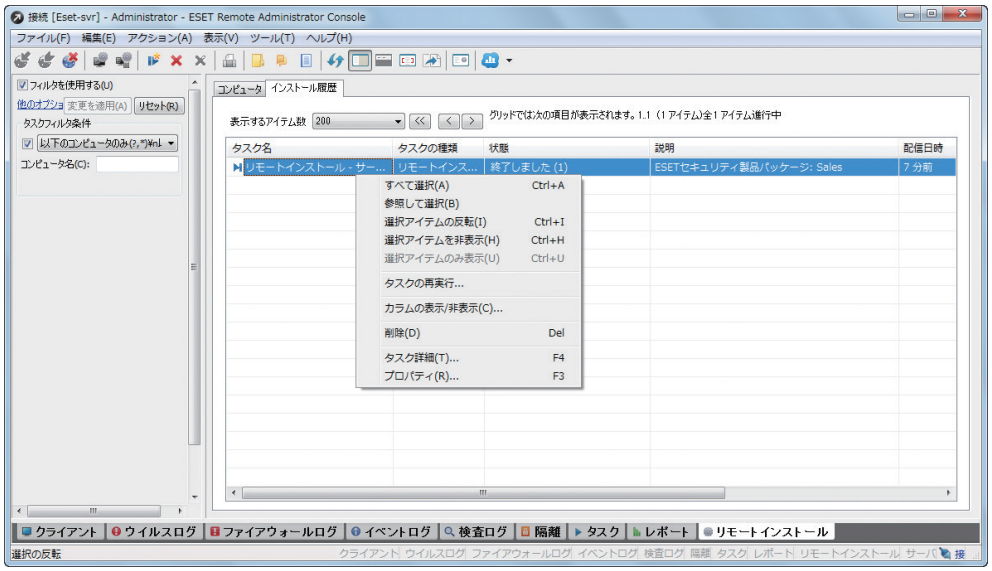
[インストール履歴] タブに示された情報をフィルタ処理することもできます。左側のペインにある [フィルタを使用する] オプションをチェックして、フィルタをオンにします。続いて [タスクフィルタ条件] をチェックして、フィルタの条件を設定し、[コンピュータ名:] フィールドにコンピュータ名を入力します。コンピュータ名には、ワイルドカードも使えます。[リセット] ボタンをクリックすると、フィルタ条件を削除し、フィルタ処理を無効にできます。

タスク名	タスク名、事前に定義されたタスクはタスクタイプと同じです。
タスクのタイプ	タスクのタイプ、より多くの情報については、タスクを参照してください。
状態	現在タスクの完成状態。
説明	タスクアクションの簡単説明。
展開する日付	受け入れまでの時間と経過した時間。
受信日付	タスクの実行時点から受け入れまでの時間と経過した時間。
コメント	インストールタスクに割り当てられた注意。

インストールタスクをダブルクリックすると、[プロパティ] ウィンドウが現れます。

●タスクの再実行

[リモートインストール] タブの [インストール履歴] タブにあるタスクをもう一度実行する場合は、目的のタスク(または選択した複数のタスク)を右クリックし、コンテキストメニューから [タスクの再実行...] を選択します。[タスクの再実行] ウィザードが表示されるので、[続行] をクリックすれば [コンピュータのログオン設定] 画面に進むことができます。または、[続行] をクリックする前に実行するタスクを変更できます。



再実行するどのタスクも、[インストール履歴] タブに新しいレコード(行)を生成します。タスクが警告付き完了の状態で終了する場合、そのタスクをダブルクリックし、[プロパティ] ウィンドウで [詳細] タブに切り替え、[状態テキスト] で詳細を確認します。[状態テキスト] がトリミングされている場合、マウスカーソルを重ねるだけでテキスト全体が現れます。

3.5 ERA Consoleのオプション

ERA Consoleは、[ツール] -> [コンソールオプション] メニューで設定できます。

3.5.1 [接続]

ERA Consoleの各種設定にアクセスするには、ERACのメインメニューの[ツール]->[コンソールオプション]をクリックするか、[ファイル] -> [接続の編集] をクリックします。このタブは、ERACからERASへの接続を設定する場合に使用します。詳細については、「ERASへの接続」を参照してください。

[接続] タブでは、接続先サーバーを選択でき、さらにERA Consoleの起動時にそのサーバーに接続するかどうかを指定できます。ERAConsoleが接続できるサーバーは、一度に1つだけです。複製サーバーを追加するには、[ツール] -> [サーバオプション] -> [複製設定] メニューで複製を設定する必要があります。

NOTE

ERA Serverに接続するポートは、[ツール]->[サーバオプション]->[その他の設定]でカスタマイズできます(「[その他の設定]」を参照)。

[追加/削除]
新しいERA Serverの追加、または既存のサーバーの変更に使用します。このオプションをクリックすると、[接続サーバの編集]ウィンドウが開きます。新規接続を追加するには、IPアドレスまたはサーバーのホスト名、接続で使用するポート、およびコメント(オプション)を入力します。[追加/保存] ボタンをクリックして、このウィンドウの上部にあるサーバーリストに接続を追加します。

コンソールのスタートアップ時に、選択したサーバへ接続する	あらかじめ指定された ERA Server にコンソールが自動的に接続します。
コンソールのスタートアップ時に、接続に失敗した場合、メッセージを表示する	通信エラーが発生した場合、警告が表示されます。

3.5.2 [カラム－表示/非表示]

このタブでは、個々のタブに表示する属性（カラム）を指定できます。変更はカスタム表示モード（[クライアント] タブ）に反映されます。他のモードを変更することはできません。

カラムを特定のタブに表示するには、タブの一覧でタブ名をクリックし、表示するカラムを選択します。

対象ペイン	表示するカラムを変更するペインを選択します。
表示するカラムの選択	ペインに表示するカラムを選択します。必要な情報がすべてペインに含まれるように注意して選択しますが、同時にデータの透過性を維持する必要があります。
すべてクリア	選択したペインの［表示するカラムの選択］ウィンドウで、チェックボックスをすべてオフにします。
すべて設定	選択したペインの［表示するカラムの選択］ウィンドウで、チェックボックスをすべてオンにします。
既定	選択したペインの［表示するカラムの選択］ウィンドウで、チェックボックスをすべてリセットして既定値に戻します。
すべて既定値に戻す	すべてのペインの［表示するカラムの選択］ウィンドウで、チェックボックスをすべてリセットして既定値に戻します。

3.5.3 [配色]

このタブでは、さまざまな色をシステム関連の特定のイベントに関連付けて、問題があるクライアントをわかりやすく表示できます（状況に応じた強調表示）。たとえば、ウイルス定義データベースの日付が多少古いクライアント（[クライアント：1つ前のバージョン]）を、古いデータベースを使用しているクライアント（[クライアント :古いバージョン、もしくはN/A]）と区別できます。

[ペインとカラム] リストで、ペインとカラムの色を選択して割り当てます。次に、表示色を選択します。

NOTE

[クライアント：古いバージョン、もしくはN/A] の色が使用されるのは、クライアント上のESET Endpoint Securityウイルスデータベースのバージョンが登録されていない場合やサーバーより古い場合です。この色は、サーバー上のESETセキュリティ製品のバージョンが、クライアントより古い場合、または登録されていない場合にも、使用されます。

[クライアント :最終アクセス] では、この配色を使用する間隔を指定できます。

3.5.4 [パス]

ERA Consoleの各種設定にアクセスするには、ERACのメインメニューの[ツール]->[コンソールオプション]をクリックします。

[パス]タブでは、ERA Consoleが作成したレポートの保存先を指定できます。レポートの作成と表示の詳細については、「[レポート]」を参照してください。

3.5.5 [日付 /時刻]

[日付 /時刻] ペインでは、ERA Consoleの詳細なオプションをカスタマイズできます。また、ERA Consoleウィンドウに表示するすべてのレコードで使用する時刻書式を、ここで選択することもできます。

絶対	絶対時間（例 :"14:30:00"）がコンソールに表示されます。
相対	相対時間（例 :"2 週間前 "）がコンソールに表示されます。
地域	Windows の設定から取得した地域設定に従ってコンソールに時間が表示されます。
UTC時間をローカルタイムに変換する（ローカルタイムを使用）	このチェックボックスをオンにすると、時間が現在地のローカル時刻に変換されます。オンにしていない場合は、GMT-UTC 時間が表示されます。

3.5.6 ペイン

[ペイン] タブでは、ERA Consoleで表示するタブ/ペインを選択します。

[表示ペイン] セクションで、ERA Consoleの下部に表示するペイン/タブを選択し、[OK] をクリックします。

NOTE

・ERA Consoleの [表示] メニューで関連する項目をクリックすると、非表示のタブも表示に切り替わります。
・[タブを非表示にする] をクリックすれば、タブ／ペインリストのコンテキストメニューからタブを直接非表示にできます。
・すべてのタブを非表示にすることはできません。少なくとも1つのタブは表示したままにしておく必要があります。

3.5.7 [その他の設定]

[その他の設定] ペインでは、ESET ERA Consoleの詳細なオプションを設定できます。

● [フィルタ設定]

[変更を自動的に適用する]

有効にすると、個々のタブでフィルタ設定を変更するたびに、そのフィルタ設定によって新しい出力が生成されます。無効にすると、[変更を適用] をクリックした場合にのみフィルタリングが実行されます。

NOTE

ERA ConsoleをERA Serverに常時接続するように管理者のコンピュータで設定している場合は、[最小化した際、タスクバーに表示する] オプションを有効にし、使用していないコンソールを最小化しておくことをお勧めします。問題の発生時には、タスクトレイアイコンが赤くなります。この場合、管理者は対処する必要があります。また、[問題のあるクライアントが存在する場合、タスクトレイのアイコン色を変更する] オプション（アイコンの色の変化をトリガするイベント）を調整することをお勧めします。

● [Remote Administratorのアップデート]

新しいバージョンのESET Remote Administratorがないかをチェックできます。既定値の [毎月] のままにしておくことをお勧めします。新しいバージョンが入手できる場合、プログラムの起動時にERA Consoleに通知が表示されます。

● [システムトレイ設定]

タスクトレイアイコンを表示する	ERA Console が Windows のタスクトレイアイコンとして表示されます。
最小化時にタスクバーに表示する	最小化した ERA Console ウィンドウに Windows のタスクバーからアクセスできます。
問題のあるクライアントが存在する場合、ハイライトされたタスクトレイアイコンを使用する	このオプションを［編集］ボタンと組み合わせて使用し、タスクトレイアイコンの色の変化をトリガするイベントを定義します。
管理対象外のコンピュータが検出された場合ハイライトされたタスクトレイアイコンを使用する	管理対象外のコンピュータが検出されると、タスクトレイアイコンの色が変化します。

NOTE

無視リストが更新された場合、既定の検索タスクが終了した場合、クライアントが新たに追加された場合、またはクライアントが削除された場合、システムトレイアイコンも更新されます。ただし、更新までには、5 ～ 15秒間の遅延があります。

自動更新を使用する	個々のタブのデータを、指定した間隔で自動的に更新します。
グリッドラインを表示する	このオプションをオンにすると、すべてのタブの個々のセルをグリッドラインで区切ることができます。
クライアントを「サーバ/コンピュータ/MAC」ではなく、「サーバ/名前」で表示する	一部のダイアログウィンドウでのクライアントの表示モードが変更されます（[新規タスク] など）。このオプションでは表示のみが変更されます。
ネットワークアクションの実行時にIPアドレスではなくホスト名を使用する	クライアントでネットワークアクションを実行する（クライアントタブセクションを参照）ときに、IP アドレスではなくホスト名を使用します。
オプション情報メッセージの表示	情報を伝えるメッセージすべての無効（[すべて非表示]）と有効（[すべて表示]）を切り替えます。このオプションが有効な場合、ERA Console に下線を引いた青色のメッセージが表示されます。これらのメッセージをクリックするとポップアップウィンドウが開き、製品の使用に関するヒントが表示されます。

3.6 アクセス権限

ERAには既定で2つのアカウントが用意されています。

●Administratorでは、すべての機能および設定を完全に制御できるほか、接続されているすべてのクライアントワークステーションを管理することができます。

●Read-Onlyは、ERASに接続しているESETクライアントソリューションの状態を表示する場合に適しています。クライアントワークステーション用のタスクの作成、インストールパッケージやリモートインストールの作成などはできません。ライセンスマネージャ、ポリシーマネージャ、および通知マネージャにアクセスすることもできません。

ERASに接続するためのパスワードは、どちらの表示モードに関しても設定できます。パスワードは、一部のユーザーにはERASに対する完全なアクセス権を付与し、その他のユーザーには読み取り専用アクセス権を付与する場合に特に便利です。パスワードを設定するには、ユーザマネージャーツールを使用します。

3.7 ESET Configuration Editor

ESET Configuration EditorはERACの重要なコンポーネントであり、さまざまな目的で使用します。最も重要な目的は次の作成操作です。

●インストールパッケージで使用するコンフィグレーションの作成

●タスクまたはポリシーとしてクライアントに送信するコンフィグレーションの作成

●通常の（.xml形式の）コンフィグレーションファイルの作成

Configuration EditorはERACを構成するコンポーネントであり、その本体はcfgedit.exeファイルです。

管理者は、Configuration Editorを使用して、ESETセキュリティ製品で使用可能なさまざまなパラメータをリモートで設定できます。特に、クライアントワークステーションにインストールしたセキュリティ製品を対象とします。また、設定を.xmlファイルにエクスポートして、ERACでのタスクの作成や ESET Endpoint Securityへの設定のローカルインポートなど、後でさまざまな目的に使用することもできます。

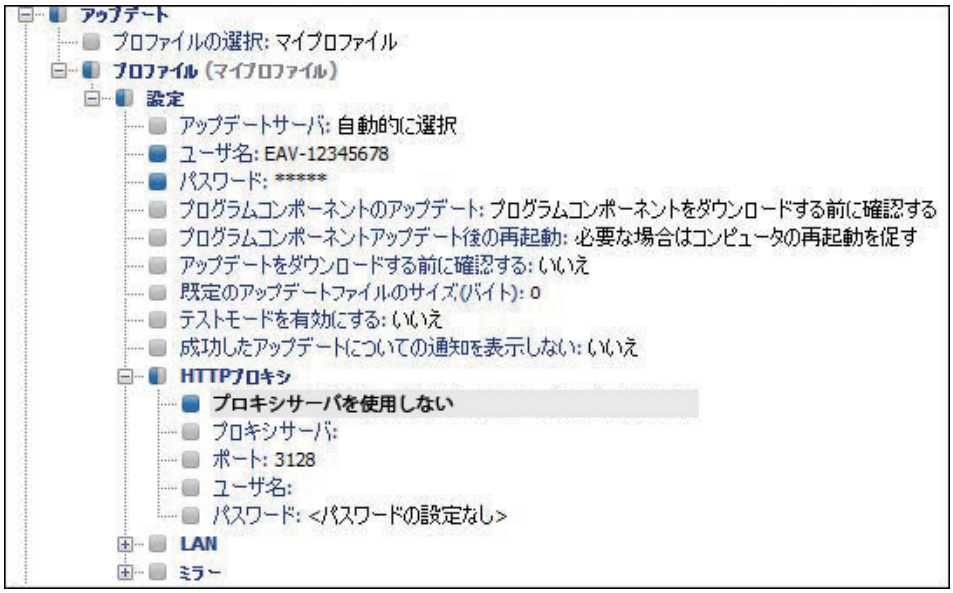
Configuration Editorで使用する構造は、ツリー形式の構造に設定を保存した.xmlテンプレートです。このテンプレートはcfgedit.exeファイルに保存されています。設定項目等の追加に対応するために、ERASおよびERACを定期的にアップデートすることをお勧めします。

3.7.1 コンフィグレーションの階層化

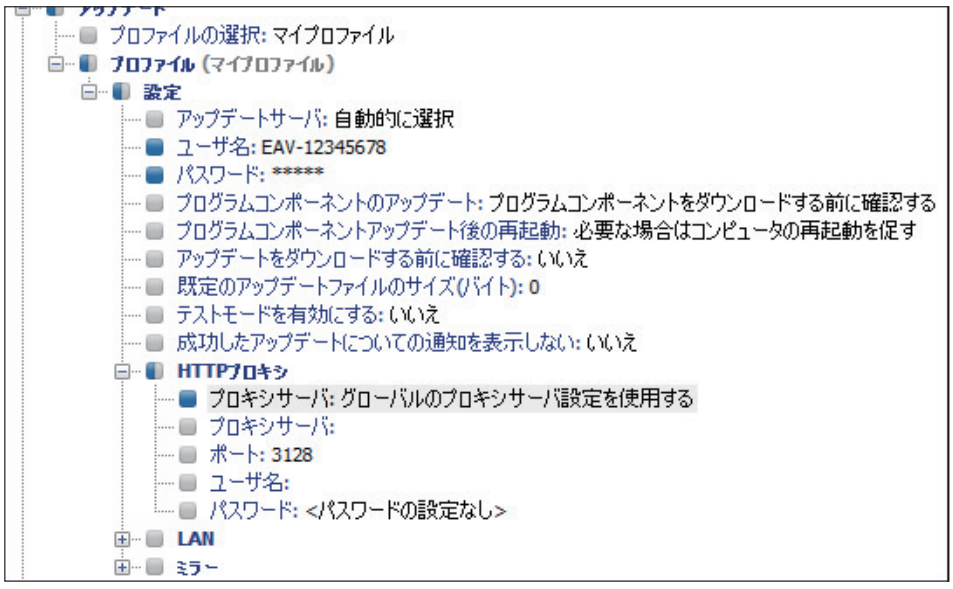
Configuration Editorで値を変更すると、変更箇所に青いシンボル■が表示されます。グレーのアイコン■が表示されたエントリは変更されていないので、.xml出力のコンフィグレーションファイルには書き込まれません。

クライアントにコンフィグレーションを適用する際、.xml出力のコンフィグレーションファイルに保存された変更(■)のみが適用されます。それ以外の項目はどれも変更されません。この動作によって、それまでの変更を維持したまま、内容が異なるコンフィグレーションを段階的に適用できます。

次の図に例を示します。このコンフィグレーションでは、ユーザ名 EAV-12345678とパスワードが挿入され、プロキシサーバーの使用が禁止されています。



2回目にクライアントに送信されるコンフィグレーション(次の図を参照)では、ユーザ名 EAV-12345678やパスワードなど、それまでの変更が保持されます。また、プロキシサーバーの使用が許可され、サーバーのアドレスとポートが定義されています。



3.7.2 キーコンフィグレーションエントリ

このセクションでは、クライアント製品でよく利用される設定について説明します。

● [ESETカーネル] > [設定] > [リモート管理]
ここでは、クライアントコンピュータとERASとの間の通信を有効にすることができます（[リモート管理サーバに接続する]）。ERASの名前またはIPアドレスを入力します（プライマリ/セカンダリサーバアドレス）。[サーバへの接続間隔] オプションは、既定値の10分のままにしておく必要があります。テストの目的であれば、この値を0に設定してもかまいません。その場合は、10秒ごとに接続が確立されます。パスワードを設定する場合は、ERASで指定したパスワードを使用してください。詳細については、「[保護] タブ」の [クライアントのパスワード] オプションを参照にしてください。パスワード設定の追加情報については、ここでも説明します。

● [ESETカーネル] > [設定] > [ライセンスキー]
クライアントコンピュータでは、ライセンスキーの追加や管理は不要です。ライセンスキーはサーバー製品でのみ使用します。

● [ESETカーネル] > [設定] >ESET Live Grid
ここでは、不審なファイルを分析のためにESETのラボに提出するときに使用するESET Live Grid早期警告システムの動作を定義します。ESETソリューションを大規模ネットワークに展開する場合は、[不審なファイルの提出] オプションと [匿名の統計情報を提出する] オプションが特に重要です。それぞれを [分析のために提出しない] または [いいえ] に設定した場合、ESET Live Gridシステムは完全に無効になります。ユーザーの操作を必要とせずに自動的にファイルを提出するには、それぞれで [通知せずに提出する] および [はい] を選択します。インターネット接続にプロキシサーバーを使用している場合は、[カーネル] -> [設定] -> [プロキシサーバ] で接続パラメータを指定します。
既定では、クライアント製品はERASに不審なファイルを提出し、そこからESETのサーバーにファイルが提出されます。そのため、ERASでプロキシサーバーを正しく設定する必要があります（[ツール] -> [サーバオプション] -> [詳細] -> [詳細設定を編集] -> [ERA Server] -> [設定] -> [プロキシサーバ]）。

● [ESETカーネル] > [設定] > [設定パラメータの保護]
管理者はパラメータ設定をパスワードで保護できます。パスワードを設定すると、クライアントワークステーションでパラメータ設定にアクセスするときにそのパスワードが要求されます。ただし、パスワードは、ERACによるコンフィグレーションの変更には影響しません。

● [ESETカーネル] > [設定] > [スケジューラ/プランナー]
このキーにはスケジューラ/プランナーのオプションがあるので、管理者は定期的なウイルス検査のスケジュールなどを設定できます。

▸▸▸ NOTE
すべてのESETセキュリティソリューションには、事前定義されたタスク（定期的な自動アップデートや起動時の重要なファイルの自動チェックなど）が既定で用意されています。

● [カーネル] > [設定] > [ユーザインタフェースの既定値]
[ユーザインタフェースの既定値] の設定（[スプラッシュ画面を表示する] / [スプラッシュ画面を表示しない]）は、クライアントの既定の設定に対する変更にのみ適用されます。クライアントの設定はユーザー別に管理され、リモートで変更することはできません。この設定をリモートで変更するには、[ユーザー設定を無視するオプションを [はい] に設定する必要があります。[ユーザー設定を無視する] オプションは、5.0以降のESETセキュリティ製品を実行する

クライアントのみで使用可能です。

●アップデート（機能）

Configuration Editorのこのブランチでは、アップデートプロファイルを適用する方法を定義できます。通常は、事前定義されたプロファイル［マイプロファイル］を修正し、［アップデートサーバ］、［ユーザ名］、および［パスワード］の設定を変更すれば済みます。アップデートサーバーを［自動的に選択］に設定すると、すべてのアップデートがESETのアップデートサーバーからダウンロードされます。この場合は、購入時に提供されたユーザー名とパスワードを指定してください。ローカルサーバー（ミラー）からアップデートを受け取るようにクライアントワークステーションを設定する方法については、「ミラーサーバー」を参照してください。スケジューラの使用の詳細については、「スケジューラ」を参照してください。

▸▸▸ NOTE

ノートパソコンなどのポータブルデバイス向けに、2つのプロファイルを設定できます。1つはミラーサーバーからアップデートを受け取るためのプロファイルで、もう1つはESETのサーバーからアップデートを直接ダウンロードするためのプロファイルです。詳細については、このドキュメントの最後にある「ノートパソコン向けの組み合わせアップデート」を参照してください。

[Chapter 4]
ESET クライアントソリューションのインストール

4.1 インストールについて

ここでは、Microsoft Windowsオペレーティングシステムへの ESETクライアントソリューションのインストールについて説明します。インストールは、ワークステーションで直接実行できるほか、ERASからリモートで実行することもできます。ここでは、リモートインストールのさまざまな方法についても説明します。

NOTE

サーバーへのESET製品のインストールでリモートインストール機能を使用することは、技術的には可能ですが、お勧めしません（ワークステーションにのみ使用してください）。

4.2 手動インストール

手動インストールは、ESET ライセンス製品をインストールするコンピュータのAdministrator権限が必要になります。この方法は、小規模なネットワークやERAを使用しないシナリオに適しています。

ERAには、手動インストールの方法がいくつか用意されています。

●手動インストール(Windowsの場合)

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(.msi)をそのまま利用してインストールを行います。クライアントPC 用ソフトウェアの各種設定は、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、接続設定など最低限必要となる設定を、各自、ソフトウェア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PC 用ソフトウェア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PC 用ソフトウェアからのエクスポートを利用した場合、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。
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(.exe) ●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。

※各インストーラーは、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。

●手動インストール(Mac OS Xの場合)

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。

●手動インストール(Androidの場合)

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)	Android端末の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。

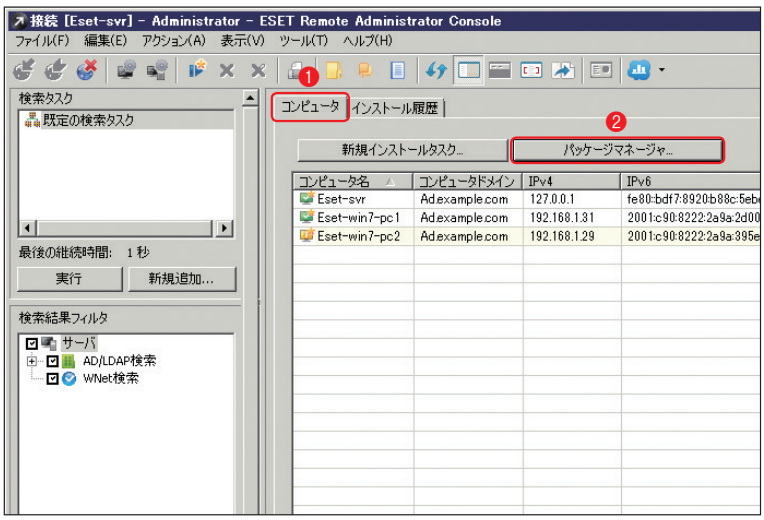
4.2.1 設定組み込み済みインストーラーの作成手順（Windows編）

ここでは、設定組み込み済みインストーラーの作成手順を紹介します。

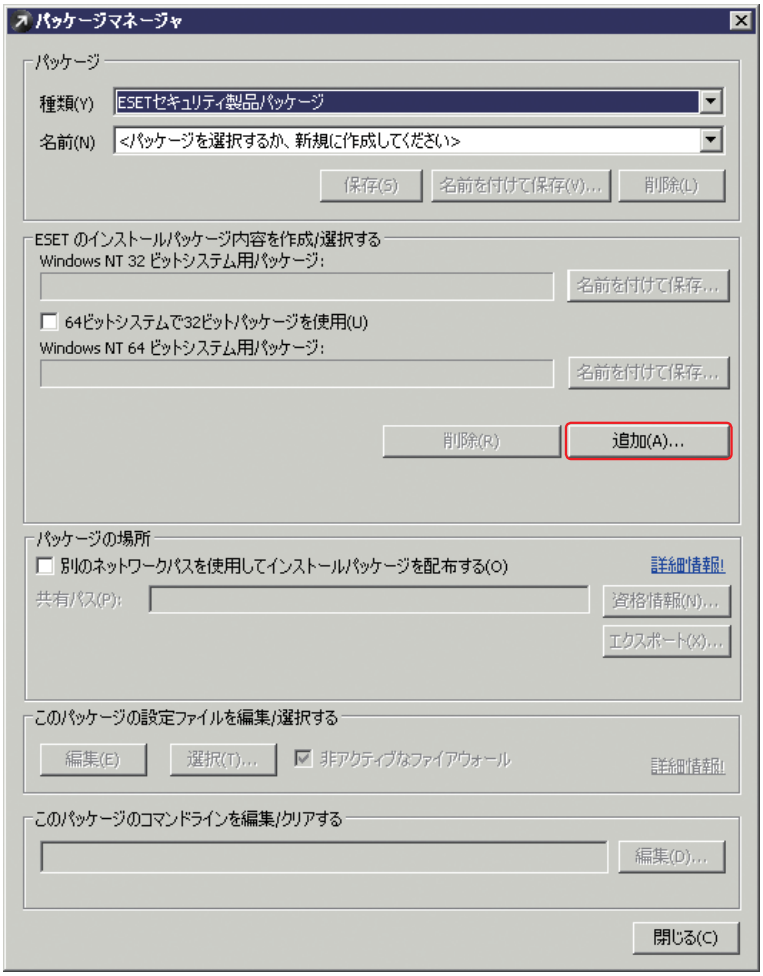
1 インストーラー(.msi) を準備します。Windows用プログラム(ESET Endpoint SecurityまたはESET Endpoint アンチウイルスなど)のインストーラーを、ERACをインストールしたコンピュータの任意のフォルダーに保存します。インストーラー(.msi)は、弊社ユーザーズサイトからダウンロードできます。インストーラー(.msi)のダウンロード手順の詳細については、ESETライセンス製品 ご利用の手引をご参照ください。

2 ERASにログオンします。ERACを起動し、ERASにログオンします。

3 [リモートインストール] タブをクリックし、[リモートインストール] ペインを開きます。

4 

❶ [コンピュータ] タブをクリックし、❷ [パッケージマネージャ] をクリックして [パッケージマネージャ] ウィンドウを開きます。

5 

[パッケージマネージャ] ウィンドウが開きます。[追加] ボタンをクリックします。

6 [ESETアンチウイルスのインストーラー作成] ダイアログが開きます。[...] ボタンをクリックします。

CAUTION

[ウェブからダウンロード] ボタンを利用してインストーラーをダウンロードしないでください。このボタンをクリックしてダウンロードしたインストーラーは、弊社のサポート対象外となります。インストーラーのダウンロードは、必ず、弊社ユーザーズサイトから行ってください。

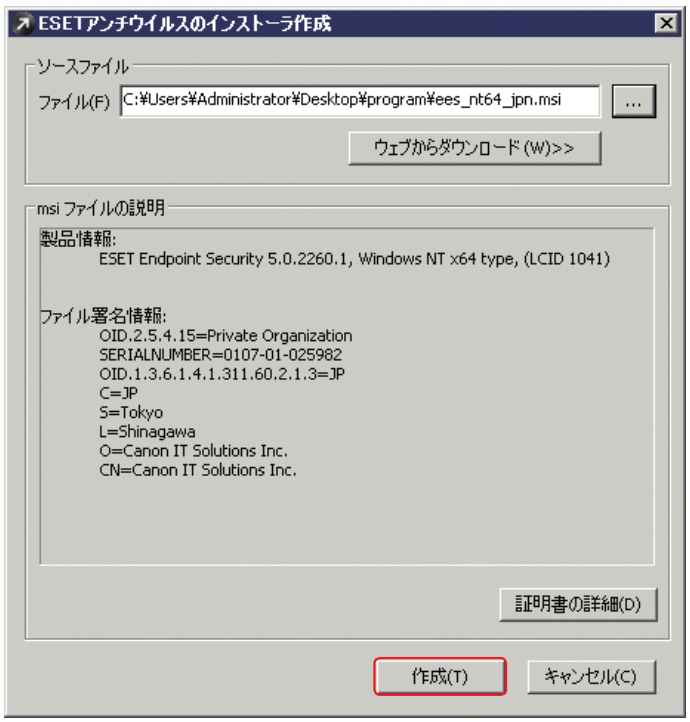
7 [開く] ダイアログが開きます。登録するインストーラーを選択し、[開く] ボタンをクリックします。

▸▸▸ NOTE

Windows用プログラムのインストーラーには、以下の6種類があり、拡張子は「.msi」です。

製品	プラットフォーム	ファイル名
ESET Endpoint Securityのインストーラー	32bit版	ees_nt32_JPN
	64bit版	ees_nt64_JPN
ESET Endpoint アンチウイルスのインストーラー	32bit版	eea_nt32_JPN
	64bit版	eea_nt64_JPN
ESET File Security for Microsoft Windows Serverのインストーラー	32bit版	efsw_nt32_JPN
	64bit版	efsw_nt64_JPN

8

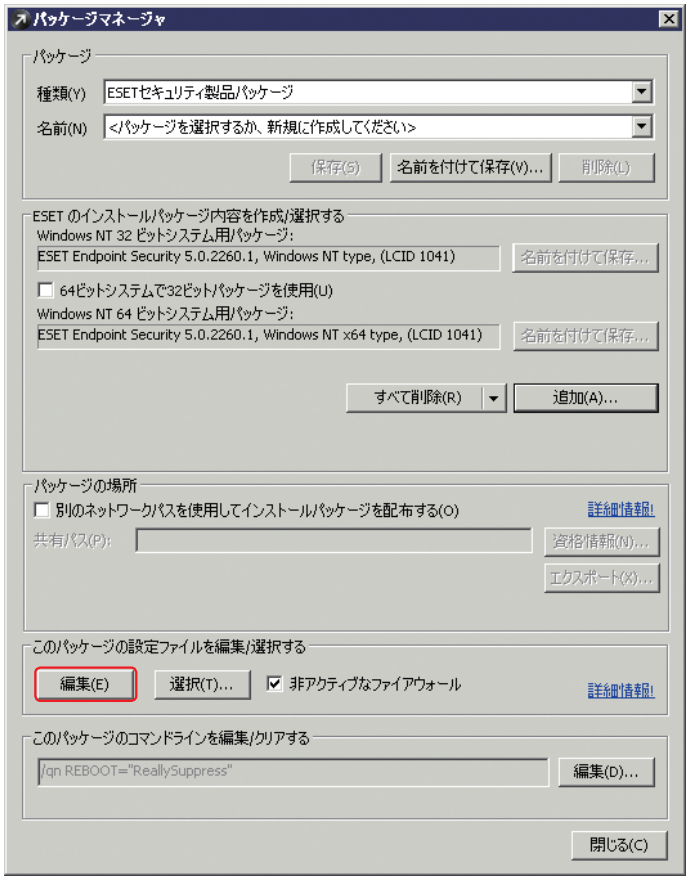


[ESETアンチウイルスのインストーラー作成] ダイアログに戻ります。選択したファイルの内容を確認し、[作成] ボタンをクリックします。

NOTE

32bit版インストーラーと64bit版インストーラーを同時に編集したいときは、手順5～8の作業を繰り返し、32bit版/64bit版両方のインストーラーを登録します。

9



[ESETインストールパッケージの編集] ダイアログに戻ります。[編集] ボタンをクリックします。

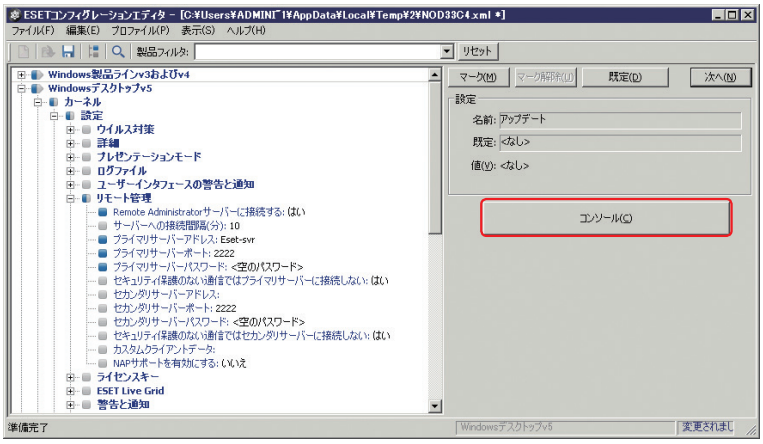
NOTE

[選択] ボタンをクリックすると、あらかじめ作成しておいた設定ファイルを利用して設定組み込み済みインストーラーを作成できます。[ファイルを開く] ダイアログが開いたら、作成に利用する設定ファイルを選択し、[開く] ボタンをクリックします。その後、手順13に進んでください。

10 32bit版/64bit版両方のインストーラーを登録した場合は、[プラットフォームを選択する] ダイアログが表示されます。32bit版/64bit版両方に設定を反映するときは、[変更を保存した際、両方のプラットフォームを更新する] にチェックを入れ、[OK] ボタンをクリックします。

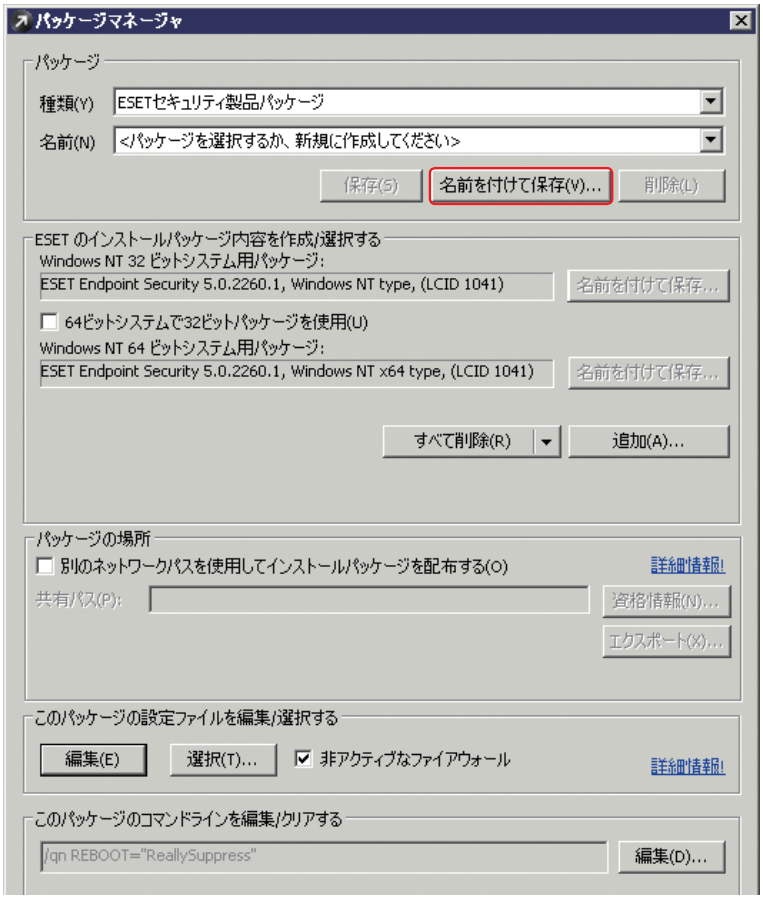
NOTE

どちらか一方のみ更新したい場合は、[変更を保存した際、両方のプラットフォームを更新する] のチェックを外し、ドロップダウンリストから反映したいプラットフォームを選択して[OK] ボタンをクリックします。

11 

ESET コンフィグレーションエディタが起動します。ツリーから設定を変更する項目を選択し、右側のウィンドウで設定を行います。すべての設定が終わったら、[コンソール] ボタンをクリックします。

12 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。

13 

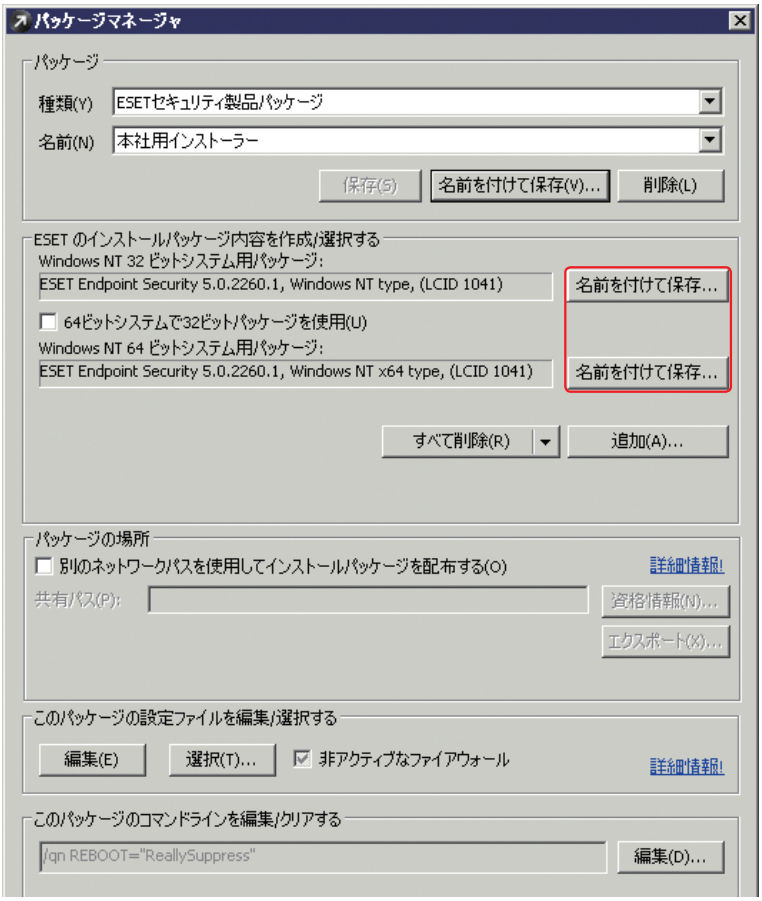
インストールパッケージの名前を保存します。[名前を付けて保存] ボタンをクリックします。

14 [名前を付けて保存] ダイアログが開きます。インストーラーの名前を入力し、[保存] ボタンをクリックします。設定を組み込んだパッケージの作成がバックグラウンドで実行されます。

CAUTION

インストールパッケージの作成中は、ERACの他の操作ができなくなりますのでご注意ください。

15

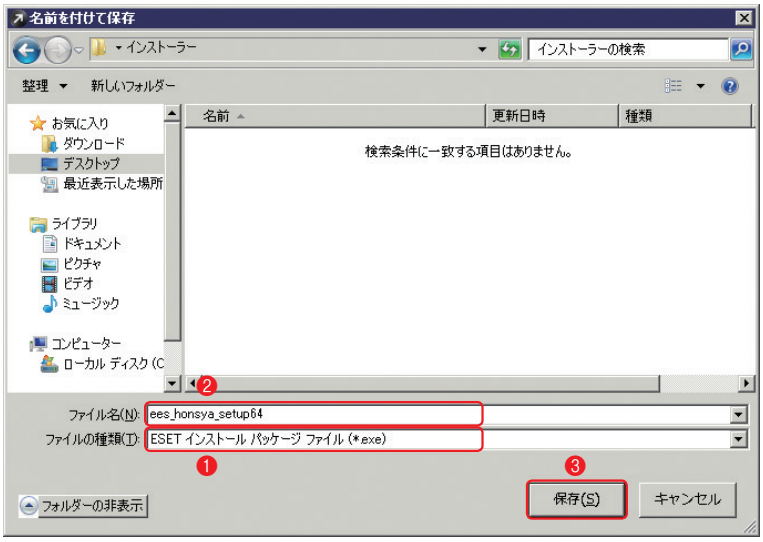


作成した設定組み込み済みインストーラーの保存を行います。保存したいパッケージの [名前を付けて保存] ボタンをクリックします。リモートインストールで利用するインストーラーを作成している場合、手順15、16の作業は不要です。

NOTE

[このパッケージのコマンドラインを編集/クリアする] は、リモートインストール時には利用できますが、設定組み込み済みインストーラーでは利用できません。

16



[名前を付け保存] ダイアログが開きます。❶ファイルの種類を「*.exe」に設定し、❷ファイル名を入力して、❸[保存] ボタンをクリックします。32bit版/64bit版両方の作成を行った場合は、手順15、16の作業を繰り返し、両方のインストーラーを保存します。

17 設定組み込み済みインストーラーの作成を終了します。[閉じる]ボタンをクリックし、[パッケージマネージャ]ウィンドウを閉じます。

コラム

インストール用バッチファイルの作成方法

保存したexeファイルを直接実行すると、ウィザードが表示されます。設定組み込み済みイントーラーによる手動インストールを実施するときは、インストール用バッチファイル(「.bat」のファイル)を作成しておくと、クライアント用プログラムのインストールがスムーズに行えます。インストール用バッチファイルは、Windowsに標準で搭載されている「メモ帳」などのテキストエディターを利用して作成できます。実際のインストール作業は、作成したインストール用バッチファイルと設定組み込み済みインストーラーをすべて1つのフォルダーに保存します。次にこれをクライアントPCにコピーし、インストール用バッチファイルを実行します。なおバッチファイルは、必ず「setupess32.bat」のような拡張子に「.bat」を付けたファイル名で保存してください。また、インストール用バッチファイルに指定できるオプションスイッチの詳細については、●●ページをご参照ください。

バッチファイルの作成例

●バッチファイルの内容

(設定したファイル名).exe /qb! reboot="force"
(半角スペース)

●設定内容

(設定したファイル名).exe	作成した設定組み込み済インストーラーのファイル名です。利用するインストーラーのファイル名に合わせてください。
qb!	インストールの進捗状況を表示するオプションです。
reboot="force"	インストール完了後にシステムの再起動を行うオプションです。

4.2.2 設定組み込み済みインストーラーの作成手順（Mac OS X編）

ここでは、付属のインストーラー(.dmg)を使って、設定組み込み済みインストーラー(.pkg)を作成する手順を説明します。

1 インストーラー(.dmg)をダブルクリックします。

2 [インストール]をダブルクリックします。

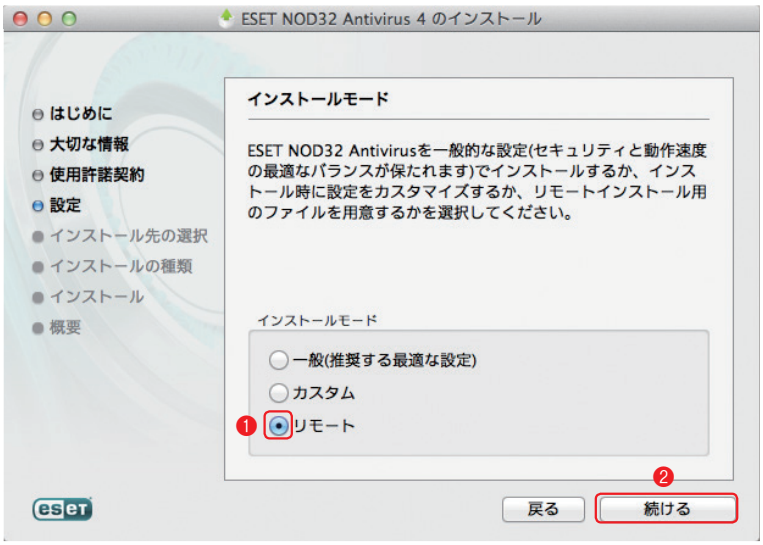
3 インストーラーが起動します。[続ける]ボタンをクリックします。

4 「はじめに」が表示されます。内容を確認し、[続ける]ボタンをクリックします。

5 「大切な情報」が表示されます。内容を確認し、[続ける]ボタンをクリックします。

6 「使用許諾契約」が表示されます。内容を確認し、[続ける]ボタンをクリックします。

7 「使用許諾契約」に同意します。[同意する]ボタンをクリックします。

8 

インストールモードを選択します。❶[リモート]にチェックを入れ、❷[続ける]ボタンをクリックします。

9 [アップデートサーバーリスト]ダイアログが表示されます。[編集]ボタンをクリックします。

10 アップデートサーバーの情報を登録します。[アップデートサーバー] 欄に接続先のサーバー情報を入力し、[追加] ボタンをクリックします。

NOTE

社内に設置されたミラーサーバーを利用する場合は、IPアドレス(またはホスト名) とポート番号を「http://xxx.xxx.xxx.xxx:ポート番号」の形式で入力してください。

11 [アップデートサーバーリスト] に情報が登録されるので、[OK]ボタンをクリックします。

12 登録したアップデートサーバーを選択します。[アップデートサーバー] のドロップダウンメニューから手順11で登録した情報を選択し、[続ける] ボタンをクリックします。

NOTE

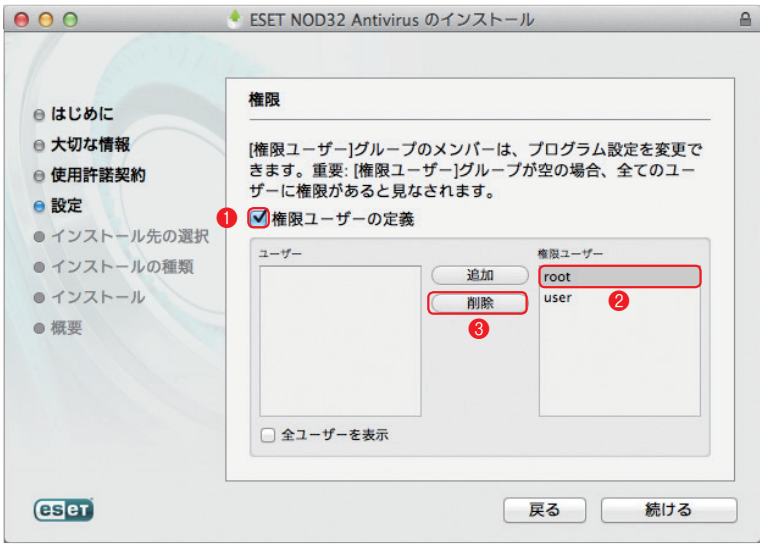
アップデートサーバーに接続認証が設定されているときは、「ユーザー名」「パスワード」の入力も行います。

13 プロキシサーバーを設定します。アップデートなどのHTTP通信がプロキシサーバーを経由する場合、この設定を行う必要があります。[システム設定を利用する (推奨)] にチェックが入っていることを確認し、[続ける] ボタンをクリックします。

14 管理サーバーの設定を行います。[リモート管理サーバの使用] にチェックを入れ、[リモート管理サーバ] 欄にIPアドレス (またはホスト名) を入力します。[続ける] ボタンをクリックします。

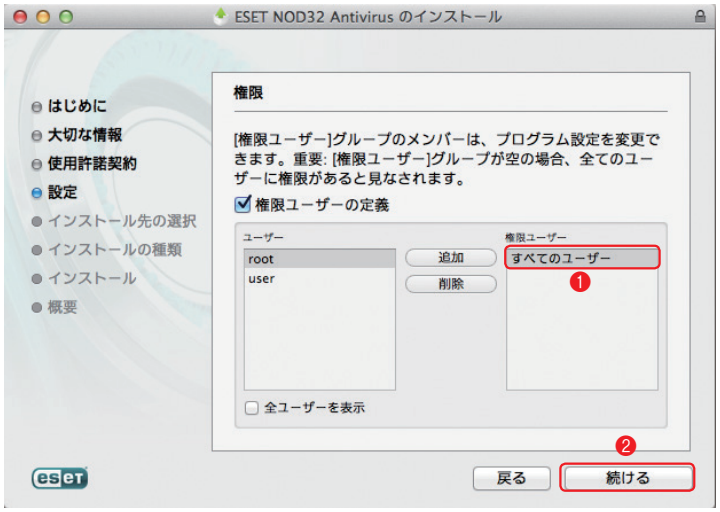
NOTE

管理サーバーを利用しない場合は、この設定を行う必要はありません。

15 

権限ユーザーの設定を行います。❶[権限ユーザーの定義] にチェックを入れます。❷「権限ユーザー」グループに登録されているユーザーをクリックし、❸[削除] をクリックします。この作業を繰り返し、すべてのユーザーを「権限ユーザー」グループから除去します。

16



❶「権限ユーザー」グループのユーザーをすべて除去すると「すべてのユーザー」に表示が変わります。❷[続ける] ボタンをクリックします。

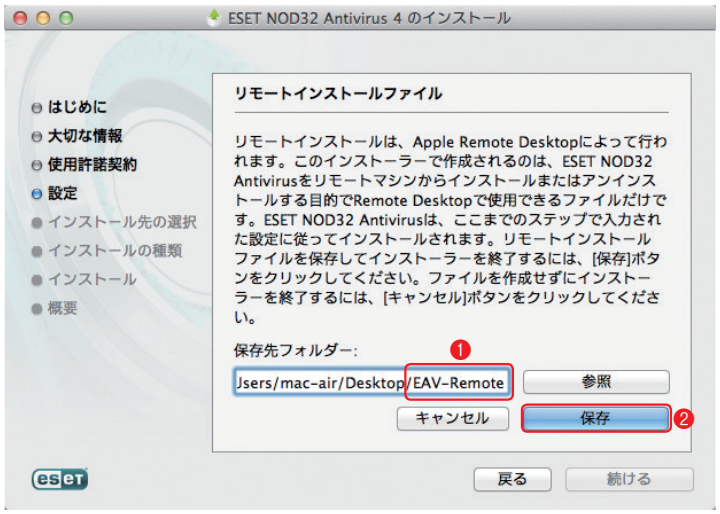
17 ThreatSense.Netの設定を行います。[ThreatSense.Net早期警告システムを有効にする] にチェックが入っていることを確認し、[続ける] ボタンをクリックします。

18 特殊なアプリケーションの設定を行います。ドロップダウンメニューから [望ましくない可能性があるアプリケーションの検出を有効にする] を選択し、[続ける] ボタンをクリックします。

19 保存先を設定します。[参照] ボタンをクリックします。

20 保存先を選択し、[開く] ボタンをクリックします。

21



[開く] ダイアログが開きます。❶入力された保存先をクリックして保存するフォルダー名を追加します。ここで入力した名称のフォルダーが保存先フォルダー内に新規作成されます。設定組み込み済みインストーラー(.pkg)は、このフォルダー内に保存されます。❷[保存] ボタンをクリックします。

NOTE

手順19で[参照] ボタンをクリックして保存先を選択した場合は、保存先フォルダー名の追加入力を行わないと、設定組み込み済みインストーラー(.pkg)の作成ができません。また、既定値で設定されている[/tmp]フォルダーは、Finderの既定値では表示されないフォルダーです。「/tmp」フォルダーを表示するには、メニューバーの[移動] をクリックし、[フォルダーへ移動] を選択して[/tmp] と入力して、[移動] ボタンをクリックします。

22 設定組み込み済みインストーラー（.pkg）が指定したフォルダー内に作成されます。「EAV4_Remote_Install.pkg」が、設定組み込み済みインストーラー（.pkg）です。「EAV4_Remote_Uninstall.sh」は、アンインストール用のシェルスクリプトです。

CAUTION

設定組み込み済インストーラー(.pkg)にはデジタル署名が追加されません。そのため、OS X v10.8 Mountain Lionのローカル環境にてこのインストーラーを使用される際は、一時的に「Gatekeeper」の機能を無効にする必要があります。

4.3 リモートインストール

ERAには、リモートインストールの方法がいくつか用意されています。

●リモートインストール(Windowsの場合)

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。
※リモートインストールの詳細については「ユーザーズガイド　導入・運用編」をご参照ください。

●リモートインストール(Mac OS Xの場合)

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。

4.3.1 要件

リモートインストールの基本要件は、信頼性の高いクライアントサーバー通信を提供する、適切に設定されたTCP/IPネットワークです。ERAを使用してクライアントソリューションをインストールすると、直接インストールする場合より、クライアントワークステーションに対する条件が厳しくなります。リモートインストールの場合は、下記の条件を満たす必要があります。

Windows

(1) クライアントコンピュータとERASがLAN経由で通信が可能なこと

(2) クライアントコンピュータが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) クライアントコンピュータがワークグループ環境のメンバの場合、各クライアントコンピュータ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) クライアントコンピュータのOSがWindows 2000/XP/Vista/7/8/10、Windows Server 2003/2008/2012であること

(5) クライアントコンピュータ側の通信ポートが通信可能な状態になっていること

※使用するポート番号については、下記Webページに記載がございます。併せてご覧ください。

[ETLR40004]ESET Remote Administratorで使用するポート番号について

http://canon-its.jp/supp/eset/etlr40004.html

(6) クライアントコンピュータで「Remote Registry」サービスが開始されていること

(7) クライアントコンピュータの共有フォルダおよびプリンター共有が有効になっていること

(8) クライアントコンピュータのフォルダオプションで「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。

(9) Windows Vista以降のOS(Windows Server 2003/2008/2012)の場合、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、コンピュータの管理者権限を持ったアカウントで動作させて下さい。

NOTE

最近のバージョンのMicrosoft Windows(Windows Vista、Windows Server 2008/2012およびWindows 7/8/10)ではセキュリティポリシーが強化され、ローカルシステムアカウントの権限が制限されました。これにより、ユーザーが特定のネットワーク操作を実行できない場合があります。ERAサービスをローカルユーザーアカウントで実行している場合は、特定のネットワーク設定でプッシュインストールの問題が発生する可能性があります(ドメインからワークグループにリモートでインストールするときなど)。Windows Vista、Windows Server 2008/2012、またはWindows 7/8/10を使用する場合、十分なネットワーキング権限を付与したアカウントでERAサービスを実行することをお勧めします。ERAを実行するユーザーアカウントを指定するには、[スタート]->[コントロールパネル]->[管理ツール]->[サービス]に移動します。リストからESET Remote Administrator Serverサービスを選択して、[ログオン]タブをクリックします。ESET Remote Administratorでは、この設定が詳細インストールのシナリオに埋め込まれているので、インストール時に[詳細]->[すべてカスタマイズ可能]を選択する必要があります。Windows Vista、Windows Server 2008/2012、またはWindows 7/8/10の対象ワークステーションでプッシュインストールを使用している場合は、ERA Serverと対象ワークステーションが同じドメインにあることを確認してください。管理者はWindows Vista、Windows 7/8/10とWindows Server 2008/2012へのUAC(ユーザーアクセス制御)を無効にすることをお勧めします。

Mac OS X
(1) リモートログイン (SSH共有) が有効であること
(2) 各クライアントコンピュータ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

特にネットワーク内にワークステーションが複数存在する場合は、インストールの前にすべての要件を確認することを強くお勧めします ([リモートインストール] タブで [コンピュータ] タブを選択し、該当するクライアントを右クリックしてコンテキストメニューの [プッシュインストールの診断] を選択します)。

WMIの要件
WMIリモートインストールメソッドでは次の要件を満たす必要があります。

(1) 対象のコンピュータで、WMIが有効であり、起動されている必要があります。既定では有効です。
(2) リモート接続に使用するユーザーアカウントに管理者権限がなければなりません。
(3) WMIの接続許可は、対象のコンピュータでのファイアウォール内でなければなりません。DCOM (分散コンポーネントオブジェクトモデル) の着信接続に対してポート135を有効にする必要があります。また、1024以降のいずれかのポート (通常では1026-1029) を有効にする必要があります。

既定のWindowsファイアウォールは、対象のマシンで次のコマンドを実行することで構成できます。

netsh firewall set service RemoteAdmin enable

(4) リモートコンピュータへの接続用アカウントはドメインアカウントであり、ローカルな管理者権限がなければなりません。アカウントがローカルアカウントである場合でもWMIは動作できますが、リモートシステムでは、ユーザーアカウント制御 (UAC) を無効にしてください。
詳細については、http://msdn.microsoft.com/en-us/library/aa826699%28v=vs.85%29.aspxを参照してください。

4.3.2 リモートプッシュインストール

このリモートインストール方法はリモートコンピュータにESET製品をリモートでプッシュインストールします。すべてのターゲットワークステーションはネットワーク接続されている必要があります。プッシュインストールを始める前に、弊社ユーザーズサイトからインストールファイルをダウンロードし、ESET Endpoint SecurityまたはESET Endpoint アンチウイルスインストールパッケージを作成します。事前に作成したコンフィグレーションファイルをインストールパッケージに含めることもできます。インストールの前に、「要件」を参照してください。

プッシュインストールを開始するには、次の手順を実行します。

1 「リモートインストール」ペインを開きます。

2 「コンピュータ」タブを開きます。「探索タスク」の「既定の検索タスク」を選択します。

3 「コンピュータ」タブに表示されているコンピュータの一覧から、インストール対象のコンピュータを選択します。

4 リモートプッシュインストールを行うコンピュータを選択し、[新規インストールタスク] ボタンをクリックします。
リモートプッシュインストールのためのウィザードが開始されます。

5 [新規インストールタスク] ウィンドウでは、新規インストールタスクタイプを選択します。既定では [Windows プッシュ] と [インストール] オプションが選択されています。[続行] ボタンをクリックすると、[コンピュータのログオンの設定] ダイアログが表示されます。

6 [コンピュータのログオンの設定] ダイアログでは、対象のコンピュータに対して管理者権限のある「ユーザ名」および「パスワード」を設定します。
個々のコンピュータに対して個別に「ユーザ名」および「パスワード」を設定する場合には、対象のコンピュータを選択して資格情報の [設定] ボタンをクリックします。すべてのコンピュータに対して共通の「ユーザ名」および「パスワード」を設定する場合には、[すべて設定]ボタンをクリックします。

7 [ログオン情報] ダイアログでは、「ユーザ名」および「パスワード」を入力します。
ドメインアカウントを利用する場合は、「ドメイン」を選択し、ドメイン名の入力を行います。
ドメインアカウントを利用しない場合は、「ワークグループ」を選択します。
「OK」ボタンをクリックして [コンピュータのログオンの設定] ダイアログに戻ります。

8 [次へ]ボタンをクリックして [タスクの設定] ダイアログに移ります。

9 [タスクの設定] ダイアログでは、対象のクライアントにインストールするパッケージを選択します。
「種類」では「ESETセキュリティ製品パッケージ」を選択します。
「名前」ではインストール対象にインストールするパッケージを選択します。
「時間設定」では、対象のクライアントにパッケージをインストールするタイミングを設定します。
すぐにインストールを開始する場合には、[今すぐタスクを実行する] を選択します。
指定のタイミングでインストールを開始する場合は [指定日時にタスクを実行する] を選択し、開始する日時を設定します。

10 [終了]ボタンをクリックしてウィザードを閉じます。

※タスクの状況は「リモートインストール」ペインの「インストール履歴」タブで確認できます。

▸▸▸ POINT

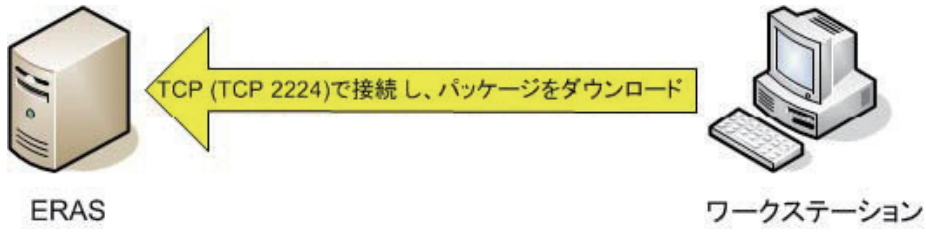
既定では、同時プッシュインストールスレッドの最大数は20に設定されています。この限度を超過する数のコンピュータにプッシュインストールタスクを送信した場合は、超過分のコンピュータに対するタスクが待ち行列に入れられ、スレッドが空くまで待機します。パフォーマンス上の理由のためにこの値を増やさないことをお勧めしますが、必要と判断した場合は、Configuration Editorで限度を変更できます（[ESET Remote Administrator]->[ERA Server]->[設定]->[リモートインストール]）。

リモートインストールプロセスの詳細は以下のとおりです。

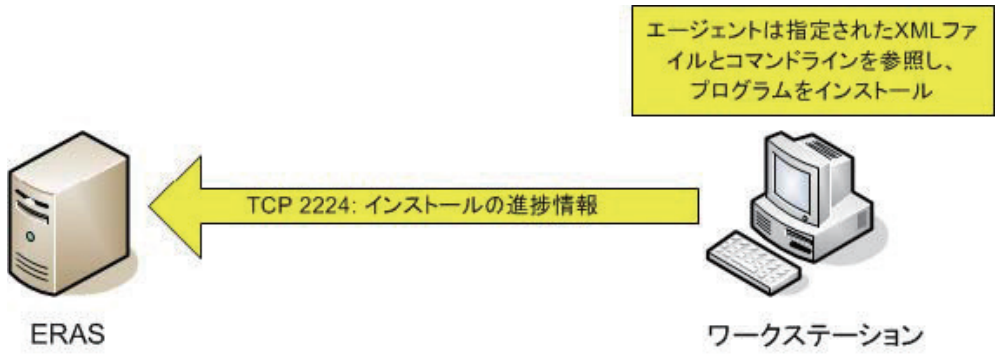
1 管理共有admin$を利用して、ERASからワークステーションにeinstaller.exeエージェントが送信されます。

2 エージェントがシステムアカウントの下でサービスとして起動します。

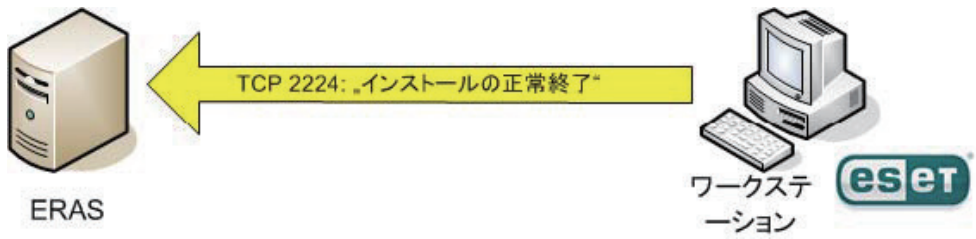
3 エージェントがその"親"であるERASとの接続を確立し、対応するインストールパッケージをTCPポート2224でダウンロードします。



4 手順2で定義した管理者アカウントの下で、エージェントがパッケージをインストールします。.xml形式の対応するコンフィグレーションとコマンドラインパラメータも適用されます。



5 インストールが完了した直後に、エージェントからERASにメッセージが返送されます。ESETセキュリティ製品によっては再起動が必要なものがあり、その場合は必要に応じて画面で再起動を求められます。



4.3.3 ログオンスクリプト/電子メールによるリモートインストール

ログオンスクリプトを利用したリモートインストールと電子メールを利用したリモートインストールの手順はほぼ同じです。ERAでは、ログオンスクリプトまたは電子メールを介してインストーラを実行できます。

4.3.3.1 ログオンスクリプトへのエクスポート

ログオンスクリプトでエージェント(einstaller.exe)を実行するように修正するには、テキストエディタを利用できます。また、エージェント(einstaller.exe)は、電子メールクライアントを使って電子メール添付ファイルとして送信できます。どちらの方式を使用する場合も、使用するエージェント(einstaller.exeファイル)が正しいことを確認しておいてください。

einstaller.exeを実行するには、現在ログオンしているユーザが管理者である必要はありません。必要な管理者のユーザ名、パスワード、およびドメインは、エージェントがERASから取得します。詳細については、「4.3.3.2 既定のログオン/ログオン情報」を参照してください。

4.3.3.1.1 ログオンスクリプトでeinstaller.exeへのパスを入力する

1 [リモートインストール]ペインを開き、[コンピュータ]タブを開きます。

2 [新規インストールタスク...]ボタンをクリックします。[新規インストールタスク]画面に進みます。

3 [エクスポート]を選択し、[続行]ボタンをクリックして、[エクスポートタイプ]画面に進みます。

4 [エクスポートタイプ]画面で支援インストールタイプを以下の中から選択し、[次へ]ボタンをクリックして、[パッケージ]画面に進みます。

● [Windowsのフォルダにエクスポート]
このオプションは、管理特権のないユーザーが使用するコンピュータにeinstaller.exeを配信する場合に適しています。管理ログオン資格情報は、管理特権のあるユーザーがeinstaller.exeを実行していない限り、インストーラが実行されているときにERAサーバーから取得します。

● [Windowsのログオンスクリプトにエクスポート]
このオプションは、[Windowsのフォルダにエクスポートする]と同じですが、管理されるコンピュータのログオンスクリプトで使用できるように、[終了]画面でエージェント(einstaller.exe)をエクスポートしたフォルダーへのリンクを取得できます。

● [WSUSエクスポート(Windows Server Update Services)]
このオプションを選択すると、次のステップで選択するインストールパッケージ全体を実行可能な*.msiインストールファイルとしてダウンロードします。インストールパッケージはWSUSの一部として目的のコンピュータに配信される場合があります。

● [GPO(グループポリシーオブジェクト)]
このオプションを選択すると、次のステップで選択するインストールパッケージ全体をダウンロードします。インストールパッケージはGPO経由で目的のコンピュータに配信される場合があります。

5 [パッケージ] 画面の [フォルダにエクポート] セクションで [フォルダ] の隣にある [...] をクリックして、エージェントのエクスポート先ディレクトリを選択します。[Windowsのログオンスクリプトにエクスポート] オプションが選択されている場合、einstaller.exeファイル（または*.msiインストーラ）が選択したフォルダーにエクスポートされ、ネットワーク内で利用可能になります。続いて、[次へ] ボタンをクリックします。

6 エージェントが選択したフォルダーに保存され、[終了] 画面が表示されます。[Windowsのログオンスクリプトにエクスポート] オプションを選択した場合は、エージェント（einstaller.exe）をエクスポートしたフォルダーへのリンクが表示されます。[終了] ボタンをクリックします。

4.3.3.1.2 エージェント（einstaller.exe）を電子メールに添付する

1 [リモートインストール] ペインを開き、[コンピュータ] タブを開きます。

2 [新規インストールタスク...] ボタンをクリックします。[新規インストールタスク] 画面に進みます。

3 [電子メール] を選択し、[続行] ボタンをクリックして、[パッケージ] 画面に進みます。

4 インストールする [パッケージ] の [種類] と名前を選択し、[次へ] ボタンをクリックします。

CAUTION

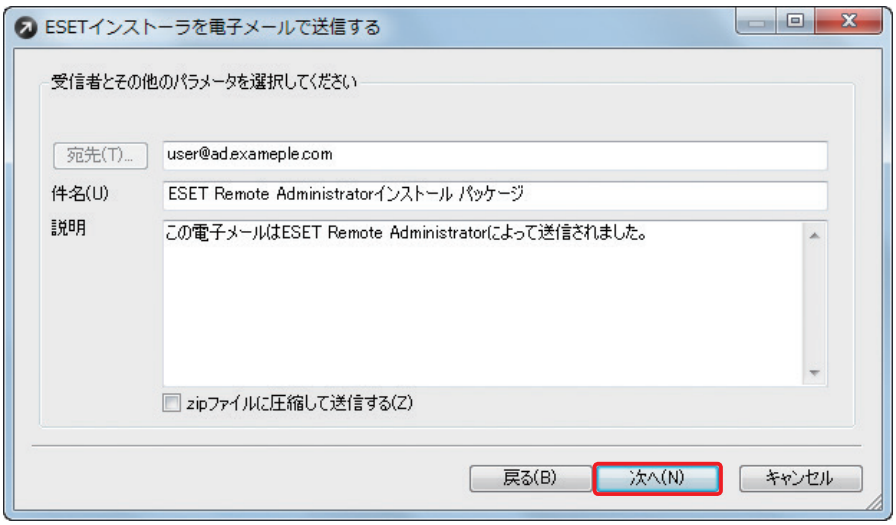
ユーザーのコンピュータからESETセキュリティ製品をアンインストールする場合、[種類] リストボックスで[Windows用のESETセキュリティ製品とNOD32バージョン2をアンインストールする]のオプションを選択します。

5 [宛先] ボタンをクリックして、アドレスブックからインストール対象のコンピュータで受信するメールアドレスを選択するか、個々のアドレスを入力します（複数入力が可能です）。

6 必要に応じて「件名」を修正します。

7 必要に応じて [説明] を修正します。

8 エージェントを圧縮パッケージとして送信する場合は、[.zipファイルに圧縮して送信する] チェックボックスをオンにします。

9 

[次へ] ボタンをクリックして、メッセージを送信します。

リモートインストールプロセスの過程で、ERASへの逆接続が行われ、エージェント（einstaller.exe）は、［設定］ウィンドウで定義した既定のログオン情報からの設定を採用します。［電子メール］オプションが選択されている場合、［新規インストールタスク］画面に表示される［設定...］ボタンをクリックすると、［設定］ウィンドウが表示されます。

パッケージのインストールを実行するアカウントは、管理者権限があるアカウントにする必要があります。ドメイン管理者のアカウントを使用することをお勧めします。［既定のログオン］ダイアログウィンドウに挿入された値は、ERASのサービスが再開されるたびに消去されます。

4.3.3.2 既定のログオン／ログオン情報

［既定のログオン］ウィンドウまたは［ログオン情報］ウィンドウでは、ネットワーク上にあるクライアントコンピュータへのアクセスやインストールしたESET製品の管理に必要な、ユーザー資格情報とドメイン情報を設定します。

請求されたクライアントのデータは次のとおりです。

●ユーザ名
●パスワード
●ドメイン/ワークグループ

データを入力し終えたら、（［既定のログオン］ウィンドウで）［ログオンの設定］または（［ログオン情報］ウィンドウで）［OK］ボタンをクリックして、サーバーに情報を保存します。

CAUTION

この情報がサーバで保持されるのは、次回のサーバの再起動までの期間のみです。

CAUTION

［既定のログオン］ウィンドウにログオン情報はサーバに格納済みですというメッセージが表示された場合は、設定がサーバに格納済みです。格納されている設定を変更する場合は、［上書き］ボタンをクリックして、新しいログオン情報の設定を続けます。

4.3.4 クライアントのアップグレード

EES/EAVバージョン5以降がインストールされたクライアントには、このタイプのインストールを指定します。バージョン5以降、einstaller.exeエージェントがなくてもERAがクライアント側でアップグレードプロセスを開始できる新しいアップグレードメカニズムが実装されています。このメカニズムは、新しいバージョンのプログラムにクライアントをアップグレードするプログラムコンポーネントのアップデート(PCU)と同様に機能します。バージョン5以降のEES/EAVクライアントでは、このタイプのアップグレードを強くお勧めします。

NOTE

インストールパッケージでカスタムコンフィグレーションファイルを定義していても、アップグレードでは無視されます。

[クライアントのアップグレード]コマンドを使用すると、クライアントまたはクライアントのグループをリモートでアップグレードできます。

1 アップグレードするクライアントを選択するために選択ツールを使用する場合は、最初の手順で[クライアント特殊フィルタの追加]ボタンをクリックします。選択を終了したら、[次へ]をクリックして続行します。

NOTE

[クライアント特殊フィルタの追加]オプションをクリックすると新しいウィンドウが開き、サーバー別([サーバ]セクション)またはグループ別([グループ]セクション)にクライアントを追加できます。

2 [パッケージ設定]ウィンドウでは、クライアントのアップグレードに使用するESET製品パッケージの種類と名前を選択するために、それぞれに該当するプルダウンメニューを使用できます。選択を終了したら、[次へ]をクリックして続行します。

3 [タスクの設定]ウィンドウでは、アップグレードタスクの既定の名前と説明を変更できます。また、タスクをすぐに実行する場合は[今すぐタスクを実行する]、タスクの実行日として後の日付を設定する場合は[指定日時にタスクを実行する]を選択します。[終了]をクリックして、実行するタスクを登録します。

NOTE

このタスクはプライマリサーバーに直接接続するクライアント上で動作します。

4.3.5 インストールの繰り返しの回避

エージェントによるリモートインストールプロセスが正常に完了すると、同じインストールパッケージが繰り返しインストールされないようにするフラグがリモートクライアントに設定されます。このフラグは、次のレジストリキーに書き込まれます。

HKEY_LOCAL_MACHINE¥Software¥ESET¥ESET Remote Installer

einstaller.exeエージェントで定義されているパッケージの種類と名前がこのレジストリのデータと一致すると、インストールは実行されません。これによって、同じワークステーションでインストールが繰り返されることがなくなります。

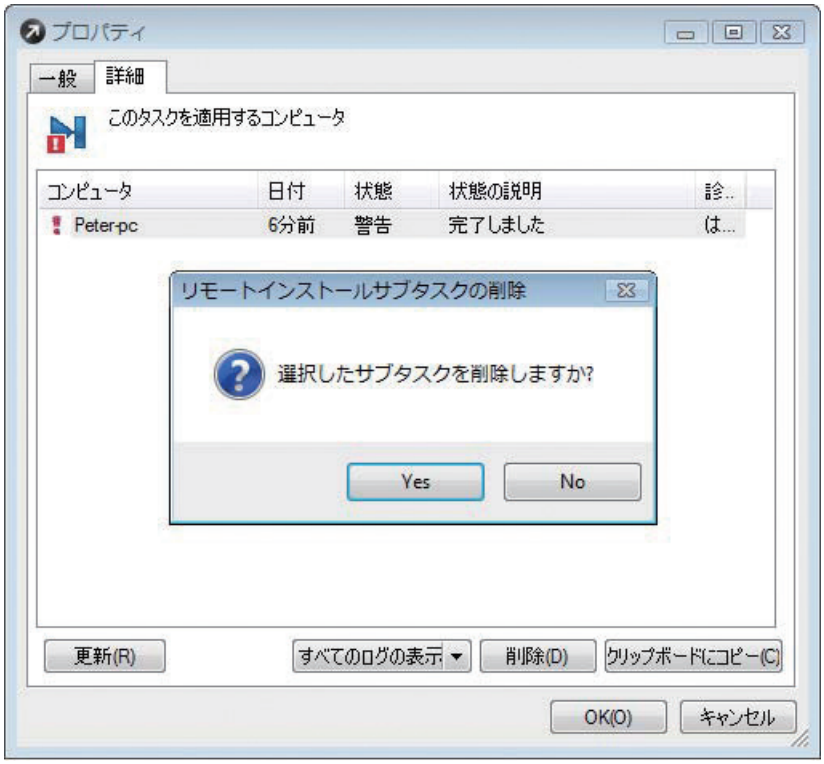
NOTE

リモートプッシュインストールでは、このレジストリキーは無視されます。

ERASには、インストールの繰り返しを防ぐ別の機能があります。この機能は、インストーラ側からERAS（TCP 2224）への接続を確立するときに有効になります。ワークステーションに関連するエラーメッセージがない場合、またはインストールが正常に完了した場合、新たなインストールの試行は拒否されます。

%TEMP%¥einstaller.logにあるインストーラログに次のエラーが記録されます。

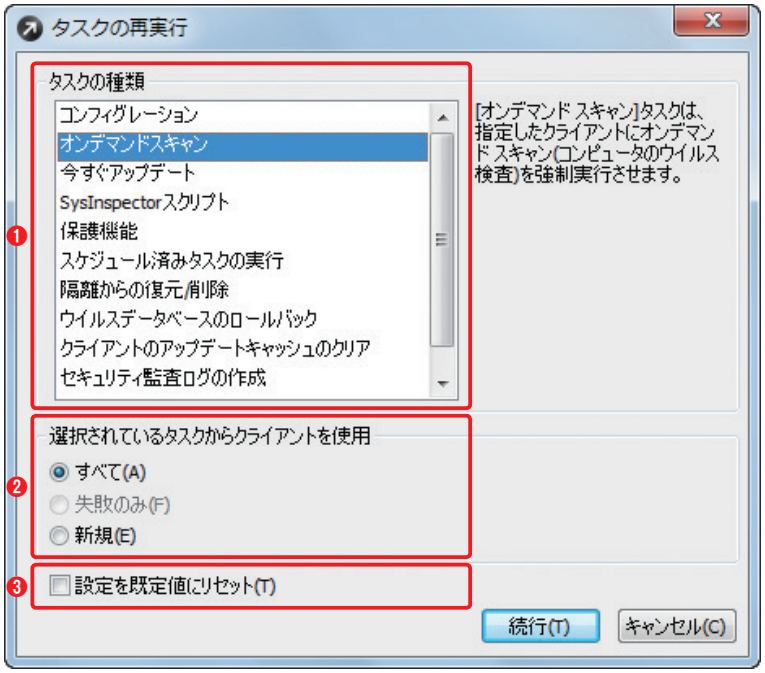
ESETインストーラは、サーバーによって終了されました'X:2224'。



ERASでインストールの繰り返しが拒否されないようにするには、[リモートインストールタスクの詳細] タブの関連するエントリを削除する必要があります。エントリを削除するには、そのエントリを選択して [削除] ボタンをクリックし、[はい] をクリックして確定します。

4.3.6　タスクの再実行

[タスク] タブをクリックすることで、[クライアント] タブから開始したすべてのタスクを検索できます。また、[タスク] タブに表示された目的のタスクを右クリックし、コンテキストメニューから [タスクの再実行...] を選択すると、そのタスクを再度実行できます。



[タスクの再実行] ウィンドウには、次のようなオプションが提示されます。また、[続行] ボタンをクリックすると、❶ [タスクの種類] で選択されたタスクの詳細設定画面が表示されます。

❶タスクの種類
実行するタスクを再選択できます。

❷選択されているタスクからクライアントを使用
実行するタスクの適用先となるクライアントを次から選択します。

[すべて] - 以前に関与したすべてのクライアント
[失敗のみ] - 以前に失敗したタスクのクライアント
[新規] - 後続のいずれかのダイアログウィンドウで選択するクライアント

❸設定を既定値にリセット
以前に実行したタスクの既定値の設定を変更していた場合、[設定を既定値にリセット] のチェックボックスにチェックを入れると、タスクをその既定値設定でもう一度実行するようになります。

4.3.7 新規インストールタスク

[リモートインストール] タブで [新規インストールタスク...] をクリックすると、[新規インストールタスク] ウィンドウが表示され、次の中から [リモートインストール] タイプを選択できます。

●[Windowsプッシュ]
選択したリモートコンピュータで、ESETクライアントソリューションのリモートインストールをサービスとして実行します。このインストール方法では、インストールエージェントを対象のコンピュータにプッシュできるようにするために、ローカルな管理資格情報が必要です。リモートコンピュータでネットワーク共有を有効にし、オンライン状態にしておく必要があります。

●[Windowsプッシュ (WMI)]
ESET Remote Administrator 5.3の新機能です。詳細を定義したネットワーク共有からインストールパッケージを配置し、実行します。

●[Windowsアップグレードクライアント]
管理されたワークステーションでESETウィルス対策ソリューション (バージョン4.2以降) を最も確実にアップグレードする方法です。管理者資格情報は不要ですが、リモートコンピュータでネットワーク共有を有効にしておく必要があります。

●[Linux]
SSHアクセスが有効なほとんどのLinux配信で、ESETクライアントソリューションをコマンドラインタイプでインストールします。

●[Mac]
SSHアクセスが有効なMac OS Xシリーズオペレーティングシステムで動作するコンピュータで、ESETクライアントソリューションをコマンドラインタイプでインストールします。インストールパッケージの実行が可能です。

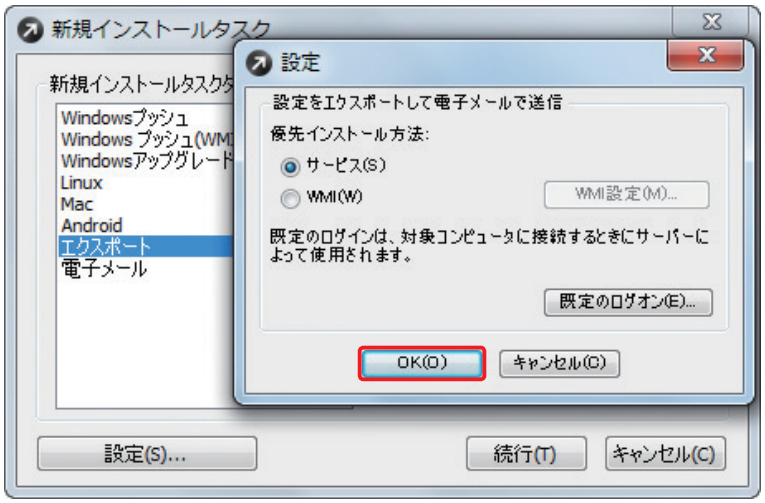
●[Android]
Androidを搭載したデバイスに分かりやすいダウンロード手順を送信し、シングルクリックでの登録プロセスを有効にします。

●[エクスポート]
外部のコンピュータにESETクライアントソリューションを配備するために、目的のパッケージを実行可能インストーラ (einstaller.exeファイル) としてエクスポートします。エクスポートしたインストーラをWMIメソッドで使用する場合、エクスポートを始める前に、[エクスポート] メソッドの [設定...] を修正します。

●[電子メール]
小規模なインストールエージェントを電子メールにより配信して、対象とするユーザーに実行する手順を指示します。

4.3.7.1　詳細設定

[新規インストールタスク] ウィンドウで新規インストールタイプに [エクスポート] または [電子メール] を選択した場合は、[設定] ボタンが表示され、このボタンをクリックすると、詳細設定を行えます。



推奨のインストール方法

●[サービス]

[設定] ダイアログにアクセスしなくても、既定ではこの方法が選択されます。

●[WMI]

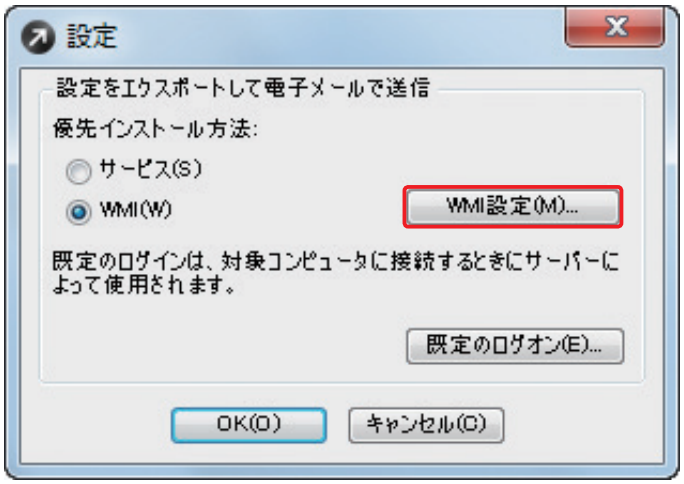
対象のコンピュータにおいてWMIからインストーラを入手できるようにする場合、この方法を選択し、[WMIセットアップ...] をクリックして [インストーラ共有の構成] に進みます。

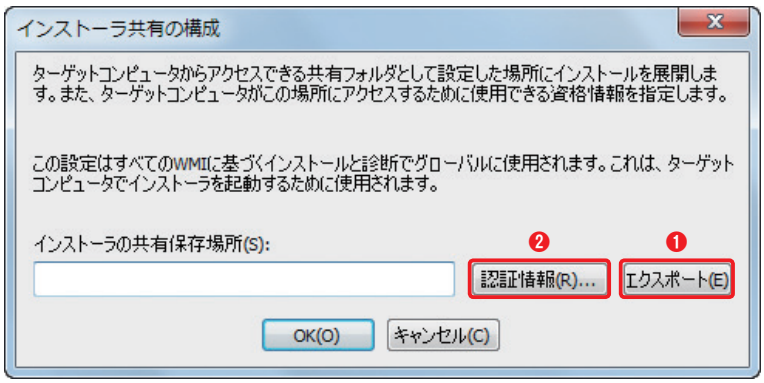
●[既定のログオン...] ボタン

Windows NTベースのシステムに対してユーザー名とパスワードを設定します。

4.3.7.2　インストーラ共有の構成

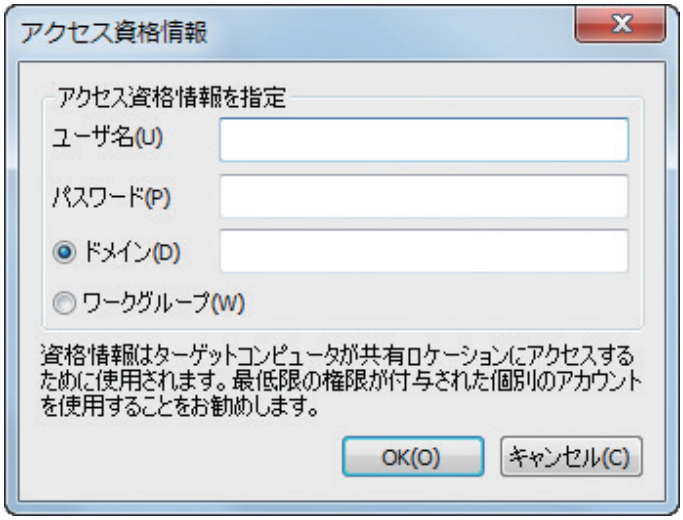
[Windowsプッシュ (WMI)] のインストールを実行する場合、または [新規インストールタスク] ウィンドウで [電子メール] または [エクスポート] オプションを選択し、[優先インストール方法] として [WMI] を選択する場合、インストーラの共有場所の詳細設定を行う必要があります。[WMI設定] ボタンをクリックすると、[インストーラ共有の構成] ウィンドウが表示され、詳細設定を行えます。





❶ [エクスポート] ボタンをクリックすると、インストーラーのエクスポートフォルダ（共有場所）を設定できます。

❷ [認証情報] ボタンをクリックすると、[アクセス資格情報] ウィンドウが表示され、選択したインストーラの共有場所にアクセスするための認証情報を設定できます。



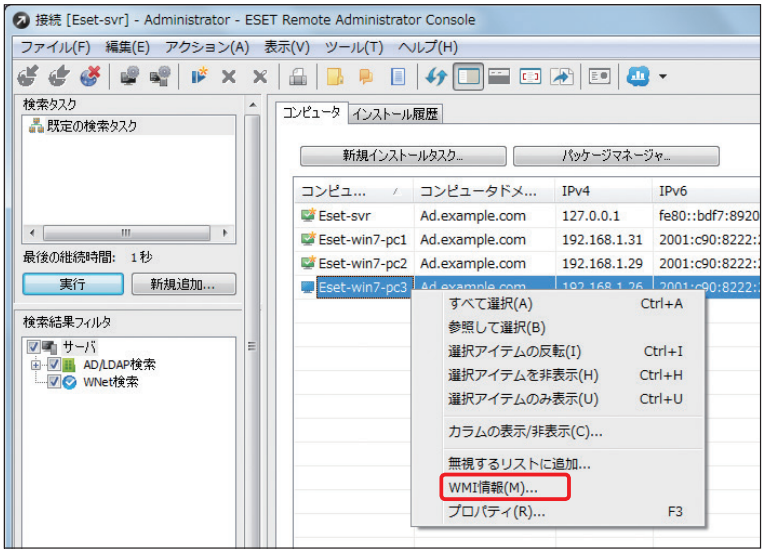
オペレーティングシステムで環境変数が構成される場合、共有場所へのパスにこれらを使用できます（ローカルファイルが選択される場合）。

NOTE

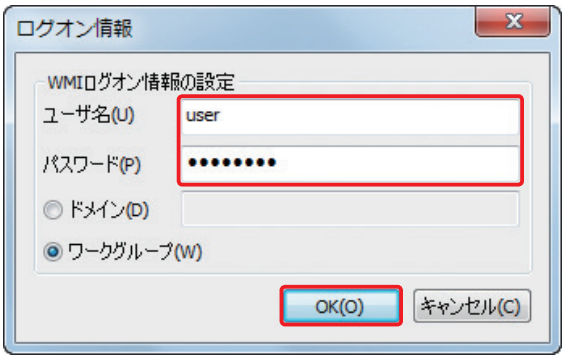
インストールパッケージを配信する際に共有場所を使用する場合でも、対象のコンピュータはERA ServerをTCP/IPで引き続き識別する必要があります。

4.3.7.3 WMI情報

管理されたコンピュータのWMI情報を表示および編集する場合、次の手順で行います。

1 

選択したコンピュータのコンテキストメニューから、[WMI情報] をクリックします。

2 

[ログオン情報] を入力し、[OK] ボタンをクリックします。

3 情報がコンピュータからERA Consoleにダウンロードされるまで待ちます。

4 WMI情報は数秒後に表示されます。

4.3.7.4 WSUSのエクスポート

一部のESETクライアントソリューションを [WSUS] [(Windows Server Update Services)] の一部としてインストールされるようにする場合、[WSUS Export (Windows Server Update Services)] オプションを選択したうえで、インストーラパッケージをERA Server 5.3からエクスポートできます。

[WSUS] のインストールと構成に関する詳細情報は、https://technet.microsoft.com/en-us/library/dd939822(v=ws.10).aspxから段階的なガイドとして入手できます。

WSUSは、WSUSサーバーにインストールされた証明書で署名されたパッケージのみを配布します。このような証明書は、ローカル更新パブリッシャー (LUP) で生成できます。証明書MMCスナップインを使用して、WSUSサーバーにインストールします。

エクスポートした.msiインストーラファイルと.xml構成ファイルを両方とも、LUPで作成したパッケージに追加し、パッケージをLUPで承認します。これ以降、承認したパッケージはWindows Updateの一部として配布されることになります。

4.3.7.5 GPOのエクスポート

ドメイン環境でのActive Directoryで、ESETクライアントソリューションをグループポリシーソフトウェアインストールの一部として導入する場合、[GPOのエクスポート(グループポリシーオブジェクト)] オプションを選択したうえで、ERA Server 5.3からインストーラパッケージをエクスポートできます。エクスポートした.msiインストーラと.xml構成ファイルを(読み取りアクセスのある)共有フォルダにコピーし、共通のGPOで管理される対象のコンピュータで入手できるようにします。

グループポリシー管理コンソールで、GPOを新たに作成するか、または目的のActive Directory Organization Unitに既存のGPOをリンクします。

GPOへのリンクは、グループポリシー管理コンソールで、リンクしたいGPOを右クリックし、[編集] をクリックします。グループポリシー管理エディターが表示されるので、[コンピュータ構成] (または [ユーザー構成]) > [ポリシー] > [ソフトウェアの設定] > [ソフトウェアのインストール] とクリックします。右側の空白のウィンドウ内で右クリックし、[新規] を選択し、[パッケージ...] をクリックして、共有フォルダにコピーした.msiインストーラを参照します。

●共有フォルダにコピーした.msiインストーラへのネットワークパスを入力する

●導入方法の選択

a) 割り当て
ソフトウェアをインストールする

b) 公開
追加/削除プログラムにソフトウェアを提示する(ユーザーが割り当てたGPO限定)

c) 詳細
割り当て済みまたは公開済みオプションを構成し、パッケージに修正を適用する

グループポリシーが適用され、対象のコンピュータが再起動した後に(またはユーザーが割り当てたGPOの場合はログオフ/ログオンした直後に)、ソフトウェアは自動的にインストールされます。

4.4 大規模ネットワーク環境でのインストール

大規模ネットワークにプログラムを展開する場合は、ネットワークにあるすべてのコンピュータに対してプログラムのリモートインストールを実行できるツールを使用することが重要です。

グループポリシーを使用したインストール

Active Directory環境では、グループポリシーインストールによって、この作業を効率的に実施できます。インストールではMSIインストーラを使用します。このインストーラは、ドメインに接続しているすべてのクライアントにグループポリシーを通じて直接配布されます。

ログインしたワークステーションにESET Endpoint SecurityまたはESET Endpoint アンチウイルスを自動的にインストールするようにドメインコントローラを設定する手順は次のとおりです。

1 ドメインコントローラ上に共有フォルダを作成します。すべてのワークステーションがこのフォルダに対して"読み取り"権限を持っている必要があります。

2 ESET Endpoint SecurityまたはESET Endpoint アンチウイルスインストールパッケージ(.msi)をこの共有フォルダにコピーします。

3 プログラムに適用する.xmlコンフィグレーションファイルを、同じ共有フォルダに追加します。ファイル名はcfg.xmlとします。コンフィグレーションファイルは、ESET Configuration Editorを使用して作成できます。詳細については、「ESET Configuration Editor」を参照してください。

4 [スタート]-> [プログラム]-> [管理ツール]-> [Active Directoryユーザーとコンピューター]をクリックします。

5 ドメイン名を右クリックし、[プロパティ]-> [グループポリシー]-> [編集]-> [ユーザーの構成] を選択します。

6 [ソフトウェアの設定] を右クリックし、[新規作成]-> [パッケージ] を選択します。

7 [ファイルを開く] ウィンドウで、共有インストールパッケージへのUNCパス(¥¥computer_name¥path¥installation_package. msi) を指定し、[開く] をクリックします。[参照] オプションを使用してインストールパッケージを指定しないでください。このオプションを使用すると、UNCネットワークパスではなく、ローカルネットワークパスとして表示されるからです。

8 次に表示されるダイアログウィンドウで、[割り当て] オプションを選択します。続いて [OK] をクリックして、ウィンドウを閉じます。

上記の手順を実行すると、ドメインに参加している各コンピュータにインストーラパッケージがインストールされます。現在起動して稼働中のコンピュータにパッケージをインストールするには、それらのコンピュータのユーザーがログアウトした後、ログインし直す必要があります。

ユーザーがパッケージのインストールを許可または拒否できるようにする場合は、手順8で [割り当て] ではなく [公開] を選択します。ユーザーが次回ログインしたときに、[コントロールパネル] -> [プログラムの追加と削除] -> [プログラムの追加] -> [ネットワークからプログラムを追加] にパッケージが追加されます。ユーザーは、そこからパッケージをインストールできます。

[Chapter 5]
クライアントコンピュータの管理

5.1 タスク

ERASに正しく接続されていて、ERACに表示されているクライアントワークステーションは、さまざまな種類のタスクを使用して設定および管理できます。

ステージⅠ－新規タスク

1 1つのタスクを1つまたは複数のクライアントワークステーションに適用するには、[クライアント]ペインで目的のワークステーションを選択して右クリックし、コンテキストメニューを開きます。

2 [新規タスク]をクリックして、実行するタスクの種類を選択します。

NOTE

ERACのメインメニューから[アクション]->[新規タスク]をクリックして、タスクウィザードを開くこともできます。

ステージⅡ－以下のいずれかのタスクを選択します。

- ●コンフィグレーションタスク
- ●オンデマンドスキャン(駆除無効/駆除有効)
- ●今すぐ更新
- ●SysInspectorスクリプト
- ●保護機能
- ●スケジュールされたタスクの実行
- ●隔離からの復元/削除
- ●ウイルスデータベースのロールバック
- ●クライアントのアップデートキャッシュをクリアする
- ●セキュリティ監査ログの作成
- ●通知の表示

3 目的のタスクを選択したら、各章の説明にあるタスク固有のアクションを実行します(上記の各リンクを参照)。

ステージⅢ－クライアントの選択

4 クライアントの選択は、[クライアントの選択]ウィンドウで変更できます。このウィンドウは、タスクを設定すると表示されます。クライアントの選択範囲を調整するには、[すべてのアイテム](ウィンドウの左半分)のクライアントの概要ツリーからクライアントを[選択したアイテム]リスト(ウィンドウの右半分)に追加します。または、リストに登録済みのクライアントエントリを削除します。

NOTE

［指定追加］をクリックすると新しいウィンドウが開き、［クライアント］ペインからクライアントを追加できます。また、サーバー別またはグループ別、あるいはその両方でクライアントを追加することもできます。

ステージⅣ－タスクを完了する。

以後の項目では、クライアントワークステーションで行うタスクのそれぞれの種類の概略を示します。そこでは、タスクの種類それぞれに事例のシナリオが付随しています。

NOTE

指定した間隔が経過するか、または製品の新バージョンが入手可能になったら、ERAアップデートのチェックウィンドウが表示されます。ESETのWebサイトから製品の最新アップデートをダウンロードするには、［Webサイトにアクセス］をクリックします。

5.1.1 コンフィグレーションタスク

コンフィグレーションタスクは、クライアントワークステーションの保護設定の変更に使用します。コンフィグレーションタスクは、変更パラメータが含まれるコンフィグレーションパッケージでクライアントワークステーションに配布されます。ESET Configuration Editorで作成した.xmlファイルまたはクライアントからエクスポートされた.xmlファイルもコンフィグレーションタスクに使用できます。下記の例は、対象のコンピュータのユーザー名とパスワードを変更するコンフィグレーションタスクを作成する方法を示しています。この例で使用していないスイッチおよびオプションはすべて、この章の最後に示します。

まず、タスクの配布先のワークステーションを指定します。ERACの[クライアント]ペインでこれらのワークステーションを指定します。

1. 選択したいずれかのワークステーションを右クリックして、コンテキストメニューから [新規タスク] -> [コンフィグレーションタスク] を選択します。

2. [クライアントの設定] ウィンドウが開きます。このウィンドウは、コンフィグレーションタスクウィザードとして機能します。[作成]、[選択]、または [テンプレートから作成] をクリックすることによって、コンフィグレーションファイルの作成元を指定できます。

3. [作成] ボタンをクリックして、ESET Configuration Editorを開き、適用するコンフィグレーションを指定します。Windows製品ラインv5>アップデート>プロファイル>設定>ユーザー名及びパスワードに移動します。

4. ESET提供のユーザー名とパスワードを挿入して右にある [コンソール] をクリックし、タスクウィザードに戻ります。[コンフィグレーションの作成/選択] フィールドに、パッケージへのパスが表示されます。

5. 必要な変更が含まれるコンフィグレーションファイルがすでにある場合は、[選択] をクリックしてそのファイルを見つけ、コンフィグレーションタスクに割り当てます。

6. または、[テンプレートから作成] をクリックして、.xmlファイルを選択し、必要に応じて変更を加えます。

7. 作成または編集したコンフィグレーションファイルを表示または編集するには、[表示] ボタンまたは [編集] ボタンをクリックします。

8. [次へ] をクリックして [クライアントの選択] ウィンドウに進みます。このウィンドウには、タスクの配布先のワークステーションが表示されます。この手順では、選択したサーバーまたはグループからクライアントを追加できます。[次へ] をクリックして次の手順に進みます。

9. 最後のダイアログウィンドウ [タスクレポート] に、コンフィグレーションタスクのプレビューが表示されます。タスクの名前または説明を入力します（オプション）。指定した日または時間の経過後に実行されるようにタスクを設定するには、[指定日時にタスクを実行する] オプションを使用します。[タスクが正常に完了した場合、タスクを自動的に削除する] オプションによって、対象のワークステーションに正常に配布されたタスクがすべて削除されます。

10. [終了] をクリックして、実行するタスクを登録します。

5.1.2 オンデマンドスキャンタスク

[新規タスク] コンテキストメニューオプションには、2種類のオンデマンドスキャンが含まれます。1つ目のオプションは [オンデマンドスキャン (駆除無効)] で、このスキャンではログが作成されるだけで、感染ファイルに対してアクションは実行されません。2つ目のオプションは、[オンデマンドスキャン (駆除有効)] です。

[オンデマンドスキャン] ウィンドウには、[検査のみ (駆除なし)] を除き、この2つのオプションに同じ既定の設定があります。[検査のみ(駆除なし)]オプションでは、スキャナで感染ファイルを駆除するかどうかを指定します。下記の例は、オンデマンドスキャンタスクを作成する方法を示しています。

1 [設定セクション] ドロップダウンメニューでは、オンデマンドスキャンタスクを指定するESET製品の種類を選択できます。対象のワークステーションにインストールされているESET製品の種類を選択します。

NOTE

[このセクションをオンデマンドスキャンから除外する] オプションによって、選択した製品の種類に対するウィンドウ内のすべての設定が無効になります。これらの設定は、[設定セクション] で指定した製品の種類がインストールされているワークステーションには適用されません。このため、指定した製品がインストールされているクライアントはすべて、宛先のリストから除外されます。管理者がクライアントを受信者として指定し、上記のパラメータを使用して製品を除外した場合、タスクは失敗し、タスクを適用できなかったという通知が発行されます。これを回避するには、管理者は、常に、タスクが割り当てられるクライアントを指定する必要があります。

2 [プロファイル名] では、タスクに適用する検査プロファイルを選択できます。

3 [検査ドライブ] セクションで、クライアントコンピュータ上のスキャン対象ドライブの種類を選択します。選択が大まかすぎる場合は、スキャン対象オブジェクトへの正確なパスを追加できます。このためには、[パス] フィールドまたは [パスを追加] ボタンを使用します。スキャン対象ドライブの元のリストを復元するには、[履歴のクリア] を選択します。

4 [次へ] をクリックして [クライアントの選択] ダイアログウィンドウおよび [タスクレポート] ダイアログウィンドウに進みます。これらのダイアログウィンドウの詳細については、「タスク」を参照してください。

5 クライアントワークステーションでタスクの実行が終了すると、ERASに結果が送信されます。これらの結果は、ERACの [スキャンログ] ペインに表示できます。

5.1.3 今すぐアップデートタスク

このタスクの目的は、対象のワークステーションでアップデートを強制することです（ウイルス定義データベースのアップデートおよびプログラムコンポーネントのアップグレード）。

1 [クライアント] ペインでいずれかのワークステーションを右クリックし、[新規タスク] -> [今すぐアップデート] を選択します。

2 タスクから特定の種類のESETセキュリティ製品を除外する場合は、[設定セクション] ドロップダウンメニューでそれらの製品を選択し、[このセクションを更新タスクから除外する] オプションを選択します。

3 今すぐ更新タスクで特定のアップデートプロファイルを使用するには、[プロファイル名を指定する] オプションを有効にして、目的のプロファイルを選択します。[ユーザ定義プロファイル名] を選択して、プロファイル名を入力することもできます。[履歴のクリア] をクリックすると、このフィールドの値は既定値に戻ります。

4 [次へ] をクリックすると、[クライアントの選択] および [タスクレポート] ダイアログウィンドウに進みます。これらのダイアログの詳細については、「タスク」を参照してください。

5.1.4 SysInspectorスクリプト

SysInspectorスクリプトでは、対象のコンピュータでスクリプトを実行できます。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するのに使用されます。詳細については、ESET SysInspectorのヘルプページを参照してください。

1 「タスク」の説明にあるステージⅠとステージⅡを完了した後、[選択] をクリックして、対象のワークステーションで実行するスクリプトを選択します。

2 [表示と編集] をクリックしてスクリプトを調整します。

3 [次へ] をクリックして [クライアントの選択] ダイアログウィンドウおよび [タスクレポート] ダイアログウィンドウに進みます。これらのダイアログウィンドウの詳細については、「タスク」を参照してください。

4 クライアントワークステーションでタスクが終了すると、[タスク] ペインの [状態] カラムに該当の情報が表示されます。

NOTE

SysInspectorスクリプトは、バージョン5以降のWindows用のESET Security製品のみサポートされます。

5.1.5　保護機能

このタスクは管理者のセキュリティ製品（Windows ESET Security製品のバージョン5とそれ以降）の保護機能の状態への変更を容認します。

各保護機能には-変更しない、一時的な無効化および有効にするという3つの段階があります。各機能の横にあるチェックボックスを選択することにより、これらを切り替えることができます。保護機能は無効にされている場合（一時的な無効化）に、一時的な無効化の時間間隔を設定できます。この間隔は10分から無限（次のコンピュータ再起動まで完全に機能を無効化します）に設定することができます。

5.1.6　スケジュールタスクを実行

このタスクは、クライアント上で実行可能なスケジュール済みのタスクをトリガします。事前定義されたスケジューラを選択出来ます。スケジュールされたぞれぞれのタスクにはIDが付いていて、ドロップダウンメニューからタスクを選択するか､IDを入力することが出来ます。特定のクライアントに関するスケジューラにあるタスクを見るには、クライアントタブにあるコンテキストメニューからタスクを始めます。

クライアントに実行したいタスクを選んでから、保護機能を変更したいクライアントを選び、タスクを終了します。

5.1.7　隔離からの復元/削除

このタスクでは、指定した隔離オブジェクトをクライアント隔離から復元または削除できます。

1. 隔離から復元/削除ウィンドウを開き（タスクを参照）、隔離されたオブジェクトに対して実行するアクションに応じて、復元または削除をクリックします。

NOTE

ウイルスの可能性があると判断されて検出・隔離されたオブジェクトを復元する場合、[除外も追加する] を選択できます。このオプションを選択しないと、ウイルス対策プログラムにより、その操作が阻止されるか、オブジェクトが再度隔離に追加されます。

2. 隔離されたオブジェクトが復元または削除去れる条件を選択し [次へ] をクリックします。

NOTE

[隔離] タブで隔離エントリを直接右クリックして [隔離からの復元/削除] オプションを選択し、[隔離からの復元/削除] ウィンドウを開いた場合は、条件を指定する必要はありません（ハッシュオプションが自動的に選択され、隔離されたファイルのハッシュコードが識別子として使用されます）。

3. 復元または削除するクライアントを選択して（「タスク」を参照）、[次へ] をクリックします。

4. [タスクレポート] ウィンドウで設定内容を確認し、タスクに名前を付けて、タスクを適用する日時を指定します。必要に応じてクリーンアップオプションを指定することもできます。[終了] をクリックして確定します。詳細については、「タスク」を参照してください。

5.1.8 ウイルスデータベースのロールバック

新しいウイルスデータベースが不安定になったり、壊れたりしている可能性が疑われる場合は、以前のバージョンへのロールバックと選定された期間における更新を無効にすることができます。また、以前に無効にしたアップデートを有効にすることができます。

1 ウイルスデータベースのアップデートの無効化/有効化

X時間無効にします-ウイルスデータベースが以前のバージョンへのロールバックされるようになり（クライアントが作成したスナップショットに基づいて）、選定された時間帯にアップデートが無効になります。無限を選んで、アップデートを完全に無効することが出来ますがセキュリティリスクが高いため、データベースアップデートを完全に無効にするときは注意してください。

CAUTION

無限という選択肢はクライアントコンピュータが再起動した後もアクティブのままになっています。

以前無効化したアップデートを有効化する-ウイルスデータベースのアップデートが再び有効になります。

2 このタスクのクライアントを選んで、[次へ] をクリックします。

3 [タスクレポート] ウィンドウで設定内容を確認し、タスクに名前を付けて、タスクを適用する日時を指定します（必要に応じてクリーンアップオプションを指定することもできます）、終了をクリックして確定します。詳細については、[タスク] を参照してください。

5.1.9 クライアントのアップデートキャッシュをクリアする

ウイルス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、クライアントのアップデートキャッシュをクリアでき、最新のアップデートをダウンロードできます。このタスクはESET Security Productsバージョン5以降用です。

1 タスクをスタートさせ、[次へ] をクリックします。

2 このタスクを適用するクライアントを選んで、[次へ] をクリックします。

3 [タスクレポート] ウィンドウで設定内容を確認し、タスクに名前を付けて、タスクを適用する日時を指定します（必要に応じてクリーンアップオプションを指定することもできます）、終了をクリックして確定します。詳細については、「タスク」を参照してください。

5.1.10 セキュリティ監査ログの作成タスク

このタスクは、ESET Mobile Securityをインストールしたデバイスにのみ適用されます。

セキュリティ監査ログでは、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がチェックされます。詳細なレポートが生成され、指定したしきい値をアイテムの値が下回っているかどうか、またはセキュリティリスクの可能性があること（デバイスの可視性が有効になっているなど）をアイテムの値が示しているかどうかが示されます。

デバイスに対してセキュリティ監査を実行する手順は、次のとおりです。

1 [クライアント] ペインからクライアントの名前を右クリックして、コンテキストメニューから [新規タスク] -> [セキュリティ監査ログの作成] を選択します。

2 [次へ] をクリックすると、[クライアントの選択] ウィンドウおよび [タスクレポート] ウィンドウに進みます。これらのウィンドウの詳細については、「タスク」を参照してください。

5.1.11 通知の表示タスク

このタスクは、ESET Mobile Securityをインストールしたデバイスにのみ適用されます。

デバイスに通知（警告メッセージなど）を送信する手順は、次のとおりです。

1 [クライアント] ペインでクライアントの名前を右クリックして、コンテキストメニューから [新規タスク] -> [通知の表示] を選択します。

2 該当するフィールドに通知のタイトルとメッセージの本文を入力して、通知のレベルを選択します。

3 [次へ] をクリックすると、[クライアントの選択] ウィンドウおよび [タスクレポート] ウィンドウに進みます。これらのウィンドウの詳細については、「タスク」を参照してください。

5.1.12 タスクの終了

タスク設定の最後に、タスクのプレビューが表示されます。プレビューにはすべてのタスクパラメータが含まれており、必要に応じて [戻る] をクリックして、変更できます。

ウィンドウの2番目のセクションには、下記の設定があります。

名前	タスクの名前
説明	タスクの説明
指定日時にタスクを実行する	クライアントコンピュータにタスクを配信する時刻
タスクが正常に完了した場合、タスクを自動的に削除する	正常に実行されたタスクがすべて、自動的に削除されます。

5.2 グループマネージャ

グループマネージャは、クライアントの管理、クライアントのグループ分け、クライアントのグループごとに異なる設定、タスク、制限などの適用などを可能にする高機能なツールです。このツールには、[ツール] -> [グループマネージャ] またはCTRL＋Gで簡単にアクセスできます。グループはERASごとに独立しているので、重複することはありません。

社内ネットワークで各自のニーズに適合するように独自のグループを作成できるほか、グループマネージャのメインウィンドウから [Active Directoryの同期] を使用して、ERACのクライアントグループをMicrosoft Active Directoryに同期化する処理を実行することもできます。

クライアントグループには大きく分けて次の2種類があります。

●静的グループ
●パラメータグループ

静的グループとパラメータグループはどちらもERA内のさまざまな場所で使用でき、それによってクライアント管理機能の大幅な向上を図ることができます。

5.2.1 静的グループ

静的グループは、ネットワーク内のクライアントを、名前の付いたグループおよびサブグループに分けるために作成します。たとえば、マーケティングを担当するすべてのクライアントで構成する「マーケティング」という名前のグループを作成し、さらに、地区営業のような、専門のサブグループを作成することもできます。

[静的グループ] のメインウィンドウは2つに分かれています。左側には、既存のグループおよびサブグループが階層構造で表示されます。選択したグループに属するクライアントは、ウィンドウの右側に一覧表示されます。既定では、選択したグループに属するクライアントのみが一覧表示されます。現在選択されているグループのサブグループに属するクライアントを表示する場合は、ウィンドウの右側にあるサブグループのクライアントを表示するチェックボックスをクリックします。

新しいグループを作成するには、作成をクリックしてグループの名前を入力します。現在選択しているグループを親グループとする新しいサブグループが作成されます。メイングループを新規作成する場合は、階層ツリーのルートである [静的グループ] を選択します。親グループフィールドには、新規作成したグループの親クライアントの名前が表示されます (ルートの場合は"/")。コンピュータが存在する場所 (ビジネス部門、サポートなど) を示す名前を使用することをお勧めします。説明フィールドを使用すると、グループの詳細を説明できます (「オフィスCのコンピュータ」、「本社ワークステーション」など)。新規に作成して設定したグループを、後から編集することもできます。

▸▸▸ NOTE

タスクを親グループに送信すると、そのサブグループを含むすべてのワークステーションでも、このタスクを受け取ります。

将来の使用に備えて、空のグループを作成することもできます。

[OK] をクリックしてグループを作成します。グループの名前と説明が左側に表示され、[追加/削除] ボタンがアクティブになります。グループに属するクライアントを追加するには、このボタンをクリックします (追加するクライアントをダブルクリックするか、左から右へドラッグアンドドロップします)。クライアントを見つけて追加するには、クライアント名の全部または一部を [クイック検索] フィールドに入力します。入力した文字列を含むクライアントがすべて表示されます。すべてのクライアントにマークを付けるには、[すべて選択] をクリックします。更新をクリックすると、最近サーバーに接続した新しいクライアントの有無を確認できます。

クライアントを手動で選択しにくい場合は、指定追加をクリックするとオプションがさらに表示されます。

[[クライアント] ペインに読み込まれたクライアントを追加] オプションを選択すると、クライアントセクションに表示されているすべてのクライアントが追加されます。一部のクライアントのみを追加する場合は、[選択したアイテムのみを追加] オプションを選択します。すでに別のサーバーまたはグループに所属しているクライアントを追加するには、左右のリストから選択して [追加] をクリックします。

[追加/削除] ダイアログウィンドウで [OK] をクリックして、静的グループマネージャのメインウィンドウに戻ります。新しいグループが、対応するクライアントと共に表示されます。

グループ内のクライアントを追加または削除するには追加/削除をクリックし、グループ全体を削除するには削除ボタンをクリックします。クライアントとグループのリストをコピーするには、クリップボードにコピーをクリックします。グループのクライアントの表示を更新するには、更新をクリックします。
現在選択しているグループのクライアントを.xmlファイルとの間でインポートまたはエクスポートすることもできます。

5.2.2 パラメータグループ

静的グループに加えて、パラメータグループも役に立ちます。グループの条件が満たされると、クライアントが特定のパラメータグループに動的に割り当てられます。パラメータグループの利点として、フィルタ、ポリシー、レポート、通知など、さまざまな場所にパラメータグループを使用できることが挙げられます。

パラメータグループのメインウィンドウは、4つのセクションで構成されています。[パラメータグループ] には、作成済みの親グループおよびサブグループが一覧表示されます。[パラメータグループ] リストから特定のグループを選択すると、そのグループに属するクライアントが [選択したグループ] セクションに一覧表示されます。

NOTE

親グループを選択すると、リストにはそのサブグループのメンバも表示されます。

選択したグループのパラメータは、このウィンドウの [パラメータ] セクションに一覧表示されます。パラメータは、[編集...] をクリックして、いつでも編集または追加できます。

[同期状態] セクションには、同期プロセスの進捗状況バーが表示されます。

1. 新規グループを作成するには、[作成] をクリックします。この新しいグループは、現在選択している親グループのサブグループとして作成されます。メイングループを作成する場合は、階層ツリーのルートである [パラメータグループ] を選択します。[親グループ] フィールドには、新規作成したグループの親クライアントの名前が表示されます (ルートの場合は"/")。新しいグループの [名前] と簡単な [説明] を入力します。

2. 次に、[クライアントフィルタパラメータ] を作成します。このパラメータは、[編集...] をクリックした後にオプションを選択することによって [ルールエディタ] に作成できます。ここで、ルールがトリガされて適用されるために必要な条件を指定できます。条件を選択して、下の [パラメータ] ウィンドウで、ルールの横にある [指定] をクリックして指定します。すべての条件が一致した場合にのみこのルールを適用するか、いずれかの条件が一致した場合にこのルールを適用するかを選択することができます。

3. [スティッキー] の横にあるチェックボックスを選択すると、条件に一致するクライアントが自動的にこのグループに追加されますが、条件に一致しないクライアントが存在しても削除されることはありません。スティッキーグループの内容は、ルートレベルで手動でリセットできます。

NOTE

このパラメータは、グループを新規作成するときにのみ設定できます。

既存のグループを編集するには、[パラメータグループ] リストから目的のグループを選択し、ウィンドウ下部の [編集...] をクリックします。グループを削除する場合は、目的のグループを選択して [削除] をクリックします。

グループリストは、[更新] をクリックして、手動で更新できます。ファイルからグループをインポートするには、新規グループのインポート先とする [パラメータグループ] セクションでグループを選択し、[インポート...] をクリックします。[はい] をクリックして選択を確定します。インポートするファイルを探し出して [開く] をクリックします。選択した場所に、グループ (およびそのすべてのサブグループ) がインポートされます。グループ (およ

びそのすべてのサブグループ）をエクスポートするには、[パラメータグループ] セクションでグループを選択し、[インポート...] 上の矢印をクリックして [エクスポート...] を選択します。[はい] をクリックして確定し、エクスポートファイルの名前と場所を選択して [保存] をクリックします。

NOTE

[パラメータグループ] セクションに既に存在するグループは、マウスを使用してドラッグアンドドロップできます。

NOTE

パラメータグループを使用して簡単にデータやクライアントのフィルタリングをすることができます。たとえば、Windows XPがインストールされたコンピュータだけに対するレポートを生成する場合、特定のオペレーティングシステムがインストールされたコンピュータだけからなるパラメータグループを作成し、フィルタ対象として使用します。インストールパッケージを作成するとき、[コンフィグレーションエディタ]->[カーネル]->[設定]->[リモート管理] の順に選択して、独自の [カスタムクライアントデータ] を設定できます。パラメータグループのパラメータとして、[カスタムクライアントデータ] オプションを設定します。このパッケージをインストールしたユーザーはすべて、このグループのメンバになります。

5.2.3 Active Directoryの同期

Active Directoryと同期する機能では、Active Directoryで定義されている構造に基づいて自動的にグループを作成します（対応するクライアントも作成します）。この機能を使用すると、管理者はクライアントをグループ別に並べ替えることができます。ただし、そのクライアント名が、Active Directory（AD）の側にあるオブジェクトの種類computerと一致し、クライアントがADのグループに属している場合に限ります。

同期の方法を決定するオプションには大きく分けて次の2つがあります。

[グループの同期] オプションを使用すると、どのADグループを同期するかを選択できます。[すべてのグループ] オプションを使用すると、ADグループに属するERAクライアントがあるかどうかに関係なく、ADツリー構造全体を同期できます。次の2つのオプション（[ERA Serverクライアントを含むグループのみ] と [ERAプライマリサーバクライアントを含むグループのみ]）を選択すると、同期の条件はより厳格となり、既存のERAクライアントが属するグループのみが同期します。

[同期の種類] オプションを使用して、同期するADグループを既存のADグループに追加するか（[ADグループのインポート]）、同期するADグループで既存のADグループを全面的に置き換えるか（[ADグループの同期]）を定義します。

ブランチの同期オプションは同期するActive Directoryの特別ブランチを選択することができます。[同期する] オプションを使用すると、ADの同期スケジュールを一定の間隔に設定できます。

ESETコンフィグレーションエディターを利用して、詳細に設定することもできます。
Active Directory同期の詳細設定はESET Remote Administrator>ERAサーバー>設定>グループ>Active Directory同期オプションから行うことができます。既定では、全ての項目が同期されます。他のActive Directoryオブジェクトに該当するチェックボックスをオンにすると、そのオブジェクトを追加できるようになります。

NOTE

ERASをActive Directoryと同期させる場合は、ERASが配置されているコンピュータからドメインコントローラーにアクセスできなければなりません。ドメインコントローラーに対する認証を設定するには、[ツール]->[サーバオプション]->[詳細]->[詳細設定を編集]->[ESET Remote Administrator]->[ERAサーバー]->[設定]->[Active Directory] に移動します。サーバー名の形式はLDAP://servernameです。空の場合は、グローバルカタログ（GC）が使用されます。

5.3 ポリシー

ポリシーは、多くの面でコンフィグレーションタスクに似ていますが、ワークステーションに送信する1回限りのタスクではない点が異なります。ポリシーとは、ESETセキュリティ製品の特定のコンフィグレーション設定を継続的に保守する機能です。クライアントに対して強制的に適用されるコンフィグレーションがポリシーであるとも言えます。

5.3.1 基本原則と操作

[ツール]->[ポリシーマネージャ...]を選択して、ポリシーマネージャにアクセスします。画面左側のポリシーツリーには、個々のサーバーに存在するポリシーのリストが表示されます。画面右側は、[グローバル]、[選択されたポリシー]の2つのセクションで構成されています。管理者は、これらのセクションにあるオプションを使用してポリシーの管理と設定が可能です。

ポリシーマネージャーの主要な機能には、ポリシーの作成、編集、削除などがあります。クライアントは、ERASからポリシーを受け取ります。ERASでは複数のポリシーを使用でき、各ポリシーにはこれらポリシーどうしや上位サーバーから設定を引き継ぐことができます。

上位サーバーからポリシーを受け取る手法を継承といい、継承によって作成したポリシーを「マージしたポリシー」といいます。継承は親子の原則に基づき、子ポリシーは親ポリシーの設定を継承します。

5.3.2 ポリシーの作成方法

既定のインストールでは、"サーバポリシー"という1つのポリシーのみが実装されます。このポリシーの内容は、ESETコンフィグレーションエディターで設定できます。[編集] をクリックして、選択したESETセキュリティ製品（またはクライアント）のパラメータを定義します。すべてのパラメータは包括的な構造でまとめられ、エディタではすべてのアイテムにアイコンが割り当てられています。クライアントでは、青いアイコンで表示されているアクティブなパラメータのみを使用できます。グレーで表示されたすべての非アクティブなパラメータは、対象のコンピュータでは変更されません。継承したポリシーおよびマージしたポリシーにも同様の原則が適用されます。つまり、子ポリシーでは、親ポリシーにあるアクティブなパラメータのみを使用できます。

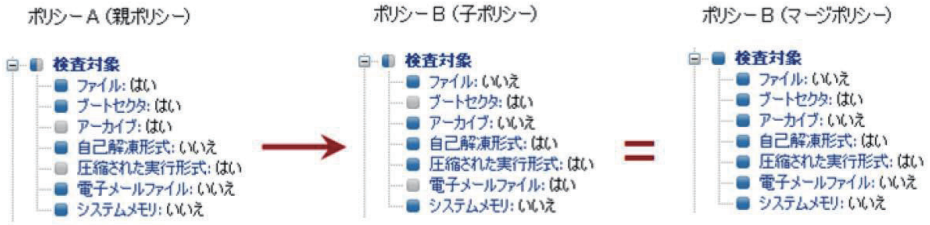
ERA Serverでは複数のポリシーを扱うことができます（新しい子ポリシーの追加）。新しいポリシーでは、ポリシー名、親ポリシーへのリンク、およびコンフィグレーションの各オプションを使用できます（コンフィグレーションは、既存のポリシーまたは.xmlコンフィグレーションファイルからコピーできるほか、空にしておくこともできます）。ERACを通じて現在接続しているサーバー上でのみ、ポリシーを作成できます。下位サーバーでポリシーを作成するには、そのサーバーに直接接続する必要があります。

各ポリシーには、2つの基本的な属性があります。子ポリシーを上書きする及び複製可能なポリシーを下に移動する。これらの属性では、アクティブなコンフィグレーションパラメータを子ポリシーでどのように使用するかを定義します。

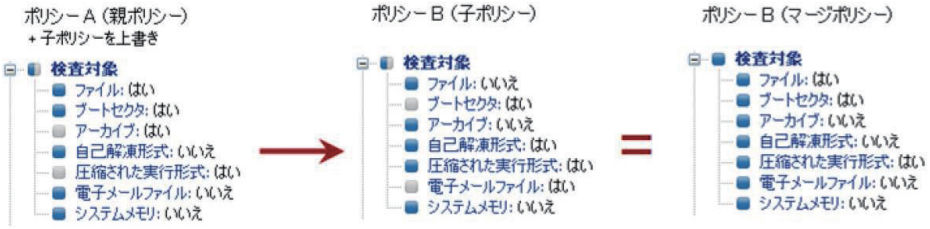
子ポリシーを上書きする	継承したポリシーに、アクティブなパラメータをすべて適用します。子ポリシーが異なる場合は、その子ポリシーに対して［子ポリシーを上書きする］がアクティブであっても、マージしたポリシーには親ポリシーから取得したアクティブなパラメータがすべて含まれます。親ポリシーから取得した非アクティブなパラメータは、すべて子ポリシーに合わせて調整されます。［子ポリシーを上書きする］属性が有効ではない場合、マージで得られるポリシーでは、親ポリシーのこれらのパラメータよりも子ポリシー側の設定が優先します。このようにマージしたポリシーは、他のポリシーに親ポリシーとしてリンクしている場合は、それらのポリシーにも適用されます。
複製可能なポリシーを下に移動する	下位サーバーへのポリシーの複製をアクティブにします。つまり、下位サーバーに対する既定のポリシーとして機能し、下位サーバーに接続したクライアントに割り当てることもできます。

ポリシーは、.xmlファイルによるインポートとエクスポートができるほか、グループからインポートすることもできます。詳細については、「ポリシーのインポート/エクスポート」を参照してください。

●ポリシーをマージした場合



●子ポリシーを上書きした場合



5.3.3 仮想ポリシー

ポリシーツリーには、作成したポリシーや他のサーバーから複製したポリシー（複製タブを参照）のほかに、既定の親ポリシーとプライマリクライアントの既定のポリシーが含まれています。このポリシーは、仮想ポリシーと呼ばれています。

既定の親ポリシーは、グローバルポリシー設定の中で上位サーバーに存在し、下位サーバーの既定のポリシーとして選択されます。複製したサーバーではない場合、このポリシーは空です（この後で説明します）。

プライマリクライアントの既定のポリシーは、グローバルポリシー設定の中では上位サーバーではなく、指定のサーバーに存在し、プライマリクライアントに既定で適用するポリシーとして選択されます。所定のERASに接続する新しいクライアント（プライマリクライアント）を作成すると、ポリシールールで指定されたポリシーがない限り、プライマリクライアントの既定のポリシーが自動的に適用されます（詳細についてはクライアントに対するポリシーの割り当てを参照）。仮想ポリシーは、同じサーバーに存在する他のポリシーにリンクしています。

5.3.4　ポリシーツリー構造でのポリシーの役割と用途

ポリシーツリーにある各ポリシーの左側には、アイコンが表示されまています。このアイコンの意味は次のとおりです。

1) 青いアイコンが付いたポリシーは、指定のサーバーにあるポリシーを表します。青いアイコンには、次の3つのサブグループがあります。

白いターゲットのアイコン－そのサーバーで作成されたポリシーです。さらに、このポリシーは下位に複製できません。つまり、下位サーバーからクライアントに割り当てることはできず、子サーバーの親ポリシーとしても機能できません。このポリシーは、そのサーバーの範囲でのみ使用できます。つまり、そのサーバーに接続したクライアントにのみ適用できます。また、同じサーバーにある別のポリシーの親ポリシーとしても使用できます。

青いターゲットのアイコン－同様にそのサーバーで作成されたポリシーですが、[子ポリシーを上書きするオプション] オプションが選択されています（詳細については、「ポリシーの作成方法」を参照してください）。

下向き矢印付きのアイコン－複製されたポリシーです。つまり、[複製可能なポリシーを下に移動する] オプションが有効になっています。このポリシーは、指定のサーバーとその子サーバーに適用できます。

[プライマリクライアントの既定のポリシー] のアイコン。

2) グレーのアイコンのポリシーは、他のサーバーで生成されたポリシーを表します。

上向き矢印付きのアイコン－子サーバーから複製されたポリシーです。このポリシーは、表示するか、[ポリシーブランチの削除] オプションを使用して削除することのみが可能です。このオプションではポリシー自体が削除されるわけではなく、ポリシーツリーに表示されなくなるだけです。そのため、複製すると再び表示されるようになる可能性があります。下位サーバーのポリシーが表示されないようにするには、[使用されない外部サーバポリシーをポリシーツリーに表示しない] オプションを使用します。

下向き矢印付きのアイコン－上位サーバーから複製されたポリシーです。他のポリシーの親ポリシーとして使用できるほか、クライアントへの割り当てや（[クライアントの追加]）、削除（[ポリシーの削除]）が可能です。削除処理では複製したポリシーだけが削除されるので、上位サーバーから複製すると再び表示されるようになります（上位サーバーで [複製可能なポリシーを下に移動する] 属性が無効になっている場合は除きます）。

▸▸▸ NOTE

構造の中でのポリシーの移動や割り当ては、親ポリシーを選択して実行できるほか、マウスを使用してドラッグアンドドロップすることでも可能です。[プライマリクライアントの既定のポリシー] および[下位サーバーのための既定のポリシー] は、ポリシーツリー構造におけるポリシーの右クリックを使用して設定することもできます。

.xmlファイルとの間で既存のポリシールールをインポートまたはエクスポートするには、[インポート...] ボタンまたは [エクスポート...] ボタンをクリックします。インポート時の名前の競合（既存のポリシーとインポートしたポリシーの名前が同じ状態）は、インポートしたポリシーの名前の後ろにランダムな文字列を割り当てることによって解決できます。

5.3.5 ポリシーの表示

ポリシーツリー構造におけるポリシーは、[表示] ...または [マージを表示] ...をクリックして、[コンフィグレーションエディタ] に直接表示することができます。

マージを表示	継承によって作成された、マージされたポリシーが表示されます（継承のプロセスで親ポリシーの設定が適用されます）。現在のポリシーはすでにマージされたポリシーなので、既定でこのオプションが表示されます。
表示	親ポリシーとマージされる前の元のポリシーが表示されます。

下位サーバーでは、上位サーバーから継承されたポリシーで次のオプションを使用できます。

マージを表示	上記と同じです。
上書き部分を表示	このボタンは、[子ポリシーを上書きする] 属性を持つポリシーに適用されます。このオプションで表示されるのは、強制的に適用されるポリシーの部分、つまり子ポリシーで他の設定より優先される部分のみです。
非強制部分を表示	[上書き部分を表示] オプションとは逆の処理が行われます。つまり、上書きが適用されない有効なアイテムのみが表示されます。

▸▸▸ NOTE

ポリシーツリーアイテムをダブルクリックして、マージを表示することができます。

5.3.6 ポリシーのインポート/エクスポート

[ポリシーマネージャ] を使用して、ポリシーおよびポリシールールをインポートまたはエクスポートできます。.xmlファイルとの間で既存のポリシーをインポートまたはエクスポートするには、[ポリシーのインポート...] ボタンまたは [ポリシーのエクスポート...] ボタンをクリックします。また、[グループからインポート...] ボタンをクリックして、ポリシーをグループからインポートすることもできます。ポリシールールをインポートまたはエクスポートするには、[インポート...] ボタンまたは [エクスポート...] ボタンをクリックします。また、ポリシールールウィザードを使用して、ルールを作成することもできます。

インポート時の名前の競合（既存のポリシーとインポートしたポリシーの名前が同じ状態）は、インポートしたポリシーの名前にランダムな文字列を追加することによって解決できます。この方法で競合を解決できない場合（新しい名前が長すぎる場合など）、インポートは終了し、未解決のポリシー名の競合という警告が表示されます。競合しているポリシーまたはポリシールールを削除するか、名前を変更することで競合を解決します。

5.3.7　クライアントに対するポリシーの割り当て

クライアントにポリシーを割り当てる際の主なルールとして、次の2点があります。

1.ローカル（プライマリ）クライアントには、あらゆるローカルポリシーまたは上位サーバーから複製したあらゆるポリシーを割り当てることができます。

2.下位サーバーから複製したクライアントには、［複製可能なポリシーを下に移動する］属性を持つあらゆるローカルポリシーまたは上位サーバーから複製したあらゆるポリシーを割り当てることができます。これらのクライアント自身のプライマリサーバーから、これらのクライアントにポリシーを適用することはできません（そのためには、ERACを使用してそのサーバーに接続する必要があります）。

▸▸▸ NOTE

重要な特徴として、各クライアントには何らかのポリシーが割り当てられるという点があります(ポリシーを持たないクライアントはあり得ません)。また、クライアントからポリシーを削除することもできません。単に他のポリシーに変更することができるだけです。どのようなポリシーのコンフィグレーションであっても、クライアントに適用されないようにするには、空のポリシーを作成します。

5.3.7.1　プライマリクライアントの既定のポリシー

ポリシーを割り当てる方法として、プライマリクライアントの既定のポリシーを自動的に適用する方法があります。この既定のポリシーは、グローバルポリシー設定で設定できる仮想ポリシーです。このポリシーは、プライマリクライアント、つまりERASに直接接続されているクライアントに適用されます。詳細については、「仮想ポリシー」を参照してください。

5.3.7.2　手動による割り当て

手動でポリシーを割り当てる方法には2種類あります。［クライアント］ペインでクライアントを右クリックし、コンテキストメニューから［ポリシーの設定］を選択する方法と、ポリシーマネージャで［クライアントの追加］->［追加/削除］を選択する方法です。

ポリシーマネージャで［クライアントの追加］をクリックすると、［設定］/［削除］ダイアログウインドウが開きます。このウィンドウの左側には、「サーバ/クライアント」の形式でクライアントの一覧が表示されます。［複製可能なポリシーを下に移動する］を選択している場合、このウィンドウには、下位サーバーから複製されたクライアントも表示されます。ポリシーの適用先とするクライアントを選択し、ドラッグアンドドロップするか［>>］をクリックして、［選択したアイテム］に移動します。新しく選択したクライアントには黄色のアスタリスクが表示されますが、これらのクライアントは、［<<］ボタンをクリックするかCキーを押すと、［選択したアイテム］から削除できます。［OK］をクリックして選択内容を確定します。

▸▸▸ NOTE

選択内容を確定した後で［設定/削除］ダイアログウィンドウをもう一度開いても、［選択したアイテム］からクライアントを削除することはできず、ポリシーの置き換えのみが可能です。

［指定追加］機能を使用してクライアントを追加することもできます。この機能では、すべてのクライアントの一括追加、選択したクライアントの追加、選択したサーバーまたは、グループにあるクライアントの追加が可能です。

5.3.7.3 ポリシールール

ポリシールールツールを使用すると、管理者は、より包括的な方法でクライアントのワークステーションにポリシーを自動的に割り当てることができます。サーバーに接続したクライアントには、直ちにポリシールールが適用されます。このルールは、プライマリクライアントの既定のポリシーおよび手動割り当てよりも優先します。プライマリクライアントの既定のポリシーは、現在のルールの中にそのクライアントに該当するものが存在しない場合にのみ適用されます。同様に、手動で割り当てた適用対象ポリシーが存在し、それがポリシールールと競合する場合は、ポリシールールで適用されるコンフィグレーションが優先します。

ポリシーマネージャにはポリシールールに関するタブがあり、そこでポリシールールの作成と管理が可能です。この作成と適用のプロセスは、電子メールクライアントでのルールの作成と管理のプロセスにきわめてよく似ています。つまり、各ルールには1つ以上の条件を設定でき、ルールのリストの中で上位にあるルールほど、高い重要性を持っています（ルールはリストの中で上下に移動できます）。

新しいルールを作成するには、[新規作成...] ボタンをクリックします。次に、名前、説明、クライアントフィルタパラメータ、およびポリシー（指定の条件に一致するすべてのクライアントに適用するポリシー）を入力します。

フィルタ条件を設定するには、[編集] ボタンをクリックします。

使用できる条件は次のとおりです。

FROM プライマリサーバ	プライマリサーバーに存在する場合（プライマリサーバーに存在しない場合）
IS 新規クライアント	新しいクライアントである場合（新しいクライアントではない場合）
HAS 新規フラグ	[新規クライアント] フラグを設定した（設定していない）クライアントに適用
プライマリサーバ IN（指定）	プライマリサーバーの名前に指定の文字列がある場合（ない場合）
対象のERAグループ（指定）	指定のグループに属するクライアントの場合
ERAグループNOT IN（指定）	指定のグループに属していないクライアントの場合
ドメイン/ワークグループ IN（指定）	指定のドメインに属している（属していない）クライアントの場合
コンピュータ名マスク（指定）	コンピュータ名が指定の名前である場合
クライアント名マスクIN（指定）	クライアント名が指定のクライアント名である場合
HAS IPv4マスク（指定）	指定のIPv4 アドレスとマスクで定義されたグループに属するクライアントの場合
HAS IPv4範囲（指定）	指定のIPv4 アドレスの範囲で定義されたグループに属するクライアントの場合
HAS IPv6ネットワーク識別（指定）	指定のIPv6 アドレスとマスクで定義されたグループに属するクライアントの場合
HAS IPv6範囲（指定）	指定のIPv6 アドレスの範囲で定義されたグループに属するクライアントの場合
HAS 定義済みポリシー（指定）	指定のポリシーを使用している（使用していない）クライアントの場合
製品名 IN	製品名が指定の名前である（ない）場合
製品バージョンIS（指定）	製品バージョンが指定のバージョンである（ない）場合
クライアントのカスタム情報1マスクIN	クライアントのカスタム情報に指定のマスクが含まれる（含まれない）場合
クライアントのカスタム情報2マスクIN	クライアントのカスタム情報に指定のマスクが含まれる（含まれない）場合
クライアントのカスタム情報3マスクIN	クライアントのカスタム情報に指定のマスクが含まれる（含まれない）場合
クライアントのコメントマスクIN	クライアントのコメント情報に指定のマスクが含まれる（含まれない）場合
HAS（NOT）保護状態（指定）	クライアントの保護状態が指定の状態である（ない）場合
定義データベースのバージョンIS（指定）	ウイルス定義データベースが指定のバージョンである（ない）場合
最終アクセス ISが（指定）より古い	前回の接続が指定の時刻より前（後）の場合
IS 再起動待ち	クライアントが再起動を待機している場合（待機していない場合）
サーバーローカル時刻IN	サーバーのローカル時刻が指定時間内である（ない）場合

ポリシールールは、.xmlファイルとの間でインポートまたはエクスポートできるほか、ポリシールールウィザードを使用して自動的に作成することもできます。このウィザードでは、既存のグループ構造に基づいてポリシー構造を作成し、対応するポリシールールを作成して、作成したポリシーをグループに関連付けることができます。ポリシールールのインポートとエクスポートの詳細については、「ポリシーのインポート/エクスポート」を参照してください。

ポリシールールを削除するには、ポリシーマネージャのウィンドウで [削除] ボタンをクリックします。すべてのルールを直ちに適用するには、[ポリシールールを今すぐ実行] をクリックします。

ポリシールールウィザード

ポリシールールウィザードでは、既存のグループ構造に基づいてポリシー構造を作成できます。また、作成したポリシーに対応するポリシールールを作成することで、そのポリシーをグループに関連付けることができます。

1 最初の手順では、まずグループの編成を求められます。目的のグループ構造設定が存在しない場合は、グループマネージャボタンをクリックして、まずグループを設定します。それから、次へをクリックします。

2 2番目の手順では、新しいポリシールールの影響を受けるクライアントグループのカテゴリーを指定するように求められます。目的のチェックボックスを選択してから次へをクリックします。

3 親ポリシーの選択

4 最終手順では、単純なプロセスステータスメッセージが表示されます。終了ボタンをクリックして、ポリシールールウィザードウィンドウを閉じます。

ポリシールールタブで、新しいポリシールールがリストに表示されます。ルール名の横にあるチェックボックスをクリックして、特定のルールを有効にします。

ポリシールールのインポートとエクスポートおよび名前の競合の詳細については、ポリシーのインポート/エクスポートを参照してください。

5.3.8 ポリシーの削除

ルールの作成と同様、ポリシーの削除は、現在接続しているサーバーに存在するものについてのみ可能です。他のサーバーからポリシーを削除するには、ERACを使用してそのサーバーに直接接続する必要があります。

NOTE

ポリシーは、親ポリシー、下位サーバーの既定のポリシー、プライマリクライアントの既定のポリシーなどとして、他のサーバーやポリシーにリンクしていることがあります。したがって、削除ではなく、他のポリシーへの置き換えが必要な場合があります。削除および置き換えのオプションを確認するには、[ポリシーの削除] ボタンをクリックします。目的のポリシーがポリシー階層の中で占める位置によっては、以下の説明にあるオプションの中には利用できないものがあります。

削除対象のポリシーのプライマリクライアントに適用する新しいポリシー	削除するポリシーに代わり、新しいポリシーをプライマリクライアントに対して選択できます。プライマリクライアントには、プライマリクライアントの既定のポリシーを適用できるほか、そのクライアントと同じサーバーにある他のポリシーも適用できます（[クライアントの追加] による手動割り当てまたは [ポリシールール] による強制適用）。置き換えて新たに適用するポリシーとしては、指定のサーバーにあるあらゆるポリシーまたは複製したポリシーを使用できます。
削除対象のポリシーの子ポリシーに適用する新しい親ポリシー	削除するポリシーが他の子ポリシーの親ポリシーとなっている場合は、その親ポリシーに代替のポリシーを指定する必要があります。その場合、そのサーバーにあるポリシーまたは上位サーバーから複製したポリシーで代替できますが、N/A フラグを設定することでその子ポリシーには代替ポリシーを割り当てないことも可能です。子ポリシーが存在しない場合でも、代替のポリシーを割り当てることを強くお勧めします。この削除プロセスを実行しているときに、他のユーザーがそのポリシーに子ポリシーを割り当てると競合の原因となるからです。
現在削除／変更されているポリシーの複製クライアントに適用する新しいポリシー	この場合は、下位サーバーから複製したクライアントの新しいポリシーを選択できます。これは、現在削除しようとしているポリシーに適用されていたものです。置き換えて新たに適用するポリシーとしては、指定のサーバーにあるあらゆるポリシーまたは複製したポリシーを使用できます。
下位サーバの新しい既定のポリシー	削除するポリシーが仮想ポリシー（「グローバルポリシー設定」を参照）として機能している場合は、他のポリシーで代替する必要があります（詳細については「仮想ポリシー」を参照してください）。置き換えて新たに適用するポリシーとしては、指定のサーバーにあるあらゆるポリシーまたは N/A フラグを使用できます。
プライマリクライアントの新しい既定のポリシー	削除するポリシーが仮想ポリシー（「グローバルポリシー設定」を参照）として機能している場合は、他のポリシーで代替する必要があります（詳細については「仮想ポリシー」を参照してください）。同じサーバーにあるポリシーで置き換えることができます。

ポリシーの [複製可能なポリシーを下に移動する] オプションを無効にして [OK] または [適用] をクリックした場合、またはポリシーツリーから他のポリシーを選択した場合も、同じダイアログが表示されます。これによって、[ポリシーが現在削除または変更されている複製クライアントに適用する新しいポリシー] または [下位サーバの新しい既定のポリシー] が有効になります。

5.3.9 特殊設定

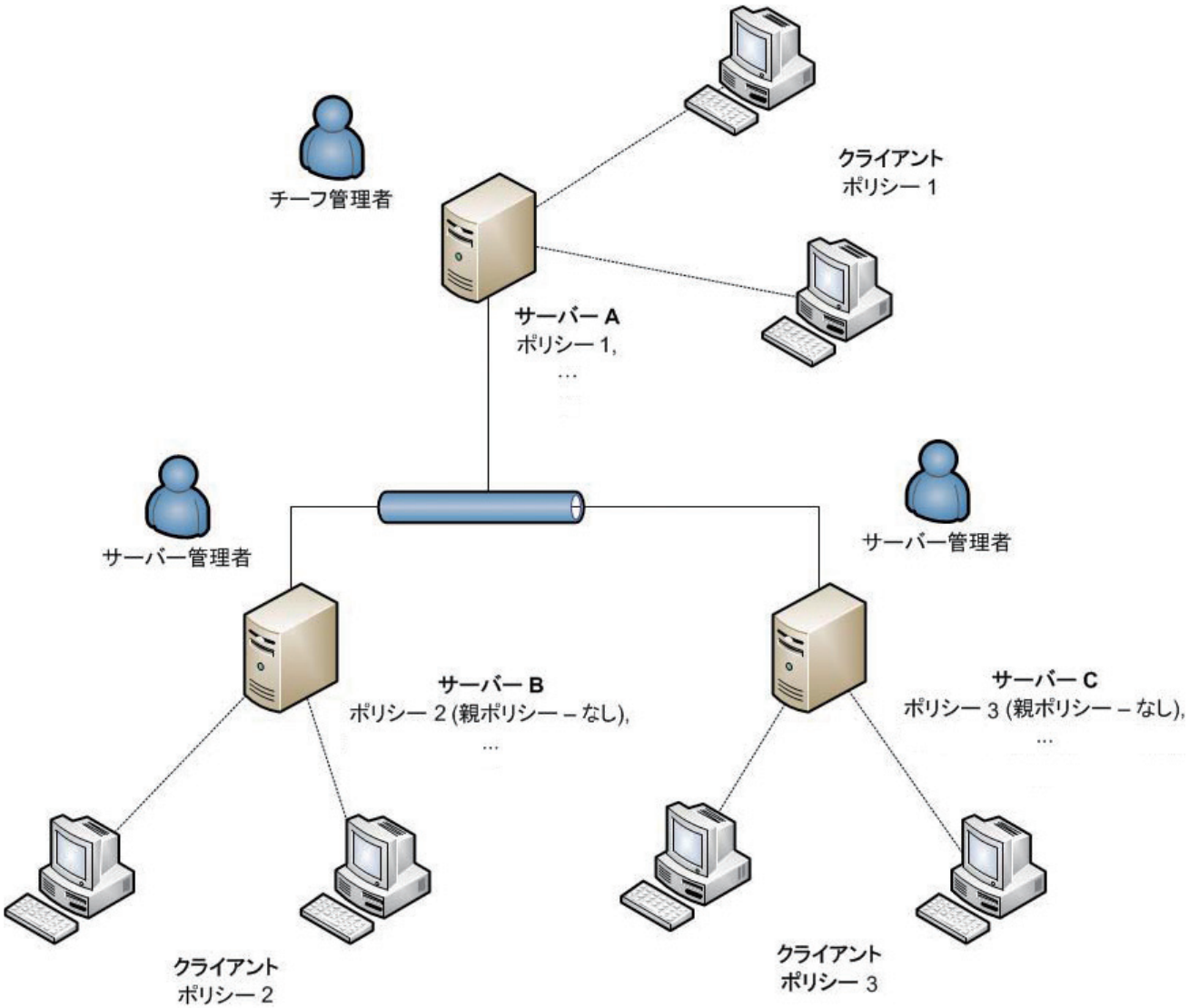
ポリシーに関連する次の2つの特殊設定は、ポリシーマネージャではなく、[ツール] -> [サーバオプション] -> [詳細] -> [詳細設定を編集] -> [ESET Remote Administrator] -> [ERAサーバー] -> [設定] -> [ポリシー] にあります。

ポリシー適用の間隔（分）	この機能は、指定した間隔でポリシーに適用されます。既定の設定をお勧めします。
ポリシーの使用を無効にする	このオプションを有効にすると、サーバーへのポリシーの適用がキャンセルされます。ポリシーに問題がある場合、このオプションを使用することをお勧めします。ポリシーを適用しないクライアントを一部のクライアントに限定するには、空のポリシーを割り当てる方法をお勧めします。

5.3.10　ポリシー展開のシナリオ

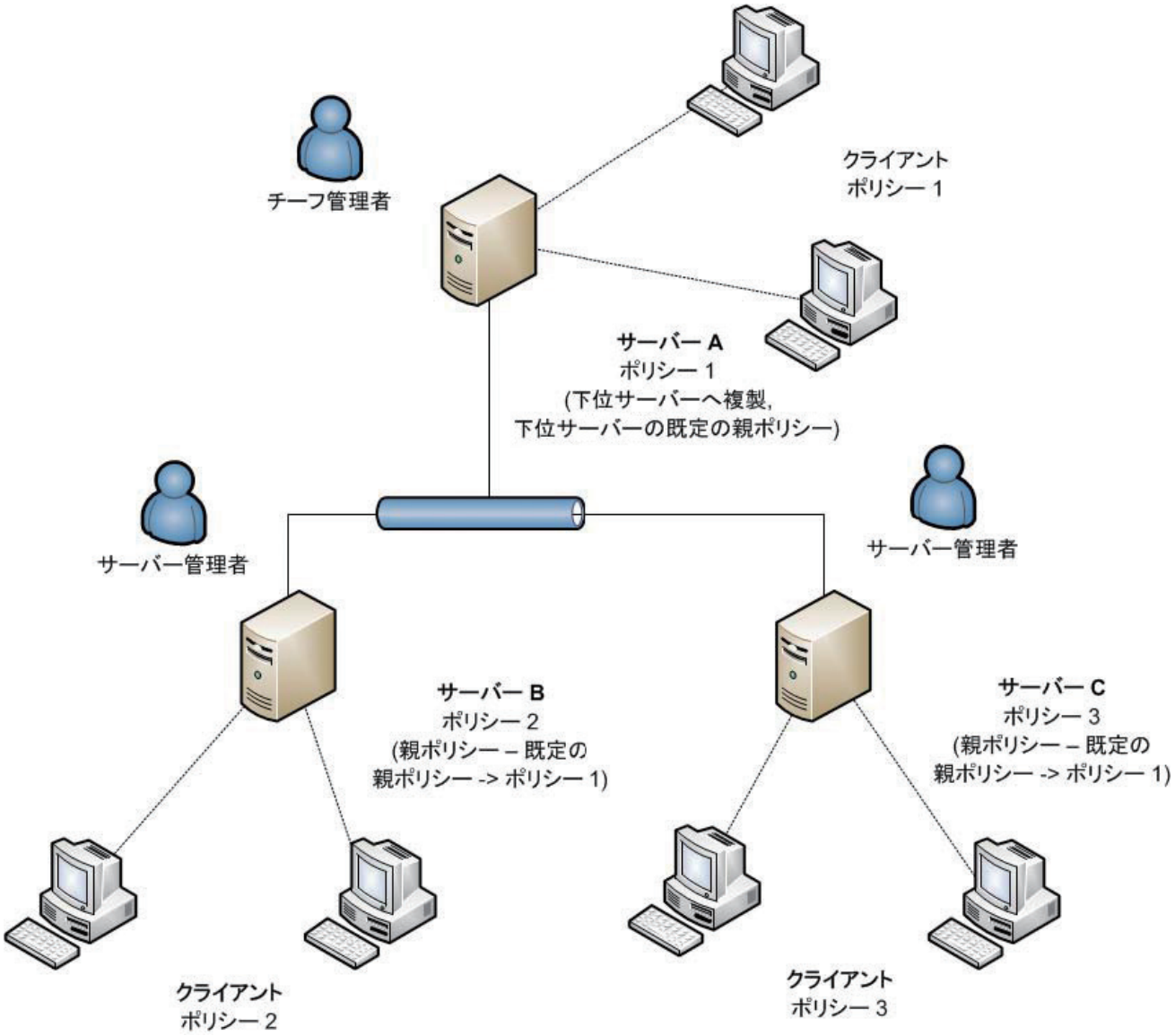
5.3.10.1　各サーバーがスタンドアロンの単位で存在し、ポリシーをローカルで定義

このシナリオを理解するために、1台のメインサーバーと2台の下位サーバーで構成する小規模なネットワークを考えます。各サーバーにはいくつかのクライアントが存在します。サーバーごとに、1つ以上のポリシーが作成されています。下位サーバーは別々の支社に設置されていて、いずれもそれぞれのローカル管理者の管理下にあります。各管理者は、それぞれのサーバーに接続するクライアントごとに割り当てるポリシーを決定します。メインの管理者は、ローカル管理者が決定するコンフィグレーションには介入せず、下位サーバーのクライアントにはポリシーを一切割り当てません。サーバーポリシーの観点からこのネットワークを見ると、サーバーAには下位サーバーの既定のポリシーが存在しないことになります。また、サーバーBとサーバーCには、N/Aフラグ、または既定の親ポリシーとは別のローカルポリシーが親ポリシーとして設定されているということにもなります（たとえば、サーバーBとサーバーCには、上位サーバーから割り当てられた親ポリシーが存在していません）。



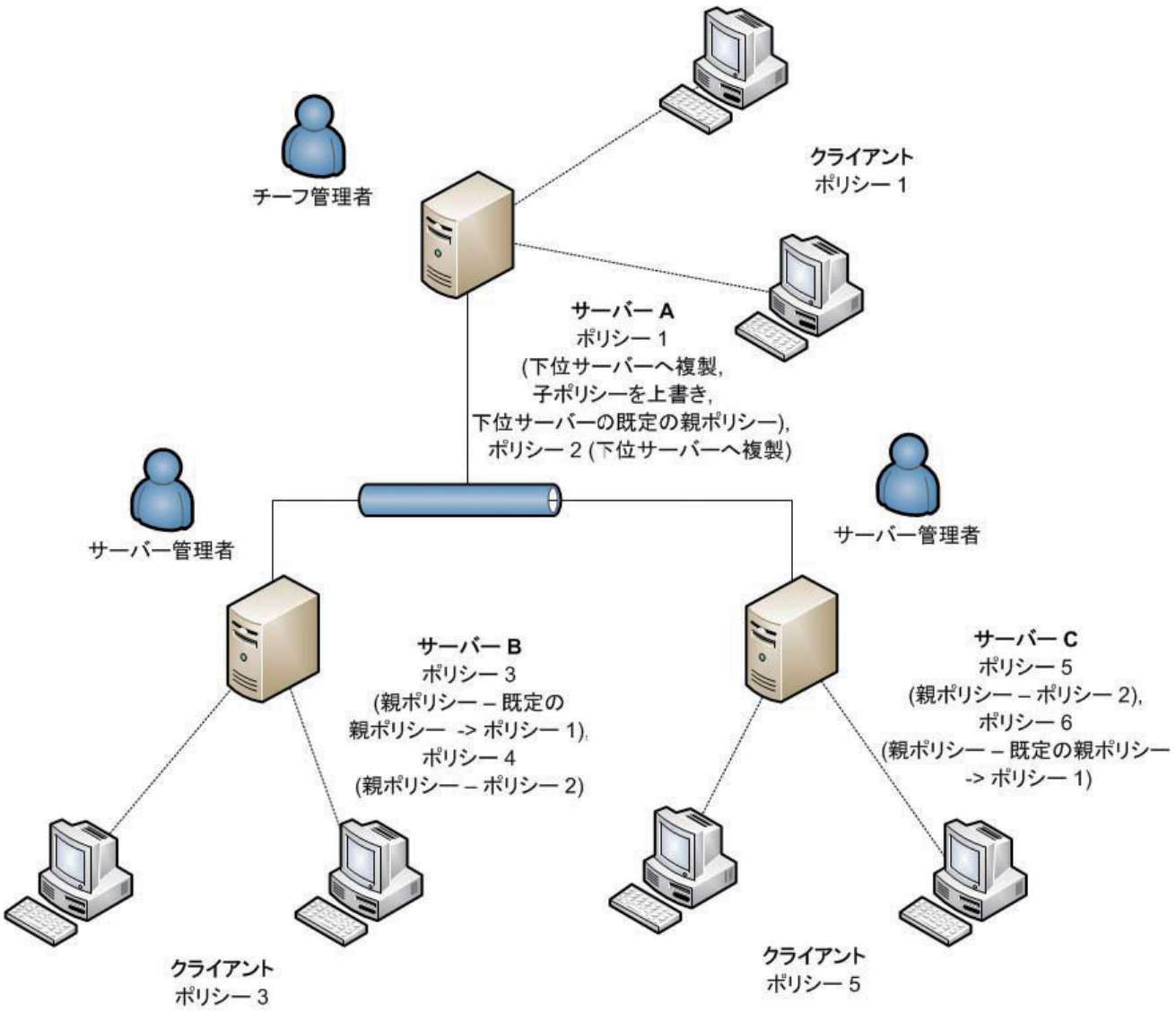
5.3.10.2 各サーバーの個別管理-ポリシーをローカルで管理するが、既定の親ポリシーを上位サーバーから継承

このシナリオにも、前のシナリオのコンフィグレーションが適用されます。ただし、サーバーAでは下位サーバーの既定のポリシーが有効になっており、下位サーバーのポリシーには、マスタサーバーから既定の親ポリシーのコンフィグレーションが継承されています。このシナリオでは、ポリシー設定の面でローカル管理者に大きな自由度が与えられています。下位サーバーの子ポリシーに既定の親ポリシーを継承できる一方、ローカル管理者はそのポリシーを変更して独自のポリシーを作成することもできます。



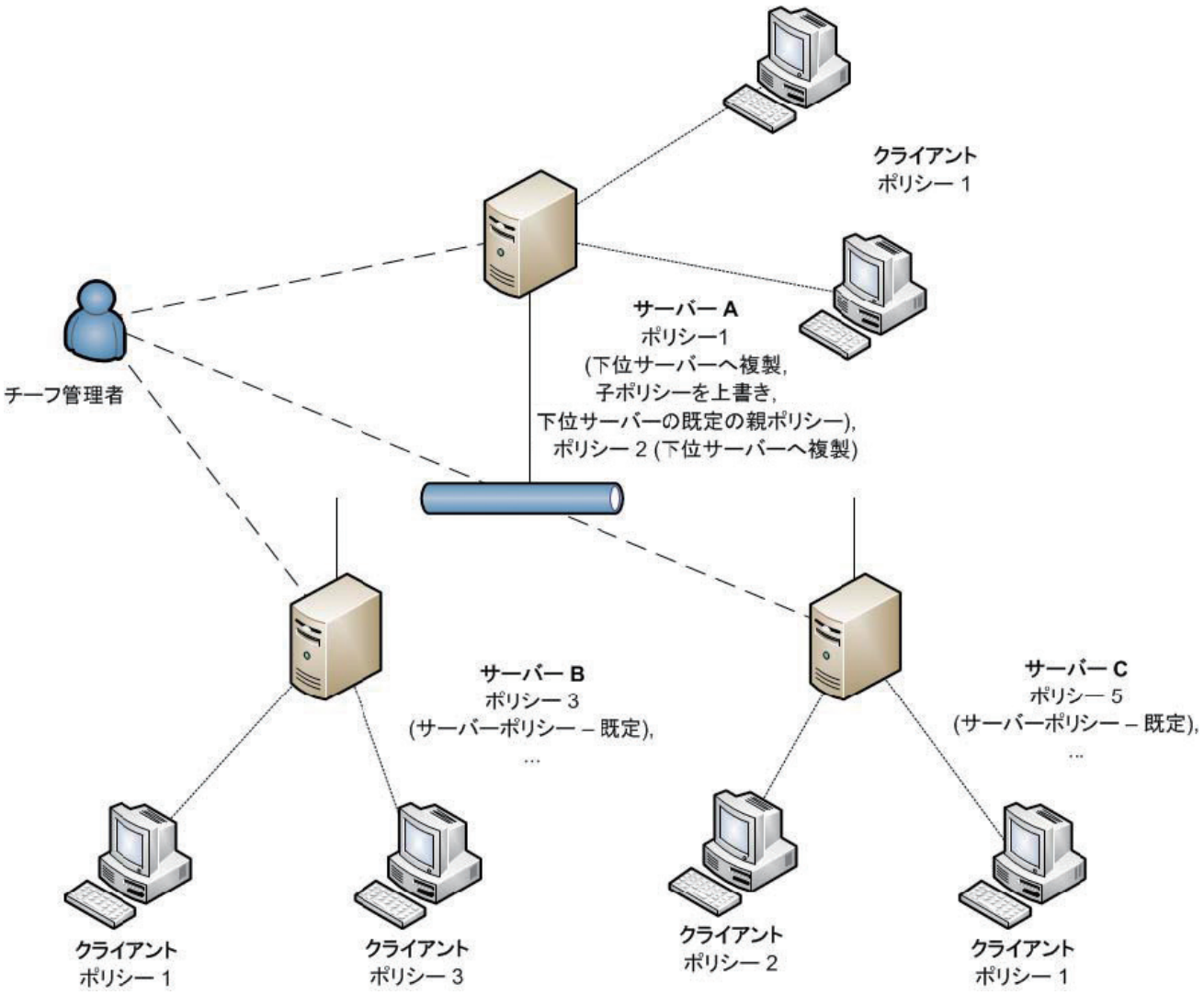
5.3.10.3　上位サーバーからのポリシーの継承

このシナリオのネットワークモデルは、前の2つのシナリオと同じです。また、マスタサーバーには、既定の親ポリシーのほかに、下位に複製可能で下位サーバーの親ポリシーとして機能するポリシーもあります。ポリシー 1（下の図を参照）では、[子ポリシーを上書きする] 属性が有効になっています。ここでもローカル管理者には大きな自由度がありますが、下位に複製するポリシー、およびローカルポリシーの親ポリシーとして機能するポリシーはメインの管理者が定義します。[子ポリシーを上書きする] 属性は、選択したポリシーのコンフィグレーションが、ローカルサーバーでのコンフィグレーションより優先することを示します。



5.3.10.4 上位サーバーのみからのポリシーの割り当て

このシナリオは、ポリシー管理の中央集中型システムです。クライアントのポリシーの作成、変更、および割り当てはメインサーバーのみで行われ、ローカル管理者にはこれらのポリシーを変更する権限がありません。すべての下位サーバーでは、内容が空の基本的な1つのポリシー（既定ではサーバーポリシーというタイトル）のみを保持します。このポリシーは、プライマリクライアントの既定の親ポリシーとして機能します。



5.3.10.5 ポリシールールの使用

この例では、ポリシールールに基づいてポリシーを自動的に割り当てる方法を扱います。この方法は、単独のシナリオとして使用するのではなく、これまでに説明した各種シナリオと組み合わせ、それらを補うように使用します。

ローカル管理者がそれぞれのサーバーを管理している場合、それぞれのローカル管理者がそのクライアントに個別のポリシールールを作成できます。このシナリオでは、ポリシールールどうしが競合していないことが重要です。たとえば、ポリシールールに基づいて上位サーバーがクライアントにポリシーを割り当てる場合、同時に下位サーバーがローカルのポリシールールに基づいて別のポリシーを割り当てると競合が発生します。

中央集中型システムでは、管理プロセス全体をメインサーバーで扱うので、競合が発生する可能性は大幅に低くなります。

5.3.10.6 グループの使用

状況によっては、クライアントのグループにポリシーを割り当てることで、これまでのシナリオを補うことができます。グループは手動で作成できるほか、[Active Directoryの同期] オプションを使用して作成することもできます。

クライアントは手動でグループに追加することも（静的グループ）、グループのプロパティによって自動的に追加することもできます（パラメータグループ）。詳細については、「グループマネージャ」を参照してください。

クライアントのグループにポリシーを割り当てるには、ポリシーマネージャ（[クライアントの追加] -> [指定追加]）で一時的な割り当てオプションを使用するか、ポリシールールを使用して自動的にポリシーを配布します。

次のようなシナリオを考えます。

それぞれ別々のADグループに属するクライアントごとに異なるポリシーを割り当て、別のADグループにクライアントが移動したときには、クライアントのポリシーを自動的に変更できるようにすることを管理者が計画しているとします。

1. まず、グループマネージャで、[Active Directoryの同期] をニーズに従って設定します。ここで重要なのは、ADの同期スケジュールを適切に設定することです（使用可能なオプションは、毎時、日毎、週毎、月毎です）。
2. 最初の同期が正常に完了すると、[静的グループ] セクションにADグループが表示されます。
3. 新しいポリシールールを作成し、ルールの条件として [ERAグループIN] や [ERAグループNOT IN] を指定します。
4. 条件に追加するADグループを指定します。
5. 次に、ルールの条件に一致するクライアントに適用するポリシーを定義し、[OK] をクリックしてルールを保存します。

NOTE

手順3 ～ 5を実行する代わりに、ポリシールールウィザードを使用できます。このウィザードでは、既存のグループ構造に基づいてポリシー構造を作成できます。また、作成したポリシーに対応するポリシールールを作成することで、そのポリシーをグループに関連付けることができます。

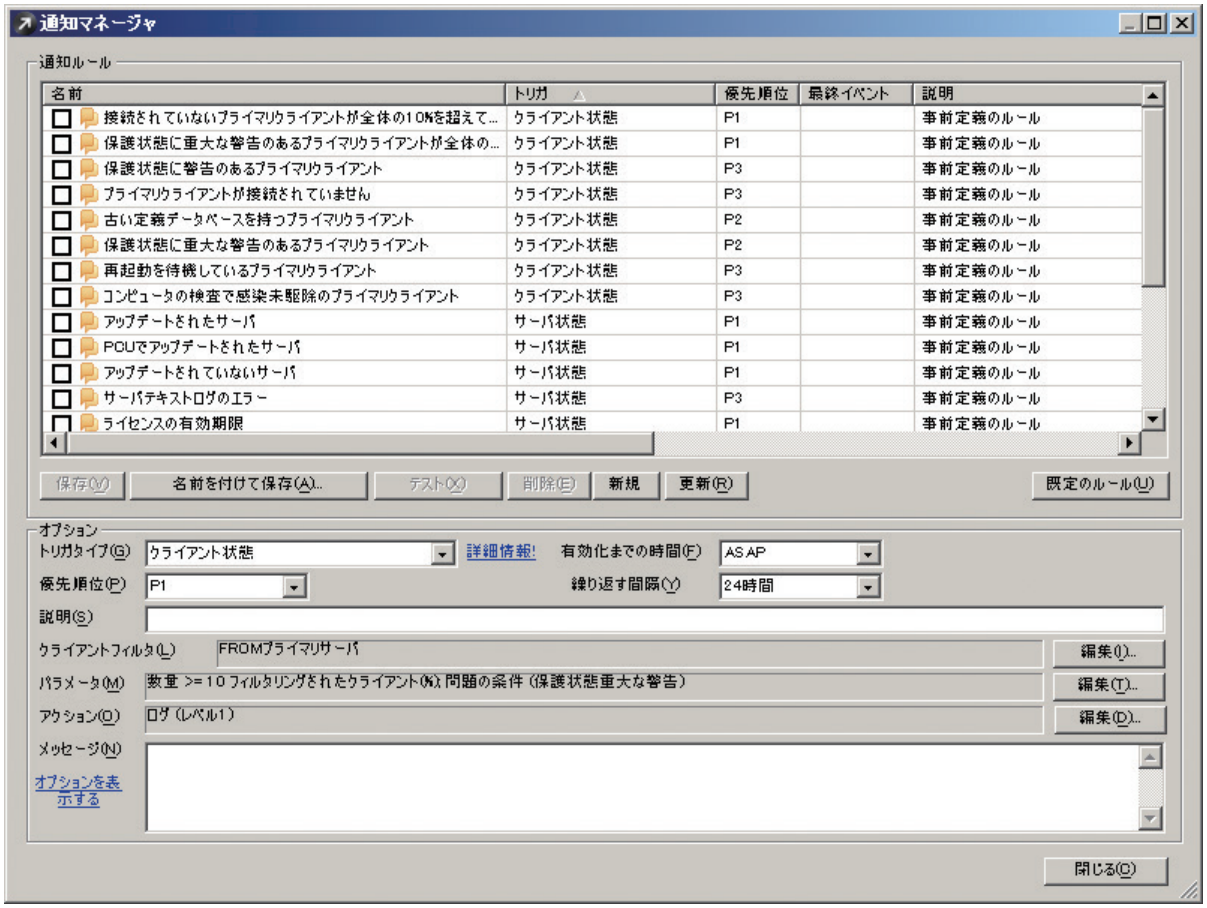
このようにして、ADグループごとに特定のポリシールールを定義できます。特定のクライアントへの特定のポリシーの割り当ては、特定のADグループにおけるクライアントのメンバシップによって決まります。ADの同期は定期的に実行されるようにスケジュールされているので、ポリシールールが適用されるときには、クライアントのADグループのメンバシップに発生した変更がすべて更新されたうえで考慮されます。つまり、ポリシーは、ADグループに応じて自動的にクライアントに適用されます。ルールとポリシーをすべて定義しておけば、以降は管理者がポリシーの適用に関して何らか操作する必要はありません。

この方法の主な利点は、ADグループのメンバシップとポリシーの割り当てが直接、自動的にリンクされる点です。

5.4 通知マネージャ

システム管理者およびネットワーク管理者に重要なイベントについて通知する機能は、ネットワークのセキュリティおよび整合性において不可欠な側面です。エラーコードや悪意のあるコードに関する早期の警告によって、後で問題を解消するために必要となる時間と経費の膨大な損失を防ぐことができます。次の3つのセクションでは、ERAで提供される通知オプションの概要を示します。

[通知マネージャ] のメインウィンドウを開くには、[ツール] -> [通知マネージャ] をクリックします。



メインウィンドウは、2つのセクションに分かれています。

1. ウィンドウ上部の [通知ルール] セクションには、既存の (事前定義またはユーザー定義の) ルールのリストが表示されます。通知メッセージを生成するには、このセクションのルールを選択する必要があります。既定では、有効になっている通知はありません。そのため、目的のルールがアクティブであるかどうかを確認することをお勧めします。ルールのリストの下にある機能ボタンには、[保存] (ルールに対する変更の保存)、[名前を付けて保存...] (ルールに対する変更を新しい名前で保存)、[削除]、[既定に戻す] (選択したトリガタイプの既定の設定を復元)、[更新]、および [既定のルール] (既定のルールでリストを更新) があります。

既定では、[通知マネージャ] ウィンドウには、事前定義のルールが含まれています。ルールを有効にするには、そのルールの横にあるチェックボックスをオンにします。指定可能な通知ルールは、次のとおりです。これらのルールが有効になっていて、ルール条件が満たされる場合、ログエントリが生成されます。

接続されていないプライマリクライアントが全体の10%を超えている	10%を超えるクライアントが1 週間以上サーバーに接続されていない場合、ルールがすぐに実行されます。
保護状態に重大な警告のあるプライマリクライアントが全体の10%を超えている	10%を超えるクライアントで、保護状態の重大な警告が生成され、1 週間以上サーバーに接続されていない場合、ルールがすぐに実行されます。
保護状態に警告のあるプライマリクライアント	サーバーに1 週間以上接続されていない保護状態の警告があるプライマリクライアントが1 台以上ある場合。
プライマリクライアントが接続されていません	サーバーに1 週間以上接続されていないクライアントが1 台以上ある場合。
古い定義データベースを持つプライマリクライアント	ウイルス定義データベースが現在のバージョンより2 バージョン以上古いクライアントがあって、そのクライアントが1 週間以上サーバーから切断されていない場合。
保護状態に重大な警告のあるプライマリクライアント	1 週間以上サーバーから切断されていない保護状態の重大な警告があるクライアントがある場合。
再起動を待機しているプライマリクライアント	再起動を待機しているクライアントがあって、そのクライアントが1 週間以上サーバーから切断されていない場合。
コンピュータの検査で感染未駆除のプライマリクライアント	コンピュータの検査で駆除できなかった侵入物が1 つ以上存在するクライアントがあって、そのクライアントが1 週間以上サーバーから切断されていない場合、ルールがすぐに実行されます。
アップデートされたサーバ	サーバーがアップデートされた場合。
PCUでアップデートされたサーバ	PCUでサーバーがアップデートされた場合。
アップデートされていないサーバ	サーバーが6 日以上アップデートされていない場合、ルールがすぐに実行されます。
サーバテキストログのエラー	サーバーのログにエラーエントリが含まれる場合。
ライセンスの有効期限	現在のライセンスが今後20 日以内に期限切れになる状態にあり、その期限切れの後に、クライアントスロットの最大数が現在のクライアント数を下回る場合、ルールがすぐに実行されます。
ライセンスの制限	空きクライアントスロット数が、使用可能なすべてのクライアントスロット数の10%を下回る場合。
新規ウイルスログ	新規に検出されたウイルスのログ
ウイルス大規模感染の可能性	すべてのクライアントの10%以上で、クライアントのウイルスログエントリに記録されている重大な警告の頻度が1 時間に1,000 件を超える場合。
ネットワーク攻撃の可能性	すべてのクライアントの10%以上で、クライアントのESET パーソナルファイアウォールのログエントリに記録されている重大な警告の頻度が1 時間に1,000 件を超える場合。
新しいプライマリクライアント	新規クライアントがサーバーに接続された場合、ルールがすぐに実行されます。
新しく複製されたクライアント	クライアントのリストに新しく複製されたクライアントがある場合、ルールが1 時間後に実行されます。
完成したタスク	クライアントで完了したタスクがある場合、ルールがすぐに実行されます。

特に示されていない場合、すべてのルールは24時間後に実行および繰り返され、プライマリサーバーおよびプライマリクライアントに適用されます。

2.ウィンドウの下半分の [オプション] セクションには、現在選択されているルールに関する情報が表示されます。このセクション内のすべてのフィールドおよびオプションについては、「ルールの作成」でサンプルのルールを使用して説明しています。

各ルールで、[トリガ] と呼ばれる、ルールを有効にする基準を指定できます。指定可能なトリガは、次のとおりです。

クライアント状態	一部のクライアントで問題が発生した場合にルールが実行されます。
サーバ状態	一部のサーバーで問題が発生した場合にルールが実行されます。
終了したタスクイベント	指定されたタスクの終了後にルールが実行されます。
新規クライアントイベント	新規クライアントがサーバーに接続された場合にルールが実行されます（複製されたクライアントを含む）。
大規模感染イベント	多数のクライアントで大規模感染事件が発生した場合にルールが実行されます。
受信ログイベント	管理者が一定の時間内のログについての通知を受けるようにする場合にルールが実行されます。

トリガの種類に基づいて他のルールオプションの有効化または無効化が可能なので、新しいルールの作成時にはまずトリガの種類を設定することをお勧めします。
[優先順位] ドロップダウンメニューを使用すると、ルールの優先順位を選択できます。[P1] が優先順位の最上位で、[P5] が優先順位の最下位です。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。通知メッセージに優先順位を割り当てるには、%PRIORITY%変数を使用します。[優先順位] メニューの下に、[説明] フィールドがあります。各ルールに、「検出された侵入物に関して警告するルール」など、意味のある説明を付けることをお勧めします。

通知の形式は、通知マネージャのメインウィンドウの下部のセクションにある [メッセージ] フィールドで編集できます。テキストには、特殊変数%VARIABLE_NAME%を使用できます。使用可能な変数のリストを表示するには、[オプションを表示する] をクリックします。

●Rule_Name
●Rule_Description
●Priority－通知ルールの優先順位
●Triggered－前回の通知が送信された日付（繰り返しは除外）
●Triggered_Last－前回の通知が送信された日付（繰り返しを含む）
●Client_Filter－クライアントフィルタパラメータ
●Client_Filter_Short－クライアントフィルタの設定（短縮形式）
●Client_List－クライアントのリスト
●Parameters－ルールパラメータ
●Primary_Server_Name－このサーバーの名前
●Server_Last_Updated－サーバーの前回のアップデート
●Virus_Signature_Db_Version－ウイルス定義データベースの最新バージョン
●Pcu_List-最新PCUリスト
●Pcu_List_New_Eula-新しいEulaを含む最新のPCUリスト
●Last_Log_Date－前回のログの日付
●Log_List-問題のあるログのリスト
●Log_List_Full-ヘッダーおよび詳細な情報のついた問題のあるログのリスト
●Task_Result_List－完了したタスクのリスト
●Log_Text_Truncated－通知を有効にしたログテキスト（切り詰め）
●License_Info_Merged－ライセンス情報（概要）
●License_Info_Full－ライセンス情報（完全）
●License_Days_To_Expiry－有効期限までの日数
●License_Expiration_Date－最も近い期限
●License_Clients-ライセンスクライアント
●License_Customer-ライセンス顧客
●License_Clients_Left－現在のライセンスでサーバーに接続可能なクライアントの空きスロット数
●Actual_Clients_Count－サーバーに現在接続されているクライアント数

5.4.1　クライアント状態

[クライアントフィルタ] ウィンドウで、クライアントフィルタのパラメータを定義します。ルールの適用時には、クライアントフィルタ条件を満たすクライアントのみが考慮されます。フィルタ基準は次のとおりです。

FROMプライマリサーバ	プライマリサーバーのクライアントのみ（否定の NOT FROM も適用できます）。
プライマリサーバIN	出力にプライマリサーバーを含めます。
HAS新規フラグ	" 新規 " フラグが付いているクライアント（否定の HAS NOT も適用できます）。
対象のERAグループ	指定されたグループに属するクライアント。
ドメイン/ワークグループIN	指定されたドメインに属するクライアント。
コンピュータ名マスクIN	指定されたコンピュータ名を持つクライアント。
HAS IPv4マスク	指定された IPv4 マスクに該当するクライアント。
HAS IPv4範囲	指定された IPv4 アドレス範囲内のクライアント。
HAS IPv6ネットワーク識別	特定の IPv6 ネットワークの識別コードを持つクライアント。
HAS IPv6範囲	指定された IPv6 アドレス範囲内のクライアント。
HAS定義済みポリシー	指定されたポリシーが割り当てられているクライアント（否定の HAS NOT も適用できます）。

通知ルールにクライアントフィルタを指定したら、[OK] をクリックしてルールパラメータに進みます。クライアントパラメータによって、通知アクションを実行するためにクライアントまたはクライアントグループが満たす必要のある条件が定義されます。指定可能なパラメータを表示するには、[パラメータ] セクションの [編集...] ボタンをクリックします。

どのパラメータが使用できるかは、選択したトリガの種類によって異なります。クライアント状態のトリガに使用可能なパラメータは、次のとおりです。

HAS 保護状態に警告がある	[保護状態] カラムで検出されたあらゆる警告。	
HAS 保護状態に重大な警告がある	[保護状態] カラムで検出された重大な警告。	
HAS 定義データベースのバージョン	ウイルス定義データベースに関する問題（指定可能な値は次の 6 つ）。	
	前のバージョン	ウイルス定義データベースのバージョンが現在のものより 1 つ古い。
	古いバージョンまたは N/A	ウイルス定義データベースのバージョンが現在のものより 2 つ以上古い。
	5 バージョンより古い、もしくは N/A	ウイルス定義データベースのバージョンが現在のものより 6 つ以上古い。
	10 バージョンより古い、もしくは N/A	ウイルス定義データベースのバージョンが現在のものより 11 以上古い。
	7 日間より前、もしくは N/A	ウイルス定義データベースのバージョンが現在のものより 8 日以上古い。
	14 日間より前、もしくは N/A	ウイルス定義データベースのバージョンが現在のものより 15 日以上古い。
HAS 最終アクセス警告	前回の接続が、指定された期間より前に確立されています。	
HAS 最終脅威イベント	[ウイルス] カラムにウイルス警告があります。	
HAS 最終イベント	[最終イベント] カラムにエントリがあります。	
HAS 最終ファイアウォールイベント	[ファイアウォールイベント] カラムにファイアウォールイベントエントリがあります。	
HAS 新規フラグ	クライアントに [新規] フラグが設定されています。	
IS再起動待ち	クライアントは再起動を待機しています。	
HAS 最新の検査結果でウイルスが検出されている	クライアントで前回のスキャン時に、指定された数のウイルスが検出されました。	
HAS 最新の検査でウイルスが未駆除のままになっている	クライアントで前回のスキャン時に、指定された数の駆除されていないウイルスが検出されました。	

すべてのパラメータを否定で指定できますが、すべての否定を使用できるというわけではありません。trueおよびnot trueの2つの論理値を使用できるパラメータでのみ、否定を指定することをお勧めします。たとえば、[[新規] フラグ有り] パラメータでは、[新規] フラグが付いているクライアントのみが対象となります。このパラメータに否定的な値を指定すると、このフラグが付いていないすべてのクライアントが対象となります。

上記の条件はすべて、論理的に組み合わせたり逆にしたりできます。[ルールを適用するタイミング] ドロップダウンメニューには、選択肢として次の2つが用意されています。

すべてのオプションが一致	指定されたパラメータがすべて一致した場合にのみルールが実行されます。
いずれかのオプションが一致	少なくとも 1 つの条件が満たされた場合にルールが実行されます。

ルールに指定されているパラメータが満たされると、管理者によって定義されているアクションが自動的に実行されます。アクションを設定するには、[アクション] セクションの [編集...] をクリックします。

ルールの有効化は1時間から3ヶ月までの期間、遅延できます。すぐにルールを有効化する場合は、[有効化までの時間] ドロップダウンメニューで [ASAP] を選択します。既定では、[通知マネージャ] は10分ごとに有効化されるため、[ASAP] を選択した場合、タスクは10分以内に実行されます。このメニューから特定の時間を選択した場合は、その時間が経過したときにアクションが自動的に実行されます (ルールの条件が満たされた場合)。

[繰り返す間隔...] メニューを使用すると、アクションを繰り返す間隔を指定できます。ただし、ルールを有効にする条件が満たされる必要があります。[ERAサーバ] -> [詳細] -> [詳細設定を編集] -> [ESET Remote Administrator] -> [サーバ] -> [設定] -> [通知] -> [通知処理の間隔 (分)] の順にクリックして、サーバーがアクティブなルールを確認して実行する間隔を指定できます。

既定値は10分です。この既定値を短くしないことをお勧めします。サーバーの性能が大きく低下する可能性があるためです。

5.4.2 サーバー状態

[サーバルールパラメータ] ウィンドウでは、特定のサーバー状態に関連するルールのトリガとなるパラメータを設定できます。このルールがトリガされると、通知が送信されます。パラメータを設定するには、特定の条件の横にあるラジオボタンをクリックします。これで、その隣にあるGUI要素がアクティブになり、条件のパラメータを変更できるようになります。

アップデートされたサーバ	サーバーが最新状態です。		
アップデートされていないサーバ	サーバーがアップデートされていない期間が、指定された期間を超えています。		
監査ログ	[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と実行されたアクションを監視して記録します。ログエントリをタイプでフィルタリングすることができます。[サーバログ] を参照してください。		
サーバログ	サーバログに次のエントリの種類が含まれています。		
	エラー	エラーメッセージ	
	エラー+警告	エラーメッセージと警告メッセージ	
	エラー＋警告＋情報 (レベル 2)	エラーメッセージ、警告メッセージおよび情報を伝えるメッセージ	
	ログエントリをタイプでフィルタリングする	サーバログで監視するエラーおよび警告のエントリを指定する場合はこのオプションを有効にします。通知が正常に機能するように、ログレベル ([ツール]- > [サーバオプション]- > [ログ]) を対応するレベルに設定する必要があります。指定可能なログエントリは、次のとおりです。	
		ADSI_SYNCHRONIZE	Active Directory グループ同期
		CLEANUP	サーバーのクリーンアップタスク
		CREATEREPORT	オンデマンドのレポート生成
		DEINIT	サーバーのシャットダウン
		INIT	サーバーの起動
		INTERNAL 1	内部サーバーメッセージ
		INTERNAL 2	内部サーバーメッセージ
		LICENSE	ライセンス管理
		MAINTENANCE	サーバーの保守タスク
		NOTIFICATION	通知管理
		PUSHINST	プッシュインストール
		RENAME	内部構造の名前変更
		REPLICATION	サーバーの複製
		POLICY	ポリシー管理
		POLICYRULES	ポリシールール
		SCHEDREPORT	自動的に生成されたレポート
		SERVERMGR	内部サーバースレッド管理
		SESSION	サーバーのネットワーク接続
		SESSION_USERACTION	さまざまなユーザーアクション
		THREATSENSE	ThreatSense.Net- 統計情報の提出
		UPDATER	サーバーのアップデートおよびミラーの作成

役に立つパラメータの例として [UPDATER] があります。[通知マネージャ] がサーバログでアップデートおよびミラー作成に関連する問題を検出したときに、このパラメータによって通知メッセージが送信されます。

ライセンスの有効期限	ライセンスは、指定された日数後に期限切れになるか、またはすでに期限切れになっています。期限切れによってライセンスのクライアント数が現在接続されているクライアント数を下回る場合に通知を送信するには、[ライセンスのクライアント数がサーバーデータベースの実際のクライアント数を下回る場合にのみ警告する] を選択します。
制限ライセンス	空きクライアントの割合が指定された値を下回る場合。

ルールに指定されているパラメータが満たされると、管理者によって定義されているアクションが自動的に実行されます。アクションを設定するには、[アクション] セクションの [編集...] をクリックします。

ルールの有効化は、1時間から3カ月までの期間、遅延できます。すぐにルールを有効化する場合は、[有効化までの時間] ドロップダウンメニューで [ASAP] を選択します。既定では、[通知マネージャ] は10分ごとに有効化されるため、[ASAP] を選択した場合、タスクは10分以内に実行されます。このメニューから特定の時間を選択した場合は、その時間が経過したときにアクションが自動的に実行されます (ルールの条件が満たされた場合)。

[繰り返す間隔...] メニューを使用すると、アクションを繰り返す間隔を指定できます。ただし、ルールを有効にする条件が満たされる必要があります。[ツール] -> [サーバオプション] -> [詳細] -> [詳細設定を編集] -> [ESET Remote Administrator] -> [ERAサーバ] -> [設定] -> [通知] -> [通知処理の間隔(分)] の順にクリックして、サーバーがアクティブなルールを確認して実行する間隔を指定できます。

既定値は10分です。この既定値を短くしないことをお勧めします。サーバーの性能が大きく低下する可能性があるためです。

5.4.3 タスクの完了イベント

選択したタスクの完了後にルールがトリガされます。[既定] 設定では、タスクの種類がすべて選択されています。

ルールに指定されているパラメータが満たされると、管理者によって定義されているアクションが自動的に実行されます。アクションを設定するには、[アクション] セクションの [編集...] をクリックします。

ルールの有効化は、1時間から3カ月までの期間、遅延できます。すぐにルールを有効化する場合は、[有効化までの時間] ドロップダウンメニューで [ASAP] を選択します。既定では、[通知マネージャ] は10分ごとに有効化されるため、[ASAP] を選択した場合、タスクは10分以内に実行されます。このメニューから特定の時間を選択した場合は、その時間が経過したときにアクションが自動的に実行されます (ルールの条件が満たされた場合)。

5.4.4 新しいクライアントイベント

[クライアントフィルタ] ウィンドウで、新規にクライアントフィルタのパラメータを定義します。ルールの適用時には、クライアントフィルタ条件を満たすクライアントのみが考慮されます。フィルタ基準は次のとおりです。

FROMプライマリサーバ	プライマリサーバーのクライアントのみ (否定の NOT FROM も適用できます)。
プライマリサーバIN	出力にプライマリサーバーを含めます。
ドメイン/ワークグループIN	指定されたドメインに属するクライアント。
コンピュータ名マスクIN	指定されたコンピュータ名を持つクライアント。
HAS IPv4マスク	指定された IPv4 マスクに該当するクライアント。
HAS IPv4範囲	指定された IPv4 アドレス範囲内のクライアント。
HAS IPv6ネットワーク識別	指定された IPv6 アドレス範囲のクライアント。
HAS IPv6範囲	指定された IPv6 アドレス範囲内のクライアント。
HAS定義済みポリシー	指定されたポリシーが割り当てられているクライアント (否定の HAS NOT も適用できます)。

ルールに指定されているパラメータが満たされると、管理者によって定義されているアクションが自動的に実行されます。アクションを設定するには、[アクション] セクションの [編集...] をクリックします。

ルールの有効化は、1時間から3カ月までの期間、遅延できます。すぐにルールを有効化する場合は、[有効化までの時間] ドロップダウンメニューで [ASAP] を選択します。既定では、[通知マネージャ] は10分ごとに有効化されるため、[ASAP] を選択した場合、タスクは10分以内に実行されます。このメニューから特定の時間を選択した場合は、その時間が経過したときにアクションが自動的に実行されます (ルールの条件が満たされた場合)。

5.4.5 大規模感染イベント

この通知は、大規模感染事件の定義された基準が満たされると直ちにトリガーされますが、1つ1つの事件や定義された基準を超える事件をレポートするわけではありません。

[クライアントフィルタ] ウィンドウで、大規模感染イベントのフィルタリングパラメータを定義します。ルールの適用時には、クライアントフィルタ条件を満たすクライアントのみが考慮されます。フィルタ基準は次のとおりです。

FROMプライマリサーバ	プライマリサーバーのクライアントのみ (否定の NOT FROM も適用できます)。
プライマリサーバIN	出力にプライマリサーバーを含めます。
HAS新規フラグ	[新規] フラグが付いているクライアント (否定の HAS NOT も適用できます)。
対象のERAグループ	指定されたグループに属するクライアント。
ドメイン/ワークグループIN	指定されたドメインに属するクライアント。
コンピュータ名マスクIN	指定されたコンピュータ名を持つクライアント。
HAS IPv4マスク	指定された IPv4 マスクに該当するクライアント。
HAS IPv4範囲	指定された IPv4 アドレス範囲内のクライアント。
HAS IRv6ネットワーク識別	指定された IPv6 アドレス範囲のクライアント。
HAS IPv6範囲	指定された IPv6 アドレス範囲内のクライアント。
HAS定義済みポリシー	指定されたポリシーが割り当てられているクライアント (否定の HAS NOT も適用できます)。

通知ルールにクライアントフィルタを指定したら、[OK] をクリックしてルールパラメータに進みます。クライアントパラメータによって、通知アクションを実行するためにクライアントまたはクライアントグループが満たす必要のある条件が定義されます。指定可能なパラメータを表示するには、[パラメータ] セクションの [編集...] ボタンをクリックします。

ログタイプ	監視するログの種類を選択します。	
ログレベル	指定されたログのログエントリレベル。	
	レベル 1- 重大な警告	致命的なエラーのみ。
	レベル 2- レベル 1 +警告	レベル 1 と同じで、警告通知も発行されます。
	レベル 3- レベル 2 +通常	レベル 2 と同じで、情報を提供する通知も発行されます。
	レベル 4- レベル 3 +診断	レベル 3 と同じで、診断を提供する通知も発行されます。
60分に1,000件	発生件数の入力と期間の選択をして、通知が送信される場合に達する必要のあるイベント頻度を指定します。既定の頻度は、1 時間に 1,000 件です。	
数量	クライアント数 (絶対値またはパーセント値)。	

[スロットルの間隔] は、通知を送信する時間間隔です。たとえば、スロットルの間隔が1時間に設定された場合、データはバックグランドで収集され、1時間ごとに通知を受け取ります (大規模感染が存在し続け、トリガーがアクティブな場合)。

5.4.6 受信ログイベント

このオプションは、一定の時間内のすべてのログについて通知を受けるようにする場合に使用します。

[クライアントフィルタ] ウィンドウで、クライアントフィルタのパラメータを定義します。ルールの適用時には、クライアントフィルタ条件を満たすクライアントのみが考慮されます。フィルタ基準は次のとおりです。

FROMプライマリサーバ	プライマリサーバーのクライアントのみ（否定の NOT FROM も適用できます）。
プライマリサーバIN	出力にプライマリサーバーを含めます。
HAS新規フラグ	[新規] フラグが付いているクライアント（否定の HAS NOT も適用できます）。
対象のERAグループ	指定されたグループに属するクライアント。
ドメイン/ワークグループIN	指定されたドメインに属するクライアント。
コンピュータ名マスクIN	指定されたコンピュータ名を持つクライアント。
HAS IPv4マスク	指定された IPv4 マスクに該当するクライアント。
HAS IPv4範囲	指定された IPv4 アドレス範囲内のクライアント。
HAS IR6ネットワーク識別	指定された IPv6 アドレス範囲のクライアント。
HAS IPv6範囲	指定された IPv6 アドレス範囲内のクライアント。
HAS定義済みポリシー	指定されたポリシーが割り当てられているクライアント（否定の HAS NOT も適用できます）。

通知ルールにクライアントフィルタを指定したら、[OK] をクリックしてルールパラメータに進みます。クライアントパラメータによって、通知アクションを実行するためにクライアントまたはクライアントグループが満たす必要のある条件が定義されます。指定可能なパラメータを表示するには、[パラメータ] セクションの [編集...] ボタンをクリックします。

ログタイプ	監視するログの種類を選択します。	
ログレベル	指定されたログのログエントリレベル。	
	レベル 1- 重大な警告	致命的なエラーのみ。
	レベル 2- レベル 1 +警告	レベル 1 と同じで、警告通知も発行されます。
	レベル 3- レベル 2 +通常	レベル 2 と同じで、情報を提供する通知も発行されます。
	レベル 4- レベル 3 +診断	レベル 3 と同じで、診断を提供する通知も発行されます。

ルールに指定されているパラメータが満たされると、管理者によって定義されているアクションが自動的に実行されます。アクションを設定するには、[アクション] セクションの [編集...] をクリックします。

[スロットルの間隔] は、通知を送信する時間間隔です。たとえば、スロットルの間隔が1時間に設定された場合、データはバックグランドで収集され、1時間ごとに通知を受け取ります（トリガーがアクティブな場合）。

5.4.7 アクション

ルールに指定されているパラメータが満たされると、管理者によって定義されているアクションが自動的に実行されます。アクションを設定するには、[アクション] セクションの [編集...] をクリックします。アクションエディタには、次のオプションが用意されています。

電子メール	ルールの通知テキストが、指定されている電子メールアドレスに送信されます。[件名] で、件名を指定できます。アドレスブックを開くには、[宛先] をクリックします。
SNMPトラップ	SNMP 通知が生成されて送信されます。
実行(サーバ上)	このオプションを有効にして、サーバーで実行するアプリケーションを指定します。アプリケーションへのフルパスを入力します。
ファイルにログを保存する	指定されたログファイルにログエントリが生成されます。フォルダへのフルパスを入力します。通知の [レベル] は設定可能です。
Syslogにログを保存する	システムログに通知が記録されます。通知の [レベル] は設定可能です。
ログ	サーバログに通知が記録されます。通知のレベルは設定可能です。
レポートを実行	このオプションを選択すると、[テンプレート名] ドロップダウンメニューをクリックすることができます。レポートに使用するテンプレートを選択します。テンプレートの詳細については、「レポート」を参照してください。

この機能が正常に動作するように、ERA Serverでログを有効にする必要があります ([ツール] -> [サーバオプション] -> [ログ])。

5.4.8 SNMPトラップを使用した通知

SNMP (簡易ネットワーク管理プロトコル) は、ネットワークに関する問題の監視と特定に適した簡単な管理プロトコルとして広く普及しています。このプロトコルの機能の1つとして、特定のデータを送信するトラップがあります。ERAでは、トラップを使用して通知メッセージを送信します。

トラップツールを効果的に実行するには、ERASをインストールしたコンピュータにSNMPプロトコルを正しくインストールし、設定する必要があります ([スタート] -> [コントロールパネル] -> [プログラムの追加と削除] -> [Windowsコンポーネントの追加と削除])。SNMPサービスの設定については、以下の記事を参照してください。
http://support.microsoft.com/ kb/315154
ERASでは、SNMP通知ルールを有効にする必要があります。

通知は、SNMPマネージャに表示されます。SNMPマネージャは、コンフィグレーションファイルeset_ras.mibのインポート先であるSNMPサーバーに接続している必要があります。このコンフィグレーションファイルはERAインストールの標準コンポーネントで、通常はC:¥Program Files¥ESET¥ESET Remote Administrator¥Server¥フォルダにあります。

5.4.9 ルール作成例

作成済みのERAグループのいずれかのクライアントワークステーションの保護状態に問題が発生したときに管理者に電子メール通知を送信するルールを作成する方法を以下に説明します。また、この通知はlog.txtという名前のファイルに保存されます。

1 [トリガの種類] ドロップダウンメニューで [クライアント状態] を選択します。

2 [優先順位]、[有効化までの時間] および [繰り返す間隔] の各オプションを事前定義された値のままにします。このルールには優先順位3が自動的に割り当てられ、24時間後に有効になります。

3 [説明] フィールドで、[クライアントの保護状態の異常を通知] と入力します。

4 [クライアントフィルタ] セクションで [編集...] をクリックし、[対象のERAグループ] のみを有効にします。ウィンドウの下部にある [指定] リンクをクリックし、対象のグループにチェックを入れます。

5 [パラメータ] -> [編集...] でルールのパラメータを指定します。ここでは、[HAS 保護状態に警告がある] と [HAS 保護状態に重大な警告がある] の2つのみチェックします。パラメータ部分では"すべての条件が一致"を"いずれかの条件が一致"に変更します。

6 [アクション] セクションに進み、[編集...] ボタンをクリックします。[アクション] ウィンドウで、[電子メール] を有効にし、電子メールの受信者 ([宛先...]) と件名 ([表題]) を指定します。[ファイルにログを保存する] チェックボックスをオンにし、作成するログファイルの名前とパスを入力します。必要に応じて、ログファイルの [レベル] を選択することもできます。[OK] をクリックしてアクションを保存します。

7 最後に、[メッセージ] テキスト領域で、ルールが有効になったときに電子メールの本文で送信する内容を指定します例:"クライアント%CLIENT_LIST%から保護状態の問題が報告されています"。

8 [名前を付けて保存...] をクリックしてルールの名前 ("保護状態の問題"など) を指定し、通知ルールの一覧でルールを選択します。

これでルールは有効になります。対象のグループに所属するクライアントで保護状態の問題が発生すると、このルールが実行されます。[閉じる] をクリックして、通知マネージャを終了します。

5.5 クライアントの詳細情報

ERAでは、実行中のプロセスやスタートアッププログラムなどに関する情報をクライアントワークステーションから取得できます。この情報を取得するには、ERASと直接統合されているESET SysInspectorツールを使用します。ESET SysInspectorは、さまざまな便利な機能を提供するほか、オペレーティングシステムを詳しく検査してシステムログを生成します。このツールを開くには、ERACのメインメニューから [ツール] -> [ESET SysInspector] をクリックします。
特定のクライアントで問題が発生した場合、そのクライアントにESET SysInspectorログを要求できます。そのためには、[クライアント] ペインでクライアントを右クリックし、[データのリクエスト] - [SysInspector情報をリクエスト] を選択します。ログを取得できるのは5.x以降の製品のみです。それより前のバージョンでは、この機能はサポートされていません。
次のオプションを備えたウィンドウが表示されます。

スナップショットを作成する(結果のログをクライアントでも保持する)	クライアントコンピュータにログのコピーを保存します。
指定した時刻より前の最新のスナップショットとの比較を含める	比較ログが表示されます。比較ログは、以前のログが存在する場合に、そのログと現在のログをマージすることによって生成されます。以前のログとして、指定した日時より前の最新のログが選択されます。

[OK] をクリックして、選択したログを取得し、サーバーに保存します。ログを開いて表示する手順は次のとおりです。

個々のクライアントワークステーションのESET SysInspectorオプションは、クライアントの [プロパティ] - [SysInspector] タブにあります。このウィンドウは3つのセクションに分かれており、一番上のセクションには、特定のクライアントから取得した最新のログに関するテキスト情報が表示されます。[更新] をクリックすると、最新情報を読み込むことができます。

[リクエストオプション] ウィンドウの中央のセクションは、クライアントワークステーションにログを要求する前述のプロセスで表示されるウィンドウとほぼ同じです。[リクエスト] ボタンを使用して、クライアントからESET SysInspectorログを取得します。

一番下のセクションには次のボタンがあります。

表示	先頭のセクションに表示されているログを ESET SysInspector で直接開きます。
名前を付けて保存...	現在のログをファイルに保存します。[次に ESET SysInspector ビューアを起動し、ファイルを表示する] オプションを選択しておくと、保存後にログが自動的に開きます([View] をクリックした場合と同様です)。

ログのサイズとデータ転送速度が原因となって、ローカルクライアントによっては新しいログファイルを生成して表示するまでに時間がかかることがあります。クライアントの [プロパティ] -> [SysInspector] でログに割り当てた日時は、サーバーへの配信日時を表します。

5.6 ファイアウォール ルール マージウィザード

ファイアウォール ルールマージウィザードにより、選択したクライアントのファイアウォール ルールをマージできます。これは特に、学習モードのクライアントで収集されたすべてのファイアウォール ルールを含む単一のコンフィグレーションを作成する必要がある場合に役立ちます。その方法で作成したコンフィグレーションは、コンフィグレーションタスクを介してクライアントに送信できます。また、ポリシーとして適用することもできます。

ウィザードは、[ツール] -> [ファイアウォールルールマージウィザード] から実行します。

[Chapter 6]
ERA サーバオプション

6.1 一般

ERA Serverの設定は、ERA Serverに接続しているERA Consoleから、［ツール］->［サーバオプション］にあります。

［一般］タブには、基本的なERA Server情報が表示されます。

サーバ情報	ここには、基本的な ERA Server の情報が表示されます。［パスワード変更］ボタンをクリックして、ERA サーバオプションの［セキュリティ］タブを開きます。
ライセンス情報	購入した ESET セキュリティ製品のクライアントライセンス数、およびサーバーコンピュータにインストールされている Endpoint アンチウイルスまたは ESET Endpoint Security の現在のバージョンが表示されます。ライセンスが切れていても、新しいライセンスを既に購入している場合には、［ライセンスマネージャ］ボタンをクリックしてダイアログを開き、新しいライセンスを参照できます。
定義データベースのバージョン	提供されたアップデート情報および使用されているセキュリティ製品に基づいて、定義データベースの現在のバージョンが表示されます。
パフォーマンス	サーバー、クライアント間の接続および一般的なパフォーマンス情報が表示されます。

6.1.1 ライセンス管理

ERAが正常に機能するように、ライセンスキーを設定する必要があります。ライセンスマネージャーによって、ライセンスキーを設定することができます。

ERA 5.x以降では、複数のライセンスキーのサポートが追加されています。この機能によって、ライセンスキーの管理がより簡単になります。

ライセンスマネージャにはサーバオプションの [一般] タブにある [ライセンスマネージャ] ボタンをクリックするか、メニューの [ツール] -> [ライセンスマネージャ] からアクセスできます。

新しいライセンスキーを追加するには:

1. [ライセンスマネージャ] を開きます。
2. [参照] をクリックして、目的のライセンスキーファイルを選択します (ライセンスキーのファイル拡張子は.licです)。
3. [開く] をクリックして、確定します。
4. ライセンスキーの情報が正しいことを確認して、[サーバにアップロード] を選択します。
5. [OK] をクリックして、確定します。

[サーバにアップロード] ボタンは、[参照] ボタンを使用してライセンスキーを選択した場合にのみアクティブになります。現在表示されているライセンスキーに関する情報は、ウィンドウのこの部分に表示されます。これによって、キーをサーバーにコピーする前に最終確認を行えます。

ウィンドウの中央部分には、サーバーによって現在使用されているライセンスキーに関する情報が表示されます。サーバーに存在するすべてのライセンスキーの詳細を表示するには、[詳細...] ボタンをクリックします。

ライセンスマネージャのウィンドウの下部は、ライセンスで問題が発生したときの通知に使用されます。使用可能なオプションは次のとおりです。

ライセンス期限警告	ライセンスの期限が切れる X 日前に警告が表示されます。
ライセンスのクライアント数がサーバデータベースの実際のクライアント数を下回る場合にのみ警告する	ライセンスキーまたはライセンスの一部の期限切れによって、現在接続されているクライアントまたは ERAS のデータベース内のクライアントの数を許容クライアント数が下回る場合にのみ警告が表示されます。
警告するタイミングを限定する	空きクライアントスロットの数が指定した値(%単位)を下回る場合に警告が表示されます。

6.2 セキュリティ

バージョン5.x以降のESETセキュリティソリューション（ESET Endpoint Securityなど）では、クライアントとERASとの間の暗号化されていない通信（ポート2222でのTCPプロトコルによる通信）をパスワードで保護できます。以前のバージョンとの互換性を保持するには、[クライアント（ESETセキュリティ製品）の非認証アクセスを有効にする]チェックボックスをオンにする必要があります。

NOTE

ERASと（3.x以降の）すべてのクライアントで認証が有効になっている場合には、[クライアント（ESETセキュリティ製品）の非認証アクセスを有効にする]をオフにすることができます。

コンソールセキュリティ設定

● [Windows/ドメイン認証を使用する]
Windows/ドメイン認証が有効になり、ERA Serverへのフルアクセス権を持つ管理者グループの定義や、[その他のすべてのユーザーを読み取り専用アクセスユーザーとして処理する]チェックボックスをオンにして、読み取り専用アクセス権を付与したグループの定義ができます。このチェックボックスを選択すると、[他のドメインに所属しないWindows/ドメインユーザーに読み取りロールを使用する]オプションがアクティブになります。このオプションにより、これらのユーザーはERACの設定変更ができなくなります。

●ユーザーのコンソールへのアクセスは、[ユーザマネージャ]ツールによって管理されます。

サーバーのセキュリティ設定

クライアントのパスワード	ERAS にアクセスするクライアントのパスワードを設定します。
複製のパスワード	下位 ERA Server を指定の ERAS に複製する場合のパスワードを設定します。
ESETリモートインストーラ(エージェント)のパスワード	ERAS（リモートインストールに関係）にアクセスするインストーラエージェントのパスワードを設定します。
クライアントの非認証アクセスを有効にする(ESETセキュリティ製品)	有効なパスワードが指定されていないクライアントが ERAS にアクセスできるようにします（現在のパスワードが［クライアントのパスワード］と異なる場合）。
複製の非認証アクセスを有効にする	複製で使用する有効なパスワードが指定されていない下位 ERA Server のクライアントが ERAS にアクセスできるようにします。
ESETリモートインストーラの非認証アクセスを有効にする(エージェント)	有効なパスワードが指定されていない ESET リモートインストーラが ERAS にアクセスできるようにします。

NOTE

［既定］は事前定義された設定を適用するだけで、パスワードをリセットすることはありません。

NOTE

安全性を高める場合は、複雑なパスワードを要求できます。[ツール]->[ESETコンフィグレーションエディタ]->[リモート管理]->[ERAサーバ]->[設定]->[保護]->[複雑なパスワードを要求する]の順にクリックし、このオプションを[はい]に設定します。これを有効にした場合、新規のパスワードはいずれも、8文字以上の長さでなければならず、アルファベットの小文字、大文字、及び数字または記号を含む必要があります。

6.2.1 ユーザマネージャ

ユーザマネージャツールはコンソールサーバー認証のユーザーアカウントの管理を容認します。Administrator（フルアクセス）及びRead-Only（読み取り専用）アカウントが事前定義されています。

新規をクリックし、コンソールサーバー認証のユーザーアカウントを追加します。ユーザー名、パスワード及び特定の許可を定義します。

説明フィールドはユーザーのカスタム説明のためのもので、必須ではありません。

許可はユーザーの接続レベルと実行出来る特定作業を定義します。それぞれのユーザーのコンソールへの接続ために、特定のユーザーを選択して、コンソール認証のためのパスワードの隣の変更...をクリックし、コンソールアクセスパスワードを変更できます。

NOTE

事前定義されたアカウント（Administrator及びRead-Only）では設定の変更はできません。

選択されたERA Serverユーザーに複数のWindows/ドメイン認証グループを追加出来ます。もしWindows/ドメインユーザーが複数のユーザーに割り当てられたら、ユーザーリストにいるユーザーが役目を働くことになります。ユーザリストの横にある上向きおよび下向きの矢印はユーザーの順を定義します。

6.2.2 コンソールアクセスパスワード

コンソールアクセスパスワードを変更するには、ユーザマネージャでパスワードを変更します。現在のパスワードを入力してから、新しいパスワードを二回入力します（確認用）。キャッシュに保管されているパスワードも変更するの横にあるチェックボックスをクリックすると、アプリケーション起動時に使われたキャッシュされたパスワード（ユーザーはERACアクセスする度にその入力が不要になります）が変更されるようになります。

NOTE

このダイアログで設定したパスワードはサーバーに直接送信されます。これはOKをクリックした直後に変更が実行され、元に戻すことはできません。

6.3 サーバの保守

[サーバの保守] タブで正しく設定されている場合、ERA Serverのデータベースは、自動的に保守され最適化されるため、さらに設定を行う必要はありません。クリーンアップの設定は以下のとおりです。

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します。
クリーンアップの設定	時間パラメータによるログの削除。
クリーンアップの詳細設定	ログ記録の数によるログの削除。

クリーンアップ後に保つ必要のあるログエントリ数とサーバーが受信するログのレベルを指定します。たとえば、[ログ記録の数による高度な駆除設定] で、[最後の600000件を除くすべてのウイルスログを削除] を選択し、[レベル3-レベル2+通常] と定義した [ウイルス] に対する [ログ収集パラメータ] のレベルを選択すると、重大なエラーに関する情報、警告通知および情報を提供する通知を含む最後の600000件の記録はデータベースに保たれます。[時間パラメータによる駆除] を使用してログエントリを制限することもできます。

クリーンアップスケジューラ	上記の選択したオプションを指定された間隔で実行します。このオプションの横の [変更] をクリックして時間パラメータを設定します。[今すぐクリーンアップ] をクリックして直ちにクリーンアップを開始します。
圧縮と修復のスケジューラ	指定した時間間隔で、指定した時間にデータベースを圧縮します。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。このオプションの横の [変更] をクリックして時間パラメータを設定します。[今すぐ圧縮] をクリックして直ちに圧縮と修復を開始します。

NOTE

[クリーンアップ] と [圧縮と修復] の両方のツールによって時間とリソースを有効活用できます。スケジューリングしてサーバーの負荷が最小のときに実行することをお勧めします(たとえば、夜、[クリーンアップ] を実行し、週末に [圧縮と修復] を実行するなど)。

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 [圧縮と修復] タスクが実行されます。

6.3.1 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します。ログの種類の横にあるドロップダウンメニューで、オプションごとにログのレベルを選択します。

なし	どのログも受信しません。
レベル1-重大な警告	致命的なエラーのみ受信します。
レベル2-レベル1+警告	レベル 1 および、警告通知を受信します。
レベル3-レベル2+通常	レベル 2 および、情報を提供する通知を受信します。
レベル4-レベル3+診断	レベル 3 および、診断を提供する通知を受信します。
すべて	すべてのログを受信します。

6.3.2 時間パラメータによるクリーンアップ

時間間隔による駆除の主なクリーンアップ設定は以下のとおりです。

この期間接続されていないクライアントを削除(クライアントを完全に削除します。)	指定月数（日数）を超える期間 ERAS に接続していないすべてのクライアントを削除します。
これより古いウイルスログを削除	指定月数（日数）以上経過したすべてのウイルス事件（検出されたウイルス）を削除します。
これより古いファイアウォールログを削除	指定月数（日数）以上経過したすべてのファイアウォールログを削除します。
これより古いイベントログを削除	指定月数（日数）以上経過したすべてのシステムイベントを削除します。
これより古いHIPSログを削除	指定月数（日数）以上経過したすべての HIPS（Host-based Intrusion Prevention System）ログを削除します。
これより古いデバイスコントロールログを削除	指定月数（日数）以上経過したすべてのデバイスコントロールログを削除します。
これより古いWebコントロールログを削除	指定月数（日数）以上経過したすべての Web コントロールログを削除します。
これより古い迷惑メール対策ログを削除	指定月数（日数）以上経過したすべての迷惑メール対策ログを削除します。
これより古いグレーリストログを削除	指定月数（日数）以上経過したすべてのグレーリストログを削除します。
これより古い検査ログを削除	指定月数（日数）以上経過したすべてのスキャンログを削除します。
これより古いモバイルログを削除	指定月数（日数）以上経過したすべてのモバイルログを削除します。
これより古くクライアントのない隔離エントリーを削除	割り当て先のクライアントがなく、生成から指定月数（日数）以上経過したすべての隔離エントリを削除します。
これより古い未登録のコンピュータエントリーを削除	生成から指定月数（日数）以上経過したすべての未登録コンピュータ（ERA の管理下にないコンピュータ）のエントリを削除します。
これよりも古く終了状態のタスクエントリのみを削除	終了状態で、生成から指定月数（日数）以上経過したすべてのタスクエントリを削除します。
これより古いタスクエントリをすべて削除	生成から指定月数（日数）以上経過したすべてのタスクエントリ（状態にかかわらず）を削除します。

6.3.3 ログ記録の数による高度なクリーンアップ設定

ログ記録の数による高度な駆除設定

最新の600000件を除いて全てのウイルスログを削除	指定した数の記録を除くすべてのウイルス事件（検出されたウイルス）を削除します。
最新の600000件を除いて全てのファイアウォールログを削除	指定した数の記録を除くすべてのファイアウォールログを削除します。
最新の600000件を除いて全てのイベントログを削除	指定した数の記録を除くすべてのシステムイベントを削除します。
最新の300000件を除いて全てのHIPSログを削除	指定した数の記録を除くすべての HIPS（Host-based Intrusion Prevention System）ログを削除します。
最新の300000件を除いて全てのデバイスコントロールログを削除	指定した数の記録を除くすべてのデバイスコントロールログを削除します。
最新の300000件を除いて全てのWebコントロールログを削除	指定した数の記録を除くすべての Web コントロールログを削除します。
最新の300000件を除いて全ての迷惑メール対策ログを削除	指定した数の記録を除くすべての迷惑メール対策ログを削除します。
最新の300000件を除いて全てのグレーリストログを削除	指定した数の記録を除くすべてのグレーリストログを削除します。
最新の300000件を除いて全ての検査ログを削除	指定した数の記録を除くすべてのスキャンログを削除します。
最新の300000件を除いて全てのモバイルログを削除	指定した数の記録を除くすべてのモバイルログを削除します。

6.4 ログ

ログのパラメータを設定するには、ERA Consoleのメインメニューの [ツール] -> [サーバオプション] を選択し [ログ] タブを開きます。
[ログ] タブでは、ログの透過性を維持するための各種オプションが用意されており、また領域を節約するために、定期的にERAのメインデータベースを圧縮することができます。

1.監査ログ
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と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] が選択されている場合、新しいログファイルが作成され ([ローテーション実行サイズ (MB)])、日毎に削除されます ([ローテーションログの削除期限 (日)])。左側のドロップダウンメニューでログレベルを変更することができます。

[ログの表示] をクリックして、現在の監査ログを表示します。

● [OSのアプリケーションログに記録する] を使用すると、情報をシステムイベントビューアログ ([Windowsコントロールパネル] -> [管理ツール] -> [イベントビューア] の順にクリック) にコピーできます。左側のドロップダウンメニューでログレベルを変更することができます。

● [Syslogにログを保存する] オプションは、指定したSyslogサーバー (既定では、サーバーはlocalhost、ポートは514) にログメッセージを送信します。Syslogの詳細設定をするには、[ツール] -> [サーバオプション] -> [詳細] -> [詳細設定を編集] -> [設定] -> [ログ] の順にクリックします。ここでSyslogオプション (Syslogサーバ名、Syslogサーバポート、Syslogファシリティおよびログレベル) を編集できます。

▸▸▸ NOTE

Syslog重大度はログタイプごとに設定する必要があります。サーバログの場合、[サーバログのSyslogファシリティ] の設定になり、デバッグログの場合、[デバッグログのSyslogファシリティ] の設定になります。

ログの [レベル] は、ログや含まれる情報の詳細さの度合いを示します。

レベル1-ユーザおよびグループ	ユーザーおよびグループ関連アクティビティ（静的グループ、パラメータグループ、グループ内クライアントの追加 / 削除など）を記録します。
レベル2-レベル1＋クライアントアクション	上記およびすべての ERA クライアント関連アクティビティ（新規フラグの設定 / クリア、クライアントポリシーの設定、データのリクエストなど）
レベル3-レベル2＋タスクおよび通知	上記およびすべてのタスク関連アクティビティ（タスクの作成 / 削除、通知の作成 / 削除など）。
レベル4-レベル3＋レポート	上記およびすべてのレポート関連アクティビティ（レポートの作成 / 削除、レポートテンプレートの選択 / 削除）。
レベル5-全てのイベント	すべてのログ関連アクティビティ（HIPS ログのクリア、ウイルスログのクリアなど）。

2.サーバログ

実行中、ERA Serverでは、そのアクティビティに関するログ（[ログファイル名]）が作成されます。このログは、[ログレベル] を設定できます。

NOTE

テキストファイルの出力は、既定で%ALLUSERSPROFILE%¥Application Data¥Eset¥ESET Remote Administrator¥Server¥logs¥era.logに保存されます。

● [テキストファイルにログを保存する] が選択されている場合、新しいログファイルが作成され（[ローテーション実行サイズ（MB）]）、日毎に削除されます（[ローテーションログの削除期限（日）]）。

NOTE

[テキストファイルにログを保存する] では、[ログレベル] を [レベル2-レベル1＋セッションエラー] にしておき、ログレベルを上げるのは、問題が発生した場合や、ESETカスタマサポートの指示があった場合のみにすることをお勧めします。

● [OSのアプリケーションログに記録する] を使用すると、情報をシステムイベントビューアログ（[Windowsコントロールパネル] -> [管理ツール] -> [イベントビューア] の順にクリック）にコピーできます。

● [Syslogにログを保存する] オプションは、指定したSyslogサーバー（既定では、サーバーはlocalhost、ポートは514）にログメッセージを送信します。Syslogの詳細設定をするには、[ツール] -> [サーバオプション] -> [詳細] -> [詳細設定を編集] -> [設定] -> [ログ] の順にクリックします。ここでSyslogオプション（Syslogサーバ名、Syslogサーバポート、Syslogファシリティおよびsyslogレベル）を編集できます。

ログの [レベル] は、ログや含まれる情報の詳細さの度合いを示します。

レベル1-重要な情報	誤作動（この場合は ESET カスタマサポートにお問い合わせください）。
レベル2-レベル1＋重要なセッション情報	サーバー通信に関する情報（ERA Server に誰がログインしたか、日時と理由）。
レベル3-レベル2＋各種の情報	ERA Server の内部処理に関する情報。
レベル4-レベル3＋インストーラ	エージェント（einstaller.exe）に関する情報（ERA Server に関する情報 - エージェントの接続 / 切断およびその結果）。
レベル5-レベル4＋クライアント	クライアント情報（ERA Server に関する情報 - クライアントの接続 / 切断およびその結果）。

NOTE

[ログレベル] は[レベル2-レベル1＋セッションエラー] に設定したままにすることをお勧めします。

3. [デバッグログ] オプションは、通常は無効にしておくことをお勧めします。この設定はトラブルシューティングを行う場合に使用します。

6.4.1 監査ログビュアー

監査ログはERACユーザーが行う全ての変更と実行するアクションを記録します。これは、潜在的な不正アクセスを含み管理者がERAC関連活動を追跡するのを助けます。

NOTE

監査ログビューアはデータベースに記録された変更を表示します。監査ログは他のログ（例えば、ファイルログとその他）を含んでいません。

監査ログビューアーは、[ログ] タブの [監査ログ] セクションにある [ログの表示] ボタンをクリックして起動します。

監査ログビューアーは、画面左側で表示するログのフィルタリングを行い、画面右側上部で表示するログの件数を指定できます。

ユーザ	指定のユーザーの記録のみ表示します。
ドメインログイン名	指定のドメインの記録のみ表示します。
IPアドレス	オプション（アドレス、範囲またはマスク）を選び、適切なフィールドにアドレスを入力します。これらのオプションは IPv4 アドレスと IPv6 アドレスの両方に共通です。
アクションタイプ	指定のアクションの記録のみ表示します。
フィルター適用	フィルターパラメータを適用します。
デフォルト	フィルターパラメータをリセットします。

監査ログエントリのリスト

日付	アクションが実行された日付。この日付と時刻はサーバーマシンの時間設定に基づいています。
ユーザ	アクションを行ったユーザーのユーザー名。
ドメインのログイン名	このアクションを実行するユーザーのウインドウズドメインログインネーム Windows/Domain ログインタイプが使われた時のみに表示されます。アクションを行ったユーザーが Windows / ドメイン認証をしている場合に、利用したユーザー名を表示します。
コンソールIPアドレス	ERAC ユーザーがアクションを実行した起点となるコンソールの IP アドレス。
アクション	ユーザーによって実行されたアクション。
オブジェクト	このアクションによって影響を受けるオブジェクト

NOTE

情報追加（利用できる場合）はログ内の特定の行をダブルクリックした後に表示されます。

6.5 複製設定

ERA Serverの各種設定を設定するには、ERA Consoleのメインプログラムウィンドウで [ツール] -> [サーバオプション] をクリックし [複製] タブを開きます。

複製は、複数のERA Serverがインストールされている大規模ネットワーク（複数の支社がある企業のネットワークなど）で使用されます。[複製設定] タブでは、ネットワークで稼働している複数のERA Server間でのデータの複製を設定できます。組織内で複数のERA Serverを設定する方法については、「大規模ネットワークでのRAサーバの設定」を参照してください。

複製を設定するには、下記の複製オプションを使用します。

[複製先の設定]

複製先を有効にする	大規模ネットワークでの複製を有効にします（「複製設定」を参照）。
上位サーバ	上位 ERA Server の IP アドレスまたは名前。このサーバーがローカル ERA Server からデータを収集します。
ポート	複製に使用するポートを指定します。
次の分数ごとに複製(分)	複製の間隔を設定します。
複製	各種ログに対応したチェックボックスで、チェックされたログが複製の対象になります。

[複製先の状態]

今すぐ複製	複製プロセスを開始します。
すべてのクライアントを複製の対象にする	有効にすると、変更のないクライアントも含めてすべてのクライアントが複製されます。

[複製元の設定]

複製元を有効にする	ローカル ERA Server が、[許可されているサーバ] フィールドにリストアップされた他のサーバーからデータを収集できるようにします。ERA Server が複数ある場合には、カンマで区切ります。

6.5.1 大規模ネットワークでの複数設定

複製は、複数のERA Serverがインストールされている大規模ネットワーク（複数の支社がある企業のネットワークなど）で使用されます。詳細については、「インストール」を参照してください。

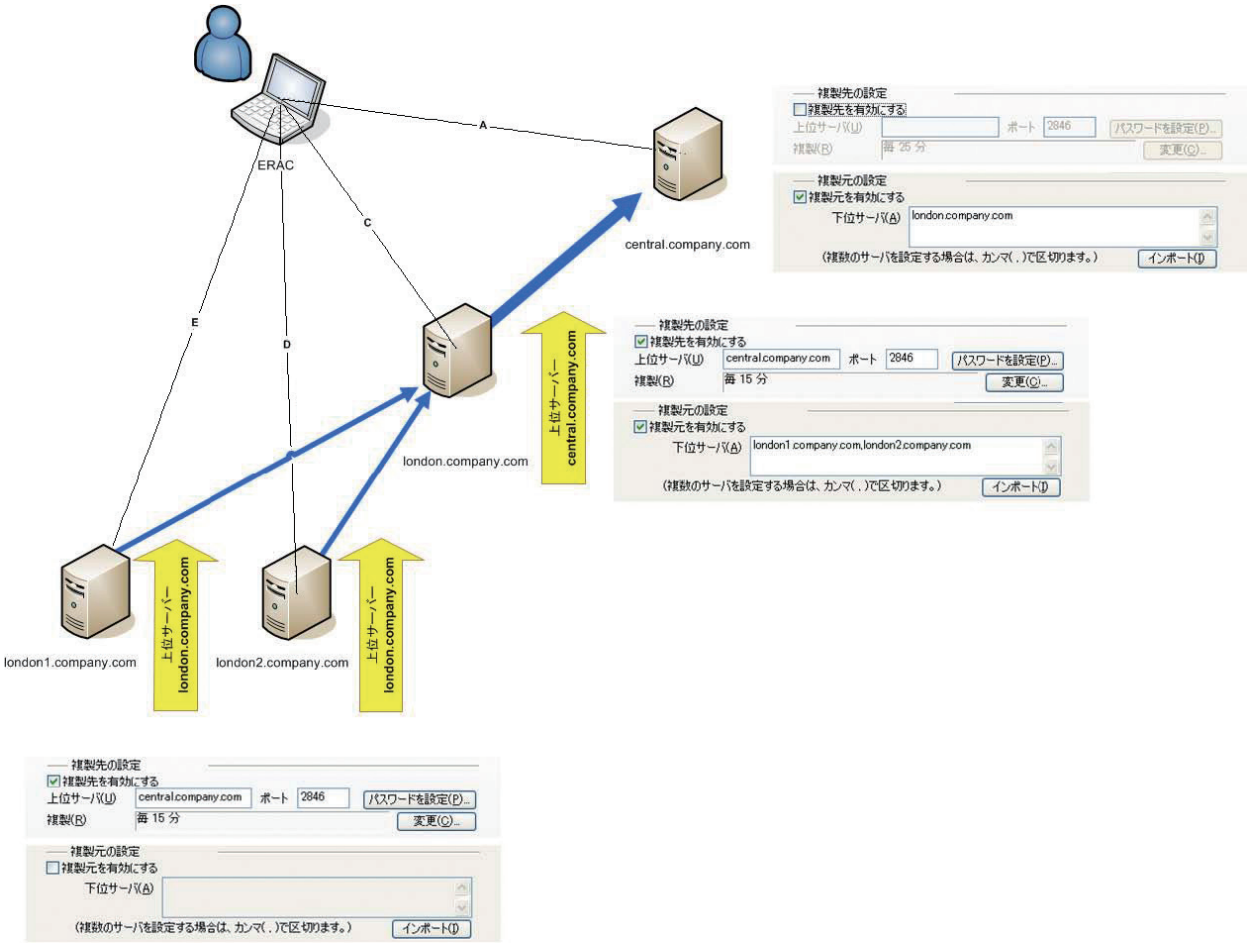
[複製] タブ（[ツール] -> [サーバオプション]）のオプションは、次の2つのセクションに分かれています。

- [複製先の設定]
- [複製元の設定]

[複製先の設定] セクションは、下位ERA Serverの設定に使用します。[複製先を有効にする] オプションを有効にして、マスタERAS（上位サーバー）のIPアドレスまたは名前を入力する必要があります。これによって、下位サーバーからマスタサーバーにデータが複製されます。[複製元の設定] では、マスタ（上位）ERA Serverで下位ERA Serverからのデータを受け取るか、マスタサーバーにデータを転送するように設定できます。[複製元を有効にする] を有効にして、下位サーバーの名前をカンマ区切りで指定する必要があります。

複製階層の中ほどに位置する（つまり、下位サーバーと上位サーバーの両方を持つ）ERA Serverに対して、これら両方のオプションを有効にする必要があります。

前述のシナリオはすべて次の図に示しています。ベージュ色のコンピュータは、個々のERA Serverを表します。各ERASは、[複製] ダイアログウィンドウ内で、それぞれの名前（混乱を避けるために%Computer Name%と同じにします）と対応する設定によって表されます。



NOTE

一部のログは自動的に複製されますが、詳細ログおよびクライアント設定ログはオンデマンドでのみ複製されます。これは、ログによっては関係のない可能性があるデータが大量に含まれている場合があるためです。たとえば、すべてのファイルをログに記録するオプションが有効になっているスキャンログでは、大量のディスク容量が消費されます。このような情報は通常必要なく、手動でリクエストできます。下位サーバーでは、削除されたクライアントに関する情報が自動的に送信されることはありません。このため、下位サーバーから削除されたクライアントに関する情報が上位サーバーで引き続き保存される場合があります。上位サーバーで[クライアント] タブからクライアントが削除されるようにする場合は、[サーバオプション]->[詳細]->[詳細設定を編集]->[設定]->[複製]で、複製されたクライアントを元になるサーバーで削除できるようにするオプションを選択します。

ERASのログ保守レベルを設定するには、[ツール]->[サーバオプション]->[詳細]->[詳細設定を編集]->[設定]->[サーバの保守] の順にクリックします。

状態が変更されたクライアントのみを複製する場合は、[すべてのクライアントを複製の対象にする] のチェックを外します。

6.6 アップデート

[サーバオプション] モジュールの [アップデート] ウィンドウで、ESET Remote Administrator Serverのアップデートパラメータを定義します。このウィンドウは、2つのセクションに分かれています。上のセクションにはサーバーアップデートオプションがリストアップされ、下のセクションでは、ミラーリングのパラメータをアップデートします。ESET Remote Administrator Serverには、クライアントワークステーション用のローカルアップデートサーバーを作成するミラーサーバーの機能があります。

以下に、すべての要素および機能について説明します。

アップデートサーバ	ESET のアップデートサーバー。既定値の［自動選択］のままで使用することをお勧めします。
アップデートインターバル	新しいアップデートファイルを入手できるかどうかチェックする間隔の最大値を指定します。
アップデートユーザー名	ESET Remote Administrator がアップデートサーバーへの認証に使用するユーザー名。
アップデートパスワード	ESET Remote Administrator がアップデートサーバーへの認証に使用するパスワード。

ウイルス定義データベースおよびプログラムコンポーネントの定期的なアップデートは、ウイルスの検出を確実なものとする重要な要素です。ただし、大規模ネットワークの管理者はアップデートに関連した問題（間違った警告、モジュール関連トラブルなど）を経験することがあります。アップデートサーバーに接続するオプションは次の3つです。

定期的なアップデート	ウイルス定義データベースは定期アップデートサーバーによってリリースされるタイミングでアップデートされます。
リリース前のアップデート	このオプションが有効な場合、アップデート時にベータ版がダウンロードされます。このオプションは、実稼働環境では有効にしないことをお勧めします。テスト目的のみに使用してください。
遅延アップデート	このオプションを有効にすると、12 時間遅れでアップデートを取得します。つまり、実稼働環境でテストされ、安定と見なされるアップデートを取得します。

ESET Remote Administratorの最新のコンポーネントをすべてダウンロードするアップデートタスクを開始するには、[今すぐ更新] をクリックします。アップデートには、重要なコンポーネントや機能が含まれていることがあります。したがって、アップデートが適切かつ自動的に機能することを確認することは、非常に重要です。アップデートで問題が発生した場合は、[アップデートキャッシュのクリア] を選択して、一時的にアップデートファイルを保存しているフォルダーをクリアします。

ESET Remote Administrator Serverのミラーリングの設定は、ESET Endpoint アンチウイルスと同じです。ミラーリングの重要な要素についての説明を以下に示します。

アップデートミラーを作成	ミラーリング機能を有効にします。このオプションが無効の場合、アップデートコピーは作成されません。
ミラーを保存するフォルダ	アップデートファイルの保存専用のローカルまたはネットワークのディレクトリー。
アップデートファイルを内部HTTPサーバ経由で配布する	内部 HTTP サーバーを使用してアップデートにアクセスできるようにします。
HTTPサーバポート	ESET Remote Administrator Server が更新サービスを提供するポートを指定します。
認証	アップデートファイルのアクセスに使用される認証方式を指定します。使用可能なオプションは、[なし]、[Basic]、NTLM] です。認証で base64 エンコーディングを使用するには、[Basic] を選択します。[NTLM] オプションを選択すると、安全なエンコーディング方式を使用してエンコーディングできます。認証には、アップデートファイルを共有しているワークステーション上で作成されたユーザーが使用されます。

このウィンドウの全機能を、あらかじめ定義された値に戻すには、下のセクションで [既定] をクリックします。

NOTE

HTTPサーバーの方式を使用する場合は、1つのERAミラーからアップデートするクライアントを400以下にすることをお勧めします。クライアントがそれより多い大規模ネットワークでは、複数のERA (EAV) ミラーサーバー間でミラーアップデートを分散することをお勧めします。ミラーを1つのサーバーで集中管理する必要がある場合は、IISなど、別の種類のHTTPサーバーを使用することをお勧めします。

ERASでミラーリング機能を有効にするには、管理者が、購入した製品のライセンスキーを登録し、ユーザー名とパスワードを入力する必要があります。管理者がESET Endpoint アンチウイルスのライセンスキー、ユーザー名、およびパスワードを使用した後でESET Endpoint Securityにアップグレードした場合には、元のライセンスキー、ユーザー名、およびパスワードも入れ替える必要があります。

NOTE

ESET Endpoint アンチウイルスのクライアントはESET Endpoint Securityのライセンスを使用してアップデートすることもできますが、ESET Endpoint アンチウイルスのライセンスを使用してESET Endpoint Securityのクライアントをアップデートすることはできません。

6.6.1 ミラーサーバー

ミラー作成機能を使用すると、ローカルアップデートサーバーを作成できます。クライアントコンピュータは、インターネット上にあるESETのサーバーからウイルス定義アップデートをダウンロードせずに、ネットワーク上にあるローカルミラーサーバーに接続します。このソリューションの大きな利点は、インターネットの帯域幅消費を削減し、ネットワーク通信を最小化できることです。このコンフィグレーションでは、ミラーサーバーをインターネットに常時接続しておくことが重要です。

ミラー作成機能が使用できる場所は次の3つです。

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

管理者は、ミラー作成機能を有効にする方式を選択します。

大規模なネットワークでは、複数のミラーサーバーを作成して（企業の各部門用など）、そのうちの1つをカスケードスタイルで中央ミラーサーバー（本社など）として設定できます。これは、複数のクライアントを持つERASのコンフィグレーションと同様です。

ERASでミラー作成機能を有効にするには、管理者が、購入した製品のライセンスキーを登録し、ユーザー名とパスワードを入力する必要があります。管理者がESET Endpoint アンチウイルスのライセンスキー、ユーザー名、およびパスワードを使用した後でESET Endpoint Securityにアップグレードした場合には、元のライセンスキー、ユーザー名、およびパスワードも入れ替える必要があります。

NOTE

ESET Endpoint アンチウイルスクライアントはESET Endpoint Securityのライセンスを使用してアップデートすることもできますが、ESET Endpoint アンチウイルスのライセンスを使用してESET Endpoint Securityのクライアントをアップデートすることはできません。Mac OS X用のESET NOD32アンチウイルスにはミラー機能は搭載していません。

6.6.1.1 ミラーサーバーの動作

ミラーサーバーをホストするコンピュータは常時稼動が前提であり、インターネットまたは複製に使用する上位ミラーサーバーに接続されている必要があります。ミラーサーバーのアップデートパッケージをダウンロードするには、次の2通りの方法があります。

1.HTTPプロトコルを使用する（推奨）
2.共有ネットワークドライブを使用する（SMB）

ESETのアップデートサーバーへのアクセスには認証を受ける必要があります。中央のミラーサーバーは、ユーザー名（通常はEAV-XXXXXXXの形式）とパスワードを使用してアップデートサーバーにアクセスしなければなりません。

NOTE

統合されたHTTPサーバーを使用する場合は（認証なし）、ライセンス対象外のクライアントがネットワークの外部からそのサーバーにアクセスできないようにしてください。

既定の統合されたHTTPサーバーはTCPポート2221でリスンするので、他のアプリケーションでこのポートを使用していないことを確認してください。

NOTE

ERAミラーのHTTPサーバーの方式を使用する場合は、1つのミラーからアップデートするクライアントを400以下にすることをお勧めします。クライアントがそれより多い大規模ネットワークでは、複数のERA（EAV）ミラーサーバー間でミラーアップデートを分散することをお勧めします。ミラーを1つのサーバーで集中管理する必要がある場合は、IISなど、別の種類のHTTPサーバーを使用することをお勧めします。

2つ目の方法（共有ネットワークフォルダによる方法）では、アップデートパッケージを収めたフォルダの共有（"読み取り"権限）が必要です。このシナリオでは、アップデートフォルダに対して"読み取り"権限を持つユーザーのユーザー名とパスワードをクライアントワークステーションに入力する必要があります。

NOTE

ESETクライアントソリューションではシステムユーザーアカウントが使用されるので、現在ログインしているユーザーのネットワークアクセス権限とは権限が異なっています。"Everyone"がネットワークドライブにアクセス可能であり、現在のユーザーがそれらのドライブにアクセスできる場合でも、認証が必要です。また、ローカルサーバーへのネットワークパスを定義するには、UNCパスを使用してください。<ディスク>:¥形式を使用することはお勧めしません。

共有ネットワークフォルダを使用する方法では、一意のユーザー名（NODUSERなど）を作成することをお勧めします。このアカウントは、すべてのクライアントマシンでアップデートのダウンロードのみに使用します。NODUSERアカウントには、アップデートパッケージを収めた共有ネットワークフォルダに対する"読み取り"権限が必要です。

ネットワークドライブに対する認証では、COMPUTER名¥UserやDOMAIN名¥Userのように完全な形式で認証データを入力してください。

6.6.1.2 アップデートの種類

ウイルス定義データベースのアップデート（ESETソフトウェアカーネルのアップデートが収録されていることもあります）のほか、プログラムコンポーネントのアップグレードも入手できます。プログラムコンポーネントのアップグレードではESETセキュリティ製品に新しい機能が追加されるので、再起動が必要になります。

ミラーサーバーを使用すると、管理者は、ESETのアップデートサーバー（または上位のミラーサーバー）からのプログラムアップグレードの自動ダウンロードを無効にして、クライアントに配布できないようにすることができます。新しいバージョンと既存のアプリケーションの間に競合がないことを管理者が確認した後、手動で配布を開始できます。

既定では、プログラムコンポーネントは自動的にダウンロードされないので、ERASで手動で設定する必要があります。詳細については、「ミラーの有効化および設定の方法」を参照してください。

6.6.1.3 ミラーの有効化および設定の方法

ミラーがERAに直接統合されている場合は、ERACを使用してERASに接続し、次の手順を実行します。

●ERACで、[ツール] -> [サーバオプション] -> [アップデート] をクリックします。

●[アップデートサーバ] ドロップダウンメニューから [自動的に選択] を選択するか（ESETのサーバーからアップデートをダウンロードします）、ミラーサーバーへのURL/UNCパスを入力します。

●アップデートインターバルを設定します（60分に設定することをお勧めします）。

●前の手順で [自動的に選択] を選択した場合は、製品の購入後に受け取ったユーザー名（アップデート用ユーザー名）とパスワード（アップデートパスワード）を入力します。上位サーバーにアクセスする場合は、そのサーバーの有効なドメインユーザー名とパスワードを入力してください。

●[アップデートミラーを作成] オプションを選択し、アップデートファイルを保存するフォルダへのパスを入力します。デフォルトでは、これはミラーフォルダへの相対パスです。[アップデートファイルを内部HTTPサーバ経由で配布する] [アップデートファイルを内部HTTPサーバ経由で配布する] の隣にあるチェックボックスが選択されている限り、アップデートは [HTTPサーバポート]（デフォルトでは2221）に定義されたHTTPポート上で使用可能です。[認証] を [なし] に設定します（詳細については、「ミラーサーバーの動作」を参照してください。

NOTE

アップデートで問題が発生した場合は、[アップデートキャッシュのクリア] オプションを選択して、一時的なアップデートファイルが保存されているフォルダをフラッシュします。

●[ミラーダウンロードされたPCU] オプションでは、プログラムコンポーネントのミラーリングを有効にすることができます。PCUのミラーリングを設定するには、[詳細] -> [詳細設定を編集] に移動し、[ESET Remote Administrator] -> [ERA Server] -> [設定] -> [ミラー] を選択します。

●[選択したプログラムコンポーネントのためにミラーを作成する] で、ダウンロードする言語コンポーネントを選択します。ネットワークで使用するすべての言語バージョンのコンポーネントを選択する必要があります。ネットワークにインストールしない言語バージョンをダウンロードすると、不要なネットワークトラフィックが発生します。

ミラー機能は、Windows用プログラムのESET Endpoint アンチウイルスのプログラムインタフェースから直接使用することもできます。ミラーサーバーの実装にどちらを使用するかは、管理者が自由に決定できます。

ESET Endpoint アンチウイルスでミラーサーバーを有効にして起動する手順は、次のとおりです。

1 ESET Endpoint アンチウイルスをインストールします。

2 [詳細設定] ウィンドウ (F5) で、[ツール] > [ライセンス] をクリックします。[追加] …をクリックし、*.licファイルに行き [開く] をクリックします。これによってライセンスがインストールされ、ミラー機能を設定できるようになります。

3 [アップデート] ブランチから [一般] > [詳細設定] ボタンをクリックし、[ミラー] タブをクリックします。

4 [配布用アップデートを作成する] および [内部のHTTPサーバーよりアップデートファイルを提供する] の隣のチェックボックスを選択します。

5 アップデートファイルを保存するフォルダ ([配布用ファイルの保存先フォルダ]) へのフルディレクトリーパスを入力します。

6 [ユーザ名] と [パスワード] の各値は、ミラーフォルダにアクセスするクライアントワークステーションの認証データとして使用されます。ほとんどの場合、これらのフィールドに値を入力する必要はありません。

7 [認証] を [なし] に設定します。

8 ダウンロードするコンポーネントを選択します (ネットワークで使用するすべての言語バージョンのコンポーネントを選択する必要があります)。ESETのアップデートサーバーに存在するコンポーネントのみが表示されます。

6.7 その他の設定

[その他の設定] タブでは、電子メールによるインストールパッケージ送信に使用する [SMTP] サーバーのアドレス、および管理者の電子メール送信に使用する電子メールアドレスを設定できます。サーバーによる認証が必要な場合、該当するユーザー名とパスワードを指定します。

新規クライアント

新規クライアントを許可する	オンにすると、ERA Server に初めて接続した直後に、新規クライアントがクライアントリストに自動的に追加されます。複製により他の ERA Server からインポートされるクライアントは、複製時にクライアントリストに自動的に追加されます。
新規クライアントの新規フラグを自動的にリセットする	オンにすると、新規クライアントが ERA Server に初めて接続しても、新規フラグが自動的には設定されません。詳細については、[クライアント] タブの説明を参照してください。

ポート

ポートをカスタマイズできます。

コンソール	ERA Console が ERA Server への接続に使用するポート（既定では 2223）。
クライアント	ESET クライアントが ERA Server への接続に使用するポート（既定では 2222）。
このサーバの複製ポート	ERA が上位の ERA Server への複製に使用するポート（既定では 2846）。
ESETリモートインストーラ（エージェント）	リモートインストールエージェント(ESET リモートインストーラ)がリモートインストールに使用するポート(既定では 2224)。
Webサーバ	Web サーバーへの接続に使用するポート（既定では 2225）。

NOTE

ポート設定の変更内容を反映するには、ERAサーバーサービスを再起動する必要があります。

ESET Live Guide

収集	疑わしいファイルと統計情報が、指定した間隔で ERAS によりクライアントから ESET のサーバーに転送されます。場合によっては、クライアントからこの情報を直接収集できないこともあります。

ダッシュボード

Webサーバのリストを設定する	ここをクリックしてダッシュボードの Web サーバーリストへアクセスします。

6.8 詳細

[サーバオプション] ウィンドウの [詳細] タブでは、ESETコンフィグレーションエディターからサーバーの詳細設定にアクセスして変更できます。警告メッセージを読み、注意して先に進んでください。

詳細設定では、次の設定などが可能です。

最大ディスク領域使用率(%)	超過すると、一部のサーバー機能は、使用できないことがあります。ERAS に接続している場合は、制限を超過すると通知が ERAC に表示されます。
優先する通信プロトコルのエンコード方式	エンコード方式の種類を定義します。既定の設定をお勧めします。
MACアドレスの名前変更を有効にする(有効から別の有効に)	有効な MAC アドレスの名前変更を有効にします。既定では名前変更は許可されません。つまり、MAC アドレスは、クライアントの一意の識別子の一部です。1 台の PC に複数のエントリーがある場合は、このオプションを無効にしてください。また、MAC アドレスを変更した後もクライアントを同じクライアントとして識別したい場合も、このオプションを無効にすることをお勧めします。
コンピュータ名の変更を有効にする	クライアントコンピュータの名前変更を許可します。有効すると、コンピュータ名はクライアントの一意の識別子の一部になります。
プッシュインストール時に既定のサーバログオンも使用する	ERAS では、ログオンスクリプトおよび電子メールによるリモートインストールの場合にのみユーザー名とパスワードを設定できます。事前定義された値をリモートプッシュインストールでも使用する場合は、このオプションを有効にします。

[Chapter 7]
ESET Remote Administrator Maintenance Tool

7.1 ERA Serverを停止

ESET Remote Administrator Maintenance Toolの目的は、サーバーの動作および保守に関する特定の作業を実行することです。[スタート] > [プログラム] > [ESET] > [ESET Remote Administrator Server] >ESET Remote Administrator Maintenance Toolとクリックすることによってアクセスできます。

ESET Remote Administrator Maintenance Toolを開始し、[次へ] をクリックすると、ERA Server情報ウィンドウが表示されます。このツールには、インストールされているERA Serverに関する概要情報が表示されます。[詳細情報] をクリックすると、表示されている情報の詳細を別のウィンドウで確認できます。[クリップボードにコピー] をクリックすれば、表示されている情報をコピーできます。また、[更新] をクリックして情報の表示を更新することもできます。情報を確認したら、[次へ] をクリックして次の手順に進み、以下のうちからタスクを選択します。

- ●ERA Serverを停止
- ●ERA Serverを起動
- ●データベースの転送
- ●データベースを外部ファイルにバックアップ
- ●データベースを外部ファイルから復元
- ●テーブルを削除
- ●保管データを外部ファイルにバックアップ
- ●保管データを外部ファイルから復元
- ●新しいライセンスキーをインストール
- ●サーバのコンフィグレーションを変更

各タスクの設定の最後に、[すべての設定をファイルに保存] をクリックすると、現在のタスクの設定を保存できます。この設定は、[ファイルからすべての設定をロード] をクリックすることによって、いつでも使用できます。タスクの設定の各手順にも、[すべての設定をファイルに保存] オプションと [ファイルからすべての設定をロード] オプションが用意されています。

7.1.1 ERA Serverの停止

このタスクでは、ESET Remote Administrator Serverサービスを停止します。

NOTE

サービス名はERA_SERVERです。このサービスの実行可能ファイルは、"C:¥Program Files¥ESET¥ESET Remote Administrator¥Server¥era.exe" です。

7.2 ERA Serverを起動

このタスクでは、ESET Remote Administrator Serverサービスを開始します。

NOTE

サービス名はERA_SERVERです。このサービスの実行可能ファイルは、"C:¥Program Files¥ESET¥ESET Remote Administrator¥Server¥era.exe"です。

7.3 データベースの転送

このタスクを使用すると、データベース形式を変換できます。次のデータベース間の変換が可能です。

●MS Access
●MS SQL Server

まず、データベース接続を確認します。この手順は、新しいライセンスキーをアップロードし、サーバー設定を変更することを除いて、すべてのタスクに共通しています。

MS Accessデータベースの場合は、.mdbファイルへのパスを指定します。既定では、ERA Serverのインストール時に指定したパスが使用されます。

他のすべてのデータベース形式では、次のパラメータも設定する必要があります。

●接続文字列: 変換元のデータベースを特定するために使用する特殊な文字列
●ユーザ名: データベースへのアクセスに使用するユーザー名
●パスワード: データベースへのアクセスに使用するパスワード
●スキーマ名: スキーマの名前

[現在のサーバーのコンフィグレーションをロード] をクリックして、ERA Serverの現在の設定を使用します。[接続のテスト] をクリックして、データベース接続をテストします。接続を確立できない場合は、パラメータに誤りがないかどうかをチェックします。データベーステストが成功したら、[次へ] をクリックして次の手順に進みます。

次に、変換先のデータベースを選択します。変換が正常に完了した後、サーバーに接続して新しいデータベースを使用する場合は、[サーバの接続設定を置換する] を選択します。このオプションを選択しなかった場合、新しいデータベースが作成されますが、サーバーでは新しいデータベースバージョンにアップデートされません。

MS Accessデータベースも含め、すべてのデータベースの種類について、データベーステーブルを自動的に作成するか ([新しいデータベース内に自動的にテーブルを作成する])、または次の手順でデータベースにテーブルを挿入するか ([スクリプトの表示] -> [ファイルに保存]) を選択します。

7.4 データベースを外部ファイルにバックアップ

このツールでは、データベースのバックアップファイルを作成できます。このウィンドウでは、バックアップ元のデータベースを選択します。バックアップ元のデータベースは、次の手順で指定したバックアップファイルにコピーされます。

ウィンドウの下部にあるオプションのパラメータを使用すると、既存のファイルの上書き（[存在する場合は上書きする]）や、バックアッププロセス中にESET Remote Administrator Serverを停止する指定（[タスクの処理中はサーバを停止する]）が可能です。[次へ] をクリックして、タスクの実行を確定します。

7.5 データベースを外部ファイルから復元

このタスクを使用すると、バックアップファイルからデータベースを復元できます。このウィンドウでは、データベースの種類を選択します。

MS Accessデータベースも含め、すべてのデータベースの種類について、データベーステーブルを自動的に作成するか（[新しいデータベース内に自動的にテーブルを作成する]）、または次の手順でデータベースにテーブルを挿入するか（[スクリプトの表示] -> [ファイルに保存]）を選択します。

次の手順では、データベースの復元のファイルを選択します。ウィンドウの下部にあるオプションのパラメータを使用すると、前の手順で選択したものとは異なる種類のデータベースからのファイルのインポート（[別の種類のデータベースからのインポートを許可する]）や、データベースの復元中にESET Remote Administrator Serverを停止する指定（[タスクの処理中はサーバを停止する]）が可能です。[次へ] をクリックして、タスクの実行を確定します。

7.6 テーブルを削除

データベースから現在のテーブルが削除されます。結果的に、データベースは、ERA Serverのインストール直後の状態に戻ります。最初のウィンドウの設定は、データベースの変換の設定と似ています（「データベースの変換」を参照）。このウィンドウでは、データベースの種類を選択します。次の手順では、この操作の確定を求められます。[はい、同意します] を選択し、[次へ] をクリックして操作を確定します。

NOTE

データベースにMS SQL、My SQLを使用している場合は、ERA Serverを停止してからテーブルを削除することをお勧めします。

MS Accessデータベースを使用している場合は、既定の空のデータベースに置換されます。

7.7 保管データを外部ファイルにバックアップ

このタスクはストレージのバックアップを実行します。このバックアップは、保管データフォルダ（デフォルトではC:¥ProgramData¥ESET¥ESET Remote Administrator¥Server¥storage¥）の全データを外部ダンプファイル（*.dmp）に保存します。重要なサーバーのログおよび設定が指定のフォルダに保存されます。すでに存在する.dmpファイルを上書きしたい場合は、［存在する場合は上書きする］にチェックを入れます。保管データのバックアップタスクによってサーバーのパフォーマンスが低下することがあるため、［タスク処理中はサーバを停止する］オプションを選択した状態にしておくことをお勧めします。［次へ］に続いて［スタート］をクリックするとタスクが開始されます。

7.8 保管データを外部ファイルから復元

このタスクは、以前に保存されたダンプ(*.dmp)ファイルから保管データの復元を実行します。フォルダアイコンをクリックして、ダンプファイルが存在するフォルダに行きます。保管データの復元タスクによってサーバーのパフォーマンスが低下することがあるため、[タスク処理中はサーバを停止する]オプションを選択した状態にしておくことをお勧めします。[次へ]に続いて[開始]をクリックするとタスクが開始されます。

7.9 新しいライセンスキーをインストール

サーバーで使用する新しいライセンスキーを追加するには、新しいライセンスキーの場所を入力します。

必要に応じて、既存のライセンスキーを上書きします（[すでに存在する場合は上書きする]）。また、必要に応じて、サーバーを再起動します（[サーバを強制的に起動する（実行中でない場合）]）。[次へ] をクリックして確定し、操作を完了します。

7.10 サーバーのコンフィグレーションを変更

ERACをインストール済みであれば、このタスクではESETコンフィグレーションエディターが起動します。タスクを完了するとESETコンフィグレーションエディターのウィンドウが開き、ERA Serverの詳細設定を編集できます。この設定には、[ツール] -> [サーバオプション] -> [詳細] -> [詳細設定を編集] を選択してアクセスすることもできます。

NOTE

この機能を使用するには、ERA Consoleがインストールされている必要があります。[ファイルからすべての設定をロード] オプションを使用して、サーバー設定を.xmlファイルに保存して、後でアップロードすることができます。

7.11 コマンドラインインターフェイス

ESET Remote Administrator Maintenance Tool (ERAtool.exe) は、コマンドラインツールとしての機能も果たし、スクリプトへの統合も可能です。ツールを動作させると、パラメータを構文解析して、指定された順番で各アクションを実行します。引数が与えられない場合は、代わりに対話形式のウィザードが実行されます。

以下のコマンドがサポートされています。

/startserverまたは/startservice	ESET Remote Administrator サーバーのサービスを起動します。
/stopserverまたは/stopservice	ESET Remote Administrator サーバーのサービスを停止します
/gui	すべてのタスク終了後に対話形式のウィザードを起動します

スラッシュで始まらないパラメータはすべて、実行されるべきコンフィグレーションスクリプトのファイル名として解釈されます。コンフィグレーションスクリプトは、対話形式のウィザードで設定を保存することによって作成されます。

▸▸▸ NOTE

ERAtool.exeは、管理者権限を必要とします。ERAtool.exeを呼び出すスクリプトが必要な権限を持たない場合、Windowsが権限アップのための対話形式プロンプトを表示するか、または別のコンソールプロセスでのツールを実行します(ツール出力はありません)。

[Chapter 8]
トラブルシューティング

8.1 FAQ

ここでは、ERAのインストールと運用に関連して、最も頻繁に寄せられる質問や問題に対する解決策について説明します。

8.1.1 Windows Server 2003へのESET Remote Administratorのインストールに失敗する

原因:

原因の1つとして、ターミナルサーバーがシステム上で実行モードで稼働していることが考えられます。

解決策:

Microsoftでは、ターミナルサーバーサービスを実行しているシステムにプログラムをインストールする際には、ターミナルサーバーを"インストール"モードに切り替えることを推奨しています。そのためには、[コントロールパネル]->[プログラムの追加と削除] を使用するか、コマンドプロンプトを開いてchange user /installコマンドを発行します。インストール後、change user /executeと入力して、ターミナルサーバーを実行モードに戻します。このプロセスの詳細な手順については、以下の記事を参照してください。http://support.microsoft.com/kb/320185.

8.1.2 GLEエラーコードの意味

ESET Remote Administrator Consoleを使用してESET Endpoint SecurityまたはESET Endpoint アンチウイルスをインストールするときに、GLEエラーが生成されることがあります。GLEエラーコードの意味を確認するには、次の手順を実行します。

1) [スタート] -> [ファイル名を指定して実行] をクリックして、コマンドプロンプトを開きます。cmdと入力し、[OK] をクリックします。

2) コマンドプロンプトで、net helpmsg error_number<エラーコード>と入力します。

例: net helpmsg 55

結果:指定されたネットワークリソースまたはデバイスは利用できません。

8.2 よく検出されるエラーコード

ERAの操作中に、機能や操作に伴う問題を示すエラーコードを含むエラーメッセージが表示されることがあります。この後の章では、プッシュインストールの実行時によく検出されるエラーコード、およびERASログで検出されるエラーについて説明します。

8.2.1 ESET Remote Administratorを使用してESET Endpoint SecurityまたはESET Endpoint アンチウイルスをリモートでインストールするときに表示されるエラーメッセージ

SCエラーコード6、GLEエラーコード53：対象のコンピュータにIPC接続を確立できませんでした
IPC接続を確立するには、次の要件を満たしている必要があります。

1.ERASがインストールされているコンピュータと対象のコンピュータにTCP/IPスタックがインストールされている。
2.Microsoftネットワークのファイルとプリンタの共有がインストールされている。
3.ファイル共有ポートが開いている（135～139、445）。
4.対象のコンピュータがPING要求に応答する。

SCエラーコード6、GLEエラーコード67：対象のコンピュータにESETインストーラをインストールできませんでした
クライアントのシステムドライブ上で管理共有ADMIN$にアクセスできる必要があります。

SCエラーコード6、GLEエラーコード1326：対象のコンピュータにIPC接続を確立できませんでした。原因はおそらくユーザ名かパスワードの誤りです
管理者のユーザ名およびパスワードが誤って入力されているか、まったく入力されていません。

SCエラーコード6、GLEエラーコード1327：対象のコンピュータにIPC接続を確立できませんでした
管理者のパスワードフィールドが空白です。パスワードフィールドが空白の場合、リモートプッシュインストールは機能しません。

SCエラーコード11、GLEエラーコード5：対象のコンピュータにESETインストーラをインストールできませんでした
十分なアクセス権限がないため、インストーラはクライアントコンピュータにアクセスできません（アクセスが拒否されました）。

SCエラーコード11、ESETエラーコード1726：対象のコンピュータにNOD32インストーラをインストールできませんでした
このエラーコードは、プッシュインストールを1回試行した後、プッシュインストールのウィンドウを閉じずにインストールを繰り返し試行した場合に表示されます。

8.2.2 era.logでよく検出されるエラーコード

0x1203-UPD_RETVAL_BAD_URL
更新モジュールエラーです。アップデートサーバー名が正しく入力されていません。

0x1204-UPD_RETVAL_CANT_DOWNLOAD
このエラーは、次の場合に発生します。

●HTTP経由のアップデート
400～500のHTTPエラーコード（エラー401、403、404、および407を除く）がアップデートサーバーから返された場合
CISCOベースのサーバーからダウンロードするアップデートで、HTTP認証応答の形式が変更されている場合

●共有フォルダからのアップデート
認証が正しくないというカテゴリおよびファイルが見つからないというカテゴリのどちらにも属さないエラー（接続が切断されました、サーバーが存在しませんなど）が返された場合

●両方のアップデート方法
upd.verファイルに登録されているサーバーの中に見つからないものがある場合（このファイルは%ALLUSERS PROFILE% ¥Application Data¥ESET¥ESET Remote Administrator¥Server¥updfilesにあります）
フェールセーフサーバーに接続できなかった場合（レジストリ内の対応するESETエントリが削除されたことが原因であることが考えられます）

●ERASでのプロキシサーバーの不適切な設定
管理者は正しい形式でプロキシサーバーを指定する必要があります。

0x2001-UPD_RETVAL_AUTHORIZATION_FAILED
アップデートサーバーに対する認証に失敗しました。ユーザ名またはパスワードが正しくありません。

0x2102-UPD_RETVAL_BAD_REPLY
この更新モジュールエラーは、プロキシサーバーを介してインターネットに接続している場合、つまりWebwasherプロキシを使用している場合に発生することがあります。

0x2104-UPD_RETVAL_SERVER_ERROR
500より大きいHTTPエラーコードを示す更新モジュールエラーです。ESET HTTPサーバーを使用している場合、エラー500はメモリの割り当てに関する問題を示します。

0x2105-UPD_RETVAL_INTERRUPTED
この更新モジュールエラーは、プロキシサーバーを介してインターネットに接続している場合、つまりWebwasherプロキシを使用している場合に発生することがあります。

8.3 ERASの問題の診断方法

ERASで問題が発生している疑いがある場合や、ERASが正しく機能していない場合は、次の手順を実行することをお勧めします。

1 ERASのログを確認します。ERACのメインメニューから[ツール]->[サーバオプション]をクリックします。[サーバオプション]ウィンドウで[ログ]タブをクリックし、[ログを表示]をクリックします。

2 エラーメッセージが表示されない場合は、[サーバオプション]ウィンドウで[ログレベル]をレベル5に上げます。問題の追跡が終わったら、この値を既定値に戻すことをお勧めします。

3 問題のトラブルシューティングを行うには、同じタブでデータベースデバッグログを有効にします。[デバッグログ]セクションを参照してください。[デバッグログ]は、問題を再現する場合にのみ有効にすることをお勧めします。

4 このドキュメントに記載されているエラーコード以外のものが表示される場合は、サポートセンターにお問い合わせください。サポートセンターへのお問い合わせでは、プログラムの動作、問題を再現する方法、問題を回避する方法などを説明してください。使用しているすべてのESET セキュリティ製品のプログラムバージョンも確認しておくことが非常に重要です。

[Chapter 9]
ヒント

9.1 スケジューラ

ESET Endpoint アンチウイルスとESET Endpoint Securityにはタスクスケジューラが統合されており、定期的なコンピュータの検査やアップデートなどをスケジュールできます。指定したすべてのタスクがスケジューラに表示されます。

ERAで設定できるタスクは次のとおりです。

●外部アプリケーションの実行
●ログの保守
●コンピュータの検査
●コンピュータステータスのスナップショットの作成
●アップデート
●自動スタートアップファイルのチェック

ほとんどの場合、外部アプリケーションの実行タスクを設定する必要はありません。自動スタートアップファイルのチェックタスクは既定のタスクです。パラメータを変更しないことをお勧めします。インストール後に変更を行っていなければ、ESET Endpoint アンチウイルスとESET Endpoint Securityでは、このタイプのタスクが2つ事前定義されています。最初のタスクでは、ユーザーがログオンするたびにシステムファイルがチェックされます。2つ目のタスクでは、ウイルス定義データベースが正常にアップデートされた後、最初のタスクと同じ処理が行われます。管理者にとっては、コンピュータの検査タスクとアップデートタスクが最も便利です。

コンピュータの検査	クライアントで（通常はローカルドライブの）定期的なウイルススキャンを行います。
アップデート	このタスクは ESET クライアントソリューションをアップデートします。このタスクは事前定義されたタスクで、既定では 60 分ごとに実行されます。通常、パラメータを変更する必要はありません。ただし、ノートパソコンは例外です。ノートパソコンの所有者は、ローカルネットワーク外でインターネットに接続することがよくあるためです。その場合は、1 つのタスクで 2 つのアップデートプロファイルを使用するようにアップデートタスクを変更できます。これによって、ローカルのミラーサーバーと ESET のアップデートサーバーのどちらからでもノートパソコンをアップデートできるようになります。

スケジュール設定はESETコンフィグレーションエディターの [Windows製品ラインv3およびv4] > [ESETカーネル] > [設定] > [スケジューラ/プランナー] >などにもあります。

詳細については、「ESETコンフィグレーションエディター」を参照してください。

ダイアログウィンドウに既存のタスクが表示される場合もあれば（タスクを変更するには、[編集] をクリックします）、何も表示されない場合もあります。これは、クライアント（設定済みで動作しているクライアントなど）から設定を開いたか、タスクが設定されていない既定のテンプレートで新しいファイルを開いたかによって決まります。

すべての新しいタスクには属性IDが割り当てられています。既定のタスクには10進数のID（1、2、3など）が割り当てられ、カスタムタスクには16進数のキー（4AE13D6Cなど）が割り当てられます。このキーは、タスクの新規作成時に自動的に生成されます。
タスクのチェックボックスがオンの場合、そのタスクが有効であり、指定クライアントで実行される予定であることを示します。

[スケジュールタスク] ウィンドウの各種ボタンの機能は次のとおりです。

追加	新しいタスクを追加します。
編集	選択されたタスクを変更します。
IDの変更	選択されたタスクの ID を変更します。
詳細	選択されたタスクについての概要情報を表示します。
削除マークを付ける	.xml ファイルの適用時に、このボタンをクリックして選択したタスク（同一 ID を持つ複数のタスク）が、対象のクライアントから削除されます。
リストから削除	選択されたタスクを一覧から削除します。.xml 形式のコンフィグレーションファイルの一覧からタスクを削除しても、そのタスクが対象のワークステーションから削除されるわけではありません。

新しいタスクを作成する場合（[追加] ボタン）や既存のタスクを編集する場合（[編集] ボタン）は、いつタスクを実行するかを指定する必要があります。特定の期間が経過した後にタスクを繰り返し実行できるほか（毎日12時、毎週金曜日など）、イベントでタスクをトリガすることもできます（アップデートが正常に完了した後、毎日最初にコンピュータを起動したときなど）。

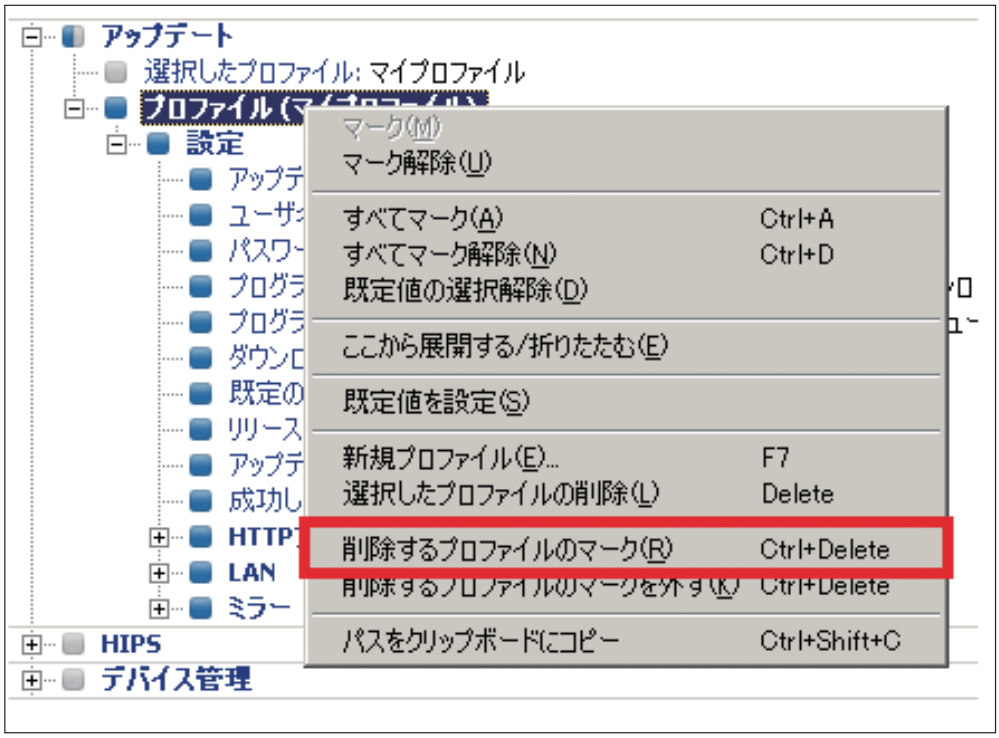
オンデマンドのコンピュータ検査タスクの最後の手順では [特殊設定] ウィンドウが表示され、検査に使用する設定、つまり使用する検査プロファイルと検査の対象を定義できます。

アップデートタスクの最後の手順では、指定したタスクの中で実行するアップデートプロファイルを指定します。このタスクは事前定義されたタスクで、既定では60分ごとに実行されます。通常、パラメータを変更する必要はありません。ただし、ノートパソコンは例外です。ノートパソコンの所有者は、社内ネットワーク外でインターネットに接続することもよくあるためです。最後のダイアログで2種類のアップデートプロファイルを指定すると、ローカルサーバーとESETのアップデートサーバーのどちらからでもアップデートができるようになります。

9.2 既存のプロファイルの削除

誤って重複して作成されたプロファイル（アップデートプロファイルまたは検査プロファイル）が見つかることがあります。スケジューラの他の設定を損なうことなく、このようなプロファイルをリモートで削除するには、次の手順を実行します。

●ERACで [クライアント] タブをクリックし、問題があるクライアントをダブルクリックします。
●クライアントの [プロパティ] ウィンドウで [コンフィグレーション] タブをクリックします。[ダウンロードしたコンフィグレーションを新しいコンフィグレーションタスクで使用します] オプションを選択し、[新規タスク] ボタンをクリックします。
●新規タスクウィザードで、[編集] をクリックします。
●Configuration Editorで、Ctrl＋Dキーを押してすべての設定を選択解除します（グレー表示にします）。新たな変更箇所は青で表示されるので、誤って変更することを防止できます。
●削除するプロファイルを右クリックし、コンテキストメニューから [削除するプロファイルのマーク] を選択します。タスクをクライアントに配信すると、これらのプロファイルが直ちに削除されます。



●ESETコンフィグレーションエディターで [コンソール] ボタンをクリックし、設定を保存します。
●選択したクライアントが、右側の [選択したアイテム] カラムに表示されていることを確認します。[次へ] をクリックし、[終了] をクリックします。

9.3 XML形式のクライアントコンフィグレーションのエクスポートとその他の機能

ERACの [クライアント] タブでクライアントを選択します。右クリックして、コンテキストメニューの [コンフィグレーション] を選択します。[名前を付けて保存...] をクリックして、指定のクライアントに割り当てられたコンフィグレーションを.xmlファイルにエクスポートします。この.xmlファイルは、後でさまざまな操作に使用できます。

●リモートインストールの場合は、事前に定義しておくコンフィグレーションのテンプレートとして.xmlファイルを使用できます。つまり、新しい.xmlファイルは作成されず、既存の.xmlファイルが新しいインストールパッケージに割り当てられます ([選択])。

●複数のクライアントを設定する場合、選択したクライアントでは、あらかじめダウンロードされた.xmlファイルを受信し、そのファイルで定義されている設定を採用します (新しいコンフィグレーションファイルは作成されません。[選択] ボタンで既存のファイルを割り当てることのみ可能です)。

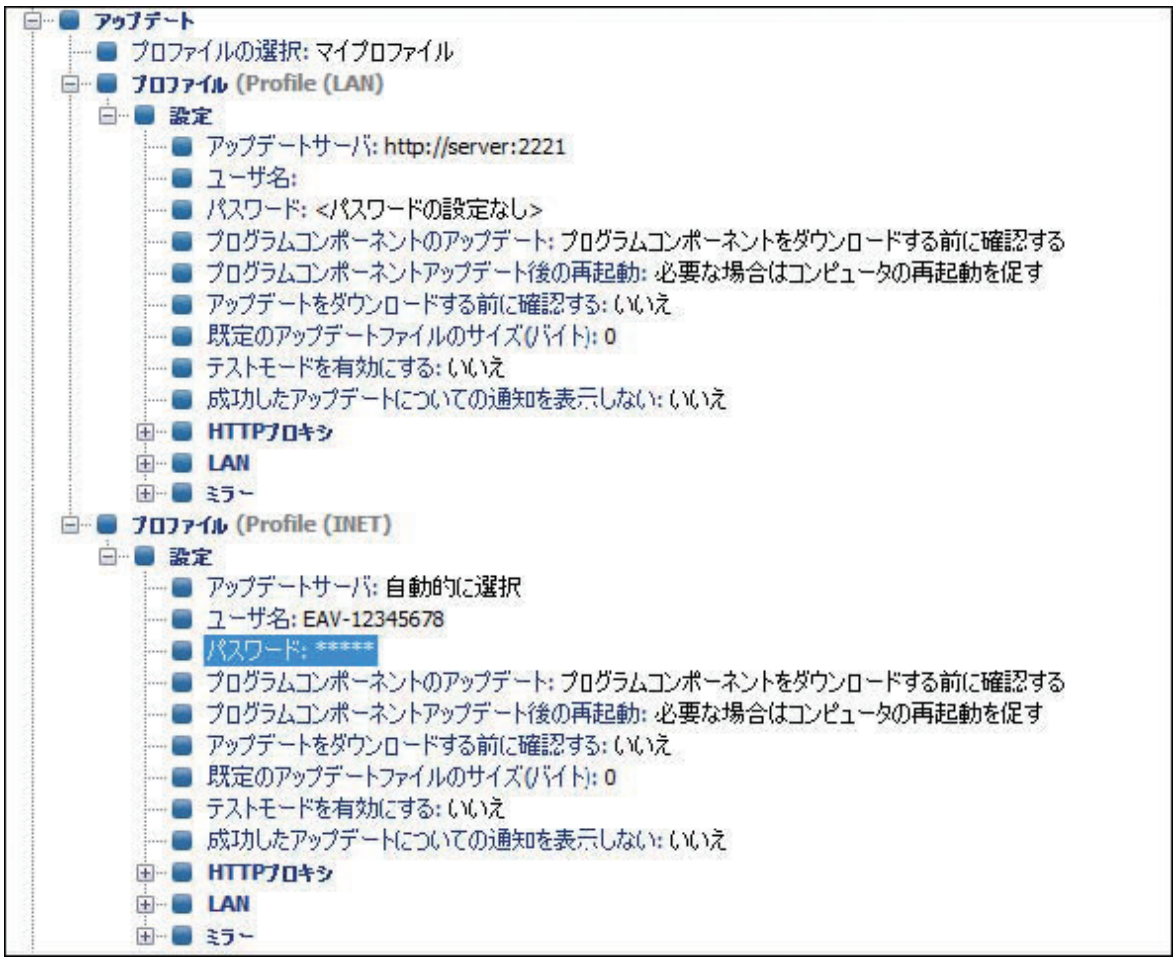
例

ESETセキュリティ製品が1台のワークステーションにだけインストールされているとします。設定をプログラムのユーザーインタフェースで直接調整します。終了したら、設定を.xmlファイルにエクスポートします。この.xmlファイルは、他のワークステーションへのリモートインストールに使用できます。"ポリシーベース"モードを適用することになっている場合、ファイアウォール ルールの微調整などのタスクでは、この方法が非常に便利です。

9.4 ノートパソコン向けの組み合わせアップデート

ローカルネットワークにノートパソコンなどのモバイルデバイスがある場合は、2つのプロファイルを使用する組み合わせアップデートの設定をお勧めします。この場合のプロファイルで既定に設定されたアップデートサーバーは、ESETのアップデートサーバーとローカルのミラーサーバーです。組み合わせアップデートでは、まず、ノートパソコンからローカルのミラーサーバーに接続します。この接続ができない場合、つまり、ノートパソコンがオフィスの外にある場合は、ESETのサーバーから直接アップデートをダウンロードします。

1. コンフィグレーションエディタを開き、対象製品の [アップデート機能] を開きます。
2. メインメニューの [プロファイル] -> [新規プロファイル] をクリックします。
3. [既定のプロファイルを使用する] のチェックを外して、プロファイル名を入力します。
4. 新規に作成したプロファイルの設定を開き、アップデートサーバーを設定します。
5. 必要に応じてユーザー名とパスワード、HTTPプロキシ等の設定を行います。
   ※上記2～5までの作業で、ESETから直接アップデートを行うプロファイル（INET）、LAN内のミラーからアップデートを行うプロファイル（LAN）を作成します。
6. 対象製品の [スケジューラー/プランナー] を開きます。
7. [スケジューラー/プランナー] の [編集] ボタンをクリックします。



8 タスクを新規作成するには、[追加] をクリックします。[スケジュールタスク] ドロップダウンメニューから [アップデート] を選択し、[次へ] をクリックします。タスク名 ("組み合わせアップデート"など) を入力し、60分間隔で繰り返し実行するように指定して、プライマリプロファイルとセカンダリプロファイルの選択に進みます。

9 ノートパソコンのワークステーションで先にミラーサーバーに接続する場合は、プライマリプロファイルをLAN、セカンダリプロファイルをINETとします。プロファイルLANからアップデートできない場合に限り、プロファイルINETが適用されます。

9.5 ERAを使用したサードパーティ製品のインストール

ESET製品のリモートインストールに加えて、ESET Remote Administratorではその他のプログラムをインストールできます。ただし、カスタムインストールパッケージが.msi形式である必要があります。カスタムパッケージのリモートインストールの実行に使用するプロセスは、「リモートプッシュインストール」に記載されているプロセスとよく似ています。

主な違いは、下記に示した、パッケージ作成プロセスです。

1. ERACから [リモートインストール] タブをクリックします。
2. [コンピュータ] タブを選択し、コンテンツ内の任意の場所を右クリックします。コンテキストメニューの [パッケージの管理] を選択します。
3. [パッケージの種類] ドロップダウンメニューから [カスタムパッケージ] を選択します。
4. [追加] をクリックして、[ファイルを追加] をクリックし、目的のmsiパッケージを選択します。
5. [パッケージエントリファイル] ドロップダウンメニューからファイルを選択し、[作成] をクリックします。
6. 元のウィンドウに戻ると、.msiファイルのコマンドラインパラメータを指定できます。コマンドラインパラメータは、指定したパッケージのローカルインストールに使用するものと同じです。
7. [名前を付けて保存...] をクリックして、パッケージを保存します。
8. [閉じる] をクリックして、インストールパッケージエディタを終了します。

新規作成したカスタムパッケージは、前の章で説明したリモートインストールと同じ方法でクライアントワークステーションに配布できます。リモートプッシュインストール、ログオンスクリプトによるインストール、または電子メールによるインストールによって、パッケージが対象のワークステーションに送信されます。パッケージを実行した時点以降、インストールはMicrosoft Windowsインストーラサービスによって処理されます。

NOTE

カスタム作成されたサードパーティのインストールパッケージでは、パッケージ毎に100MByteのサイズ制限があることに注意してください。

[Chapter 10]
ESET SysInspector

10.1 ESET SysInspectorの概要

ESET SysInspectorは、お使いのコンピュータを徹底的に検査し、収集されたデータを総合的に表示するアプリケーションです。インストールされているドライバーやアプリケーション、ネットワーク接続、重要なレジストリーエントリーなどの情報は、疑わしいシステム動作（ソフトウェアやハードウェアの互換性の問題やマルウェア感染によるものなど）の調査に役立てることができます。

ESET SysInspectorにアクセスする方法は2通りあります。ESET Securityソリューションの統合バージョンを使用するか、または弊社サイトから無償のスタンドアロンバージョン（SysInspector.exe）をダウンロードします。どちらのバージョンも機能的には同じであり、同一のプログラムコントロールをもっています。唯一の相違は、出力の管理の仕方にあります。スタンドアロンバージョンまたは統合バージョンのどちらでも、システムスナップショットを.xmlファイルにエクスポートし、ディスクに保存することができます。ただし、統合バージョンでは、[ツール] > [ESET SysInspector] を使って、システムスナップショットを直接保存することもできます（ESET Remote Administratorを除く）。

10.1.1 ESET SysInspectorの起動

ESETのWebサイトからダウンロードしたSysInspector.exe実行可能ファイルを実行するだけで、ESET SysInspectorを起動できます。

アプリケーションがシステムを検査している間、しばらくお待ちください。お使いのハードウェアと収集されるデータによって異なりますが、これには数分間かかる可能性があります。

10.2 ユーザーインタフェースとアプリケーションの使用

メインウィンドウは、使いやすいように4つの主要セクションに分かれています。プログラムのコントロールはメインウィンドウの上部、ナビゲーションウィンドウは左側、説明ウィンドウは中央右側、詳細ウィンドウはメインウィンドウの下部右側にそれぞれ配置されています。ログ状況のセクションには、ログの基本パラメータ（使用されているフィルタ、フィルタタイプ、ログは比較の結果かどうかなど）が一覧表示されます。

10.2.1 プログラムコントロール

ここでは、ESET SysInspectorで使用可能なすべてのプログラムコントロールについて説明します。

ファイル
[ファイル] をクリックすると、後で調査するために現在のシステムステータスを保存したり、以前に保存されたログを開いたりできます。公開を目的としている場合は、[送信に適切] でログを生成することをお勧めします。この形式のログでは、機密情報 (現在のユーザー名、コンピュータ名、ドメイン名、現在のユーザー特権、環境変数など) は省かれます。

NOTE
以前に保存したESET SysInspectorレポートをメインウィンドウにドラッグアンドドロップするだけで、それらのレポートを開くことができます。

[ツリー]
すべてのノードを展開したり閉じたりできます。また、選択したセクションをサービススクリプトにエクスポートすることもできます。

[リスト]
プログラム内でのナビゲーションをより容易にするための機能のほか、オンラインでの情報検索などの他のさまざまな機能が含まれます。

[ヘルプ]
アプリケーションとその機能に関する情報が含まれます。

[詳細]
この設定は、メインウィンドウに表示される情報に影響し、情報を処理しやすくなります。"基本"モードでは、システム内の一般的な問題に対する解決策を見つけるための情報にアクセスできます。"中間"モードでは、あまり一般的でない詳細が表示されます。"完全"モードのESET SysInspectorでは、極めて具体的な問題の解決に必要な全ての情報が表示されます。

[フィルタリング]
アイテムのフィルタリングは、システム内の疑わしいファイルまたはレジストリエントリを見つけるために最もよく使用される方法です。スライダを調整することで、リスクレベルによってアイテムをフィルタできます。スライダーを最左端 (リスクレベル1) にすると、全ての項目が表示されます。スライダを右に動かすと、現在のリスクレベルより低いリスクレベルのアイテムが除外され、表示されたレベルのアイテムよりも疑わしいアイテムのみが表示されます。スライダーを最右端にすると、既知の有害な項目のみが表示されます。

リスク6～9に分類されている全ての項目には、セキュリティリスクが生じる可能性があります。

NOTE
項目のリスクレベルは、項目の色とリスクレベルのスライダーの色を比べることにより迅速に判別できます。

[検索]

[検索] を使用して、特定のアイテムを、その名前または名前の一部によって簡単に見つけることができます。検索要求の結果は、説明ウィンドウに表示されます。

[戻る]

左矢印または右矢印をクリックすることで、説明ウィンドウ内で前に表示された情報に戻ることができます。左矢印と右矢印をクリックする代わりに、それぞれ BackSpaceキーとスペースキーを使用できます。

[ステータスセクション]

ナビゲーションウィンドウ内の現在のノードを表示します。

重要

赤で表示されているアイテムは、プログラムによって潜在的な危険性があるとマークされた不明アイテムです。項目が赤で表示されている場合でも、ファイルの削除が可能であることを意味するわけではありません。削除する前に、ファイルが本当に危険かどうか、または不要かどうかを確認してください。

10.2.2 ESET SysInspectorにおけるナビゲーション

ESET SysInspectorでは、さまざまな種類の情報が、ノードと呼ばれる複数の基本セクションに分けられています。サブノードがある場合は、各ノードをサブノードに展開して追加情報を確認することができます。ノードの展開/折りたたみを行うには、ノードの名前をダブルクリックするか、またはノードの名前の横にある＋または－をクリックします。ナビゲーションウィンドウでノードおよびサブノードのツリー構造内を参照すると、説明ウィンドウに各ノードのさまざまな詳細情報が表示されます。説明ウィンドウでアイテムを参照すると、各アイテムの追加の詳細情報が詳細ウィンドウに表示されます。

ナビゲーションウィンドウのメインノード、および説明ウィンドウと詳細ウィンドウの関連情報についての説明を次に示します。

[実行中のプロセス]
このノードには、ログの生成時に実行されていたアプリケーションとプロセスに関する情報が含まれます。説明ウィンドウには、プロセスによって使用されたダイナミックライブラリとシステム内のそれらのライブラリの場所、アプリケーションベンダの名前、ファイルのリスクレベルなど、各プロセスに関する追加の詳細情報が表示されます。

詳細ウィンドウには、ファイルサイズやハッシュなど、説明ウィンドウで選択した項目に関する追加情報が表示されます。

▸▸▸ NOTE

オペレーティングシステムは、複数の重要なカーネルコンポーネントで構成されます。これらのコンポーネントは、毎日24時間稼動し、他のユーザーアプリケーションに対して基本的かつ重要な機能を提供します。場合によっては、ESET SysInspectorツールに表示されるそれらのプロセスのファイルパスが¥??¥で始まることもあります。これらの記号はプロセスの起動前最適化を可能にするもので、システムにとって安全です。

[ネットワーク接続]
説明ウィンドウには、ナビゲーションウィンドウで選択したプロトコル（TCPまたはUDP）を使用してネットワーク経由で通信するプロセスとアプリケーションのリストが、アプリケーションの接続先となるリモートアドレスと共に表示されます。DNSサーバーのIPアドレスをチェックすることもできます。

詳細ウィンドウには、ファイルサイズやハッシュなど、説明ウィンドウで選択した項目に関する追加情報が表示されます。

[重要なレジストリエントリ]
スタートアッププログラムやブラウザヘルパオブジェクト（BHO）を指定するものなど、システムに関するさまざまな問題に関連することが多い選択されたレジストリエントリのリストが表示されます。

説明ウィンドウには、特定のレジストリエントリにどのファイルが関連しているかが示されます。詳細ウィンドウでは、追加の詳細情報を確認できます。

[サービス]
説明ウィンドウには、Windowsサービスとして登録されているファイルのリストが表示されます。詳細ウィンドウで、サービスを開始するための設定方法と、ファイルに関する特定の詳細を確認できます。

[ドライバ]
システムにインストールされているドライバのリストです。

［重要なファイル］
説明ウィンドウには、Microsoft Windowsオペレーティングシステムに関連する重要なファイルの内容が表示されます。

［システムスケジューラタスク］
Winodwsタスクスケジューラによって指定の時刻 /間隔で起動されるタスクのリストを示します。

［システム情報］
ハードウェアとソフトウェアに関する詳細情報と、set環境変数、ユーザー権限、およびシステムイベントログに関する情報を表示します。

［ファイルの詳細］
［プログラムファイル］フォルダ内の重要なシステムファイルおよびファイルのリストです。ファイル固有の追加情報は、説明ウィンドウと詳細ウィンドウに表示されます。

［バージョン情報］
ESET SysInspectorのバージョンに関する情報とプログラムモジュールのリストです。

10.2.2.1 キーボードショートカット

ESET SysInspectorで使用できるショートカットキーは、次のとおりです。

ファイル

Ctrl＋O	既存のログを開きます。
Ctrl＋S	作成したログを保存します。

生成

Ctrl＋G	コンピュータの標準状態のスナップショットを生成します。
Ctrl＋H	機密情報もログ記録できるコンピュータの状態のスナップショットを生成します。

項目のフィルタリング

1, O	良好、リスクレベル1～9の項目が表示されます。
2	良好、リスクレベル2～9の項目が表示されます。
3	良好、リスクレベル3～9の項目が表示されます。
4, U	不明、リスクレベル4～9の項目が表示されます。
5	不明、リスクレベル5～9の項目が表示されます。
6	不明、リスクレベル6～9の項目が表示されます。
7, B	危険、リスクレベル7～9の項目が表示されます。
8	危険、リスクレベル8～9の項目が表示されます。
9	危険、リスクレベル9の項目が表示されます。
-	リスクレベルを下げます。
＋	リスクレベルを上げます。
Ctrl＋9	フィルタリングモード、同等以上のレベル
Ctrl＋O	フィルタリングモード、同等レベルのみ

表示

Ctrl＋5	ベンダによる表示、全てのベンダ
Ctrl＋6	ベンダによる表示、Microsoftのみ
Ctrl＋7	ベンダによる表示、他の全てのベンダ
Ctrl＋3	完全な詳細を表示します。
Ctrl＋2	中程度の詳細を表示します。
Ctrl＋1	基本的な表示です。
BackSpace	1ステップ戻ります。
Space	1ステップ進みます。
Ctrl＋W	ツリーを展開します。
Ctrl＋Q	ツリーを折りたたみます。

その他のコントロール

Ctrl＋T	検索結果で選択した後、項目の元の場所に移動します。
Ctrl＋P	項目についての基本情報を表示します。
Ctrl＋A	項目についての完全情報を表示します。
Ctrl＋C	現在の項目のツリーをコピーします。
Ctrl＋X	項目をコピーします。
Ctrl＋B	選択したファイルについての情報をインターネット上で検索します。
Ctrl＋L	選択したファイルが格納されているフォルダを開きます。
Ctrl＋R	該当するエントリをレジストリエディタで開きます。
Ctrl＋Z	ファイルまでのパスをコピーします（項目がファイルに関連付けられている場合）。
Ctrl＋F	検索フィールドに切り替えます。
Ctrl＋D	検索結果を閉じます。
Ctrl＋E	サービススクリプトを実行します。

比較

Ctrl＋Alt＋O	比較元と比較先のログを開きます。
Ctrl＋Alt＋R	比較を取り消します。
Ctrl＋Alt＋1	全ての項目を表示します。
Ctrl＋Alt＋2	追加された項目のみを表示します。ログには現在のログにある項目が表示されます。
Ctrl＋Alt＋3	削除された項目のみを表示します。ログには前回のログにある項目が表示されます。
Ctrl＋Alt＋4	置き換えられた項目のみを表示します（ファイルも含まれます）。
Ctrl＋Alt＋5	ログ間の相違のみを表示します。
Ctrl＋Alt＋C	比較結果を表示します。
Ctrl＋Alt＋N	現在のログを表示します。
Ctrl＋Alt＋P	前回のログを開きます。

その他

F1	ヘルプを表示します。
Alt＋F4	プログラムを閉じます。
Alt＋Shift＋F4	確認せずにプログラムを閉じます。
Ctrl＋I	統計をログに記録します。

10.2.3 比較

比較機能を使用すると、ユーザーは既存の2つのログを比較できます。この機能により、両方のログで共通していない一連のアイテムが表示されます。システムの変更を追跡するには、この機能が適しています。これは、悪意のあるコードの活動を検出するのに有用なツールです。

起動後、新しいログが作成され、新しいウィンドウに表示されます。[ファイル] > [ログの保存] に移動して、ログをファイルに保存します。これで、ログファイルを後で開いて表示できるようになります。既存のログを開くには、[ファイル] -> [ログを開く] メニューを使用します。ESET SysInspectorのメインプログラムウィンドウで一度に表示できるログは1つです。

2つのログの比較には、現在アクティブなログと、ファイルに保存されているログを表示できるという利点があります。ログを比較するには、[ファイル] > [ログの比較] オプションを使用し、[ファイルの選択] を選択します。プログラムのメインウィンドウで、選択したログがアクティブなログと比較されます。比較ログには、2つのログの相違のみが表示されます。

NOTE

2つのログファイルを比較する場合は、[ファイル] ->[ログの保存] を選択し、ログをZIPファイルとして保存します。これで、両方のファイルが保存されます。後でそのファイルを開くと、保存されているログが自動的に比較されます。

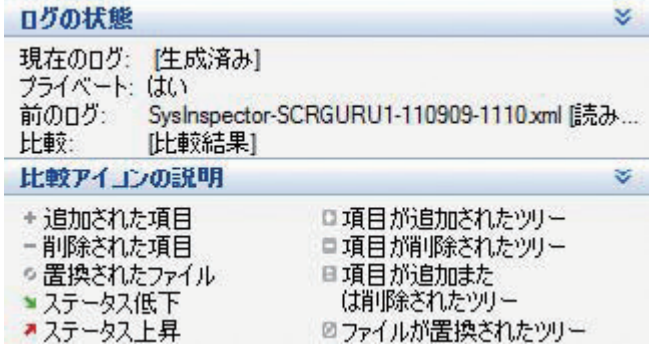
表示されたアイテムの横に、比較対象のログの相違を示す記号がESET SysInspectorによって表示されます。

のマークの付いた項目はアクティブログのみに見つかり、開かれた比較ログには見つからなかったものです。が付いているアイテムは、開かれているログにのみ存在し、アクティブなログには存在しないものです。

項目の横に表示される全ての記号について次に説明します。

- 以前のログには存在しない新しい値
- 新しい値を含むツリー構造セクション
- 以前のログにのみ存在する、削除された値
- 削除された値を含むツリー構造セクション
- 変更されている値/ファイル
- 変更された値/ファイルを含むツリー構造セクション
- リスクレベルが、以前のログよりも低下している
- リスクレベルが、以前のログよりも上昇している

左下隅に表示される説明セクションでは、全ての記号が説明され、比較対象のログの名前も表示されます。



比較ログはいずれもファイルに保存して、後で開くことができます。

例

システムに関する初期情報を記録したログを生成して、previous.xmlという名前のファイルに保存します。システムに変更を行った後、ESET SysInspectorを開いて、新しいログを生成します。current.xmlという名前のファイルにログを保存します。

これら2つのログの相違を追跡するには、[ファイル] > [ログの比較] に移動します。2つのログの相違を示した比較ログが作成されます。

次のコマンドラインオプションを使用した場合も同様の結果が得られます。

SysIsnpector.exe current.xml previous.xml

10.3 コマンドラインパラメータ

ESET SysInspectorでは、次のパラメータを使用してコマンドラインからレポートを生成できます。

/gen	GUIを実行せずにコマンドラインから直接ログを生成します。
/privacy	機密情報を除外してログを生成します。
/zip	生成されたログを圧縮ファイルとして直接ディスクに格納します。
/silent	ログ生成の進捗状況バーは表示されません。
/help, /?	コマンドラインパラメータに関する情報を表示します。

例

特定のログを直接読み込むには、次のように指定します。SysInspector.exe"c:¥clientlog.xml"

ログを現在の場所に生成するには、次のように指定します。SysInspector.exe /gen

ログを特定のフォルダに生成するには、次のように指定します。SysInspector.exe /gen="c:¥folder¥"

ログを特定のファイル/場所に生成するには、次のように指定します。SysInspector.exe /gen="c:¥folder¥mynewlog.xml"

ログを、機密情報を除外して直接圧縮ファイルとして生成するには、次のように指定します。SysInspector.exe /gen="c: ¥mynewlog.zip" /privacy /zip

2つのログを比較するには、次のように指定します。SysInspector.exe"current.xml""original.xml"

››› NOTE

ファイル/フォルダの名前に空白が含まれている場合は、名前を引用符(逆コンマ)で囲む必要があります。

10.4 サービススクリプト

サービススクリプトは、ESET SysInspectorを使用するユーザーがシステムから不要なオブジェクトを簡単に削除できるよう手助けをするツールです。

サービススクリプトを使用すると、ユーザーはESET SysInspectorログの全体、または選択した部分をエクスポートできます。エクスポートした後、不要なオブジェクトに削除対象のマークを付けることができます。その後、修正したログを実行して、マークを付けたオブジェクトを削除できます。

サービススクリプトは、過去にシステムの問題を診断した経験のある上級ユーザー向けです。そうではないユーザーが変更を行うと、オペレーティングシステムの障害を引き起こす可能性があります。

例

コンピュータが、ご使用のウイルス対策プログラムでは検出されないウイルスに感染している疑いがある場合は、次の手順を実行してください。

- ESET SysInspectorを実行して、システムスナップショットを新規に生成します。
- ツリー構造の左側のセクションで最初の項目を選択して、Ctrlキーを押しながら最後の項目を選択し、全ての項目をマークします。
- 選択したオブジェクトを右クリックし、[選択したセクションをサービススクリプトにエクスポート] コンテキストメニューオプションを選択します。
- 選択したオブジェクトが新しいログにエクスポートされます。
- 新しいログを開いて、削除対象のすべてのオブジェクトの-属性を+に変更します。オペレーティングシステムの重要なファイルやオブジェクトにマークが付いていないことを確認してください。
- ESET SysInspectorを起動し、[ファイル] > [サービススクリプトの実行] をクリックして、スクリプトへのパスを入力します。
- [OK] をクリックしてスクリプトを実行します。

10.4.1 サービススクリプトの生成

サービススクリプトを生成するには、ESET SysInspectorのメインウィンドウで、メニューツリー（左ペイン）の任意のアイテムを右クリックします。コンテキストメニューで、[すべてのセクションをサービススクリプトにエクスポート] オプションまたは [選択したセクションをサービススクリプトにエクスポート] オプションを選択します。

NOTE

2つのログを比較しているときは、サービススクリプトをエクスポートすることはできません。

10.4.2 サービススクリプトの構造

スクリプトのヘッダの最初の行には、エンジンバージョン(ev)、GUIバージョン(gv)、およびログバージョン(lv)に関する情報が記載されています。このデータを使用して、スクリプトを生成した.xmlファイル内の変更内容を追跡し、実行中に不整合が発生するのを防ぐことができます。スクリプトのこの部分は変更しないでください。

ファイルの残りの部分は、複数のセクションに分かれており、そこでアイテムを編集する(つまり、アイテムがスクリプトによって処理されることを示す)ことができます。アイテムの前にある"-"記号を"+"記号に置き換えることで、アイテムが処理対象としてマークされます。スクリプト内の各セクションは、空の行によって区切られています。各セクションには、番号とタイトルが付けられています。

01) Running processes(実行中のプロセス):
このセクションには、システム内で実行されているすべてのプロセスのリストが含まれます。各プロセスは、そのUNCパスと、それに続くアスタリスク(*)で囲まれたPIDとCRC16ハッシュコードによって識別されます。

例:

```
01) Running processes:
-¥SystemRoot¥System32¥smss.exe *4725*
-C:¥Windows¥system32¥svchost.exe *FD08*
+ C:¥Windows¥system32¥module32.exe *CF8A*
[...]
```

この例では、プロセスmodule32.exeが選択されています("+"記号でマークされています)。このプロセスは、スクリプトの実行時に終了します。

02) Loaded modules(読み込まれたモジュール):
このセクションには、現在使用されているシステムモジュールのリストが示されます。

例:

```
02) Loaded modules:
-c:¥windows¥system32¥svchost.exe
-c:¥windows¥system32¥kernel32.dll
+ c:¥windows¥system32¥khbekhb.dll
-c:¥windows¥system32¥advapi32.dll
[...]
```

この例では、モジュールkhbekhb.dllが"+"でマークされています。スクリプトが実行されると、この特定のモジュールを使用しているプロセスが認識され、それらが終了されます。

03) TCP connections(TCP接続):
このセクションには、既存のTCP接続に関する情報が含まれます。

例:

03) TCP connections:
-Active connection: 127.0.0.1:30606->127.0.0.1:55320, owner: ekrn.exe
-Active connection: 127.0.0.1:50007->127.0.0.1:50006,
-Active connection: 127.0.0.1:55320->127.0.0.1:30606, owner: OUTLOOK.EXE
-Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]

スクリプトを実行すると、マークされたTCP接続内のソケットの所有者が見つけられ、ソケットが停止されて、システムリソースが解放されます。

04) UDP endpoints (UDPエンドポイント):
このセクションには、既存のUDPエンドポイントに関する情報が含まれます。

例:

04) UDP endpoints:
-0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
-0.0.0.0, port 4500 (ipsec-msft)
-0.0.0.0, port 500 (isakmp)
[...]

スクリプトが実行されると、マークされたUDPエンドポイントのソケットの所有者が分離され、ソケットが停止されます。

05) DNS server entries (DNSサーバー関連のエントリ):
このセクションには、現在のDNSサーバーのコンフィグレーションに関する情報が含まれます。

例:

05) DNS server entries:
+ 204.74.105.85
-172.16.152.2
[...]

スクリプトが実行されると、マークされたDNSサーバーエントリが削除されます。

06) Important registry entries (重要なレジストリエントリ):
このセクションには、重要なレジストリエントリに関する情報が含まれます。

例:

06) Important registry entries:
* Category: Standard Autostart (3 items)
HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
-HotKeysCmds= C:¥Windows¥system32¥hkcmd.exe
-IgfxTray= C:¥Windows¥system32¥igfxtray.exe
HKCU¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
-Google Update="C:¥Users¥antoniak¥AppData¥Local¥Google¥Update¥GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
HKLM¥Software¥Microsoft¥Internet Explorer¥Main
+ Default_Page_URL= http://thatcrack.com/
[...]

スクリプトが実行されると、マークされたエントリが削除されるか、0Byte値に縮小されるか、またはその既定値にリセットされます。特定のエントリに適用されるアクションは、エントリのカテゴリと特定のレジストリのキー値によって異なります。

07) Services (サービス):
このセクションには、システム内の登録済みサービスのリストが示されます。

例:

07) Services:
-Name: Andrea ADI Filters Service, exe path: c:¥windows¥system32¥aeadisrv.exe, state: Running, startup: Automatic
-Name: Application Experience Service, exe path: c:¥windows¥system32¥aelupsvc.dll, state: Running, startup: Automatic
-Name: Application Layer Gateway Service, exe path: c:¥windows¥system32¥alg.exe, state: Stopped, startup: Manual
[...]

スクリプトが実行されると、マークされたサービスとそれらの依存サービスは停止され、アンインストールされます。

08) Drivers (ドライバ):
このセクションには、インストール済みのドライバのリストが示されます。

例:

08) Drivers:
-Name: Microsoft ACPI Driver, exe path: c:¥windows¥system32¥drivers¥acpi.sys, state: Running, startup: Boot
-Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:¥windows¥system32¥drivers¥adihdaud.sys, state: Running, startup: Manual
[...]

スクリプトを実行すると、選択したドライバは停止します。ドライバによっては、停止するようになっていないことがあります。

09) Critical files (不可欠なファイル) :
このセクションには、オペレーティングシステムが正常に機能するために不可欠なファイルに関する情報を記載しています。

例:

09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
-MAPI=1
[...]
* File: system.ini
- [386Enh]
-woafont=dosapp.fon
-EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
-127.0.0.1 localhost
-::1 localhost
[...]

選択したアイテムは、削除されるか、またはその元の値にリセットされます。

10.4.3　サービススクリプトの実行

目的のアイテムをすべてマークし、スクリプトを保存して閉じます。[ファイル] メニューの [サービススクリプトの実行] オプションを選択して、ESET SysInspectorのメインウィンドウから、編集したスクリプトを直接実行します。スクリプトを起動すると、次のような内容のメッセージが表示されます。「サービススクリプト"%Scriptname%"を実行しますか?」これを確認すると、実行しようとしているサービススクリプトが署名されていないという別の警告が表示される場合があります。[実行] をクリックしてスクリプトを起動します。

ダイアログウィンドウに、スクリプトが正常に実行されたことが示されます。

スクリプトの一部だけが処理された可能性がある場合、次のような内容のメッセージがダイアログウィンドウに表示されます。「サービススクリプトは部分的に実行されました。エラーレポートを表示しますか?」[はい] を選択して、実行されなかった操作が記載されている複雑なエラーレポートを表示します。

スクリプトが認識されなかった可能性がある場合、次のような内容のメッセージがダイアログウィンドウに表示されます。「選択したサービススクリプトは署名されていません。署名されていない不明なスクリプトを実行すると、コンピュータのデータに深刻なダメージを与えるおそれがあります。スクリプトを実行し、アクションを実行してもよろしいですか?」これは、スクリプト内の不整合（見出しが損傷している、セクションタイトルが壊れている、セクション間の空の列が失われているなど）によって引き起こされた可能性があります。スクリプトファイルを再度開いてスクリプト内のエラーを修正するか、または新しいサービススクリプトを作成します。

10.5 FAQ

01 ESET SysInspectorを実行するには管理者特権が必要ですか？

ESET SysInspectorを実行するには管理者特権は必要ありませんが、収集される情報の中には管理者アカウントからのみアクセスできるものもあります。標準ユーザーまたは制限付きユーザーが実行した場合は、動作環境に関する情報の収集量は少なくなります。

02 ESET SysInspectorではログファイルが作成されますか？

ESET SysInspectorでは、コンピュータの設定のログファイルを作成できます。このログファイルを保存するには、メインメニューの［ファイル］＞［ログを保存］を選択します。ログはXML形式で保存されます。既定では、ファイルは% USERPROFILE%¥My Documents¥ディレクトリーに保存されます。ファイルの命名規則は、SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XMLとなります。ログファイルを保存する前に、そのファイルの場所と名前を、必要に応じて別のものに変更できます。

03 ESET SysInspectorのログファイルを表示するにはどうしたらいいですか？

ESET SysInspectorで作成されたログファイルを表示するには、プログラムを実行し、メインメニューで［ファイル］＞［ログを開く］を選択します。ログファイルをESET SysInspectorアプリケーションにドラッグアンドドロップすることもできます。ESET SysInspectorのログファイルを頻繁に表示する必要がある場合は、デスクトップにSYSINSPECTOR.EXEファイルへのショートカットを作成することをお勧めします。こうしておくと、ログファイルをこのショートカットにドラッグアンドドロップして表示することができます。セキュリティ上の理由で、Windows VistaとWindows7では異なるセキュリティアクセス許可を持つウィンドウ間でのドラッグアンドドロップが許可されない場合があります。

04 ログファイル形式は使用できますか？ SDKは使用できますか？

現時点では、ログファイル形式やSDKは使用できません。プログラムのリリース後、お客様のフィードバックと要望に基づいて提供する可能性があります。

05 ESET SysInspectorでは、特定のオブジェクトによってもたらされるリスクはどのように評価されますか？

多くの場合、ESET SysInspectorは、各オブジェクトの特性を検証して悪意のある活動である可能性を重み付けする一連のヒューリスティックルールを使用して、オブジェクト（ファイル、プロセス、レジストリキーなど）にリスクレベルを割り当てます。これらのヒューリスティックに基づいて、オブジェクトに1-良好（緑）～9-危険（赤）のリスクレベルが割り当てられます。左側のナビゲーションペインでは、オブジェクトが持つ最大リスクレベルを基にセクションが色分けされます。

06 リスクレベル"6-不明（赤）"は、オブジェクトが危険であることを意味しますか？

ESET SysInspectorの評価により、オブジェクトが悪意のあるものであることが確定されるわけではありません。セキュリティの専門家による判断が必要です。ESET SysInspectorは、セキュリティの専門家が、システムのどのオブジェクトについて動作が異常でないかどうかを詳細に検証する必要があるかを、迅速に判断できるように設計されています。

07 ESET SysInspectorの実行時にインターネットに接続するのはなぜですか？

多くのアプリケーションと同様に、ESET SysInspectorには、このソフトウェアがESETから発行されたものであって、改変されていないことを確認できるよう、"証明書"のデジタル署名が付けられています。証明書を検証するために、オペレーティングシステムは証明機関にソフトウェア発行元を問い合わせて確認します。これは、Microsoft Windows環境で動作する全てのデジタル署名プログラムの標準的な動作です。

08 アンチステルス技術とはどのようなものですか？

アンチステルス技術は、ルートキットを効率的に検出するためのものです。

ルートキットとして動作する悪意のあるコードによってシステムが攻撃を受けると、ユーザーはデータの喪失や盗難などの被害を受けます。専用のルートキット対策ツールが無ければ、ルートキットの検出はほとんど不可能です。

09 "MSによって署名済み"としてマークされたファイルが、異なる"会社名"エントリを同時に持つことがあるのはなぜですか？

実行可能ファイルのデジタル署名を識別するときに、ESET SysInspectorは、まずファイルに埋め込まれたデジタル署名をチェックします。デジタル署名が見つかったら、その情報を使ってファイルが検証されます。デジタル署名が見つからない場合、ESIは、処理する実行可能ファイルに関する情報を収めた対応するCATファイル（セキュリティカタログ-% systemroot%¥system32¥catroot）の検索を開始します。該当するCATファイルが見つかると、そのCATファイルのデジタル署名が実行可能ファイルの検証プロセスに適用されます。

"Signed by MS"というマークのあるファイルが、異なる"CompanyName"エントリを持つ場合があるのはこのためです。

例:

Windows 2000では、C:¥Program Files¥Windows NTにハイパーターミナルアプリケーションがあります。このアプリケーションの主要な実行可能ファイルはデジタル署名されていませんが、ESET SysInspectorでは、そのファイルをMicrosoftによって署名されたファイルとマークします。この理由は、C:¥WINNT¥system32¥CatRoot¥{F750E6C3-38EE-11D1-85E5-00C04FC295EE}¥sp4.catにおける参照がC:¥Program Files¥Windows NT¥hypertrm.exe（ハイパーターミナルアプリケーションの主要な実行可能ファイル）をポイントし、sp4.catがMicrosoftによってデジタル署名されているためです。

[Chapter 11]
ESET SysRescue

11.1 概要

ESET SysRescueは、ESET Securityソリューションのうちの1つ（ESET Endpoint アンチウイルス、ESET Endpoint Security、またはサーバー向け製品のいずれか）を収めた起動可能ディスクを作成するためのユーティリティです。ESET SysRescueの主な利点は、ESET Securityソリューションがホストオペレーティングシステムから独立して稼動することで、ディスクおよびファイルシステム全体に直接アクセスできることにあります。これにより、オペレーティングシステムが実行中の場合など、通常は削除できないマルウェアを削除できます。

11.2 最低要件

ESET SysRescueは、Windows Vistaに基づくMicrosoft Windowsプレインストール環境（Windows PE）バージョン2.x内で動作します。

Windows PEは、無料パッケージであるWindows自動インストールキット（Windows AIK）の一部なので、ESET SysRescueを作成する前に、Windows AIKをインストールしておく必要があります（http://go.eset.eu/AIK）。64bitシステムでESET SysRescueを作成する場合は、32bitインストールパッケージのESET Securityソリューションを使用する必要があります。ESET SysRescueはWindows AIK 1.1以上をサポートします。

▸▸▸ NOTE

Windows AIKはサイズが1 GBを超えるので、スムーズにダウンロードするには高速インターネット接続が必要です。

ESET SysRescueは、ESET Securityソリューションのバージョン5.0以上で使用できます。

サポートされるオペレーティングシステム：

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- KB926044を適用したWindows Server 2003 Service Pack 1
- Windows Server 2003 Service Pack 2
- KB926044を適用したWindows XP Service Pack 2
- Windows Vista Service Pack 3

11.3 レスキュー CDの作成方法

ESET SysRescueウィザードを開始するには、[スタート] > [プログラム] > [ESET] > [ESET Remote Administrator] > [ESET SysRescue] をクリックします。

まず、Windows AIKとブートメディアの作成に適したデバイスがあるかどうかがチェックされます。コンピュータにWindows AIKがインストールされていない場合（または破損していたり正しくインストールされていない場合）、インストールするオプションまたはWindows AIKフォルダへのパスを入力するオプションがウィザードに表示されます（http://go.eset. eu/AIK）。

▸▸▸ NOTE

Windows AIKはサイズが1 GBを超えるので、スムーズにダウンロードするには高速インターネット接続が必要です。

次のステップでは、ESET SysRescueを保存する対象のメディアを選択します。

11.4 対象の選択

CD/DVD/USBに加えて、ISOファイルにESET SysRescueを保存することもできます。後で、ISOイメージをCD/DVDに書き込んで使用することができます。

対象メディアにUSBを選択した場合に、特定のコンピュータでブートが行われないことがあります。一部のBIOSバージョンでは、BIOSに関する問題が報告されることがあります。ブートマネージャの通信（Windows Vistaなど）と起動処理が終了し、次のエラーメッセージが表示されます。

ファイル: ¥ boot ¥ bcd
状態: 0xc000000e
情報: ブート設定データの読み込み時にエラーが発生しました

このメッセージが表示された場合、USBメディアでなくCDを選択することをお勧めします。

11.5 設定

ESET SysRescueの作成を開始する前に、インストールウィザードでは、コンパイルパラメータがESET SysRescueウィザードの最終ステップで表示されます。それらのパラメータを変更するには、[変更...] ボタンをクリックします。使用可能なオプションは次のとおりです。

●フォルダ
●ESETアンチウイルス
●詳細
●インターネットプロトコル
●起動可能なUSBデバイス（対象のUSBデバイスの選択時）
●書き込み（対象のCD/DVDドライブの選択時）

MSIインストールパッケージを指定していなかったり、コンピュータにESET Securityソリューションをインストールしていないと、[作成] ボタンは使用できません。インストールパッケージを選択するには、[変更] ボタンをクリックして、[ESETアンチウイルス] タブに移動します。ユーザー名とパスワードを入力しなかった場合も（[変更] > [ESETアンチウイルス]）、[作成] ボタンは無効になります。

11.5.1 フォルダ

一時フォルダは、ESET SysRescueのコンパイル時に必要なファイルの作業ディレクトリーです。

ISOフォルダは、コンパイルの完了後に、生成されたISOファイルが保存されるフォルダです。

このタブには、全てのローカルドライブとマッピングされているネットワークドライブ、および使用可能な空き領域がリストされます。表示されているフォルダの一部が、空き領域の不十分なドライブにある場合、十分な空き領域のある別のドライブを選択することをお勧めします。ディスクの空き領域が不足していると、コンパイルが途中で終了する場合があります。

外部アプリケーション-ESET SysRescueメディアから起動後に実行またはインストールする追加プログラムを指定できます。

外部アプリケーションを含める-外部プログラムをESET SysRescueのコンパイルに追加できます。

選択されたフォルダ-ESET SysRescueディスクに追加するプログラムを格納するフォルダです。

11.5.2 ESETアンチウイルス

ESET SysRescue CDを作成する際、コンパイラが使用するESETファイルのソースとして、2種類を選択できます。

ESS/EAVフォルダ-コンピュータ上のESET Securityソリューションのインストール先フォルダに含まれる既存ファイル。

[MSIファイル]-MSIインストーラに含まれているファイルが使用されます。

次に、選択によっては、(nup)ファイルの場所を更新できます。通常、既定オプション[ESS/EAVフォルダ/MSIファイル]が設定されているはずです。ウイルス定義データベースの古いバージョンまたは新しいバージョンを使用するためといった場合によっては、カスタムの[アップデートフォルダ]を選択してもかまいません。

ユーザー名とパスワードのソースとして、次の2つのうちのどちらかを使用できます。

ユーザー名とパスワードは、現在インストールされている設定が反映されます。

ユーザー指定-対応するテキストボックスに入力されたユーザー名とパスワードが使用されます。

NOTE

ESET SysRescue CD上のESET Securityソリューションは、インターネット経由、またはESET SysRescue CDが実行されているコンピュータにインストールされているESET Securityソリューションからアップデートされます。

11.5.3 詳細設定

[詳細] タブでは、コンピュータのメモリ容量に従ってESET SysRescue CDを最適化できます。[576 MB以上] を選択すると、CDのコンテンツがシステムメモリ (RAM) に書き込まれます。[576 MB未満] を選択すると、WinPEが実行されるときに常にRecovery CDにアクセスされます。

[外部ドライバ] セクションでは、特定のハードウェア用のドライバ (通常はネットワークアダプタ) を挿入できます。WinPEは、幅広いハードウェアをサポートするWindows Vista SP1をベースにしていますが、時にはハードウェアが認識されないこともあります。そのようなときは、ドライバを手動で追加する必要があります。ESET SysRescueのコンパイルにドライバを追加するには、手動 ([追加] ボタン) と自動 ([自動検索] ボタン) の2つの方法があります。手動で追加する場合は、該当する.infファイルへのパスを選択する必要があります (適用可能な*.sysファイルがそのフォルダ内になければなりません)。自動的に追加する場合は、指定のコンピュータのオペレーティングシステムでドライバが自動的に検索されます。自動追加は、ESET SysRescue CDの作成先コンピュータで使用しているのと同じネットワークアダプタを備えたコンピュータで、ESET SysRescueを使用する場合にのみ使うことをお勧めします。作成時にESET SysRescueドライバがコンパイルに組み込まれるため、ユーザーが後で検索する必要はありません。

11.5.4 インターネットプロトコル

ここでは、ESET SysRescueの後で、基本ネットワーク情報を設定し、事前定義接続を設定することができます。

IPアドレスをDHCP (動的ホスト構成プロトコル) サーバーから自動的に取得するには、[自動的にIPアドレスを取得する] を選択します。

あるいは、ネットワーク接続で、手動で指定したIPアドレス (静的IPアドレスとも呼ばれる) を使用することもできます。適切なIP設定を構成するには、[カスタム] を選択します。このオプションを選択する場合、[IPアドレス] を指定し、LANおよび高速インターネット接続の場合は [サブネットマスク] を指定する必要があります。[優先DNSサーバー] および [代替DNSサーバー] に、プライマリおよびセカンダリのDNSサーバーアドレスを入力します。

11.5.5 起動可能なUSBデバイス

対象のメディアとしてUSBデバイスを選択した場合、[起動可能なUSBデバイス] タブで、使用可能なUSBデバイスのいずれかを選択できます (複数のUSBデバイスがある場合)。

ESET SysRescueのインストール先として適切な対象 [デバイス] を選択します。

CAUTION

選択したUSBデバイスは、ESET SysRescueの作成時にフォーマットされます。デバイス上の全てのデータが削除されます。

[クイックフォーマット] オプションを選択した場合、フォーマットによりすべてのファイルが領域から除去されますが、ディスクの不良セクタは検査されません。USBデバイスが事前にフォーマット済みであって損傷を受けていないことが確実であれば、このオプションを使用します。

11.5.6 書き込み

書き込み先メディアとしてCDまたはDVDを選択した場合、[書き込み] タブで書き込みパラメータを追加指定できます。

[ISOファイルを削除する] -ESET SysRescue CDの作成後に一時ISOファイルを削除する場合、このチェックボックスをオンにします。

[削除有効] -高速消去と完全消去を選択できます。

[書き込みデバイス] -書き込みに使用するデバイスを選択します。

CAUTION

これは既定のオプションです。再書き込み可能なCD/DVDを使用した場合、CD/DVD上のすべてのデータが消去されます。

[メディア] セクションには、CD/DVDデバイス内のメディアに関する情報が表示されます。

[書き込み速度] -ドロップダウンメニューから速度を選択します。書き込み速度を選択する際には、書き込みデバイスの処理能力と使用するCD/DVDの種類を考慮に入れる必要があります。

11.6 ESET SysRescueの操作

レスキュー CD/DVD/USBが効果的に機能するためには、ESET SysRescueブートメディアからコンピュータを起動する必要があります。ブートの優先度はBIOSで変更できます。また、コンピュータの起動時にブートメニューを使用することもできます。通常は、マザーボード/BIOSのバージョンによって、F9～F12のいずれかのキーを使用します。

ブートメディアからのブート後にESET Securityソリューションが起動します。ESET SysRescueが使用されるのは特定の状況に限られているので、標準バージョンのESET Securityソリューションにある保護モジュールやプログラム機能の中には不要なものもあります。ESET SysRescueの機能は、[コンピュータの検査]、[アップデート]および[設定]の一部のセクションのみに絞り込まれます。ウイルス定義データベースをアップデートする機能は、ESET SysRescueの最も重要な機能です。コンピュータ検査を開始する前にこのプログラムをアップデートすることをお勧めします。

11.6.1 ESET SysRescueの使用

Windowsの通常起動またはセーフモード起動時に、ウイルスが自動的に起動する場合、またはOSによって起動されている場合にウイルスファイルを削除できない（ロックがかかっている）ことがあります。ESET SysRescueは単独でPCを起動することが可能なため、そのようなウイルスを駆除することが可能です。

別表-サードパーティーライセンス

ESETは、以下のサードパーティライセンスに従うサードパーティコードがソフトウェアに含まれることを了承します。

3-clause BSD License ("New BSD License")

Copyright (c) ＜YEAR＞,＜OWNER＞
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the＜ORGANIZATION＞nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2004-2007 Sara Golemon＜sarag@libssh2.org＞
Copyright (c) 2005,2006 Mikhail Gusarov＜dottedmag@dottedmag.net＞
Copyright (c) 2006-2007 The Written Word, Inc.
Copyright (c) 2007 Eli Fant＜elifantu@mail.ru＞
Copyright (c) 2009 Daniel Stenberg
Copyright (C) 2008, 2009 Simon Josefsson
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE."