ESET Remote Administrator
ユーザーズマニュアル

■お断り

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

○ 本マニュアルの著作権は、キヤノンＩＴソリューションズ株式会社に帰属します。本マニュアルの一部または全部を無断で複写、複製、改変することはその形態を問わず、禁じます。

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

○ Microsoft、Windows、Windows Server、Internet Explorer、Active Directory、.NET Framework、SQL Serverは、米国Microsoft Corporationの米国、日本およびその他の国における登録商標または商標です。

○ Mac、Mac OS、OS X、Finderは、米国およびその他の国で登録されているApple Inc.の商標です。

○ Android Robotのイラストは、Googleが作成、提供しているコンテンツをベースに変更したもので、クリエイティブ・コモンズの表示 3.0 ライセンスに記載の条件に従って使用しています。

改定日　2017/4/30

目　次

Chapter 1 ESET Remote Administrator について	1.1 はじめに ..... 5 1.2 プログラムのアーキテクチャー ..... 6 1.3 展開シナリオ ..... 8 1.4 サポート対象製品 10
Chapter 2 システム要件	2.1 サポート対象のオペレーティングシステム ..... 11 2.2 ハードウェア ..... 11 2.3 データベース ..... 12 2.4 使用されるポート ..... 13 2.5 ERA Web コンソール対応　Web ブラウザー 15
Chapter 3 インストール	3.1 インストール概要 ..... 16 3.2 Windows 版オールインワンインストール ..... 19 3.3 Windows 版コンポーネントインストール ..... 59 3.4 Linux 版　コンポーネントインストール ..... 101 3.5 ESET Remote Administrator のアップグレード 146
Chapter 4 最初の手順	4.1 ERA Web コンソールを開く ..... 154 4.2 展開 ..... 161 4.3 モバイルデバイスの展開 266
Chapter 5 ERA Web コンソールの使用方法	5.1 ERA Web コンソールの画面構成 ..... 273 5.2 ダッシュボード ..... 276 5.3 コンピューター ..... 281 5.4 脅威 ..... 319 5.5 レポート ..... 320 5.6 モバイルデバイス管理 326
Chapter 6 ESET Remote Administrator の管理	6.1 ERA サーバインストール後のステータス概要の確認 ..... 329 6.2 動的グループテンプレート ..... 334 6.3 グループ ..... 342 6.4 ユーザー管理 ..... 373 6.5 ポリシー ..... 380 6.6 クライアントタスク ..... 422 6.7 サーバータスク ..... 449 6.8 通知 ..... 488 6.9 証明書 ..... 497 6.10 アクセス権 ..... 520 6.11 サーバーの設定 ..... 543 6.12 ライセンス管理 548
Chapter 7 ESET Remote Administrator のコンポーネント設定	7.1 各コンポーネントの設定 551

Chapter 8
その他

8.1 診断ツール 562
8.2 ミラーツール 565
8.3 FAQ 570

Chapter 1 ESET Remote Administrator について

1.1 はじめに

「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システムです。

ESET Remote Administrator 自体は、セキュリティ対策機能を提供していません。セキュリティ対策には、Microsoft Windows Server 用の ESET File Security などの ESET 製品をインストールしておくことを推奨します。

1.2 プログラムのアーキテクチャー

ESET Remote Administrator は前のバージョンの ESET Remote Administrator からアーキテクチャーが大きく異なります。そのため、古いバージョンの ESET Remote Administrator との互換性はありません。ただし、前のバージョンの ESET 製品とは互換性があります。

ESET Remote Administrator をご利用いただくには次のコンポーネントをインストールする必要があります。

- ESET Remote Administrator Server（以下、ERA サーバー）
- ESET Remote Administrator Web Console（以下、ERA Web コンソール）
- ESET Remote Administrator Agent（以下、ERA エージェント）

次のサポートコンポーネントは必要に応じてインストールしてください。

- ESET Remote Administrator Proxy（以下、ERA プロキシ）
- Rogue Detection Sensor（以下、RD Sensor）
- Mobile Device Connector

1.2.1 ERA サーバー

ERA サーバーは、ERA エージェント経由でサーバーに接続しているクライアントからの情報収集とクライアントへの様々なリクエストの送信が行えます。

リクエストには、オンデマンド検査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 Web コンソールの画面で作成の操作を行います。ERA サーバーは ERA Web コンソールとクライアントコンピューターの接続ポイントで、すべての情報が ERA サーバーで処理、保守、または変更されクライアントと ERA Web コンソールに転送されます。

データを正しく処理するには、ERA サーバーがデータベースサーバーに安定して接続されている必要があります。パフォーマンスの強化を行いたい場合は、別のコンピューターにデータベースサーバーをインストールすることを推奨します。

1.2.2 ERA Web コンソール

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

1.2.3 ERA エージェント

ERA エージェントは ERA サーバーとクライアント間の通信を行うサービスです。ESET 製品は ERA サーバーと直接通信をせずに、ERA エージェント経由で通信を行います。

ERA エージェントがインストールされ、ERA サーバーと通信ができるクライアントコンピューターは管理されている状態として表示されます。ESET 製品のインストールの有無に関わらず、ERA エージェントをコンピューターにインストールすることができます。

ERA エージェントは、社内の Active Directory の GPO を利用して展開することができます。また、ERA サーバーに接続していない場合でも、ERA エージェントはクライアントコンピューターとのイベントに対応することができます。

1.2.4 ERA プロキシ

ERA プロキシは ERA サーバーの軽量バージョンで、クライアントにインストールされている ERA エージェントと接続して、ERA サーバーへデータを送信することができます。ERA プロキシを拠点ごとに設置することで、複数の ERA エージェントから ERA サーバーへのトラフィックを分散させることができます。また、ERA サーバーを経由することなく、ERA エージェントへ設定データ（グループ、ポリシー、タスクなど）の配布を行えます。

多くのクライアントを持つ、中規模または大規模ネットワークの場合（例えば、10,000 台以上のクライアント）、複数の ERA プロキシで負荷を分散し、メインの ERA サーバーの負荷を軽減します。また、ブランチオフィスの各クライアントにインストールされている ERA エージェントが、メインの ERA サーバーに直接接続せずに、ブランチオフィスの同じローカルネットワーク上の ERA プロキシ経由に接続することができます。これにより、ブランチオフィス内の通信が向上します。

ERA プロキシは、すべてのローカル ERA エージェントからの接続を受け入れ、データをコンパイルし、メインの ERA サーバー（または別の ERA プロキシ）にアップロードします。これにより、ネットワークおよびデータベースクエリのパフォーマンスを劣化させずに、対応できるクライアント数を増やすことができます。

ERA プロキシが正しく機能するには、ERA プロキシがインストールされているホストコンピューターに、ERA エージェントがインストールされ、ネットワークの上位レベル（ERA サーバーまたは上位 ERA プロキシ）に接続されている必要があります。
詳細は、「1.3.2 中規模ネットワーク（ERA プロキシを利用）」を参照してください。

! 重 要

ERA プロキシと ERA サーバーを接続するためには、ERA プロキシ側に ERA エージェントをインストールする必要があります。

1.2.5 RD Sensor

RD Sensor は、ネットワーク内の未登録のコンピューターを検索するツールです。自動で検索を行い、検出されたコンピューターは定義済みレポートで報告され、ERA サーバーのコンピューターリストに自動的に追加されます。
RD Sensor はネットワーク上のコンピューターを検出し、その情報を ERA サーバーに送信します。ERA サーバーは、ネットワーク上で検出されたコンピューターが ERA で既に管理されているかどうかを判断します。既に検出されたコンピューターを記憶し、同じ情報を 2 回送信しません。
サーバー同期タスクによって、ネットワーク構造（ドメイン、LDAP、Windows ネットワーク）内のすべてのコンピューターが ERA サーバーのコンピューターリストに自動的に追加されます。
RD sensor はネットワーク構造内に無いコンピューターを検出し、ESET Remote Administrator サーバーに追加する場合に便利です。

1.2.6 Mobile Device Connector

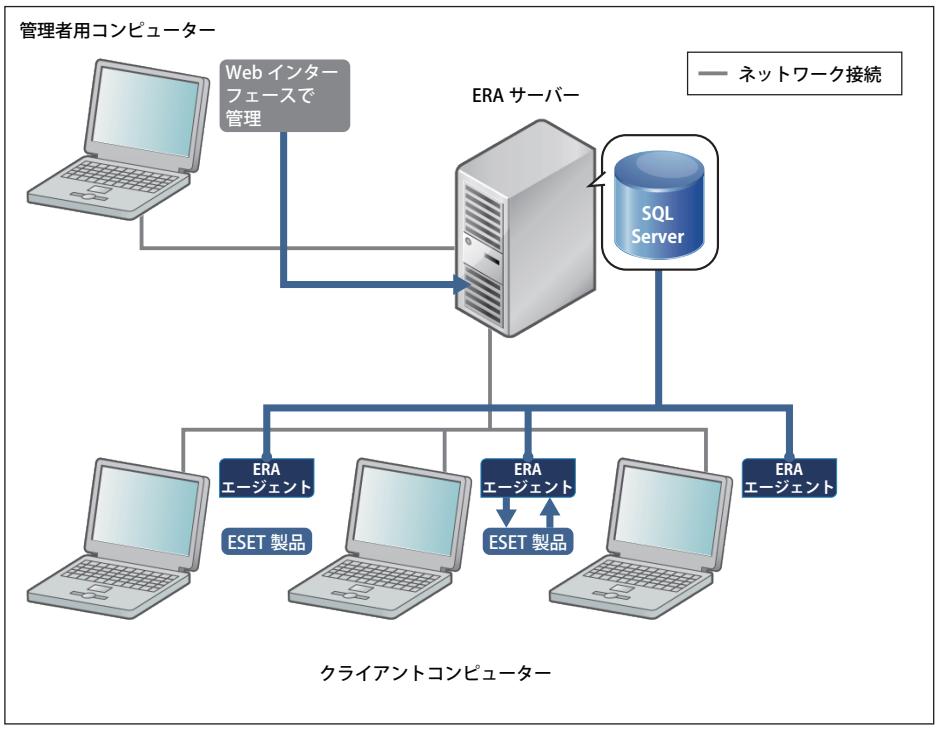
Mobile Device Connector は、モバイルデバイスを管理し、Android 用のクライアント用プログラム「ESET Endpoint Security for Android」を管理するアプリケーションです。ERA サーバーでモバイルデバイスの管理を行う場合、Mobile Device Connector をインストールしたサーバーを用意する必要があります。Mobile Device Connector は、ERA サーバーが実行されているサーバーにインストールできるほか、ERA サーバーが実行されていないサーバーにインストールすることもできます。Mobile Device Connector のインストのインストール方法については、「3 インストール」をご参照ください。

1.3 展開シナリオ

様々なネットワーク環境の展開シナリオについて紹介します。各コンポーネントのインストール手順については、該当する Chapter を参照してください。

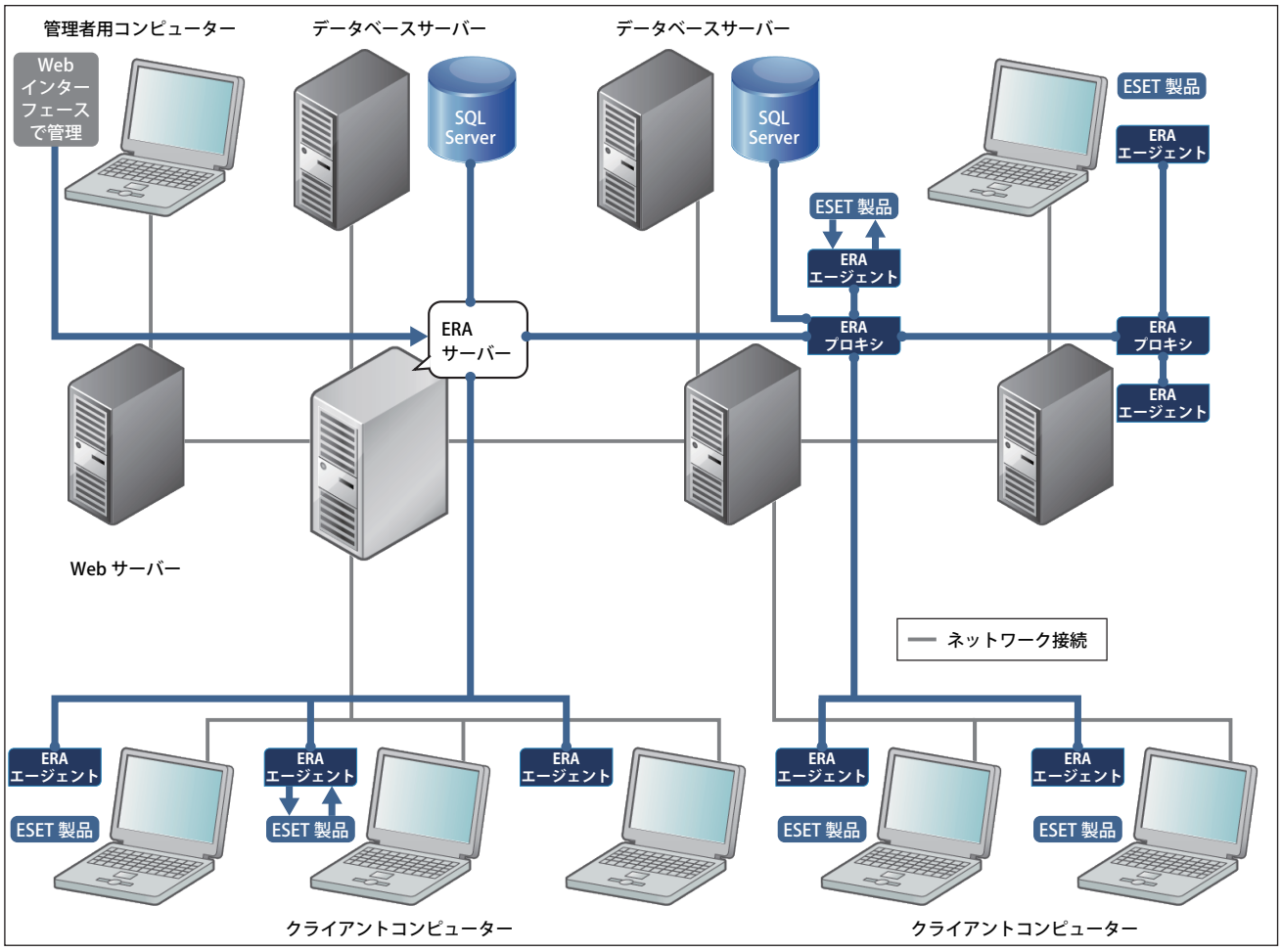
1.3.1 小規模ネットワーク（1 台のサーバー）

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



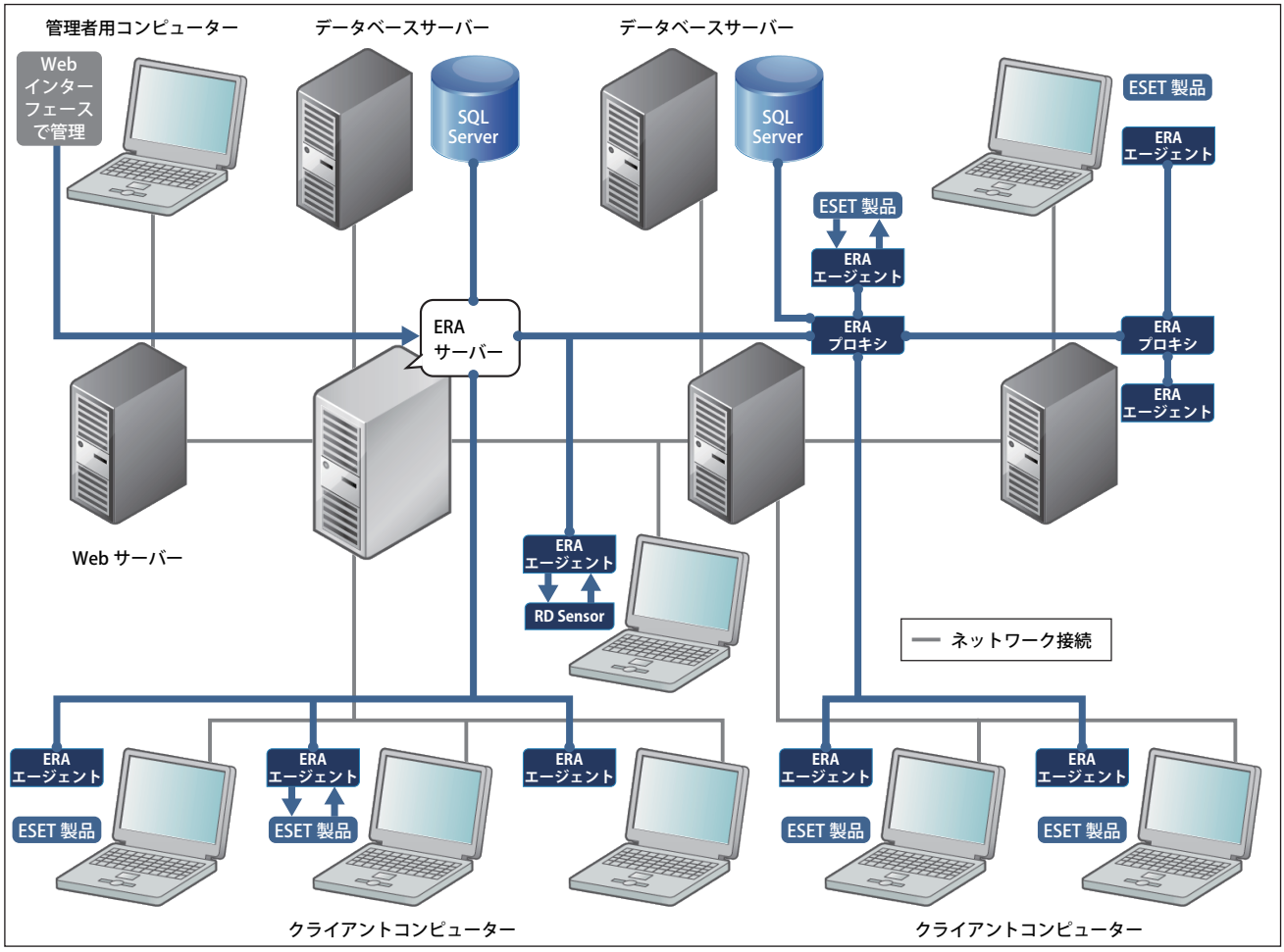
1.3.2 中規模ネットワーク（ERA プロキシを利用）

複数の拠点がある中規模のネットワーク環境（10,000 クライアント程度）では、ERA プロキシを利用することをお勧めします。リモート拠点のローカルネットワーク上の ERA エージェントのデータを ERA プロキシで集約し、本社の ERA サーバーへ接続します。ERA プロキシを使用するには、ERA プロキシがインストールされているホストコンピューターに ERA エージェントがインストールされ、ネットワークの上位レベルの ERA サーバーへの接続が必要です。



1.3.3 大規模ネットワーク

大規模のネットワーク環境（10,000 クライアント以上）では、RD Sensor と ERA プロキシを利用することをお勧めします。RD Sensor は、ネットワーク内のコンピューターを検出することができます。ERA プロキシでは、ERA エージェントを ERA プロキシに接続させることにより、パフォーマンス上重要な、ERA サーバーの負荷を分散させます。ERA プロキシを利用しても、ERA エージェントを直接 ERA サーバーに接続することも可能です。



1.4 サポート対象製品

ESET Remote Administrator V6 で管理可能な ESET 製品については、弊社ホームページを参照してください。
http://eset-support.canon-its.jp/faq/show/143?site_domain=business

Chapter 2 システム要件

ESET Remote Administrator をインストールするためのシステム要件を記載しています。最新のシステム要件に関しては、以下、弊社ホームページを参照してください。
https://eset-info.canon-its.jp/business/endpoint_protection_adv/spec.html#anc08

2.1 サポート対象のオペレーティングシステム

ESET Remote Administrator の、各コンポーネントは Windows、Linux でサポートされています。
最新のサポート対象のオペレーティングシステムについては、以下、弊社ホームページを参照してください。

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

2.2 ハードウェア

ESET Remote Administrator のハードウェア要件については、以下、弊社ホームページを参照してください。

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

2.3 データベース

ESET Remote Administrator のサポート対象データベースサーバーについては、以下、弊社ホームページを参照してください。

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

ERA サーバーまたは ERA プロキシをインストールするときに使用するデータベースサーバーを指定できます。
オールインワンインストーラーを用いてインストールを行った場合、インストールする OS により Microsoft SQL Server 2008 R2 Express または Microsoft SQL Server 2014 R2 Express がインストールされます。（インストールパッケージに含まれています。）Microsoft SQL Server Express Edition にはデータベースサイズの上限（10 GB）があります。また、ドメインコントローラーへのインストールはできません。
現在の環境で稼動している既存の Microsoft SQL Server を使用できますが、最低要件を満たしている必要があります。

! 重 要

ERA サーバーおよび ERA プロキシは統合バックアップを使用しないため、データベースサーバーをバックアップし、データ損失を防止することを推奨します。

2.3.1 データベースサーバーハードウェア

データベースサーバーハードウェア要件については、以下、弊社ホームページを参照してください。

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

2.4 使用されるポート

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

2.4.1 ERA サーバー

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

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

2.4.2 ERA Web コンソール

プロトコル	ERA Web コンソールがリスンするポート	説明
TCP	443	SSL を利用した ERA Web コンソールへのログイン

2.4.3 ERA プロキシ

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

2.4.4 HTTP プロキシ

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

2.4.5 ERA エージェント

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

2.4.6 ERA エージェント（リモート展開用）

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

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

! 重　要

上記のポートが他のアプリケーションによって使用されていないことを確認してください。

! 重　要

ネットワーク内のファイアウォールで、上記のポート経由の通信が許可されていることを確認してください。

2.4.7 Mobile Device Connector

モバイルデバイスを ERA サーバーで管理するときに使用します。

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

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

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

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

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

2.5 ERA Web コンソール対応 Web ブラウザー

ERA Web コンソールの対応ブラウザーについては、以下、弊社ホームページを参照してください。

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

Chapter 3 インストール

この章では、ESET Remote Administrator が対応している 2 種類のプラットフォーム（Windows/Linux）に対するインストールと、その操作について説明します。

インストール概要	P16 参照
Windows 版オールインワンインストール	P19 参照
Windows 版コンポーネントインストール	P59 参照
Linux 版コンポーネントインストール	P101 参照

3.1 インストール概要

ESET Remote Administrator のインストーラーは、多様なシステム環境へのサポートを想定し、以下の形式に分かれています。
インストーラーファイルは、ユーザーズサイトに公開されています。
システム環境とインストール方法に合わせ、ダウンロードを行ってください。

- ESET Remote Administrator6 オールインワンインストーラー（Windows 版）
- ESET Remote Administrator6 各コンポーネントのインストーラー（Windows 版・Linux 版）

3.1.1　インストール方法

インストール方法は、使用するシステム環境に合わせて 2 種類に分かれています。

■オールインワンインストール（Windows 版のみ対応）

ESET Remote Administrator6 オールインワンインストーラーを使用し、1 台のサーバーコンピューターに対して ESET Remote Administrator を一括でインストールします。
また、インストール中に Microsoft SQL ServerExpress のインストールと設定を自動で行います。
Windows 版のみ対応しています。

ワンポイント
Microsoft SQL ServerExpress の最大データベースサイズは、10 GB です。

ワンポイント
フェールオーバー環境へインストールする場合は、コンポーネントインストールを行ってください。フェールオーバー環境へのインストールについては、「3.3.9　フェールオーバー環境へのインストール」を参照してください。

■コンポーネントインストール（Windows 版 /Linux 版）

各コンポーネントのインストーラーを使用し、必要なプログラムを個別に手動でインストールします。システム環境に合わせて、コンポーネントをカスタマイズしながらインストールすることができます。
別途、SQL Server のインストールと設定を行う必要があります。
Windows と Linux、それぞれのプラットフォームでのインストール操作が可能です。

ESET Remote Administrator は、次のコンポーネントで構成されています。

■基本コンポーネント（実行に必要となる必須プログラム）

- ERA サーバー　　：サーバーコンピューター上での実行プログラム
- ERA Web コンソール：ESET Remote Administrator のインターフェース
- ERA エージェント　：クライアントコンピューター上での実行プログラム

ERA エージェントは、ERA サーバーが実行されているコンピューター上へのインストールは任意となっています。

■オプションコンポーネント

- ERA プロキシ
- RD Sensor
- Apache HTTP プロキシ
- Mobile Device Connector

各コンポーネントは、32bit 版と 64bit 版が用意されています。

!重 要

Apache HTTP プロキシを選択してインストールすると、インストールされた Apache HTTP プロキシを ESET 製品がプロキシサーバーとして利用するポリシーが作成され、既定で ESET Remote Administrator で管理されるすべてのコンピューターに割り当てられるためご注意ください。

!重 要

本マニュアルでは、64bit 版のインストーラーフォルダーである x64 フォルダーを、Windows は C: ¥、Linux は /root に保存しています。
各コンポーネントのインストーラーは、次の場所に保存されている状態で、操作を解説します。
Windows：C:¥x64¥installers
Linux：/root/x64

!重 要

オールインワンインストーラーを保存するフォルダーのパスに日本語が含まれている場合、インストールを実行することができません。パスに日本語が含まれていないフォルダーにオールインワンインストーラーを保存し、インストールを行ってください。

3.2 Windows 版オールインワンインストール

ここでは ESET Remote Administrator6 オールインワンインストーラー（以下、オールインワンインストーラー）を使用したインストールの操作を解説します。
オールインワンインストーラーでは、ウィザードを起動して基本コンポーネントとオプションコンポーネントをインストールすることができます。また、システム上にデータベースサーバーがインストールされていない場合、Microsoft SQL Server Express のインストールと接続構成を自動で設定します。
選択できる一括インストールの対象は、次の 3 つです。

- ERA サーバー
- ERA プロキシ
- Mobile Device Connector

オールインワンインストーラーは、解凍したフォルダー内の「Setup.exe」です。

! 重　要

オールインワンインストーラーは、Windows 版のみです。

3.2.1 ERA サーバー 一括インストール

ERA サーバーの稼動に必要なコンポーネントを一括でインストールします。
インストール中に、各コンポーネントが ERA サーバーに接続するための各種証明書の生成と認証を自動で行います。

次の選択したコンポーネントがインストールされます。

- Microsoft SQL Server Express
- ERA サーバー
- ERA エージェント
- Apache Tomcat
- ERA Web コンソール
- RD Sensor
- Apache HTTP プロキシ
- Mobile Device Connector

! 重　要

Apache HTTP プロキシをインストールすると、ESET 製品が Apache HTTP プロキシをプロキシサーバーとして利用するポリシーが作成されます。
このポリシーは、既定で ESET Remote Administrator で管理されるすべてのコンピューターに割り当てられます。
社内で構築したミラーサーバーからウイルス定義データベースをアップデートする場合や、社内のプロキシサーバーを利用してインターネットに接続する場合は、Apache HTTP プロキシのインストールは不要です。

ERA サーバーの一括インストールには、次の条件が必要です。

- ERA サーバーが使用するネットワーク通信ポートが空いていること
- JAVA SE の最新版への更新
- Microsoft .NET Framework 3.5 のインストール

操作手順

1. Setup.exe をダブルクリックします。

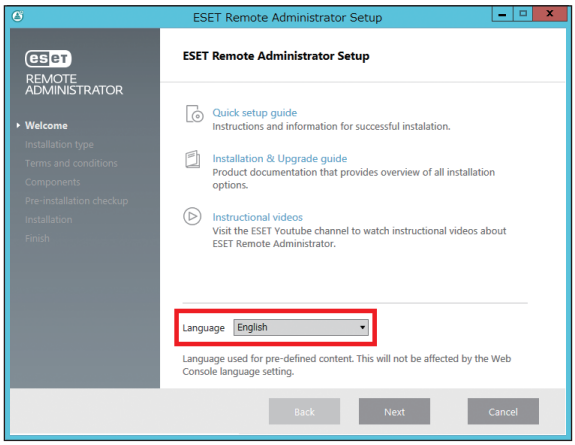
32bit 版、64bit 版とも、同じアイコンです。

! 重　要

オールインワンインストーラーを保存するフォルダーのパスに日本語が含まれている場合、インストールを実行することができません。パスに日本語が含まれていないフォルダーにオールインワンインストーラーを保存し、インストールを行ってください。

続く

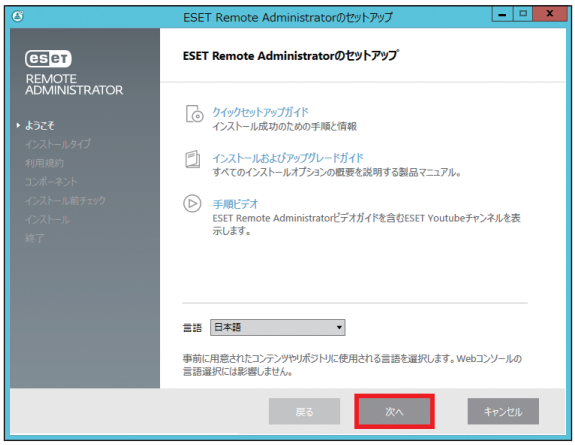
2 「Language」から［日本語］を選択します。



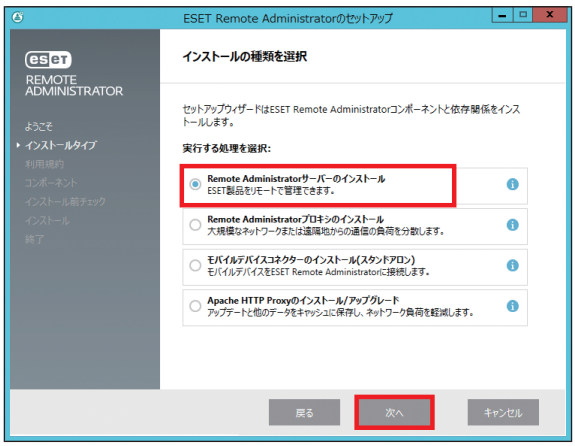
! 重 要

必ず日本語を選択してください。
日本語を選択しない場合は、リポジトリの設定が海外の値になり、サポート対象外となります。

3 インストーラーの表示が日本語に切り替わります。［次へ］ボタンをクリックします。

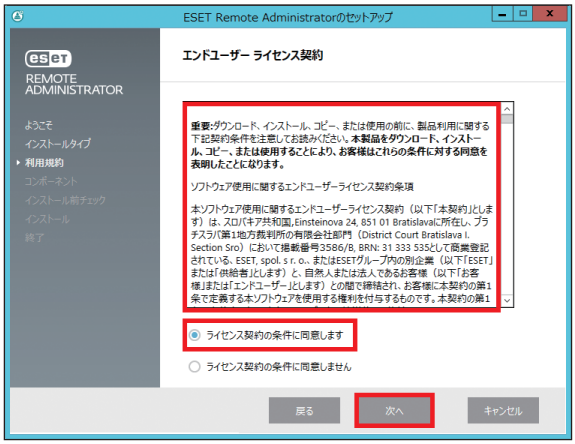


4 「実行する処理を選択 :」の［Remote Administrator サーバーのインストール］を選択し、［次へ］ボタンをクリックします。

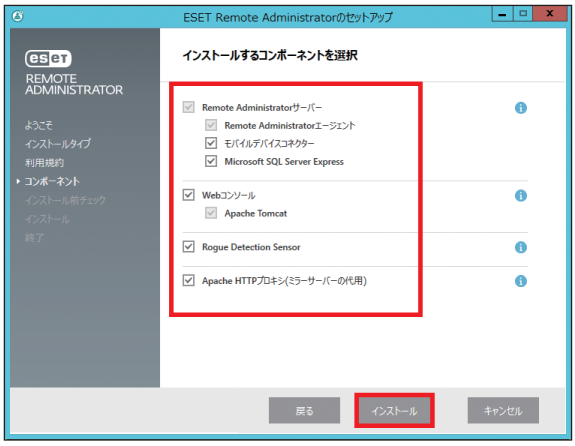


続く

5 「エンドユーザー ライセンス契約」を一読して同意する場合、［ライセンス契約の条件に同意します］を選択し、［次へ］ボタンをクリックします。



6 インストールするコンポーネントを選択し、［インストール］ボタンをクリックします。



ワンポイント

同一サーバー上に Mobile Device Connector もインストールする場合は、モバイルデバイスコネクターにチェックを入れてインストールを行ってください。

システム要件の確認が行われます。
システム要件を満たしている場合、Microsoft SQL Server Express のインストールが開始されます。

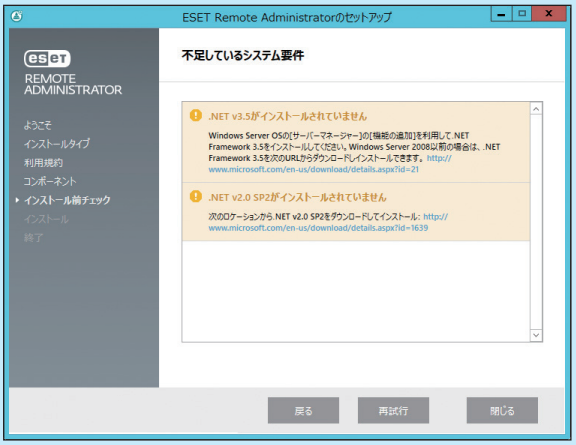
続く

表示されている順番に、コンポーネントのインストールが行われます。
「Microsoft SQL Server Express」のインストールが終了した後、「ESET Remote Administrator Server セットアップ」が開始されます。

ワンポイント

システム要件を満たしていなかった場合

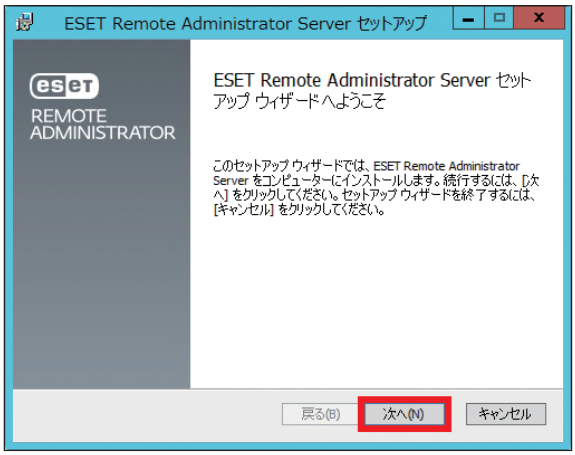
「不足しているシステム要件」画面が表示され、不足しているシステムが表示されます。
メッセージに従い、不足しているシステムのインストールを行ってください。
※ Windows Server 2008 R2 以降のサーバーに「Microsoft .NET Framework 3.5」をインストールする場合は、サーバーマネージャーの機能の追加より実施してください。



!重 要

「Microsoft SQL Server Express」を選択した場合、インストール先としてドメインコントローラーを選択することはできません。

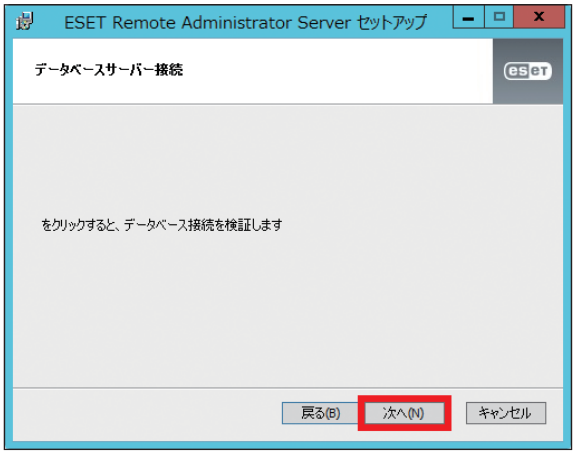
7 「ESET Remote Administrator Server セットアップ ウィザードへようこそ」の［次へ］ボタンをクリックします。



続く

8 ［次へ］ボタンをクリックします。

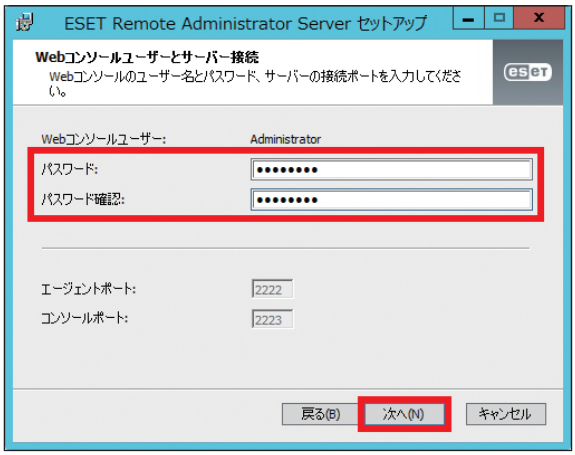
先にインストールされた、Microsoft SQL Server Express との接続確認が行われます。



接続が確認されると「Web コンソールユーザーとサーバー接続」へ自動で切り替わります。

9 「パスワード :」と「パスワード確認 :」に任意のパスワードを設定し、［次へ］ボタンをクリックします。

ERA Web コンソールへログインするための、Administrator の初期パスワードを設定します。



続く

⑩ 項目を入力し、［次へ］ボタンをクリックします。

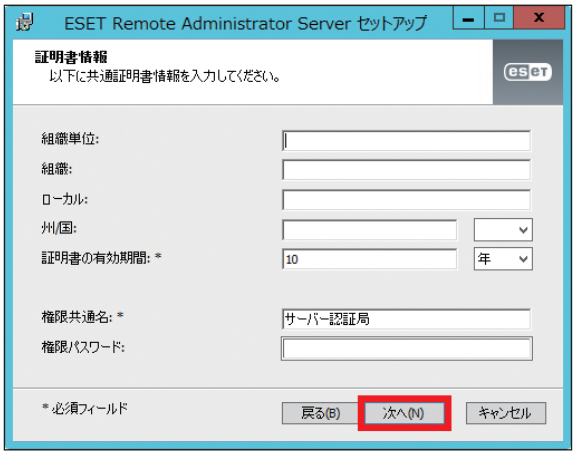
「証明書情報」では、インストール中に自動生成される、サーバー / クライアント通信の証明書へ登録する情報を入力します。入力した内容は、ERA Web コンソールの認証局に反映されます。

組織単位	部署名
組織	会社名
ローカル	都道府県名
州 / 国	組織の国籍
証明書の有効期間	初期設定で 10 年が設定されます。
権限共通名	認証局の名前
権限パスワード	認証局パスワード

※権限パスワードを設定した場合は、証明書使用時に必要となりますので、必ず覚えておいてください。

! 重　要

証明書の有効期間は初期設定のまま変更しないでください。証明書の有効期間が 2038 年以上に設定されている場合は、Mac OS X が証明書エラーになり、管理できません。

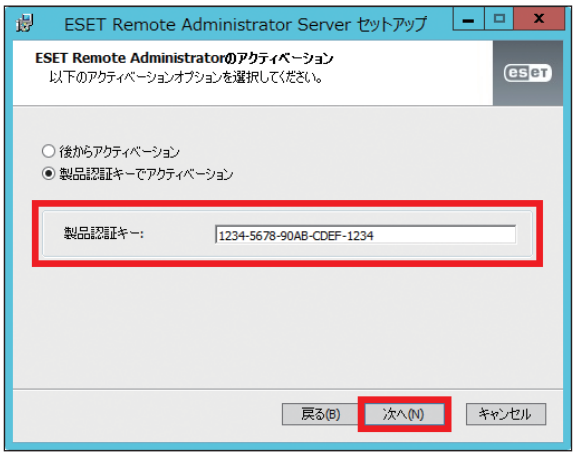


ワンポイント

入力した内容は、インストールが終了した後に、確認することができます。
「権限パスワード :」は認証局のパスワードです。設定した場合、各種証明書を作成、修正する際に必要となります。
「組織単位 :」「組織 :」「ローカル :」「州 / 国 :」の各項目への入力は、英数字のみとなっています。
各証明書については、「6.9　証明書」を参照してください。

続く

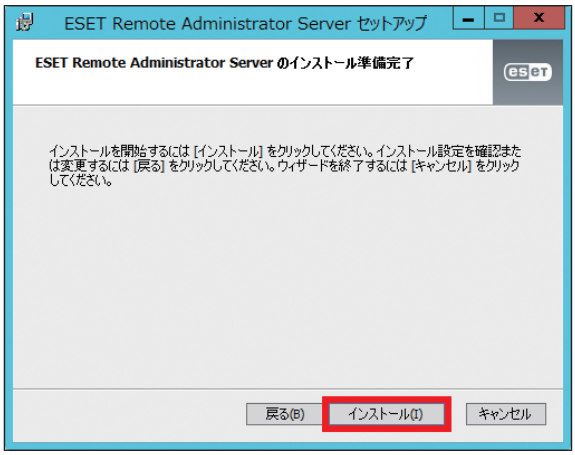
⑪［製品認証キーでアクティベーション］を選択し、テキストボックスに製品認証キーを入力後、［次へ］ボタンをクリックします。



ワンポイント

インストール時にアクティベーションを行う場合は、手順 7 の操作を行います。
「後からアクティベーション」を選択した場合の操作については、「6.12.2　アクティベーション」を参照してください。

⑫［インストール］ボタンをクリックします。

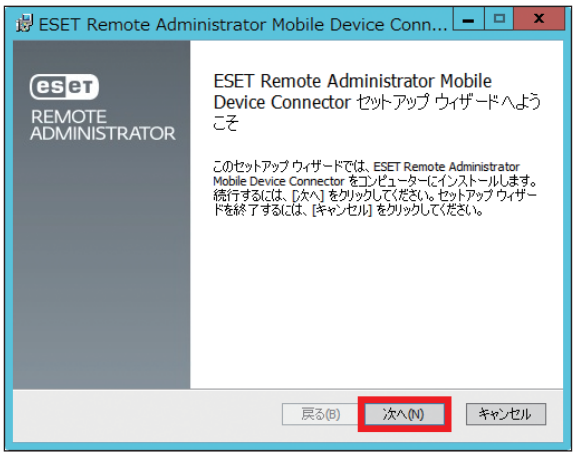


インストールが開始されます。

続く

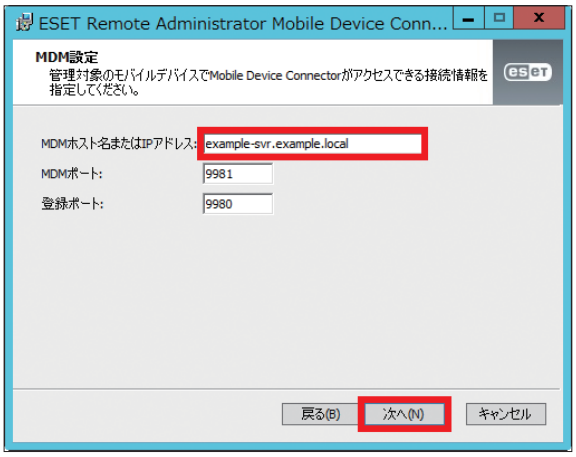
⑬ [完了] ボタンをクリックします。

続けて、その他の選択したコンポーネントがインストールされます。22 ページの手順 6 で「モバイルデバイスコネクター」のインストールを選択している場合は、モバイルデバイスコネクターのインストーラーが起動します。[次へ] をクリックして、手順 14 に進んでください。モバイルデバイスコネクターのインストールを選択していない場合は、30 ページの手順 20 に進んでください。



続く

14 Mobile Deviece Connector をインストールするサーバーのホスト名または IP アドレスを入力して、［次へ］ボタンをクリックします。

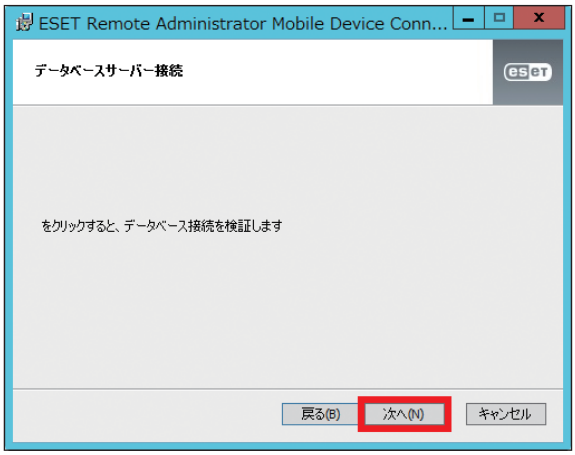


! 重　要

MDM ホスト名にサーバーのホスト名を入力する場合は、接続するモバイルデバイスが入力したホスト名の名前解決を行える必要があります。

15 ［次へ］ボタンをクリックします。

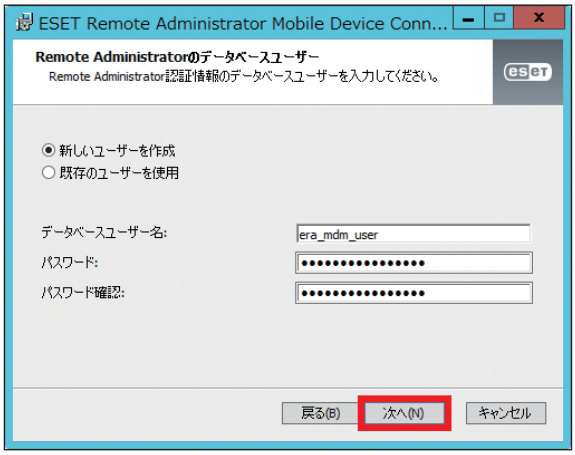
先にインストールされた、Microsoft SQL Server Express との接続確認が行われます。



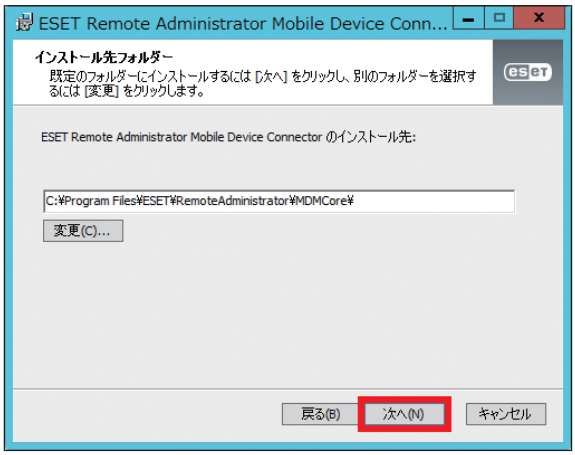
接続が確認されると、データベースユーザーの作成画面が表示されます。

続く

16 ［次へ］ボタンをクリックします。



17 インストール先フォルダーの確認画面が表示されます。［次へ］ボタンをクリックします。



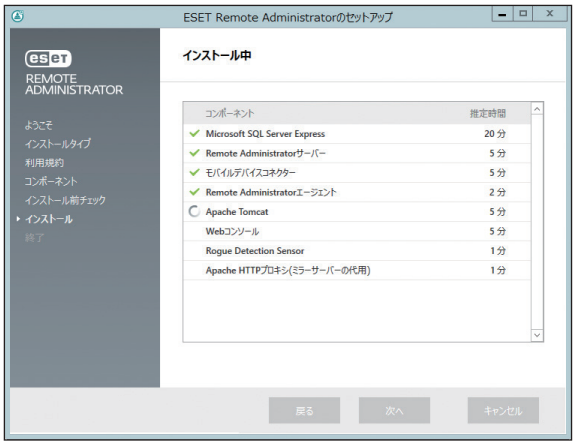
接続が確認されると「Web コンソールユーザーとサーバー接続」へ自動で切り替わります。

18 ［インストール］ボタンをクリックすると、Mobile Device Connector のインストールが開始されます。

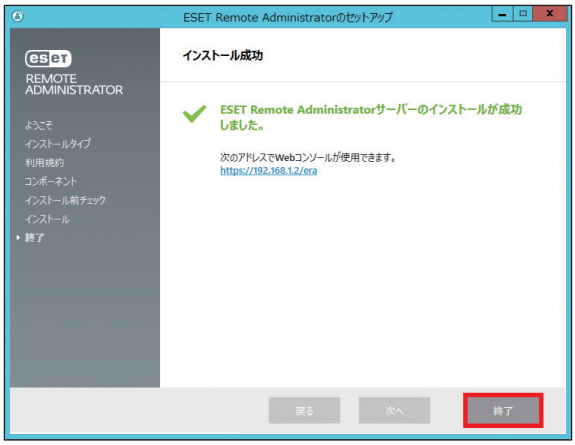
続く

19 インストールが完了したら［完了］ボタンをクリックします。

続けて、その他の選択したコンポーネントがインストールされます。



20 ［終了］ボタンをクリックします。



インストール終了後、スタート＞すべてのプログラムに ESET フォルダーが作成されます。
「ESET Remote Administrator Web Console」をクリックすると、ERA Web コンソールが起動します。
操作については、「4.1 ERA Web コンソールを開く」の操作手順 2 以降を参照してください。

3.2.2 ERA プロキシ 一括インストール

「ERA プロキシ」の稼動に必要なコンポーネントを一括でインストールします。
次の選択したコンポーネントがインストールされます。

- Microsoft SQL Server Express
- ERA プロキシ
- ERA エージェント
- RD Sensor

ワンポイント

「ERA プロキシ一括インストール」は、副系統（セカンダリ）のサーバーコンピューターを対象としています。

ERA プロキシのインストールには、次の条件が必要です。

- ERA サーバーと ERA Web コンソールが、主系統（プライマリ）サーバーコンピューター上にインストールされている
- ピア証明書（プロキシ）が作成されていて、ローカルドライブに保存されている
- 認証局が作成されていて、公開鍵がローカルドライブに保存されている

ワンポイント

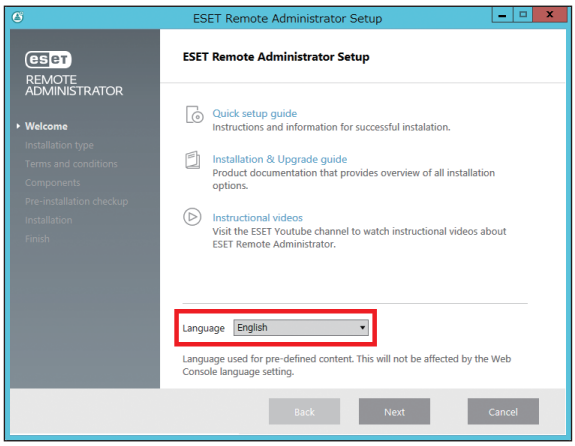
ピア証明書（プロキシ）と認証局公開鍵ファイルのエクスポートの操作については、「6.9 証明書」を参照してください。

操作手順

1. Setup.exe をダブルクリックします。

32bit 版、64bit 版とも、同じアイコンです。

2. 「Language」から［日本語］を選択します。

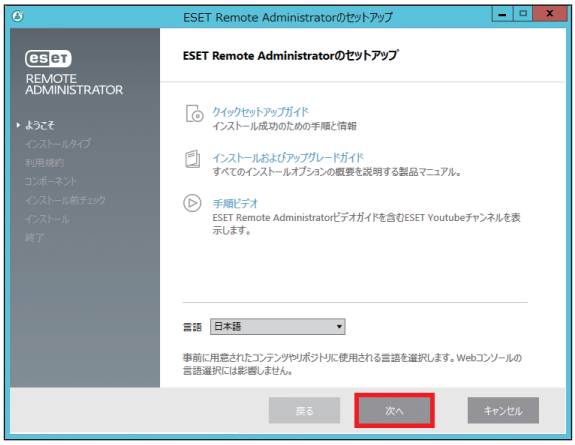


！重 要

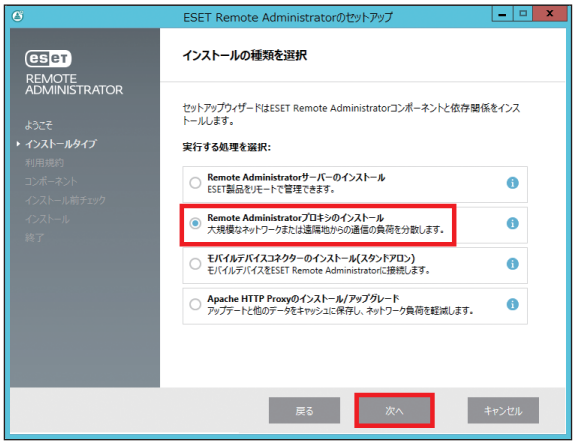
必ず日本語を選択してください。
日本語を選択しない場合は、リポジトリの設定が海外の値になり、サポート対象外となります。

続く

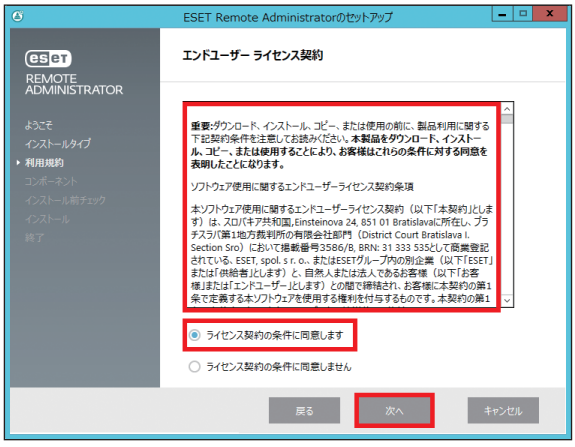
3 インストーラーの表示が日本語に切り替わります。［次へ］ボタンをクリックします。



4 「実行する処理を選択：」の［Remote Administrator プロキシのインストール］を選択し、［次へ］ボタンをクリックします。



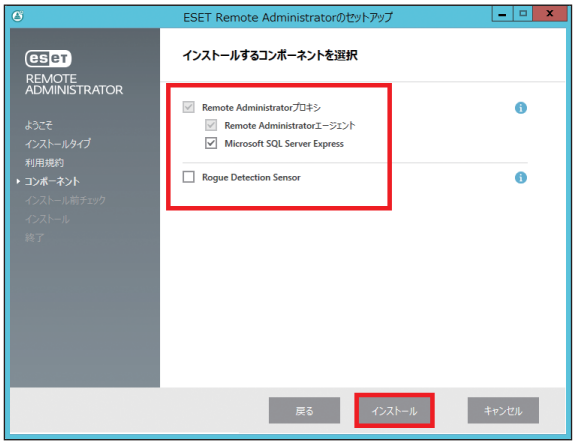
5 「エンドユーザー ライセンス契約」を一読して同意する場合、［ライセンス契約の条件に同意します］を選択し、［次へ］ボタンをクリックします。



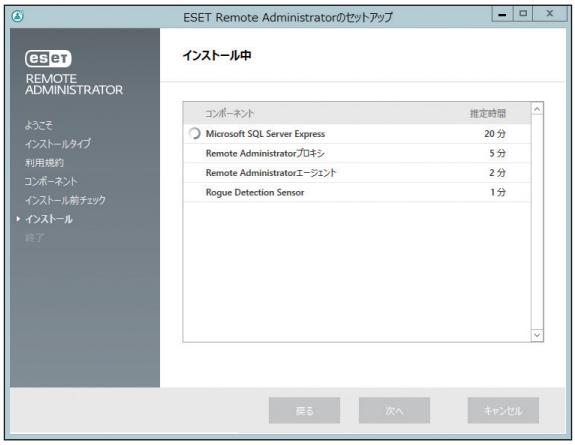
続く

6 インストールするコンポーネントにチェックを入れ、［インストール］ボタンをクリックします。

・Microsoft SQL Server Express
・ERA プロキシ
・RD Sensor



システム要件の確認が行われます。
システム要件を満たしている場合、Microsoft SQL Server Express のインストールが開始されます。



表示されている順番に、コンポーネントのインストールが行われます。
「Microsoft SQL Server Express」のインストールが終了した後、「ESET Remote Administrator Proxy セットアップ」が開始されます。

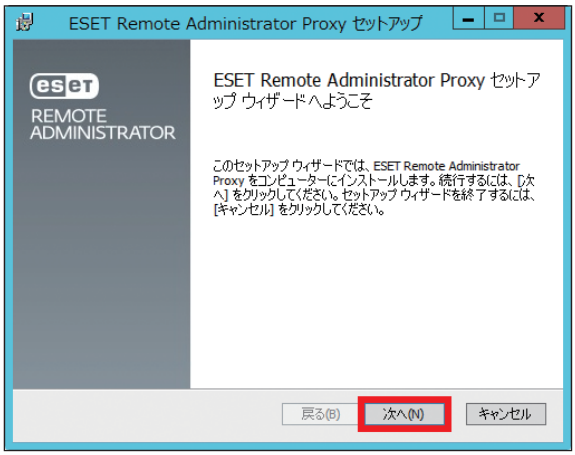
続く

ワンポイント

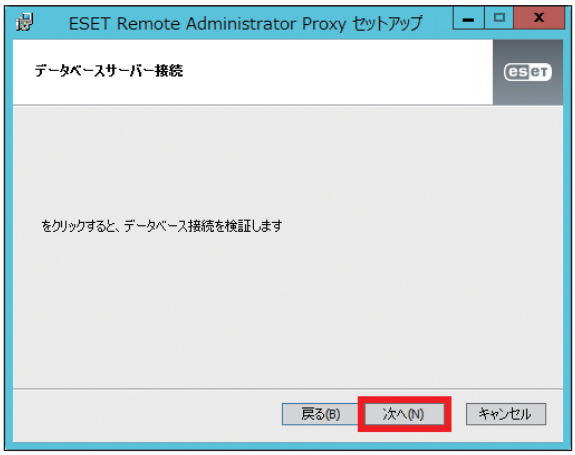
システム要件を満たしていなかった場合

「不足しているシステム要件」画面が表示され、不足しているシステムが表示されます。
メッセージに従い、不足しているシステムのインストールを行ってください。
※ Windows Server 2008 R2 以降のサーバーに「Microsoft .NET Framework 3.5」をインストールする場合は、サーバーマネージャーの機能の追加より実施してください。

7 「ESET Remote Administrator Proxy セットアップ ウィザードへようこそ」の［次へ］ボタンをクリックします。



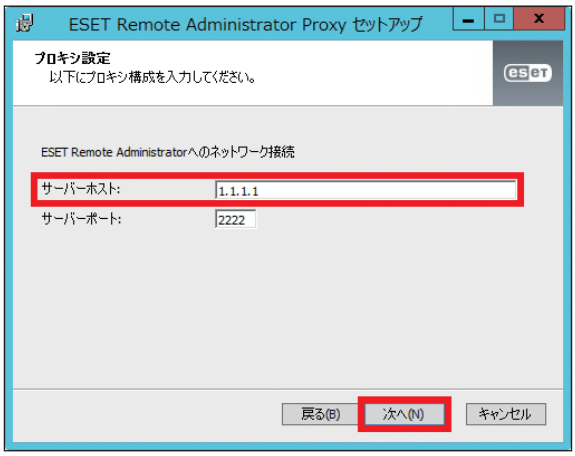
先にインストールされた、「Microsoft SQL Server Express」との接続確認が行われます。



接続が確認されると「プロキシ設定」へ自動で切り替わります。

続く

8 「サーバーホスト :」に、ERA サーバーがインストールされている主系統（プライマリ）サーバーコンピューターの名前または IP アドレスを入力し、［次へ］ボタンをクリックします。

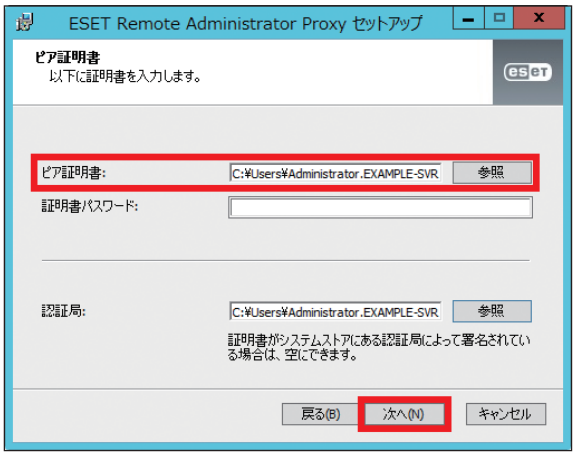


ワンポイント

「サーバーホスト :」には、サーバーの名前のほか、IP アドレスを設定できます。
既定の「サーバーポート :」は「2222」です。

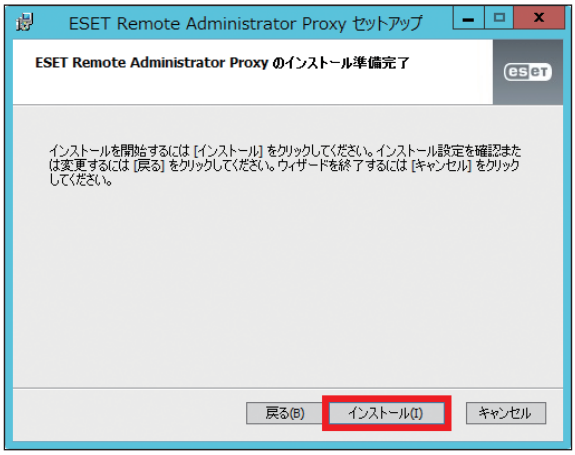
9 「ピア証明書 :」および「認証局 :」に、ローカルディスクに保存したピア証明書と、認証局の公開鍵を参照設定し、［次へ］ボタンをクリックします。

ピア証明書と公開鍵の参照設定は、必須の項目です。
「証明書パスワード :」には、ピア証明書のパスワードを入力します。
パスワードを設定していない場合は、入力は不要です。

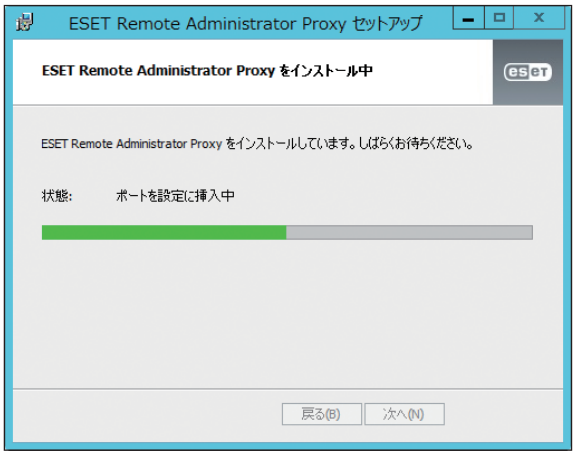


続く

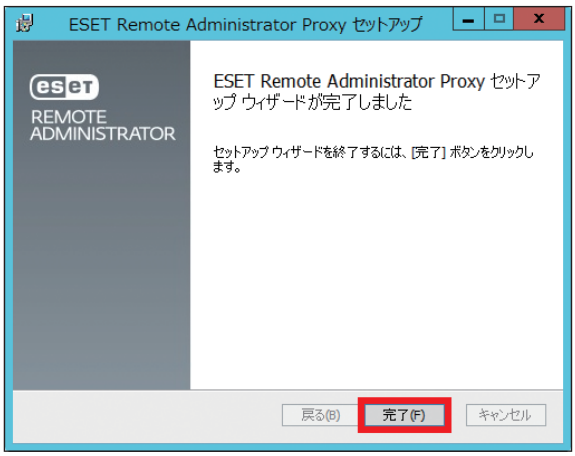
10 ［インストール］ボタンをクリックします。



ERA プロキシのインストールが開始されます。



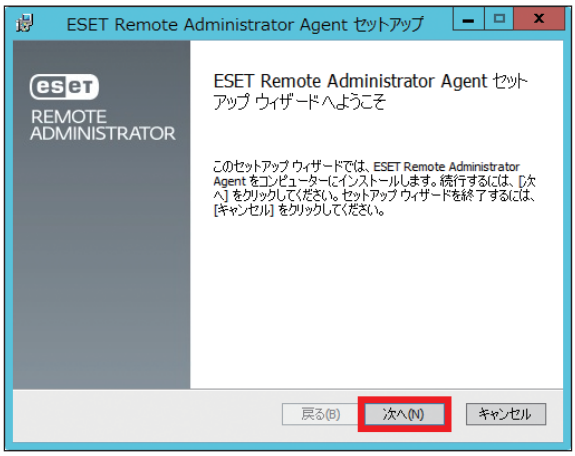
11 ［完了］ボタンをクリックします。



続けて、ERA エージェントのセットアップウィザードが起動します。

続く

12 「ESET Remote Administrator Agent セットアップ ウィザードへようこそ」の［次へ］ボタンをクリックします。



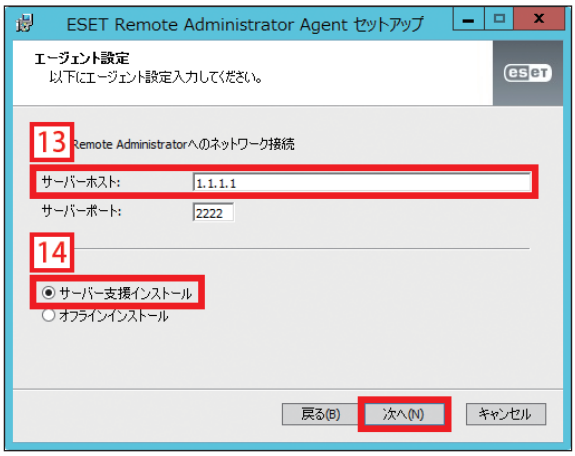
13 「サーバーホスト :」に、主系統（プライマリ）サーバーコンピューターの名前または IP アドレスを入力します。

ワンポイント

「サーバーホスト :」には、ERA サーバーの名前のほか、IP アドレスを設定できます。
既定の「サーバーポート :」は「2222」です。

14 ［サーバー支援インストール］を選択し、［次へ］ボタンをクリックします。

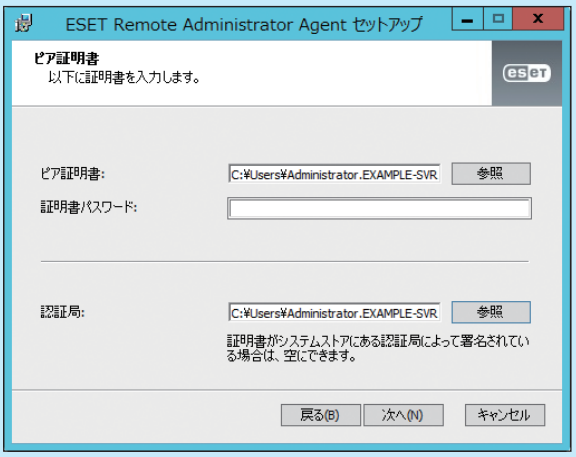
「サーバー支援インストール」
Web コンソール管理者の認証情報を指定します。証明書は、インストール中に自動ダウンロードされます。
「オフラインインストール］
ERA Web コンソールからエクスポートした、ピア証明書（プロキシ）を指定します。ピア証明書のエクスポートの操作については「6.9.1.3　ピア証明書のエクスポート」を参照してください。



続く

ワンポイント

［オフラインインストール］を選択した場合、次の画面で、ピア証明書および認証局証明書の参照を求められます。



また、ピア証明書にパスワードを設定している場合は、「証明書パスワード :」の入力が必要です。
証明書については「6.9　証明書」を参照してください。

［次へ］ボタンをクリックすると、手順 20 の画面へ切り替わります。

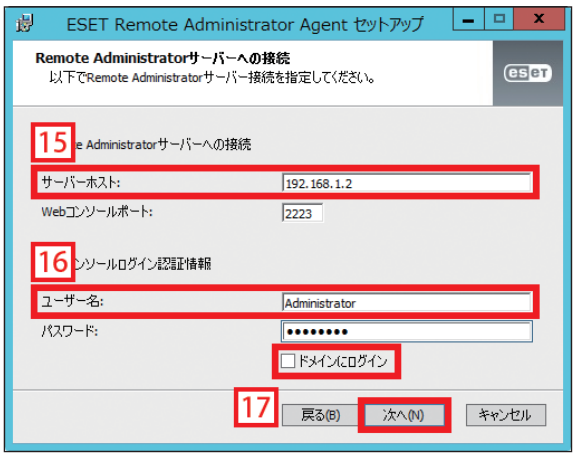
15 「サーバーホスト :」に記載されている内容が、手順 13 で入力した内容と同じであることを確認します。

ワンポイント

既定の「Web コンソールポート :」は「2223」です。

16 「ユーザー名 :」「パスワード :」に、ERA Web コンソールの管理者ユーザー名とパスワードを入力します。

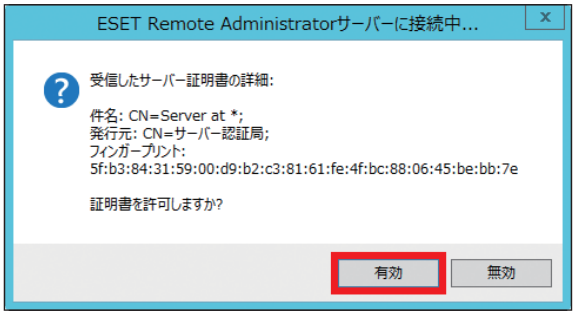
17 ［ドメインにログイン］のチェックを外し、［次へ］ボタンをクリックします。



続く

⑱ [有効] ボタンをクリックします。

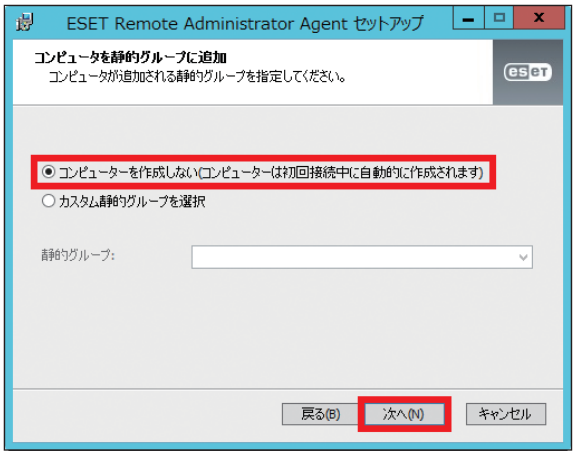
手順 9 において参照設定した、ピア証明書を許可します。



ワンポイント

手順 14 において［サーバー支援インストール］を選択したことで、Web コンソール管理者の認証証明書をダウンロードするための許可が必要となります。

⑲ [コンピューターを作成しない（コンピューターは初回接続中に自動的に作成されます）] を選択し、[次へ] ボタンをクリックします。

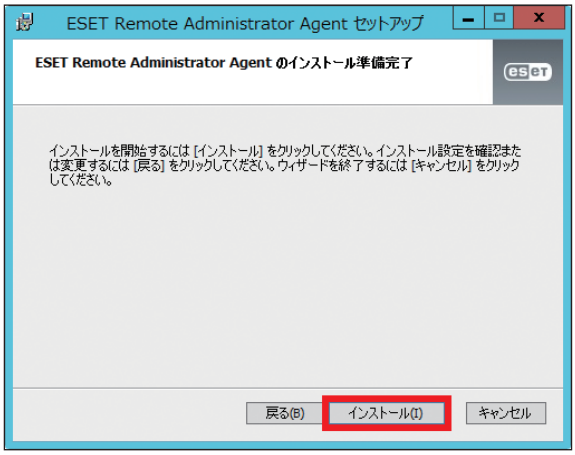


ワンポイント

［カスタム静的グループを選択］を選択すると、コンピューターを追加する静的グループを選択できます。

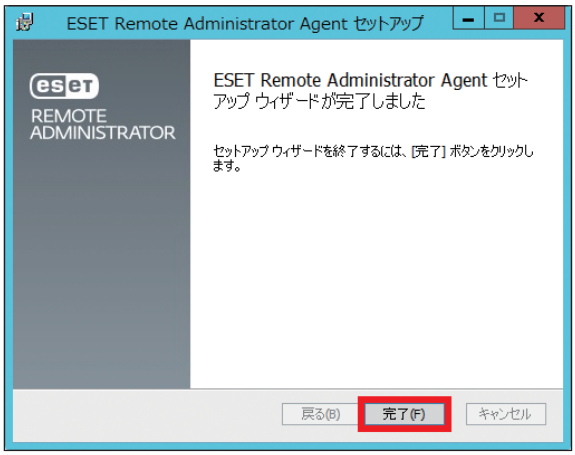
続く

20 [インストール] ボタンをクリックします。

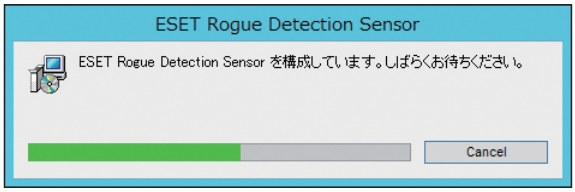


ERA エージェントのインストールが開始されます。

21 [完了] ボタンをクリックします。



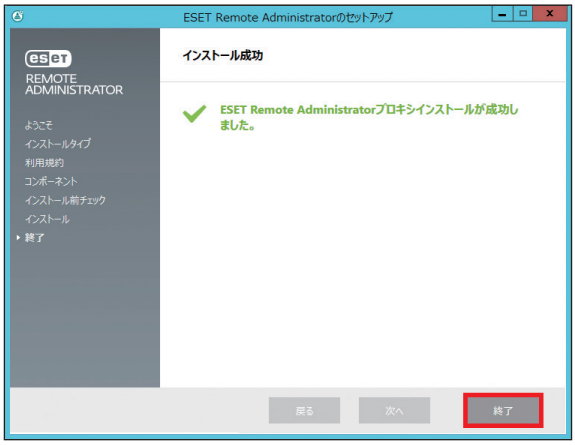
ERA エージェントのインストールが終了しました。
続けて、RD Sensor がインストールされます。



インストールが終了すると、画面が切り替わります。

続く

22 [終了] ボタンをクリックします。



3.2.3 Mobile Device Connector 一括インストール

Mobile Device Connector の稼動に必要なコンポーネントを一括でインストールします。
インストール中に、各コンポーネントが ERA サーバーに接続するための各種証明書の生成と認証を自動で行います。
次の選択したコンポーネントがインストールされます。

- Microsoft SQL Server Express
- ERA エージェント
- Mobile Device Connector

! 重　要

このインストール方法は、ERA サーバーとは別のサーバーに Mobile Device Connector をインストールする場合に適しています。すでに ERA サーバーがインストールされているサーバーに Mobile Device Connector を追加でインストールする場合は「3.3.8　Mobile Device Connector のインストール」を参照してください。

Mobile Device Connector の一括インストールには、次の条件が必要です。

- Mobile Deviece Connector と Android デバイスなどのモバイルデバイスや ERA サーバー、Apple Push Notification との間で通信に利用する次のポートが開いていて使用可能であること。

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

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

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

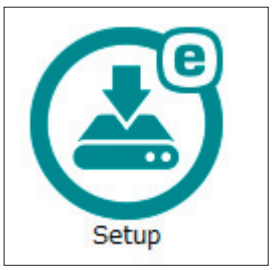
プロトコル	Apple Push Notification サービスへの通信で使用するポート	説明
TCP	5223	インターネット（Apple Push Notification サービス）への通信
TCP	2195	Mobile Device Connector からインターネット（Apple Push Notification サービス）への通信
TCP	2196	Mobile Device Connector からインターネット（Apple Push Notification サービスのフィードバックサービス）への通信
TCP	443	デバイスがポート 5223 でインターネット（Apple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

- Java Runtime Environment (JRE) がインストールされ、常に最新の公式リリースされた Java バージョンを使用していること。
- Microsoft .NET Framework 3.5 がインストールされていること。

操作手順

1. Setup.exe をダブルクリックします。

   32bit 版、64bit 版とも、同じアイコンです。

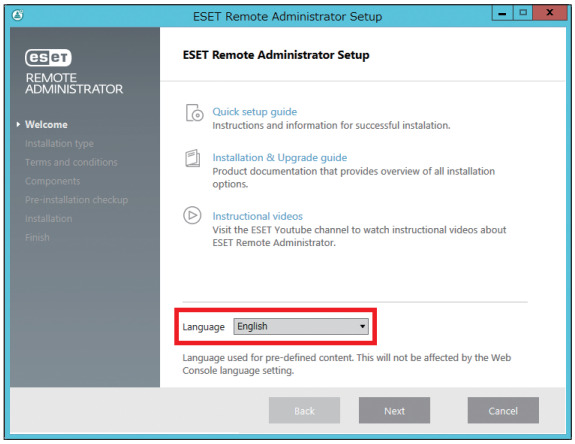


! 重　要

オールインワンインストーラーを保存するフォルダーのパスに日本語が含まれている場合、インストールを実行することができません。パスに日本語が含まれていないフォルダーにオールインワンインストーラーを保存し、インストールを行ってください。

続く

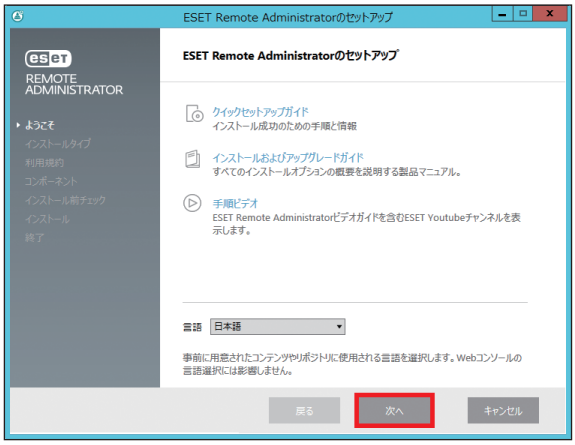
2 「Language」から［日本語］を選択します。



！重　要

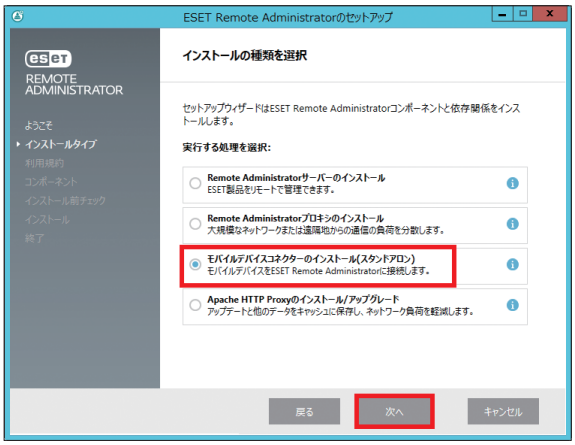
必ず日本語を選択してください。
日本語を選択しない場合は、リポジトリの設定が海外の値になり、サポート対象外となります。

3 インストーラーの表示が日本語に切り替わります。［次へ］ボタンをクリックします。

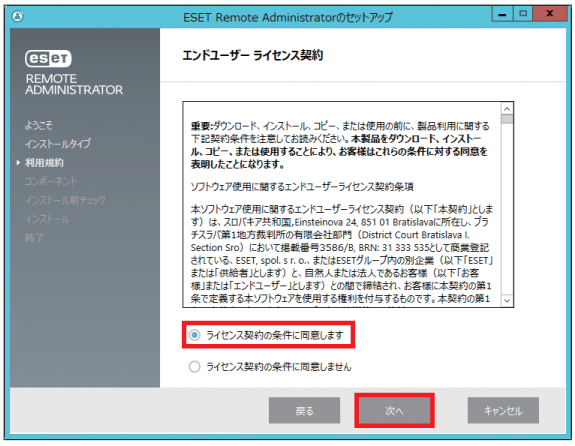


続く

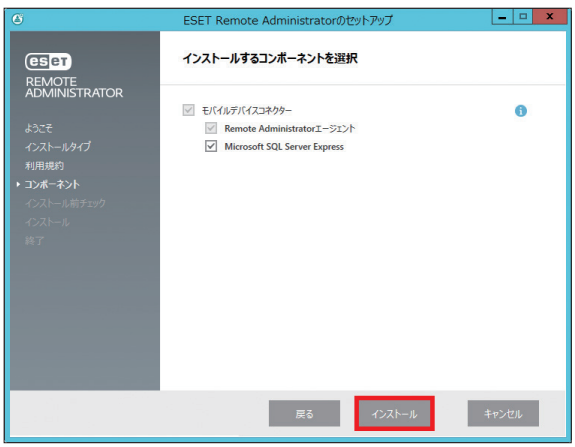
4 「実行する処理を選択 :」の［モバイルデバイスコネクターのインストール（スタンドアロン）］を選択し、［次へ］ボタンをクリックします。



5 「エンドユーザー ライセンス契約」を一読して同意する場合、［ライセンス契約の条件に同意します］を選択し、［次へ］ボタンをクリックします。

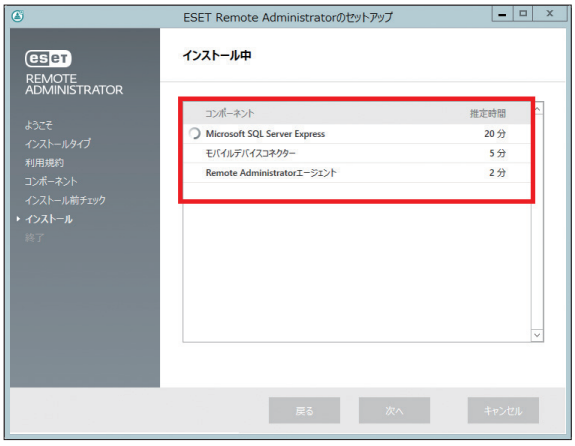


6 ［インストール］ボタンをクリックします。



続く

システム要件の確認が行われます。
システム要件を満たしている場合、Microsoft SQL Server Express のインストールが開始されます。

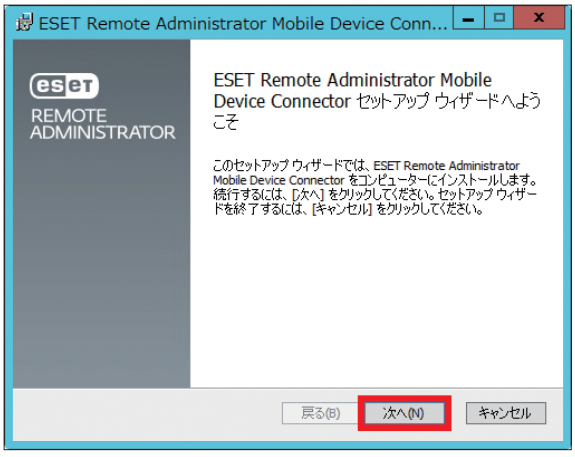


表示されている順番に、コンポーネントのインストールが行われます。
「Microsoft SQL Server Express」のインストールが終了した後、「モバイルデバイスコネクターのセットアップ」が開始されます。

ワンポイント

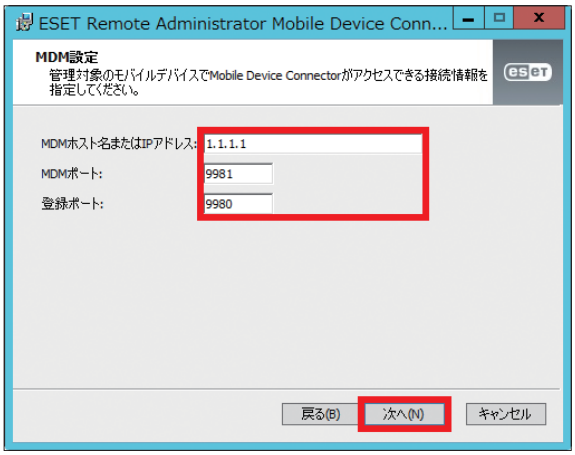
システム要件を満たしていなかった場合、「不足しているシステム要件」画面が表示され、不足しているシステムが表示されます。
メッセージに従い、不足しているシステムのインストールを行ってください。
※ Windows Server 2008 R2 以降のサーバーに「Microsoft .NET Framework 3.5」をインストールする場合は、サーバーマネージャーの機能の追加より実施してください。

7 「ESET Remote Administrator Mobile Device Connector セットアップ ウィザードへようこそ」の［次へ］ボタンをクリックします。



続く

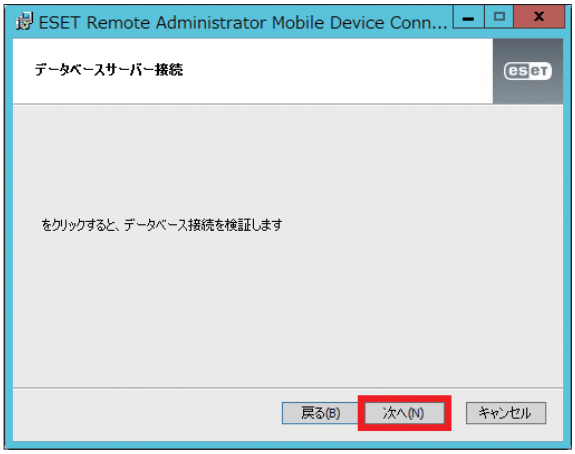
8 Mobile Deviece Connector をインストールするサーバーのホスト名または IP アドレスを入力して、［次へ］ボタンをクリックします。



! 重　要

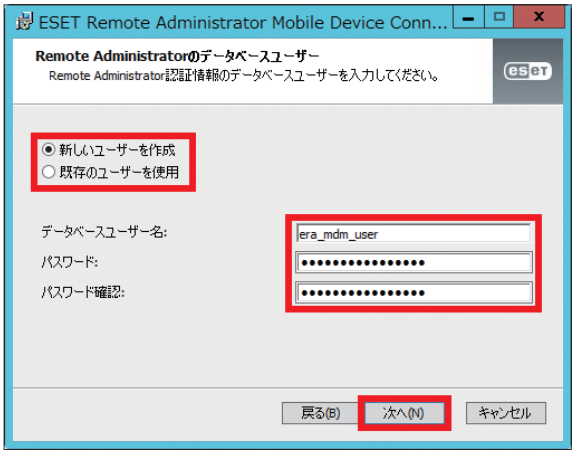
MDM ホスト名にサーバーのホスト名を入力する場合は、接続するモバイルデバイスが入力したホスト名の名前解決を行える必要があります。

9 データベースサーバーとの接続確認を行います。［次へ］ボタンをクリックします。



続く

10 新しく作成された Mobile Device Connector 用のデータベースのユーザーを設定します。新しいユーザーを作成するか、既存のデータベースユーザーを使用できます。データベースユーザー名やパスワードを入力して、［次へ］ボタンをクリックします。



11 サーバーホストに ERA サーバーの名前または IP アドレスを入力し、接続方法を以下の 2 種類から選択して、［次へ］ボタンをクリックします。ここでは、［サーバー支援インストール］を選択して、［次へ］をクリックします。

- サーバー支援インストール
  サーバー支援インストールは、ERA Web コンソール管理者の認証情報を指定する必要があります。インストールに必要な証明書はインストーラによって自動的にダウンロードされます。

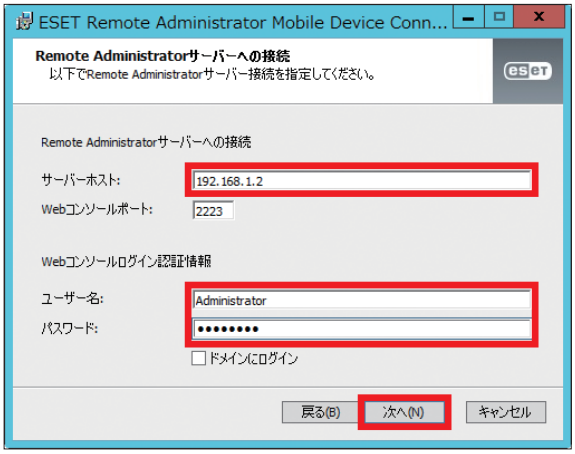
- オフラインインストール
  オフラインインストールでは、ERA Web コンソールからエクスポートしたピア証明書（プロキシ）を指定する必要があります。ピア証明書のエクスポートの操作については、「6.9.1.3　ピア証明書のエクスポート」を参照してください。

続く

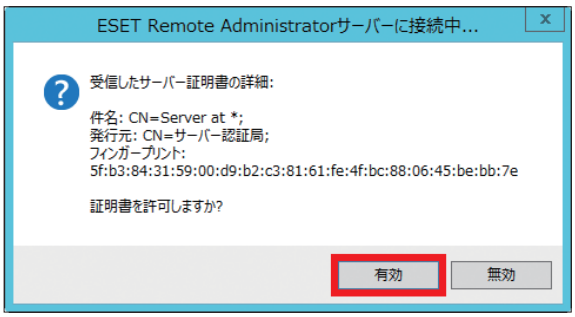
ワンポイント

手順 11 でオフラインインストールを選択した場合は、ERA Web コンソールで作成したカスタム証明書も使用でき、次の画面でピア証明書および認証局証明書の参照を求められます。［参照］ボタンをクリックして、あらかじめ用意しておいた証明書の指定を行ってください。なお、ピア証明書にパスワードを設定している場合は、証明書パスワードの設定も必要になります。証明書の指定を行ったら、［次へ］ボタンをクリックして手順 14 に進んでください。

⑫ サーバーホストに ERA サーバーの名前または IP アドレスを入力し、Web コンソールログイン認証情報 (ユーザー名 / パスワード) を指定します。［次へ］ボタンをクリックします。

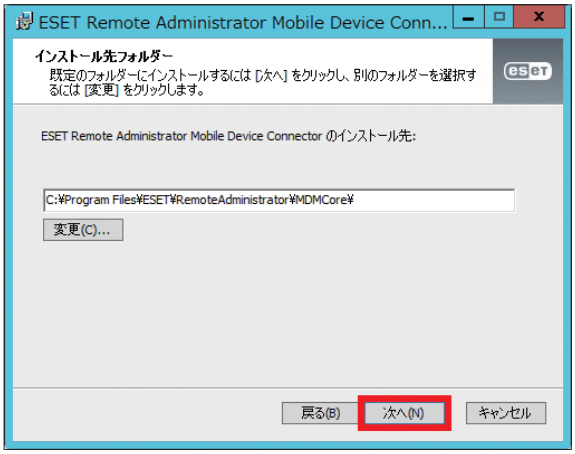


⑬ ［有効］ボタンをクリックして、ダウンロードした証明書の利用を許可します。



続く

14 インストール先フォルダーを確認して［次へ］ボタンをクリックすます。



15 ［インストール］ボタンをクリックすると、Mobile Device Connector のインストールが開始されます。

続く

16 インストールが完了したら［完了］ボタンをクリックします。続いて、「ESET Remote Administrator Agent のセットアップ」が開始されます。

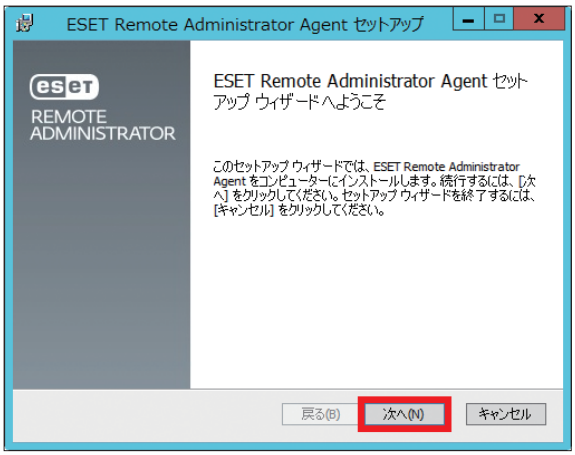
ワンポイント

すべてのプログラムのインストールが完了したら、Web ブラウザーで Mobile Device Connector が実行中かどうかを確認します。確認方法については、56 ページ手順 27、あるいは「Mobile Device Connector の動作確認」をご参照ください。

! 重 要

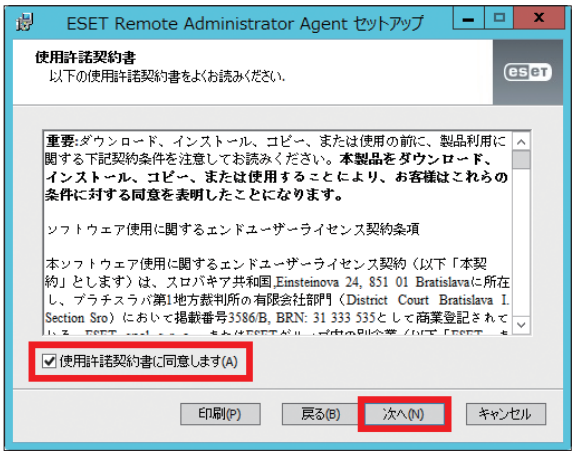
Mobile Device Connector を利用するためには Mobile Device Connector のアクティベーションが必要です。Mobile Device Connector がインストールされているコンピューターに「製品のアクティベーションタスク」を実行して、アクティベーションしてください。

17 「ESET Remote Administrator Agent セットアップ ウィザードへようこそ」の［次へ］ボタンをクリックします。



続く

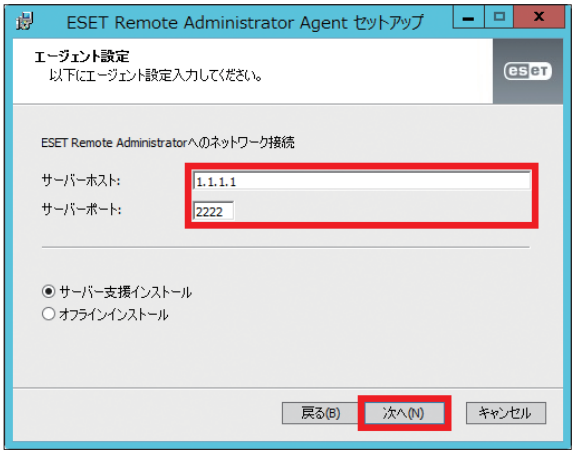
18 一読して、同意する場合は、[使用許諾契約書に同意します] にチェックを入れ、[次へ] ボタンをクリックします。



19 サーバーホストに ERA サーバーの名前または IP アドレスを入力し、接続方法を以下の 2 種類から選択して、[次へ] ボタンをクリックします。ここでは、[サーバー支援インストール] を選択して、[次へ] をクリックします。

- サーバー支援インストール
  サーバー支援インストールは、ERA Web コンソール管理者の認証情報を指定する必要があります。インストールに必要な証明書はインストーラによって自動的にダウンロードされます。

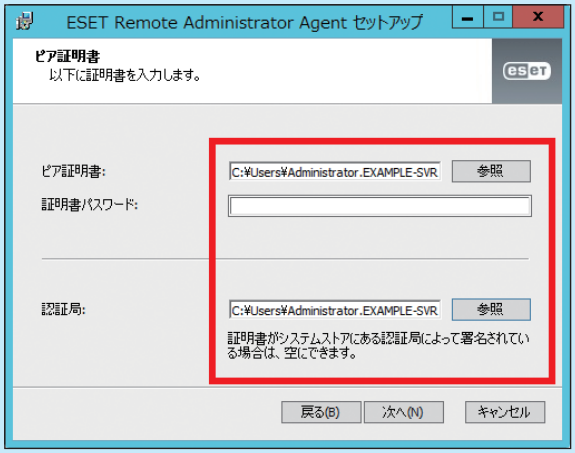
- オフラインインストール
  オフラインインストールでは、ERA Web コンソールからエクスポートしたピア証明書（プロキシ）を指定する必要があります。ピア証明書のエクスポートの操作については、「6.9.1.3 ピア証明書のエクスポート」を参照してください。



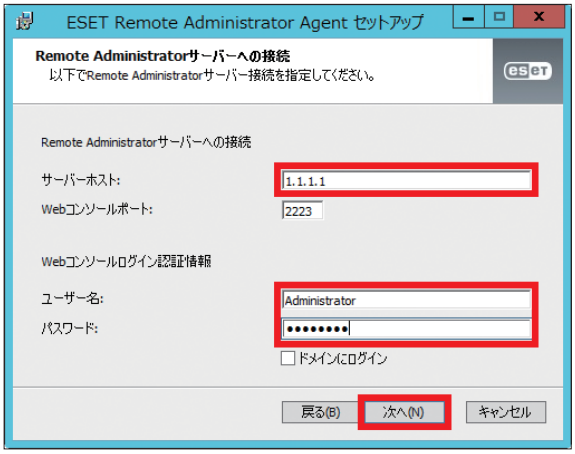
続く

ワンポイント

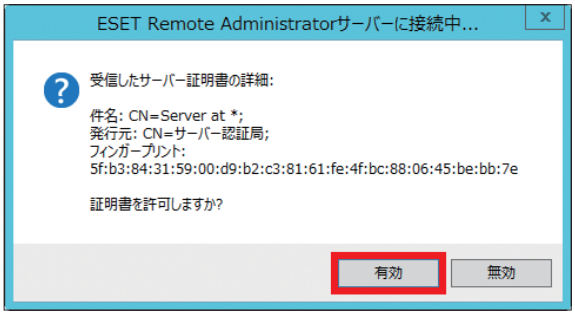
手順 19 でオフラインインストールを選択した場合は、ERA Web コンソールで作成したカスタム証明書も使用でき、次の画面でピア証明書および認証局証明書の参照を求められます。［参照］ボタンをクリックして、あらかじめ用意しておいた証明書の指定を行ってください。なお、ピア証明書にパスワードを設定している場合は、証明書パスワードの設定も必要になります。証明書の指定を行ったら、［次へ］ボタンをクリックして手順 22 に進んでください。



20 サーバーホストに ERA サーバーの名前または IP アドレスを入力し、Web コンソール管理者認証情報 (ユーザー名 / パスワード) を指定します。［次へ］ボタンをクリックします。

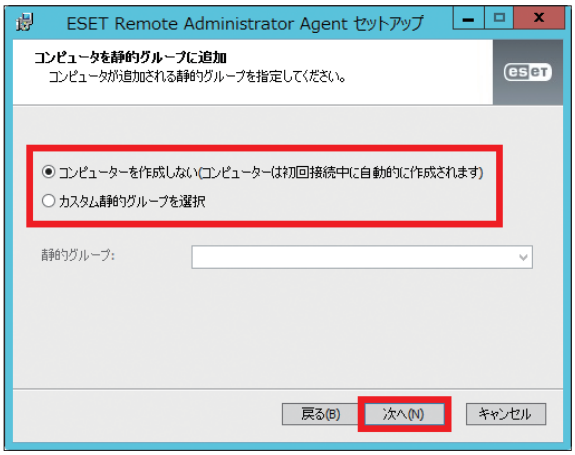


21 ［有効］ボタンをクリックして、ダウンロードした証明書の利用を許可します。



続く

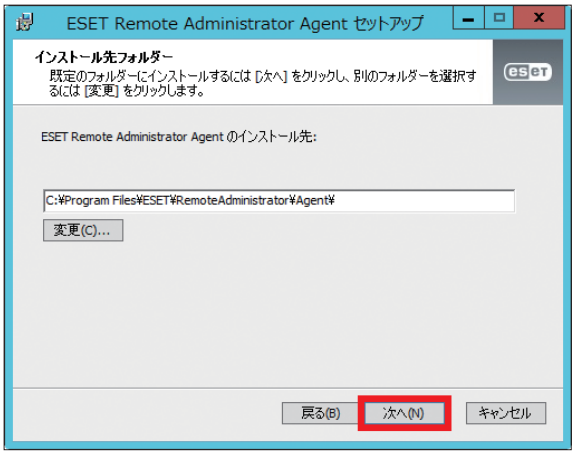
22 「コンピュータを静的グループに追加」画面が表示されます。ここでは、[コンピューターを作成しない] のチェックをオンにして、[次へ] ボタンをクリックします。



ワンポイント

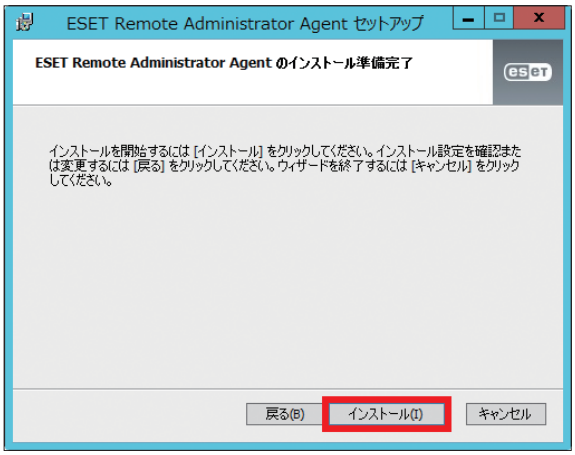
静的グループに追加したいグループ名を入力すると、静的グループに追加できます。

23 インストール先フォルダーを確認して [次へ] ボタンをクリックすます。

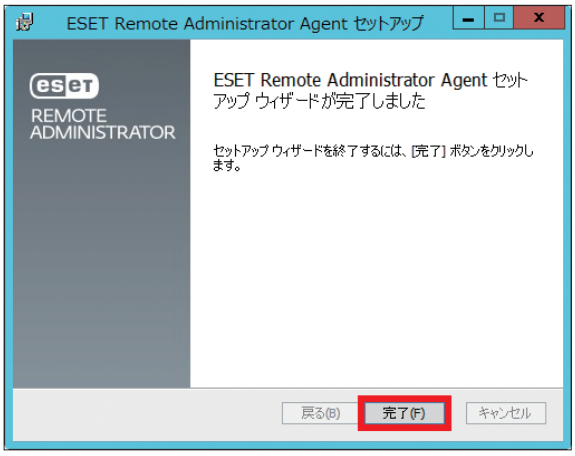


続く

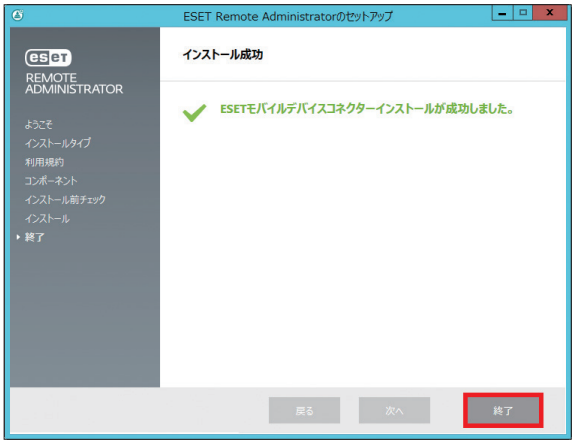
24 ［インストール］ボタンをクリックすると、ESET Remote Administrator Agent のインストールが開始されます。



25 インストールが完了したら［完了］ボタンをクリックします。



26 すべてのプログラムのインストールが完了すると、「インストール成功」画面が表示されます。［終了］ボタンをクリックします。



続く

27 すべてのプログラムのインストールが完了したら、Web ブラウザーで Mobile Device Connector が実行中かどうかを確認します。実行中の場合は、以下の画面が表示されます。

URL：https://hostname(IP アドレス）:9980

ワンポイント

Web ページを表示できない場合は、ファイアウォールとネットワークの構成を確認してください。

3.2.4 アンインストール

一括インストールした場合、アンインストールはオールインワンインストーラーから行います。

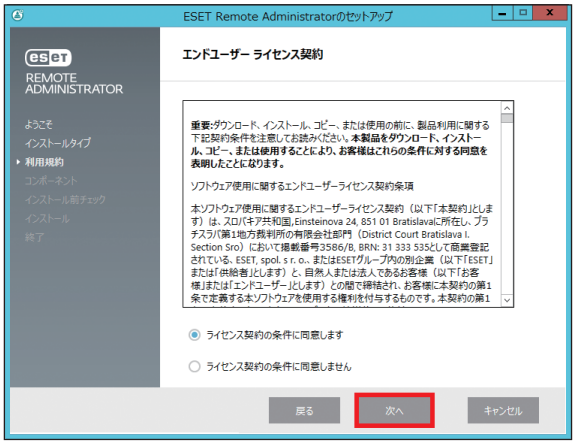
操作手順

1. Setup.exe をダブルクリックします。

2. セットアップ画面を日本語表記にし、「Remote Administrator コンポーネントのアンインストール」を選択し、［次へ］ボタンをクリックします。

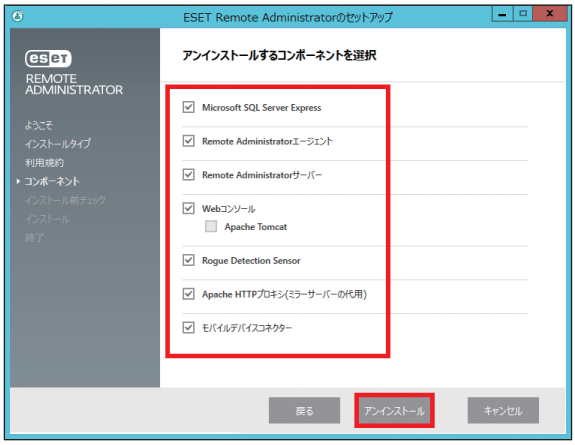
   ESET Remote Administrator を既にインストールしている状態でオールインワンインストーラーを起動した場合、「実行する処理を選択 :」の一番下に、「Remote Administrator コンポーネントのアンインストール」が追加されます。

3. 「エンドユーザー ライセンス契約」を一読して同意する場合、［ライセンス契約の条件に同意します］を選択し、［次へ］ボタンをクリックします。



続く

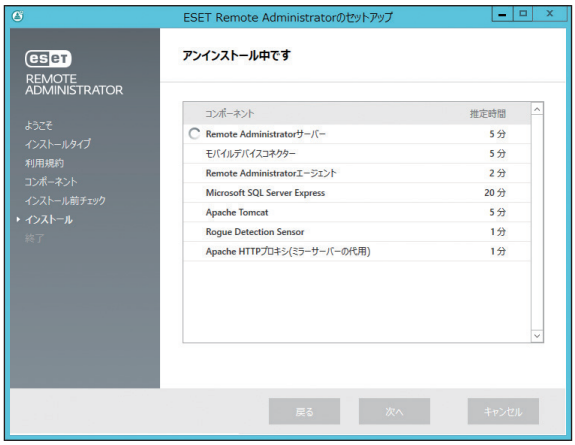
4 削除するコンポーネントにチェックを入れ、［アンインストール］ボタンをクリックします。



ワンポイント

既にインストールされているコンポーネントが表示されます。
コンポーネントをすべて削除する場合は、すべてにチェックを入れてください。

アンインストールが開始されます。
表示されている順番に、コンソールのアンインストールが行われます。



!重 要

コンポーネントのアンインストール後は、サーバーを再起動することを推奨します。

3.3 Windows 版コンポーネントインストール

コンポーネントインストールでは、必要なプログラムを個別にインストールします。
別途、SQL Server と、Apache Tomcat のインストールと設定を行う必要があります。
アンインストールは、Windows の「プログラムのアンインストール」からプログラムごとに行います。

! 重 要

Apache Tomcat は、セキュリティの向上のため、SSL（HTTPS）に接続できるように設定する必要があります。
Apache Tomcat のインストールや設定方法が不明な場合は、オールインワンインストーラーを利用して一括インストールを行うことを推奨します。

■インストーラーファイル一覧

各コンポーネントのインストーラーファイルは、以下のとおりです。
使用環境に合わせて、ファイルを選択してください。

	インストーラー	
	32bit 版	**64bit 版**
	win32¥installer	**x64¥installer**
ERA サーバー	Server_x86.msi	Server_x64.msi
モバイルデバイスコネクター	MDMCore_x86.msi	MDMCore_x64.msi
ERA エージェント	Agent_x86.msi	Agent_x64.msi
ERA Web コンソール	era.war	
RD Sensor	RDSensor_x86.msi	RDSensor_x64.msi
ERA プロキシ	Proxy_x86.msi	Proxy_x64.msi

! 重 要

本マニュアルでは、64bit 版のインストーラーフォルダーである x64 フォルダーを、C: ¥ に保存しています。
各コンポーネントのインストーラーは、次の場所に保存されている状態で、操作を解説します。
C:¥x64¥installers

それぞれのファイルをダブルクリックすると、インストーラーが起動します。また、各インストーラーの画面は英語表記となっています。

■インストーラーの日本語化

各コンポーネントのインストーラーは、日本語に対応しています。
インストール画面を日本語表記にする場合は、それぞれのインストーラーをコマンドプロンプトから起動します。
以下は、解凍した x64 フォルダーを C ドライブに保存している状態で、ERA サーバーのインストーラーファイルである Server_x64.msi を、日本語で起動する場合のコマンドです。

! 重　要

この操作は必須の操作です。日本語化しない場合は、リポジトリの設定が海外の値になり、サポート対象外となります。

操作手順

コマンドプロンプトを起動し、以下を入力します。

起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥Server_x64.msi TRANSFORMS=":ja-JP.mst"`

※網掛け部分を、各インストーラーのファイル名に変えて実行します。

ワンポイント

コマンドプロンプトの実行対象を、インストーラーが保存されているフォルダーに変更しない場合は、msiexec /i 以降に、インストーラーの絶対パスまたは相対パスを、現在の実行対象に合わせて指定してください。

3.3.1 SQL サーバーの準備

コンポーネントインストールの場合、事前に SQL サーバーのインストールと設定を行う必要があります。
また、既にインストール済みの SQL Server がシステム上にある場合は、SQL の設定「認証」を混合モードに変更してください。

! 重 要

本マニュアルでは、直前に「Microsoft SQL Server 2008 R2 Express」をインストールした状態で、操作を説明しています。

3.3.2 ERA サーバーのインストール

ERA サーバーのインストールでは、準備として ERA サーバーと SQL Server の接続を検証し、正常に接続できた場合、インストールが開始されます。

ERA サーバーのインストールには、次の条件が必要です。

- SQL Server のインストールと設定
- ERA サーバーが使用するネットワーク通信ポートが空いていること
- Java Ver.7.0 以上のインストール、または最新版への更新
- Microsoft .NET Framework 3.5 のインストール

※ Windows Server 2008 R2 以降のサーバーに「Microsoft .NET Framework 3.5」をインストールする場合は、サーバーマネージャーの機能の追加より実施してください。

ワンポイント

SQL Server の詳細は、「3.3.1 SQL サーバーの準備」を参照してください。
ERA サーバーが使用するネットワーク通信ポートについては、「2.4 使用されるポート」を参照してください。
ESET Remote Administrator は、Java Standard Edition 7 以上に対応していますが、最新版への更新を推奨しています。

操作手順

1. 「Server_x64.msi」を日本語表記で起動します。32bit 版の場合は、インストーラー名が「Server_x86.msi」となります。

   起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥Server_x64.msi TRANSFORMS=":ja-JP.mst"`

   ERA サーバーセットアップウィザードが起動します。

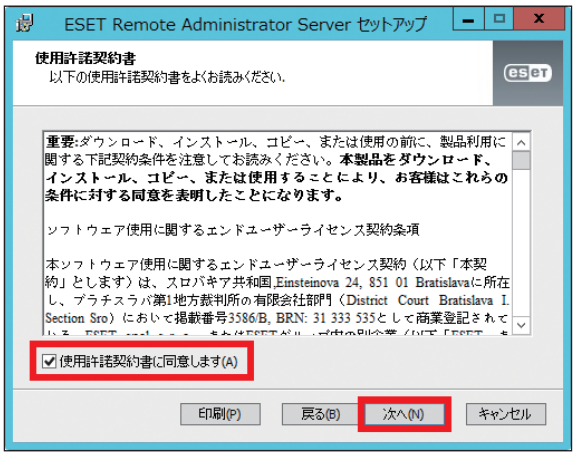
ワンポイント

インストーラーの日本語化については、「3.3 Windows 版コンポーネントインストール」の「■インストーラーの日本語化」を参照してください。

続く

2 ［次へ］ボタンをクリックします。

3 一読して同意する場合、［使用許諾契約書に同意します］にチェックを入れ、［次へ］ボタンをクリックします。

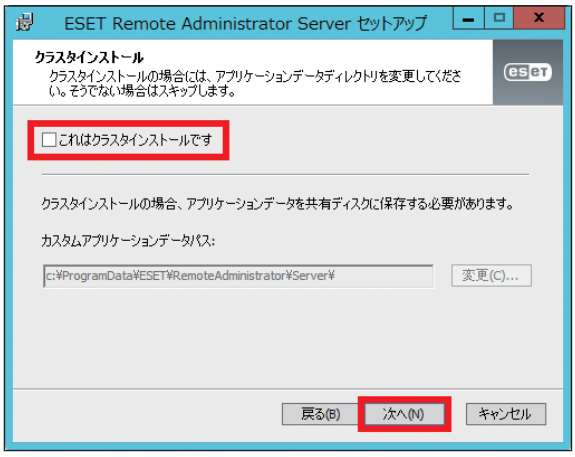


ワンポイント

チェックを外して［次へ］ボタンをクリックした場合、次の画面には進みません。

続く

4 ［これはクラスタインストールです］のチェックを外し、［次へ］ボタンをクリックします。

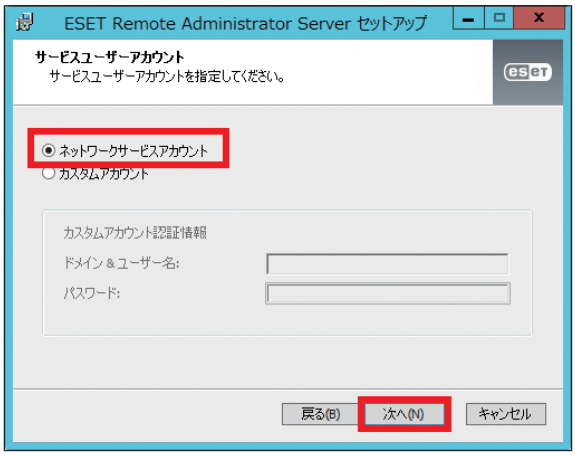


ワンポイント

フェールオーバー環境へのインストールの場合は、「これはクラスタインストールです」にチェックを入れ、「カスタムアプリケーションデータパス :」には、クラスタ内のすべてのコンピューターが接続できる共有の場所を指定します。
フェールオーバー環境へのインストールについては、「3.3.9 フェールオーバー環境へのインストール」を参照してください。

5 ［ネットワークサービスアカウント］を選択し、［次へ］ボタンをクリックします。

ネットワークサービス以外の Windows アカウントを利用する場合は、「カスタムアカウント」を選択し、「カスタムアカウント認証情報」である、「ドメイン & ユーザー名 :」および「パスワード :」を設定します。

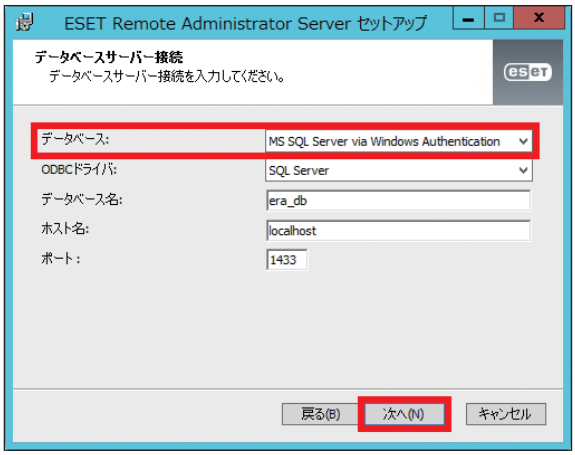


続く

6 「データベース :」から［MS SQL Server via Windows Authentication］を選択し、［次へ］ボタンをクリックします。

Windows 認証経由で、データベースサーバーへの接続設定を行います。

データベース	MySQL Server/MS SQL Server/Windows 認証による MySQL Server から選択します。
ODBC ドライバ	MySQL ODBC5.1Driver/MySQL ODBC5.2 Unicode Driver/MySQL ODBC5.3 Unicode Driver/SQL Server/SQL Server Native Client10.0/ODBC Driver 11 for SQL Server から選択します。
データベース名	既定の「era_db」が入力されています。変更可能です。
ホスト名	データベースサーバーのホスト名または IP アドレスを入力します。
ポート	既定値「1433」が入力されています。データベースサーバーへの接続に使用するポート番号を入力します。



接続確認を行います。接続が確認されると、次の画面に切り替わります。

ワンポイント

接続されるデータベースに、ERA サーバーのデータ（パスワードやログなど）が蓄積されます。
また ESET Remote Administrator の適切な実行のため、ERA サーバーが大きいパケットサイズを許可するよう MySQL を設定する必要があります。

続く

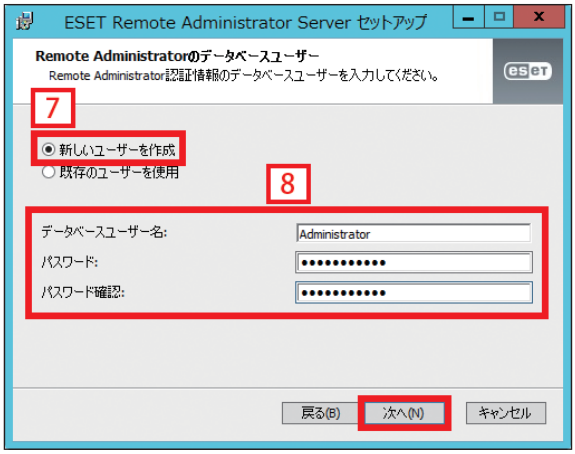
7 データベースユーザーを設定します。［新しいユーザーを作成］を選択します。

ワンポイント

既存のデータベースユーザーを使用する場合は、「既存のユーザーを使用」を選択し、「データベースユーザー名 :」および「パスワード :」を入力してください。

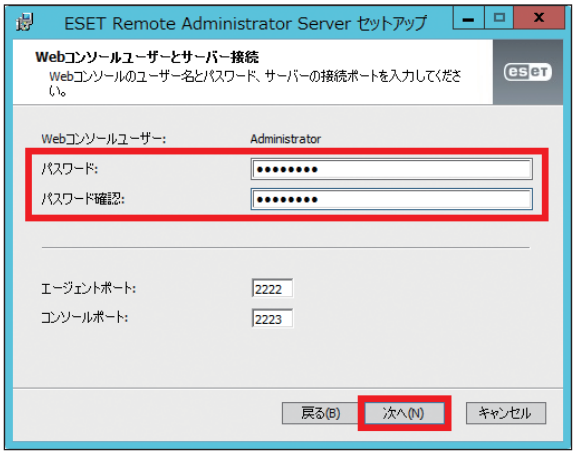
8 「データベースユーザー名 :」、「パスワード :」および「パスワード確認 :」を入力し、［次へ］ボタンをクリックします。

データベース管理者のユーザー名とパスワードを設定します。



9 「パスワード :」および「パスワード確認 :」を入力し、［次へ］ボタンをクリックします。

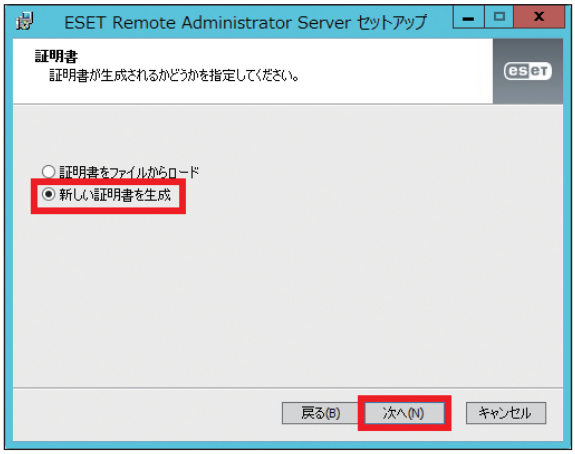
Web コンソールにログインするための初期パスワードを設定します。
「Web コンソールユーザー :」には、適宜「Administrator」が適用されます。



続く

10 ［新しい証明書を生成］を選択し、［次へ］ボタンをクリックします。

「新しい証明書を生成」を選択することで、インストール中にサーバー証明書および各証明書が自動生成されます。



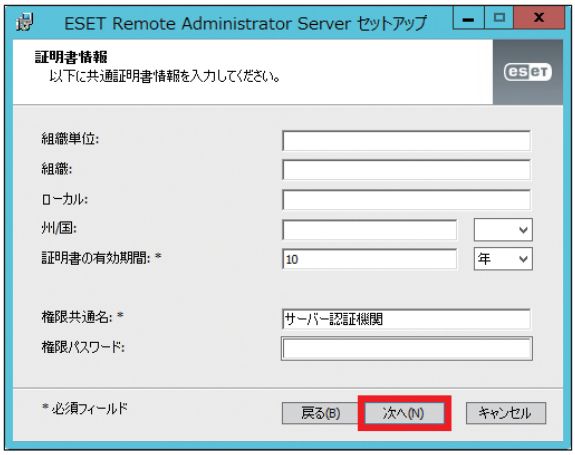
11 項目を入力し、［次へ］ボタンをクリックします。

「証明書情報」では、生成されるサーバー / クライアント通信の証明書へ登録する情報を入力します。
入力した内容は、ERA Web コンソールの認証局に反映されます。

組織単位	部署名
組織	会社名
ローカル	都道府県名
州 / 国	組織の国籍
証明書の有効期間	初期設定で 10 年が設定されます。
権限共通名	認証局の名前
権限パスワード	認証局パスワード

! 重　要

証明書の有効期間は初期設定のまま変更しないでください。証明書の有効期間が 2038 年以上に設定されている場合は、Mac OS X が証明書エラーになり、管理できません。



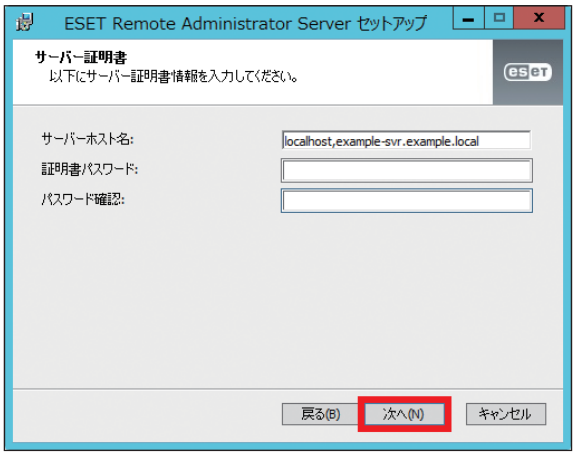
続く

ワンポイント

ここで入力した内容は、インストールが終了した後に確認することができます。
「権限パスワード :」は認証局のパスワードです。設定した場合、各種証明書を作成、修正する際に必要となります。
「組織単位 :」「組織 :」「ローカル :」「州 / 国 :」の各項目への入力は、英数字のみとなっています。
各証明書については、「6.9　証明書」を参照してください。

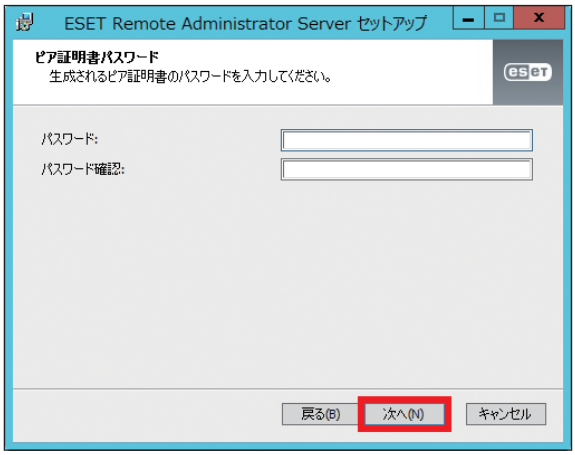
⑫ サーバー証明書のパスワードを入力し、［次へ］ボタンをクリックします。

生成されるサーバー証明書にアクセスするためのパスワードを設定します。設定は任意です。



⑬ ピア証明書のパスワードを入力し、［次へ］ボタンをクリックします。

生成されるピア証明書にアクセスするためのパスワードを設定します。設定は任意です。

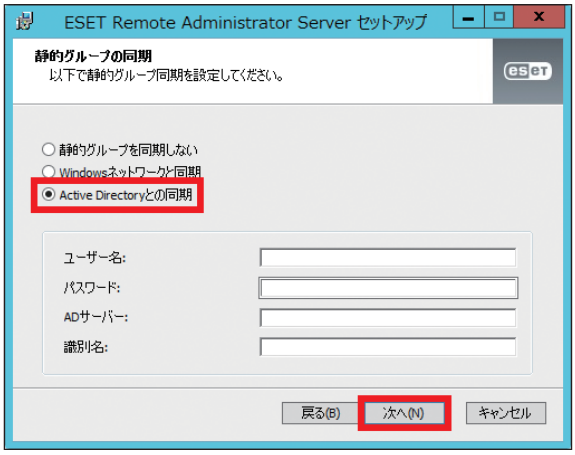


続く

14 同期方法を選択し、［次へ］ボタンをクリックします。

「静的グループの同期」では、静的グループを形成する、クライアントコンピューターの検索先を指定します。

静的グループを同期しない	クライアントコンピューターを検索しない。
Windows ネットワークと同期	Windows ワークグループネットワーク内から検索する。
Active Directory との同期	Active Directory 内から検索する。

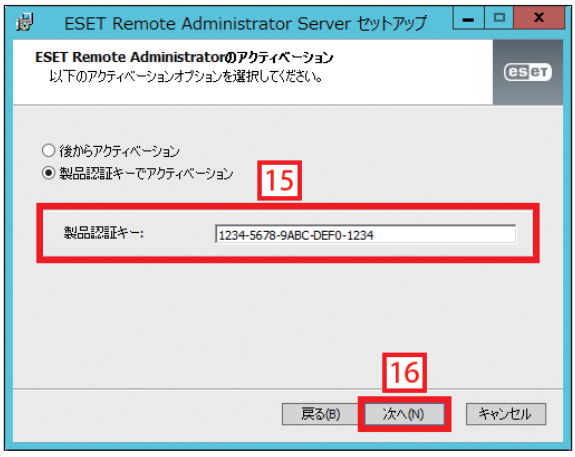


ワンポイント

［Active Directory との同期］を選択することにより、ERA によって Active Directory 内で検索されたクライアントコンピューターはすべて静的グループに追加されます。
静的グループの詳細については「6.3 グループ」を参照してください。
各項目への設定は任意です。
・「ユーザー名 :」/「パスワード :」 ドメインにログインするためのユーザー名とパスワードを入力します。
・「AD サーバー :」 接続するサーバー名、または IP アドレスを入力します。
・「識別名 :」 Active Directory のパスを入力します。

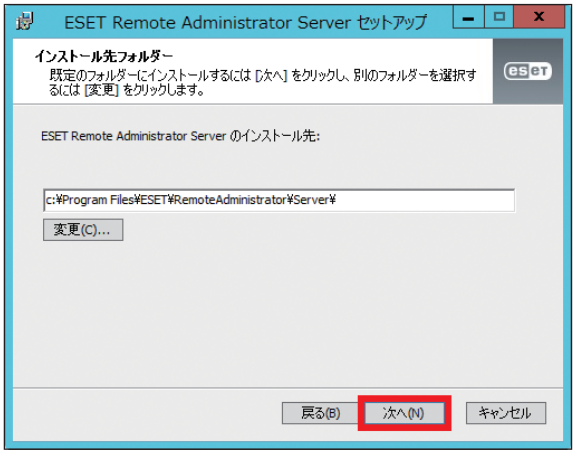
15 ［製品認証キーでアクティベーション］を選択し、テキストボックスに製品認証キーを入力します。

16 ［次へ］ボタンをクリックします。

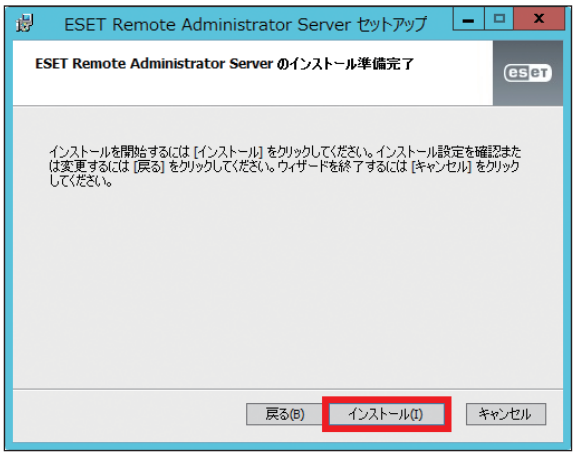


続く

⑰ インストール先フォルダーを確認し、［次へ］ボタンをクリックします。



⑱ ［インストール］ボタンをクリックします。



インストールが開始されます。

⑲ ［完了］ボタンをクリックします。

ワンポイント

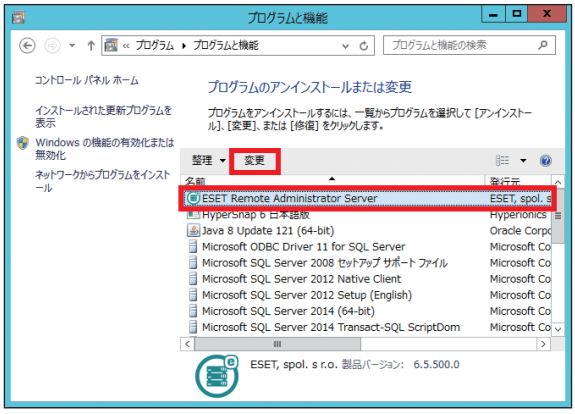
ERA サーバーインストール後、同一コンピューターに ERA エージェントをインストールすることで、クライアントコンピューターと同じ方法でサーバーコンピューターを管理することができます。

■コンポーネントの修復とアンインストール

個別にインストールしたコンポーネントの変更やアンインストールは、Windows の「プログラムと機能」から行います。

操作手順

1. スタート＞コントロールパネル＞プログラム＞「プログラムと機能」をクリックします。
2. 対象の ERA コンポーネントを選択し、［変更］ボタンをクリックします。

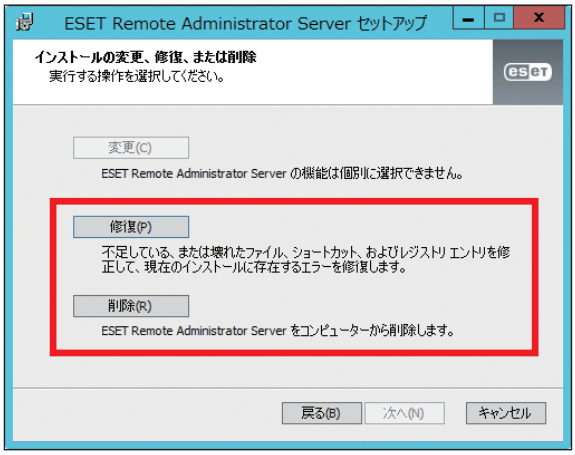


選択したコンポーネントのインストーラーが起動し、セットアップウィザードが表示されます。

3. ［次へ］ボタンをクリックします。

続く

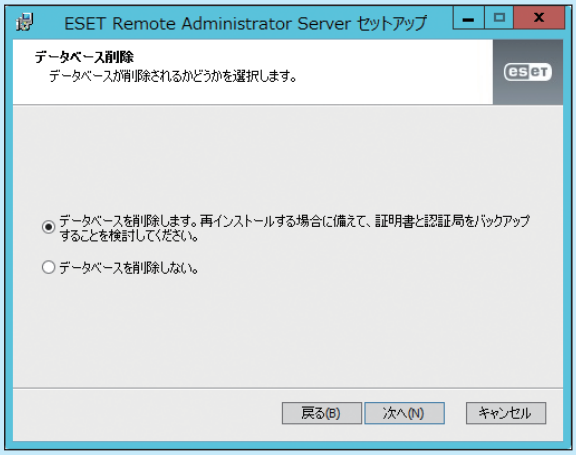
4 ［修復］ボタンまたは［削除］ボタンをクリックします。



修復または削除、それぞれの画面へ進みます。

ワンポイント

［削除］ボタンをクリックした場合は、「データベース削除」画面が表示されます。



・［データベースを削除します。再インストールする場合に備えて、証明書と証明局をバックアップすることを検討してください。］を選択した場合の証明書と証明局のバックアップ操作については、「6.9　証明書」を参照してください。
・［データベースを削除しない］を選択してアンインストールした後、ESET Remote Administrator を再インストールする際は、既存のデータベースが存在する状態でのインストールとなります。

ERA エージェント 6.3 以降ではアンインストール時にパスワード入力画面が表示されます。ERA からポリシーでパスワード保護の設定を行っている場合は、設定したパスワードを入力してください。パスワード保護の設定を行っていない場合は、何も入力せず空欄のまま次に進んでください。

3.3.3 ERA エージェントのインストール

ERA エージェントのインストールでは、ERA サーバーとの接続情報を設定します。
また ERA エージェントは、クライアントコンピューターでの実行を前提としているプログラムのため、サーバーコンピューターへのインストールは任意となっています。

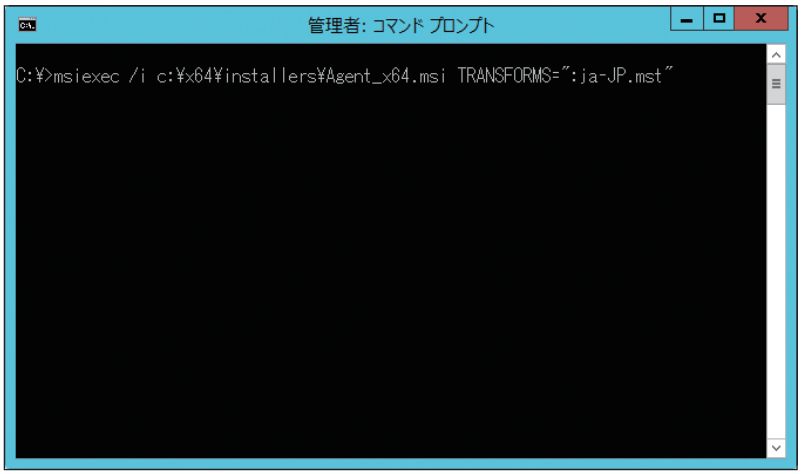
! 重 要

本マニュアルでは、ERA サーバーと同一コンピューターへインストールします。

操作手順

1 「Agent_x64.msi」を日本語表記で起動し、セットアップウィザードが表示されたら［次へ］ボタンをクリックします。32bit 版の場合は、インストーラー名が「Agent_x86.msi」となります。

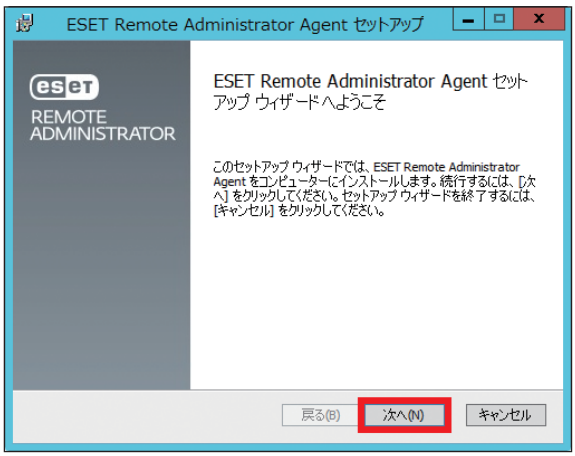
起動コマンド：C:¥>msiexec /i C:¥x64¥installers¥Agent_x64.msi TRANSFORMS=":ja-JP.mst"



ERA エージェントのセットアップウィザードが起動します。

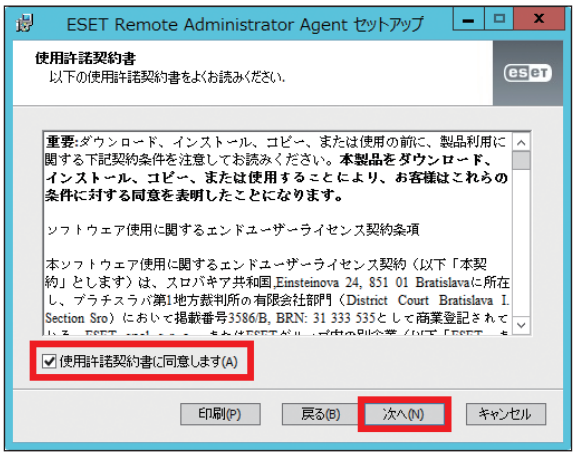
ワンポイント

インストーラーの日本語化については、「3.3 Windows 版コンポーネントインストール」の「■インストーラーの日本語化」を参照してください。



続く

2 一読して同意する場合、［使用許諾契約書に同意します］にチェックを入れ、［次へ］ボタンをクリックします。

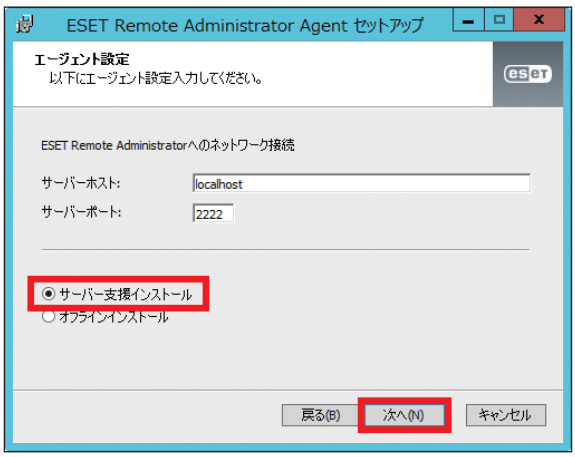


ワンポイント

チェックを外して［次へ］ボタンをクリックした場合、次の画面には進みません。

3 ［サーバー支援インストール］を選択し、［次へ］ボタンをクリックします。

「サーバー支援インストール」
Web コンソール管理者の認証情報を指定します。証明書は、インストール中に自動ダウンロードされます。
「オフラインインストール」
ESET Remote Administrator よりエクスポートした、ピア証明書（エージェント）を指定します。ピア証明書のエクスポートの操作については「6.9.1.3 ピア証明書のエクスポート」を参照してください。



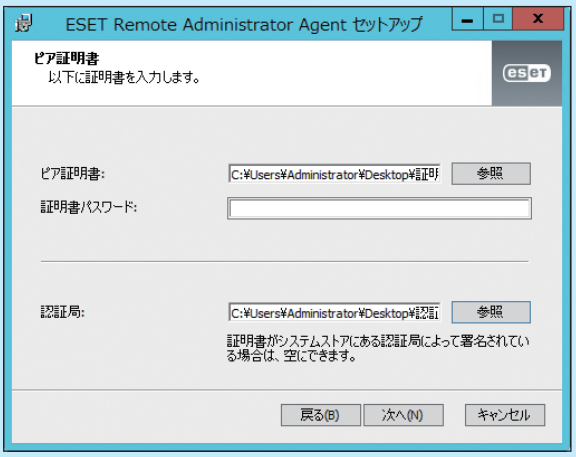
ワンポイント

「サーバーホスト :」には、サーバーの名前のほか、IP アドレスを設定できます。
ERA エージェントを、副系統（セカンダリ）サーバー、またはクライアントコンピューターへインストールする場合は、ERA サーバーが稼動している主系統（プライマリ）サーバーの名前、または IP アドレスを指定します。
既定の「サーバーポート :」は「2222」です。

続く

ワンポイント

オフラインインストールを選択した場合、ピア証明書および認証局証明書の参照を求められます。

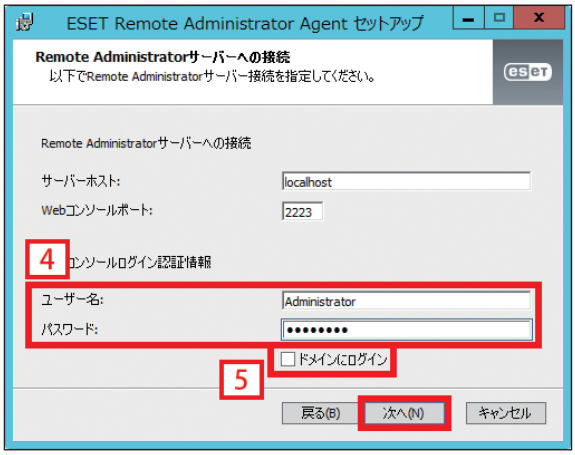


また、ピア証明書にパスワードを設定している場合は、「証明書パスワード :」の入力が必要です。
［次へ］ボタンをクリックすると、手順 7 の画面へ切り替わります。

4 ERA Web コンソールにログインするための「ユーザー名 :」と「パスワード :」を入力します。

「ユーザー名 :」「パスワード :」には、Web コンソール管理者のユーザー名と初期パスワードを入力します。

5 ［ドメインにログイン］のチェックを外し、［次へ］ボタンをクリックします。



サーバーと接続し、証明書のダウンロード準備に移ります。

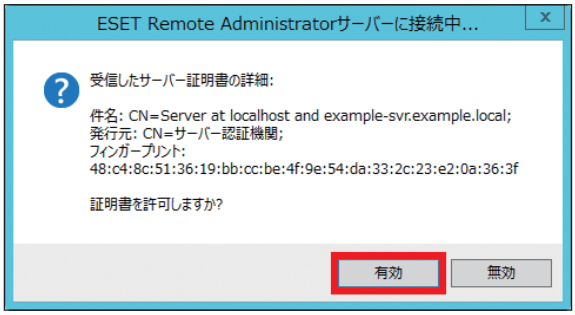
ワンポイント

「サーバーホスト :」には、サーバーの名前のほか、IP アドレスを設定できます。
ERA エージェントを、副系統（セカンダリ）サーバー、またはクライアントコンピューターへインストールする場合は、ERA サーバーが稼動している主系統（プライマリ）サーバーの名前、または IP アドレスを指定します。
既定の「Web コンソールポート :」は「2223」です。

続く

6 ［有効］ボタンをクリックします。

「3.3.2 ERA サーバーのインストール」の手順 12 ～ 15 において設定した、サーバー証明書を許可します。

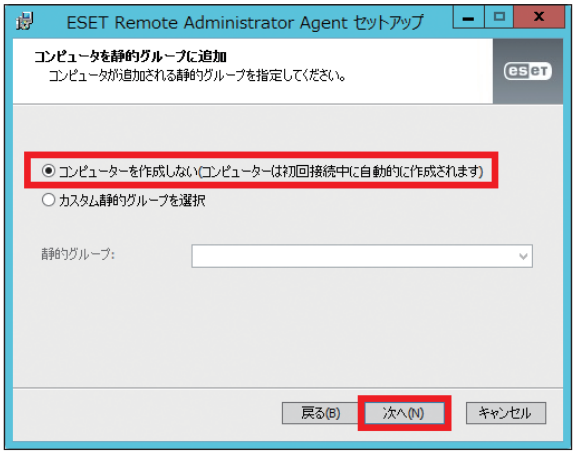


ワンポイント

手順 3 で［サーバー支援インストール］を選択したことで、Web コンソール管理者の認証証明書をダウンロードするための許可が必要となります。

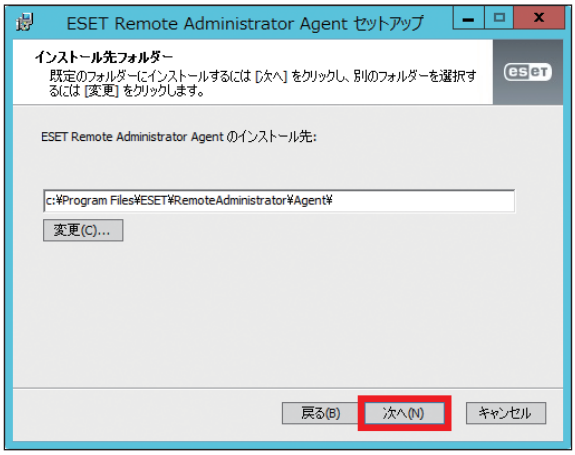
7 追加先の静的グループを選択し、［次へ］ボタンをクリックします。

静的グループへの追加方法を指定します。
「コンピューターを作成しない（コンピューターは初回接続中に自動的に作成されます）」を選択した場合は、初回接続時に最上位の静的グループへ、このコンピューターを追加します。
「カスタム静的グループを選択」を選択した場合は、「静的グループ :」から、既存の静的グループを選択します。

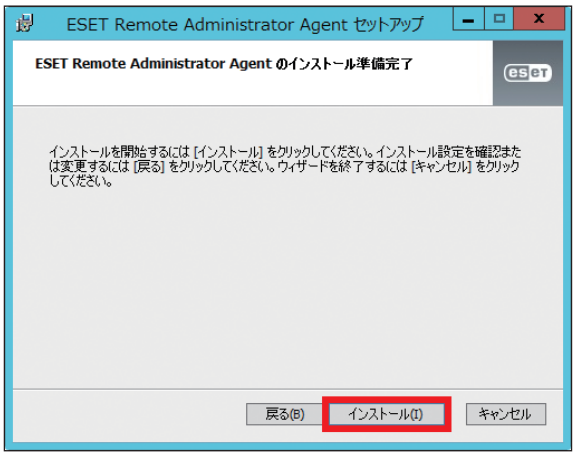


続く

8 インストール先を確認し、［次へ］ボタンをクリックします。

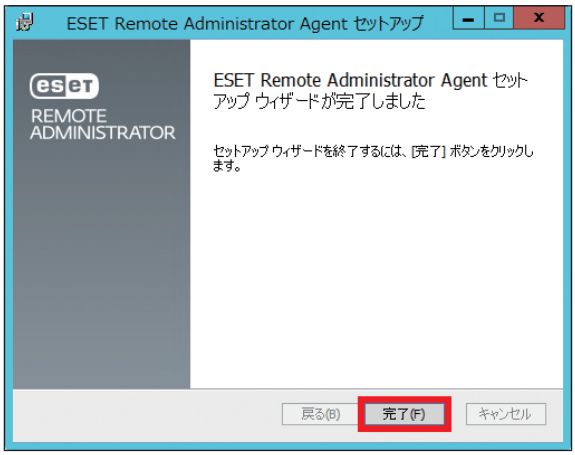


9 ［インストール］ボタンをクリックします。



ERA エージェントのインストールが開始されます。

10 ［完了］ボタンをクリックします。



3.3.4 ERA Web コンソールのインストール

ERA Web コンソールをインストールすることで、ERA サーバーのインターフェースが確立し、ブラウザー上で ESET Remote Administrator を管理することができます。

ERA Web コンソールのインストールには、次の条件が必要です。

- ERA サーバーのインストール
- Java Ver.7.0 以上のインストール、または最新版への更新
- Apache Tomcat Ver.7.0 以上のインストール

! 重　要

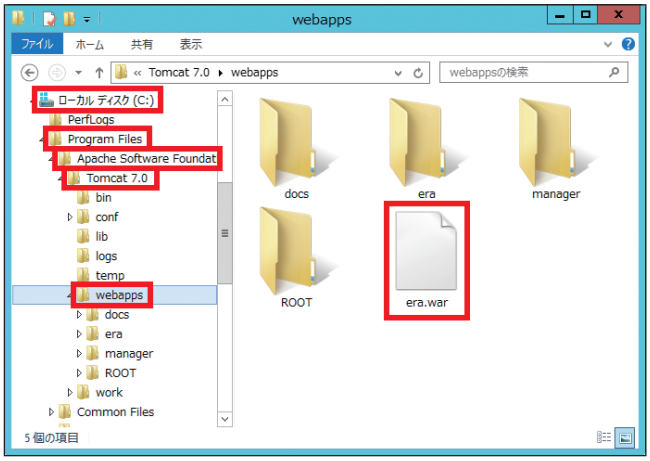
ERA Web コンソールのセキュリティ向上のために、Apache Tomcat は SSL での接続に対応する設定を行うことを強く推奨します。コンポーネントでの Web コンソールのインストールは上級者向けとなります。
Apache Tomcat の設定が不明な場合は、「3.2　Windows 版オールインワンインストール」を参照し、オールインワンインストーラーをご利用ください。

ERA Web コンソールのインストールには、「era.war」ファイルを使用します。

操作手順

1. 上記条件を満たした状態で、「era.war」ファイルを次のフォルダーに保存します。

   C:¥program files(x86)¥Apache software Foundation¥Tomcat7.0¥webapp



続く

2 ブラウザーを開き、アドレスバーに https://localhost/era/ を入力します。

ERA Web コンソール画面が表示されます。

ワンポイント

上記 URL で ERA Web コンソールに接続できない場合は、Apache Tomcat で SSL 接続に対応した設定が不足している可能性があります。その場合は、接続先を、http://localhost:8080/era/ に変更してください。

3 パスワードを入力する前に、言語選択のリストから、日本語を選択します。「3.3.2 ERA サーバーのインストール」の手順 11 で設定したパスワードを入力し［ログイン］ボタンをクリックします。

ログインできることを確認します。

ERA Web コンソールでの操作については、「6.1 ERA サーバインストール後のステータス概要の確認」を参照してください。

3.3.5 RD Sensor のインストール

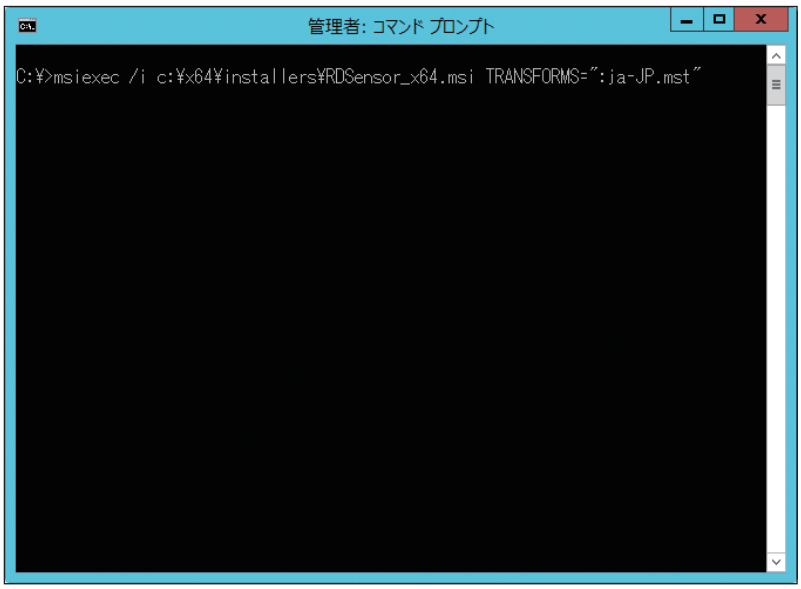
「RD Sensor」のインストールには、次の条件が必要です。

- ERA サーバーへの接続
- ERA エージェントのクライアントコンピューターへのインストール
- 「Windows Packet Capture」（以下、WinPcap）最新バージョンのインストール
- ポートに対する適切な設定

操作手順

1 「RDSensor_x64.msi」を日本語表記で起動し、セットアップウィザードが表示されたら［次へ］ボタンをクリックします。32bit 版の場合は、インストーラー名が「RDSensor_x86.msi」となります。

起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥RDSensor_x64.msi TRANSFORMS=":ja-JP.mst"`



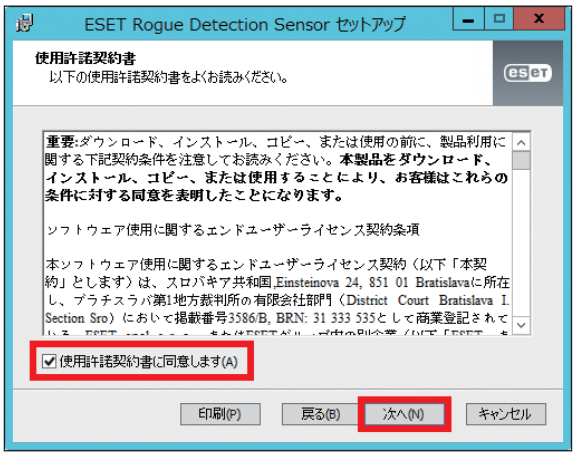
ワンポイント

インストーラーの日本語化については、「3.3 Windows 版コンポーネントインストール」の「■インストーラーの日本語化」を参照してください。

「RD Sensor」のセットアップウィザードが起動します。

続く

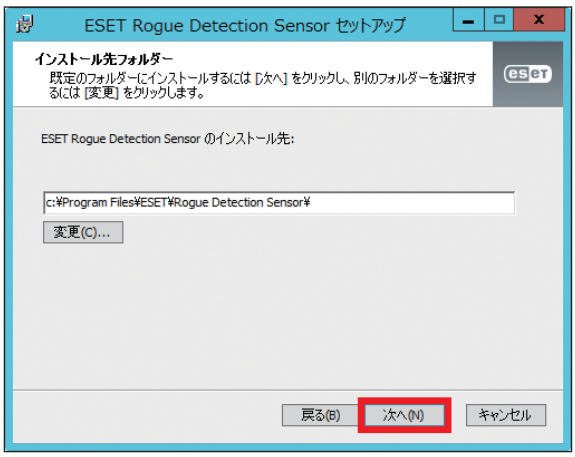
2 一読して同意する場合、［使用許諾契約書に同意します］にチェックを入れ、［次へ］ボタンをクリックします。



ワンポイント

チェックを外して［次へ］ボタンをクリックした場合、次の画面には進みません。

3 「インストール先フォルダー」を確認し、［次へ］ボタンをクリックします。



4 ［インストール］ボタンをクリックします。

続く

5 [完了] ボタンをクリックします。

「RD Sensor」のインストールは終了です。

3.3.6 ERA プロキシのインストール

ERA プロキシのインストールには、次の条件が必要です。

- SQL Server が構成済みであること
- ERA サーバーと ERA Web コンソールのサーバーコンピューター上へのインストール
- ERA エージェントのローカルコンピューター上へのインストール
- ピア証明書（プロキシ）の作成とローカルコンピューターへの保存
- 有効なライセンスがあること
- 認証局が作成されていて、公開鍵がローカルコンピューターへ保存されている

ワンポイント

ERA プロキシのインストールでは、証明書の自動ダウンロードである、サーバー支援インストールはサポートされていないため、事前にピア証明書（プロキシ）と認証局の公開鍵のエクスポートが必要です。操作については、「6.9 証明書」を参照してください。

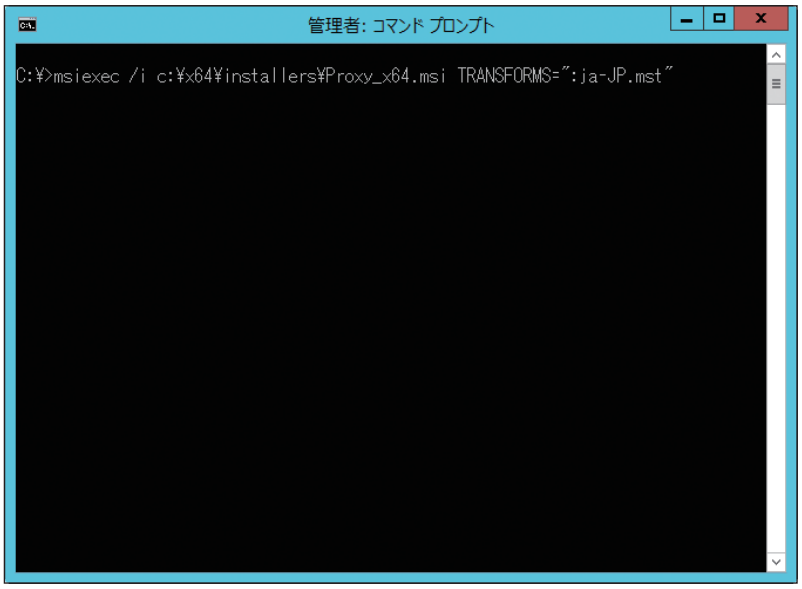
！重 要

複数サーバーで構成している環境の場合、ERA プロキシは、副系統（セカンダリ）サーバーへインストールします。本マニュアルでは、ERA サーバーと同一のサーバーコンピューターへインストールする操作を説明します。

操作手順

1. 「Proxy_x64.msi」を日本語表記で起動し、セットアップウィザードが表示されたら［次へ］ボタンをクリックします。32bit 版の場合は、インストーラー名が「Proxy_x86.msi」となります。

   起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥Proxy_x64.msi TRANSFORMS=":ja-JP.mst"`

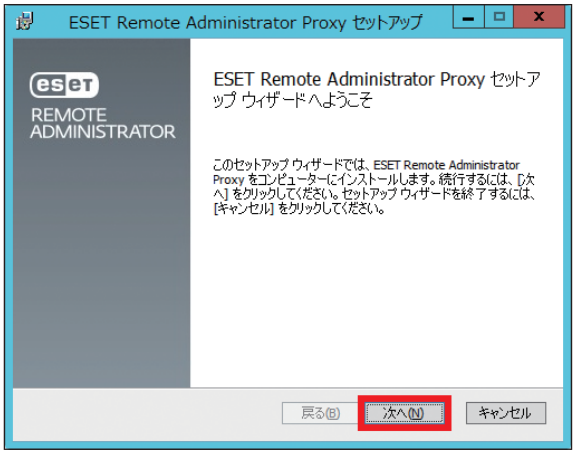


ワンポイント

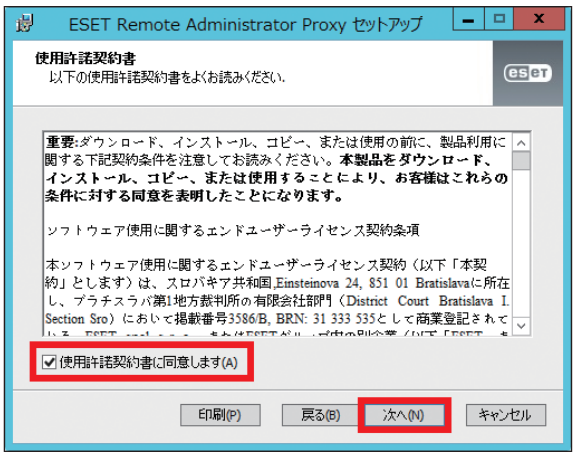
インストーラーの日本語化については、「3.3 Windows 版コンポーネントインストール」の「■インストーラーの日本語化」を参照してください。

続く

「ERA プロキシ」のセットアップウィザードが起動します。



2 一読して同意する場合、［使用許諾契約書に同意します］にチェックを入れ、［次へ］ボタンをクリックします。

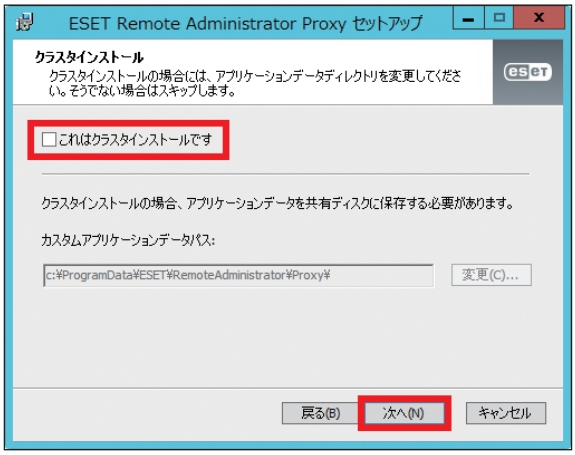


ワンポイント

チェックを外して［次へ］ボタンをクリックした場合、次の画面には進みません。

続く

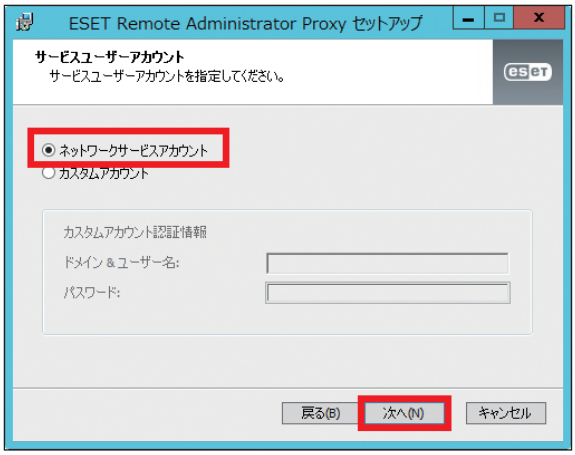
3 ［これはクラスタインストールです］のチェックを外し、［次へ］ボタンをクリックします。



ワンポイント

フェールオーバー環境へのインストールの場合は、「これはクラスタインストールです」にチェックを入れ、「カスタムアプリケーションデータパス」には、クラスタ内のすべてのコンピューターが接続できる共有の場所を指定します。フェールオーバー環境へのインストールについては、「3.3.9　フェールオーバー環境へのインストール」を参照してください。

4 ［ネットワークサービスアカウント］を選択し、［次へ］ボタンをクリックします。



ワンポイント

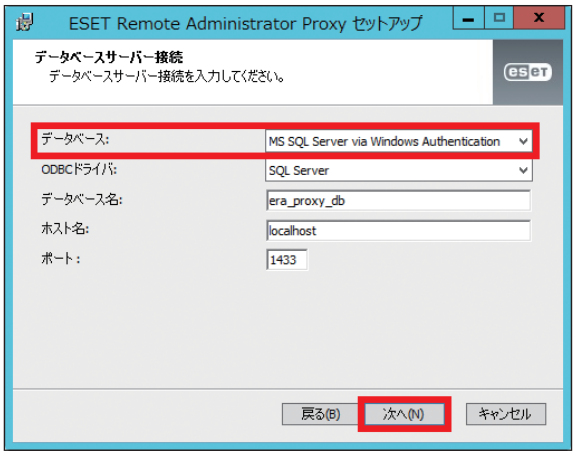
ネットワークサービス以外の Windows アカウントを利用する場合は、「カスタムアカウント」を選択し、「カスタムアカウント認証情報」である、「ドメイン & ユーザー名 :」および「パスワード」を設定します。

続く

5 「データベース :」から、[MS SQL Server via Windows Authentication] を選択し、[次へ] ボタンをクリックします。

Windows 認証経由で、SQL Server への接続設定を行います。

データベース	MySQL Server/MS SQL Server/Windows 認証による MySQL Server から選択
ODBC ドライバ	MySQL ODBC5.1Driver/MySQL ODBC5.2 Unicode Driver/MySQL ODBC5.3 Unicode Driver/SQL Server/SQL Server Native Client10.0/ODBC Driver 11 for SQL Server から選択します。
データベース名	既定の「era_proxy_db」が入力されています。変更可能です。
ホスト名	サーバーコンピューターのホスト名または IP アドレスを入力します。
ポート	既定値「1433」が入力されています。サーバー接続に使用するポート番号を入力します。



接続が確認されると、次の画面に切り替わります。

ワンポイント

接続されるデータベースに、ERA プロキシのデータ（パスワードやログなど）が蓄積されます。

続く

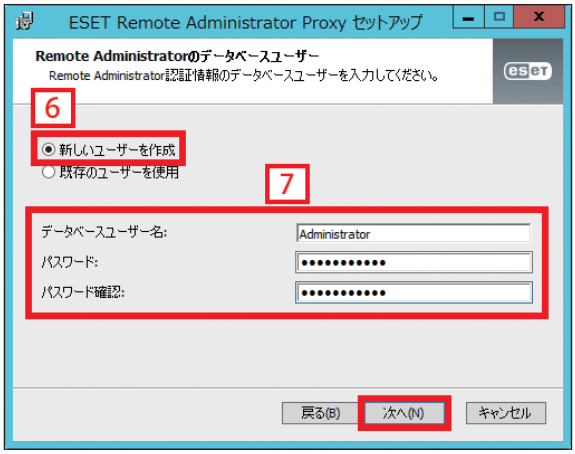
6 データベースユーザーを設定します。任意のユーザーデータベースを選択します。

ワンポイント

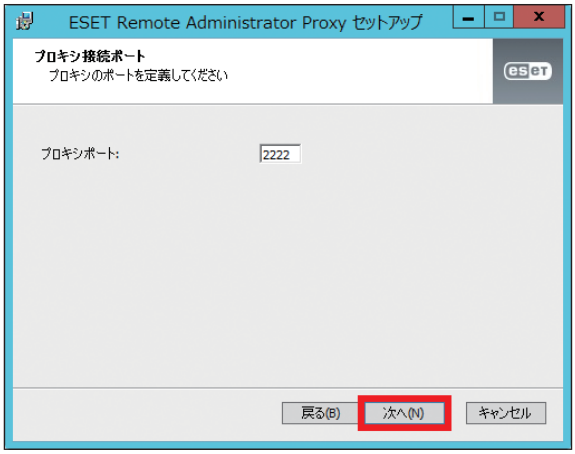
既存のデータベースユーザーを使用する場合は、「既存のユーザーを使用」を選択し、「データベースユーザー名 :」および「パスワード :」を入力してください。

7 「データベースユーザー名 :」、「パスワード :」および「パスワード確認」を入力し、［次へ］ボタンをクリックします。

データベース管理者のユーザー名とパスワードを入力します。



8 プロキシ接続ポートを確認し、［次へ］ボタンをクリックします。

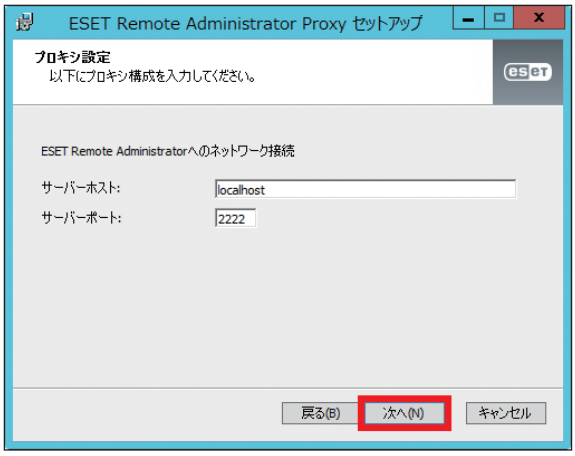


続く

9 「サーバーホスト :」と「サーバーポート :」を確認し、［次へ］ボタンをクリックします。

! 重 要

「サーバーホスト :」のホスト名が、「3.3.2 ERA サーバーのインストール」の手順 14 で設定した、サーバー証明書の「サーバーホスト名 :」の値と一致していることを確認します。
一致していない場合は、「受信したサーバー証明書が無効です」というエラーが表示されます。

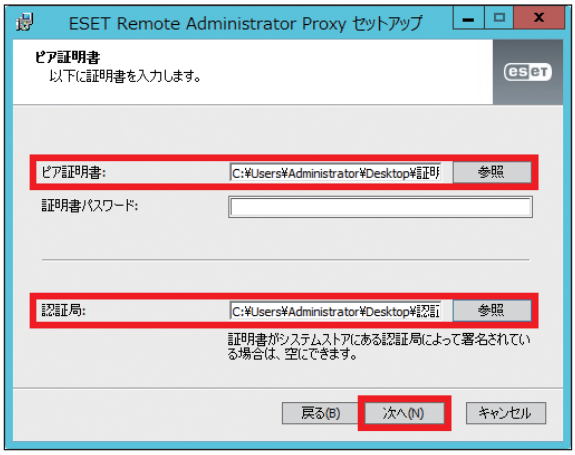


ワンポイント

「サーバーホスト :」には、サーバーの名前または IP アドレスを設定できます。
また、複数サーバーで構成している環境において、ERA プロキシを、副系統（セカンダリ）サーバー、またはクライアントコンピューターへインストールする場合は、ERA サーバーが稼動している主系統（プライマリ）サーバーの名前、または IP アドレスを指定します。
既定の「サーバーポート :」は「2222」です。

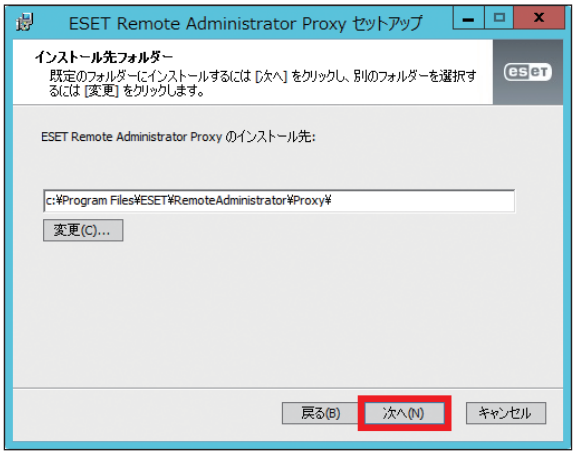
10 「ピア証明書 :」および「認証局 :」に、保存したピア証明書と認証局の公開鍵を参照設定し、［次へ］ボタンをクリックします。

ピア証明書と認証局の参照設定は、必須の項目です。
「証明書パスワード :」は、ピア証明書のパスワードを入力します。
パスワードを設定していない場合、入力は不要です。



続く

⓫ インストール先フォルダーを確認し、［次へ］ボタンをクリックします。



⓬ ［インストール］ボタンをクリックします。

インストールが開始されます。

⓭ ［完了］ボタンをクリックします。

インストールが終了します。

3.3.7 Apache HTTP プロキシのインストール

Apache HTTP プロキシは、キャッシュプロキシサーバーとして使用できます。Apache HTTP プロキシをインストールすることで、以下を実行します。

- 最新のウイルス定義データベースのキャッシュ
- 製品コンポーネントのアップデートファイルのキャッシュ
- ネットワーク上のインターネットトラフィックの最小化

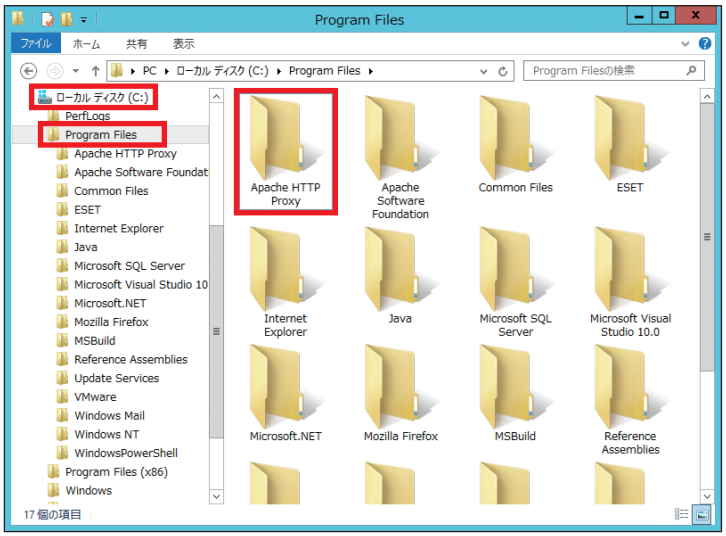
! 重 要

社内で構築したミラーサーバーからウイルス定義データベースをアップデートする場合や、社内のプロキシサーバーを利用してインターネットに接続する場合は、Apache HTTP プロキシのインストールは不要です。また、Apache HTTP プロキシをコンポーネントとしてインストールした場合、Apache HTTP プロキシをプロキシサーバーとして利用するように、ESET 製品の設定を変更する必要があります。

操作手順

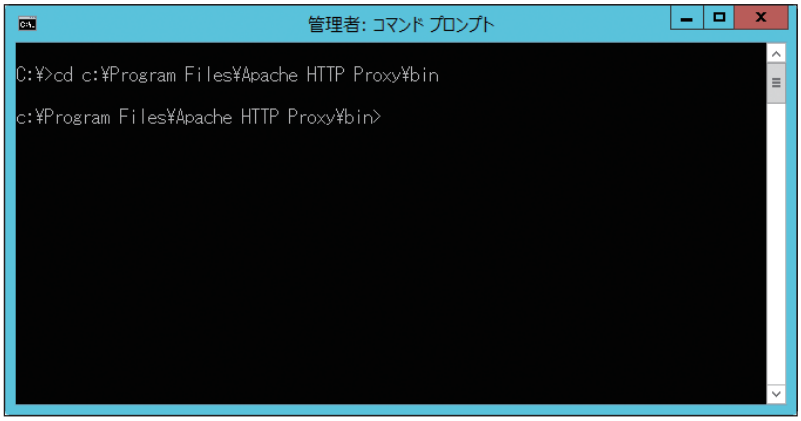
1. 「ApacheHttp.zip」を任意の場所に展開し、展開したフォルダーの名前を「Apache HTTP Proxy」に変更します。

2. 「Apache HTTP Proxy」フォルダーを、C:¥Program Files¥ へ保存します。



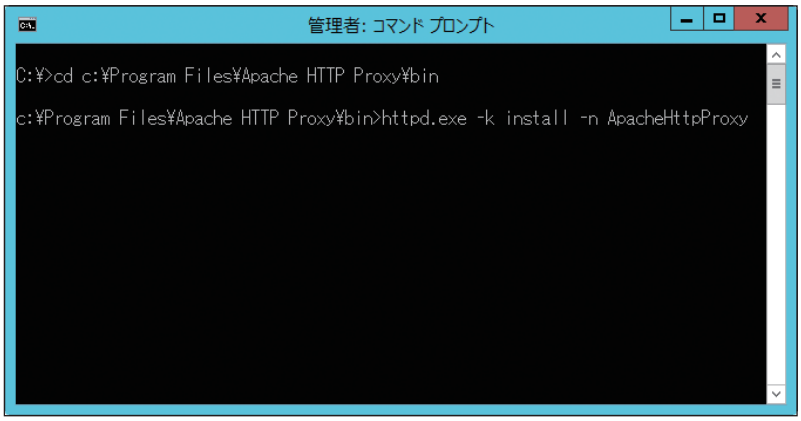
続く

3 コマンドプロンプト画面を開き、カレントフォルダーを C:¥Program Files¥Apache HTTP Proxy¥bin に変更します。

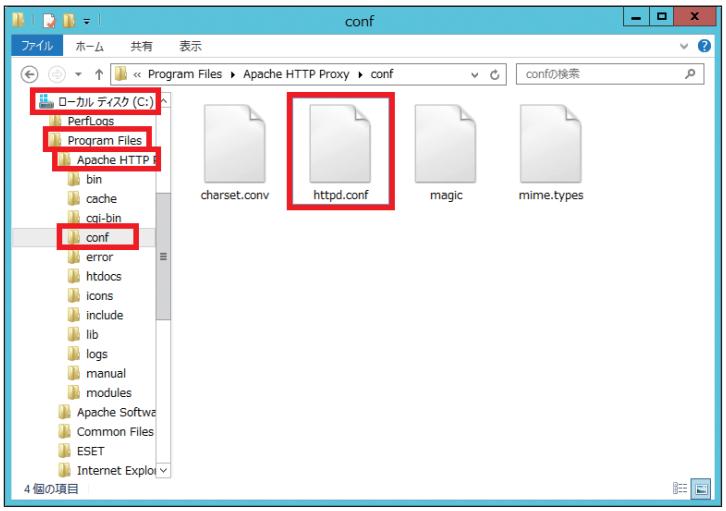


4 「Apache HTTP Proxy」をインストールします。

コマンド：`httpd.exe -k install -n ApacheHttpProxy`



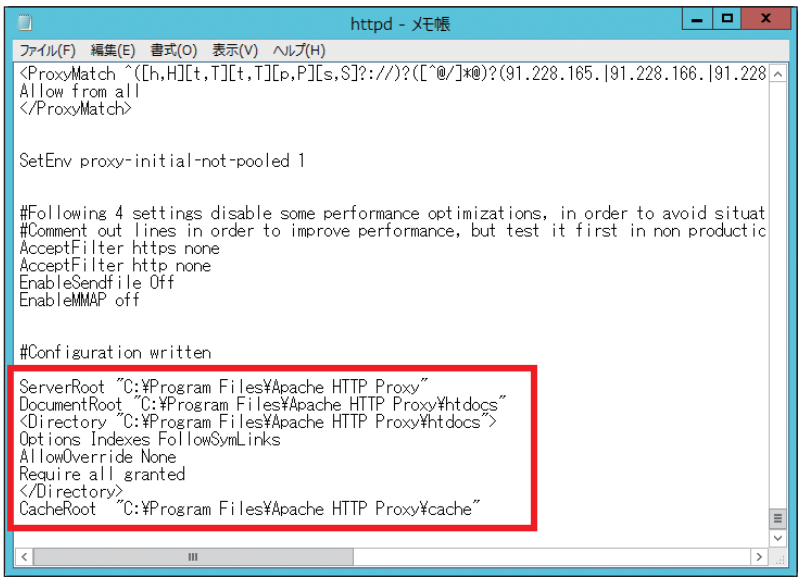
5 C:¥Program Files¥Apache HTTP Proxy¥conf に保存されている「httpd.conf」ファイルをメモ帳で開きます。



続く

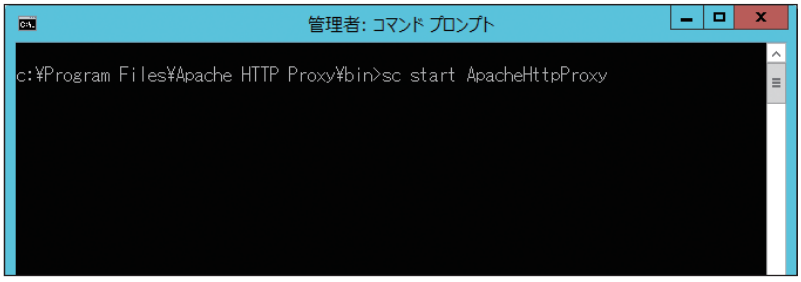
6 開いた「httpd.conf」ファイルの末尾に次の行を追加し、上書き保存をします。

```
ServerRoot "C:¥Program Files¥Apache HTTP Proxy"
DocumentRoot "C:¥Program Files¥Apache HTTP Proxy¥htdocs"
<Directory "C:¥Program Files¥Apache HTTP Proxy¥htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:¥Program Files¥Apache HTTP Proxy¥cache"
```



7 コマンドプロンプトで、「Apache Http Proxy」のサービスを開始します。

コマンド：`sc start ApacheHttpProxy`

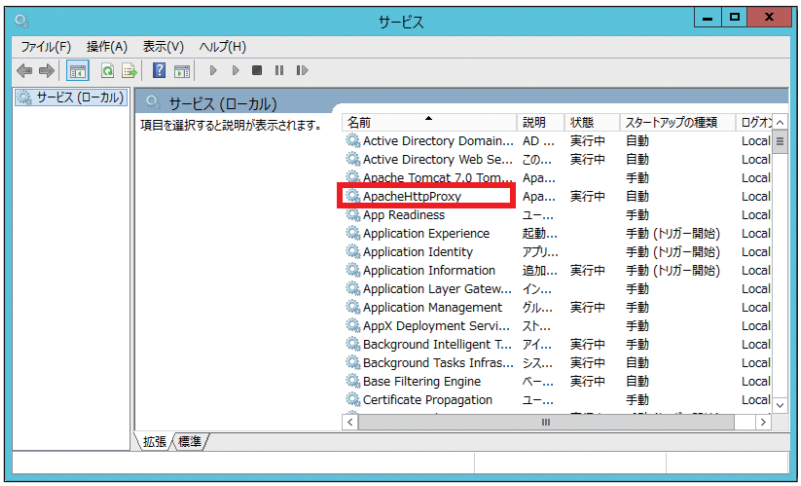


以上で、Apache HTTP プロキシのインストールは終了です。

ワンポイント

インストール後、Apache HTTP プロキシのサービスは自動で起動します。

管理ツール「サービス」で、状態を確認することができます。



3.3.8 Mobile Device Connector のインストール

Mobile Device Connector は、ERA サーバーが実行されているサーバーとは別のサーバーにインストールすることもできます。例えば、インターネットから Mobile Device Connector をインストールしたサーバーにアクセスできるようにすると、場所に関係なく、ユーザーのモバイルデバイスを常時管理できます。

! 重　要

このインストール方法は、すでに ERA サーバーがインストールされているサーバーに Mobile Device Connector を追加でインストールする場合に適しています。ERA サーバーとは別のサーバーに Mobile Device Connector をインストールする場合は「3.2.3　Mobile Device Connector 一括インストール」を参照してください。

Mobile Device Connector のインストールには、次の条件が必要です。

- Mobile Deviece Connector と Android デバイスなどのモバイルデバイスや ERA サーバー、Apple Push Notification との間で通信に利用する次のポートが開いていて使用可能であること。

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

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

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

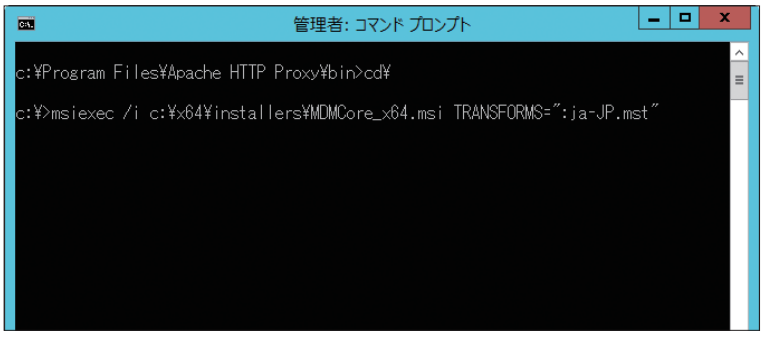
プロトコル	Apple Push Notification サービスへの通信で使用するポート	説明
TCP	5223	インターネット（Apple Push Notification サービス）への通信
TCP	2195	Mobile Device Connector からインターネット（Apple Push Notification サービス）への通信
TCP	2196	Mobile Device Connector からインターネット（Apple Push Notification サービスのフィードバックサービス）への通信
TCP	443	デバイスがポート 5223 でインターネット（Apple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

- Java Runtime Environment (JRE) がインストールされ、常に最新の公式リリースされた Java バージョンを使用していること。
- Microsoft .NET Framework 3.5 がインストールされていること。

操作手順

1. 「MDMCore_x64.msi」を日本語表記で起動し、セットアップウィザードが表示されたら［次へ］ボタンをクリックします。32bit 版の場合は、インストーラー名が「MDMCore_x86.msi」となります。

起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥MDMCore_x64.msi TRANSFORMS=":ja-JP.mst"`



ワンポイント

インストーラーの日本語化については、「3.3 Windows 版コンポーネントインストール」の「■インストーラーの日本語化」を参照してください。

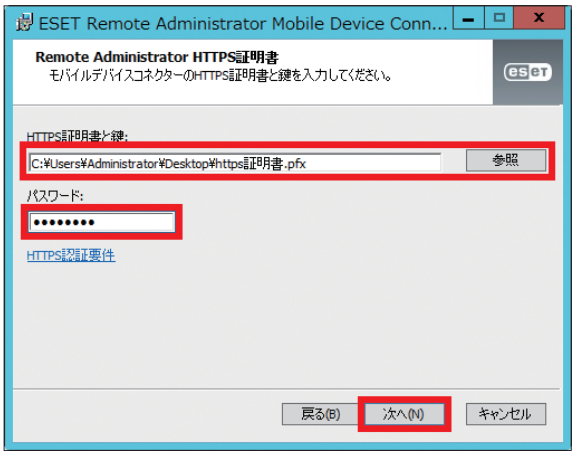
続く

「Mobile Device Connector」のセットアップウィザードが起動します。

2 一読して同意する場合、［使用許諾契約書に同意します］にチェックを入れ、［次へ］ボタンをクリックします。

続く

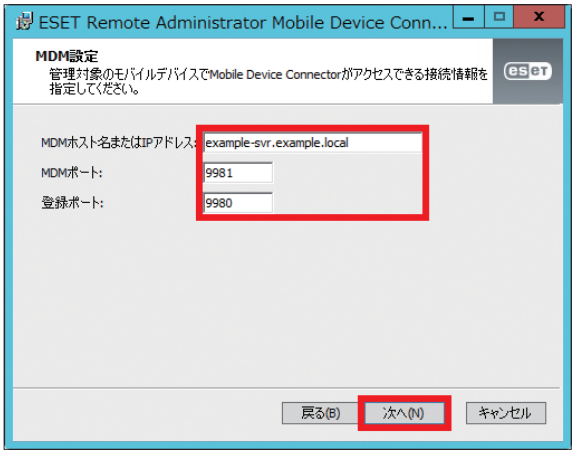
3 ［参照］をクリックして、HTTPS 証明書と鍵、必要に応じてパスワードを入力し、［次へ］ボタンをクリックします。



! 重　要

pfx 形式の HTTPS 証明書（SSL 証明書）が必要です。ERA サーバーで作成したピア証明書（モバイルデバイスコネクター）を使用できます。自己署名証明書の使用許可ができないモバイルデバイスを使用する場合は、信頼できる第三者機関（認証局）が発行する証明書を使用してください。
参照する HTTPS 証明書の CommonName または subjectAltName は、MDM ホスト名と一致する必要があります。Web コンソールのピア証明書（作成する場合は、作成画面の項目「ホスト」「共通名」と MDM ホスト名が一致するようにします。詳しくは「6.9.1.2　新しい証明書の作成」を参照してください。

4 Mobile Device Connector をインストールするサーバーのホスト名または IP アドレスを入力して、［次へ］ボタンをクリックします。



! 重　要

MDM ホスト名にサーバーのホスト名を入力する場合は、接続するモバイルデバイスが入力したホスト名の名前解決を行える必要があります。

続く

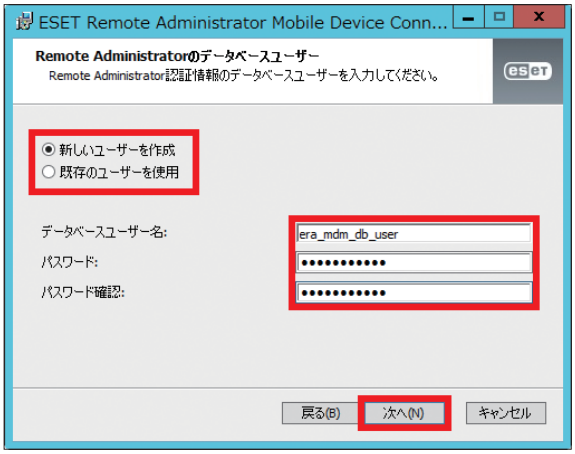
5 Mobile Device Connector が使用する新しいデータベースを作成します。次の接続詳細情報を指定し、[次へ] ボタンをクリックすると、Mobile Device Connector インストーラがデータベースを作成します。

- データベース：Windows 認証による MySQL Server/MS SQL Server/MS SQL Server
- ODBC ドライバ：MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server
- データベース名 : 定義済みの名前を使用するか、必要に応じて変更できます。
- ホスト名 : ホスト名またはデータベースサーバーの IP アドレス
- ポート : データベースとの接続で使用されます。
- データベース管理者アカウントのユーザー名 / パスワード

ワンポイント

作成するデータベースは、ERA データベースで使用するものと同じデータベースサーバーを指定することをお勧めしますが、必要に応じて別のデータベースサーバーを使用できます。

6 新しく作成された Mobile Device Connector 用のデータベースのユーザーを設定します。新しいユーザーを作成するか、既存のデータベースユーザーを使用できます。データベースユーザー名やパスワードを入力して、［次へ］ボタンをクリックします。



続く

7 サーバーホストに ERA サーバーの名前または IP アドレスを入力し、接続方法を以下の 2 種類から選択して、［次へ］ボタンをクリックします。ここでは、［サーバー支援インストール］を選択して、［次へ］をクリックします。

- サーバー支援インストール
  サーバー支援インストールは、ERA Web コンソール管理者の認証情報を指定する必要があります。インストールに必要な証明書はインストーラによって自動的にダウンロードされます。

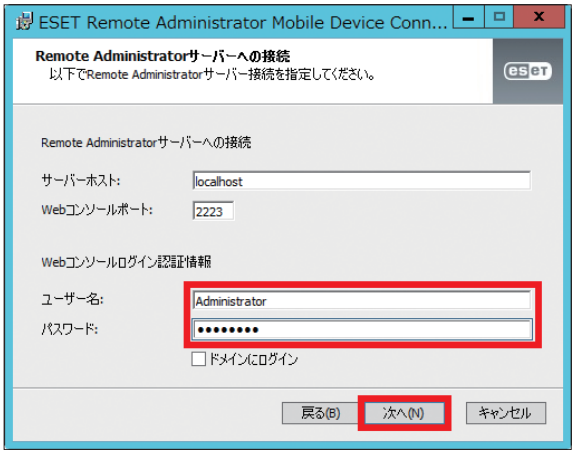
- オフラインインストール
  オフラインインストールでは、ERA Web コンソールからエクスポートしたピア証明書（プロキシ）を指定する必要があります。ピア証明書のエクスポートの操作については、「6.9.1.3　ピア証明書のエクスポート」を参照してください。

ワンポイント

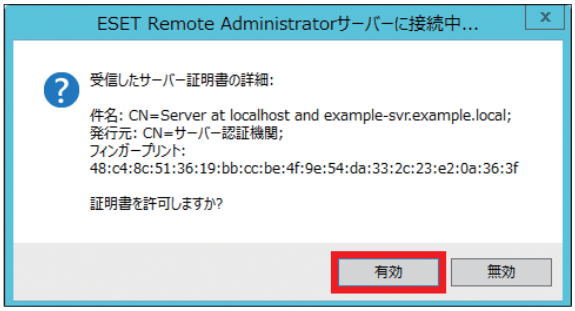
手順 7 でオフラインインストールを選択した場合は、ERA Web コンソールで作成したカスタム証明書も使用でき、次の画面でピア証明書および認証局証明書の参照を求められます。［参照］ボタンをクリックして、あらかじめ用意しておいた証明書の指定を行ってください。なお、ピア証明書にパスワードを設定している場合は、証明書パスワードの設定も必要になります。証明書の指定を行ったら、［次へ］ボタンをクリックして手順 10 に進んでください。

続く

8 Web コンソール管理者認証情報 (ユーザー名 / パスワード) を指定し、[次へ] ボタンをクリックします。



9 [有効] ボタンをクリックして、ダウンロードした証明書の利用を許可します。



10 インストール先フォルダーを確認して [次へ] ボタンをクリックします。

続く

⑪［インストール］ボタンをクリックすると、Mobile Device Connector のインストールが開始されます。

⑫インストールが完了したら［完了］ボタンをクリックしてインストーラーを終了します。Web ブラウザーで Mobile Device Connector が実行中かどうかを確認します。実行中の場合は、以下の画面が表示されます。

URL：https://hostname(IP アドレス）:9980

！重　要

Web コンソールのピア証明書で作成した HTTPS 証明書を使用してインストールした場合や、アラートで「HTTP 証明書チェーンが不完全です。登録は許可されていません」と出る場合は、Windows サーバーの中間認証局ストアに HTTPS 証明書をインポートする必要があります。詳しくは「4.3　モバイルデバイスの展開 - ● Mobile Device Connector の HTTPS 証明書チェーンのインストール手順」を参照してください。

ワンポイント

Web ページを表示できない場合は、ファイアウォールとネットワークの構成を確認してください。

3.3.9 フェールオーバー環境へのインストール

ESET Remote Administrator は、フェールオーバー環境において稼動することが可能です。
フェールオーバー環境へは、コンポーネントインストールを行ってください。
オールインワンインストーラーはフェールオーバー環境には未対応となっています。

フェールオーバー環境へインストールする場合は、事前にサーバーコンピューター上でのフェールオーバークラスタの作成が必要です。

操作手順

1. サーバーコンピューター上で、フェールオーバークラスタを作成します。

! 重 要

Windows Server2012、または Windows Server2008 上で、フェールオーバークラスタを作成する操作については、Microsoft のサポートページを参照してください。

- Windows Server2012　フェールオーバークラスタの作成
- Windows Server2008　フェールオーバークラスタの作成

2. サーバーコンピューターに、ERA サーバー、ERA エージェントをインストールします。

   共有ドライブには、アプリケーションデータが保存されているドライブを指定してください。

3. クラスタリングを構成している他のサーバーコンピューターにも、ERA サーバー、ERA エージェントをインストールします。

4. クラスタ構成マネージャーを起動し、ERA サーバー、ERA エージェントのクラスタサービスを作成します。

   サービスが起動します。

5. 該当する依存関係を設定します。

6. 手順 1 で作成したクラスタを初期化します。

ワンポイント

ERA エージェントは、ERA サーバーに依存します。

! 重 要

フェールオーバー環境において、ERA サーバーのデータベースと Web サーバー（Web コンソール）は、サポート対象ではありません。

3.4 Linux 版　コンポーネントインストール

ESET Remote Administrator の Linux OS へのインストールは、システム環境や使用状況を考慮し、各コンポーネントをカスタマイズしながらインストールする必要があります。

3.4.1 インストール概要

Linux OS へのインストールは、サーバーコンピューター上で稼動している Linux のディストリビューションによって、手順と入力コマンドが異なります。
現在使用している Linux のディストリビューションを確認し、対応する操作を行ってください。

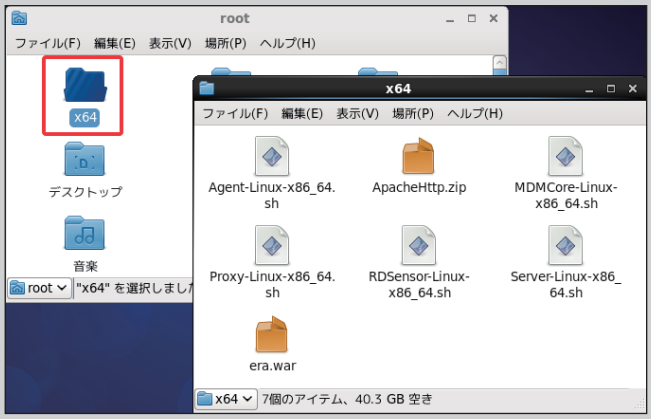
! 重　要

本マニュアルで対応している Linux ディストリビューションは、次の 3 種類です。
- CentOS
- Red Hat Enterprise Linux（以下 RHEL）
- SUSE Linux Enterprise（以下 SUSE Linux）

さらに各コンポーネントのインストーラーが正しく接続できるよう、事前にデータベースサーバーと ODBC ドライバーのインストールと設定を行ってください。
操作は、sudo コマンドで許可されたユーザー権限、もしくは Linux の管理者（root）権限で実行します。

! 重　要

本マニュアルでの操作は、Linux の管理者権限である root を使って操作を行います。
使用するデータベースサーバーは MySQL です。
ESET Remote Administrator のインストールでの必要な設定は、「3.4.2　CentOS/RHEL での準備」または「3.4.3　SUSE Linux での準備」を参照してください。
また、ダウンロードした各コンポーネントのインストーラーを、/root/x64 フォルダーに保存した状態で説明します。
x64 フォルダーは、手動で作成してください。



■事前準備と手順の確認

●事前準備

＜ディストリビューション共通＞

- ESET Remote Administrator の、必須パッケージを確認しインストールしてください。
- 必須プログラムである JAVA および Tomcat を、別途インストールしてください。
- 各コンポーネントのインストーラーファイルには、実行権限の付与を行ってください。
- ESET Remote Administrator に対応した MySQL と MySQL 用の ODBC ドライバーをインストールしてください。

! 重 要

Java は Standard Edition 7 以上に対応しています。また、ESET Remote Administrator では、最新版への更新を推奨しています。
Tomcat は、Ver.6.0 以上に対応しています。
MySQL は、Ver5.5 および Ver5.6、ODBC ドライバー 5.3 以上に対応しています。

＜ SUSE Linux ＞

- パッケージリポジトリに unixODBC_23 が含まれる状態にして、unixODBC_23 を使用してください。

! 重 要

SELinux が有効（enforcing モード）である場合、/etc/selinux フォルダーの config ファイルを開き、次の行を修正します。
変更前：SELINUX=enforcing
↓
変更後：SELINUX=disabled
修正後、サーバーを再起動してください。

●インストールの手順

データベースサーバーの準備から、ESET Remote Administrator への初回ログインまでのインストール手順を確認します。

手順	内容	参照章	
		CentOS/RHEL	SUSE Linux
1	MySQL の設定	「3.4.2.1 MySQL」	「3.4.3.1 MySQL」
2	ODBC の設定	「3.4.2.2 MySQL ODBC」	「3.4.3.2 MySQL ODBC」
3	ERA サーバー必須パッケージのインストール	「3.4.4 ERA サーバーのインストール」の「■必要パッケージとインストールコマンド」	
4	ダウンロードした ERA サーバーインストーラーの root/x64 フォルダーへの保存	参照ページなし	
5	ERA サーバーのインストール	「3.4.4 ERA サーバーのインストール」	
6	ERA Web コンソールのインストール	「3.4.5 ERA Web コンソールのインストール」	
7	ERA Web コンソールの接続確認	「3.4.5 ERA Web コンソールのインストール」手順 4 ～ 7	

3.4.2　CentOS/RHEL での準備

3.4.2.1　MySQL

MySQL のインストール後に、設定ファイルの変更を行います。さらに、MySQL の管理者パスワードを設定します。

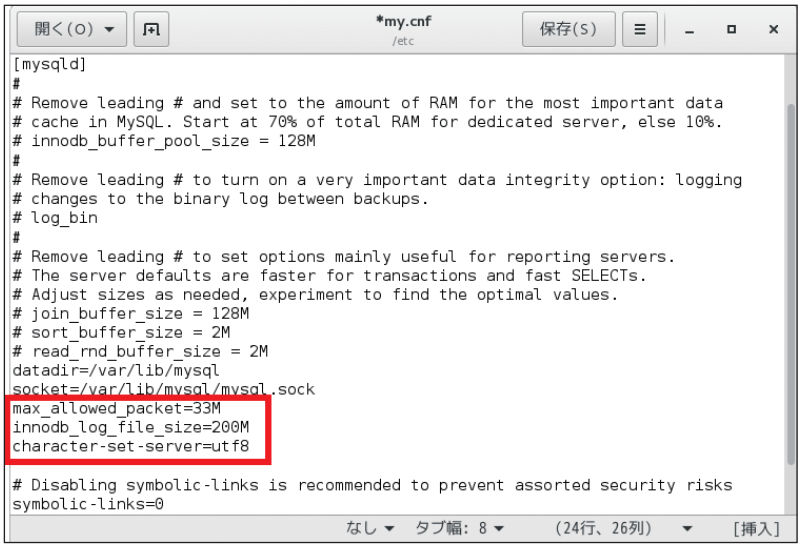
■データベースの設定

操作手順

1. MySQL をインストールします。
2. 続けて、データベースの追加オプションを my.cnf に設定します。

［mysqld］以下に次の行を追加し、上書き保存した後ファイルを閉じます。

```
max_allowed_packet=33M
innodb_log_file_size=200M
character-set-server=utf8
```



! 重　要

my.cnf ファイルは使用環境によって、/etc/mysql フォルダーまたは /etc フォルダーのどちらかに保存されています。手順 2 を実行する前にファイルの保存場所を確認してください。

ワンポイント

ESET Remote Administrator は、大きな BLOB 形式のデータをデータベースに格納します。そのため、大容量のパケットを受け入れられるように MySQL のパケットサイズを設定する必要があります。

続く

3 mysqld を起動します。

CentOS/RHEL6 の場合
コマンド：`/etc/init.d/mysqld start`
CentOS/RHEL7 の場合
コマンド：`systemctl start mysqld`

■管理者パスワードの設定

MySQL に接続し、データベース管理者（root）に対してパスワードを設定します。

1 MySQL のコンソール画面に接続します。

コマンド：`mysql -u root --host 127.0.0.1`
プロンプトが mysql> となり、MySQL のコンソールに入ります。

2 mysql データベースを指定します。

コマンド：`use mysql;`

3 root に対して、パスワードを設定します。

コマンド：`update user set password=PASSWORD("XXXXXXX") where User='root';`

!重 要

ここで設定した MySQL の管理者パスワードは、ERA サーバーおよび ERA プロキシのインストールの際に必要となります。

4 変更を更新し、MySQL コンソール画面を閉じます。

コマンド：`quit`

5 mysql を再起動します。

CentOS/RHEL6 の場合
コマンド：`/etc/init.d/mysqld restart`
CentOS/RHEL7 の場合
コマンド：`systemctl restart mysqld`

6 service もしくは systemctl コマンドを使用して、MySQL の稼動確認をします。

ワンポイント

MySQL に再接続する場合は、設定したパスワードを入力します。
コマンド：`mysql -u root --host 127.0.0.1 -p`
設定したパスワードを入力すると、MySQL のコンソール画面に接続します。

!重 要

サーバーリブート後も MySQL が自動的に起動するように設定してください。

3.4.2.2 MySQL ODBC

MySQL ODBC ドライバーのインストール後に設定ファイルを変更します。

操作手順

1. MySQL ODBC ドライバー（mysql-connector-odbc Ver.5.3 以上）をインストールします。
2. /etc フォルダーにある odbcinst.ini ファイルをテキストエディターで開き「MySQL」以下の行を、次の内容へ変更します。

```
Description =ODBC for MySQL
Driver      =/usr/lib64/libmyodbc5w.so
Setup       =/usr/lib64/libmyodbc5w.so
Threading   =0
FileUsage   =1
```

3. odbcinst.ini ファイルを上書き保存し、ファイルを閉じます。

3.4.3 SUSE Linux での準備

3.4.3.1 MySQL

MySQL のインストール後に、my.cnf ファイルを新規作成します。さらに、MySQL の管理者パスワードを設定します。

ワンポイント

ESET Remote Administrator は、大きな BLOB 形式のデータをデータベースに格納します。そのため、大容量のパケットを受け入れられるように MySQL のパケットサイズを設定する必要があります。

操作手順

■ my.cnf ファイルの作成

1. MySQL をインストールします。
2. テキストエディターを開き、以下のように内容を変更します。

```
# For advice on how to change settings please see
# http://dev.mysql.com/doc/refman/5.6/en/server-configuration-defaults.html

[mysqld]
#
# Remove leading # and set to the amount of RAM for the most important data
# cache in MySQL. Start at 70% of total RAM for dedicated server, else 10%.
# innodb_buffer_pool_size = 128M
#
# Remove leading # to turn on a very important data integrity option: logging
# changes to the binary log between backups.
# log_bin
#log-bin=mysql-bin

#
# Remove leading # to set options mainly useful for reporting servers.
# The server defaults are faster for transactions and fast SELECTs.
# Adjust sizes as needed, experiment to find the optimal values.
# join_buffer_size = 128M
# sort_buffer_size = 2M
# read_rnd_buffer_size = 2M
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
max_allowed_packet=33M
innodb_log_file_size=200M
character-set-server=utf8

# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0

# Recommended in standard MySQL setup
sql_mode=NO_ENGINE_SUBSTITUTION,STRICT_TRANS_TABLES

[mysqld_safe]
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
```

続く

3 /etc フォルダーに、「my.cnf」と名前を付けて保存します。

4 mysqld を再起動します。

コマンド：`/etc/init.d/mysql restart`
/tmp フォルダーに mysql.sock ファイルが作成されます。

■管理者パスワードの設定

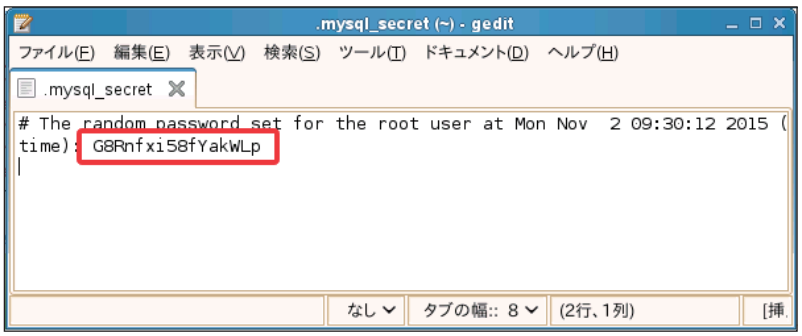
MySQL に接続し、データベース管理者（root）に対してパスワードを設定します。

操作手順

1 MySQL のコンソール画面に接続します。

コマンド：`mysql -u root -p --host 127.0.0.1`
初期パスワードを求められます。

2 root フォルダーの .mysql_secret ファイルに記載されている初期パスワードを入力します。



プロンプトが mysql> となり、MySQL のコンソールに入ります。

！重 要

初期パスワードは、ランダムで発行されます。実際の初期パスワードは、画面とは別のものとなります。

3 root に対して、パスワードを設定します。

コマンド：`set password for 'root'@'localhost'=password('XXXXXXX');`

！重 要

ここで設定した MySQL の管理者パスワードは、ERA サーバーおよび ERA プロキシのインストールの際に必要となります。

4 変更を更新し、MySQL コンソール画面を閉じます。

コマンド：`quit`

5 mysql を再起動します。

コマンド：`/etc/init.d/mysqld restart`

6 service コマンドを使用して、MySQL の稼動確認をします。

ワンポイント

MySQL に再接続する場合は、設定したパスワードを入力します。
コマンド：`mysql -u root --host 127.0.0.1`
設定したパスワードを入力すると、MySQL のコンソール画面に接続します。

3.4.3.2 MySQL ODBC

MySQL ODBC ドライバーのインストール後に、現在の odbcinst_23.ini ファイルを無効にし、新たに作成します。

! 重 要

SUSE Linux では、unixODBC_23 パッケージを使用してください。

操作手順

1. My ODBC ドライバーをインストールします。
2. /etc/unixODBC フォルダーにある、odbcinst_23.ini ファイルの名前を変更します。

   変更前：odbcinst_23.ini
   ↓
   変更後：odbcinst_23.ini.org
3. テキストエディターを開き、次の内容へ変更します。

```
[PostgreSQL]
Description=ODBC for PostgreSQL
Driver=/usr/lib/psqlodbcw.so
Setup=/usr/lib/libodbcpsqlS.so
Driver64=/usr/lib64/psqlodbcw.so
Setup64=/usr/lib64/libodbcpsqlS.so
FileUsage=1

[MySQL]
Description=ODBC for MySQL
Driver=/usr/lib64/libmyodbc5w.so
Setup=/usr/lib64/libmyodbc5w.so
#Driver64=/usr/lib64/libmyodbc5.so
#Setup64=/usr/lib64/libodbcmyS.so
FileUsage=1
Threading=0

[MySQL ODBC 5.3 Unicode Driver]
Driver=/usr/lib64/libmyodbc5w.so
UsageCount=1

[MySQL ODBC 5.3 ANSI Driver]
Driver=/usr/lib64/libmyodbc5a.so
UsageCount=1
```

4. /etc/unixODBC フォルダーに、「odbcinst_23.ini」と名前を付けて保存します。

3.4.4 ERA サーバーのインストール

ERA サーバーのインストールでは、MySQL に接続し ERA サーバーのデータベースを作成します。
そのためインストーラーの起動と同時に、MySQL への接続情報が必要となります。
設定が必要な項目は、「■ ERA サーバー オプション設定の確認」を参照してください。

ERA サーバーのインストールには、次の条件とパッケージが必要です。

- 管理者権限を使用した、MySQL のインストールと設定
- ODBC ドライバーのインストールと設定
- ERA サーバーが使用するネットワーク通信ポートが空いていること
- JAVA の最新版への更新

ワンポイント

MySQL および ODBC ドライバーの構成は、「3.4.2 CentOS/RHEL での準備」または「3.4.3 SUSE Linux での準備」を参照してください。
ERA サーバーが使用するネットワーク通信ポートについては、「2.4 使用されるポート」を参照してください。

■必要パッケージとインストールコマンド

下表は、ESET Remote Administrator に必要な、Linux のパッケージ一覧です。（）内は CentOS/RHEL でのパッケージ名です。インストールされていない場合は、yum 等を利用してインストールしてください。

必要パッケージ	詳細
openSSL（openssl）	サポート対象は openssl-1.0.1e-30 以降です。
xvfb（xorg-xll-server-Xvfb）	グラフィカルインターフェースを使用しない、Linux サーバーシステムでの適切なレポート印刷に必要です。
Cifs-utils（cifs-utils）	Windows OS への ERA エージェントの展開に必要です。
Qt4 WebKit libraries Ver4.8	PDF と PS 形式でレポートを出力するために必要です。 「3.4.5.1 Qt4 WebKit パッケージのインストール」参照
Kinit + klist（krb5-workstation）	ActiveDirectory との同期と、ドメインユーザーでのログイン中に Kerberos 認証に必要です。
Wbinfo + ntlm_auth（samba-winbind-clients）	SMTP サーバーとのドメインアカウント + NTLM 認証で使用されます。
Ldapsearch（openldap-clients）	ActiveDirectory との同期機能に使用されます。
Snmptrap（net-snmp-utils）	SNMP トラップを送信するために使用されます。使用しない場合、インストールは不要です。
SELinux devel package（policycoreutils-devel）	SELinux を使用している場合、インストールが必要です。

■ ERA サーバー インストールオプション一覧

ERA サーバーインストールでのオプションの一覧です。必須となっているオプションは、インストールと同時に設定します。

オプション	説明	設定値	必須
--locale	ESET Remote Administrator の言語設定	ja_JP（日本語）	○
--skip-license	ライセンス認証の省略		-
--skip-cert	証明書生成の省略		-
--license-key	ESET のライセンスキーの入力 インストール後に入力可能		-
--product-guid	製品 GUID	設定しない場合は自動生成	-
--server-port	ERA サーバーのポート番号	2222（既定値）	-
--console-port	ERA Web コンソールのポート番号	2223（既定値）	-
--server-root-password	ERA Web コンソールの管理者初期パスワード	8 文字以上	○
--db-type	データベースサーバーの種類	MySQL Server/ Microsoft SQL Server	-
--db-driver	データベースサーバーの接続に使用する ODBC ドライバー		○
--db-hostname	データベースサーバーのコンピューター名または IP アドレス		○
--db-port	データベースサーバーのポート番号	3306（既定値）	○
--db-name	ERA サーバーデータベース名 指定しない場合、era_db を自動作成		-
--db-admin-username	データベースサーバーの管理者名 インストールで使用	データベースサーバーの管理者名と同一	○
--db-admin-password	データベースサーバーの管理者パスワード	データベースサーバーの管理者パスワードと同一	○
--db-user-username	ERA サーバーが使用するデータベースのユーザー名	16 文字以内	○
--db-user-password	ERA サーバーが使用するデータベースのユーザーパスワード		○
--cert-hostname ※ 1	ERA サーバーがインストールされるコンピューターの名前または IP アドレス		○
--server-cert-path ※ 2	ピア証明書（サーバー）のパス		-
--server-cert-password	サーバーピア証明書のパスワード		-
--peer-cert-password	ピア証明書（エージェント）のパスワード		-
--cert-auth-path	認証局ファイルへのパス		-
--cert-auth-common-name	認証局共通名の設定		-
--cert-organizational-unit	部署名		-
--cert-organization	組織名		-

オプション	説明	設定値	必須
--cert-locality	所在地		-
--cert-state	都道府県		-
--cert-country	所在国	JP	-
--cert-validity	証明書の有効期間の日数または年数		-
--cert-validity-unit	証明書有効期間の単位		-
--ad-server	アクティブディレクトリのサーバーコンピューター名		-
--ad-user-name	アクティブディレクトリのネットワークへの検索権限を保有するユーザー名		-
--ad-user-password	アクティブディレクトリのネットワークへの検索権限を保有するユーザーパスワード		-
--ad-cdn-include	アクティブディレクトリのパス		-
--help	オプション一覧の表示		
--uninstall	アンインストール		-
--keep-database	アンインストール時にデータベースを削除しない		-

※ 1 変動 IP アドレスの指定には、「＊」（アスタリスク）を設定します。

※ 2 --skip-cert を指定した場合に使用します。

! 重 要

説明書の有効期間は、初期設定の 10 年のまま変更しないでください。
証明書の有効期間が 2038 年以上に設定されている場合は、Mac OS X が証明書エラーになり、管理できません。

ワンポイント

オプション一覧はターミナル上で確認することができます。
コマンド：`./x64/Server-Linux-x86_64.sh -help`

■ ERA サーバー オプション設定の確認

ERA サーバーインストールの際に必要となるオプション設定を確認します。
インストーラーの実行時に、インストールする環境に合わせて最低限以下のオプションを指定してください。必要に応じて他のオプションを指定してください。

設定内容	使用するオプション	設定例
ESET RemoteAdministrator での使用言語	--locale	=ja_JP
ライセンス認証の省略	--skip-license	—
ODBC ドライバーの種類	--db-driver	=MySQL
データベースサーバーのコンピューター名または IP アドレス	--db-hostname	=127.0.0.1
データベースサーバー接続のポート番号	--db-port	=3306
データベースサーバーの管理者名	--db-admin-username	=root
データベースサーバーの管理者パスワード	--db-admin-password	=XXXXXXX
ERA Web コンソールの管理者初期パスワード	--server-root-password	=XXXXXXX
ERA サーバーが利用するデータベースのユーザー名	--db-user-username	=era_server_user
ERA サーバーが利用するデータベースのユーザーパスワード	--db-user-password	=XXXXXXX
ERA サーバーのコンピューター名または IP アドレス	--cert-hostname	=*

! 重　要

Locale は必ず ja_JP を選択してください。ja_JP を選択しない場合は、リポジトリが海外の値となり、サポート対象外となります。

ワンポイント

この設定例では ERA サーバーデータベース名である --db-name を指定しないため、既定のデータベース名である era_db が作成されます。必要に応じて、--db-name を指定してください。
データベースサーバーの管理者名とパスワード（--db-admin-username および --db-admin-password）には、MySQL 管理者と同じものを指定します。
その他のパスワードは任意のパスワードを指定します。設定したパスワードは忘れないようにしてください。

操作手順

1 root フォルダーのターミナルを開きます。

続く

2 ERA サーバーインストーラーに実行権限を付与します。

コマンド：`chmod +x ./x64/Server-Linux-x86_64.sh`

ERA サーバーインストーラーのアクセス権限が変わります。

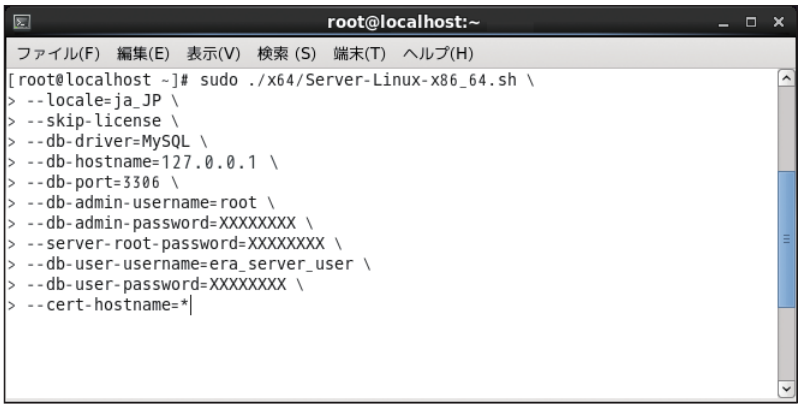
3 ERA サーバーインストーラーを起動します。

コマンド：`sudo ./x64/Server-Linux-x86_64.sh \`

続く

4 続けて、オプションと設定値を入力します。

```
--locale=ja_JP \
--skip-license \
--db-driver=MySQL \
--db-hostname=127.0.0.1 \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=XXXXXXXX \
--server-root-password=XXXXXXXX \
--db-user-username=era_server_user \
--db-user-password=XXXXXXXX \
--cert-hostname=*
```



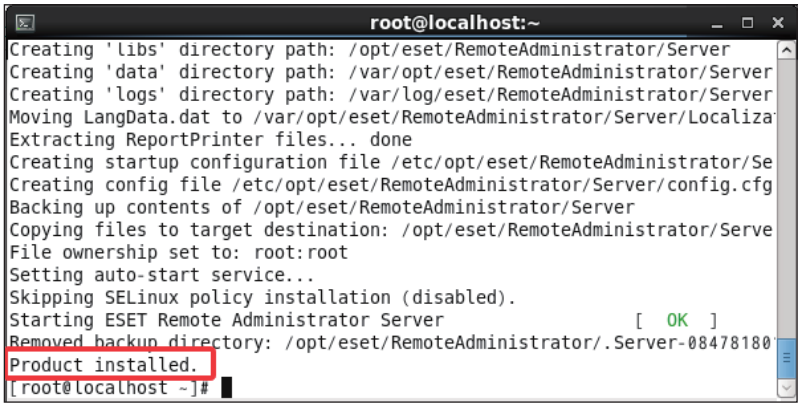
! 重　要

--db-hostname に localhost を指定すると、MySQL サーバーの仕様でローカルコンピューターの UNIX ソケットファイルを使用します。そのため、TCP/IP でローカルコンピューターのデータベースに接続する場合は、'127.0.0.1' を指定してください。

続く

5 【Enter】キーを押します。

コマンドに記載したオプションの設定に従って、ERA サーバーのインストールが開始されます。



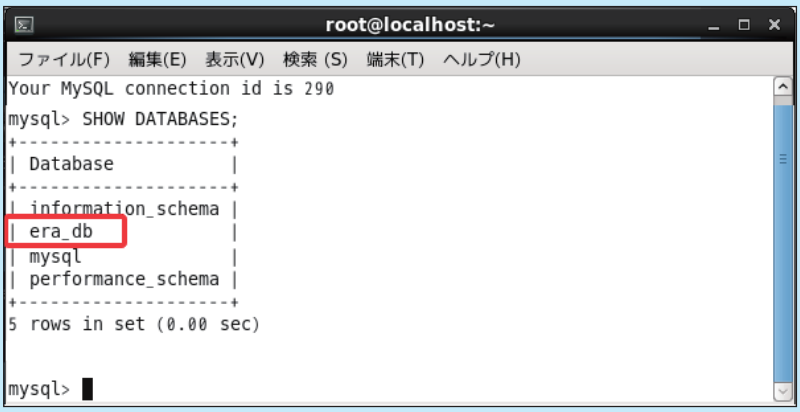
Product installed. が表示されたら、インストールは終了します。
ERA サーバーおよび ERA サーバーサービスは、/opt/eset/RemoteAdministrator/Server フォルダーにインストールされます。

6 ERA サーバーサービスの稼動を確認します。

コマンド：`ps -ef | grep eraserver`
/opt/eset/RemoteAdministrator/Server/ERAServer のプロセスが表示されたら、ERA サーバーは稼働中です。

ワンポイント

MySQL に接続し、作成された ERA サーバーのデータベースを確認することができます。



3.4.5 ERA Web コンソールのインストール

ERA Web コンソールが正しくインストールされると、ESET Remote Administrator をブラウザー上で開くことができます。

! 重 要

ERA Web コンソールのセキュリティ向上のために、Apache Tomcat の SSL 接続の設定が必要です。

ERA Web コンソールのインストールには、次の条件が必要です。

- ERA サーバーのインストール
- Apache Tomcat Ver.6.0 以上のインストール

以下の手順は Apache Tomcat Ver.6.0 の場合の例です。

操作手順

1. root フォルダーのターミナルを開きます。
2. era.war ファイルを、tomcat6/webapps フォルダーにコピーします。次のコマンドを実行します。

コマンド（CentOS/RHEL）：`sudo cp ./x64/era.war /var/lib/tomcat6/webapps/`
コマンド（SUSE）：`sudo cp ./x64/era.war /srv/tomcat6/webapps/`

※画面は CentOS/RHEL での操作です。
era.war ファイルが、webapps フォルダーへコピーされます。

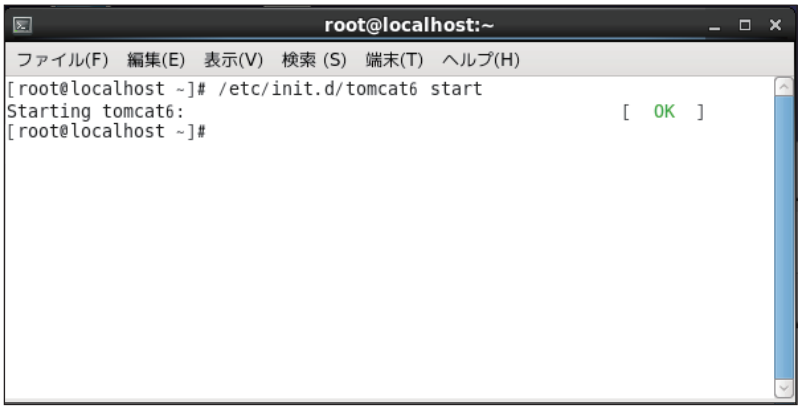
ワンポイント

era.war ファイルを tomcat6/webapps フォルダーへ、直接コピーすることも可能です。

続く

❸ Tomcat サービスを起動します。

コマンド：/etc/init.d/tomcat6 restart



Tomcat が起動します。

ワンポイント

ERA Web コンソールのセキュリティ向上のため Apache Tomcat は SSL での接続に対応する設定を行うことを強く推奨します。

❹ ブラウザーを開き、アドレスバーに https://localhost/era/ を入力します。

Web コンソール画面が表示されます。
ユーザー名には、Administrator が表示されます。

ワンポイント

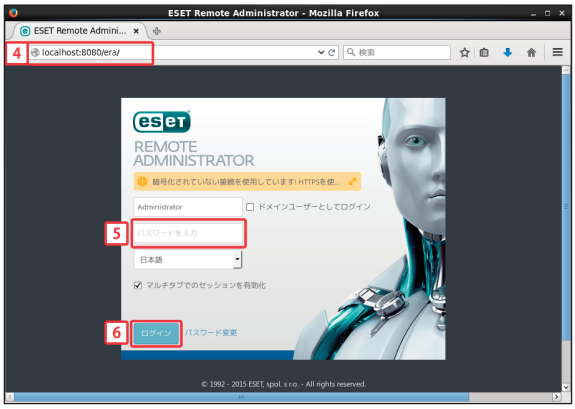
サーバーにリモート接続している場合は、https:// コンピューター名または IP アドレス /era を入力してください。
※網掛けの箇所を、使用環境に合わせて適宜変更してください。
また、上記の URL で ERA Web コンソールに接続できない場合は、Apache Tomcat の SSL に対応した接続設定が不足している可能性があります。
その場合は、接続先を、http://localhost:8080/era/ に変更してください。

❺ Administrator でログインします。

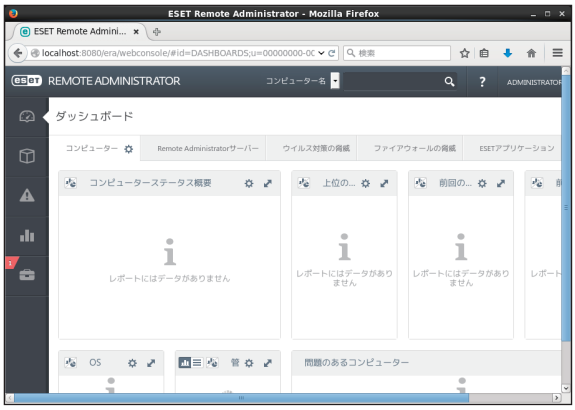
「パスワードを入力」には、「3.4.4　ERA サーバーのインストール」の手順 4 で、--server-root-password に対して設定した、ERA Web コンソールの初期パスワードを入力します。

続く

6 ［ログイン］ボタンをクリックします。



ERA Web コンソールへログインします。



ユーザー名 Administrator は、ESET Remote Administrator の既定の管理者となっています。

3.4.5.1 Qt4 WebKit パッケージのインストール

ESET Remote Administrator のレポートを PDF および PS 形式で出力するために必要なパッケージです。

! 重 要

ESET Remote Administrator においての有効なバージョンは Qt Ver4.8（Qt4）となっています。qtwebkit 2.0.X または 2.3.4 以上をインストールしてください。

操作手順

＜ CentOS/RHEL ＞

1. EPEL リポジトリをインストールします。

   コマンド：`yum install epel-release`

2. インストールした EPEL を通常使用するリポジトリから除外するため、repo ファイルの設定を変更します。

   /etc/yum.repos.d フォルダーの epel.repo ファイルを開き、「epel」以下に記載してある次の行を変更します。
   変更前：`enabled=1`
   ↓
   変更後：`enabled=0`

3. Qt WebKit パッケージをインストールします。

   コマンド：`yum --enablerepo=epel install qtwebkit`

   ワンポイント

   有効なバージョンの Qt WebKit パッケージが公式リポジトリに存在しない場合は、別途サードパーティなどのリポジトリやインターネットからダウンロードしてインストールするか、対象のコンピューター上でコンパイルしてください。

4. X.Org パッケージをインストールします。

   コマンド：`yum install xorg-x11-server-Xvfb.x86_64`

! 重 要

X Window System をインストールしている場合、以下の操作手順 5 および操作手順 6 は実施しないでください。

5. X クライアントからの接続許可を追加します。

   コマンド：`export DISPLAY=localhost:0`

6. /etc フォルダーの profile ファイルに、次の行を追記し、上書き保存します。

   `export DISPLAY=localhost:0`
   追記する場所は任意です。

7. 日本語フォントのパッケージをインストールします。

   日本語フォントのパッケージについて、特に指定はありません。

＜ SUSE Linux ＞

1. Qt WebKit パッケージをインストールします。

   コマンド：`zypper install libQtWebKit4`

2. ERA サーバーを再起動します。

   コマンド：`sudo service eraserver restart`

3. 日本語フォントのパッケージをインストールします。

   日本語フォントのパッケージについて、特に指定はありません。

3.4.6 ERA エージェントのインストール

ERA エージェントのインストールでは、ERA サーバーおよび ERA Web コンソールとの接続情報の指定が必要となります。設定が必要な項目は、「■ ERA エージェント オプション設定の確認」を参照してください。

また ERA エージェントは、クライアントコンピューターでの実行を前提としているプログラムのため、サーバーコンピューターへのインストールは任意となっています。

ワンポイント

ERA サーバーへの接続は、次の 4 つのパターンから選択して指定します。
・ERA サーバーコンピューター名とポート番号
・ERA サーバーの IPv4 アドレスとポート番号
・ERA サーバーの IPv6 アドレスとポート番号
・SRV レコード
SRV レコードは、DNS サーバーを使用してる場合に指定が可能です。
SRV レコードを指定した場合、ポート番号は不要です。また、SRV レコードのプレフィックスを「_NAME ._tcp」としてください。
※網掛け箇所を、適宜変更します。例）_era._tcp など

ERA エージェントのインストールには、次の条件が必要です。

- ERA サーバーおよび ERA Web コンソールのインストール
- ピア証明書（エージェント）の作成とエクスポート
- 認証局の作成と、公開鍵（以下 証明局ファイル）のエクスポート
- サーバーコンピューターがネットワーク接続していること
- OpenSSL が openssl-1.0.1e-30 以上であること

■ ERA エージェントインストールオプション一覧

ERA エージェントのインストールでのオプションの一覧です。必須となっているオプションは、インストールと同時に設定します。

また、ERA エージェントのインストールでは、ERA サーバーとの接続のためにピア証明書（エージェント）と認証局ファイル（以下、証明書ファイル）の指定が必要となっています。

インストール時の証明書ファイルの指定は、次の 2 つの方法から選択します。

- **サーバー支援インストール**

ERA エージェントのインストール中に、証明書ファイルを自動ダウンロードします。

そのため ERA Web コンソール管理者のアカウント情報を指定する必要があります。

インストールコマンドで、次のオプションを設定します。

ERA Web コンソールの管理者名	`--webconsole-user`
ERA Web コンソールの管理者パスワード	`--webconsole-password`
ERA Web コンソールのポート番号	`--webconsole-port`

- **オフラインインストール**

あらかじめエクスポートした証明書ファイルの、保存場所を指定します。

別途、ESET Remote Administrator から、証明書ファイルをエクスポートする必要があります。

インストールコマンドで、次のオプションを設定します。

保存したピア証明書（エージェント）のパス	`--cert-path`
ピア証明書のパスワード	`--cert-password`
認証局ファイルの保存場所	`--cert-auth-path`

ワンポイント

オフラインインストールの場合は、次の方法で認証局ファイルのパスワードを設定してください。

・ERA サーバーのインストール時に --cert-auth-password および --peer-cert-password オプションを設定する

・ESET Remote Administrator 上で、認証局およびピア証明書（エージェント）を新たに作成する

証明書への操作については「6.9 証明書」を参照してください。

! 重 要

ここでは、サーバー支援インストールを使用して ERA エージェントをインストールします。

オフラインインストールを使用したインストール操作については、「4.2.2.6 Linux へのローカル展開」の「■オフラインインストール」を参照してください。

● ERA エージェントインストール オプション一覧

オプション	説明	設定値	必須※1
--skip-license	ライセンス認証の省略		-
--hostname	ERA サーバーのコンピューター名または IP アドレス		○
--port	ERA サーバーのポート番号	2222（既定値）	○
--cert-path※2	ピア証明書（エージェント）ファイルのパス		○1
--cert-auth-path	認証局ファイルのパス		○1
--cert-password※3	ピア証明書（エージェント）ファイルのパスワード		○1
--cert-auth-password	認証局のパスワード		-
--product-guid	製品 GUID	設定しない場合は自動生成	-
--cert-content※2	サーバーとエージェントとの安全な通信チャネルを設定するために使用される PKCS12 暗号化認証局秘密鍵の Base64 暗号化内容		-
--cert-auth-content	ピア証明書（プロキシまたはサーバー）を検証するために使用される DER 暗号化認証局秘密鍵の Base64 暗号化内容		-
--webconsole-hostname※4	ERA Web コンソールのコンピューター名または IP アドレス		-
--webconsole-user	ERA Web コンソール管理者名	Administrator	○2
--webconsole-password	ERA Web コンソール管理者パスワード		○2
--webconsole-port	ERA Web コンソールのポート番号	2223	○2
--help	オプション一覧の表示		
--uninstall	アンインストール		

※1　○1 および○2 は、証明書ファイルの指定方法を選択することで必須種別が変わります。

※2　--cert-path、--certcontent のどちらかを使用します。

※3　ピア証明書にパスワードを設定している場合は、このオプションを使用してパスワードを指定します。

※4　--hostname と同一の場合は、設定する必要はありません。

ワンポイント

オプション一覧はターミナル上で確認することができます。
コマンド：`./x64/Agent-Linux-x86_64.sh -help`

■ ERA エージェント オプション設定の確認

ERA エージェントのインストールの際に必要となるオプション設定をインストーラーの実行時に、インストールする環境に合わせて最低限以下のオプションを指定してください。
必要に応じて他のオプションを指定してください。

設定内容	使用するオプション	設定例
ライセンス認証の省略	--skip-license	-
ERA サーバーのコンピューター名または IP アドレス	--hostname	=1.1.1.1
ERA サーバーのポート番号	--port	=2222
ERA Web コンソールのポート番号	-- webconsole-port	=2223
ERA Web コンソールの管理者名	--webconsole-user	=Administrator
ERA Web コンソールの管理者パスワード	--webconsole-password	=YYYYYYY

! 重 要

ここでは、ERA サーバーのコンピューター名または IP アドレスの指定である --hostname の設定値を 1.1.1.1 としています。

操作手順

1. root フォルダーのターミナルを開きます。
2. ERA エージェントインストーラーに実行権限を付与します。

   コマンド：`chmod +x ./x64/Agent-Linux-x86_64.sh`

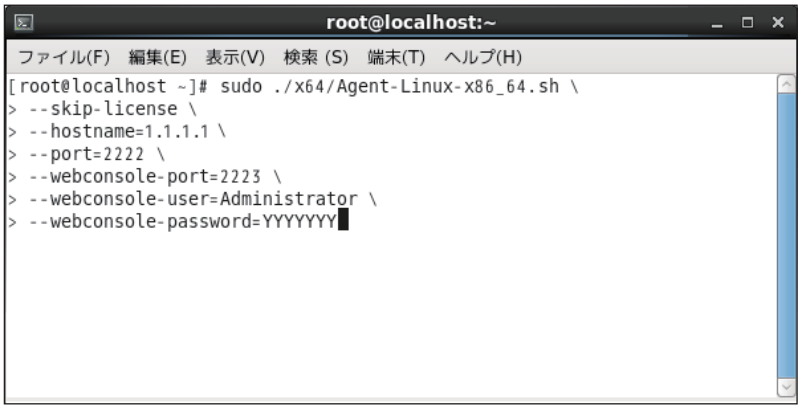
   ERA エージェントインストーラーのアクセス権限が変わります。
3. ERA エージェントインストーラーを起動します。

   コマンド：`sudo ./x64/Agent-Linux-x86_64.sh \`

続く

4 続けて、オプションと設定値を入力します。

```
--skip-license \
--hostname=1.1.1.1 \
--port=2222 \
--webconsole-port=2223 \
--webconsole-user=Administrator \
--webconsole-password=YYYYYYY
```



5 【Enter】キーを押します。

コマンドに記載したオプションの設定に従って、ERA エージェントのインストールが開始されます。

Product installed. が表示されたら、インストールは終了します。

ERA エージェントは、/opt/eset/RemoteAdministrator/Agent フォルダーにインストールされます。

6 ERA エージェントの稼動を確認します。

コマンド：`ps -ef | grep eraagent`

/opt/eset/RemoteAdministrator/Agent/ERAAgent のプロセスが表示されたら、ERA エージェントは稼働中です。

3.4.7 ERA プロキシのインストール

ERA プロキシのインストールでは、MySQL に接続し ERA プロキシのデータベースを作成します。
また、ERA サーバーとの接続設定を行います。
そのためインストーラーの起動と同時に、MySQL と ERA サーバーへの接続情報が必要となります。
設定が必要なオプションの項目は、「■ ERA プロキシオプション設定の確認」を参照してください。

ERA プロキシのインストールには、次の条件が必要です。

- MySQL のインストールと設定
- ODBC ドライバーのインストールと設定
- ERA サーバーと ERA Web コンソールの、サーバーコンピューター上へのインストール
- ERA エージェントの、ローカルコンピューター上へのインストール
- ピア証明書（プロキシ）の作成とエクスポート
- 認証局の作成と、認証局ファイルのエクスポート
- 有効なライセンスがあること

! 重 要

MySQL と ODBC ドライバーの構成は、「3.4.2 CentOS/RHEL での準備」または「3.4.3 SUSE Linux での準備」を参照してください。
ERA サーバーと ERA Web コンソールのインストールは、「3.4.4 ERA サーバーのインストール」、「3.4.5 ERA Web コンソールのインストール」を参照してください。
ERA エージェントのインストールは、「3.4.6 ERA エージェントのインストール」を参照してください。

ワンポイント

MySQL への接続は、次の 4 つの情報から選択して指定します。
・ERA サーバーコンピューター名
・ERA サーバーの IPv4 アドレス
・ERA サーバーの IPv6 アドレス
・DNS リソースレコード
DNS リソースレコードは、DNS サーバーを使用している場合に指定が可能です。

■ ERA プロキシインストールオプション一覧

ERA プロキシインストールでのオプションの一覧です。必須となっているオプションは、インストールと同時に設定します。

オプション	説明	設定値	必須
--skip-license	ライセンス認証の省略		-
--product-guid	製品 GUID	設定しない場合は自動生成	-
--db-type	使用するデータベースの種類	MySQL Server/ Microsoft SQL Server	○
--db-driver	データベースサーバー接続に使用する ODBC ドライバー		○
--db-hostname	データベースサーバーのコンピューター名または IP アドレス		○
--db-port	データベースサーバーのポート番号	3306（既定値）	○
--db-name	ERA プロキシデータベース名 指定しない場合、era_proxy_db を自動作成		-
--db-admin-username	ERA プロキシデータベース管理者名 インストールで使用	データベースサーバー管理者名と同一	○
--db-admin-password	ERA プロキシデータベース管理者パスワード	データベースサーバー管理者パスワードと同一	○
--db-user-username	ERA プロキシデータベースのユーザー名 ERA プロキシで使用し、データベースへ接続	16 文字以内	○
--db-user-password	ERA プロキシデータベースのユーザーパスワード		○
--hostname	サーバーのホスト名または IP アドレス		○
--port	接続先 ERA サーバーのポート番号または ERA プロキシのポート番号	サーバー：2222 プロキシ：2222	○
--proxy-port	ERA プロキシで使用されるポート	2222（既定値）	-
--cert-path ※1	ピア証明書（プロキシ）のパス		○
--cert-content ※1	サーバーとエージェントとの安全な通信チャネルを設定するために使用される PKCS12 暗号化公開鍵証明書と秘密鍵の Base64 暗号化内容		-
--cert-auth-path ※2	認証局ファイルのパス		○
--cert-auth-content ※2	ピア証明書（プロキシまたはサーバー）を検証するために使用される DER 暗号化認証局秘密鍵の Base64 暗号化内容		-
--cert-password ※3	ピア証明書（プロキシ）のパスワード		-
--cert-auth-password	認証局のパスワード		-
--keep-database	データベースの確保		-
--help	オプション一覧の表示		
--uninstall	アンインストール		-

※ 1　--cert-path、--cert-content のどちらかを使用します。

※ 2　--cert-auth-path、--cert-auth-content のどちらかを使用します。

※ 3　ピア証明書にパスワードを設定している場合は、このオプションを使用してパスワードを指定します。

ワンポイント

オプション一覧はターミナル上で確認することができます。
コマンド：`./x64/Proxy-Linux-x86_64.sh --help`

■ ERA プロキシオプション設定の確認

ERA プロキシインストールの際に必要となるオプション設定を確認します。
インストーラーの実行時に、インストールする環境に合わせて最低限以下のオプションを指定してください。
必要に応じて他のオプションを指定してください。

設定内容	使用するオプション	設定例
ライセンス認証の省略	-skip-license	-
ODBC ドライバーの種類	--db-driver	=MySQL
MySQL のコンピューター名または IP アドレス	--db-hostname	=1.1.1.1
MySQL 接続のポート番号	--db-port	=3306
ERA プロキシデータベースの管理者名	--db-admin-username	=root
ERA プロキシデータベースの管理者パスワード	--db-admin-password	=XXXXXXX
ERA プロキシのユーザー名	--db-user-username	=era_proxy_user
ERA プロキシのユーザーパスワード	--db-user-password	=XXXXXXX
ERA サーバーのコンピューター名または IP アドレス	--hostname	=1.1.1.1
ERA サーバーのポート番号	--port	=2222
ピア証明書（プロキシ）の保存場所	--cert-path	=./ デスクトップ…
認証局ファイルの保存場所	--cert-auth-path	=./ デスクトップ…

ワンポイント

この設定例では ERA プロキシデータベース名である --db-name を指定しないため、既定のデータベース名である era_proxy_db が作成されます。必要に応じて、--db-name を指定してください。
ERA プロキシデータベースの管理者名とパスワード（--db-admin-username および --db-admin-password）には、MySQL 管理者と同じものを指定します。
その他のオプション設定については、「■ ERA プロキシインストールオプション一覧」を参照してください。

! 重 要

ここでは、MySQL および ERA サーバーのコンピューター名または IP アドレス（--db-hostname および --hostname）の設定値を 1.1.1.1 としています。
また、インストールに必要となるピア証明書（プロキシ）と認証局ファイルは、事前にデスクトップ（./ デスクトップ）へエクスポートしています。

証明書の操作については、「6.9 証明書」を参照してください。

操作手順

1. root フォルダーのターミナルを開きます。

2. ERA プロキシインストーラーに実行権限を付与します。

   コマンド：`chmod +x ./x64/Proxy-Linux-x86_64.sh`

   ERA プロキシインストーラーのアクセス権限が変わります。

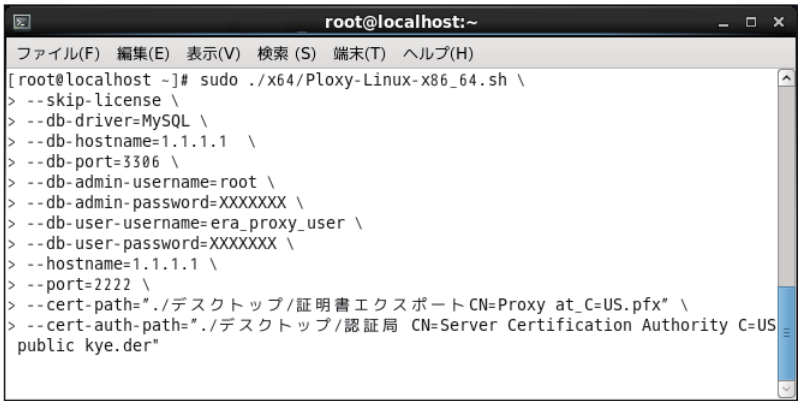
3. ERA サーバーインストーラーを起動します。

   コマンド：`sudo ./x64/Proxy-Linux-x86_64.sh \`

続く

4 続けて、オプションと設定値を入力します。

```
--skip-license \
--db-driver=MySQL \
--db-hostname=1.1.1.1  \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=XXXXXXX \
--db-user-username=era_proxy_user \
--db-user-password=XXXXXXX \
--hostname=1.1.1.1 \
--port=2222 \
--cert-path="./ デスクトップ / 証明書エクスポート CN=Proxy at_C=US.pfx" \
--cert-auth-path="./ デスクトップ / 認証局 CN=Server Certification Authority C=US public key.der"
```



ワンポイント

エクスポートされた証明書のファイル名にスペースが含まれる場合は、--cert-path の設定値の前後に「""」（ダブルクォーテーション）を入力します。

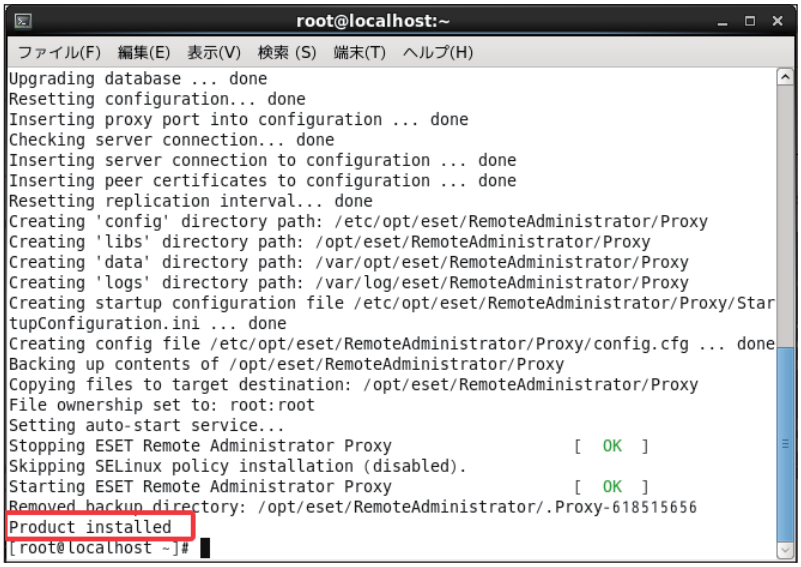
! 重　要

--db-hostname に localhost を指定すると、MySQL サーバーの仕様でローカルコンピューターの UNIX ソケットファイルを使用します。そのため、TCP/IP でローカルコンピューターのデータベースに接続する場合は、'127.0.0.1' を指定してください。

続く

5 【Enter】キーを押します。

コマンドに記載したオプションの設定に従って、ERA プロキシのインストールが開始されます。



Product installed. が表示されたら、インストールは終了します。

ERA プロキシは、/opt/eset/RemoteAdministrator/Proxy フォルダーにインストールされます。

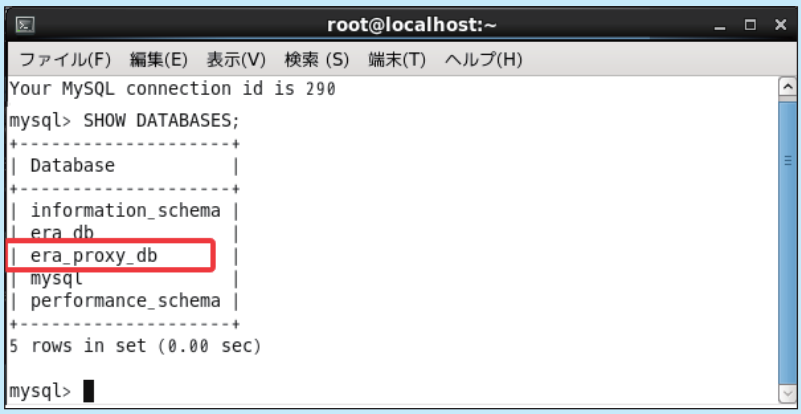
6 ERA プロキシサービスの稼動を確認します。

コマンド：`ps -ef | grep eraproxy`

/opt/eset/RemoteAdministrator/Proxy/ERAProxy のプロセスが表示されたら、ERA プロキシは稼働中です。

ワンポイント

MySQL に接続し、作成された ERA プロキシのデータベースを確認することができます。



3.4.8 RD Sensor のインストール

RD Sensor のインストールには、次の条件が必要です。

- ERA サーバーへの接続
- ERA エージェントの対象コンピューターへのインストール
- ポートに対する適切な設定

操作手順

1. root フォルダーのターミナルを開きます。
2. RD Sensor インストーラーに実行権限を付与します。

   コマンド：`chmod +x ./x64/RDSensor -Linux-x86_64.sh`

   RD Sensor インストーラーのアクセス権限が変わります。

3. RD Sensor のインストーラーを起動します。

   コマンド：`sudo ./x64/RDSensor-Linux-x86_64.sh --skip-license`

   インストールが開始されます。
   インストール完了後に RD Sensor が起動します。

続く

❹ 稼動確認を行います。

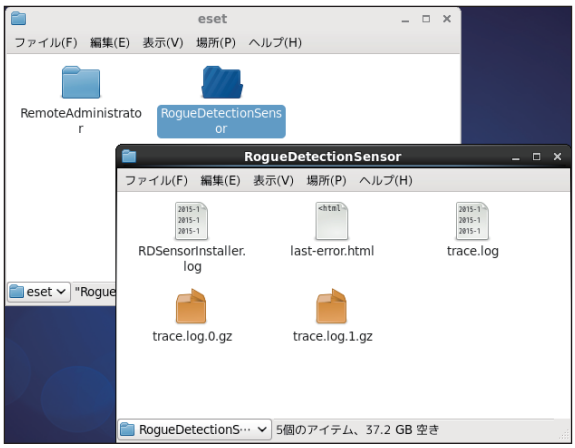
コマンド：`ps -ef | grep eraresensor`

/opt/eset/RogueDetectionSensor/RDSensor のプロセスが表示されたら、RD Sensor は稼働中です。

ワンポイント

稼動していない場合は、次のコマンドで起動してください。
コマンド：`sudo service rdsensor restart`

RD Sensor は、/var/log/eset/RemoteAdministrator/RogueDetectionSensor/trace.log にインストールされます。



3.4.9 Mobile Device Connector のインストール

Mobile Device Connector は、ERA サーバーが実行されているサーバーとは別のサーバーにインストールできます。例えば、インターネットから Mobile Device Connector をインストールしたサーバーにアクセスできるようにすると、場所に関係なく、ユーザーのモバイルデバイスを常時管理できます。

Mobile Device Connector のインストールには、pfx 形式の HTTPS 証明書（SSL 証明書）、ERA サーバーとの接続のためにピア証明書（エージェント）と認証局ファイル（以下、証明書ファイル）の指定が必要となっています。また、Mobile Device Connector が使用する新しいデータベースを作成する必要もあります。インストール時の証明書ファイルの指定は、次の 2 つの方法から選択します。

- **サーバー支援インストール**

ERA エージェントのインストール中に、証明書ファイルを自動ダウンロードします。
そのため ERA Web コンソール管理者のアカウント情報を指定する必要があります。
インストールコマンドで、次のオプションを設定します。

HTTPS 証明書のパス	`--https-cert-path=`
ERA Web コンソールの管理者名	`--webconsole-user`
ERA Web コンソールの管理者パスワード	`--webconsole-password`
ERA Web コンソールのポート番号	`--webconsole-port`
ERA サーバーへの接続 (名前または IP アドレス)	`--hostname=`

- **オフラインインストール**

あらかじめエクスポートした証明書ファイルの、保存場所を指定します。別途、ERA サーバーから、証明書ファイルをエクスポートする必要があります。ピア証明書のエクスポートの操作については、「6.9.1.3 ピア証明書のエクスポート」を参照してください。
インストールコマンドで、次のオプションを設定します。

HTTPS 証明書のパス	`--https-cert-path=`
保存したピア証明書（エージェント）のパス	`--cert-path`
ピア証明書のパスワード	`--cert-password`
認証局ファイルの保存場所	`--cert-auth-path`
ERA サーバーへの接続 (名前または IP アドレス)	`--hostname=`

! 重 要

pfx 形式の HTTPS 証明書（SSL 証明書）が必要です。ERA サーバーで作成したピア証明書（モバイルデバイスコネクター）を使用できます。自己署名証明書の使用許可ができないモバイルデバイスを使用する場合は、信頼できる第三者機関（認証局）が発行する証明書を使用してください。
参照する HTTPS 証明書の CommonName または subjectAltName は、MDM ホスト名と一致する必要があります。Web コンソールのピア証明書（作成する場合は、作成画面の項目「ホスト」「共通名」と MDM ホスト名が一致するようにします。詳しくは「6.9.1.2 新しい証明書の作成」を参照してください。

- **データベース作成のためのオプション**

Mobile Device Connector のインストールでは、Mobile Device Connector が使用する新しいデータベースを作成する必要があります。データベースは、MySQL または MSSQL を利用できます。それぞれ、次のパラメーターを指定する必要があります。

- MySQL データベースの場合

--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=

- MSSQL データベースの場合

--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=

- MySQL/MSSQL データベースが既に存在する場合

--db-use-existing-db=
または
--db-drop-existing-db=

- **インストールスクリプトの例**
  - HTTPS 証明書を httpscert.pfx、ERA サーバーの IP アドレスを 192.168.1.1、Mobile Device Connector の IP アドレスを 192.168.1.2 とした場合

```
sudo ./MDMCore-Linux-x86_64.Sh \
--https-cert-path="./httpscert.pfx" \
--port=2222 \
--db-type="MySQL" \
--db-driver="MySQL" \
--db-admin-username="root" \
--db-admin-password=xxxxxxxx \
--db-user-password=xxxxxxxx \
--db-hostname="127.0.0.1" \
--db-use-existing-db \
--webconsole-password=xxxxxxxx \
--hostname=192.168.1.1 \
--mdm-hostname=192.168.1.2
```

ワンポイント

使用可能なパラメータヘルプメッセージの出力) の一覧については、次のオプションを利用します。
--help
また、インストーラのログは、以下のフォルダーで確認できます。
/var/log/eset/mdminstaller.log

ERA サーバーで HTTPS 証明書を作成する場合は、「6.9.1.2　新しい証明書の作成」を参考にしてください。
コマンドラインで HTTPS 証明書を作成する場合は次の手順で行います。

操作手順

1. サーバの秘密鍵を作成します。

   openssl genrsa 2048 > httpscert.key

2. 秘密鍵から証明書署名要求（CSR）を作成します。

   openssl req -new -subj "/C=JP/ST=Tokyo/L=Shinagawa/O=CITS/OU=Tech/CN=era_server" -key httpscert.key > httpscert.csr
   ここで指定する CN（コモンネーム）は --mdm-hostname= と同一にしなければ "MDM ホスト名が HTTPS 証明書と一致しません " のエラーが表示され、モバイルデバイスコネクタと ESET Remote Administrator サーバ間の接続に失敗します。

3. 認証局から提供された署名済み証明書（CRT）を使用して、サーバの秘密鍵、署名付き公開鍵を含む、PFX ファイルを作成します。

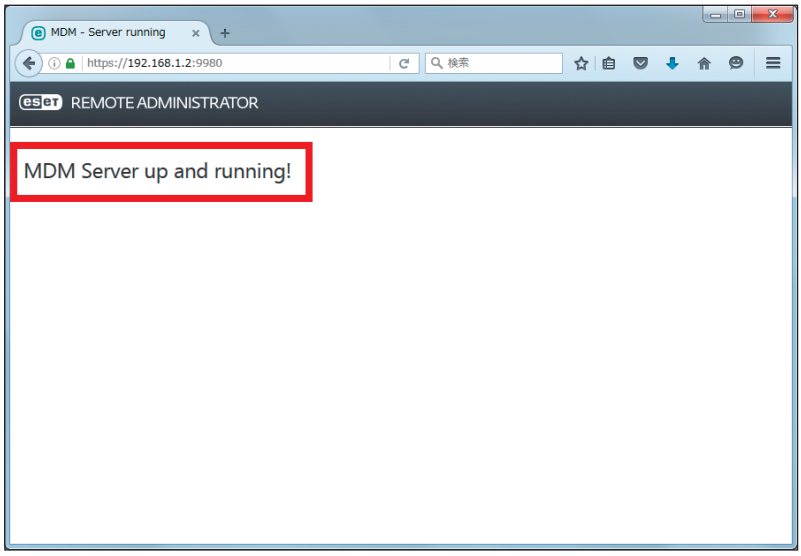
   openssl pkcs12 -passout pass: -export -in httpscert.crt -inkey httpscert.key -out httpscert.pfx

   ※自己署名証明書の使用は推奨されていませんが、仮に使用する場合は以下のように作成します。
   openssl x509 -days 3650 -req -signkey httpscert.key < httpscert.csr > httpscert.crt

- **Mobile Device Connector の動作確認**

インストールが完了したら、Web ブラウザーで Mobile Device Connector が実行中かどうかを確認します。実行中の場合は、以下の画面が表示されます。

URL：https://hostname(IP アドレス）:9980



ワンポイント

Web ページを表示できない場合は、ファイアウォールとネットワークの構成を確認してください。

Mobile Device Connector のインストールオプション一覧

設定内容	使用するオプション	必須
--help	ヘルプを表示する	-
--version	バージョン情報を表示する	-
--uninstall	アンインストールを行う	-
--keep-database	アンインストール時にデータベースの情報を削除しない	-
--skip-license	ライセンス認証の省略	-
--cert-auto-confirm	サーバ支援インストール時にサーバーから受け取ったピア証明書を受け入れる	-
--log-path=dir	インストールログの保存ディレクトリの設定	-
--installdir=dir	プログラムのインストール先ディレクトリの設定 (既定値は "/opt/eset/RemoteAdministrator/MDMCore")	-
--product-guid=globally unique identifier	製品 GUID（設定しない場合は、自動生成）	-
--mdm-port=port	Mobile Device Connector のポート番号 (既定値は '9981')	-
--mdm-enrollment-port=port	Mobile Device Connector 接続のポート番号 (既定値は '9980')	-
--mdm-hostname=hostname	Mobile Device Connector サーバーのコンピューター名または IP アドレス	○
--db-type=dbtype	データベースサーバーの種類	○

設定内容	使用するオプション	必須
--db-driver=dbdriver	データベースサーバーの接続に使用する ODBC ドライバー	○
--db-hostname=hostname	データベースサーバーのコンピューター名または IP アドレス (既定値は localhost)	○
--db-port=port	データベースサーバーのポート番号 (MySQL の既定値は '3306'、MSSQL の既定値は '1433')	-
--db-name=name	データベースの名称 (既定値は era_mdm_db)	-
--db-admin-username=username	データベースサーバーの管理者名（インストールで使用）	○
--db-admin-password=password	データベースサーバーの管理者パスワード	○
--db-user-username=username	Mobile Device Connector が使用するデータベースのユーザー名 (既定値は era_mdm_db_user)	-
--db-user-password=password	Mobile Device Connector が使用するデータベースのパスワード	○
--cert-path=filepath	ピア証明書（エージェント）ファイルのパス	○※1
--cert-password=password	ピア証明書（エージェント）ファイルのパスワード	○※1
--cert-auth-path=filepath	認証局ファイルのパス	○※1
--https-cert-path	HTTPS 証明書ファイルのパス	○
--https-cert-password	HTTPS 証明書ファイルのパスワード	○※2
--hostname=host	ERA サーバーのコンピューター名または IP アドレス	○
--port=port	ERA サーバーのポート番号 (既定値は '2222')	-
--webconsole-hostname=	ERA Web コンソールのコンピューター名または IP アドレス	○※3
--webconsole-use-domain	ERA Web コンソールにドメインユーザーとして接続する場合のドメイン名	-
--webconsole-port=	ERA Web コンソールのポート番号 (既定値 '2223')	-
--webconsole-user=	ERA Web コンソール管理者名 (既定値は 'Administrator')	○※3
--webconsole-password=	ERA Web コンソール管理者パスワード	○※3

※ 1　オフラインインストールを行う場合は必須
※ 2　HTTPS 証明書にパスワードが設定されている場合は必須
※ 3　サーバー支援インストールを行う場合は必須

操作手順

! 重 要

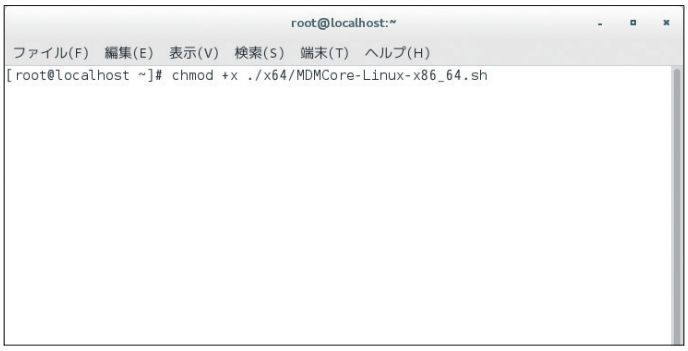
ここでは、Mobile Device Connector のインストールに必要となる ERA ピア証明書（エージェント）をインストーラが自動取得するサーバー支援インストールを行う手順を紹介しています。オフラインインストールを行う場合は、ERA サーバーからエクスポートした ERA ピア証明書（エージェント）をインストール元フォルダー内（ここでは、/root//x64 フォルダー）などにあらかじめコピーしておいておき、--cert-path= や --cert-password= などのオプションを指定してインストールを行ってください。
また、ここでは、MySQL および ERA サーバーのコンピューター名または IP アドレス（--db-hostname、--mdm-hostname および --hostname）の設定値を 1.1.1.1 としています。--mdm-hostname にコンピューター名を設定する場合は、接続するモバイルデバイスが設定したコンピューター名の名前解決を行える必要があります。
また、インストールに必要となる HTTPS 証明書は、/root/x64 フォルダーに httpscert.pfx のファイル名で保存しています。

1. root フォルダーのターミナルを開きます。

2. Mobile Device Connector のインストーラーに実行権限を付与します。

   コマンド：chmod +x ./x64/MDMCore-Linux-x86_64.sh

   Mobile Device Connector のインストーラーのアクセス権限が変わります。



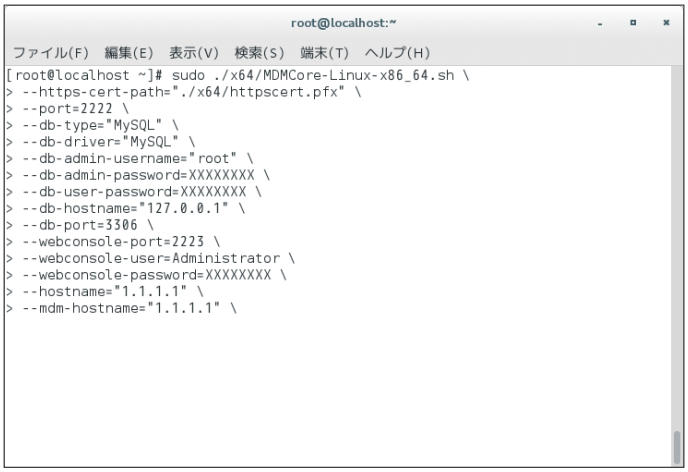
3. Mobile Device Connector のインストーラーを起動します。

   コマンド：sudo ./x64/x64/MDMCore-Linux-x86_64.sh \

続く

4 続けて、オプションと設定値を入力します。

```
--https-cert-path="./x64/httpscert.pfx" \
--port=2222 \
--db-type="MySQL" \
--db-driver="MySQL" \
--db-admin-username="root" \
--db-admin-password=XXXXXXXX \
--db-user-password=XXXXXXXX \
--db-hostname="127.0.0.1" \
--db-port=3306 \
--webconsole-port=2223 \
--webconsole-user=Administrator \
--webconsole-password=XXXXXXXX \
--hostname="1.1.1.1." \
--mdm-hostname="1.1.1.1" \
```



ワンポイント

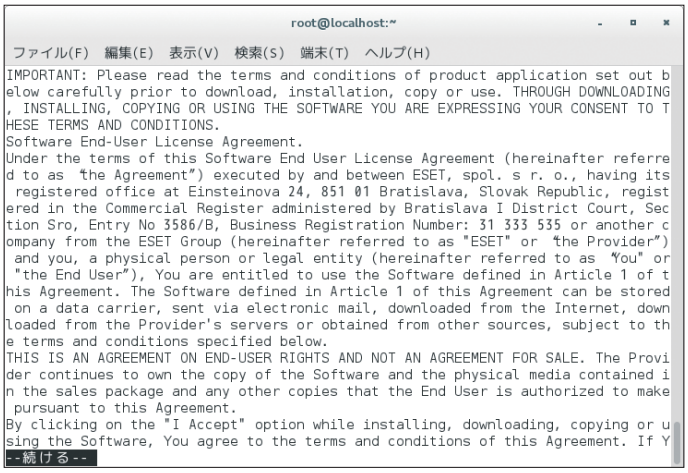
オフラインインストールを行うときは、以下のオプションを追加してインストールを行ってください。また、エクスポートされた証明書のファイル名にスペースが含まれる場合は、--cert-path の設定値の前後に「""」（ダブルクォーテーション）を入力します。

--cert-path= フォルダー名 / ファイル名
--cert-password= エージェント証明書のパスワード（パスワードが設定されていない場合は不要）

続く

5 【Enter】キーを押します。

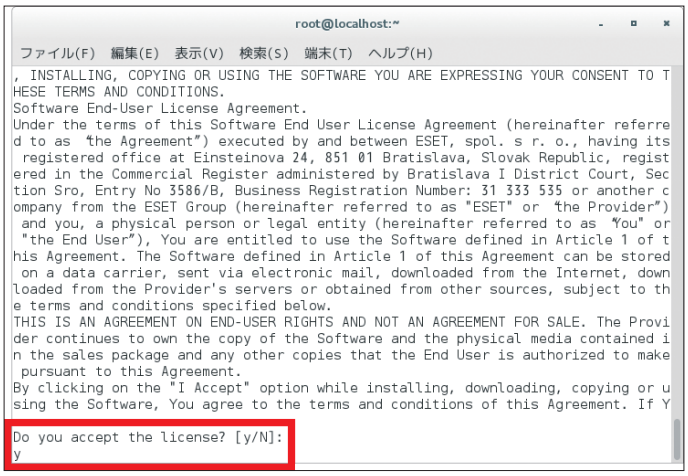
コマンドに記載したオプションの設定に従って、Mobile Device Connector のインストールが開始されます。使用許諾契約書が表示されたら、【Enter】キーを押しながら内容を確認します。



ワンポイント

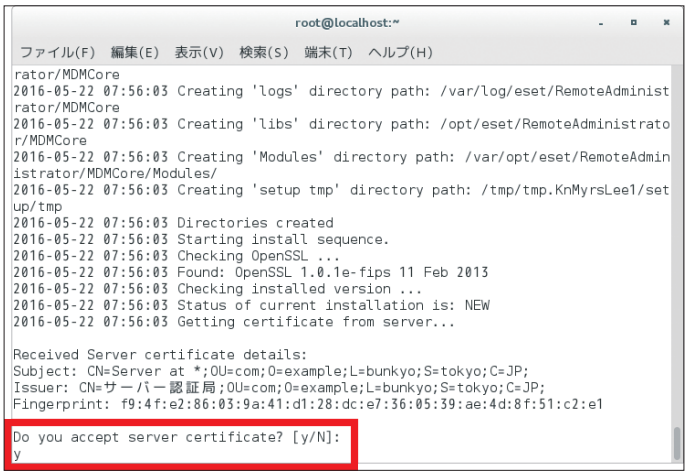
【Q】キーを押すと、使用許諾契約書の表示をスキップできます。

6 使用許諾契約書の内容をすべて表示すると、使用許諾契約書の内容に同意するかどうかを確認する文字が表示されます。【y】キーを押し、続いて【Enter】キーを押しします。

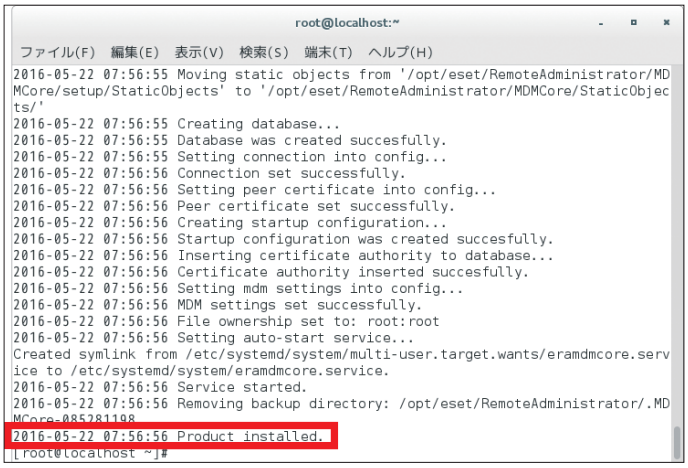


続く

7 ERA サーバーから自動取得したピア証明書（エージェント）を受け入れるかどうかを確認する文字が表示されます。【y】キーを押し、続いて【Enter】キーを押します。



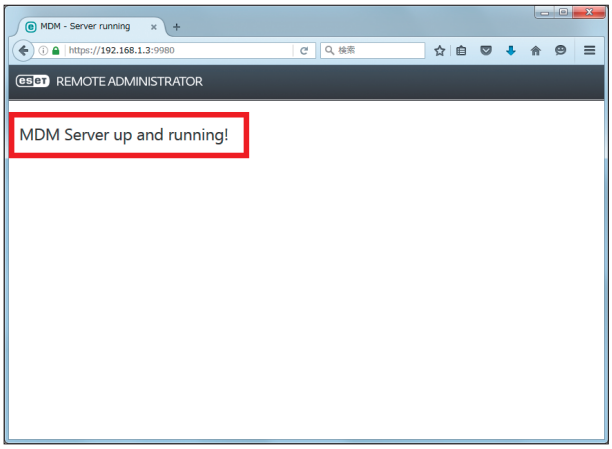
8 Product installed. と表示されたら、インストールは終了です。



続く

9 Web ブラウザーで以下の URL を開き、Mobile Device Connector が実行中かどうかを確認します。実行中の場合は、以下の画面が表示されます。

URL：https://hostname(IP アドレス）:9980



ワンポイント

Web ページを表示できない場合は、ファイアウォールとネットワークの構成を確認してください。

3.4.10　各コンポーネントのアンインストール

アンインストールは各コンソールのインストーラーを起動し、アンインストールオプションを設定します。
ここでは ERA サーバーを例にして、アンインストールの操作を説明します。

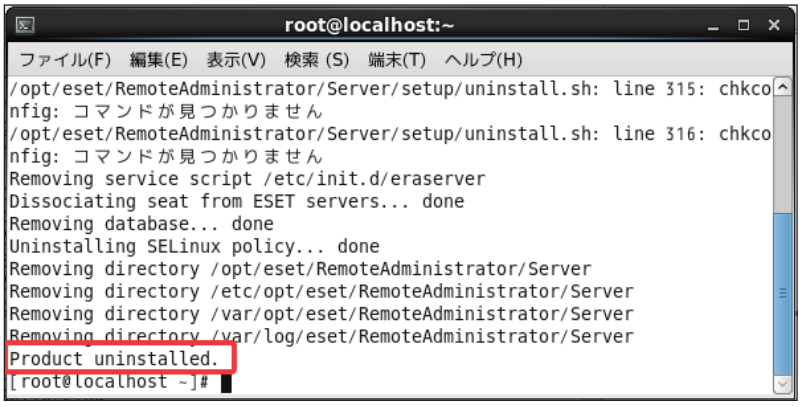
操作手順

1. ERA サーバーインストーラーの起動に続けて、アンインストールオプションを入力します。

```
sudo ./x64/ Server -Linux-x86_64.sh --uninstall
```

ワンポイント
他のコンポーネントをアンインストールする場合は、適切なインストーラー名を入力してください。
※コマンドの、網掛け箇所を適宜変更します。

ERA サーバーのアンインストールが開始されます。



Product uninstalled. と表示されたら、アンインストールは終了です。

ワンポイント
アンインストール後に次の点を確認してください。
・サービス eraserver Service .sh が削除されている
・/etc/opt/eset/RemoteAdministrator/ Server フォルダーが削除されている
※網掛け箇所は、アンインストールするコンポーネントによって変わります。

!重 要

各コンポーネントの構成およびデータベースファイルはそれぞれアンインストール中に削除されます。
ERA サーバー・ERA プロキシのデータベースファイルを保持するにはアンインストールオプションに続けて、次のコマンドを入力します。

```
--uninstall --keep-database
```

また、データベースの復元が必要になる場合に備え、アンインストールを実行する前にデータベースダンプを実施しバックアップを作成することを推奨しています。

3.5 ESET Remote Administrator のアップグレード

ここでは ESET Remote Administrator V6 から上位のバージョンにアップグレードする手順を説明します。アップグレードには、2 種類の方法があります。

- 「Remote Administrator コンポーネントアップグレード」タスクを使用してアップグレード
- コンポーネントプログラムのインストーラーからアップグレード

! 重 要

オールインワンインストーラーを利用して、アップグレードはできません。

■ 「Remote Administrator コンポーネントアップグレード」タスクを使用してアップグレード

「Remote Administrator コンポーネントアップグレード」タスクを使用してアップグレードします。この方法は、ERA Ver6.1 以降からアップグレードするときのみ利用できます。

このタスクの使用方法は「■ Remote Administrator コンポーネントアップグレード」を参照してください。

タスクを使用してアップグレード可能なコンポーネントは以下の通りです。

- ERA サーバー
- ERA エージェント
  タスクのターゲットとして選択された場合、このタスクはネットワークのすべてのコンピューター上でインストールされた ERA エージェントを更新します。
- ERA プロキシ
- ERA Web コンソール
  ERA Web コンソールはオールインワンインストーラーでインストールした場合と Linux コンピューターで以下のいずれかのディレクトリにインストールされた場合にのみタスクを使用してアップグレードができます。
  /var/lib/tomcat8/webapps/, /var/lib/tomcat7/webapps/, /var/lib/tomcat6/webapps/, /var/lib/tomcat/webapps/）
- ERA モバイルデバイスコネクター

手動でアップグレードする必要があるコンポーネントは以下の通りです。

- Apache Tomcat（Apache Tomcat を最新の状態に保つことを強くお勧めします。）
- Apache HTTP Proxy
  オールインワンインストーラーで実行可能。
- ERA Rogue Detection Sensor

RD Sensor のアップグレードについては、ソフトウェアインストールタスクでリポジトリから新しいバージョンを指定してインストールを実行してください。

! 重 要

アップグレードを行う前に、すべての証明書（認証局、サーバー証明書、プロキシおよびエージェント証明書）をバックアップを行ってください。証明書をバックアップするには以下の方法があります。

1. 古い ERA サーバーから認証局証明書を .der ファイルにエクスポートし、外部ストレージに保存します。
2. 古い ERA サーバーからピア証明書（ERA エージェント、ERA サーバー、ERA プロキシ）と秘密鍵を .pfx ファイルにエクスポートし、外部ストレージに保存します。

このタスクを実行するときには、すべてのグループをターゲットとして選択し、ERA インフラストラクチャ全体がアップグレードされるようにします。

●アップグレード前の注意点

アップグレードを実行するコンピューターがインターネット（ESET 社リポジトリ）に接続できる必要があります。また、以下のような点に注意してください。

- ［アクセス権］-［権限設定］を新規作成または編集している場合

！重　要

ESET Remote Administrator V6.5 からアクセス権の仕様が変更されています。［アクセス権］-［権限設定］を新規作成または編集している場合はアップグレード完了後に以下の設定を確認し、必要に応じて再設定してください。

・［アクセス権］-［権限設定］の中の［静的グループ］の値は引き継がずに［すべて］に設定されます。
・監査ログを生成するためには、［アクセス権］-［権限設定］の［機能］で［サーバー設定］に対して書き込み権限を付与する必要があります。

- ERA モバイルデバイスコネクターをアップグレードする場合

！重　要

Mobile Device Connector は v6.5 から HTTPS 証明書内に含まれる CN(共通名) と Mobile Device Connector をインストール際に指定したホスト名、もしくは IP アドレスが一致しない場合、証明書エラーのため ERA サーバーからモバイルデバイスを操作できなくなります。

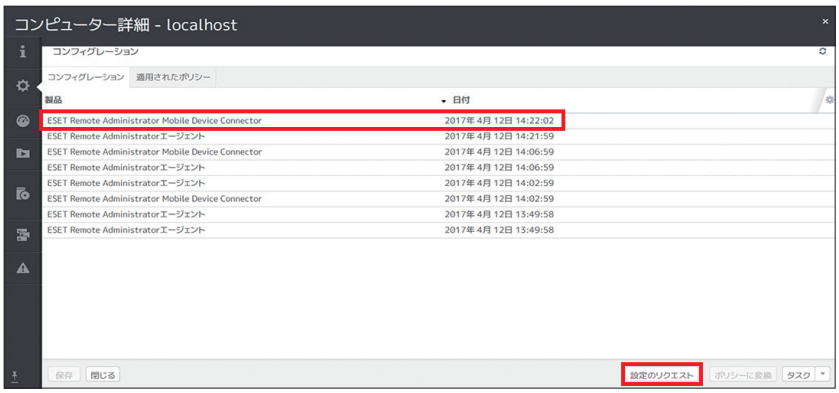
アップグレードの際は、事前に HTTPS 証明書を更新するポリシーを Mobile Device Connector に適用し、設定した期限までにモバイルデバイスから Mobile Device Connector へ接続し、モバイルデバイス内部の HTTPS 証明書を更新する必要があります。

操作手順

1. Mobile Device Connector の HTTPS 証明書の確認

1. ［コンピューター］タブから Mobile Device Connector がインストールされたコンピューターを選択し、［コンピューター詳細］-［コンフィグレーション］タブを選びます。

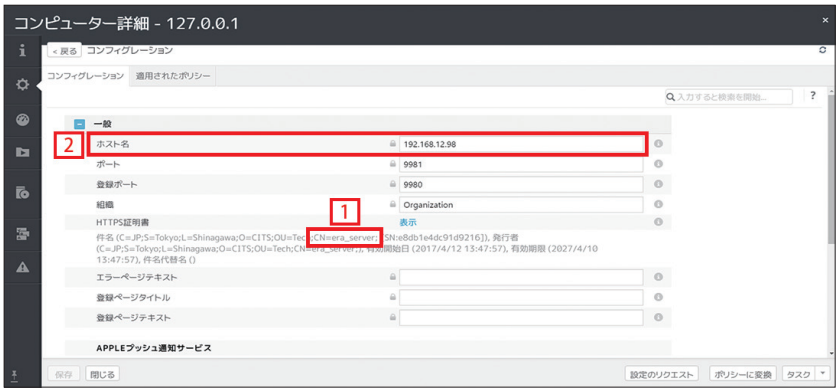
2. ［設定のリクエスト］をクリックし、クリックした当日の日付の ESET Remote Administrator Mobile Device Connector のコンフィグレーションを開きます。



続く

3 赤枠 1 で囲んだ "CN" と赤枠 2 のホスト名の値が一致していることを確認します。

一致していない場合は、以降の作業を実施して "CN" と " ホスト名 " を一致させてからバージョンアップしてください。



2. 更新する Mobile Device Connector の HTTPS 証明書の作成

「6.9.1.2　新しい証明書の作成」の手順を参照して HTTPS 証明書を作成します。

手順を作成する際に入力するモバイルデバイスコネクターの「ホスト」と「共通名」は 1- ③の手順の赤枠 2 のホスト名です。

3. 作成した HTTPS 証明書の割り当て

1 ［ESET Remote Administrator Mobile Device Connector］の新しいポリシーを作成します。

2 ［HTTPS 証明書］を選択します。

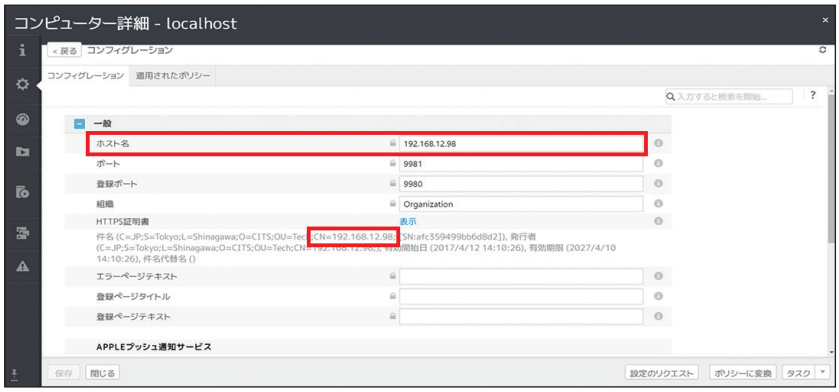
3 カスタム証明書を選択し、作成した証明書（httpscert.pfx）を登録します。

4 ［証明書変更を強制する］に日付を設定し、設定した日付までにすべてのモバイルデバイスが Mobile Device Connector へアクセスするようにして、モバイルデバイス内部の証明書を更新する必要があります。

5 作成したポリシーを Mobile Device Connector に割り当てます。

4. 設定変更後の証明書確認

1. の手順で HTTPS 証明書を確認し、変更後の HTTPS 証明書が適用され "CN" がホスト名と一致していることを確認します。



- ERA サーバーインスタンスがフェールオーバークラスターにインストールされている場合
  ERA サーバーインスタンスがフェールオーバークラスタにインストールされている場合は、各クラスタノードで手動で ERA サーバーコンポーネントをアップグレードする必要があります。ERA サーバーをアップグレードした後は、コンポーネントアップグレードタスクを実行して、残りのインフラストラクチャ（クライアントコンピューターの ERA エージェントなど）をアップグレードできます。

- ERA エージェントが systemd で実行されている Linux クライアントにインストールされている場合
  インフラストラクチャで systemd を実行する Linux クライアント（SysV init scripts または upstart のディストリビューションは影響を受けません）に ERA エージェントがインストールされている場合は、コンポーネントアップグレードタスクを実行する前に、以下のスクリプトしてください。これはバージョン 6.1.450.0 以前でのみ必要です。

```
#!/bin/sh -e
systemd_service=eraagent.service
systemd_service_path="/etc/systemd/system/$systemd_service"
if ! grep "^KillMode=" "$systemd_service_path" > /dev/null
then
echo "Applying 'KillMode' change to '$systemd_service_path'"
sed -i 's/¥[Service¥]/[Service]¥nKillMode=process/' "$systemd_service_path"
else
echo "'KillMode' already set.No changes applied."
exit 0
fi
systemctl daemon-reload
if systemctl is-active $systemd_service > /dev/null
then
echo "Restarting instance of '$systemd_service'"
systemctl restart $systemd_service
fi
```

・Microsoft Windows で Apache HTTP プロキシをアップグレードする場合
Microsoft Windows で Apache HTTP プロキシを使用し、httpd.conf ファイルにカスタム設定がある場合（ユーザー名とパスワードなど）は、元の httpd.conf ファイル（C:¥Program Files¥Apache HTTP Proxy¥conf¥ にある）をバックアップします。カスタム設定を使用しない場合は、httpd.conf ファイルをバックアップする必要がありません。

!重　要

Apache HTTP Proxy を正常にアップグレードした後で、元の httpd.conf ファイルでカスタム設定を行っている場合（ユーザー名とパスワードなど）、バックアップした httpd.conf ファイルの設定をコピーし、カスタム設定のみを新しい httpd.conf ファイルに適用します。新しいアップグレード済みバージョンの Apache HTTP Proxy で元の httpd.conf ファイルを使用しないでください。正しく動作しません。カスタム設定のみをコピーし、新しい httpd.conf ファイルを使用してください。なお、新しい httpd.conf ファイルを手動でカスタマイズすることもできます。設定については、3.3.7　Apache HTTP プロキシのインストールを参照してください。

- 1 つ以上のコンポーネントが既に新しいバージョンにアップグレードされている場合
  1 つ以上のコンポーネントが既に新しいバージョンにアップグレードされている場合は、Remote Administrator コンポーネントアップグレードタスクを使用できません。コンポーネントプログラムのインストーラーからアップグレードを行ってください。
  また、ERA サーバーがフェールオーバークラスタにインストールされている場合は、各クラスタノードで手動で ERA サーバーのコンポーネントをアップグレードする必要があります。

■コンポーネントプログラムのインストーラーからアップグレード

コンポーネントプログラムのインストーラーからアップグレードを行うときは、「3.3 Windows 版コンポーネントインストール」や「3.4 Linux 版 コンポーネントインストール」を参考に、各コンポーネント毎にインストーラーを実行します。

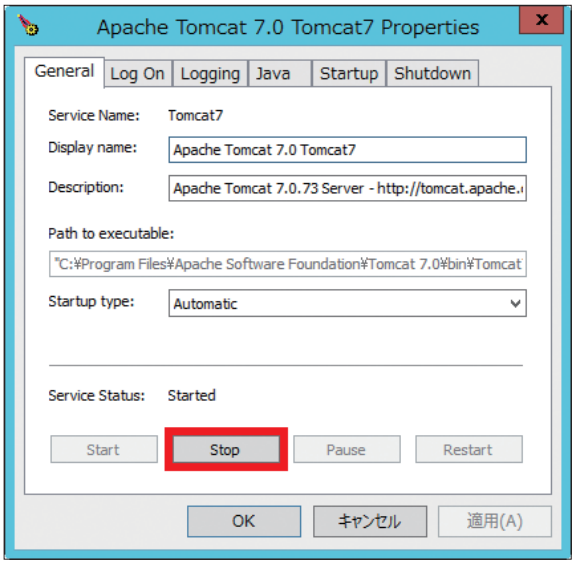
● Windows 版の ESET Remote Administrator のアップグレードの手順

Windows 版の ESET Remote Administrator のアップグレードは、最初に Apache Tomcat のバックアップを保存してから、「3.3 Windows 版コンポーネントインストール」の章を参考にして、各コンポーネント毎にインストーラーを実行します。Apache Tomcat のバックアップは、Apache Tomcat のサービスを停止してから行ってください。

操作手順

1. 「%TOMCAT_HOME%¥bin（たとえば、C:¥Program Files¥Apache Software Foundation¥Tomcat 7.0¥bin）」内にある実行ファイル（たとえば「tomcat7w.exe」）をダブルクリックします。

2. Apache Tomcat のプロパティが表示されます。［General］タブにある［Stop］ボタンをクリックします。



3. 「C:¥Program Files¥Apache Software Foundation¥Tomcat 7.0¥webapps¥¥era¥WEB-INF¥classes¥sk¥eset¥era¥g2webconsole¥server¥modules¥config」フォルダー内にある「EraWebServerConfig.properties」ファイルをバックアップします。

ワンポイント

上記のフォルダーは、64bit 版の Windows を利用している場合のバックアップ対象のフォルダーです。32bit 版の Windows を利用しているときは、「C:¥Program Files (x86)¥Apache Software Foundation¥Tomcat 7.0¥webapps¥era¥WEB-INF¥classes¥sk¥eset¥era¥g2webconsole¥server¥modules¥config」フォルダー内にある「EraWebServerConfig.properties」ファイルをバックアップします。

続く

4 バックアップが完了したら、バックアップ元のフォルダー（64bit 版の Windows の場合、「C:¥Program Files¥Apache Software Foundation¥Tomcat 7.0¥webapps¥era」フォルダー内にあるすべてのファイルとフォルダーを削除します。

ワンポイント

上記のフォルダーは、64bit 版の Windows を利用している場合のフォルダーです。32bit 版の Windows を利用しているときは、「C:¥Program Files (x86)¥Apache Software Foundation¥Tomcat 7.0¥webapps¥era」フォルダー内にあるすべてのフォルダーとファイルを削除します。

5 ERA Web コンソール用のインストーラーファイル「era.war」を「C:¥Program Files¥Apache Software Foundation¥Tomcat 7.0¥webapps¥era」フォルダーにコピーします。

ワンポイント

上記のフォルダーは、64bit 版の Windows を利用している場合のフォルダーです。32bit 版の Windows を利用しているときは、「C:¥Program Files (x86)¥Apache Software Foundation¥Tomcat 7.0¥webapps¥era」フォルダーに「era.war」ファイルをコピーします。

6 手順 3 でバックアップしておいた「EraWebServerConfig.properties」ファイルを「C:¥Program Files¥Apache Software Foundation¥Tomcat 7.0¥webapps¥¥era¥WEB-INF¥classes¥sk¥eset¥era¥g2webconsole¥server¥modules¥config」フォルダーにコピーします。

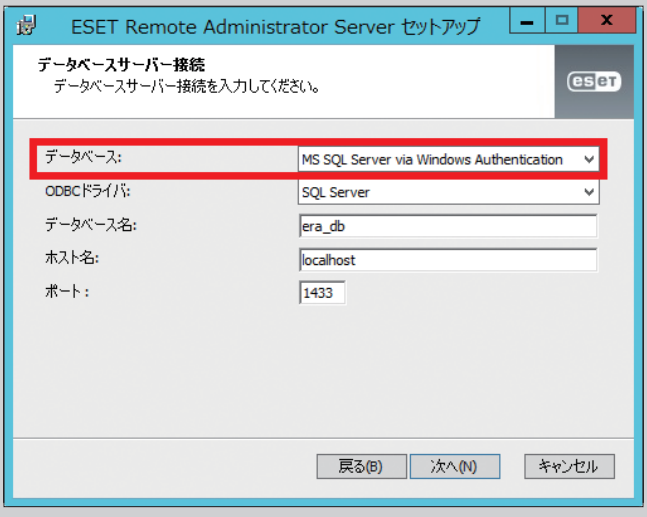
ワンポイント

上記のフォルダーは、64bit 版の Windows を利用している場合です。32bit 版の Windows を利用しているときは、「C:¥Program Files (x86)¥Apache Software Foundation¥Tomcat 7.0¥webapps¥era¥WEB-INF¥classes¥sk¥eset¥era¥g2webconsole¥server¥modules¥config」フォルダーにバックアップしておいた「EraWebServerConfig.properties」ファイルをコピーします。

7 各コンポーネント毎にインストーラーを実行してください。Windows 版のアップグレードの場合は、画面に表示される内容に従って設定してください。

! 重　要

オールインワンインストーラーを利用してインストールした ERA サーバーをアップグレードする場合は、データベースサーバー接続の画面で、データーベースは「MS SQL Server via Windows Authentication」を選択してください。



● Linux 版 ESET Remote Administrator のアップグレード手順

Linux 版の ESET Remote Administrator のアップグレードについては、「3.4 Linux 版 コンポーネントインストール」の章を参考にして、各コンポーネントのインストーラーを実行してください。Linux 版のアップグレードの場合は、インストールオプションを指定せずにインストーラーを実行してください。

ワンポイント

ESET Remote Administrator のアップグレード手順については、以下のサポートページの Q&A を参考にしてください。Q&A の URL：
http://eset-support.canon-its.jp/faq/show/4737?site_domain=business

Chapter 4 最初の手順

この章では、ESET Remote Administrator のインストール後に実施する推奨される初期手順について説明します。
ESET Remote Administrator がインストールされた後に、次の手順に沿って初期手順を実施します。

STEP1	ブラウザーで ERA Web コンソールを開く	「4.1.1 ERA Web コンソールのログイン画面の表示」参照
STEP2	ERA Web コンソールにログインする	「4.1.2 ERA Web コンソールのログイン」参照
STEP3	ERA 構造へクライアントコンピューターを追加する	「4.2.1 ESET Remote Administrator 構造へのクライアントコンピューターの追加」参照
STEP4	クライアントコンピューターでエージェントを展開する	「4.2.2 ERA エージェントの展開」参照

4.1 ERA Web コンソールを開く

ERA Web コンソールは、ERA サーバーと通信するメインインターフェースです。すべての ESET セキュリティソリューションを一元管理できるコントロールパネルと考えることができます。Web ベースのインターフェースであり、あらゆる場所からインターネットに接続している任意のデバイスを使用してアクセスできます。

4.1.1 ERA Web コンソールのログイン画面の表示

ブラウザーで ERA Web コンソールを開くには、以下の方法があります。

■ローカルサーバー（Web コンソールをホストするコンピューター）で開く

- ブラウザーに次の URL を入力します。
  https://localhost/era/

- Windows2008、2003 シリーズの場合
  ［スタート］>［すべてのプログラム］>［ESET］>［ESET Remote Administrator］>［ESET Remote Administrator Web Console］をクリックします。

- Windows2012 シリーズの場合
  【Windows】キー押下（または、画面左下の Windows マークをクリック）>［アプリの画面に移行］>［ESET Remote Administrator Web Console］をクリックします。

■ローカルサーバー以外から Web サーバーに接続して開く

ブラウザーに次の形式で URL を入力します。

https:// yourservername /era/

※「yourservername」は Web サーバーの実際の名前または IP アドレスに置き換えてください。

! 重　要

Web コンソールは安全なプロトコル（HTTPS）を使用するため、セキュリティ証明書または信頼できない接続に関するメッセージがブラウザーで表示される場合があります（正確なメッセージの内容は使用中のブラウザーによって異なります）。これは、ブラウザーでアクセスしようとしているサイトの出所を確認しようとしているためです。次の操作は、ERA Web コンソール URL にアクセスしようとしている場合にのみ適用されます。

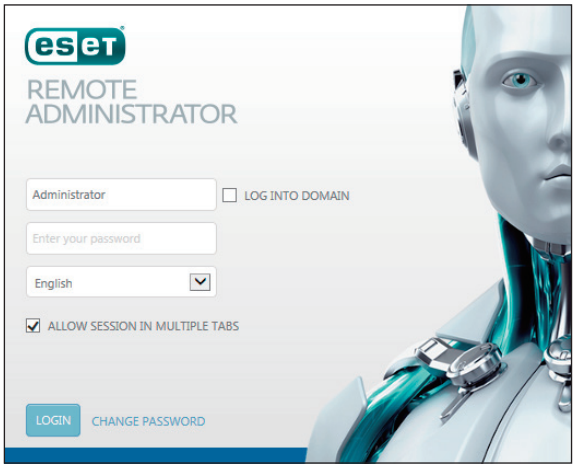
例として

- Internet Explorer の場合は、［このサイトの閲覧を続行する］をクリックします。
- Firefox の場合は、［危険性を理解した上で接続するには］を選択し、［例外を追加］ボタンをクリックしてから、［セキュリティ例外を承認］ボタンをクリックします。

操作手順

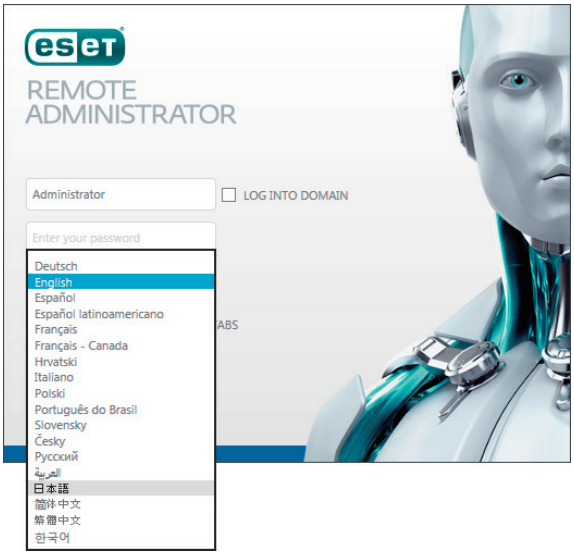
1. 前述のいずれかの方法で ERA Web コンソールを開きます。

   Web サーバーが起動している（ERA Web コンソールサービスが起動している）場合、次の画面が表示されます。



続く

2 「表示言語」リストから［日本語］を選択します。



! 重　要

ログイン画面が表示されない場合や、ログイン画面が読み込み中のまま止まっているように見える場合は、ERA サーバーサービス（ESET Remote Administrator Server サービス）を再起動してください。ERA サーバーサービスが起動し、再度実行されたら、Apache Tomcat サービスを再起動します。この手順を実行すると、Web コンソールログイン画面が正しく読み込まれます。

4.1.2　ERA Web コンソールのログイン

ログイン方法は、目的に合わせて 2 種類に分かれています。

- Administrator のアカウントを使用してログインする
- 使用するアカウントのパスワードを変更してログインする

4.1.2.1　ERA Web コンソールのログイン

ユーザーが ERA Web コンソールにログインするには、ログイン認証情報（ユーザー名とパスワード）が必要です。

操作手順

1 ユーザー名には、「Administrator」が表示されます。

2 「パスワードを入力」には、「3.2.1　ERA サーバー 一括インストール」の操作手順 9 で設定したパスワードを入力します。

ワンポイント

コンポーネントインストールを行った場合は、「3.3.2　ERA サーバーのインストール」の操作手順 11 で設定したパスワードを入力してください。

続く

❸［ログイン］ボタンをクリックします。

!重　要

HTTP 経由で ERA Web コンソールにアクセスして、「暗号化されていない接続です！HTTPS を使用するように Web サーバーを構成してください」または「Web ページが見つかりません」（Internet Explorer）という警告メッセージが表示された場合は、セキュリティの理由から、HTTPS を使用するように ERA Web コンソールを設定することをお勧めします。

!重　要

権限設定がないユーザーは、Web コンソールにログインできますが、関連情報は表示されません。Web コンソールのモジュールで読み取り／書き込み／修正権限を付与するには、該当する権限設定を作成し、ユーザーに割り当てる必要があります。詳細については「6.10　アクセス権」を参照してください。

!重　要

同じ IP アドレスからログインの試みが 10 回失敗すると、この IP アドレスからのさらなるログインの試みは約 10 分間一時的にブロックされます。ログイン試行の IP アドレス禁止は、既存のセッションには影響しません。

!重　要

同じ IP アドレスから無効なセッション ID を 15 回使用すると、この IP アドレスからの今後のすべての接続が約 15 分間ブロックされます。期限切れのセッション ID はカウントされません。期限切れのセッション ID がブラウザーにある場合は、攻撃とみなされません。15 分間の IP アドレス禁止はすべてのアクション（有効な要求を含む）に適用されます。

ワンポイント

ドメインユーザーとしてログインする場合は、[ドメインにログインする]にチェックを入れます。ログインに利用するドメインユーザーは Active Directory 側でリモートデスクトップでログインできるようにアクセス許可の設定を実施し、ユーザー名のフィールドに「ユーザーログオン名（Windows 2000 より以前）（W）:」を入力します。

ワンポイント

［マルチタブでのセッションを有効化］にチェックを入れると、ブラウザーの複数のタブで ERA Web コンソールを開くことができます。

4.1.2.2 パスワードを変更してログイン

パスワードを変更するには、パスワード変更画面で新しいパスワードを設定し、ERA Web コンソールにログインします。

操作手順

1. ［パスワードの変更］をクリックします。

2. 赤枠の中に、現在使用しているパスワードを入力します。

   新しいパスワードが未入力のため、画面上にエラーが表示されます。

続く

3 「新しいパスワードを入力」には、これから使用したいパスワードを入力します。確認のため、「新しいパスワードを再入力」にも同じように入力します。

! 重 要

新しいパスワードは、8 文字以上で設定してください。
また、入力した新しいパスワードが 12 文字に満たない場合は、画面上に警告が表示されます。

パスワードには、小文字、大文字、数字、句読点、その他の文字を 3 種類以上組み合わせて使用することを推奨します。

4 [ログイン] ボタンをクリックします。

続く

5 [OK] ボタンをクリックします。

ワンポイント

パスワードを変更せずにログイン画面に戻る場合は、[別のアカウントを使用] をクリックします。

4.2 展開

ESET Remote Administrator のインストールが成功した後は、ERA エージェントと ESET セキュリティ製品（ESET Endpoint Security、ESET Endpoint アンチウイルス など）をネットワークのクライアントコンピューターに展開する必要があります。
展開の手順は次のとおりです。

STEP1	クライアントコンピューターを ERA グループ構造に追加する （この手順は ERA エージェントをサーバータスクを用いてリモート展開する場合のみ必要です）	P161 参照
STEP2	ERA エージェントをクライアントコンピューターに展開する	P173 参照
STEP3	ESET 製品をクライアントコンピューターに展開する	P256 参照

4.2.1 ESET Remote Administrator 構造へのクライアントコンピューターの追加

ERA エージェントをサーバータスクを用いてリモート展開するために、ESET Remote Administrator にクライアントを追加するには、3 つの方法があります。

Active Directory 同期	静的グループ同期サーバータスクを実行する	P161 参照
名前 /IP の手動入力	自動的に検出または追加されないコンピューターを手動で追加する	P164 参照
RD Sensor の使用	RD Sensor を使用してコンピューターを追加する	P167 参照

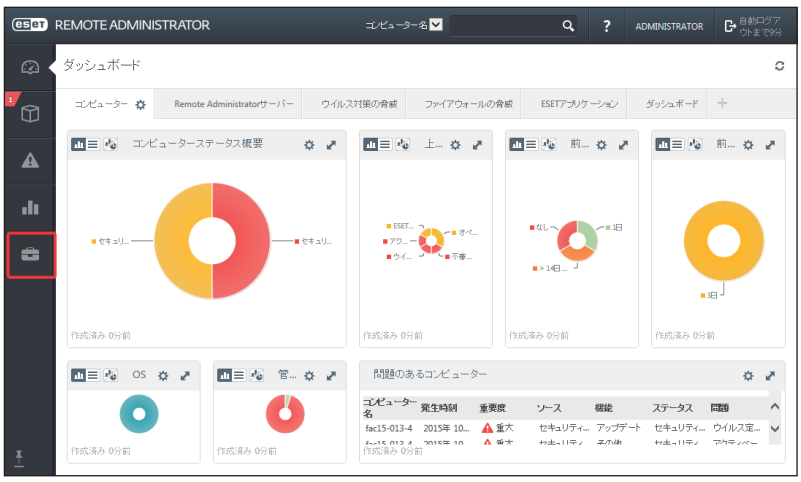
4.2.1.1 Active Directory 同期の使用

「管理」メニューの「サーバータスク」には、ESET Remote Administrator インストール時に定義済みの既定のタスクが作成されます。「静的グループの同期」のタスクを実行して Active Directory（以下 AD）同期を行います。

操作手順

1 ［管理］メニューをクリックします。

「管理」画面が表示されます。



続く

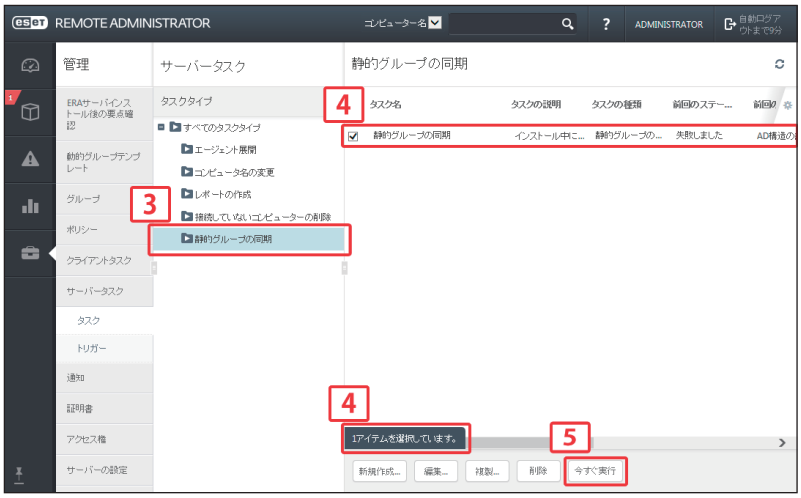
2 [サーバータスク] サブメニューをクリックします。

3 「タスクタイプ」リストから [静的グループの同期] を選択します。

4 タスクの一覧から [静的グループの同期] にチェックを入れます。

選択したアイテム数を案内するメッセージが表示されます。

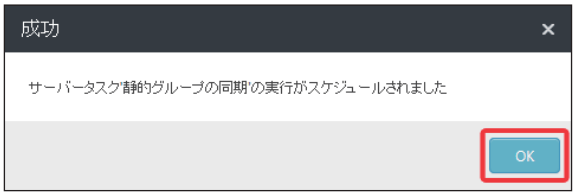
5 [今すぐ実行] ボタンをクリックします。



タスクのスケジュールが成功すると「成功」画面が表示されます。

続く

6 [OK] ボタンをクリックします。



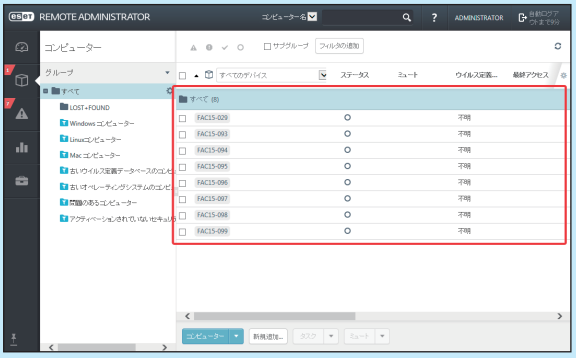
操作手順 4 で選択したタスクの状態が更新されます。

! 重 要

EERA サーバーと AD が同一サーバー上に無い場合は、手順 3 の後に次の操作を行う必要があります。
1. タスクの一覧から［静的グループの同期］にチェックを入れます。
2.［編集］ボタンをクリックします。
3.「設定」の「サーバー」「ログイン」「パスワード」を入力します。
4.［終了］ボタンをクリックします。
手順 4 の操作を続けて行ってください。

ワンポイント

同期の実行が成功すると、「コンピューター」画面に一覧で表示されます。
AD 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。
画面の詳細については「5.3 コンピューター」を参照してください。



ワンポイント

新しい AD 同期タスクを作成する場合は、新しいコンピューターを追加するグループを選択し、「同期するオブジェクト」、「コンピューター作成の競合処理」、「同期モード」、「サーバー接続設定」を設定します。「同期モード」は［Active Directory/Open Directory/LDAP］を選択します。
詳細は「6.7.3.5 静的グループの同期」を参照してください。

4.2.1.2 名前 /IP の手動入力

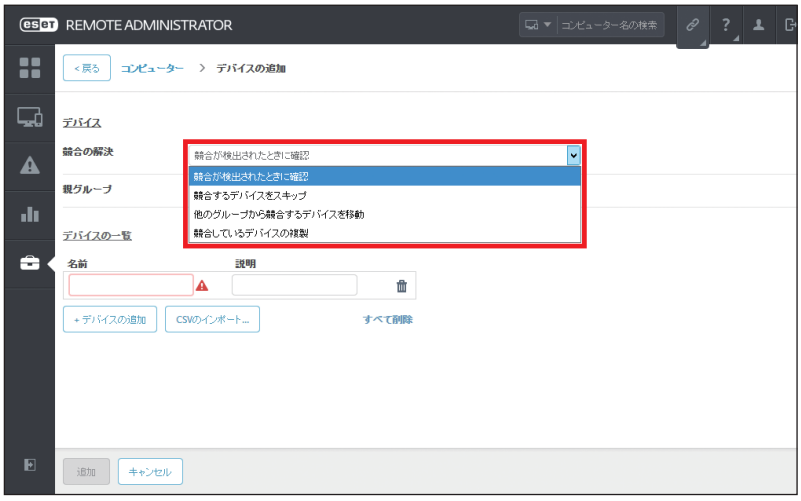
自動的に検出または追加されないコンピューターを手動で追加します。

操作手順

1. ［コンピューター］メニューをクリックします。
2. 「グループ」リストからコンピューターを追加したい静的グループ（ここでは［LOST+FOUND］）を選択します。
3. ［新規追加］ボタンをクリックします。
4. ［コンピューター］をクリックします。

5. 「競合の解決」を選択します。

「名前」が未入力のため、画面上にエラーが表示されます。



続く

6 「名前」に追加するコンピューターの IP アドレスまたはホスト名を入力し、【Enter】キーを押します。

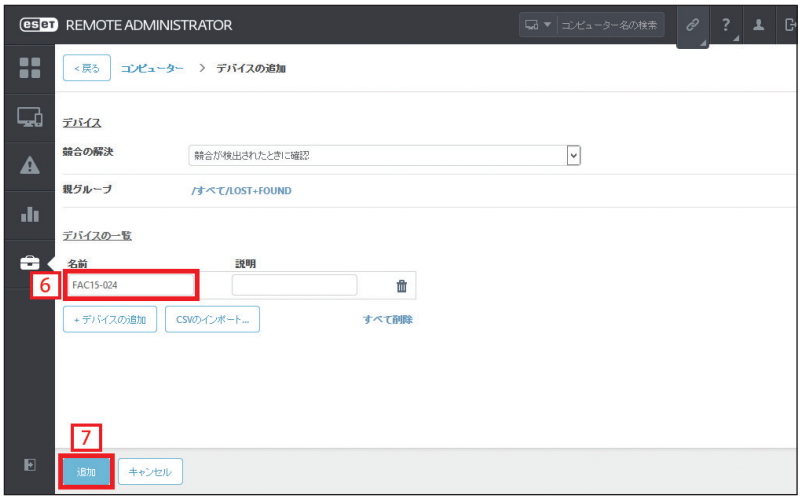
! 重 要

複数のコンピューターを追加する場合は、［+ デバイスの追加］ボタンをクリックして続けて入力することができます。ただし、複数のコンピューターをまとめて追加すると時間がかかる場合がありますので、台数が多い場合は複数回に分けて追加してください。
不用になった行は右端の［削除］ボタンをクリックして、削除しておきます。

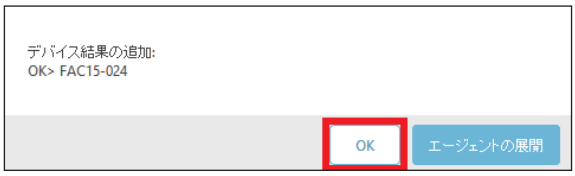
ワンポイント

必要に応じて「説明」を追加します。

7 ［追加］ボタンをクリックします。



8 ［OK］ボタンをクリックします。



続く

!重 要

「競合が検出されたときに確認」を選択している場合、追加したコンピューターがすでに存在している（ここでは指定した親グループに既に存在している）と、確認画面が表示されます。重複したコンピューターの処理方法を選択してください。

スキップ	画面に表示されているコンピューターの追加の処理は行われません。複数のコンピューターを追加している場合は、次のコンピューターの追加の処理を行います。
再試行	再度、追加の処理を行います。
移動	指定した親グループへ移動します。
複製	指定した親グループ内に追加されます。
キャンセル	追加処理を取り消します。

ワンポイント

続けて ERA エージェントの展開を行う場合は、［エージェントの展開］ボタンをクリックします。
詳細は「4.2.2 ERA エージェントの展開」を参照してください。

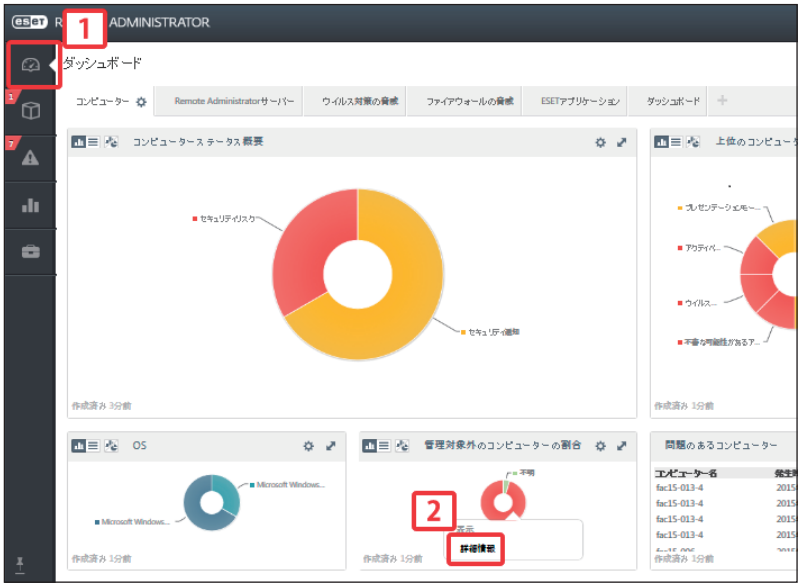
4.2.1.3 RD Sensor の使用

AD 同期を使用しない場合は、RD Sensor を使用すると ESET Remote Administrator 構造へコンピューターを簡単に追加することができます。
RD Sensor はネットワーク内のコンピューターを自動的に検索し、その情報を ERA サーバーに送信しているため、管理対象外になっているコンピューターの情報を一覧で確認することができます。一覧から ESET Remote Administrator 構造へ追加するコンピューターを選択することができます。

■ 1 台のコンピューターを追加する

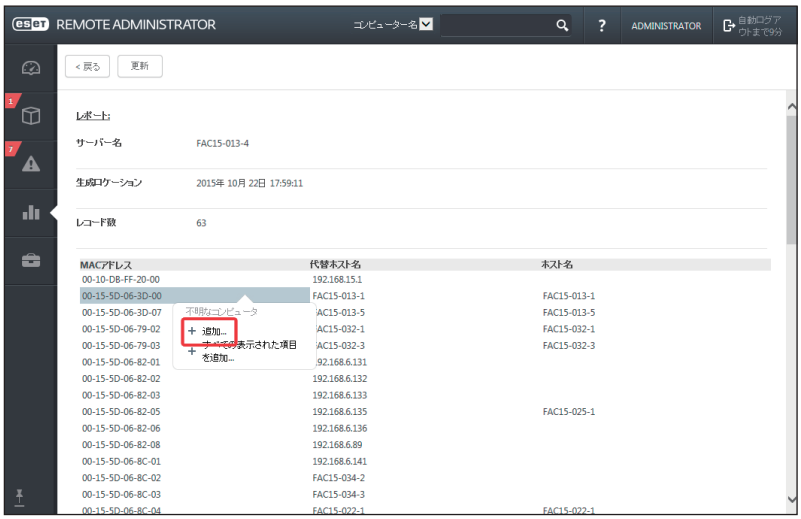
操作手順

1. ［ダッシュボード］メニューをクリックします。
2. 「管理対象外コンピューターの割合」レポートのグラフから［Rogue］（赤い部分）をクリックし、「表示」コンテキストメニューから［詳細情報］を選択します。



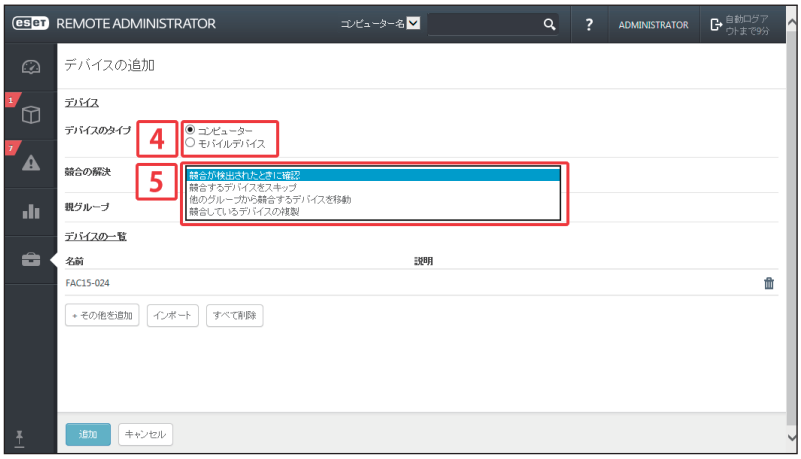
続く

3 RD Sensor で検出されたコンピューターの一覧から追加するコンピューターの行をクリックし、「不明なコンピューター」コンテキストメニューから［追加］を選択します。

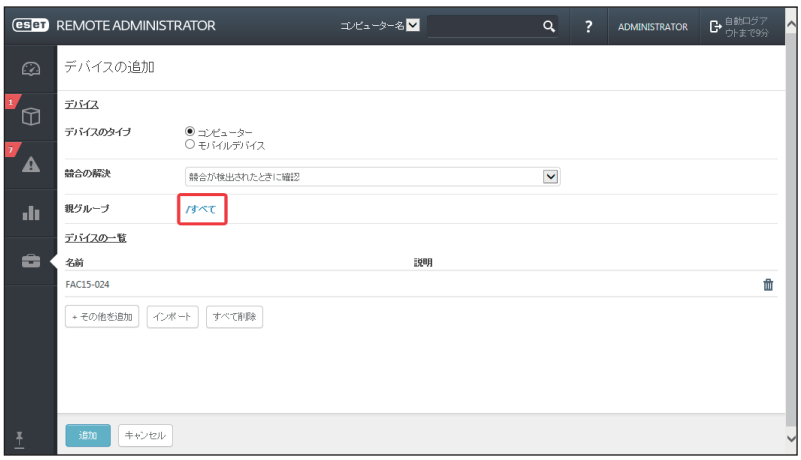


4 「デバイスのタイプ」を選択します。

5 「競合の解決」を選択します。



6 「親グループ」の［/ すべて］をクリックします。



続く

7 コンピューターを追加したい静的グループ（ここでは［LOST+FOUND］）を選択し、［OK］ボタンをクリックします。

8 「名前」を確認または必要に応じて変更します。

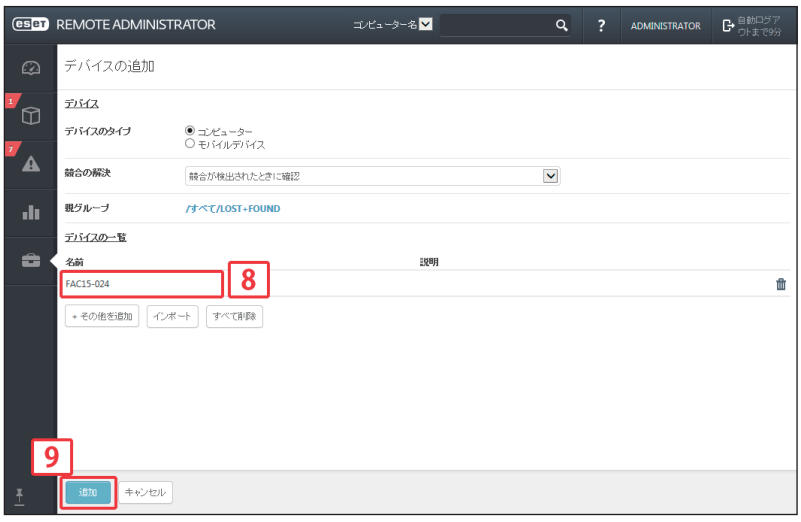
ワンポイント

定義済みの名前を使用するか、独自の名前を指定できます。ここで設定する名前は、実際のホスト名ではなく、ERA Web コンソールで使用される表示名です。

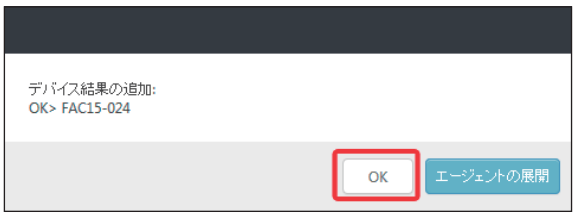
ワンポイント

必要に応じて「説明」を追加します。

9 ［追加］ボタンをクリックします。



10 ［OK］ボタンをクリックします。

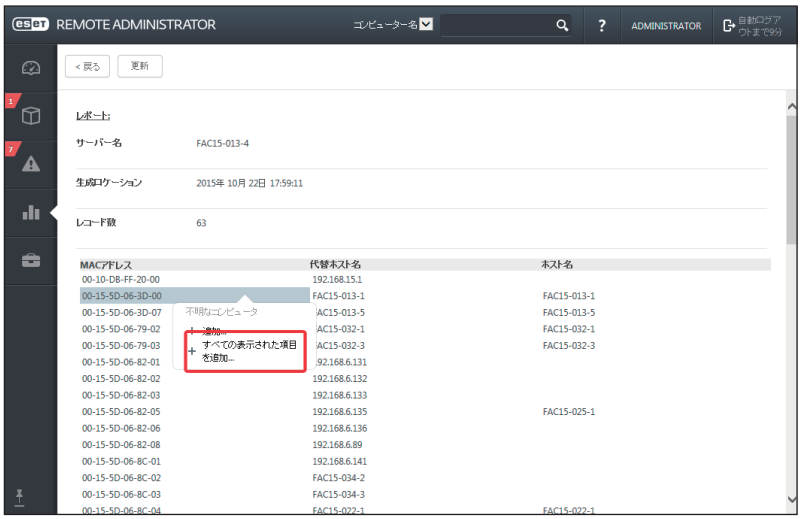


■表示されているすべてのコンピューターを追加する

操作手順

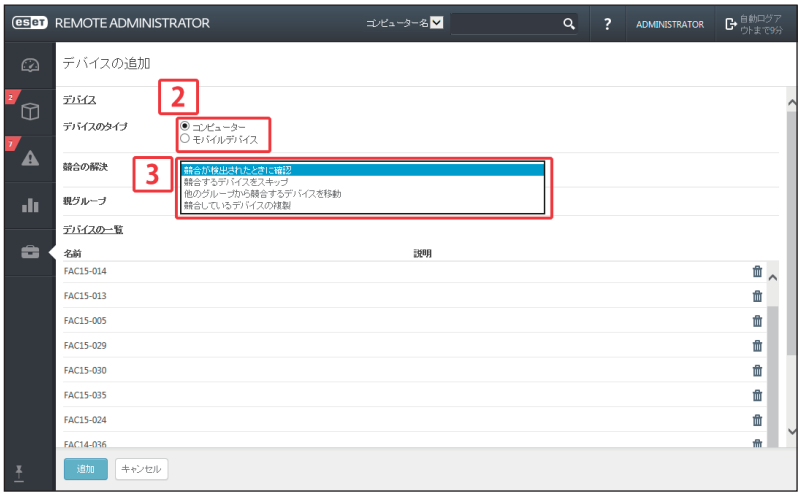
「■ 1 台のコンピューターを追加する」手順 2 の続き

1. RD Sensor で検出されたコンピューターの一覧いずれかの行をクリックし、「不明なコンピューター」コンテキストメニューから［すべての表示された項目を追加］を選択します。



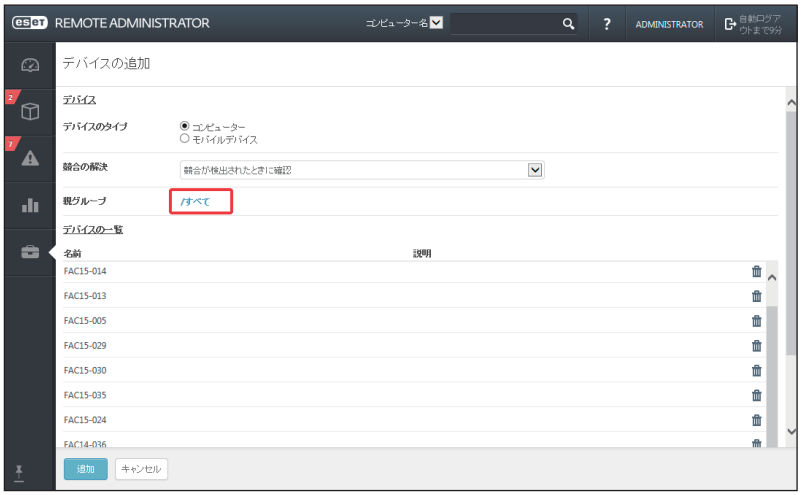
2. 「デバイスのタイプ」を選択します。

3. 「競合の解決」を選択します。



続く

4 「親グループ」の［/ すべて］をクリックします。



5 コンピューターを追加したい静的グループ（ここでは［LOST+FOUND］）を選択し、［OK］ボタンをクリックします。

6 「デバイスの一覧」に追加するコンピューターのリストが表示されます。追加しないコンピューターがある場合は、この時点で行の右端の［削除］ボタンをクリックします。

ワンポイント

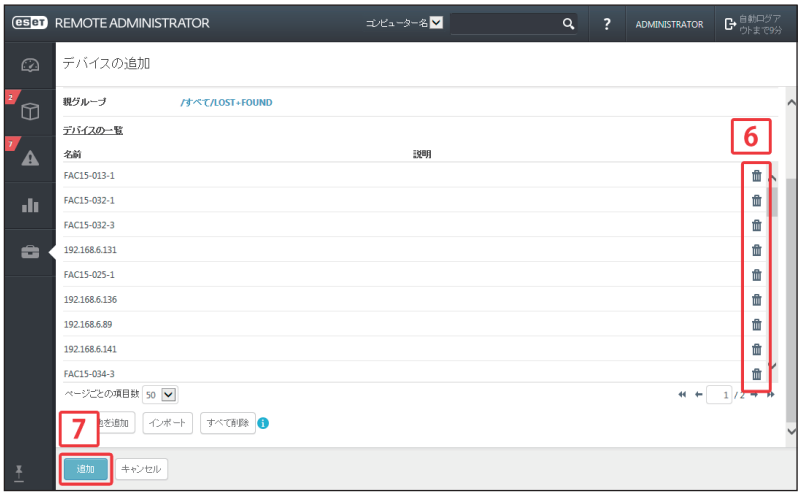
コンピューターの台数が多い場合は複数ページに跨って表示されるため、画面右下のページ移動ボタンで確認してください。

ワンポイント

必要に応じて「説明」を入力します。

続く

7 [追加] ボタンをクリックします。



8 [OK] ボタンをクリックします。

ワンポイント

RD Sensor 検査の結果は、detectedMachines.log ログファイルに書き込まれます。このファイルには、ネットワーク上で検出されたコンピューターのリストが含まれます。detectedMachines.log ファイルは ERA サーバーの次の場所にあります。

- Windows
  C:¥ProgramData¥ESET¥Rouge Detection Sensor¥Logs¥detectedMachines.log
- Linux
  var/log/eset/RemoteAdministrator/RogueDetectionSensor/detectedMachines.log

4.2.2 ERA エージェントの展開

ERA エージェントをクライアントコンピューターに展開します。クライアントコンピューターで実行中の ESET セキュリティソリューションは ERA エージェント経由でのみ ERA サーバーと通信するため、ERA エージェントは非常に重要な役割を果たします。
ERA エージェントの展開には ERA サーバーとの接続情報である、ピア証明書（エージェント）および証明局の公開鍵ファイル（以下　証明書ファイル）が必要です。

ERA エージェント展開の前提条件は次のとおりです。

- ERA サーバーおよび ERA Web コンソールのサーバーコンピューターへのインストール
- ピア証明書（エージェント）の作成とエクスポート※1
- 認証局の作成と、公開鍵ファイルのエクスポート※1
- クライアントコンピューターとサーバーコンピューターが正しく接続されていること

※1　エクスポートは、管理ツールでのインストールおよびオフラインインストール時のみ

ERA エージェントの展開方法にはリモート展開とローカル展開の手法があり、リモート、ローカル共にいくつかの具体的な展開方法を選択することが可能です。
さらに、ERA エージェントのインストーラーには、32bit 版と 64bit 版が用意されています。使用環境を確認し、適切な ERA エージェントインストーラーの選択と展開操作を行ってください。

! 重　要

この章では、64bit 版のインストーラーを使用して操作の説明をします。
インストーラーの保存先は、Windows は C:¥x64¥installers、Linux OS は /root/x64、Mac OS X は /User/user/Desktop としています。

! 重　要

ERA エージェントのインストールには、管理者権限が必要です。

ワンポイント

コンピューターメニュー画面、管理メニュー内の ERA エージェントの展開を選択すると、「展開オプションを選択」画面が表示され、展開方法を選択できます。

GPO または SCCM を利用して展開	4.2.2.1　ERA エージェントのリモート展開	P175 参照
オールインワンインストーラーを作成（Windows 製品のみ）	4.2.2.2　オールインワンインストーラー	P194 参照
エージェントライブインストーラの作成	4.2.2.3　エージェントライブインストーラー	P210 参照
サーバータスクを利用したエージェントインストール	4.2.2.1　ERA エージェントのリモート展開	P175 参照
Web サイトから ERA エージェントをダウンロード（ローカルエージェント展開の手順）	4.2.2.4　Windows へのローカル展開	P229 参照
スタンドアロン展開ツールを使用する	■スタンドアロン展開ツールを使用	P210 参照

■リモート展開

ERA Web コンソールから ERA エージェントを配布する「サーバータスク」を設定する方法と、GPO（グループポリシーオブジェクト）または SCCM（Microsoft System Center Configration manager）を使用する方法があります。

■ローカル展開

ERA エージェントのインストーラーまたはエージェントライブインストーラーを使用して、クライアントコンピューターに保存したインストーラーから展開します。ローカル展開は次の 4 種類です。

オールインワンインストーラー	ERA エージェントと ESET 製品の設定を組み込んだオールインワンインストーラーを作成し、使用します（Windows のみ対応）
エージェントライブインストーラー	ERA Web コンソールから生成されたスクリプトファイルを使用します。
サーバー支援インストール	ERA エージェントのインストーラーを使用します。ERA サーバーから証明書を自動的にダウンロードします。※ Mac OS X では非対応。
オフラインインストール	ERA エージェントのインストーラーを使用します。証明書を事前にエクスポートし、手動で設定する必要があります。

4.2.2.1 ERA エージェントのリモート展開

リモート展開は、サーバータスクを使用する方法と、GPO（グループポリシーオブジェクト）または SCCM（Microsoft System Center Configration manager）を使用する方法のどちらかを選択することができます。
サーバータスクを使用する場合は、ERA Web コンソールでの操作となります。

ワンポイント

ERA エージェントをクライアント数が多いグループに展開する場合、ERA エージェントの通信間隔が短いとネットワークの負荷が高くなる可能性がありますので、事前にポリシー設定の通信間隔を設計することをお奨めします。

! 重 要

サーバータスクを使用したリモート展開の場合、すべてのクライアントコンピューターがインターネットに接続している必要があります。

■リモート展開と権限

管理者権限以外のユーザーが、サーバータスクを使用した ERA エージェントのリモート展開をできるようにする場合は、そのユーザーに適切な権限が設定されている必要があります。

次の権限は、サーバータスクを使用した ERA エージェントのリモート展開で必要です。

- 展開が実行されるグループとコンピューターの使用権限
- 静的グループすべてへのアクセスがある証明書の使用権限
- サーバータスクとトリガーセクションのエージェント展開の使用権限
- エージェント展開の使用権限

! 重 要

エージェント展開の権限では、ユーザーがリモート展開を実行し、サーバータスクの「エージェント展開」タスクと組み合わせて使用されます。

■ GPO や SCCM を使用したリモート展開

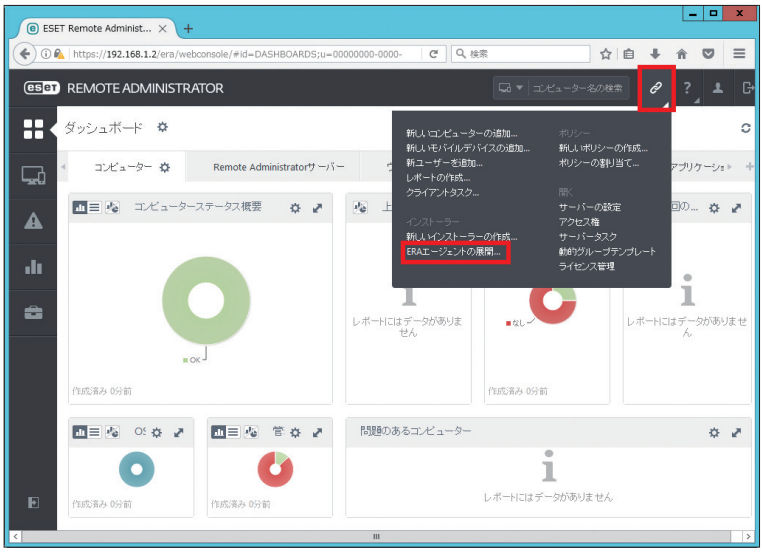
GPO や SCCM を使用したリモート展開では、ERA エージェントのインストーラーである「Agent_x64.msi」や「Agent_x86.msi」をベースにして「install_config.ini」ファイルを最初に作成します。ERA エージェントのインストーラーは、弊社ユーザーズサイトから事前にダウンロードしておく必要があります。「install_config.ini」ファイルを作成したら、次に GPO や SCCM でリモート展開を行います。

STEP1	「「install_config.ini」ファイルの作成」	P176 参照
STEP2	GPO または SCCM を使用したリモート展開	P183 参照

●「install_config.ini」ファイルの作成

操作手順

1 ERA Web コンソールの［クイックリンク］セクションをポイントし、［ERA エージェントの展開］をクリックします。

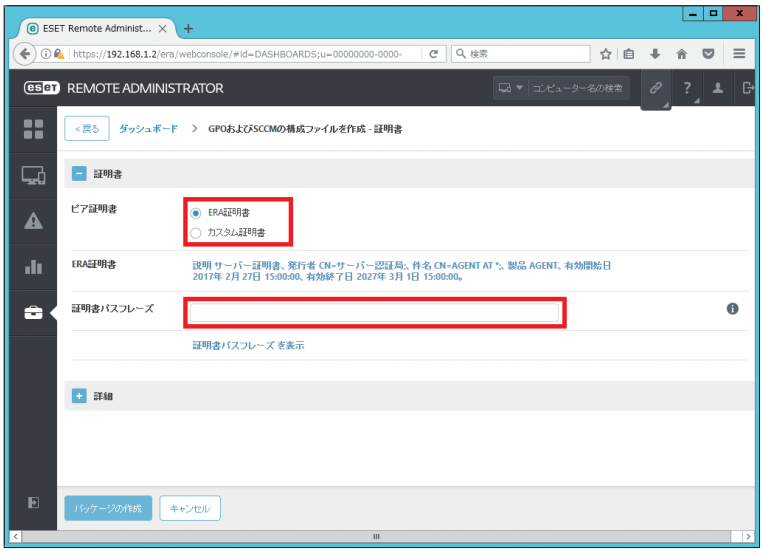


2 「GPO または SCCM を利用して展開」の［スクリプトの作成］をクリックします。

「GPO および SCCM の構成ファイルを作成」画面が表示されます。

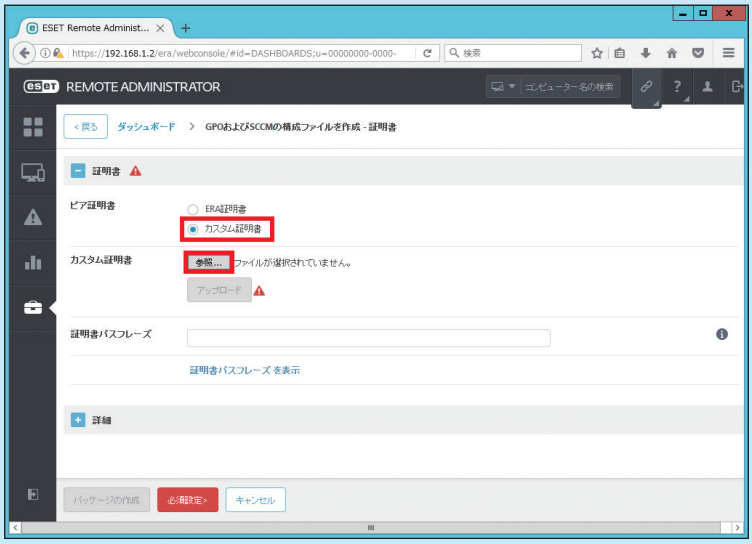
続く

3 「証明書」の設定を行います。ピア証明書の選択（ここでは［ERA 証明書］）を行い、ピア証明書にパスフレーズを設定しているときは、パスフレーズを入力します。



ワンポイント

証明書には、ピア証明書および ERA 認証局が使用可能な証明書に基づいて自動的に選択されます。自動選択されたものとは別の証明書を使用する場合は、選択されている ERA 証明書をクリックし、使用可能な証明書のリストを表示して、使用する証明書を選択します。カスタム証明書を使用する場合は、「カスタム証明書」をクリックして選択し、.pfx 証明書ファイルをアップロードします。

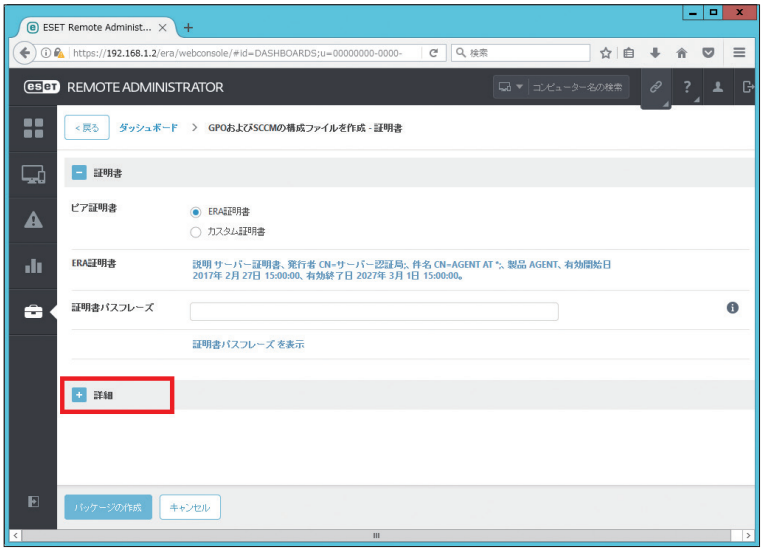


ワンポイント

パスフレーズは、ERA のインストール中にパスフレーズを指定した場合やカスタム証明書を作成し、パスフレーズを設定しているときに入力します。パスフレーズの設定を行っていないときは、証明書パスフレーズフィールドは空欄にします。

続く

4 オールインワンインストーラーのカスタマイズを行うときは、［詳細］をクリックします。

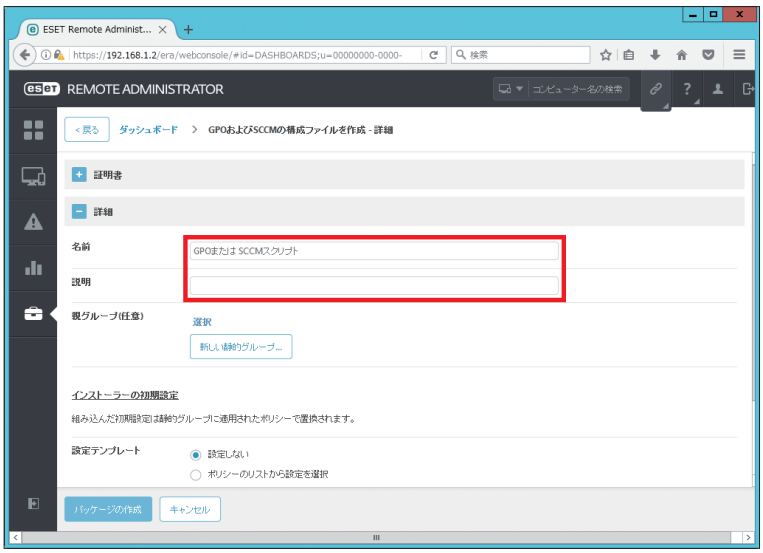


ワンポイント

［詳細］をクリックすると、ERA エージェントと ESET ライセンス製品のポリシー設定、ERA サーバーホスト名とポート、親グループの設定などを行えます。

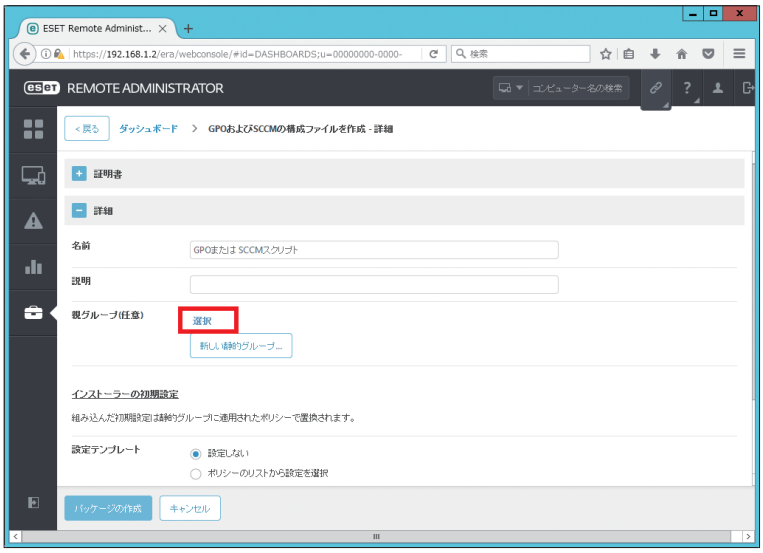
「詳細」の設定画面が展開されます。

5 「名前」と「説明」を必要に応じて入力します。



続く

6 必要に応じて ERA エージェントインストーラーで使用するクライアントコンピューターの親静的グループを選択します。すでに作成済みの親静的グループから選択するときは、[選択]をクリックします。

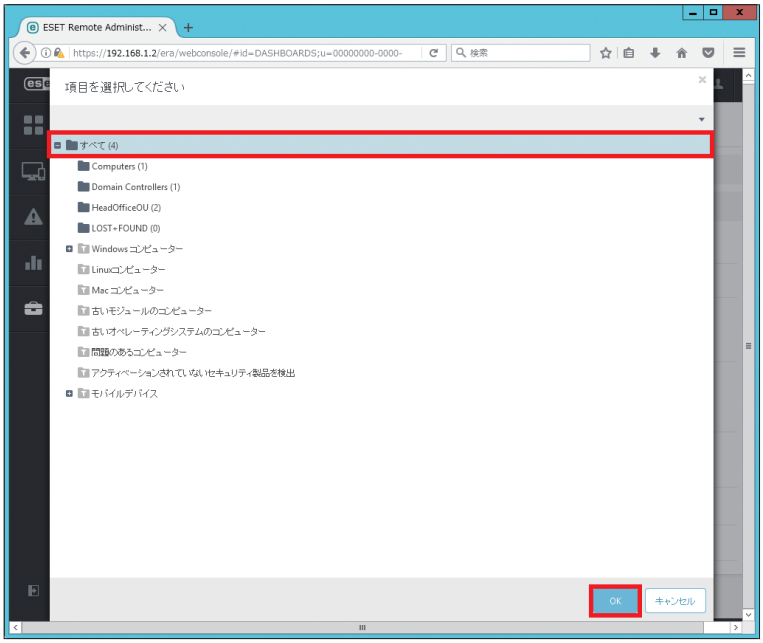


グループの選択画面が表示されます。

ワンポイント

新しい親静的グループを作成する場合は、[新しい静的グループ] をクリックして、画面の指示に従って操作します。新しいグループを作成すると、そのグループが自動的に選択されます。

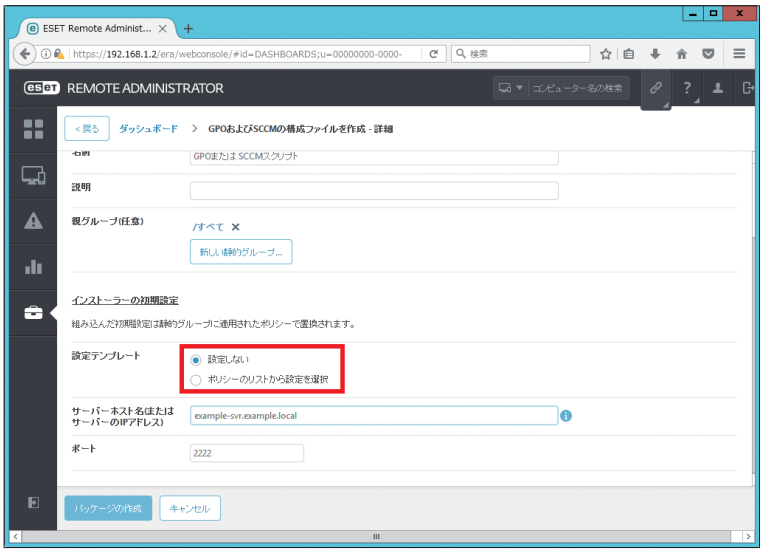
7 所属させるグループを選択し、[OK] ボタンをクリックします。



「GPO および SCCM の構成ファイルを作成」画面に戻ります。親グループに手順 7 で選択したグループが表示されます。

続く

8 インストーラーの初期設定を行います。設定テンプレートを「設定しない」または「ポリシーのリストから設定を選択」の中から選択します。

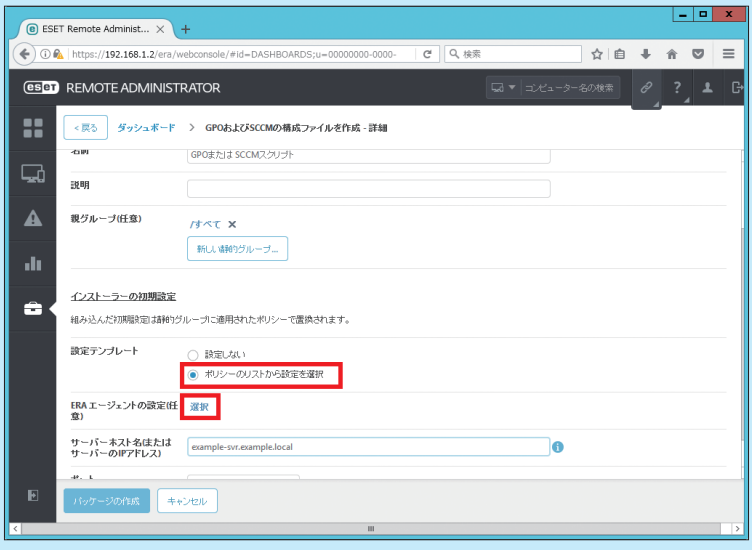


ワンポイント

設定テンプレートは、インストールするクライアントコンピューターのポリシーを設定します。

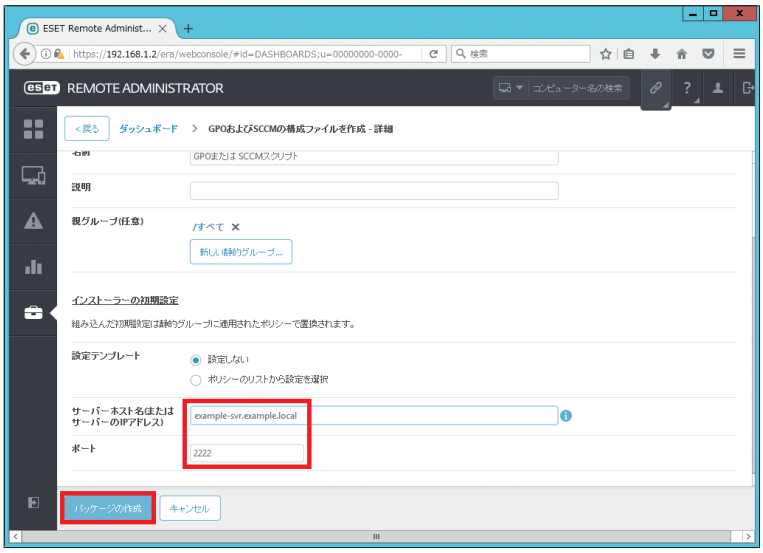
・設定しない - 親静的グループにマージされたポリシーのみが適用されます。

・ポリシーのリストから設定を選択する - 選択したポリシーを ERA エージェントに適用する場合は、このオプションを使用します。「ERA エージェントの設定（任意）」の［選択］をクリックして、使用可能なポリシーのリストから設定したいポリシーを選択します。適したポリシーがないときは、ERA Web コンソールの「管理」の「ポリシー」セクションで新しいポリシーを作成するか、既存のポリシーをカスタマイズしておき、最初の手順から「install_config.ini」ファイルの作成をやり直します。



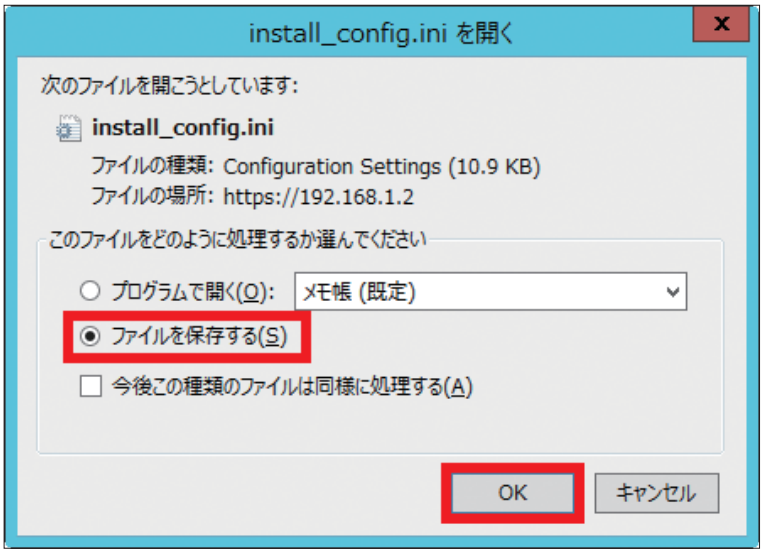
続く

9 必要に応じて、ERA サーバーホスト名または IP アドレスとポート番号を設定し、［パッケージの作成］をクリックします。



保存画面が表示されます。

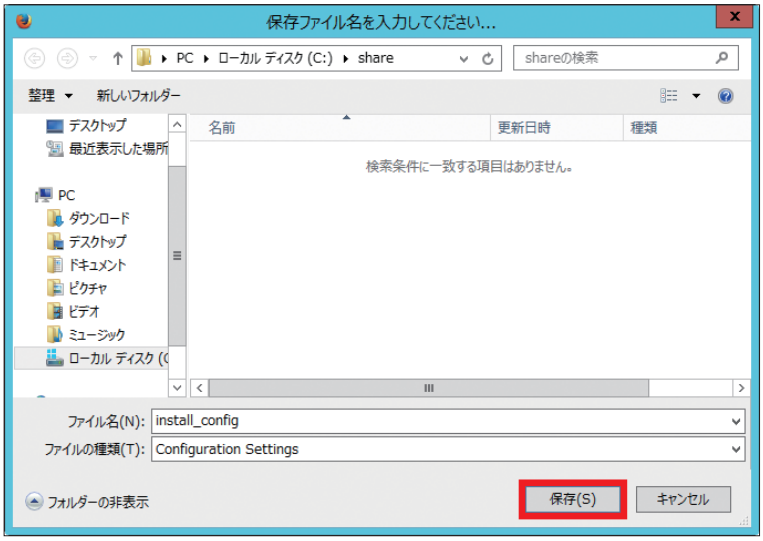
10 ［ファイルを保存する］をクリックしてオンにし、［OK］ボタンをクリックします。



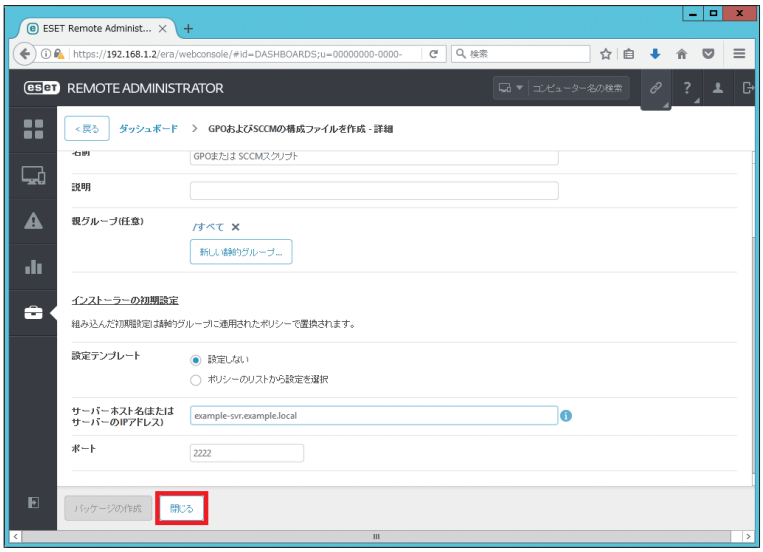
ファイルの保存画面が表示されます。

続く

⑪「install_config.ini」ファイルの保存先を選択し、［保存］ボタンをクリックします。



⑫［閉じる］ボタンをクリックします。「install_config.ini」ファイルの作成は完了です。



● GPO でのリモート展開

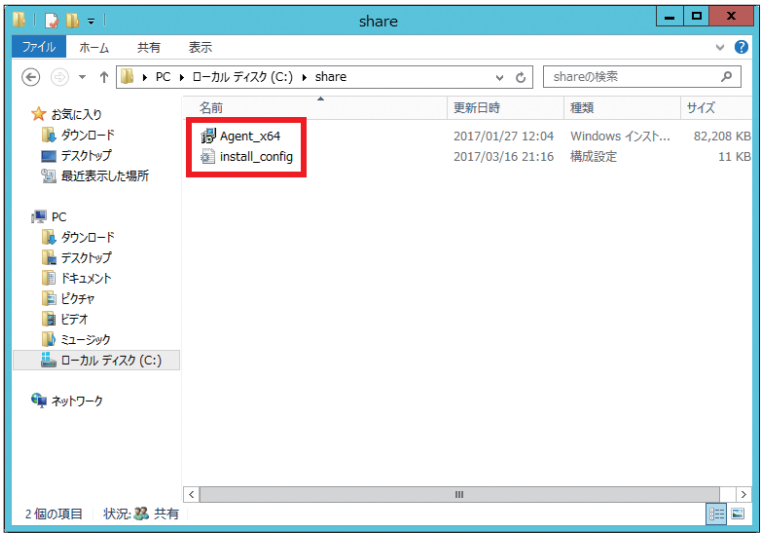
GPO（グローバルポリシーオブジェクト）を使用して、リモート展開します。GPO では、Windows 上で有効なポリシーを作成します。

GPO でのリモート展開に必要な条件は次のとおりです。

- ERA エージェントインストーラー「Agent_x86.msi」または「Agent_x64.msi」の用意
- 「install_config.ini」ファイルの用意
- 読み取り / 実行権限を付与している、クライアントコンピューターが接続可能な共有フォルダーの用意

操作手順

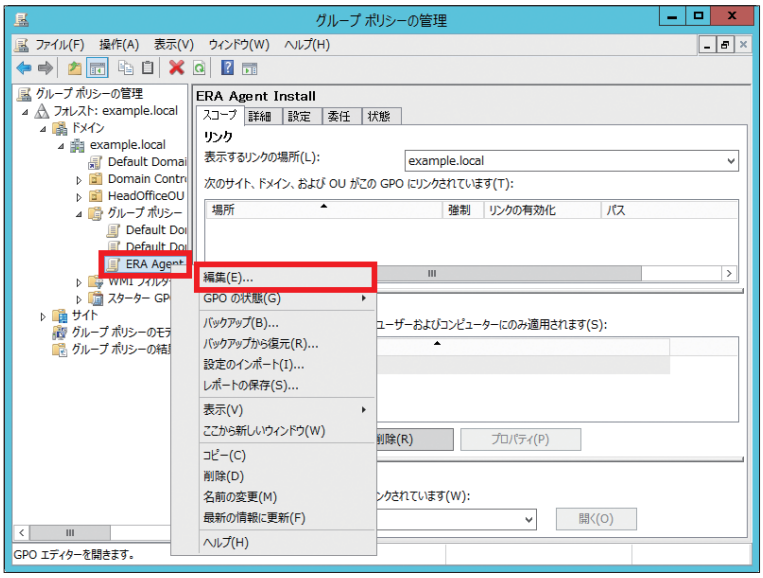
1. ERA エージェントのインストーラーである「Agent_x86.msi」または「Agent_x64.msi」と、作成した「install_config.ini」ファイルをクライアントコンピューターから接続可能な共有フォルダーに保存します。



2. GPO を起動します。

続く

3 左側のフォレストツリーに表示されている展開対象が含まれる「グループポリシーオブジェクト」を右クリックし、[編集] をクリックします。

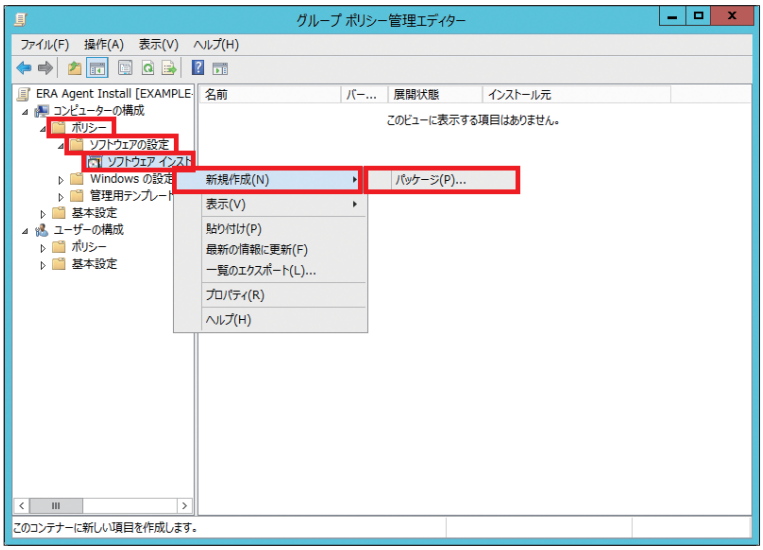


「グループポリシー管理エディター」画面が表示されます。

! 重 要

対象のクライアントコンピューターを含む既存のグループポリシーオブジェクトがない場合は、新しく作成してください。

4 左側のコンピューター構成以下に表示されている、[ポリシー] をダブルクリックし、[ソフトウェアの設定] をダブルクリックします。「ソフトウェアのインストール」を右クリックし、[新規作成] > [パッケージ] とクリックします。

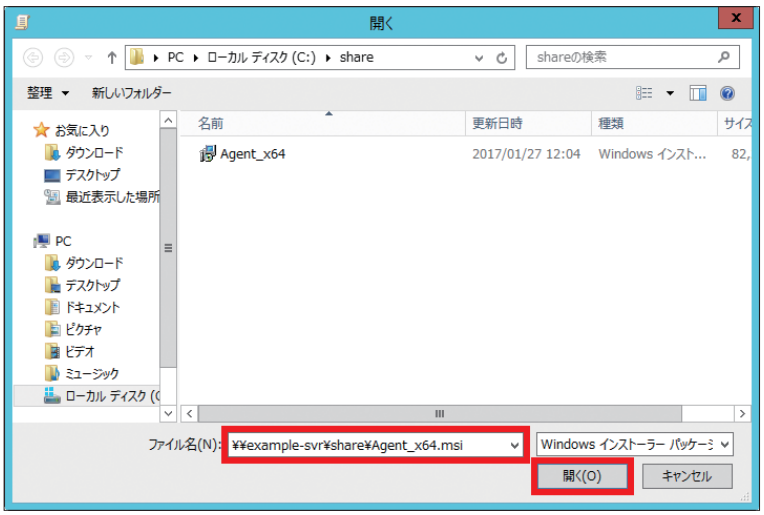


既存の .msi ファイルの選択画面が表示されます。

続く

5 「開く」ダイアログボックスのファイル名をインストーラパッケージの完全な汎用命名規則（UNC）パスで入力し、［開く］ボタンをクリックします。

例：¥¥example-svr¥share¥Agent_x64.msi

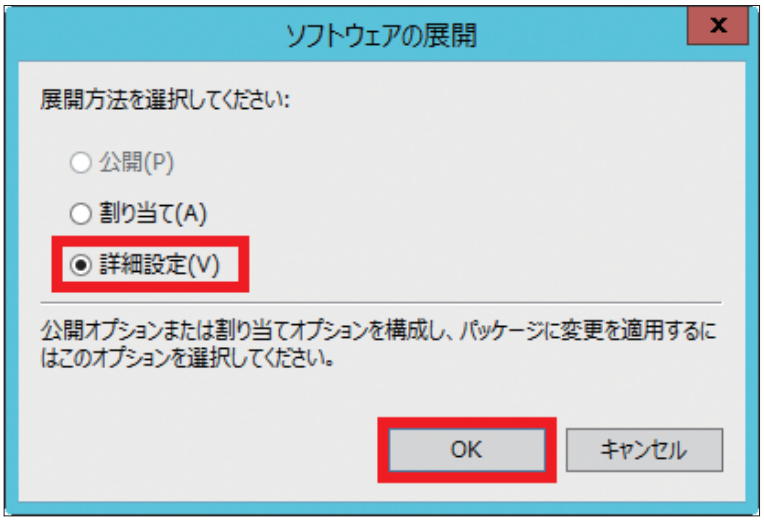


! 重 要

「開く」ダイアログボックスに入力するファイル名は、UNC パスを使用する必要があります。

「ソフトウェアの展開」画面が表示されます。

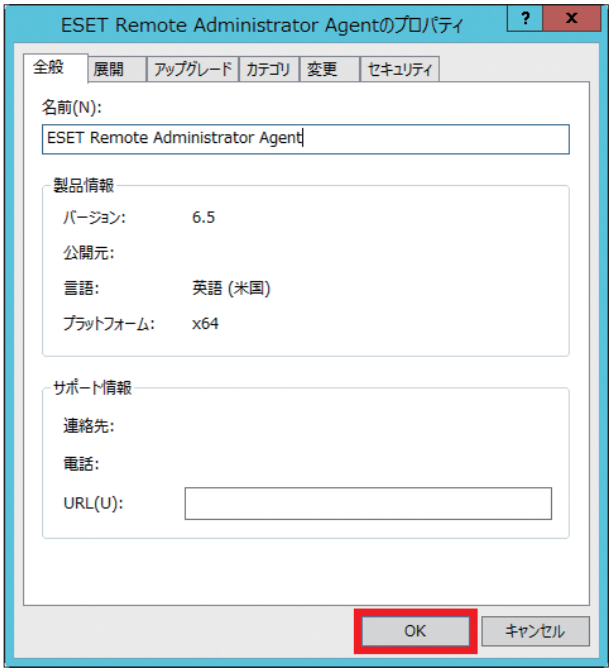
6 ［詳細設定］を選択し、［OK］ボタンをクリックします。



「ESET Remote Administrator Agent のプロパティ」画面が表示されます。

続く

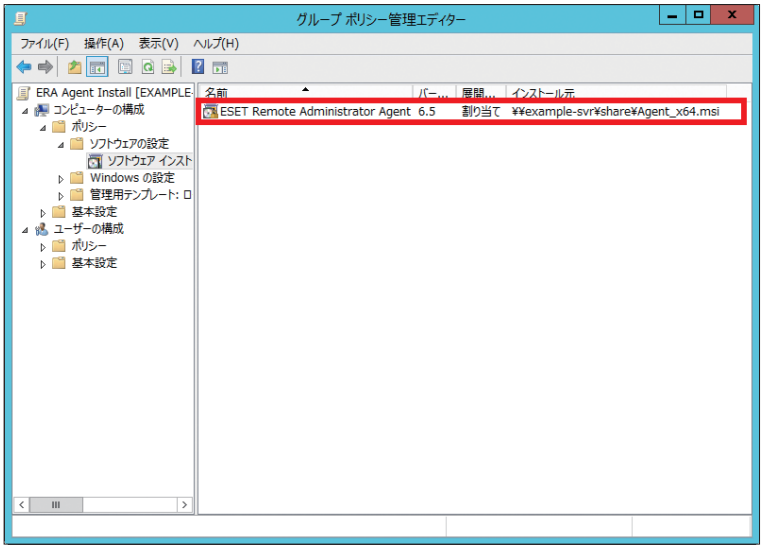
7 [OK] ボタンをクリックします。



「グループポリシー管理エディター」画面に戻ります。

8 設定した「ESET Remote Administrator Agent」のポリシーが作成されます。

選択した ESET エージェントインストーラーのパスが、汎用命名規則（以下 UNC）パスであることを確認し、「グループポリシー管理エディター」を閉じます。



■サーバータスクを使用したリモート展開

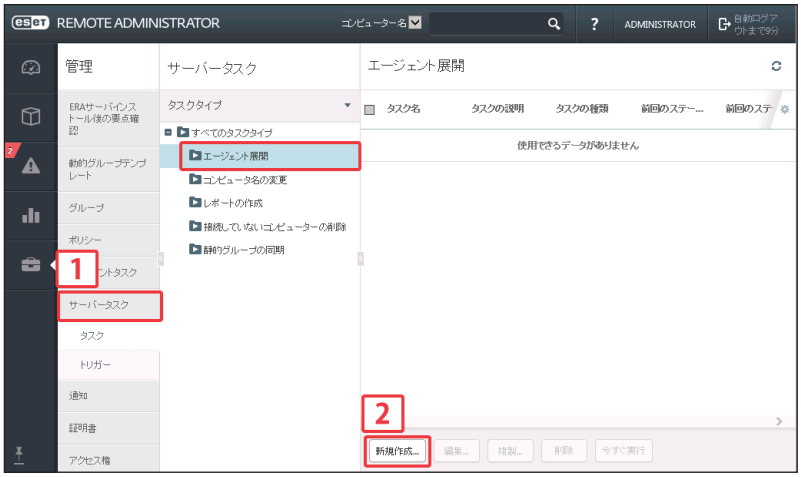
サーバータスクを使用して、リモート展開します。サーバータスクは、ERA Web コンソールの管理メニューから実行します。

操作手順

1 サーバータスクの新規作成画面を表示します。

ERA Web コンソールの［管理］メニュー > ［サーバータスク］サブメニューを選択します。
表示される「タスクタイプ」から、［エージェント展開］をクリックします。

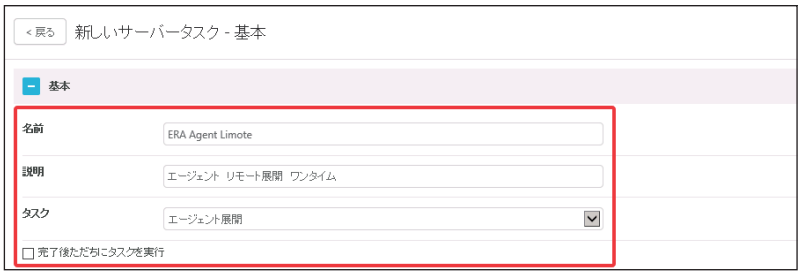
2 ［新規作成］ボタンをクリックします。



「新しいサーバータスク - 基本」画面が表示されます。

3 「名前」、「説明」を入力し、「タスク」に［エージェント展開］が選択されていることを確認します。

タスク作成後にタスクを即時実行する場合は、［完了後ただちにタスクを実行］をオンにします。



続く

4 ［設定］をクリックし、［適切なエージェントの自動解決］にチェックを入れます。

ワンポイント

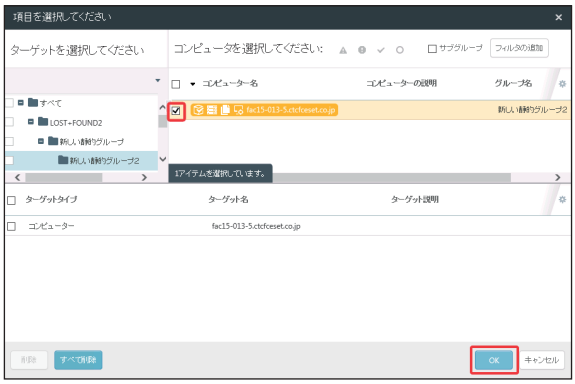
複数のオペレーティングシステム（Windows、Linux、Mac OS X）がネットワークにある場合、［適切なエージェントの自動解決］をオンにすることで、オペレーティングシステムに合った ERA エージェントのインストーラーを自動的に選択します。インストーラーを手動で選択するには、［適切なエージェントの自動解決］をオフにし、ダウンロード可能なエージェントのリストから、使用するパッケージを選択します。

5 「ターゲット」の［0 対象］をクリックします。

ターゲットを選択する画面が表示されます。

6 対象となるネットワーク上のクライアントコンピュータにチェックを入れ、［OK］ボタンをクリックします。

「ターゲットを選択してください」のエリアでは、すべての静的および動的グループが表示されます。
「コンピューターを選択してください」のエリアでは、選択したグループに含まれるクライアントコンピューターが表示され、チェックを入れたコンピューターが下のリストに表示されます。



「新しいサーバータスク ー設定」画面に戻ります。

続く

7 「ユーザー名」「パスワード」に、リモートインストールの実行に十分な権限を持つユーザーの情報を入力します。

ワンポイント

Mac OS X/Linux は、リモート展開を行う場合に SSH を利用します。「ユーザー名」と「パスワード」は、エージェント展開を行いたいコンピューターに SSH でログインできる管理者権限のアカウントを設定してください。

8 「サーバーホスト名（またはサーバーの IP アドレス）」に、クライアントコンピューターから接続する ERA サーバーのホスト名または IP アドレスを入力します。

ワンポイント

「サーバーホスト名（またはサーバーの IP アドレス）」が空白の場合は、ERA サーバーのホスト名が使用されます。

9 「ピア証明書」から［ERA 証明書］を選択します。

ワンポイント

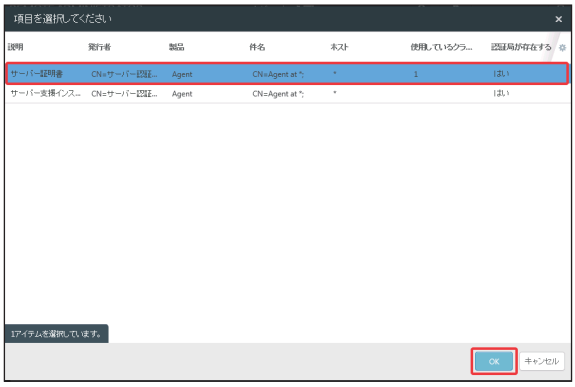
ピア証明書には、ERA 既定のピア証明書と認証局または独自の証明書を使用できます。
ERA 証明書　　：ERA で作成されたセキュリティ証明書と認証局の公開鍵ファイル
カスタム証明書　：独自の証明書
証明書の詳細については、「6.9 証明書」を参照してください。

10 「ERA 証明書」から［<証明書が選択されていません>］をクリックします。

証明書の一覧が表示されます。

続く

⑪ 証明書を選択し、［OK］ボタンをクリックします。



「新しいサーバータスクー設定」画面に戻ります。

「ERA 証明書」に選択した証明書が表示されます。

ワンポイント

指定した証明書にパスワードを設定している場合は、「証明書パスフレーズ」を入力してください。
カスタム証明書を選択している場合は、カスタム証明書のパスワードを「証明書パスフレーズ」に入力してください。

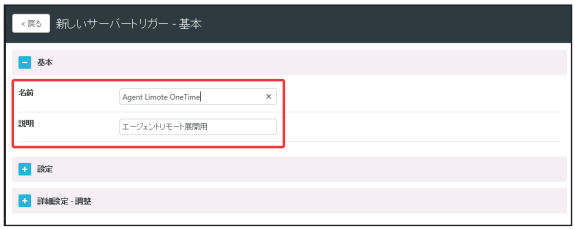
⑫ ［トリガー］をクリックし、［新規追加］ボタンをクリックします。

トリガーはタスクを実行するイベントの設定です。

「新しいサーバートリガー ー基本」画面が表示されます。

続く

13 「名前」「説明」を入力します。



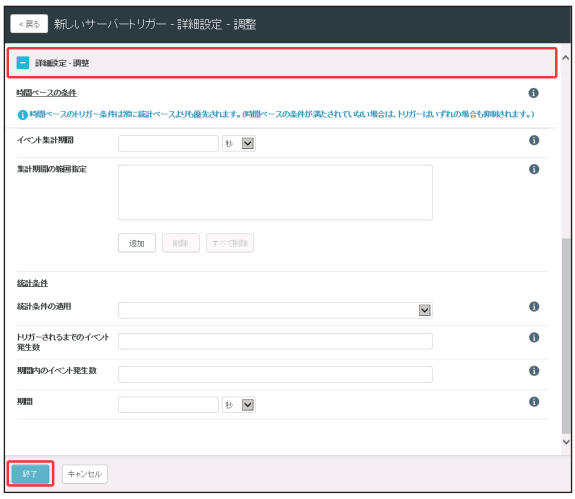
14 [設定] をクリックし、「トリガータイプ」から、タスクを実行する条件を選択します。

必要に応じ、「1 度だけ実行」、「ランダム遅延間隔」、「設定した時間に実行されなかった場合は即時実行」、「ローカル時刻を使用」の設定を行います。

!重 要

トリガーの画面構成および設定項目の詳細については、「6.7.4 トリガー」を参照してください。

15 [詳細設定—調整] をクリックし、必要に応じて各項目を設定して、[終了] ボタンをクリックします。



「新しいサーバータスクートリガー」画面に戻ります。

!重 要

「詳細設定ー調整」セクションの画面構成および設定項目の詳細については、「6.7.4.2 詳細設定 ー 調整」を参照してください。

続く

16 [サマリー] をクリックし、設定内容を確認して、問題がなければ [終了] ボタンをクリックします。

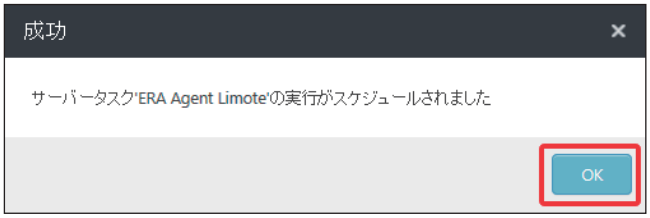
「サーバータスク」画面に戻ります。

17 エージェント展開のタスクリストから、作成したエージェント展開用のタスクにチェックを入れます。

18 [今すぐ実行] ボタンをクリックします。

タスクの実行がスケジュールされると「成功」画面が表示されます。

19 [OK] ボタンをクリックします。

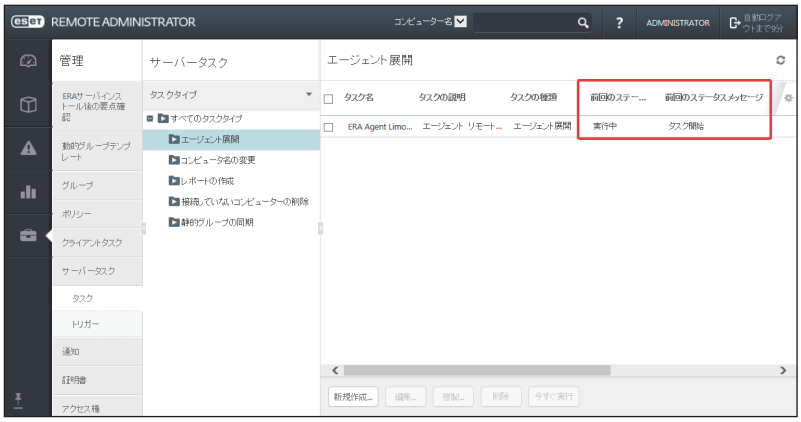


ワンポイント

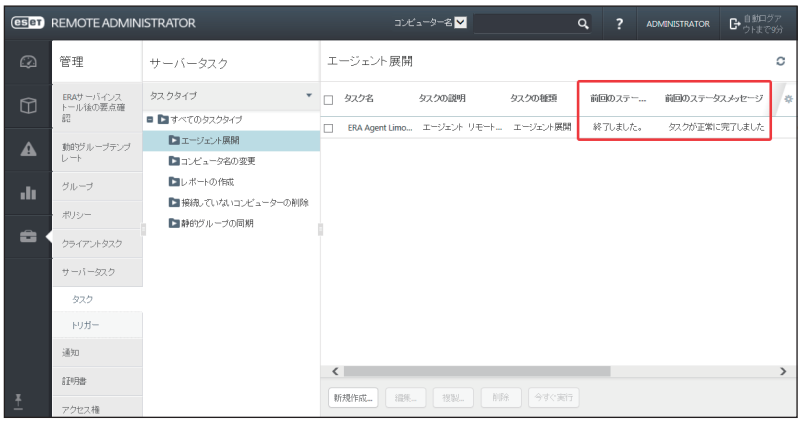
をクリックすると、画面の表示を更新することができます。

続く

タスクの実行が開始されると、「前回のステータス」には「実行中」、「前回のステータスメッセージ」には「タスク開始」と表示されます。

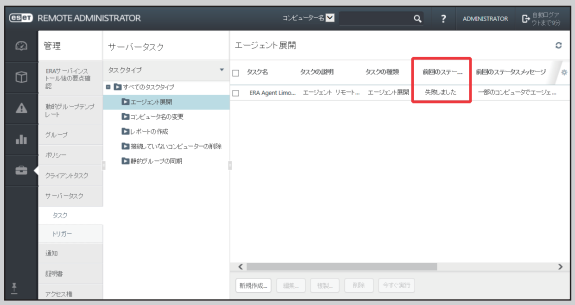


タスクの実行が終了すると、「前回のステータス」には「終了しました。」、「前回のステータスメッセージ」には「タスクが正常に完了しました。」と表示されます。



! 重 要

タスクの実行が失敗した場合は、「前回のステータス」に「失敗しました」と表示されます。
失敗したタスクをクリックし、「サーバータスク」コンテキストメニューから［詳細］をクリックして、原因を確認してください。
画面の詳細は、「6.7.1 サーバータスク画面の構成」の「●サーバータスクの詳細確認画面」を参照してください。



! 重 要

ERA エージェントのリモート展開中に問題が発生した場合（サーバータスクのエージェント展開が失敗する場合）は、「4.2.2.7 トラブルシューティング - エージェント展開」を参照してください。

4.2.2.2 オールインワンインストーラー

オールインワンインストーラーは、ERA エージェントと ESET ライセンス製品（ESET Endpoint Seccurity や ESET Endpoint Antivirus など）を含んだインストールパッケージです。オールインワンインストーラーは、ERA Web コンソールのスタートアップウィザードまたはクイックリンクから作成できます。
クリックリンクからオールインワンインストーラーを作成するときは、ERA エージェントと ESET ライセンス製品のポリシー設定、ERA サーバーホスト名とポート、親グループを設定してくおくことができます。スタートアップウィザードから作成するときは、これらの設定を行うことはできません。
作成したオールインワンインストーラーは、クライアントコンピューターで実行することで、ERA エージェントと ESET ライセンス製品のインストールを行えます。

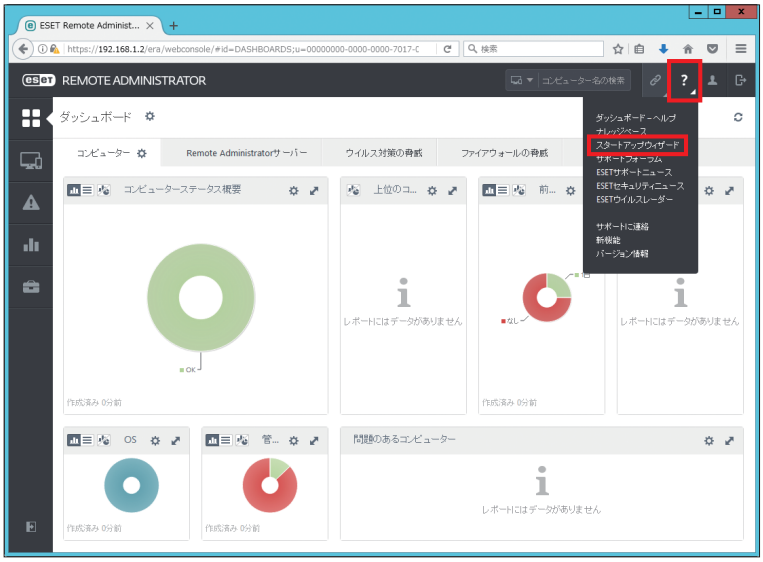
! 重 要

オールインワンインストーラーは、「.exe」ファイルの形式の Windows 用のみを作成できます。他の OS 向けのオールインワンインストーラーは作成できません。

■スタートアップウィザードからオールインワンインストーラーを作成する

操作手順

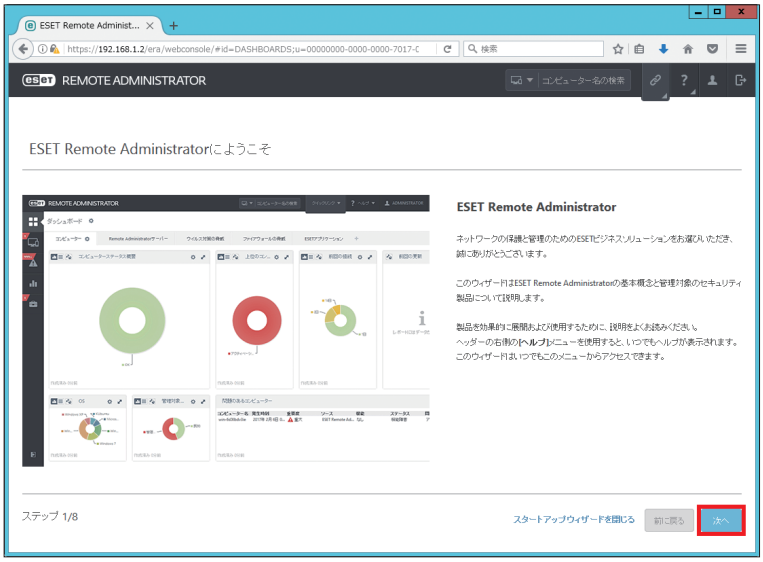
1. ERA Web コンソールの［ヘルプ］セクションをポイントし、［スタートアップウィザード］をクリックします。



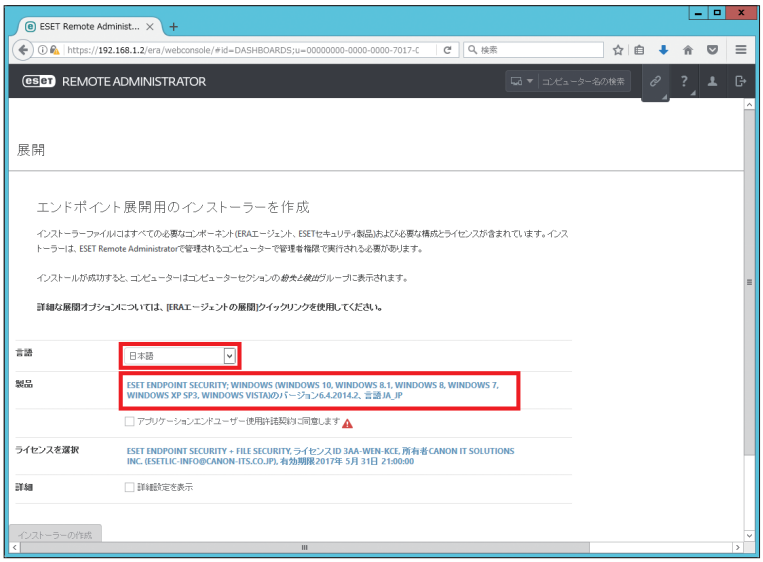
「セットアップウィザード」が表示されます。

続く

2 セットアップウィザードの「展開」画面が表示されるまで、［次へ］ボタンをクリックします。



3 言語に「日本語」が選択されていることを確認し、「製品」に選択されている［ESET ライセンス製品］をクリックします。



ESET ライセンス製品の選択画面が表示されます。

ワンポイント

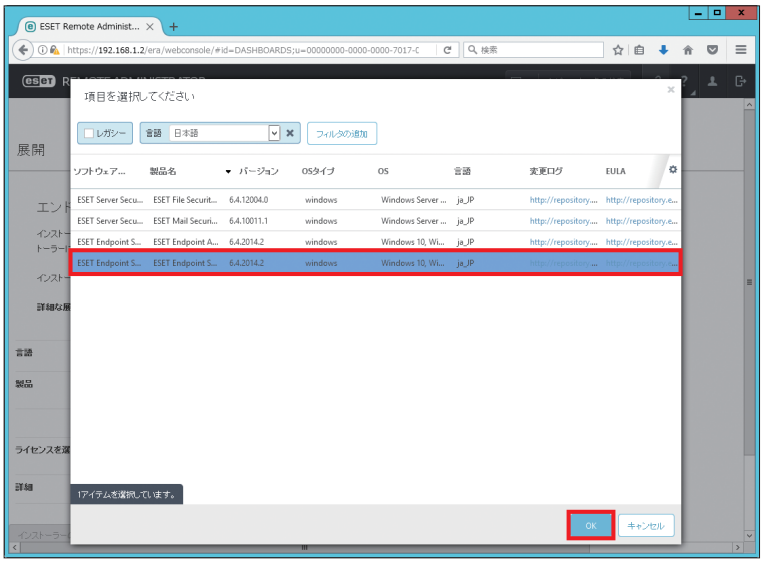
「展開」画面では、当初、最新版の ESET Endpoint Security」が選択されています。この製品で問題ないときは、手順 6 に進んでください。手順 3 は、当初選択されている ESET ライセンス製品とは別の ESET ライセンス製品のオールインワンインストーラーを作成したいときに行います。

! 重 要

オールインワンインストーラーを作成できるのは、Windows 用の ESET ライセンス製品のみです。他の OS 用の製品でオールインワンインストーラーを作成することはできません。

続く

4 オールインワンインストーラーを作成したい ESET ライセンス製品をクリックして選択し、[OK] ボタンをクリックします。

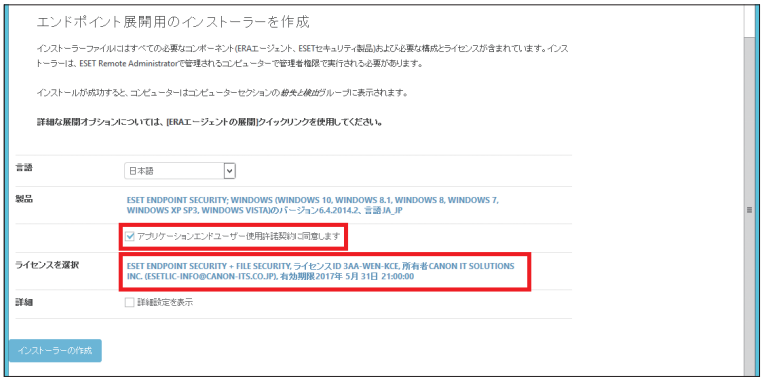


「展開」画面に戻ります。

! 重 要

標準では最新のバージョンの Windows 用 ESET ライセンス製品のみが表示されます。古いバージョンの ESET ライセンス製品を選択したいときは、[レガシー] のチェックをオンにします。なお、Ver6.3 以前のバージョンの ESET ライセンス製品選択すると、自動製品アクティベーションが動作しません。Ver6.3 以前のバージョンは、インストール完了後に別途製品のアクティベーションを行う必要があります。ESET 製品バージョンが Ver 6.4 以上の場合は、インストール中に自動的にアクティベーションされます。

5 [アプリケーションエンドユーザー使用許諾契約に同意します] のチェックをオンにし、ライセンスが選択されていることを確認します。



ワンポイント

ライセンス管理にライセンスが登録済みの場合は、そのライセンスが自動選択されます。複数のライセンスが登録されているときは、選択中のライセンスをクリックすると、ライセンスの選択画面が表示され、利用するライセンスを選択できます。また、ライセンスが登録されていないときは、ライセンスなしでオールインワンインストーラーが作成されます。ライセンスなしでオールインワンインストーラーを作成したときは、ESET ライセンス製品のインストール完了後に別途、製品のアクティベーションを行います。ライセンスの追加と削除は、ホームグループがすべてに設定され、そのグループのライセンスに対する書き込み権限がある管理者にのみ許可されています。

続く

6 [詳細設定の表示]をオンにすると、証明書に関する設定が行えます。ERAのインストール時にパスフレーズを設定したときは、この設定をオンにして、「証明書パスフレーズ」にパスフレーズを入力します。この設定を行わないときは、手順 7 に進んでください。

! 重 要

[ESET AV REMOVER を有効にする] をオンにしないでください。ESET AV REMOVER の利用はサポート対象外となります。

ワンポイント

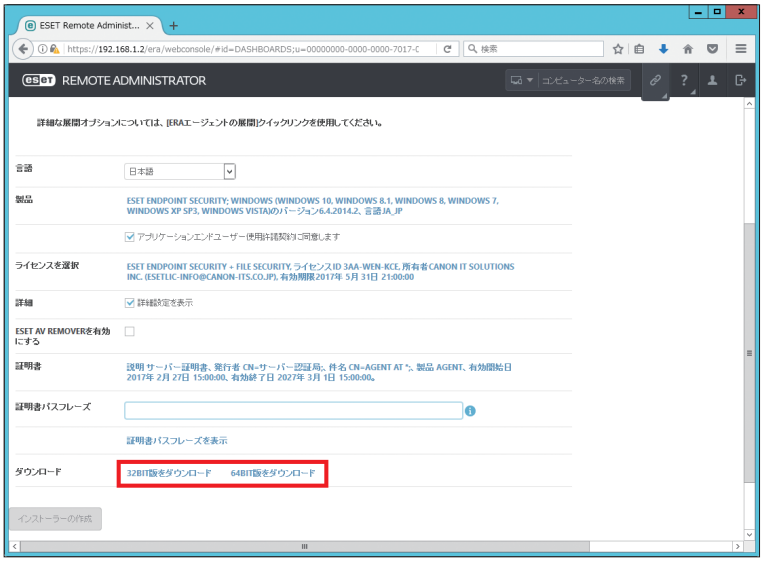
カスタム証明書を利用したいときは、表示されている証明書をクリックします。証明書の選択画面が表示されるので、利用したいカスタム証明書を選択して、[OK] ボタンをクリックします。カスタム証明書にパスフレーズを設定しているときは、「証明書パスフレーズ」にパスフレーズを入力します。

7 すべての設定が完了したら、[インストーラーの作成] ボタンをクリックします。

ダウンロードのページが展開され、ダウンロードするインストーラーの選択画面が表示されます。

続く

8 ダウンロードするインストーラー（ここでは、［64bit 版をダウンロード］）をクリックします。

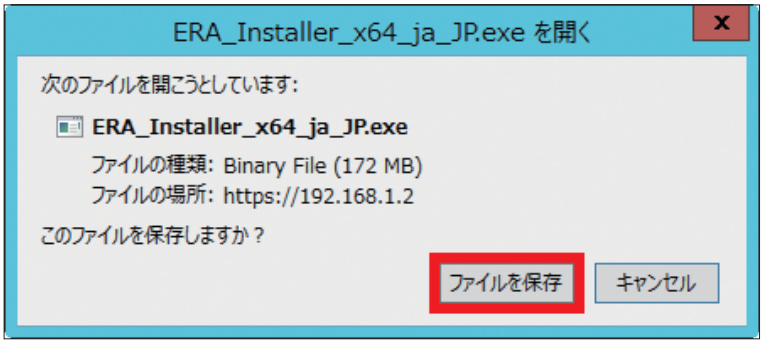


リポジトリから選択したインストーラーのダウンロードが行われます。

！重　要

ご利用のネットワーク環境によってはオールインワンインストーラーのダウンロードに時間がかかる場合があります。
プログレスバーが動かない場合でも、プログラムのダウンロードを行っていますのでしばらくお待ちください。

9 ファイルの保存画面が表示されたときは、［ファイルを保存］ボタンをクリックします。



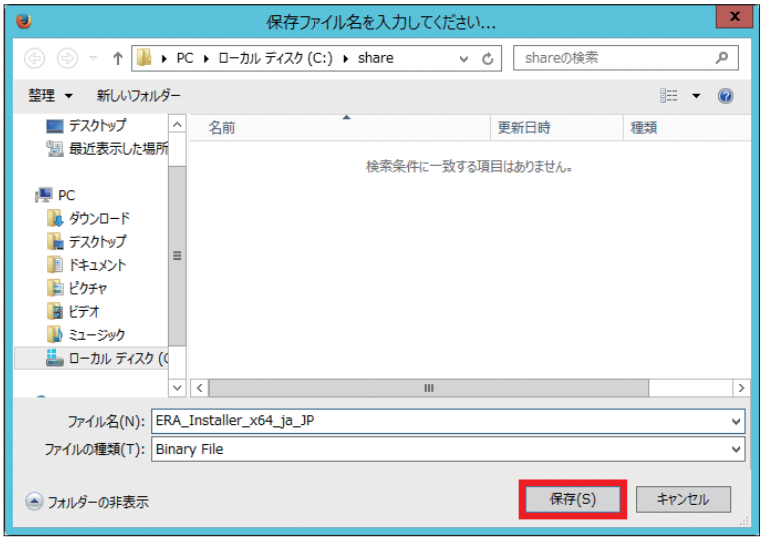
ファイルの保存画面が表示されます。

ワンポイント

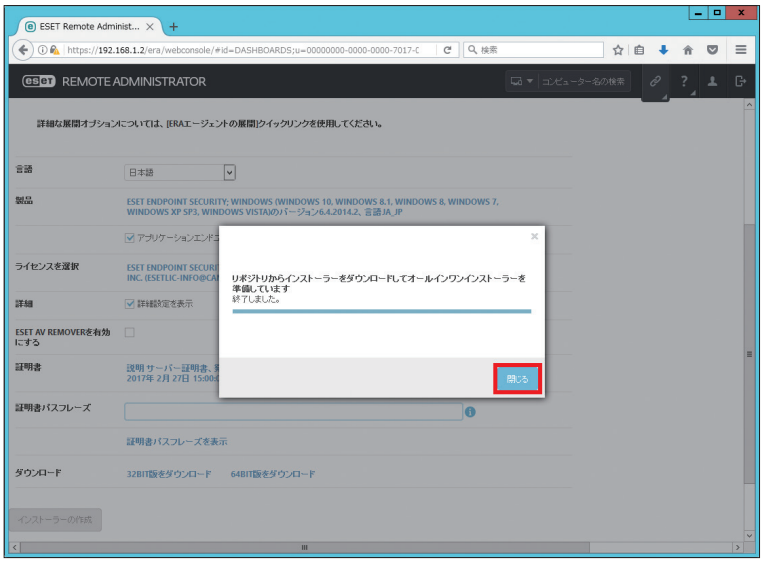
Web ブラウザーにダウンロードファイルの自動保存が設定されているときは、手順 9 の画面は表示されません。指定フォルダーにオールインワンインストーラーが自動保存されます。

続く

⑩ オールインワンインストーラーの保存先を選択し、［保存］ボタンをクリックします。

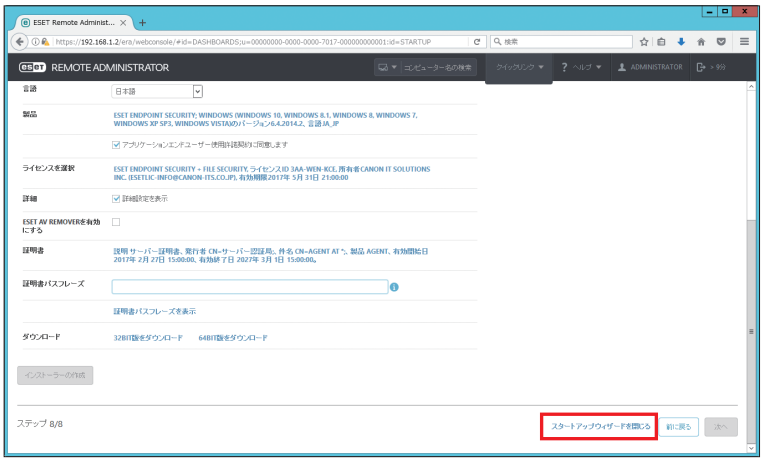


⑪ ［閉じる］ボタンをクリックすると、「展開」画面に戻ります。



続く

⑫［スタートアップウィザードを閉じる］をクリックします。これで、オールインワンインストーラーの作成は完了です。



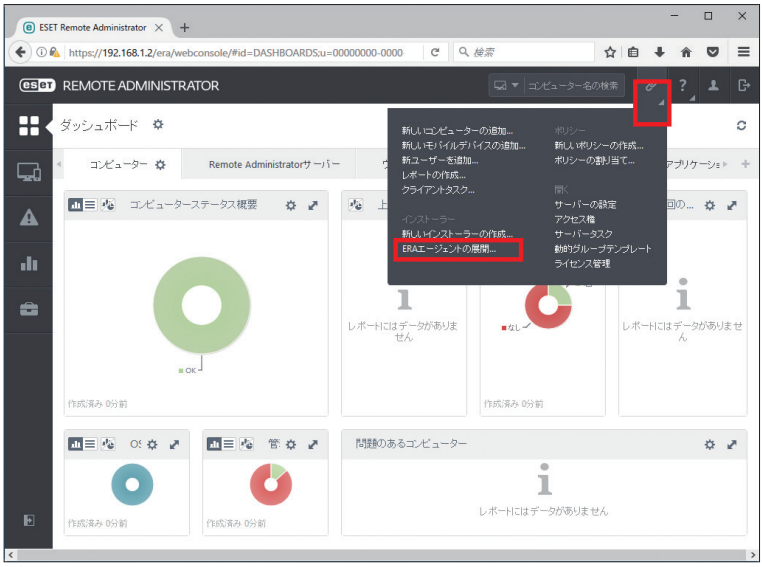
ワンポイント

［32bit 版をダウンロード］または［64bit 版をダウンロード］をクリックすると、再度、選択したインストーラーの作成を実行できます。32bit 版と 64bit 版の両方のオールインワンインストーラーを作成したいときは、両方のダウンロードを実行してください。

■オールインワンインストーラーの作成手順

操作手順

①ERA Web コンソールの［クイックリンク］セクションをポイントし、［ERA エージェントの展開］をクリックします。

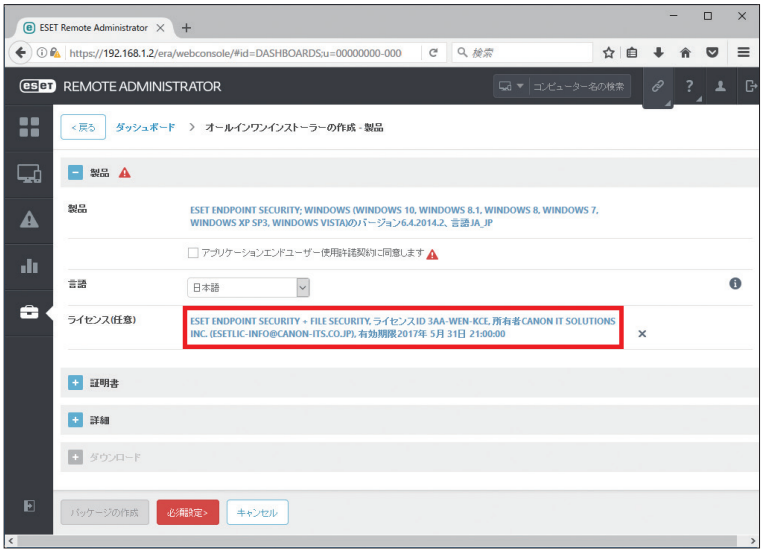


続く

2 「オールインワンインストーラーを作成（Windows 用のみ）」の［インストーラーの作成］をクリックします。

「オールインワンインストーラーの作成 - 製品」画面が表示されます。

3 「製品」に選択されている［ESET ライセンス製品］をクリックします。



ESET ライセンス製品の選択画面が表示されます。

ワンポイント

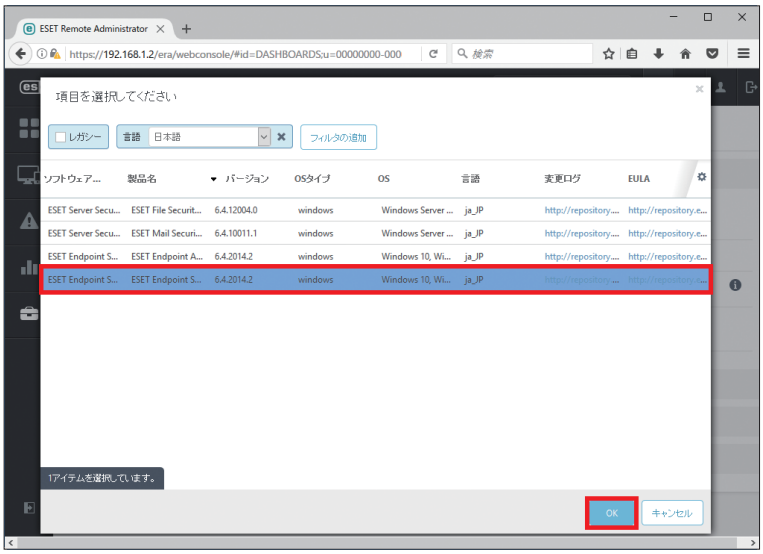
「オールインワンインストーラーの作成 - 製品」画面では、当初、最新版の ESET Endpoint Security」が選択されています。この製品で問題ないときは、手順 6 に進んでください。手順 3 は、当初選択されている ESET ライセンス製品とは別の ESET ライセンス製品のオールインワンインストーラーを作成したいときに行います。

! 重 要

オールインワンインストーラーを作成できるのは、Windows 用の ESET ライセンス製品のみです。他の OS 用の製品でオールインワンインストーラーを作成することはできません。

続く

4 オールインワンインストーラーを作成したい ESET ライセンス製品をクリックして選択し、[OK] ボタンをクリックします。

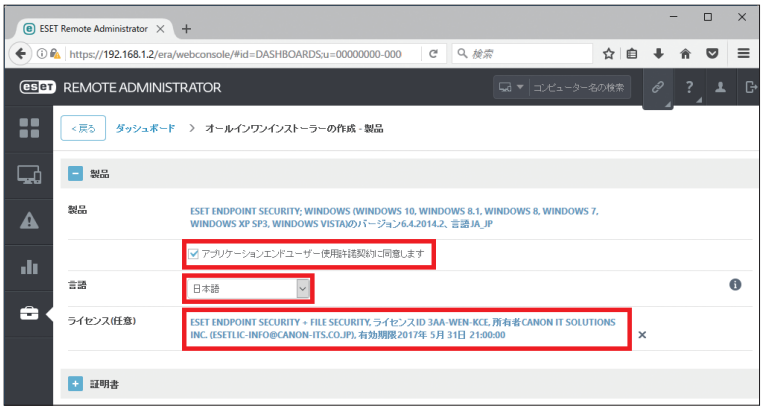


「オールインワンインストーラーの作成 - 製品」画面に戻ります。

! 重 要

標準では最新のバージョンの Windows 用 ESET ライセンス製品のみが表示されます。古いバージョンの ESET ライセンス製品を選択したいときは、[レガシー] のチェックをオンにします。なお、Ver6.3 以前のバージョンの ESET ライセンス製品選択すると、自動製品アクティベーションが動作しません。Ver6.3 以前のバージョンは、インストール完了後に別途、製品のアクティベーションを行う必要があります。ESET 製品バージョンが Ver 6.4 以上の場合は、インストール中に自動的にアクティベーションされます。

5 [アプリケーションエンドユーザー使用許諾契約に同意します] のチェックをオンにし、言語に「日本語」が選択されていることおよび、ライセンスが選択されていることを確認します。

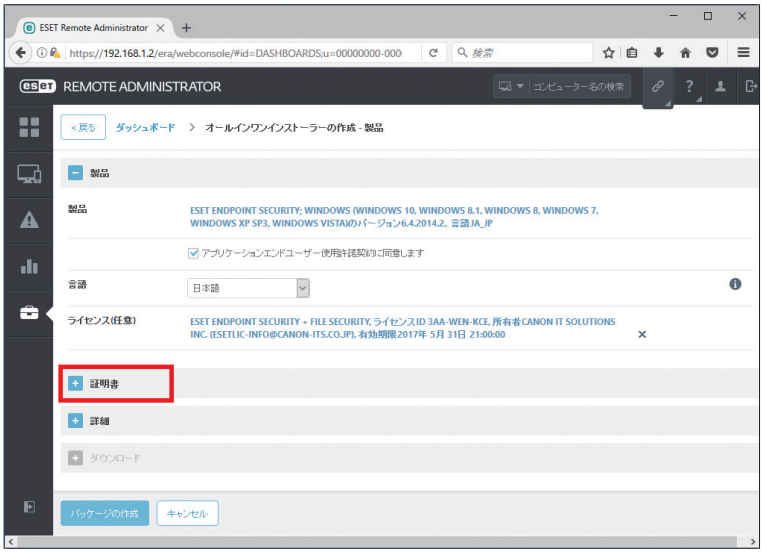


ワンポイント

ライセンス管理にライセンスが登録済みの場合は、そのライセンスが自動選択されます。複数のライセンスが登録されているときは、選択されているライセンスをクリックすると、ライセンスの選択画面が表示され、利用するライセンスを選択できます。また、表示されているライセンスの✕をクリックすると、選択中のライセンスを削除できます。ライセンスを削除したときは、ライセンスなしでオールインワンインストーラーが作成されます。ESET ライセンスの製品のアクティベーションは、ESET ライセンス製品のインストール完了後に行います。

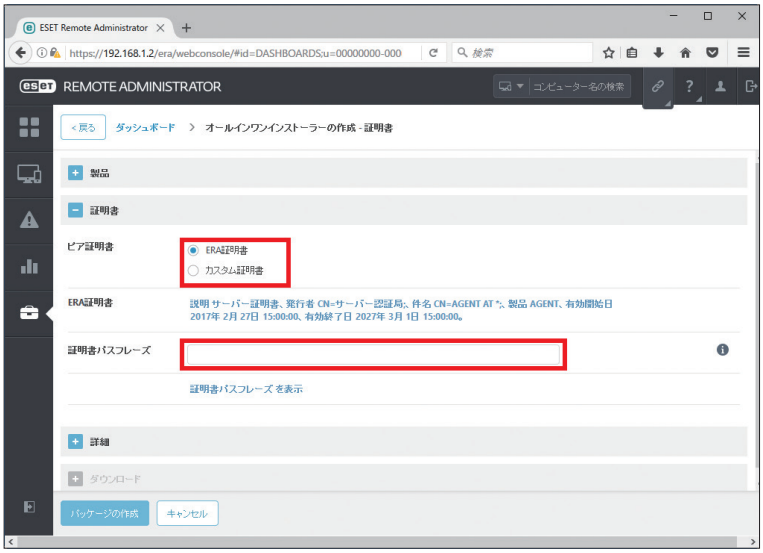
続く

6 [証明書] をクリックします。



「オールインワンインストーラーの作成 - 証明書」画面が展開されます。

7 ピア証明書の選択（ここでは［ERA 証明書］）を行い、ピア証明書にパスフレーズを設定しているときは、パスフレーズを入力します。



ワンポイント

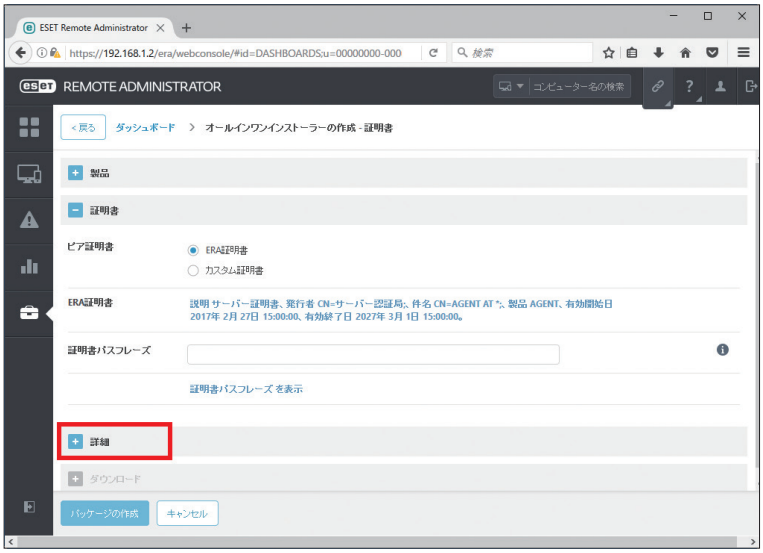
証明書には、ピア証明書および ERA 認証局が使用可能な証明書に基づいて自動的に選択されます。自動選択されたものとは別の証明書を使用する場合は、選択されている ERA 証明書をクリックし、使用可能な証明書のリストを表示して、使用する証明書を選択します。カスタム証明書を使用する場合は、［カスタム証明書］をクリックして選択し、.pfx 証明書ファイルをアップロードします。

!重 要

証明書パスフレーズは .exe ファイルに埋め込まれているため、抽出できます。

続く

8 オールインワンインストーラーのカスタマイズを行うときは、［詳細］をクリックします。

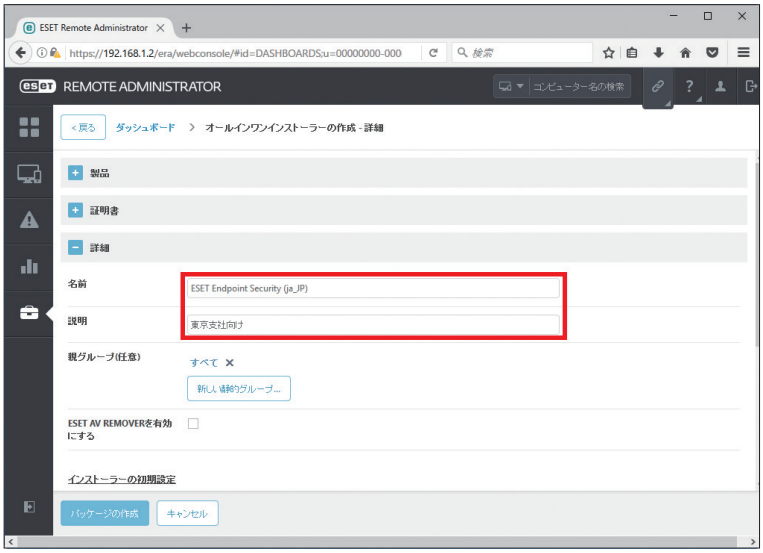


ワンポイント

［詳細］をクリックすると、ERA エージェントと ESET ライセンス製品のポリシー設定、ERA サーバーホスト名とポート、親グループの設定、ESET AV REMOVER の設定などを行えます。

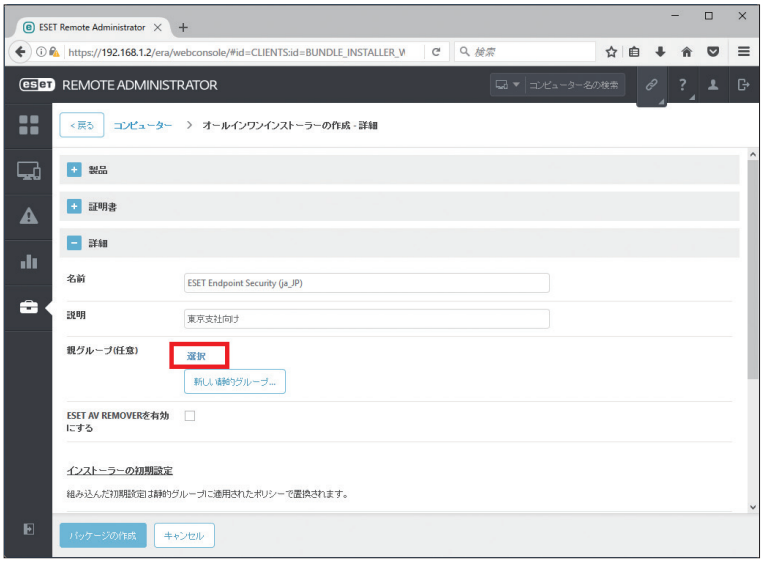
「オールインワンインストーラーの作成 - 詳細」画面が展開されます。

9 「名前」と「説明」を必要に応じて入力します。



続く

10 必要に応じてオールインワンインストーラーパッケージを使用するクライアントコンピューターの親静的グループを選択します。すでに作成済みの親静的グループから選択するときは、[選択] をクリックします。

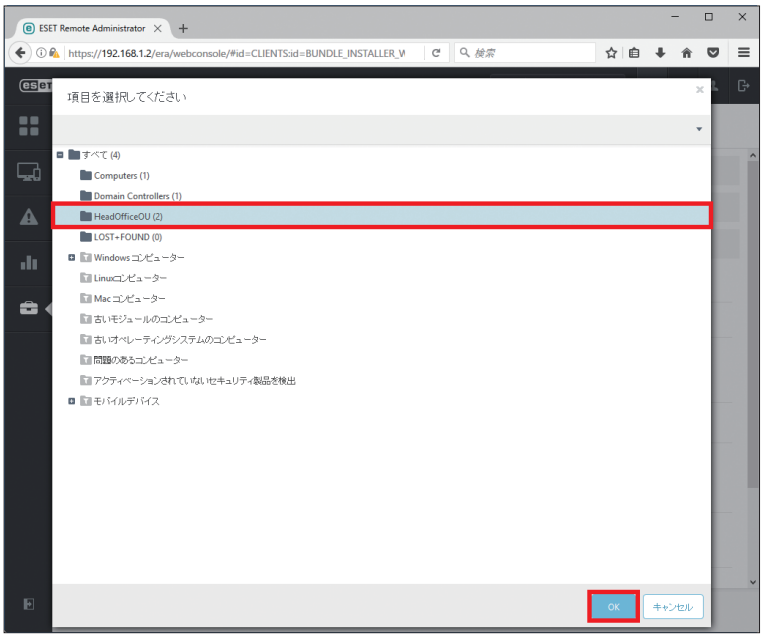


グループの選択画面が表示されます。

ワンポイント

新しい親静的グループを作成する場合は、[新しい静的グループ] をクリックして、画面の指示に従って操作します。新しいグループを作成すると、そのグループが自動的に選択されます。

11 所属させるグループを選択し、[OK] ボタンをクリックします。



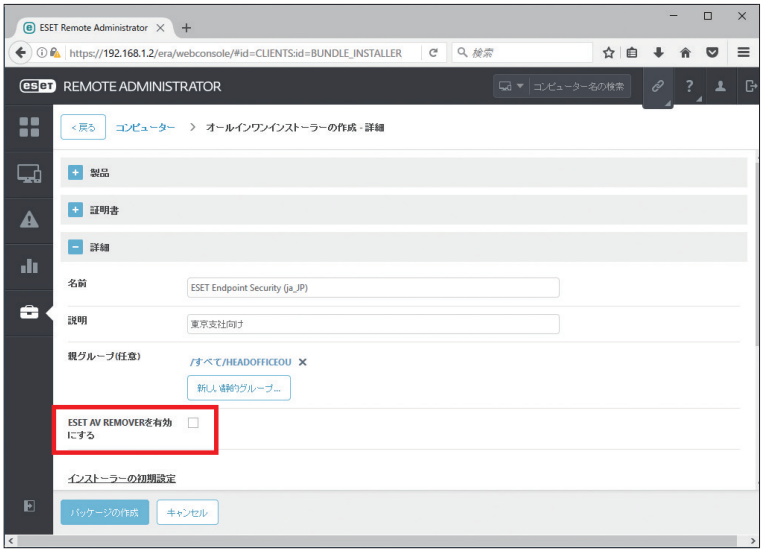
「オールインワンインストーラーの作成」画面に戻ります。親グループに手順 11 で選択したグループが表示されます。

続く

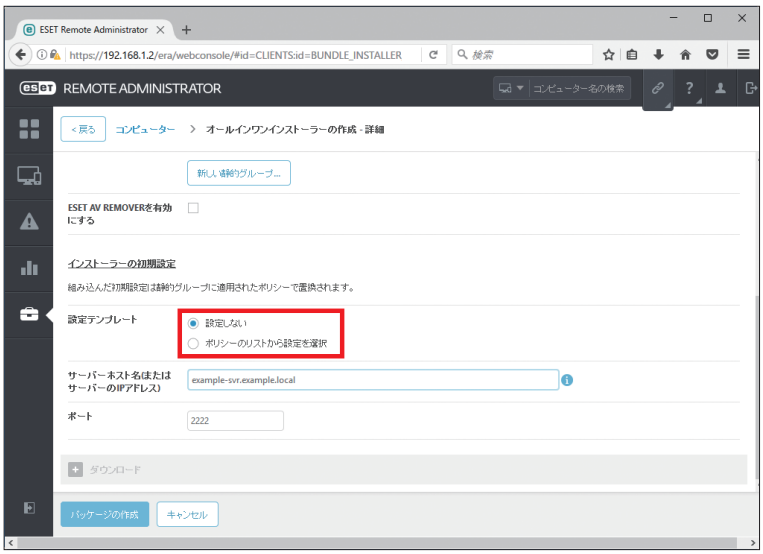
⑫ ESET AV REMOVER を使用するかどうか設定します。［ESET AV REMOVER を有効にする］はオンにしないでください

! 重 要

ESET AV REMOVER の利用はサポート対象外となります。



⑬ インストーラーの初期設定を行います。設定テンプレートを［設定しない］または［ポリシーのリストから設定を選択］の中から選択します。



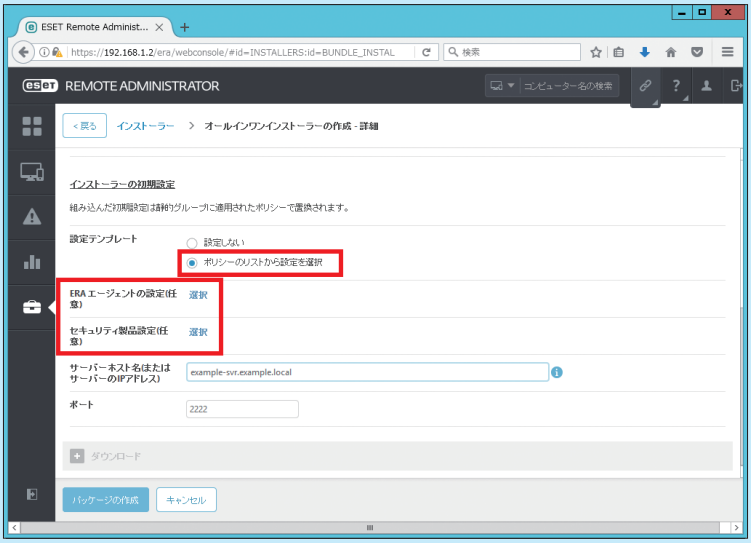
続く

ワンポイント

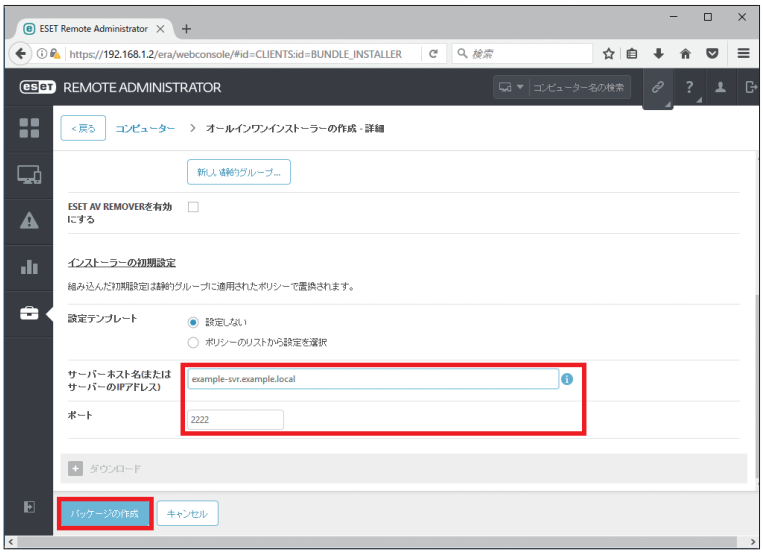
設定テンプレートは、インストールするクライアントコンピューターのポリシーを設定します。

・設定しない - 親静的グループにマージされたポリシーのみが適用されます。

・ポリシーのリストから設定を選択する - 選択したポリシーを ERA エージェントまたは ERA 製品に適用する場合は、このオプションを使用します。2 つの項目の［選択］をクリックして、使用可能なポリシーのリストから設定したいポリシーを選択します。適したポリシーがないときは、「管理」の「ポリシー」セクションで新しいポリシーを作成するか、既存のポリシーをカスタマイズしておき、最初の手順からやり直します。



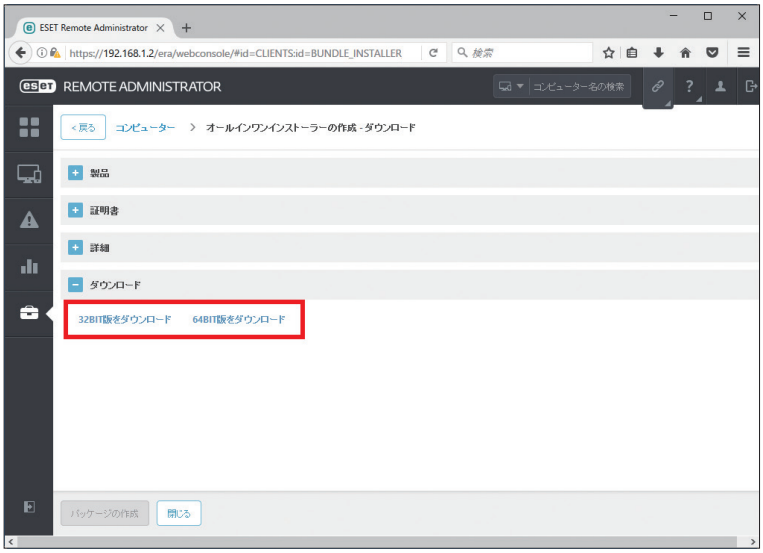
14 必要に応じて、ERA サーバーホスト名または IP アドレスとポート番号を設定し、［パッケージの作成］をクリックします。



ダウンロードのページが展開され、ダウンロードするインストーラーの選択画面が表示されます。

続く

⑮ ダウンロードするインストーラーをクリック（ここでは、[64bit 版]）します。

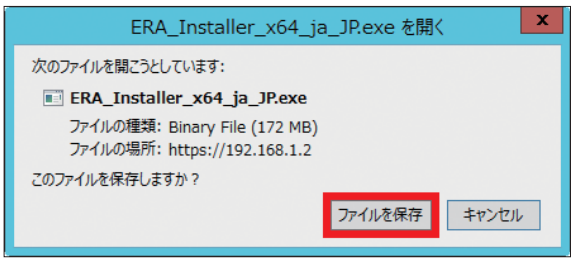


リポジトリから選択したインストーラーのダウンロードが行われます。

! 重 要

ご利用のネットワーク環境によってはオールインワンインストーラーのダウンロードに時間がかかる場合があります。
プログレスバーが動かない場合でも、プログラムのダウンロードを行っていますのでしばらくお待ちください。

⑯ ファイルの保存画面が表示されたときは、[ファイルを保存] ボタンをクリックします。



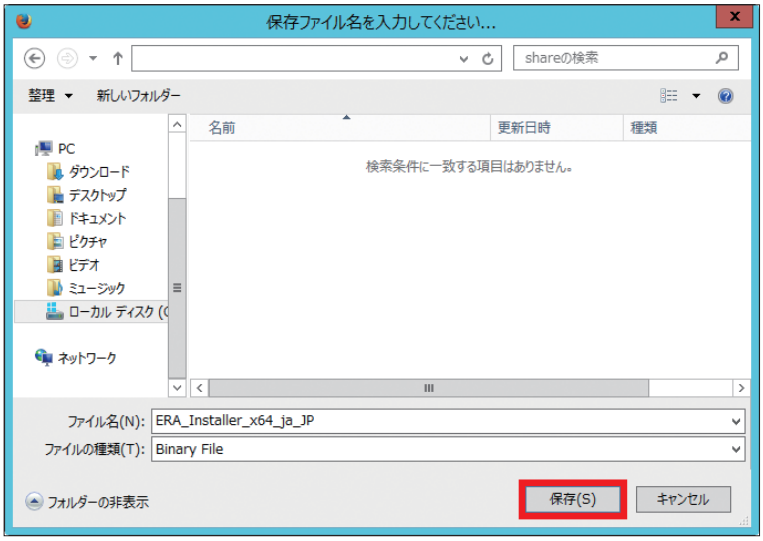
ファイルの保存画面が表示されます。

ワンポイント

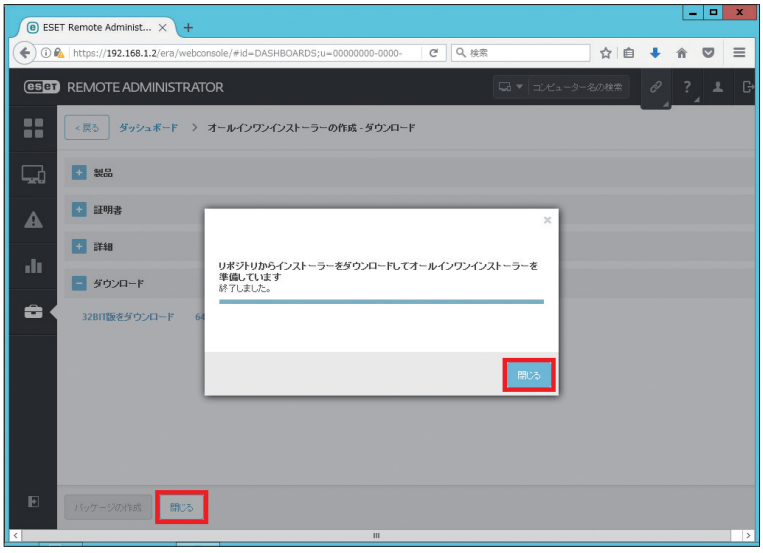
Web ブラウザーにダウンロードファイルの自動保存が設定されているときは、手順 16 の画面は表示されません。指定フォルダーにオールインワンインストーラーが自動保存されます。

続く

⑰ オールインワンインストーラーの保存先を選択し、［保存］ボタンをクリックします。



⑱ ［閉じる］ボタンをクリックし、「オールインワンインストーラーの作成 - ダウンロード」画面に戻ったら［閉じる］ボタンをクリックします。これでオールインワンインストーラーの作成は完了です。



ワンポイント

「オールインワンインストーラーの作成」画面で、再度、［32bit 版をダウンロード］または［64bit 版をダウンロード］をクリックすると、選択したインストーラーの作成を実行できます。32bit 版と 64bit 版の両方のオールインワンインストーラーを作成したいときは、両方の作成を行ってください。

■スタンドアロン展開ツールを使用

ERA Web コンソール上で作成したオールインワンインストーラーをリモートでインストールするスタンドアロン展開ツールを使用できます。スタンドアロン展開ツールを使用すると、リモートからクライアントコンピューターにオールインワンインストーラーを使用して、ERA エージェントと ESET 製品をインストールすることができます。
スタンドアロン展開ツールは、弊社ユーザーズサイトからダウンロードできます。

! 重 要

スタンドアロン展開ツールは英語版のみとなります。
スタンドアロン展開ツールを実行するためには、以下の要件を満たす必要があります。

- サーバータスクを利用したエージェントインストールと同様の要件（ポートの開放と管理者権限）を満たす必要があります。
- インストールに利用するオールインワンインストーラーのファイル名に「x86」または「x64」という文字を含める必要があります。
- 実行する対象のコンピューターはすべて同じプラットフォーム（64 ビットまたは 32 ビットの OS）である必要があります。

4.2.2.3 エージェントライブインストーラー

エージェントライブインストーラーは、証明書情報を付加したスクリプトファイルです。
クライアントコンピューター上で実行し、ESET ダウンロードサーバーのインストーラーに接続して、ERA エージェントを展開します。そのため、クライアントコンピューターがインターネットに接続していなければなりません。
また、エージェントライブインストーラーは ERA Web コンソール上で作成し、ユーザーへ配布します。
配布手段としては、電子メールおよびリムーバブルメディア（USB メモリーなど）を想定しており、展開を行うのはユーザーです。

ワンポイント

エージェントライブインストーラーでの展開は、リモートおよびその他のローカル展開が適していない場合の使用を推奨しています。

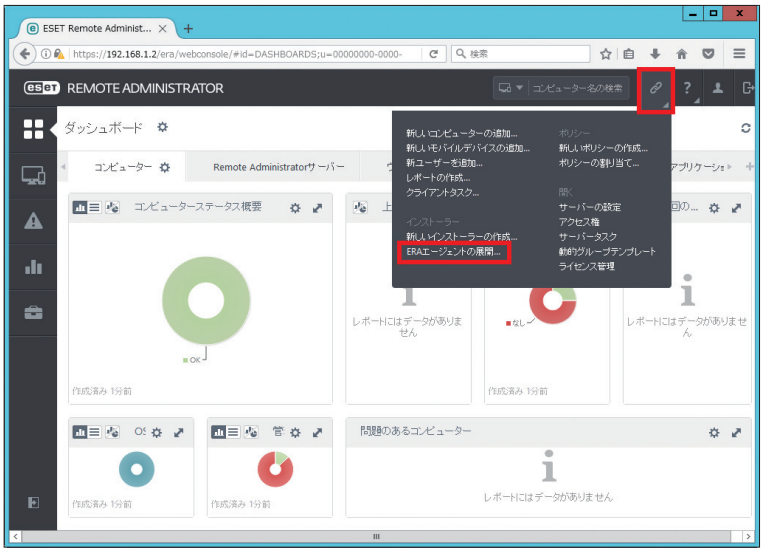
! 重 要

クライアントコンピューターが Windows XP SP2 の場合は、Microsoft Windows Server 2003 Administration Tools Pack が必要です。別途インストールしてください。

■エージェントインストーラーの生成とダウンロード

操作手順

1. ERA Web コンソールの［クイックリンク］セクションをポイントし、［ERA エージェントの展開］をクリックします。



2. 「エージェントライブインストーラーの作成」の［インストーラーの作成］をクリックします。

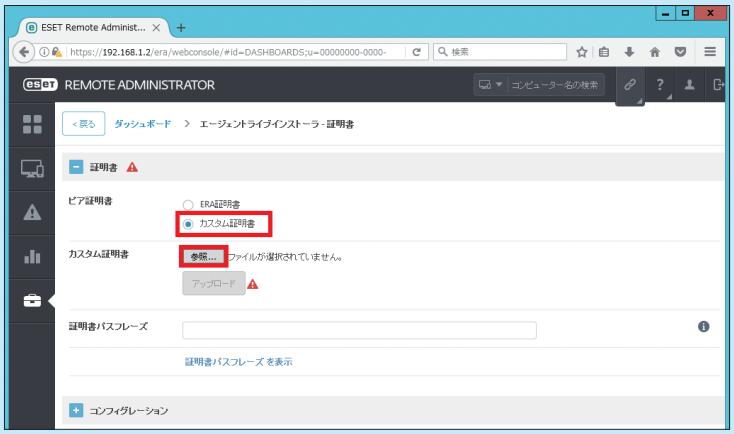
「エージェントライブインストーラー - 証明書」画面が表示されます。

続く

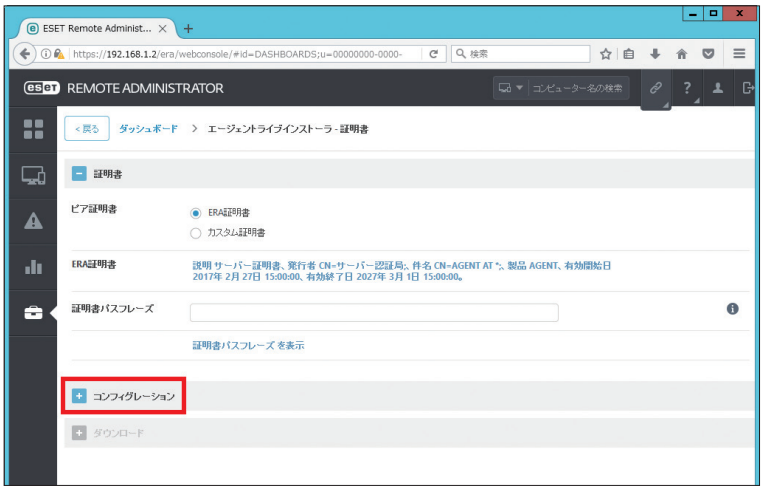
3 ピア証明書の選択（ここでは［ERA 証明書］）を行います。ピア証明書にパスフレーズを設定しているときは、パスフレーズを入力します。

ワンポイント

証明書には、ピア証明書および ERA 認証局が使用可能な証明書に基づいて自動的に選択されます。自動選択されたものとは別の証明書を使用する場合は、選択されている ERA 証明書をクリックし、使用可能な証明書のリストを表示して、使用する証明書を選択します。カスタム証明書を使用する場合は、［カスタム証明書］をクリックして選択し、.pfx 証明書ファイルをアップロードします。



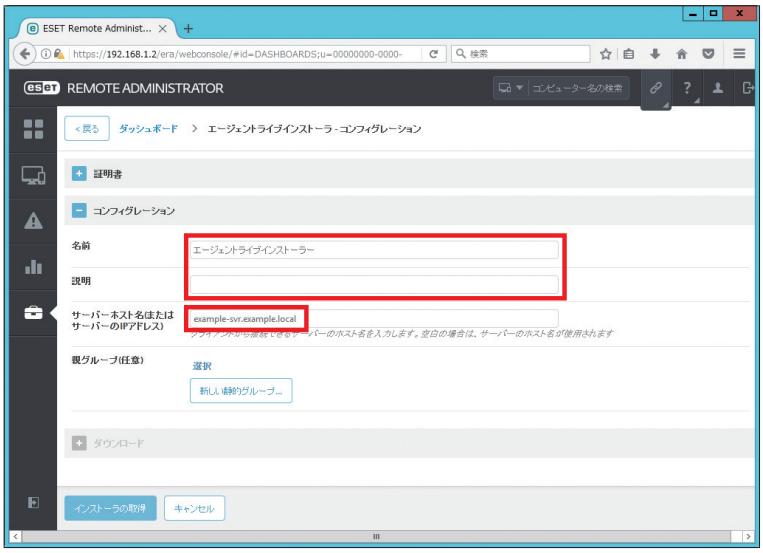
4 ［コンフィグレーション］をクリックします。



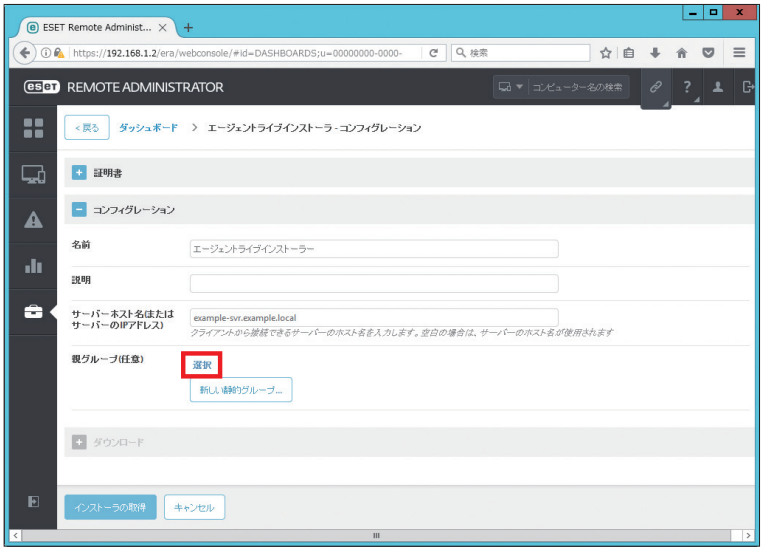
「コンフィグレーション」画面が展開されます。

続く

5 「名前」と「説明」を必要に応じて入力し、ERA サーバーホスト名または IP アドレスとポート番号を必要に応じて設定します。



6 必要に応じて ERA エージェントを使用するクライアントコンピューターの親静的グループを選択します。すでに作成済みのの親静的グループから選択するときは、［選択］をクリックします。



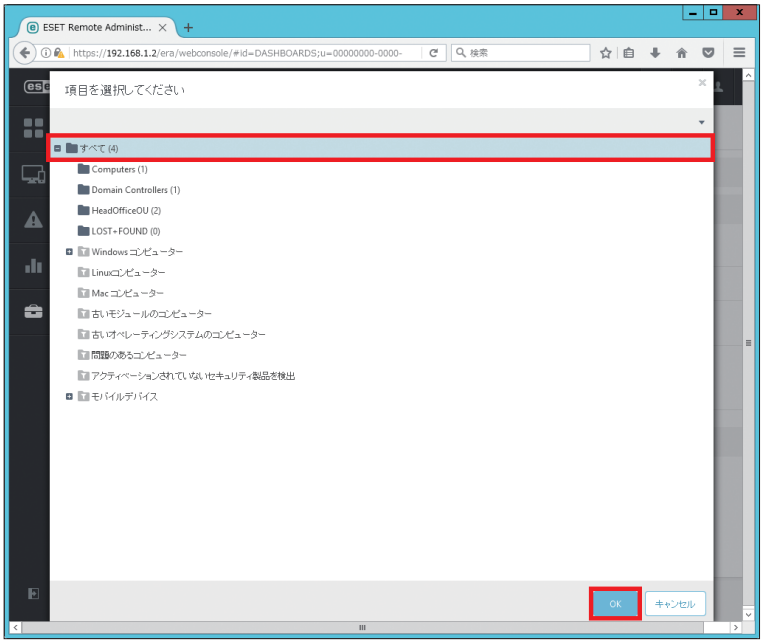
グループの選択画面が表示されます。

ワンポイント

新しい親静的グループを作成する場合は、［新しい静的グループ］をクリックして、画面の指示に従って操作します。新しいグループを作成すると、そのグループが自動的に選択されます。

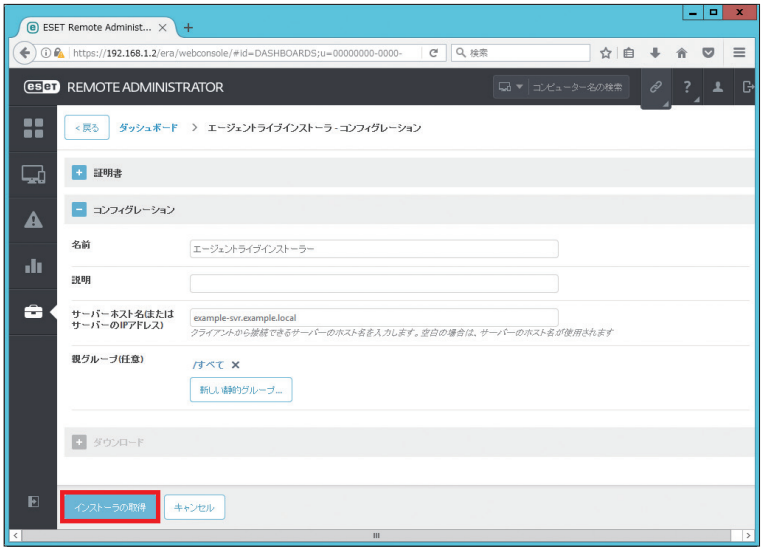
続く

7 所属させるグループを選択し、［OK］ボタンをクリックします。



「エージェントインストーラー」画面に戻ります。親グループに手順 6 で選択したグループが表示されます。

8 ［インストーラーの取得］をクリックします。

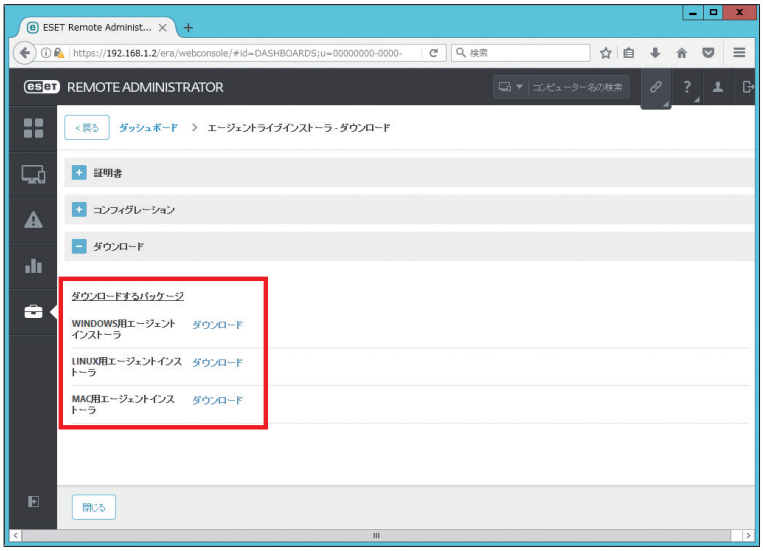


「ダウンロードするパッケージ」が表示され、Windows 用、Linux 用および Mac OS X 用のエージェントインストーラーファイルのリンクが生成されます。

続く

9 「使用する OS 用のエージェントライブインストーラ」の［ダウンロード］をクリックし、ファイルを保存します。

展開先のコンピューターに合わせて、ダウンロードしてください。



Windows 用をダウンロードした場合は、EraAgentInstaller.zip が保存されます。

zip ファイルには、EraAgentInstaller.bat が格納されています。

MacOS X/Linux 用をダウンロードした場合は、EraAgentInstaller.tar が保存されます。

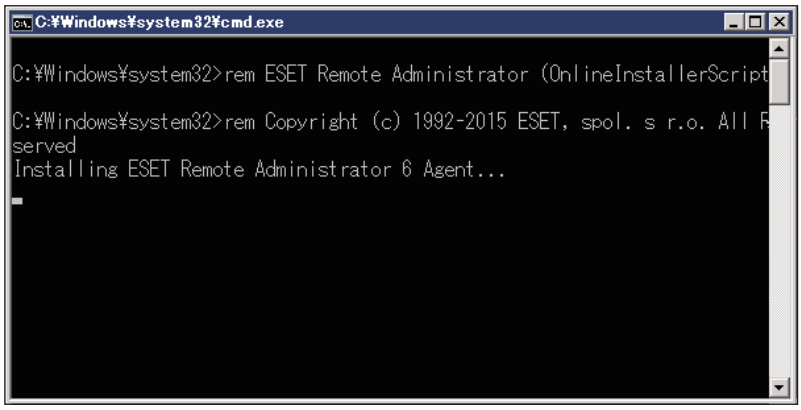
.tar ファイルには、EraAgentInstaller.sh が格納されています。

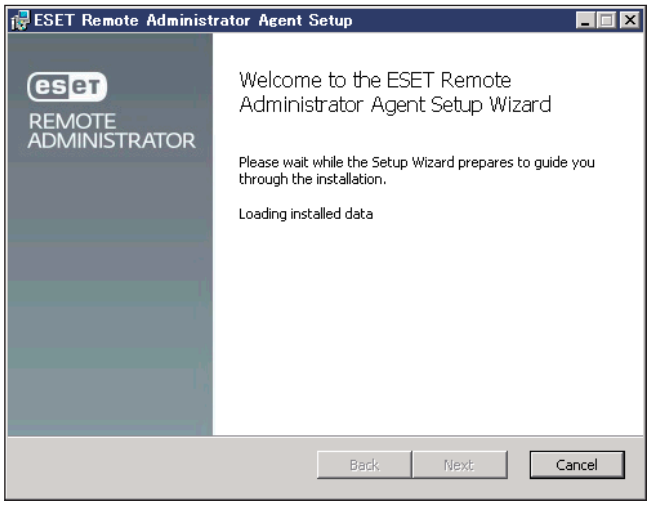
■エージェントライブインストーラーの実行

● Windows の場合

クライアントコンピューターで EraAgentInstaller.zip を展開し、格納されている EraAgentInstaller.bat を実行します。

インストーラーが起動します。





インストーラーの画面が消えると、インストールは終了です。

ワンポイント

クライアントコンピューター上で、ERA エージェントが正しく展開されているかを調べるには、ステータスログを確認します。ステータスログは次の場所に保存されています。

C:¥ProgramData¥ESET¥RemoteAdministrator¥Agent¥EraAgentApplicationData¥Logs¥status.html

また、ERA エージェントに何らかの問題がある場合は、「4.2.2.7 トラブルシューティング - エージェント展開」を参照してください。

● Mac OS X の場合

操作手順

1. クライアントコンピューターで EraAgentInstaller.tar を展開しておきます。

続く

② Finder を開き、［アプリケーション］＞［ユーティリティ］とクリックします。

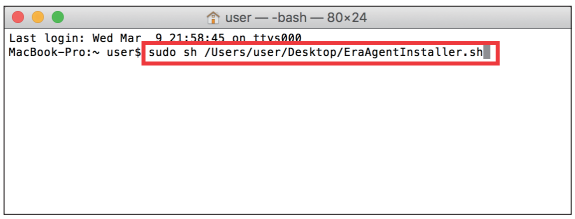
③ ［ターミナル］をダブルクリックします。

④ ターミナルで、次のコマンドを入力します。
起動コマンド：sudo sh / インストーラーの展開先パス名 /EraAgentInstaller.sh

例）起動コマンド：sudo sh /User/user/EraAgentInstaller.sh

ワンポイント

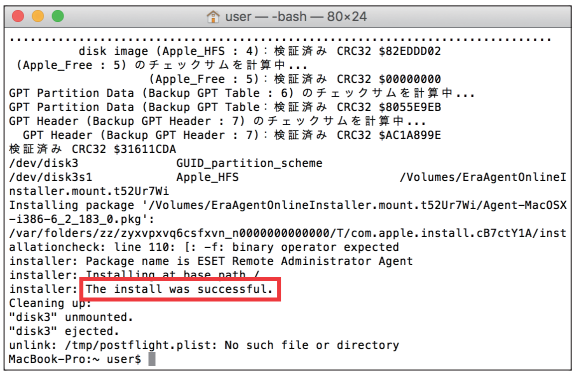
ここでは、デスクトップにエージェントライブインストーラー（EraAgentInstaller.tar）が展開されていることを前提に解説しています。エージェントライブインストーラーの展開先フォルダー名は、実際の実行環境に合わせて変更してください。また、「EraAgentInstaller.sh」をターミナル上にドラッグ＆ドロップすることでパスを簡単に入力できます。



続く

5 「Password:」と表示されたら、管理者パスワードを入力します。入力したパスワードは表示されません。

6 ESET ダウンロードサーバーからインストーラーがダウンロードされ、ERA エージェントの展開が行われます。「The install was successful」と表示されたら、インストールは終了です。ターミナルを閉じます。



ワンポイント

クライアントコンピューター上で、ERA エージェントが正しく展開されているかを調べるには、ステータスログを確認します。ステータスログは次の場所に保存されています。

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/status.html

また、ERA サーバーに接続していないなど、ERA エージェントに何らかの問題がある場合は、「4.2.2.7 トラブルシューティング - エージェント展開」を参照してください。

● Linux の場合

操作手順

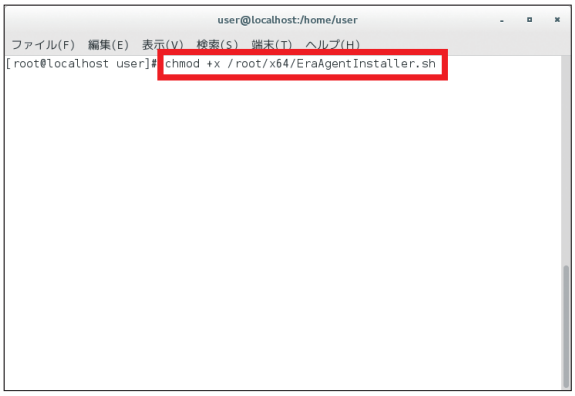
1 クライアントコンピューターで EraAgentInstaller.tar を展開しておきます。

2 ターミナルを開きます。

続く

3 インストーラーに実行権限を付与します。root 権限で次のコマンドを入力します。

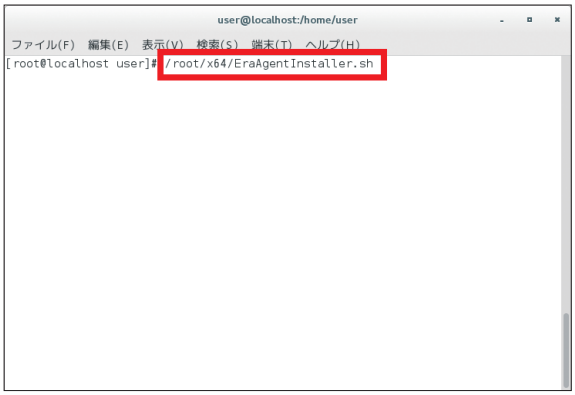
コマンド：chmod +x /x64/EraAgentInstaller.sh



インストーラーのアクセス権限が変更されます。

4 インストーラーを実行します。次のコマンドを入力します。

例）実行コマンド：/root/x64/EraAgentInstaller.sh

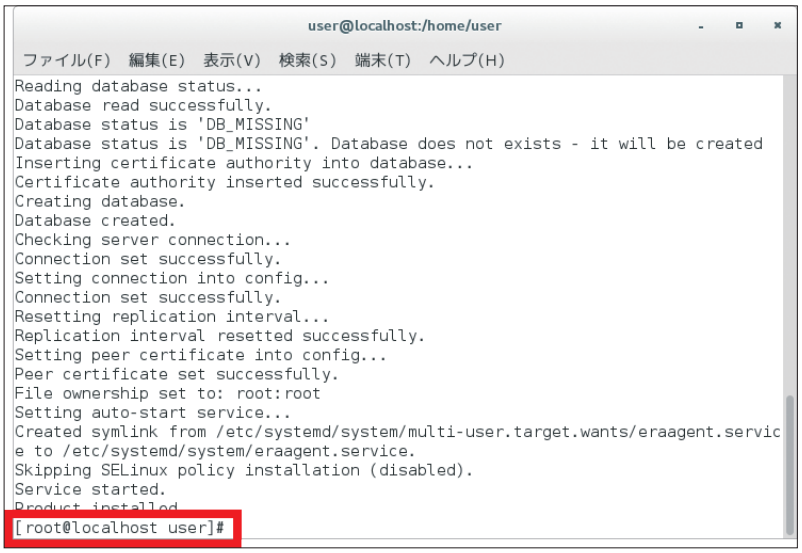


ワンポイント

ここでは、/root/x64 にエージェントライブインストーラー（EraAgentInstaller.tar）が展開されていることを前提に解説しています。エージェントライブインストーラーの展開先フォルダー名は、実際の実行環境に合わせて変更してください。

続く

5 ESET ダウンロードサーバーからインストーラーがダウンロードされ、ERA エージェントの展開が行われます。「Product installed.」と表示されたら、インストールは終了です。ターミナルを閉じます。

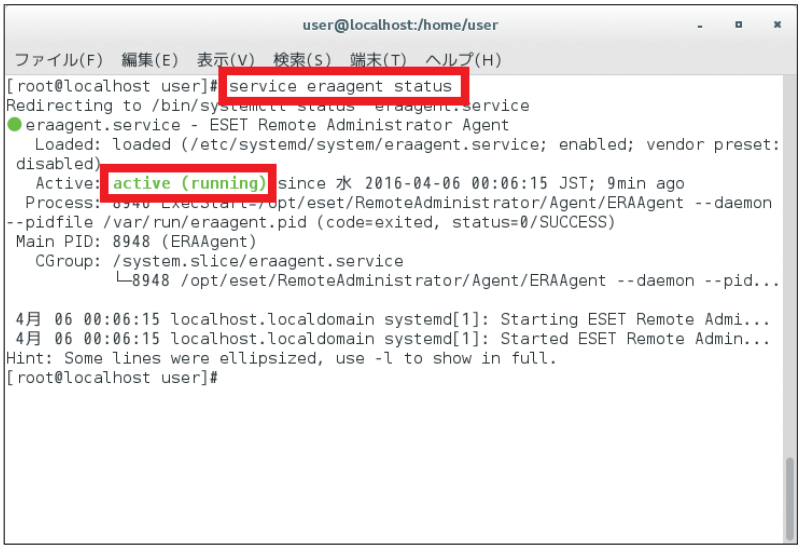


ワンポイント

ERA エージェントは、/opt/eset/RemoteAdministrator/Agent フォルダーにインストールされます。

6 ERA エージェントの稼働を確認します。次のコマンドを入力します。

例）コマンド：service eraserver status



「…を実行中」または「…running」と表示されたら、ERA エージェントは稼働中です。

ワンポイント

ERA サーバーに接続していないなど、ERA エージェントに何らかの問題がある場合は、「4.2.2.7 トラブルシューティング - エージェント展開」を参照してください。

■ ESET ダウンロードサーバーを使用しないエージェントライブインストーラー

● Windows の場合

ESET ダウンロードサーバーでなく、ネットワーク内の共有フォルダー、またはローカルコンピューター内に保存している ERA エージェントのインストーラーを使用して、ERA エージェントを展開する場合は、エージェントライブインストーラーである EraAgentInstaller.bat の書き換えまたは変換を行います。

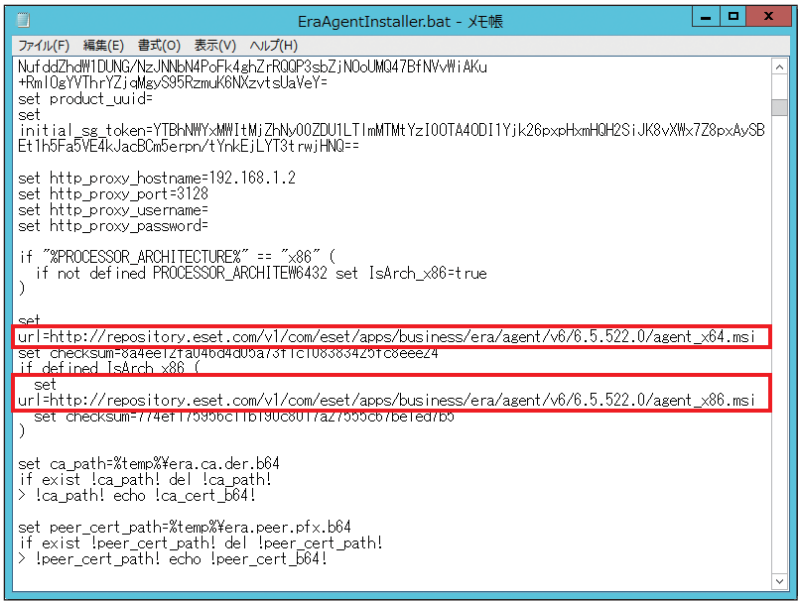
ネットワーク内の共有フォルダーに保存した ERA エージェントインストーラーを使用する場合

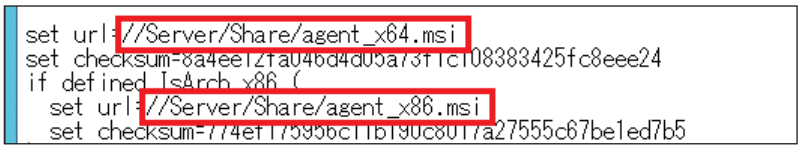
ネットワーク内の共有フォルダーに保存した ERA エージェントインストーラーを使用する場合は、手動で書き換えを行います。

操作手順

1. EraAgentInstaller.bat に記載されている次の 2 行の URL を、ネットワーク内の共有フォルダーに保存している Agent_x64.msi および Agent_x86.msi に書き換えます。

   ここでは共有フォルダーを、//Server/Share/Agent_x64.msi および //Server/Share/Agent_x86.msi としています。
   ※書き換え手段は任意です。





ワンポイント

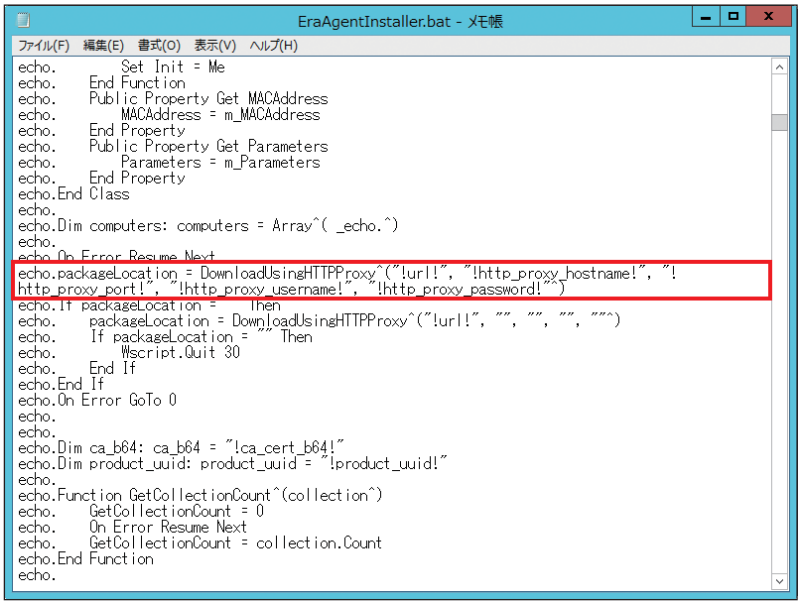
フォルダー階層の区切り文字には、「/」（スラッシュ）または「¥」（円マーク）で表示します。

! 重 要

インストールパッケージが実行されるユーザーアカウントは、ローカル共有フォルダーへの書き込み権限がある必要があります。

続く

2 「echo.packageLocation =」で始まる行の内容を、「echo.packageLocation = "!url!"」に変更します。



3 EraAgentInstaller.bat を更新します。

書き換えた EraAgentInstaller.bat ファイルは、書き換え前のファイルと同様にクライアントコンピューター上で実行し、展開します。

エージェントライブインストーラ 設定変換ツールを使って変換する場合

ローカルコンピューターに保存した ERA エージェントインストーラーを使用する場合は、「エージェントライブインストーラ 設定変換ツール」を使って EraAgentInstaller.bat を変換します。このツールは Windows のみ対応しています。

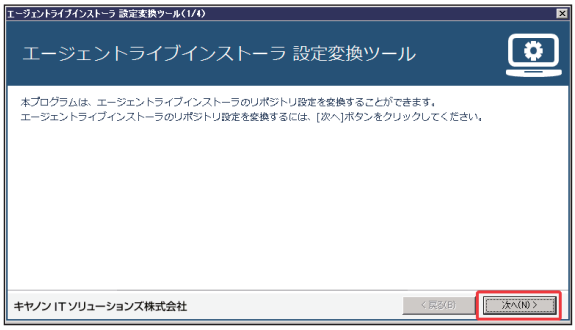
操作手順

1 「エージェントライブインストーラ 設定変換ツール」である setup.exe をダブルクリックします。

エージェントライブインストーラ 設定変換ツールが起動し、「エージェントライブインストーラ 設定変換ツール (1/4)」画面が表示されます。

続く

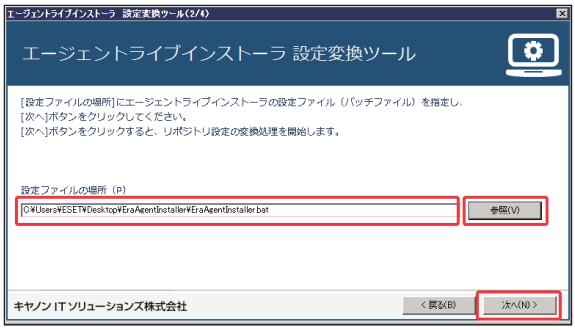
2 ［次へ］ボタンをクリックします。



「エージェントライブインストーラ 設定変換ツール（2/4）」画面が表示されます。

3 「設定ファイルの場所」に、作成した EraAgentInstaller.bat を参照設定します。

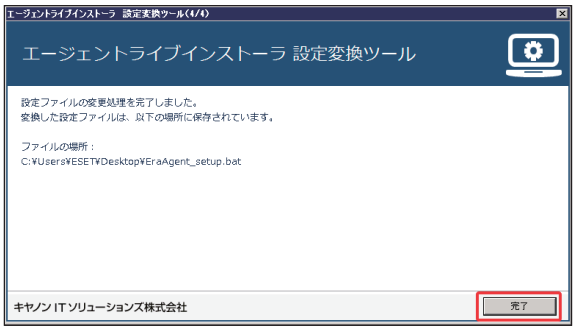
［参照］ボタンをクリックしてファイルを選択し、［次へ］ボタンをクリックします。



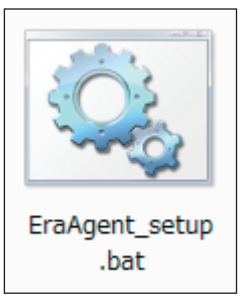
変換が始まります。

変換が終了すると「エージェントライブインストーラ 設定変換ツール（4/4）」画面が表示されます。

4 作成された変換ファイルの場所を確認し、［完了］ボタンをクリックします。



EraAgent_setup.bat が作成されていることを確認します。



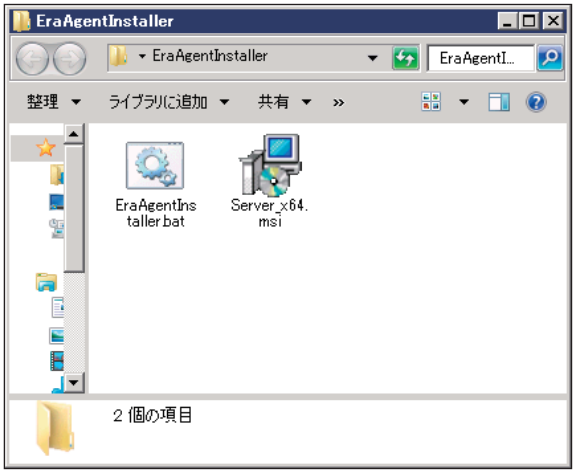
続く

EraAgent_setup.bat の実行

5 クライアントコンピューター上の任意のフォルダーに、ERA エージェントのインストーラーである Agent_x64.msi（または Agent_x86.msi）と、EraAgent_setup.bat を保存します。

! 重 要

保存先のフォルダーのパスに（）が含まれているとエラーになるため、含まないようにしてください。



6 EraAgent_setup.bat を実行します。

インストーラーが起動します。
インストーラーの画面が消えると、インストールは終了です。

● Mac OS X の場合

ESET ダウンロードサーバーではなく、ローカルコンピューター内に保存している ERA エージェントのインストーラーを使用して ERA エージェントを展開する場合は、エージェントライブインストーラーである EraAgentInstaller.sh の書き換えを行います。

ローカルコンピューター内に保存した ERA エージェントのインストーラーを使用する場合

ローカルコンピューター内に保存した ERA エージェントのインストーラーを使用する場合は、手動で書き換えを行います。

続く

操作手順

1 EraAgentInstaller.sh に記載されている「eraa_installer_url=」で始まる以下の 2 行の URL を、ローカルコンピューター内に保存している Agent-OSX-i386.dmg のパスに書き換えます。

ここではローカルの保存先を、/Users/Admin/Desktop/Agent-Macosx-i386.dmg としています。
※書き換え手段は任意です。

書き換え前

EraAgentInstaller.sh

```
B07apWdKF0ZMtQthPqaTD8LIBoiOdZ1iuOxLoD/leusTfpoN/
NIs4Lcv9wDqQu6JjsLMfPI1kHaaIx8cxaPPT8dGSPVcRXcs3PX4nhLECB2qgT8hElv5icGP2iIYK8KW1UHNuf
ddZhdW1DUNG/NzJNNbN4PoFk4ghZrRQQP3sbZjNOoUMQ47BfNVvWiAKu
+RmlOgYVThrYZjqMgyS95RzmuK6NXzvtsUaVeY="
eraa_product_uuid=""

eraa_installer_url="http://repository.eset.com/v1/com/eset/apps/business/era/agent/
v6/6.5.376.0/agent-macosx-i386.dmg"
eraa_installer_checksum="9b28a28ea75d0325f1b3f56661e747bbe84ba895"
eraa_initial_sg_token="ZDI2NjQwM2MtZWJlYS00ZmZiLWFmMGUtYjBmMWE4OTY2ODAwNVVBmvVvSOShai
XOvcCC2SzgFlWUMUJCsGpkNAQC344Jb/0A7Y0n5OIFKUWDukkuBvKbTQ=="

arch=$(uname -m)
if $(echo "$arch" | grep -E "^(x86_64|amd64)$" 2>&1 >> /dev/null)
then
    eraa_installer_url="http://repository.eset.com/v1/com/eset/apps/business/era/
agent/v6/6.5.376.0/agent-macosx-i386.dmg"
    eraa_installer_checksum="9b28a28ea75d0325f1b3f56661e747bbe84ba895"
fi

if test -z $eraa_installer_url
then
  echo "No installer available for '$arch' arhitecture. Sorry :/"
  exit 1
fi

local_params_file="/tmp/postflight.plist"
echo "$local_params_file" >> "$files2del"
```

↓

書き換え後

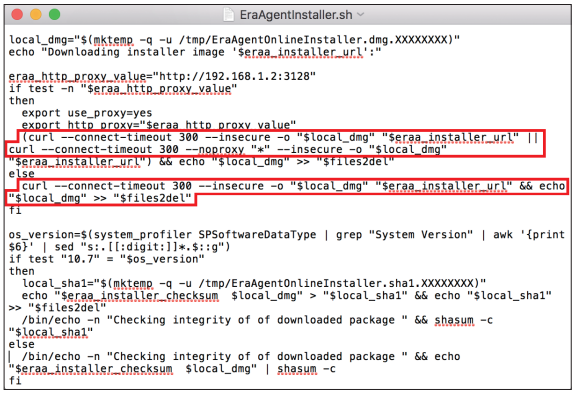
EraAgentInstaller.sh — 編集済み

```
B07apWdKF0ZMtQthPqaTD8LIBoiOdZ1iuOxLoD/leusTfpoN/
NIs4Lcv9wDqQu6JjsLMfPI1kHaaIx8cxaPPT8dGSPVcRXcs3PX4nhLECB2qgT8hElv5icGP2iIYK8KW1UHNuf
ddZhdW1DUNG/NzJNNbN4PoFk4ghZrRQQP3sbZjNOoUMQ47BfNVvWiAKu
+RmlOgYVThrYZjqMgyS95RzmuK6NXzvtsUaVeY="
eraa_product_uuid=""

eraa_installer_url="/Users/Admin/Desktop/Agent-Macosx-i386.dmg"
eraa_installer_checksum="9b28a28ea75d0325f1b3f56661e747bbe84ba895"
eraa_initial_sg_token="ZDI2NjQwM2MtZWJlYS00ZmZiLWFmMGUtYjBmMWE4OTY2ODAwNVVBmvVvSOShai
XOvcCC2SzgFlWUMUJCsGpkNAQC344Jb/0A7Y0n5OIFKUWDukkuBvKbTQ=="

arch=$(uname -m)
if $(echo "$arch" | grep -E "^(x86_64|amd64)$" 2>&1 >> /dev/null)
then
    eraa_installer_url="/Users/Admin/Desktop/Agent-Macosx-i386.dmg"
    eraa_installer_checksum="9b28a28ea75d0325f1b3f56661e747bbe84ba895"
fi

if test -z $eras_installer_url
then
  echo "No installer available for '$arch' arhitecture. Sorry :/"
  exit 1
fi

local_params_file="/tmp/postflight.plist"
echo "$local_params_file" >> "$files2del"

echo "<?xml version=\"1.0\" encoding=\"UTF-8\"?>" >> "$local_params_file"
echo "<!DOCTYPE plist PUBLIC \"-//Apple//DTD PLIST 1.0//EN\" \"http://www.apple.com/
```

続く

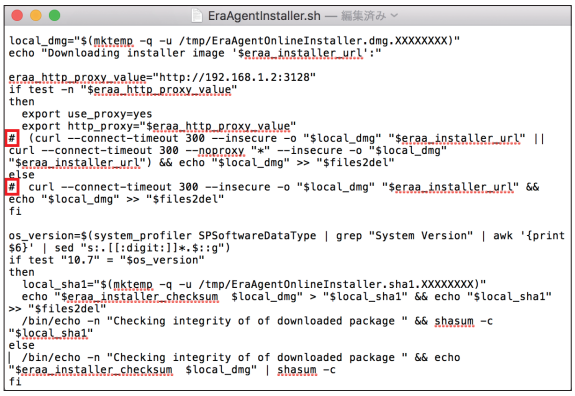
2 「(curl --connect-timeout 300」で始まる以下の 2 行の先頭に「#」を記述してコメントアウトします。

書き換え前

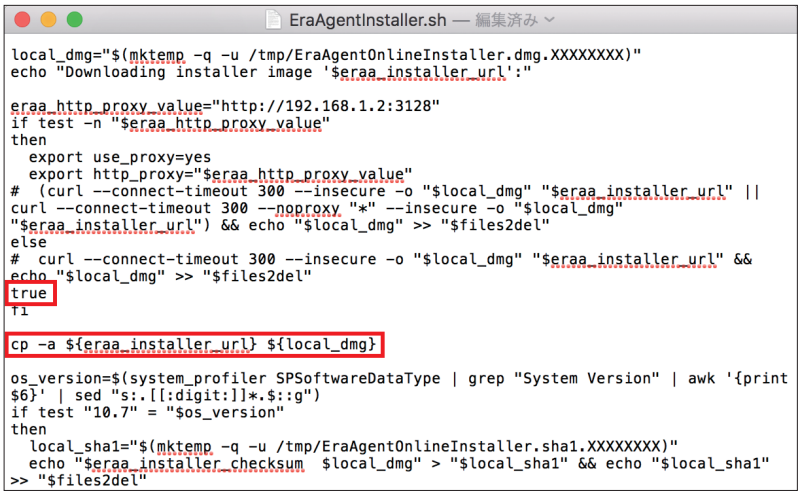


↓

書き換え後



3 手順 2 の 2 番目にコメントアウトした行の次行に「true」の文字列を追加し、その下の「fi」の次行に「cp -a ${eraa_installer_url} ${local_dmg}」の文字列を追加します。



4 EraAgentInstaller.sh を更新します。

書き換えた EraAgentInstaller.sh ファイルは、書き換え前のファイルと同様にクライアントコンピューター上で実行し、展開します。

● Linux の場合

ESET ダウンロードサーバーではなく、ローカルコンピューター内に保存している ERA エージェントのインストーラーを使用して ERA エージェントを展開する場合は、エージェントライブインストーラーである EraAgentInstaller.sh の書き換えを行います。

ローカルコンピューター内に保存した ERA エージェントのインストーラーを使用する場合
ローカルコンピューター内に保存した ERA エージェントのインストーラーを使用する場合は、手動で書き換えを行います。

操作手順

1. EraAgentInstaller.sh に記載されている「eraa_installer_url=」で始まる以下の 2 行の URL を、ローカルコンピューター内に保存している Agent-Linux-x86_64.sh のパスに書き換えます。

   ここではローカルの保存先を、/root/Agent-Linux-x86_64.sh としています。
   ※書き換え手段は任意です。

   書き換え前

```
qQu6JjsLMfPI1kHaaIx8cxaPPT8dGSPVcRXcs3PX4nhLECB2qgT8hEIv5icGP2iIYK8KW1UHNufddZhd
W1DUNG/NzJNNbN4PoFk4ghZrRQQP3sbZjNOoUMQ47BfNVvWiAKu+RmlOgYVThrYZjqMgyS95RzmuK6NX
zvtsUaVeY=↓
eraa_product_uuid=""↓
eraa_installer_url="http://repository.eset.com/v1/com/eset/apps/business/era/age
nt/v6/6.5.417.0/agent-linux-i386.sh"↓
eraa_installer_checksum="1f606fd0e4fb5f5de88bebf722667f85a0516ff5"↓
eraa_initial_sg_token="ZDI2NjQwM2MtZWJlYS00ZmZiLWFmMGUtYjBmMWE4QTY2ODAwNVVBmvVvS
OShaiXOvcCC2SzgFIWUMUJCsGpkNAQC344Jb/0A7Y0n5OIFKUWDukkuBvKbTQ==↓
↓
arch=$(uname -m)↓
if $(echo "$arch" | grep -E "^(x86_64|amd64)$" 2>&1 >> /dev/null)↓
then↓
    eraa_installer_url="http://repository.eset.com/v1/com/eset/apps/business/era
/agent/v6/6.5.417.0/agent-linux-x86_64.sh"↓
    eraa_installer_checksum="e9bzf43f0fadz3100eb0b5ea5c3ba6e14240aaae"↓
fi↓
↓
if test -z $eraa_installer_url↓
then↓
  echo "No installer available for '$arch' arhitecture. Sorry :/"↓
  exit 1↓
fi↓
↓
local_cert_path="$(mktemp -q -u)"↓
echo $eraa_peer_cert_b64 | base64 -d > "$local_cert_path" && echo "$local_cert_p
ath" >> "$cleanup_file"↓
↓
if test -n "$eraa_ca_cert_b64"↓
then↓
  local_ca_path="$(mktemp -q -u)"↓
  echo $eraa_ca_cert_b64 | base64 -d > "$local_ca_path" && echo "$local_ca_path"
 >> "$cleanup_file"↓
```

↓

書き換え後

```
qQu6JjsLMfPI1kHaaIx8cxaPPT8dGSPVcRXcs3PX4nhLECB2qgT8hEIv5icGP2iIYK8KW1UHNufddZhd
W1DUNG/NzJNNbN4PoFk4ghZrRQQP3sbZjNOoUMQ47BfNVvWiAKu+RmlOgYVThrYZjqMgyS95RzmuK6NX
zvtsUaVeY=↓
eraa_product_uuid=""↓
eraa_installer_url="/root/Agent-Linux-x86_64.sh"↓
eraa_installer_checksum="1f606fd0e4fb5f5de88bebf722667f85a0516ff5"↓
eraa_initial_sg_token="ZDI2NjQwM2MtZWJlYS00ZmZiLWFmMGUtYjBmMWE4QTY2ODAwNVVBmvVvS
OShaiXOvcCC2SzgFIWUMUJCsGpkNAQC344Jb/0A7Y0n5OIFKUWDukkuBvKbTQ==↓
↓
arch=$(uname -m)↓
if $(echo "$arch" | grep -E "^(x86_64|amd64)$" 2>&1 >> /dev/null)↓
then↓
    eraa_installer_url="/root/Agent-linux-x86_64.sh"↓
    eraa_installer_checksum="e9bzf43f0fadz3100eb0b5ea5c3ba6e14240aaae"↓
fi↓
↓
if test -z $eraa_installer_url↓
then↓
  echo "No installer available for '$arch' arhitecture. Sorry :/"↓
  exit 1↓
fi↓
↓
local_cert_path="$(mktemp -q -u)"↓
echo $eraa_peer_cert_b64 | base64 -d > "$local_cert_path" && echo "$local_cert_p
ath" >> "$cleanup_file"↓
↓
if test -n "$eraa_ca_cert_b64"↓
then↓
```

続く

2 「(wget --connect-timeout 300」で始まる以下の 2 行の先頭に「#」を記述してコメントアウトします。

書き換え前

```
↓
eraa_http_proxy_value="http://192.168.1.2:3128"↓
if test -n "$eraa_http_proxy_value"↓
then↓
  export use_proxy=yes↓
  export http_proxy="$eraa_http_proxy_value"↓
  (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$era
a_installer_url" || wget --connect-timeout 300 --no-proxy --no-check-certificate
 -O "$local_installer" "$eraa_installer_url" || curl --connect-timeout 300 -k "$
eraa_installer_url" > "$local_installer") && echo "$local_installer" >> "$cleanu
p_file"↓
else↓
  (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$era
a_installer_url" || curl --connect-timeout 300 -k "$eraa_installer_url" > "$loca
l_installer") && echo "$local_installer" >> "$cleanup_file"↓
fi↓
↓
echo -n "Checking integrity of installer script " && echo "$eraa_installer_check
sum  $local_installer" | shalsum -c↓
↓
chmod +x "$local_installer"↓
```

↓

書き換え後

```
↓
eraa_http_proxy_value="http://192.168.1.2:3128"↓
if test -n "$eraa_http_proxy_value"↓
then↓
  export use_proxy=yes↓
  export http_proxy="$eraa_http_proxy_value"↓
#  (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$er
aa_installer_url" || wget --connect-timeout 300 --no-proxy --no-check-certificat
e -O "$local_installer" "$eraa_installer_url" || curl --connect-timeout 300 -k "
$eraa_installer_url" > "$local_installer") && echo "$local_installer" >> "$clean
up_file"↓
else↓
#  (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$er
aa_installer_url" || curl --connect-timeout 300 -k "$eraa_installer_url" > "$loc
al_installer") && echo "$local_installer" >> "$cleanup_file"↓
fi↓
↓
echo -n "Checking integrity of installer script " && echo "$eraa_installer_check
sum  $local_installer" | shalsum -c↓
↓
chmod +x "$local_installer"↓
```

3 手順 2 の 2 番目にコメントアウトした行の次行に「true」の文字列を追加し、その下の「fi」の次行に「cp -a ${eraa_installer_url} ${local_installer}」の文字列を追加します。

```
↓
eraa_http_proxy_value="http://192.168.1.2:3128"↓
if test -n "$eraa_http_proxy_value"↓
then↓
  export use_proxy=yes↓
  export http_proxy="$eraa_http_proxy_value"↓
#  (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$er
aa_installer_url" || wget --connect-timeout 300 --no-proxy --no-check-certificat
e -O "$local_installer" "$eraa_installer_url" || curl --connect-timeout 300 -k "
$eraa_installer_url" > "$local_installer") && echo "$local_installer" >> "$clean
up_file"↓
else↓
#  (wget --connect-timeout 300 --no-check-certificate -O "$local_installer" "$er
aa_installer_url" || curl --connect-timeout 300 -k "$eraa_installer_url" > "$loc
al_installer") && echo "$local_installer" >> "$cleanup_file"↓
true↓
fi↓
↓
cp -a ${eraa_installer_url} ${local_installer}↓
echo -n "Checking integrity of installer script " && echo "$eraa_installer_check
sum  $local_installer" | shalsum -c↓
↓
chmod +x "$local_installer"↓
↓
local_migration_list="$(mktemp -q -u)"↓
tee "$local_migration_list" 2>&1 > /dev/null << __LOCAL_MIGRATION_LIST__↓
↓
__LOCAL_MIGRATION_LIST__↓
test $? = 0 && echo "$local_migration_list" >> "$cleanup_file"↓
↓
for dir in /sys/class/net/*/↓
do↓
  if test -f "$dir/address"↓
```

4 EraAgentInstaller.sh を更新します。

書き換えた EraAgentInstaller.sh ファイルは、書き換え前のファイルと同様にクライアントコンピューター上で実行し、展開します。

4.2.2.4 Windows へのローカル展開

インストーラーを使用して、クライアントコンピューターへ ERA エージェントをローカル展開します。

●インストーラーの日本語化

ERA エージェントのインストーラーはダブルクリックすると起動します。ですが、そのままでは英語での表記となっています。
インストール画面を日本語表記にする場合は、インストーラーをコマンドプロンプトから起動してください。
次の手順は、ERA エージェントのインストーラーファイルである Agent_x64.msi を、日本語で起動する場合の操作です。

!重 要

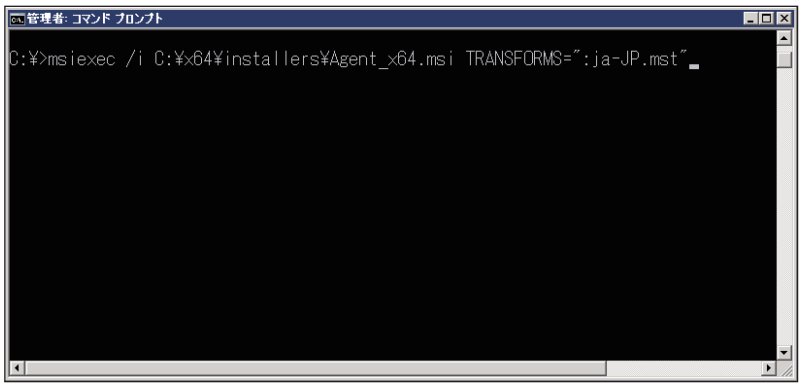
この操作は任意の操作です。必要に応じて行ってください。

操作手順

コマンドプロンプトを起動し、次のコマンドを入力します。
起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥Agent_x64.msi TRANSFORMS=":ja-JP.mst"`

ワンポイント

実行対象を、インストーラーが保存されているフォルダーに変更しない場合は、現在の実行対象に合わせて、msiexec /i 以降にインストーラーの絶対パス、または相対パスを指定してください。



ワンポイント

インストーラーを使用してインストールする際にログを残す場合は、次のコマンドを入力してください。
コマンド：`msiexec /i C:¥x64¥installers¥Agent_x64.msi /lv* c:¥temp¥installer_log.txt TRANSFORMS=":ja-JP.mst"`
※網掛けの箇所は、使用環境に合わせて適宜変更してください。保存先のフォルダーは事前に作成してください。

■サーバー支援インストール

サーバー支援インストールは、インストール中に ERA Web コンソール管理者の認証情報を指定することで、EAR サーバーとの接続に必要な証明書ファイルを自動でダウンロードします。

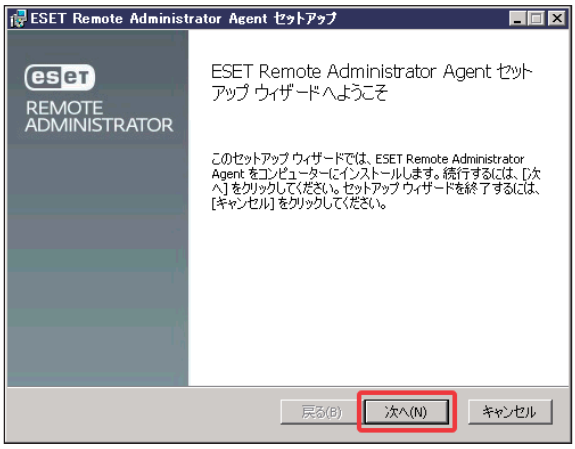
! 重 要

ここでは、ERA エージェントのインストーラーである Agent_x64.msi を、C:¥x64¥installers に保存した状態で操作を説明します。

操作手順

1 コマンドプロンプトから「Agent_x64.msi」を起動し、セットアップウィザードが表示されたら［次へ］ボタンをクリックします。

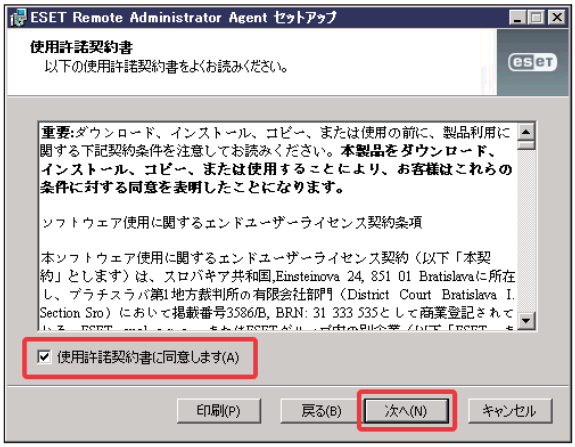
起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥Agent_x64.msi TRANSFORMS=":ja-JP.mst"`
ERA エージェントのセットアップウィザードが起動します。



ワンポイント

インストーラーの日本語化については、「3.3 Windows 版コンポーネントインストール」の「■インストーラーの日本語化」を参照してください。

2 使用許諾契約書を一読し同意する場合、［使用許諾契約書に同意します］にチェックを入れ、［次へ］ボタンをクリックします。

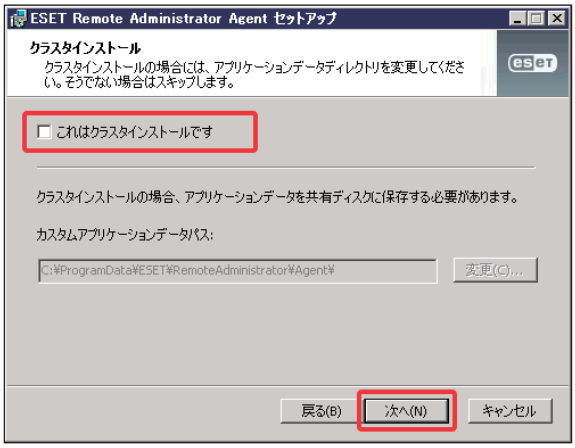


ワンポイント

チェックを外して［次へ］ボタンをクリックした場合、次の画面には進みません。

続く

❸［これはクラスタインストールです］のチェックを外し、［次へ］ボタンをクリックします。

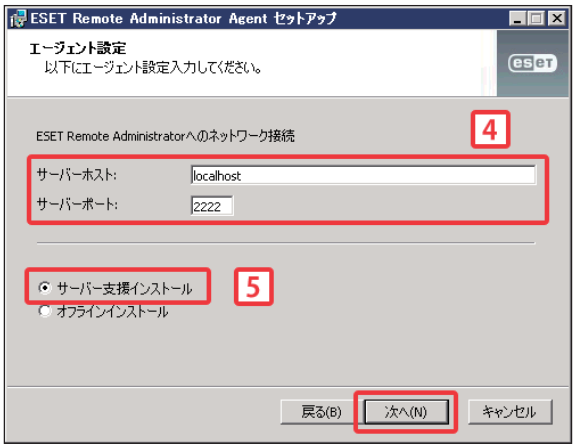


ワンポイント

フェールオーバー環境へのインストールの場合は、［これはクラスタインストールです］にチェックを入れます。「カスタムアプリケーションデータパス」には、クラスタ内のすべてのコンピューターが接続できる共有の場所を指定します。
フェールオーバー環境への操作は、「3.3.9 フェールオーバー環境へのインストール」を参照してください。

❹「サーバーホスト：」に ERA サーバーのホスト名（または IP アドレス）を入力し、「サーバーポート：」に使用するポートを入力します。

❺［サーバー支援インストール］を選択し、［次へ］ボタンをクリックします。



ワンポイント

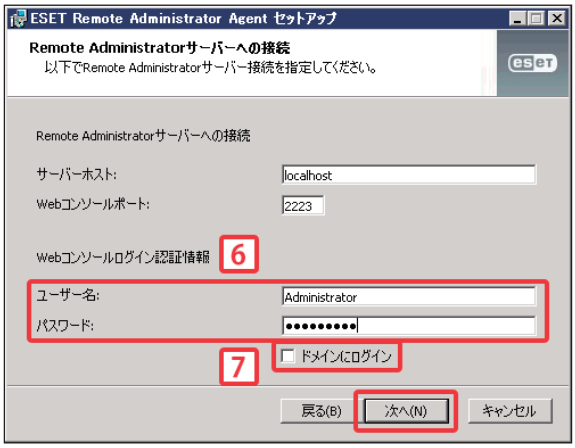
「サーバーホスト :」には、サーバーコンピューターの名前のほか、IP アドレスを設定できます。
ERA エージェントを、副系統（セカンダリ）サーバー、またはクライアントコンピューターへインストールする場合は、ERA サーバーが稼動している主系統（プライマリ）サーバーの名前、または IP アドレスを指定します。
既定の「サーバーポート :」は「2222」です。

続く

6 ERA Web コンソール管理者の「ユーザー名 :」と「パスワード :」を入力します。

ワンポイント
ERA Web コンソールの認証情報です。

7 ［ドメインにログイン］のチェックを外し、［次へ］ボタンをクリックします。



クリックするとサーバーと接続し、証明書のダウンロード準備に移ります。

ワンポイント
「サーバーホスト :」には、サーバーの名前のほか、IP アドレスを設定できます。
ERA エージェントを、副系統（セカンダリ）サーバー、またはクライアントコンピューターへインストールする場合は、ERA サーバーが稼動している主系統（プライマリ）サーバーの名前、または IP アドレスを指定します。
既定の「Web コンソールポート :」は「2223」です。

8 ［有効］ボタンをクリックします。

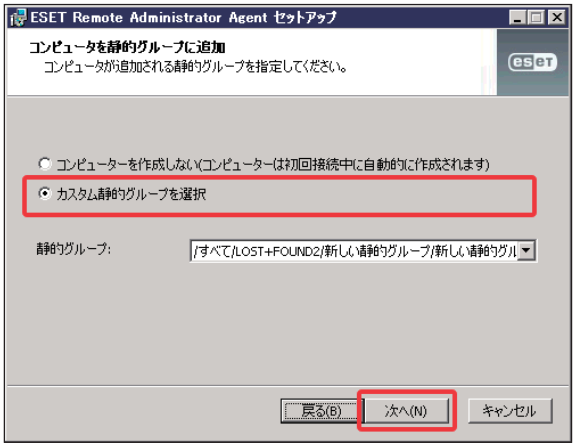
サーバー証明書を許可します。

ワンポイント
手順 4 において［サーバー支援インストール］を選択したことで、証明書ファイルをダウンロードするための許可が必要となります。

9 ［カスタム静的グループを選択］を選択し、「静的グループ :」から、コンピューターを所属させる静的グループを選択します。

続く

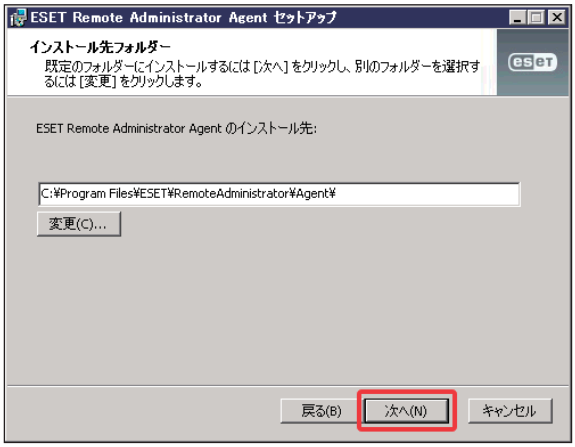
10 ［次へ］ボタンをクリックします。



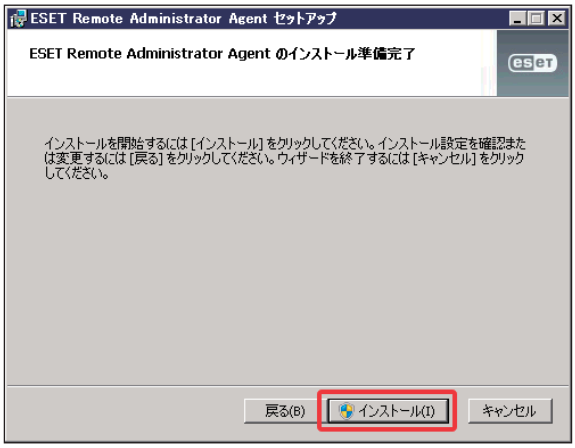
ワンポイント

［コンピューターを作成しない（コンピューターは初回接続中に自動的に作成されます）］を選択した場合、Agent が ERA サーバーと通信できた時に ERA のコンピューターに表示されます。この時、所属する静的グループは、登録されているコンピューターとして存在する場合は、そのグループ、存在しない場合は、「LOST+FOUND」グループです。

11 インストール先を確認し、［次へ］ボタンをクリックします。



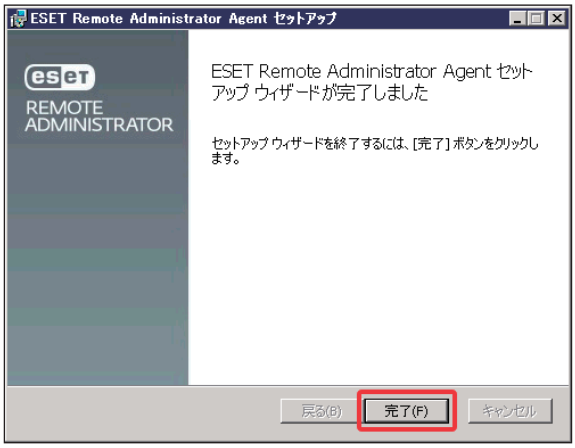
12 ［インストール］ボタンをクリックします。



ERA エージェントのインストールが開始されます。

続く

⑬ [完了] ボタンをクリックします。



! 重 要

クライアントコンピューター上で、ERA エージェントが正しく展開されているかを調べるには、ステータスログを確認します。ステータスログは次の場所に保存されています。

C:¥ProgramData¥ESET¥RemoteAdministrator¥Agent¥EraAgentApplicationData¥Logs¥status.html

また、ERA サーバーに接続していないなど、ERA エージェントに何らかの問題がある場合は、「4.2.2.7 トラブルシューティング - エージェント展開」を参照してください。

■オフラインインストール

オフラインインストールでは、ERA サーバーとの接続情報である、ピア証明書（エージェント）および証明局の公開鍵（以下　証明書ファイル）が必要です。ピア証明書（エージェント）および証明局の証明書ファイルは、ERA エージェントを展開したいクライアントコンピューターにあらかじめエクスポートしておいてください。ERA エージェントのオフラインインストールでは、ピア証明書（エージェント）および証明局の証明書ファイルの保存場所をインストール作業中に指定する必要があります。証明書の詳細については、「6.9　証明書」を参照してください。

! 重　要

オフラインインストールでは、「サーバー支援インストールのエージェント証明書」は使用できません。サーバー証明書（エージェント）または個別に作成した証明書（エージェント）を使用してください。

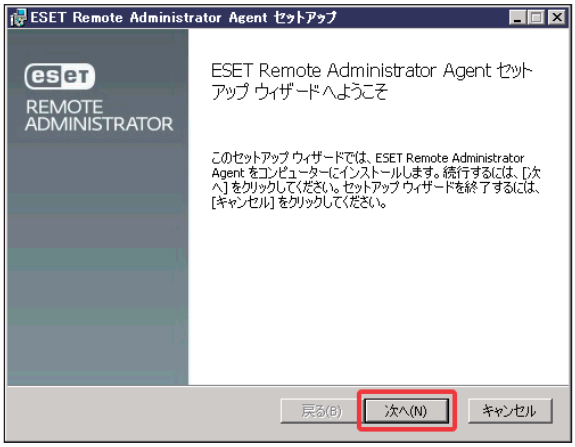
! 重　要

ここでは、ERA エージェントのインストーラーである Agent_x64.msi を、C:¥x64¥installers に保存した状態で操作を説明します。

操作手順

1. コマンドプロンプトから「Agent_x64.msi」を起動し、セットアップウィザードが表示されたら［次へ］ボタンをクリックします。

   起動コマンド：`C:¥>msiexec /i C:¥x64¥installers¥Agent_x64.msi TRANSFORMS=":ja-JP.mst"`
   ERA エージェントのセットアップウィザードが起動します。

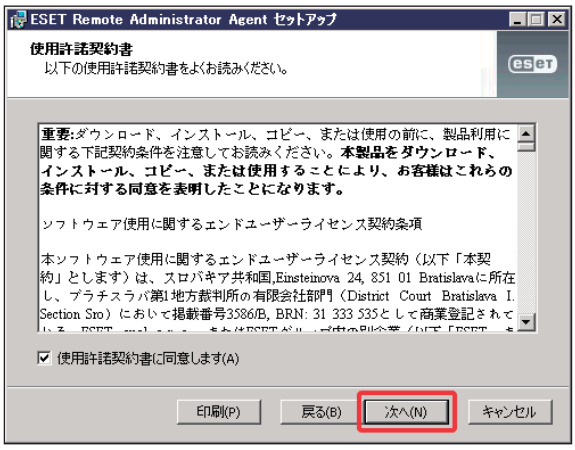


ワンポイント

インストーラーの日本語化については、「3.3　Windows 版コンポーネントインストール」の「■インストーラーの日本語化」を参照してください。

続く

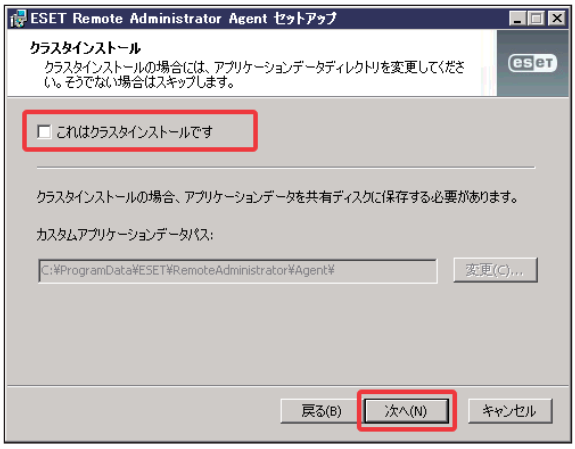
2 使用許諾契約書を一読し同意する場合、［使用許諾契約書に同意します］にチェックを入れ、［次へ］ボタンをクリックします。



ワンポイント

チェックを外して［次へ］ボタンをクリックした場合、次の画面には進みません。

3 ［これはクラスタインストールです］のチェックを外し、［次へ］ボタンをクリックします。



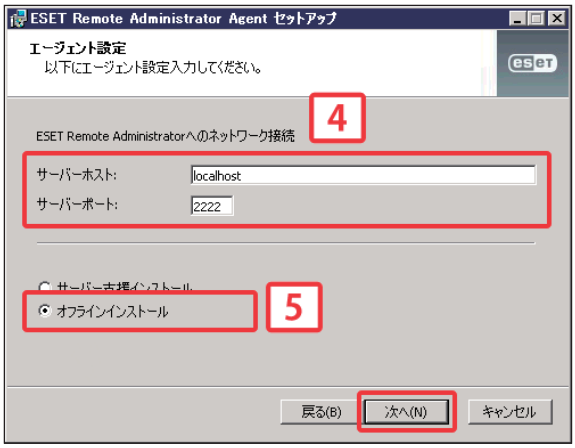
ワンポイント

フェールオーバー環境へのインストールの場合は、［これはクラスタインストールです］にチェックを入れます。「カスタムアプリケーションデータパス」には、クラスタ内のすべてのコンピューターが接続できる共有の場所を指定します。
フェールオーバー環境への操作は、「3.3.9 フェールオーバー環境へのインストール」を参照してください。

続く

4 「サーバーホスト：」に ERA サーバーのホスト名（または IP アドレス）を入力し、「サーバーポート：」に使用するポートを入力します。

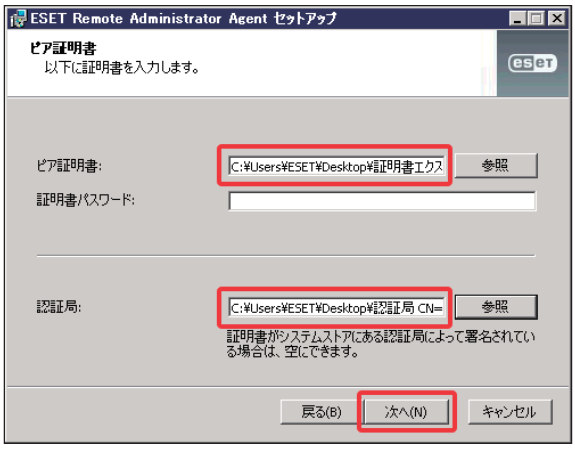
5 ［オフラインインストール］を選択し、［次へ］ボタンをクリックします。



ワンポイント

「サーバーホスト：」には、サーバーコンピューターの名前のほか、IP アドレスを設定できます。
ERA エージェントを、副系統（セカンダリ）サーバー、またはクライアントコンピューターへインストールする場合は、ERA サーバーが稼動している主系統（プライマリ）サーバーの名前、または IP アドレスを指定します。
既定の「サーバーポート：」は「2222」です。

6 「ピア証明書：」および「証明局：」に、ローカルコンピューター上にに保存したピア証明書と証明局の公開鍵を参照設定し、［次へ］ボタンをクリックします。



！重　要

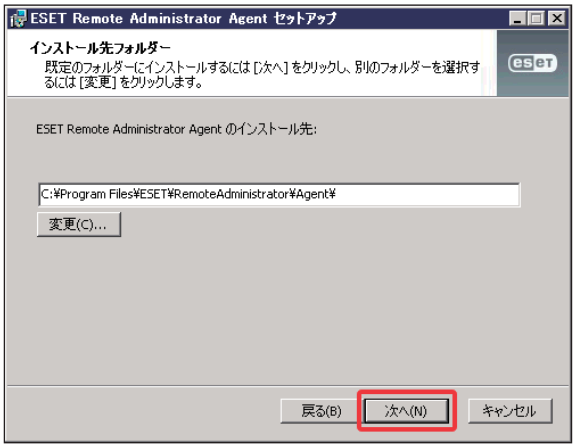
「ピア証明書」に「サーバー支援インストールのエージェント証明書」は設定しないでください。サーバー証明書（エージェント）または個別に作成した証明書（エージェント）を使用してください。

ワンポイント

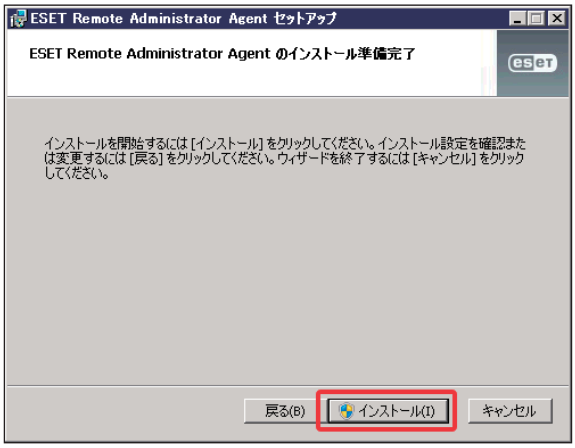
証明書にパスワードを設定している場合は、「証明書パスワード：」の入力が必要です。

続く

7 インストール先を確認し、［次へ］ボタンをクリックします。

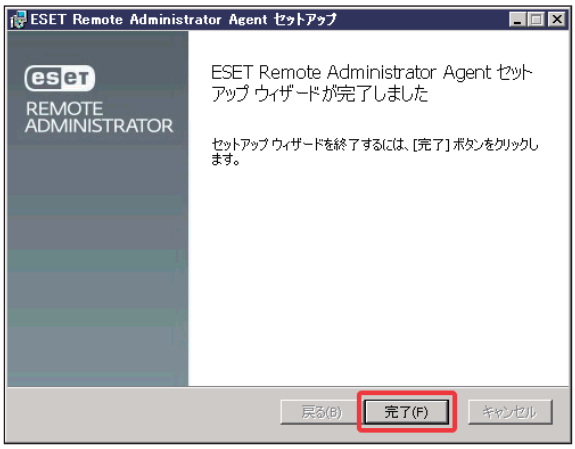


8 ［インストール］ボタンをクリックします。



ERA エージェントのインストールが開始されます。

9 ［完了］ボタンをクリックします。



! 重 要

クライアントコンピューター上で、ERA エージェントが正しく展開されているかを調べるには、ステータスログを確認します。ステータスログは次の場所に保存されています。

C:¥ProgramData¥ESET¥RemoteAdministrator¥Agent¥EraAgentApplicationData¥Logs¥status.html

また、ERA エージェントに何らかの問題がある場合は、「4.2.2.7 トラブルシューティング - エージェント展開」を参照してください。

4.2.2.5 Mac OS X へのローカル展開

■オフラインインストール

オフラインインストールでは、ERA サーバーとの接続情報である、ピア証明書（エージェント）および証明局の公開鍵（以下　証明書ファイル）が必要です。ピア証明書（エージェント）および証明局の証明書ファイルは、ERA エージェントを展開したいクライアントコンピューターにあらかじめエクスポートしておいてください。ERA エージェントのオフラインインストールでは、ピア証明書（エージェント）および証明局の証明書ファイルの保存場所をインストール作業中に指定する必要があります。証明書の詳細については、「6.9　証明書」を参照してください。

! 重　要

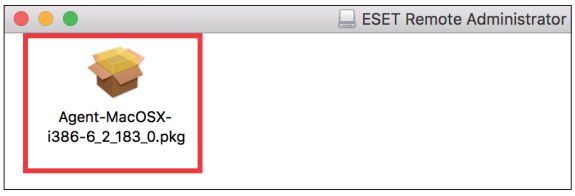
オフラインインストールでは、「サーバー支援インストールのエージェント証明書」は使用できません。サーバー証明書（エージェント）または個別に作成した証明書（エージェント）を使用してください。

! 重　要

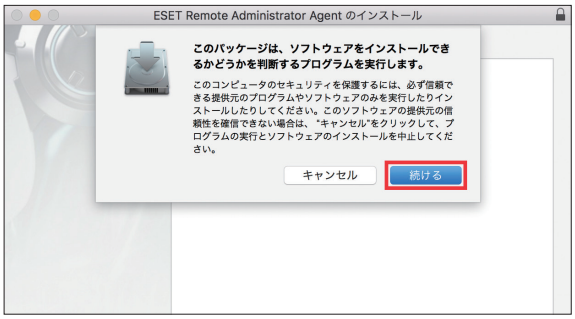
ここでは、ERA エージェントのインストーラーである Agent-MacOSX-i386.dmg とピア証明書（エージェント）および証明局の証明書ファイルを、デスクトップの「inst」フォルダーに保存した状態で操作を説明します。

操作手順

1. ERA エージェントのインストーラーをダブルクリックします。
2. インストールパッケージファイル（.pkg）をダブルクリックします。

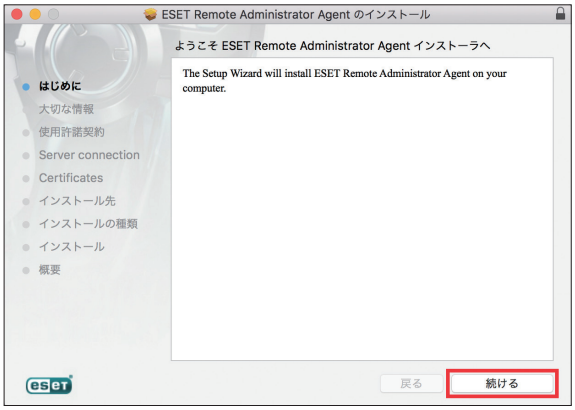


3. インストーラーが起動します。［続ける］ボタンをクリックします。

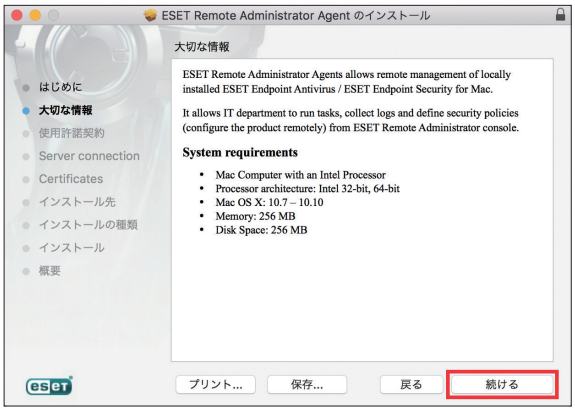


続く

4 [続ける] ボタンをクリックします。



5 [続ける] ボタンをクリックします。

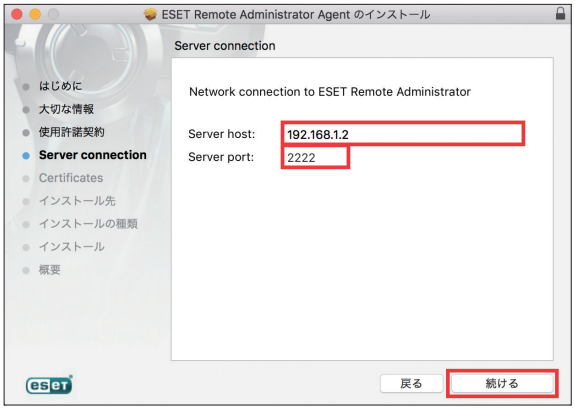


6 [続ける] ボタンをクリックします。

続く

7 「同意する」ボタンをクリックします。

8 「Server host：」に ERA サーバーのホスト名（または IP アドレス）を入力し、「Server port：」に使用するポートを入力して、［続ける］ボタンをクリックします。

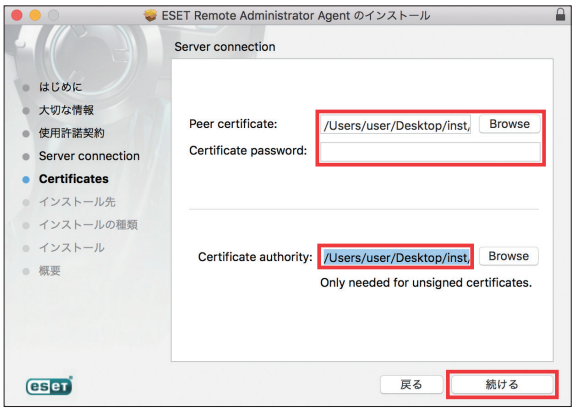


ワンポイント

「Server host:」には、サーバーコンピューターの名前のほか、IP アドレスを設定できます。ERA エージェントを、副系統（セカンダリ）サーバー、またはクライアントコンピューターへインストールする場合は、ERA サーバーが稼動している主系統（プライマリ）サーバーの名前、または IP アドレスを指定します。
既定の「Server port:」は「2222」です。

続く

9 「Peer certificate:」および「Certificate authority:」に、あらかじめ保存しておいたピア証明書（Peer certificate）と証明局（Certificate authority）の公開鍵を参照設定し、[続ける] ボタンをクリックします。



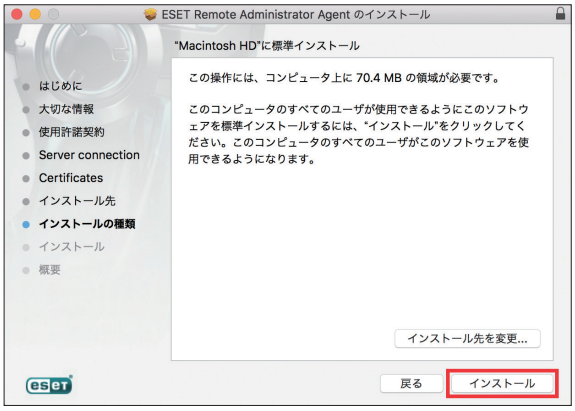
! 重 要

「Peer certificate:」に「サーバー支援インストールのエージェント証明書」は設定しないでください。サーバー証明書（エージェント）または個別に作成した証明書（エージェント）を使用してください。

ワンポイント

証明書にパスワードを設定している場合は、「Certificate password:」の入力が必要です。

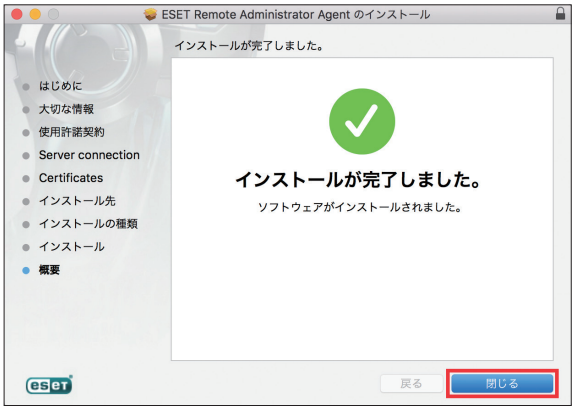
10 [インストール] ボタンをクリックします。



11 ユーザー名とパスワードを入力して、[ソフトウェアをインストール] ボタンをクリックします。

続く

⑫ インストールが完了したら、［閉じる］ボタンをクリックします。



ワンポイント

クライアントコンピューター上で、ERA エージェントが正しく展開されているかを調べるには、ステータスログを確認します。ステータスログは次の場所に保存されています。
/Library/Application Support/com.eset.remoteadministrator.agent/Logs/status.html
また、ERA サーバーに接続していないなど、ERA エージェントに何らかの問題がある場合は、「4.2.2.7 トラブルシューティング - エージェント展開」を参照してください。

■アンインストール

ERA エージェントのアンインストール操作を説明します。

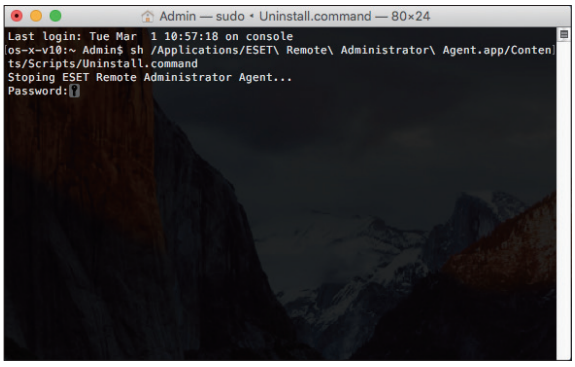
操作手順

① Finder を開き、［アプリケーション］＞［ユーティリティ］とクリックします。

② ［ターミナル］をダブルクリックします。

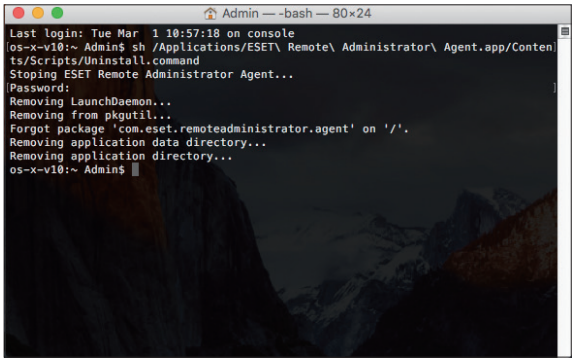
③ ターミナルで、次のコマンドを入力します。「Password：」と表示されたときは、管理者パスワードを入力します。

起動コマンド：
sh /Applications/ESET\Remote\Administrator\Agent.app/Contents/Scripts/Uninstall.command



続く

4 ERA エージェントのアンインストールが開始されます。



以上で、ERA エージェントのアンインストールは終了です。
アプリケーション一覧より、ERA エージェントがアンインストールされていることを確認してください。

4.2.2.6 Linux へのローカル展開

ERA エージェントの展開では ERA サーバーとの接続情報である、ピア証明書（エージェント）および証明局の公開鍵（以下　証明書ファイル）が必要です。
Linux OS への ERA エージェント展開では、証明書ファイルの指定方法によってインストーラーに指定するオプションが変わります。
証明書ファイルの指定方法とオプションは、次のとおりです。

■サーバー支援インストール

インストール中に ERA Web コンソール管理者の認証情報を指定することで、EAR サーバーとの接続に必要な証明書ファイルを自動でダウンロードします。そのため ERA Web コンソール管理者の情報を指定します。
インストールコマンドで、次のオプションの設定が必要です。

ERA Web コンソールの管理者名	--webconsole-user
ERA Web コンソールの管理者パスワード	--webconsole-password
ERA Web コンソールのポート番号	--webconsole-port

■オフラインインストール

あらかじめクライアントコンピューターにエクスポートした、証明書ファイルを指定する必要があります。
別途、ERA Web コンソールから、証明書ファイルをエクスポートします。
インストールコマンドで、次のオプションの設定が必要です。

保存したピア証明書（エージェント）のパス	--cert-path
ピア証明書のパスワード	--cert-password
認証局ファイルの保存場所	--cert-auth-path

そのほか、指定が必要な項目は、「● ERA エージェント　インストールオプション一覧」を参照してください。

ワンポイント

オフラインインストールの場合は、次の方法で認証局ファイルのパスワードを設定してください。
・ERA サーバーのインストール時に --cert-auth-password および --peer-cert-password オプションを設定する
・ESET Remote Administrator 上で、認証局およびピア証明書（エージェント）を新たに作成する
証明書への操作については「6.9　証明書」を参照してください。

ワンポイント

ERA サーバーへの接続は、次の 4 つのパターンから選択して指定します。
・ERA サーバーコンピューター名とポート番号
・ERA サーバーの IPv4 アドレスとポート番号
・ERA サーバーの IPv6 アドレスとポート番号
・SRV レコード
SRV レコードは、DNS サーバーを使用している場合に指定が可能です。
SRV レコードを指定した場合、ポート番号は不要です。また、SRV レコードのプレフィックスを「_ NAME._tcp」としてください。
※網掛け箇所を、適宜変更します。例）_era._tcp など

● ERA エージェント　インストールオプション一覧

ERA エージェントのインストールでのオプションの一覧です。必須となっているオプションは、インストールと同時に設定します。

オプション	説明	設定値	必須※1
--skip-license	ライセンス認証の省略		-
--hostname	ERA サーバーのコンピューター名または IP アドレス		○
--port	ERA サーバーのポート番号	2222（既定値）	○
--cert-path※2	ピア証明書（エージェント）ファイルのパス		○ 1
--cert-auth-path	認証局のファイルのパス		○ 1
--cert-password※3	ピア証明書（エージェント）ファイルのパスワード	認証局のパスワードと同一	○ 1
--cert-auth-password	認証局のパスワード		-
--product-guid	製品 GUID	設定しない場合は自動生成	-
--cert-content※2	サーバーとエージェントとの安全な通信チャネルを設定するために使用される PKCS12 暗号化公開鍵証明書と秘密鍵の Base64 暗号化内容		-
--cert-auth-path または --cert-auth-content	ピア証明書（プロキシまたはサーバー）を検証するために使用される DER 暗号化認証局秘密鍵の Base64 暗号化内容		-
--webconsole-hostname※4	ERA Web コンソールのコンピューター名または IP アドレス		-
--webconsole-user	ERA Web コンソール管理者名	Administrator	○ 2
--webconsole-password	ERA Web コンソール管理者パスワード		○ 2
--webconsole-port	ERA Web コンソールのポート番号	2223	○ 2
--help	オプション一覧の表示		
--uninstall	アンインストール		-

※ 1　○ 1 および○ 2 は、証明書ファイルの指定方法を選択することで必須種別が変わります。

※ 2　--cert-path、--certcontent のどちらかを使用します。

※ 3　ピア証明書にパスワードを設定している場合は、このオプションを使用してパスワードを指定します。

※ 4　--hostname と同一の場合は、設定する必要はありません。

ワンポイント

オプション一覧はターミナル上で確認することができます。
コマンド：`./x64/Agent-Linux- x 86_64.sh -help`

■ ERA エージェント展開の設定確認

ERA エージェントのインストールの際に必要となるオプション設定を確認します。
インストーラーの起動と共に、次のオプションを指定してください。

!重 要

ここでは、オフラインインストールを使用して ERA エージェントをインストールします。
サーバー支援インストールを使用したインストール操作については、「3.4.6 ERA エージェントのインストール」を参照してください。

設定内容	使用するオプション	設定例
ライセンス認証の省略	--skip-license	-
ERA サーバーのコンピューター名または IP アドレス	--hostname	=1.1.1.1
ERA サーバーのポート番号	--port	=2222
保存したピア証明書（エージェント）のパス	--cert-path	./ デスクトップ ...
ピア証明書（エージェント）のパスワード	--cert-password	XXXXXXX
認証局ファイルのパス	--cert-auth-path	./ デスクトップ ...

!重 要

ここでは、便宜的に ERA サーバーのコンピューター名または IP アドレスの指定である --hostname の設定値を 1.1.1.1 としています。ERA エージェントのインストーラーである Agent-Linux-x86_64.msi を、/root/x64 フォルダーに保存した状態で説明します。
x64 フォルダーは、手動で作成してください。
また、インストールに必要となる証明書ファイルは、事前にデスクトップ（./ デスクトップ）にエクスポートしています。

証明書の操作については、「6.9 証明書」を参照してください。

●インストール

操作手順

1. root フォルダーのターミナルを開きます。
2. ERA エージェントインストーラーに実行権限を付与します。

コマンド：`chmod +x ./x64/Agent-Linux-x86_64.sh`

ERA エージェントインストーラーのアクセス権限が変わります。

3. ERA エージェントインストーラーを起動します。

コマンド：`sudo ./x64/Agent-Linux-x86_64.sh \`

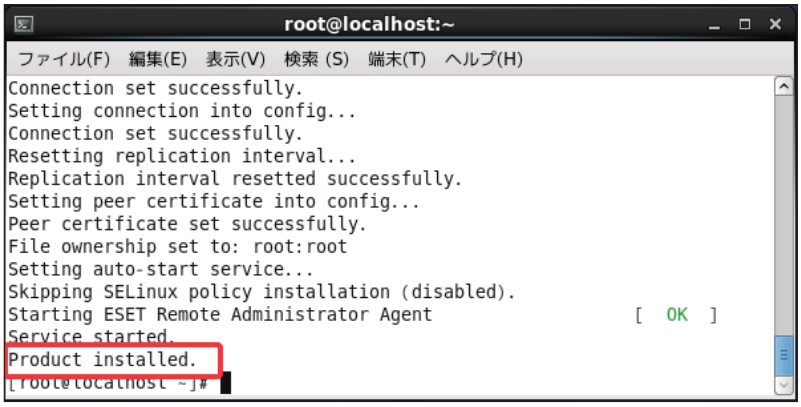
4. 続けて、オプションと設定値を入力します。

```
--skip-license \
--hostname=1.1.1.1 \
--port=2222 \
--cert-path="./ デスクトップ / 証明書エクスポート CN=Agent at_C=US.pfx" \
--cert-password=XXXXXXXX \
--cert-auth-path="./ デスクトップ / 認証局 CN=Server Certification Authority C=US public key.der
```

続く

5 【Enter】キーを押します。

コマンドに記載したオプションの設定に従って、ERA エージェントのインストールが開始されます。



Product installed. が表示されたら、インストールは終了します。

ERA エージェントは、/opt/eset/RemoteAdministrator/Agent フォルダーにインストールされます。

6 ERA エージェントの稼動を確認します。

コマンド：`sudo service eraagent status`
`sudo initctl status eraagent`

「... を実行中」または「...running」と表示されたら、ERA エージェントは稼働中です。

! 重 要

ERA の認証局以外で作成、署名した証明書を使用する場合は、サーバーコンピューター上にほかの認証局がすでにインストールされているため、インストールの際に、認証局のファイルパスである --cert-auth-path オプションを設定する必要があります。

ワンポイント

ERA エージェントの動作は、クライアントコンピューターのステータスログから確認することができます。
ステータスログの保管場所：/ver/log/eset/RemoteAdministrator/Agent/trace.log
または　/ver/log/eset/RemoteAdministrator/Agent/status.html

4.2.2.7 トラブルシューティング - エージェント展開

ERA エージェント展開中には問題が発生し、展開が正しく行われない場合があります。
ここでは、問題の詳細と対策の確認方法と、解決策を解説します。

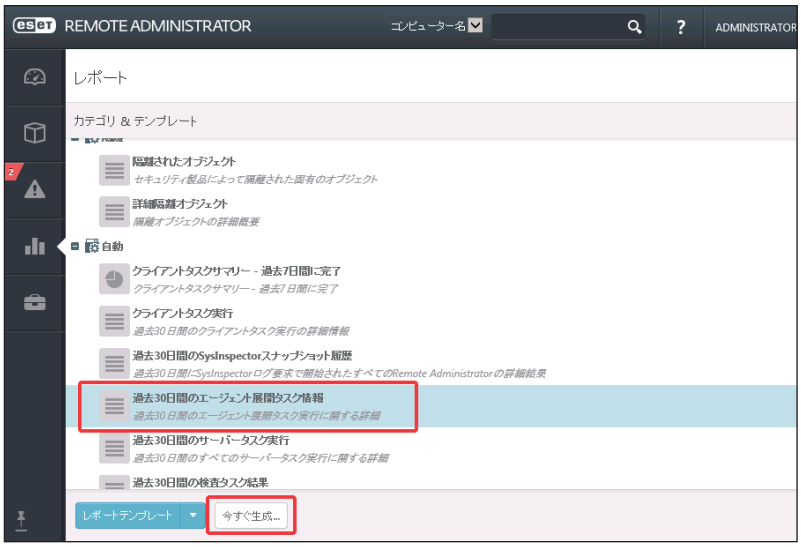
■ Windows

● ERA エージェント展開の進行状況と原因の確認

ERA エージェント展開の進行状況の確認は、レポートで行います。

操作手順

1. ERA Web コンソールの［レポート］メニューをクリックします。
2. 「自動」の［過去 30 日間のエージェント展開タスク情報］を選択し、［今すぐ生成 ...］ボタンをクリックします。



選択したレポートのテーブルが表示されます。

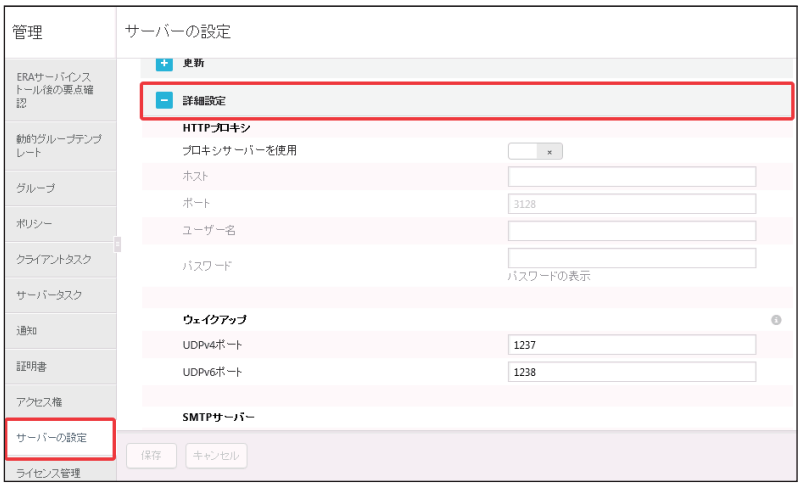
進行状況列に、ERA エージェントの展開が失敗した理由を説明するエラーメッセージが表示されます。

ERA サーバーのトレースログでの詳細確認

発生した問題の詳細を確認する必要がある場合は、ERA サーバーのトレースログファイル（trace.log）の出力内容を事前に設定しておくことで、ERA エージェント展開の失敗の原因や、問題の解決方法がトレースログに出力されます。

操作手順

1. ERA Web コンソールの［管理］メニューをクリックします。
2. ［サーバーの設定］>［詳細設定］をクリックします。



3. 「ロギング」に移動し、「トレースログの詳細レベル」から、［エラー］を選択します。

4. ［保存］ボタンをクリックします。

続く

5 サーバータスクに移り、エージェント展開をもう一度実行します。

ERA サーバーの最新のログファイルの保存場所は、次のとおりです。

C:¥ProgramData¥ESET¥RemoteAdministrator¥Server¥EraServerApplicationData¥Logs¥trace.log

ERA エージェントのインストールログファイルである、Client ra-agent-install.log は次の場所に保存されます。

C:¥Users¥%user%¥AppData¥Local¥Temp¥ra-agent-install.log

完全なロギングを有効にする

trace.log ファイルへの、完全なロギングを有効にするには、次の操作を行ってください。

1. 上記の trace.log と同じフォルダーに、traceAll（拡張子なし）のファイルを作成します。
2. ERA サーバーサービスを再開します。

●表に従って考えられる原因を確認する

エラーメッセージ	考えられる原因
接続できませんでした	・クライアントがネットワークで到達できません。ファイアウォールが通信をブロックします。 ・受信ポート 135、137、138、139、445 がクライアントのファイアウォールまたは Windows Firewall で開いていません。受信ファイルとプリンター共有例外の許可が使用されていません。 ・クライアントのホスト名を解決できませんでした。有効な FQDN コンピューター名を使用してください。
アクセスは拒否されました	・ドメインに参加しているサーバーからドメインに参加しているクライアントに展開するときには、ドメイン¥ドメイン管理者の形式でドメイン管理者グループのメンバーであるユーザーの資格情報を使用します。 ・ドメインに参加しているサーバーからドメインに参加しているクライアントに展開するときには、ネットワークサービスから ERA サーバーサービスを一時的に昇格し、ドメインアカウント管理者の下で実行できます。 ・サーバーから同じドメインにないクライアントに展開するときには、ターゲットコンピューターの UAC フィルタリングを無効にします。 ・サーバーから同じドメインにないクライアントに展開するときには、管理者の形式で管理者グループのメンバーであるローカルユーザーの資格情報を使用します。ターゲットコンピューター名が自動的にログインの最初に追加されます。 ・管理者アカウントのパスワードが設定されていません。 ・不十分なアクセス権です。 ・ADMIN$ 管理共有が使用できません。 ・IPC$ 管理共有が使用できません。 ・簡易ファイル共有の使用が有効です。
パッケージがリポジトリに見つかりません	・リポジトリへのリンクが正しくありません。 ・リポジトリが使用できません。 ・リポジトリには特定の必要なパッケージがありません。

●問題を解決して、展開を正常に実行する

考えられる原因に応じて、適切なトラブルシューティング手順を実施します。

考えられる原因	対応策
クライアントがネットワークで到達できません	ERA サーバーからクライアントの接続を確認します。 応答がある場合は、リモートでクライアントコンピューターにログインします（リモートデスクトップ経由など）。
クライアントのホスト名を解決できませんでした	DNS の問題に対する考えられる解決策には次の点があります（ただしこれに限定されません）。ERA エージェント展開の問題が発生しているクライアントまたはサーバーの IP アドレスとホスト名の nslookup コマンドを使用します。結果はコンピューターからの情報と一致するはずです。例えば、ホスト名の「nslookup」は、問題のホストで ipconfig コマンドによって表示される IP アドレスを解決します。 nslookup コマンドはクライアントとサーバーで実行される必要があります。 重複する DNS レコードがあるかどうか手動で調査します。
ファイアウォールが通信をブロックしています	クライアントとサーバーの両方で、ファイアウォール設定と、これらの 2 台のコンピューター間に存在する他のファイアウォール（該当する場合）を確認します。
ポート 2222 と 2223 が、クライアントとサーバーの両方のファイアウォールで開いていません	クライアントとサーバーの両方で、ファイアウォール設定と、これらの 2 台のコンピューター間に存在する他のファイアウォール（該当する場合）を確認します。さらに、クライアントとサーバー、2 台のコンピューター間のすべてのファイアウォールでこれらのポートが開いていることを確認してください。
管理者アカウントのパスワードが設定されていません	管理者アカウントの適切なパスワードを設定します（空のパスワードは使用しないでください）。
不十分なアクセス権です	エージェント展開タスクの作成時にドメイン管理者の認証情報を使用してください。ワークグループにクライアントコンピューターがある場合、その特定のコンピューターでローカル管理者アカウントを使用します。
ADMIN$ 管理共有が使用できません	クライアントコンピューターで共有リソース ADMIN$ を有効にする必要があります。他の共有（[スタート] > [コントロールパネル] > [管理ツール] > [コンピューター管理] > [共有フォルダ] > [共有]）間でこれがあることを確認してください。
IPC$ 管理共有が使用できません	クライアントが IPC にアクセスできることを確認します。クライアントのコマンドプロンプトから次のコマンドを実行します。 「net use ¥¥servername¥IPC$servername」は ERA サーバーの名前です。
簡易ファイル共有の使用が有効です	「アクセスが拒否されました」というエラーメッセージが表示され、ドメインとワークグループの両方を含む混合環境を使用している場合は、エージェント展開の問題が発生しているすべてのコンピューターで、[簡易ファイル共有を使用する] または [共有ウィザードを使用する] を無効する操作を行ってください。 例）「Windows 7 での操作」 1. [スタート] > 検索ボックスで「フォルダ」と入力 2. フォルダオプションをクリック 3. 表示タブの詳細設定ボックスの [共有ウィザードを使用] のチェックを外す
リポジトリへのリンクが正しくありません	ERA Web コンソールの [管理] > [サーバー設定] に移動し、[詳細設定] > [リポジトリ] をクリックして、リポジトリの URL が正しいことを確認します。
リポジトリには特定の必要なパッケージがありません	通常、このエラーメッセージは、ERA リポジトリに接続していないときに表示されます。インターネット接続を確認してください。

! 重 要

新しい Windows オペレーティングシステム（Windows 7、Windows 8 など）では、ERA エージェント展開タスクを実行するために、Administrator ユーザーアカウントを有効にする必要があります。
Administrator ユーザーアカウントを有効にするには、コマンドプロンプトで . 次のコマンドを入力します。

```
net user administrator /active:yes
```

■ Linux と Mac OS X

Linux または Mac OS X でエージェント展開が動作しない場合、一般的に、SSH の問題が原因です。
クライアントコンピューターを確認し、SSH デーモンが実行中であることを確かめてください。
修正終了後に、ERA エージェントの展開を再度実行します。

4.2.3 製品インストール

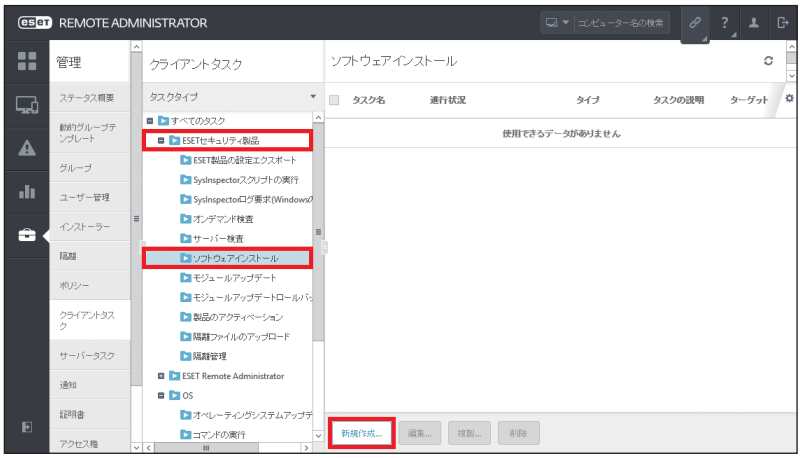
ESET 製品をクライアントコンピューターに展開します。
クライアントコンピューターに ERA エージェントを展開することにより、ESET 製品をクライアントコンピューターにインストールすることができます。

4.2.3.1 ESET 製品のリモートインストール

ESET 製品のリモートインストールの設定は、クライアントタスクから行います。

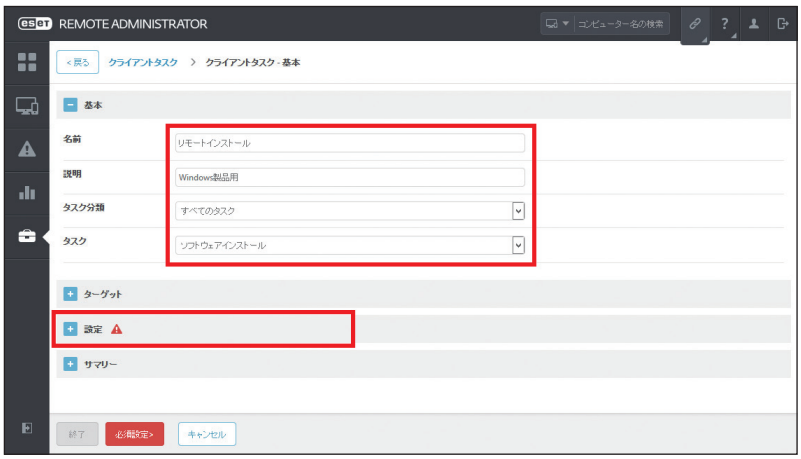
操作手順

1. ERA Web コンソールの［管理］メニューから［クライアントタスク］サブメニューを選択します。
2. ［ESET セキュリティ製品］の［ソフトウェアインストール］を選択し、［新規作成 ...］ボタンをクリックします。



「クライアントタスク－基本」画面が表示されます。

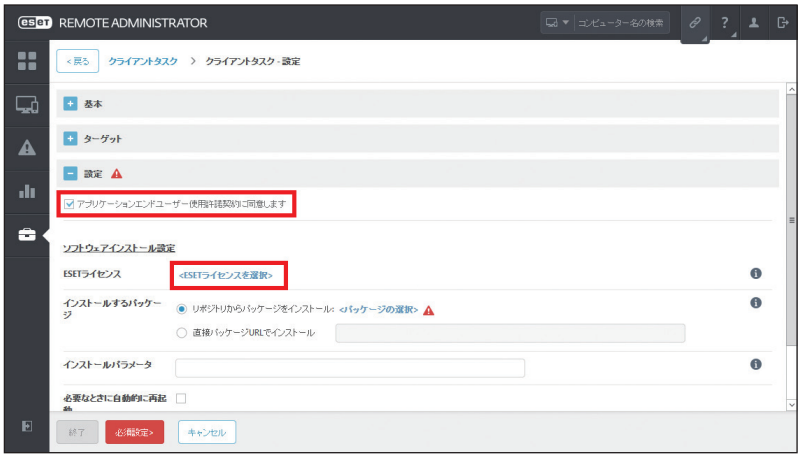
3. 「名前」「説明」を入力し、「タスク」に、［ソフトウェアインストール］が選択されているのを確認します。［設定］をクリックします。



「設定」画面が表示されます。

続く

4 ［アプリケーションエンドユーザー使用許諾契約に同意します］にチェックを入れ、［< ESET ライセンスを選択>］をクリックします。

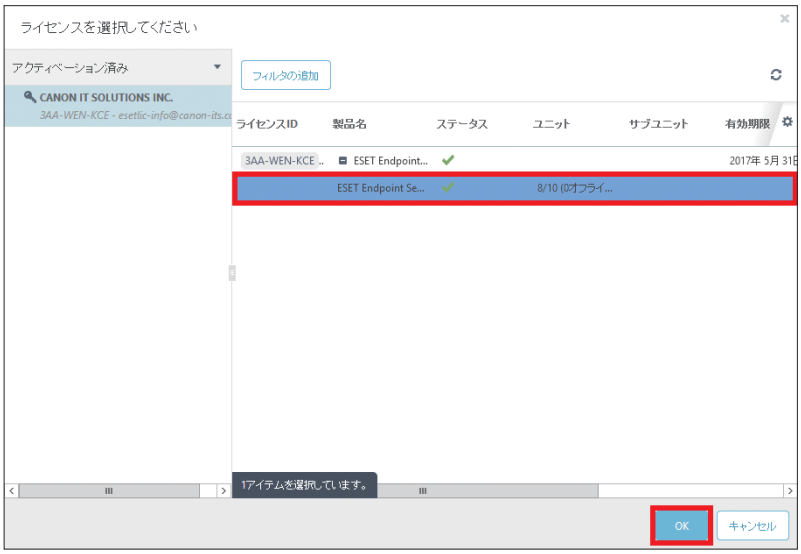


「ライセンスを選択してください」画面が表示されます。

ワンポイント

「アプリケーションエンドユーザー使用許諾契約」の詳細については、「6.12　ライセンス管理」を参照してください。

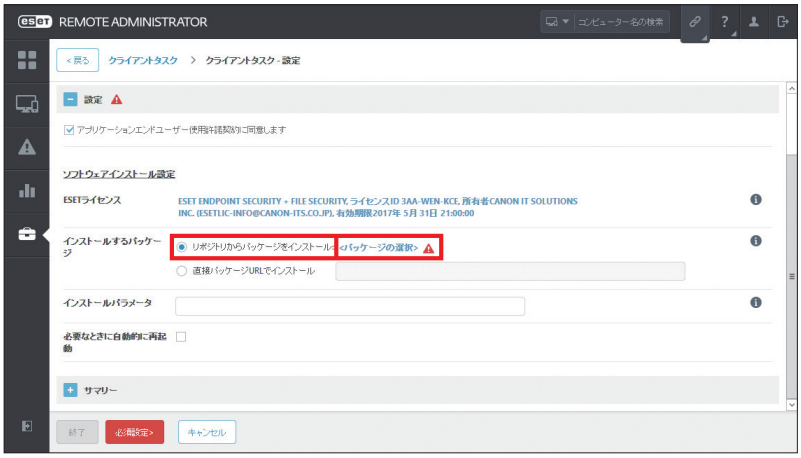
5 利用するライセンスを選択して、［OK］ボタンをクリックします。



「設定」画面に戻ります。

続く

6 ［リポジトリからパッケージをインストール］を選択し、［<パッケージの選択>］をクリックします。

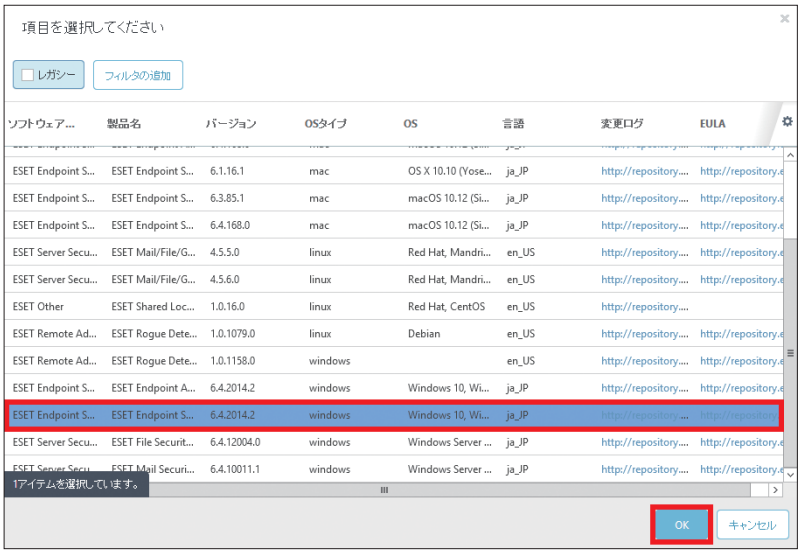


ESET 製品の一覧が表示されます。

ワンポイント

インストールパッケージの URL を指定する場合は、［直接パッケージ URL でインストール］を選択し、URL をテキストボックスに入力します。
例）ローカルの場合：file://c:¥install¥ees_nt64_JPN.msi
この場合、認証が必要な URL は使用しないでください。

7 インストールする ESET 製品を選択し、［OK］ボタンをクリックします。



「インストールするパッケージ」に、指定した ESET 製品が表示されます。

続く

8 インストール後に再起動が必要な場合の動作を選択します。

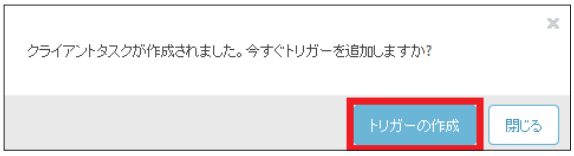
インストール後に自動的に再起動を行う場合は、［必要なときに自動的に再起動］にチェックを入れます。
設定後［終了］ボタンをクリックします。
「インストールパラメーター」は、必要に応じて入力します。

ダイアログボックスが表示されます。

ワンポイント

［必要なときに自動的に再起動］のチェックを外すと、クライアントコンピューターの再起動については、使用しているユーザーの判断に任せることになります。

9 ［トリガーの作成］をクリックします。



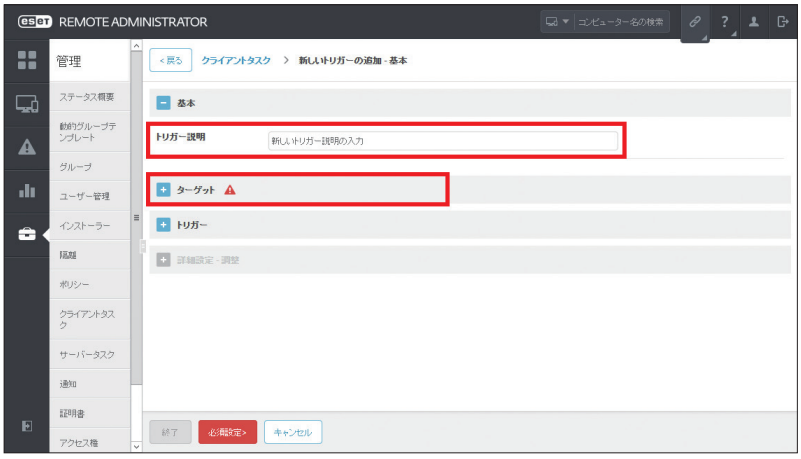
「新しいトリガーの追加 - 基本」画面が表示されます。

ワンポイント

［閉じる］をクリックすると、タスクの作成のみが行われ、タスクの実行は行われませんん。作成したタスクを目的のコンピューターやグループに対して実行するには、実行開始時にトリガーの設定を行う必要があります。

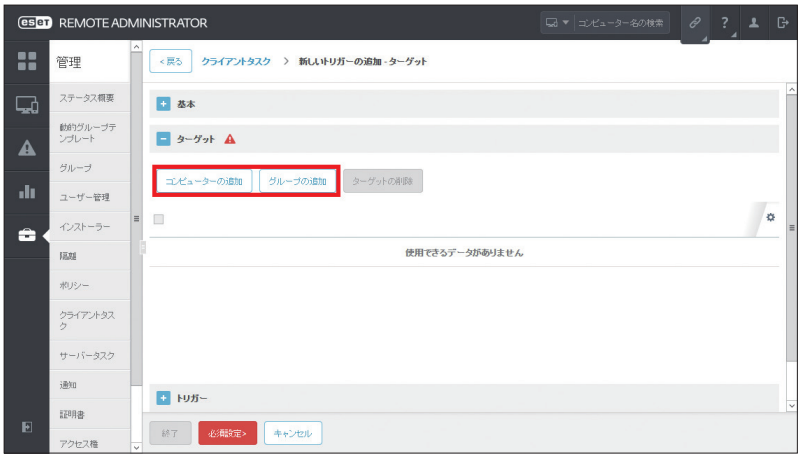
続く

10 必要に応じて「トリガーの説明」を入力し、［ターゲット］をクリックします。



「新しいトリガーの追加 - ターゲット」画面が表示されます。

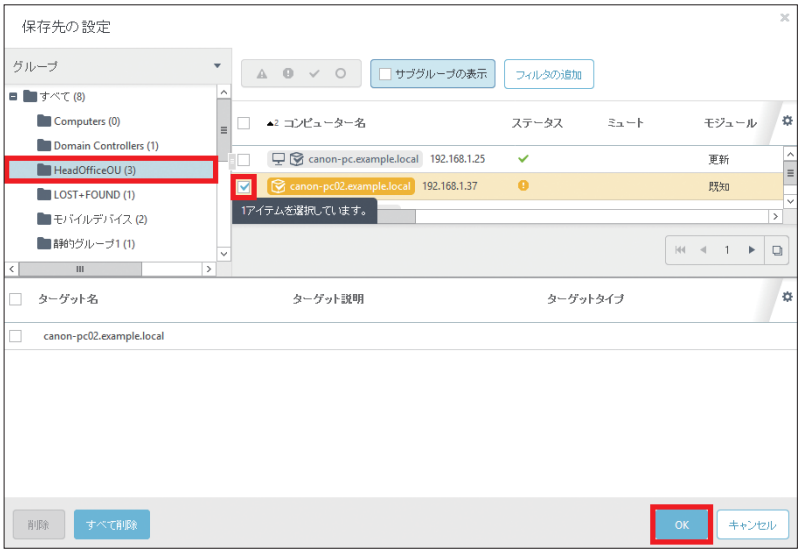
11 ［コンピューターの追加］または［グループの追加］（ここでは、［コンピューターの追加］）をクリックします。



ターゲットコンピューターまたはグループを選択する画面が表示されます。

続く

⑫ タスクを受信するコンピューターすべてにチェックを入れ、［OK］ボタンをクリックします。

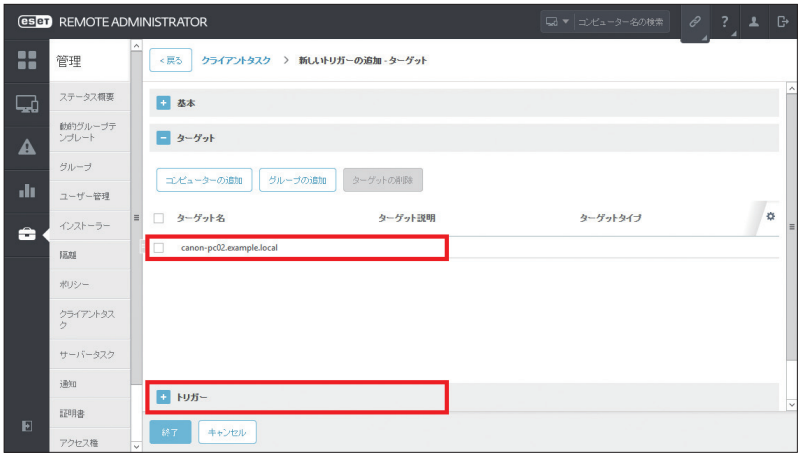


「新しいトリガーの追加 - ターゲット」画面に戻ります。

ワンポイント

手順 11 で［グループの追加］をクリックしたときは、手順 12 でタスクを受信するグループすべてにチェックを入れて、［OK］ボタンをクリックします。

⑬ ターゲットに手順 12 で選択したコンピューターまたはグループが登録されます。［トリガー］をクリックします。

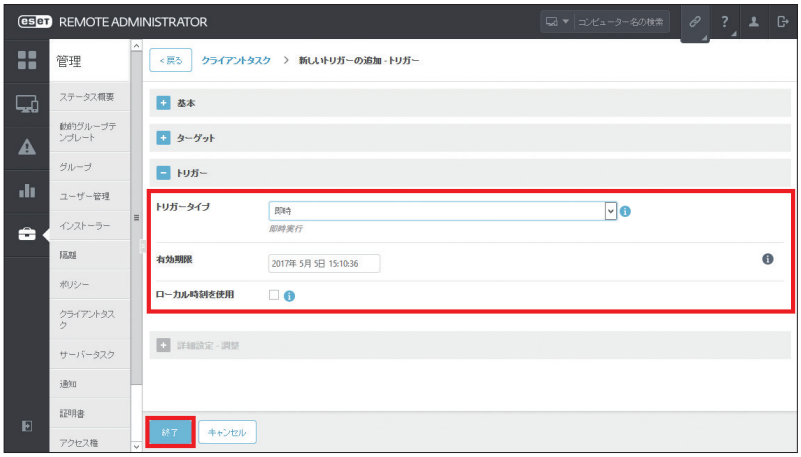


「新しいトリガーの追加 - トリガー」画面が表示されます。

続く

14 「トリガータイプ」からトリガーの種類を選択して、［終了］ボタンをクリックします。

必要に応じ「有効期限」と「ローカル時刻を使用」を設定します。

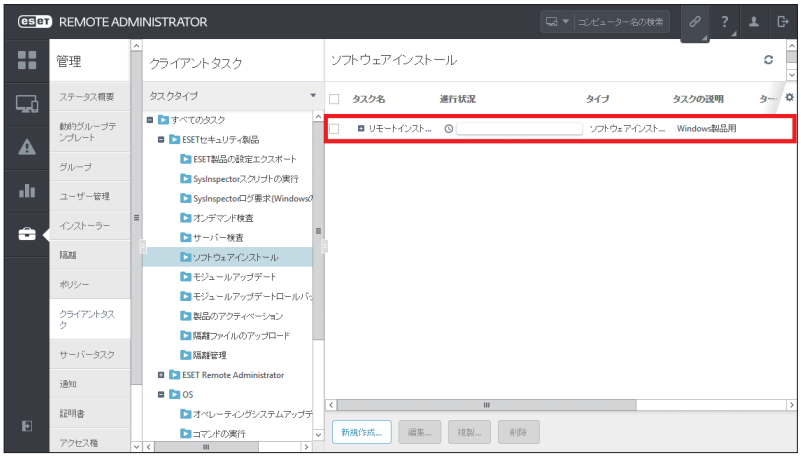


ソフトウェアインストールの一覧画面に戻ります。

ワンポイント

トリガータイプの「直ちに実行」は、タスクをすぐに送信します。
「ローカル時刻を使用」のローカル時刻は、クライアントコンピューターの時刻を表します。

15 設定したタスクが表示されます。



!重 要

リポジトリに接続してインストールを実行するためには、ERA サーバーおよび ERA エージェントがインターネットに接続できる必要があります。インターネットに接続していない場合は、クライアントソフトウェアをローカルでインストールしてください。

4.2.3.2 コマンド入力からの製品インストール

コマンドプロンプトから、msiexec を使用して製品インストールを実行することができます。

!重 要

次に記載する設定は、msiexec の表示オプションである、/qf（完全なユーザーインターフェースレベル）では使用できません。
また、使用する msiexec の適切なバージョンについては、公開されているドキュメントを参照してください。

■サポートされているパラメーター

ESET 製品インストールでサポートされているパラメーターは次のとおりです。

パラメーター	指定値	内容	コマンド例
APPDIR=<path>	有効なフォルダーパス	アプリケーション インストールフォルダー	例）ees_nt64_ENU.msi /qn APPDIR=C:¥ESET¥ ADDLOCAL= DocumentProtection
APPDATADIR=<path>	有効なフォルダーパス	アプリケーションデータ インストールフォルダー	
MODULEDIR=<path>	有効なフォルダーパス	モジュールインストール フォルダー	
ADDLOCAL=<list>	コンポーネント インストール	ローカルでインストール される必須以外の機能の リスト	例）ees_nt64_ENU.msi /qn ADDLOCAL=<list>

ワンポイント

ADDLOCAL プロパティの詳細については、Windows Installer Guide Properties Property Reference（https://msdn.microsoft.com/en-us/library/aa367536(v=vs.85).aspx）を参照してください。

ADDLOCAL で指定する<list>は、インストールするすべての機能名をカンマ区切りで記載します。
インストールする機能を選択するときには、パス全体（すべての親機能）が明示的にリストに含まれる必要があります。
正しい使用方法については、「●追加ルール」を参照してください。

■ ESET Endpoint の機能ツリー

機能ツリー	機能名	機能の存在※1
コンピューター	コンピューター	必須
コンピューター / ウイルス・スパイウェア対策	ウイルス対策	必須
コンピューター / ウイルス・スパイウェア対策 > リアルタイムファイルシステム保護	RealtimeProtection	必須
コンピューター / ウイルス・スパイウェア対策 / コンピューターの検査	検査	必須
コンピューター / ウイルス・スパイウェア対策 > ドキュメントの保護	ドキュメント保護	任意
コンピューター / デバイス制御	DeviceControl	任意
ネットワーク	ネットワーク	プレースホルダー
ネットワーク / パーソナルファイアウォール	ファイアウォール	任意
Web とメール	WebAndEmail	プレースホルダー
Web とメールプロトコルフィルタリング	ProtocolFiltering	非表示
Web と電子メール /Web アクセス保護	WebAccessProtection	任意
Web と電子メール / 電子メールクライアント保護	EmailClientProtection	任意
Web と電子メール / 電子メールクライアント保護 / メールプラグイン	MailPlugins	非表示
Web と電子メール / 電子メールクライアント保護 / 迷惑メール対策保護	迷惑メール対策	任意
Web と電子メール /Web コントロール	WebControl	任意
配布用アップデート	UpdateMirror	任意
Microsoft NAP のサポート	MicrosoftNAP	任意

※ 1・必須　　：常にインストールされる機能です。
　・オプション　　：インストールを選択解除できる機能です。
　・非表示　　：他の機能が正常に動作するための必須の論理機能です。
　・プレースホルダー　：製品には影響がない機能です。ただし、サブ機能とともにリストに含まれます。

●追加ルール

- WebAndEmail 機能のいずれかをインストールするように設定する場合、非表示の ProtocolFiltering 機能もリストに記載する必要があります。
- EmailClientProtection サブ機能のいずれかをインストールするように設定する場合、非表示の MailPlugins 機能もリストに記載する必要があります。

例）ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
　　ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins

■ CFG_ プレースホルダーのリスト

コマンド	内容	設定値
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	PUA	0 - 無効、1 - 有効
CFG_LIVEGRID_ENABLED=1/0	LiveGrid	0 - 無効、1 - 有効
FIRSTSCAN_ENABLE=1/0	インストール後の新しい初回検査をスケジュールします。	0 - 無効、1 - 有効
CFG_EPFW_MODE=0/1/2/3		0 - 自動、1 - 対話、2 - ポリシー、3 - 学習
CFG_PROXY_ENABLED=0/1		0 - 無効、1 - 有効
CFG_PROXY_ADDRESS=<ip>	プロキシ IP アドレス	
CFG_PROXY_PORT=<port>	プロキシポート番号	
CFG_PROXY_USERNAME=<user>	認証用のユーザー名	
CFG_PROXY_PASSWORD=<pass>	認証のパスワード	

4.2.3.3 インストールの失敗時に表示されるメッセージの一覧

インストールの失敗時にタスクの結果やエージェントトレースログに以下のようなメッセージが表示されている場合、それらの情報をもとに適切な対処を行ってください。

- インストールパッケージが見つかりません。
- 必須の新しいバージョンの Windows インストーラーサービス
- 別のバージョンまたは競合する製品が既にインストールされています。
- 別のインストール既に実行中です。そのインストールを完了してから、このインストールを続行してください。
- インストールまたはアンインストールは正常に完了しましたが、コンピューターの再起動が必要です。
- タスク失敗 - エラーがあります。エージェントトレースログを確認して、インストーラーの戻りコードをチェックする必要があります。

4.3 モバイルデバイスの展開

Mobile Device Connector をインストールしたサーバーを用意すると、ERA サーバーでモバイルデバイスの管理を行えます。Mobile Device Connector は、ERA サーバーが動作しているサーバーにインストールできるほか、ERA サーバーが動作していないサーバーにインストールすることもできます。Mobile Device Connectorのインストール方法については、「3 インストール」をご参照ください。モバイルデバイスの展開は、次の手順で行います。

STEP1	モバイルデバイスを ERA のグループ構造に追加する
STEP2	ESET Endpoint Security for Android/ESET iOS Management Profile を展開する。Apple Device Enrollment Program（DEP）で登録する

ワンポイント

モバイルデバイスの展開を開始する前に、製品アクティベーションクライアントタスクを使用して、Mobile Device Connector のアクティベーションを行っておいてください。Mobile Device Connector のアクティベーションの手順は、クライアントコンピューターで ESET セキュリティ製品をアクティベーションする場合と同じです。アクティベーションの詳細については、「6.6.2 新しいクライアントタスクの作成」または「6.5.3.1 ESET セキュリティ製品 ■製品のアクティベーション」をご参照ください。なお、Mobile Device Connector は、ライセンス単位を使用しません。

● iOS デバイスを登録する場合の注意点

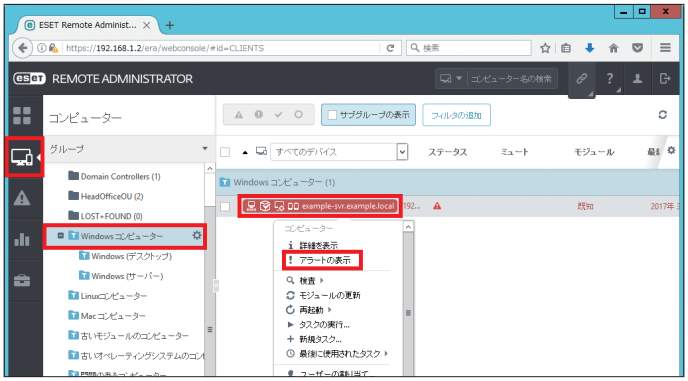
ESET モバイルデバイスコネクターで iOS デバイスを登録するには、HTTPS サーバーが完全なチェーン認証を送信する必要がありますが、Windows 環境では証明書チェーンを自動的に送信できません。Windows 環境をご利用のときは、次の手順で証明書チェーンでエラーが出ていないかを確認し、送信できていない場合は HTTPS 証明書チェーンのインストールを行ってください。なお、証明書が自己署名ルート CA を表す場合は、この設定を行う必要はありません。

●証明書チェーンのエラー確認手順

証明書チェーンでエラーが出ていないか確認するときは、以下の手順で行います。なお、オールインワンインストーラーを利用して Mobile Deviece Connector を一括インストールした後、Mobile Device Connetor のポリシーで、HTTPS 証明書を変更していない場合は、エラーは表示されません。

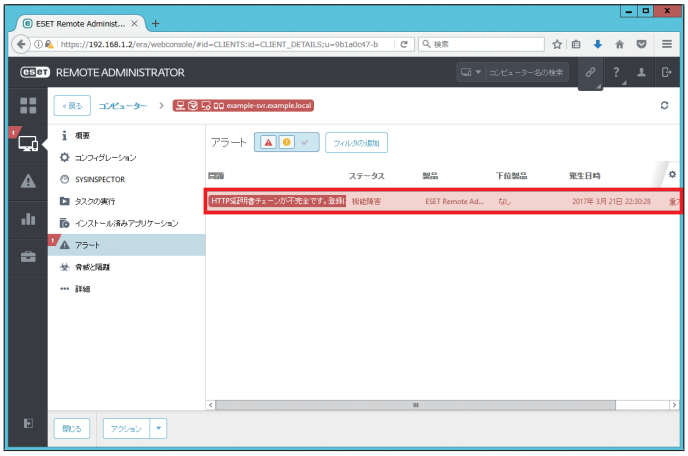
操作手順

1. Web コンソールの［コンピューター］をクリックし、［Windows コンピューター］をクリックします。ESET モバイルデバイスコネクターをインストールしている Windows サーバーをクリックし、［アラート表示］をクリックします。



続く

2 証明書チェーンが送信できていない場合は、赤いエラーが表示されます。

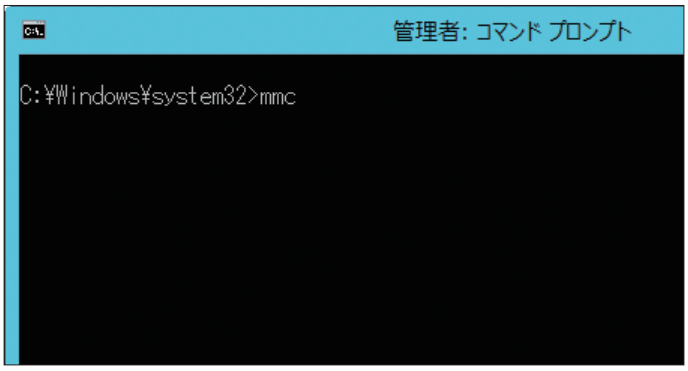


● Mobile Device Connector の HTTPS 証明書チェーンのインストール手順

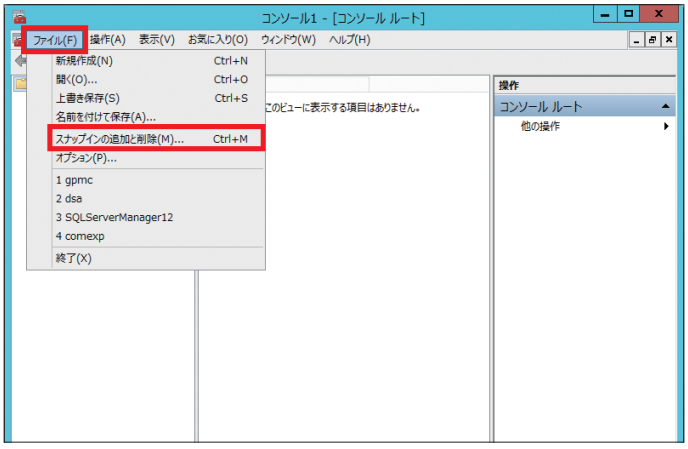
Mobile Device Connector の HTTPS 証明書チェーンのインストールは、モバイルデバイスコネクターをインストールしている Windows サーバー上で以下の手順を実行します。

操作手順

1 ［mmc.exe］を実行し、管理コンソールを開きます。

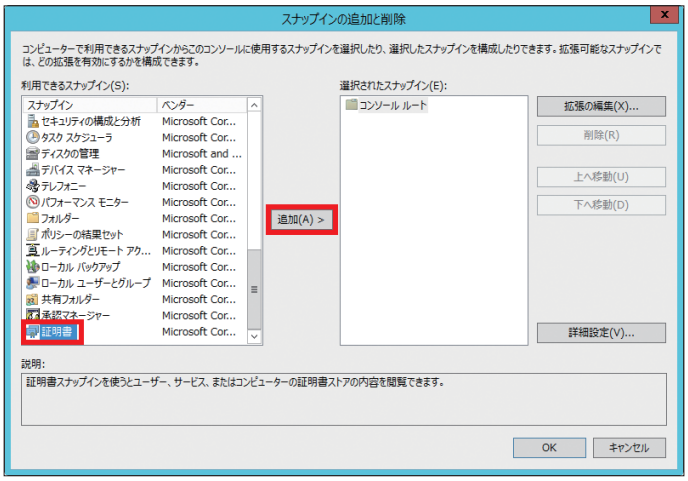


2 ［ファイル］をクリックし、［スナップインの追加と削除］をクリックします。

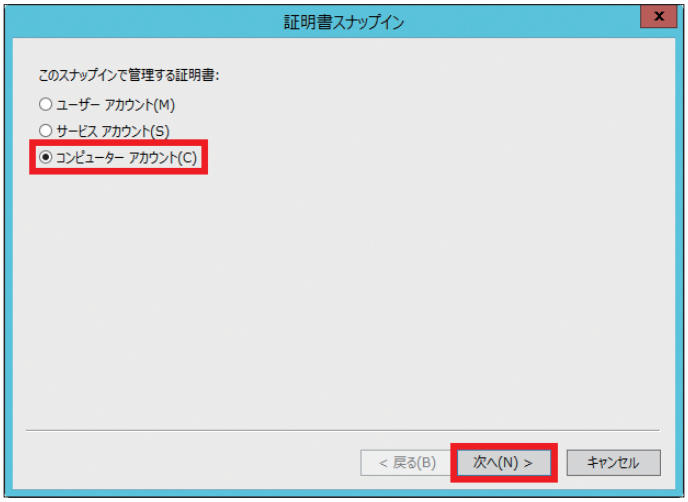


続く

3 「スナップインの追加と削除」画面が表示されます。「利用できるスナップイン」で、[証明書] を選択し、[追加] をクリックします。

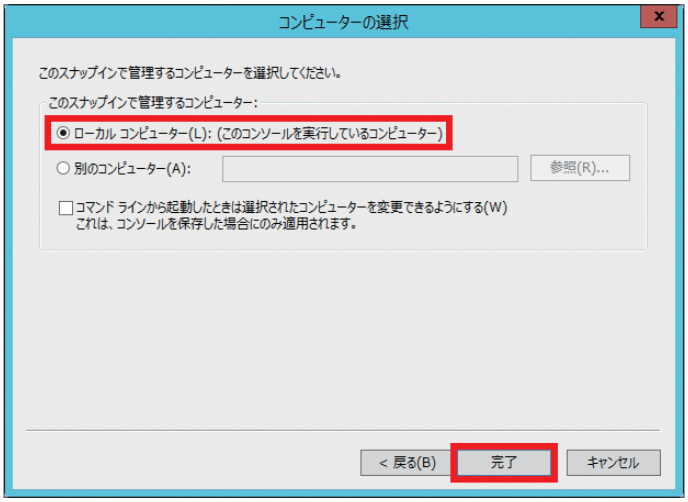


4 「証明書スナップイン」画面が表示されます。[コンピューターアカウント] を選択し、[次へ] をクリックします。

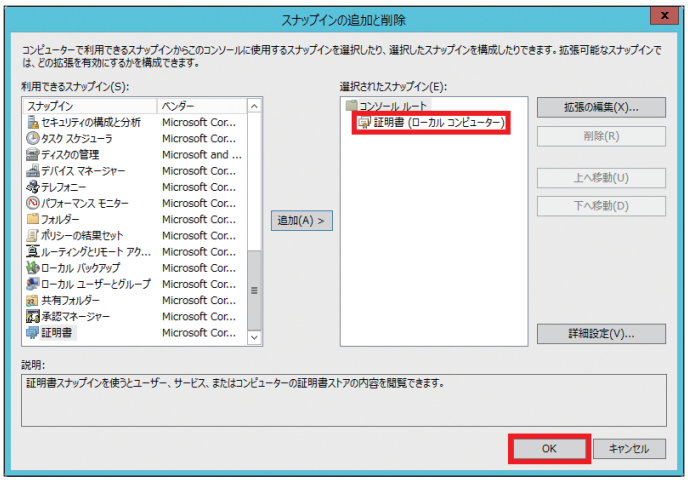


続く

5 「コンピューターの選択」画面が表示されます。このスナップインで管理するコンピューターで［ローカルコンピューター（このコンソールを実行しているコンピューター）］を選択し、［完了］をクリックします。

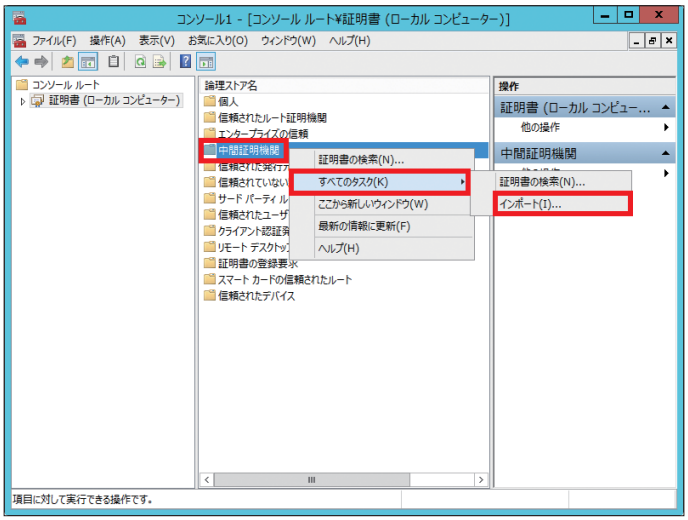


6 「選択されたスナップイン」のコンソールルートに「証明書」が追加されます。［OK］をクリックして、管理コンソールに戻ります。



続く

7 中間認証局を選択し、コンテキストメニューで［すべてのタスク］をクリックし、［インポート］をクリックして、画面の指示に従って HTTPS 証明書チェーンをインポートします。



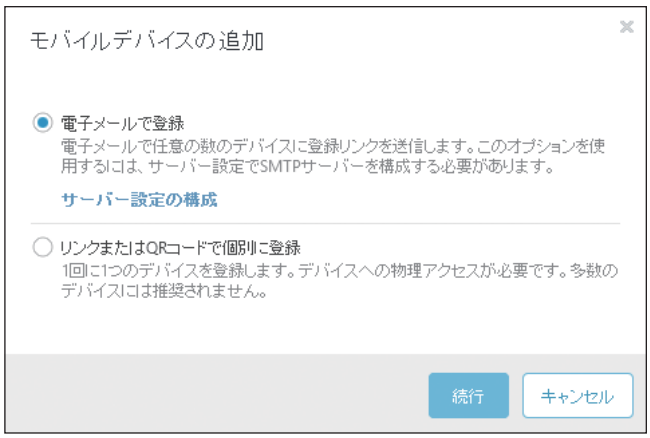
8 ESET Remote Administrator、Mobile Device Connector サービスを再起動します。

! 重 要

Windows 版、Linux 版どちらの場合も証明書の CommonName または SubjectAltName は、MDM ホスト名と一致する必要があります。ERA Web コンソールで証明書を作成する場合は、「ホスト名」と「共通名」に Mobile Device Connector インストール時に設定した「MDM ホスト名」と同じ IP アドレス（名前解決ができる環境でホスト名を設定していた場合はホスト名）を設定してください。詳しくは Windows の場合は「6.9.1.2 新しい証明書の作成」、Linux の場合は「3.4.9 Mobile Device Connector のインストール」を参照してください。

4.3.1 ERA のグループ構造へのモバイルデバイスの追加

ERA のグループ構造へのモバイルデバイスの追加は、ERA Web コンソールの［コンピューター］セクションまたは［管理］セクションの［グループ］から行えます。これらの画面で、モバイルデバイスを追加する静的グループを選択し、［新規追加］→［モバイルデバイス］とクリックすると、「モバイルデバイスの追加」画面が表示され、モバイルデバイスの登録方法を以下の 2 種類から選択できます。また、iOS デバイスを追加する場合は、上記の方法に加えて、「Apple Device Enrollment Program（DEP）」を利用してモバイルデバイスの追加を行うこともできます。「Apple Device Enrollment Program（DEP）」については、「4.3.3 ESET iOS Managemet Profile の展開 - Apple Device Enrollment Program（DEP）を使用した登録」をご参照ください。



- 電子メールで登録 - 電子メールでのモバイルデバイスの一括登録を行います。この方法では、モバイルデバイスのユーザー／所有者の操作が必要になります。多数のモバイルデバイスを登録する必要がある場合、または物理的にアクセスできない既存のモバイルデバイスがある場合に、このオプションが最適です。この方法では、モバイルデバイス登録用の情報が記載された電子メールがユーザーに送付されます。メールを受け取ったユーザーがメール記載の内容を元に操作を行ってモバイルデバイスの登録を行います。
- リンクまたは QR コードでの個別登録 - この方法では、1 台ごとにモバイルデバイスの登録を行います。複数のモバイルデバイスを登録したいときは、モバイルデバイスごとに同じ手順を繰り返す必要があります。少ない数のモバイルデバイスを登録するときに、この方法で登録されることをお勧めします。また、この方法は、ユーザー／モバイルデバイスの所有者に何もさせずに、管理者が登録作業すべてを行いたいときに最適です。また、すべての設定を行った後にユーザーにモバイルデバイスを配布したいときにもこの方法で登録できます。

! 重　要

電子メールでの一括登録用に SMTP サーバーの設定を行っておくことをお勧めします。SMTP サーバーの設定については、「6.11 サーバーの設定 - ■詳細設定」をご参照ください。

4.3.2 ESET Endpoint Security for Android の展開

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

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

●イントールの方法

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

- 電子メールを利用したインストール
- ローカルインストール

●電子メールを利用したインストール

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

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

2. 管理者より設定ファイルとインストール APK ファイルを配布
   管理者は、設定ファイル、インストール APK ファイル、インストール手順の簡単な説明を電子メールでエンドユーザーに送信します。インストール APK ファイルは、ユーザーが Google Play Store からダウンロードすることもできます。

各種ダウンロードリンクは、管理者が提供します。インストール後、ユーザーがアプリケーション設定ファイルを開きます。設定がインポートされ、設定ファイルにライセンス情報が含まれている場合は、アプリケーションがアクティベートされます。
※設定ファイルには、ESET Remote Administrator への接続情報は含まれません。

●ローカルインストール

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

ユーザーズサイトからダウンロード

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

Google Play Store からダウンロード

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

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

4.3.3 ESET iOS Management Profile の展開

ESET iOS Management Profile の展開は、モバイルデバイスを ERA のグループ構造へ追加したときに表示される登録リンクや QR コードを利用する方法と、Apple Device Enrollment Program（DEP）を利用する方法があります。登録リンクや QR コードを利用するときは、管理者がこれらの情報とインストール手順の簡単な説明を電子メールでエンドユーザーに送信します。エンドユーザーが、受け取った電子メールに記載されている登録リンクをタップすると、ESET iOS Management Profile のインストールを行えます。詳細なインストール手順については、「5.3.6 モバイルデバイスの手動追加」の「● iOS デバイスに ESET iOS Management Profile を展開する」をご参照ください。

● Apple Device Enrollment Program（DEP）を使用した登録

Apple Device Enrollment Program（DEP）は、Apple が提供している新しい企業向けの iOS デバイス登録方法です。DEP では、iOS デバイスに直接接続することなく、最低限のユーザー操作で iOS デバイスを ERA のグループ構造に登録でき、管理者は iOS デバイスのセットアップ処理をカスタマイズできます。たとえば、ユーザーが iOS デバイスから MDM プロファイルを削除できないようにすることができます。
DEP を使用して登録を行うには、Apple DEP アカウントを取得して、モバイルデバイスコネクターをインストールしている ERA MDM サーバーを Apple 社が提供している DEP サーバーと接続（リンク）する必要があります。また、DEP 要件を満たした既存の iOS デバイスと、将来購入するすべての iOS デバイスを登録できます。

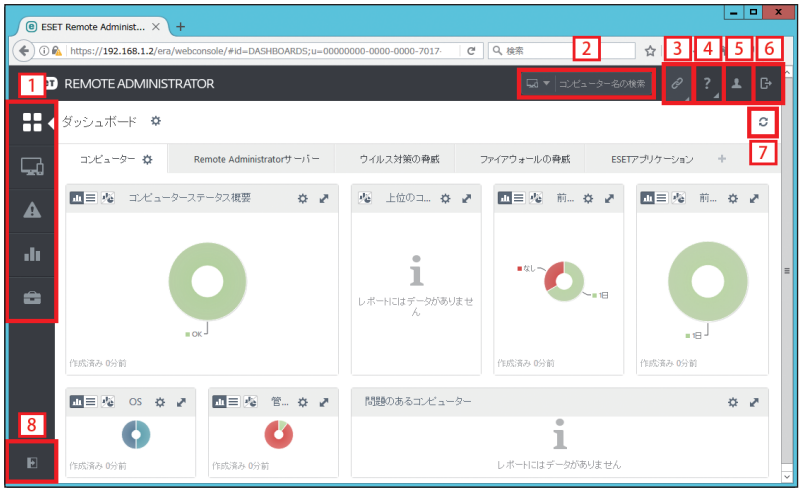
Chapter 5 ERA Web コンソールの使用方法

この章では、ERA Web コンソールの画面構成と、「ダッシュボード」メニューから「レポート」メニューまでについて説明します。「管理」メニューについては「Chapter6　管理」を参照してください。
ERA Web コンソールは ERA サーバーと通信をするメインインターフェイスです。すべての ESET 製品を管理するコントロールパネルと考えることができます。Web ベースのインターフェースであり、ネットワークに接続している任意のデバイス（「2.5　ERA Web コンソール対応　Web ブラウザー」参照）を使用してアクセスすることができます。

5.1　ERA Web コンソールの画面構成

5.1.1　ERA Web コンソールの基本画面構成

ERA Web コンソールの基本の画面構成について記載します。



1	メニュー	カーソルを合わせるとメニューが表示されます。 ［管理］メニューを選択すると、さらにサブメニューが表示されます。
2	検索	コンピューター名もしくは IPv4/IPv6 アドレス、説明フィールドの内容を入力してコンピューターを検索できます。
3	クイックリンク	「クイックリンク」に表示されているメニューをクリックすると、該当の設定画面に遷移します。
4	ヘルプ	オンラインヘルプが表示されます。オンラインヘルプの内容は、日本でのサポート条件が異なる場合がありますのでご注意ください。
5	ログインユーザー	ログインしているユーザー名が表示されます。クリックすると、ユーザーが ERA Web コンソールで使用するタイムゾーンを変更できます。
6	ログアウト	セッションのタイムアウト時間が表示されます。タイムアウト時間は、設定変更することができます。 また、カーソルを合わせると、「ログアウト」表示に変更されログアウトできます。
7	ページの更新	クリックすると現在のページが更新されます。

8	**メニューの展開**	メニューを展開します。クリックすると、「メニュー」を展開して表示します。

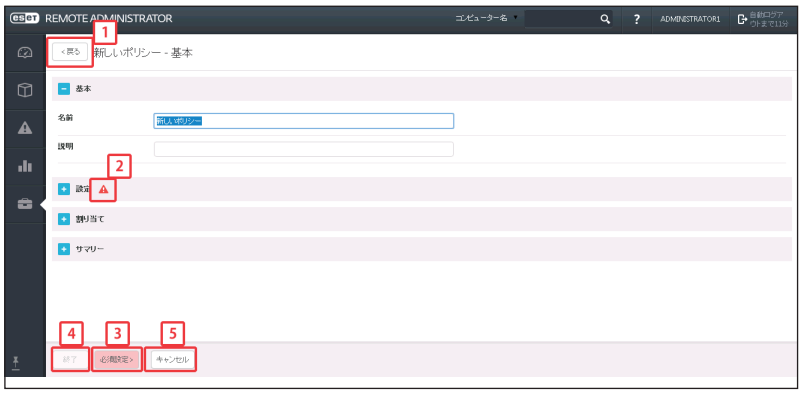
5.1.2 各メニュー画面

各行をクリックすると、その行のメニューが表示されます。表示されるデータは、フィルタリングや並べ替えをすることができます。

1	**全選択**	表示されている、すべてのデータを選択できます。	
2	**ソート**	データの並べ替えた項目に、表示されます。	
3	**項目名**	項目名をクリックして、並べ替えることができます。	
4	**コンテキストメニュー**	更新	表示データが更新されます。
		列を編集	「テーブルに表示されるテーブル列を確認してください」画面が表示され、表示される項目を追加、削除することができます。
		列の自動調整	項目の幅が、自動調整されます。
		選択をクリア	選択しているデータの、選択を解除します。
		テーブルソート	コンピューター名で、並べ替えることができます。
		マルチソート	「マルチカラムでソート」画面が表示され、複数の項目を使用して、並べ替えることができます。
5	**メニュー**	クリックしたデータに対するメニューが表示されます。クリックしたデータに合わせて、メニューが変わります。	

5.1.3 オブジェクトのウィザード

ESET Remote Administrator の各オブジェクトは、ウィザードを使用して編集ができます。必要な項目がすべて入力されるまで、［終了］ボタンは使用できません。



1	**戻る**	1 つ前の画面に戻ります。
2	**必須項目**	必須項目に表示されます。
3	**必須設定**	入力が完了していない必須項目に移動します。
4	**終了**	必要な項目が全て入力されると［終了］ボタンがクリックでき、入力内容を保存できます。
5	**キャンセル**	入力データを破棄して 1 つ前の画面に戻ります。

5.2 ダッシュボード

ダッシュボードは、クライアントから収集した情報や、ERA サーバーのパフォーマンス情報などを表示することができる機能です。ダッシュボードは様々なレポートで構成されていて、レポートの追加、既存のダッシュボードの変更、サイズ変更、移動をしてカスタマイズすることができます。

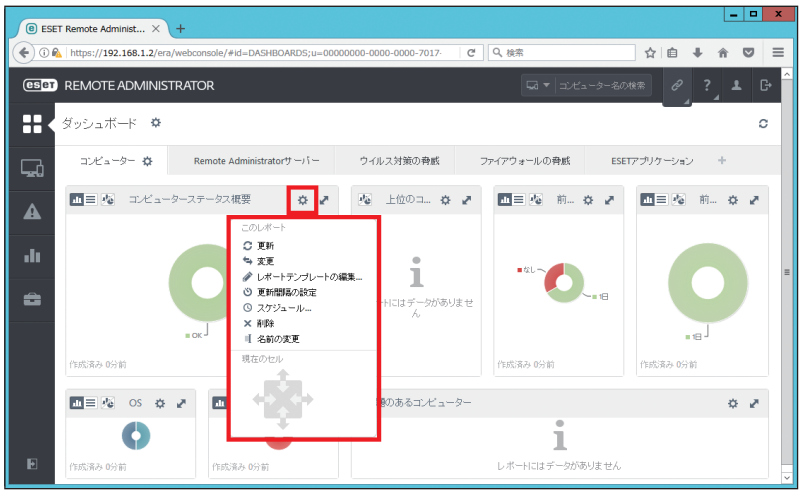
5.2.1 ダッシュボード画面の構成

表示するレポートは、ユーザーごとに、種類や位置、大きさ等を自由にカスタマイズすることができます。

1	コンピューター	オペレーティングシステムの概要、管理対象外のコンピューターの割合、問題のあるコンピューターなどクライアントマシンの状態が確認できます。
2	Remote Administrator サーバー	サーバーネットワークの負荷、サーバー CPU の負荷、ネットワークの問題など ERA サーバー自体に関する情報を確認できます。
3	ウイルス対策の脅威	ウイルス対策の脅威やウイルス対策の脅威があるユーザーなどウイルス対策モジュールからのレポートを確認できます。
4	ファイアウォールの脅威	検出されたファイアウォールイベントやファイアウォールイベントが発生したコンピューターなど特定の日数内に発生したイベントを確認できます。
5	ESET アプリケーション	古いバージョンの ERA コンポーネント、最新のアプリケーションと古いアプリケーションの比率を示すステータスを確認できます。
6	ダッシュボードを追加	レポートフィールドが空の新しいダッシュボードタブを追加することができます。
7	表示切り替え	テーブル表示とグラフ表示を切り替えることができます。
8	グラフタイプを変更	グラフの種類を変更することができます。
9	全画面の切り替え	該当の情報を全画面表示へ切り替えます。

5.2.2 表示内容の変更

ダッシュボードに表示させるレポートを変更したり、新しく項目を追加したりすることができます。
設定されているレポートの ボタンをクリックするとメニューが表示されます。



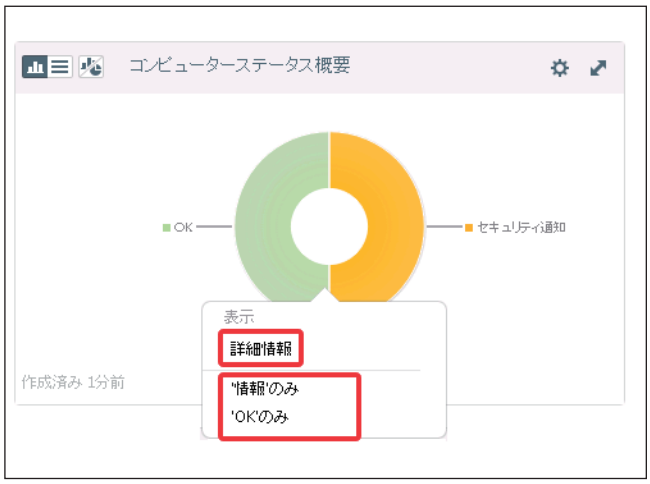
	更新	表示されているレポートを更新します。
	変更	表示させるレポートの種類を変更します。
	レポートテンプレートの編集	表示させるレポートの詳細を変更します。詳細は「5.5.2 レポートテンプレートの編集」を参照してください。
	更新間隔の設定	レポートの更新間隔を 30 秒～ 20 日で設定できます。なお、デフォルトの更新間隔は 2 分です。
	スケジュール	レポート生成のスケジュールを設定します。
	削除	表示されているレポートを削除します。
	名前の変更	表示されているレポートの名前を変更します。
	現在のセル	上下左右の矢印をクリックしてセルの大きさを変更します。

ワンポイント

レポート名称をクリックしてドラッグすると、ダッシュボードの表示場所を変更することができます。

5.2.3 詳細情報の表示

表示されているグラフをクリックし、[詳細情報] から、詳細情報や該当の値のみをデータとして表示させることができます。表示される内容は、データによって異なります。



詳細情報	コンピューター名と説明、静的グループ名など、クリックしたデータの元データが表示されます。
情報のみ **OK のみ**	選択しているデータに合わせて、表示されるメニューが変わります。 表示されている値に対する詳細情報、情報、緊急、セキュリティリスク、セキュリティ通知、コンピューターの一覧が表示されます。 コンピューターの一覧は、100 レコードまで表示されます。

! 重 要

レポートの詳細表示は最初の 1000 レコードまで表示されます。

5.2.4 ダッシュボードの追加

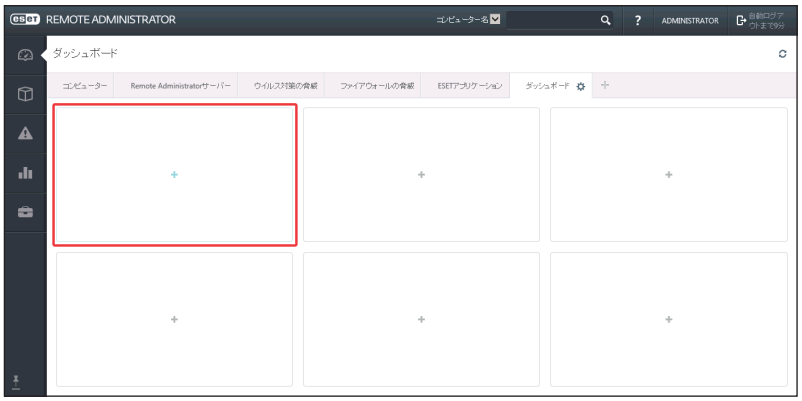
ダッシュボードに新たなレポートを追加する方法について説明します。新しいレポートテンプレートの作成方法については「5.5.1 レポートテンプレートの作成と編集」を参照してください。

操作手順

1. [（ダッシュボードを追加）] をクリックします。

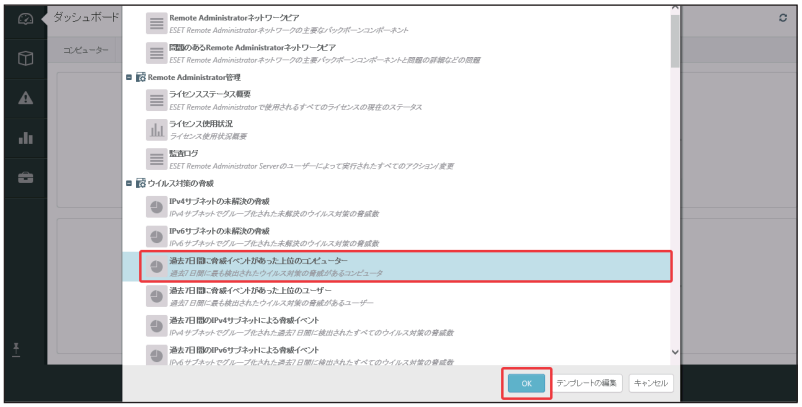
2. 新しいダッシュボードの名前を入力して、[OK] ボタンをクリックします。

3. ダッシュボードに表示されている、空の四角をクリックします。



続く

4 表示させたいテンプレートを選択して、［OK］ボタンをクリックします。

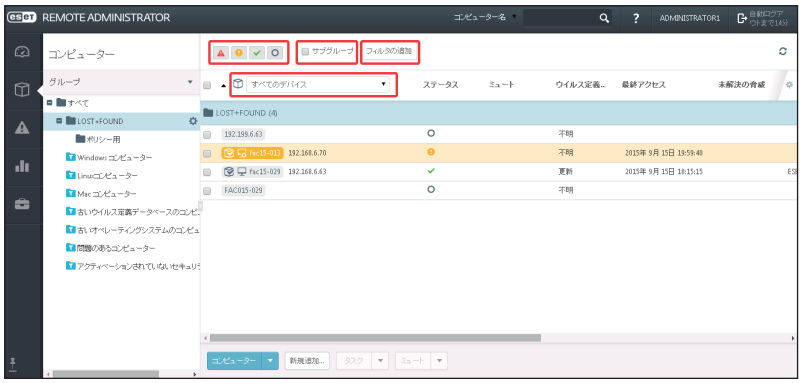


5.3 コンピューター

ESET Remote Administrator に追加したすべてのコンピューターがグループに分かれて表示されます。グループを選択すると、該当するグループに属するコンピューターが表示されます。
コンピューターは 1 つの静的グループに属します。グループは、ERA Web コンソール画面でのフィルタリングだけでなく、グループごとにポリシーを割り当てたり、タスクを設定することができます。

5.3.1 コンピューターのフィルタリング

「コンピューター」画面の上部にあるフィルターを使用してコンピューターをフィルタリングすることができます。複数の条件を指定した場合の論理演算子は AND です。文字列は一部一致での検索です。



アイコン	アイコンを選択してフィルターをかけることができます。複数のアイコンを組み合わせることもできます。例えば、警告のあるクライアントコンピューターを表示させるには、黄色のアイコンのみをオンにします。エラー、警告両方を確認するには、 2 つのアイコンをオンにします。 ：エラーのあるコンピューターが表示されます。 ：警告のあるコンピューターが表示されます。 ：問題のないコンピューターが表示されます。 ：管理対象外のコンピューターが表示されます。
サブグループ	現在選択されているグループのサブグループを含むクライアントが表示されます。
フィルタの追加	フィルターの条件をリストから選択し、追加することができます。 追加できる条件：名前、説明、IPv4 アドレス、IPv6 アドレス、ミュート、ウイルス定義データベース、接続時間、未解決の脅威、適用されたポリシー数、OS タイプ、OS 名、OS バージョン、OS サービスパック、OS プラットフォーム
すべてのデバイス	リストからデバイスの種類を選択できます。

! 重　要

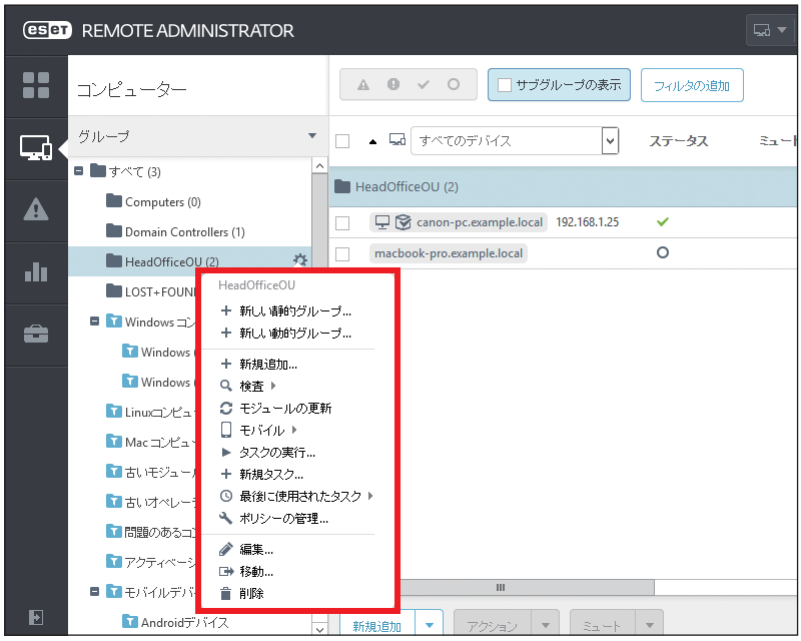
リスト内で該当のコンピューターを検索することができなかった場合は、すべてのフィルターをオフにして確認してください。

5.3.2 表示グループの編集

静的グループ／動的グループの作成、編集、新規追加が行えます。編集を行いたいグループの ボタンをクリックするとメニューが表示されます。

ワンポイント

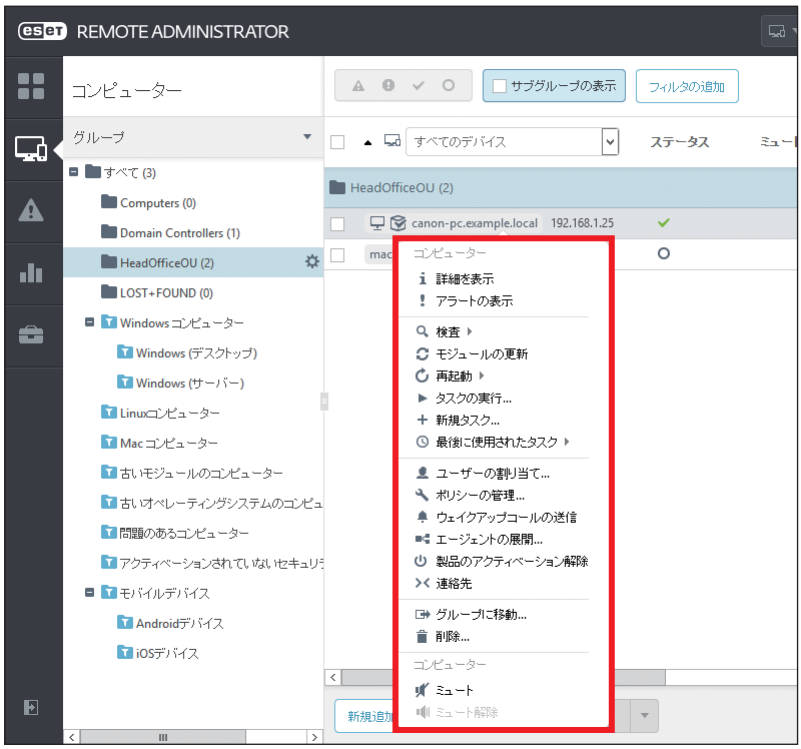
静的グループは、手動でクライアントコンピューターを指定したグループです。動的グループは、条件を指定したグループのため、グループ内のクライアントコンピューターは変動します。グループの詳細は、「6.3 グループ」を参照してください。



+	**新しい静的グループ**	新しい静的グループを作成します。
+	**新しい動的グループ**	新しい動的グループを作成します。
+	**新規追加**	クライアントコンピューターを手動で追加します。
🔍	**検査**	クライアントコンピューターのオンデマンド検査が実行されます。検査方法は「駆除して検査する」または「駆除せず検査する」から選択できます。
↻	**モジュールの更新**	モジュールアップデートタスク（アップデートを手動でトリガー）を実行します。
📱	**モバイル**	モバイルデバイスへのタスクを実行します。
▶	**タスクの実行**	作成済みのタスクを選択して実行します。
+	**新規タスク**	新規でタスクを作成して、実行します。
🕒	**最後に使用されたタスク**	最後に使用したタスクを選択して、実行します。
🔧	**ポリシーの管理**	選択したクライアントにポリシーを割り当てます。ポリシーはグループだけでなく、クライアント（複数のクライアント）に割り当てることができます。
✎	**編集**	作成されたグループの内容を編集します。
→	**移動**	別の親グループに移動します。
🗑	**削除**	リストからグループを削除します。ただし、ネットワーク内にクライアントコンピューターがある場合は、「LOST+FOUND」グループに表示されます。

5.3.3 クライアントコンピューターの操作

一覧に表示されているクライアントコンピューターをクリックすると、クライアントコンピューターの操作メニューが表示されます。

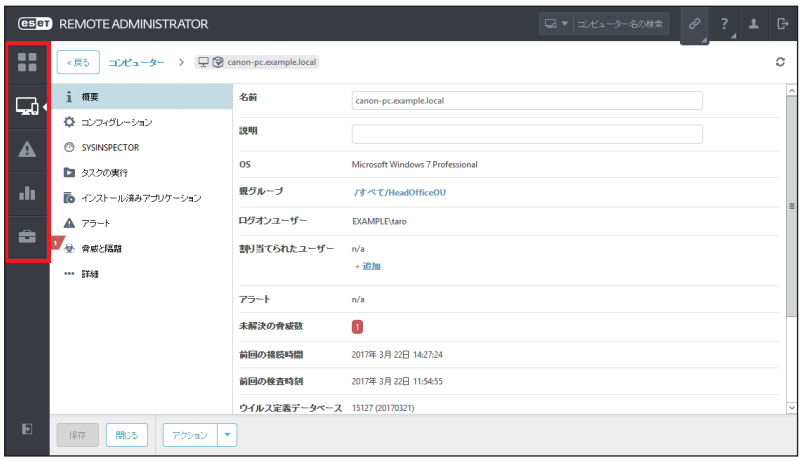


	詳細を表示	クライアントコンピューターの詳細情報を確認、変更できます。
	アラートの表示	選択したクライアントコンピューターの警告を表示します。
	検査	クライアントコンピューターのオンデマンド検査が実行されます。検査方法は「駆除して検査する」または「駆除せず検査する」から選択できます。
	モジュールの更新	モジュールアップデートタスク（アップデートを手動でトリガー）を実行します。
	再起動	選択したクライアントコンピューターの再起動またはシャットダウンが行えます。
	タスクの実行	作成済みのタスクを選択して実行します。
	新規タスク	新規でタスクを作成して、実行します。
	■最後に使用されたタスク	最後に使用したタスクを選択して、実行します。
	■ユーザーの割り当て	選択したコンピューターにユーザーを割り当てます。
	ポリシーの管理	選択したクライアントにポリシーを割り当てます。ポリシーはグループだけでなく、クライアント（複数のクライアント）に割り当てることができます。
	ウェイクアップコールの送信	クライアントと ERA エージェントとの即時通信を開始します。これは、ERA エージェントが ERA サーバーに接続するときに、定期間隔を開けずに通信を行います。例えば、クライアントですぐにタスクを実行する場合や、ポリシーをすぐに適用する場合に使用できます。変更する場合は、ウェイクアップコールを使用するまでに約 1 分間待機します。

	エージェントの展開	「ERA エージェント」の展開を行います。
	製品のアクティベーション解除	選択したクライアントコンピューターのアクティベーションを解除します。
	連絡先	リモートデスクトッププロトコル経由で対象デバイスに接続できる .rdp ファイルを生成してダウンロードします。
	グループに移動	選択したコンピューターを別のグループに移動します。
	削除	選択したクライアントコンピューターを完全に削除します。
	ミュート	選択したクライアントコンピューターからの ERA への通知を停止します。

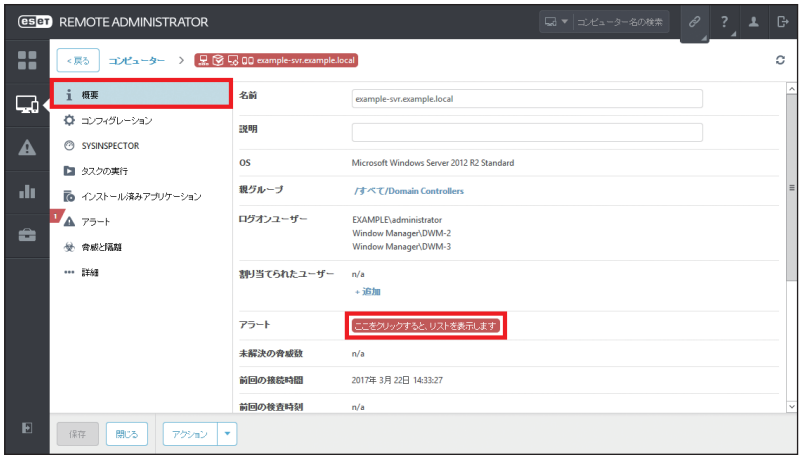
5.3.4 クライアントコンピューターの詳細確認画面

選択したクライアントコンピューターの「詳細」メニューでは、そのコンピューターの情報を確認することができます。
選択したクライアントコンピューターの状態を、カテゴリ別に表示します。



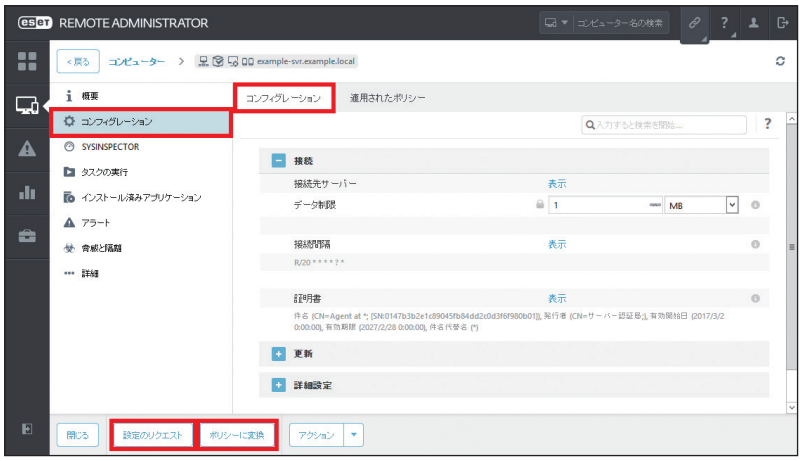
■概要

クライアントコンピューターの名前やシステム情報、親グループが表示されます。
「名前」、「説明」、「親グループ」の項目については、この画面での変更が可能です。
「アラート」をクリックすると、「アラート」画面にジャンプします。



■コンフィグレーション

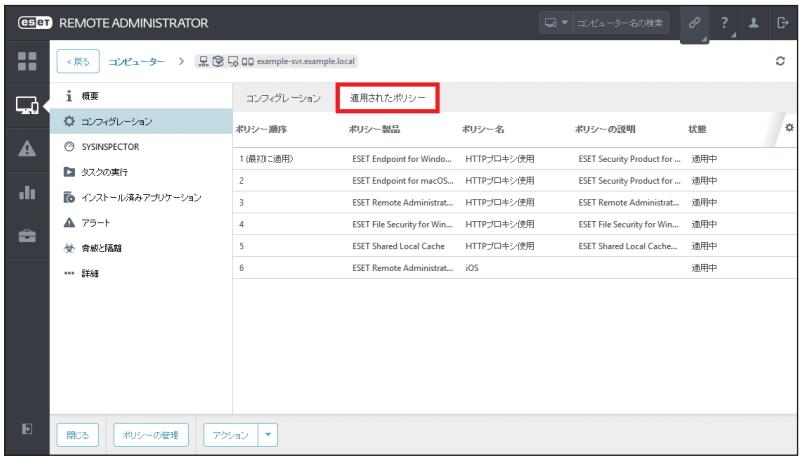
「コンフィグレーション」タブでは、クライアントコンピューターの全体の構成と接続が表示されます。



!重　要

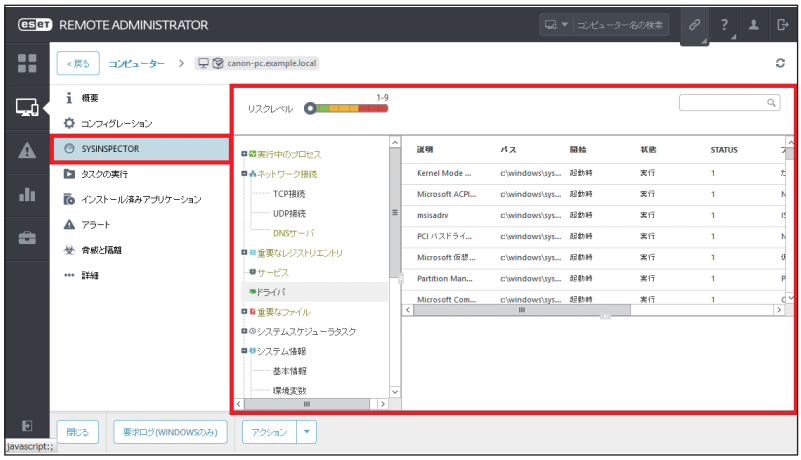
最新の設定情報を取得するためには、クライアントコンピューターに「ESET 製品の設定エクスポート」のクライアントタスクを実行する必要があります。「設定のリクエスト」をクリックすると、「ESET 製品の設定エクスポート」タスクを実行できます。
また、取得したコンフィグレーションからポリシーを作成する場合は、［ポリシーに変換］ボタンをクリックします。

「適用されたポリシー」タブでは、クライアントコンピューターに適用されたポリシーとその状態が表示されます。



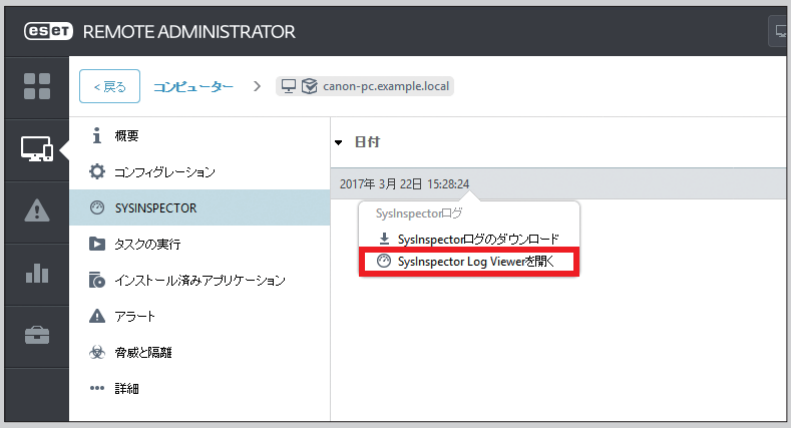
SYSINSPECTOR

SYSINSPECTOR によるクライアントコンピューターに関する詳細な情報（ログ）の取得とその表示を行えます。取得できる情報は、実行中のプロセスやネットワークの状態、重要なレジストリ、サービス、デバイスドライバー、システム情報など多岐に渡ります。



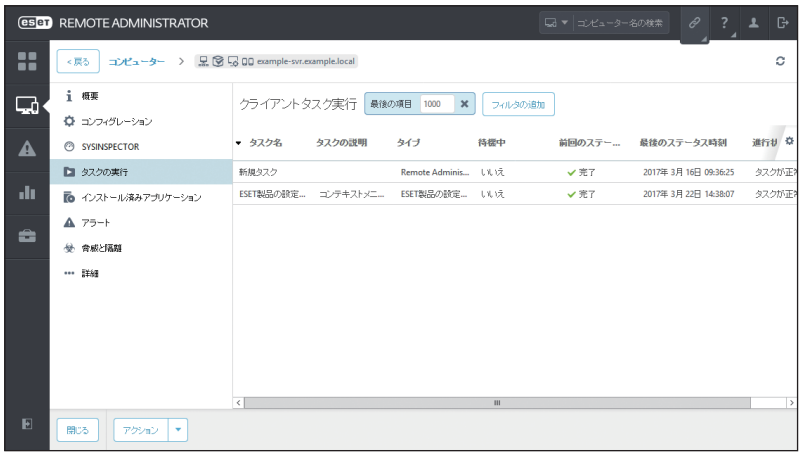
! 重　要

クライアントコンピューターに関する詳細な情報を表示するには、SYSINSPECTOR 機能を備えたクライアントセキュリティ製品（Windows 用の ESET Endpint Security や ESET Endpoint Antivirus など）がインストールされたクライアントコンピューターから SysInspector ログを取得する必要があります。SysInspector ログの取得は、[要求ログ（WINDOWS のみ）] をクリックすることで行えます。また、情報の表示を行うときは、取得されたログをクリックし、[SysInspector Log Viewer を開く] をクリックします。



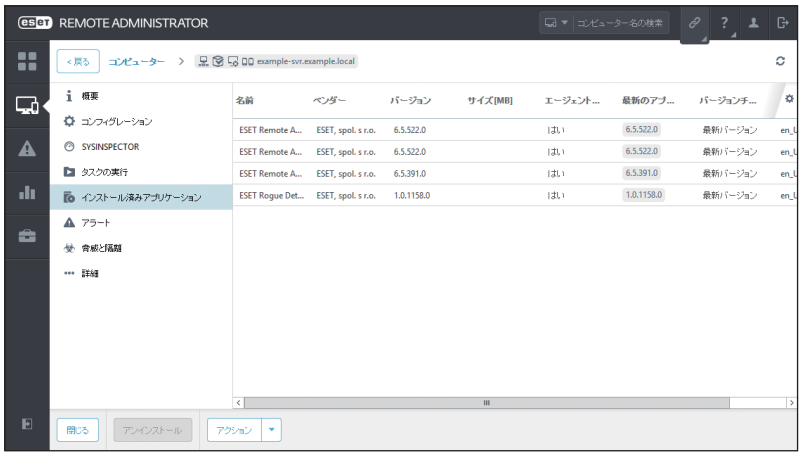
■タスクの実行

クライアントコンピューターに対して実行されるタスクとステータスが一覧で表示されます。



■インストール済みアプリケーション

クライアントコンピューターにインストールされているアプリケーションとバージョンなどが表示されます。



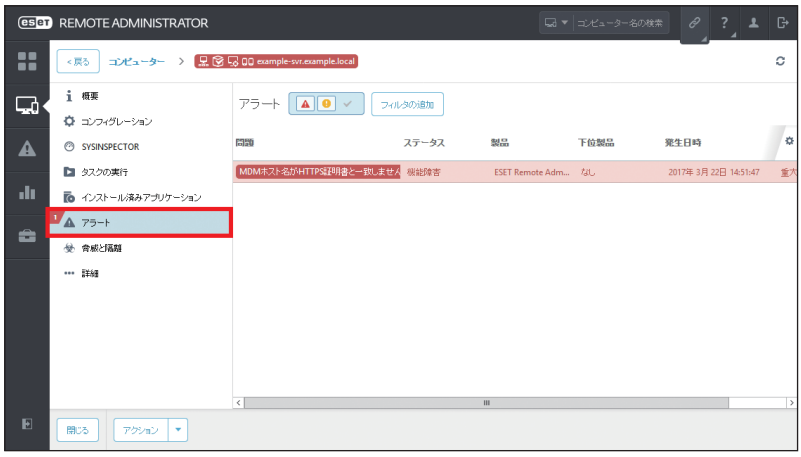
!重　要

初期設定では、クライアントコンピューターにインストールされている ESET 製品のみ表示されます。
クライアントコンピューターにインストールされているすべてのアプリケーションを表示するためには、ERA エージェントの設定を変更してください。

ERA エージェントの設定方法については、「7.1.1　ERA エージェントの設定項目」を参照してください。
設定箇所：「インストールされている ESET 製品以外のアプリケーションを報告」を有効

■アラート

クライアントコンピューターで発生している問題と発生日時、重要度などが表示されます。



!重　要

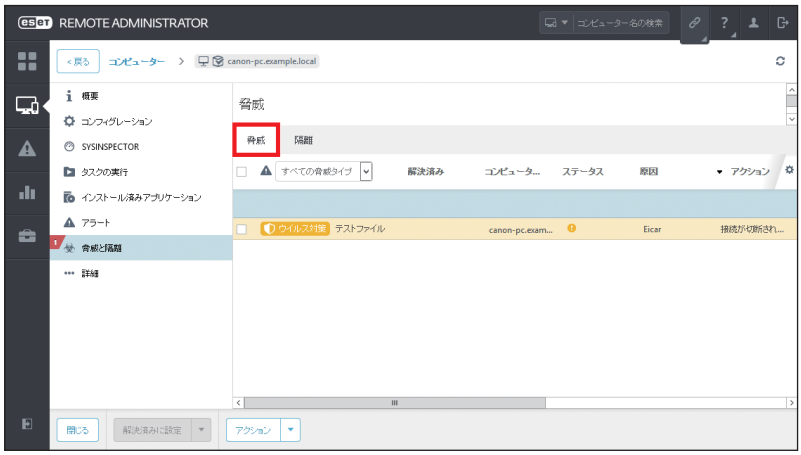
初期設定では、クライアントコンピューターに最新のパッチが適用されていない場合や、ファイアウォールとウイルス対策機能が有効ではない場合にアラートが表示されます。
それぞれのアラートを通知したくない場合は、ERA エージェントの設定を変更してください。

ERA エージェントの設定方法については、「7.1.1　ERA エージェントの設定項目」を参照してください。

設定箇所：「オペレーションシステムが最新ではない場合に報告」を無効
「ネットワーク ファイアウォールの問題を報告」を無効
「ウイルスおよびスパイウェア保護の問題を報告」を無効

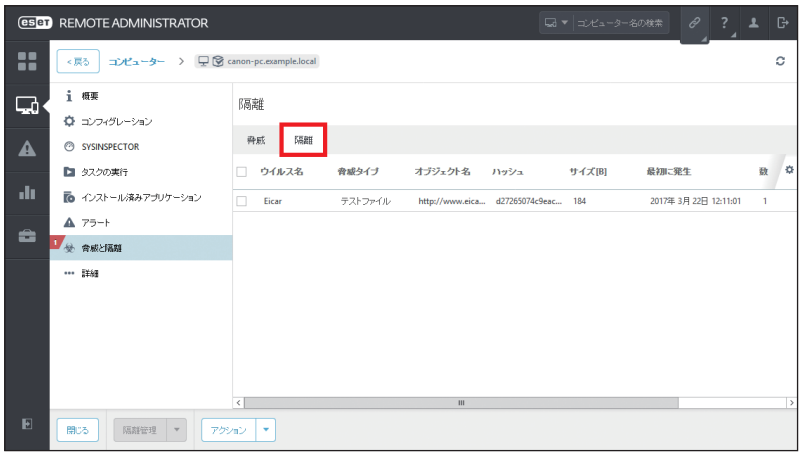
■脅威と隔離

「脅威」タブでは、クライアントコンピューターで発見された脅威、原因などが表示されます。



ワンポイント

検出された脅威をクリックし、［詳細を表示］をクリックすると発見された脅威に関する詳細な情報が表示されます。また、［解決済みに設定］をクリックすると、選択した脅威が「脅威」タブから非表示になります。



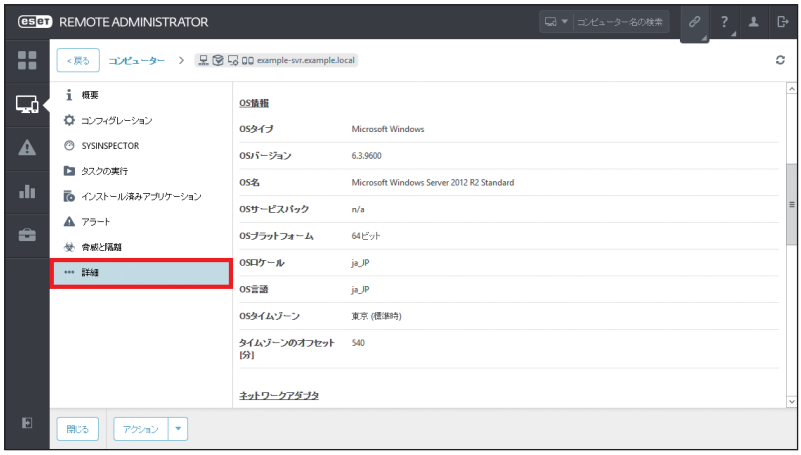
「隔離」タブでは、クライアントコンピューターで隔離されているウイルスの情報が表示されます。隔離されているウイルスに対して、削除や復元やアップロードを行うタスクを配信することが可能です。

ワンポイント

検出されたウイルスをクリックし、「削除」「復元と除外」「復元」「アップロード」などの操作を行えます。「復元と除外」および「復元」は、ヒューリスティック検索機能で検出した未知のウイルスにのみ実行可能です。また、［アップロード］をクリックすると、検出したウィルスを共有ディレクトリにアップロードできます。この機能は、隔離されたファイルをさらに調査する場合など、上級者ユーザーにのみ推奨されます。

■詳細

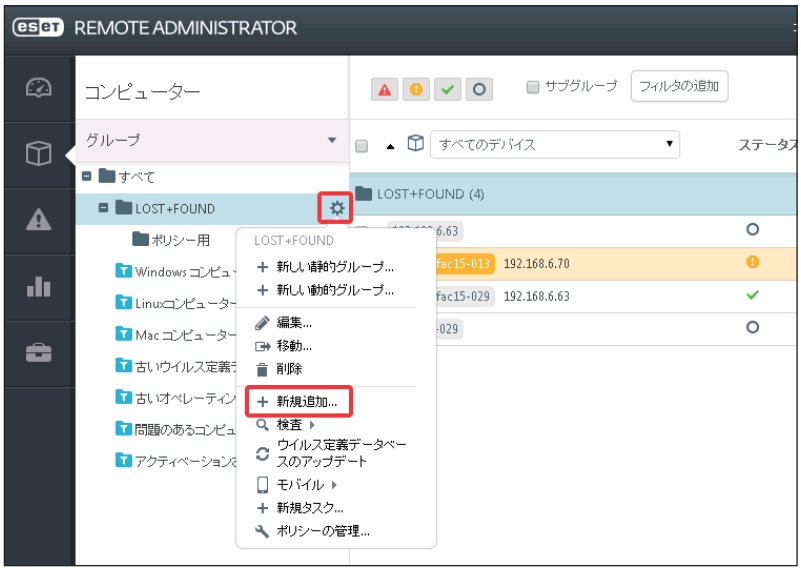
クライアントコンピューターを製造したメーカーやモデル名、利用中の OS、ネットワークアダプタやデバイス ID をなどの情報を表示できます。



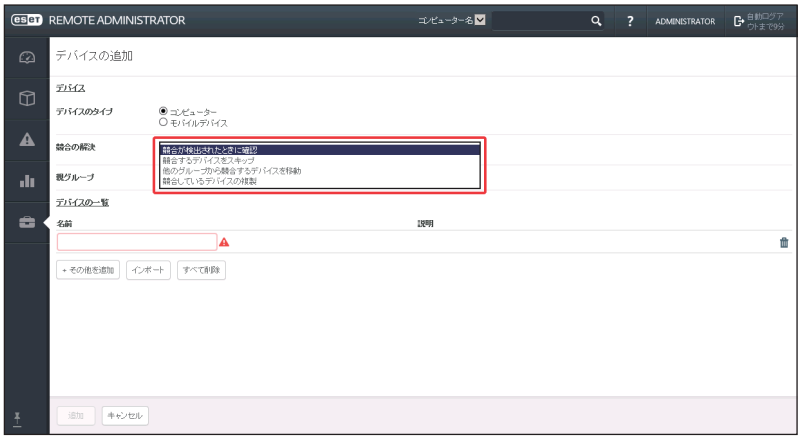
5.3.5 コンピューターの手動追加

コンピューターを手動で追加する方法を説明します。

1 追加するグループのコンテキストメニューから［新規追加］を選択します。



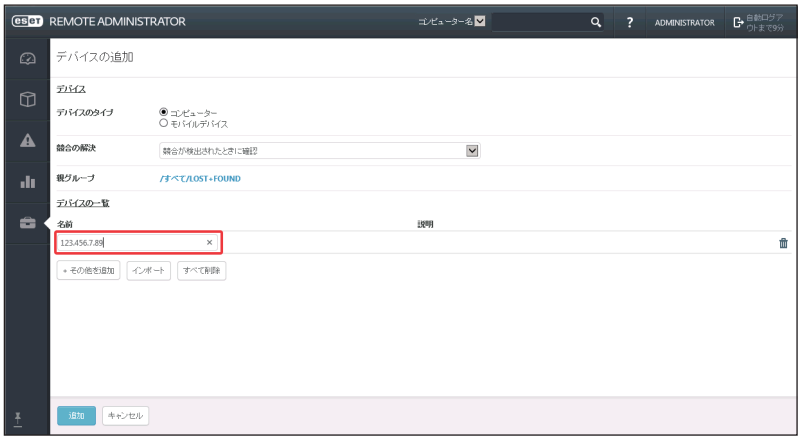
2 「競合の解決」を選択します。



競合が検出されたときに確認	競合が検出された場合に、アクションを選択する画面が表示されます。
競合するデバイスをスキップ	重複するコンピューターは追加されません。
他のグループから競合するデバイスを移動	競合しているコンピューターを元のグループから削除して、新しいグループに移動します。
競合しているデバイスの複製	新しいコンピューターとして追加されます。異なる名前が自動で振られます。

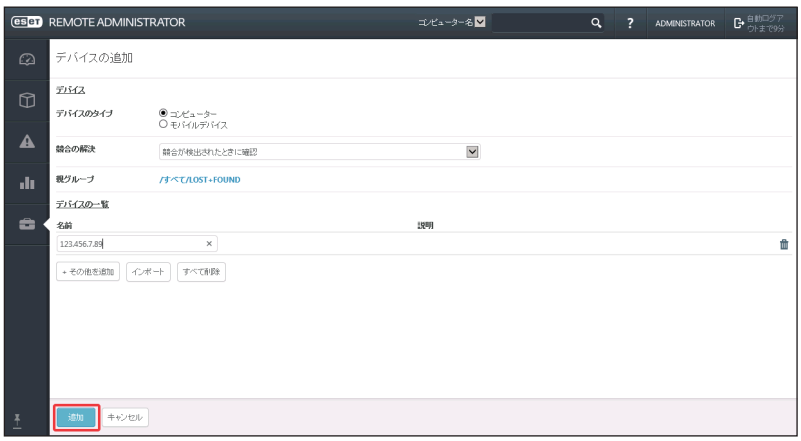
続く

3 「名前」に追加するコンピューターの名前もしくは IP を入力します。

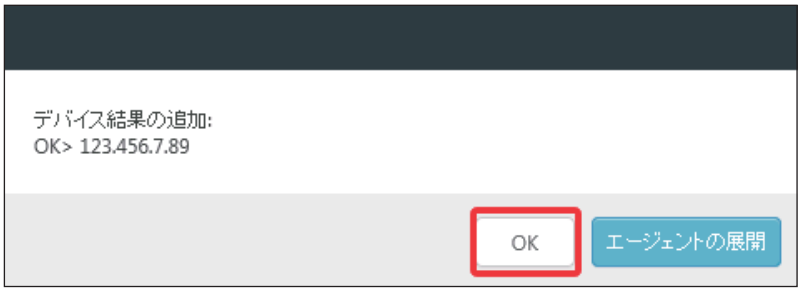


4 [追加] ボタンをクリックします。

一覧に追加したクライアントコンピューターが表示されます。



5 [OK] ボタンをクリックします。



ワンポイント

エージェントの展開については「4.2.2 ERA エージェントの展開」を参照してください。

! 重 要

複数のコンピューターを追加すると時間がかかる場合があります。DNS の逆引き検索を実行する場合があります。

5.3.6 モバイルデバイスの手動追加

ここでは、モバイルデバイスを手動で追加する方法を説明します。モバイルデバイスの登録は、次の手順で行います。

STEP1	モバイルデバイスを ERA のグループ構造に追加する	P293 参照
STEP2	モバイルデバイスに展開する	P308 参照

5.3.6.1 モバイルデバイスを ERA のグループ構造に手動で追加する

モバイルデバイスを ERA のグループ構造に手動で追加するには、電子メールで登録する方法とリンクまたは QR コードを利用する方法があります。

●電子メールで登録する

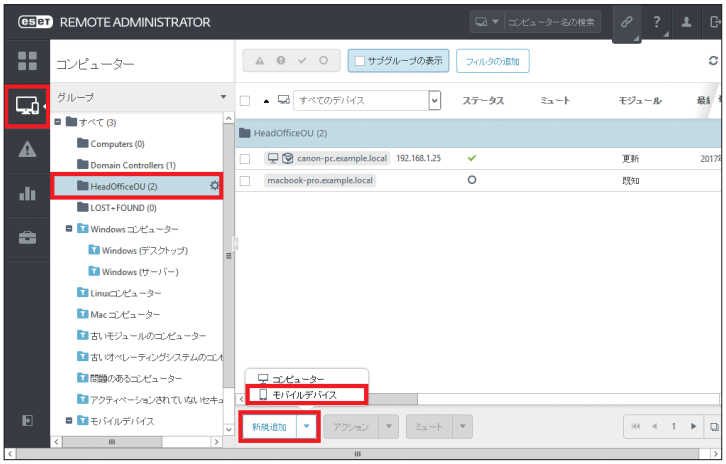
モバイルデバイスの登録を電子メールで行う方法は、モバイルデバイスの一括登録に最適です。登録リンクを任意の数のデバイスにメールで送信できます。各モバイルデバイスは電子メールアドレスに基づいて一意のワンタイムトークンを受信します。ここでは、登録したいモバイルデバイスの電子メールアドレスなどの情報を記載しておいた CSV 形式のファイルを利用して、電子メールで一括登録を行う手順を解説します。電子メールで登録を行うときは、SMTP サーバーを設定する必要があります。SMTP サーバーの設定については、「6.11 サーバーの設定 - ■詳細設定」をご参照ください。

! 重 要

電子メールでの登録に利用される情報は、「電子メールアドレス」「デバイス名」「説明」の 3 項目です。あからじめ、これらの項目を区切り文字（セミコロン、カンマ、スペース、またはタブ）で区切って記述した電子メール登録用の CSV 形式のファイルを用意しておいてください。なお、必須項目は、電子メールアドレスのみですが、モバイルデバイス登録後に識別しやすくするために「デバイス名」を入力しておくことをお勧めします。デバイス名を空欄にすると、電子メールアドレスがデバイス名として利用されます。また、ファイルを保存するときは、文字コードに「UTF-8」を利用してください。文字コードに「Shift-JIS」を利用すると、日本語が文字化けする場合があります。

操作手順

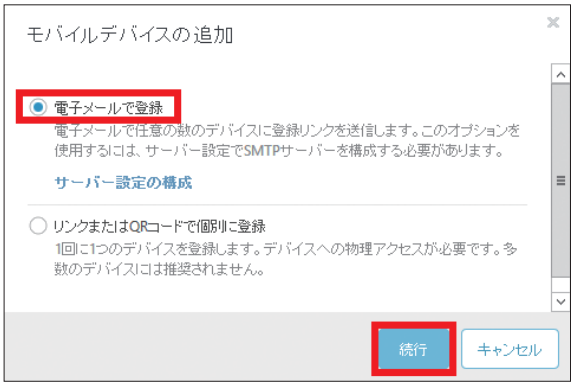
1. ERA Web コンソールを開き、［コンピューター］セクションをクリックします。モバイルデバイスを登録したいグループをクリックし、［新規追加］＞［モバイルデバイス］をクリックします。



「モバイルデバイスの追加」画面が表示されます。

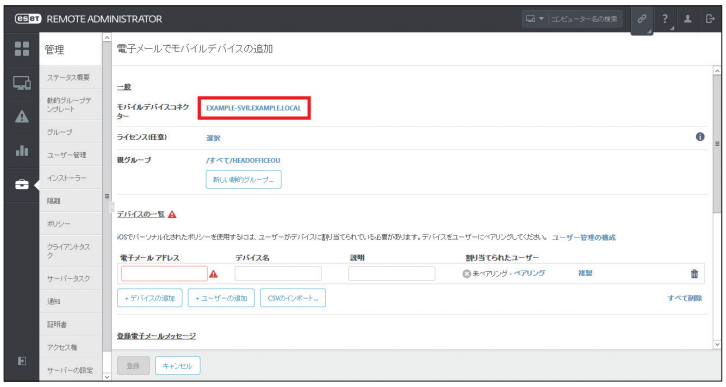
続く

2 ［電子メールで登録］をクリックし、［続行］ボタンをクリックします。



「電子メールでモバイルデバイスの追加」画面が表示されます。

3 「モバイルデバイスコネクター」にモバイルデバイスコネクターをインストールしたサーバーが表示されていることを確認します。

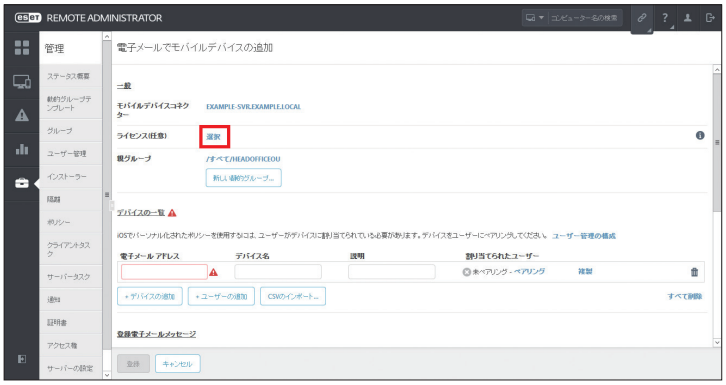


ワンポイント

モバイルデバイスコネクターをインストールしたサーバーが複数あるときは、表示中のサーバー名をクリックして、モバイルデバイスの登録に利用するサーバーを選択します。

続く

4 「ライセンス（任意）」の［選択］をクリックします。

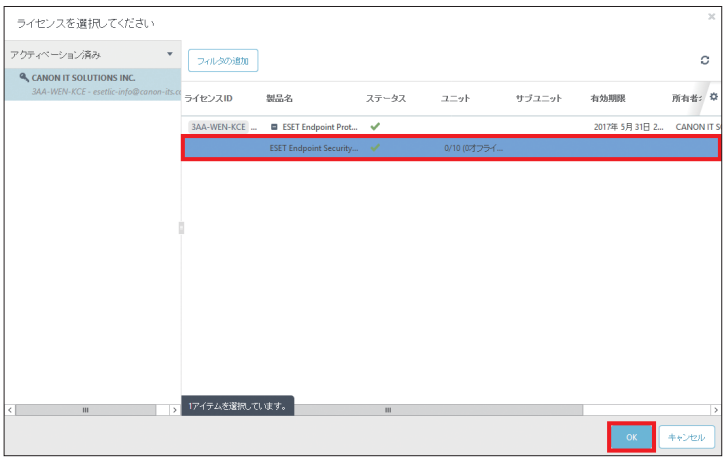


「ライセンスを選択してください」画面が表示されます。

ワンポイント

ライセンスの選択を行うと、製品アクティベーションクライアントタスクがモバイルデバイス用に作成されます。アクティベーションが行われるとライセンスが消費されます（各モバイルデバイスごとに 1 つ）。

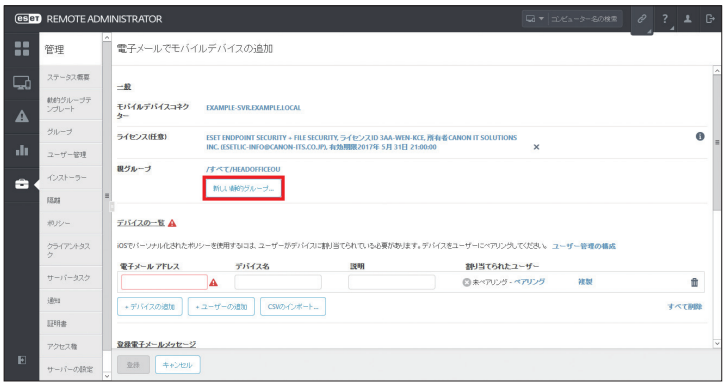
5 アクティベーションで使用するライセンスを選択し、［OK］をクリックします。



「ライセンス（任意）」に選択したライセンスが表示されます。

続く

6 新しい静的グループを作成して、モバイルデバイスを登録したいときは、［新しい静的グループ］をクリックします。現在、選択中の静的グループに登録するときは手順 10 に進んでください。

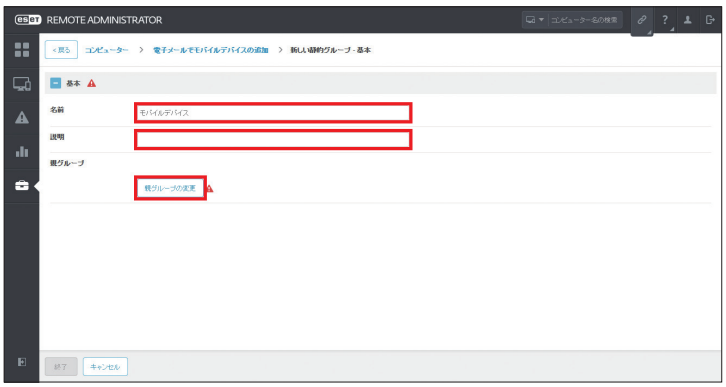


「新しい静的グループ - 基本」画面が表示されます。

ワンポイント

モバイルデバイス用の特定の静的グループがない場合は、新しい静的グループ（モバイルデバイスなど）を作成することをお勧めします。既存のグループがある場合は、現在選択中のグループをクリックすると、ポップアップウィンドウが開き、既存の静的グループを選択できます。

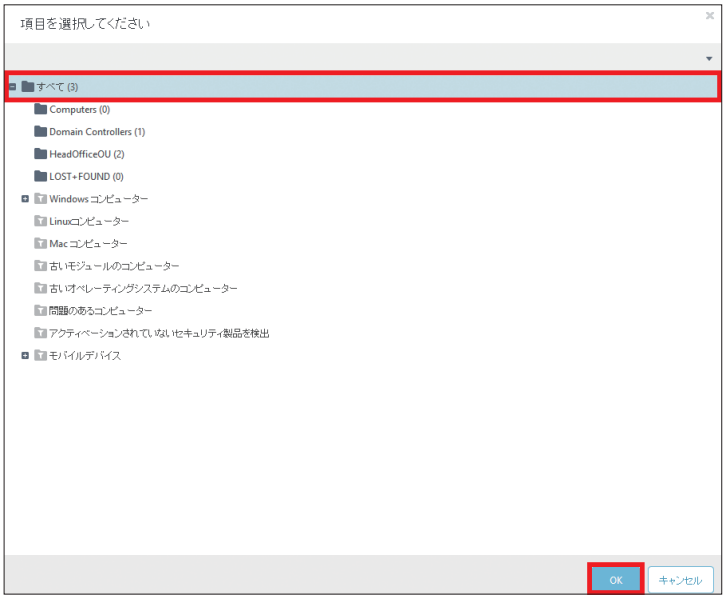
7 作成するグループの名前を入力し、必要に応じて説明を入力します。［親グループの変更］をクリックします。



「項目を選択してください」画面が表示されます。

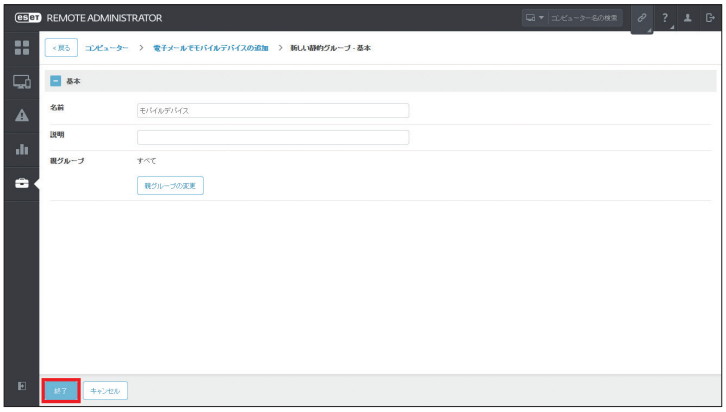
続く

8 作成したグループを配置したいグループを選択し、［OK］をクリックします。



「新しい静的グループ - 基本」画面に戻ります。

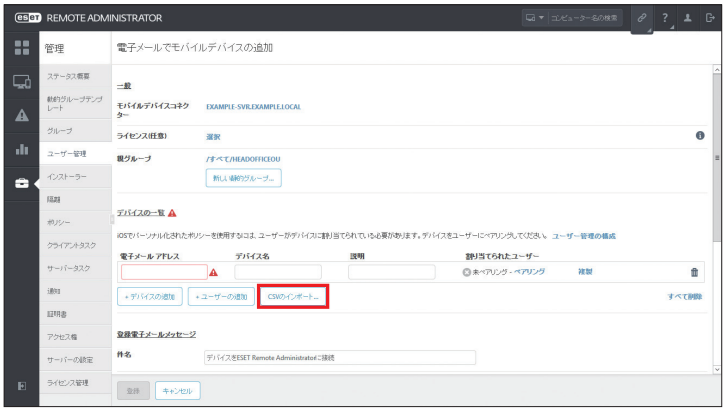
9 ［終了］をクリックします。



「電子メールでモバイルデバイスの追加」画面に戻ります。

続く

10 [CSV のインポート] をクリックします。

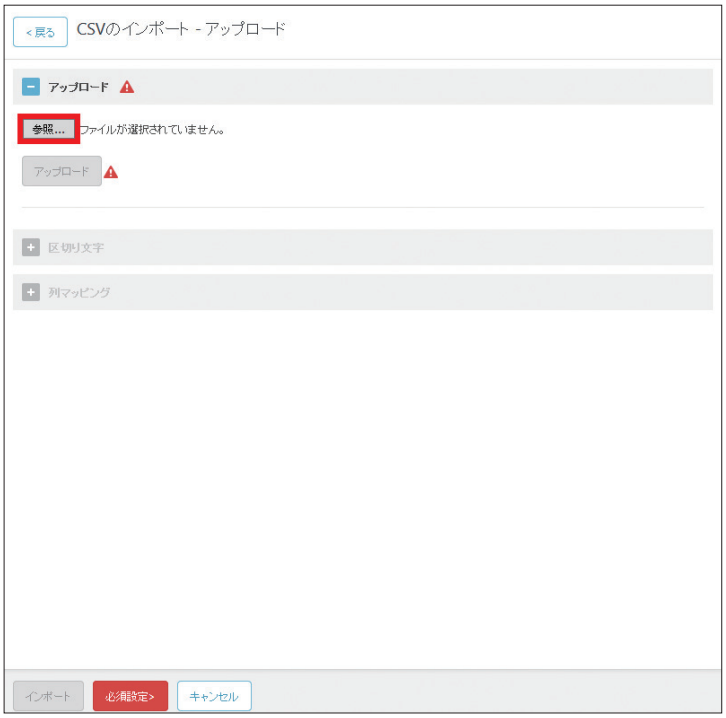


「CSV のインポート - アップロード」画面が表示されます。

ワンポイント

電子メールアドレスやデバイス名、説明の各項目に手動で入力することでも電子メールで登録を行えます。また、すべての項目入力後に［デバイスの追加］をクリックすると、新しい入力欄が追加されます。［ユーザーの選択］をクリックすると、既存のユーザーリストから電子メールでモバイルデバイスの登録を行うユーザーを選択できます。なお、Android デバイスは、ユーザーがモバイルデバイスに割り当てられていなくても登録できますが、iOS デバイスを電子メールで登録するときは、ユーザーがモバイルデバイスに割り当てられている必要があります。

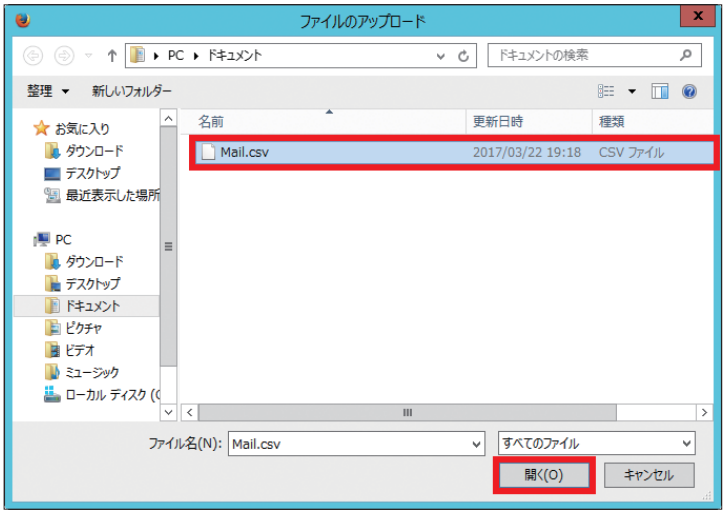
11 [参照] をクリックします。



「ファイルのアップロード」画面が表示されます。

続く

⑫ 用意しておいた CSV 形式のファイルを選択し、［開く］ボタンをクリックします。

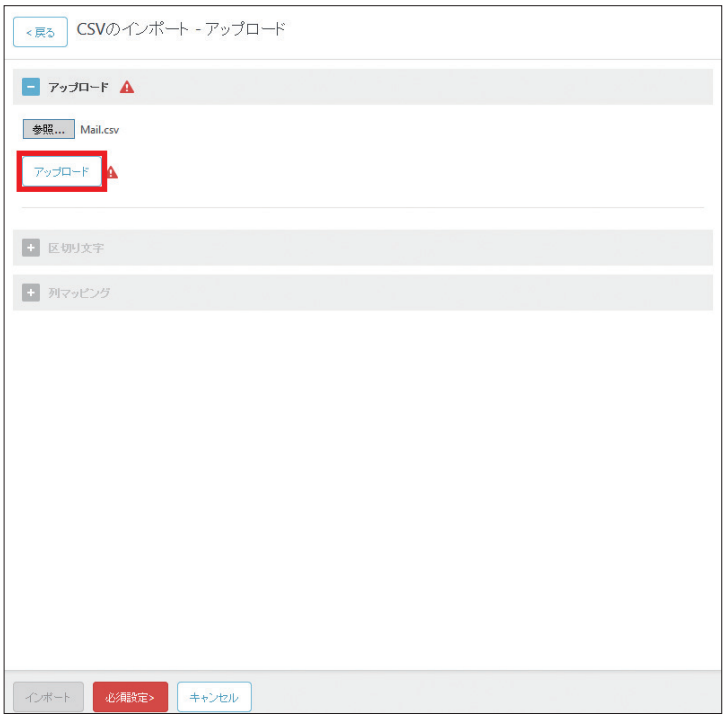


「CSV のインポート - アップロード」画面に戻ります。

ワンポイント

CSV 形式のファイルの拡張子は、「.CSV」である必要はありません。たとえば、「.TXT」でも登録を行えます。

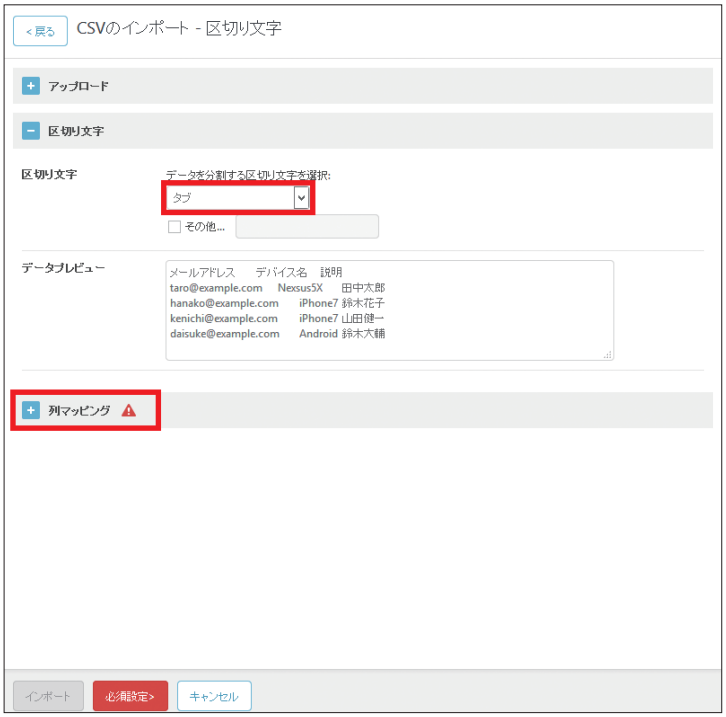
⑬ ［アップロード］をクリックします。



読み込んだ CSV 形式のファイルのプレビューが表示されます。

続く

14 区切り文字を「データを分割する区切り文字の選択」から選択し、［列マッピング］をクリックします。

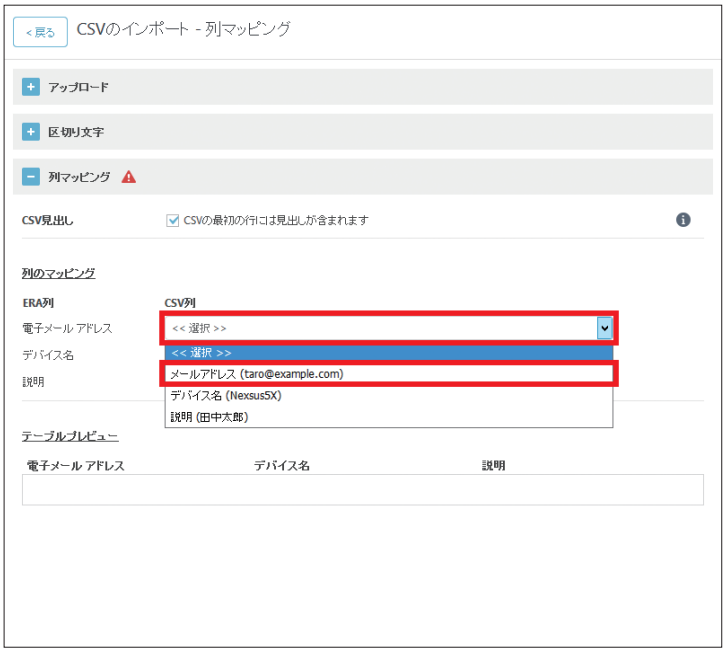


「列マッピング」が展開されます。

ワンポイント

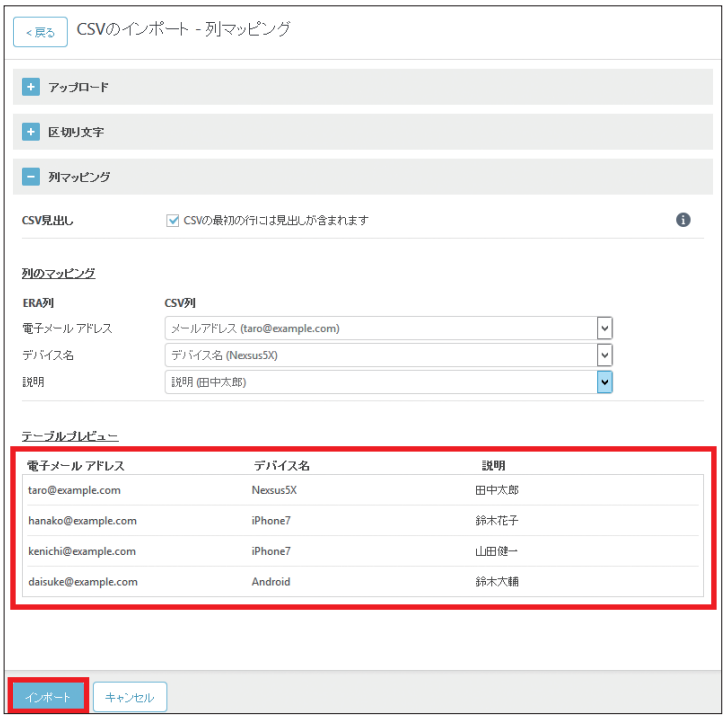
「データを分割する区切り文字の選択」に CSV 形式のファイルの作成に利用した区切り文字がないときは、［その他］のチェックをオンにして、利用した区切り文字を入力します。

15 電子メールアドレスの［<<選択>>］をクリックして、電子メールアドレスに利用する CSV 列を選択します。同様にデバイス名や説明の選択も行います。



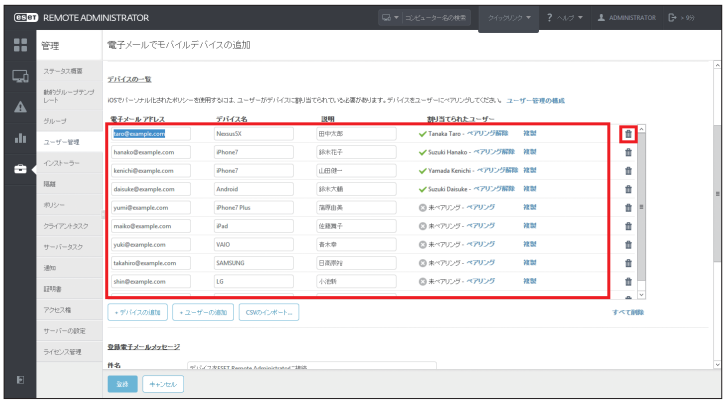
続く

16 CSV 列を選択すると、「テーブルプレビュー」が表示されます。作成した CSV 形式通りに文字列が並んでいることを確認し、［インポート］をクリックします。



CSV 形式のファイルから情報が読み込みまれます。

17 CSV 形式のファイルから読み込まれた情報に問題がないかを確認します。

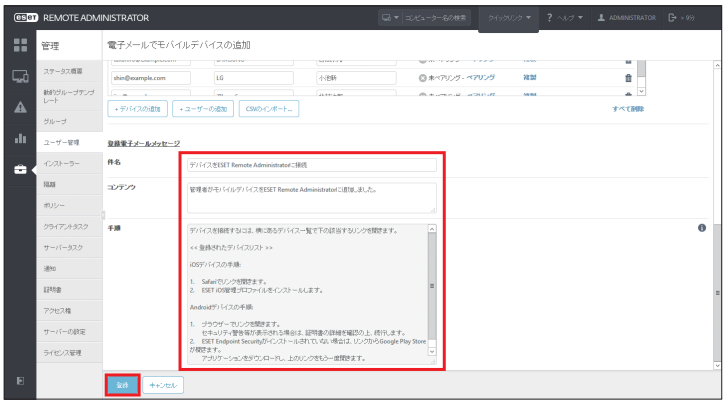


ワンポイント

読み込まれた情報が間違っていたときは、その欄をクリックして再編集します。また、登録された情報を削除したいときは、🗑をクリックします。

続く

18 登録電子メールメッセージの内容を確認し、［登録］をクリックします。入力した電子メールアドレスに登録リンクと手順が記載された電子メールが送信されます。モバイルデバイスの登録を完了するには、電子メール記載の手順に従って、電子メールに記載されているリンクをタップして、ESET Endpoint Security for Android のインストールを行ったり、iOS の ESET iOS Management Profile のインストールを行ったりします。



ワンポイント

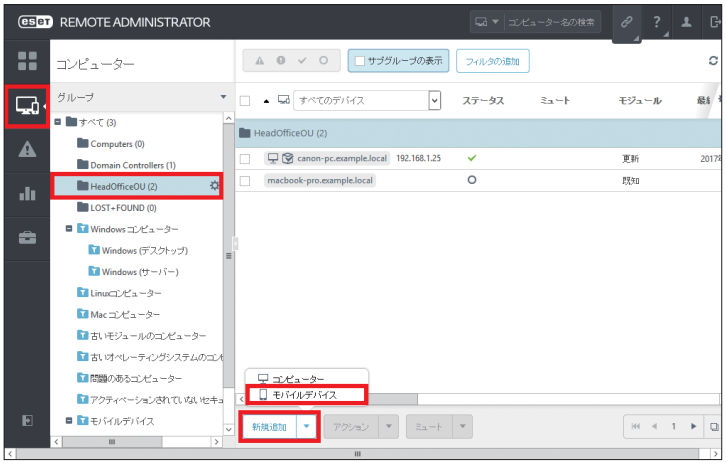
送信される電子メールのメッセージは、件名および内容をカスタマイズできます。必要に応じて、カスタマイズを行ってください。なお、別表示されている手順部分の内容については、カスタマイズすることはできません。

●リンクまたは QR コードで登録する

リンクまたは QR コードで登録する方法は、一度の操作で 1 台のモバイルデバイスしか登録できませんが、ユーザー / モバイルデバイスの所有者に何もさせずに、管理者自身がすべての作業を行った後に、モバイルデバイスを配布するといった用途に最適です。リンクまたは QR コードで登録するには、以下の手順で行います。

操作手順

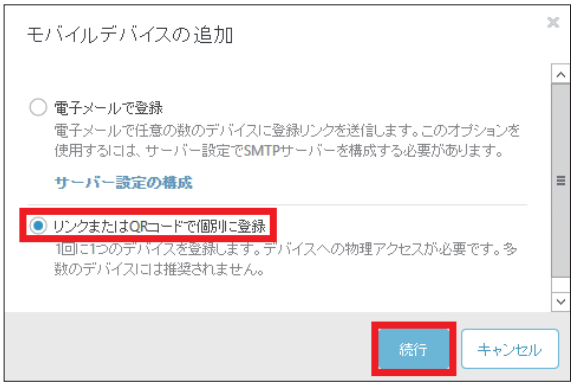
1 ERA Web コンソールを開き、［コンピューター］セクションをクリックします。モバイルデバイスを登録したいグループをクリックし、［新規追加］＞［モバイルデバイス］とクリックします。



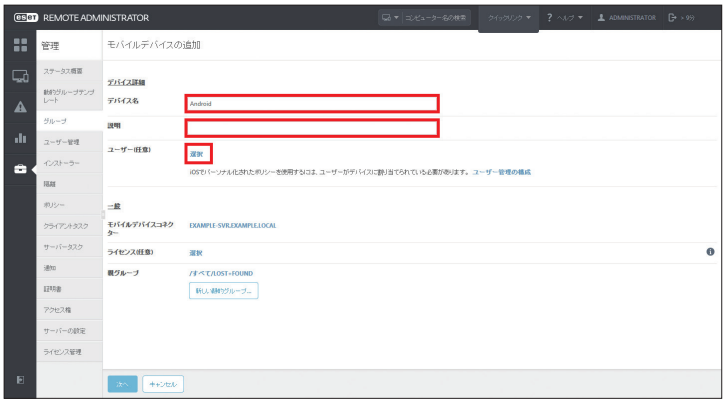
「モバイルデバイスの追加」画面が表示されます。

続く

2 ［リンクまたは QR コードで個別に登録］をクリックし、［続行］をクリックします。



3 登録するデバイス名を入力し、必要に応じて説明を入力します。ユーザーを登録するモバイルデバイスに割り当てるときは、［選択］をクリックします。



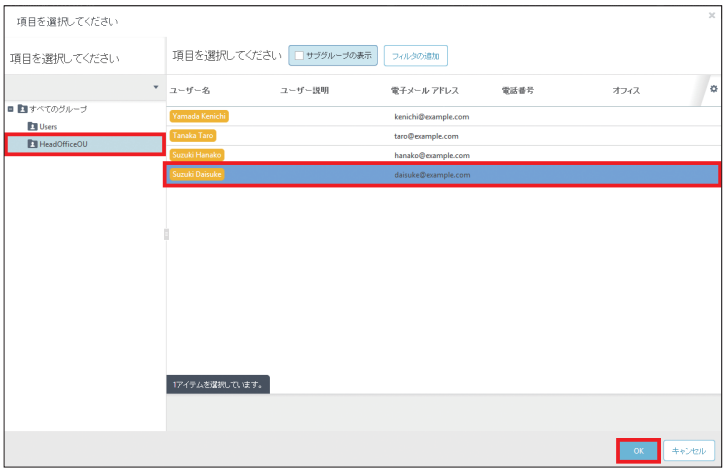
「項目を選択してください」画面が表示されます。

ワンポイント

iOS デバイスでパーソナル化されたポリシーを使用するには、ユーザーがデバイスに割り当てられている必要があります。

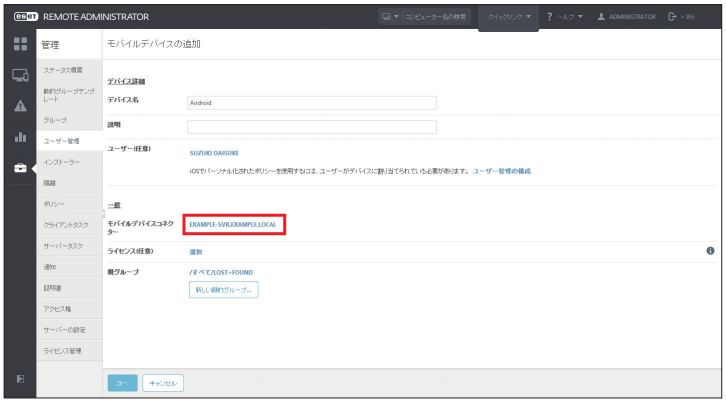
続く

4 割り当てたいユーザーが登録されているグループをクリックし、割り当てたいユーザーをクリックして、[OK] をクリックします。



選択したユーザーが「ユーザー（任意）」に登録されます。

5 「モバイルデバイスコネクター」にモバイルデバイスコネクターをインストールしたサーバーが表示されていることを確認します。

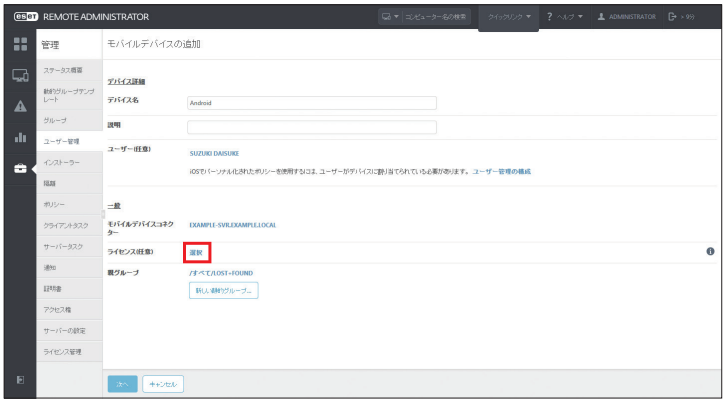


ワンポイント

モバイルデバイスコネクターをインストールしたサーバーが複数あるときは、表示中のサーバー名をクリックして、モバイルデバイスの登録に利用するサーバーを選択します。

続く

6 ［ライセンス（任意）］の［選択］をクリックします。

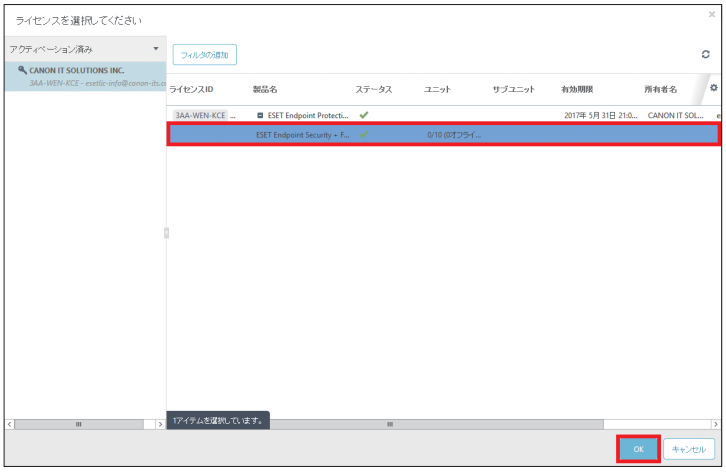


「ライセンスを選択してください」画面が表示されます。

ワンポイント

ライセンスの選択を行うと、製品アクティベーションクライアントタスクがモバイルデバイス用に作成されます。ライセンス単位が取得されます（各モバイルデバイスごとに 1 つ）。

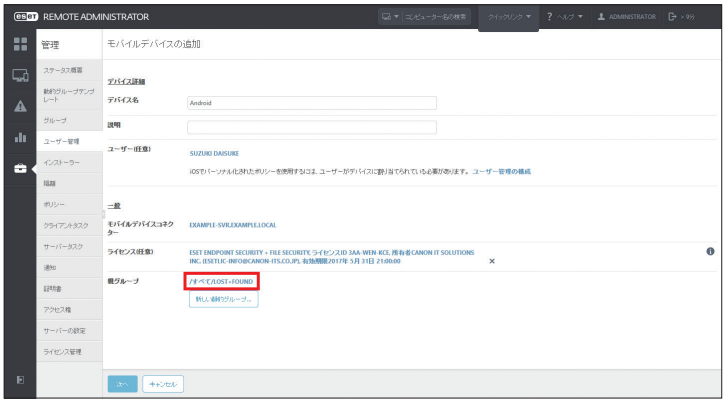
7 アクティベーションで使用するライセンスを選択し、［OK］をクリックします。



「ライセンス（任意）」に選択したライセンスが表示されます。

続く

8 親グループの変更を行うときは、現在、選択中の親グループをクリックします。

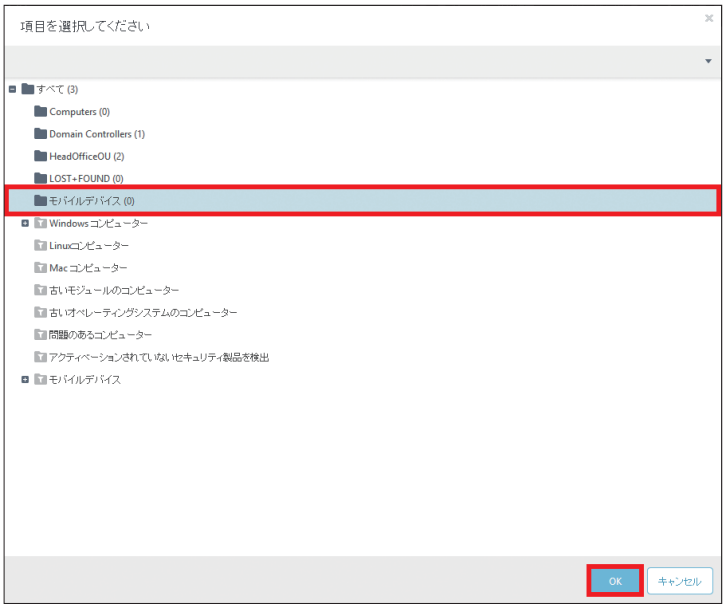


「項目を選択してください」画面が表示されます。

ワンポイント

モバイルデバイス用の特定の静的グループがない場合は、新しい静的グループ（モバイルデバイスなど）を作成することをお勧めします。新しいグループを作成し、そのグループにモバイルデバイスを登録したいときは、[新しい静的グループ] をクリックして画面の指示に従ってください。

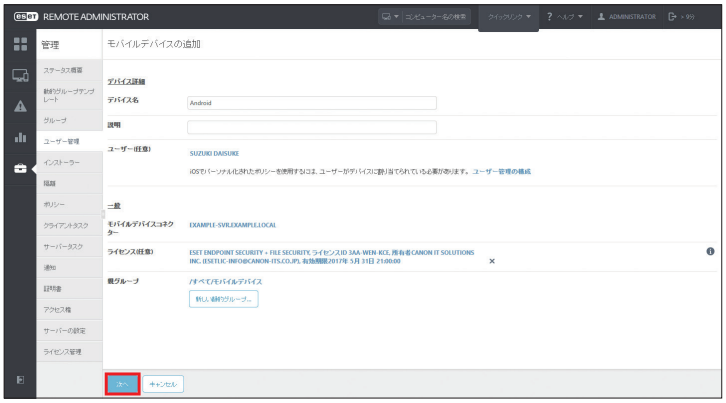
9 モバイルデバイスを登録したいグループをクリックし、[OK] をクリックします。



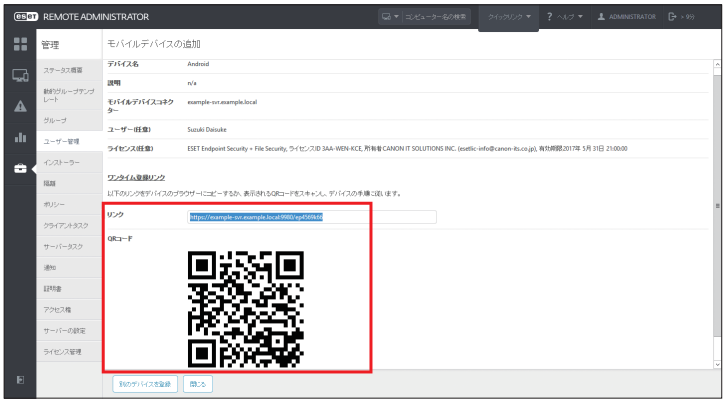
親グループに選択したグループが表示されます。

続く

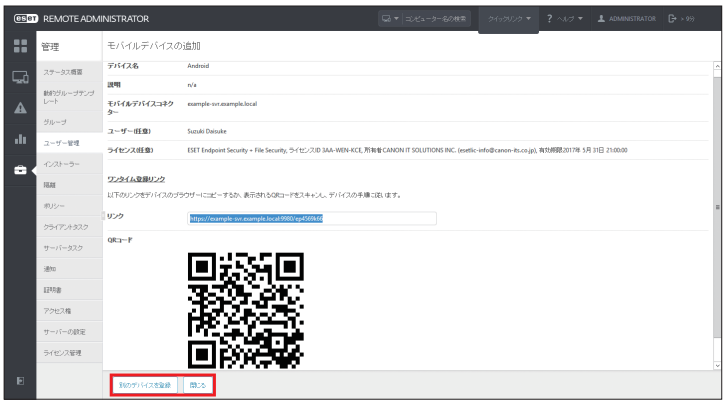
10 [次へ] をクリックします。



11 登録リンクと QR コードが表示されます。登録リンクをモバイルデバイスの Web ブラウザーに手動で入力するか、この URL を電子メールなどでモバイルデバイスに送信します。また、QR コードを使用することもできます。



12 別のモバイルデバイスを登録するときは、[別のデバイスを登録] をクリックして手順 2 からの作業を繰り返します。モバイルデバイスの登録を終了するときは、[閉じる] をクリックします。



5.3.6.2 モバイルデバイスに展開する

モバイルデバイスを ERA のグループ構造に追加したら、続いて、Android デバイスには、ESET Endpoint Security for Android を展開し、iOS デバイスには ESET iOS Management Profile の展開を行います。

● Android デバイスに ESET Endpoint Security for Android を展開する

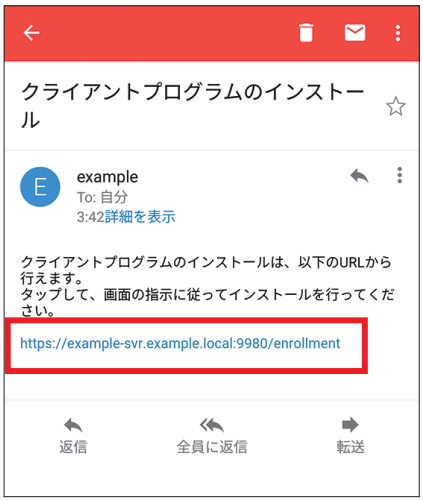
ここでは、登録リンクを利用した ESET Endpoint Security for Android のインストールの方法を紹介します。管理者は、デバイス登録を行ったときに表示された登録リンクを電子メールでユーザーに送信しておく必要があります。

ワンポイント

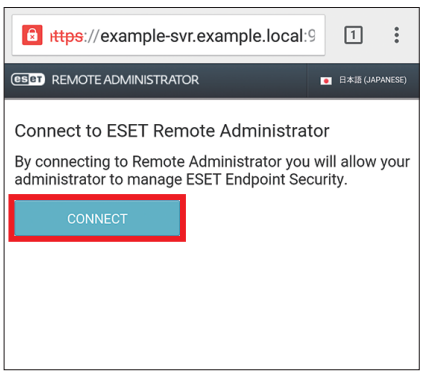
ESET Endpoint Security for Android のローカルインストールの方法については、「4.3.2 ESET Endpoint Security for Android の展開」の「●ローカルインストール」をご参照ください。

操作手順

1 メールアプリで登録リンクが記載されたメールを開き、リンクをタップします。



2 [CONNECT] ボタンをタップします。

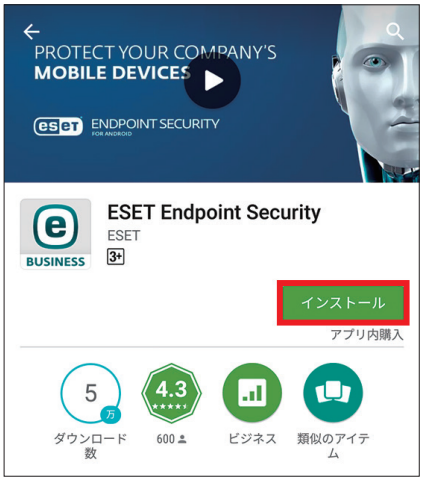


ワンポイント

セキュリティの警告画面が表示されたときは、[詳細設定] をタップして、[...（ドメイン名）にアクセスする] をタップします。

続く

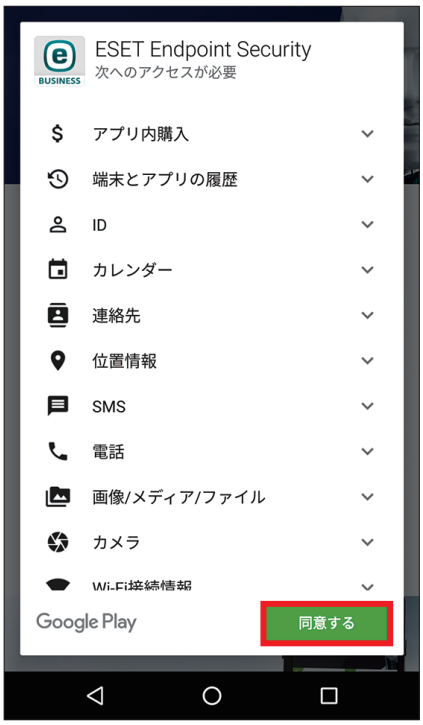
3 Google Play Store に移動し［インストール］ボタンをタップします。



ワンポイント

インストールするバージョンと Android のバージョンによりインストールとセットアップ中の画面に差異があります。

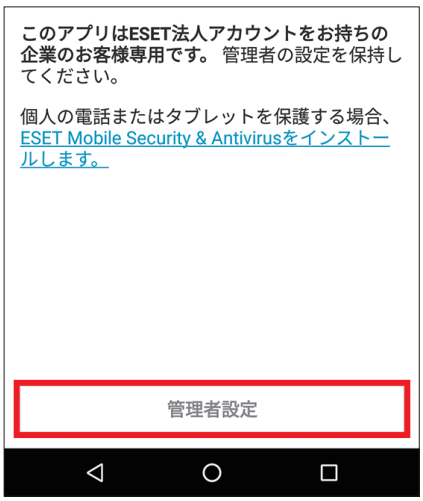
4 ［同意する］ボタンをタップすると、インストールが開始されます。



続く

5 インストールが完了したら、［開く］ボタンをタップします。

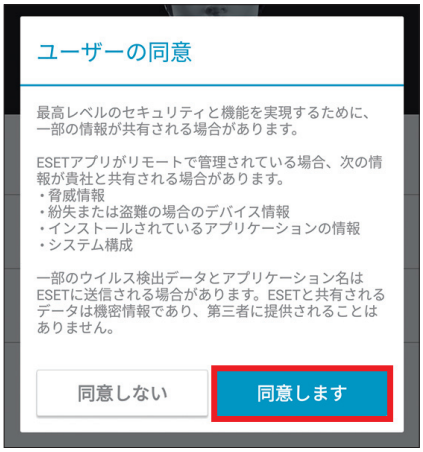
6 ［管理者設定］ボタンをタップします。



続く

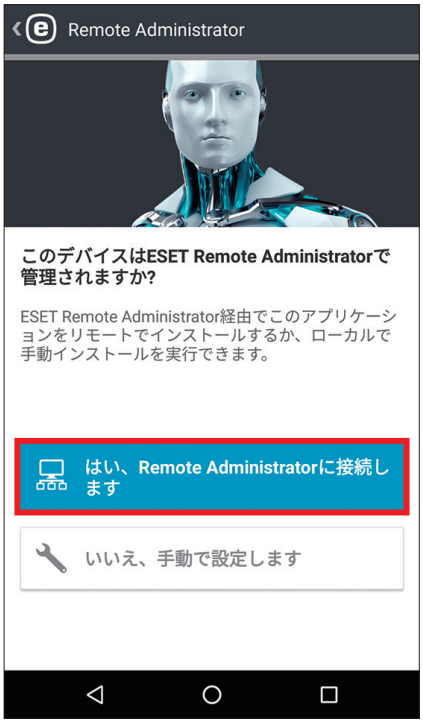
7 [同意します] ボタンをタップします。

8 [同意します] ボタンをタップします。

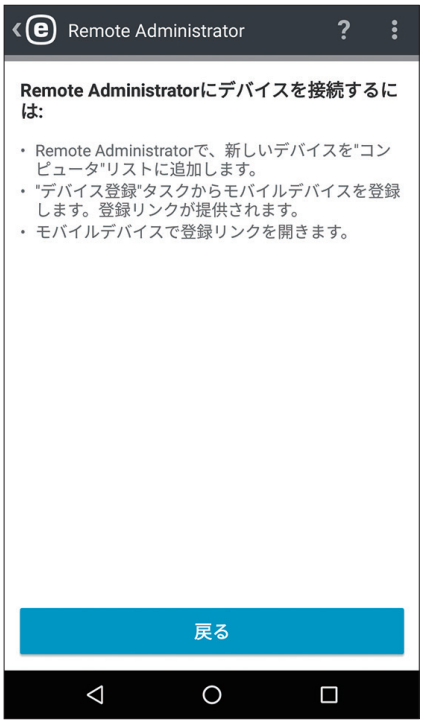


続く

9 ［はい、Remote Administrator に接続します］ボタンをタップします。

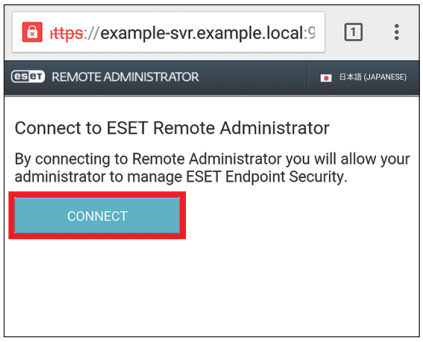


10 Remote Administrator に接続するための情報が表示されます。ホームボタンをタップして、再度、メールアプリで登録リンクが記載されたメールを開き、リンクをタップします。

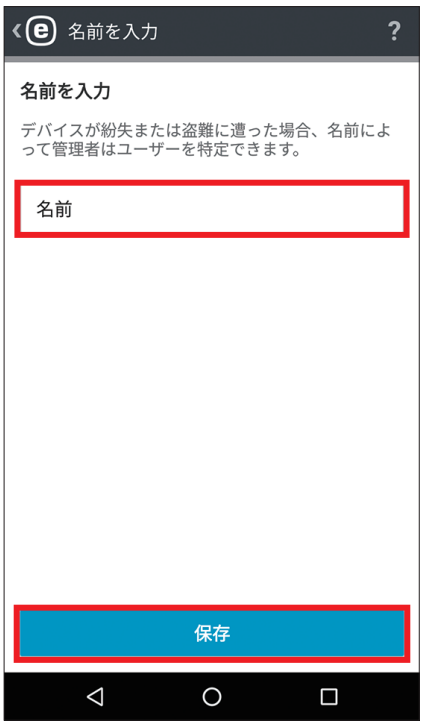


続く

11 [CONNECT] ボタンをタップします。



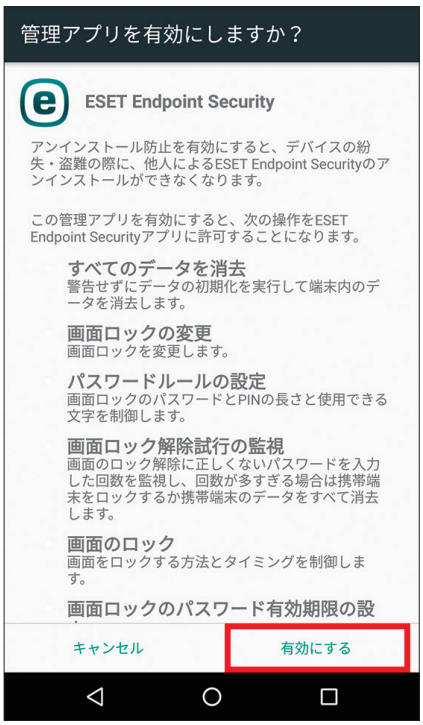
12 名前の入力画面が表示されます。必要に応じて名前の修正を行い、[保存] ボタンをタップします。



続く

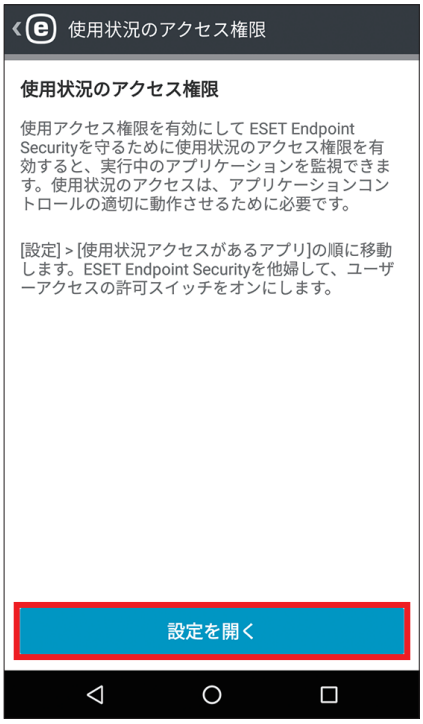
13 [有効] ボタンをタップします。

14 [有効にする] をタップします。



続く

15 ［設定を開く］ボタンをタップします。



16 ［ESET Endpoint Security］をタップします。

続く

⑰「使用状況へのアクセスを許可」の右側にあるスライドバーをタップします。

⑱「セットアップが完了しました」と表示されます。［閉じる］ボタンをクリックします。ESET Endpoint Security for Android のインストールはこれで完了ですが、この時点では、まだアクティベーションや管理パスワードの設定は行われていません。アクティベーションや管理パスワードの設定は、ERA サーバーから行えます。

アクティベーションの詳細については、「6.6.3.1　ESET セキュリティ製品」の「■製品のアクティベーション」を参照してください。

管理パスワードの設定は、ポリシーで行うことができます。詳細は、「6.5　ポリシー」を参照してください。

● iOS デバイスに ESET iOS Management Profile を展開する

ここでは、登録リンクを利用した ESET iOS Management Profile のインストールの方法を紹介します。管理者は、デバイス登録を行ったときに表示された登録リンクを電子メールでユーザーに送信しておく必要があります。

操作手順

1. メールアプリで登録リンクが記載されたメールを開き、リンクをタップします。

2. プロファイルのインストール画面が表示されます。［インストール］をタップします。

3. ［インストール］をタップします。

続く

4 ［信頼］をタップすると、プロファイルのインストールが行われます。

5 イントールが完了したら、［完了］をタップします。この時点では、まだアクティベーションが行われていません。アクティベーションは、ERA サーバーから行います。アクティベーションの詳細については、「6.6.3.1　ESET セキュリティ製品」の「■製品のアクティベーション」を参照してください。

ワンポイント

iOS デバイスが ERA サーバーに接続できない場合は、Mobile Device Connector と Apple Push Notification の通信で使用するポートが解放されているか確認してください。詳細は「2.4.7　Mobile Device Connector」を参照してください。

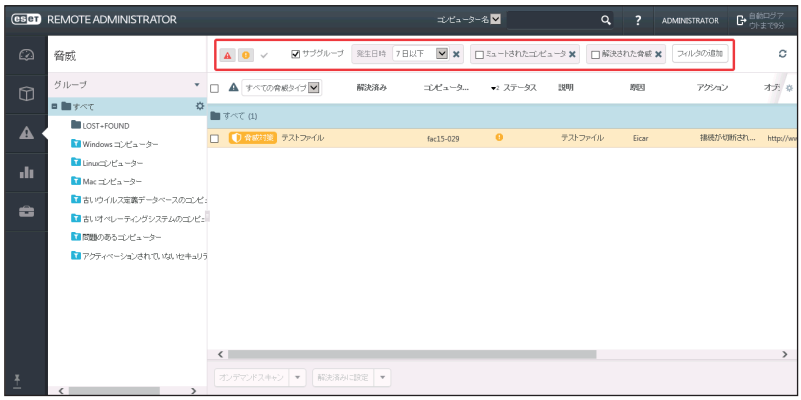
続く

5.4 脅威

管理するコンピューターで検出された脅威を確認できます。グループや脅威タイプを組み合わせて検出された脅威を表示させることができます。

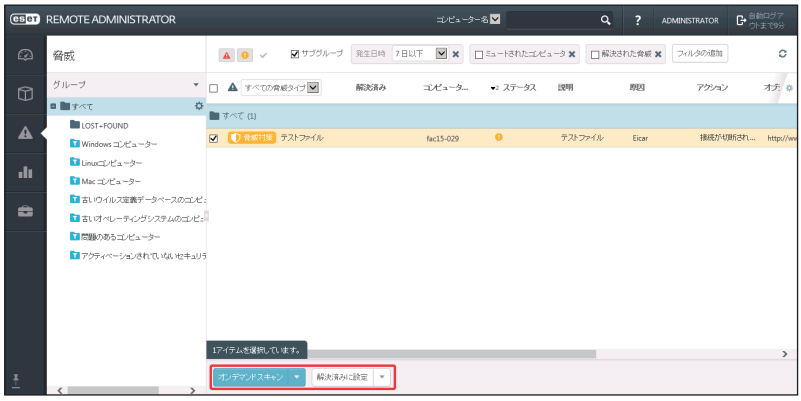
5.4.1 脅威画面の構成

リスト上部のフィルターを使用して脅威をフィルタリングできます。



ワンポイント

既定では、すべてのタイプの脅威が表示されますが、ウイルス対策、ファイアウォールなどの種別でフィルタリングすることができます。



オンデマンドスキャン	脅威を検知したクライアントでのオンデマンド検査が実行されます。
解決済みに設定	未解決の脅威を「解決された脅威」に変更することができます。リスト上部の「解決された脅威」フィルタを選択すると、「解決された脅威」を確認することができます。

ワンポイント

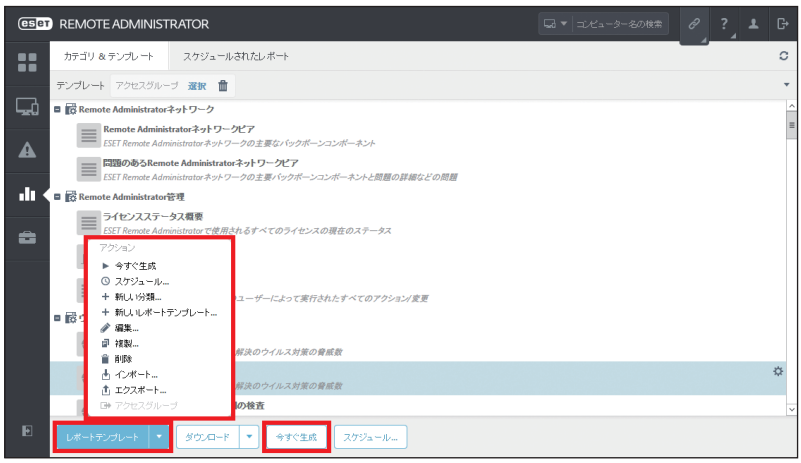
脅威を報告したクライアントからの通知を停止する場合は、該当の脅威をクリックして表示されるメニューから「ミュート」を設定します。

5.5 レポート

クライアントから収集した情報や、ERA サーバーの情報をグラフや表にまとめることができる機能です。データベースからデータにアクセスしてフィルタリングできます。

5.5.1 レポートテンプレートの作成と編集

任意のレポートテンプレートを選択して、[レポートテンプレート] ボタンをクリックすると、テンプレートの編集メニューが表示されます。



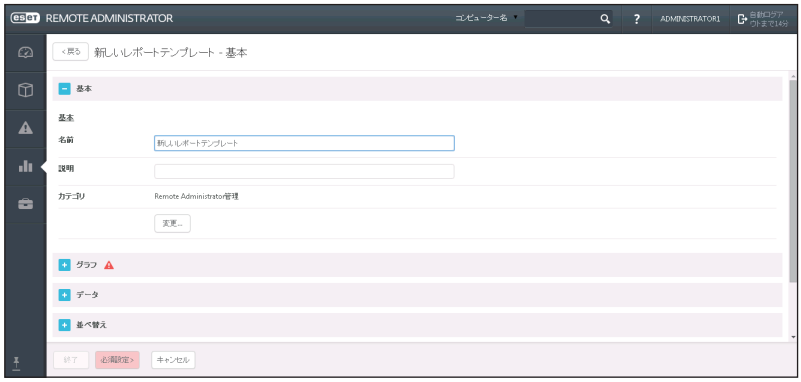
	今すぐ生成	レポートが生成され、出力データを確認できます。リストからレポートを選択しないと押すことができません。
	スケジュール	レポート生成のスケジュールを設定します。
	新しい分類	「名前」と「説明」を入力して、レポートテンプレートの新しいカテゴリを作成します。
	新しい レポートテンプレート	新規のレポートテンプレートを作成します。現在選択しているレポートのカテゴリが設定されます。
	編集	既存のレポートテンプレートを編集します。
	複製	選択しているレポートテンプレートが複製されますので、設定等を変更して新たなレポートテンプレートを作成します。
	削除	選択したレポートテンプレートを削除します。
	インポート	レポートテンプレートを ERA にインポートし追加することができます。
	エクスポート	選択しているレポートテンプレートをテキストファイルで保存します。

5.5.2 レポートテンプレートの編集

「レポートテンプレート」から［新しいレポートテンプレート］、［編集］、［複製］を選択すると、「新しいレポートテンプレート」画面が表示されます。基本・グラフ・データ・並べ替え・フィルタ・サマリーと別れていますので必要に応じて設定、変更を行います。

■基本

テンプレートに関する基本情報を編集します。テンプレートの名前、説明、カテゴリを入力または変更できます。

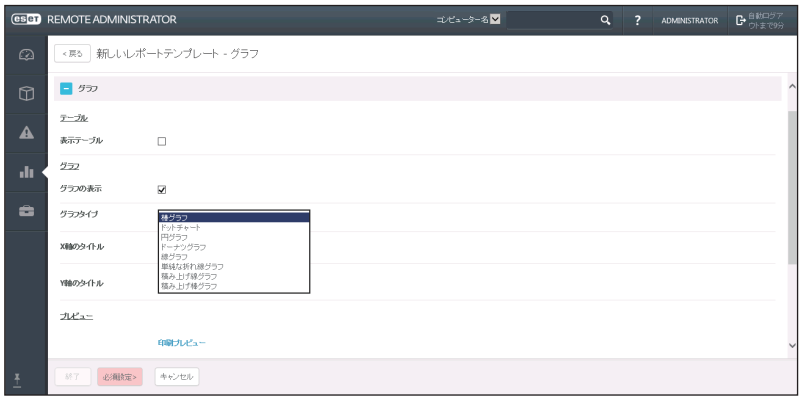


ワンポイント

カテゴリの変更は既存のカテゴリと新規に追加したカテゴリから選択できます。

■グラフ

表示させるレポートの種類を編集します。情報を表形式で表示するテーブルと、グラフ形式での表示が選択できます。



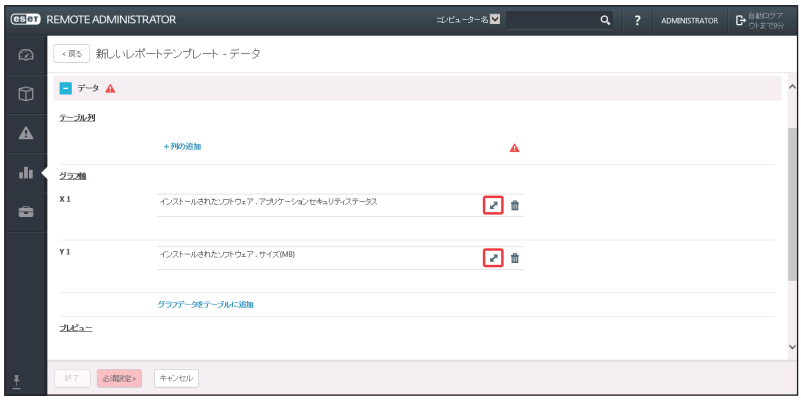
ワンポイント

印刷プレビューをクリックすると、選択した内容にあわせてデータをリアルタイムで確認することができます。

棒グラフ	長方形棒で表示する値に比例した大きさで表示されます。
ドットチャート	ドットを使用して、定量値（棒グラフに類似しています）で表示されます。
円グラフ	円形のグラフで、扇形に分割し値が表示されます。
ドーナツグラフ	円グラフに類似していますが、ドーナツグラフは複数種類のデータを含めることができます。
線グラフ	直線の線分でつないだ、一連のデータ要素として情報が表示されます。
単純な折れ線グラフ	データ要素を表示せず、値に基づいた折れ線で情報が表示されます。
積み上げ線グラフ	異なる単位のデータを分析する場合に使用します。
積み上げ棒グラフ	単純棒グラフに類似していますが、複数のデータ型を異なる単位で棒に積み上げて表示されます。

■データ

表示する情報を選択します。グラフ項目で設定した内容によって選択する項目が変わります。



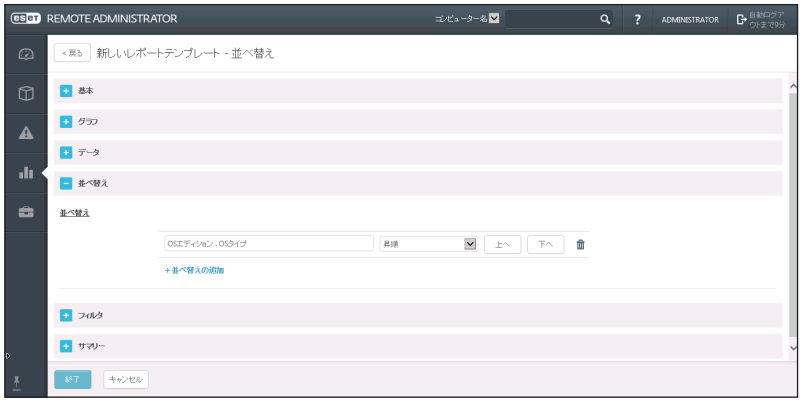
テーブル列	テーブルの情報は、選択したレポートの種類に基づき自動的に追加されます。
グラフ軸	X 軸及び Y 軸のデータを選択します。Y 軸は X 軸で選択した項目によって選択する項目が異なります。

ワンポイント

をクリックすると、名前、ラベル、書式フォーマットを変更することができます。変更できる項目は、選択した内容によって異なります。

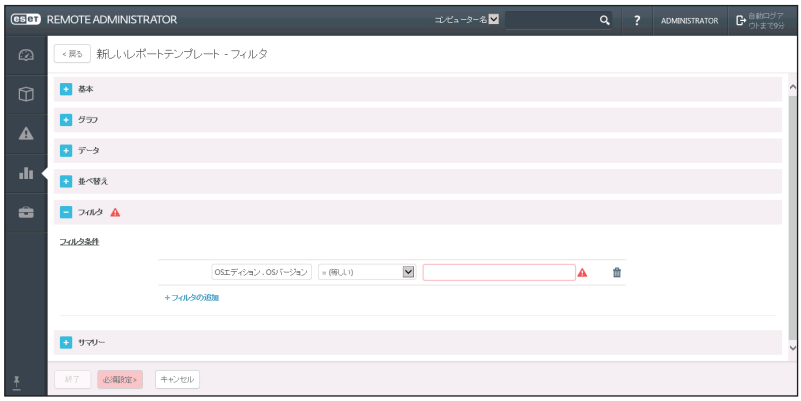
■並べ替え

選択しているデータ間の関係性を定義することができます。開始情報と並べ替え方法の昇順、降順を指定できます。複数の指定をすることもできます。



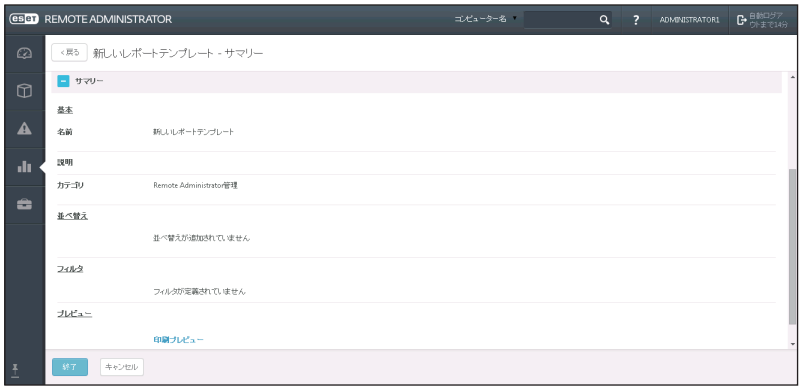
■フィルタ

条件を設定して、表示させるデータを絞り込みます。絞り込みのオプションと関数を設定します。
設定しているデータによって表示されるオプションが異なります。



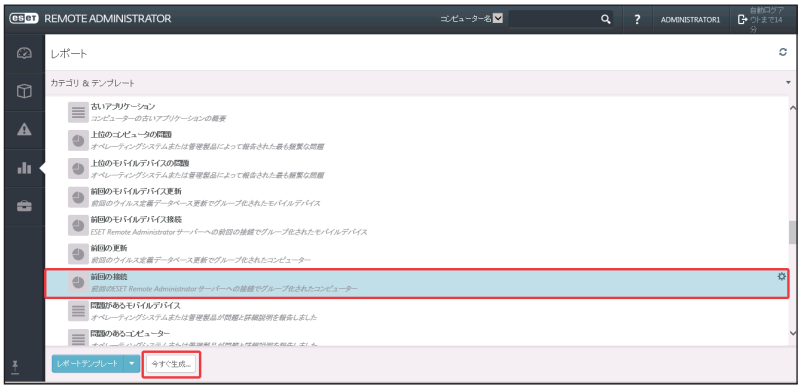
■サマリー

設定した内容を確認できます。



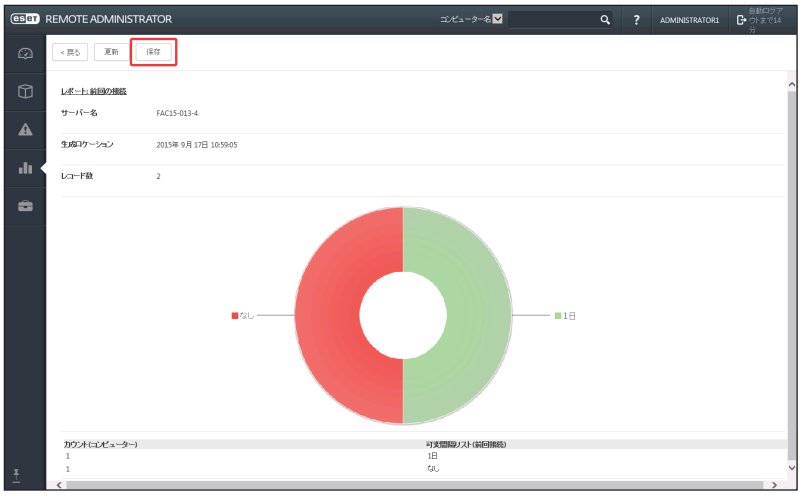
5.5.3 レポートの生成と保存

1 レポートテンプレートを選択し、［今すぐ生成］ボタンをクリックします。



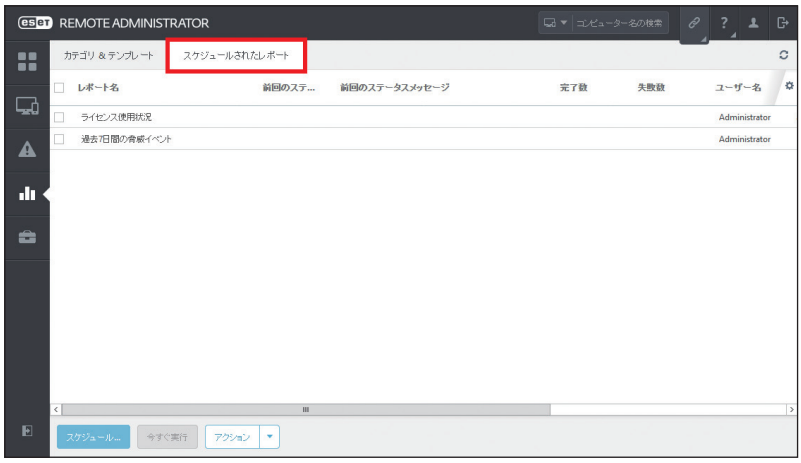
2 レポートが作成されます。

レポートを保存する場合は、［保存］ボタンをクリックします。
［保存］ボタンをクリックすると、サーバータスクの「レポートの作成」にリンクされます。詳細は、「6.7.3.3 レポートの作成」を参照してください。



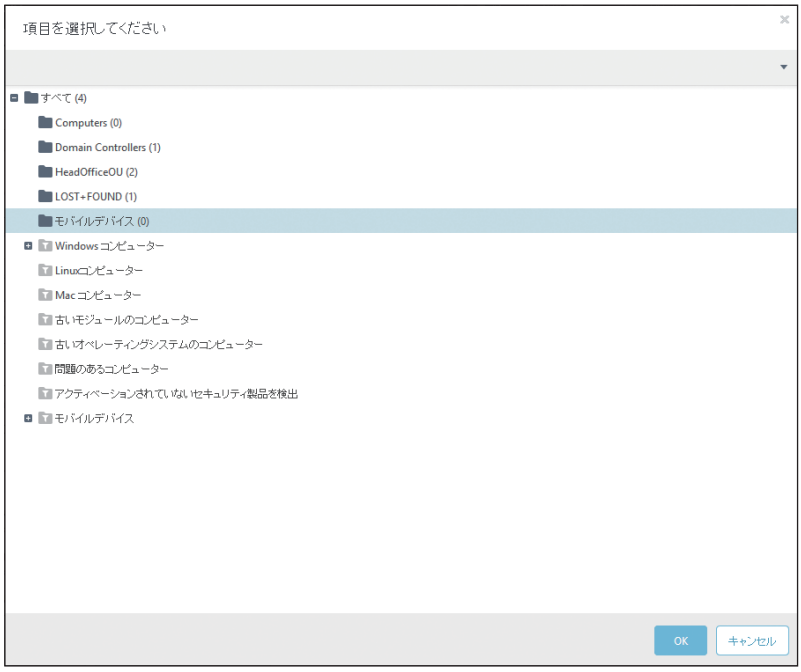
5.5.4 スケジュールされたレポート

［スケジュールされたレポート］タブをクリックすると、スケジュール設定されたレポートの一覧と前回の実行結果を確認できます。また、スケジュールされたレポートをクリックして、［今すぐ実行］をクリックすると、選択したスケジュールを即時実行できます。



5.5.5 アクセスグループの切り替え

アクセスグループフィルターボタンでは、ユーザーが静的グループを選択し、属するグループに応じて、表示されるオブジェクトをフィルタリングできます。



5.6 モバイルデバイス管理

ESET Remote Administrator でモバイルデバイス管理機能を活用するには、Mobile Device Connector を、オールインワンインストーラーまたはコンポーネントインストーラーでインストールを行い、ポリシーのインストール、登録、構成、および適用を行います。Mobile Device Connector のインストール方法については、「3 インストール」をご参照ください。

! 重 要

Mobile Device Connector のインストールを行ったら、製品アクティベーションクライアントタスクを使用して、Mobile Device Connector のアクティベーションを行っておいてください。Mobile Device Connector は、アクティベーションを行ってもライセンスにはカウントされません。

ワンポイント

ユーザー情報を Active Directory や LDAP と同期したい場合は、ERA サーバーでユーザー同期サーバータスクを実行します。これにより、ユーザー管理の目的で、ユーザーが Active Directory または LDAP と自動的に同期されます。

●モバイルデバイス管理の手順

モバイルデバイスの管理は、次の流れで行います。iOS デバイスの管理を行う場合は、手順 1 からの作業を行い、Android デバイスのみの管理を行う場合は、手順 1 ～ 2 を行う必要はありません。手順 3 から作業を行ってください。

操作手順

1. APN 証明書を作成します。APN 証明書は iOS デバイスを登録する Mobile Device Connector で使用されます。APN 証明書の詳細については、「6.9.3 APN 証明書」をご参照ください。
2. iOS デバイスを Mobile Device Connector に登録するための ESET Mobile Device Connector のポリシーを作成します。iOS デバイス登録用のポリシー作成方法の詳細については「6.5.3.1 iOS デバイス登録用のポリシーを作成する」をご参照ください。
3. モバイルデバイスを登録します。モバイルデバイスの登録手順については、「5.3.6 モバイルデバイスの手動追加」をご参照ください。
4. 製品アクティベーションクライアントタスクを使用してモバイルデバイスをアクティベーションします。アクティベーションの詳細については、「6.6.3.1 ESET セキュリティ製品」の「■製品のアクティベーション」を参照してください。各モバイルデバイスでライセンス単位が使用されます。
5. ユーザーの編集を行うことで、カスタム属性を構成したり、ユーザーが利用しているモバイルデバイスの割り当てを行います。ユーザーの編集の詳細については「6.4 ユーザー管理」をご参照ください。
6. ポリシーを適用して、モバイルデバイスを管理できます。たとえば、Exchange ActiveSync アカウントを作成すると、iOS デバイスのポリシーを管理でき、iOS デバイスのメールアカウント、連絡先、カレンダーなどの管理を行えます。また、iOS デバイスで制限を適用し、Wi-Fi 接続の設定を追加することもできます。モバイルデバイスのポリシーの詳細については、「6.5 ポリシー」をご参照ください。

MDM 構成プロファイル

プロファイルを構成し、管理されたモバイルデバイスでポリシーと制限を適用できます。以下のプロファイルを設定できます。

プロファイル名	説明
パスコード	アイドル状態から復帰するたびに、エンドユーザーはパスコードでデバイスを保護する必要があります。これにより、管理されたデバイスの機密企業情報が確実に保護されます。複数のプロファイルが 1 つのデバイスでパスコードを適用する場合は、最も厳しいポリシーが適用されます。
制限	制限プロファイルは、デバイス機能、アプリケーション、iCloud、セキュリティ、およびプライバシーに関連付けられた特定の権限の使用を制限し、管理されたデバイスのユーザーが使用できる機能を制限します。
Wi-Fi 接続リスト	社内の Wi-Fi の接続情報などを記載した Wi-Fi プロファイルを管理しているデバイスに、プッシュできます。これによって、Wi-Fi の接続先の情報が変更されたときでも、その設定をすぐに管理しているデバイスにすぐに反映できます。
VPN 接続リスト	VPN プロファイルは、企業の仮想プライベートネットワーク設定です。VPN プロファイルを関しているデバイスにプッシュすることで、ユーザーは外出先などの社外からでも安全に社内のネットワークににアクセスできます。 接続名 - デバイスに表示される接続名を表示します。 接続タイプ - このプロファイルで有効にされる接続のタイプを選択します。各接続タイプにより異なる機能が有効になります。 サーバー - 接続中のサーバーのホスト名または IP アドレスを入力します。
メールアカウント	管理者は IMAP/POP3 電子メールアカウントを構成できます。
Exchange ActiveSync アカウント	Exchange ActiveSync プロファイルにより、エンドユーザーは企業のプッシュベースの電子メールインフラストラクチャにアクセスできます。あらかじめ入力されたルックアップ値フィールドとオプションがあり、iOS 5 以上にのみ適用されます。
CalDAV - カレンダーアカウント	CalDAV には構成オプションがあり、エンドユーザーはエンタープライズ CalDAV サーバーとワイヤレスで同期できます。
CardDAV - 連絡先アカウント	このセクションでは、CardDAV サービスの固有の構成が行えます。
登録されたカレンダーアカウント	登録されたカレンダーはカレンダー構成を提供します。

Chapter 6 ESET Remote Administrator の管理

この章では、管理者がクライアントコンピューターおよび ERA サーバーの設定を管理する機能について説明します。「管理」メニューは、ESET Remote Administrator のメイン構成コンポーネントです。「管理」メニューでは、ESET Remote Administrator の初期設定およびメンテナンス作業を効率よく行うことができます。

「管理」メニューに表示されるサブメニューは次のとおりです。

6.1 ERA サーバインストール後のステータス概要の確認	ESET Remote Administrator の初期設定に必要な項目の確認と設定をします。
6.2 動的グループテンプレート	動的グループテンプレートの作成や管理をします。
6.3 グループ	クライアントコンピューターの管理や分類をします。
6.4 ユーザー管理	モバイルデバイスの管理目的で、ユーザーとユーザーグループを管理します。
6.5 ポリシー	クライアントコンピューターで実行される ESET 製品に特定の設定を割り当てます。
6.6 クライアントタスク	ERA サーバーからクライアントコンピューターにアクションを要求します。
6.7 サーバータスク	ERA サーバー上で発生する日常的な処理を自動化します。
6.8 通知	クライアントコンピューターおよび、ネットワーク上で発生したアラートの通知を管理します。
6.9 証明書	ERA サーバー、ERA エージェント、ERA プロキシ間の通信を認証するための、証明書を管理します。
6.10 アクセス権	ERA Web コンソールのユーザーとその権限を管理します。
6.11 サーバーの設定	ERA サーバーの設定を管理します。
6.12 ライセンス管理	購入した ESET 製品のライセンス情報を管理します。

6.1 ERA サーバインストール後のステータス概要の確認

ESET Remote Administrator の初期構成の説明が表示されます。「管理」メニューを使用する前に要点を確認することを推奨します。

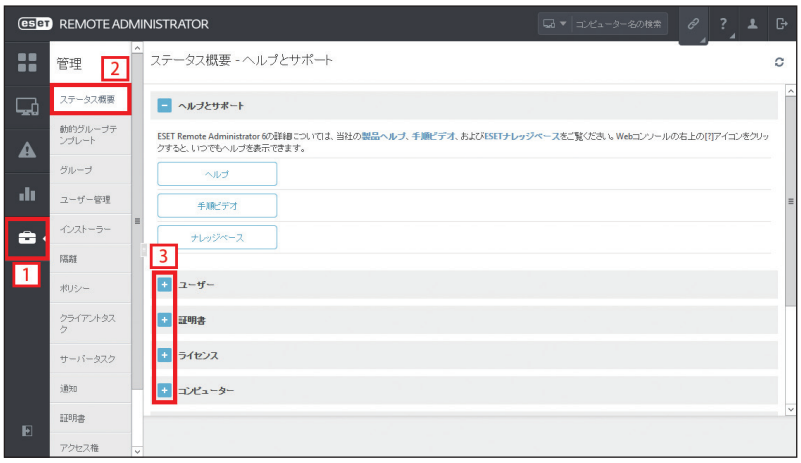
操作手順

1. ［管理］メニューをクリックします。

   「管理」画面が表示されます。

2. ［ステータス概要］サブメニューをクリックします。

3. 確認するセクションの ＋ をクリックします。



セクションの内容が表示されます。

■ヘルプとサポート

ESET Remote Administrator のヘルプや手順ビデオ、サポートページを表示できます。

ヘルプ	ESET Remote Administrator のヘルプが表示されます。
手順ビデオ	YouTube の「ESET Knowledgebase」が表示されます。
ナレッジベース	弊社サポートページが表示されます。

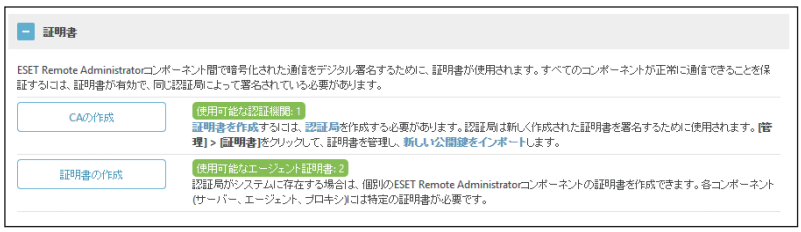
■ユーザー

ESET Remote Administrator のインストール中に既定の管理者アカウントが作成されます。ESET Remote Administrator でさまざまなレベルの管理を行えるように、新たにユーザーを追加し権限を設定するための要点が表示されます。

ローカルユーザーの追加	「新しいローカルユーザー」画面が表示されます。 画面の詳細は、「6.10.1.2　新しいローカルユーザーの作成」を参照してください。

■証明書

ESET Remote Administrator コンポーネント間で暗号化された通信をデジタル署名するためには証明書が使用され、その証明書は認証局（CA）によって著名されている必要があります。個別の ESET Remote Administrator コンポーネントの証明書とそれを著名する認証局を作成するための要点が表示されます。



CA の作成	「認証局の作成」画面が表示されます。 画面の詳細は、「6.9.2.2　新しい認証局の作成」を参照してください。
証明書の作成	「証明書の作成」画面が表示されます。 画面の詳細は、「6.9.1.2　新しい証明書の作成」を参照してください。

■ライセンス

ESET Remote Administrator バージョン 6 以降は、新しい ESET ライセンスシステムを使用します。新しいライセンスを追加するための要点が表示されます。

製品認証キー	「ライセンスの追加ー製品認証キー」画面が表示されます。 画面の詳細は、「6.12.2　アクティベーション」を参照してください。
セキュリティ管理者	日本では使用しません。
オフラインライセンスファイル	ELA（ESET License Administrator）を利用して発行したオフラインライセンスファイルの登録画面が表示されます。

■コンピューター

ESET Remote Administrator では、グループでコンピューターを分類し管理します。グループにコンピューターを追加するための要点が表示されます。

コンピュータの追加	「デバイスの追加」画面が表示されます。 画面の詳細は、「5.3.5　コンピューターの手動追加」を参照してください。
管理対象外の コンピューターの追加	ROUGE（管理外）コンピューターのリストが追加された状態で「デバイスの追加」画面が表示されます。 画面の詳細は、「5.3.5　コンピューターの手動追加」を参照してください。
新規同期タスク	「新しいサーバータスク」画面が表示されます。 画面の詳細は、「6.7.2　新しいサーバータスクの作成」を参照してください。

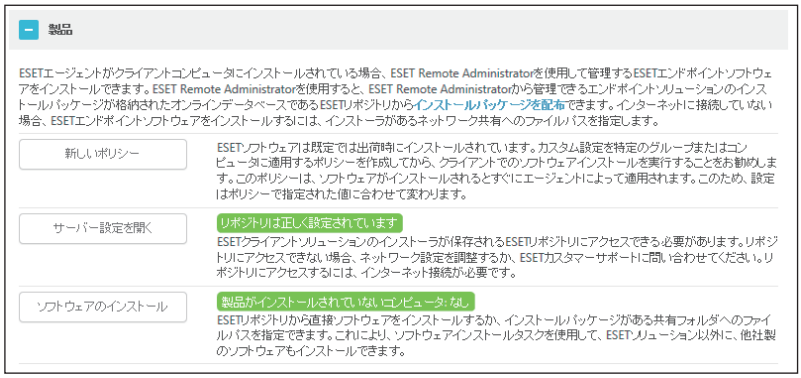
■エージェント

ESET Remote Administrator を使用して、コンピューターと ESET 製品を管理するには、ERA エージェントが必要です。ネットワークのコンピューターに ERA エージェントを展開するための要点が表示されます。

新しいポリシー	「新しいポリシー」画面が表示されます。 画面の詳細は、「6.5.2　新しいポリシーの作成」を参照してください。
エージェントの展開	「展開オプションを選択」画面が表示されます。 画面の詳細は、「4.2.2　ERA エージェントの展開」を参照してください。

■製品

ERA エージェントがクライアントコンピューターにインストールされている場合、ESET Remote Administrator を使用して ESET 製品のインストールやポリシー（設定）の適用を行うことができます。クライアントコンピューターを管理するための要点が表示されます。



新しいポリシー	「新しいポリシー」画面が表示されます。 画面の詳細は、「6.5.2　新しいポリシーの作成」を参照してください。
サーバー設定を開く	「サーバーの設定」画面が表示されます。 画面の詳細は、「6.11　サーバーの設定」を参照してください。
ソフトウェアのインストール	「クライアントタスク」画面が表示されます。「タスク」には［ソフトウェアインストール］が選択され、「ターゲット」には製品がインストールされていないコンピューターが追加されている状態で表示されます。 画面の詳細は、「6.6.2　新しいクライアントタスクの作成」と「6.6.3.1　ESET セキュリティ製品」の「■ソフトウェアインストール」を参照してください。

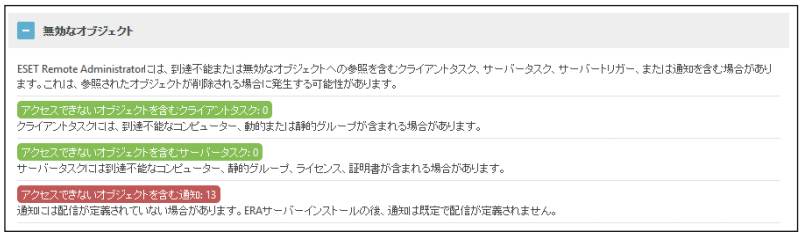
■ SMTP 設定

ESET Remote Administrator は、既存の SMTP サーバーに接続することにより、通知やレポートなどを電子メールで送信できます。SMTP サーバーに接続するための要点が表示されます。

サーバー設定を開く	「サーバーの設定」画面が表示されます。 画面の詳細は、「6.11　サーバーの設定」を参照してください。

■無効なオブジェクト

到達不能または無効なオブジェクトへの参照を含むクライアントタスク、サーバータスク、サーバートリガー、および通知のリストを表示できます。



アクセスできないオブジェクトを含むクライアントタスク	ESET Remote Administrator のクライアントタスクが表示されます。画面の詳細は、「6.6　クライアントタスク」を参照してください。
アクセスできないオブジェクトを含むサーバータスク	「サーバータスク - すべてのタスクタイプ」が表示されます。画面の詳細は、「6.7　サーバータスク」を参照してください。
アクセスできないオブジェクトを含む通知	「通知」が表示されます。画面の詳細は、「6.8　通知」を参照してください。

6.2 動的グループテンプレート

ある特定の条件に合致するコンピューターをグループに配置したい場合は、その特定の条件を設定した動的グループを作成します。特定の条件を動的グループに設定するには、定義済みルールを使用して動的グループテンプレートを作成する必要があります。各テンプレートは 1 つまたは複数のルールから構成されます。
動的グループには、次のような状態で配置されます。

- クライアントコンピューターの現在の状態を ERA エージェントに保存します。
- クライアントコンピューターが ESET Remote Administrator に接続するたびに、動的グループテンプレートで定義された条件が評価され、条件を満たす場合に動的にそのグループに割り当てられます。
- 動的グループは、コンピューターの状態に基づいてフィルタリングされています。1 台のコンピューターに複数のフィルタが適用される場合があり、複数の動的グループを割り当てることができます。

6.2.1 動的グループテンプレート画面の構成

「動的グループテンプレート」画面の構成について説明します。

1	**テンプレートリスト**	すべてのテンプレートのリストが表示されます。		
2	**新規テンプレート**	新しく動的グループテンプレートを作成します。「新規テンプレート」画面が表示されます。画面の詳細は「6.2.2 新しい動的グループテンプレートの作成」を参照してください。		
3	**テンプレートの編集**	選択しているテンプレートを編集します。「動的グループテンプレートの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいテンプレートとして保存することができます。 画面の詳細は「6.2.2 新しい動的グループテンプレートの作成」を参照してください。		
4	**削除**	選択しているテンプレート（複数選択可）を完全に削除します。		
5	**複製**	選択しているテンプレートの内容をコピーした状態で「新規テンプレート」画面が表示されます。画面の詳細は「6.2.2 新しい動的グループテンプレートの作成」を参照してください。		
6	**「動的グループテンプレート」コンテキストメニュー**	動的グループテンプレートリストから選択しているテンプレートに使用できるメニューが表示されます。		
			詳細	選択しているテンプレートの「クライアントタスク詳細－サマリー」画面が表示されます。

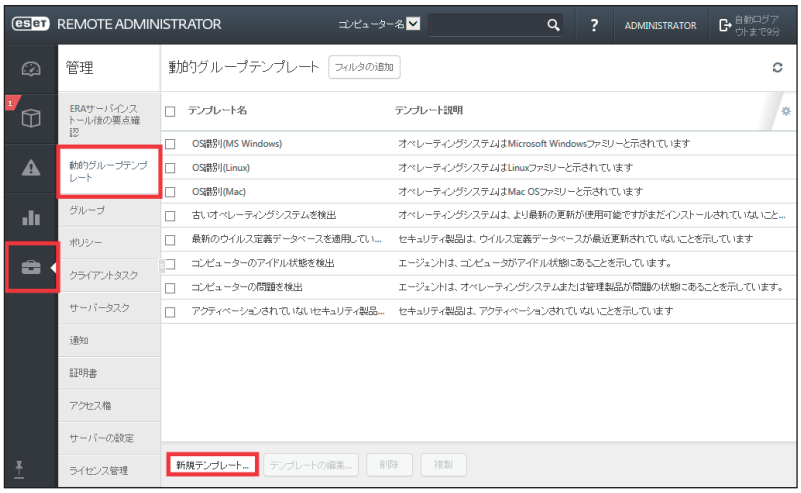
6	「動的グループテンプレート」コンテキストメニュー		編集	選択しているテンプレートを編集します。「動的グループテンプレートの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいテンプレートとして保存することができます。 画面の詳細は「6.2.2　新しい動的グループテンプレートの作成」を参照してください。
			複製	選択しているテンプレートの内容をコピーした状態で「新規テンプレート」画面が表示されます。 画面の詳細は「6.2.2　新しい動的グループテンプレートの作成」を参照してください。
			削除	選択しているテンプレートを完全に削除します。
			アクセスグループ	選択したテンプレートを特定の動的グループに移動できます。サブメニューから［移動］をクリックすると、グループの選択画面が表示されます。移動先グループを選択し、［OK］をクリックすると、選択したグループにテンプレートが移動します。

6.2.2　新しい動的グループテンプレートの作成

新しい動的グループテンプレートを作成するには、2 種類の方法があります。

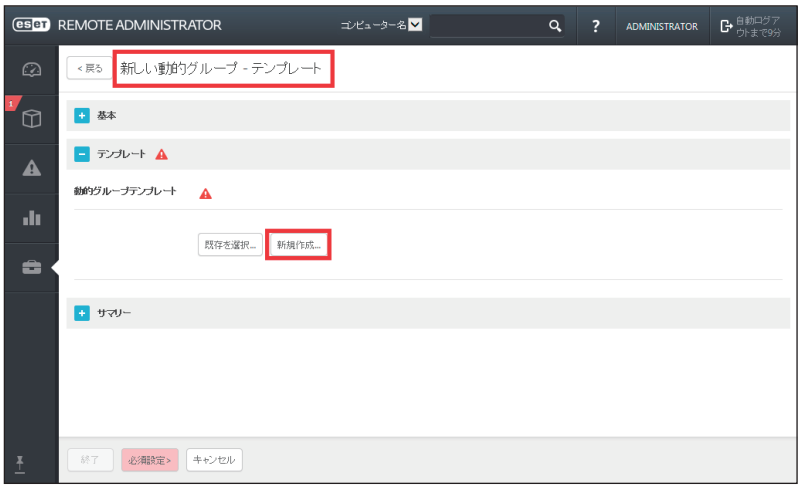
■「動的グループテンプレート」画面から作成する

・［管理］メニュー > ［動的グループテンプレート］サブメニュー > ［新規テンプレート］ボタンをクリックします。



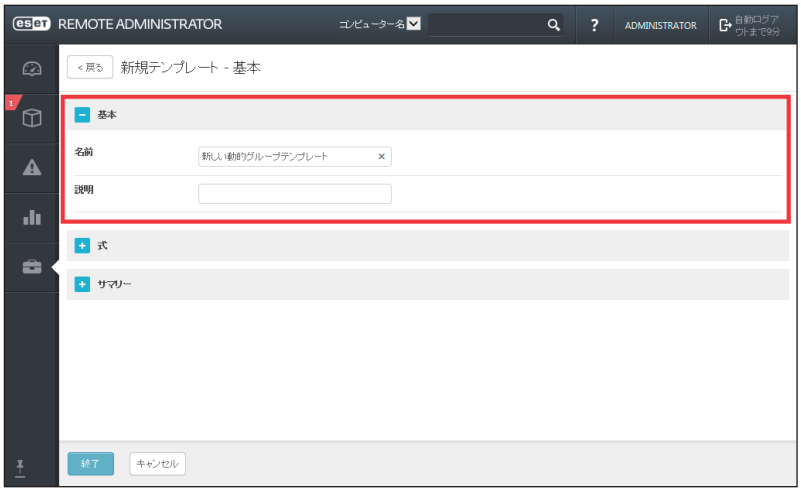
■「新しい動的グループの作成」画面または「動的グループの編集」画面から作成する

- 画面の表示方法については、「6.3.2.2 新しい動的グループの作成」を参照してください。



操作手順

1. いずれかの方法で「新規テンプレート」画面を表示します。
2. 「基本」の各項目を入力します。



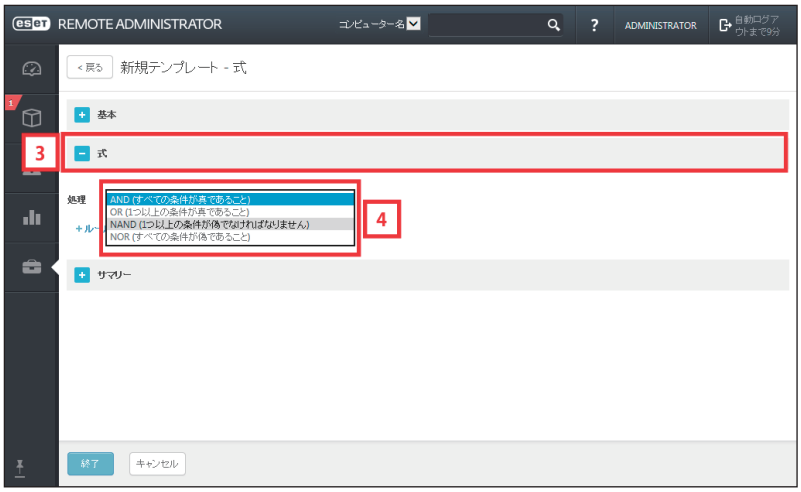
■基本

項目名	説明	必須
名前	作成する動的グループテンプレートの名前を入力します。画面には、ここで設定した名前が表示されます。	○
説明	作成する動的グループテンプレートの説明を入力します。	-

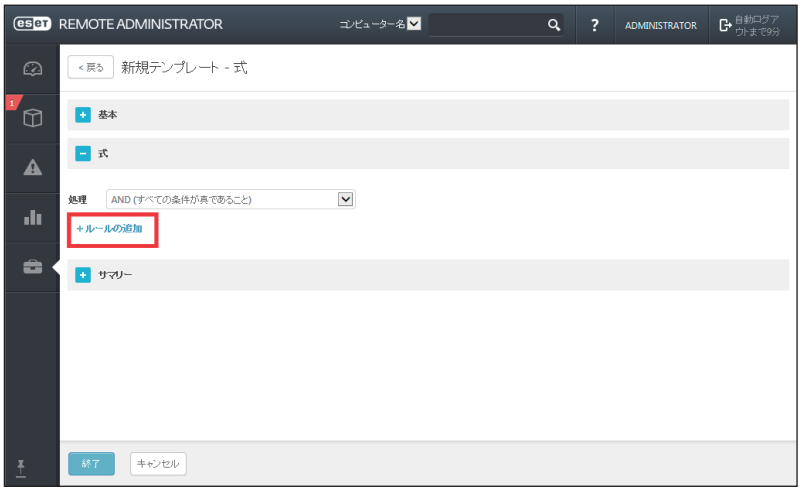
続く

3 ［式］をクリックします。

4 「処理」を選択します。



5 ［ルールの追加］をクリックします。

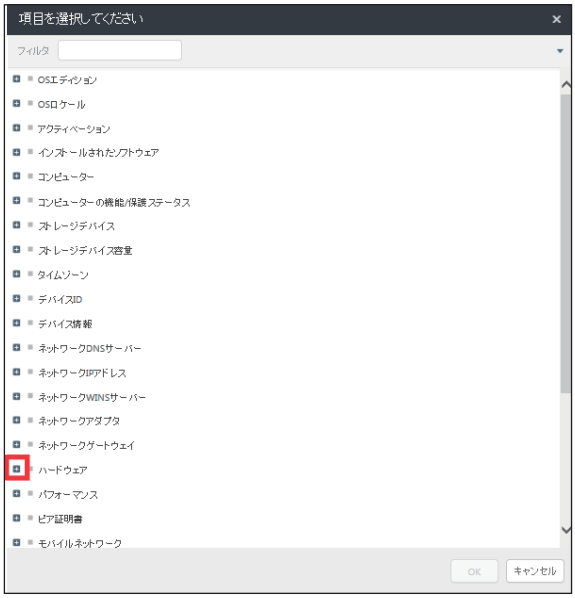


ルールを選択する画面が表示されます。

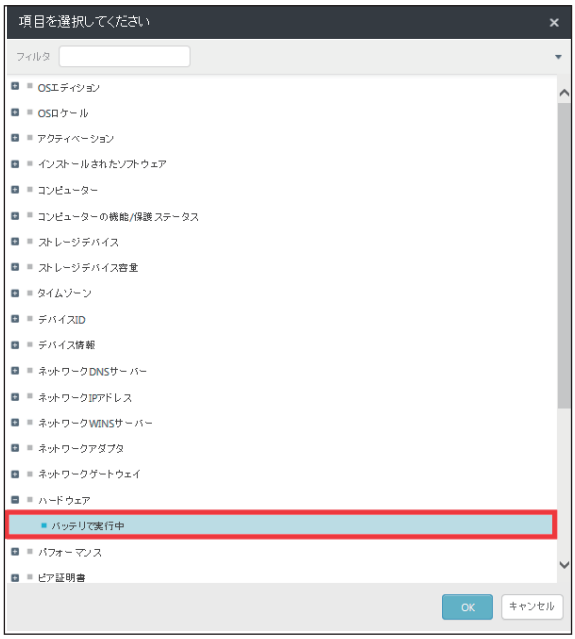
続く

6 追加するカテゴリの ⊞ をクリックします。

項目リストが表示されます。



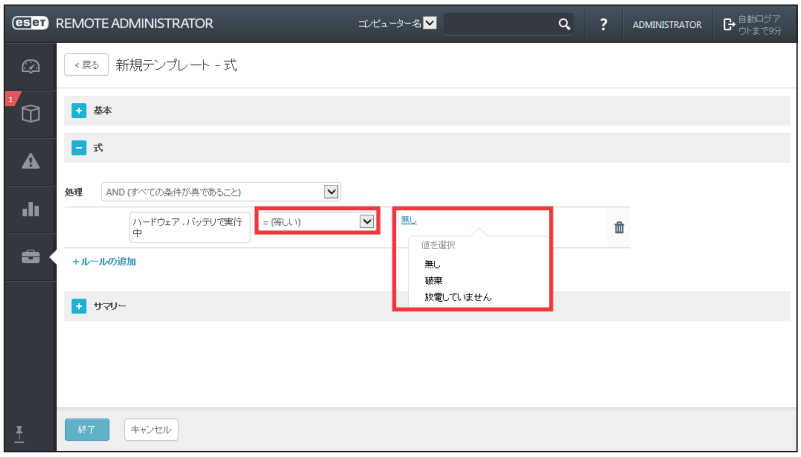
7 追加する項目を選択します。



8 [OK] ボタンをクリックします。

続く

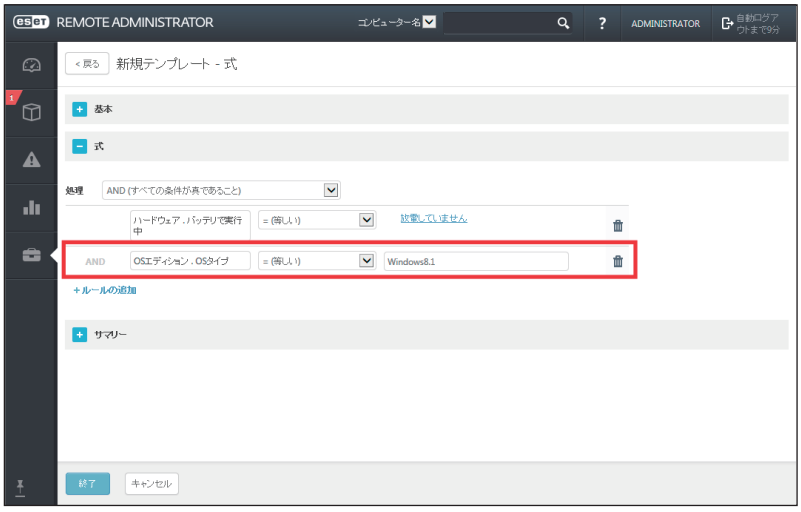
9 追加したルールの「条件」を選択または入力し、ルールと条件に関する「演算子」を選択します。



■式

項目名	説明		必須
処理	ルールに追加する処理の論理演算子を選択します。		○
ルールの追加	［+ルールの追加］をクリックし、項目リストから条件に合った項目を選択します。		-
	ルール名	リストから選択したカテゴリと項目名が表示されます。	-
	論理演算子	追加したルールと右側で指定する条件との関係を選択します。 演算子と設定に関しては「6.7.4.1　各トリガータイプの設定項目」の「・ルールエディタ」を参照してください。	○
	条件	ルールに対する条件を選択または入力します。 ・ワイルドカード「＊」（アスタリスク）、「?」（クエスチョン）が使えます。	○
	削除	追加したルールを削除します。	-

10 複数のルールを追加する場合は、手順 5 ～手順 9 を繰り返します。



続く

⑪［サマリー］をクリックします。

「基本」および「式」に入力した内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。

⑫［終了］ボタンをクリックします。

「動的グループテンプレート」画面のテンプレートリストに、作成した動的グループテンプレートが表示されます。

ワンポイント

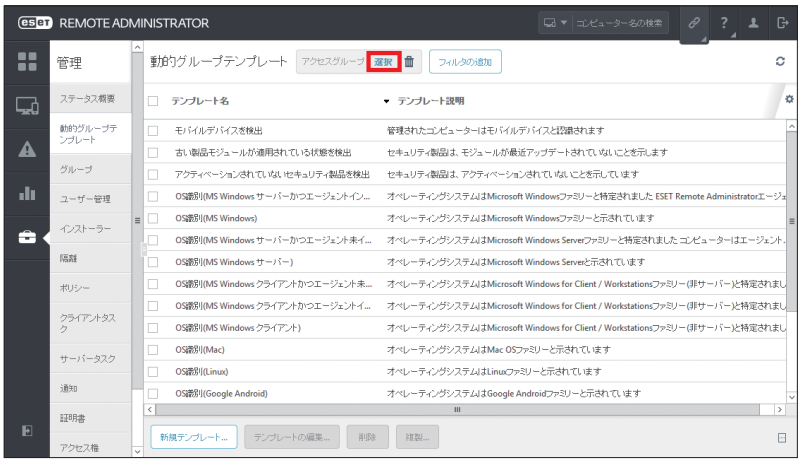
作成した動的グループテンプレートは、複数の動的グループに適用できます。
動的グループに動的グループテンプレートを適用する方法については、「6.3.2.2 新しい動的グループの作成」を参照してください。

■アクセスグループを切り替える

特定のグループ向けに作成された動的グループテンプレートを表示したいときは、以下の手順でアクセスグループを切り替えます。

操作手順

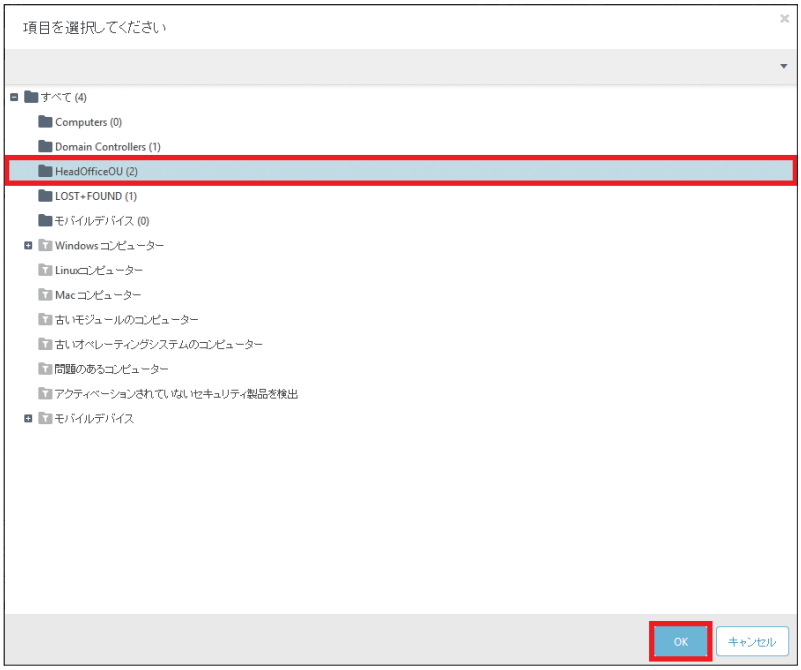
①「アクセスグループ」の［選択］をクリックします。



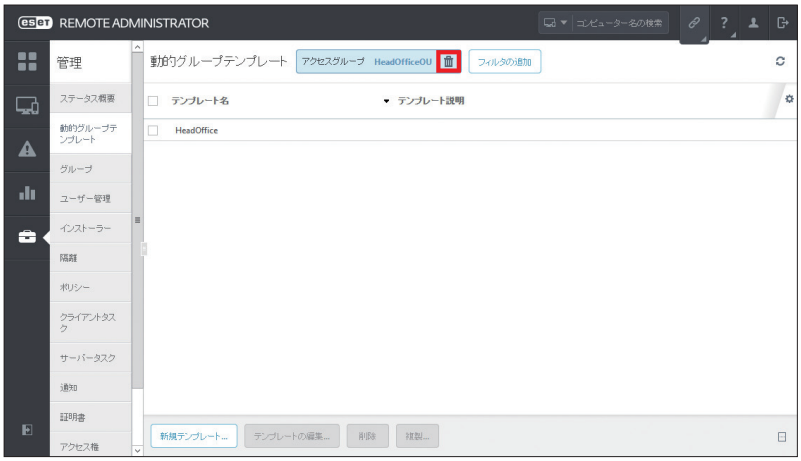
「項目を選択してください」画面が表示されます。

続く

2 表示したいグループを選択し、［OK］をクリックします。



3 選択したグループ用の動的グループテンプレートが表示されます。アクセスグループの選択を解除したいときは、🗑をクリックします。



ワンポイント

［フィルタの追加］を利用すると、「名前」または「説明」による動的テンプレートの絞り込みが行えます。［フィルタの追加］をクリックして、フィルター条件を選択する画面が表示されたら、フィルター条件を選択し、［OK］をクリックすると、フィルター条件の入力ボックスが表示されます。入力ボックスにキーワードを入力して、「Enter」キーを押すと、絞り込みが行われます。

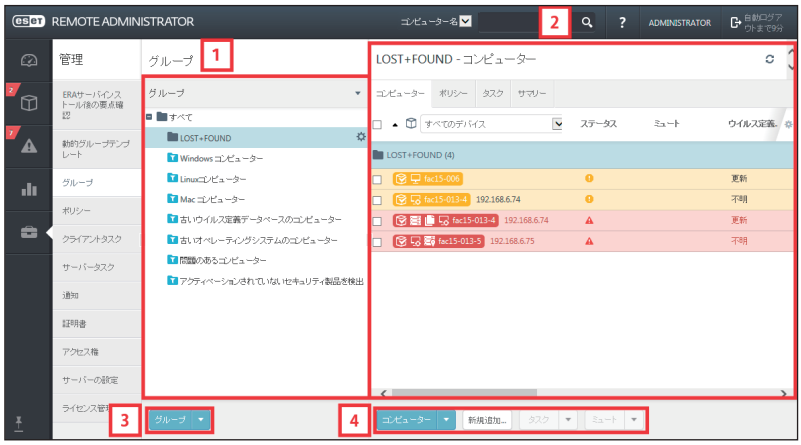
6.3 グループ

クライアントコンピューターをグループに配置することで、コンピューターの管理と分類が効率よく行えます。定義済みのグループおよびグループテンプレートを使用して、新しくグループを作成することもできます。
クライアントグループには 2 種類あります。

静的グループ	静的グループは、クライアントコンピューターの追加／削除を手動で行い、明示的に管理するクライアントグループです。静的グループは 1 つだけ属することができます（複数の静的グループに属することはできません）。 既定の静的グループは次の 2 種類です。 • 「すべて」グループ： ERA サーバーネットワーク内のすべてのコンピューターのメイングループです。各コンピューターに既定のポリシーを適用する際に使用されます。グループは常に表示され、グループ名を変更することはできません。 • 「LOST+FOUND」グループ： 初めて ERA サーバーに接続し、静的グループを定義していないコンピューターは、自動的にこのグループに属します。グループ名は変更できますが、削除または移動はできません。
動的グループ	動的グループは、特定の条件で定義され、条件を満たすクライアントコンピューターが自動的に追加／削除されるクライアントグループです。複数の動的グループに属することができます。 特定の条件は、動的グループテンプレートにルールとして定義します。クライアントコンピューターは ERA エージェントでフィルタリングされるため、追加情報を EAR サーバーに転送する必要はありません。ERA エージェントは、クライアントコンピューターが属する動的グループを、独自に判断し ERA サーバーに通知します。 一部の定義済み動的グループは、ESET Remote Administrator をインストールした後に使用できます。必要に応じて新しく動的グループを作成します。作成時には、まずテンプレートを作成し、次に新しく動的グループを作成します。

6.3.1 グループ画面の構成

「グループ」画面の構成について説明します。

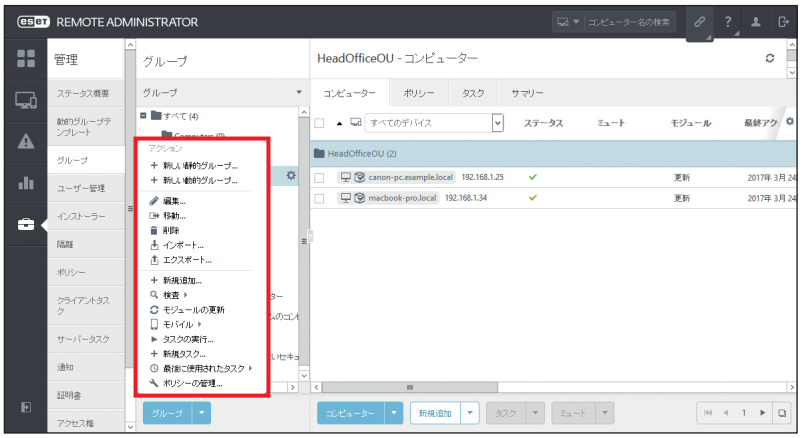


1	**グループリスト**	すべてのグループのリストが表示されます。 • 静的グループは黒色のフォルダで表示されます。 • 動的グループは青色のフォルダで表示されます。	
2	**選択中グループの詳細**	グループリストから選択しているグループの詳細が表示されます。	
		「コンピューター」タブ	グループメンバーのコンピューターのリストが表示されます。 画面の詳細は、「6.3.5.1 「コンピューター」タブ画面の構成」を参照してください。
		「ポリシー」タブ	グループに割り当てられたポリシーのリストが表示されます。 画面の詳細は、「6.3.6.1 「ポリシー」タブ画面の構成」を参照してください。
		「タスク」タブ	グループに割り当てられたタスクのリストが表示されます。 画面の詳細は、「6.3.6.2 「タスク」タブ画面の構成」を参照してください。
		「サマリー」タブ	名前、説明、グループ階層などの概要が表示されます。 画面の詳細は、「6.3.6.3 「サマリー」タブ画面の構成」を参照してください。
3	**グループ**	新しいグループの作成や選択中のグループの編集、削除などのアクションメニューが表示されます。 表示されるアクションの詳細は、「■［グループ］ボタンとコンテキストメニューのアクション」を参照してください。	
4	**2 の各タブで使用するボタン**	2 の各タブに応じて、表示されるボタンが変わります。 表示されるボタンの詳細は、「6.3.5.1 「コンピューター」タブ画面の構成」「6.3.6.1 「ポリシー」タブ画面の構成」「6.3.6.2 「タスク」タブ画面の構成」「6.3.6.3 「サマリー」タブ画面の構成」を参照してください。	

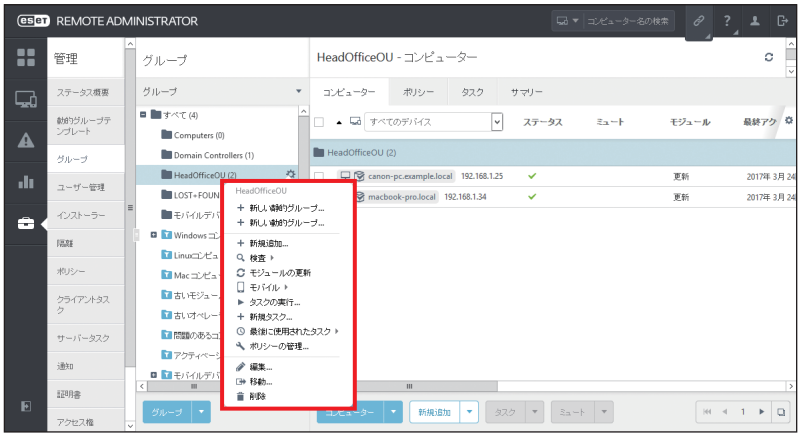
［グループ］ボタンとコンテキストメニューのアクション

［グループ］ボタンとコンテキストメニューに表示されるアクションについて説明します。

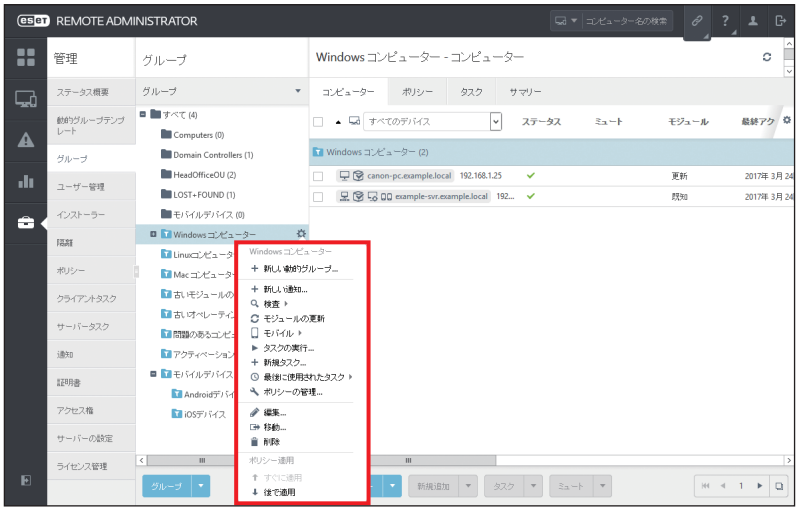
- ［グループ］ボタンのメニュー



- 静的グループのコンテキストメニュー



- 動的グループのコンテキストメニュー



	新しい静的グループ	静的グループを選択している場合に使用できます。 新しい静的グループを作成します。「新しい静的グループ」画面が表示されます。 画面の詳細は、「6.3.2.1　新しい静的グループの作成」を参照してください。
	新しい静的グループ	新しい動的グループを作成します。「新しい動的グループ」画面が表示されます。 画面の詳細は、「6.3.2.2　新しい動的グループの作成」を参照してください。
	編集	選択しているグループを編集します。「静的または動的グループの編集」画面が表示されます。 画面の詳細は、「6.3.2.1　新しい静的グループの作成」または「6.3.2.2　新しい動的グループの作成」を参照してください。
	移動	選択しているグループを別グループの子グループとして移動します。 ※静的グループの移動先は、静的グループのみ指定できます。 操作については、「6.3.3　グループの移動」を参照してください。
	削除	選択しているグループを完全に削除します。
	インポート	選択しているグループに、テキストファイル（.txt）などで作成されたコンピューターのリストをインポートします。「クライアントのインポート」画面が表示されます。 追加するコンピューターが既にグループに存在する場合は、選択したオプションに基づいて競合を解決します。 操作については、「6.3.4.2　クライアントコンピューターのインポート」を参照してください。
		競合するデバイスをスキップ：静的グループが存在し、テキストファイル（.txt）に記載されているコンピューターがグループに既に存在する場合、そのコンピューターはスキップされ、インポートされません。これに関する情報が表示されます。
		他のグループから競合するデバイスを移動：静的グループが存在し、テキストファイル（.txt）に記載されているコンピューターがグループに既に存在する場合、インポート前にコンピューターを他の静的グループに移動する必要があり、インポート後、そのコンピューターは移動後の場所から元の場所に戻ります。
		競合しているデバイスの複製：静的グループが存在し、テキストファイル（.txt）に記載されているコンピューターがグループに既に存在する場合、そのコンピューターの複製が同じ静的グループ内に作成されます。元のコンピューターは、完全な情報と一緒に表示され、複製はコンピューター名のみ表示されます。
	エクスポート	静的グループを選択している場合に使用できます。 選択しているグループのメンバーをテキストファイル（.txt）のリストにエクスポートします。 ※親グループを選択している場合は、子グループメンバーのエクスポートを確認するメッセージが表示されます。 操作については、「6.3.4.1　クライアントコンピューターのエクスポート」を参照してください。
	新規追加	静的グループを選択している場合に使用できます。 選択している静的グループに新しいデバイスを追加します。「デバイスの追加」画面が表示されます。 画面の詳細は、「6.3.5.2　クライアントコンピューターの追加」を参照してください。

	検査	脅威を報告したクライアントでオンデマンド検査を実行するタスクをスケジュールします。定義済み検査プロファイルを使用してクライアントを検査します。スケジュールされた検査は「タスク」タブに表示されます。 画面の詳細は、「6.3.6.2 「タスク」タブ画面の構成」を参照してください。	
		駆除して検査する	感染したオブジェクトが検出された場合、自動的に駆除されます。
		駆除せずに検査する	感染したオブジェクトが検出された場合、隔離されます。
	モジュールの更新	モジュールのアップデートタスクをスケジュールします。スケジュールされたタスクは「タスク」タブに表示されます。画面の詳細は、「6.3.6.2 「タスク」タブ画面の構成」を参照してください。	
	モバイル	選択しているグループにモバイルデバイスを配置します。	
		登録	モバイルデバイスを登録します。「クライアントタスク」画面が表示されますので「モバイルデバイスコネクター」の設定を行います。
		検索	Android デバイスの GPS 座標を検索します。 ※ iOS デバイスでは使用できません。
		ロック	不審なアクティビティが検出されたり、デバイスを紛失した場合などに、モバイルデバイスをロックします。
		ロック解除	モバイルデバイスのロックが解除されます。
		警報	Android デバイスに対し、リモートで大音量の警報音をトリガーします。デバイスがミュートに設定されていても、警報音が作動します。 ※ iOS デバイスでは使用できません。
		ワイプ	Android デバイスに保存されているアクセス可能なデータが完全に消去されます。 ※ iOS デバイスでは使用できません。
	新規タスク	選択しているグループに新しいクライアントタスクを作成します。「ターゲット」に選択しているグループが追加されている状態で、「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。	
	最後に実行されたタスク	最後に実行されたタスクを再度、実行できます。	
	ポリシーの管理	選択しているグループにポリシーを割り当てます。「ポリシーアプリケーション順序」画面が表示されます。 画面の詳細は、「6.5.5.2 複数のポリシーを適用順にグループに割り当てる」の「■ポリシーアプリケーション順序画面」を参照してください。	
	すぐに適用	動的グループのコンテキストメニューから使用できます。 グループリストの表示順を繰り上げます。	
	後で適用	動的グループのコンテキストメニューから使用できます。 グループリストの表示順を繰り下げます。	

6.3.2 新しいグループの作成

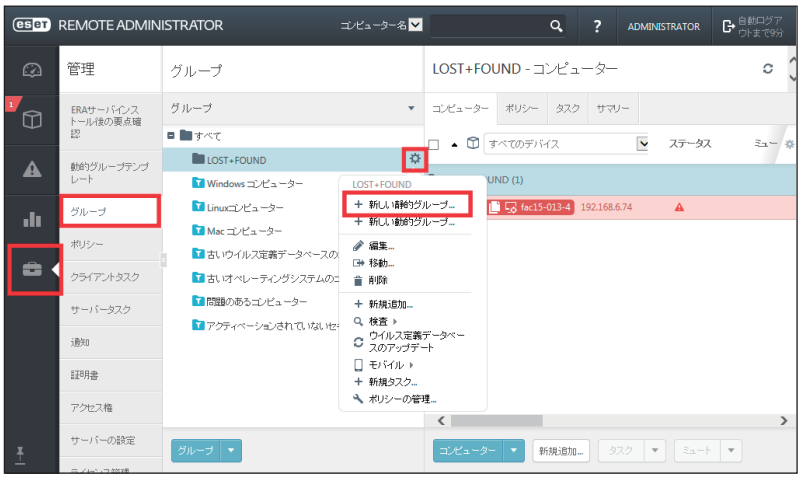
静的グループまたは動的グループを新しく作成する方法を説明します。

6.3.2.1 新しい静的グループの作成

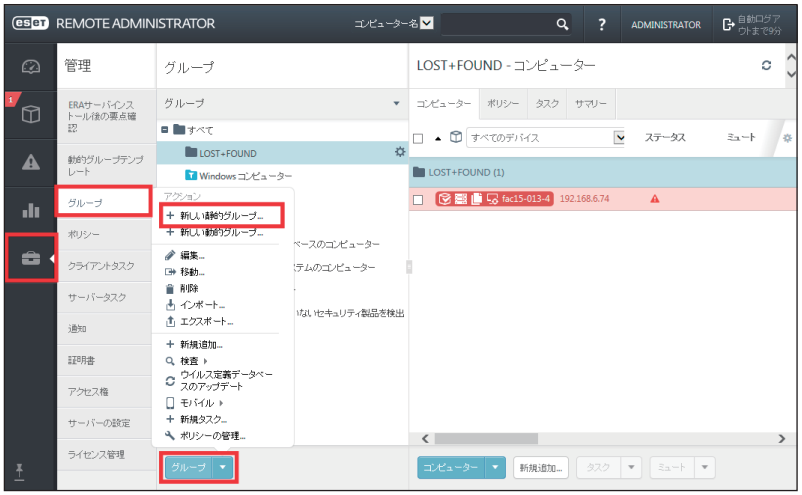
新しい静的グループを作成するには、3 種類の方法があります。

■「管理」メニューから作成する

- ［グループ］> 親グループに指定する静的グループを選択 > ⚙ >［新しい静的グループ］を選択します。

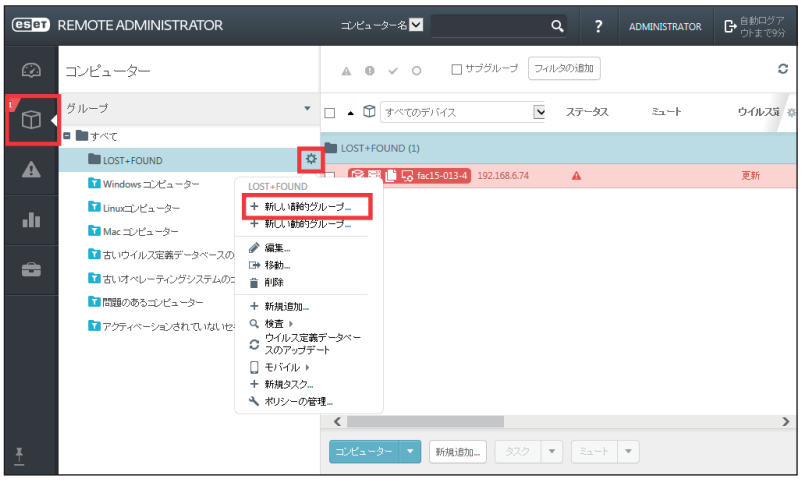


- ［グループ］> 親グループに指定する静的グループを選択 >［グループ］ボタン >［新しい静的グループ］を選択します。



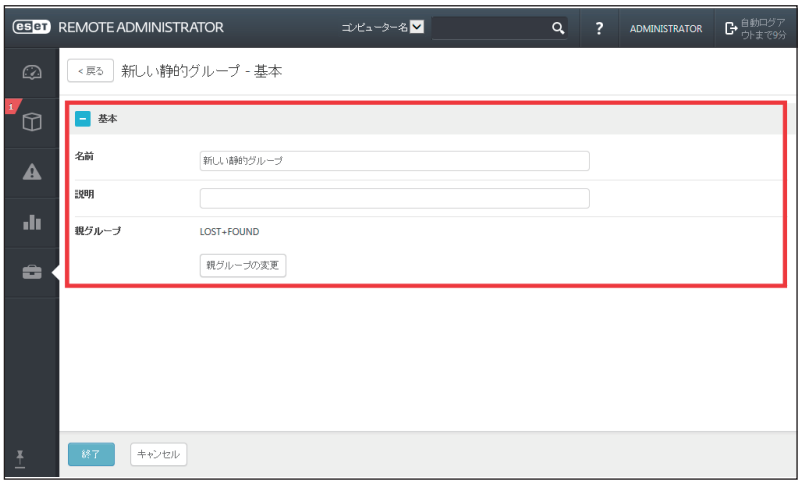
■「コンピューター」メニューから作成する

- 親グループに指定する静的グループを選択 > ⚙ > [新しい静的グループ] を選択します。



操作手順

1. いずれかの方法で「新しい静的グループ」画面を表示します。
2. 各項目を入力します。



■基本

項目名	説明	必須
名前	作成する動的グループテンプレートの名前を入力します。画面には、ここで設定した名前が表示されます。	○
説明	作成する静的グループの説明を入力します。	-
親グループ※ 1	作成する静的グループの親グループを選択します。既定では、新しい静的グループの作成時に選択しているグループが表示されます。親グループを変更する場合は、[グループの変更] ボタンをクリックし、ツリーから親グループを選択します。	○

！重　要

※ 1　静的グループの親グループは、静的グループである必要があります。これは、動的グループには静的グループを含めることができないためです。

3 ［終了］ボタンをクリックします。

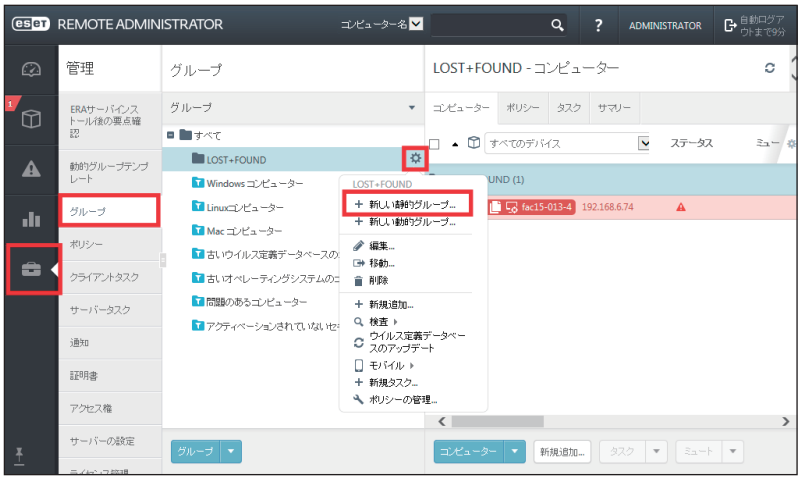
指定した親グループの配下に、作成した静的グループが表示されます。

6.3.2.2　新しい動的グループの作成

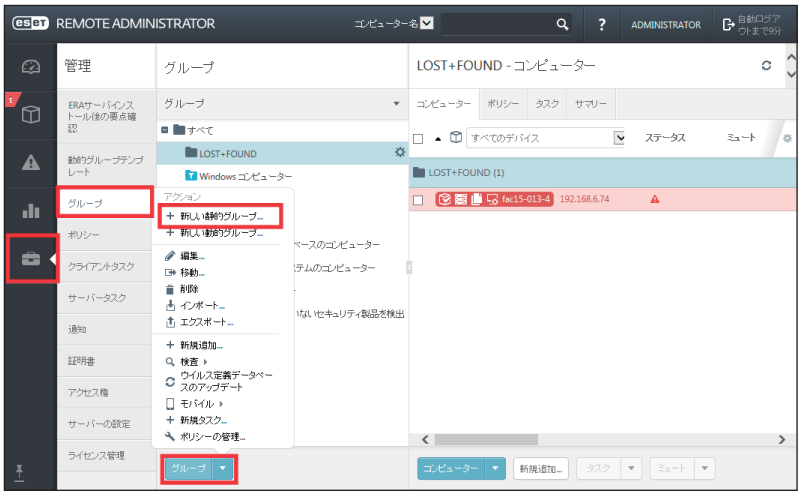
新しい動的グループを作成するには、3 種類の方法があります。

■「管理」メニューから作成する

- ［グループ］> 親グループに指定するグループを選択 > ⚙ > ［新しい動的グループ］を選択します。



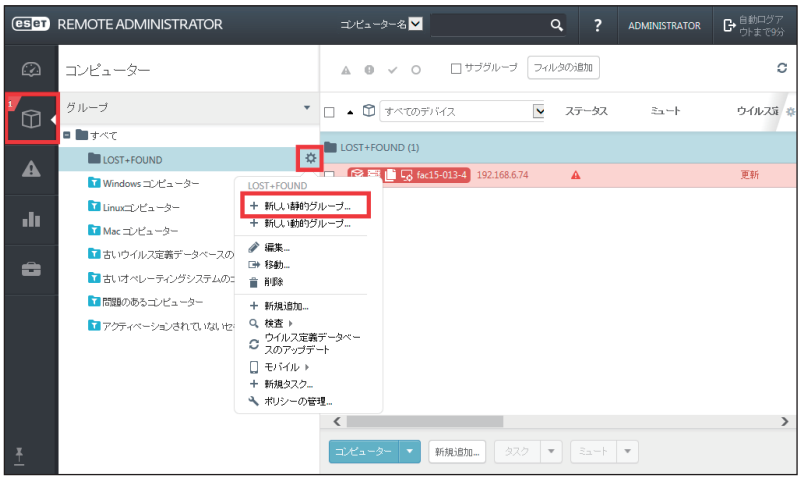
- ［グループ］> 親グループに指定するグループを選択 > ［グループ］ボタン > ［新しい動的グループ］を選択します。



続く

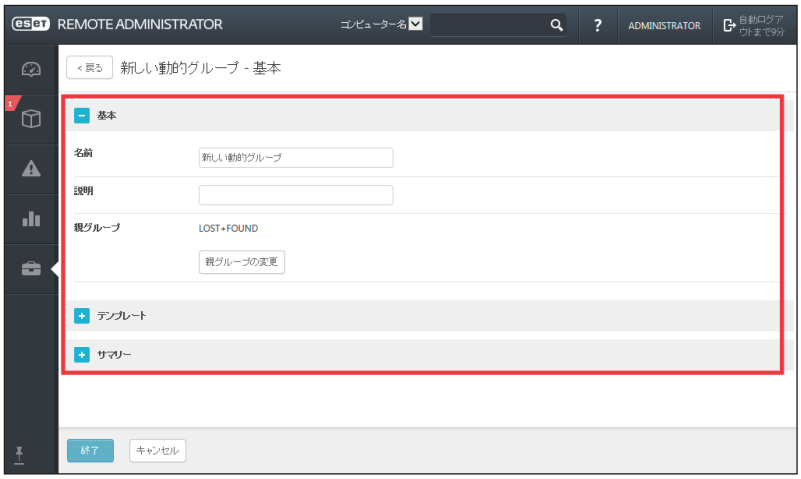
■「コンピューター」メニューから作成する

- 親グループに指定するグループを選択 > ⚙ > [新しい動的グループ] を選択します。



操作手順

1. いずれかの方法で「新しい動的グループ」画面を表示します。
2. 各項目を入力します。



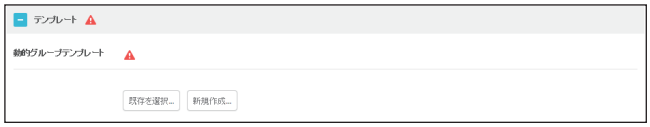
■基本

項目名	説明	必須
名前	作成する動的グループの名前を入力します。画面には、ここで設定した名前が表示されます。	○
説明	作成する動的グループの説明を入力します。	-
親グループ※ 1	作成する動的グループの親グループを選択します。既定では、新しい動的グループの作成時に選択しているグループが表示されます。親グループを変更する場合は、[グループの変更] ボタンをクリックし、ツリーから親グループを選択します。	○

!重 要

※ 1 動的グループは、静的グループまたは動的グループに属することができます。ただし、最上位のグループは常に静的です。
特定の静的グループの下の動的グループは、ツリーの階層の深さに関係なく、静的グループのコンピューターだけをフィルタリングします。さらにネストされた動的グループの場合、さらに下の階層の動的グループは上のグループの結果をフィルタリングします。

■テンプレート



項目名	説明		必須
動的グループテンプレート	動的グループを作成するにはテンプレートを選択します。テンプレートを選択するには、2 種類の方法があります。		○
	既定を選択	定義済みのテンプレートまたは既に作成したテンプレートのリストが表示されますので、該当するものを選択します。	-
	新規作成	既定のリストのいずれも適していない場合は、新しいテンプレートを作成し、適用します。 新しいテンプレートの作成方法については、「6.2.2 新しい動的グループテンプレートの作成」を参照してください。	-

■サマリー

「基本」および「テンプレート」に入力した内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。

3 ［終了］ボタンをクリックします。

指定した親グループの配下に、作成した動的グループが表示されます。

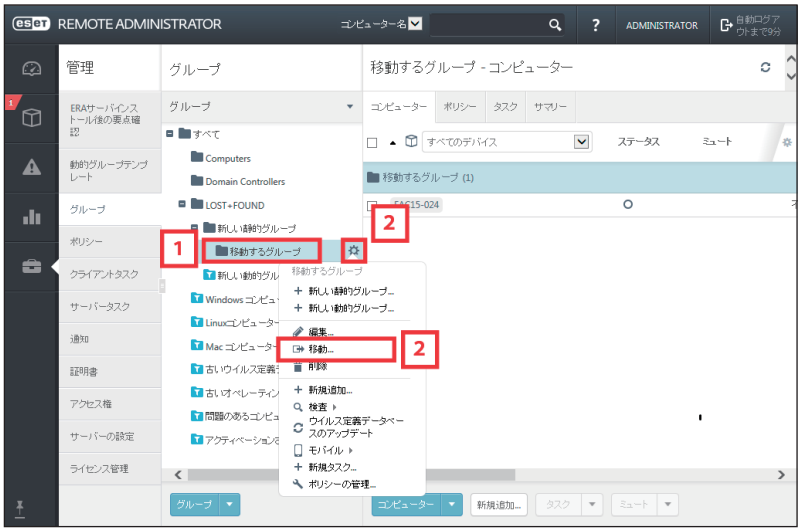
続く

6.3.3 グループの移動

選択しているグループを別のグループに移動することができます。移動したグループはそのグループのサブフォルダになります。

操作手順

1. グループリストから移動するグループを選択します。
2. ⚙ をクリックし、［移動］を選択します。



グループリストが表示されます。

3. 移動先のグループを選択します。

4. ［OK］ボタンをクリックします。

移動先に指定したグループのサブフォルダとして表示されます。

！重 要

静的グループは、動的グループに移動できません。定義済み静的グループ（「LOST+FOUND」など）は、他のグループに移動できません。

ワンポイント

移動した動的グループは、移動前の場所に関係なく、テンプレートに基づきクライアントコンピューターをフィルタリングします。

6.3.4 静的グループのエクスポート／インポート

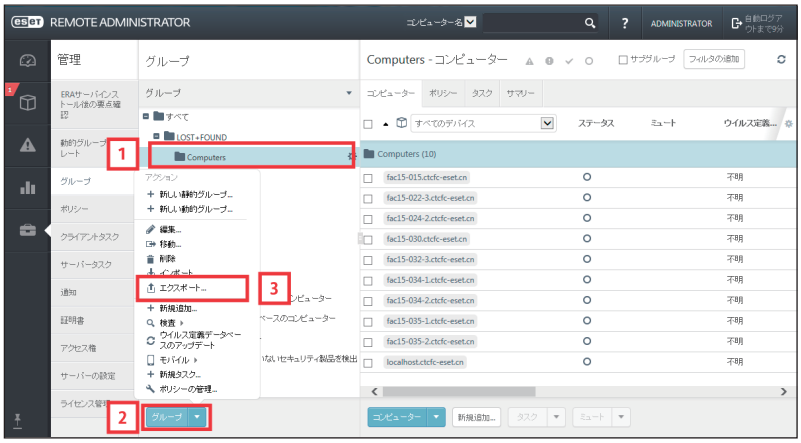
ERA の構造内にあるコンピューターリストはエクスポートすることができます。リストをエクスポートし、バックアップとして保存すると、グループ構造を復元する場合などに、後からリストをインポートすることができます。

6.3.4.1 クライアントコンピューターのエクスポート

選択しているグループおよび子グループに属しているコンピューターリストをテキストファイル（.txt）にエクスポートします。

操作手順

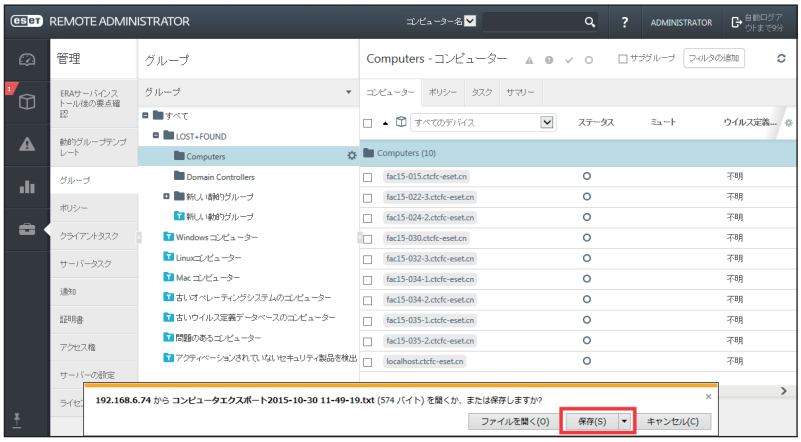
1. グループリストからエクスポートするグループを選択します。
2. ［グループ］ボタンをクリックします。
3. ［エクスポート］を選択します。



保存の確認メッセージが表示されます。

続く

4 ［保存］ボタンをクリックします。



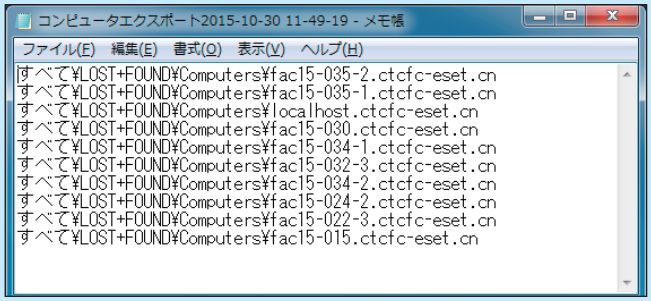
クライアントコンピューターのリストがテキストファイルにエクスポートされます。

！重　要

動的グループは、動的グループテンプレートで定義された条件に合ったコンピューターへのリンクに過ぎないため、エクスポートできません。

ワンポイント

エクスポートされたテキストファイルには、最上位グループからのパスが書き出されます。



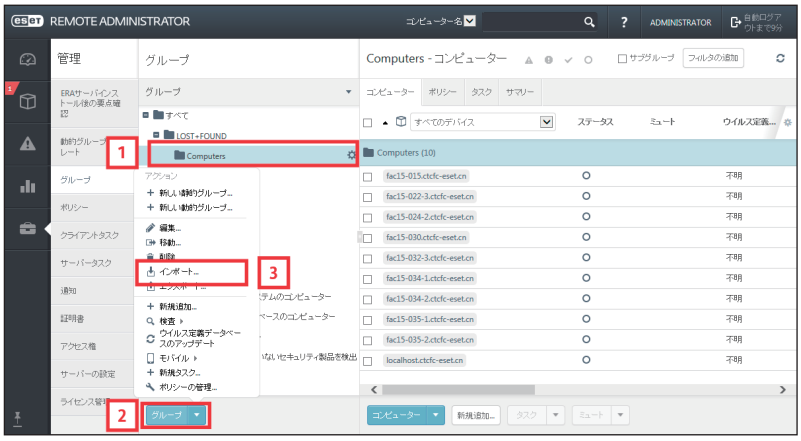
続く

6.3.4.2 クライアントコンピューターのインポート

静的グループからエクスポートしたテキストファイル（.txt）は、ERA コンソールに再度インポートすることができ、既存のグループ構造に含めることができます。

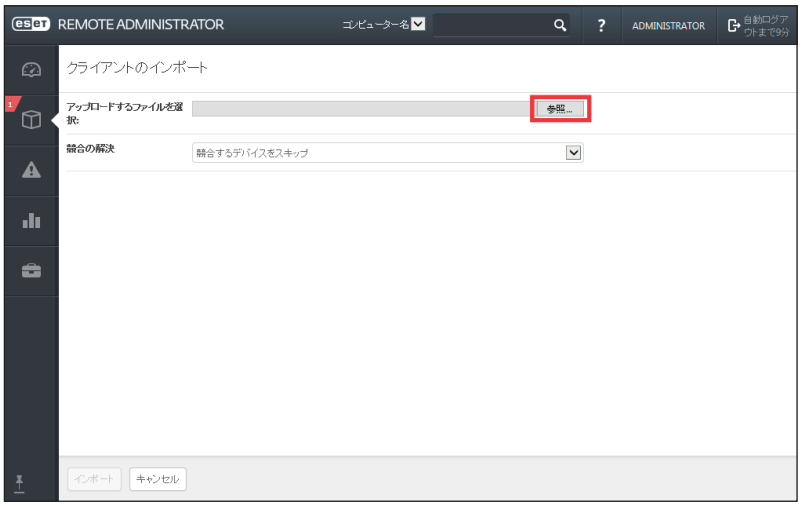
操作手順

1. グループリストからインポートするグループを選択します。
2. ［グループ］ボタンをクリックします。
3. ［インポート］を選択します。

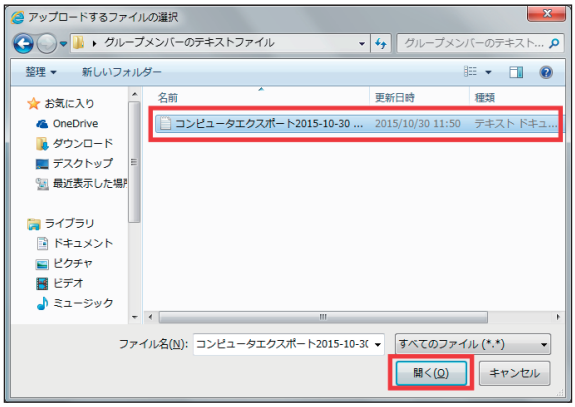


「クライアントのインポート」画面が表示されます。

4. 「アップロードするファイルを選択」の［参照］ボタンをクリックします。

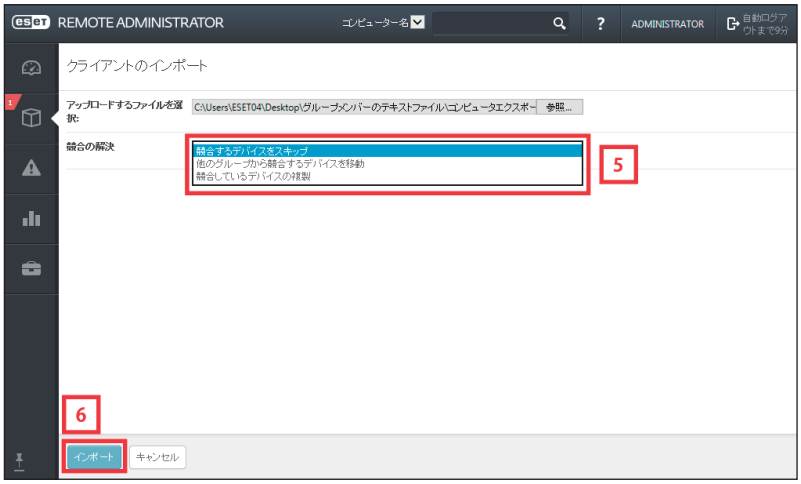


5 アップロードするファイルを選択し、［開く］ボタンをクリックします。



6 「競合の解決」を選択します。

7 ［インポート］ボタンをクリックします。



クライアントコンピューターのリストがインポートされます。

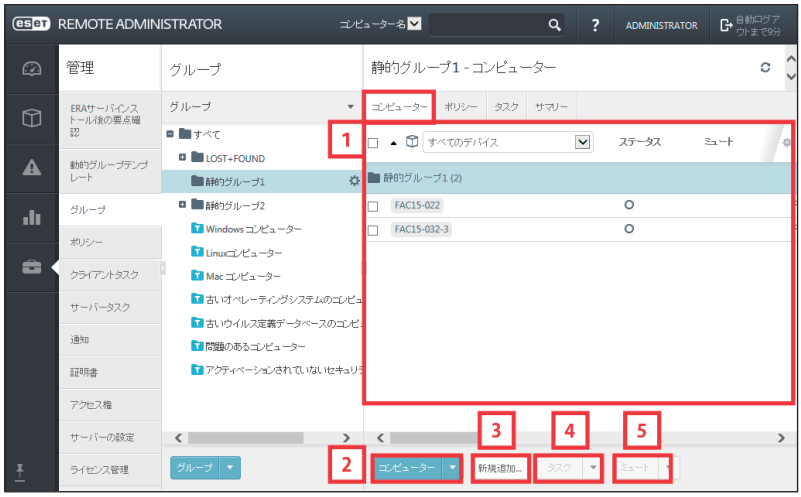
続く

6.3.5 静的グループへのクライアントコンピューターの追加

特定の静的グループへクライアントコンピューターを配置するには、手動で追加する必要があります。

6.3.5.1 「コンピューター」タブ画面の構成

「コンピューター」タブには、選択しているグループに属しているクライアントコンピューターのリストが表示されます。クライアントコンピューターの詳細情報の確認や新規追加、削除などが行えます。

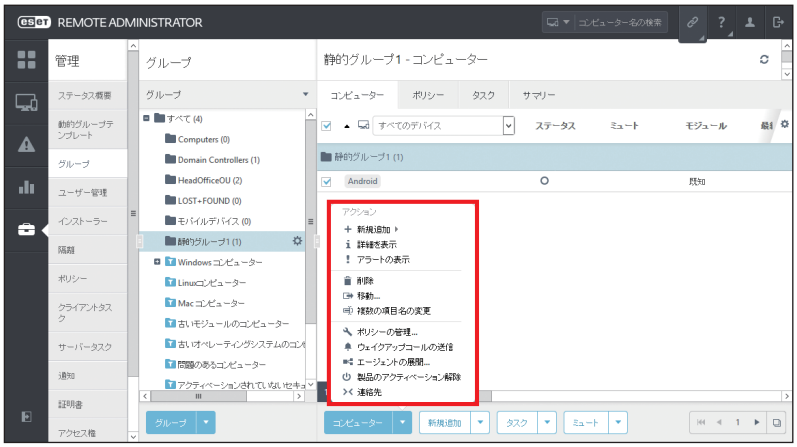


1	コンピューターリスト	グループリストから選択しているグループに割り当てられたクライアントコンピューターリストが表示されます。
2	コンピューター	コンピューターリストから選択しているクライアントコンピューターに使用できるアクションが表示されます。 表示されるアクションの詳細は、「■［コンピューター］ボタンとコンテキストメニューおよび［タスク］ボタンのアクション」を参照してください。
3	新規追加	静的グループを選択している場合に使用できます。 選択している静的グループに新しいデバイスを追加します。「デバイスの追加」画面が表示されます。 画面の詳細は、「6.3.5.2　クライアントコンピューターの追加」を参照してください。
4	タスク	コンピューターリストから選択しているクライアントコンピューターにスケジュールできるタスクのアクションが表示されます。 表示されるアクションの詳細は、「■［コンピューター］ボタンとコンテキストメニューおよび［タスク］ボタンのアクション」を参照してください。
5	ミュート	選択しているクライアントコンピューターの ERA エージェントから ESET Remote Administrator への通知を停止します。情報の集約だけが行われます。
	ミュート解除	ESET Remote Administrator への報告を再開します。

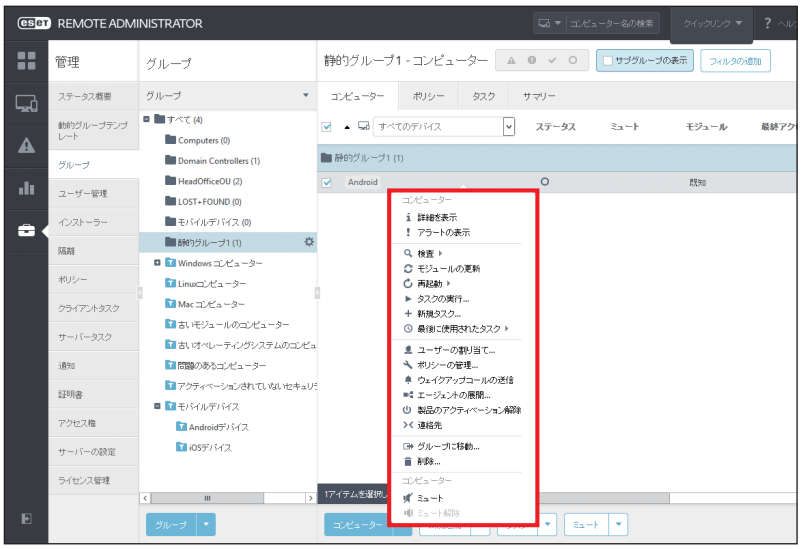
■［コンピューター］ボタンとコンテキストメニューおよび［タスク］ボタンのアクション

［コンピューター］ボタンと「コンピューター」コンテキストメニュー、および［タスク］ボタンのアクションについて説明します。

- ［コンピューター］ボタンのメニュー



- 「コンピューター」コンテキストメニュー



- ［タスク］ボタン

	新規追加	グループリストから静的グループを選択している場合に使用できます。選択している静的グループに新しいコンピューターまたはモバイルデバイスを手動で追加できます。追加するデバイスは、サブメニューから選択できます。コンピューターをクリックすると、「デバイスの追加」画面が表示されます。モバイルデバイスをクリックすると、「モバイルデバイスの追加」画面が表示されます。 画面の詳細は、「6.3.5.2　クライアントコンピューターの追加」を参照してください。
	詳細を表示	選択しているクライアントコンピューターの情報を確認します。「コンピュータ詳細」画面が表示されます。 画面の詳細は、「5.3.4　クライアントコンピューターの詳細確認画面」を参照してください。
	アラートの表示	クライアントコンピューターで発生している問題と発生日時、重要度などが表示されます。 画面の詳細は、「5.3.4　クライアントコンピューターの詳細確認画面 ■アラート」を参照してください。
	削除	選択しているクライアントコンピューター（複数選択可）をグループから削除します。
	移動	選択しているクライアントコンピューター（複数選択可）を別グループに移動します。 ※移動先は、静的グループのみ指定できます。
	複数の項目名の変更	選択しているクライアントコンピューター（複数選択可）の名前を 1 つの画面でまとめて変更します。
	検査	脅威を報告したクライアントでオンデマンド検査を実行するタスクをスケジュールします。定義済み検査プロファイルを使用してクライアントを検査します。スケジュールされた検査は「タスク」タブに表示されます。 画面の詳細は、「6.3.6.2 「タスク」タブ画面の構成」を参照してください。
		駆除して検査する：感染したオブジェクトが検出された場合、自動的に駆除されます。
		駆除せずに検査する：感染したオブジェクトが検出された場合、隔離されます。
	モジュールの更新	モジュールアップデートタスク（アップデートを手動でトリガー）を実行します。スケジュールされたタスクは「タスク」タブに表示されます。 画面の詳細は、「6.3.6.2 「タスク」タブ画面の構成」を参照してください。

続く

	モバイル	選択しているモバイルデバイスに以下のタスクを実行します。		
			再登録	選択中のモバイルデバイスを再登録します。「電子メールでモバイルデバイスの追加」画面が表示されるので、登録に関する設定を行います。
			検索	Android デバイスの GPS 座標を検索します。 ※ iOS デバイスでは使用できません。
			ロック	不審なアクティビティが検出されたり、デバイスを紛失した場合などに、モバイルデバイスをロックします。
			ロック解除	モバイルデバイスのロックが解除されます。
			警報	Android デバイスに対し、リモートで大音量の警報音をトリガーします。デバイスがミュートに設定されていても、警報音が作動します。 ※ iOS デバイスでは使用できません。
			ワイプ	Android デバイスに保存されているアクセス可能なデータが完全に消去されます。 ※ iOS デバイスでは使用できません。
	再起動	選択しているコンピューターに再起動またはシャットダウンするタスクを割り当てます。		
			再起動	再起動するタスクを割り当てます。
			シャットダウン	シャットダウンするタスクを割り当てます。
	タスクの実行	このオプションを使用すると、このグループのデバイスで実行されるクライアントタスクを選択できます。		
	新規タスク	選択しているグループに新しいクライアントタスクを作成します。「ターゲット」に選択しているグループが追加されている状態で、「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。		
	最後に使用されたタスク	最後に実行されたタスクを再度、実行できます。		
	ユーザーの割り当て	選択したデバイスにユーザーの割り当てを行います。「項目を選択してください」画面が表示されるので、デバイスに割り当てたいユーザーを選択し、[OK] ボタンをクリックします。		
	ポリシーの管理	選択しているグループにポリシーを割り当てます。「ポリシーアプリケーション順序」画面が表示されます。 画面の詳細は、「6.5.5.2 複数のポリシーを適用順にグループに割り当てる」の「■ポリシーアプリケーション順序画面」を参照してください。		
	ウェイクアップコールの送信	選択しているクライアントコンピューターと ERA エージェントとの即時通信を開始します。これは、ERA エージェントが ERA サーバーに接続するときに、定期間隔を開けずに通信を行います。例えば、クライアントですぐにタスクを実行する場合や、ポリシーをすぐに適用する場合に使用できます。 変更する場合は、ウェイクアップコールを使用するまでに約 1 分間待機します。		
	エージェントの展開	ERA エージェントの展開を行います。展開オプションを選択する画面が表示されます。 画面の詳細は、「4.2.2 ERA エージェントの展開」を参照してください。		

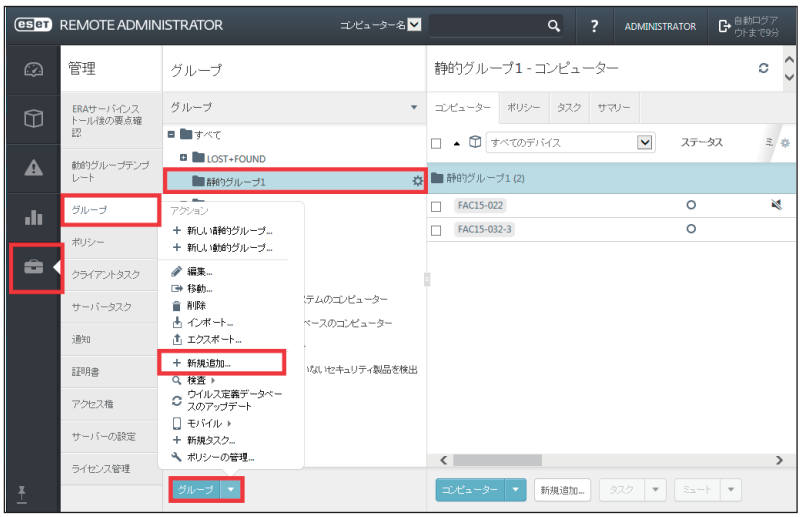
	製品のアクティベーションを解除	選択中のデバイスのアクティベーションを解除します。
	連絡先	リモートデスクトッププロトコル経由で対象デバイスに接続できる .rdp ファイルを生成してダウンロードします。
	グループに移動	選択中のデバイスを別のグループに移動します。移動先を選択する画面が表示されるので、移動先のグループを選択し、[OK] ボタンをクリックします。
	ミュート	選択しているクライアントコンピューターの ERA エージェントから ESET Remote Administrator への通知を停止します。情報の集約だけが行われます。
	ミュート解除	ESET Remote Administrator への通知を再開します。

6.3.5.2 クライアントコンピューターの追加

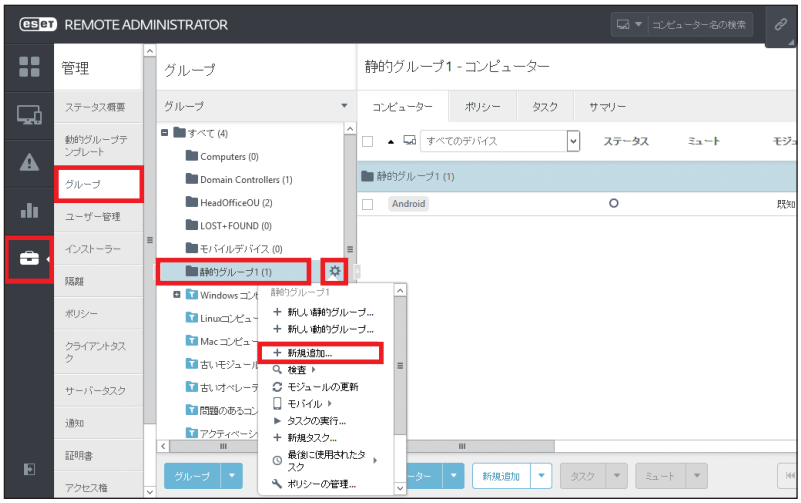
静的グループにクライアントコンピューターを追加するには、6 種類の方法があります。

■「管理」メニューから作成する

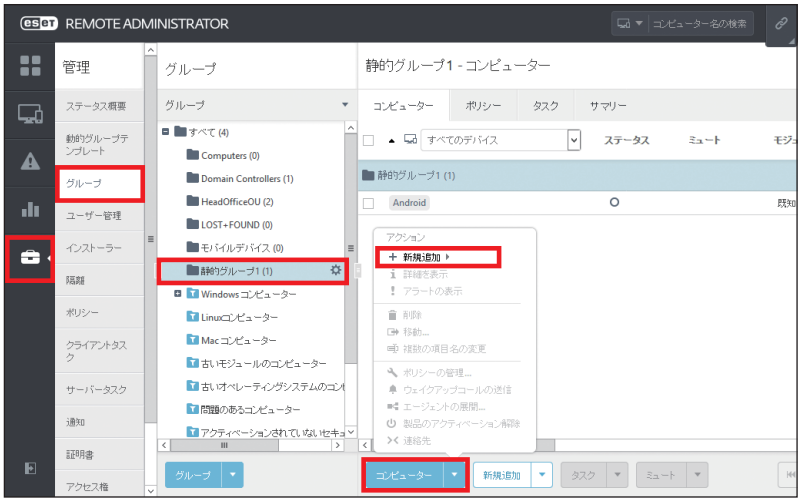
- [グループ] > 追加するグループを選択 > [グループ] ボタン > [新規追加] を選択します。



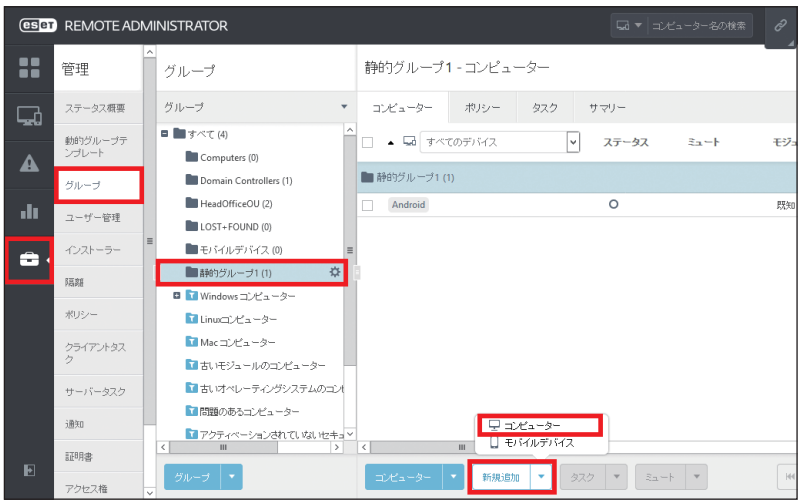
- [グループ] > 追加するグループを選択 > ⚙ > [新規追加] を選択します。



- ［グループ］> 追加するグループを選択 >［コンピューター］ボタン >［新規作成］を選択します。

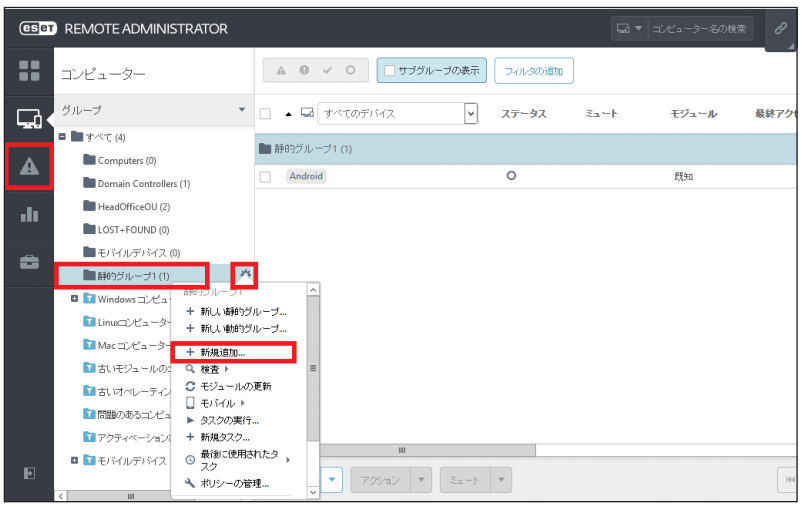


- ［グループ］> 追加するグループを選択 >［新規追加］ボタン >［コンピューター］を選択します。

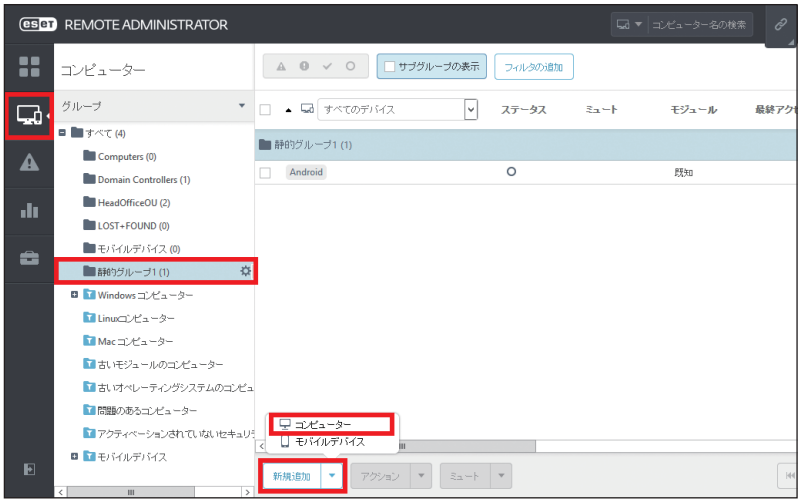


■「コンピューター」メニューから作成する

- 追加するグループを選択 > ⚙ >［新規追加］を選択します。

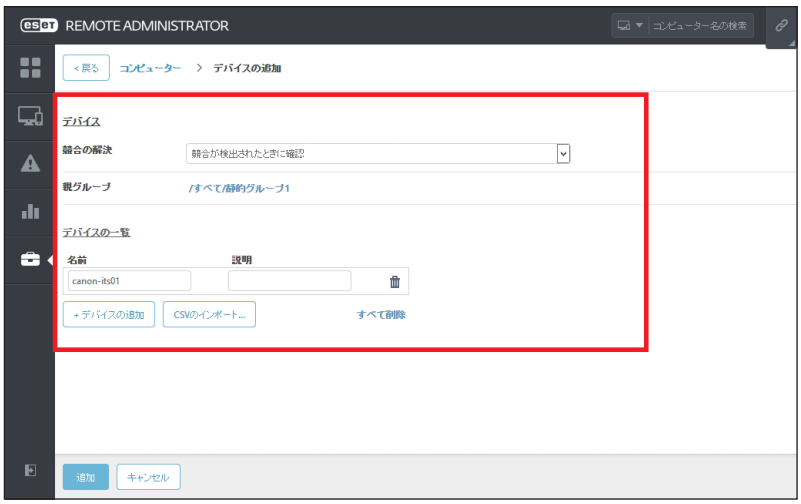


・追加するグループを選択 > [新規追加] ボタン > [コンピューター] を選択します。



操作手順

1. いずれかの方法で「デバイスの追加」画面を表示します。
2. 各項目を入力します。



■デバイスの追加

項目名	説明		必須
競合の追加	選択したコンピューターが既に追加されていた場合の解決方法を選択します。		○
	競合が検出されたときに確認	競合が検出された場合に、アクションを選択する画面が表示されます。	-
	競合するデバイスをスキップ	重複するコンピューターは追加されません。	-
	他のグループから競合するデバイスを移動	競合しているコンピューターを元のグループから削除して、新しいグループに移動します。	-
	競合するデバイスの複製	新しいコンピューターとして追加されます。異なる名前が自動で振られます。	-
親グループ	選択したグループが表示されます。変更する場合はクリックします。		○
名前	追加するコンピューターの IP アドレスまたはホスト名を入力します。		○
説明	追加するコンピューターの説明を入力します。		-
削除	行を削除します。		-
デバイスの追加	追加するデバイスの入力欄を追加します。		-
CSV のインポート	追加するコンピューターのリストを CSV ファイルでインポートします。		-
すべて削除	デバイス一覧に表示されているコンピューターのリストをすべて削除します。		-

! 重　要

複数のコンピューターを追加する場合は、［デバイスを追加］ボタンをクリックして続けて入力することができます。ただし、複数のコンピューターをまとめて追加すると時間がかかる場合がありますので、台数が多い場合は複数回に分けて追加してください。

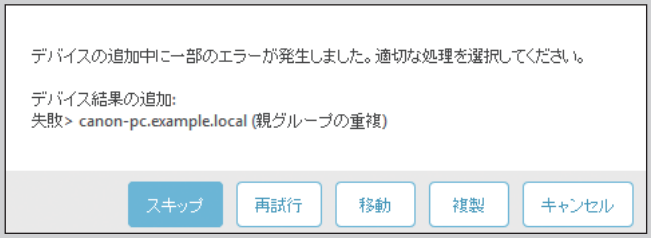
3 ［追加］ボタンをクリックします。

4 ［OK］ボタンをクリックします。

静的グループにクライアントコンピューターが追加されます。

! 重 要

「競合が検出されたときに確認」を選択している場合、追加したコンピューターが指定した親グループに既に存在していると、確認画面が表示されます。重複したコンピューターの処理方法を選択してください。



スキップ	画面に表示されているコンピューターの追加の処理は行われません。複数のコンピューターを追加している場合は、次のコンピューターの追加の処理を行います。
再試行	再度、追加の処理を行います。
移動	指定した親グループへ移動します。
複製	指定した親グループ内に追加されます。
キャンセル	追加処理を取り消します。

ワンポイント

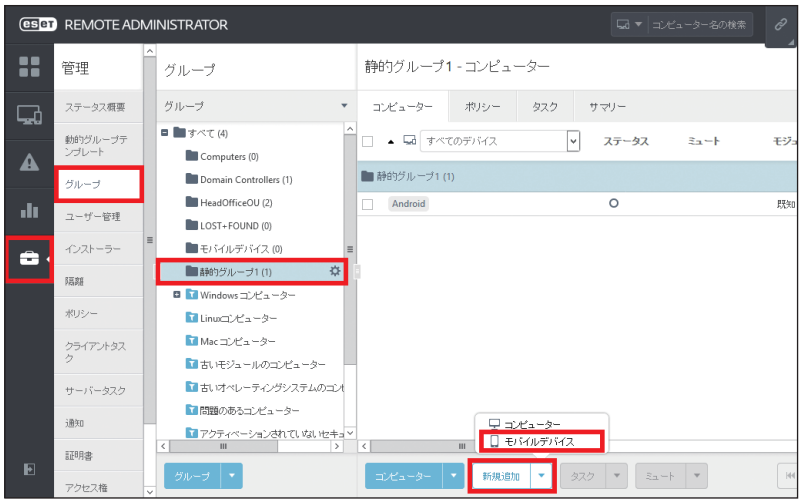
続けてエージェントの展開を行う場合は、［エージェントの展開］ボタンをクリックします。エージェント展開については、「4.2.2 ERA エージェントの展開」を参照してください。

6.3.5.3 モバイルデバイスの追加

静的グループにモバイルデバイスを追加するには、2 種類の方法があります。

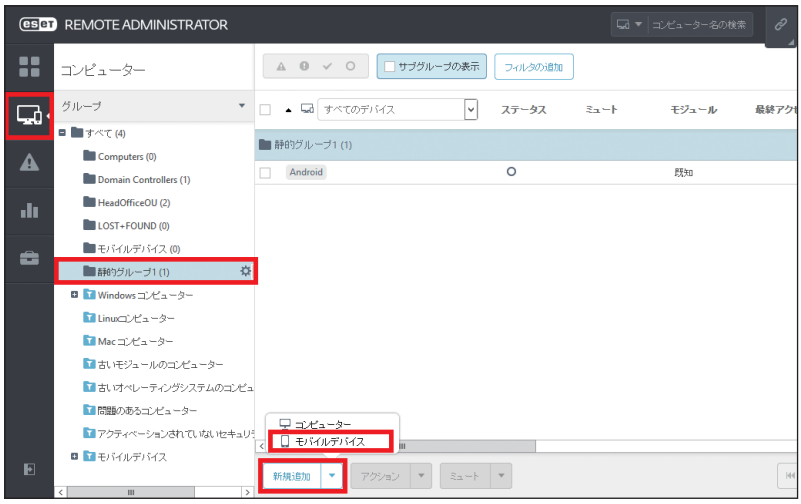
■「管理」メニューから作成する

- ［グループ］> 追加するグループを選択 >［新規追加］ボタン >［モバイルデバイス］を選択します。



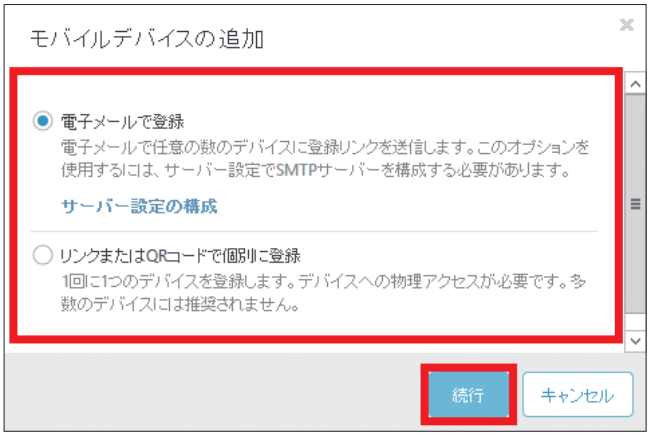
■「コンピューター」メニューから作成する

- 追加するグループを選択 > [新規追加] ボタン > [モバイルデバイス] を選択します。



操作手順

1. いずれかの方法で「モバイルデバイスの追加」画面を表示します。登録方法を選択し、[続行] ボタンをクリックします。



続く

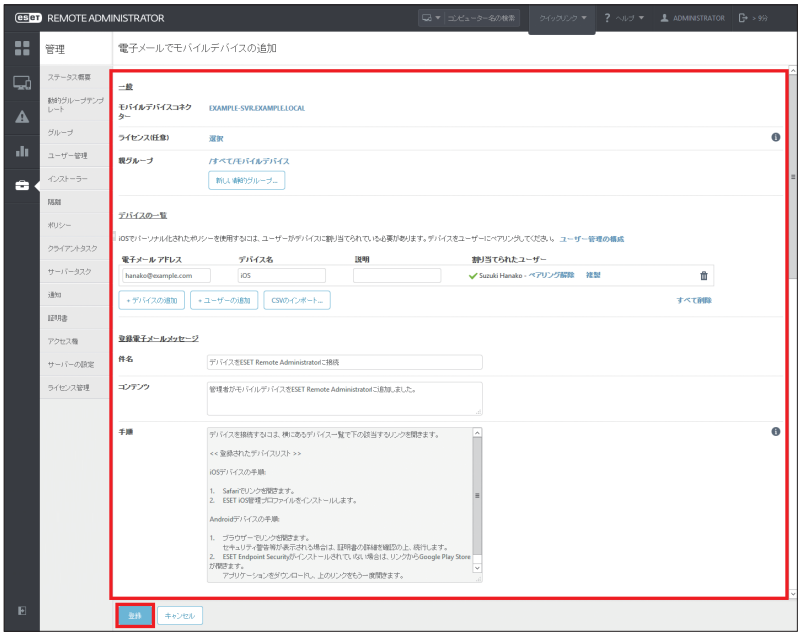
■モバイルデバイスの追加

項目名	説明
電子メールで登録	電子メールでモバイルデバイス登録用のリンクを送信します。複数のモバイルデバイスをまとめて登録するときにお勧めの方法です。この方法を利用するには、SMTP サーバーの設定を行う必要があります。SMTP サーバーの設定については、「6.11 サーバーの設定 - ■詳細設定」を参照してください。
リンクまたは QR コードで個別に登録	1 回の操作で 1 台のモバイルデバイスを登録できます。ユーザー / モバイルデバイスの所有者に何もさせずに、管理者自身がすべての作業を行った後に、モバイルデバイスを配布するという用途にお勧めです。登録には、モバイルデバイス登録用のリンクまたは QR コードを利用します。登録用リンクは、モバイルデバイスの Web ブラウザーに手動で入力するか、リンクを電子メールなどでモバイルデバイスに送信して利用します。QR コードを利用する場合は、画面に表示された QR コードをモバイルデバイスで読み込んで利用します。モバイルデバイスに QR コード読み込み用アプリのインストールが必要になります。

2 各項目の入力を行います。

●電子メールで登録する場合

手順 1 で「電子メールで登録」を選択したときは、以下の項目の設定を行います。設定が終わったら、［登録］をクリックして手順 4 に進みます。



続く

項目名	説明	必須
モバイルデバイスコネクター	自動的に選択されます。複数のモバイルデバイスコネクターがある場合は、使用するモバイルデバイスコネクターを選択できます。表示されているモバイルデバイスコネクターの名称をクリックして、利用するモバイルデバイスコネクターを選択し、［OK］ボタンをクリックします。	○
ライセンス	ライセンスを選択します。選択をクリックして、アクティベーションで使用するライセンスを選択します。製品アクティベーションクライアントタスクがモバイルデバイス用に作成されます。ライセンス単位が取得されます（各モバイルデバイスに 1 つ）。	-
親グループ	登録するモバイルデバイスの親グループを設定します。表示されているグループをクリックすると、既存のグループの中から登録したい親グループを選択できます。また、［新しい静的グループ］をクリックすると、グループの新規作成が行えます。	○
電子メールアドレス	登録メールが送信されるモバイルデバイスを利用しているユーザーの電子メールアドレスを入力します。	○
デバイス名	登録するモバイルデバイスのデバイス名を入力します。	-
説明	登録するモバイルデバイスの説明を入力します。	-
割り当てられたユーザー	［ペアリング］をクリックすると、有力した電子メールアドレスとユーザー管理に登録されているユーザー情報のペアリングを行います。また、電子メールアドレスを入力したときに、その電子メールアドレスが登録されたユーザーがあるときは、自動的にそのユーザーとペアリングが行われます。通常、1 つ以上のユーザーをモバイルデバイスに割り当てることをお勧めします。また、iOS デバイスでパーソナル化されたポリシーを使用する場合は、ユーザーをモバイルデバイスに割り当てる必要があります。	-
複製	その行に入力された情報の複製を作成します。	-
［削除］	その行に入力された情報を削除します。	-
デバイスの追加	新しいモバイルデバイス登録用のエントリを作成します。	-
ユーザーの追加	ERA に登録されているユーザーのリストを利用して、登録メールを送信したいユーザーを登録します。この機能を利用するには、電子メールアドレスがユーザー情報に登録済みである必要があります。	-
CSV のインポート	追加するモバイルデバイスのリストが含まれた .csv ファイルをアップロードします。.csv ファイルには、最低限、電子メールアドレスが記載されている必要があります。デバイス名と説明に関しては、任意です。この方法は、数多くのモバイルデバイスを一度に登録したいときにお勧めの方法です。CSV のインポートの詳細については、「5.3.6.1　モバイルデバイスを ERA のグループ構造に手動で追加する」を参照してください。	-
登録電子メールメッセージ	登録したユーザーに送信される電子メールメッセージの内容が表示されます。送信される電子メールのメッセージは、件名および内容をカスタマイズできます。なお、別表示されている手順部分の内容については、カスタマイズすることはできません。	-

続く

●リンクまたは QR コードで個別に登録する場合

手順 1 で［リンクまたは QR コードで個別に登録］を選択したときは、以下の項目の設定を行います。設定が終わったら、［次へ］をクリックして、手順 3 に進んでください。

項目名	説明	必須
デバイス名	登録を行うモバイルデバイスの名称を入力します。	○
説明	登録を行うモバイルデバイスの説明を入力します。	-
ユーザー（任意）	登録するモバイルデバイスに割り当てるユーザーを設定します。［選択］をクリックすると、「項目を選択してください」画面が表示されるので、リストから割り当てたいユーザーを選択して、［OK］ボタンをクリックします。iOS デバイスでパーソナル化されたポリシーを使用する場合は、ユーザーをモバイルデバイスに割り当てる必要があります。	-
モバイルデバイスコネクター	自動的に選択されます。複数のモバイルデバイスコネクターがある場合は、使用するモバイルデバイスコネクターを選択できます。表示されているモバイルデバイスコネクターの名称をクリックして、利用するモバイルデバイスコネクターを選択し、［OK］ボタンをクリックします。	○
ライセンス（任意）	ライセンスを選択します。選択をクリックして、アクティベーションで使用するライセンスを選択します。製品アクティベーションクライアントタスクがモバイルデバイス用に作成され、ライセンス単位が取得されます（各モバイルデバイスに 1 つ）。	-
親グループ	登録するモバイルデバイスの親グループを設定します。表示されているグループをクリックすると、既存のグループの中から登録したい親グループを選択できます。また、［新しい静的グループ］をクリックすると、グループの新規作成が行えます。	○

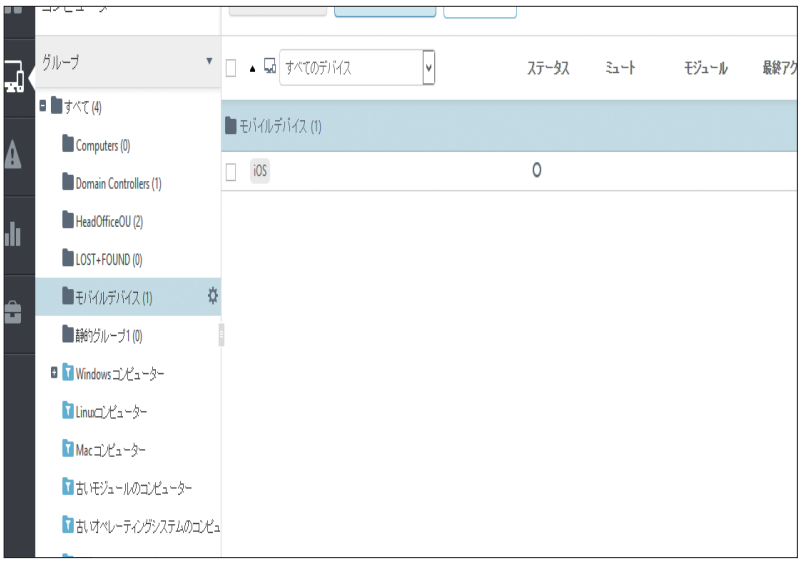
続く

3 手順 1 で［リンクまたは QR コードで個別に登録］を選択したときは、モバイルデバイス登録用のリンクと QR コードが表示されます。表示されたリンクをユーザーに電子メールで送付するなどして登録を行います。登録したいモバイルデバイスで QR コードを読み取ることでも登録できます。［閉じる］をクリックして手順 4 に進んでください。

ワンポイント

［別のデバイスを登録］をクリックすると、別のモバイルデバイスの登録を行えます。

4 選択した親グループにモバイルデバイスが登録されます。

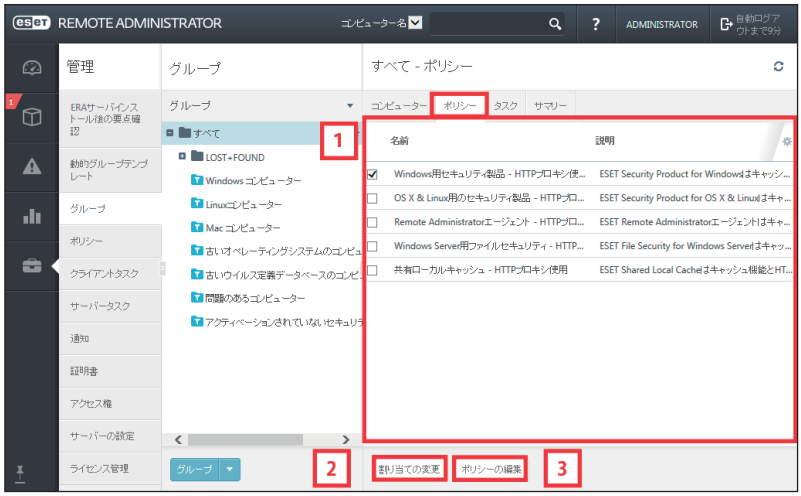


6.3.6 その他のタブ

「ポリシー」タブ、「タスク」タブ、「サマリー」タブの画面について説明します。

6.3.6.1 「ポリシー」タブ画面の構成

「ポリシー」タブには、選択しているグループに割り当てられたポリシーのリストが表示されます。ポリシーの編集や割り当ての変更が行えます。



1	**ポリシーリスト**	選択しているグループに割り当てられたポリシーリストが表示されます。
2	**割り当ての変更**	選択しているグループに割り当てられているポリシーリストを変更します。「ポリシーアプリケーション順序」画面が表示されます。 画面の詳細は、「6.5.5.2 複数のポリシーを適用順にグループに割り当てる」を参照してください。
3	**ポリシーの編集**	選択しているポリシーを編集します。「ポリシーの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいポリシーとして保存することができます。 画面の詳細は、「6.5.2 新しいポリシーの作成」を参照してください。

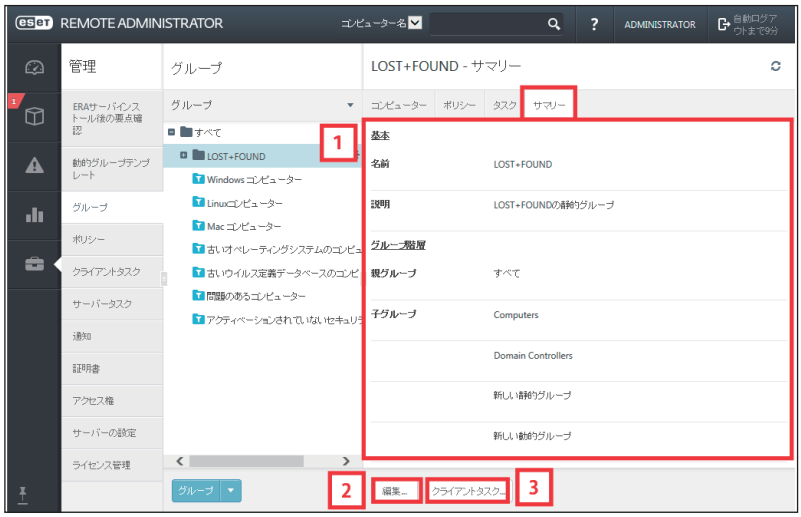
6.3.6.2 「タスク」タブ画面の構成

「タスク」タブには、選択しているグループに割り当てられたタスクのリストが表示されます。新しいタスクの作成や編集、削除などが行えます。

1	タスクリスト	選択しているグループに割り当てられたタスクリストが表示されます。		
2	タスク	選択しているタスクアクションメニューが表示されます。		
			新規作成	新しいクライアントタスクを作成します。「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。
			編集	選択しているタスクを編集します。「クライアントタスクの編集」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。
			複製	選択しているタスクの内容をコピーした状態で「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。
			削除	選択しているタスク（複数選択可）を削除します。
3	クライアントタスク	新しいクライアントタスクを作成します。「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。		

6.3.6.3 「サマリー」タブ画面の構成

「サマリー」タブには、選択しているグループの内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、［編集］ボタンから変更します。



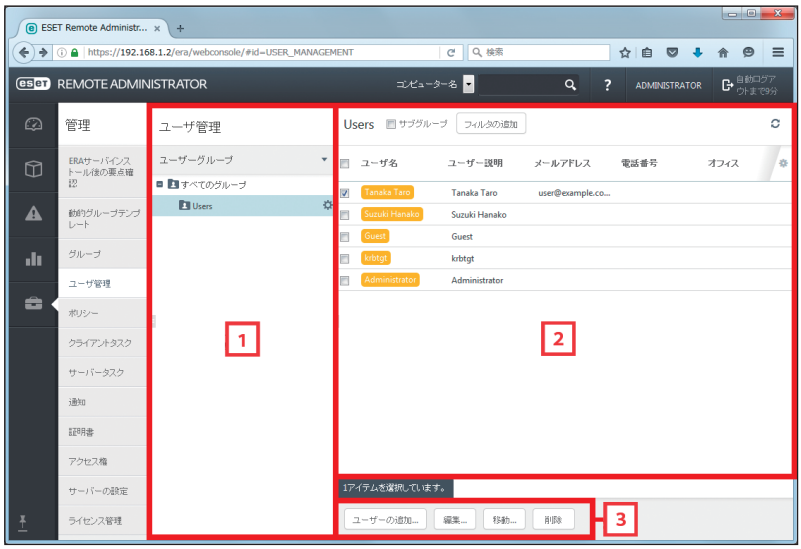
1	サマリー	選択しているグループの内容が、読み取り専用の状態で表示されます。
2	編集	選択しているグループを編集します。「静的または動的グループの編集」画面が表示されます。 画面の詳細は、「6.3.2.1 新しい静的グループの作成」または「6.3.2.2 新しい動的グループの作成」を参照してください。
3	クライアントタスク	新しいクライアントタスクを作成します。「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。

6.4 ユーザー管理

このセクションでは、iOS デバイス管理の目的で、ユーザーとユーザーグループを管理できます。モバイルデバイス管理は、iOS デバイスに割り当てられたポリシーを使用して実施できます。ユーザー管理を行うときは、最初にユーザー同期サーバータスクを実行して、ユーザーを Active Directory と同期することをお勧めします。次に、ユーザーを修正したり、カスタム属性の追加を行います。

6.4.1 ユーザー管理の画面構成

「ユーザー管理」画面の構成について説明します。

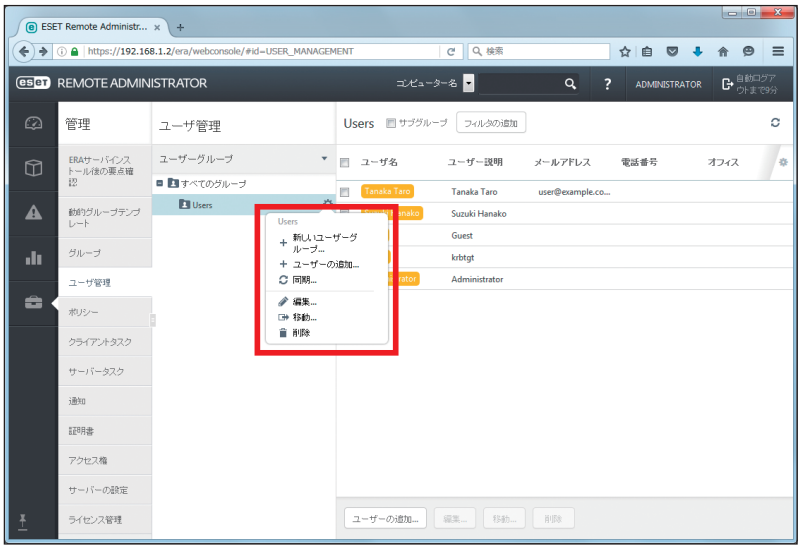


1	**グループリスト**	すべてのユーザーグループのリストが表示されます。オレンジ色でハイライト表示されたユーザーにはデバイスが割り当てられていません。
2	**選択中のグループの詳細**	グループリストから選択しているグループに属しているユーザーの一覧が表示されます。
3	**操作ボタン**	ユーザーの追加を行えるほか、選択したユーザーの編集、移動、削除などを行うための操作ボタンが配置されています。

■コンテキストメニューのアクション

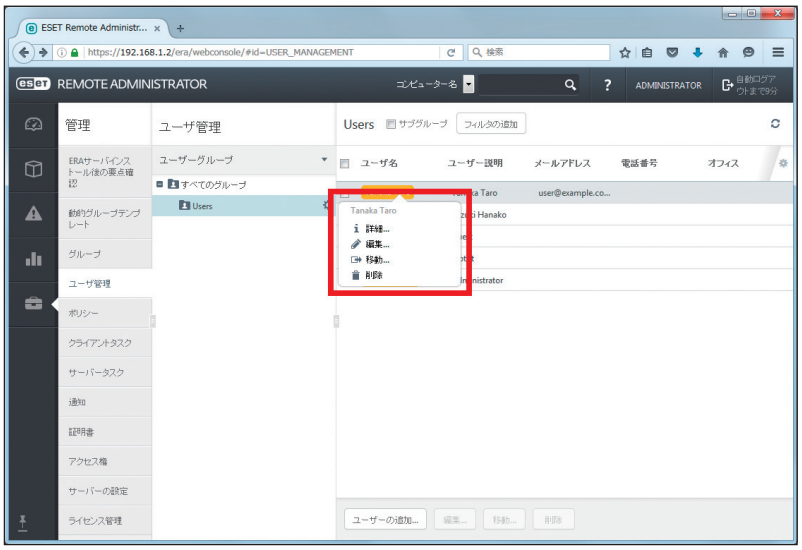
コンテキストメニューに表示されるアクションについて説明します。

- グループのコンテキストメニュー



+	**新しいユーザーグループ ...**	新しいユーザーグループを作成できます。
+	**ユーザーの追加 ...**	新しいユーザーを追加します。
	同期	新しいサーバータスクのユーザー同期を作成します。
	編集 ...	選択したユーザーまたはユーザーグループを編集できます。
	移動 ...	ユーザーまたはユーザーグループを選択し、別ユーザーグループのサブグループとして移動することができます。
	削除	選択したユーザーまたはユーザーグループを完全に削除します。

- ユーザーのコンテキストメニュー



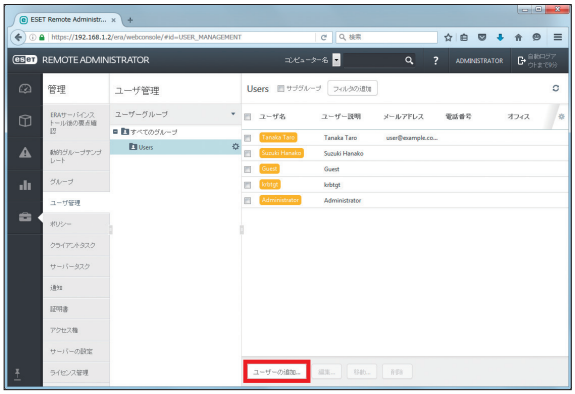
	詳細	ユーザー詳細メニューには、電子メールアドレス、オフィスまたはロケーション、カスタム属性、および割り当てられたコンピューターの情報などが表示されます。ユーザーは複数のコンピューター / モバイルデバイスに割り当てることができます。ユーザーの名前、説明、または親グループを変更できます。ポリシーを作成するときに使用できるカスタム属性がここに表示されます。
	編集	選択したユーザーの情報を編集できます。カスタム属性の設定やコンピューター / モバイルデバイスへの割り当てなどを行えます。ユーザーは複数のコンピューター / モバイルデバイスに割り当てることができます。ユーザーの名前、説明、または親グループなどの情報も変更できます。
	移動	選択したユーザーを、別ユーザーグループに移動することができます。
	削除	選択したユーザーを削除します。

6.4.2 新しいユーザーの追加

新しいユーザーを作成する方法を説明します。

操作手順

1. [管理] > [ユーザー管理] > とクリックし、[ユーザーの追加] をクリックします。



2. [ユーザー名]、[メールアドレス]、[電話番号] などに、追加するユーザーの情報を入力して、[追加] をクリックします。追加したユーザーが既に ERA サーバーにある場合は、[競合解決] ドロップダウンメニューから、実行するアクションを選択します。

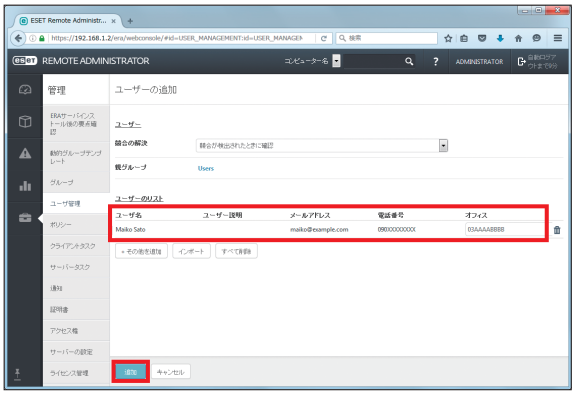
- 競合が検出されたときに確認
  この設定を行うと競合が検出された場合にプログラムのアクション (以下のオプションを参照) を選択するように求められます。

  競合するユーザーをスキップ：同じ名前のユーザーは追加されません。これは、既存のユーザーの ERA のカスタム属性が保持されることも保証します (Active Directory のデータで上書きされない)。

  競合するユーザーの上書き：ERA の既存のユーザーは Active Directory のユーザーによって上書きされます。同じ SID のユーザーが 2 人いる場合、ERA の既存のユーザーは前の場所から削除されます (ユーザーが別のグループにある場合でも削除されます)。

- 競合するユーザーをスキップ
  この設定を行うと競合が検出された場合に、競合するユーザーの追加をスキップします。

- 競合するユーザーの上書き
  この設定を行うと競合が検出された場合に、競合するユーザーの情報を上書きします。



ワンポイント

［+その他を追加］をクリックすると、登録したいユーザーを追加できます。また、複数のユーザーを同時に追加する場合は、［インポート］をクリックして、追加するユーザーのリストを含む CSV ファイルをアップロードします。

6.4.3 ユーザーの編集

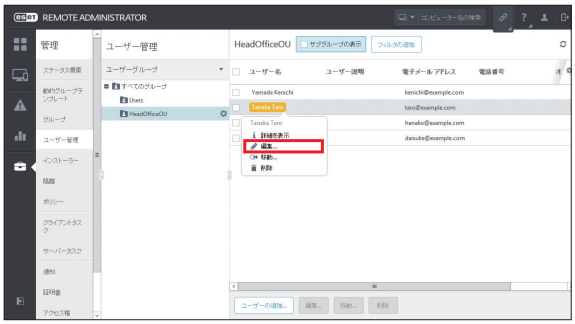
ユーザーの基本情報の変更やカスタム属性の設定、コンピューター / モバイルデバイスへの割り当てなどを行いたいときは、ユーザーの編集を行います。

! 重 要

カスタム属性が定義されたユーザーのユーザー同期タスクを実行するときは、ユーザー作成競合処理をスキップするように設定してください。スキップをしない場合は、ユーザーデータが Active Directory のデータによって上書きされます。

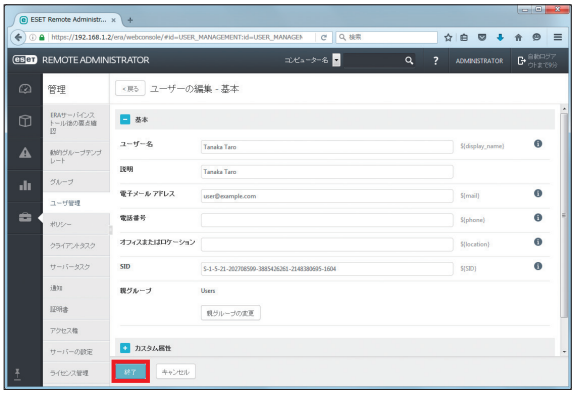
操作手順

1 情報を編集したいユーザーをクリックし、［編集］をクリックします。



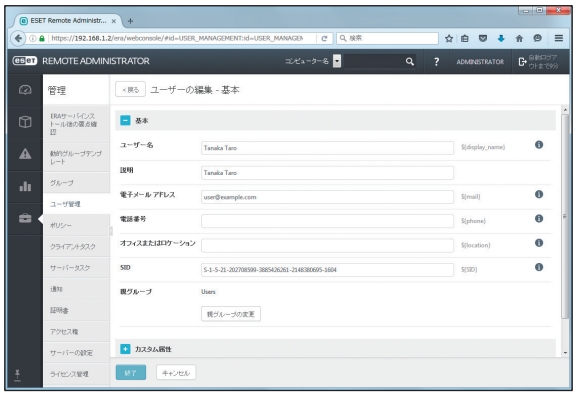
続く

2 各項目の編集を行い、［終了］をクリックして編集内容を保存します。



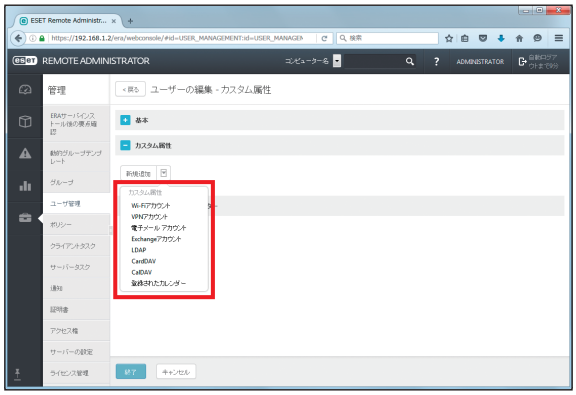
■基本

ユーザー同期タスクを使用してユーザーを作成し、一部のフィールドを空欄にする場合は、必要に応じてこれらを手動で設定できます。ユーザー名、説明、電子メールアドレス、電話番号、オフィスまたはロケーションなどの情報を編集できます。また、親グループの変更も行えます。



■カスタム属性

カスタム属性の編集を行えます。既存のカスタム属性がある場合は、その編集を行えます。既存のカスタム属性がない場合は、新しい属性を追加できます。新しい属性を追加するには、［新規追加］をクリックして、追加するカテゴリを選択します。



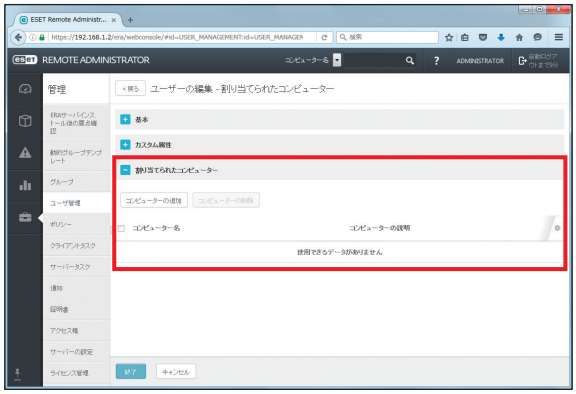
項目名	説明
Wi-Fi アカウント	プロファイルを使用して、社内の Wi-Fi 設定を管理しているデバイスに直接プッシュして登録します。
VPN アカウント	認証資格情報、証明書、およびその他の必要な情報とともに VPN を設定し、ユーザーが簡単に VPN にアクセスできるようにします。
電子メールアカウント	電子メールアカウントの設定を行います。この項目は、IMAP または POP3 の電子メールアカウントで使用されます。Exchange サーバーを使用する場合は、Exchange ActiveSync 設定を使用します。
Exchange アカウント	社内で Microsoft Exchange を利用している場合は、ここですべての設定を作成し、ユーザーの電子メール、カレンダー、および連絡先へのアクセスを設定する時間を最小化できます。
LDAP (属性エイリアス)	社内で連絡先用に LDAP を使用している場合に特に便利です。連絡先フィールドを対応する iOS 連絡先フィールドにマッピングできます。
CalDAV	これには、CalDAV 仕様を使用するすべてのカレンダーの設定が含まれます。
CardDAV	CardDAV 仕様で同期されるすべての連絡先の同期情報をここで確立できます。
登録されたカレンダー	CalDAV カレンダーが設定されている場合は、ここで、他のカレンダーへの読み取りアクセスを定義できます。

ワンポイント

一部のフィールドは、変数 (プレースホルダー) として iOS デバイスのポリシーを作成するときに使用できる属性になります。たとえば、ログイン ${exchange_login/exchange} または電子メールアドレス ${exchange_email/exchange} などがあります。

■割り当てられたコンピューター

ここでは、ユーザーにコンピューターやモバイルデバイスの割り当てを行えます。[コンピューターの追加] をクリックして、割り当てるコンピューター／モバイルデバイスを選択し、[OK] をクリックします。また、ユーザーには複数のコンピューター／モバイルデバイスを割り当てることができます。

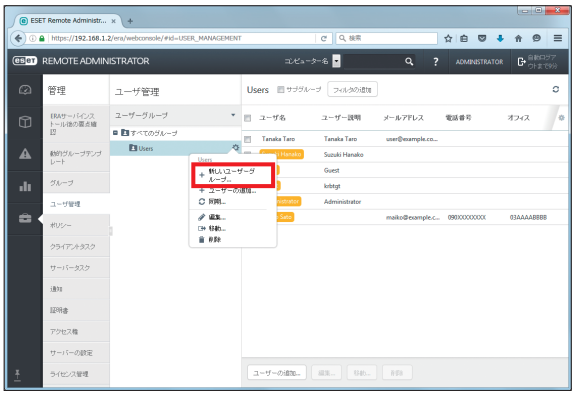


6.4.4 新しいユーザーグループの作成

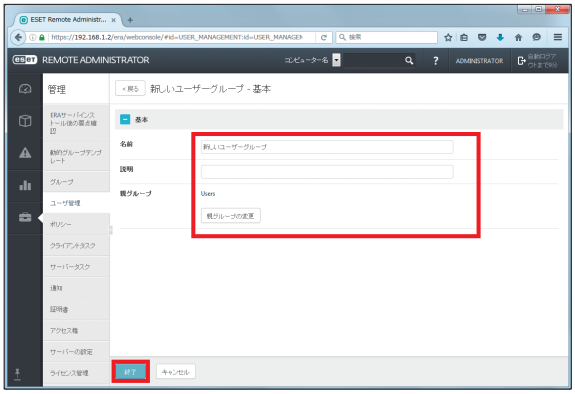
新しいユーザーグループを作成する方法を説明します。

操作手順

1. [管理] > [ユーザー管理] とクリックして、⚙をクリックし、[新しいユーザーグループ ...] をクリックします。



2. 新しいユーザーグループの名前を入力し、説明 (任意) を入力します。既定では、新しいユーザーグループの作成時に選択したグループが親グループに設定されています。親グループを変更する場合は、親グループの変更をクリックし、ツリーから親グループを選択します。[終了]をクリックして、新しいユーザーグループを作成します。



ワンポイント

アクセス権から権限設定を使用して、このユーザーに特定の権限を割り当てることができます。アクセス権の詳細については、「6.10 アクセス権」をご参照ください。

6.5 ポリシー

ポリシーは、クライアントコンピューターで実行されている ESET 製品に特定の設定を割り当てるために使用されます。ポリシーを利用した場合、各クライアントコンピューターの ESET 製品の設定を手動で変更する必要はなく、個別のコンピューターとグループ（静的と動的）に直接適用できます。

! 重 要

Windows、Mac OS X の場合、ポリシーを適用した設定項目は、クライアントコンピューター側での設定変更ができなくなります。

! 重 要

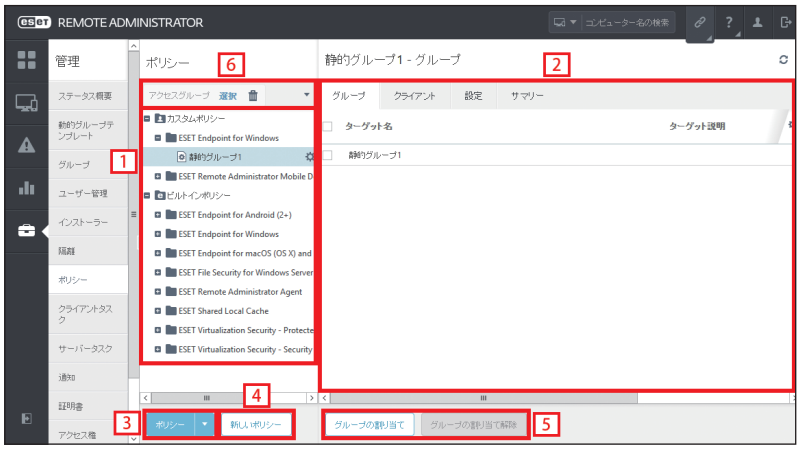
コンピューターまたはグループに、複数のポリシーを割り当てることができます。
複数のポリシーを割り当てた場合の適用順については、「6.5.4 ポリシーの適用」を参照してください。

! 重 要

ポリシーを適用した後は、適用したポリシーを削除してもクライアントコンピューターの構成が自動的に元の設定に戻ることはありません。クライアントコンピューターに適用された最後のポリシーに従って、構成が維持されます。
クライアントコンピューターがコンピューターの設定を変更する特定のポリシーが適用された動的グループのメンバーになった場合も、同じことが発生します。クライアントコンピューターが動的グループから削除されても、設定は保持されます。
このため、既定の設定に戻せるように、「すべて」グループに既定の設定で作成したポリシーを割り当てておくことを推奨します。この方法を使えば、クライアントコンピューターが設定を変更した動的グループから削除された場合に、既定の設定を使用できます。

6.5.1 ポリシー画面の構成

「ポリシー」画面の構成について説明します。

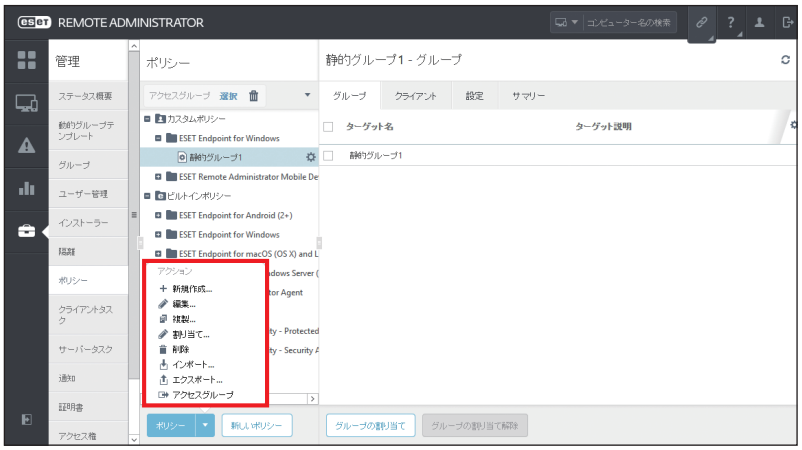


1	**ポリシーリスト**	すべてのポリシーのリストが表示されます。
2	**選択中ポリシーの詳細**	ポリシーリストから選択したポリシーに関する詳細が表示されます。
	「グループ」タブ	割り当てられたグループのリストが表示されます。
	「クライアント」タブ	割り当てられたクライアントのリストが表示されます。
	「設定」タブ	対象製品名と設定内容が表示されます。
	「サマリー」タブ	名前、説明などの概要が表示されます。
3	**ポリシー**	新しいポリシーの作成や選択中のポリシーの編集、削除などのアクションメニューが表示されます。 表示されるアクションの詳細は、「■［ポリシー］ボタンと「ポリシー」コンテキストメニューのアクション」を参照してください。
4	**新しいポリシー**	新しいポリシーの作成を行います。詳細については、「6.5.2 新しいポリシーの作成」を参照してください。
5	**2 の各タブで使用するボタン**	2 の各タブに応じて、表示されるボタンが変わります。 表示されるボタンの詳細は、「6.5.5.3 「グループ」タブ画面の構成」「6.5.6.3 「クライアント」タブ画面の構成」「6.5.8.1「設定」タブ画面の構成」「6.5.8.2「サマリー」タブ画面の構成」を参照してください。
6	**アクセスグループ**	「アクセスグループ」では、ユーザーが静的グループを選択し、属するグループに応じて、表示されるオブジェクトをフィルタリングできます。［選択］をクリックすると、フィルタリングするグループを選択できます。また、 をクリックすると、フィルターリングを解除できます。

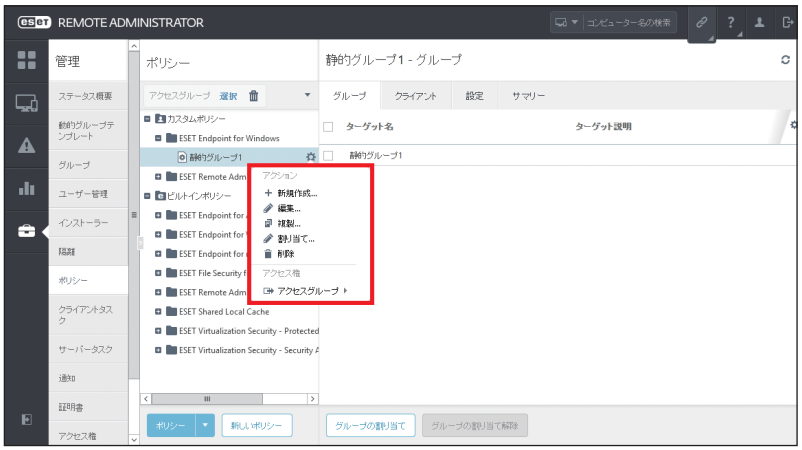
［ポリシー］ボタンと「ポリシー」コンテキストメニューのアクション

［ポリシー］ボタンと「ポリシー」コンテキストメニューに表示されるアクションについて説明します。

- ［ポリシー］ボタンのメニュー



- 「ポリシー」コンテキストメニュー



	新規作成	新しいポリシーを作成します。「新しいポリシー」画面が表示されます。 画面の詳細は、「6.5.2　新しいポリシーの作成」を参照してください。
	編集	選択しているポリシーを編集します。「ポリシーの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいポリシーとして保存することができます。 画面の詳細は、「6.5.2　新しいポリシーの作成」を参照してください。
	複製	選択しているポリシーの内容をコピーした状態で「新しいポリシー」画面が表示されます。 画面の詳細は、「6.5.2　新しいポリシーの作成」を参照してください。
	割り当て	選択しているポリシーを割り当てるターゲットを指定します。「ポリシー編集－割り当て」画面が表示されます。 画面の詳細は、「6.5.2　新しいポリシーの作成」を参照してください。
	削除	選択しているポリシーを完全に削除します。
	インポート	選択しているポリシーに、DAT ファイル（.dat）で作成されたポリシーの設定をインポートします。「ポリシーのインポート」画面が表示されます。 操作については、「6.5.7.2　ポリシーのインポート」を参照してください。

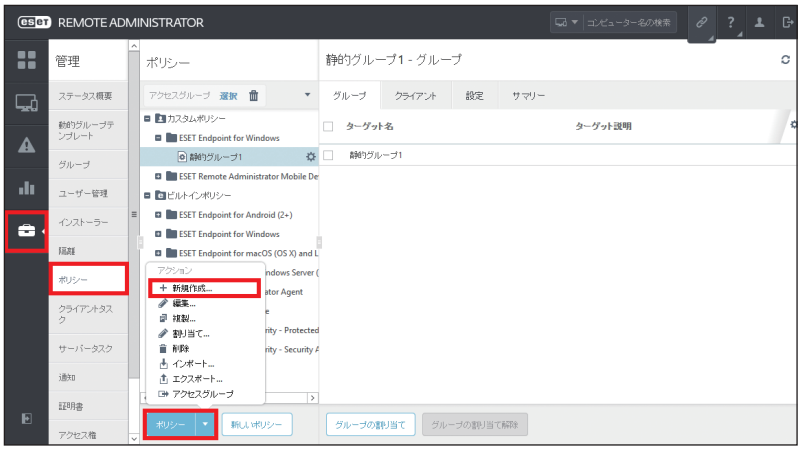
	エクスポート	選択しているポリシーの設定を DAT ファイル（.dat）にエクスポートします。 ※複数のポリシーを一括してエクスポートすることはできません。 操作については、「6.5.7.1　ポリシーのエクスポート」を参照してください。
	アクセスグループ	選択したポリシーを別のグループに移動します。［ポリシー］ボタン >「アクセスグループ」またはコンテキストメニューの［ポリシー］>［アクセスグループ］>［移動］とクリックすると、グループの選択画面が表示されます。

6.5.2　新しいポリシーの作成

ポリシーを新しく作成する方法を説明します。

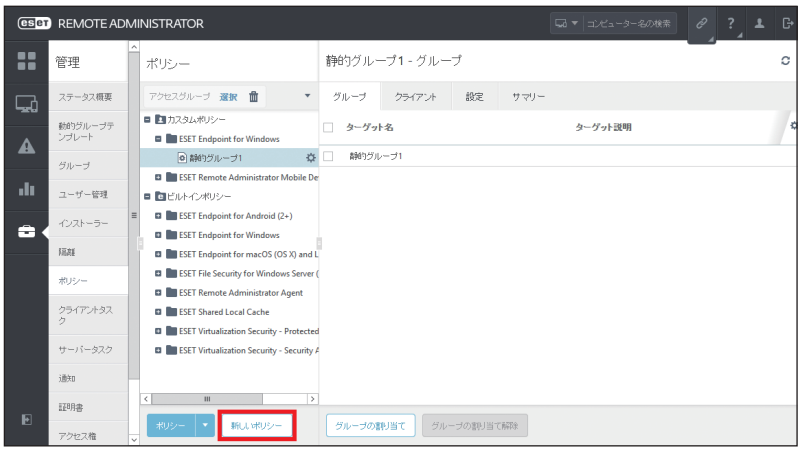
■「管理」メニューから作成する

・［ポリシー］>［ポリシー］ボタン >［新規作成］を選択します。



■［新しいポリシー］ボタンから作成する

・［新しいポリシー］ボタンをクリックします。

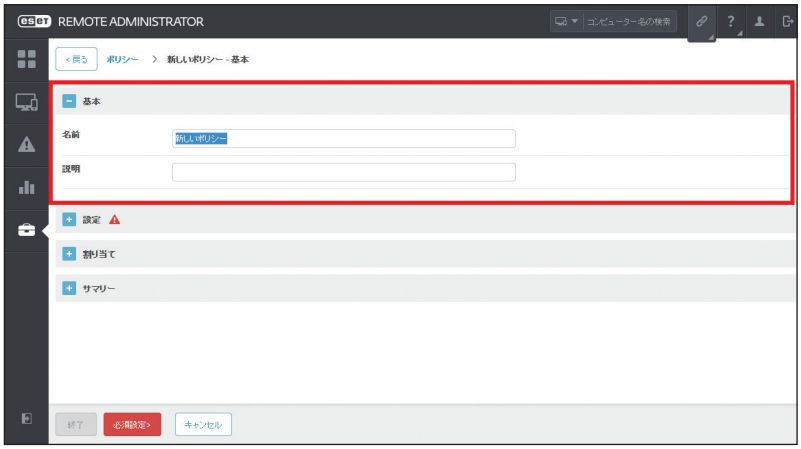


続く

操作手順

1 いずれかの方法で「新しいポリシー」画面を表示します。

2 「基本」の各項目を入力します。



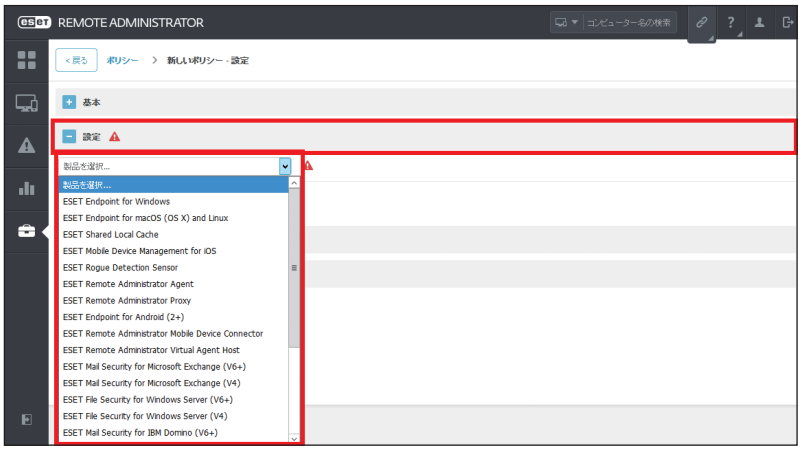
■基本

項目名	説明	必須
名前	作成するポリシーの名前を入力します。画面には、ここで設定した名前が表示されます。	○
説明	作成するポリシーの説明を入力します。	-

3 [設定] をクリックします。

4 ドロップダウンメニューから対象製品を選択します。

選択した製品の設定項目が表示されます。



続く

！重 要

ESET Endpoint Security および ESET Endpoint アンチウイルス用の設定は、［ESET Endpoint for Windows］を選択してください。
ESET Endpoint Security for OS X、ESET Endpoint アンチウイルス for OS X および ESET NOD32 アンチウイルス for Linux Desktop 用の設定は、［ESET Endpoint for mac0S（OS X）and Linux］を選択してください。
ESET File Security for Linux 用の設定は、［ESET Mail/File/Gateway Security for Linux/BSD/Solaris（V4）］を選択してください。
ESET Endpoint Security for Android の設定は、［ESET Endpoint for Android（V2+）］を選択してください。
iOS の設定は、［ESET Mobile Device Management for iOS］を選択してください。
製品によっては、ESET Remote Administrator のポリシーから設定できない項目があります。
また、選択肢の中には、日本ではリリースされていない製品の設定も含まれています。

5 該当するカテゴリをクリックし、各項目を入力します。

■設定

続く

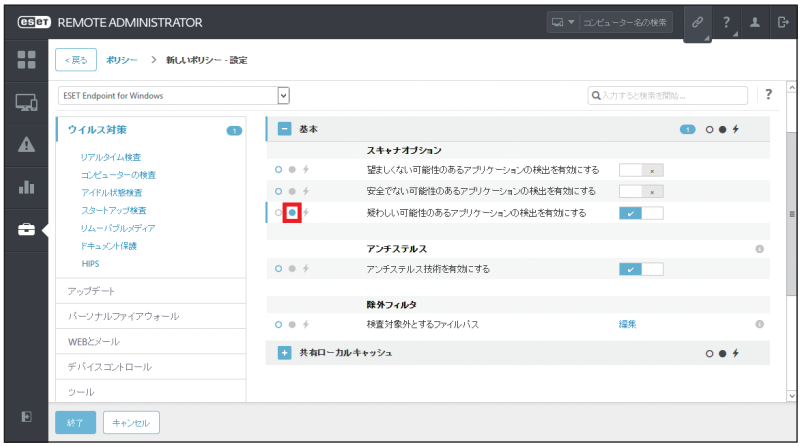
項目名	説明	必須
製品リスト	設定する製品を選択します。選択した製品に合わせたカテゴリや設定項目が下部に表示されます。	○
検索ボックス	製品を選択後に右上部に表示されます。設定したい項目を検索する場合にキーワードを入力します。該当する項目が黄色で表示されます。	-
カテゴリ	製品を選択後に左部に表示されます。目的のカテゴリをクリックすると右部に設定項目が表示されます。すべてのセクションのルールの合計数が右端に表示されます。 ※製品によっては表示されません。	○
設定項目範囲	選択した製品または選択したカテゴリに合わせた設定項目が表示されます。必要に応じて設定を編集します。	-
	追加したルールの数が表示されます。 セクションバーでは、セクション内で定義したルール数が表示されます。 カテゴリでは、カテゴリ内で定義したルールの総数が表示されます。	
	追加したいルールをポイントすると表示されます。ポイントしているルールを追加します。 セクションバーでは、セクション内のすべてのルールを追加します。	
	追加したルールをポイントすると表示されます。ポイントしているルールを削除します。 セクションバーでは、セクション内のすべてのルールを削除します。	
	フラグ フラグによってポリシーで処理される設定を追加します。各設定に対して、次のフラグのいずれかを選択できます。	
	このフラグの設定はポリシーによって設定されません。設定が適用されないため、他のポリシーによって後から変更できます。	
	選択した設定がクライアントコンピューターに送信され、ローカルに構成されていた内容に関係なく適用されます。ポリシーのマージの場合には、後のポリシーによって上書きされます。また、他のポリシーによって後から変更できます。	
	クライアントコンピューターに送信され、ローカルに構成されていた内容に関係なく適用されます。ポリシーのマージの場合には、後のポリシーによって上書きされません。	
	ポイントするとルールの説明が表示されます。	

ワンポイント

ポリシーのマージについては、「6.5.4.3 ポリシーのマージ」を参照してください。

続く

6 追加するルールの ● をクリックします。



適用フラグが設定されます。

ワンポイント

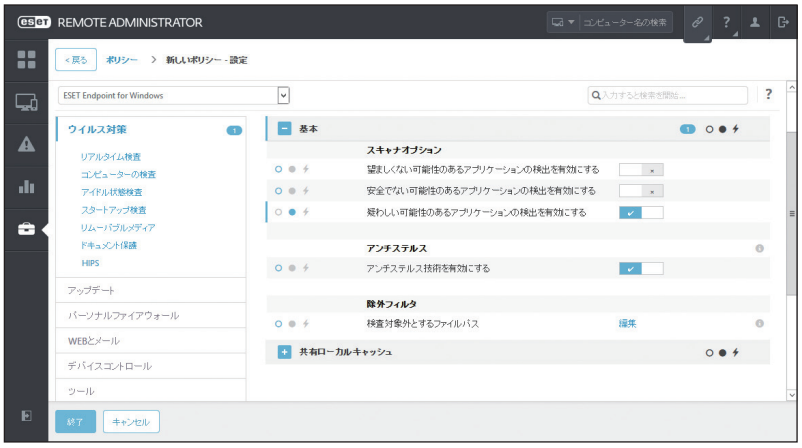
表示しているセクションのすべてのルールを追加する場合は、セクションバーの右側の ● をクリックします。

ワンポイント

追加したルールを削除する場合は、削除するルール ○ をクリックします。

表示しているセクションで追加したすべてのルールを削除する場合は、セクションバーの右側の ○ をクリックします。

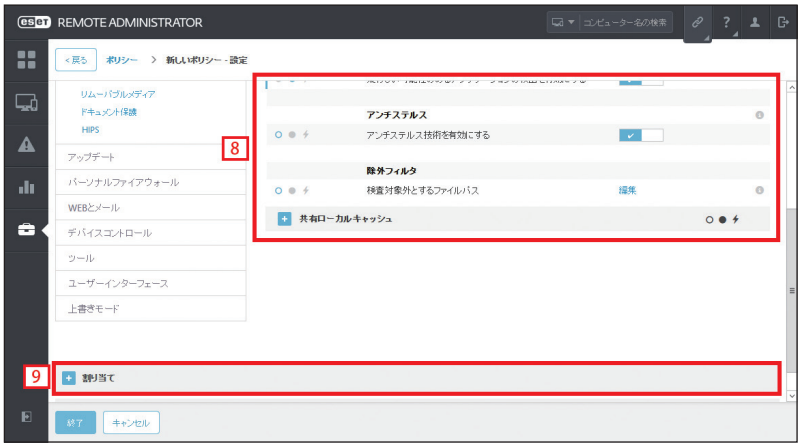
7 必要に応じて「フラグ」を変更します。



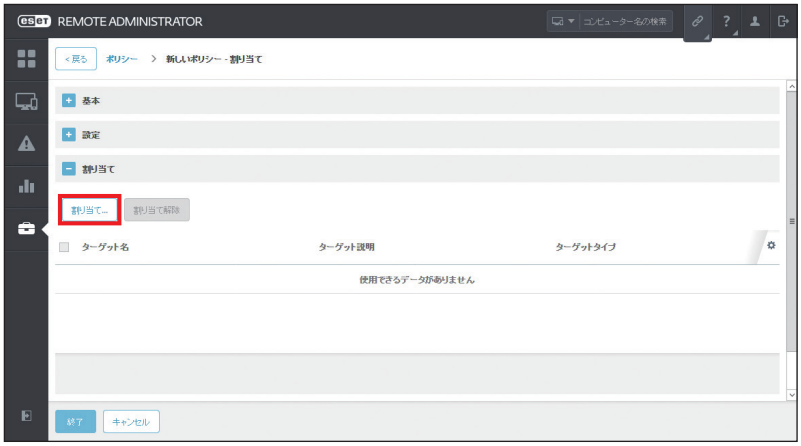
8 複数のルールを追加する場合は、手順 5 ～手順 7 を繰り返します。

続く

9 [割り当て] をクリックします。



10 [割り当て] ボタンをクリックします。



ターゲットを選択する画面が表示されます。

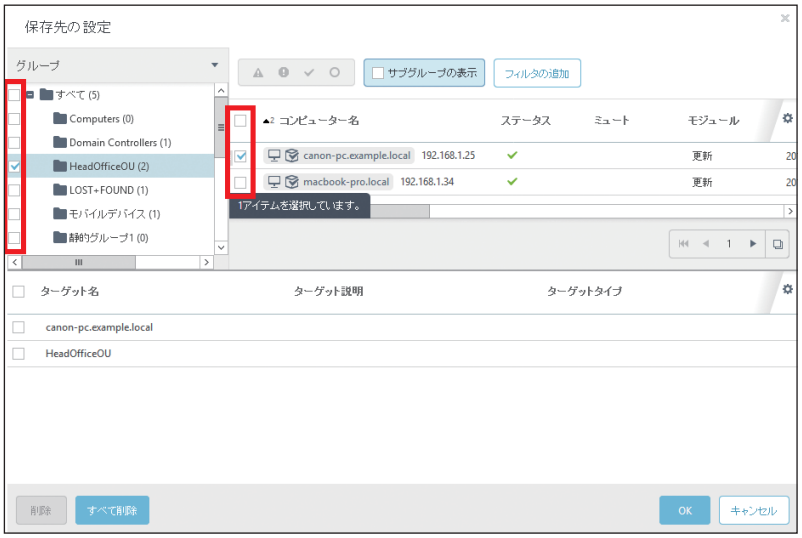
■割り当て

項目名	説明	必須
割り当て	作成するポリシーを割り当てるターゲットを設定します。ターゲットを選択する画面が表示されます。	○
割り当て解除	ターゲットリストから割り当てを解除する行にチェックを入れると表示されます。選択したターゲットへのポリシーの割り当てを解除します。	-
ターゲットリスト	ターゲットを選択する画面で選択したターゲットリストが表示されます。	-

続く

11 ターゲットを選択します。

グループを選択する場合は左上部のグループリストを、コンピューターを選択する場合は右上部のコンピューターリストにチェックを入れます。
下部のターゲットリストに選択したターゲットが表示されます。



ワンポイント

割り当てたクライアントコンピューターを削除する場合は、ターゲットリストから削除するクライアントコンピューターにチェックを入れ、［削除］ボタンをクリックします。
割り当てたすべてのターゲットを削除する場合は、［すべて削除］ボタンをクリックします。

12 ［OK］ボタンをクリックします。

ターゲットリストが表示されます。

13 ［サマリー］をクリックします。

「基本」および「割り当て」に入力した内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。

14 ［終了］ボタンをクリックします。

ポリシーが作成されます。

6.5.3 iOS デバイス管理用のポリシーを作成する

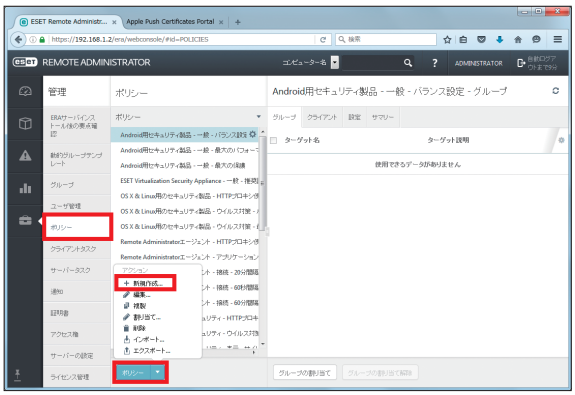
ここでは、iOS デバイスの管理を ERA サーバーで行うためのポリシーの作成方法を解説します。

6.5.3.1 iOS デバイス登録用のポリシーを作成する

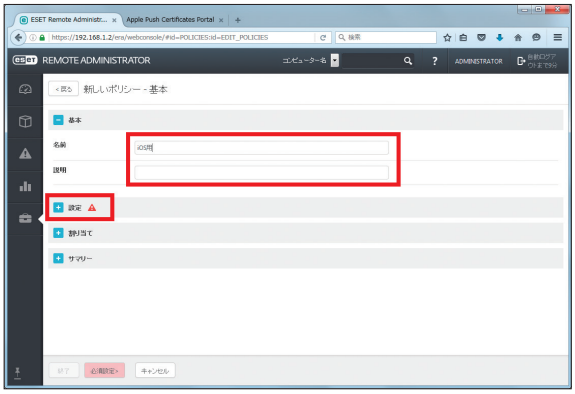
ここでは、Mobile Device Connector で APNS(Apple Push Notification Services) および iOS デバイス登録機能を有効にするための新しいポリシーを作成する方法の例を示します。これは iOS デバイスの登録に必要です。このポリシーを構成する前に、Apple Push Certificates Portal で Apple 社の署名付きの APN 証明書を作成しておく必要があります。Apple 社の署名付き APN 証明書の詳細な作成手順については、「6.9.3 APN 証明書」をご参照ください。

操作手順

1. ［ポリシー］タブ＞［ポリシー］＞［新規作成］をクリックし、新しいポリシーを作成します。

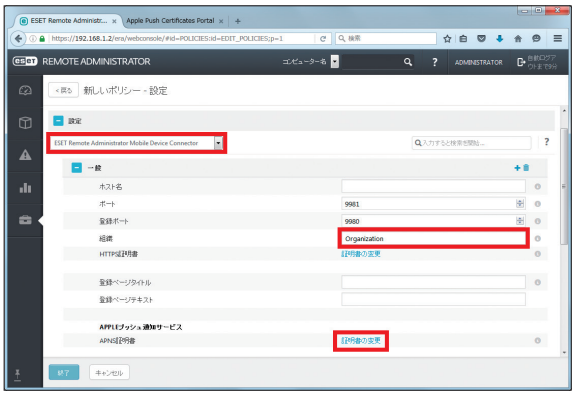


2. 必要に応じて作成するポリシーの名前を入力し、［設定］をクリックします。



続く

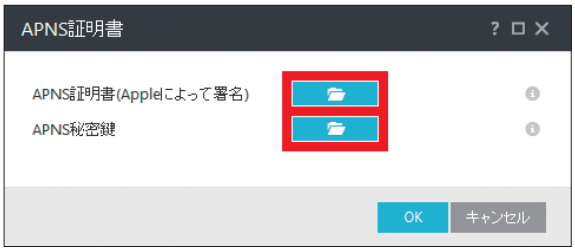
3 ドロップダウンリストから［ESET Remote Administrator Mobile Device Connector］を選択します。組織の入力を行い、APNS 証明書の［証明書の変更］をクリックします。



！重　要

組織の項目欄には実際の組織名を入力してください。組織名は、プロファイルの作成に利用されます。

4 をクリックして、Apple 社の署名付き APN 証明書と秘密鍵をアップロードします。



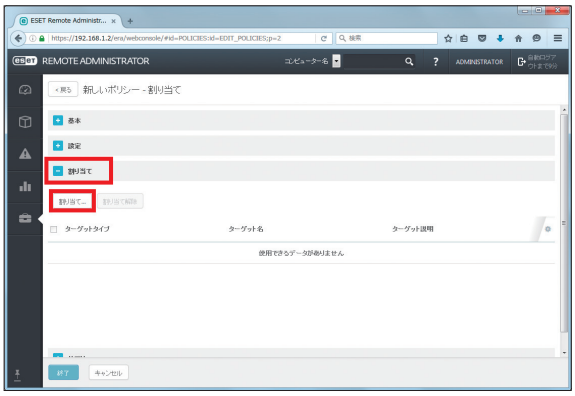
5 Apple 社の署名付き APN 証明書と秘密鍵をアップロードしたら［OK］ボタンをクリックします。

ワンポイント

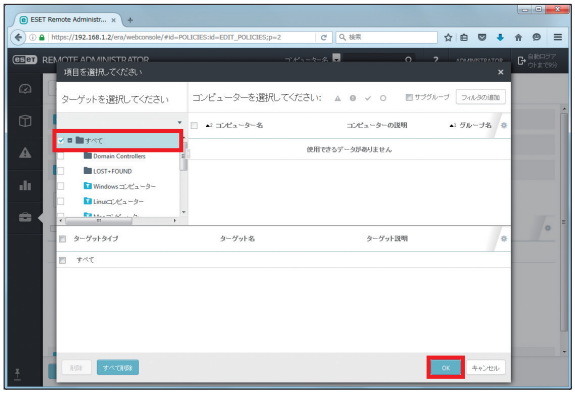
その他の各設定項目の詳細については、「7.1.4　Mobile Device Connector の設定項目」をご参照ください。

続く

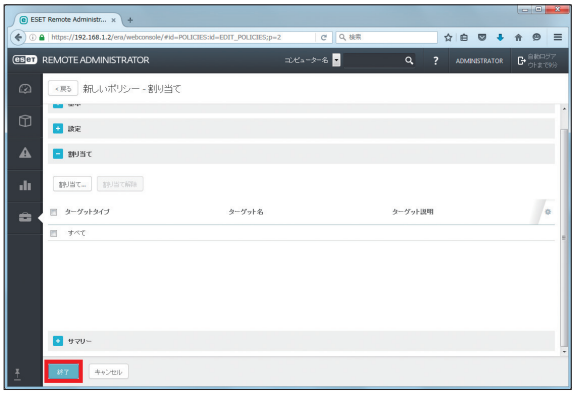
6 ［割り当て］＞［割り当て ...］とクリックして作成するポリシーを割り当てるコンピューター（Mobile Device Connector がインストールされているサーバー）を選択します。



7 作成するポリシーを割り当てるコンピューターをクリックし、［OK］をクリックします。



8 ［終了］ボタンをクリックします。



6.5.3.2 Exchange ActiveSync アカウントのポリシーを作成する

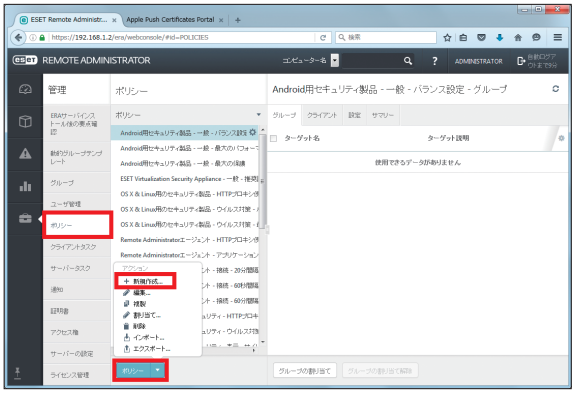
このポリシーを使用して、ユーザーの iOS デバイスの Microsoft Exchange メールアカウント、連絡先、カレンダーを構成できます。このようなポリシーを使用する利点は、各デバイスのポリシーを個別に設定せずに、1 つのポリシーで複数の iOS デバイスに適用できる点です。これは Active Directory ユーザー属性を使用して実現されます。たとえば、${exchange_login/exchange} のような変数を指定する必要があります。これは、特定のユーザーの AD の値で置換されます。

ワンポイント

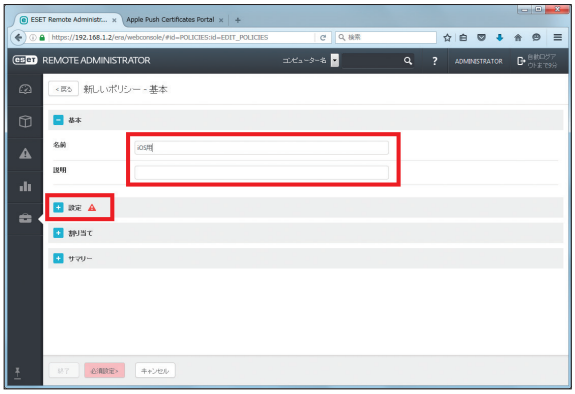
Microsoft Exchange または Exchange ActiveSync を使用していない場合は、各サービス（メールアカウント、連絡先アカウント、LDAP アカウント、カレンダーアカウント、登録されたカレンダーアカウント）を手動で構成できます。

操作手順

1 ［ポリシー］タブ>［ポリシー］>［新規作成］をクリックし、新しいポリシーを作成します。

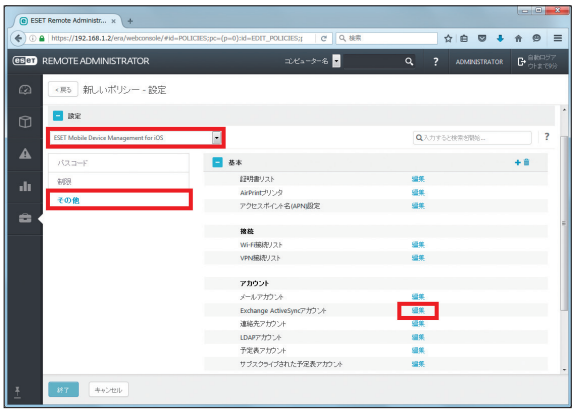


2 必要に応じて作成するポリシーの名前を入力し、［設定］をクリックします。

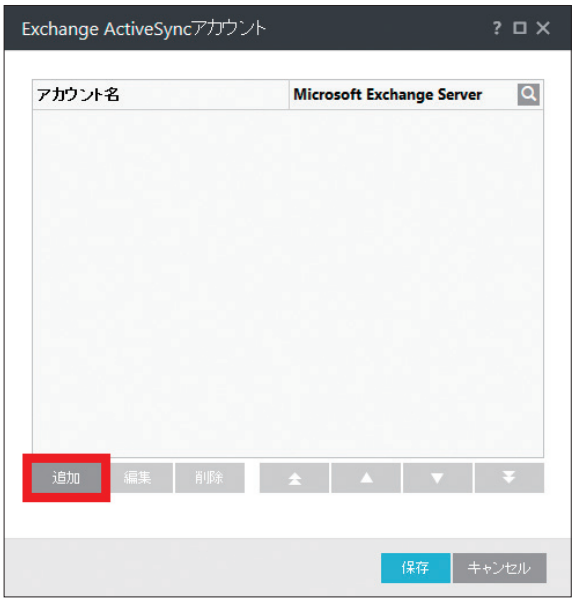


続く

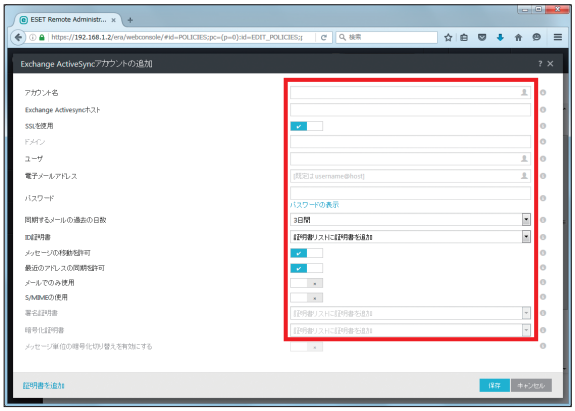
3 ドロップダウンリストから［ESET Mobile Device Management for iOS］を選択し、［その他］をクリックしてカテゴリを展開し、Exchange ActiveSync アカウントの横にある編集をクリックします。



4 ［追加］をクリックします。



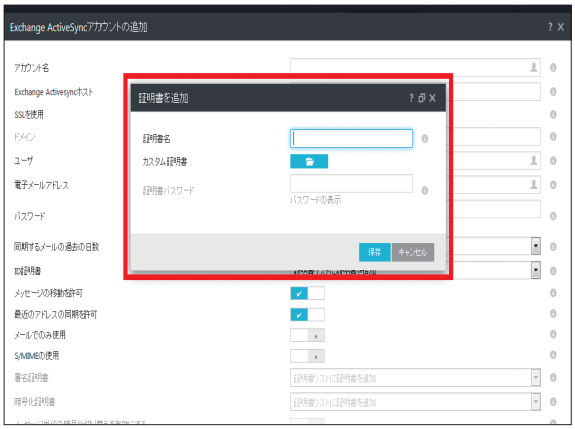
5 Exchange ActiveSync アカウントの詳細を指定します。ユーザーやメールアドレスなど、特定のフィールドで変数をドロップダウンリストから選択して使用できます。これらの変数は、ポリシーが適用されるときに、ユーザー管理の実際の値で置換されます。



続く

項目名	説明
アカウント名	Exchange アカウントの名前を入力します。これは、ユーザーまたは管理者がメール / 連絡先 / カレンダーアカウントを特定するためのものです。
Exchange ActiveSync ホスト	Exchange サーバーのホスト名または IP アドレスを指定します。
SSL を使用	このオプションは、デフォルトでは有効になっています。Exchange サーバーが認証で Secure Sockets Layer（SSL）を使用するかどうかを指定します。
ドメイン	このフィールドは任意です。このアカウントが属するドメインを入力できます。
ユーザー	Exchange ログイン名。ドロップダウンリストから該当する変数を選択し、各ユーザーの Active Directory から属性を使用します。
電子メールアドレス	ドロップダウンリストから該当する変数を選択し、各ユーザーの Active Directory から属性を使用します。
パスワード	任意。このフィールドを空欄にすることをお勧めします。空欄にする場合、ユーザーが独自のパスワードを作成する必要があります。
同期するメールの過去の日数	ドロップダウンリストからメールを同期する過去の日数を選択します。
ID 証明書	ActiveSync に接続するための認証情報。
メッセージの移動を許可	有効な場合、アカウント間でメッセージを移動できます。
最近のアドレスの同期を許可	このオプションが有効な場合、ユーザーは最近使用したアドレスをデバイス間で同期できます。
メールでのみ使用	メールアプリのみがこのアカウントから電子メールメッセージを送信することを許可する場合は、このオプションを有効にします。
S/MIME を使用	送信メールメッセージで S/MIME 暗号化を使用する場合は、このオプションを有効にします。
署名証明書	MIME データを署名するための認証資格情報。
暗号化証明書	MIME データを暗号化するための認証資格情報。
メッセージ単位の暗号化切り替えを有効にする	ユーザーは各メッセージを暗号化するかどうかを選択できます。

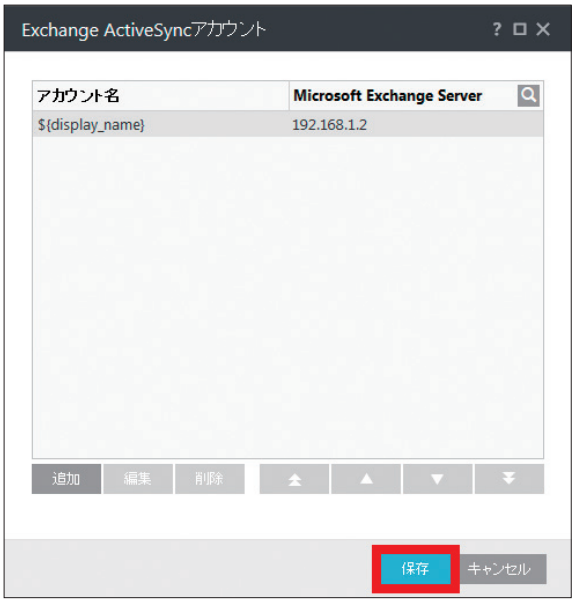
6 ［証明書の追加］をクリックすると、必要に応じて、特定の Exchange 証明書（ユーザー ID、デジタル署名、暗号化証明書）を追加できます。



続く

7 すべての設定を行ったら［保存］ボタンをクリックします。

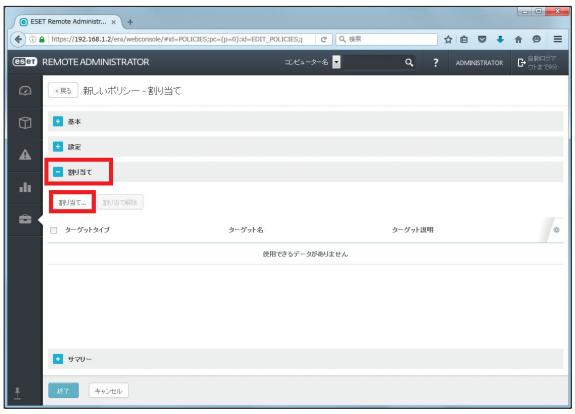
8 ［保存］ボタンをクリックします。



ワンポイント

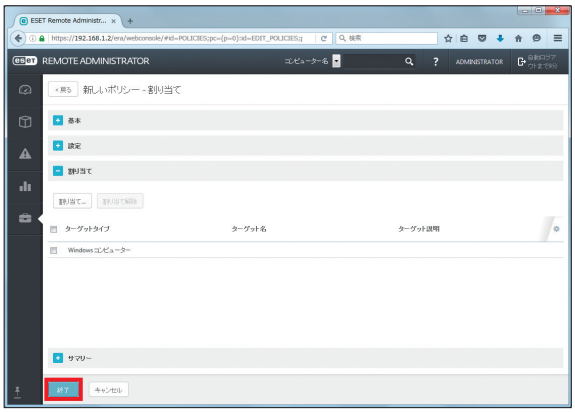
手順 4 からの操作を繰り返して行うことで複数のアカウントを追加できます。

9 ［割り当て］＞［割り当て ...］とクリックして作成するポリシーを受信コンピュータ／モバイルデバイスまたはグループ全体を選択します。



続く

10 作成するポリシーを受信コンピュータ／モバイルデバイスの設定が完了したら、[終了] ボタンをクリックします。



6.5.3.3 iOS および Wi-Fi 接続で制限を適用するポリシーの作成

iOS デバイスのポリシーを作成し、特定の制限を適用できます。また、複数の Wi-Fi 接続を定義し、たとえばユーザーが別のオフィスに移動したときにそこに設置された Wi-Fi ネットワークに自動的に接続させることができます。また、VPN 接続でも同様のことができます。

iOS デバイスに適用できる制限はカテゴリに一覧表示されます。たとえば、FaceTime とカメラの使用を無効にしたり、特定の iCloud 機能を無効にしたり、セキュリティとプライバシーオプションを微調整したり、選択したアプリケーションを無効にしたりできます。

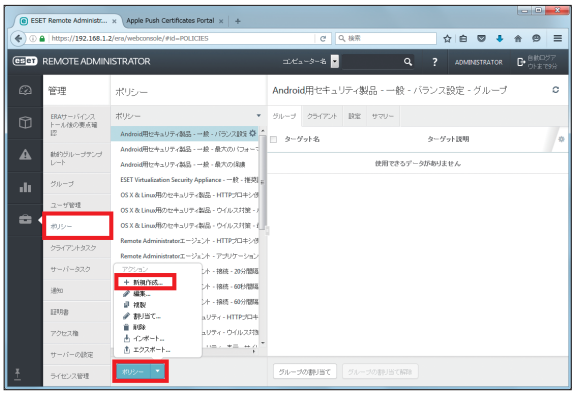
! 重 要

適用できる制限とできない制限は、iOS デバイスにインストールされている iOS のバージョンによって異なります。iOS 8.x 以降がサポートされます。

操作手順

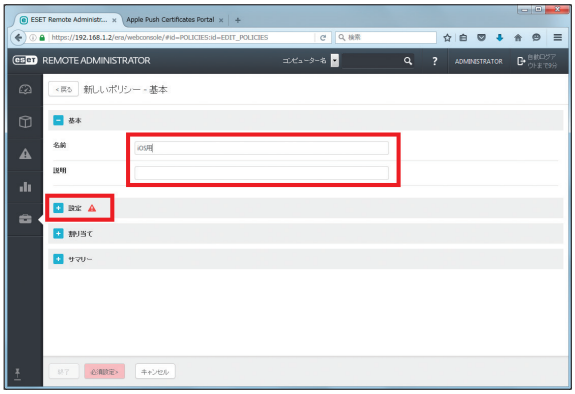
ここでは、カメラと FaceTime アプリを無効にし、Wi-Fi 接続詳細を一覧に追加して、ネットワークが検出されるたびに iOS デバイスを Wi-Fi ネットワークに自動接続させる方法の例を示します。自動参加オプションを使用する場合は、iOS デバイスが既定でネットワークに接続します。ポリシー設定は、ユーザーが手動で選択した Wi-Fi ネットワークを上書きします。

1 [ポリシー] タブ> [ポリシー] > [新規作成] をクリックし、新しいポリシーを作成します。

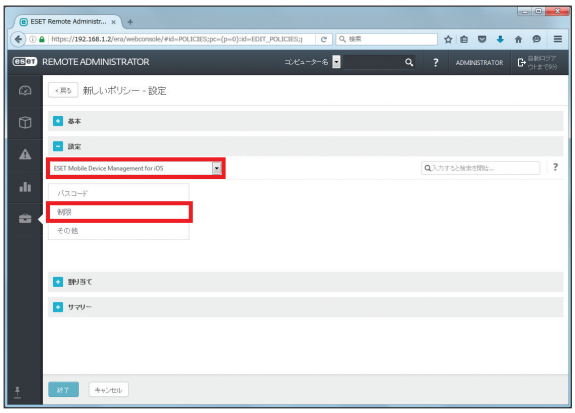


続く

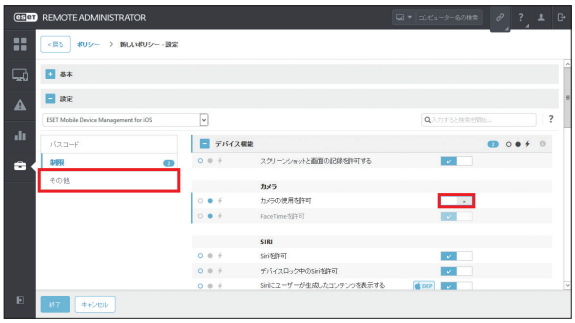
2 必要に応じて作成するポリシーの名前を入力し、［設定］をクリックします。



3 ドロップダウンリストから［ESET Mobile Device Management for iOS］を選択し、［制限］をクリックします。

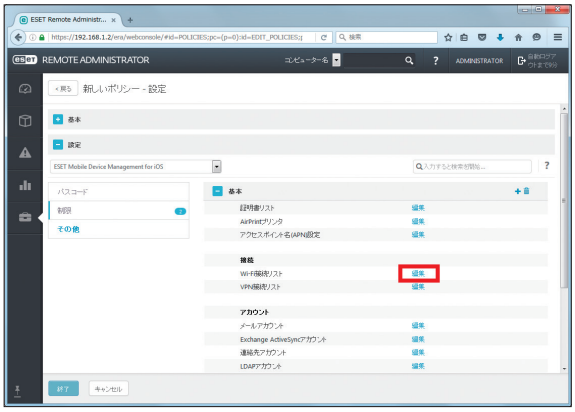


4 ［カメラの使用を許可］のスチッチをクリックして無効にします。カメラが無効になるため、FaceTime も自動的に無効になります。FaceTime のみを無効にする場合は、カメラを有効にした状態で、［FaceTime を許可］のスイッチを使用して無効にします。［その他］をクリックします。



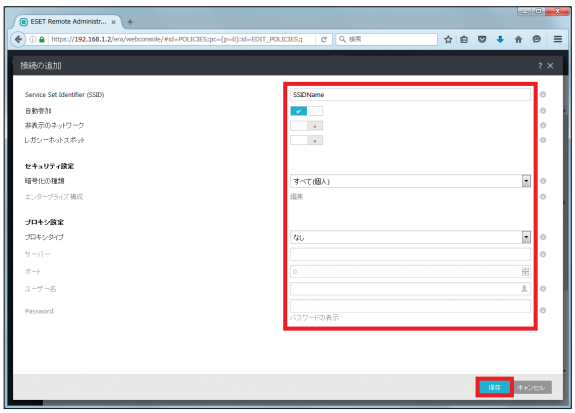
続く

5 Wi-Fi 接続リストの［編集］をクリックします。



6 Wi-Fi 接続リストのウィンドウが開きます。［追加］をクリックます。

7 追加する Wi-Fi ネットワークの接続詳細情報を設定します。すべての情報を設定したら、［保存］ボタンをクリックします。



続く

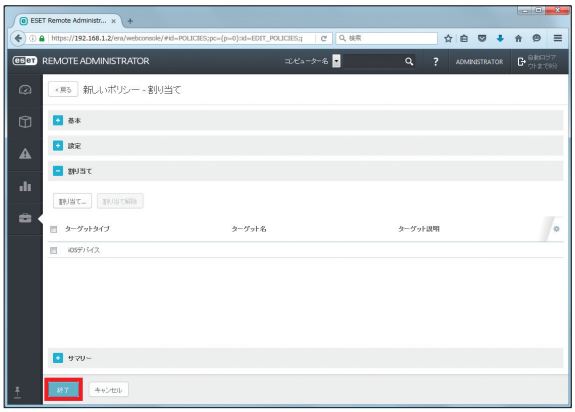
項目名	説明
Service Set Identifier（SSID）	使用される Wi-Fi ネットワークの SSID。
自動参加	任意（既定では有効）。デバイスが自動的にこのネットワークに参加します。
非表示のネットワーク	任意（既定では無効）SSID の公開を行っていないネットワークへに接続します。
レガシーホットスポット	任意（既定では無効）レガシーホットスポットへの接続を許可します。
暗号化種類	ドロップダウンリストから該当する暗号化の方法を選択します。
エンタープライズ構成	暗号化の種類でエンタープライズ向けの暗号化を選択した場合に設定できます。認証方法などの詳細設定を行えます。
プロキシ設定	任意。ネットワークがプロキシを使用する場合に設定します。

8 ［保存］ボタンをクリックします。

9 ［割り当て］＞［割り当て ...］とクリックして作成するポリシーを受信コンピュータ／モバイルデバイスまたはグループ全体を選択します。

続く

10 作成するポリシーを受信コンピュータ／モバイルデバイスの設定が完了したら、[終了] ボタンをクリックします。

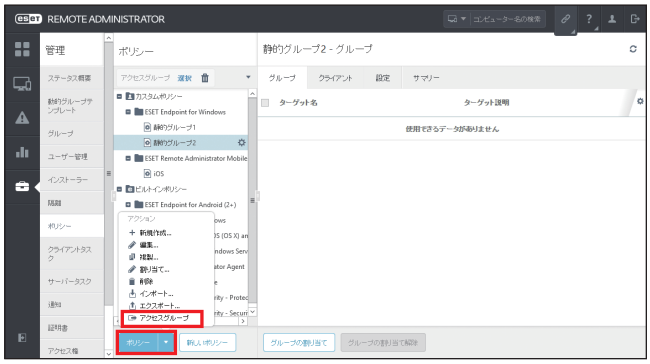


6.5.3.4 「アクセスグループ」でポリシーを別グループに移動

作成したポリシーを別グループに移動する方法を説明します。

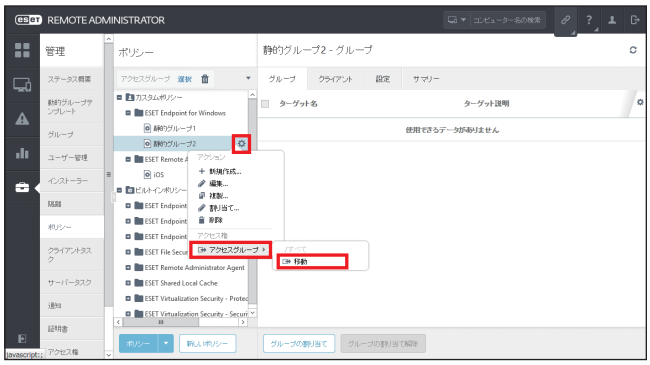
■「管理」メニューから移動する

・[ポリシー] > [アクセスグループ] を選択します。



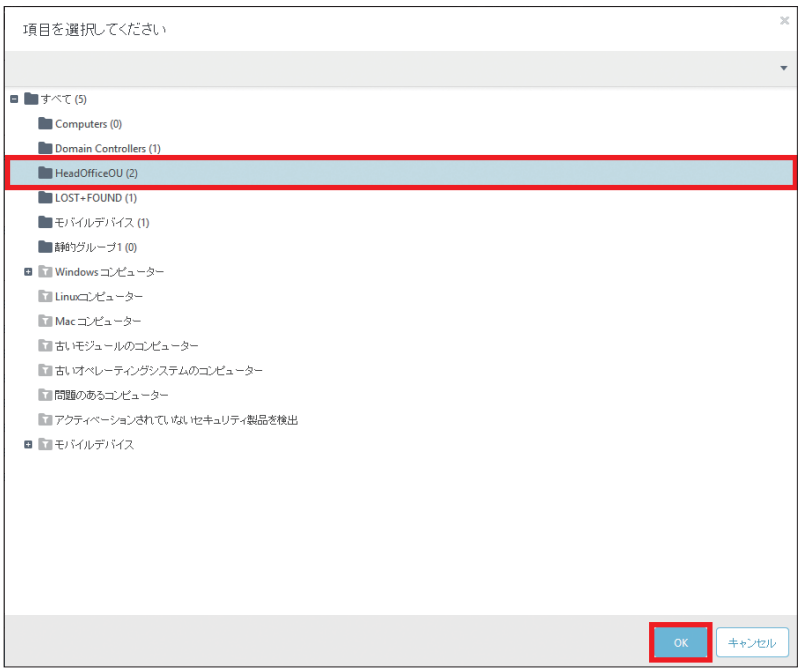
■コンテキストメニューから移動する

・ > [アクセスグループ] > [移動] を選択する



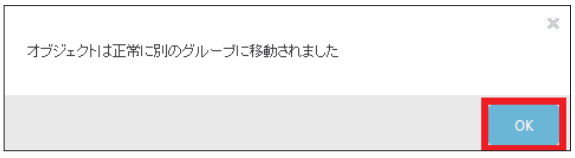
操作手順

1. いずれかの方法で「項目を選択してください」画面を表示します。
2. 移動先のグループをクリックし、[OK] ボタンをクリックします。



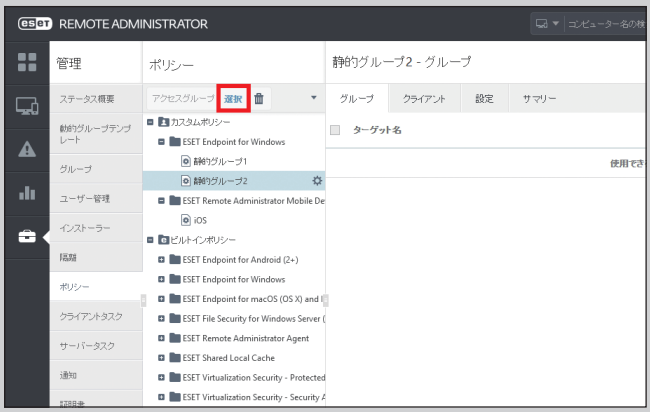
手順 2 で選択したグループに、選択したポリシーが移動してダイアログボックスが表示されます。

3. [OK] ボタンをクリックします。



! 重 要

選択したポリシーが目的のグループに移動したかどうかを確認したいときは、「アクセスグループ」のフィルターを利用します。「アクセスグループ」の［選択］をクリックすると「項目を選択してください」画面が表示されるので、表示したいグループをクリックして、［OK］ボタンをクリックします。選択したグループのポリシーが一覧表示されます。フィルターを解除したいときは、🗑をクリックします。



6.5.4 ポリシーの適用

グループおよびクライアントコンピューターには、複数のポリシーを割り当てることができます。
ポリシーを適用する順序は重要です。クライアントコンピューターに適用されるポリシーは、グループの順序とグループに割り当てられたポリシーの順序に基づきます。
次の手順に沿って、クライアントコンピューターに有効なポリシーを決定します。

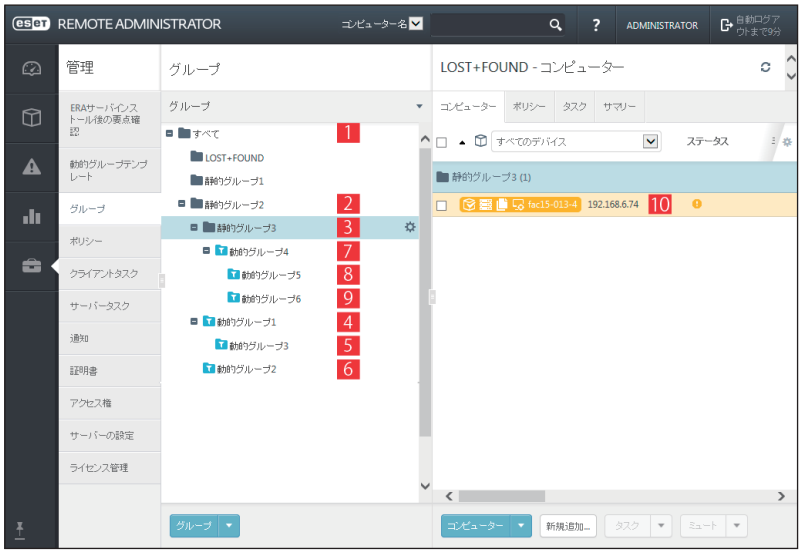
STEP1	クライアントが配置されているグループの順序を確認する	「6.5.4.1 グループの順序」参照
STEP2	割り当てられたポリシーでグループを置換する	「6.5.4.2 ポリシーの列挙」参照
STEP3	ポリシーを統合して最終設定を取得する	「6.5.4.3 ポリシーのマージ」参照

6.5.4.1 グループの順序

ポリシーは、グループツリーの最上位の「すべて」グループから上位階層順に適用されます。これにより、グループツリーの最上位にすべてのコンピューターに対して適用するポリシーを作成し、子グループに対して個別のポリシーを適用できます。ツリーの上位にあるグループにアクセスできる ERA ユーザーは、フラグを使用して下位のグループのポリシーを上書きできます。グループにポリシーを割り当てる場合は、次の順序に沿って適用されます。

ルール 1	静的グループは最上位の「すべて」グループから評価する。
ルール 2	すべての階層において、静的グループはツリーの表示順に評価する。
ルール 3	特定の階層のすべての静的グループがリストに入った後、動的グループを評価する。
ルール 4	動的グループの子グループは、リストの表示順に評価する。
ルール 5	任意の階層の動的グループに子グループがある場合は、リストに追加され、子グループが検索される。子グループが無くなったら、親レベルの次の動的グループがリストに入る。
ルール 6	コンピューターは最後に評価する。

上記のルールに沿った実際の処理は次のとおりです。



処理手順

1. ルール 1 に従い、最上位グループの「すべて」がリストに追加されます。
   同階層に他のグループがないため、次の階層のグループが評価されます。

2. 第 2 階層グループの「LOST+FOUND」「静的グループ 1」および「静的グループ 2」が評価されます。ここで、実際のコンピューターは「すべて」「静的グループ 2」「静的グループ 3」だけに属しているとします。その場合、メンバーが属していない「LOST+FOUND」「静的グループ 1」を評価する必要はありません。「静的グループ 2」は、第 2 階層で評価される唯一のグループです。

3. 第 3 階層グループの「静的グループ 3」「動的グループ 1」「動的グループ 2」が評価されます。ルール 2 に従い、「静的グループ 3」が最初にリストに追加されます。ルール 3 に従い、「静的グループ 3」が最後の静的グループであるため、次に「動的グループ 1」を評価します。同階層の「動的グループ 2」を評価する前に、ルール 5 に従い、「動的グループ 1」の子グループを評価する必要があります。

4. 第 4 階層グループの「動的グループ 3」がリストに追加されます。子グループが無いため、親階層の第 3 階層に上がります。

5. 第 3 階層グループの「動的グループ 2」がリストに追加されます。子グループが無いため、第 3 階層のグループは終了です。次の階層に進みます。

6. 第 4 階層グループの「動的グループ 4」とコンピューター自体が評価されます。ルール 6 に従い、コンピューターは最後に評価します。「動的グループ 4」がリストに追加されます。2 つの子グループがあるため、同階層の次のグループに進む前に子グループを評価する必要があります。

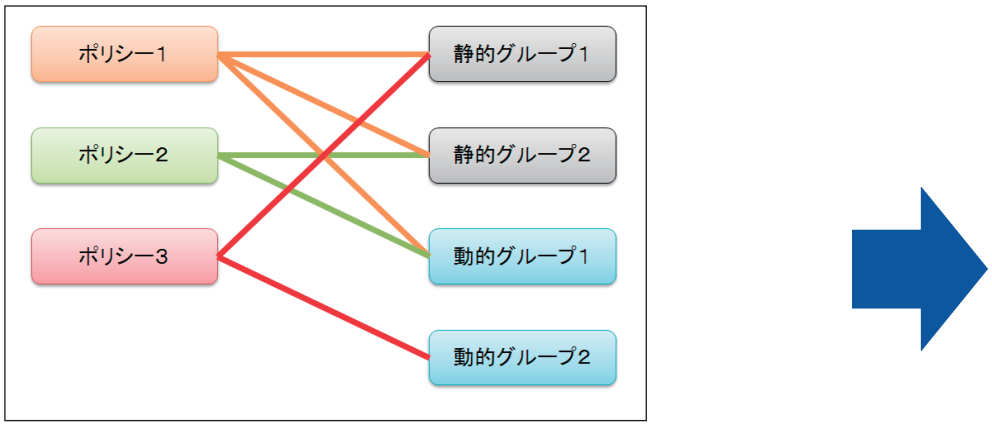
7. ルール 4 に従い、「動的グループ 5」と「動的グループ 6」がリストに追加されます。いずれも子グループが無いため、最後にコンピューターがリストに追加され、評価が終了します。

以上のように整理すると、作成されたポリシーの適用順序は次のとおりです。

1. すべて
2. 静的グループ 2
3. 静的グループ 3
4. 動的グループ 1
5. 動的グループ 3
6. 動的グループ 2
7. 動的グループ 4
8. 動的グループ 5
9. 動的グループ 6
10. コンピューター

6.5.4.2 ポリシーの列挙

グループの順序を把握したら、グループに割り当てられたポリシーで各グループを置換します。ポリシーは、グループに割り当てられた順序で一覧表示されます。ポリシーが無いグループはリストから削除されます。グループに複数のポリシーが割り当てられている場合は、ポリシーの優先度を編集できます。各ポリシーは 1 つの製品（ERA エージェント、ERA プロキシ、ESET Endpoint Security など）だけを構成します。
例として、前述のグループには次のようにポリシーが割り当てられているとします。



「静的グループ 1」にはポリシーが割り当てられていますが、実際にはコンピューターが属していないため、ポリシーの適用順序からは除外されています。
ポリシーの適用順序は次のように変換され、最終リストが決定されます。

1	すべて	ポリシーが無いため削除
2	静的グループ 2	ポリシー 1、ポリシー 2
3	静的グループ 3	ポリシーが無いため削除
4	動的グループ 1	ポリシー 1、ポリシー 2
5	動的グループ 3	ポリシーが無いため削除
6	動的グループ 2	ポリシー 3
7	動的グループ 4	ポリシーが無いため削除
8	動的グループ 5	ポリシーが無いため削除
9	動的グループ 6	ポリシーが無いため削除
10	コンピューター	ポリシーが無いため削除

1	ポリシー 1
2	ポリシー 2
3	ポリシー 1
4	ポリシー 2
5	ポリシー 3

6.5.4.3 ポリシーのマージ

通常、クライアントに適用されたポリシーは、複数のポリシーが最終的に 1 つのポリシーにマージされたものです。ポリシーは 1 つずつマージされます。ポリシーをマージするときの原則は、前のポリシーで構成された設定が、後のポリシーによって上書きされるということです。この動作を変更するには、ポリシーフラグ（「6.5.2 新しいポリシーの作成」の「■設定」参照）を使用します。設定は 1 つずつマージされます。
グループの構造とポリシーの順序によってポリシーのマージ方法が決まります。任意の 2 つのポリシーをマージしても、順序によっては結果が異なる場合があります。

! 重 要

グループツリーの上位にあるグループには、より汎用的なポリシー（アップデートサーバーの設定など）を割り当てることを推奨します。通常、マージの際に下位のポリシーが上位の設定を上書きします（ポリシーフラグで定義されている場合を除く）ので、より特定のポリシー（デバイスコントロール設定など）はグループツリーの下位に割り当てます。

6.5.5 グループへのポリシーの割り当て

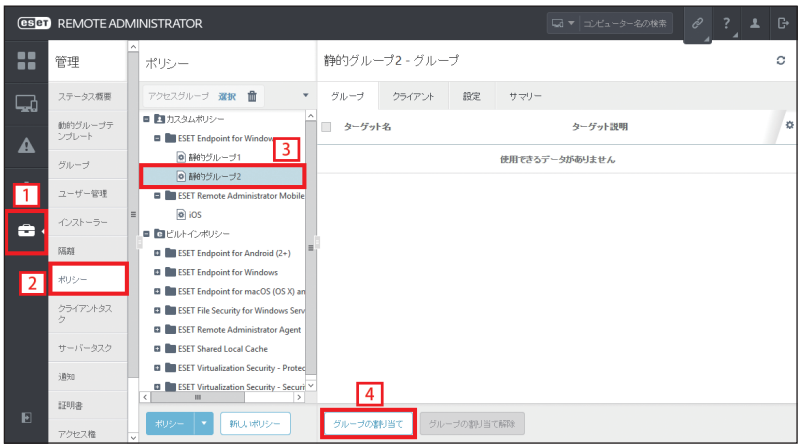
作成したポリシーは、静的または動的グループに割り当てることができます。

6.5.5.1 1 つのポリシーをグループに割り当てる

1 つのポリシーを複数のグループにまとめて割り当てる方法を説明します。

操作手順

1. ［管理］メニューをクリックします。
2. ［ポリシー］サブメニューをクリックします。
3. ポリシーリストから割り当てるポリシーを選択します。
4. ［グループの割り当て］ボタンをクリックします。



グループリストが表示されます。

5. 割り当てるグループにチェックを入れます。

続く

6 [OK] ボタンをクリックします。

グループにポリシーが割り当てられます。

6.5.5.2 複数のポリシーを適用順にグループに割り当てる

「ポリシーアプリケーション順序」画面を使って、複数のポリシーを適用したい順番に割り当てる方法を説明します。

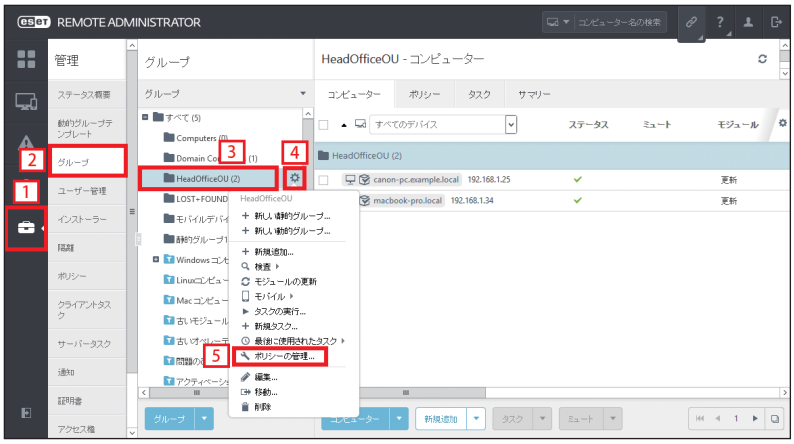
操作手順

1 [管理] メニューをクリックします。

2 [グループ] サブメニューをクリックします。

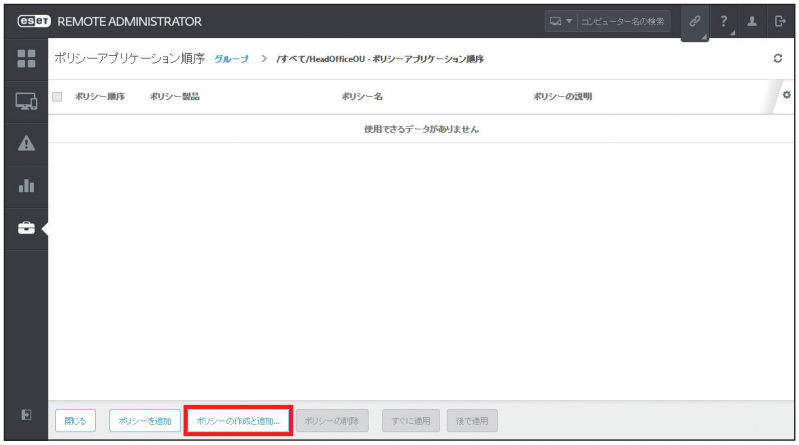
3 グループリストから割り当てるグループを選択します。

4 をクリックし、[ポリシーの管理] を選択します。



「ポリシーアプリケーション順序」画面が表示されます。

5 [ポリシーの作成と追加] ボタンをクリックします。



ポリシーリストが表示されます。

続く

6 追加したい順番に該当のポリシーにチェックを入れます。

ワンポイント

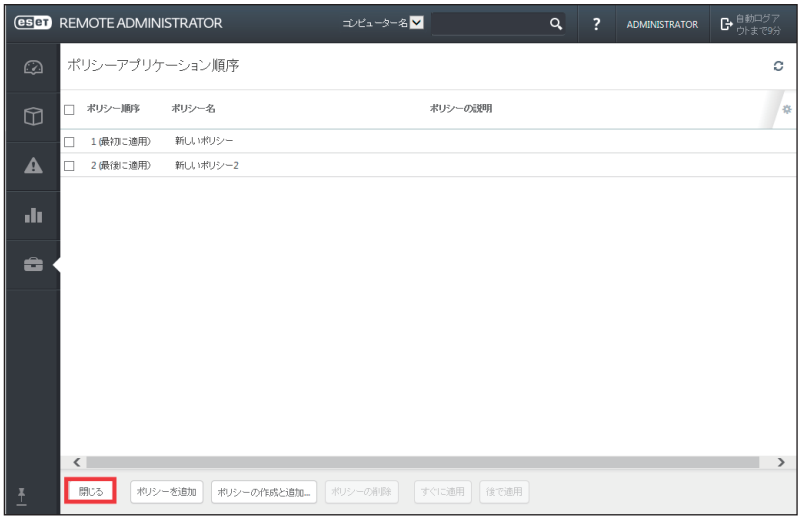
チェックを入れ順番を記憶しますので、適用したい順番に沿ってチェックを入れてください。順番は後から変更できます。

7 [OK] ボタンをクリックします。

チェックを入れた順番にポリシーアプリケーション順序リストに追加されます。

8 [閉じる] ボタンをクリックします。

複数のポリシーが適用順にグループに割り当てられます。

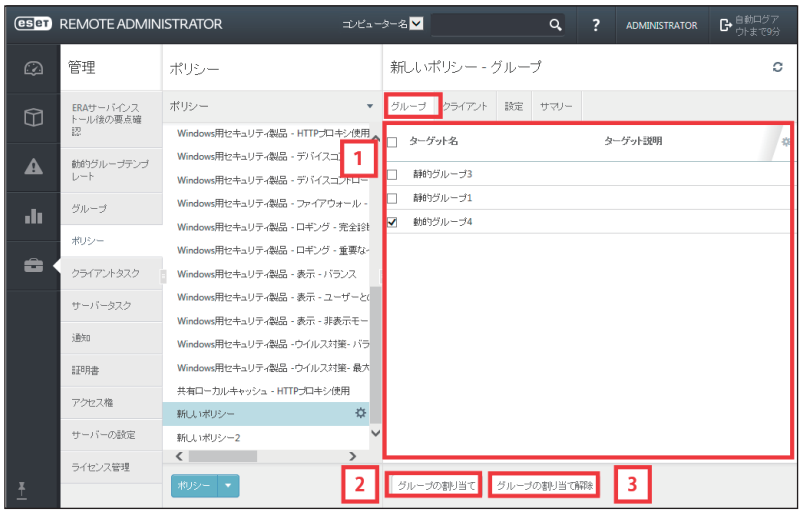


■ポリシーアプリケーション順序画面

ポリシー順序リスト	適用される順番にポリシーリストが表示されます。	
	ポリシー順序	適用される順番が表示されます。
	ポリシー名	ポリシー名が表示されます。
	ポリシーの説明	ポリシーの説明が表示されます。
ポリシーを追加	ポリシーリストが表示されます。追加するポリシーを選択します。	
ポリシーの作成と追加	新しいポリシーを作成し、追加します。「新しいポリシー」画面が表示されます。 画面の詳細については、「6.5.2 新しいポリシーの作成」を参照してください。	
ポリシーの削除	選択しているポリシー（複数選択可）を削除します。	
すぐに適用	選択しているポリシーの順序を繰り上げます。	
後で適用	選択しているポリシーの順序を繰り下げます。	

6.5.5.3 「グループ」タブ画面の構成

「グループ」タブには、選択しているポリシーが割り当てられているグループのリストが表示されます。グループの割り当てや割り当ての解除が行えます。



1	**グループリスト**	選択しているポリシーが割り当てられているグループリストが表示されます。
2	**グループの割り当て**	選択しているポリシーをグループに割り当てます。
3	**グループの割り当て解除**	選択しているグループから選択しているポリシーの割り当てを解除します。

6.5.6 クライアントコンピューターへのポリシーの割り当て

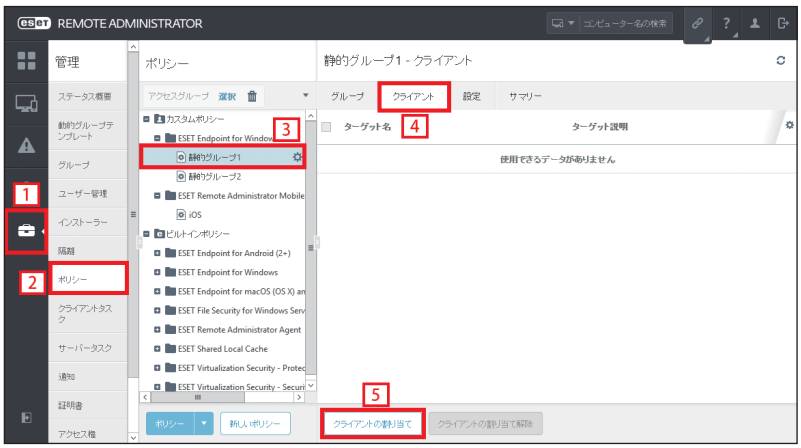
作成したポリシーは、クライアントコンピューターに割り当てることができます。

6.5.6.1 1 つのポリシーをクライアントコンピューターに割り当てる

1 つのポリシーを複数のクライアントコンピューターにまとめて割り当てる方法を説明します。

操作手順

1. ［管理］メニューをクリックします。
2. ［ポリシー］サブメニューをクリックします。
3. ポリシーリストから割り当てるポリシーを選択します。
4. ［クライアント］タブをクリックします。
5. ［クライアントの割り当て］ボタンをクリックします。



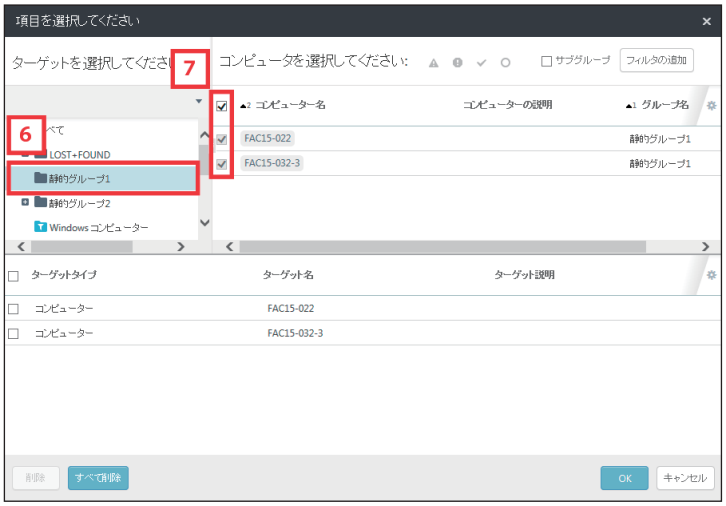
ターゲットを選択する画面が表示されます。

続く

6 割り当てるコンピューターが属しているグループを選択します。

7 コンピューターリストから割り当てるコンピューターにチェックを入れます。

下部のターゲットリストに選択したコンピューターが表示されます。



8 [OK] ボタンをクリックします。

「クライアント」タブのターゲットリストに、追加したコンピューターが表示されます。

ワンポイント

割り当てたクライアントコンピューターを削除する場合は、ターゲットリストから削除するクライアントコンピューターにチェックを入れ、[削除] ボタンをクリックします。
割り当てたすべてのターゲットを削除する場合は、[すべて削除] ボタンをクリックします。

6.5.6.2 複数のポリシーを適用順にクライアントコンピューターに割り当てる

「ポリシーアプリケーション順序」画面を使って、複数のポリシーを適用したい順番に割り当てる方法を説明します。

操作手順

1 [管理] メニューをクリックします。

2 [グループ] サブメニューをクリックします。

3 グループリストからクライアントコンピューターが属しているグループを選択します。

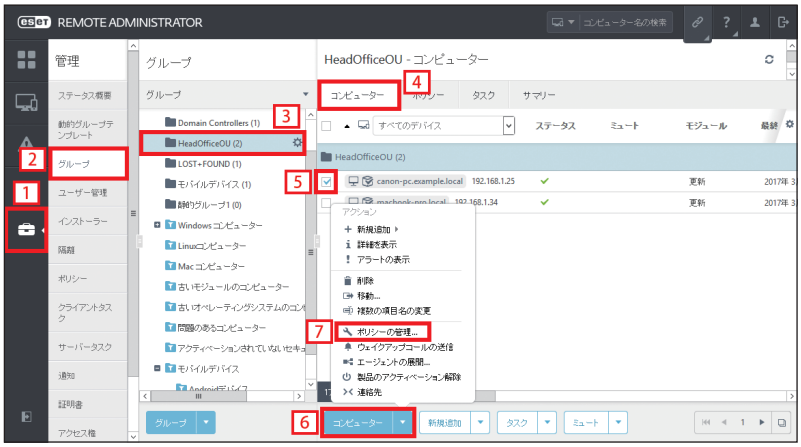
4 [コンピューター] タブをクリックします。

5 コンピューターリストから割り当てるクライアントコンピューターにチェックを入れます。

6 [コンピューター] ボタンをクリックします。

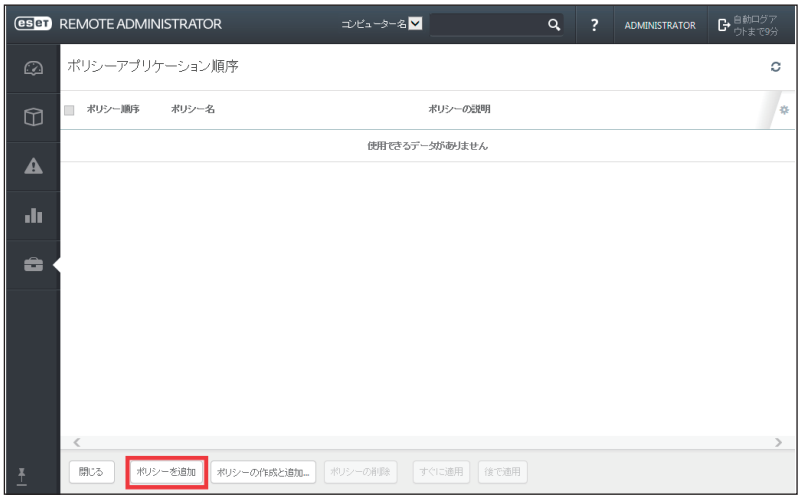
続く

7 ［ポリシーの管理］を選択します。



「ポリシーアプリケーション順序」画面が表示されます。

8 ［ポリシーの追加］ボタンをクリックします。



9 追加したい順番に該当のポリシーにチェックを入れます。

ワンポイント

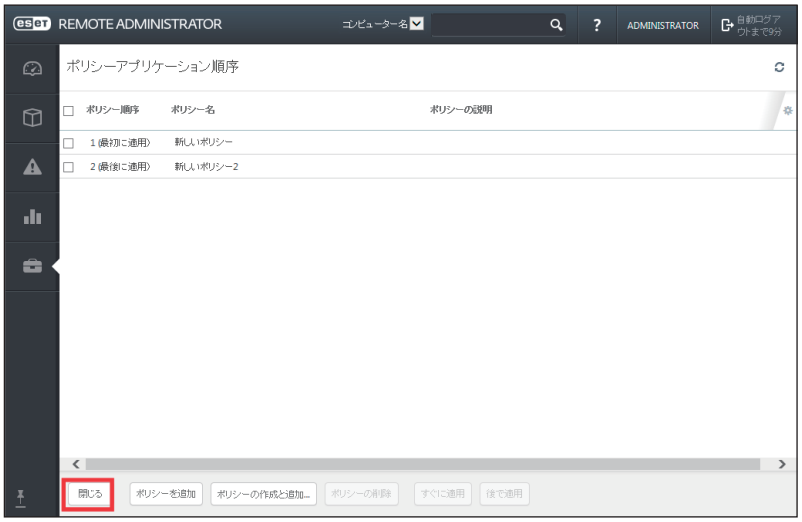
チェックを入れた順番を記憶しますので、適用したい順番に沿ってチェックを入れてください。順番は後から変更できます。

10 [OK] ボタンをクリックします。

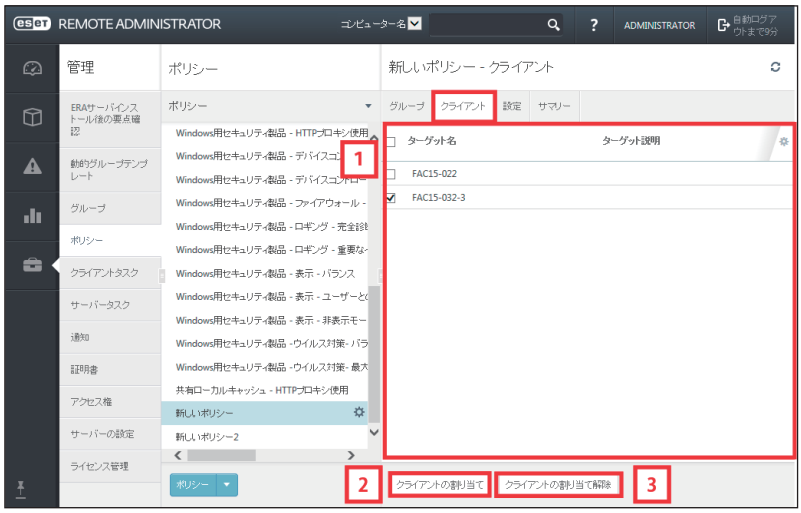
チェックを入れた順番にポリシーアプリケーション順序リストに追加されます。

11 [閉じる] ボタンをクリックします。

複数のポリシーが適用順にクライアントコンピューターに割り当てられます。
画面の詳細は、「6.5.5.2 複数のポリシーを適用順にグループに割り当てる」の「■ポリシーアプリケーション順序画面」を参照してください。



6.5.6.3 「クライアント」タブ画面の構成



1	**クライアントリスト**	選択しているポリシーが割り当てられているクライアントが表示されます。
2	**クライアントの割り当て**	選択しているポリシーにクライアントリストから選択しているクライアントを割り当てます。
3	**クライアント割り当て解除**	選択しているポリシーが割り当てられているクライアントを解除します。

6.5.7 ポリシーのエクスポート／インポート

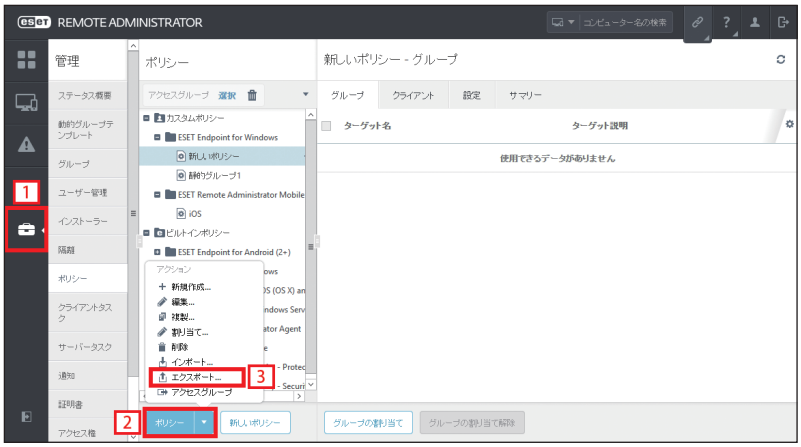
ポリシーの設定はエクスポートすることができます。設定をエクスポートし、バックアップとして保存すると、同設定の新しいポリシーを簡単に作成でき、多少のアレンジを加えたポリシーを簡単に作成することができます。

6.5.7.1 ポリシーのエクスポート

選択しているポリシートを DAT ファイル（.dat）にエクスポートする方法を説明します。
設定されているポリシーの内容は、「設定」タブで確認します。

操作手順

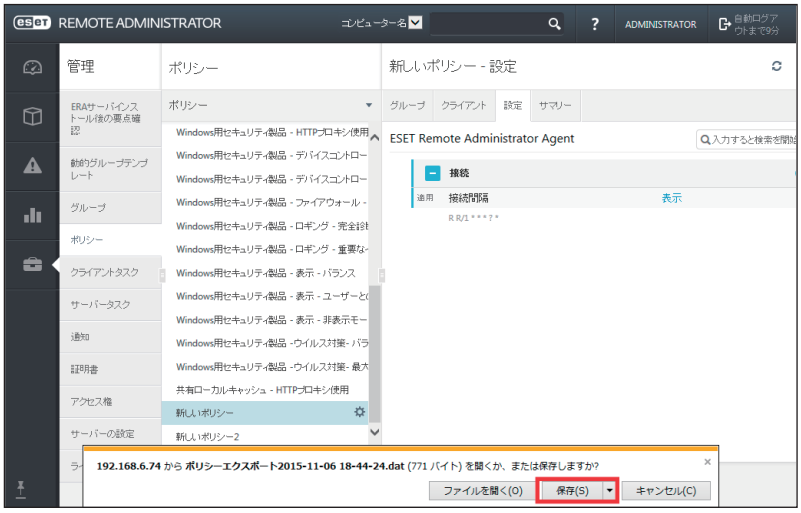
1. ポリシーリストからエクスポートするポリシーを選択します。
2. ［ポリシー］ボタンをクリックします。
3. ［エクスポート］を選択します。



保存の確認メッセージが表示されます。

続く

4 [保存] ボタンをクリックします。



ポリシーがエクスポートされます。

! 重 要

エクスポートされる内容は、選択したポリシーの設定のみです。グループやクライアントの情報はエクスポートされません。
また、複数のポリシーを一括してエクスポートすることはできません。

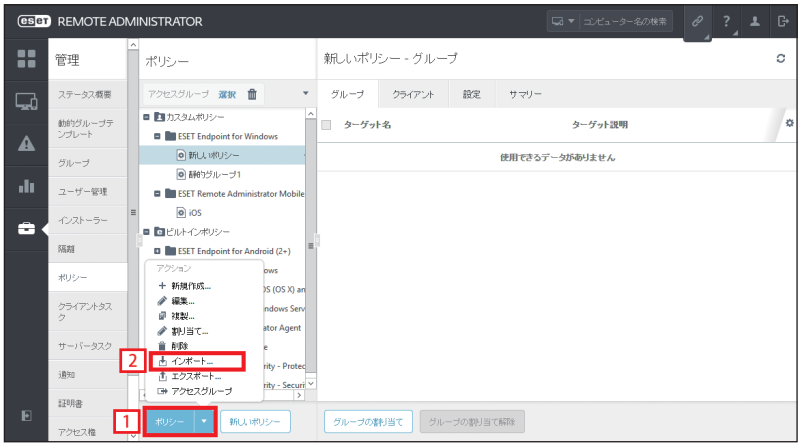
6.5.7.2 ポリシーのインポート

既存のポリシーからエクスポートした DAT ファイル（.dat）をインポートし、新しいポリシーを作成する方法を説明します。

操作手順

1 [ポリシー] ボタンをクリックします。

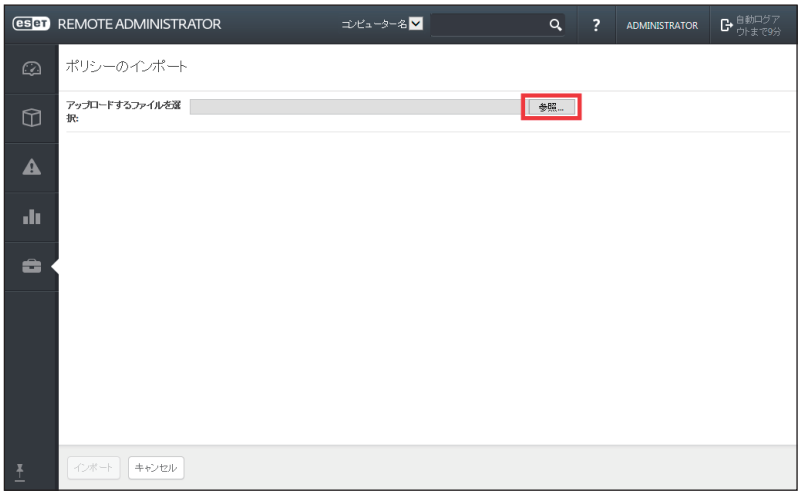
2 [インポート] を選択します。



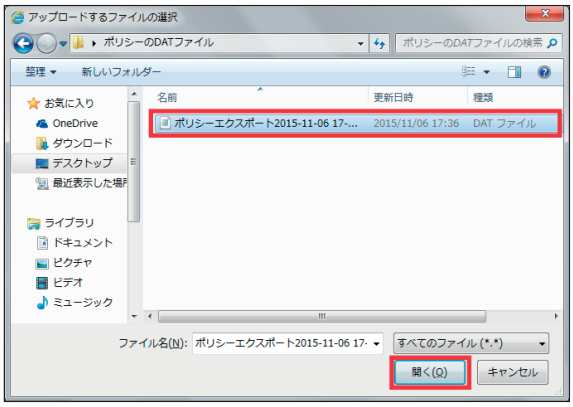
「ポリシーのインポート」画面が表示されます。

続く

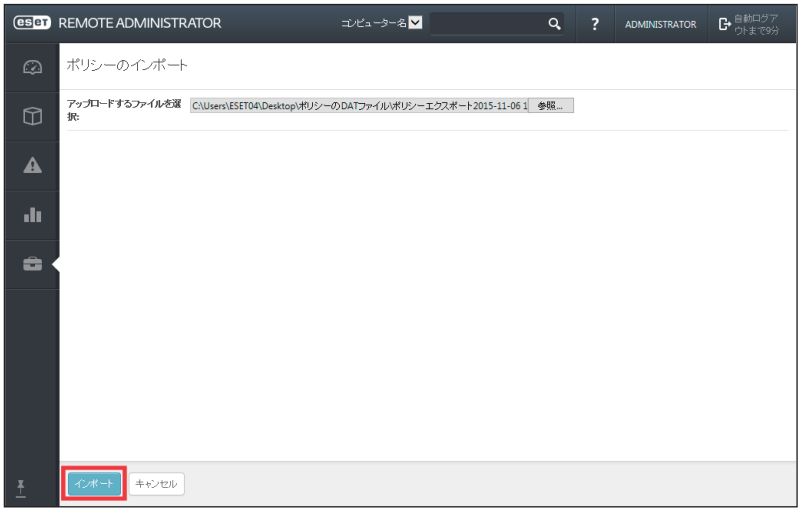
3 「アップロードするファイルを選択」の［参照］ボタンをクリックします。



4 アップロードする DAT ファイルを選択し、［開く］ボタンをクリックします。



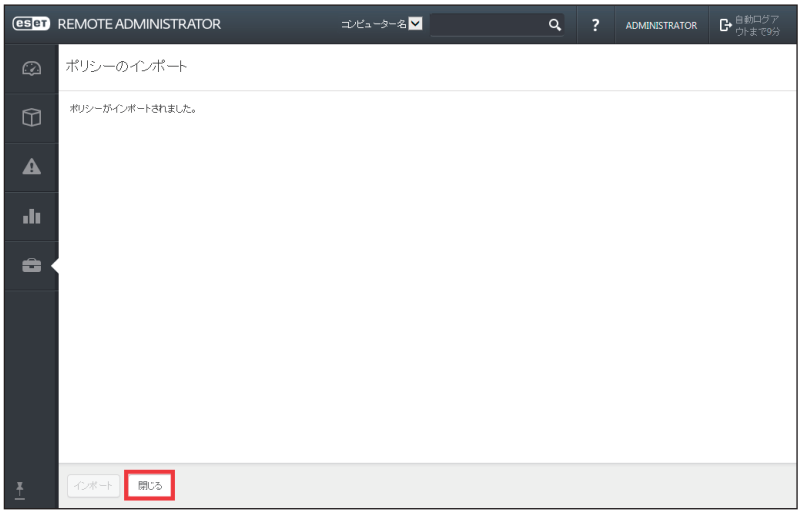
5 ［インポート］ボタンをクリックします。



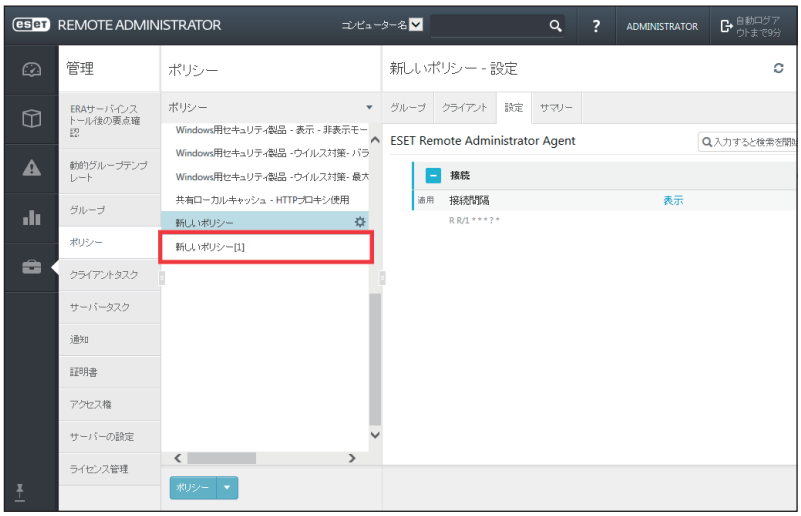
ポリシーがインポートされます。

続く

6 ［閉じる］ボタンをクリックします。



7 新しいポリシーとして追加されますので、ポリシー名を適宜変更します。



ワンポイント

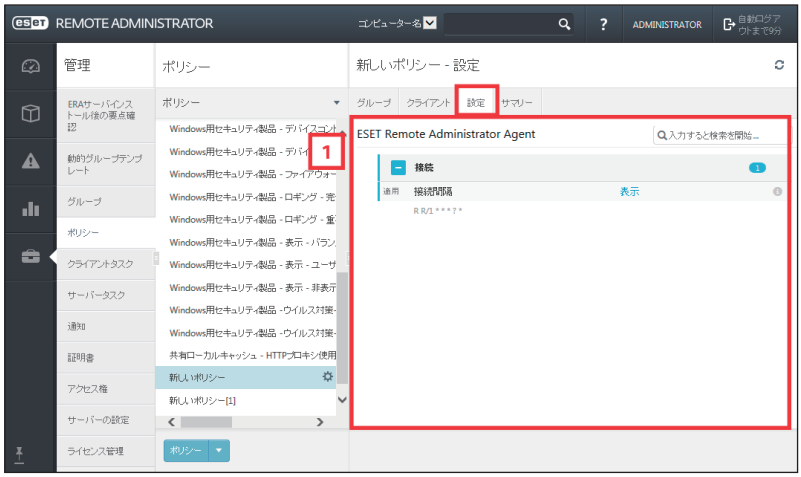
新しく作成されたポリシーを編集して、グループやクライアントを割り当ててください。

6.5.8 その他のタブ

「設定」タブ、「サマリー」タブの画面について説明します。

6.5.8.1「設定」タブ画面の構成

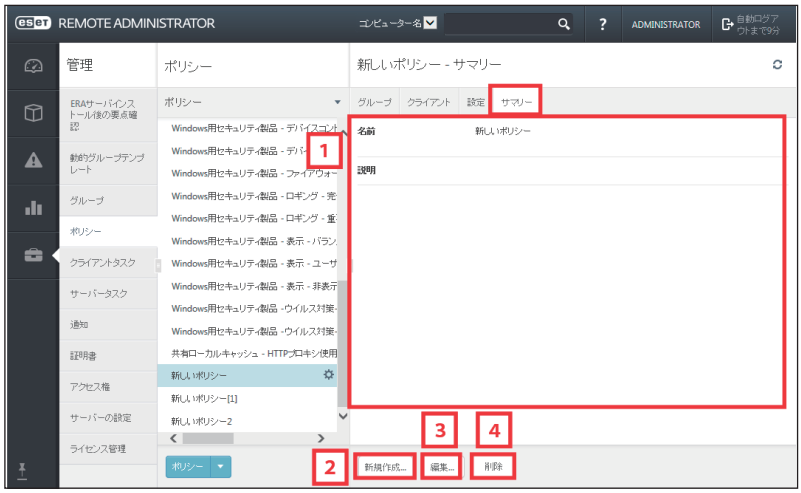
「設定」タブには、選択しているポリシーに設定されている製品とルールが表示されます。



1	**ポリシーリスト**	選択しているポリシーに設定されている製品とルールが表示されます。

6.5.8.2「サマリー」タブ画面の構成

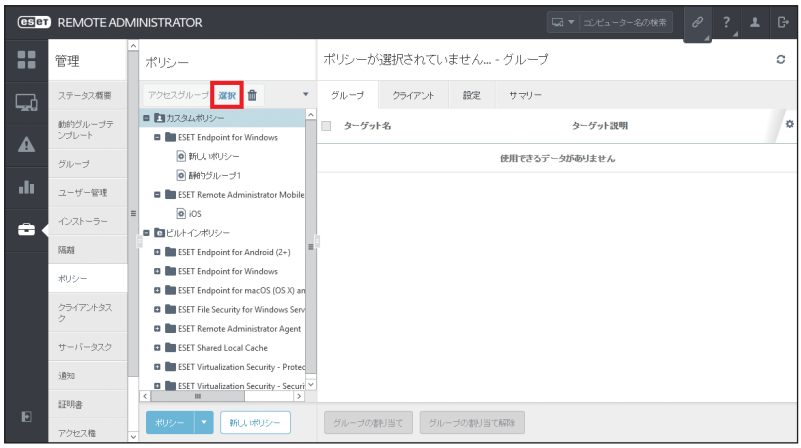
「サマリー」タブには、選択しているサマリーの内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、［編集］ボタンから変更します。



1	**サマリー**	選択しているグループに割り当てられたポリシーの内容が表示されます。
2	**新規作成**	新しいポリシーを作成します。「新しいポリシー」画面が表示されます。 画面の詳細は、「6.5.2 新しいポリシーの作成」を参照してください。
3	**編集**	選択しているポリシーを編集します。「ポリシーの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいポリシーとして保存することができます。 画面の詳細は、「6.5.2 新しいポリシーの作成」を参照してください。
4	**削除**	選択しているポリシーを完全に削除します。

6.5.8.3 アクセスグループ

「アクセスグループ」では、ユーザーが選択した静的グループに応じて、表示されるオブジェクトをフィルタリングできます。［選択］をクリックすると、フィルタリングするグループを選択できます。また、🗑をクリックすると、フィルターリングを解除できます。



6.6 クライアントタスク

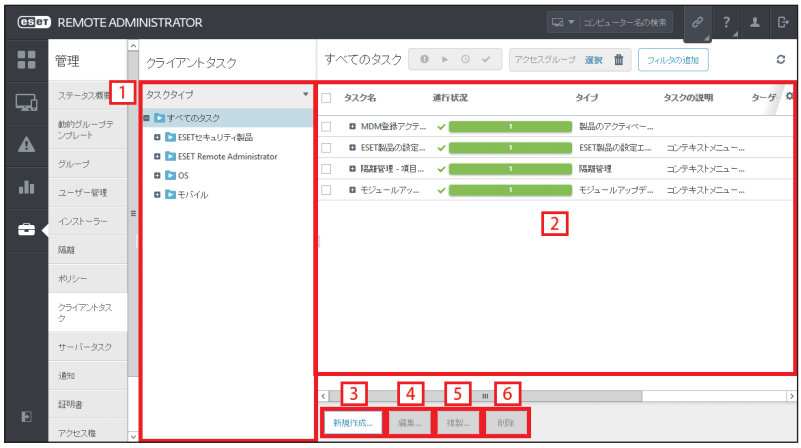
クライアントコンピューターからアクションを要求するには、クライアントタスクを使用できます。クライアントタスクはグループまたは個別のコンピューターに割り当てることができます。クライアントタスクを作成すると、設定したスケジュールに従って実行されます。

! 重 要

クライアントコンピューターは、常時 ERA サーバーに接続していないため、クライアントにタスクを反映するには、時間がかかることがあります。同じ理由から、タスク実行結果が ERA サーバーに返されるまでに時間がかかることもあります。

6.6.1 クライアントタスク画面の構成

「クライアントタスク」画面の構成について説明します。



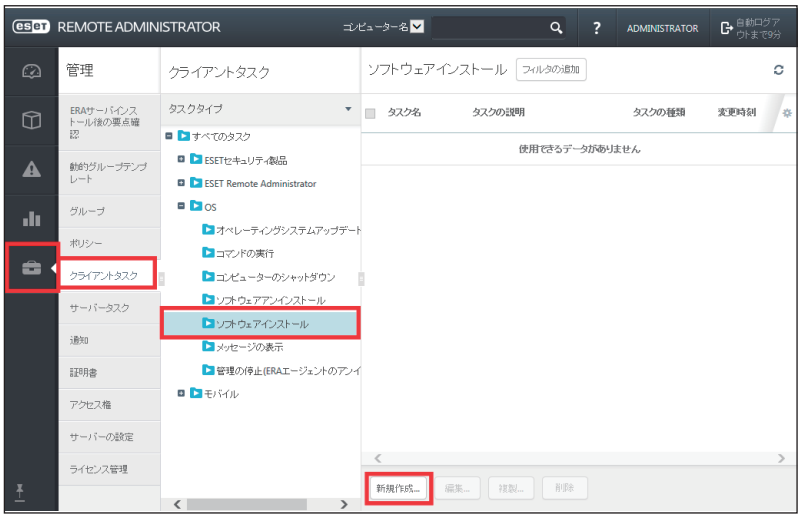
1	**タスクタイプリスト**	すべてのタスクタイプが表示されます。作成したクライアントタスクはタスクタイプごとに分類されます。
2	**選択中タスクタイプの詳細**	実行したクライアントタスクリストが表示されます。
3	**新規作成**	新しいクライアントタスクを作成します。「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。
4	**編集**	選択しているクライアントタスクを編集します。「クライアントタスクの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいクライアントタスクとして保存することができます。 ※「タスクの分類」「タスク」は変更できません。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。
5	**複製**	選択しているクライアントタスクをコピーした状態で「クライアントタスク」画面が表示されます。 画面の詳細は、「6.6.2 新しいクライアントタスクの作成」を参照してください。
6	**削除**	選択しているクライアントタスク（複数選択可）を完全に削除します。

6.6.2 新しいクライアントタスクの作成

クライアントタスクを新しく作成する方法を説明します。

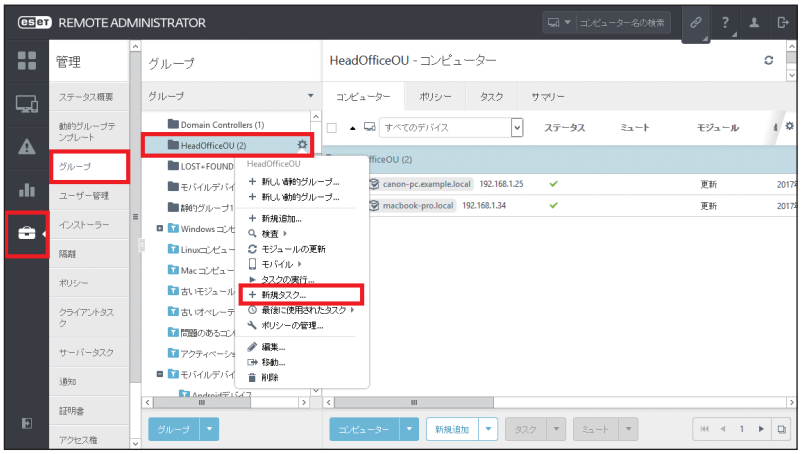
■「管理」メニューから作成する

・［クライアントタスク］> 作成するタスクタイプを選択 >［新規作成］ボタンを選択します。



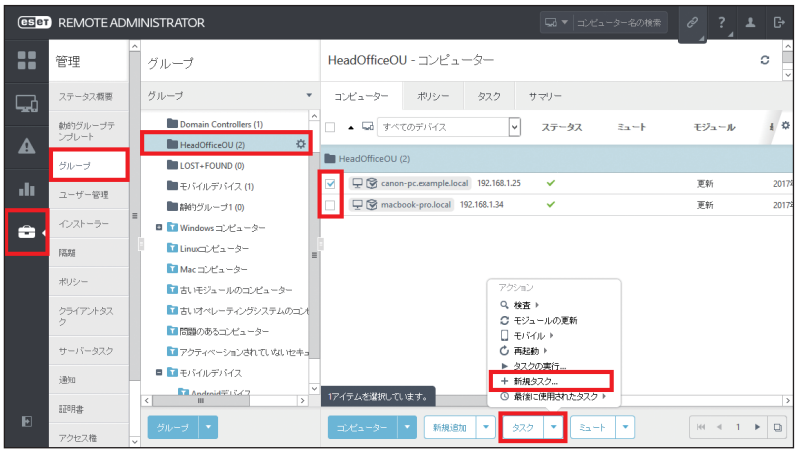
■グループに割り当てながら作成する

・［管理］メニュー >［グループ］> 割り当てる静的または動的グループを選択 > ⚙ >［新規タスク］を選択します。

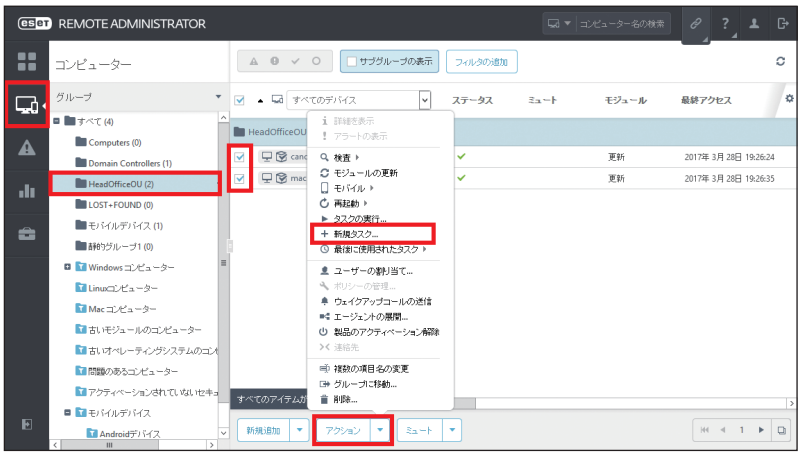


■クライアントコンピューターに割り当てながら作成する

- ［管理］メニュー > ［グループ］ > 静的または動的グループを選択 > 割り当てるコンピューターを選択 > ［タスク］ボタン > ［新規タスク］を選択します。

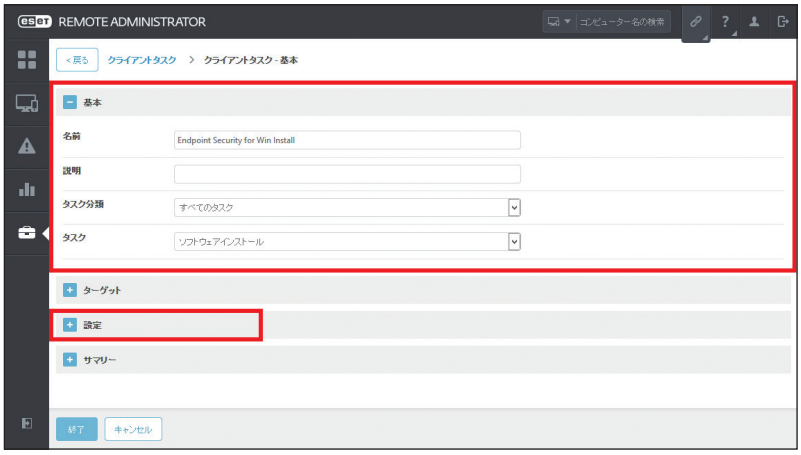


- ［コンピューター］メニュー > 静的または動的グループを選択 > 割り当てるコンピューターを選択 > ［タスク］ボタン > ［新規タスク］を選択します。



操作手順

1. いずれかの方法で「クライアントタスク」画面を表示します。
2. 「基本」の各項目を入力して、［設定］をクリックします。



■基本

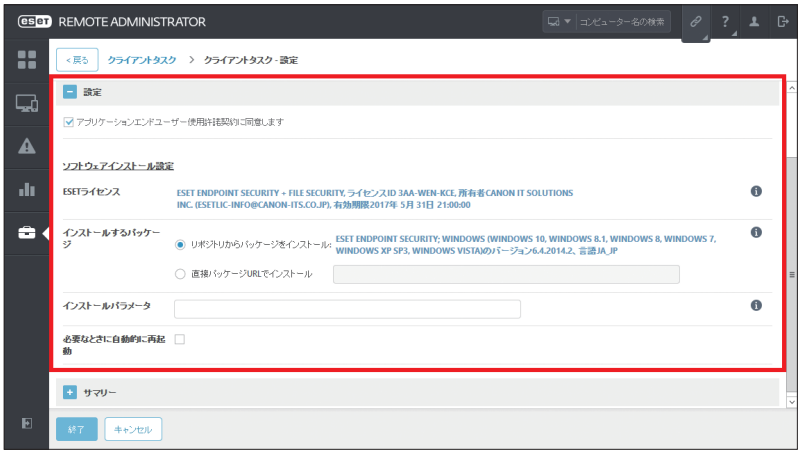
項目名	説明	必須
名前	作成するクライアントタスクの名前を入力します。画面には、ここで設定した名前が表示されます。	○
説明	作成するクライアントタスクの説明を入力します。	-
タスク分類	選択した分類に合わせて「タスク」に表示される選択肢が絞り込まれます。作成後は［すべてのタスク］で固定されます。	○
タスク	作成するクライアントタスクのタスクタイプを選択します。「クライアントタスク」画面でタスクタイプを選択している場合は、該当するタスクタイプが反映されます。	○

ワンポイント

作成したタスクを割り当てるターゲットの設定は、タスクを作成した後に行います。グループやクライアントコンピューターに割り当てながら作成を行ったときは、タスク作成後に、タスクを割り当てるグループやクライアントコンピューターの追加や削除を行えます。

続く

3 「設定」の各項目を入力します。

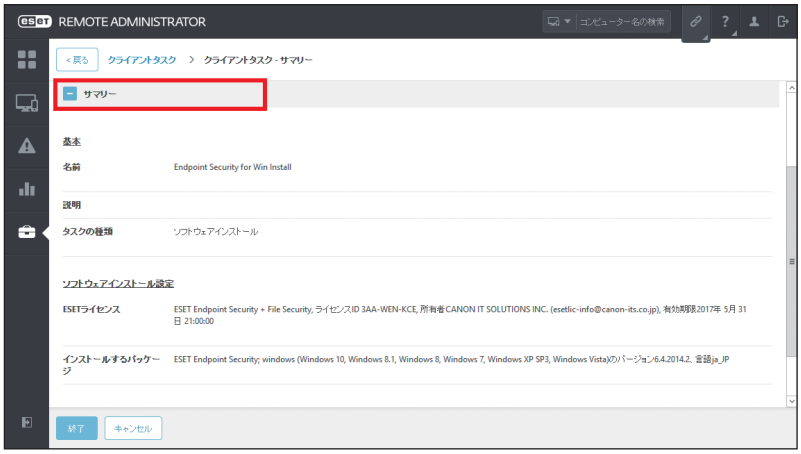


■設定

選択したタスクタイプによって、表示される項目は異なります。詳細は、「6.6.3　タスクタイプの設定」を参照してください。

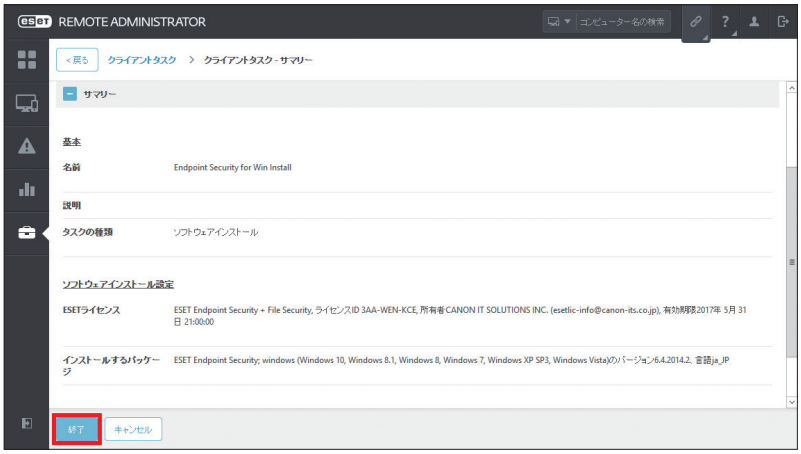
4 [サマリー] をクリックします。

「基本」および「設定」に入力した内容が読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。



続く

5 ［終了］ボタンをクリックします。

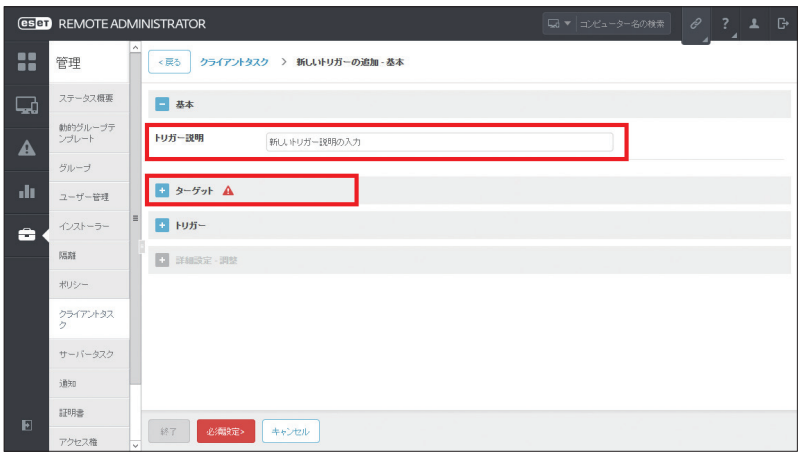


ダイアログボックスが表示されます。

6 ［トリガーの作成］をクリックします。

「新しいトリガーの追加 - 基本」画面が表示されます。

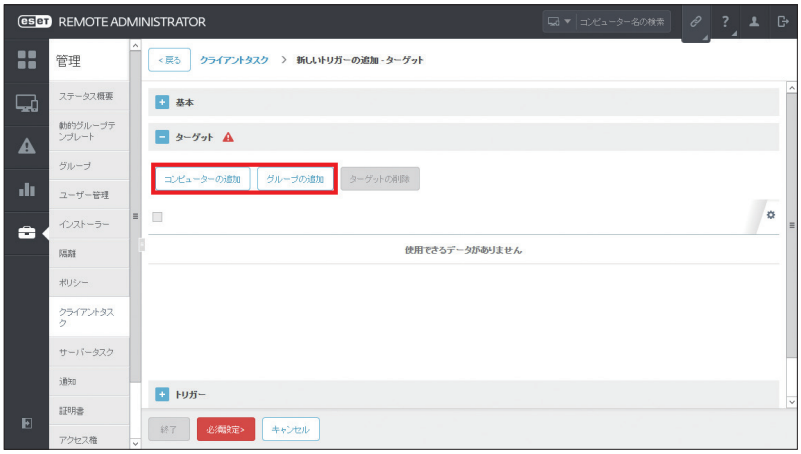
7 「トリガーの説明」を入力し、［ターゲット］をクリックします。



「新しいトリガーの追加 - ターゲット」画面が表示されます。

続く

8 ［コンピューターの追加］または［グループの追加］をクリックします。



「保存先の設定」画面が表示されます。

■ターゲット

項目名	説明	必須
コンピューターの追加	作成するクライアントタスクを割り当てるコンピューターを設定します。コンピューターを選択する画面が表示されます。	○
グループの追加	作成するクライアントタスクを割り当てるグループを設定します。グループを選択する画面が表示されます。	-
ターゲットの削除	選択したターゲットを削除します。	-
ターゲットリスト	ターゲットを選択する画面で選択したターゲットのリストが表示されます。	-

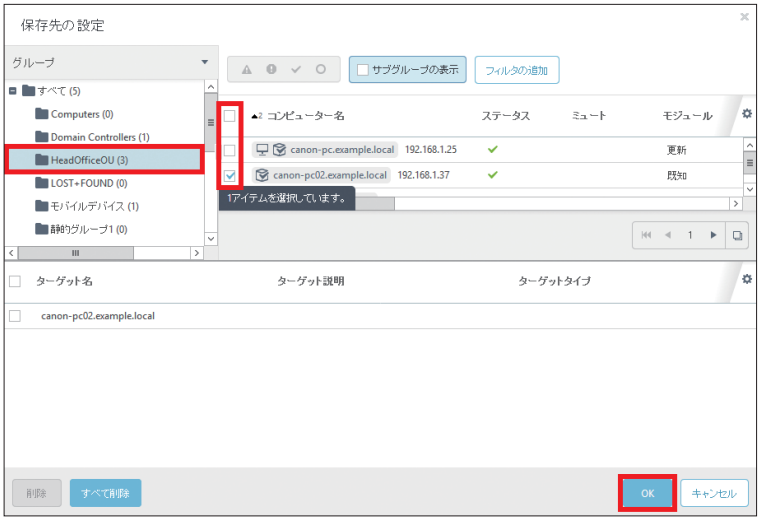
ワンポイント

コンピューターまたはグループのどちらかを追記する必要があります。

9 タスクを割り当てるグループまたはコンピューターを選択し、［OK］ボタンをクリックします。

●手順 8 で［コンピューターの追加］をクリックした場合

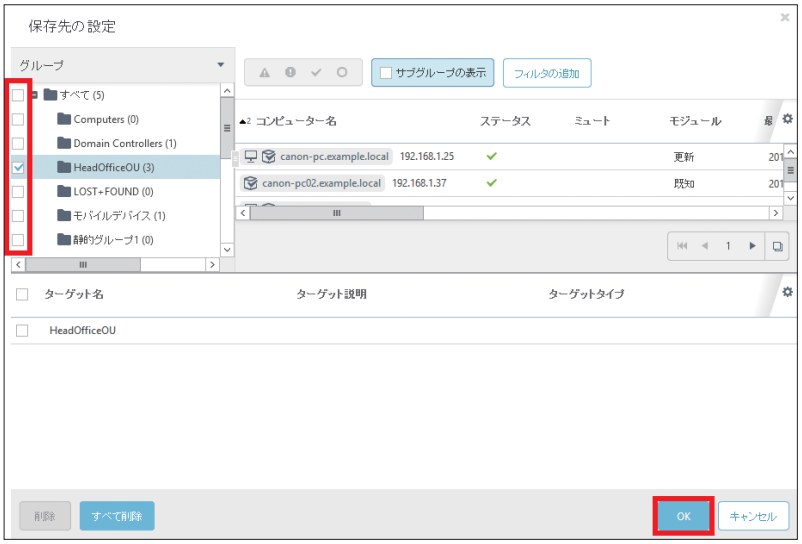
グループを選択し、タスクを割り当てるコンピューターにチェックを入れます。［OK］ボタンをクリックします。



続く

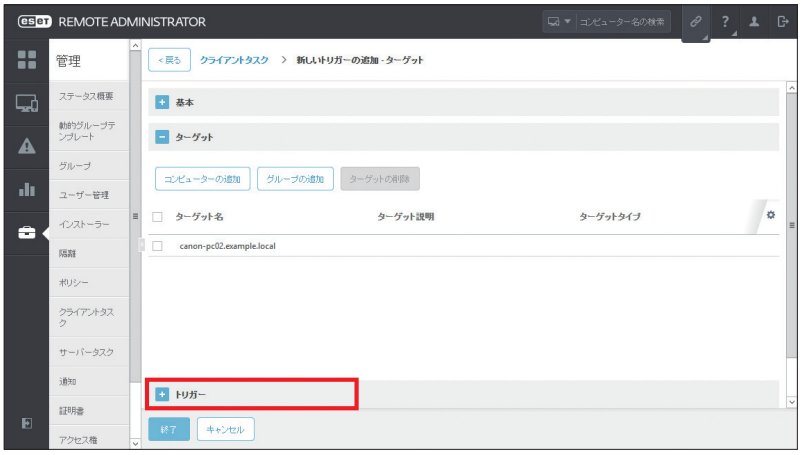
●手順 8 で［グループの追加］をクリックした場合

タスクを割り当てるグループにチェックを入れます。［OK］ボタンをクリックします。



「新しいトリガーの追加 - ターゲット」画面に戻ります。

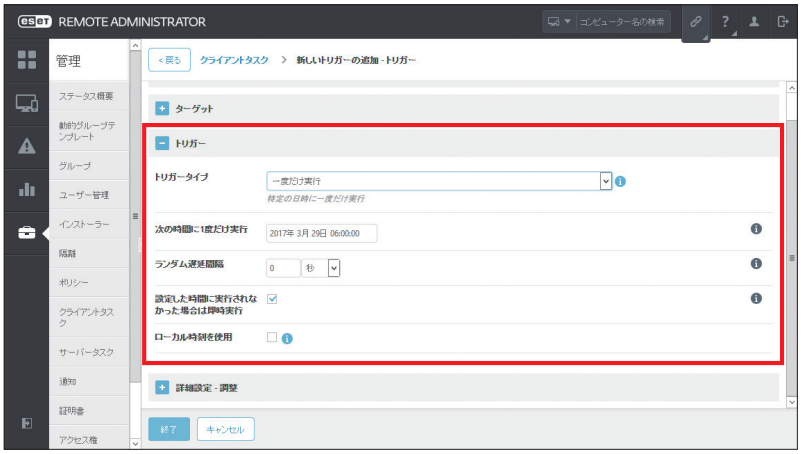
⑩［トリガー］をクリックします。



「新しいトリガーの追加 - トリガー」画面が表示されます。

続く

⓫「トリガー」の各項目を入力します。



■トリガー

トリガーとはタスクを実行させる一連の条件のことで、満たされるとタスクの実行を開始します。トリガーは ERA サーバーとエージェント（クライアント）の両方で使用できます。

項目名	説明		必須
トリガータイプ	タスクをトリガーするイベントを決定します。		○
	即時	クライアントコンピューターが ESET Remote Administrator サーバーに接続し、クライアントタスクを受信したら直ぐに実行します。有効期限までに実行できない場合は、クライアントタスクはキューから削除されます。その場合、クライアントタスク自体は削除されませんが、実行もされません。	-
	スケジュール済み	選択した時間にクライアントタスクを実行します。このタスクを 1 回だけ実行するか、繰り返し実行するかをスケジュールします。	-
	結合された動的グループトリガー	クライアントコンピューターがターゲットで選択した動的グループに加わるときにクライアントタスクを実行します。 ※静的グループまたは個別のクライアントが選択されるとこのオプションは使用できません。	-
	イベントログトリガー	ここで指定したイベントに基づいてクライアントタスクを実行します。特定のイベントがログで発生したときに呼び出されます。クライアントタスクをトリガーするログタイプ、論理演算子、およびフィルタリング条件を定義します。	-
	CRON 式	CRON 式に基づいたスケジュールでクライアントタスクを実行します。	-
選択したトリガータイプで設定する項目	トリガータイプに応じた項目が表示されます。 表示される項目については、「6.7.4.1　各トリガータイプの設定項目」を参照してください。		
ローカル時間使用	クライアントコンピューターのローカル時間です。		○

続く

12 [詳細設定 ー 調整] をクリックします。

13 「詳細設定 ー 調整」の各項目を入力します。

■詳細設定 ー 調整

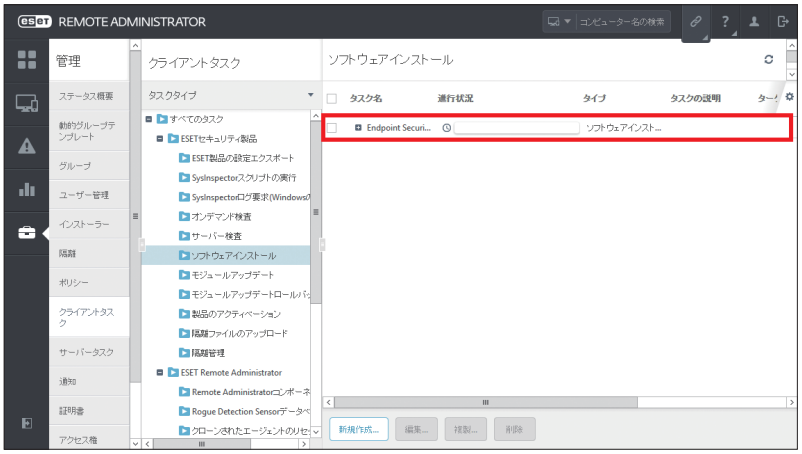
表示される項目については、「6.7.4.2　詳細設定 ー 調整」を参照してください。

ワンポイント

「詳細設定ー調整」は、「トリガータイプ」で選択した内容に従い有効になります。イベントログトリガーや結合された動的グループトリガーなど頻繁に発生するイベントでタスクがトリガーされる場合は、タスクの実行を制限するために「詳細設定 ー 調整」が使用されます。
調整条件はイベント発生時間に絞り込まれます。「時間ベースの条件」は、「統計条件」よりも優先されます。

14 [終了] ボタンをクリックします。

タスクリストに、作成したクライアントタスクが表示されます。



6.6.3 タスクタイプの設定

クライアントタスクの設定は、タスクタイプによって異なります。ここでは、設定のポイントについて説明します。

6.6.3.1 ESET セキュリティ製品

■ ESET 製品の設定エクスポート

このタスクは、クライアントにインストールされている個別の ERA コンポーネントまたは ESET 製品の設定をエクスポートし、ERA サーバーで確認するために使用します。

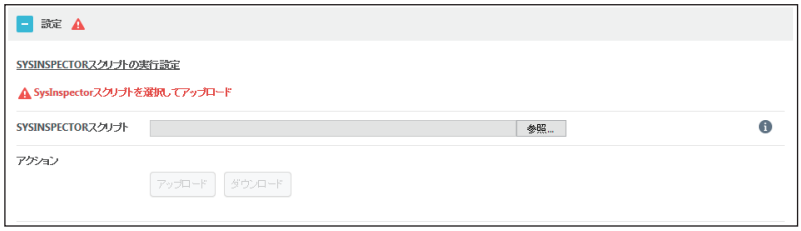
項目名	説明	必須
製品	対象のコンピューターから設定をエクスポートする ERA コンポーネントまたは ESET 製品を選択します。	○

ワンポイント

エクスポートされた設定は、「コンピューターの詳細」画面の「コンフィグレーション」タブ（「5.3.4 クライアントコンピューターの詳細確認画面」の「■コンフィグレーション」参照）で確認できます。

■ SysInspector スクリプトの実行

このタスクは、クライアントコンピューターで SysInspector のスクリプトを実行します。



項目名	説明		必須
SYSINSPECTOR スクリプト	アップロードする SysInspector スクリプトを選択します。		○
アクション	アップロード	SysInspector スクリプトを選択すると表示されます。	○
	ダウンロード	SysInspector スクリプトがアップロードされている場合に表示されます。アップロードしたスクリプトを確認できます。	-

! 重 要

このタスクを実行する前に、SysInspector スクリプトを ESET SysInspector からエクスポートする必要があります。スクリプトをエクスポートした後は、削除するオブジェクトを選択し、修正されたデータでスクリプトを実行できます。

ワンポイント

タスクが完了したら、レポートの結果を確認できます。

■ SysInspector ログ要求

このタスクは、SysInspector の機能を備えた ESET 製品をインストールしたクライアントコンピューターで SysInspector を実行し、その SysInspector ログを要求します。

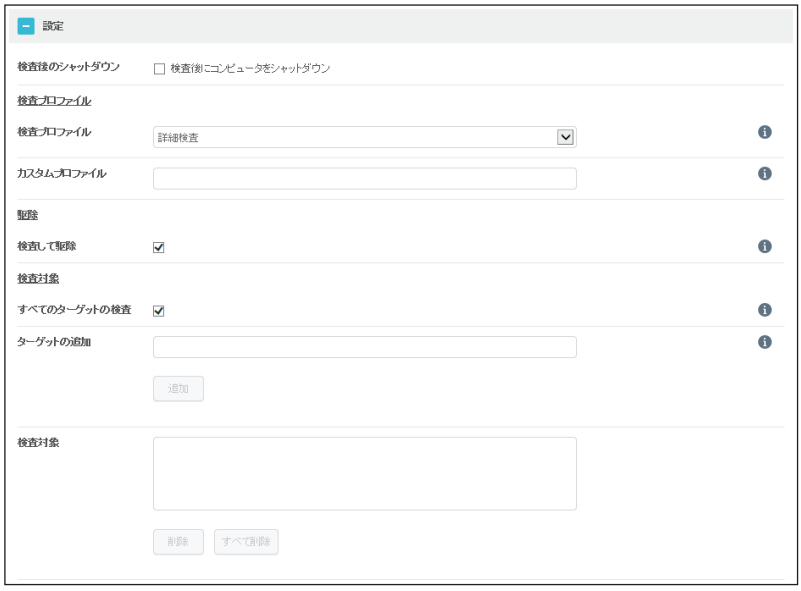
項目名	説明	必須
クライアントにログを保存	クライアントと ERA サーバーに SysInspector ログを保存する場合に選択します。 例えば、ESET Endpoint Security がクライアントにインストールされている場合、通常ログは C:¥Program Data¥ESET¥ESET Endpoint Antivirus¥SysInspector に保存されています。	-

ワンポイント

SysInspectorn ログは過去 30 日間の SysInspcector スナップショット履歴から確認できます。

■オンデマンド検査

このタスクは、定期的なスケジュール検査とは別に、クライアントコンピューターのオンデマンド検査を強制的に実行します。



項目名	説明		必須
検査後のシャットダウン	オンにすると、検査の完了後にコンピューターをシャットダウンします。		-
検査プロファイル	検査プロファイル	検査プロファイル（検査対象と方法）を選択します。検査プロファイルはクライアント設定で定義されます。	○
		詳細検査	最も詳細な検査プロファイルとして構成され、システム全体を確認します。ただし、最も検査時間がかかります。	-
		スマート検査	コンピューターの検査をすぐに開始し、ユーザーが操作しなくても感染しているファイルからウイルスを駆除します。利点は、操作が簡単で詳細な検査設定を必要としないことです。ローカルドライブにあるすべてのファイルが検査されます。検出されたマルウェアがあれば、自動的に駆除または削除されます。駆除のレベルは自動的に既定値に設定されます。	-
		コンテキストメニューから検査	定義済み検査プロファイルを使用してクライアントを検査します。検査対象をカスタマイズできます。 ※この検査プロファイルは、モバイルデバイスでサポートされていません。モバイルデバイスでは、既定のプロファイルを使用します。	-
		カスタムプロファイル	スキャン対象やスキャン方法などのスキャンパラメータを指定します。利点は、パラメータを詳細に設定できることです。設定はユーザー定義の検査プロファイルに保存され、同じパラメータで簡単に検査を繰り返し実行できます。プロファイルは、カスタムプロファイルオプションでタスクを実行する前に作成する必要があります。「カスタムプロファイル」に正確なプロファイル名を入力します。	-
	カスタムプロファイル	「検査プロファイル」で［カスタムプロファイル］を選択した場合に使用します。クライアントのカスタム検査プロファイル名を入力します（プロファイルを適用する前に定義する必要があります）。		-
駆除	検査して駆除	オンにすると、検査中に検出された感染オブジェクトは駆除されます。駆除できない場合は、感染オブジェクトは隔離されます。		-

項目名	説明		必須
検査対象	すべてのターゲットの検査	オンにすると、検査プロファイルで指定したすべてのターゲットが検査されます。オフの場合は、「ターゲットの追加」に検査対象を手動で追加する必要があります。	-
	ターゲットの追加	すべてのターゲットの検査オプションをオフにした場合に使用します。ターゲットを手動で追加する必要があります。	-
	検査対象	すべてのターゲットの検査オプションのオフにした場合に使用します。「ターゲットの追加」で追加した検査対象が表示されます。対象から解除する場合は、[削除] ボタンから削除します。	-

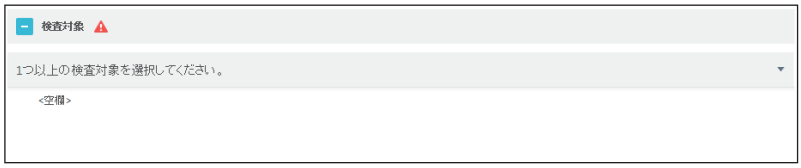
■サーバー検査

このタスクは、ESET File Security for Microsoft Windows Server 6.3 以降の製品に対して Hyper-V 検査を実行します。

! 重　要

サーバー検査タスクを使用するためには、ESET File Security for Microsoft Windows Server 6.3 以降で [詳細設定] - [ツール] - [ERA 検査対象] の設定を有効にする必要があります。

項目名	説明	必須
検査されたサーバー	検査する 1 つのサーバーを選択します。	○



項目名	説明	必須
検査対象	選択したサーバー上の検査可能なリソースが表示されます。	-

■ソフトウェアインストール

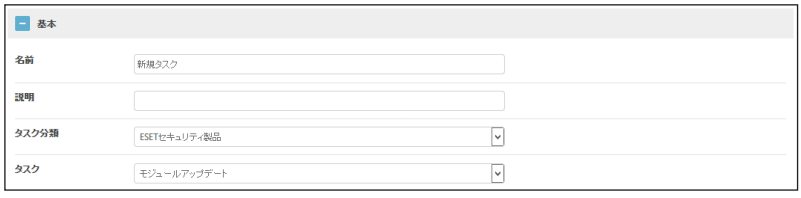
このタスクは、クライアントコンピューターにソフトウェアをインストールします。主な目的は、ESET 製品をインストールすることですが、他社のソフトウェアをインストールするためにも使用できます。

項目名	説明		必須
使用許諾契約同意	EULA への同意は必須です。		○
ESET ライセンス	インストールする ESET 製品のための適切な ESET ライセンスをリストから選択します。リストには「ライセンス管理」で登録済みのライセンスが表示されます。		○
インストールするパッケージ	インストールするパッケージを指定します。		○
	リポジトリからパッケージをインストール	ESET 製品のインストールパッケージを選択します。リポジトリからインストールする場合は、ERA サーバーとクライアントコンピューターがインターネットにアクセスできる必要があります。インターネットにアクセスできない場合は、直接パッケージ URL を指定してクライアントソフトウェアをインストールできます。	-
	直接パッケージ URL でインストール	インストールするソフトウェアパッケージへの URL パスを入力します。URL パスを入力する場合は、直接インストールパッケージを参照する必要があります。 ローカルファイルを参照する URL の例は以下のとおりです。 （例：file://¥¥pc22¥nstall¥ees.msi） ※認証が必要な URL は使用しないでください。	-
インストールパラメータ	必要に応じて、インストーラー用の任意のコマンドラインパラメータを指定します。インストールパラメータは各ソフトウェアの各インストールパッケージで有効です。指定しない場合は空欄にします。 ESET 製品のインストールオプションについては、「4.2.3.2　コマンド入力からの製品インストール」を参照してください。		-
必要なときに自動的に再起動	オンにすると、インストール後にクライアントコンピューターを強制的に再起動します。オフにすると、クライアントコンピューターを使用しているユーザーに、再起動するかどうかを判断させることができます。		○

■モジュールアップデート

このタスクは、クライアントコンピューターにインストールされている ESET 製品のモジュールのアップデートを強制的に実行します。

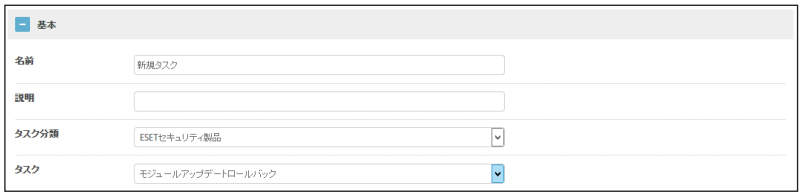
これは、すべての製品で利用できる汎用的なタスクです。



項目名	説明	必須
アップデートキャッシュのクリア	このオプションを使用すると、クライアントコンピューターのキャッシュにある一時更新ファイルを削除します。 多くの場合、失敗したモジュールのアップデートを修復するために使用します。	-

■モジュールアップデートロールバック

このタスクは、モジュールアップデートが問題を引き起こした場合や、一部のクライアントには更新を適用しない場合に使用します（テストの場合やリリース前更新のテストなど）。このタスクを適用すると、モジュールが前のバージョンにロールバックされます。



項目名	説明		必須
アクション	モジュールを現在のバージョンからのロールバック後に更新を有効にするか、定義済みの期間の間更新を無効にするかを選択します。		○
	有効な更新	更新を有効にし、クライアントコンピューターは次のモジュールアップデート更新を受信します。	-
	次の更新をロールバックして無効にする	更新は、「間隔を無効にする」で指定した期間または取り消されるまで無効です。取り消されるまでオプションを使用すると、セキュリティリスクにつながるので注意してください。	-
間隔を無効にする	「アクション」で［次の更新をロールバックして無効にする］を選択した場合に使用します。 クライアントがモジュールアップデートを受信しない期間を選択します。		-

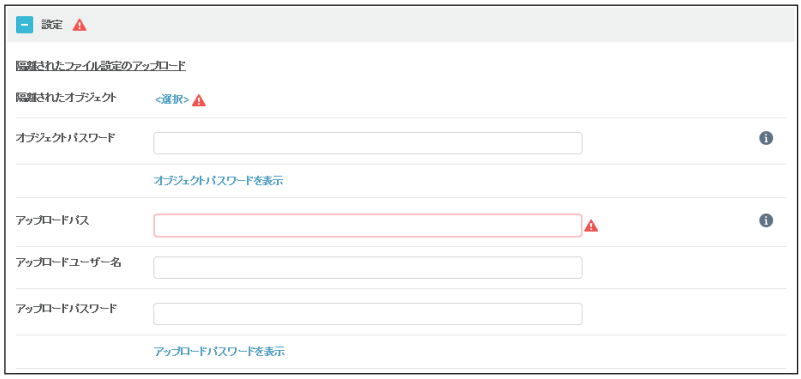
■製品のアクティベーション

このタスクは、クライアントコンピューターの ESET 製品をアクティベーションします。

項目名	説明	必須
ESET ライセンス	クライアントコンピューター ESET 製品をアクティベーションするためのライセンスをリストから選択します。リストには「ライセンス管理」で登録済みのライセンスが表示されます。	○

■隔離ファイルのアップロード

このタスクは、クライアントコンピューターで隔離されたファイルを共有ディレクトリにアップロードします。



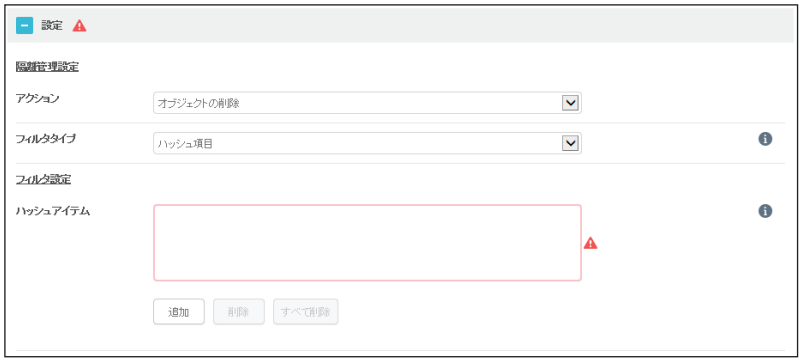
項目名	説明	必須
隔離されたオブジェクト	隔離されたオブジェクトから特定のオブジェクトを選択します。	○
オブジェクトパスワード	オブジェクトは暗号化されたアーカイブとしてアップロードされるため、その暗号化用パスワードを入力します。対応するレポートにはパスワードが表示されます。	-
アップロードパス	オブジェクトをアップロードする場所へのパスを入力します（Samba Share/Windows 共有ディレクトリアドレス（パス用のフォーマット：smb://...））。オブジェクトをアップロードするファイルサーバーの IP アドレスが「192.168.1.1」でフォルダが「share」の場合の例は以下のとおりです。（例 : smb://192.168.1.1/share） ※クライアントコンピューターから、ここで指定したファイルパスへアクセスできる必要があります。	○
アップロードユーザー名	認証が必要な場合（ネットワーク共有など）は、「アップロードパス」にアクセスするための認証情報のユーザー名を入力します。	
アップロードパスワード	認証が必要な場合（ネットワーク共有など）は、「アップロードパス」にアクセスするための認証情報のパスワードを入力します。	

! 重　要

Linux コンピューターに、このタスクを実行する場合は cifs-utils パッケージが Linux コンピューターにインストールされている必要があります。

■隔離管理

このタスクは、ERA サーバーで管理しているクライアントコンピューターで隔離されたオブジェクトを管理します。

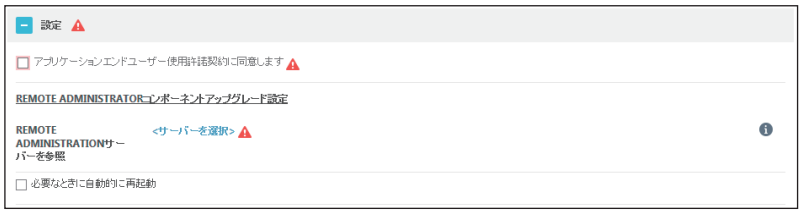


項目名	説明		必須
隔離管理設定	アクション	隔離内のオブジェクトで実行するアクションを選択します。	○
		オブジェクトの復元 / オブジェクトを元の場所に復元し、検査します。隔離の理由が存在する場合は、オブジェクトは再度隔離されます。	-
		オブジェクトを復元し、次回以降除外する / オブジェクトを元の場所に復元し、今後は隔離されません。 ※このアクションはヒューリスティック機能で検出された未知のウイルスの場合にのみ使用できます。	-
		オブジェクトの削除 / オブジェクトを完全に削除します。	-
	フィルタタイプ	隔離内のオブジェクトをフィルタリングするタイプを選択します。選択したタイプに合わせて「フィルタ設定」を入力します。 ※表示される選択肢については、「フィルタ設定」で合わせて説明します。	○
フィルタ設定	選択したフィルタタイプで設定する項目が表示されます。		○
	ハッシュ項目	既存の隔離オブジェクトからハッシュ項目を追加します。	-
		ハッシュアイテム / ［追加］ボタンをクリックし、オブジェクトリストから１つ以上選択します。	-
	発生	オブジェクトが隔離された場合の時間範囲を入力します。	-
		発生開始 / クリックするとカレンダーが表示されますので、有効な開始日付を選択してください。	-
		発生終了 / クリックするとカレンダーが表示されますので、有効な終了日付を選択してください。	-
	サイズ	隔離オブジェクトのサイズ範囲をバイトで入力します。	-
		最小サイズ（バイト） / 正しいサイズ（バイト）を０以上の数字で入力します。	-
		最大サイズ（バイト） / 「最小サイズ」以上の数字を入力します。	-
	ウイルス名	既存の隔離オブジェクトからウイルス名を選択します。	-
		ウイルス名 / ［選択］ボタンをクリックし、ウイルスリストから選択します。	-
	オブジェクト名	既存の隔離オブジェクトからオブジェクト名を選択します。	-
		ウイルス名 / ［選択］ボタンをクリックし、オブジェクトリストから選択します。	-

6.6.3.2 ESET Remote Administrator

■ Remote Administrator コンポーネントアップグレード

このタスクは、ERA コンポーネント（ERA エージェント、ERA プロキシ、ERA サーバー、MDM）をアップグレードするために使用します。例えば、ERA バージョン 6.1.28.0 から ERA バージョン 6.1.33.0 にアップグレードする場合などです。



項目名	説明	必須
使用許諾契約同意	EULA への同意は必須です。	○
REMOTE ADMINISTRATION サーバーを参照	ERA サーバーバージョンを選択します。すべての ERA コンポーネントは、選択したサーバーと互換性のあるバージョンにアップグレードされます。	○
必要なときに自動的に再起動	オンにすると、再起動が必要な場合にクライアントオペレーティングシステムを強制的に再起動します。	-

■ Rogue Detection Sensor データベースリセット

このタスクは、RD Sensor 検索キャッシュをリセットするために使用します。このタスクによって、キャッシュが削除され、検索結果を再度保存します。既に検出されたコンピューターは削除されません。検出されたコンピューターがまだキャッシュにあり、サーバーに報告されていない場合に使用します。

■クローンされたエージェントのリセット

このタスクは、ERA エージェントに割り当てられた SID をリセットします。ERA エージェントをインストール済みのマスタイメージによってコンピューターを複製した場合に、ERA エージェントの SID が同じになり、コンピューターの重複などの問題の原因となることがあります。解決するためには、このタスクを使用して SID をリセットし、一意に識別できるようにエージェントを割り当てます。

! 重　要

このタスクは注意して実行してください。ERA エージェントの SID がリセットされると、タスクを実行されたコンピューターが新しいコンピューターとして ERA サーバーに登録されます。そのため、過去にこのコンピューターに割り当てたタスクやポリシー、ログなどの情報は引き継がれません。なお、ERA サーバー上にタスク実行前の古い SID のコンピューターが残りますので、不要な場合は削除してください。

■管理の停止（ERA エージェントのアンインストール）

モバイルデバイスの場合は、MDM 登録を削除します。このタスクは、コンピューターにインストールされているエージェントを削除します。

ポリシーを適用したままこのタスクを実行すると、Windows、Mac OS X の場合、適用した設定が管理対象製品に変更可能な状態で残ります。エージェントを削除する（このタスクを実行する）前に、ポリシーの適用を解除する必要があります。次のポイントを参考にしてください。また、エージェントで実行中のすべてのタスクは破棄されます。

1. 適用した設定を、保持したくない場合は、望ましくない設定を既定の値（または望ましい値）に戻すポリシーを設定し、適用します。ポリシーが管理対象製品に適用されるまで待機します。
2. この手順を実行する前に、ポイント 1 からのポリシーがターゲットコンピューターでレプリケーションを完了するまで待機してから、ERA のリストからコンピューターを削除することを推奨します。

ターゲットコンピューターに適用されているポリシーの適用対象から、ターゲットコンピューターを割り当て解除します。管理対象製品にて、ポリシー適用した設定項目が変更可能になるまで待機します。

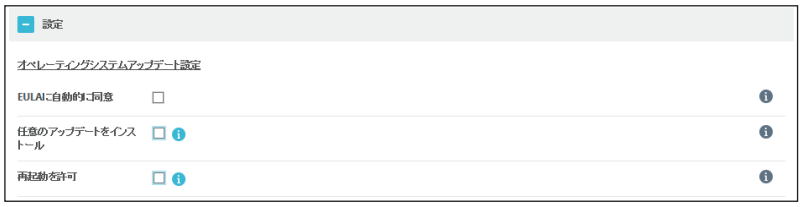
!重　要

このタスクは注意して実行してください。デバイスが管理されなくなった（エージェントが削除された）後、一部の設定が管理対象の製品に残る場合があります。ポリシーを使用して一部の設定（パスワード保護など）を既定値にリセットしてから、デバイスを管理対象から削除することを推奨します。
また、エージェントで実行中のすべてのタスクは破棄されます。データレプリケーションによっては、このタスクの実行ステータスが「実行中」、「完了」、または「失敗」にならない場合があります。

6.6.3.3　OS

■オペレーティングシステムアップデート

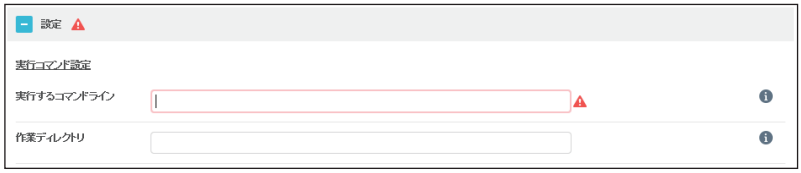
このタスクは、クライアントコンピューターのオペレーティングシステムを更新します。このタスクによって、Windows、Mac OS X、Linux オペレーティングシステムで更新が実行されます。



項目名	説明	必須
EULA に自動的に同意	アップデートでユーザーが EULA に同意する必要がある場合は、自動的に同意されます。	-
任意のアップデートをインストール	この設定は Windows オペレーティングシステムのみ適用されます。 任意に設定されている場合でもアップデートがインストールされます。	-
再起動を許可	この設定は Windows オペレーティングシステムのみ適用されます。 オペレーティングシステムが更新をインストールすると、クライアントが再起動します。	-

■コマンドの実行

このタスクは、クライアントコンピューターで特定のコマンドライン命令を実行します。管理者は、実行するコマンドラインを入力します。



項目名	説明	必須
実行するコマンドライン	クライアントで実行する特定のコマンドラインを入力します。	○
作業ディレクトリ	「実行するコマンドライン」を実行するディレクトリを入力します。	-

!重 要

コマンドの実行タスクでは日本語のディレクトリパスや日本語のファイル名は使用できません。

■コンピューターのシャットダウン

このタスクは、クライアントコンピューターをシャットダウンまたは再起動します。

項目名	説明	必須
コンピューターの再起動	オンにするとタスク完了後にクライアントコンピューターは再起動され、オフにするとシャットダウンされます。	○

■ソフトウェアアンインストール

このタスクは、ESET 製品または他社のソフトウェアをクライアントコンピューターからアンインストールします。

!重 要

このタスクは注意して実行してください。ERA エージェントをアンインストールすると、一部の設定が管理対象の製品に残る場合があります。また、他社製のウイルス対策ソフトウェアをアンインストールするためには ESET AV Remover に対応している必要があります。

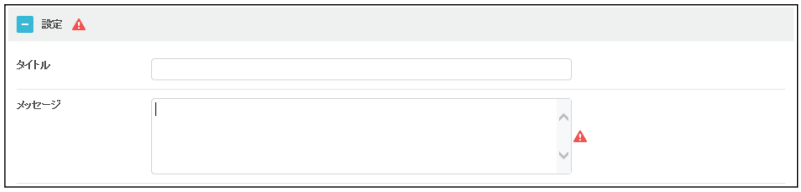
項目名	説明	必須
アンインストール	アンインストールする対象をリストから選択するか他社製の脅威対策ソフトウェアにするかを選択します。	○
パッケージ名	「アンインストール」で［リストからアプリケーション］を選択した場合に表示されます。 アンインストールする ERA コンポーネントまたは ESET 製品を選択します。選択したクライアントコンピューターにインストールされたすべてのパッケージがリストに表示されます。	-
パッケージバージョン	「アンインストール」で［リストからアプリケーション］を選択した場合に表示されます。 デフォルトでは、「パッケージ名」で選択したパッケージのバージョンだけをアンインストールします。［すべてのバージョンのパッケージをアンインストール］をクリックすると、ソフトウェアのすべてのバージョンを削除します。	-
アンインストール パラメータ	「アンインストール」で［リストからアプリケーション］を選択した場合に表示されます。 必要に応じて、アンインストーラー用の任意のコマンドラインパラメータを指定します。アンインストールパラメータ名は各ソフトウェアの各インストールパッケージで一意です。インストールパッケージ（msi）自体で使用されるプロパティだけを指定できます。Windows 用 ESET Endpoint 製品の場合、PASSWORD=< エンドポイントパスワード > パラメータを使用して、パスワード保護された製品のアンインストール用のパスワードを指定できます。 ※インストールパッケージ（msi）自体でのみ使用されるプロパティの msiexec パラメータを指定することはできません。	-
必要なときに自動的に再起動	「アンインストール」で［リストからアプリケーション］を選択した場合に表示されます。 アンインストールするために必要な場合は、オンにし、アンインストール後にクライアントコンピューターを強制的に再起動します。	-

■ソフトウェアインストール

「6.6.3.1　ESET セキュリティ製品」の「■ソフトウェアインストール」を参照してください。

■メッセージの表示

このタスクは、任意のデバイス（クライアントコンピューター、タブレット、モバイルなど）にメッセージを送信します。メッセージは画面表示としてユーザーに通知されます。



項目名	説明	必須
タイトル	表示するメッセージのタイトルを入力します。	-
メッセージ	表示するメッセージを入力します。メッセージ長は 1 以上でなければなりません。タイトルとメッセージの長さの合計は 250（メッセージは 250 文字）以下でなければなりません。	○

■管理の停止（ERA エージェントのアンインストール）

「6.6.3.2 ESET Remote Administrator」の「■管理の停止（ERA エージェントのアンインストール）」を参照してください。

6.6.3.4 モバイル

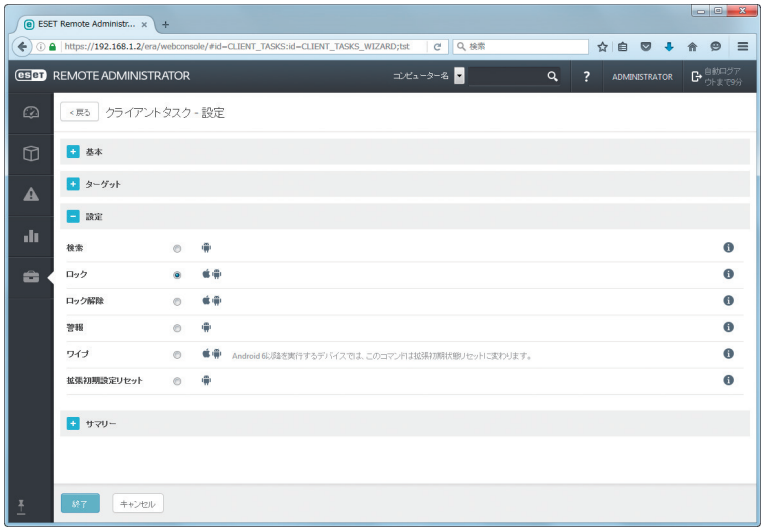
■ ESET 製品の設定エクスポート

「6.6.3.1 ESET セキュリティ製品」の「■ ESET 製品の設定エクスポート」を参照してください。

■アンチセフトアクション

このタスクは、モバイルデバイス（Android デバイスおよび iOS デバイス）を不正アクセスから保護するために使用します。ユーザーが ERA サーバーで管理している Android デバイスをなくしたり、盗まれたときには、紛失した Android デバイスの GPS 座標を要求したり、ロックを行ったり、警告音を鳴らしたり、Android デバイスに保存されたすべてのデータをリモートで消去したりできます。

iOS デバイスでは、ロック、ロック解除、拡張初期設定リセットのみ使用できます。



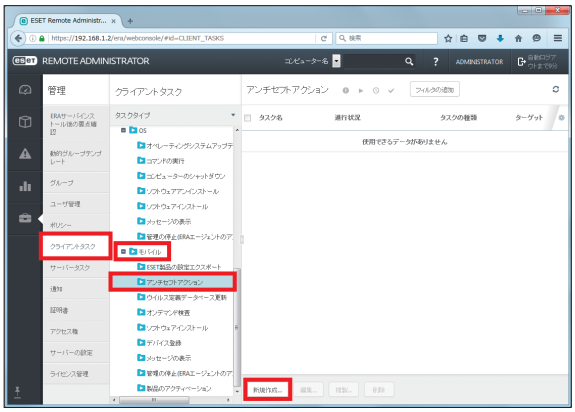
項目名	説明	必須
検索	現在位置の GPS 座標およびテキストメッセージを Android デバイスに要求します。また、より正確な位置情報が 10 分後に使用可能になった場合、Android デバイスはもう一度メッセージを送信します。受信した情報はコンピューター詳細に表示されます。	-
ロック	Android デバイスおよび iOS デバイスをロックします。Android デバイスは、管理者パスワードまたはロック解除コマンドを使用することでロック解除できます。	-
ロック解除	Android デバイスおよび iOS デバイスのロックを解除し、使用可能な状態にします。ロック解除した時点で使用されていた Android デバイスの SIM カードは信頼できる SIM として保存されます。	-
警報	Android デバイスをロックし、5 分間 (またはロック解除が実行されるまで) 大音量を再生します。	-
ワイプ	Android デバイス内のすべての使用可能なデータを完全に消去します (ファイルは上書きされます)。なお、ESET Endpoint Security for Android は Android に残ります。これには最大数時間かかる場合があります。 ※ Android 5 では使用できません。 ※ Android 6 以降では、ワイプを実行すると、拡張初期設定リセットの動作をします。 ※ Apple 社のアイコンが表示されていますが、iOS デバイスでは使用できません。	-

項目名	説明	必須
拡張初期設定リセット	Android デバイスおよび iOS デバイスでアクセスできるすべてのデータを迅速に削除します (ファイルヘッダーは破棄されます)。デバイスは既定の初期設定にリセットされます。これには数分かかる場合があります。 ※ Apple 社のアイコンが表示されていませんが、iOS デバイスで使用できます。	-

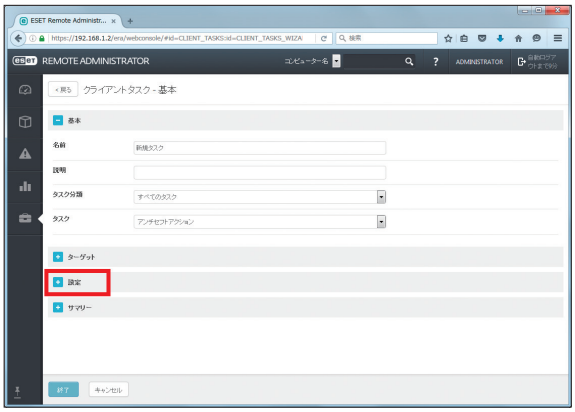
操作手順

ここでは、Android デバイス内のすべての使用可能なデータを完全に消去する「ワイプ」を例に、アンチセフトアクションの実行手順を紹介ます。

1 ［管理］>［クライアントタスク］>［モバイル］>［アンチセフトアクション］とクリックし、［新規作成］をクリックします。

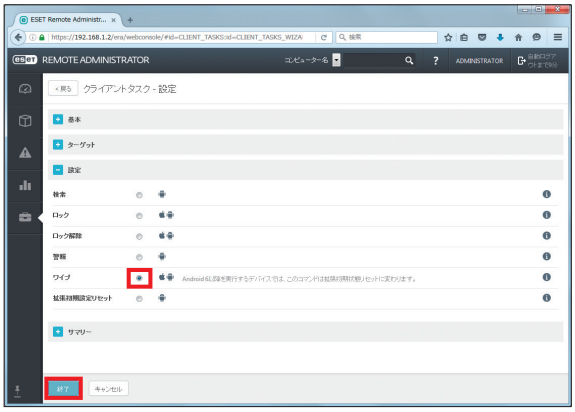


2 必要に応じて、タスクの名称を入力し、［設定］をクリックします。



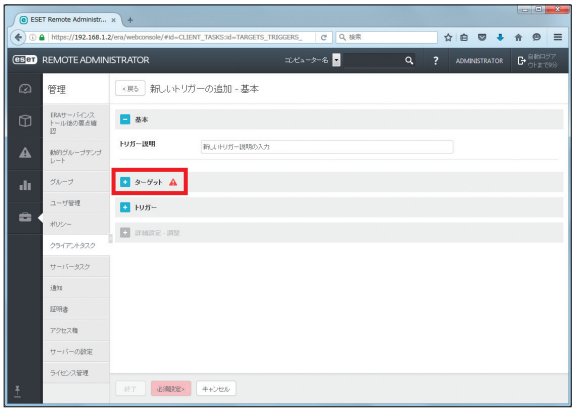
続く

3 ［ワイプ］をクリックしてオンにし、［終了］ボタンをクリックします。



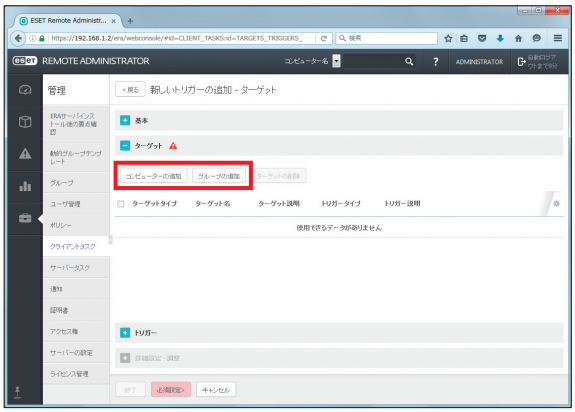
4 ［トリガーの作成］ボタンをクリックします。

5 ［ターゲット］をクリックします。

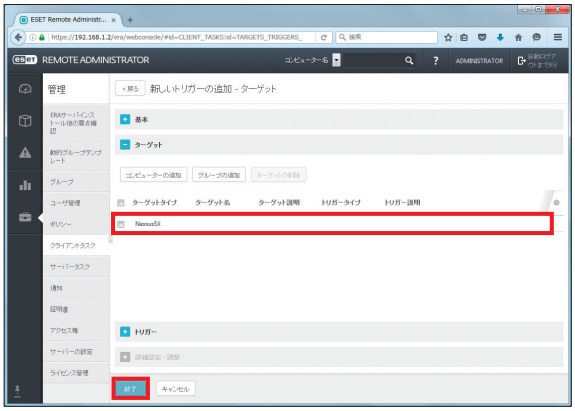


続く

6 ［コンピューターの追加］または［グループの追加］をクリックし、クライアントタスクを実行するコンピューターまたはグループを選択します。



7 クライアントタスクを実行するコンピューターまたはグループを選択したら、［終了］をクリックします。クライアントタスクが実行されます。



■オンデマンド検査

「6.6.3.1　ESET セキュリティ製品」の「■オンデマンド検査」を参照してください。

■ソフトウェアインストール

「6.6.3.1　ESET セキュリティ製品」の「■ソフトウェアインストール」を参照してください。

■メッセージの表示

「6.6.3.3　OS」の「■メッセージの表示」を参照してください。

■モジュールアップデート

「6.6.3.1　ESET セキュリティ製品」の「■モジュールアップデート」を参照してください。

■管理の停止（ERA エージェントのアンインストール）

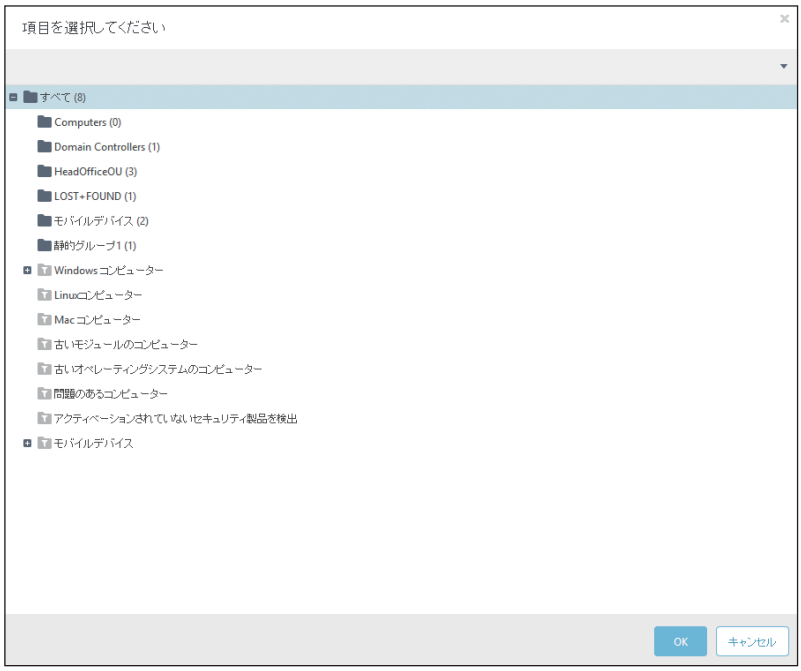
「6.6.3.2　ESET Remote Administrator」の「■管理の停止（ERA エージェントのアンインストール）」を参照してください。

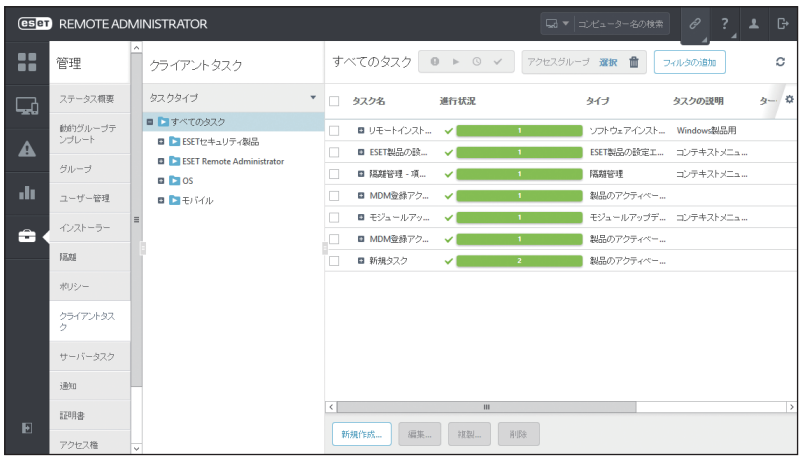
■製品のアクティベーション

「6.6.3.1　ESET セキュリティ製品」の「■製品のアクティベーション」を参照してください。

6.6.4 アクセスグループ

「アクセスグループ」では、ユーザーが選択した静的グループに応じて、表示されるオブジェクトをフィルタリングできます。［選択］をクリックすると、フィルタリングするグループを選択できます。また、🗑をクリックすると、フィルターリングを解除できます。





6.7 サーバータスク

サーバータスクでは、日常的な処理を自動化します。自動化する処理をタスクとして設定し、トリガーを適用します。タスクは、トリガーを適用することにより、ERA サーバーで発生する特定イベントの組み合わせに対して、実行することが可能となります。トリガーは、タスクの設定中に適用します。

ESET Remote Administrator では、次のタスクタイプが用意されており、スケジュールすることができます。

タスクタイプ	詳細
エージェント展開	ERA エージェントをクライアントコンピューターに配布します。
コンピューター名の変更	FQDN 形式を使用してグループのコンピューター名を変更します。
ユーザー同期	Active Directory、LDAP パラメーターなどのソースからユーザーおよびユーザーグループ情報を同期します。
レポートの生成	必要に応じてレポートを生成します。
接続していないコンピューターの削除	ESET Remote Administrator に接続していないクライアントコンピューターを ERA Web コンソールから削除します。
静的グループの同期	グループのクライアント情報を更新します。

! 重 要

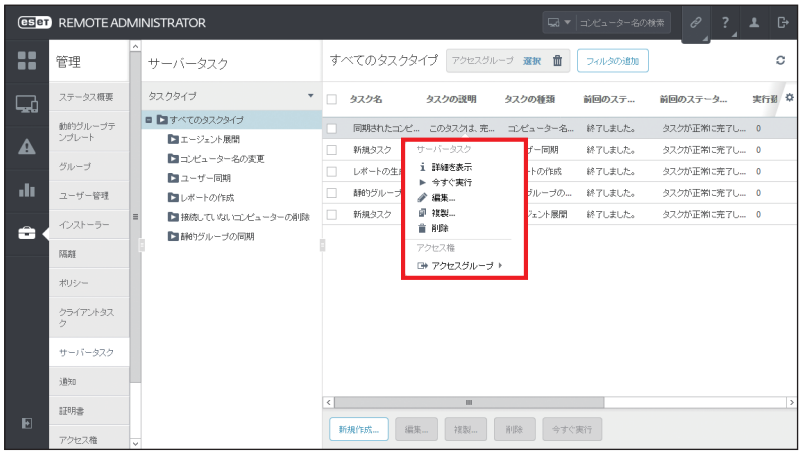
サーバータスクを、特定のクライアントに割り当てることはできません。

6.7.1 サーバータスク画面の構成

「サーバータスク」画面の構成について説明します。

1	**タスクタイプリスト**	すべてのサーバータスクタイプが表示されます。作成したサーバータスクはここに表示されるタスクタイプごとに分類されます。
2	**既存のタスクタイプ詳細**	サーバータスクのリストが表示されます。
3	**新規作成**	新しいサーバータスクを作成します。「サーバータスク」画面が表示されます。 画面の詳細は「6.7.2 新しいサーバータスクの作成」を参照してください。
4	**編集**	選択しているサーバータスクを編集します。「サーバータスクの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいサーバータスクとして保存することができます。同じ名前のタスクは保存できない為、名前の変更は必須となります。 画面の詳細は、「6.7.2 新しいサーバータスクの作成」を参照してください。
5	**複製**	選択しているサーバータスクをコピーした状態で「サーバータスク」画面が表示されます。 画面の詳細は「6.7.2 新しいサーバータスクの作成」を参照してください。
6	**削除**	選択しているサーバータスク（複数選択可）を完全に削除します。
7	**今すぐ実行**	選択しているサーバータスクを直ちに実行します。
8	**アクセスグループ**	「アクセスグループ」では、ユーザーが静的グループを選択し、属するグループに応じて、表示されるオブジェクトをフィルタリングできます。［選択］をクリックすると、フィルタリングするグループを選択できます。また、 をクリックすると、フィルタリングを解除できます。

■「サーバータスク」コンテキストメニューのアクション



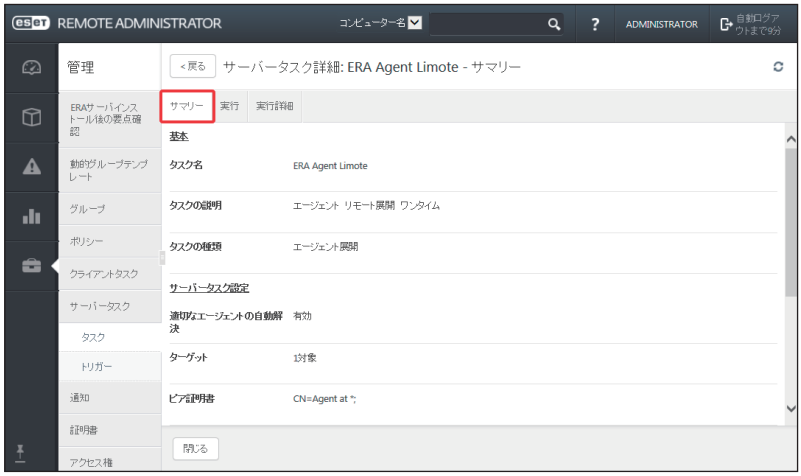
	詳細	選択しているサーバータスクの情報を確認します。「サーバータスク詳細」画面が表示されます。 画面の詳細は、「●サーバータスクの詳細確認画面」を参照してください。
	今すぐ実行	選択しているサーバータスクを直ちに実行します。
	編集	選択しているサーバータスクを編集します。「サーバータスクの編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいサーバータスクとして保存することができます。同じ名前のタスクは保存できない為、名前の変更は必須となります。 画面の詳細は、「6.7.2　新しいサーバータスクの作成」を参照してください。
	複製	選択しているサーバータスクをコピーした状態で「サーバータスク」画面が表示されます。 画面の詳細は、「6.7.2　新しいサーバータスクの作成」を参照してください。
	削除	選択しているサーバータスク（複数選択可）を完全に削除します。
	アクセスグループ	選択したタスクを別のグループに移動します。「項目を選択してください」画面が表示され、移動先のグループを選択できます。

●サーバータスクの詳細確認画面

サーバータスクの詳細確認画面では、各タブに選択したサーバータスクの設定情報や実行詳細が表示されます。

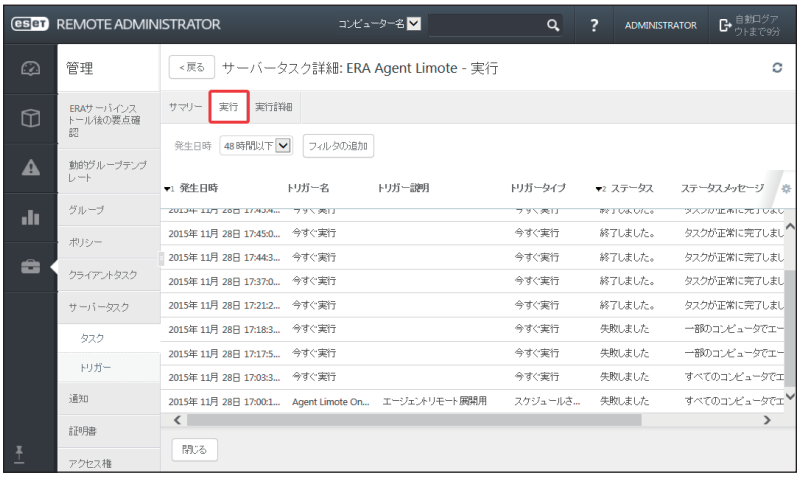
- **「サマリー」タブ**

  選択したサーバータスクの「基本」「設定」「トリガー」に入力した内容が読み取り専用の状態で表示されます。



- **「実行」タブ**

選択したサーバータスクのトリガーおよび実行結果が表示されます。



6.7.2 新しいサーバータスクの作成

新しいサーバータスクを作成する場合は、タスクタイプから目的のタスクを選択します。
サーバータスクの設定は、選択したタスクタイプに合わせて項目が変わります。
ここでは、新しくサーバータスクを作成する基本的な手順と、各サーバータスク共通画面の項目を説明します。

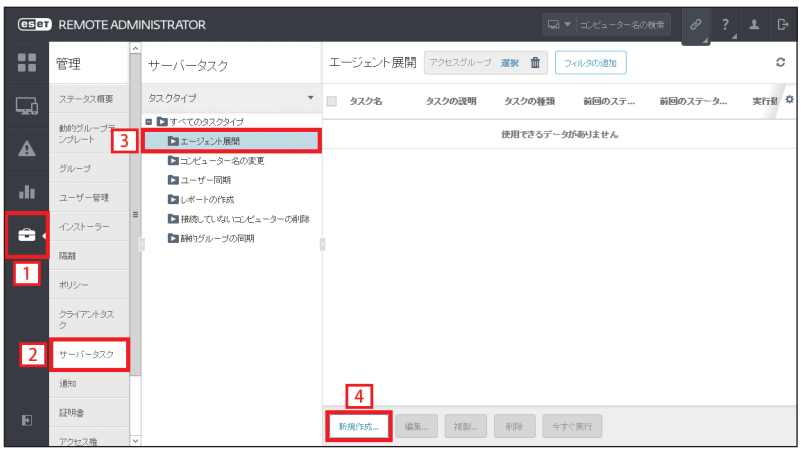
ワンポイント

タスクタイプの設定項目については、「6.7.3 各タスクタイプの設定項目」を参照してください。

操作手順

1. ［管理］メニューをクリックします。
2. ［サーバータスク］サブメニューをクリックします。
3. ［タスクタイプ］を選択します。

   ここでは、タスクタイプ「エージェント展開」を選択しています。
4. ［新規作成］ボタンをクリックします。



「新しいサーバータスク」画面が表示されます。

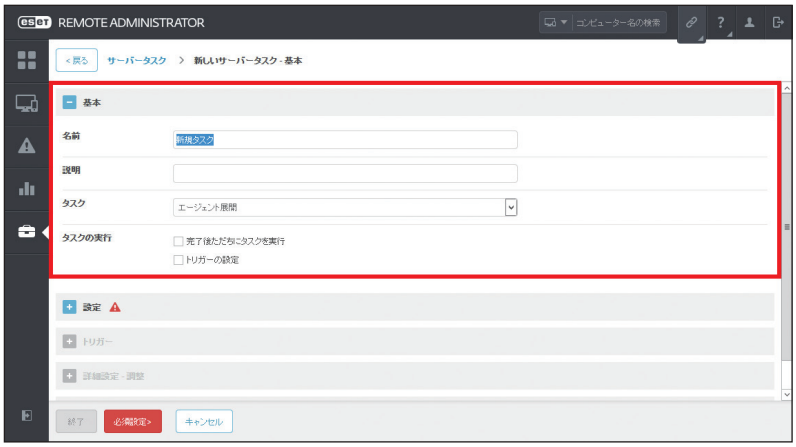
続く

5 「基本」の各項目を入力します。

各タスクタイプ共通の項目です。手順 3 で選択したタスクタイプが「タスク」へ反映されます。

ワンポイント

［すべてのタスクタイプ］を選択すると「タスク」は空欄で表示され、タスクタイプをどれか選択しない限り「設定」および「トリガー」の各目は設定できない状態で表示されます。



■基本

項目名		説明	必須
名前	作成するサーバータスクの名前を入力します。画面には、ここで設定した名前が表示されます。		○
説明	作成するサーバータスクの説明を入力します。		-
タスク	タスクタイプを選択、表示します。「サーバータスク」画面でタスクタイプを選択している場合は、該当するタスクタイプが反映されます。		○
タスクの実行	完了後ただちにタスクを実行	このタスクの設定完了と同時にタスクの実行を行います。	-
	トリガーの設定	タスクを実行するトリガーの設定を行います。トリガーの詳細について、「6.7.4.1　各トリガータイプの設定項目」をご参照ください。	

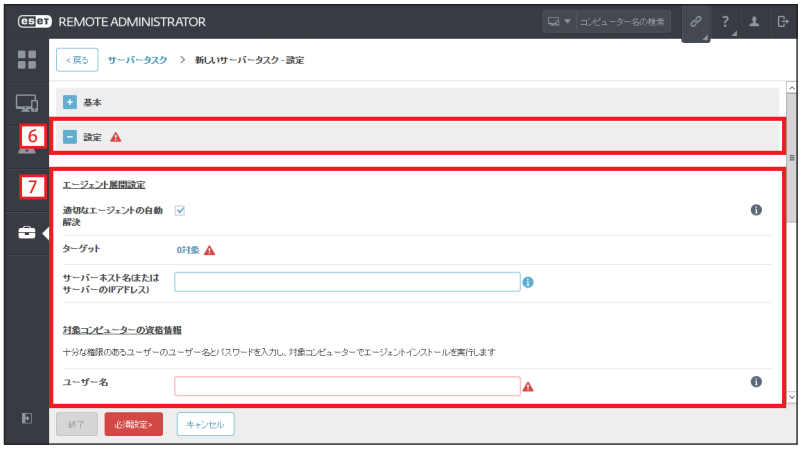
続く

6 ［設定］をクリックします。

各タスクタイプに共通して表示されるセクションです。

7 「設定」の各項目を入力します。

水色の文字はリンクです。クリックするとその項目の詳細設定画面が表示されます。



※画面は、タスクタイプ「エージェント展開」の設定項目です。

■設定

! 重 要

「設定」の項目は、選択したタスクタイプに対応した項目が表示されます。
各タスクタイプの項目詳細は、「6.7.3 各タスクタイプの設定項目」を参照してください。

8 手順 5 で［トリガーの設定］にチェックを入れたときは［トリガー］をクリックします。

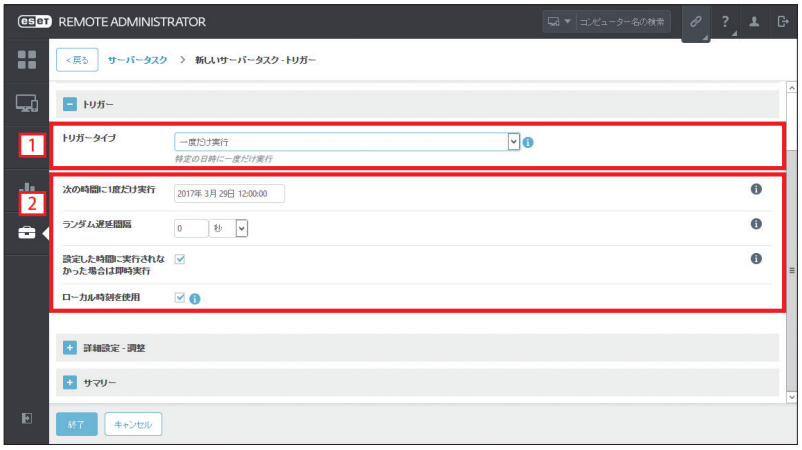
「新しいサーバータスク - トリガー」画面が表示されます。

ワンポイント

手順 5 で［完了後ただちに実行］にチェックをいれたときは、トリガーの設定を行えません。手順 12 に進んでください。

続く

9 「トリガー」の各項目を入力します。



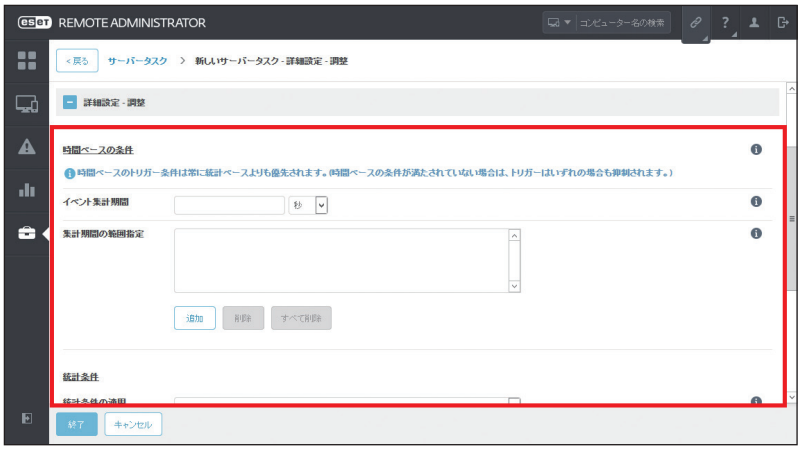
■トリガー

トリガーとはタスクを実行させる一連の条件のことです。指定した条件が満たされるとタスクの実行を開始します。

1	**トリガータイプ**	タスクをトリガーするイベントを選択します。「スケジュール済み」「動的グループ」「その他」でグループ分けされた項目の中から選択できます。トリガータイプの詳細については、「6.7.4 トリガー」をご参照ください。
2	**選択したトリガータイプよって設定する項目**	選択したトリガータイプに応じた設定項目が表示されます。表示される設定項目については、「6.7.4.1 各トリガータイプの設定項目」をご参照ください。

10 [詳細設定 - 調整] をクリックします。

11 「詳細設定 - 調整」の各項目を入力します。



続く

■詳細設定 - 調整

「詳細設定 - 調整」画面で表示される項目については、「6.7.4.2 詳細設定 ー 調整」を参照してください。

ワンポイント

「詳細設定 - 調整」画面は、「トリガータイプ」で選択した内容に従い有効になります。イベントログトリガーや結合された動的グループトリガーなど頻繁に発生するイベントでタスクがトリガーされる場合は、タスクの実行を制限するために「詳細設定 - 調整」が使用されます。
調整条件はイベント発生時間に絞り込まれます。「時間ベースの条件」は、「統計条件」よりも優先されます。

12 ［サマリー］をクリックします。

「基本」「設定」「トリガー」に入力した内容が読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。
各タスクタイプ共通して表示される確認画面です。

13 設定した内容を確認します。問題がなければ［終了］ボタンをクリックします。

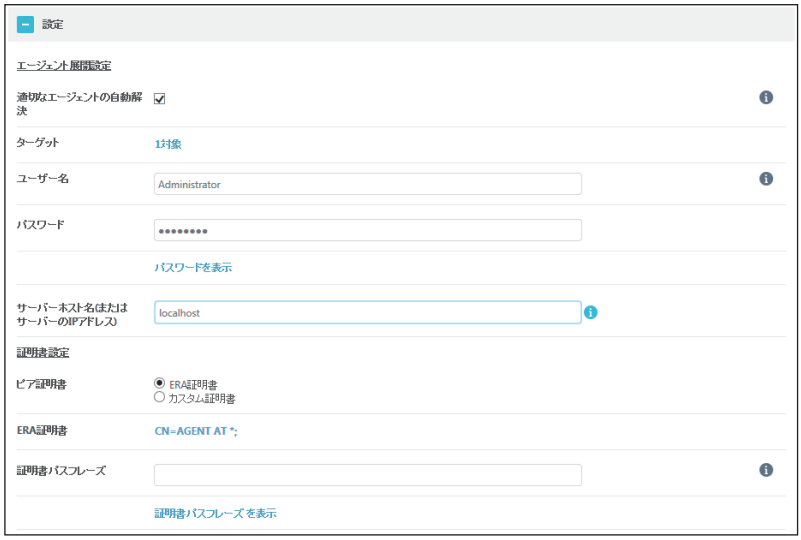
タスクリストに、作成したサーバータスクが表示されます。

6.7.3 各タスクタイプの設定項目

ここからは、各タスクタイプの「設定」セクションに表示される項目について説明します。

6.7.3.1 エージェント展開

エージェント展開は、ERA エージェントをクライアントコンピューターにリモート展開するタスクです。
タスクタイプ「エージェント展開」の詳細設定を行う画面です。



項目名	説明		必須
エージェント展開設定	適切なエージェントの自動解決	オンにすると、展開対象のクライアントコンピューターの OS に合った ERA エージェントのインストーラーを自動的に選択します。 インストーラーを手動で選択する場合は、オフにします。	-
	ターゲット	［0 対象］から、展開対象のクライアントコンピューターを選択します。 ターゲットを選択する画面が表示されます。	○
	ユーザー名	ERA エージェントのリモート展開を実行する権限を持つユーザー名を入力します。	○
	パスワード	ERA エージェントのリモート展開を実行する権限を持つユーザーパスワードを入力します。	○
	パスワードを表示	入力したパスワードを文字列表示します。	-
	サーバーホスト名（またはサーバーの IP アドレス）	クライアントコンピューターから接続できるサーバーのホスト名または IP アドレスを入力します。 空白の場合は、サーバーホスト名が使用されます。	-

項目名	説明		必須
証明書設定	ピア証明書	証明書の種類を選択します。 ERA 証明書　　：ERA で作成された認証局の証明書 カスタム証明書　：独自に用意した証明書	○
	ERA 証明書	「ピア証明書」から［ERA 証明書］を選択した場合に表示されます。 証明書の選択方法は、「■ピア証明書」を参照してください。	△
	カスタム証明書	「ピア証明書」から［カスタム証明書］を選択した場合に表示されます。 証明書の指定方法は、「■ピア証明書」を参照してください。	△
	証明書パスフレーズ	指定した証明書のパスワードです。パスワードを設定している場合に入力します。 カスタム証明書を選択している場合は、カスタム証明書のパスワードを入力します。	-

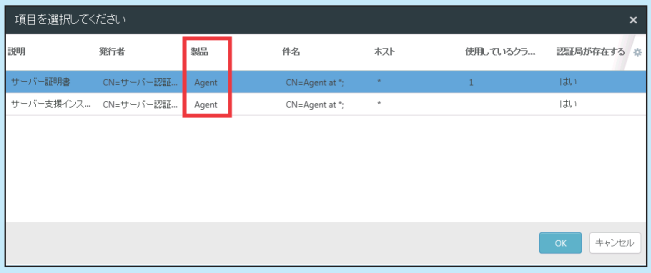
■ピア証明書

●［ERA 証明書］を選択した場合

［<証明書が設定されていません>］から、該当する ERA 既定の証明書を選択します。

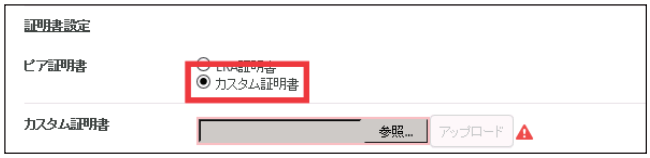
ワンポイント

証明書の選択画面では、ERA Web コンソールで作成されているすべてのピア証明書が表示されます。ここでは、「製品」の項目で「Agent」と表記されているものを選択します。



●［カスタム証明書］を選択した場合

［参照］ボタンから、カスタム証明書を参照し、［アップロード］ボタンをクリックします。



6.7.3.2 コンピューター名の変更

タスクタイプ「コンピューター名の変更」の詳細設定を行う画面です。
「コンピューター名の変更」は、FQDN 形式を使用してグループのコンピューター名を定期的に変更します。

項目名	説明		必須
グループ名	選択	静的または動的グループを選択します。グループを選択する画面が表示されます。	○
	新しい静的グループ	新しい静的グループを作成します。「新しい静的グループ」画面が表示されます。 画面の詳細は、「6.3.2.1 新しい静的グループの作成」を参照してください。	-
	新しい動的グループ	新しい動的グループを作成します。「新しい動的グループ」画面が表示されます。 画面の詳細は、「6.3.2.2 新しい動的グループの作成」を参照してください。	-
次に基づいて名前を変更		「コンピューター名」または「コンピューター FQDN」から選択します。	-

6.7.3.3 レポートの作成

「レポートの作成」は、必要に応じてレポートを生成します。

項目名	説明		必須
レポートオプションを生成	レポートテンプレート	レポートテンプレートの選択画面が表示されます。作成するレポートのテンプレートを選択します。 新しいレポートテンプレートを作成する場合は、「5.5 レポート」を参照してください。	○
レポート配信	電子メールを送信	オンにすると、生成されるレポートをメールとして送信します。表示される項目については、「■レポート配信」の「●［電子メールを送信］をオンにした場合」を参照してください。	-
	ファイルに保存	オンにすると、生成されるレポートをファイルとして保存します。表示される項目については、「■レポート配信」の「●［ファイルに保存］をオンにした場合」を参照してください。	-

■レポート配信

●［電子メールを送信］をオンにした場合

項目名	説明		必須
電子メールメッセージ	送信先	送信するメールのあて先を入力します。［CC の追加］［BCC の追加］から、CC および BCC の送信先を追加することができます。	○
	件名	送信するメールの件名を入力します。［カスタムヘッダーの追加］から、ヘッダー情報を追加することができます。	-
	メッセージの内容	作成されたレポートと共に送信するメッセージを入力します。	-
	レポートが空の場合にメールを送信	オンにすると、作成されたレポート結果が空白であってもメールを送信します。	-
	+ 印刷オプションを表示	作成されたレポートの出力形式を設定します。	-

●［ファイルに保存］をオンにした場合

項目名	説明		必須
ファイルオプション	相対ファイルパス	作成されたレポートを保存する場所を指定します。	○
	レポートが空の場合にメールを送信	オンにすると、作成されたレポート結果が空白であってもメールを送信します。	-
	+ 印刷オプションを表示	作成されたレポートの出力形式を設定します。	-

6.7.3.4 接続していないコンピューターの削除

ESET Remote Administrator に接続していないクライアントコンピューターを ERA Web コンソールから削除します。

! 重 要

接続していないコンピューターの削除は、クライアントコンピューターが 1 つだけ属することができる「静的グループ」を対象として行います。

項目名	説明		必須
グループ名	選択	グループの選択画面が表示されます。静的グループを選択します。	○
	新しい静的グループ	新しく静的グループを作成します。「新しい静的グループ」画面が表示されます。 画面の詳細は、「6.3.2 新しいグループの作成」を参照してください。	-
コンピューターが接続していない日数		削除する基準となる、接続していない日数を入力します。	○
ライセンスのアクティベーションの解除		オンにすると、削除されるクライアントコンピューターのライセンスのアクティベーション解除を実行します。	○
管理されていないコンピューターの解除		オンにすると、管理されていないクライアントコンピューターを削除します。	○

6.7.3.5 静的グループの同期

静的グループの同期は、ネットワーク内のクライアントコンピューターを検索し、指定した静的グループに配置します。対象のクライアントコンピューターや指定した静的グループの状況によって、処理の方法を選択することができます。また、使用しているネットワークの種類によって、同期設定が変わります。

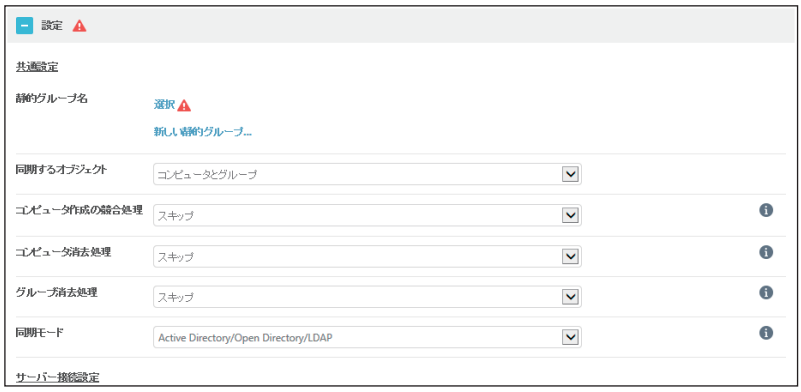
静的グループの同期で設定できるネットワークの種類は、次のとおりです。

- Active Directory/Open Directory/LDAP
- MSWindows ネットワーク
- VMware

ネットワークの種類は、「同期モード」の項目で選択します。

! 重 要

既定の設定では、タスクの受信対象は Windows コンピューターとなっています。
Windows ドメインの Linux コンピューターをこのタスクの受信対象とする場合は、この後に記載する「■静的グループの同期　Linux OS」の操作を行ってください。

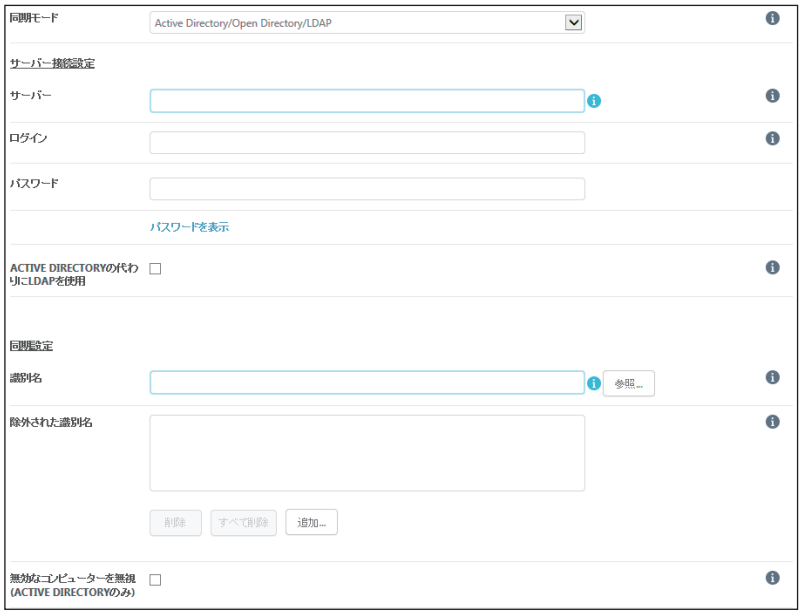


項目名	説明			必須
共通設定	静的グループ名	選択	既存の静的グループを選択します。	○
		新しい静的グループ	新規の静的グループを作成します。 詳細は、「6.3.2.1　新しい静的グループの作成」を参照してください。	-
	同期するオブジェクト	同期させる対象を、「クライアントコンピューターおよびグループ」または「クライアントコンピューター」から選択します。		○
	コンピュータ作成の競合処理	同期によって、クライアントコンピューターの競合が発生した場合の処理を、次の 2 つから選択します。 スキップ　：同期されるクライアントコンピューターを追加しない 移動　　：新しいクライアントコンピューターはサブグループに移動する		○
	コンピュータ消去処理	クライアントコンピューターが存在しない場合の処理を、「スキップ」または「削除」から選択します。		○
	グループ消去処理	グループが存在しない場合の処理を、「スキップ」または「削除」から選択します。		○
	同期モード	ネットワークの種類を次の 3 つから選択します。 ・「Active Directory/Open Directory/LDAP」 ・「MSWindows ネットワーク」 ・「VMware」 選択によって、「同期モード」より下に表示される項目が変わります。詳細は、次の「■同期モード」を参照してください。		○

■同期モード

同期モードで選択したネットワークの種類によって、同期設定以降の項目の設定内容が変わります。

● Active Directory/Open Directory/LDAP

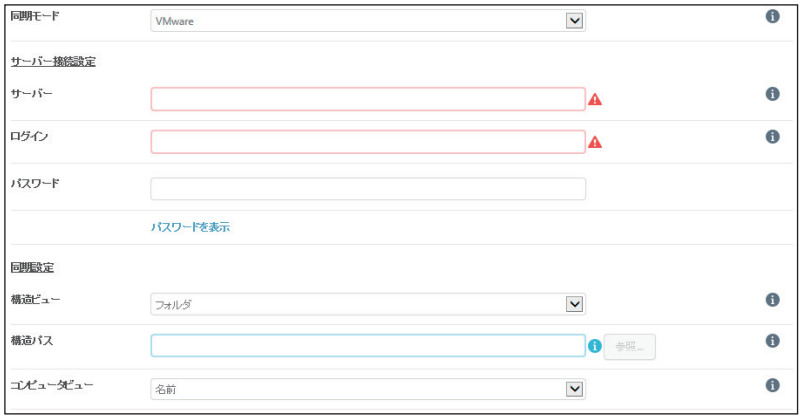


項目名	説明		必須
サーバー接続設定	サーバー	ドメインコントローラーのサーバー名または IP アドレスを入力します。	-
	ログイン	ドメインコントローラーのログイン認証情報を、「ドメイン ¥ ユーザー」の形式で入力します。	-
	パスワード	ドメインコントローラーにログインするためのパスワードを入力します。	-
	パスワードを表示	上記のパスワードを文字列表示します。	-
	ACTIVE DIRECTORY の代わりに LDAP を使用	LDAP を使用する場合は、オンにします。	-
同期設定	識別名	Active Directory ツリーのノードへのパス（識別名）。このオプションを空欄にすると、AD ツリー全体を同期します。	-
	除外された識別名	Active Directory ツリーの特定のノードを除外（無視）することを選択できます。	-
	無効なコンピューターを無視（ACTIVE DIRECTORY のみ）	Active Directory で無効なコンピューターを無視できます。タスクはこのコンピューターをスキップします。	-

MSWindows ネットワーク

項目名	説明		必須
MICROSOFT WINDOWS ネットワーク同期設定	ワークグループ	ドメインコントローラーのサーバー名または IP アドレスを入力します。	-
	ログイン	ドメインコントローラーのログイン認証情報を、「ドメイン ¥ ユーザー」の形式で入力します。	-
	パスワード	ドメインコントローラーにログインするためのパスワードを入力します。	-
	パスワードを表示	上記のパスワードを文字列表示します。	-

VMware



項目名	説明		必須
サーバー接続設定	サーバー	VMware/vCenterServer の DNS または IP アドレスを入力します。	○
	ログイン	VMware/vCenterServer のログイン認証情報を、「ドメイン ¥ ユーザー」の形式で入力します。	○
	パスワード	VMware/vCenterServer にログインするためのパスワードを入力します。	-
	パスワードを表示	上記のパスワードを文字列表示します。	-
同期設定	構造ビュー	同期中に列挙される VMware の構造ビュータイプを、「フォルダ」または「リソースプール」から選択します。	○
	構造パス	［参照］ボタンから、同期する VMware の構造パスを設定します。空白の場合は、構造全体が同期されます。	-
	コンピュータビュー	同期後のコンピューター名を、VMware の属性の「名前」、「ホスト名」、「IP アドレス」から選択します。	○

■静的グループの同期　Linux OS

Windows ドメインに参加している Linux コンピューターは、Windows Server の管理コンソールのひとつである、「Active Directory ユーザーとコンピューター」の「Computers」のプロパティ画面にテキストが表示されないため、手動でテキストを挿入する必要があります。
そのため、同じく Windows Server の管理コンソールである「ADSI エディター」を使用し、Linux コンピューターのプロパティを変更します。
次の前提条件を確認します。

- Linux コンピューターが Active Directory に存在すること
- ドメインコントローラーへの DNS サーバーのインストール
- ADSI エディターのインストール

ワンポイント

ADSI エディターは、管理コンソールとして Windows Server に包括されているサポートツールです。

操作手順

1. ［スタート］＞［すべてのプログラム］＞［管理ツール］から、「ADSI エディター」を起動します。

   ADSI エディターが起動します。

   ワンポイント

   ADSI エディターを起動した時点で、左側のペインに該当するドメインコントローラーが存在している場合は手順 6 に進んでください。

2. ［操作］メニューから［接続］を選択します。

「接続の設定」画面が表示されます。

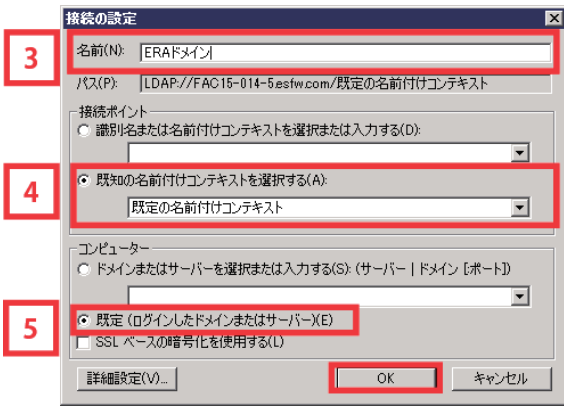
3. ドメインコントローラーの「名前」を入力します。

4. ［既定の名前付けコンテキストを選択する］を選択し、リストから［既定の名前付けコンテキスト］を選択します。

   「既定の名前付けコンテキスト」とは、ドメインコントローラーを表します。

続く

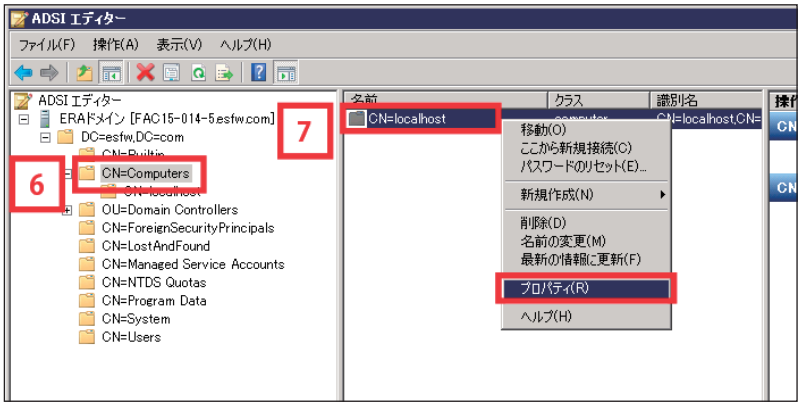
5 [既定（ログインしたドメインまたはサーバー）] を選択し [OK] ボタンをクリックします。



「ADSI エディター」ツリーに、作成したドメインコントローラーの名前が表示されます。

6 「ADSI エディター」ツリーに表示される、作成したドメインコントローラーを展開し、Linux コンピューターが表示される CN（共通名）グループまたは OU（組織単位）グループをクリックします。

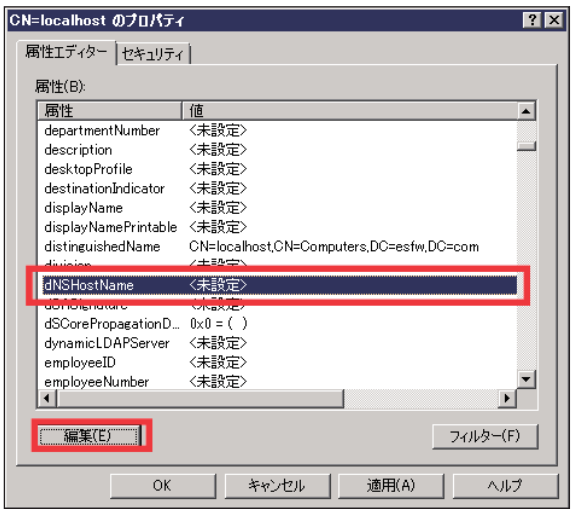
7 Linux コンピューターのホスト名を右クリックし、[プロパティ] を選択します。



選択した Linux コンピューターのプロパティが表示されます。

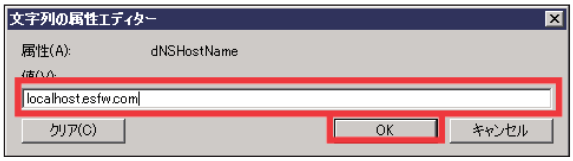
8 「属性エディター」タブの「属性」リストから、「dNSHostName」を選択し [編集] ボタンをクリックします。

「文字列の属性エディター」画面が表示されます。



続く

9 「値」のテキストボックスに Linux コンピューターのホスト名を入力し、[OK] ボタンをクリックします。

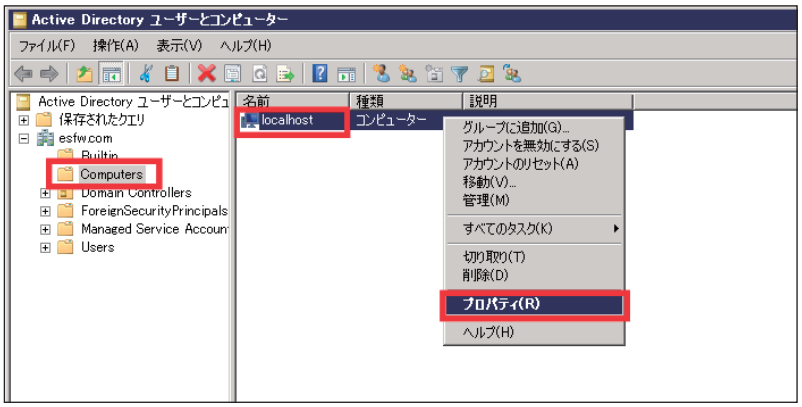


10 ADSI エディターを閉じます。

11 「Active Directory ユーザーとコンピューター」を起動します。

「Active Directory ユーザーとコンピューター」の Linux コンピューターのプロパティを確認します。

12 Linux コンピューターの［プロパティ］を選択します。



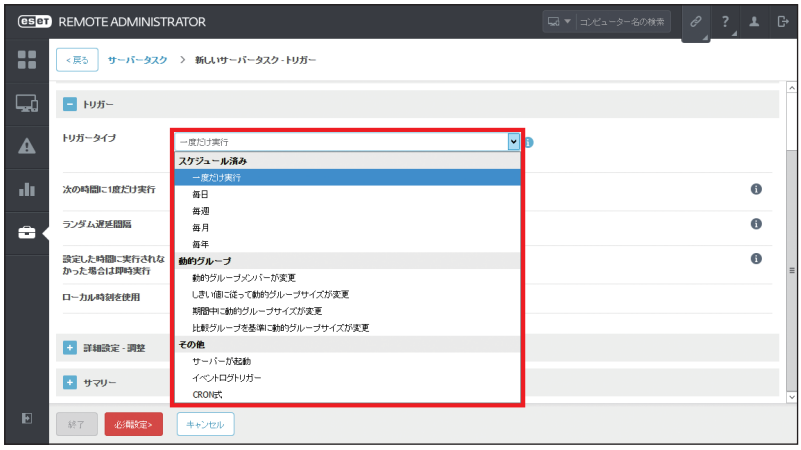
選択した Linux コンピューターのプロパティが表示されます。
テキストが表示されていることを確認します。

6.7.4 トリガー

トリガーは、設定した方法で特定のイベントに反応するセンサーです。
トリガーは設定した日時やイベントによって起動するか、または特定のシステムイベントの発生時に起動します。一般的に、処理を自動化するために用いられます。
新しく作成されたサーバータスクは、即時実行も行えますが、適用したトリガーの起動と連動して実行することもできます。

6.7.4.1 各トリガータイプの設定項目

トリガーの「設定」セクションでは、トリガーが実行されるためのイベントである「トリガータイプ」に合わせた項目を設定します。
「設定」セクションの特徴として、トリガータイプを選択することにより、設定すべき項目が切り替わります。ここでは、トリガータイプ別に設定項目を説明します。



「トリガータイプ」から選択可能なトリガータイプは、次のとおりです。

分類	トリガータイプ	詳細
スケジュール済み	一度だけ実行	特定の日時に一度だけ実行します。
	毎日	毎日繰り返して実行します。
	週	毎週繰り返して実行します。
	毎月	毎月繰り返して実行します。
	毎年	毎年繰り返して実行します。
動的グループ	動的グループメンバーが変更	動的グループの内容が変更されたときに実行します。
	しきい値に従って動的グループサイズが変更	動的グループのクライアント数が指定したしきい値よりも、上または下になったときに実行します。
	期間中に動的グループサイズが変更	動的グループのクライアント数が特定の期間で変更されたときに実行します。
	比較グループを基準に動的グループのサイズが変更	基準とする動的グループのクライアント数が比較グループ（静的または動的）に従って変更されたときに実行します。

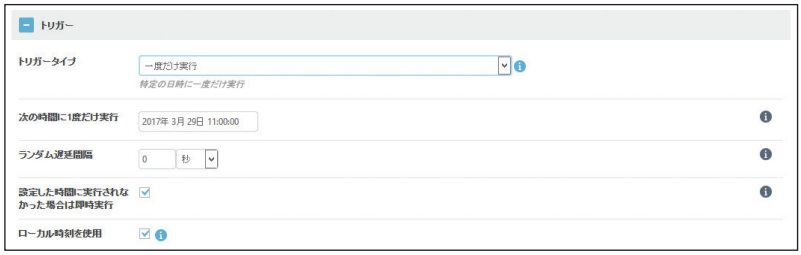
分類	トリガータイプ	詳細
その他	サーバーが起動	サーバー起動時に実行します。
	イベントログトリガー※ 1	特定のタイプのイベントがログで発生したときに実行します。
	CRON 式	CRON 式に基づく予定で実行します。

※ 1 「イベントログトリガー」の詳細は、「●イベントログトリガー」を参照してください。

■スケジュール済み

●一度だけ実行

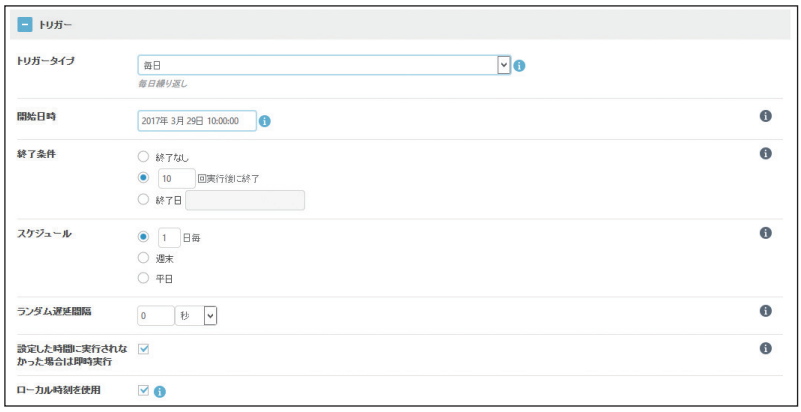
特定の日時に一度だけ実行します。



項目名	説明	必須
トリガータイプ	［一度だけ実行］を選択します。	○
次の時間に 1 度だけ実行	実行する予定時刻を指定します。 テキストボックスをクリックするとカレンダーが表示されます。	○
ランダム遅延間隔	遅延間隔を指定します。 時間単位を、「秒」「分」「時間」「日」「週」から選択します。	○
設定した時間に実行されなかった場合は即時実行	オンにすると、指定時刻にトリガー起動しなかった場合、タスクが実行できる状態になりしだい直ちにトリガーを起動します。	○
ローカル時刻を使用	対象となるクライアントコンピューターの時刻を使用します。	○

●毎日

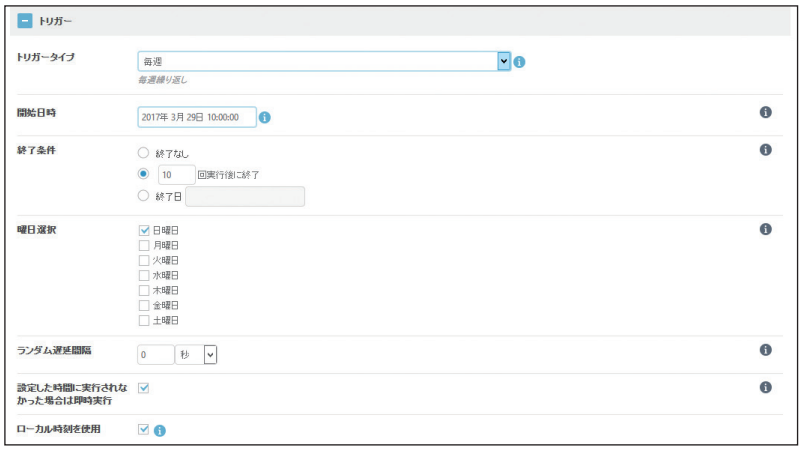
毎日繰り返して実行します。



項目名	説明	必須
トリガータイプ	［毎日］を選択します。	○
開始日時	開始日時を指定します。 テキストボックスをクリックすると、カレンダーが表示されます。	○
終了条件	終了条件を、次の 3 種類から選択します。 ・「終了なし」 ・「end after」　：終了実行回数を指定します。 ・「終了日」　：具体的な終了日を指定します。	○
スケジュール	スケジュール方法を、次の 3 種類から選択します。 ・「every」　：起動間隔の日数を指定します。 ・「週末」 ・「平日」	○
ランダム遅延間隔	遅延間隔を指定します。 時間単位を、「秒」「分」「時間」「日」「週」から選択します。	○
設定した時間に実行されなかった場合は即時実行	オンにすると、指定時刻にトリガー起動しなかった場合、タスクが実行できる状態になり直ちにトリガーを起動します。	○
ローカル時刻を使用	オンにすると、対象となるクライアントコンピューターの時刻を使用します。	○

●週

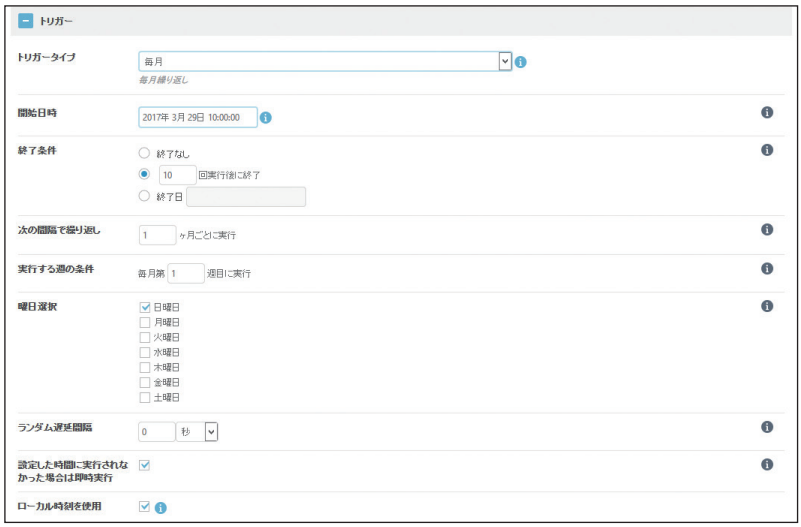
毎週繰り返して実行します。



項目名	説明	必須
トリガータイプ	［週］を選択します。	○
開始日時	開始日時を指定します。	○
終了条件	終了条件を、次の 3 種類から選択します。 ・「終了なし」 ・「end after」　：終了実行回数を指定します。 ・「終了日」　：具体的な終了日を指定します。	○
曜日選択	タスクを実行する曜日を指定します。複数選択が可能です。	○
ランダム遅延間隔	遅延間隔を指定します。 時間単位を、「秒」「分」「時間」「日」「週」から選択します。	○
設定した時間に実行されなかった場合は即時実行	オンにすると、指定時刻にトリガー起動しなかった場合、タスクが実行できる状態になりしだい直ちにトリガーを起動します。	○
ローカル時刻を使用	オンにすると、対象となるクライアントコンピューターの時刻を使用します。	○

●毎月

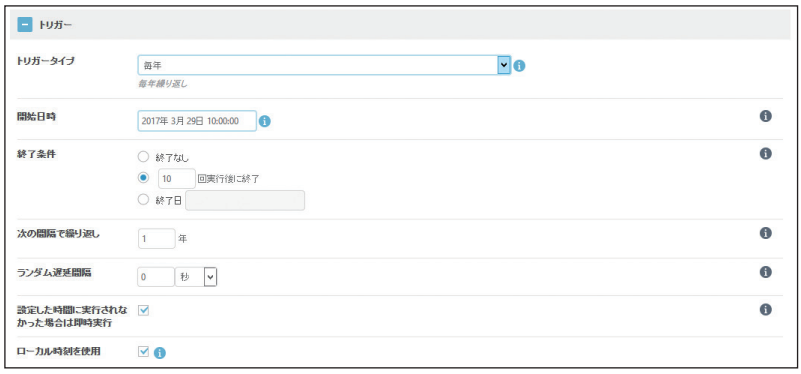
毎月繰り返して実行します。



項目名	説明	必須
トリガータイプ	［毎月］を選択します。	○
開始日時	開始日時を指定します。	○
終了条件	終了条件を、次の 3 種類から選択します。 ・「終了なし」 ・「end after」　：終了実行回数を指定します。 ・「終了日」　：具体的な終了日を指定します。	○
次の間隔で繰り返し	タスクを繰り返す間隔を、月単位で指定します。	○
実行する週の条件	タスクを月の何週目に実行するか、指定します。数値の 1 ～ 5 が入力可能です。	○
曜日選択	タスクを実行する曜日を指定します。複数選択が可能です。	○
ランダム遅延間隔	遅延間隔を指定します。 時間単位を、「秒」「分」「時間」「日」「週」から選択します。	○
設定した時間に実行されなかった場合は即時実行	オンにすると、指定時刻にトリガー起動しなかった場合、タスクが実行できる状態になりしだい直ちにトリガーを起動します。	○
ローカル時刻を使用	オンにすると、対象となるクライアントコンピューターの時刻を使用します。	○

●毎年

毎年繰り返して実行します。

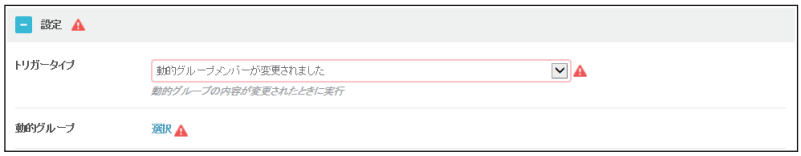


項目名	説明	必須
トリガータイプ	［毎年］を選択します。	○
開始日時	開始日時を指定します。	○
終了条件	終了条件を、次の 3 種類から選択します。 ・「終了なし」 ・「end after」　：終了実行回数を指定します。 ・「終了日」　：具体的な終了日を指定します。	○
次の間隔で繰り返し	タスクを繰り返す間隔を、年単位で指定します。	○
ランダム遅延間隔	遅延間隔を指定します。 時間単位を、「秒」「分」「時間」「日」「週」から選択します。	○
設定した時間に実行されなかった場合は即時実行	オンにすると、指定時刻にトリガー起動しなかった場合、タスクが実行できる状態になりしだい直ちにトリガーを起動します。	○
ローカル時刻を使用	オンにすると、対象となるクライアントコンピューターの時刻を使用します。	○

■動的グループ

●動的グループメンバーが変更されました

動的グループの内容が変更されたときに実行します。



項目名	説明	必須
トリガータイプ	［動的グループメンバーが変更されました］を選択します。	○
動的グループ	［選択］から、既存の動的グループを選択します。	○

●しきい値に従って動的グループサイズが変更されました

動的グループのクライアント数が指定したしきい値よりも、上または下になったときに実行します。

項目名	説明	必須
トリガータイプ	［しきい値に従って動的グループサイズが変更されました］を選択します。	○
動的グループ	［選択］から、既存の動的グループを選択します。	○
グループサイズしきい値	タスク実行のトリガーとなる、選択した動的グループサイズのしきい値を数値指定します。	○
実際のグループサイズ	グループサイズを比較する条件を、「しきい値より高い」または「しきい値より低い」から選択します。	○

●期間中に動的グループサイズが変更されました

動的グループのクライアント数が特定の期間で変更されたときに実行します。

項目名	説明	必須
トリガータイプ	［期間中に動的グループサイズが変更されました］を選択します。	○
動的グループ	［選択］から、既存の動的グループを選択します。	○
期間サイズ（分）	しきい値に到達する期間を、分単位で指定します。	○
しきい値	タスク実行をトリガーするしきい値を指定します。 しきい値の単位を、「クライアント」または「%」から選択します。	○

●比較グループと基準に動的グループのサイズが変更

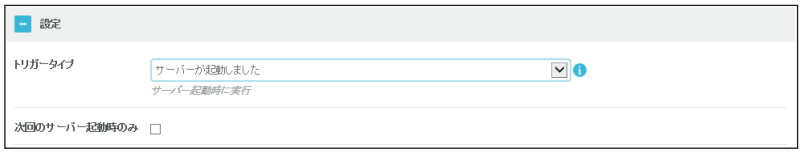
観察された動的グループのクライアント数が比較グループ（静的または動的）に従って変更されたときに実行します。

項目名	説明	必須
トリガータイプ	［比較グループと基準に動的グループのサイズが変更］を選択します。	○
監視対象の動的グループ	［選択］から、このタスクの監視対象となる動的グループを選択します。 比較グループと同一のグループは選択できません。	○
比較グループ（静的または動的）	［選択］から、監視対象の動的グループと比較するグループを選択します。 監視対象の動的グループと同一のグループは選択できません。	○
グループサイズの差	グループサイズを比較する条件を、「しきい値より高い」または「しきい値より低い」から選択します。	○
しきい値	タスク実行のトリガーとなる、しきい値を数値指定します。 しきい値の単位を、「クライアント」または「%」から選択します。	○

■その他

●サーバーが起動しました

サーバー起動時に実行します。



項目名	説明	必須
トリガータイプ	［サーバーが起動しました］を選択します。	○
次回のサーバー起動のみ	次回のサーバー起動のタイミングをトリガーとします。	○

●イベントログトリガー

特定のタイプのイベントがログで発生したときに実行します。

項目名	説明	必須
トリガータイプ	［イベントログトリガー］を選択します。	○
ログタイプ	トリガーの起因となるログに記載されるイベントを、「ファイアウォールの脅威」「ウイルス対策の脅威」「検査」から選択します。	○
フィルタの論理演算子	選択したフィルタ条件に適用される演算子を次の 4 種類より指定します。 ・AND（すべての条件が真であること） ・OR（1 つ以上の条件が真であること） ・NAND（1 つ以上の条件が偽でなければなりません） ・NOR（すべての条件が偽であること）	○
フィルタ条件	［+ フィルタの追加］から、データに適用される特定のフィルタ条件を設定します。 選択した「ログタイプ」に対応して設定できる項目が変わります。	○

項目	ファイアウォールの脅威	ウイルス対策の脅威	検査
あて先アドレス	○		
あて先アドレスバージョン	○		
あて先ポート	○		
プロセス名	○	○	
プロトコル	○		
ユーザー	○	○	○
送信元アドレス	○		
送信元アドレスバージョン	○		
送信ポート	○		
ウイルス名		○	
オブジェクト URI		○	
再起動が必要		○	
処理された脅威		○	
感染			○
駆除済み			○
検査済み			○
検査対象			○

フィルタ条件の論理演算子	選択したフィルタから、演算子を設定できます。 演算子と設定に関しては「・ルールエディタ」を参照してください。	-

・ルールエディタ

動的グループテンプレートやイベントログトリガーの条件を設定するときには、異なる条件でさまざまな演算子を使用できます。

選択したルールやフィルタ条件に使用できる演算子がリストに表示されます。

数値演算子

数値を比較します。

演算子	説明
=（等しい）	完全に一致する数値だけを検索します。
≠（等しくない）	設定した数値を除外して検索します。
>（より大きい）	設定した数値よりも大きい値を検索します。（設定した数値は検索対象から除外されます。）
≧（以上）	設定した数値よりも大きい、または等しい値を検索します。
<（より小さい）	設定した数値よりも小さい値を検索します。（設定した数値は検索対象から除外されます。）
≦（以下）	設定した数値よりも小さい、または等しい値を検索します。

文字列演算子

英数値を比較します。

演算子	説明
=（等しい）	完全に一致する文字列だけを検索します。
≠（等しくない）	設定した値を除外した文字列を検索します。
含む	設定した値が含まれる文字列を検索します。
前方一致	設定した値が先頭の文字列と一致する文字列を検索します。 例）「Microso Visual C++2010　x86 Redistributble - 10.0.30319」を検索する場合は、「Micros」、「Micr」、「Microsof」などを設定します。
後方一致	設定した値が末尾の文字列と一致する文字列を検索します。 例）「Microso Visual C++2010　x86 Redistributble - 10.0.30319」を検索する場合は、「319」、「0.30319」などを設定します。
マスク	設定した値と一致する文字列を検索します。ワイルドカード（「*」※1、「?」※2）を含めて値を設定できます。
正規表現	Perl 構文を使用して値を設定できます。設定した値と一致する文字列を検索します。
in	複数の値を設定し、まとめて検索します。設定した値と一致する文字列を検索します。 例）「Microsoft Windows」を検索する場合は、正確に「Microsoft Windows」と設定します。
in（文字列マスク）	複数の値を設定し、まとめて検索します。ワイルドカード（「*」※1、「?」※2）を含めて値を設定できます。

※1 「*」（アスタリスク）とは、任意の数の文字と一致します（0 以上）。

※2 「?」（クエスチョン）とは、1 文字だけ一致します。

ワイルドカードの入力例

- 「a*」は「a」、「aa」、「ax」、「abcde」と一致します。
- 「a?」は「aa」、「ab」、「ac」と一致しますが、「a」、「aaa」には一致しません。
- 「a??」は「aaa」、「aab」、「axy」と一致しますが、「a」、「aa」、「aaaa」には一致しません。
- 「?a* 」は「aa」、「ax」、「abcde」と一致しますが、「a」には一致しません。
- 「*a*」は「a」、「xa」、「ax」、「xax」、「dynamic」、「abba」と一致します。
- 「?*」は空白以外のすべてと一致します。

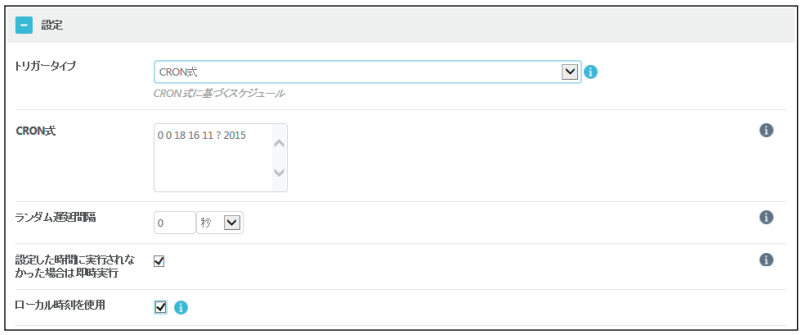
ブール値演算子

決められた値を比較します。

演算子	説明
=（等しい）	条件に決められた値のリンクが表示されます。選択した値と一致する文字列を検索します。 ※条件に表示されるリンクをクリックすると、値が切り替わるか、または「値を選択」コンテキストメニューが表示されます。
≠（等しくない）	条件に決められた値のリンクが表示されます。選択した値を除外した文字列を検索します。 ※条件に表示されるリンクをクリックすると、値が切り替わるか、または「値を選択」コンテキストメニューが表示されます。

● CRON 式

CRON 式に基づく予定で実行します。
CRON 式は、スケジュールの個別の値を表す 7 個の下位式（フィールド）から構成される文字列です。
「CRON 式」のテキストボックスに、構文を入力します。任意の許可された値を様々な組み合わせで使用できます。構文はスペースで区切ります。



項目名	説明	必須
トリガータイプ	［CRON 式］を選択します。	○
CRON 式	タスク実行の予定を CRON 式で直接記述します。 基本的な CRON 式の基本的な記述については、参考：CRON 式の記述形式を参照してください。	○
ランダム遅延間隔	遅延間隔を指定します。 時間単位を、「秒」「分」「時間」「日」「週」から選択します。	○
設定した時間に実行されなかった場合は即時実行	オンにすると、指定時刻にトリガー起動しなかった場合、タスクが実行できる状態になりしだい直ちにトリガーを起動します。	○
ローカル時刻を使用	オンにすると、対象となるクライアントコンピューターの時刻を使用します。	○

参考：CRON 式の記述形式

名前	必要	値	許可された特殊文字
秒	必須	0-59	R , - * /
分	必須	0-59	R , - * /
時間	必須	0-23	R , - * /
月の日付	必須	1-31	R , - * / L W ?
月	必須	0-11 または JAN-DEC	R , - * /
曜日	必須	1-7 または SUN-SAT	, - ? / L #
年	省略可能	空または 1970-2099	R , - * /

ワンポイント

CRON 式でランダムな値を指定する場合に、R を使用できます。
例「R R/20***?*」の場合は、ランダムな 20 分ごと（3、23、43 または 17、37、57 など）にランダムな秒（0 ～ 60）でタスクが実行されることを意味します。

■ CRON 式で使用できる特殊文字

文字種	内容
カンマ（,）	カンマはリストの項目を区切るために使用されます。たとえば、6 番目のフィールドで MON,WED,FRI（曜日）を使用すると、月曜日、水曜日、金曜日を意味します。
ハイフン（-）	範囲を定義します。たとえば、2012-2020 は 2012 年から 2020 年までの毎年を示します。
ワイルドカード（*）	フィールド内のすべての可能な値を選択するために使用されます。たとえば、分フィールドで * を使用すると毎分を意味します。ワイルドカードは曜日フィールドでは使用できません。
疑問符（?）	特定の日を選択するときには、日または曜日を指定できます。両方は指定できません。日を指定する場合は、曜日に ? を使用する必要があります。逆も同様です。たとえば、特定の日（10 日など）にトリガーを実行し、実行される曜日を考慮しない場合は、日フィールドに 10、曜日フィールドに ? を入力します。
ハッシュ（#）	「N 番目」の日を指定するために使用されます。たとえば、曜日フィールドの値 4#3 は、第 3 水曜日を意味します（第 4 日目 = 木曜日、#3 = 月の第 3 木曜日）。#5 を指定し、月に第 5 の曜日がない場合は、トリガーはその月に実行されません。
スラッシュ（/）	範囲の増分値を説明します。たとえば、2 番目のフィールド（分）の 3-59/15 は、1 時間のうちの 3 分目とその後 15 分間隔を意味します。
最後（L）	曜日フィールドで使用すると、特定の月の最後の金曜日（5L）などのコンストラクトを指定できます。日フィールドでは、月の最後の日を指定します。たとえば、1 月 31 日、2 月 28 日（閏年を除く）です。
平日（W）※ 1	W 文字は日フィールドで使用できます。この文字は特定の日に最も近い平日（月曜日から金曜日）を指定するために使用されます。たとえば、15W を日フィールドの値として指定すると、15 日に最も近い平日になります。15 日が土曜日の場合、トリガーは 14 日の金曜日に実行されます。15 日が日曜日の場合、トリガーは 16 日の月曜日に実行されます。ただし、1W を日の値に指定し、1 日が土曜日の場合、トリガーは 3 日の月曜日に実行されます。月をまたいで実行されることはありません。
ランダム（R）※ 2	R は特殊な ERA CRON 式文字であり、ランダム化された時間を指定できます。たとえば、R 0 0 * * ? * は毎日 00:00 に実行されますが、秒はランダムです（0-59）。

※ 1　L および W 文字は、LW として日フィールドで組み合わせることもできます。これは月の最後の平日を意味します。

※ 2　すべての ERA エージェントが同時に ERA サーバーに接続しないように、ランダム化された時間を使用することをお勧めします。

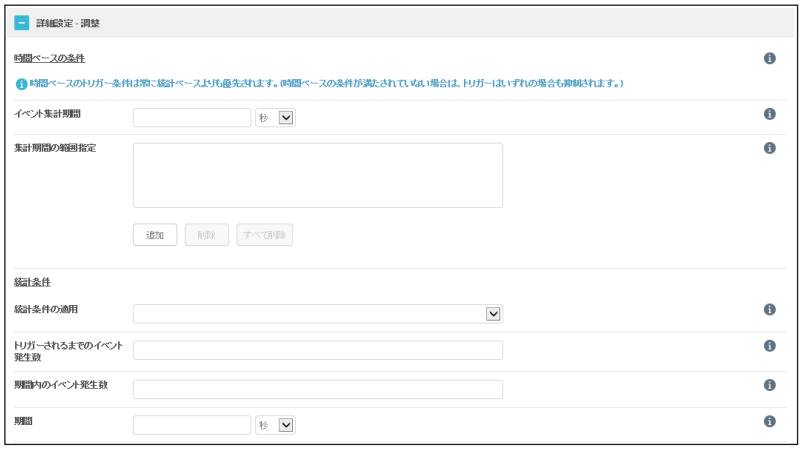
6.7.4.2 詳細設定 – 調整

「詳細設定 –調整」画面では、トリガーを実行するために必要なチェック（トリガーヒット）数や、時間範囲に関する条件項目を設定します。条件を組み合わせて、トリガー実行の細かい調整を行います。
条件には、2 つの種類があります。

時間ベースの条件項目	構成された条件のすべてが満たされる必要があります。
統計ベースの条件項目	AND 論理演算子または OR 論理演算子と組み合わせることができます。

条件は " イベント発生時間に依存する " という特徴があるため、統計ベースの条件項目よりも、時間ベースの条件項目が優先されます。
また、時間ベースの条件がすべて満たされない場合、トリガーは実行されません。

●時間ベースの条件 と 統計条件



種別	項目名	説明	必須
時間ベースの条件	イベント集計期間	指定した時間ごとにトリガーを実行します。 「秒」「分」「時間」「日」「週」から選択します。 例）10 秒を指定した場合、10 秒の間に 10 回処理が実行されても、1 回だけトリガー実行される事となります。	
	集計期間の範囲指定	トリガー実行が有効となる時間の条件を指定します。 ［追加］ボタンから、範囲指定の設定を行います。 複数の時間範囲をリストに追加できます。 例）範囲期間：1 分、繰り返し：毎日、開始日時：2015 年 1 月 1 日 21:00、スケジュール：1 日毎の場合、2015 年 1 月 1 日以降毎日 21:00 から 21:01 の 1 分間の間だけトリガー実行されます。	

種別	項目名	説明	必須
統計ベースの条件	統計条件の適用	統計条件では以下の論理演算子と組み合わせることができます。 ・「すべての統計ルールが適用されます」（AND） ・「1 つ以上の統計ルールが満たされている」（OR）	
	トリガーされるまでのイベント発生数	何回目のイベント発生時にトリガー実行するかを指定します。 例）100 を指定した場合 100 個の脅威が検出されても 100 個の脅威を含む 1 つの通知がされます。200 個の脅威が検出された場合、最後の 100 個だけが通知に含まれます。	
	期間内のイベント発生数	「期間」で指定した時間範囲内に何回イベント発生したらトリガー実行するかを指定します。 例）10 を指定した場合 指定した時間範囲内に、対象のイベントが 10 回発生すると、タスクの実行を許可します。	
	期間	「期間内のイベント発生数」の条件となる期間を指定します。「秒」「分」「時間」「日」「週」から選択します。	

●イベントログ条件

トリガータイプの［イベントログトリガー］を選択した場合は、次の項目が追加表示されます。

種別	項目名	説明	必須
イベントログ条件	シンボル	トリガーとして指定した「ログタイプ」に関して詳細な条件づけをする場合に指定します。 例）・ログタイプ「検査」の場合、「ユーザー」「感染」「検査対象」など ・ログタイプ「ウイルス対策の脅威」の場合、「ウイルス名」「処理された脅威」など	
	シンボルのあるイベント数	何回イベントが発生したらトリガー実行するかを指定します。 例）10 を指定した場合 シンボルで指定したアプリケーションが、10 回インストール確認されるたびにトリガー実行します。	
	イベント数のときに適用	イベント数のカウントの方法を次の 2 種類より選択します。 ・「行で受信」 連続でカウント（トリガー実行が考慮されない） ・「前回のトリガー実行以降に受信」 前回のトリガー実行からカウント（トリガーが実行されると、値は 0 にリセットされます）。	

ワンポイント

調整項目の設定内容によっては、トリガーの実行ができない場合があります。
また、設定した条件項目のいずれかが満たされた場合、すべてのカウント情報がリセットされます（カウントは 0 から開始します）。
これは、時間ベースおよび統計ベースの条件の両方に適用されます。
さらに、カウント側の状態情報は永続的ではなく、次のイベントでリセットされます。
・ERA エージェントまたは ERA サーバーの再起動
・トリガーの変更

■複数の制御方法例

時間ベースの条件、統計ベースの条件、共に複数のパターンを例とします。

●統計

統計トリガーは、次のパラメータを任意に組み合わせた結果に基づき実行されます。

トリガーされるまでのイベント発生数 ※ S1 とします。	トリガーとなるイベントが N 回発生するたびに実行（N= 整数） これは一連の最後のイベントの後に開始します（開始時点から N 回のイベントまでは実行しません）。
期間内のイベント発生数 ※ S2 とします。	イベントの合計回数が X 回以内である場合にトリガーが実行されます。 トリガーが実行されると、バッファがリセットされます。
シンボルのあるイベント数 ※ S3 とします。	「シンボル」として指定したイベントが、N 回連続して発生するとトリガーが実行されます。バッファ内に既にイベントがある場合は、バッファがリセットされます。 バッファは「浮動ウインドウ」モードで、FIFO キューです。新しい「シンボル」はバッファ内のすべての「シンボル」と比較されます。

※上記パラメータは、「統計条件の適用」から AND 演算子または OR 演算子と組み合わせることができます。

！重　要

見つからない値である、n/a が返された場合は、一意でないと見なされるため、前回のトリガー実行以降のバッファがリセットされます。

●時間ベース

次の条件が設定されている場合は、すべてが同時に満たされる必要があります。

集計期間の範囲指定 ※ T1 とします。	X 時間範囲内でトリガーを実行します。 範囲は限界時間の繰り返しとして指定されます。（13:00 ～ 14:00 の間または 17:00 ～ 23:30 の間など）
イベント集計期間 ※ T2 とします。	指定した X 時間ごとにトリガーを実行します。

●追加プロパティ

トリガーを実行しないイベントもあります。
次は、トリガーとならないイベントに対して実行されるアクションです。

- 複数のイベントがスキップされた場合、最後の N イベントが 1 つにグループ化されます。（抑制されたチェックのデータを格納）（N <= 100）
- N = = 0 の場合、最後のイベントだけが処理されます。（N は履歴の長さを表し、最後のイベントは常に処理する）
- トリガーにならないイベントがすべてマージされます。（最後のチェックを N 履歴チェックとマージ）

S1：発生条件（3 チェックごとにトリガー実行）

日時	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13	14	15
チェック	×	×	×	×	×	×	×		×	×		×	×		×		×
S1			1			1						1					1

S2：時間内の発生条件（チェックが 4 秒以内に発生する場合にトリガー実行）

日時	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13
チェック	×		×	×	×	×			×		×		×	×	×
S2				1										1	

S3：一意の記号値の条件（3 つの一意の値がトリガー実行を考慮しない場合にトリガー実行）

日時	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13
値	-	B	B	C	D	G	H		J	K	n/a	L	M	除外しない	除外しない
S3					1									1	

S3：一意の記号値の条件（3 つの一意の値がトリガー実行からカウントする場合にトリガー実行）

日時	00	01	02	03	04	05	06	07	トリガーが修正される	08	09	10	11	12	13	14
値	-	B	B	C	D	G	H	I		J	K	n/a	L	M	除外しない	除外しない
S3				1			1						1			

T1: 特定の時間範囲でチェックを許可（毎日 8:10 から 60 秒の間にチェックされた場合にトリガー実行）

日時	8:09:50	8:09:59	8:10:00	8:10:01	トリガーが修正される	8:10:59	8:11:00	8:11:01
チェック	×	×	×	×		×	×	×
T1			1	1		1		

この条件には状態がありません。このため、トリガー修正は結果に影響しません。

T2：時間間隔で 1 つのチェックを許可（最大 5 秒に 1 回トリガー実行）

日時	00	01	02	03	04	05	06	トリガーが修正される	07	08	09	10	11	12	13
チェック	×		×	×	×	×			×		×		×	×	×
T2	1					1			1					1	

S1+S2 の組み合わせ

• S1:5 チェックごと

• S2:4 秒以内に 3 チェック

日時	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
チェック	×	×	×	×	×		×	×	×			×		×	×		
S1															1		
S2			1				1								1		
結果			**1**				**1**								**1**		

結果は S1（論理または）S2 と列挙されます。

S1+T1 組み合わせ

• S1:3 チェックごとに許可

• T1:8:08 から始まる毎日を許可、期間は 60 秒

日時	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
チェック	×	×	×	×	×	×	×	×	×	×
S1			1			1			1	
T1					1	1	1	1	1	
結果						1			1	

結果は S1（論理および）T1 と列挙されます。

S2+T1 組み合わせ

• S2:10 秒以内に 3 チェック

• T1:8:08 から始まる毎日を許可、期間は 60 秒

日時	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
チェック	×	×	×	×	×	×	×	×	×	×
S2			1	1			1			1
T1					1	1	1	1	1	
結果							1			

結果は S2（論理および）T1 と列挙されます。

S2 の状態は、グローバル結果が 1 の場合にだけリセットされます。

S2+T2 組み合わせ

• S2:10 秒以内に 3 チェック

• T2: 最大 20 秒に 1 回許可

日時	00	01	02	03	04	05	06	07	…	16	17	18	19	20	21	22	23	24
チェック	×	×	×	×	×	×	×	×		×	×	×	×	×	×	×	×	×
S2	1	1	1			1	1	1				1	1	1	1	1		
T2			1													1		
結果			**1**													**1**		

結果は S2（論理および）T2 と列挙されます。

S2 の状態は、グローバル結果が 1 の場合にだけリセットされます。

■トリガーが頻繁に起動する

通知の頻度を下げる場合、次の推奨事項を検討してください。

1 つのイベントではなく複数のイベントがある場合にだけユーザーに対応させる場合	調整の統計条件 S1 を参照してください。
大量のイベントが発生した場合にだけトリガーを起動する	調整の統計条件 S2 を参照してください。
望ましくない値のイベントを無視する場合	調整の統計条件 S3 を参照してください。
関連する時間（業務時間など）外のイベントを無視する場合	調整の時間ベースの T1 条件を参照してください。
トリガー実行間隔を最小値に設定する	調整の時間ベースの T2 条件を参照してください。

条件を合わせて、より複雑な調整シナリオに対応することも可能です。

■トリガー感度の管理

タスクのトリガーが頻繁に起こるイベントの場合、調整の設定を使用しタスクの実行を制限します。

特定の状況の下では、調整によってトリガーの実行ができない場合があります。

設定済みの条件のいずれかが満たされた場合、すべての監視側の蓄積された情報がリセットされ、カウントは 0 から開始します。また、次のイベントでも情報はリセットされます。

- ERA エージェントまたは ERA サーバーの再起動
- トリガーの変更

上記リセットは、時間ベースおよび統計ベースの条件、共に適用されます。

! 重　要

複数の統計条件を使用すると不必要に複雑となり、トリガー結果が変わる可能性があります。
時間ベースの条件は統計条件よりも優先されるため、統計条件を 1 つだけ使用し、複数の時間ベース条件の使用を推奨しています。

6.8 通知

通知はネットワーク上の全体的な状況を追跡するために使用します。設定に基づいて新しいイベントが発生したときには、定義済みの方法（SNMP トラップサービスまたは電子メールメッセージ）で通知され、それに応じて対応できます。

6.8.1 通知画面の構成

「通知」画面の構成について説明します。

1	**通知リスト**	すべての通知のリストが表示されます。	
		通知名	通知の名前が表示されます。
		通知説明	通知の説明が表示されます。
2	**新しい通知**	新しく通知を作成します。「新しい通知」画面が表示されます。 画面の詳細は、「6.8.2 新しい通知の作成」を参照してください。	
3	**通知の編集**	選択している通知を編集します。「通知の編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいテンプレートとして保存することができます。 画面の詳細は、「6.8.2 新しい通知の作成」を参照してください。	
4	**削除**	選択している通知（複数選択可）を完全に削除します。	
5	**複製**	選択している通知の内容をコピーした状態で「新しい通知」画面が表示されます。画面の詳細は、「6.8.2 新しい通知の作成」を参照してください。	
6	**アクセスグループ**	「アクセスグループ」では、ユーザーが静的グループを選択し、属するグループに応じて、表示されるオブジェクトをフィルタリングできます。［選択］をクリックすると、フィルタリングするグループを選択できます。また、🗑をクリックすると、フィルタリングを解除できます。	

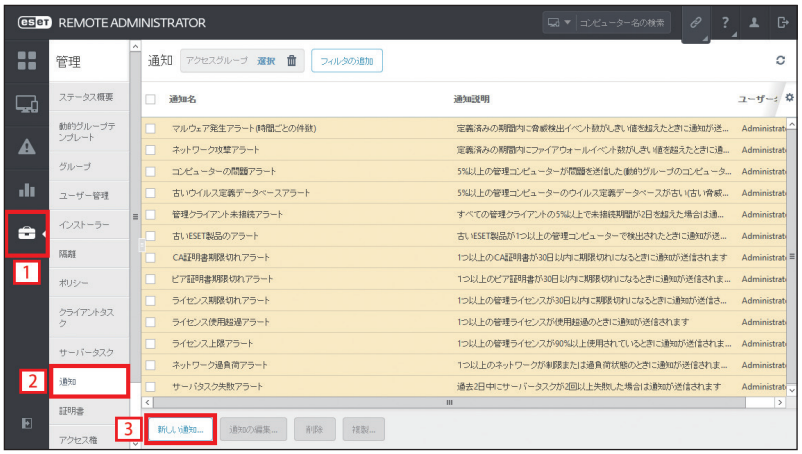
7	「通知」コンテキストメニュー	通知リストから選択している通知に使用できるメニューが表示されます。		
			編集	選択している通知を編集します。「通知の編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しいテンプレートとして保存することができます。 画面の詳細は、「6.8.2　新しい通知の作成」を参照してください。
			複製	選択している通知の内容をコピーした状態で「新しい通知」画面が表示されます。 画面の詳細は、「6.8.2　新しい通知の作成」を参照してください。
			削除	選択している通知を完全に削除します。
			アクセスグループ	選択した通知を別のグループに移動します。［アクセスグループ］>［移動］とクリックすると「項目を選択してください」画面が表示され、移動先のグループを選択できます。

6.8.2　新しい通知の作成

通知を新しく作成する方法を説明します。

操作手順

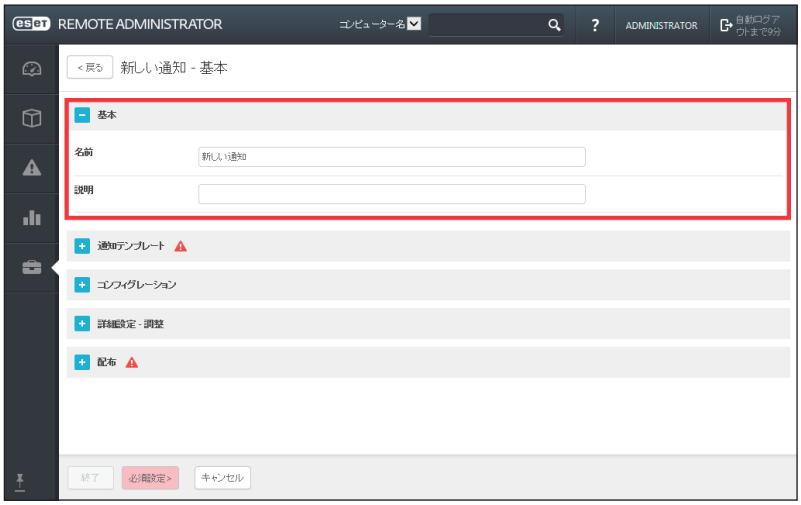
1. ［管理］メニューをクリックします。
2. ［通知］サブメニューをクリックします。
3. ［新しい通知］ボタンをクリックします。



「新しい通知」画面が表示されます。

続く

4 「基本」の各項目を入力します。

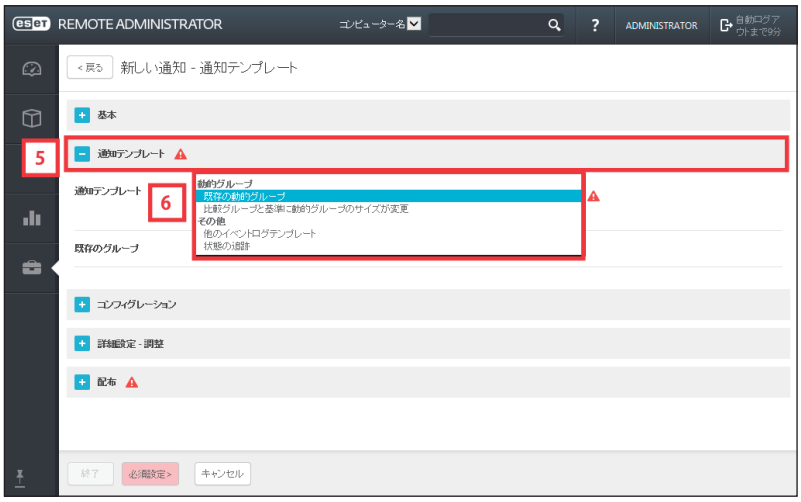


■基本

項目名	説明	必須
名前	作成する通知の名前を入力します。画面には、ここで設定した名前が表示されます。	○
説明	作成する通知の説明を入力します。	-

5 [通知テンプレート] をクリックします。

6 「通知テンプレート」を選択します。



ワンポイント

選択した通知テンプレートに合わせて、以降に表示される項目が変わります。

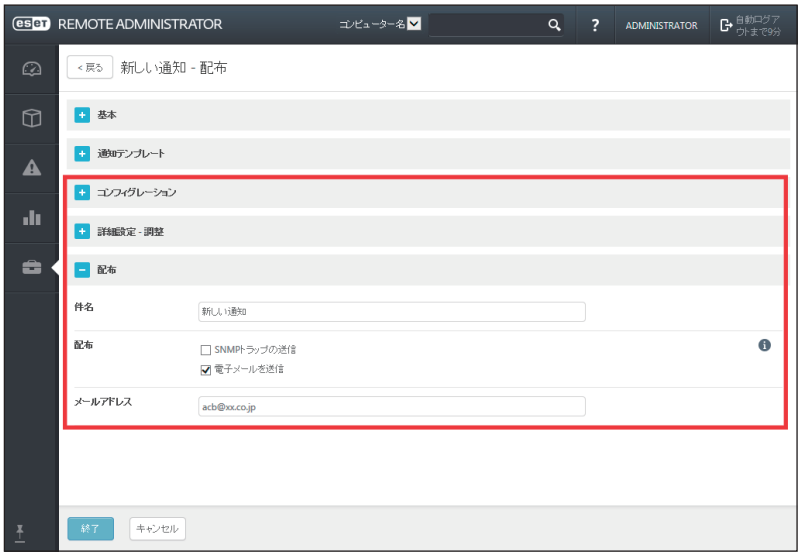
続く

■通知テンプレート

項目名	説明		必須
通知テンプレート	通知を作成するテンプレートを選択します。選択したテンプレートに合わせて、以降に表示される項目が変わります。		○
	既存の動的グループ	既存の動的グループを使用して新しく通知を作成します。	-
		既存のグループ	リストから動的グループを選択します。	○
	比較グループと基準に動的グループのサイズが変更	基準とする動的グループのクライアント数が、比較グループ（静的または動的グループ）に従って変更された場合に通知が実行されます。	-
		監視対象の動的グループ	動的グループを選択します。「比較グループ」とは異なる動的グループを指定します。	○
		比較グループ（静的または動的）	比較するグループを選択します。「監視対象の動的グループ」とは異なるグループを指定します。	○
		グループサイズの差	グループのサイズが比較される条件を選択します。	○
		しきい値	絶対数を入力します。	-
通知テンプレート	他のイベントログテンプレート	イベントログに基づいて通知が実行されます。		-
		ログタイプ	通知の基になるログタイプを選択します。	○
		フィルタの論理演算子	「フィルタ条件」に適用する論理演算子を選択します。	-
		フィルタ条件	［+ フィルタの追加］から、データに適用される特定のフィルタ条件を設定します。「ログタイプ」で選択した内容に合わせたリストが表示されます。使用可能なデータに適用される条件を選択します。	-
			フィルタ条件の論理演算子	選択したフィルタから論理演算子を選択します。 演算子と設定に関しては「ルールエディタ」を参照してください。	
	状態の追跡	ユーザーが定義したフィルタを使用してオブジェクト状態の変更を通知します。		-
		状態の追跡	状態を追跡する対象を選択します。	○
		フィルタ条件	「状態の追跡」で選択した内容に合わせたリストが表示されます。使用可能なデータに適用される条件を選択します。	○

続く

7 以降の各項目を入力します。



■コンフィグレーション

「通知テンプレート」セクションの「通知テンプレート」で選択したテンプレートに合わせて、表示される項目が変わります。

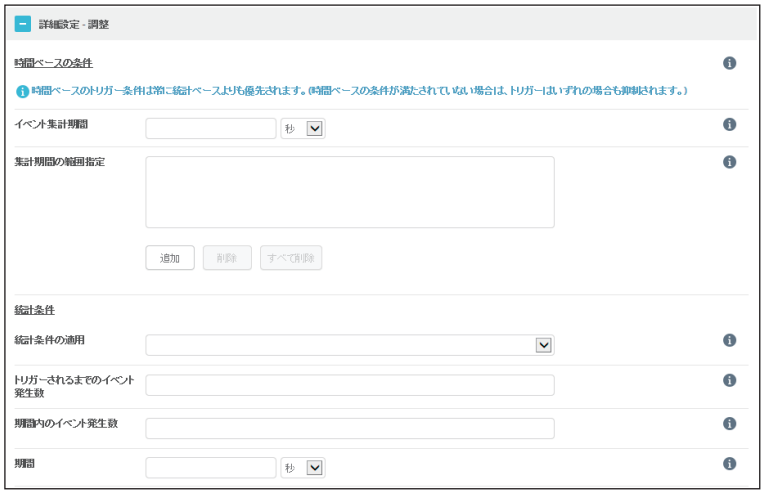
●［既存の動的グループ］を選択した場合

●その他の通知テンプレートを選択した場合

続く

項目名	説明	必須
動的グループコンテンツが変更されるたびに通知	「通知テンプレート」で［既存の動的グループ］を選択した場合に表示されます。 オンにすると、動的グループのメンバーが追加、削除または変更されると通知します。	-
通知期間	「通知テンプレート」で［既存の動的グループ］を選択した場合に表示されます。 オンにすると、新しい状態と比較するための期間を入力します。例えば、7日前のクライアント数が 10 で、しきい値が 20 クライアントに設定されていた場合、クライアント数が 30 になると通知されます。	-
しきい値	「通知テンプレート」で［既存の動的グループ］を選択した場合に表示されます。 通知をトリガーするために必要なクライアント数（0 以上の値）、またはパーセント（正または負の値）を入力します。	○
生成されたメッセージ	設定内容に従い、自動的に表示されます。	-
メッセージ	定義済みメッセージを除き、カスタムメッセージを追加できます（上記の定義済みメッセージの最後に表示されます）。これは任意ですが、通知と概要のフィルタリング効果を高めるために設定することを推奨します。	-

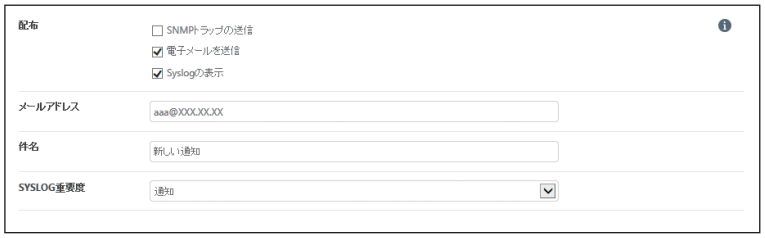
■詳細設定 – 調整



項目の説明は、6.7.4.2 詳細設定 – 調整を参照してください。

続く

■配布



項目名	説明		必須
件名	通知メッセージの件名を入力します。これは任意ですが、フィルタリングを強化する目的や通知メッセージを並べ替えるルールを作成する場合は、設定することを推奨します。		-
配布	通知メッセージの配布方法を選択します。		○
	SNMP トラップの送信	オンにすると、SNMP トラップを送信します。 簡易ネットワーク管理プロトコル（SNMP）トラップは未承認の SNMP メッセージを使用して非同期ネットワーク通知を送信します。 詳細は、「6.8.3　SNMP トラップサービスの構成方法」を参照してください。	-
	電子メールを送信	「メールアドレス」で入力したアドレスに、電子メールメッセージを送信します。	-
	Syslog の表示	オンにすると、通知とイベントメッセージを［サーバーの設定］で指定した Syslog サーバーに送信します。（ESET Remote Administrator 6.3 以降で利用可能）	-
メールアドレス	「配布」で［電子メールを送信］にチェックを入れた場合に表示されます。 通知メッセージを受信するメールアドレスを入力します。複数のアドレスを入力する場合は、「,」（カンマ） で区切ります。		○
SYSLOG 重要度	「配布」で「Syslog の表示」にチェックを入れた場合に表示されます。 送信する Syslog メッセージの重要度をドロップダウンリストから選択します。		○

8 ［終了］ボタンをクリックします。

「通知」画面の通知リストに、作成した通知が表示されます。

6.8.3 SNMP トラップサービスの構成方法

ERA サーバーで SNMP トラップの送信を行うためには、SNMP トラップサービスを構成する必要があります。

■前提条件

- ERA サーバーがインストールされているコンピューターと、SNMP トラップを受信するソフトウェアがインストールされる予定のコンピューターには、簡易ネットワーク管理プロトコルサービスをインストールする必要があります。
- 両方のコンピューターは、同じサブネットにある必要があります。
- SNMP サービスを、ERA サーバーコンピューターで構成する必要があります。

■ SNMP サービス構成（Windows）

ERA サーバーがインストールされている Windows サーバーで、以下の操作手順に従い SNMP サービスを構成します。

操作手順

1. 【Windows】キー＋【R】キーを押し、「ファイル名を指定して実行」画面を開きます。
2. 「名前」に「Services.msc」を入力し、［OK］ボタンをクリックします。

   「サービス」画面が表示されます。
3. ［SNMP Service］をダブルクリックします。

   「SNMP のプロパティ」画面が表示されます。
4. 「トラップ」タブをクリックし、「コミュニティ名」に「public」と入力します。
5. ［一覧に追加］ボタンをクリックします。
6. ［追加］ボタンをクリックします。

   「SNMP サービスの構成」画面が表示されます。
7. トラップの送信先に、SNMP トラップを受信するソフトウェアがインストールされているコンピューターのホスト名、IP または IPX アドレスを入力し、［OK］ボタンをクリックします。

   「SNMP のプロパティ」画面に戻ります。
8. 「セキュリティ」タブをクリックし、［追加］ボタンをクリックします。

   「SNMP サービスの構成」画面が表示されます。
9. 「コミュニティ名」に「public」と入力し、［追加］ボタンをクリックします。
10. ［すべてのホストから SNMP パケットを受け付ける］を選択し、［OK］ボタンをクリックします。

■ SNMP サービス構成（Linux）

ERA サーバーがインストールされている Linux サーバーで、以下の操作手順に従い SNMP サービスを構成します。以下の手順は、Linux サーバーで SNMP トラップを受信する場合の例です。

操作手順

1. 次のコマンドを実行して、snmpd パッケージをインストールします。

   「yum install net-snmp」（RHEL、CentOS）
   「yum install net-snmp-utils」

2. /etc/default/snmpd ファイルを開き、次の属性を編集します。

   ```
   #SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
   ```
   # を追加すると、この行が完全に無効になります。
   ```
   SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/
         snmp/snmpd.conf'
   ```
   この行をファイルに追加します。
   ```
   TRAPDRUN=yes
   ```
   trapdrun 属性を yes に変更します。

3. 元の snmpd.conf ファイルのバックアップを作成します。

   ```
   mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
   ```

4. 新しい snmpd.conf ファイルを作成し、次の行を追加します。

   ```
   rocommunity public
   syslocation "Testing ERA6"
   syscontact admin@ERA6.com
   ```

5. /etc/snmp/snmptrapd.conf ファイルを開き、次の行をファイルの最後に追加します。

   ```
   authCommunity log,execute,net public
   ```

6. 次のコマンドを入力して、SNMP マネージャサービスと受信トラップのロギングを開始します。

   ```
   /etc/init.d/snmpd restart
   ```
   または
   ```
   service snmpd restart
   ```

7. 次のコマンドを実行し、SNMP マネージャーが正常に動作しているかどうかを確認します。

   ※成功するとシステムのアップタイムなどの情報が取得でます。
   ```
   snmpwalk -v 2c -c public [SNMP マネージャーの IP アドレス] system
   ```

8. 次のコマンドを実行し、トラップが送信されることを確認します。

   ※成功すると SNMP マネージャーのログ（/var/log/messages など）に trap 受信のログが出力されます。
   ```
   snmptrap -v 2c -c [SNMP マネージャーの IP アドレス] '' .1.3.6.1.6.3.1.1.5.3
   ```

6.9 証明書

ESET Remote Administrator のコンポーネント間の暗号化された通信を認証するために、証明書が使用されます。すべてのコンポーネントが正常に通信できることを保証するには、証明書が有効で、同じ認証局によって署名されている必要があります。
次の手順に沿って、証明書を発行します。

STEP1	認証局を作成する	「6.9.2.2 新しい認証局の作成」参照
STEP2	ESET 製品別に証明書を作成する	「6.9.1.2 新しい証明書の作成」参照

6.9.1 ピア証明書

証明書は、ERA エージェント、ERA プロキシ、ERA サーバー、Mobile Device Connector で使用されます。製品別に用意されていますので、使用する製品に合わせて作成する必要があります。

! 重 要

証明書を作成する前に、認証局を作成してください。

6.9.1.1 ピア証明書画面の構成

「証明書」画面の構成について説明します。

1	**証明書リスト**	すべての証明書のリストが表示されます。		
2	**[アクション]ボタンおよび「証明書」コンテキストメニュー**	証明書リストから選択した証明書に使用できるアクションが表示されます。		
			新規作成	新しい証明書を作成します。「証明書の作成」画面が表示されます。 画面の詳細は、「6.9.1.2 新しい証明書の作成」を参照してください。
			証明書の使用	選択した ERA 証明書を使用したクライアントのリストを表示します。
			編集	選択している証明書を編集します。「証明書の編集」画面が表示されます。 編集できる項目は「説明」のみです。 画面の詳細は、「6.9.1.2 新しい証明書の作成」を参照してください。
			エクスポート	選択している証明書を PFX ファイル（.pfx）にエクスポートします。このファイルは、コンピューターにローカルでエージェントをインストールする場合や、Mobile Device Connector をインストールする場合に使用します。 詳細は、「6.9.1.3 ピア証明書のエクスポート」の「■証明書のエクスポート」を参照してください。
			Base64 としてエクスポート	選択している証明書をテキストファイル（.txt）にエクスポートします。 詳細は、「6.9.1.3 ピア証明書のエクスポート」の「■証明書を Base64 としてエクスポート」を参照してください。
			取り消し	選択している証明書を無効にします。無効な証明書は、ESET Remote Administrator によって許可されません。 取り消した証明書は、ピア証明書リストから削除され、取り消された証明書リストに移動されます。[取り消しを表示]ボタンから確認できます。
			アクセスグループ	選択した証明書または認証局を別のグループに移動します。[アクション]ボタン > [アクセスグループ]またはコンテキストメニューの[アクセスグループ] > [移動]とクリックすると、「項目を選択してください」画面が表示され、移動先のグループを選択できます。
3	**新規作成**	新しい証明書を作成します。「証明書の作成」画面が表示されます。 画面の詳細は、「6.9.1.2 新しい証明書の作成」を参照してください。		
4	**編集**	選択している証明書を編集します。「証明書の編集」画面が表示されます。 画面の詳細は、「6.9.1.2 新しい証明書の作成」を参照してください。		

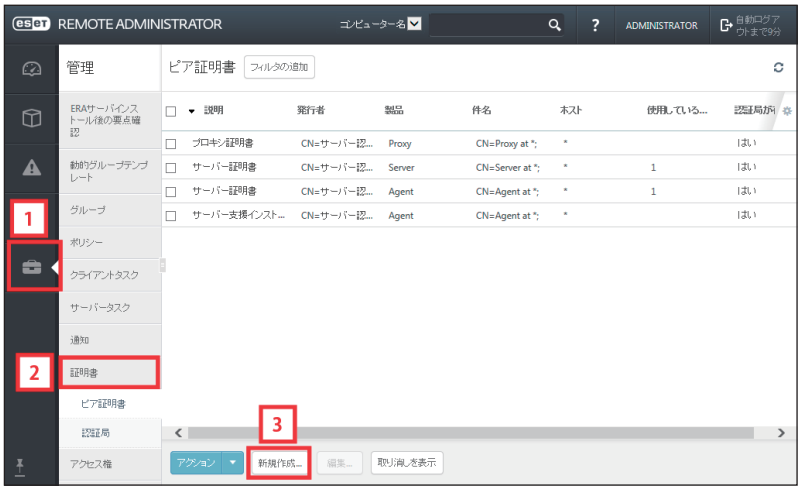
5	取り消しを表示	取り消されたすべての証明書が表示されます。
6	アクセスグループ	「アクセスグループ」では、ユーザーが静的グループを選択し、属するグループに応じて、表示されるオブジェクトをフィルタリングできます。［選択］をクリックすると、フィルタリングするグループを選択できます。また、🗑をクリックすると、フィルタリングを解除できます。

6.9.1.2 新しい証明書の作成

証明書を新しく作成する方法を説明します。

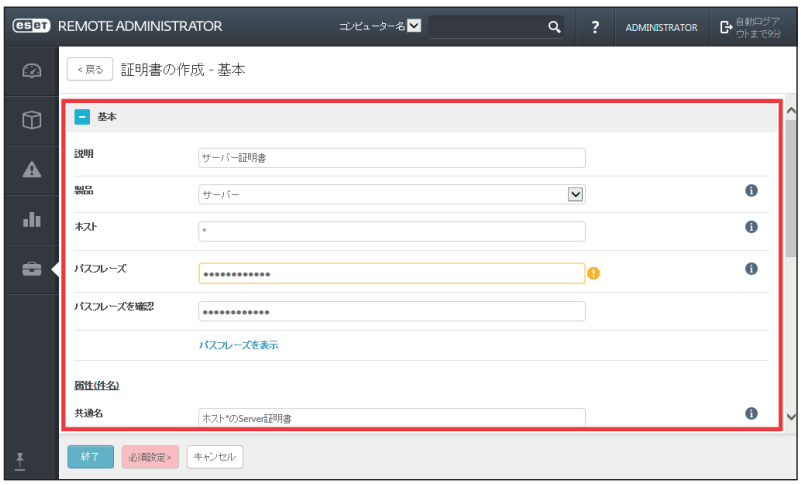
操作手順

1. ［管理］メニューをクリックします。
2. ［証明書］サブメニューをクリックします。
3. ［新規作成］ボタンをクリックします。



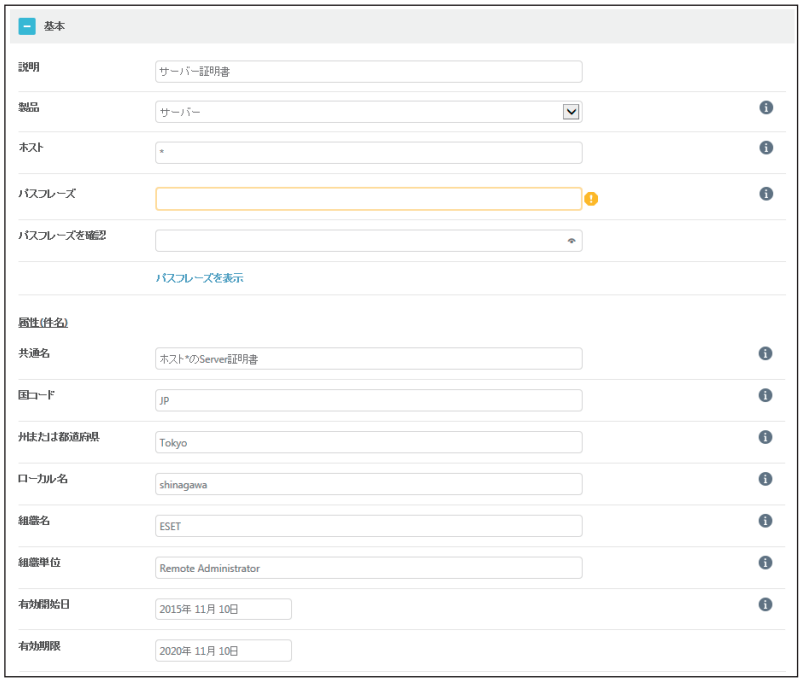
「証明書の作成」画面が表示されます。

4. 各項目を入力します。



続く

■基本



項目名	説明		必須
説明	証明書の説明を入力します。		-
製品	証明書を発行する製品を選択します。		○
	エージェント	ERA エージェントをインストールする際に必要な証明書を発行します。	-
	プロキシ	ERA プロキシをインストールする際に必要な証明書を発行します。	-
	サーバー	ERA サーバーをインストールする際に必要な証明書を発行します。	-
	モバイルデバイスコネクター	Mobile Device Connector をインストールする際に必要な証明書を発行します。	-
	仮想エージェントホスト	仮想エージェントホストをインストールする際に必要な証明書を発行します。 ※日本ではこの証明書は使用しません。	-
ホスト	この証明書を使用できるホストを DNS 名または IP アドレスを入力し定義します。複数入力する場合はスペース、「,」（カンマ）、「;」（セミコロン）で区切ります。「＊」（アスタリスク）は、特定の DNS 名または IP アドレスに関連付けられていない証明書で使用できます。なお、Mobile Device Connector の証明書の場合、「＊」（アスタリスク）を使用すると、iOS でのプロファイルインストールに失敗することがあります。		○
パスフレーズ	証明書の秘密鍵の暗号化用パスワードを入力します。パスワードを設定した場合は、インストール中にパスワードの入力が必要になります。パスワードの設定は任意です。パスワードは、12 文字以上で、小文字、大文字、数字、句読点、その他の文字を 3 種類以上組み合わせて使用する必要があります。		-

続く

項目名	説明	必須
パスフレーズを確認	確認のため、「パスフレーズ」に入力したものと同じ文字列を入力します。 ［パスフレーズを表示］をクリックすると、入力した文字列を確認できます。	-
共通名	証明書名を入力します。「製品」で選択した製品に従って、必ず「Agent」「Proxy」、「Server」を含めます。 例えば、製品でサーバーを選択した場合は、「本社 ERA 用 Server 証明書」など英字で「Server」という文字を含めます。 製品でエージェントを選択した場合は、「拠点クライアント用 Agent 証明書」など英字で「Agent」という文字を含めます。 Mobile Device Connector の場合、「ホスト」項目と同じ値にします。	○
国コード	2 文字の国コードを入力します。（例：「JP」）	-
州または都道府県	州または都道府県名を入力します。（例：「Tokyo」）	-
ローカル名	ロケーションを入力します。（例：「Shinagawa」）	-
組織名	組織名を入力します。（例：「ESET」）	-
組織単位	組織単位を入力します。（例：「Remote Administrator」）	○
有効開始日	有効期間の開始日を入力します。	○
有効期限	有効期限を入力します。	○

■署名

項目名	説明	必須
署名方法	署名方法を選択します。	○
認証局	「署名方法」で［認証局］を選択した場合に使用します。 ［認証局を選択］をクリックし、初回インストール中に作成した認証局を選択します。	-
カスタム PFX ファイル	「署名方法」で［カスタム pfx ファイル］を選択した場合に使用します。 ［参照］ボタンをクリックし、カスタム pfx ファイルを選択します。	-
認証局のパスフレーズを入力してください	「署名方法」で［認証局］を選択した場合に使用します。 「認証局」で選択した認証局にパスワードが設定している場合は入力します。	-

続く

5 [サマリー] をクリックします。

「基本」および「署名」に入力した内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。

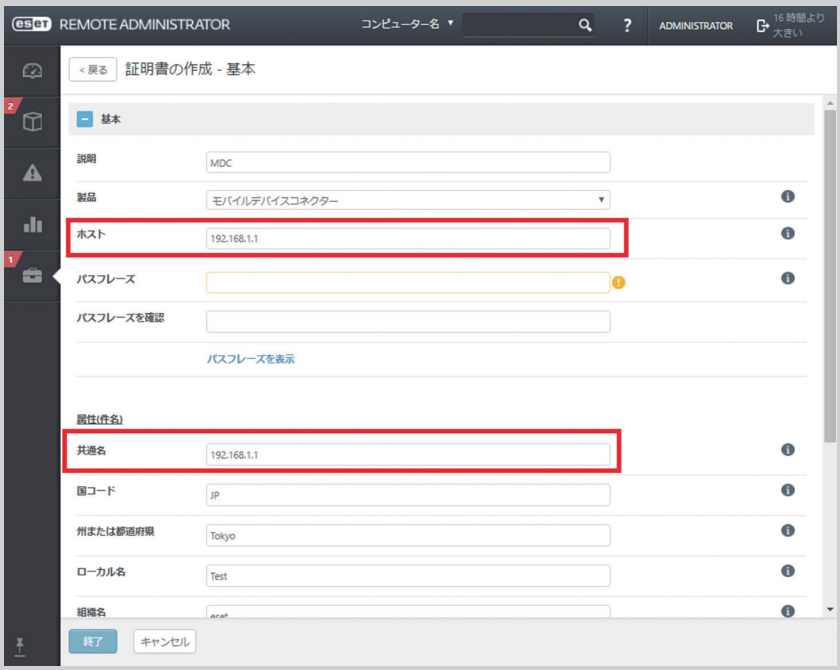
6 [終了] ボタンをクリックします。

「ピア証明書」画面の証明書リストに、選択した製品の証明書が表示されます。

! 重 要

ピア証明書（モバイルデバイスコネクター）を作成する場合は、モバイルデバイスコネクターの「ホスト名」と、ピア証明書（モバイルデバイスコネクター）の「ホスト」、「共通名」を一致させる必要があります。

モバイルデバイスコネクターのホスト名が「192.168.1.1」の場合は以下のように設定します。



モバイルデバイスコネクターのホスト名が不明の場合は、Web コンソールからモバイルデバイスコネクターがインストールされているサーバーのコンフィグレーション設定のリクエストタスクで情報を取得することで確認できます。

6.9.1.3 ピア証明書のエクスポート

作成した証明書は、ローカルコンピューターへの ERA エージェントのインストールや、ERA プロキシのインストールの際に必要です。

■証明書のエクスポート

証明書を PFX ファイルにエクスポートする方法を説明します。

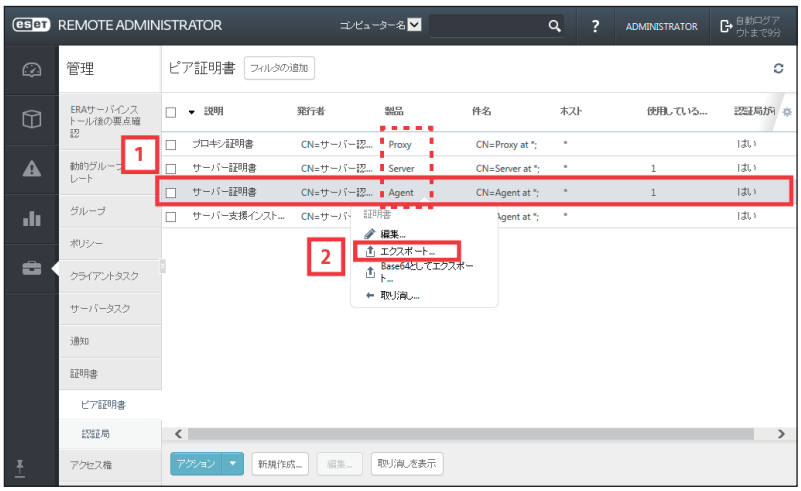
操作手順

1. 証明書リストからエクスポートする証明書をクリックします。

! 重 要

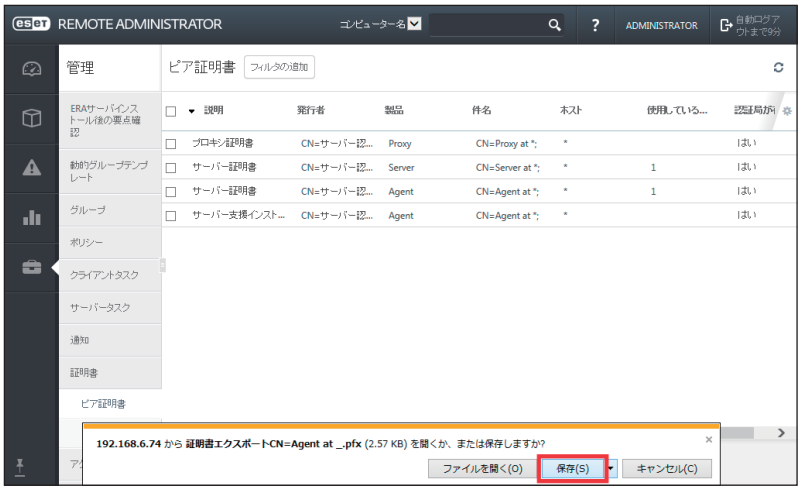
証明書を選択する際は、「製品」欄に該当する製品が表示されていることを確認してください。

2. 「証明書」コンテキストメニューから［エクスポート］を選択します。



保存の確認メッセージが表示されます。

3. ［保存］ボタンをクリックします。



指定した場所に証明書（PFX ファイル）が保存されます。

■証明書を Base64 としてエクスポート

ERA コンポーネントの証明書は ERA Web コンソールで使用できます。
証明書を Base64 形式でエクスポートする方法を説明します。

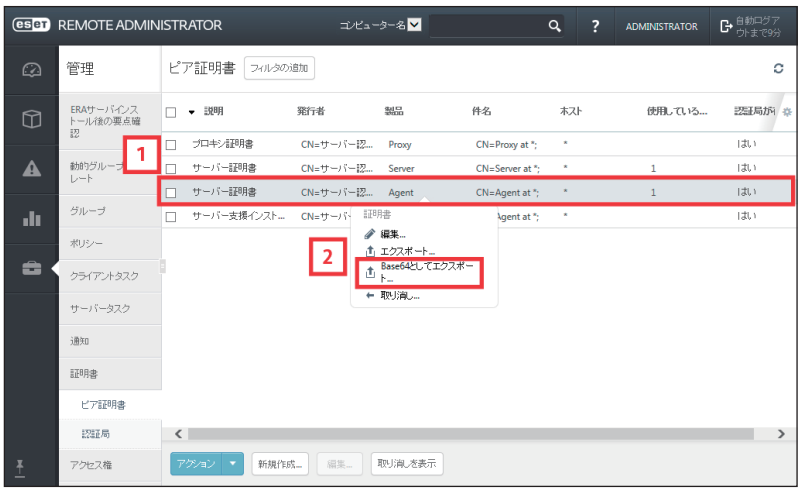
操作手順

1. 証明書リストからエクスポートする証明書をクリックします。

! 重 要

証明書を選択する際は、「製品」に該当する製品が表示されていることを確認してください。

2. 「証明書」コンテキストメニューから［Base64 としてエクスポート］を選択します。



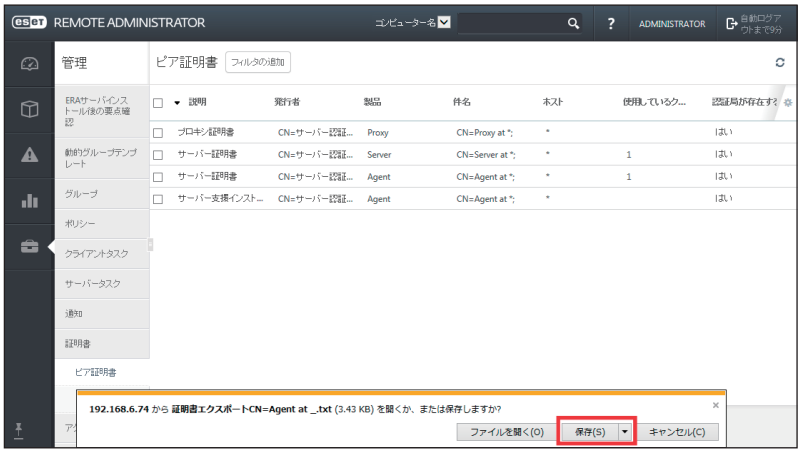
「Base64 として公開鍵をエクスポート」画面が表示されます。

3. ［ダウンロード］ボタンをクリックします。

保存の確認メッセージが表示されます。

続く

4 ［保存］ボタンをクリックします。



指定した場所に証明書（テキストファイル）が保存されます。

！重　要

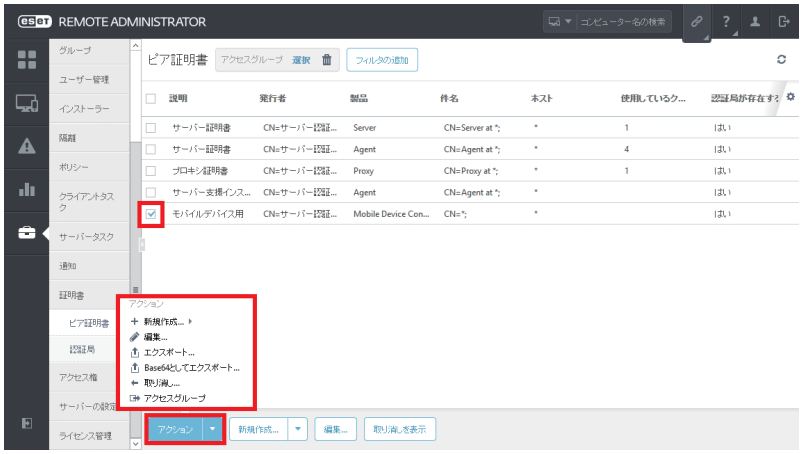
ERA サーバーに接続する ERA コンポーネントで使用可能な証明書の形式は Base64 形式です。Base64 形式ではないカスタム証明書を使用している場合は、Base64 形式に変換する必要があります。

6.9.1.4 「アクセスグループ」で証明書 / 認証局を別グループに移動

証明書や認証局を別グループに移動する方法を説明します。ここでは、証明書を例に説明していますが、認証局も同じ手順で移動できます。

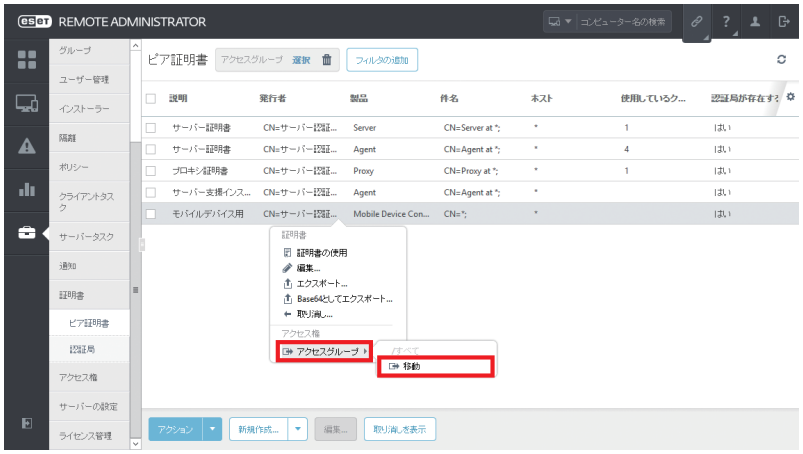
■「アクション」ボタンから移動する

- 移動させたい証明書 / 認証局にチェックを入れ、［アクション］ボタン >［アクセスグループ］を選択します。



■コンテキストメニューから移動する

・移動させたい証明書 / 認証局をクリックし、［アクセスグループ］>［移動］を選択する

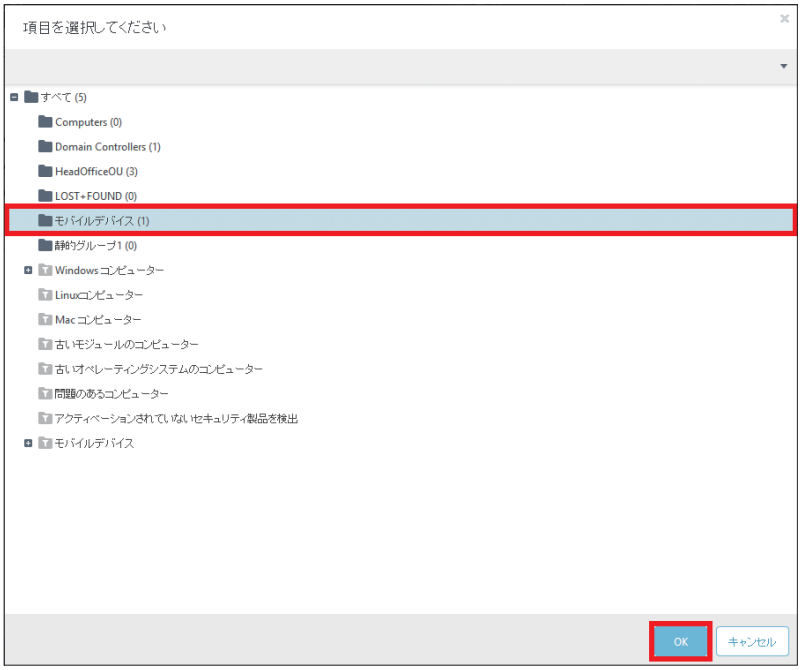


操作手順

1. いずれかの方法で「項目を選択してください」画面を表示します。

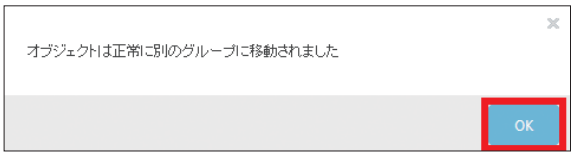
続く

2 移動先のグループをクリックし、［OK］ボタンをクリックします。



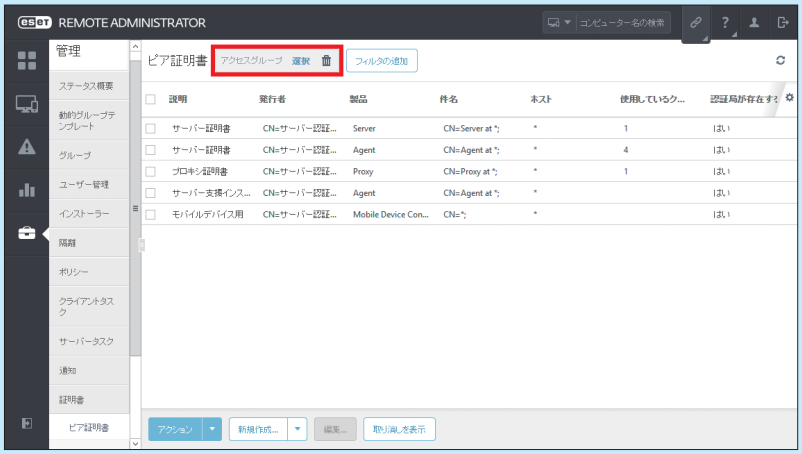
手順 2 で選択したグループに、選択したポリシーが移動してダイアログボックスが表示されます。

3 ［OK］ボタンをクリックします。



ワンポイント

選択した証明書 / 認証局が目的のグループに移動したかどうかを確認したいときは、「アクセスグループ」のフィルターを利用します。「アクセスグループ」の［選択］をクリックすると「項目を選択してください」画面が表示されるので、表示したいグループをクリックして、［OK］ボタンをクリックします。選択したグループのポリシーが一覧表示されます。フィルターを解除したいときは、🗑をクリックします。

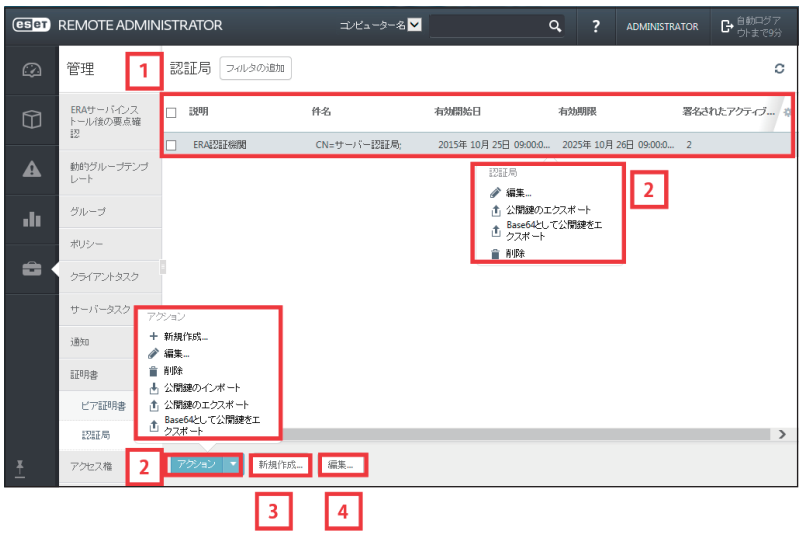


6.9.2 認証局

認証局は、証明書の発行元です。証明書を発行するには、認証局を作成する必要があります。

6.9.2.1 認証局画面の構成

「認証局」画面の構成について説明します。



1	**認証局リスト**	すべての認証局のリストが表示されます。		
2	**［アクション］ボタンおよび「認証局」コンテキストメニュー**	認証局リストから選択した認証局に使用できるアクションが表示されます。		
			新規作成	新しい認証局を作成します。「認証局の作成」画面が表示されます。 画面の詳細は、「6.9.2.2 新しい認証局の作成」を参照してください。
			編集	選択している認証局を編集します。「証明書の編集」画面が表示されます。 編集できる項目は「説明」のみです。 画面の詳細は、「6.9.2.2 新しい認証局の作成」を参照してください。
			削除	選択している認証局を完全に削除します。
			公開鍵のインポート	DER ファイルをインポートし、新しい認証局を作成します。 詳細は、「6.9.2.4 公開鍵のインポート」を参照してください。
			公開鍵のエクスポート	選択している認証局を DER ファイル（.der）にエクスポートします。 詳細は、「6.9.2.3 公開鍵のエクスポート」を参照してください。
			Base64 として公開鍵をエクスポート	選択している認証局をテキストファイル（.txt）にエクスポートします。
3	**新規作成**	新しい認証局を作成します。「認証局の作成」画面が表示されます。 画面の詳細は、「6.9.2.2 新しい認証局の作成」を参照してください。		
4	**編集**	選択している認証局を編集します。「認証局の編集」画面が表示されます。 画面の詳細は、「6.9.2.2 新しい認証局の作成」を参照してください。		

6.9.2.2 新しい認証局の作成

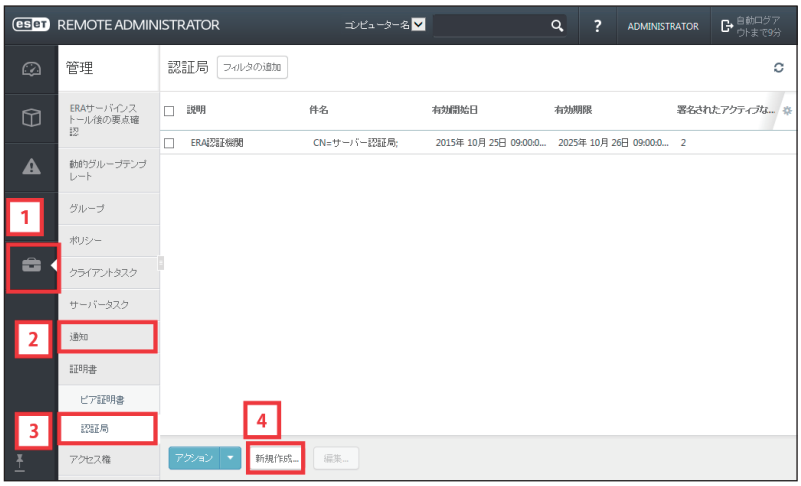
認証局を新しく作成する方法を説明します。

! 重 要

新しい認証局を作成しても、そのままでは動作しません。新しく作成した認証局を ERA サーバーコンピューターに割り当て、ERA サーバーサービスを再起動する必要があります。

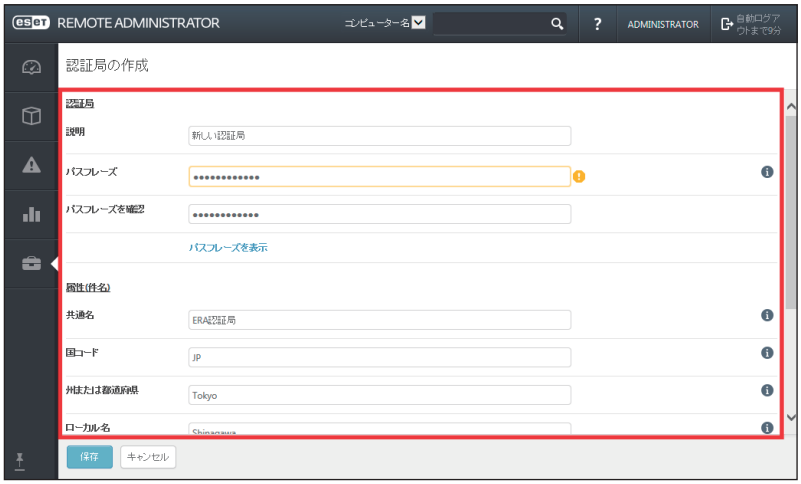
操作手順

1. ［管理］メニューをクリックします。
2. ［証明書］サブメニューをクリックします。
3. ［認証局］をクリックします。
4. ［新規作成］ボタンをクリックします。



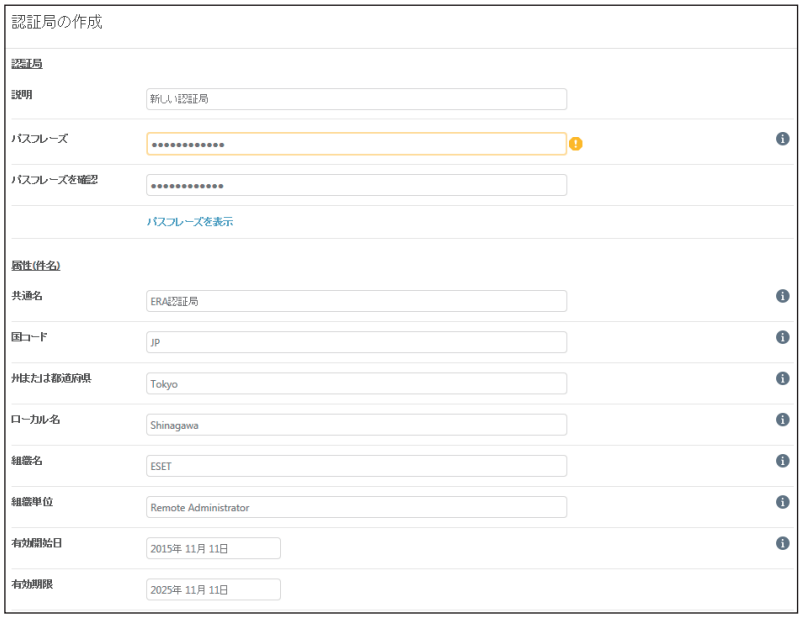
「証明書の作成」画面が表示されます。

5. 各項目を入力します。



続く

■認証局の作成



項目名	説明	必須
説明	認証局の説明を入力します。	-
パスフレーズ	認証局の秘密鍵の暗号化用パスワードを入力します。これは発行済み証明書の署名で必要です。パスワードは、12 文字以上で、小文字、大文字、数字、句読点、その他の文字を 3 種類以上組み合わせて使用する必要があります。	-
パスフレーズを確認	確認のため、「パスフレーズ」に入力したものと同じ文字列を入力します。［パスフレーズを表示］をクリックすると、入力した文字列を確認できます。	-
共通名	認証局名を入力します。認証局リストの「件名」の一部に表示されますので、複数の認証局を識別する一意の名前やわかりやすい情報を入力することを推奨します。	○
国コード	2 文字の国コードを入力します。（例：「JP」）	-
州または都道府県	州または都道府県名を入力します。（例：「Tokyo」）	-
ローカル名	ロケーションを入力します。（例：「Shinagawa」）	-
組織名	組織名を入力します。（例：「ESET」）	-
組織単位	組織単位を入力します。（例：「Remote Administrator」）	-
有効開始日	有効期間の開始日を入力します。	○
有効期限	有効期限を入力します。	○

6 ［保存］ボタンをクリックします。

「認証局」画面の認証局リストに、作成した認証局が表示されます。

6.9.2.3 公開鍵のエクスポート

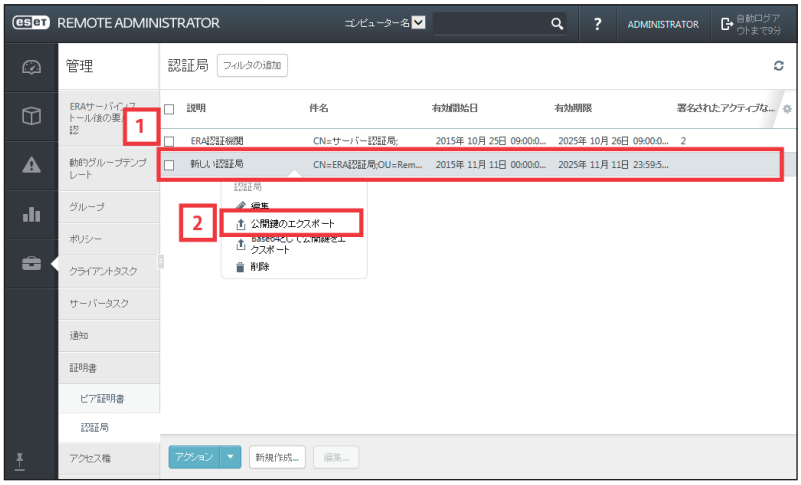
作成した認証局は、ローカルコンピューターへの ERA エージェントのインストールや、ERA プロキシのインストールの際に、公開鍵として必要になります。
作成した認証局を公開鍵としてエクスポートする方法を説明します。

■公開鍵のエクスポート

公開鍵をエクスポートする方法を説明します。

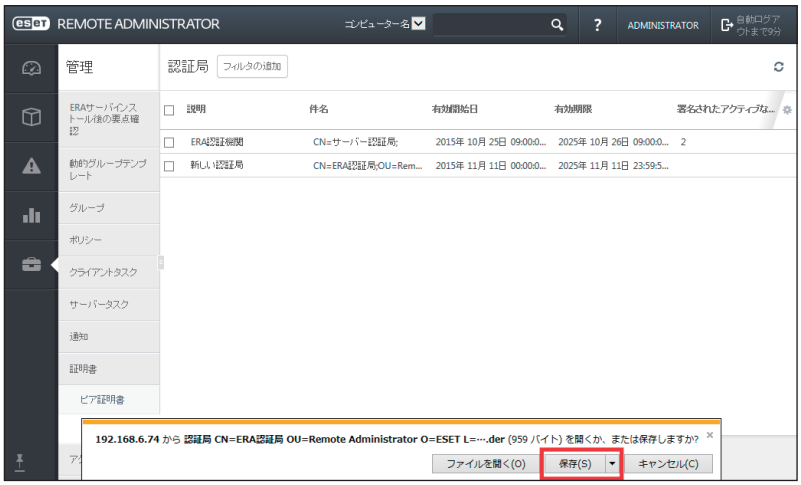
操作手順

1. 認証局リストからエクスポートする認証局をクリックします。
2. 「認証局」コンテキストメニューから［公開鍵のエクスポート］を選択します。



保存の確認メッセージが表示されます。

3. ［保存］ボタンをクリックします。



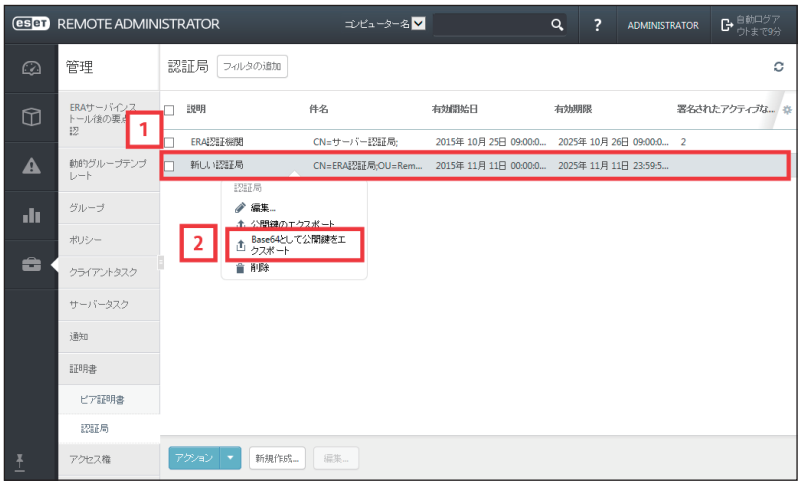
指定した場所に認証局（DER ファイル）が保存されます。

■公開鍵を Base64 としてエクスポート

公開鍵を Base64 形式でエクスポートする方法を説明します。

操作手順

1. 認証局リストからエクスポートする認証局をクリックします。
2. 「認証局」コンテキストメニューから［Base64 として公開鍵をエクスポート］を選択します。

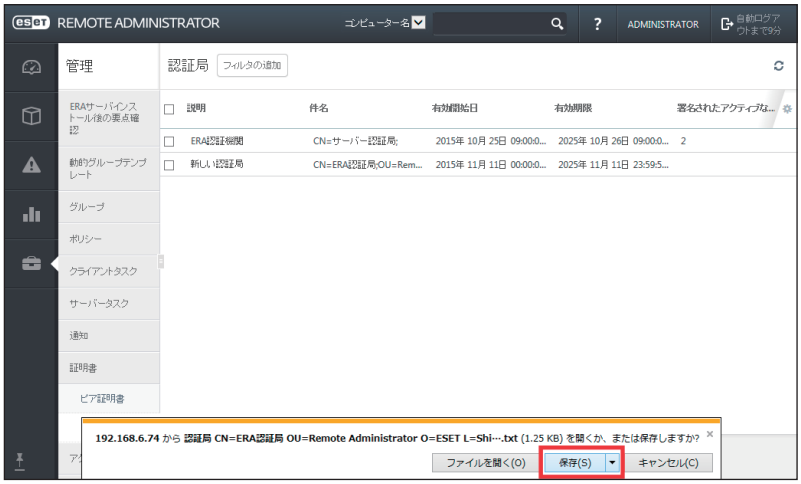


「Base64 として公開鍵をエクスポート」画面が表示されます。

3. ［ダウンロード］ボタンをクリックします。

保存の確認メッセージが表示されます。

4. ［保存］ボタンをクリックします。



指定した場所に認証局（テキストファイル）が保存されます。

！重　要

ERA サーバーに接続する ERA コンポーネントで使用可能な証明書の形式は Base64 形式です。Base64 形式ではないカスタム証明書を使用している場合は、Base64 形式に変換する必要があります。

6.9.2.4 公開鍵のインポート

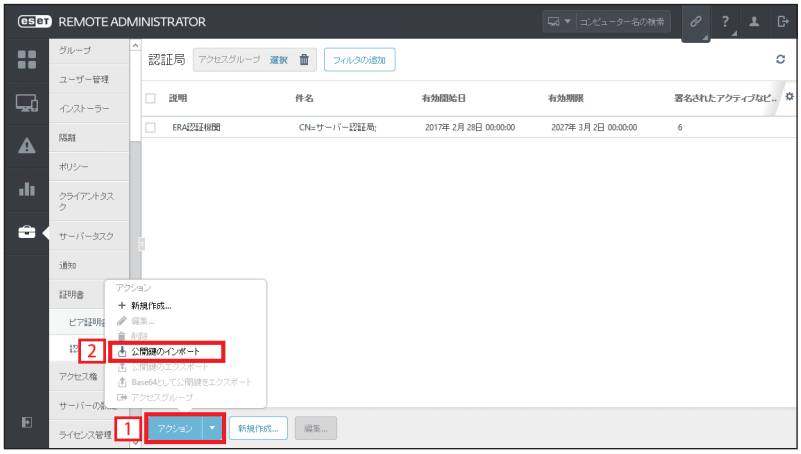
公開鍵をインポートする方法を説明します。

! 重 要

既定の ERA 認証局を削除し、インポートして認証局を作成しても、そのままでは動作しません。インポートした認証局を ERA サーバーコンピューターに割り当て、ERA サーバーサービスを再起動する必要があります。

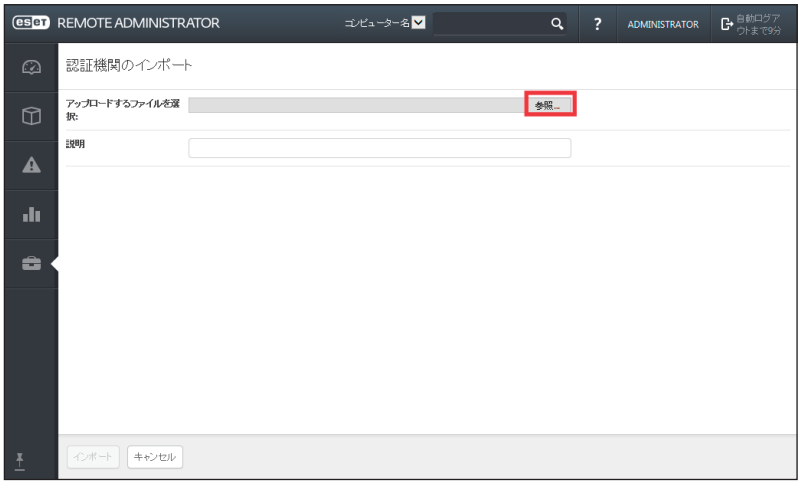
操作手順

1. ［アクション］ボタンをクリックします。
2. 「アクション」コンテキストメニューから［公開鍵のインポート］を選択します。



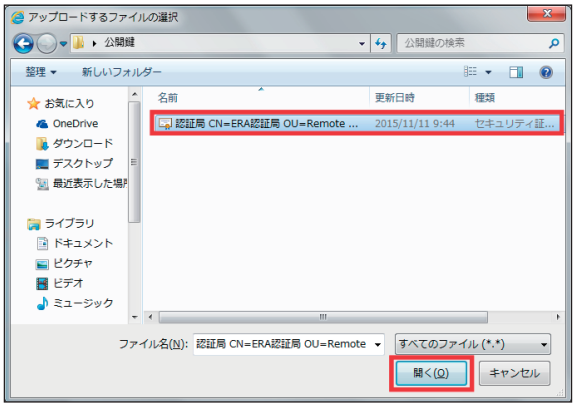
「認証機関のインポート」画面が表示されます。

3. 「アップロードするファイルを選択」の［参照］ボタンをクリックします。

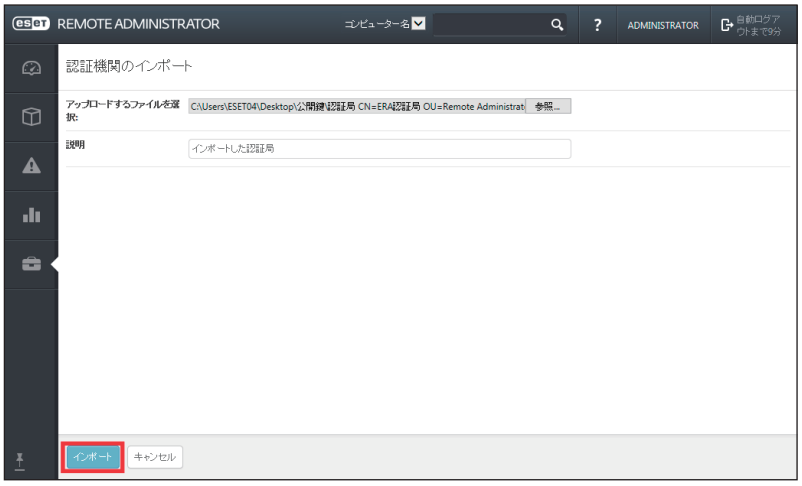


続く

4 アップロードする DER ファイルを選択し、［開く］ボタンをクリックします。

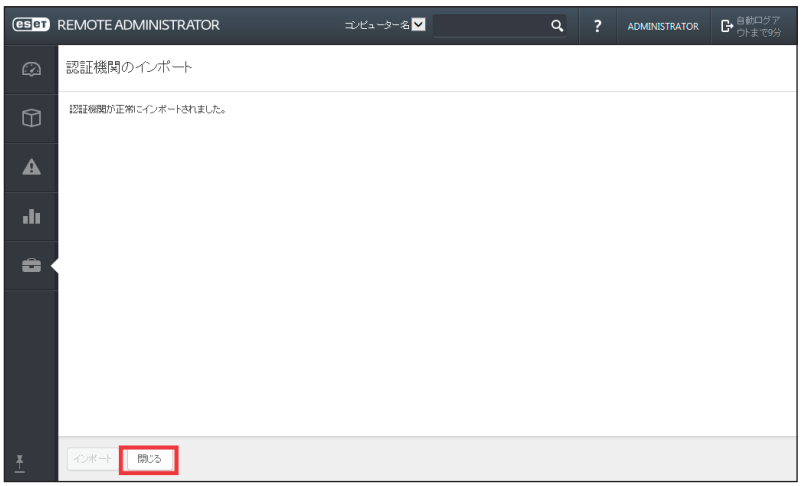


5 ［インポート］ボタンをクリックします。



選択した認証局がインポートされます。

6 ［閉じる］ボタンをクリックします。



「認証局」画面の認証局リストに、インポートした認証局が表示されます。

6.9.3 APN 証明書

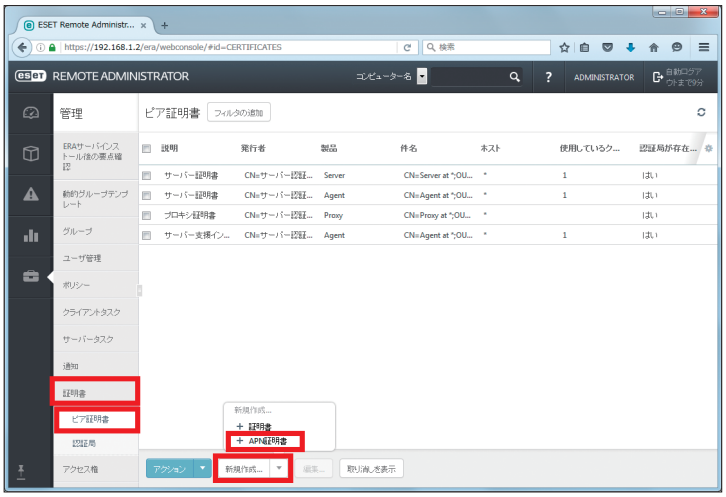
APN(Apple Push Notification) 証明書は、iOS デバイスを ERA サーバーに登録するときに必要になる Apple 社の署名付き証明書です。Apple 社の署名付きの APN 証明書は、Apple 社のポータルサイト（https://identity.apple.com/pushcert/）で作成します。
また、iOS デバイスを ERA サーバーに登録するには、Apple 社の署名付きの APN 証明書を登録した iOS デバイス登録用のポリシーを作成する必要もあります。詳細は「6.5.3.1 iOS デバイス登録用のポリシーを作成する」を参照してください。

! 重 要

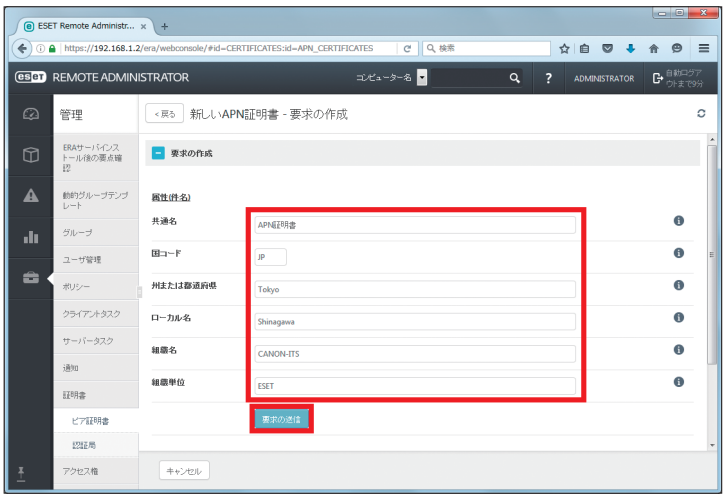
Apple 社の署名付きの APN 証明書を作成するには、Apple ID が必要です。また、ERA サーバーに有効なライセンスがある必要があります。

操作手順

1 ［管理］タブ > ［証明書］ > ［ピア証明書］をクリックし、［新規作成］ボタンをクリックしてから、［APN 証明書］を選択します。

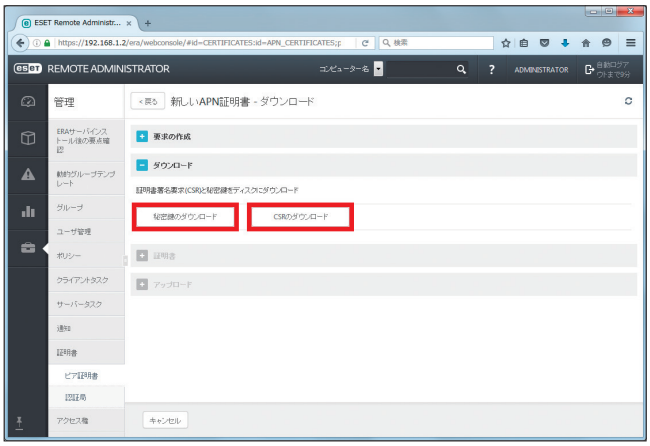


2 証明書属性 (国コード、組織名など) を指定し、［要求の送信］ボタンをクリックします。



続く

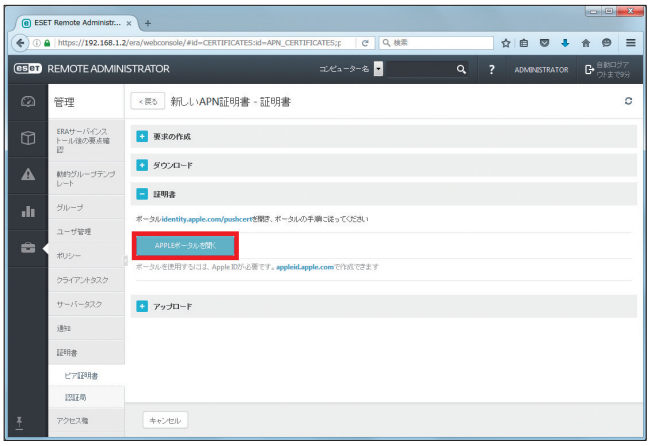
3 [CSR のダウンロード] をクリックし、証明書署名要求（CSR）をダウンロードします。[秘密鍵のダウンロード] をクリックし、秘密鍵をダウンロードします。



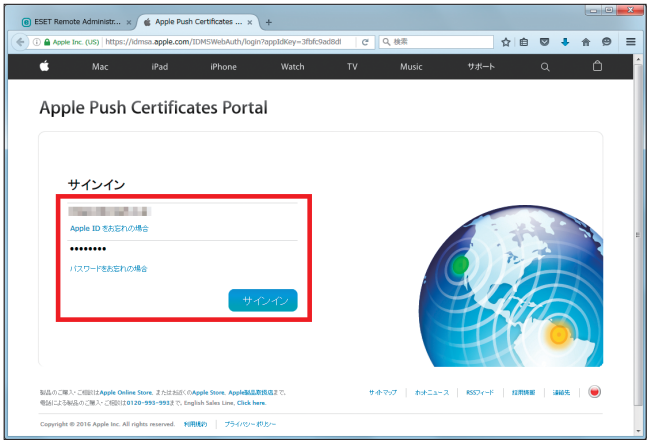
ワンポイント

証明書署名要求（CSR）は、Apple 社の署名付き APN 証明書を作成するときに利用します。秘密鍵は、iOS デバイス登録用のポリシーを作成するときに利用します。

4 [APPLE ポータルを開く] をクリックします。

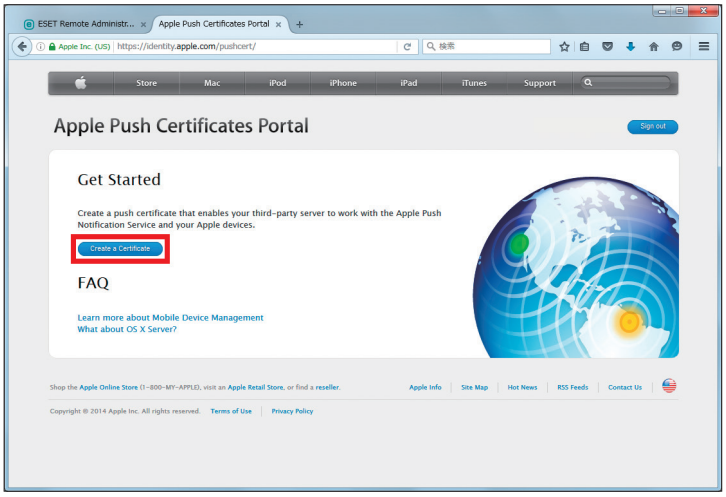


5 AppleID のメールアドレスとパスワードを入力し、Apple Push Certificates Portal にサインインします。

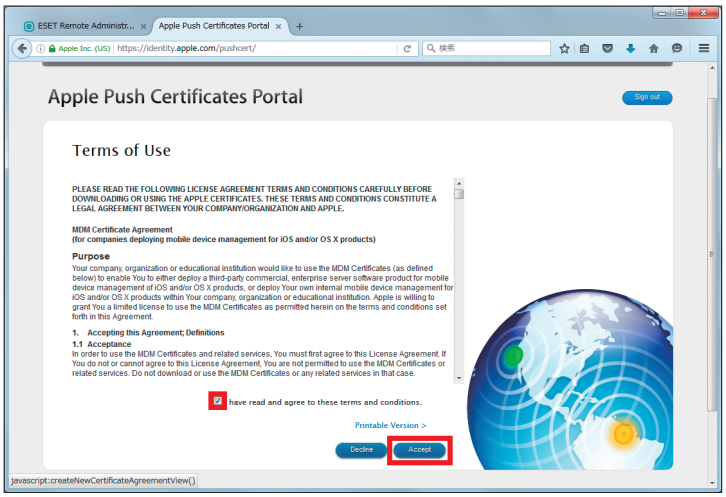


続く

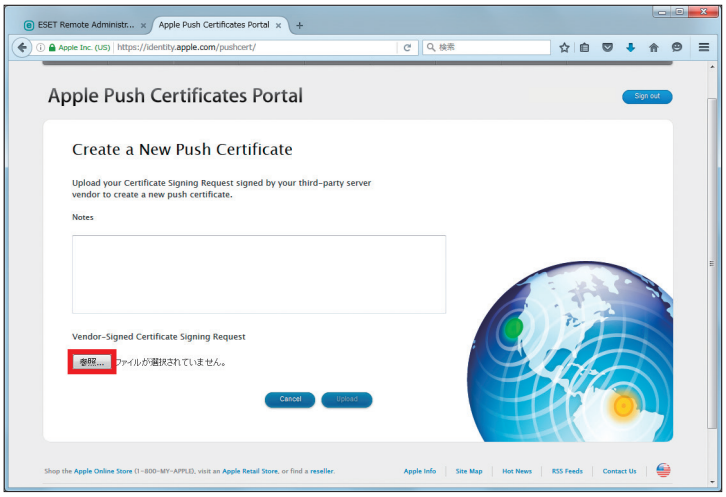
6 [Create a CertiFicate] をクリックします。



7 [I have read ...] のチェックをオンにし、[Accept] をクリックします。

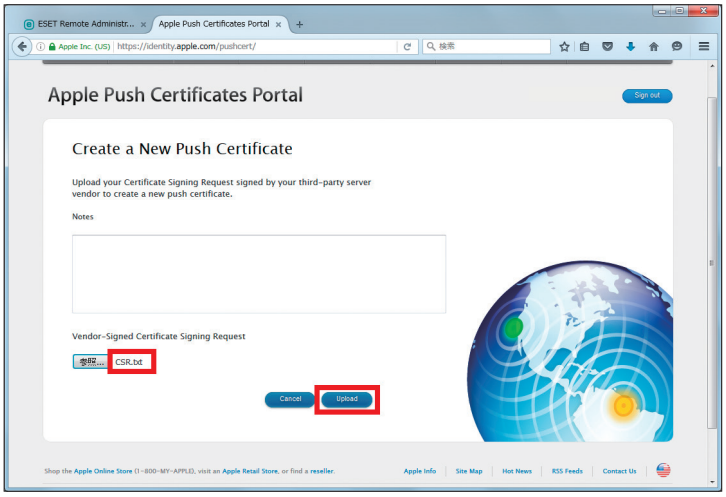


8 [参照] をクリックし、証明書署名要求（CSR）を選択します。

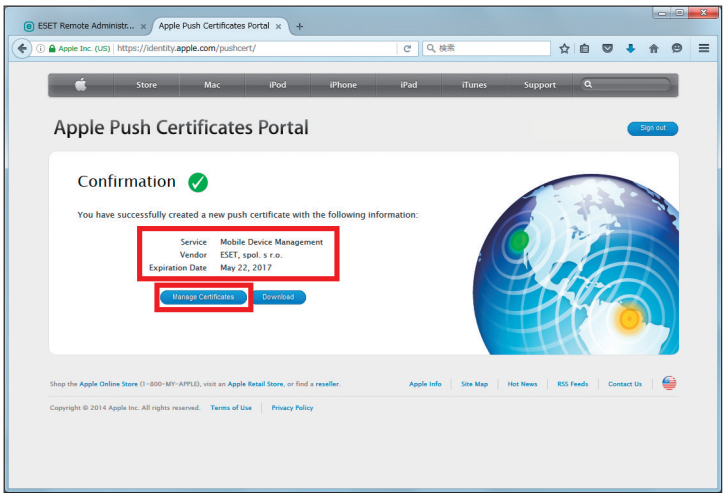


続く

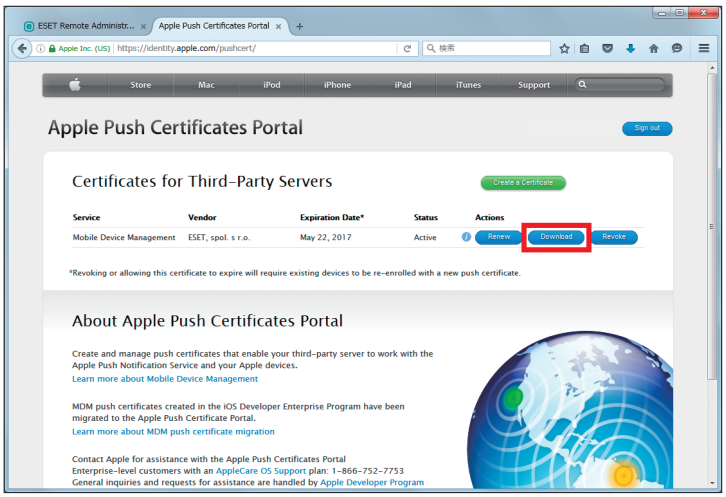
9 [Upload] をクリックします。



10 Apple 社の署名付き APN 証明書が作成されます。[Manage Certificates] をクリックします。

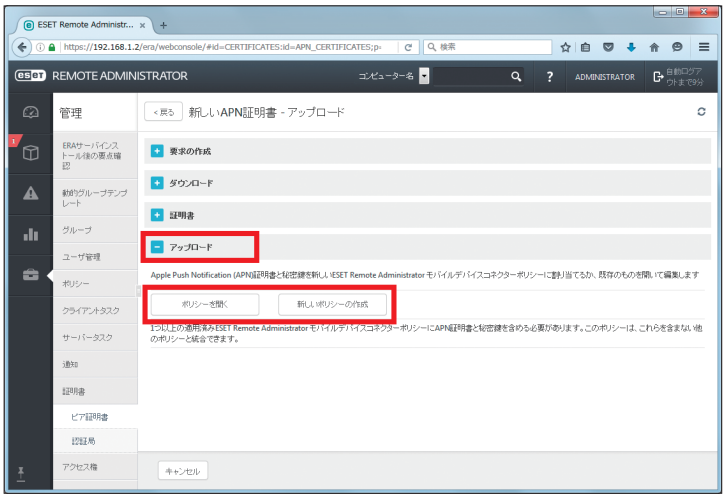


11 Apple 社の署名付き APN 証明書の状態を確認できます。[Download] をクリックして、Apple 社の署名付き証明書をダウンロードします。



続く

⑫［アップロード］をクリックして、iOS デバイス登録用のポリシーを作成して登録します。［ポリシーを開く］をクリックすると、既存の作成済みポリシーの内容を編集して、iOS デバイス登録用のポリシーを作成できます。新規のポリシーを作成する場合は、［新しいポリシーの作成］をクリックすると、ポリシーの新規作成ページが表示されます。「6.5.3.1　iOS デバイス登録用のポリシーを作成する」を参考に iOS デバイス登録用のポリシーの作成を行ってください。



ワンポイント

手順 11 でダウンロードした Apple 社の署名付き APN 証明書と手順 3 でダウンロードした秘密鍵は、iOS デバイス登録用のポリシーを作成するときに利用します。詳細は、「6.5.3.1　iOS デバイス登録用のポリシーを作成する」をご参照ください。

6.10 アクセス権

アクセス権は、ERA Web コンソールのユーザーとその権限を管理します。それぞれの機能へのアクセスは、権限設定を使用して、すべての ERA Web コンソールのユーザーに付与する必要があります。権限設定は、ESET Remote Administrator を利用するユーザーに必要な機能のアクセスレベルを個別に定義します。

6.10.1 ユーザー

特定の権限設定を持つ複数のユーザーを用意することで、安全に効率よくアクセスすることができます。
ユーザーには 2 つのタイプがあります。

ローカルユーザー	Web コンソールから作成および管理されるユーザーアカウント。
マッピングされたドメインセキュリティグループ	Active Directory によって管理および認証されるグループ。

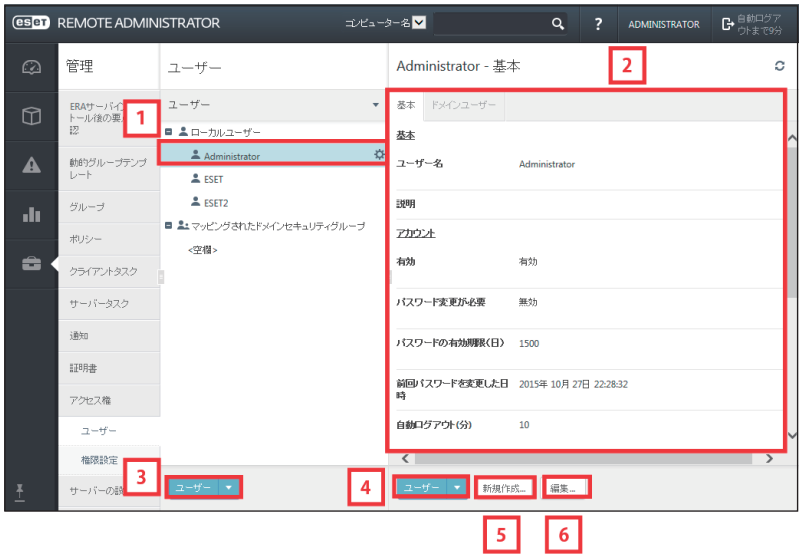
! 重 要

ERA のインストール時には、唯一のアカウントとして「Administrator」があります。「Administrator」は、すべての機能にアクセスできる管理者アカウントです。そのため、このアカウントを日常では使用せず、別の管理者アカウントを作成するか、マッピングされたドメインセキュリティグループから管理者権限設定が割り当てられた管理者を作成することを強く推奨します。このようにすると、管理者アカウントのログインパスワードを忘れた場合など、問題が発生したときに復旧することができます。「Administrator」はバックアップとして使用してください。

6.10.1.1 ユーザー画面の構成

「ユーザー」画面の構成について説明します。

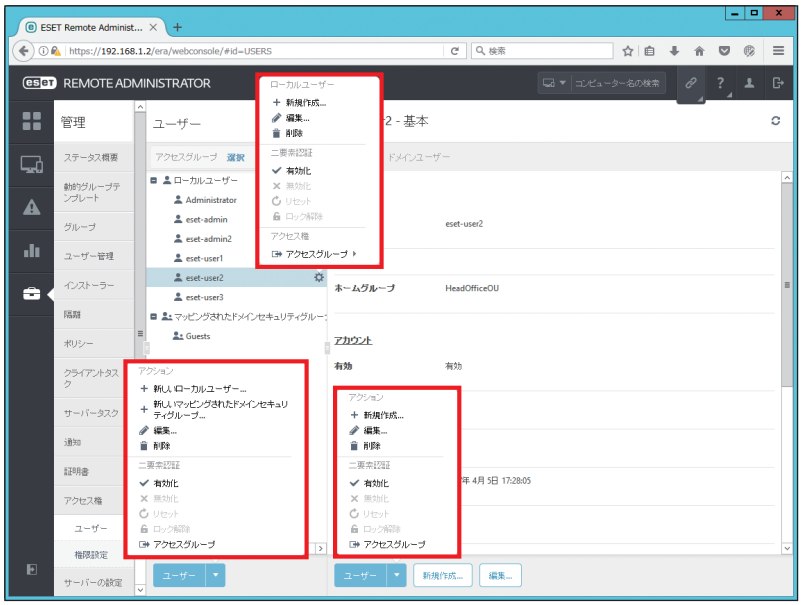
■ローカルユーザー



1	**ローカルユーザーリスト**	すべてのローカルユーザーのリストが表示されます。
2	**選択中のユーザーの詳細**	ローカルユーザーリストから選択したローカルユーザーに関する詳細が表示されます。
	「基本」タブ	選択しているローカルユーザーの概要が表示されます。
	「ドメインユーザー」タブ	マッピングされたドメインセキュリティグループを選択している場合に、ログインしているドメインユーザーの情報が表示されます。
3	**ユーザー**	新しいローカルユーザーまたはマッピングされたドメインセキュリティグループの作成、選択中のローカルユーザーの編集、削除などのアクションメニューが表示されます。 表示されるアクションの詳細は、「●［ユーザー］ボタンと「ローカルユーザー」コンテキストメニューのアクション」を参照してください。
4	**「基本」タブのユーザー**	新しいローカルユーザーの作成や選択中のローカルユーザーの編集、削除などのアクションメニューが表示されます。 表示されるアクションの詳細は、「●［ユーザー］ボタンと「ローカルユーザー」コンテキストメニューのアクション」を参照してください。
5	**新規作成**	新しいローカルユーザーを作成します。「新しいローカルユーザー」画面が表示されます。 画面の詳細は、「6.10.1.2 新しいローカルユーザーの作成」を参照してください。
6	**編集**	選択しているローカルユーザーを編集します。「ローカルユーザーの編集」画面が表示されます。 画面の詳細は、「6.10.1.2 新しいローカルユーザーの作成」を参照してください。

●［ユーザー］ボタンと「ローカルユーザー」コンテキストメニューのアクション

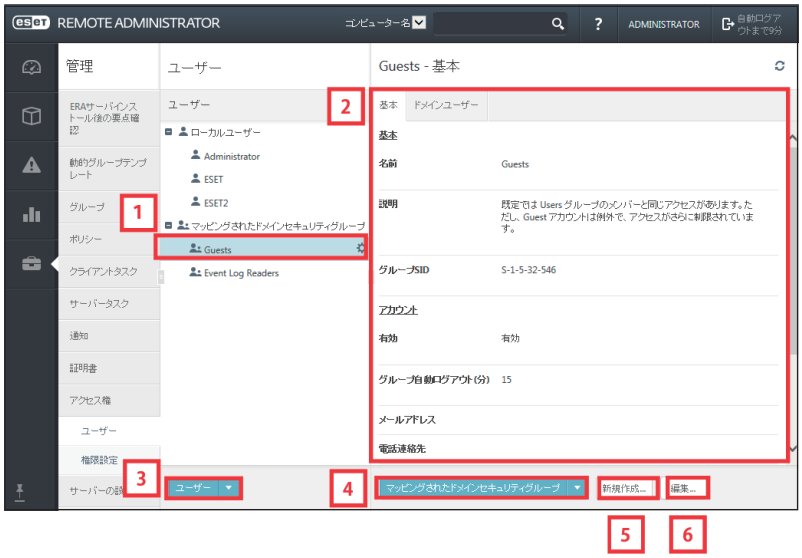
［ユーザー］ボタンと「ローカルユーザー」コンテキストメニューのアクションについて説明します。



＋	**新しいローカルユーザー**	新しいローカルユーザーを作成します。「新しいローカルユーザー」画面が表示されます。 画面の詳細は、「6.10.1.2　新しいローカルユーザーの作成」を参照してください。
＋	**新しいマッピングされたドメインセキュリティグループ**	新しいマッピングされたドメインセキュリティグループを作成します。「新しいマッピングされたドメインセキュリティグループ」画面が表示されます。 画面の詳細は、「6.10.1.3　新しいマッピングされたドメインセキュリティグループの作成」を参照してください。
＋	**新規作成**	新しいローカルユーザーを作成します。「新しいローカルユーザー」画面が表示されます。 画面の詳細は、「6.10.1.2　新しいローカルユーザーの作成」を参照してください。
	編集	選択しているローカルユーザーを編集します。
	削除	選択しているローカルユーザーを完全に削除します。
	アクセスグループ	選択したユーザーを別のグループに移動します。「項目を選択してください」画面が表示され、移動先のグループを選択できます。

※二要素認証のアクションについては対象外です。

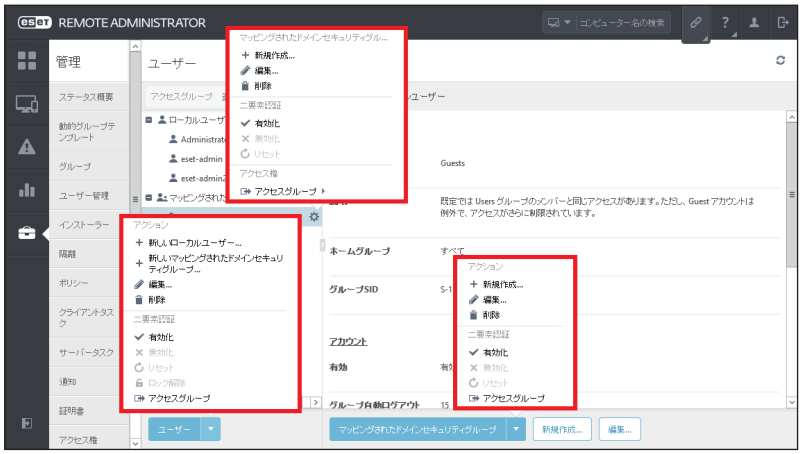
■マッピングされたドメインのセキュリティグループ



1	**マッピングされたドメインセキュリティグループリスト**	すべてのマッピングされたドメインセキュリティグループのリストが表示されます。
2	**選択中のマッピングされたドメインセキュリティグループの詳細**	マッピングされたドメインセキュリティグループリストから選択したドメインセキュリティグループに関する詳細が表示されます。
	「基本」タブ	選択しているドメインセキュリティグループの概要が表示されます。
	「ドメインユーザー」タブ	選択しているドメインセキュリティグループに属しているユーザーリストが表示されます。
3	**ユーザー**	新しいマッピングされたドメインセキュリティグループの作成や選択中のドメインセキュリティグループの編集、削除などのアクションメニューが表示されます。 表示されるアクションの詳細は、「●［ユーザー］ボタンと［マッピングされたドメインセキュリティグループ］ボタンおよびコンテキストメニューのアクション」を参照してください。
4	**マッピングされたドメインセキュリティグループ**	新しいマッピングされたドメインセキュリティグループの作成や選択中のドメインセキュリティグループの編集、削除などのアクションメニューが表示されます。 表示されるアクションの詳細は、「●［ユーザー］ボタンと［マッピングされたドメインセキュリティグループ］ボタンおよびコンテキストメニューのアクション」を参照してください。
5	**新規作成**	新しいマッピングされたドメインセキュリティグループを作成します。「新しいマッピングされたドメインセキュリティグループ」画面が表示されます。 画面の詳細は、「6.10.1.3　新しいマッピングされたドメインセキュリティグループの作成」を参照してください。
6	**編集**	選択しているドメインセキュリティグループを編集します。「マッピングされたドメインセキュリティグループの編集」画面が表示されます。 画面の詳細は、「6.10.1.3　新しいマッピングされたドメインセキュリティグループの作成」を参照してください。

●［ユーザー］ボタンと［マッピングされたドメインセキュリティグループ］ボタンおよびコンテキストメニューのアクション

［ユーザー］ボタンと［マッピングされたドメインセキュリティグループ］ボタンおよびコンテキストメニューのアクションについて説明します。



＋	**新しいローカルユーザー**	新しいローカルユーザーを作成します。「新しいローカルユーザー」画面が表示されます。 画面の詳細は、「6.10.1.2　新しいローカルユーザーの作成」を参照してください。
＋	**新しいマッピングされたドメインセキュリティグループ**	新しいマッピングされたドメインセキュリティグループを作成します。「新しいマッピングされたドメインセキュリティグループ」画面が表示されます。 画面の詳細は、「6.10.1.3　新しいマッピングされたドメインセキュリティグループの作成」を参照してください。
＋	**新規作成**	新しいマッピングされたドメインセキュリティグループを作成します。「新しいローカルユーザーマッピングされたドメインセキュリティグループ」画面が表示されます。 画面の詳細は、「6.10.1.3　新しいマッピングされたドメインセキュリティグループの作成」を参照してください。
編集	**編集**	選択しているマッピングされたドメインセキュリティグループを編集します。
削除	**削除**	選択しているマッピングされたドメインセキュリティグループを完全に削除します。
アクセスグループ	**アクセスグループ**	選択したユーザーを別のグループに移動します。「項目を選択してください」画面が表示され、移動先のグループを選択できます。

※二要素認証のアクションについては対象外です。

6.10.1.2　新しいローカルユーザーの作成

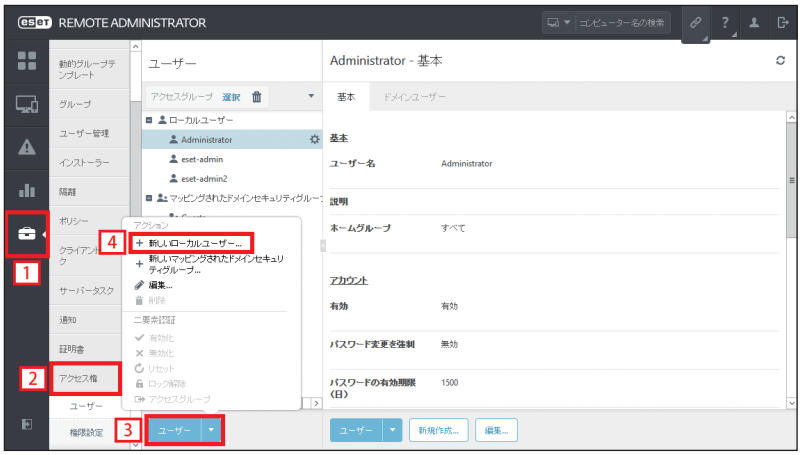
ローカルユーザーを新しく作成する方法を説明します。

ワンポイント

既定の権限設定ではなく、特定の機能のみの権限設定を割り当てたい場合は、事前に新しく権限設定を作成することを推奨します。
権限設定の作成については、「6.10.2.2　新しい権限設定の作成」を参照してください。

操作手順

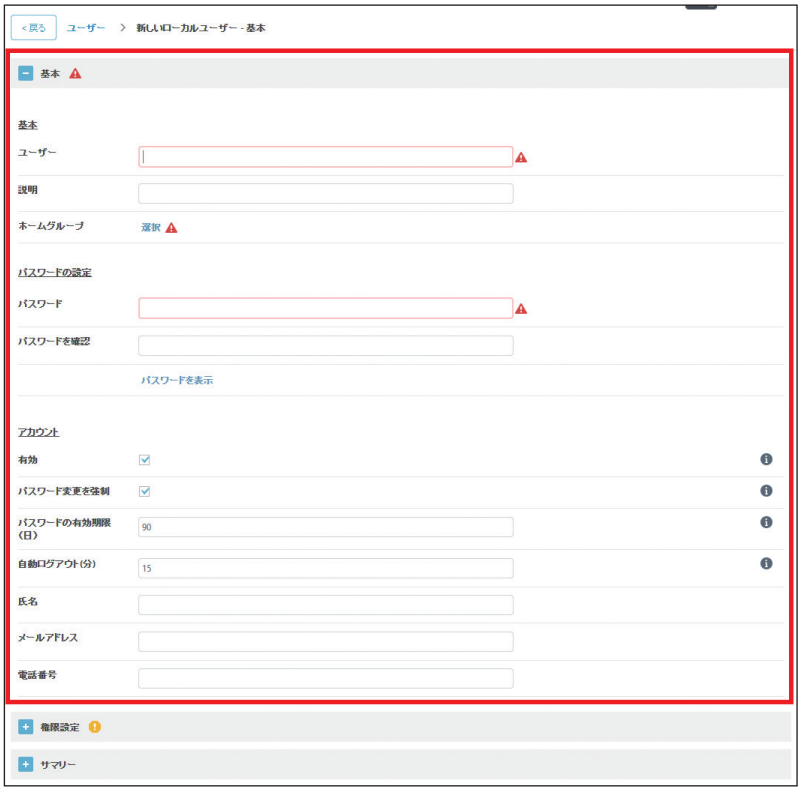
1. ［管理］メニューをクリックします。
2. ［アクセス権］サブメニューをクリックします。
3. ［ユーザー］ボタンをクリックします。
4. ［新しいローカルユーザー］を選択します。



「新しいローカルユーザー」画面が表示されます。

続く

5 「基本」の各項目を入力します。



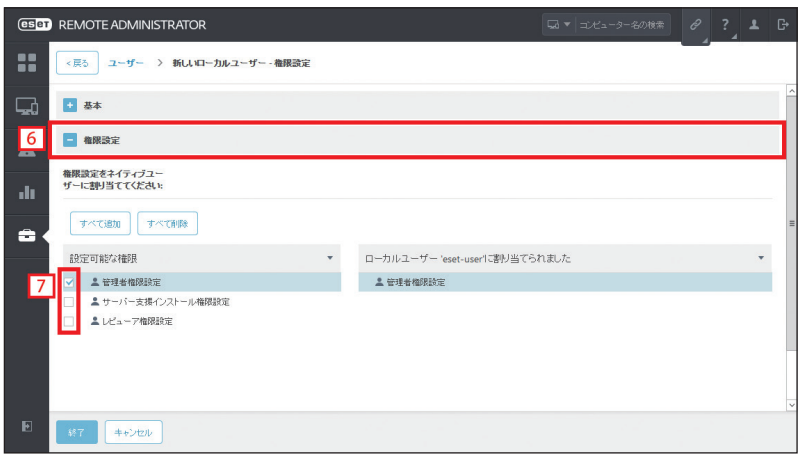
続く

■基本

項目名	説明	必須
ユーザー	作成するローカルユーザーの名前を入力します。ここで作成したユーザーがログインの際のユーザー名として使用されます。	○
説明	作成するローカルユーザーの説明を入力します。	-
ホームグループ	作成するユーザーのホームグループを選択します。［選択］をクリックすると、ドメイングループのユーザーが作成したすべての静的グループの中からホームグループを選択できます。	○
パスワード	認証用パスワードを 8 文字以上で入力します。パスワードにユーザー名を含めることはできません。 また、入力した新しいパスワードが 12 文字に満たない場合は、画面上に警告が表示されます。パスワードには、小文字、大文字、数字、句読点、その他の文字を 3 種類以上組み合わせて使用することを推奨します。	○
パスワードを確認	確認のため、「パスワード」に入力したものと同じ文字列を入力します。 ［パスワードを表示］をクリックすると、入力した文字列を確認できます。	-
有効	オンにするとユーザーアカウントが有効になり、ERA Web コンソールにログインできます。	○
パスワード変更を強制	オンにすると、ユーザーが初回ログイン後にパスワードの変更が強制されます。	○
パスワードの有効期限（日）	パスワードの有効期限を入力します。（日単位） ここで指定した日数が経過した場合にユーザーはパスワードの変更をする必要があります。	○
自動ログアウト（分）	アイドル状態の場合にユーザーが自動的にログアウトする時間（分単位）を入力します。	○
氏名	ユーザーの名前を入力します。	-
メールアドレス	ユーザーのメールアドレスを入力します。	-
電話番号	ユーザーの電話番号を入力します。	-

6 ［権限設定］をクリックします。

7 「設定可能な権限」の付与する権限設定をにチェックを入れます。



右側の欄に追加されます。

続く

■権限設定

項目名	説明		必須
設定可能な権限	ユーザーに付与する権限を選択します。		○
	管理者権限設定	フルアクセスの権限です。	-
	サーバー支援インストール権限設定	サーバー支援インストールの際に使用できる権限です。	-
	レビューア権限設定	読み取り専用の権限です。	-
	カスタムアクセス権限設定	新しく権限設定を作成している場合に表示されます。 権限設定の作成については、「6.10.2.2　新しい権限設定の作成」を参照してください。	-

8 ［サマリー］をクリックします。

「基本」および「権限設定」に入力した内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。

9 ［終了］ボタンをクリックします。

作成したローカルユーザーがリストに表示されます。

6.10.1.3 新しいマッピングされたドメインセキュリティグループの作成

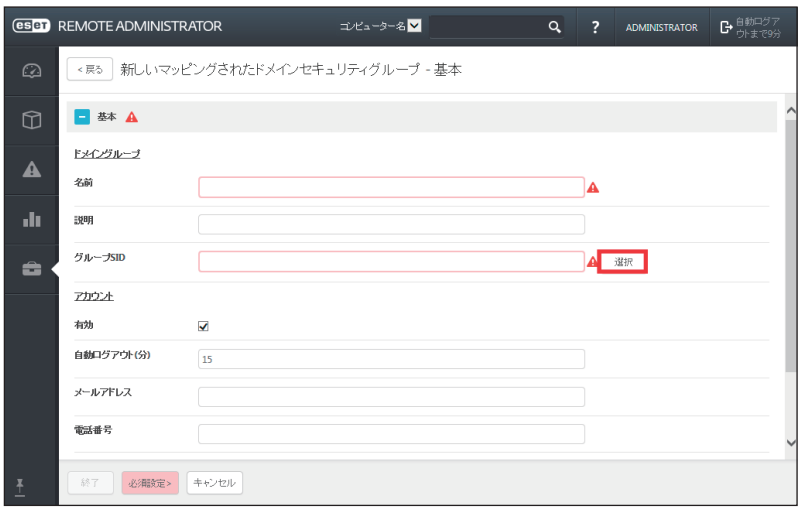
ERA サーバーに Active Directory のドメインセキュリティグループをマッピングすると、ドメインセキュリティグループのメンバーで ERA Web コンソールにログインすることができます。

操作手順

1. ［管理］メニューをクリックします。
2. ［アクセス権］サブメニューをクリックします。
3. ［ユーザー］ボタンをクリックします。
4. ［新しいマッピングされたドメインセキュリティグループ］を選択します。

「新しいマッピングされたドメインセキュリティグループ」画面が表示されます。

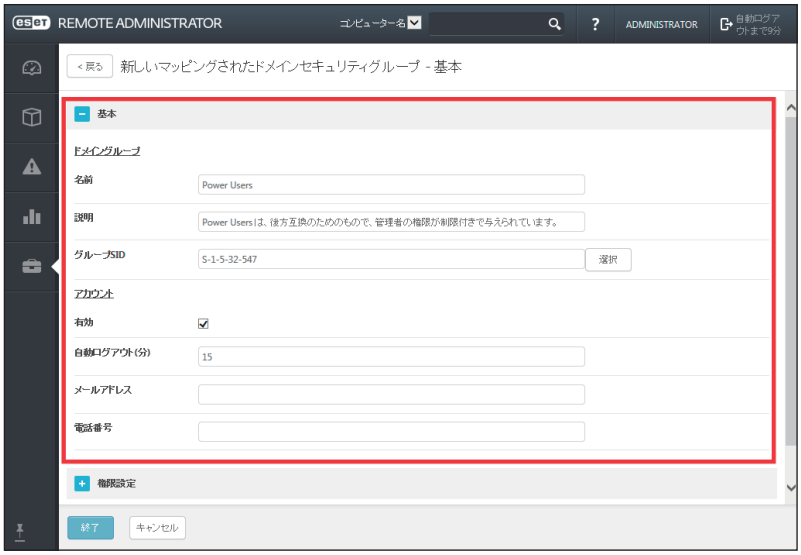
5. ［グループ SID］の［選択］ボタンをクリックします。



続く

6 該当する SID を選択し、［OK］ボタンをクリックします。

7 「基本」のその他の各項目を入力します。



■基本

項目名	説明	必須
名前	作成するドメインセキュリティグループの名前を入力します。画面には、ここで設定した名前が表示されます。 ［グループ SID］を選択すると自動的に表示されますので、必要に応じて編集します。	○
説明	作成するドメインセキュリティグループの説明を入力します。［グループ SID］を選択すると自動的に表示されますので、必要に応じて編集します。	-
グループ SID	ドメインセキュリティグループに割り当てる SID（セキュリティ ID）を選択します。	○
有効	オンにするとユーザーアカウントが有効になり、ERA Web コンソールにログインできます。	○

続く

項目名	説明	必須
自動ログアウト（分）	アイドル状態の場合にユーザーが自動的にログアウトする時間（分単位）を入力します。	○
メールアドレス	連絡先のメールアドレスを入力します。	-
電話番号	連絡先の電話番号を入力します。	-

8 ［権限設定］をクリックします。

9 「設定可能な権限」の付与する権限設定にチェックを入れます。

右側の欄に追加されます。

■権限設定

権限設定の詳細は、「6.10.1.2　新しいローカルユーザーの作成」の操作手順 7「■権限設定」を参照してください。

10 ［サマリー］をクリックします。

「基本」および「権限設定」に入力した内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。

11 ［終了］ボタンをクリックします。

作成したマッピングされたドメインセキュリティグループがリストに表示されます。

6.10.2 権限設定

権限設定は、ERA Web コンソールにアクセスするユーザーが実行できる機能や参照できる静的グループを定義します。ローカルユーザーは自身の権限を保持することができ、ドメインユーザーはマッピングされたセキュリティグループの権限を保持します。

権限は、ローカルユーザー、証明書、ポリシーなどのカテゴリに分類されており、個別に読み取り専用または書き込み／実行アクセスを許可できるようになっています。

読み取り専用の権限は、ユーザーの監査に適しています。データを表示できますが、変更はできません。

書き込み／実行では、この権限を持ったユーザーがそれぞれのオブジェクトを変更したり、実行したりすることができます。

また、特定の静的グループへのアクセス権を設定した場合は、その静的グループに登録されているコンピューターのみアクセスできます。特定の静的グループへのアクセス権を設定すると、その静的グループのサブグループすべてに自動的にアクセスできます。

続く

6.10.2.1 権限設定画面の構成

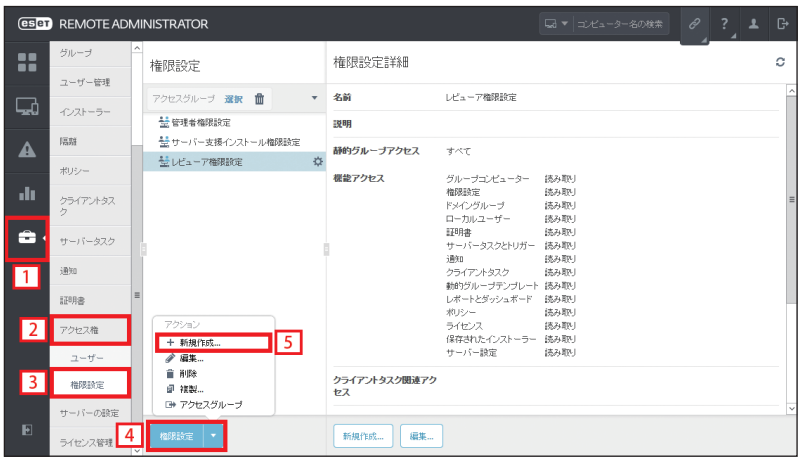
「権限設定」画面の構成について説明します。

1	**権限設定リスト**	すべての権限設定のリストが表示されます。		
2	**選択中の権限設定の詳細**	権限設定リストから選択した権限設定に関する詳細が表示されます。		
3	**［権限設定］ボタンおよび「権限設定」コンテキストメニュー**	権限設定リストから選択した権限設定に使用できるアクションが表示されます。		
			新規作成	新しい権限設定を作成します。「新しい権限設定」画面が表示されます。 画面の詳細は、「6.10.2.2 新しい権限設定の作成」を参照してください。
			編集	選択している権限設定を編集します。「権限設定の編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しい権限設定として保存することができます。 画面の詳細は、「6.10.2.2 新しい権限設定の作成」を参照してください。
			削除	選択している権限設定を完全に削除します。
			複製	選択している権限設定の内容をコピーした状態で「新しい権限設定」画面が表示されます。 画面の詳細は、「6.10.2.2 新しい権限設定の作成」を参照してください。
			アクセスグループ	選択した権限設定を別のグループに移動します。「項目を選択してください」画面が表示され、移動先のグループを選択できます。
4	**新規作成**	新しい権限設定を作成します。「新しい権限設定」画面が表示されます。 画面の詳細は、「6.10.2.2 新しい権限設定の作成」を参照してください。		
5	**編集**	選択している権限設定を編集します。「権限設定の編集」画面が表示されます。 ※［名前を付けて保存］ボタンをクリックすると、変更した内容を新しい権限設定として保存することができます。 画面の詳細は、「6.10.2.2 新しい権限設定の作成」を参照してください。		

6.10.2.2　新しい権限設定の作成

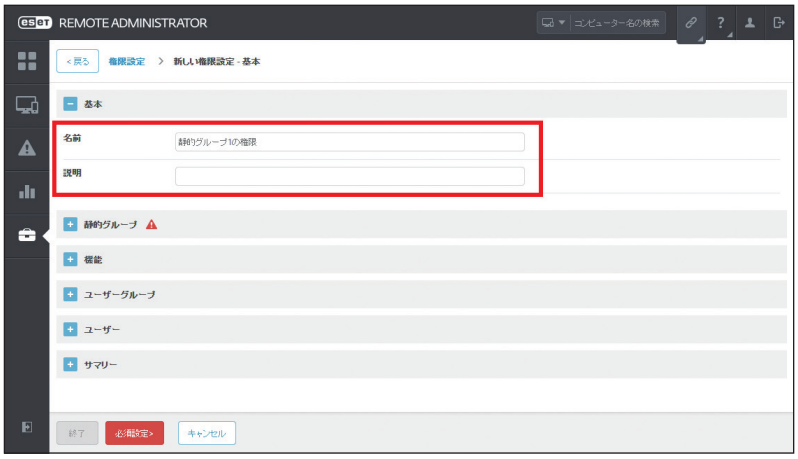
操作手順

1. ［管理］メニューをクリックします。
2. ［アクセス権］サブメニューをクリックします。
3. ［権限設定］をクリックします。
4. ［権限設定］ボタンをクリックします。
5. ［新規作成］を選択します。



「新しい権限設定」画面が表示されます。

6. 「基本」の各項目を入力します。

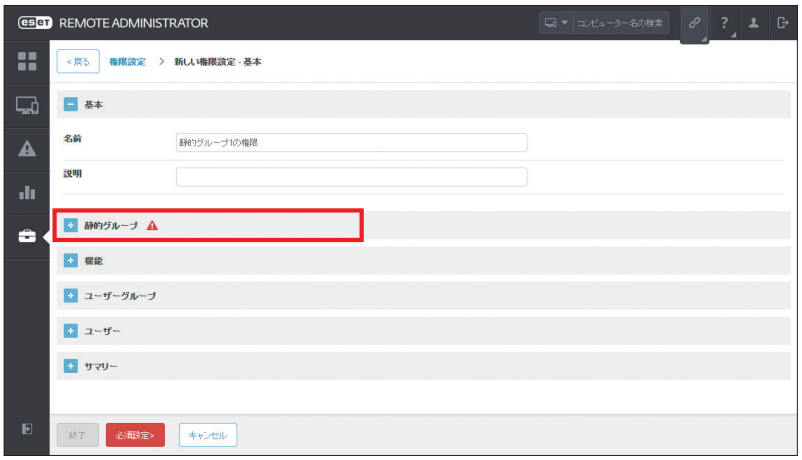


続く

■基本

項目名	説明	必須
名前	作成する権限設定の名前を入力します。画面には、ここで設定した名前が表示されます。	○
説明	作成する権限設定の説明を入力します。	-

7 [静的グループ] をクリックします。



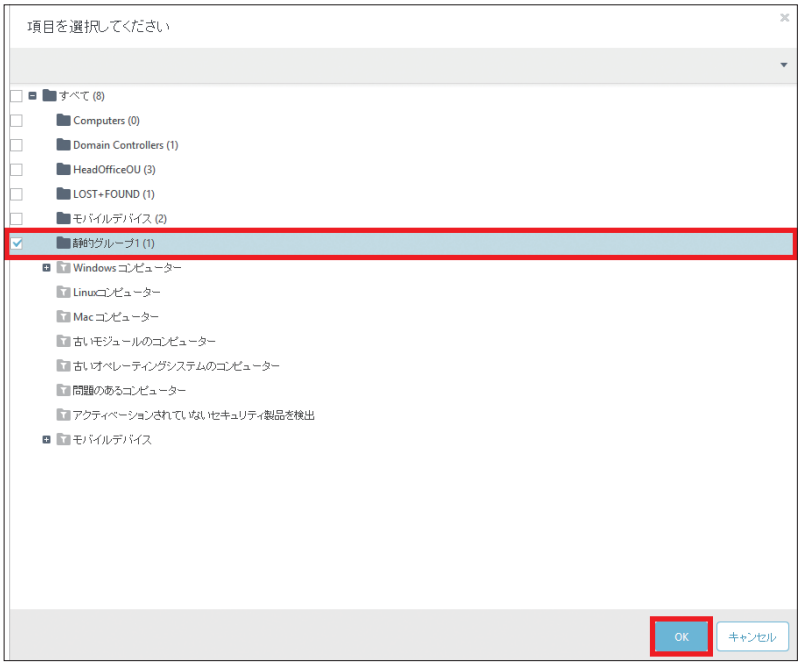
「新しい権限設定 - 静的グループ」画面が表示されます。

8 [静的グループの追加] をクリックします。

「項目を選択してください」画面が表示されます。

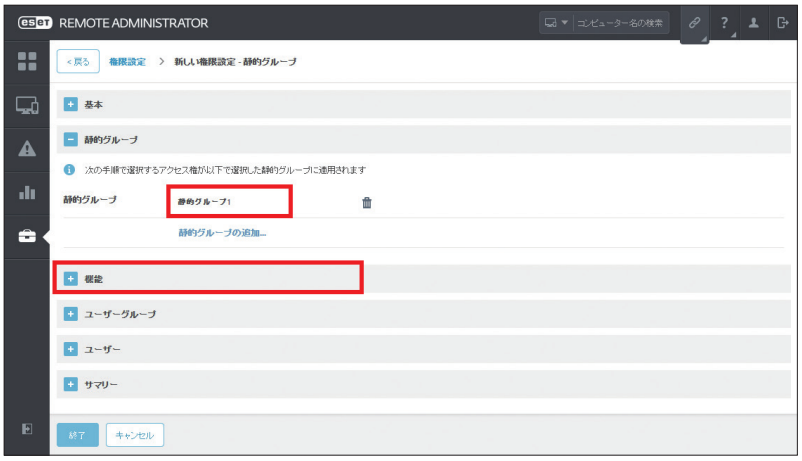
続く

9 権限を設定を行う静的グループを選択し、［OK］ボタンをクリックします。



「新しい権限設定 - 静的グループ」画面に戻ります。

10 手順 9 で選択した静的グループが登録されます。［機能］をクリックします。



「新しい権限設定 - 機能」画面が表示されます。

続く

⑪「付与された機能」の該当する機能オプションにチェックを入れます。

ワンポイント

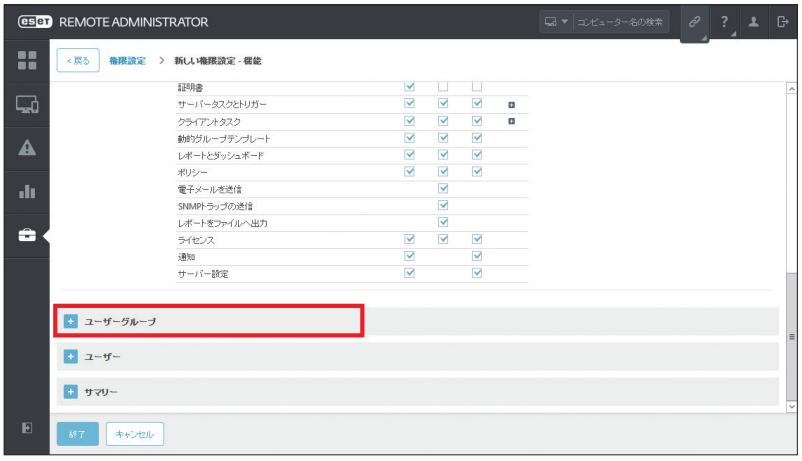
「すべての機能」の［すべての機能への読み取り専用機能を付与］は、全オプションの「読み取り」をオンにします。［すべての機能へのフルアクセスを付与］は、全オプションの「読み取り」と「使用」「書き込み」をオンにします。

■機能

項目名	説明		必須
すべての機能	「付与された機能」の表からすべてのオプションを選択、解除します。		-
	アクセスのクリア	すべてのオプションの選択を解除します。	-
	すべての機能への読み取り専用権限を付与	「読み取り」のすべてのオプションを選択します。	-
	すべての機能へのフルアクセスを付与	「読み取り」と「使用」「書き込み」のすべてのオプションを選択します。	-
付与された機能	ユーザーがアクセスできる個別機能のリストです。		○
	読み取り	選択したオプションの読み取り専用アクセス権を付与します。	-
	使用	選択したオプションの実行、付与、取り消し権を付与します。自動的に「読み取り」機能も付与されます。	-
	書き込み	選択したオプションのフルアクセス権を付与します。自動的に「読み取り」機能も付与されます。	-

続く

⑫ [ユーザーグループ] をクリックします。



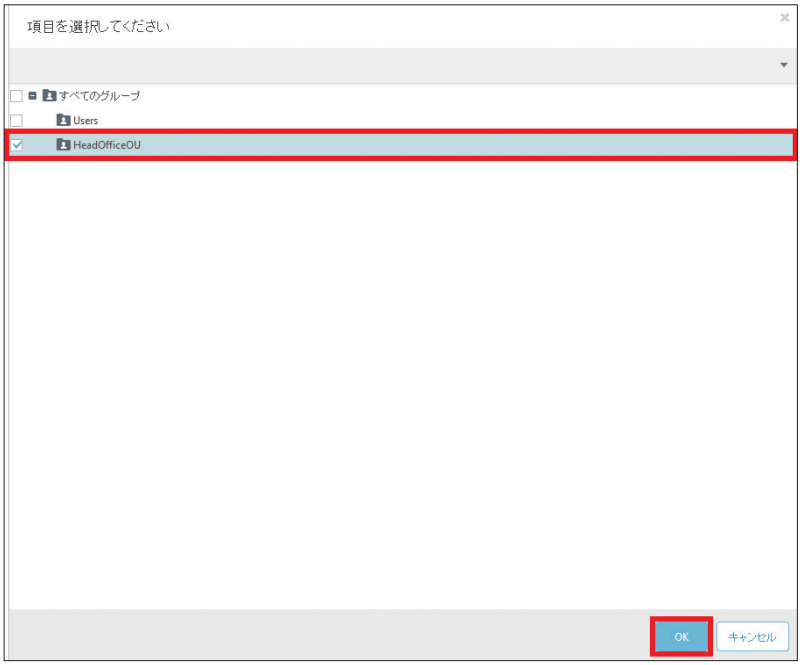
「新しい権限設定 - ユーザーグループ」画面が表示されます。

⑬ 特定のユーザーグループに権限を付与したいときは、[ユーザーグループの追加] をクリックします。

「項目を選択してください」画面が表示されます。

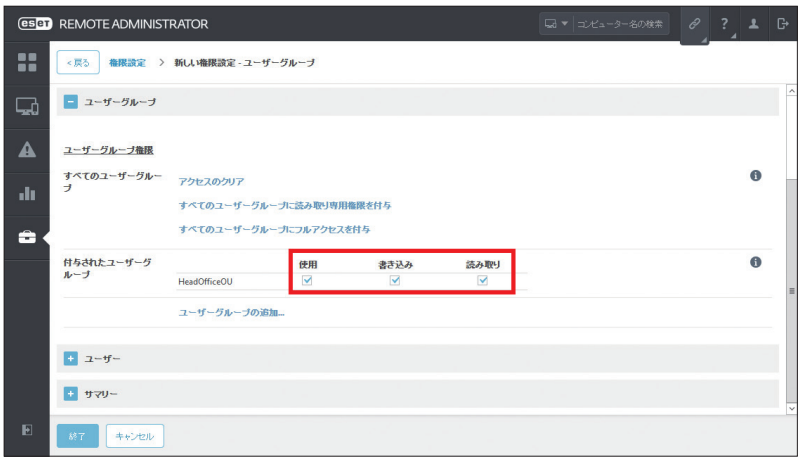
続く

14 権限を付与したいユーザーグループを選択し、［OK］ボタンをクリックします。



「新しい権限設定 - ユーザーグループ」画面に戻ります。

15 手順 14 で選択したグループが登録されます。［使用］［書き込み］［読み取り］の中からグループに付与する権限をオンにします。



続く

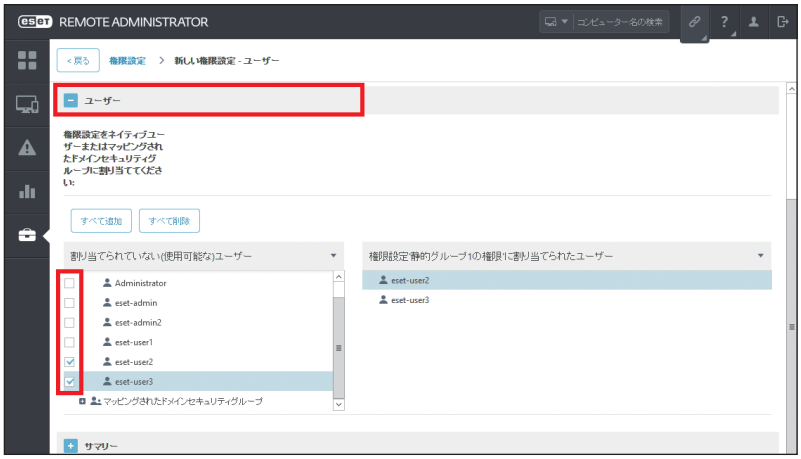
■ユーザーグループ

項目名	説明		必須
すべてのユーザーグループ	「付与されたユーザーグループ」の表からすべてのオプションを選択、解除します。		-
	アクセスのクリア	すべてのオプションの選択を解除します。	-
	すべてのユーザーグループに読み取り専用権限を付与	「読み取り」のすべてのオプションを選択します。	-
	すべてのユーザーグループにフルアクセスを付与	「使用」「書き込み」「読み取り」のすべてのオプションを選択します。	-
付与されたユーザーグループ	ユーザーグループがアクセスできる個別機能のリストです。		○
	使用	実行権限を付与します。	-
	書き込み	書き込みと読み取り権限を付与します。	-
	読み取り	読み取り権限のみを付与します。	-

16 [ユーザー] をクリックします。

17 「割り当てられていない（使用可能な）ユーザー」から権限を割り当てるユーザーまたはドメインセキュリティグループにチェックを入れます。

右側の欄に追加されます。



続く

■ユーザー

項目名	説明	必須
すべて追加	「割り当てられていない（使用可能な）ユーザー」のすべてのユーザーとマッピングされたドメインセキュリティグループを選択します。	-
すべて削除	「割り当てられていない（使用可能な）ユーザー」のすべてのユーザーとマッピングされたドメインセキュリティグループを解除します。	-
割り当てられていない（使用可能な）ユーザー	権限設定を割り当てるユーザーまたはマッピングされたドメインセキュリティグループを選択します。	○

18 ［サマリー］をクリックします。

「基本」、「機能」、「静的グループ」、「ユーザー」に入力した内容が、読み取り専用の状態で表示されます。構成を見直し、正しいことを確認します。変更が必要な場合は、各項目の入力欄で変更します。

19 ［終了］ボタンをクリックします。

「権限設定」画面の権限設定リストに、作成した権限設定が表示されます。

ワンポイント

権限の「使用」はポリシーを実行する権限、「書き込み」は編集や新規作成、削除などを行える権限です。たとえば、管理者がユーザー A に共有ポリシーグループのポリシーを修正することを許可しない場合は、次の権限設定を作成します。

・機能ポリシー：読み取りおよび使用権限を選択します
・静的グループ：共有ポリシー

これらの権限がユーザー A に割り当てられると、ユーザー A はこれらのポリシーを実行できますが、編集、新規作成、削除はできません。管理者が書き込み権限を追加する場合、ユーザー A は選択した静的グループ (共有ポリシー) 内のポリシーを新規作成、複製、編集、削除できます。

6.10.2.3 新しく作成した権限設定の割り当て

既に権限設定を割り当ててあるユーザーに、新しく作成した権限設定を追加で割り当てる場合は、ローカルユーザーを編集します。

操作手順

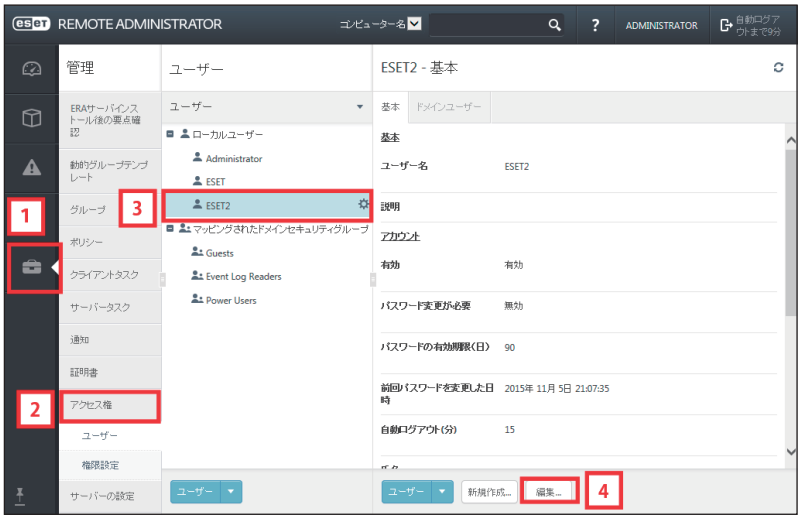
1 ［管理］メニューをクリックします。

2 ［アクセス権］サブメニューをクリックします。

3 権限設定を追加するユーザーまたはドメインセキュリティグループを選択します。

続く

4 [編集] ボタンをクリックします。

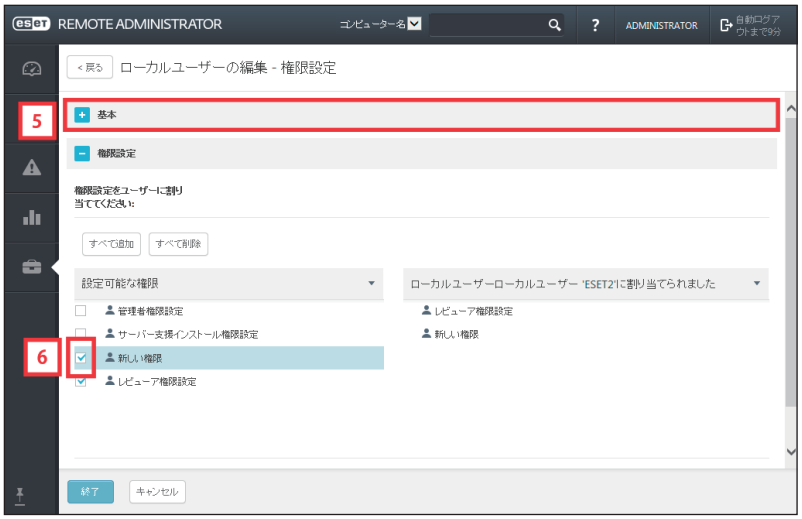


「ローカルユーザーの編集」画面が表示されます。

5 [権限設定] をクリックします。

6 「設定可能な権限」から追加で割り当てる権限設定を選択します。

右側の欄に追加されます。



7 [終了] ボタンをクリックします。

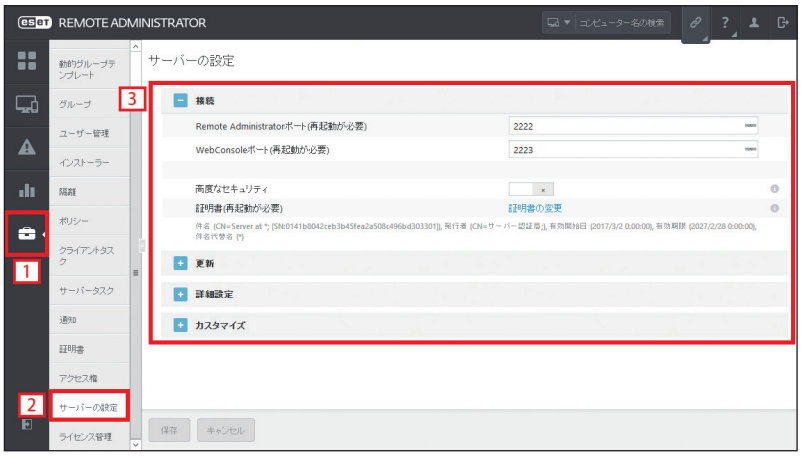
選択したユーザーに指定した権限設定が割り当てられます。

6.11　サーバーの設定

ESET Remote Administrator サーバーの設定を行います。

操作手順

1. ［管理］メニューをクリックします。
2. ［サーバーの設定］サブメニューをクリックします。
3. 各項目を入力します。



■接続

項目名	説明	必須
Remote Administrator ポート（再起動が必要）	ESET Remote Administrator サーバーと ERA エージェント間の接続用のポート番号を入力します。設定を反映させるためには、ERA サーバープロセスの再起動が必要になります。	○
Web Console ポート（再起動が必要）	ERA Web コンソールと ERA サーバー間の接続用のポート番号を入力します。設定を反映させるためには、ERA サーバープロセスの再起動が必要になります。	○
高度なセキュリティ	この設定を有効にすると、ERA サーバーに最新の TLS と新しく作成された認証局と証明書を使用し、SHA-2 を使用することができます。ただし、これにより、古いシステムとの互換性がなくなる場合があります。	-
証明書（再起動が必要）	［証明書の変更］をクリックし、ERA サーバーで使用する ERA サーバー証明書を選択します。 証明書を反映させるためには、ERA サーバープロセスの再起動が必要になります。	○

続く

■更新

項目名	説明	必須
アップデート間隔	ERA サーバーが使用するコンポーネントをアップデートする間隔を設定します。 ［間隔の変更］をクリックし、アップデートを受信する間隔として「定期間隔」または「CRON 式」を選択します。	○
アップデートサーバー	ERA サーバーが使用するコンポーネントのアップデートサーバーを入力します。 ※既定値は「AUTOSELECT」が入力されています。	○
アップデートの種類	次の 3 種類から選択します。 ［通常アップデート］　：一般公開されたアップデート ［テストモード］　　：テスト用として事前に公開されるアップデート ［遅延アップデート］　：公開されてから 12 時間以上経過しているアップデートで最新のもの ※本番環境でのテストモードの使用は推奨しません。	○

続く

■詳細設定

詳細設定
HTTPプロキシ
プロキシサーバを使用
ホスト
192.168.1.2
ポート
3128
ユーザー名
パスワード
パスワードの表示
HTTPプロキシが使用できない場合は直接接続を使用する
ウェイクアップ
UDPv4ポート
1237
UDPv6ポート
1238
SMTPサーバ
SMTPサーバーを使用
ホスト
192.168.1.2
ポート
25
ユーザー名
admin
パスワード
パスワード変更
接続セキュリティタイプ
保護されていません
認証タイプ
自動
送信元アドレス
admin@example.com
SMTPサーバーのテスト
テストメールの送信
指定したSMTPサーバー経由でテスト電子メールが送信されます。
SYSLOGサーバー
Syslogサーバーを使用する
ホスト
ポート
514
書式
BSD
転送
UDP
オクテットカウントフレーミング
静的グループ
検出されたコンピューターを自動的に組み合わせる
検出されたコンピューターと静的グループに既に存在するコンピューターとの自動ペアリングを有効にします。ペアリングはエージェント別に報告されたホスト名で動作し、信頼できない場合は無効にしてください。ペアリングが失敗すると、コンピューターは「LOST+FOUND」グループに配置されます。
リポジトリ
サーバー
AUTOSELECT
診断
クラッシュレポートを自動的にESETに送信
ロギング
トレースログの詳細レベル
警告
ログをSyslogにエクスポートする
エクスポートされたログ形式
JSON
データベースのクリーンアップ
次の時間が経過したログを消去
6
ヶ月
カスタマイズ

続く

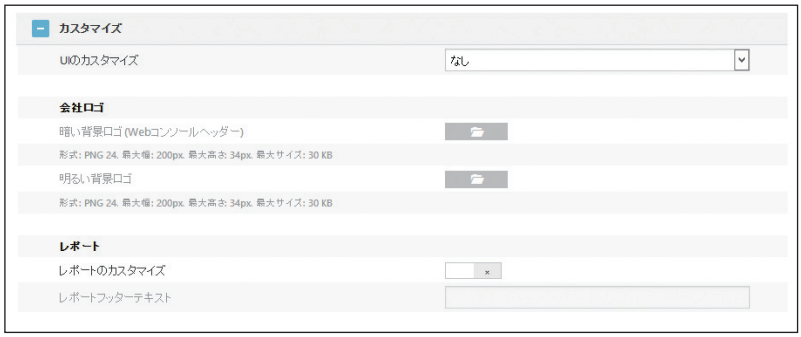
項目名	説明	必須
HTTP プロキシ	ERA サーバーが HTTP プロキシ経由でインターネットに接続する場合に設定します。 使用しない場合、HTTP プロキシの設定は不要です。	○
ウェイクアップ	ウェイクアップコールを送信するときに使用する UDP ポート番号を入力します。 ※「ウェイクアップ」の UDP ポート番号については、当該一覧下のワンポイントを参照してください。	○
SMTP サーバー	SMTP サーバーの使用有無を選択します。SMTP サーバーを使用すると、E メールによる通知を行うことができます。	○
SYSLOG サーバー	ESET Remote Administrator から通知とイベントメッセージを Syslog サーバーに送信する場合に使用します。 （ESET Remote Administrator 6.3 以降で利用可能） Syslog サーバーの IP アドレスまたはホスト名とポートを設定します。 プロトコルは「UDP」、ファシリティは「user」で Syslog が送信されます。	○
静的グループ	検出されたコンピューターと静的グループのコンピューターとの自動組み合わせを有効にします。組み合わせは ERA エージェントで報告されたホスト名で動作します。信頼できない場合は無効にしてください。組み合わせに失敗すると、コンピューターは LOST+FOUND グループに入ります。	○
リポジトリ	ESET 製品のインストールファイルが格納されているリポジトリの URL を入力します。 ※既定値は「AUTOSELECT」が入力されています。 特別な理由がない限り変更しないでください。	○
診断	ESET へのクラッシュレポートの自動送信の有無を選択します。 ※既定値はクラッシュレポートの自動送信が有効になっています。	○
ロギング	トレースログの詳細レベルを選択します。ログの詳細を設定して収集されログに記録する情報のレベル、トレース（情報）から致命的（最重要情報）までを決定することができます。 また、ログを Syslog サーバーに送信するかどうかを設定します。 （ESET Remote Administrator 6.3 以降で利用可能） 有効にした場合に、ウイルス検出のイベント、ファイアウォールのイベント、HIPS のイベント（ログレベルが Error、Citical、Fatal のイベントのみ）が JSON 形式で Syslog サーバーに送信されます。	○
データベースのクリーンアップ	定期的にデータベースのログをクリーンアップする期間を入力します。データベースの過負荷を防止するために、定期的にログをクリーンアップします。	○

ワンポイント

「ウェイクアップ」の UDP ポート番号
ウェイクアップコールは、任意の指定された ERA エージェントが即時に ERA サーバーへ接続させるために使用します。
ERA エージェントはウェイクアップコールのために設定された UDP ポートでブロードキャストをリスニングします。そのため、ウェイクアップコールが動作するには、ファイアウォールによってこのブロードキャストが遮断されてはなりません。
また、一部のシステムでは UDPv4 ポートと UDPv6 ポートが同じ場合、ウェイクアップが想定とおりに動作しないため、2 つのポートを別のポートにすることを推奨します。

続く

■カスタマイズ



項目名	説明		必須
UI のカスタマイズ	カスタムロゴを ERA Web コンソールと、サーバータスクで生成されたレポートに追加できます。次の 3 種類から選択できます。		-
	［なし］	基本デザイン、カスタムロゴなし	-
	［コブランディング］	Web コンソールとレポートのフッターにカスタムロゴを追加できます。	-
	［ホワイトラベリング (MSP ライセンスが必要)］	Web コンソールとレポートのフッターまたはヘッダーにカスタムロゴを追加できます。	-
会社ロゴ	UI のカスタマイズで、［なし］以外を選択しているときに設定できます。		-
	［暗い背景ロゴ (Web コンソールヘッダー)］	このロゴは Web コンソールの左上端に表示されます。 をクリックすると、ロゴのファイルを選択できます。	-
	［明るい背景ロゴ］	このロゴは、ヘッダー (MSP ライセンス所有者) またはサーバータスクで生成されたレポートのフッター (コブランディング設定) に表示されます。 をクリックすると、ロゴのファイルを選択できます。	-
レポートのカスタマイズ	有効に設定すると、PDF 形式で生成されたレポートの右下端に追加されるレポートフッターテキストに任意の文字列を追加できます。追加する文字列は、「レポートフッターテキスト」の入力欄に入力します。		-

4 ［編集］ボタンをクリックします。

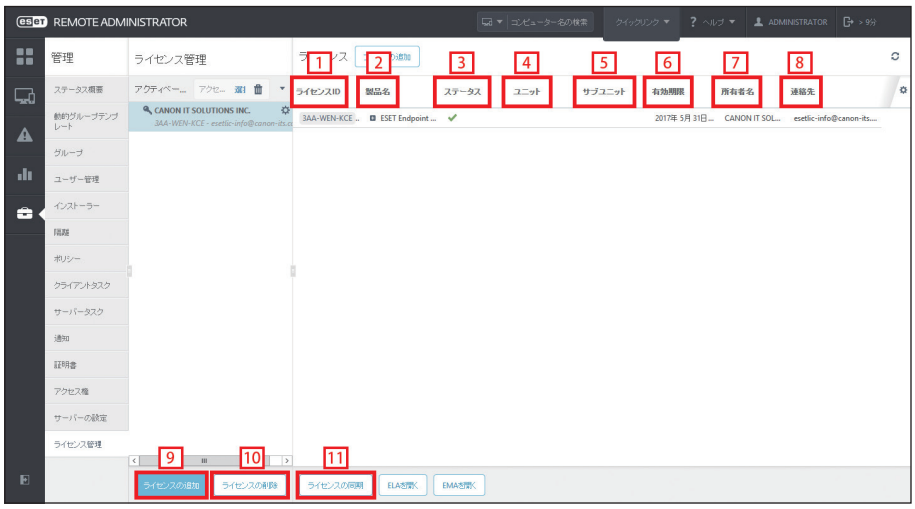
サーバーの設定が保存されます。

6.12　ライセンス管理

ESET Remote Administrator では、ESET 製品が利用するライセンスを管理することができます。
ライセンス管理を行えるのは、アクセス権の権限設定（「6.10.2　権限設定」参照）でライセンスの書き込み／実行権限が付与されているユーザー（「6.10.1.2　新しいローカルユーザーの作成」参照）のみとなります。

6.12.1　ライセンス管理画面の構成

「ライセンス管理」画面の構成について説明します。



1	**ライセンス ID**	個別識別に使用するライセンス ID が表示されます。
2	**製品名**	ライセンスの対象となる ESET 製品名が表示されます。
3	**ステータス**	各ライセンスの現在の状況が表示されます。 有効期限切れや使用超過の危険性がある場合、マウスポインターを合わせると、警告メッセージが表示されます。
4	**ユニット**	このライセンスでアクティベーションできる単位数と、オフライン単位数が表示されます。
5	**サブユニット**	ESET サーバー製品のサブ単位数（メールボックス、ゲートウェイ保護、接続）が表示されます。
6	**有効期限**	ライセンスの有効期限が表示されます。
7	**所有者名**	ライセンス所有者の名称が表示されます。
8	**連絡先**	所有者の連絡先メールアドレスが表示されます。
9	**ライセンスの追加**	新しいライセンスの追加と、アクティベーションを行います。画面の詳細は「6.12.2　アクティベーション」を参照してください。
10	**ライセンスの削除**	選択しているライセンスを完全に削除します。ライセンスを削除しても、ESET 製品のアクティベーションは、解除されません。
11	**ライセンスの同期**	現在のライセンス状況を反映させます。 ERA サーバーは 1 日 1 回ライセンスの同期を行っています。

! 重　要

期限切れのライセンスは赤色で表示されます。
ライセンスが最大数まで使用されている、30 日以内に有効期限が切れる場合は、黄色で表示されます。

ワンポイント

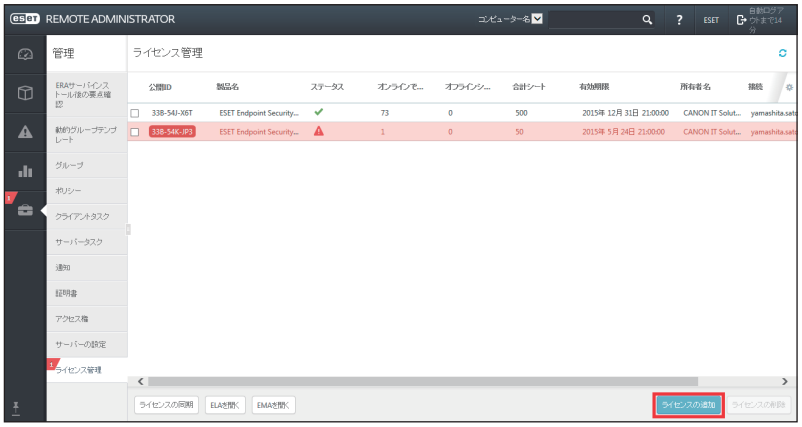
［ELA を開く］ボタンと［EMA を開く］ボタンは日本では使用しません。

6.12.2　アクティベーション

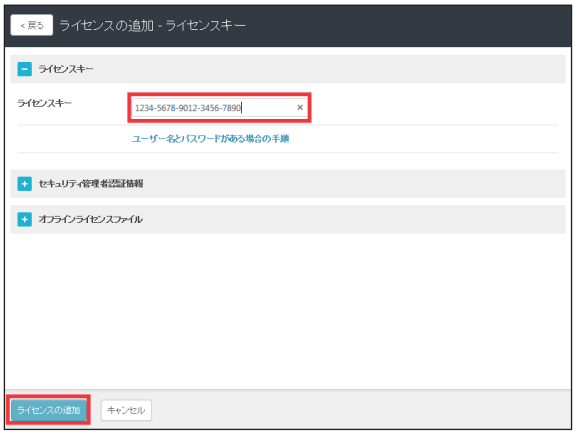
製品認証キーを使用して、アクティベーションを行います。
同様の操作で、新しいライセンスの追加を行うことができます。

操作手順

1 ［ライセンスの追加］ボタンをクリックします。



2 製品認証キーを入力して［ライセンスの追加］ボタンをクリックします。



■製品認証キー

項目名	説明	必須
製品認証キー	製品認証キーを入力します。 ※［ユーザー名とパスワードがある場合の手順］は、日本では使用しません。	○

■セキュリティ管理者認証情報

日本では使用しません。

■オフラインライセンスファイル

オフラインライセンスファイルは、インターネット接続が行えないオフライン環境のコンピューターのアクティベーションを行うときに利用します。オフラインライセンスファイルは、ユーザーズサイトから ESET License Administrator に移動し入手できます。オフラインライセンスファイルの登録は、［オフラインライセンスファイル］をクリックすることで行えます。

！重　要

ESET Remote Administrator に登録可能なオフラインライセンスファイルを作成するためには、表示されているライセンスファイルトークンの値を ESET Lisence Administrator で入力する必要があります。
オフラインライセンスファイルのダウンロード手順の詳細は以下のサポートページの Q&A を参照してください。
Q&A の URL： http://eset-support.canon-its.jp/faq/show/4327?site_domain=business

ワンポイント

ライセンスは、次の 2 つのタスクを使用して、ERA サーバーから ESET 製品に配布できます。
・ソフトウェアインストールタスク
（「6.6.3.1　ESET セキュリティ製品」の「■ソフトウェアインストール」参照）
・製品アクティベーションタスク
（「6.6.3.1　ESET セキュリティ製品」の「■製品のアクティベーション」参照）
※クライアントタスクの作成については、「6.6.2　新しいクライアントタスクの作成」を参照してください。

続く

Chapter 7 ESET Remote Administrator のコンポーネント設定

7.1 各コンポーネントの設定

セキュリティーポリシー（以下ポリシー）に設定する項目を、各コンポーネント別に説明します。

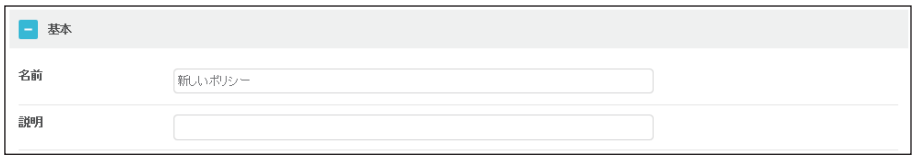
ワンポイント

ここでは、項目の説明だけを記載します。操作については、「6.5.2 新しいポリシーの作成」を参照してください。

7.1.1 ERA エージェントの設定項目

■基本

ポリシーの名前と説明を入力します。



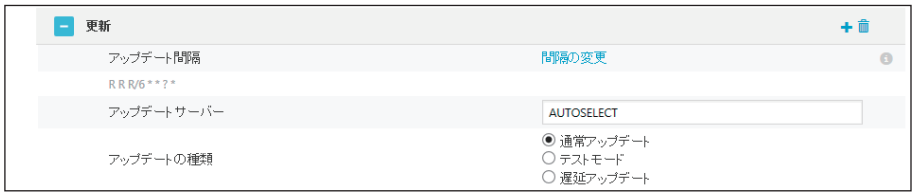
名前	作成するポリシーの名前を設定します。 既定値として「新しいポリシー」が入力されています。
説明	当該ポリシーに対する説明を記入します。適宜入力してください。

■設定

●接続

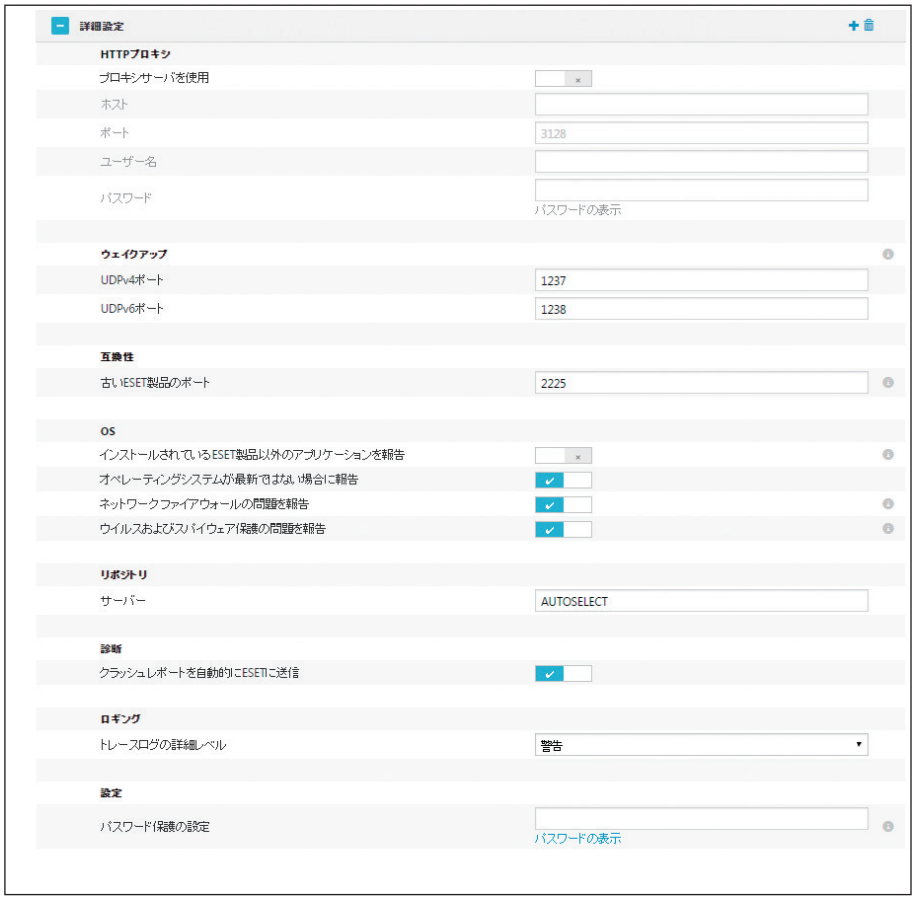
接続先サーバー	ERA エージェントが接続する、ERA サーバーを設定します。複数のサーバーを設定した場合、上位に記載されているサーバーから接続を試みます。「サーバーリストの編集」から設定します。
データ制限	ERA エージェントが、ERA サーバーへ送信するデータの上限サイズを設定します。 「単位」から、KB、MB、GB が選択可能です。
接続間隔	ERA エージェントが、ERA サーバーと行う通信間隔を設定します。 「間隔の変更」から、［定期間隔］または［CRON 式］から設定します。 間隔を短くすると、トラフィックの負荷が高くなります。
証明書	ERA エージェントが、ERA サーバーとの接続に使用する証明書を設定します。 参照しているピア証明書を変更することが可能です。

●更新



アップデート間隔	ERA エージェントが使用するモジュールをアップデートするために、ESET 社のアップデートサーバーとの通信間隔を設定します。 「間隔の変更」から、［定期間隔］または［CRON 式］から設定します。
アップデートサーバー	アップデートサーバーを設定します。 既定値として、「AUTOSELECT」が入力されています。
アップデートの種類	［通常アップデート］（一般公開されたアップデート）、［テストモード］（テスト用として事前に公開されるアップデート）、［遅延アップデート］（公開されてから 12 時間以上経過しているアップデートで最新のもの）から選択します。

●詳細設定


詳細設定
HTTPプロキシ
プロキシサーバを使用
ホスト
ポート
3128
ユーザー名
パスワード
パスワードの表示
ウェイクアップ
UDPv4ポート
1237
UDPv6ポート
1238
互換性
古いESET製品のポート
2225
OS
インストールされているESET製品以外のアプリケーションを報告
オペレーティングシステムが最新ではない場合に報告
ネットワークファイアウォールの問題を報告
ウイルスおよびスパイウェア保護の問題を報告
リポジトリ
サーバー
AUTOSELECT
診断
クラッシュレポートを自動的にESETに送信
ロギング
トレースログの詳細レベル
警告
設定
パスワード保護の設定
パスワードの表示

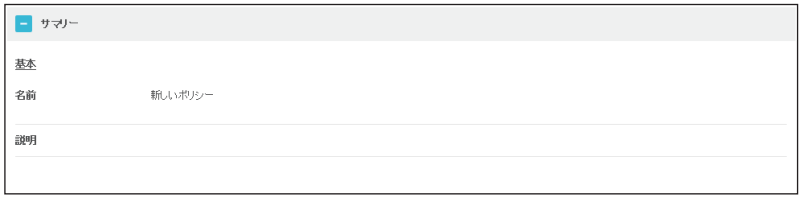
HTTP プロキシ	プロキシサーバーを使用	ERA エージェントが、HTTP プロキシ経由でインターネットに接続する場合に設定します。 使用しない場合、以下 HTTP プロキシサーバーの設定は不要です。
	ホスト	HTTP プロキシサーバーの IP アドレス、またはホスト名を設定します。
	ポート	ERA エージェントが、プロキシサーバーとの接続で使用するポートを設定します。 既定値「3128」が入力されています。
	ユーザー名	HTTP プロキシ認証が必要な場合、ユーザー名を設定します。
	パスワード	HTTP プロキシ認証が必要な場合、パスワードを設定します。
ウェイクアップ	UDPv4 ポート	ERA サーバーから任意の ERA エージェントに対して、「ウェイクアップコールの送信」を行う時に使用するポートを設定します。 既定値「1237」が入力されています。
	UDPv6 ポート	ERA サーバーから任意の ERA エージェントに対して、「ウェイクアップコールの送信」を行う時に使用するポートを設定します。 既定値「1238」が入力されています。
互換性	古い ESET の製品ポート	バージョン 5 以前の ESET 製品を ESET Remote Administrator で管理する場合に、ERA エージェントがバージョン 5 以前の ESET 製品からの通信を待ち受けするポートを設定します。 既定値「2225」が入力されています。
OS	インストールされている ESET 製品以外のアプリケーションを報告	インストール済みアプリケーション一覧に、ESET 製品だけでなく、すべてのインストール済製品を表示させる場合に設定します。 既定で無効になっています。 UNIX システムの場合、本設定は無効となります。
	オペレーティングシステムが最新ではない場合に報告	オペレーティングシステムが最新ではない場合、コンピューター詳細のアラートへ表示する場合に設定します。 既定で有効になっています。
	ネットワークファイアウォールの問題を報告	Windows SecurityCenter の情報に基づき、ファイアウォールに問題がある場合、コンピューター詳細のアラートへ表示場合に設定します。 既定で有効になっています。
	ウイルスおよびスパイウェア保護の問題を報告	Windows SecurityCenter の情報に基づき、ウイルスおよびスパイウェア保護の問題がある場合、コンピューター詳細のアラートに表示する設定です。 既定で有効になっています。
リポジトリ	サーバー	すべてのインストールファイルが格納されている、リポジトリサーバーを設定します。既定値「AUTOSELECT」が入力されています。変更時には、URL アドレス形式で記載できます。
診断	クラッシュレポートを自動的に ESET に送信	クラッシュレポートを、自動的に ESET へ送信を行う場合に設定します。 既定で有効になっています。
ロギング	トレースログの詳細レベル	ERA エージェントが、ファイルに出力するログ情報レベルを設定できます。 既定では［警告］が選択されています。
設定	パスワード保護の設定	ERA エージェントをアンインストールする場合に、ここで設定したパスワードを要求するように設定できます。なお、Windows のコンピューターにのみ有効です。 （ESET Remote Administrator 6.3 以降で利用可能）

■割り当て

当該ポリシーを割り当てる対象をグループ、コンピューターから選択して設定します。

■サマリー

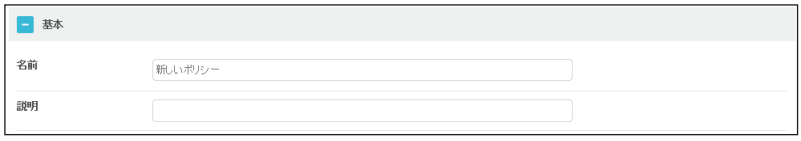
それぞれの項目の設定値が表示されます。



7.1.2 ERA プロキシの設定項目

■基本

ポリシーの名前と説明を入力します。



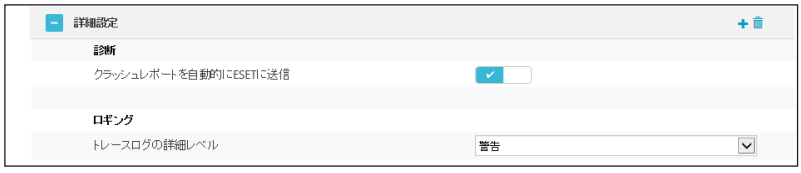
名前	作成するポリシーの名前を設定します。 既定値として「新しいポリシー」が入力されています。
説明	当該ポリシーに対する説明を記入します。適宜入力してください。

■設定

●接続

Remote Administrator ポート（再起動が必要）	ERA プロキシが、ERA サーバーと接続する場合に使用するポートを設定します。 既定値「2222」が入力されています。
接続先サーバー	ERA プロキシが、接続する ERA サーバーを設定します。複数サーバーを設定した場合、上位に記載されているサーバーから接続を試みます。「サーバーリストの編集」から選択します。
データ制限	ERA プロキシが、ERA サーバーへ送信するデータ上限サイズを設定します。 「単位」から、KB、MB、GB が選択可能です。
接続間隔	ERA プロキシが、ERA サーバーと行う通信間隔を設定します。 「間隔の変更」から、［定期間隔］または［CRON 式］から設定します。 間隔を短くすると、トラフィックの負荷が高くなります。
証明書	ERA プロキシが、ERA サーバーとの接続に使用する証明書を設定します。 参照しているピア証明書を、変更することが可能です。

●詳細設定



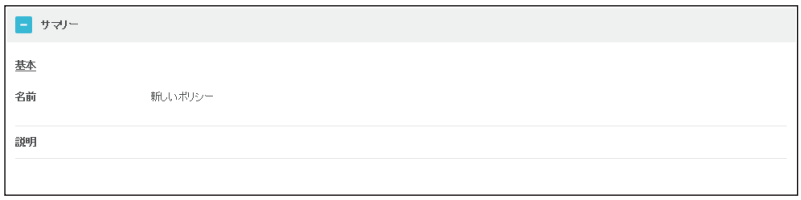
診断	クラッシュレポートを自動的に ESET に送信	クラッシュレポートを、自動的に ESET へ送信を行う場合に設定します。 既定で有効になっています。
ロギング	トレースログの詳細レベル	ERA プロキシが、ファイルに出力するログ情報レベルを設定できます。 既定で［警告］が選択されています。

■割り当て

当該ポリシーを割り当てる対象を、グループ、コンピューターから選択して設定します。

■サマリー

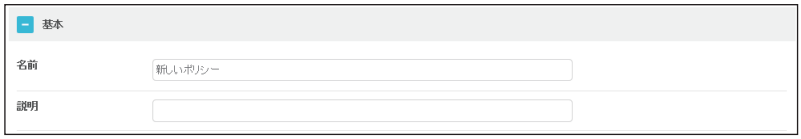
それぞれの項目の設定値が表示されます。



7.1.3 RD Sensor の設定項目

■基本

ポリシーの名前と説明を入力します。



名前	作成するポリシーの名前を設定します。 既定値として「新しいポリシー」が入力されています。
説明	当該ポリシーに対する説明を記入します。適宜入力してください。

■設定

●フィルタ

IPV4 フィルタ	IPv4 アドレスフィルタリングを有効にする	「ホワイトリスト」に含まれる IP アドレス、または「ブラックリスト」に含まれない IP アドレスを検出したい場合、有効にします。 既定でオフになっています。 無効の場合、以下 IPv4 の設定は不要です。
	フィルタ	有効にしたいフィルタリストを［ホワイトリスト］または［ブラックリスト］から選択します。
	IPV4 アドレスリスト	「フィルタ」で選択した項目のリストを作成します。
MAC アドレスプレフィックスフィルタ	MAC アドレスプレフィックスフィルタリングを有効にする	「ホワイトリスト」に含まれる MAC アドレス、または「ブラックリスト」に含まれない MAC アドレスを検出したい場合、有効にします。 既定でオフになっています。 無効の場合、以下 MAC アドレスの設定は不要です。
	フィルタリングモード	有効にしたいフィルタリストを、［ホワイトリスト］または［ブラックリスト］から選択します。
	MAC アドレスプレフィックスリスト	「フィルタ」で選択した、項目のリストを作成します。 ［MAC アドレスプレフィックスリストの編集］から選択します。

●検出

アクティブな検出	アクティブな IPv4 コンピューターを検出を有効にする	ローカルネットワークで OS がアクティブな状態のコンピューターを検出する場合、有効にします。 既定でオフになっています。 有効にすると一部のコンピューターで、ファイアウォール警告が発生する場合があります。
	アクティブな IPv6 コンピューターを検出を有効にする	ローカルネットワークで OS がアクティブな状態のコンピューターを検出する場合、有効にします。 既定でオフになっています。 有効にすると一部のコンピューターで、ファイアウォール警告が発生する場合があります。
OS 検出ポート	IPv4 検出ポート	OS がアクティブな状態であるか検出するときに、使用するポートを設定します。 ［IPv4 ポートリストの編集］で設定します。
	IPv6 検出ポート	OS がアクティブな状態であるか検出するときに、使用するポートを設定します。 ［IPv6 ポートリストの編集］で設定します。

●詳細設定

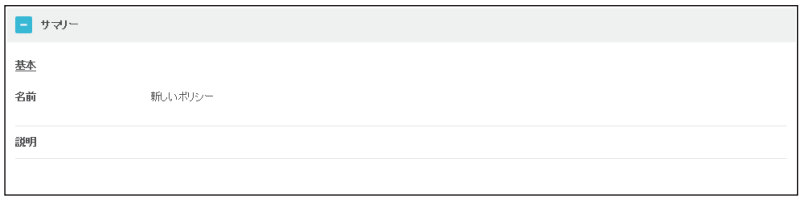
診断	クラッシュレポートを自動的に ESET に送信	クラッシュレポートを、自動的に ESET へ送信を行う場合に設定します。既定で有効になっています。

■割り当て

当該ポリシーを割り当てる対象をグループ、コンピューターから選択して設定します。

■サマリー

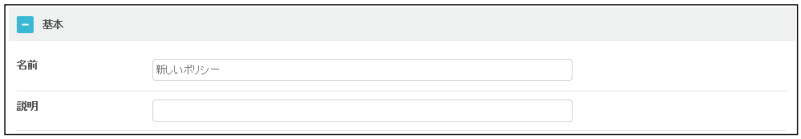
それぞれの項目の設定値が表示されます。



7.1.4 Mobile Device Connector の設定項目

■基本

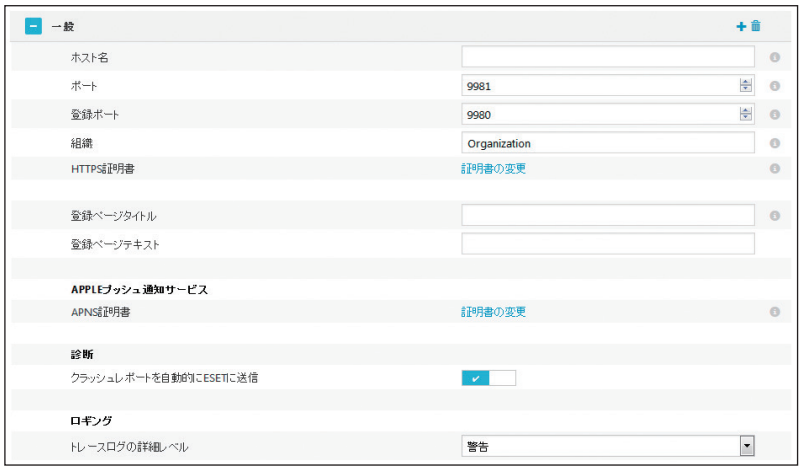
ポリシーの名前と説明を入力します。



名前	作成するポリシーの名前を設定します。 既定値として「新しいポリシー」が入力されています。
説明	当該ポリシーに対する説明を記入します。適宜入力してください。

■設定

●一般

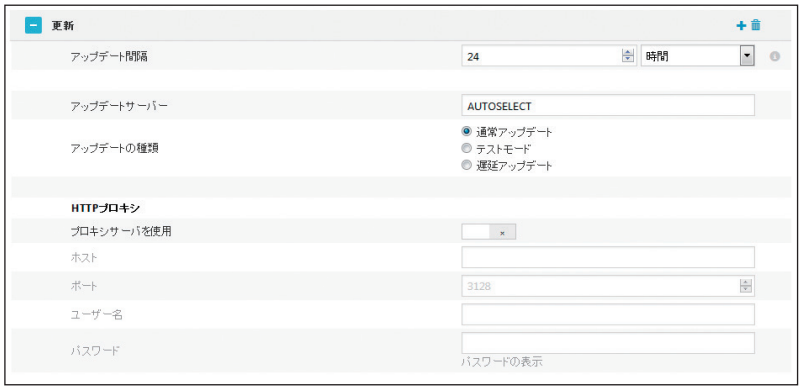


ホスト名	Mobile Device Connector サーバーのホスト名または IP アドレスを設定します。
ポート	Mobile Device Connector サーバーのポートを設定します。
登録ポート	モバイルデバイス登録で使用されるポートを設定します。
組織	登録証明書生成の組織名を設定します。
HTTPS 証明書	安全な TLS 接続と認証には証明書が必要です。HTTPS サーバー証明書は、デバイスが不正なサーバーに接続しないことを保証するために使用されます。
登録ページタイトル	デバイスに表示される登録ページのタイトルを設定します。
登録ページテキスト	デバイスに表示される登録ページのテキストを設定します。
APNS 証明書	通知を iOS デバイスに送信するには、APNS 証明書が必要です。Mobile Device Connector に Apple が署名した有効な APNS 証明書が無い場合は、iOS デバイスの登録は行えません。
クラッシュレポートを自動的に ESET に送信	有効にすると異常終了などのレポートを自動的に ESET へ送信します。
トレースログの詳細レベル	トレースログの詳細レベルを選択します。

●エージェント

接続先サーバー	エージェントの接続先 ERA サーバーを設定します。
データ制限	データ送信用の最大優先バイト数を設定します。優先度の高いログはこの制限を無視しますが、カウントはされます。この設定値が小さすぎると、ログが送信されない場合があります。
接続間隔	サーバーまたはプロキシとの接続間隔を設定します。
証明書	安全な TLS 接続と認証には証明書が必要です。プロキシ証明書は、プロキシとサーバーによって不正なプロキシが拒否されることを保証するために使用されます。

●更新



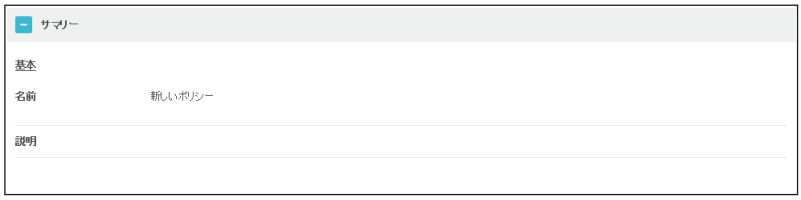
アップデート間隔	アップデート間隔を設定します。
アップデートサーバー	アップデートサーバーを設定します。
アップデートの種類	アップデートの種類を選択します。
プロキシサーバを使用	プロキシサーバーを使用する場合、有効にします。
ホスト	プロキシサーバーのホスト名または IP アドレスを設定します。
ポート	プロキシサーバーのポートを設定します。
ユーザー名	プロキシサーバーに接続するための認証情報（ユーザー名）を設定します。
パスワード	プロキシサーバーに接続するための認証情報（パスワード）を設定します。

■割り当て

当該ポリシーを割り当てる対象をグループ、コンピューターから選択して設定します。

■サマリー

それぞれの項目の設定値が表示されます。



Chapter 8 その他

8.1 診断ツール

診断ツールは、各コンポーネントの使用履歴を収集しログファイルを作成します。ログファイルは圧縮されて指定したフォルダーへ保存されます。
診断ツールは、コンポーネントの問題を解決するために使用します。

指定できる診断ツールの機能は次の 4 種類です。

1. ダンプログ	すべての履歴を log ファイルとして Logs フォルダーに保存します。
2. ダンプ処理	ダンプ処理を行い、dump ファイルを Dumps フォルダーに保存します。
3. アプリケーション情報の取得	製品名と製品バージョンを GeneralApplicationInformation フォルダーに保存します。
4. 環境設定の取得	構成情報などを Configuration フォルダーに保存します。

ワンポイント

「2. ダンプ処理」を実行する場合は、各コンポーネント（ERA サーバー、ERA プロキシ、ERA エージェント、RD Sensor、ファイルサーバー）が実行中でなければなりません。

診断ツールは Windows 版と Linux 版のすべての ERA コンポーネントに含まれています。
システム環境に合わせたファイルを実行してください。

診断ツールの実行ファイルとそのフォルダパスは次のとおりです。

	実行ファイル	フォルダパス
Windows	Diagnostic.exe	C:¥Program Files¥ESET¥RemoteAdministrator¥ Server
Linux	Diagnostic Server	/opt/eset/RemoteAdministrator/ Server

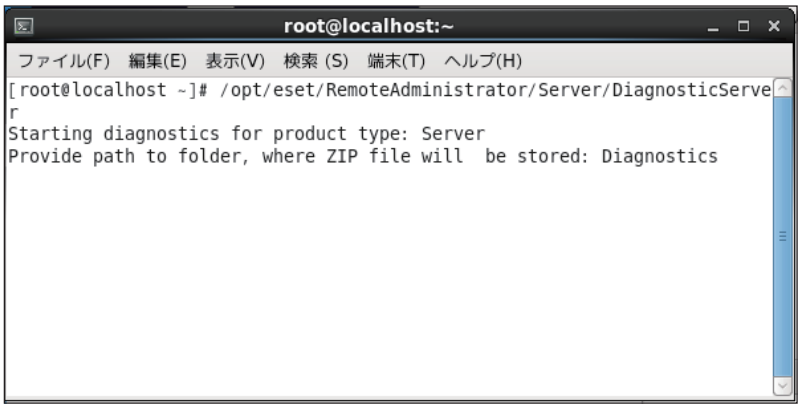
※網掛け部分はコンポーネントで変わります。該当コンポーネントに適宜変更してください。

操作手順

1 診断ツールを起動します。

Windows　：Diagnostic.exe をダブルクリックします。
Linux　　：ターミナルを開き、DiagnosticServer を起動します。
コマンド　：/opt/eset/RemoteAdministrator/Server/DiagnosticServer
指定したコンポーネントの診断ツールが起動します。

2 作成されるログファイルおよび圧縮ファイルを保存する任意のフォルダーを指定します。



※画面は Linux です

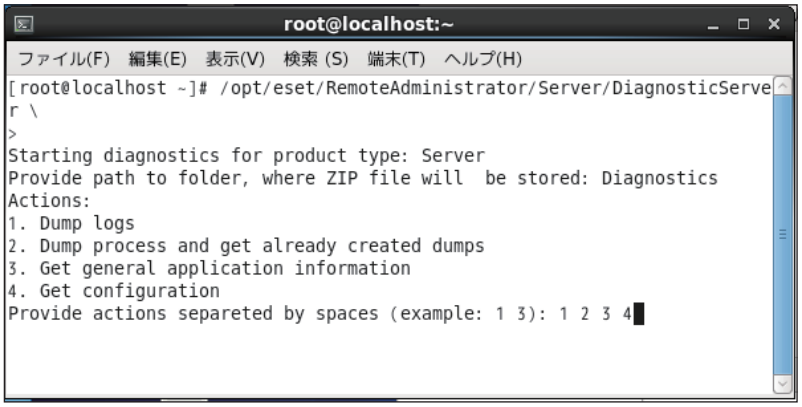
ワンポイント

指定したフォルダーが存在しない場合は、そのフォルダーが次の場所に新規作成されます。
Windows：診断ツールが保存されているフォルダー
Linux　　：root フォルダー
既存のフォルダーの場合は、フォルダーパスを指定してください。指定したフォルダーの中にログファイルおよび zip ファイルが書き込まれます。

4 つの機能が表示されます。

3 実行する機能を指定します。

1 つまたは複数の機能を指定することが可能です。その場合は、スペースで区切ってください。



※画面は Linux です

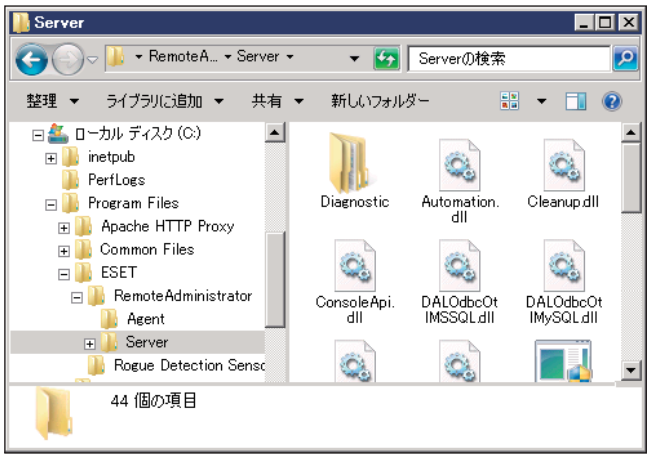
続く

ログが書き出されます。

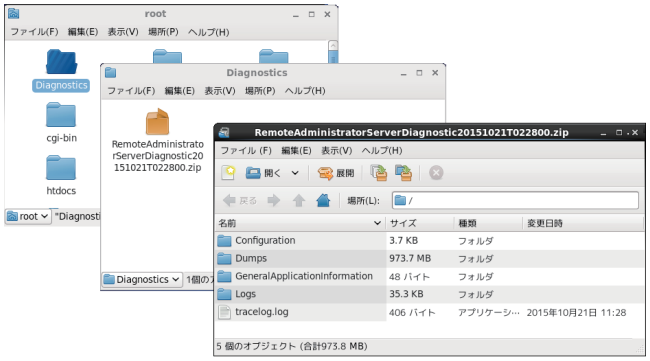
※画面は Linux です

`.zip creation finished` と表示されたら、診断ツールは終了です。
診断ツールの終了後、指定したフォルダーを確認してください。

Windows：



Linux：



ワンポイント

通常、ダンプファイルは問題が検出された時点でシステムによって作成されます。
手動で確認するには、次のフォルダーに移動してダンプファイルを挿入してください。
Windows：%temp%
Linux：/tmp

8.2 ミラーツール

ミラーツールは、ミラーサーバー用のウイルス定義データベースを ESET アップデートサーバーからダウンロードするツールです。ダウンロードしたウイルス定義データベースを IIS や Apache などの Web サーバーで公開することで、社内にウイルス定義データベースを提供するアップデートサーバーを構築することができます。
ミラーツールは Windows 用と Linux 用があります。ここでは OS 毎のミラーツールの使用方法を説明します。

8.2.1 Windows 用ミラーツールの使用方法

! 重 要

Windows 用のミラーツールは ERA サーバーをインストール可能な OS で動作します。
Windows サーバーでミラーツールを使用するには、Microsoft Visual C++ 2010 再頒布可能パッケージ（x86）のインストールが必要です。
https://www.microsoft.com/ja-JP/download/details.aspx?id=5555

操作手順

1. ユーザーズサイトより、ミラーツール「mirrortool_Win32.zip」をダウンロードし、展開します。

   展開したフォルダー内に MirrorTool.exe と updater.dll が作成されていることを確認します。

2. オフラインライセンスファイルをダウンロードします。

   オフラインライセンスファイル作成時に製品は「ESET Endpoint Antivirus for Windows」を選択し「ユーザー名とパスワードを含む」にチェックを入れてください。

   ワンポイント

   オフラインライセンスファイルのダウンロード手順は以下のサポートページの Q&A を参照してください。
   Q&A の URL： http://eset-support.canon-its.jp/faq/show/4327?site_domain=business

3. コマンドプロンプトを起動します。

4. コマンドプロンプト上で必須のパラメーターを指定して MirrorTool.exe を実行します。

続く

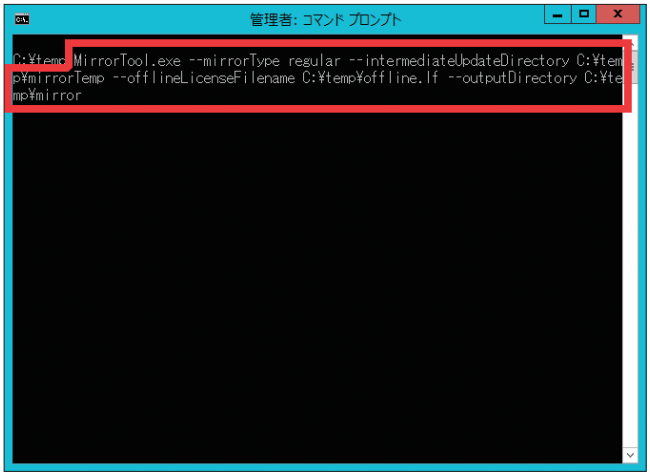
ミラーツールの必須パラメーター

必須パラメーター	説明
--mirrorType	ミラーのタイプを regular、pre-release、delayed より指定します。 regular ：既定値である通常の ESET アップロードサーバーからウイルス定義データベースをダウンロードします。 pre-release ：事前検証用のウイルス定義データベースをダウンロードします。本番環境では指定しないでください。 delayed ：regular で提供されているウイルス定義データベースの提供開始から 12 時間以上経過したウイルス定義データベースが最新として公開されています。
--interdediateUpdateDirectory	ミラーを作成するための一時ダウンロード先を指定します。（実行例では C:¥temp¥mirrortemp）
--offlineLicenseFilename	オフラインライセンスファイルを指定します。（実行例では C:¥temp¥offline.lf）
--outputDirectory	ミラーサーバー用のウイルス定義データベースの作成先を指定します。（実行例では C:¥temp¥mirror）

上記以外のパラメーターは「MirrorTool.exe --help」を実行すると表示されます。

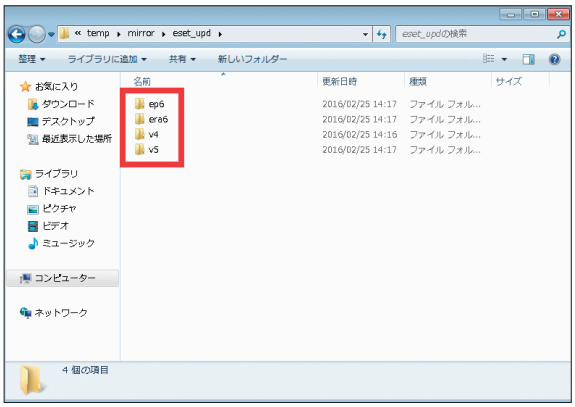
実行例）

MirrorTool.exe --mirrorType regular --intermediateUpdateDirectory C:¥temp¥mirrorTemp --offlineLicenseFilename C:¥temp¥offline.lf --outputDirectory C:¥temp¥mirror



続く

5 手順 4 の outputDirectory にて指定したフォルダーに「eset_upd」フォルダーが作成され、既定では製品バージョン毎のウイルス定義データベースのフォルダーが作成されます。



6 作成したウイルス定義データベースのフォルダーを、ファイル共有や Web サーバー等で公開し、クライアントコンピューターからアクセスできるようにします。

7 クライアントコンピューターにインストールされた ESET 製品のアップデートサーバーの設定を手順 5 で公開したアクセス先に指定します。

eset_upd 内のフォルダーは、ご利用の ESET 製品のバージョンより新しいバージョンのフォルダーを指定してください。

例えば、ESET Endpoint Security V5 をご利用の場合は、「v5」または「ep6」フォルダーを指定してください。(「v4」フォルダーは指定しないでください。)

また、「era6」フォルダーは、ESET Remote Administrator 6 からのみ指定してください。

ワンポイント

IIS での公開を行う場合、IIS の設定で「既定のドキュメント」を無効にしてください。また、「MIME の種類」に以下を追加してください。
ファイル名の拡張子：*（アスタリスク）
MIME の種類：application/octet-stream

ワンポイント

アップデートファイルは定期的に更新する必要があるため、Mirrortool.exe を定期的に実行することを推奨します。

Mirrortool.exe の定期実行例)
①C ドライブ直下に保存された Mirrortool.exe に設定するパラメーターを記述した BAT ファイルを作成する。(以下のサンプルを参照)
②タスクスケジューラに BAT ファイルを設定し、定期的に実行させる。
③IIS を有効にし、BAT ファイルで指定したアップデートファイルの保存場所を公開する。

BAT ファイル（サンプル）：

```
###Variable###
set MIRRORTOOL_PATH="C:¥MirrorTool.exe"
set MIRRORTYPE="regular"
set OUTPUTDIR=" C:¥temp¥mirror "
set INTERMIDIATE="c:¥temp¥mirrorTemp"
set LICENSE_PATH=" C:¥temp¥offline.lf "

MIRRORTOOL_PATH --mirrorType MIRRORTYPE --outputDirectory OUTPUTDIR --intermediateUpdateDirectory INTERMIDIATE
--offlineLicenseFilename LICENSE_PATH > nul
```

8.2.2 Linux 用ミラーツールの使用方法

! 重 要

Linux 用のミラーツールは ERA サーバーをインストール可能な OS で動作します。
プログラムは 32bit 用と 64bit 用に分かれています。

操作手順

1. ユーザーズサイトより、ミラーツール「mirrortool_Lin.i686.zip」（32bit 用）または「mirrortool_Lin.x86_64.zip」（64bit 用）をダウンロードし、展開します。

   展開したフォルダーに MirrorTool と updater.so が作成されていることを確認します。

2. ユーザーズサイトよりオフラインライセンスファイルをダウンロードします。

   オフラインライセンスファイル作成時に製品は「ESET Endpoint Antivirus for Windows」を選択し「ユーザー名とパスワードを含む」にチェックを入れてください。

   ワンポイント

   オフラインライセンスファイルのダウンロード手順は以下のサポートページの Q&A を参照してください。
   Q&A の URL： http://eset-support.canon-its.jp/faq/show/4327?site_domain=business

3. "chmod +x MirrorTool" コマンドで実行権限を付与した上で、必須のパラメーターを指定して MirrorTool を root 権限で実行します。

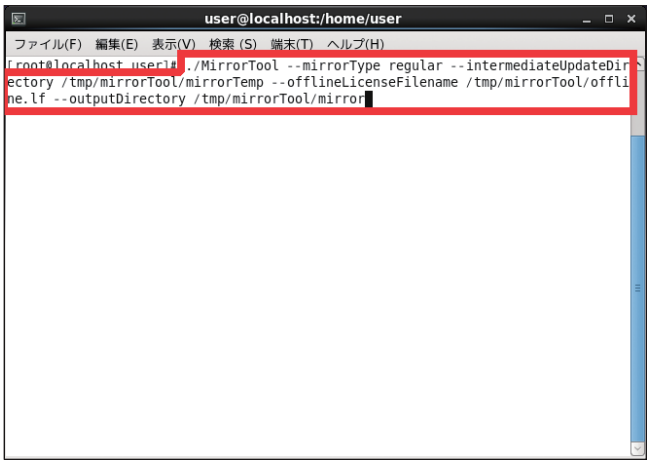
   ミラーツールの必須パラメーター

必須パラメーター	説明
--mirrorType	ミラーのタイプを regular、pre-release、delayed より指定します。 regular ：既定値である通常の ESET アップロードサーバーからウイルス定義データベースをダウンロードします。 pre-release ：事前検証用のウイルス定義データベースをダウンロードします。本番環境では指定しないでください。 delayed ：regular で提供されているウイルス定義データベースの提供開始から 12 時間以上経過したウイルス定義データベースが最新として公開されています。
--interdediateUpdateDirectory	ミラーを作成するための一時ダウンロード先を指定します。（実行例では /tmp/mirrorTool/mirrorTemp）
--offlineLicenseFilename	オフラインライセンスファイルを指定します。（実行例では /tmp/mirrorTool/offline.lf）
--outputDirectory	ミラーサーバー用のウイルス定義データベースの作成先を指定します。（実行例では /tmp/mirrorTool/mirror）

   上記以外のパラメーターは「MirrorTool --help」を実行すると表示されます。

   実行例）
   ./MirrorTool --mirrorType regular --intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp --offlineLicenseFilename /tmp/mirrorTool/offline.lf --outputDirectory /tmp/mirrorTool/mirror

続く



4 手順 3 の outputDirectory にて指定したフォルダーに「eset_upd」フォルダーが作成され、既定では製品バージョン毎のウイルス定義データベースのフォルダーが作成されます。

5 作成したウイルス定義データベースのフォルダーを、Web サーバー等で公開し、クライアントコンピューターからアクセスできるようにします。

6 クライアントコンピューターにインストールされた ESET 製品のアップデートサーバーの設定を手順 5 で公開したアクセス先に指定します。

eset_upd 内のフォルダーは、ご利用の ESET 製品のバージョンより新しいバージョンのフォルダーを指定してください。
例えば、ESET Endpoint Security V5 をご利用の場合は、「v5」または「ep6」フォルダーを指定してください（「v4」フォルダーは指定しないでください）。
また、「era6」フォルダーは、ESET Remote Administrator 6 からのみ指定してください。

ワンポイント

アップデートファイルは定期的に更新する必要があるため、MirrorTool を定期的に実行することを推奨します。

MirrorTool の定期実行例
①/root フォルダーに保存した MirrorTool に設定するパラメーターを記述したシェルスクリプト（mirrortool.sh）を作成する（以下のサンプルを参照）。
②CRON にシェルスクリプトを設定し定期的に実行させる。
例）1 時間に 1 回実行で mirrortool.sh が /tmp フォルダーに保存されている場合
30 * * * * /tmp/mirrortool.sh
③必要に応じて、Apache の設定ファイルを修正しシェルスクリプトでウイルス定義データーベースのフォルダーを公開する。

シェルスクリプト（サンプル）：

```
#!/bin/bash

###Variable###
MIRRORTOOL_PATH="/root/MirrorTool"
MIRRORTYPE="regular"
OUTPUTDIR="/tmp/mirrorTool/mirror "
INTERMIDIATE="/tmp/mirrorTool/mirrorTemp "
LICENSE_PATH="/tmp/mirrorTool/offline.lf "

${MIRRORTOOL_PATH} --mirrorType ${MIRRORTYPE} --outputDirectory ${OUTPUTDIR} --intermediateUpdateDirectory ${INTERMIDIATE} --offlineLicenseFilename ${LICENSE_PATH} > /dev/null
```

8.3 FAQ

Q: ERA エージェントのサイレントインストールの実行方法を教えてください。

A: GPO のスタートアップスクリプトを使用して実行することができます。ERA Web コンソールからサイレントインストールは実行できません。

Q:「ログイン失敗：通信エラー」と表示されて ERA Web コンソールにログインできないエラーの解決方法を教えてください。

A: ERA サーバーサービスとデータベースのサービスが起動していることを確認してください。起動していない場合は、サービスを起動してください。サービスが起動し再度実行されたら、Apache Tomcat サービスを再起動し、ERA Web コンソールを更新して、再度ログインしてください。

Q: Windows へのインストール中に設定した ERA Web コンソールの administrator のパスワードをリセットする方法を教えてください。

A: ERA サーバーのインストーラーを実行して［修復］を選択し、ERA Web コンソールの administrator のパスワードを再設定します。データベースの作成中に Windows 認証を使用しなかった場合は、ERA データベースのパスワードが必要になることがあります。

! 重　要

既存のデータベースを削除する修復オプションを選択した場合、保存されているデータを削除する可能性があるため注意してください。

Q: Linux へのインストール中に設定した ERA Web コンソールの administrator のパスワードをリセットする方法を教えてください。

A: インストールの際に作成した ERA Web コンソールの administrator とは別に、administrator と同等の権限を持つ、他のユーザー権限がある場合は、管理画面でパスワードをリセットすることができます。インストールの際に作成した administrator のみの場合、パスワードはリセットできません。ESET Remote Administrator の再インストールが必要になります。

管理者と同等の権限を持つ、ユーザーを新規作成し安全な場所に情報を保存しておくことを推奨します。

Q:「LOST + FOUND」グループに表示されるコンピューターは何ですか。

A: ERA サーバーに接続していて、どの静的グループにも所属しないコンピューターは自動的にこのグループに表示されます。このグループのコンピューターは、他の静的グループのコンピューターと同じようにグループとして操作できます。グループ名を変更することはできますが、グループの削除はできません。

Q: V5 にはクライアント情報に「カスタム情報」項目がありますが V6 でもありますか。

A: V6 では、「カスタムパラメータ / タグ付け」の作成ができません。ただし、レポートを生成し、クライアントのカスタムデータを表示できます。

Q: ブラウザーウインドウ全体を更新せずに、ページまたはページのセクションの情報を更新する方法を教えてください。

A: 更新を行いたい、ページセクションの右上にあるコンテキストメニューから、［更新］をクリックします。

Q: 脅威の駆除後に、ERA に表示される未解決の脅威数をリセットする方法を教えてください。

A: 未解決の脅威数をリセットするには、ESET Remote Administrator から該当のコンピューターの完全（詳細）検査を実施する必要があります。手動で脅威を駆除した場合は、該当の警告を解決済みに設定することができます。

Q: ERA エージェント接続間隔の CRON を設定する方法を教えてください。

A: ポリシーから設定を変更することができます。「R R/20 ***?*」の場合、ランダムな 20 分ごと（3、23、43 または 17、37、57 など）にランダムな秒（0 ～ 60）で接続することを意味します。ERA の負荷分散のためにランダムな値を設定してください。「0 * * * * ? *」（毎分：00 秒）などの正確な CRON が使用される場合、すべての ERA エージェントが同時に接続され、サーバー上で負荷のピークが発生します。

Q: ERA の証明書は、他のサードパーティの証明書を使用できますか。

A: CA（ルート認証局）または中間 CA（中間認証局）証明書で、「keyUsage」制約の「keyCertSign（電子証明書の検証）」フラグが付いている、他の証明書を使用することができます。

Q: RD Sensor が何も検出しない場合のトラブルシューティング方法を教えてください。

A: 考えられる原因として次の 3 つが挙げられます。

OS がネットワークデバイスとして検出されない場合は、管理対象外のコンピューターとして ESET Remote Administrator に送信されません。（プリンタ、ルータは除外されます。）

RD Sensor は libpcap Ver1.3.0 に対応しています。システムにインストールされているバージョンを確認してください。

RD Sensor がインストールされている仮想マシンのネットワーク接続がブリッジになっているか確認してください。

すべての要件が満たされている場合は、Nmap の OS 検出を実行し、コンピューターの OS が検出されるかどうか確認してください。

Q: RD Sensor がネットワーク上の一部のコンピューターを検出しません。

A: RD Sencer はネットワーク上の通信をモニターします。コンピューターが通信していない場合、RD Sensor で検出されません。コンピューターの DNS 設定のチェックを入れ、通信を遮断していないことを確認してください。