ESET PROTECT ソリューション

V7/V8 から V9 へのバージョンアップ手順書

～インターネット接続不可の環境の場合～

第 7 版
2023 年 8 月 9 日
キヤノンマーケティングジャパン株式会社

目次

1. はじめに 3

2. 本資料における構成の前提 4

3. 新バージョンへのバージョンアップフロー 5

4. 【STEP0】事前準備 8

5. 【STEP1】セキュリティ管理ツールのバックアップ 10

6. 【STEP2】新ミラーサーバーの構築 15

7. 【STEP3】サーバーのバージョンアップ 30

8. 【STEP4】 クライアントのバージョンアップ事前準備 45

9. 【STEP5】エージェントおよびクライアント用プログラムのバージョンアップ

■バージョンアップ方法パターン分け■ 52

パターン A：インストーラーをローカル実行してバージョンアップする場合 53

パターン B：共有フォルダを使用してセキュリティ管理ツールからバージョンアップする場合 .. 61

パターン C：Web サーバーを使用してセキュリティ管理ツールからバージョンアップする場合 80

パターン D：AD 環境で GPO を使用してバージョンアップする場合 92

10. 【STEP6】 バージョンアップ完了の確認 105

※上記手順 9(P52~P96)に関しては、お客様環境に合わせてバージョンアップ方法が異なります。
パターン分けの詳細については P52 をご確認ください。

はじめに

○本資料は、ESET PROTECT ソリューションをご利用のお客さまが旧バージョン(バージョン 7/バージョン 8)からバージョン 9 へバージョンアップする際に必要となる作業や注意事項について記載しています。

○本資料は、本資料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および名称が異なっている場合があります。また、本資料の内容は将来予告なく変更することがあります。
利用する OS やプログラムのバージョンによっては画面が異なる場合がありますので、ご注意ください。

○本製品の一部またはすべてを無断で複写、複製、改変することはその形態に問わず、禁じます。

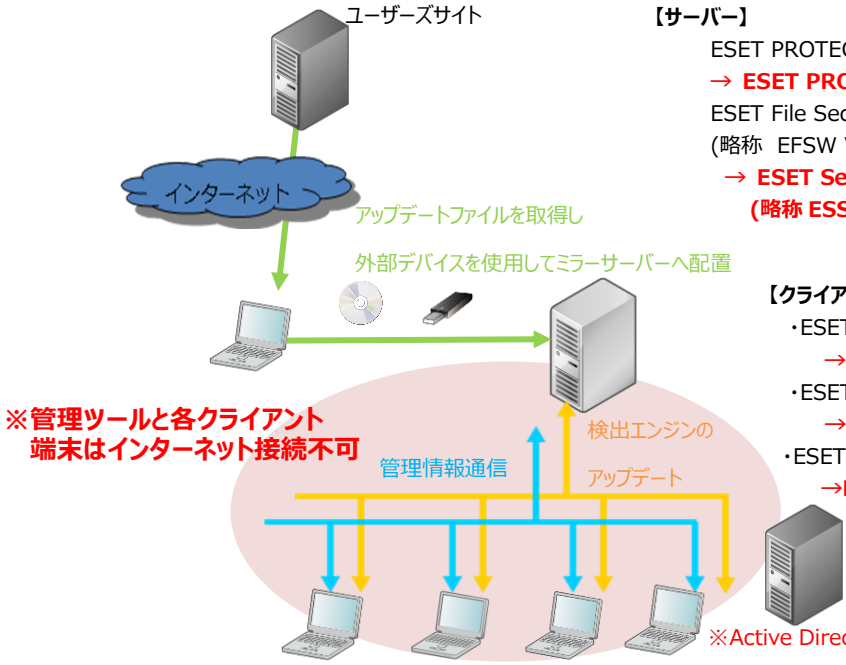
○ESET、NOD32、ThreatSense、LiveGrid、ESET Endpoint Protection、ESET Endpoint Security、ESET Endpoint アンチウイルス、ESET File Security、ESET Server Security、ESET NOD32 アンチウイルス、ESET Security Management Center、ESET PROTECT は、ESET,spol. s r. o.の商標です。Microsoft、Windows、Windows Server、Hyper-V、Active Directory、Internet Explorer、Microsoft Edge、Outlook、SmartScreen、Windows Live 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 logo、Mac OS、OS X 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。仕様は予告なく変更する場合があります。

ESET PROTECT ソリューション
V7/V8 から V9 へのバージョンアップ手順書
～インターネット接続不可の環境の場合～

1. 本資料における構成の前提

本資料は、以下の構成を前提として、V7/V8 プログラムから V9 へバージョンアップする際のフローや注意点を記載しております。以下の構成に当てはまらないバージョンや構成におきましても、本資料を参考にバージョンアップを実施いただけるように必要な情報を記載しております。

		バージョンアップ前	バージョンアップ後
全体構成		・Windows クライアント、300 台程度管理 ・モバイル管理なし ・1 台の専用サーバー機で管理機能とミラー機能を運用 ・プロキシサーバーなし ・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 ・管理ツールと各クライアント端末はインターネット接続不可	・Windows クライアント、300 台程度管理 ・モバイル管理なし ・1 台の専用サーバー機で管理機能とミラー機能を運用 ・プロキシサーバーなし ・既存サーバーを利用 ・管理ツールと各クライアント端末はインターネット接続不可
サーバー用 (Windows Server 2016)	管理	・ESET PROTECT V8.1	・ESET PROTECT V9.1
	ミラー	・ユーザーズサイトから取得したファイルを IIS で公開 または EFSW V7.3 のミラー機能で公開	ユーザーズサイトから取得したファイルを IIS で公開
	ウイルス・スパイウェア対策	・ESET File Security for Microsoft Windows Server V7.3	・ESET Server Security for Microsoft Windows Server V9.0
クライアント用 (Windows10)	管理	・ESET Management エージェント V8.1	・ESET Management エージェント V9.1
	ウイルス・スパイウェア対策	・ESET Endpoint Security V8.1 または ESET Endpoint アンチウイルス V8.1	・ESET Endpoint Security V9.1 または ・ESET Endpoint アンチウイルス V9.1



【サーバー】

ESET PROTECT V8.1 (略称 EP V8.1)
→ ESET PROTECT V9.1 (略称 EP V9.1)
ESET File Security for Microsoft Windows Server V7.3
(略称 EFSW V7.3)
→ ESET Server Security for Microsoft Windows Server V9.0 (略称 ESSW V9.0)

【クライアント】

・ESET Endpoint Security V8.1 (略称 EES V8.1)
→ ESET Endpoint Security V9.1 (略称 EES V9.1)
・ESET Endpoint アンチウイルス V8.1 (略称 EEA V8.1)
→ ESET Endpoint アンチウイルス V9.1 (略称 EEA V9.1)
・ESET Management エージェント V8.1 (略称 EM エージェント V8.1)
→ESET Management エージェント V9.1 (略称 EM エージェント V9.1)

2. 新バージョンへのバージョンアップフロー

V7.X/V8.X から V9.X へバージョンアップにあたり必要なステップは、以下の通りです。

【STEP0】事前準備

【STEP1】セキュリティ管理ツールのバックアップ

STEP1-1. SQL Server Management Studio 18 のインストール

STEP1-2. セキュリティ管理ツールのサービス停止

STEP1-3. データベースのバックアップ

STEP1-4. コンフィグレーションファイルのバックアップ

【STEP2】新ミラーサーバーの構築

パターン A: ユーザーズサイトから取得したファイルを IIS で公開している場合

A-1. ミラーサーバーの追加

パターン B: EFSW V7.3 のミラー機能で公開している場合

B-1. ミラーサーバーの作成

B-2. IIS の設定

B-3. 既存ミラーサーバーの無効化

B-4. 新ミラーサーバーの起動

B-5. バージョンアップ前クライアントのアップデート先変更

B-6. EP のアップデート先変更

B-7. EM エージェントのアップデート先変更のポリシー作成

【STEP3】サーバーのバージョンアップ

STEP3-1. 動作要件の確認

STEP3-2. ESET File Security for Microsoft Windows Server のバージョンアップ

STEP3-3. セキュリティ管理ツールのバージョンアップ

STEP3-4. データベースのバックアップ

STEP3-5. ピア証明書と認証局のバックアップ

【STEP4】クライアントのバージョンアップ事前準備

STEP4-1.バージョンアップ完了確認用の動的グループ作成

STEP4-2.動的グループへのポリシー適用

【STEP5】エージェントおよびクライアント用プログラムのバージョンアップ

※環境に合わせてバージョンアップ方法がパターン A～D に分かれます

パターン A:インストーラーをローカル実行してバージョンアップする場合

a. EM エージェントのバージョンアップ

a-1. EM エージェントバージョンアップ用の GPO または SCCM スクリプトの準備

a-2. EM エージェントバージョンアップ用のバッチファイルの準備

a-3. EM エージェントのバージョンアップ

b. クライアント用プログラムのバージョンアップ

b-1. 動作要件の確認

b-2. クライアント用プログラムのバージョンアップ用バッチファイルの準備

b-3. クライアント用プログラムのバージョンアップ

パターン B：共有フォルダを使用してセキュリティ管理ツールからバージョンアップする場合

a. EM エージェントのバージョンアップ

a-1. 共有フォルダの準備

a-2. EM エージェントのプログラムの準備

a-3. EM エージェントのバージョンアップ

b. クライアント用プログラムのバージョンアップ

b-1. 動作要件の確認

b-2. クライアント用プログラムの準備

b-3. クライアント用プログラムのバージョンアップ

パターンC:Web サーバーを使用してセキュリティ管理ツールからバージョンアップする場合

a. EM エージェントのバージョンアップ

a-1. EM エージェントをバージョンアップ

b. クライアント用プログラムのバージョンアップ

b-1. 動作要件の確認

b-2. クライアント用プログラムのバージョンアップ

パターン D:AD 環境で GPO を使用してバージョンアップする場合

a. EM エージェントとクライアント用プログラムのバージョンアップ

a-1. 動作要件の確認

a-2-1. バージョンアップの準備 ～GPO の作成～

a-2-2. バージョンアップの準備 ～GPO の配布～

a-3. EM エージェントとクライアント用プログラムのバージョンアップ

a-4. 配布した GPO の割り当て解除

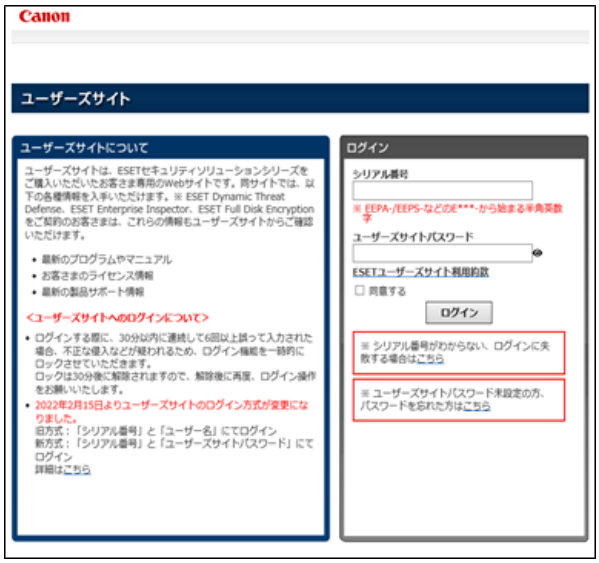
以降は共通の確認作業

【STEP6】バージョンアップ完了の確認

3.【STEP0】事前準備

インターネット接続可能端末からユーザーズサイトにアクセスし、バージョンアップに使用するインストーラーをダウンロードします。本手順でダウンロードするインストーラーは、各クライアント端末に配布して実行します。

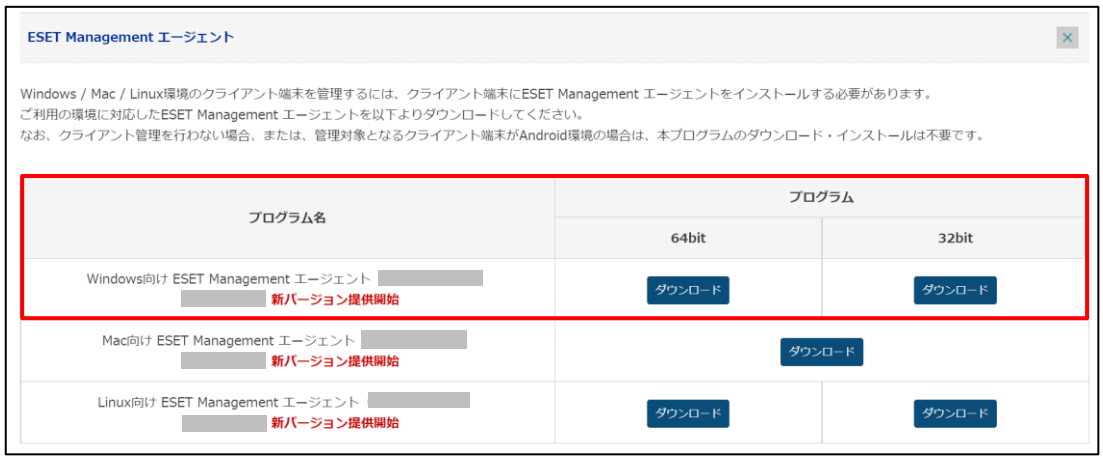
1. 以下 URL からユーザーズサイトにログインします。
   [ユーザーズサイト]
   https://canon-its.jp/product/eset/users/index.html
   ※ユーザーズサイトにログインするにはシリアル番号とユーザーズサイトパスワードが必要です。



2. ユーザーズサイトで[プログラム/マニュアル]-[最新バージョンをダウンロード]と進み、以下のインストーラーをそれぞれダウンロードします。

   ・オンプレミス型セキュリティ管理ツール(旧称：クライアント管理用プログラム)
   ESET PROTECT(Windows)(Ver.9.X.XX.X)のオールインワンインストーラー

・ESET Management エージェント
Windows 向け ESET Management エージェント(Ver.9.X.XXX.X)



・Windows 向けクライアント用プログラム
ESET Endpoint Security / ESET Endpoint アンチウイルス(Ver.9.X.XXX.X)

※インストーラーはフルモジュールインストーラーをご利用ください。

・Windows Server 向けクライアント用プログラム
ESET Server Security for Microsoft Windows Server(Ver. 9.X.XXXX.X)

4.【STEP1】セキュリティ管理ツールのバックアップ

セキュリティ管理ツールのバージョンアップを行う前にデータをフルバックアップしてください。

STEP1-1. SQL Server Management Studio 18 のインストール

1. 以下 URL より、SQL Server Management Studio 18 をダウンロードし、サーバーへインストールしてください。

   <SQL Server Management Studio ダウンロードサイト>
   https://docs.microsoft.com/ja-jp/sql/ssms
   ※インストール後、再起動が要求された場合は再起動します。

2. 「Microsoft SQL Server Management Studio18」を起動できることを確認します。
   ※初めて起動する場合、起動に少々お時間がかかります。

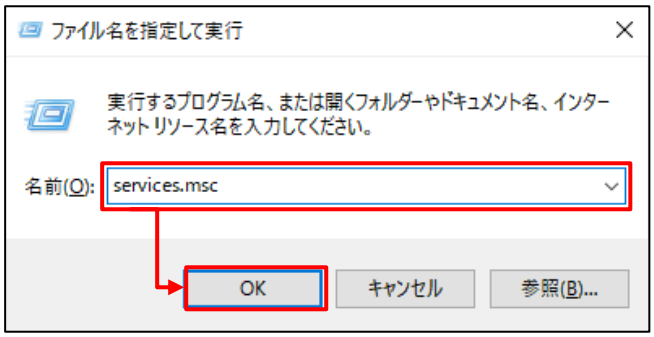
STEP1-2. セキュリティ管理ツールのサービス停止

サーバーのデータベースのバックアップを取得するために、以下の手順を参照してバージョンアップ前の EP または ESMC のサービスを停止させます。

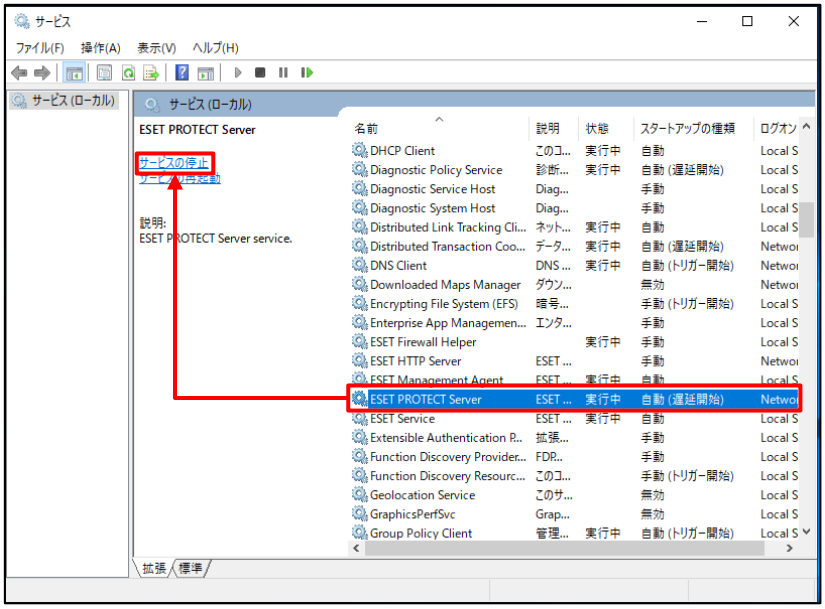
<注意>

セキュリティ管理ツールのサービスを停止するため一時的にクライアントを管理することができません。
サービスが停止している間のクライアントのログはクライアントの EM エージェント自身で保持しており、サービス起動後に通信が確立された段階でセキュリティ管理ツールにログが送付されます。

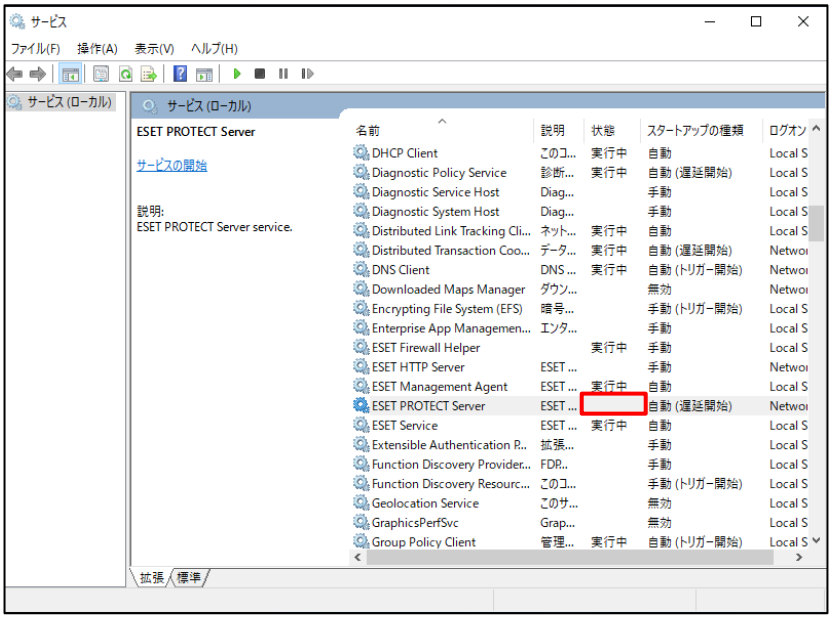
1. 「Windows キー」+「R」でファイル名を指定して実行させるウィンドウを開き「services.msc」と入力し、[OK]ボタンをクリックします。



2. 「ESET PROTECT Server」サービスまたは「ESET Security Management Center Server」サービスを選択し、サービスの停止をクリックします。
※以下は「ESET PROTECT Server」サービスを停止させる例です。



3. 「ESET PROTECT Server」サービスまたは「ESET Security Management Center Server」サービスの状態が空欄になったことを確認します。
※以下は「ESET PROTECT Server」サービスが停止した例です。

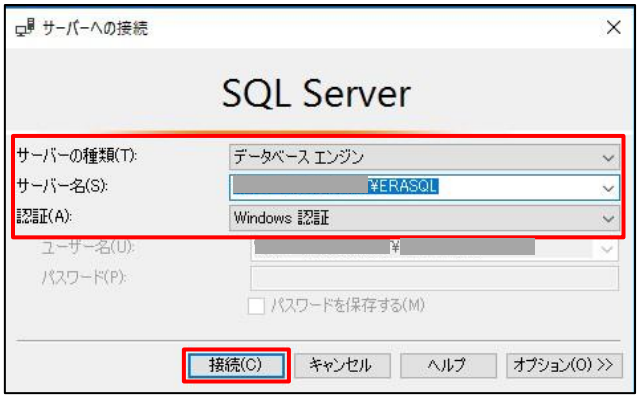


STEP1-3. データベースのバックアップ

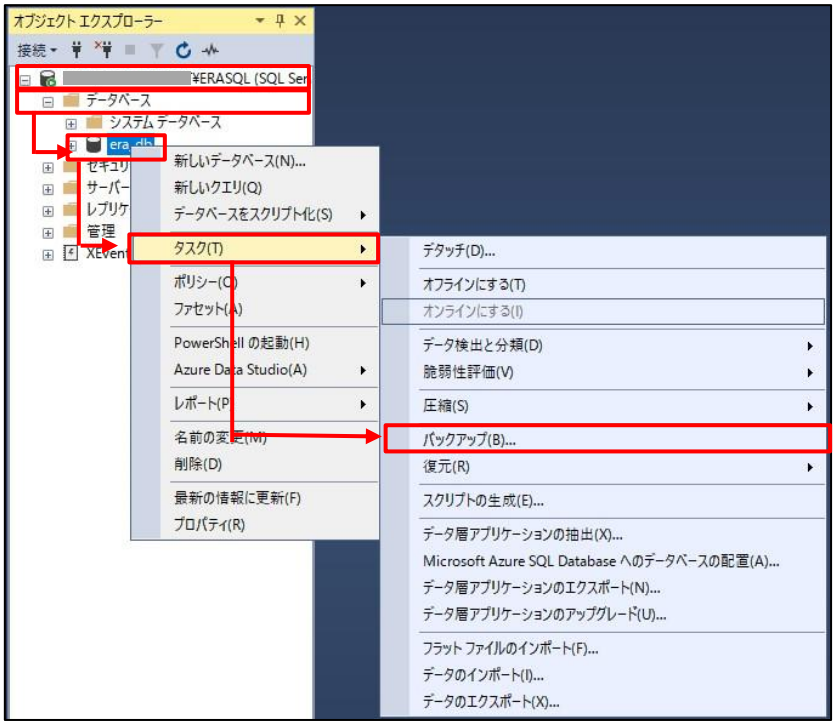
1. [Microsoft SQL Server Management Studio 18]を起動します。
※初めて起動される場合、起動までお時間がかかる場合がございます。

2. サーバーへの接続画面で、以下の通り項目を確認して[接続]ボタンをクリックします。

サーバーの種類	データベースエンジン
サーバー名	EP のサーバーで使用しているインスタンス名 ※既定は「コンピューター名¥ERASQL」
認証	Windows 認証

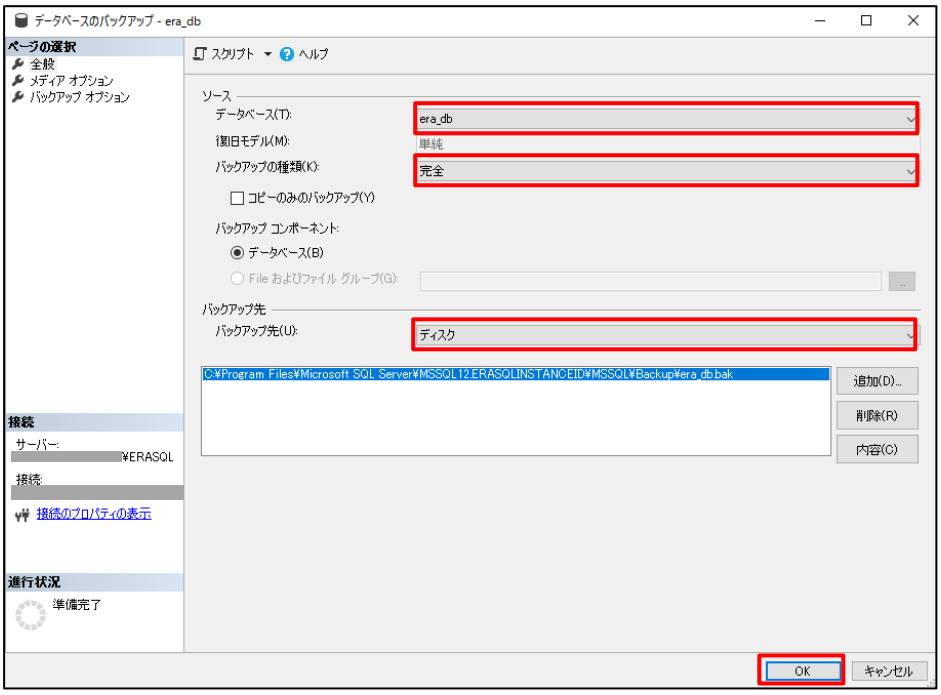


3. オブジェクトエクスプローラーより、[インスタンス名]-[データベース]-[era_db]へ移動します。
「era_db」を右クリックし、[タスク]-[バックアップ]をクリックします。

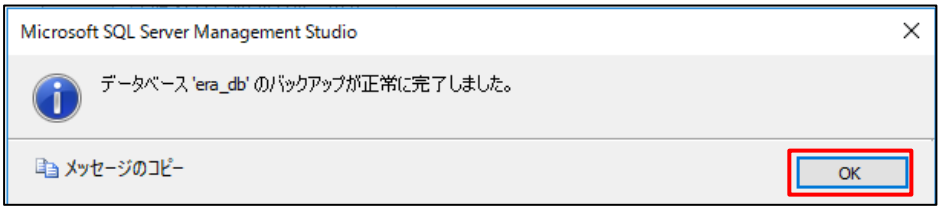


4. データベースのバックアップ画面で、以下の通り設定し、[OK]ボタンをクリックします。

データベース	era_db
バックアップの種類	完全
バックアップ先	ディスク



5. 以下のメッセージが表示されたらバックアップは正常に終了しています。
[OK]ボタンをクリックして、閉じます。



※「アクセスが拒否されました」といったエラーが出力された場合は、バックアップファイルの出力先にアクセス権限があるかご確認ください。

6. 手順 4 で作成したバックアップファイルが指定の場所に格納されていることを確認します。

STEP1-4. コンフィグレーションファイルのバックアップ

1. 以下のフォルダの「Startupconfiguration.ini」ファイルをコピーし、任意の場所に保存してください。

<Window Sever 2012/ Window Sever 2016/ Window Sever 2019 のディレクトリ>
C:¥ProgramData¥ESET¥RemoteAdministrator¥Server¥EraServerApplicationData¥Configuration

※[ProgramData]が表示されない場合は、[表示]-[隠しファイル]にチェックを入れてください。
※Mobile device Connector をインストールしている場合は、以下のフォルダの「Startupconfiguration.ini」ファイルもコピーし、任意の場所に保存してください。

<Window Sever 2012/ Window Sever 2016/ Window Sever 2019 のディレクトリ>
C:¥ProgramData¥ESET¥RemoteAdministrator¥MDMCore¥Configuration

2. バックアップ完了後、【STEP1-2】を参考に「ESET PROTECT Server」サービスまたは「ESET Security Management Center」サービスを起動してください。

<注意>

EP V9.1 のサポート OS は Windows Server 2012 以降です。
サポート OS に関しては、以下 URL をご確認ください。
https://eset-info.canon-its.jp/files/user/pdf/support/esetbe_os_era.pdf

<参考>

セキュリティ管理ツールのバージョンアップに失敗した場合、データベースとコンフィグレーションファイルのバックアップを使用して、バージョンアップ前の状態に復元することができます。
<セキュリティ管理ツールのフルバックアップをする手順、および、リストアする手順について>
https://eset-support.canon-its.jp/faq/show/119?site_domain=business

また、バージョンアップ時にデータの引き継ぎに失敗した場合は、サポートセンターまでお問い合わせください。
<お問い合わせ窓口(サポートセンター)のご案内>
https://eset-support.canon-its.jp/faq/show/883?site_domain=business

5.【STEP2】新ミラーサーバーの構築

バージョンアップ後に、検出エンジン(V9 向け)をアップデートするため、検出エンジン(V9 向け)を準備します。バージョンアップ前の環境での、ミラーサーバーの構築方法によって本手順を行ってください。

パターン A: ユーザーズサイトから取得したファイルを IIS で公開している場合

※本手順は、下記の検出エンジンを含むミラーサーバーが、既に構築されている想定です。
<クライアント用プログラムの検出エンジン(V7～8 向け)>
ユーザーズサイトより、
[検出エンジン(ウイルス定義データベース)]
-[検出エンジンダウンロードページ]
-[クライアント用プログラムの検出エンジンダウンロード]
-[Windows / Linux の「バージョン 7～8」 / Mac / Android 向けクライアント用プログラムの場合]

<セキュリティ管理ツール用の検出エンジン>
ユーザーズサイトより、
[検出エンジン(ウイルス定義データベース)]
-[検出エンジンダウンロードページ]
-[セキュリティ管理ツールの検出エンジン ダウンロード]

A-1. ミラーサーバーの追加

A-1-1. インターネット接続が可能な端末から、ユーザーズサイトにログイン後、クライアント用プログラムの検出エンジンをダウンロードし、外部デバイスなどを利用してサーバーにコピーをしてください。

[ユーザーズサイト]
https://canon-its.jp/product/eset/users/index.html
※ユーザーズサイトにログインするにはシリアル番号とユーザーズサイトパスワードが必要です。

●クライアント用プログラムの検出エンジン(V9 向け)
[検出エンジン(ウイルス定義データベース)]
-[検出エンジンダウンロードページ]
-[クライアント用プログラムの検出エンジンダウンロード]
-[Windows / Linux の「バージョン 9」向けクライアント用プログラムの場合]
※「最新」と記載がある検出エンジンをダウンロードしてください。

A-1-2. 手順 1 で用意したクライアント用プログラムの検出エンジン(V9 向け)を、IIS で公開している物理パス配下に配置してください。その際、検出エンジン(V9 向け)であることが分かるフォルダ名を設定してください。
例：「ess9_upd」など

パターン B: EFSW　V7.3 のミラー機能で公開している場合

B-1. ミラーサーバーの作成

B-1-1. インターネット接続が可能な端末から、ユーザーズサイトにログイン後、クライアント用プログラムの検出エンジンをダウンロードし、外部デバイスなどを利用してサーバーにコピーをしてください。

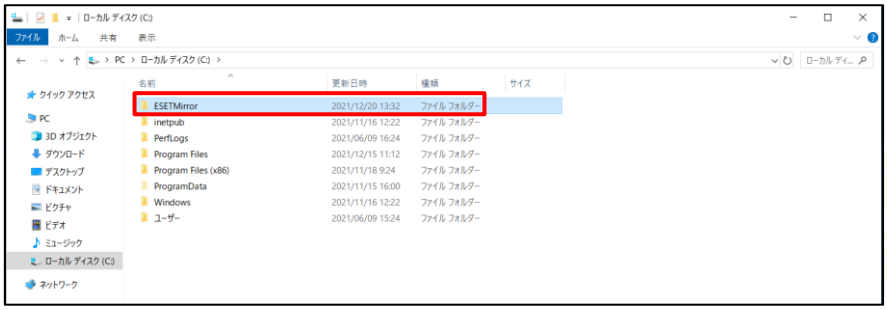
[ユーザーズサイト]
https://canon-its.jp/product/eset/users/index.html
※ユーザーズサイトにログインするにはシリアル番号とユーザーズサイトパスワードが必要です。

●クライアント用プログラムの検出エンジン(V7/8 向け)
[検出エンジン(ウイルス定義データベース)]
-[検出エンジンダウンロードページ]
-[クライアント用プログラムの検出エンジンダウンロード]
-[Windows / Linux の「バージョン 7～8」/Mac/Android 向けクライアント用プログラムの場合]
※「最新」と記載がある検出エンジンをダウンロードしてください。

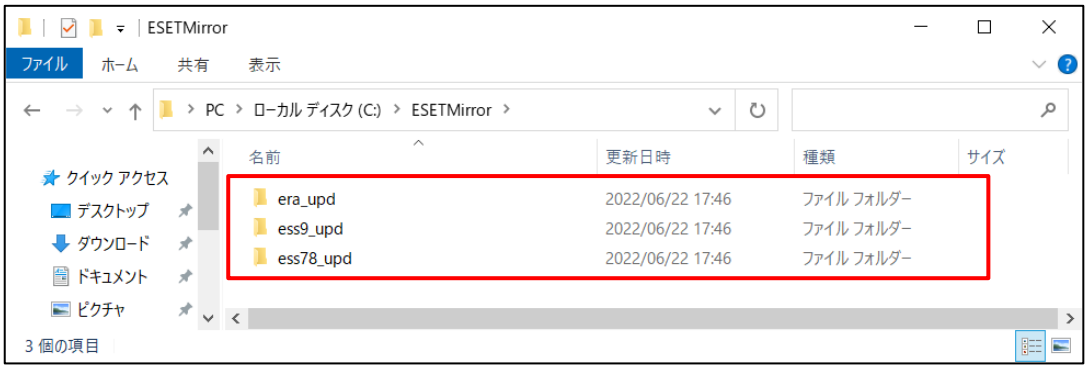
●クライアント用プログラムの検出エンジン(V9 向け)
[検出エンジン(ウイルス定義データベース)]
-[検出エンジンダウンロードページ]
-[クライアント用プログラムの検出エンジンダウンロード]
-[Windows / Linux の「バージョン 9」向けクライアント用プログラムの場合]
※「最新」と記載がある検出エンジンをダウンロードしてください。

●セキュリティ管理ツール用の検出エンジン
[検出エンジン(ウイルス定義データベース)]
-[検出エンジンダウンロードページ]
-[セキュリティ管理ツールの検出エンジン ダウンロード]
※「最新」と記載がある検出エンジンをダウンロードしてください。

B-1-2. C ドライブ直下に「ESETMirror」フォルダを作成します。



B-1-3. 作成した「ESETMirror」フォルダ配下に、「ess78_upd」フォルダ、「ess9_upd」フォルダ、「era_upd」フォルダを作成します。



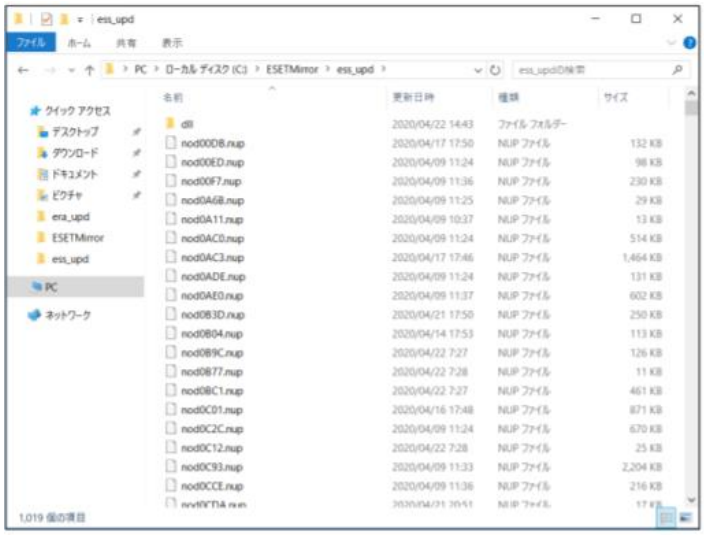
B-1-4. 「手順 B-1-1」で用意した「クライアント用プログラムの検出エンジン(V9 向け)」と「セキュリティ管理ツール用の検出エンジン」を、「手順 B-1-3」で作成した下記のフォルダへ展開します。

・「クライアント用プログラムの検出エンジン(V7/8 向け)」→「ess78_upd」フォルダへ

・「クライアント用プログラムの検出エンジン(V9 向け)」→「ess9_upd」フォルダへ

・「セキュリティ管理ツール用の検出エンジン」→「era_upd」フォルダへ

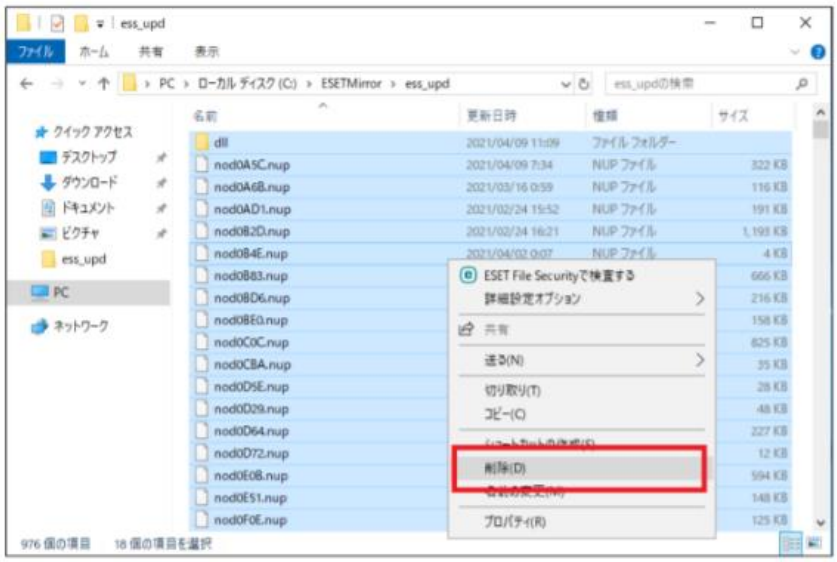
※検出エンジンを展開するフォルダを間違えないようにしてください。

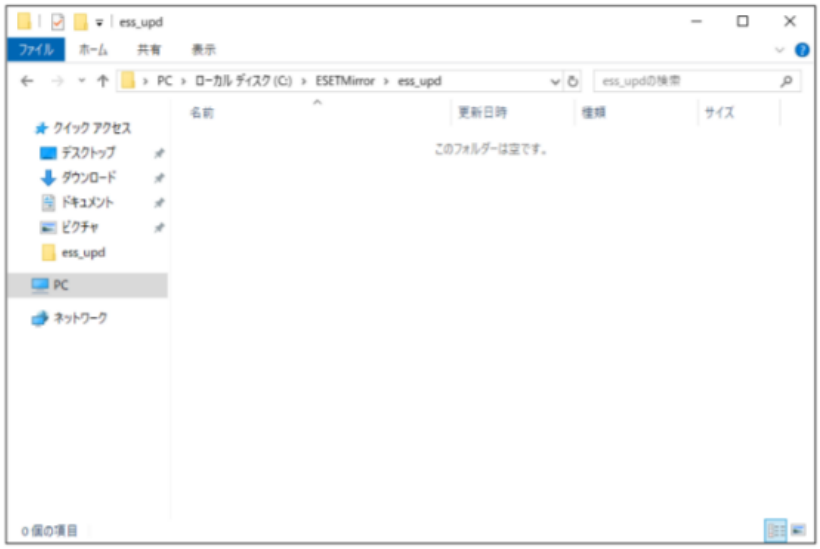


◆参考◆ ミラーサーバーの検出エンジンの更新について

ミラーサーバーに保存された検出エンジンは手動での更新が必要となります。運用に合わせて更新頻度を決めていただき、定期的に更新を行ってください。

下記画像の様に、**保存されていた検出エンジンを必ず削除してから**、新しく取得した検出エンジンを展開してください。



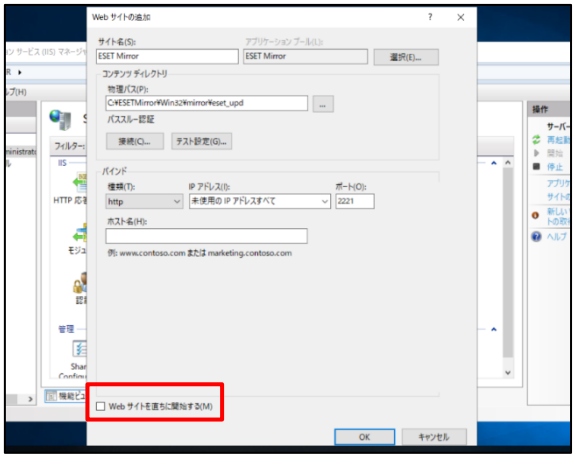


B-2. IIS の設定

IIS で検出エンジンを公開する手順につきましては下記 URL より、「2. IIS 環境の構築 <Web サーバーでの作業>」をご確認ください。

◇IIS を利用して検出エンジン（ウイルス定義データベース）を公開する手順
https://eset-support.canon-its.jp/faq/show/9499? site_domain=business

※上記 URL 内の[2. IIS 環境の構築 <Web サーバーでの作業>]-[Step.2 IIS の設定]-[手順 4]で Web サイトを作成する際、**「Web サイトを直ちに開始する」のチェックをオフ**の状態で作成してください。既存ミラーサーバーのポートと重複し、エラーが発生してしまう場合があります。



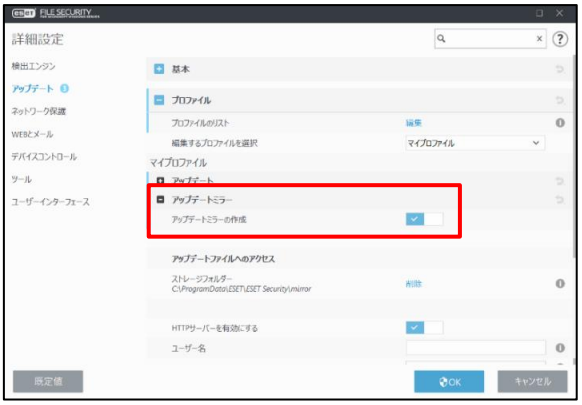
B-3. 既存ミラーサーバーの無効化

IIS で構築したミラーサーバーから検出エンジンをアップデートできるようにするため、既存ミラーサーバーを無効化します。

B-3-1. 既存ミラーサーバーのデスクトップのタスクトレーより ESET のアイコンをクリックしメイン画面を開きます。
B-3-2. F5 キーを押下し、詳細画面を開きます。

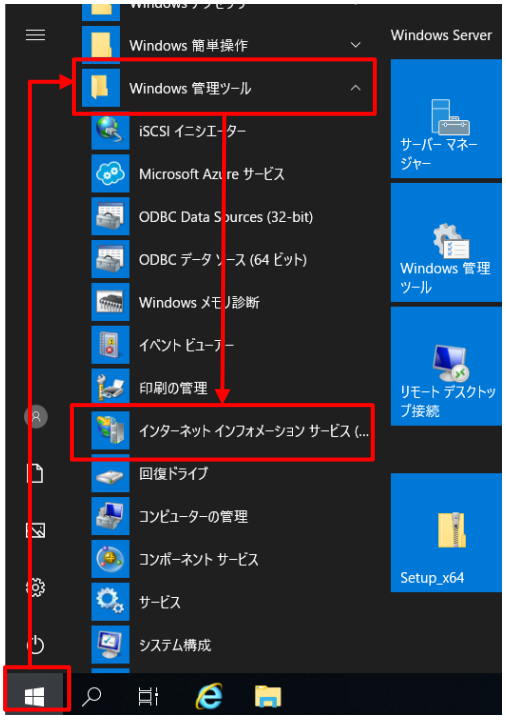
B-3-3. [アップデート]-[プロファイル]-[アップデートミラー]より、[アップデートミラーの作成]を無効にします。

※同様の設定はポリシーからも設定が可能です。

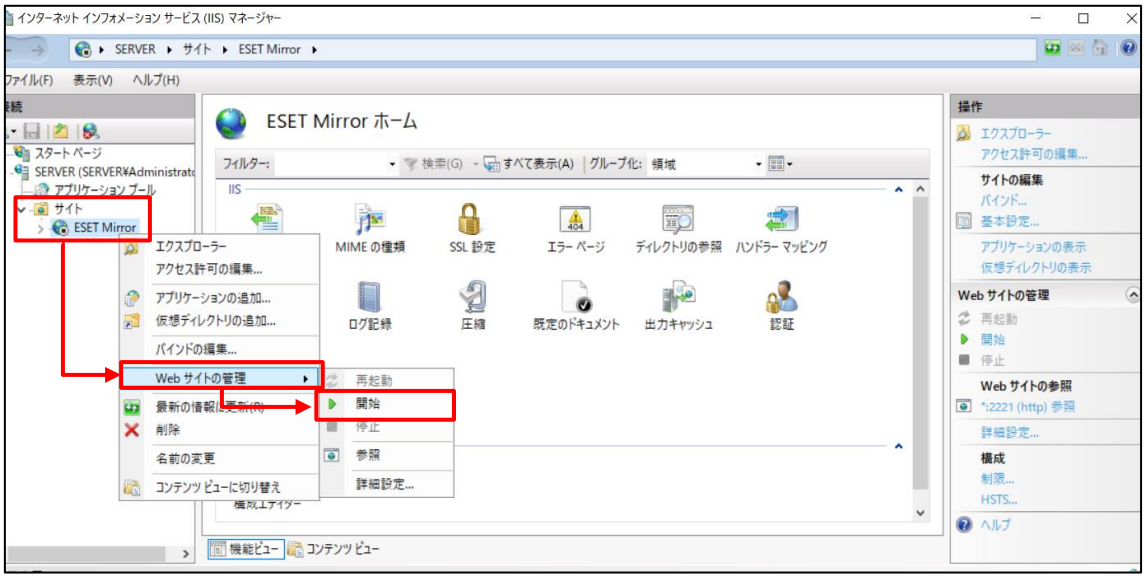


B-4.新ミラーサーバーの起動

B-4-1. [スタートメニュー]から[Windows 管理ツール]をクリックして、[インターネット インフォメーションサービス(IIS)マネージャー]を起動します。



B-4-2.「手順 B-2」で作成したサイトを右クリックし、[Web サイトの管理]-[開始]をクリックし、サイトを開始します。

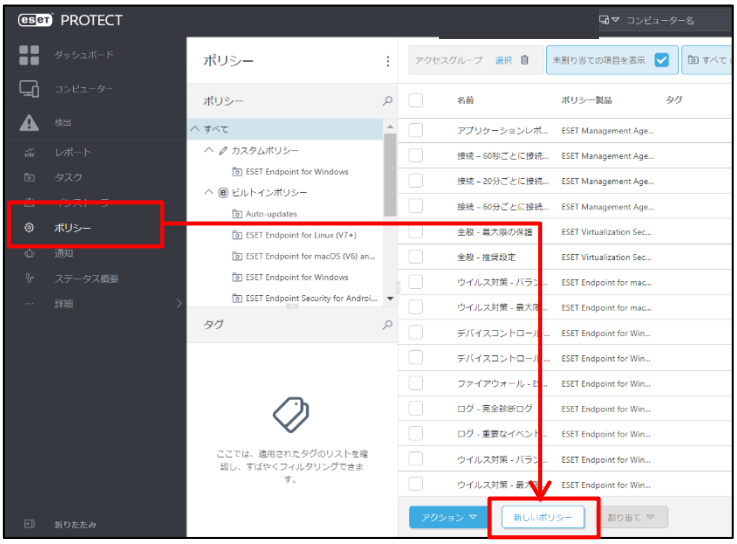


B-5. バージョンアップ前クライアントのアップデート先変更

バージョンアップ前のクライアント用プログラムが「手順 B-1」で準備した検出エンジンのアップデートができるように、ポリシーを使用してアップデート先を変更します。

※本手順を参考に、バージョンアップ後に V9 用の検出エンジンの取得先を指定するポリシーも作成してください。

B-5-1. EPC にログイン後、 [ポリシー]より、[新しいポリシー]ボタンをクリックします。



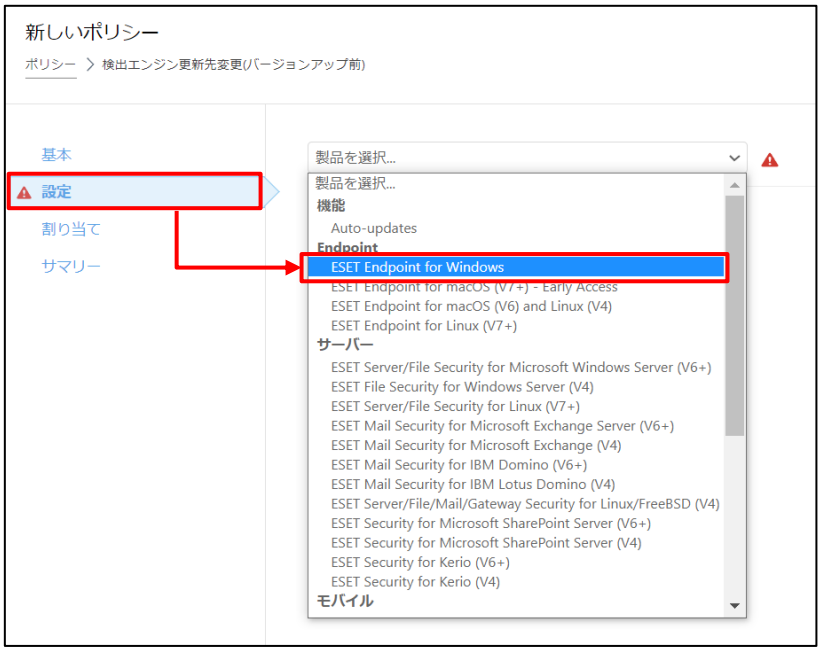
B-5-2. [基本]を展開し、任意の名前「例：検出エンジン更新先変更(バージョンアップ前)」を入力します。

※バージョンアップ後プログラム用のポリシーの場合は「例:検出エンジン更新先変更(バージョンアップ後)」と入力してください。

※[説明]の入力は任意です。

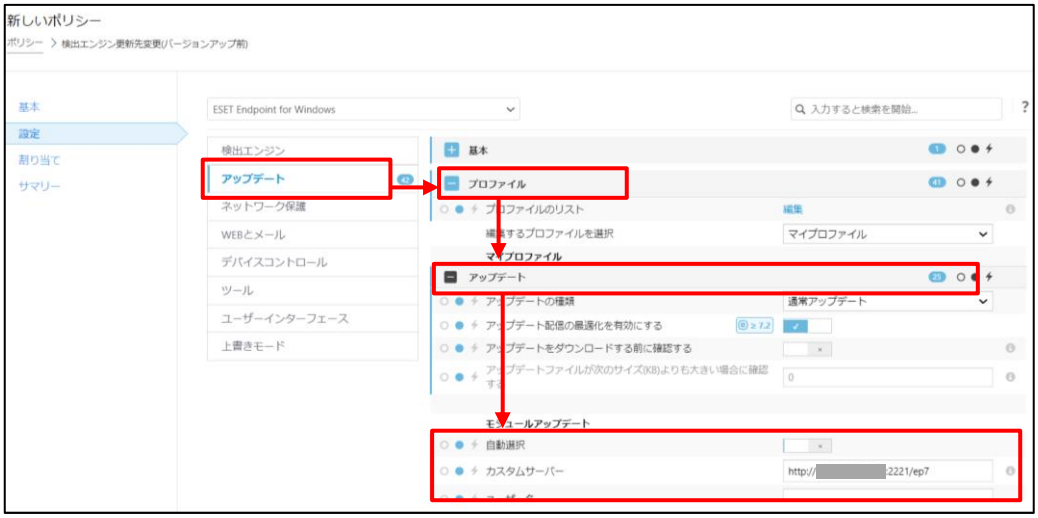
B-5-3. [設定]を展開し、製品を選択します。

※本手順では「ESET Endpoint for Windows」を選択します。



B-5-4. [アップデート]-[プロファイル]-[アップデート]と展開し、以下の通り設定します。

モジュールアップデート	
自動選択	無効
カスタムサーバー	**http://<新バージョン対応ミラーサーバーの IP アドレス>:<ポート>/ <フォルダー名>** ※フォルダー名は各バージョン用の検出エンジンのフォルダに設定した名前を指定します。 (例：バージョンアップ前は ess78_upd、バージョンアップ後は ess9_upd など)

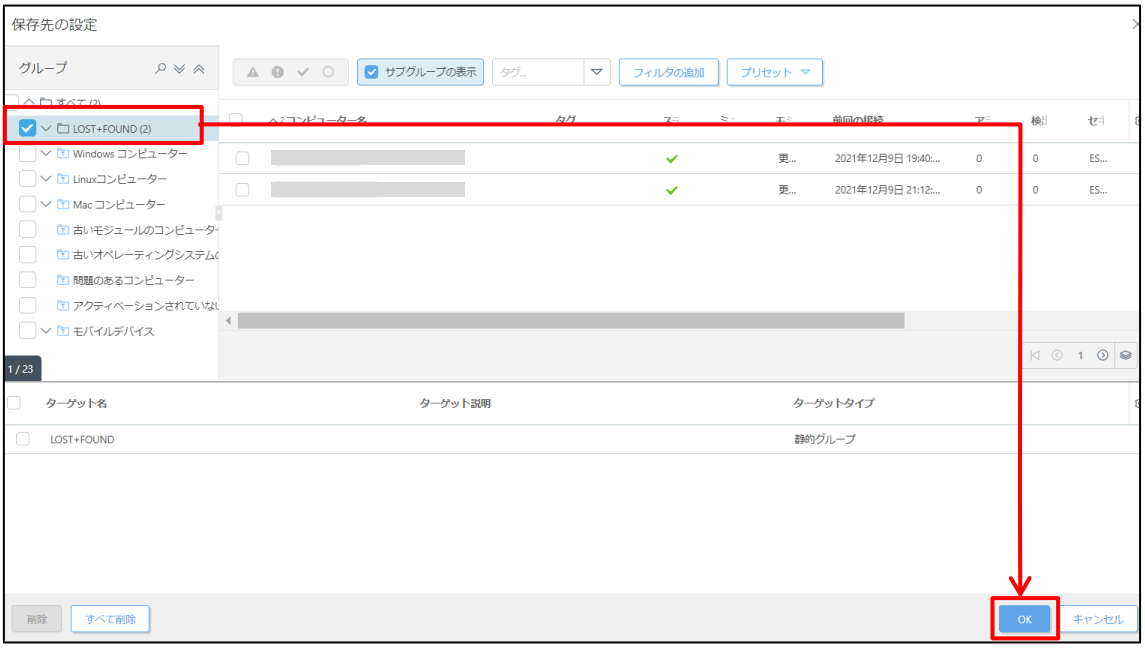


B-5-5.　[割り当て]を展開し、[割り当て…]ボタンをクリックします。

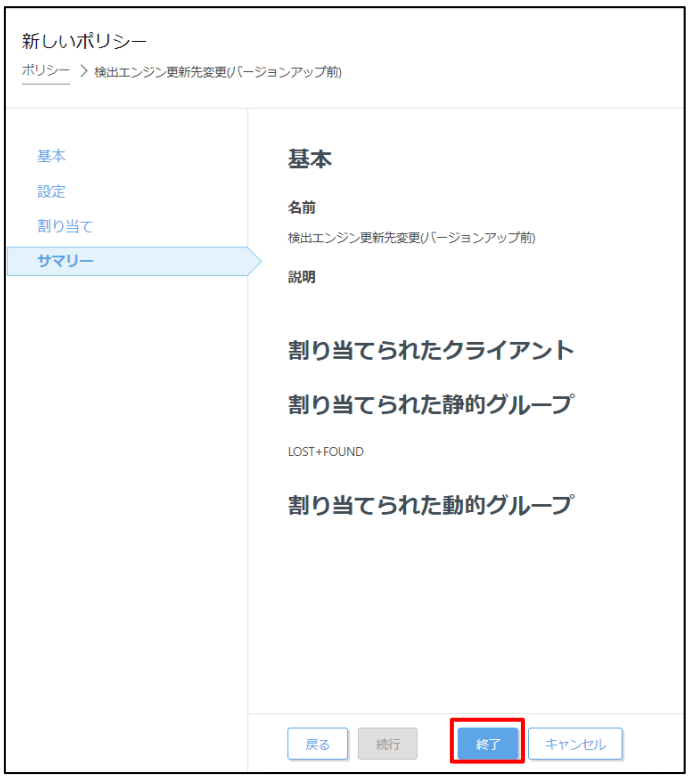
※ポリシー「検出エンジン更新先変更(バージョンアップ後)」を作成している場合は割り当てを行う必要はありません。後ほど STEP4 で作成する動的グループに割り当てを行います。

B-5-6. バージョンアップ前のクライアントが所属するグループを選択し、[OK]ボタンをクリックします。

※ここでは「LOST+FOUND」グループを選択します。



B-5-7. [サマリー]の内容を確認し、[終了]ボタンをクリックします。



しばらくすると、ポリシーが適用されます。

以上で、新バージョンに対応したミラーサーバーからのアップデート準備は完了です。

<参考>

サーバー用プログラムの ESSW または EFSW(管理ツールにインストールされているプログラムを除く)も管理している場合は、以下ご注意のうえ、ポリシーを作成してください。

① STEP2-5 のポリシー作成時の「手順 B-5-2」では、バージョンアップするサーバー用プログラムのためのポリシーであることが分かるような名前を入力してください。
② STEP2-5 のポリシー作成時の「手順 B-5-3」では、製品で「ESET Server/File Security for Windows Server(V6+)」を選択します。

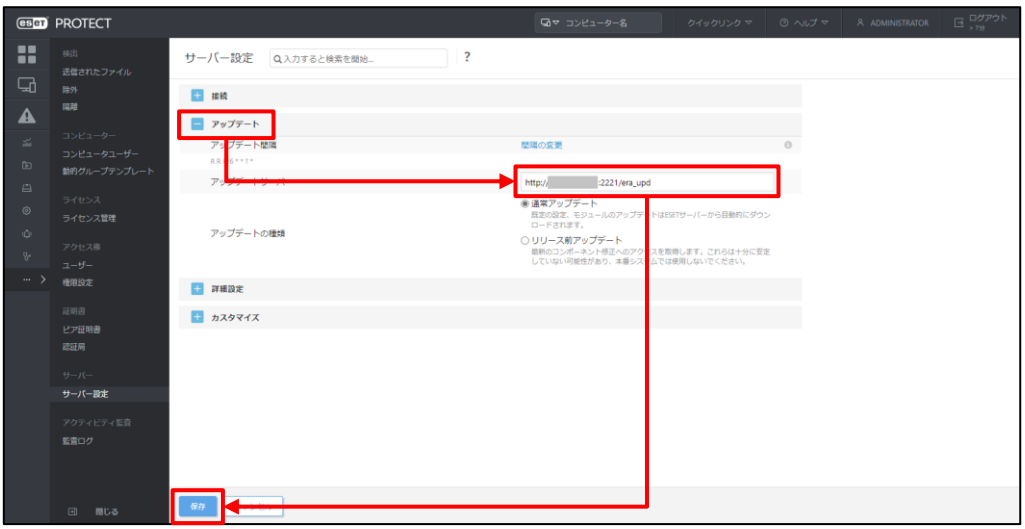
B-6. EP のアップデート先変更

EP のアップデート先を、「手順 B-1」で準備した検出エンジンのミラーサーバーからアップデートができるように設定を変更します。

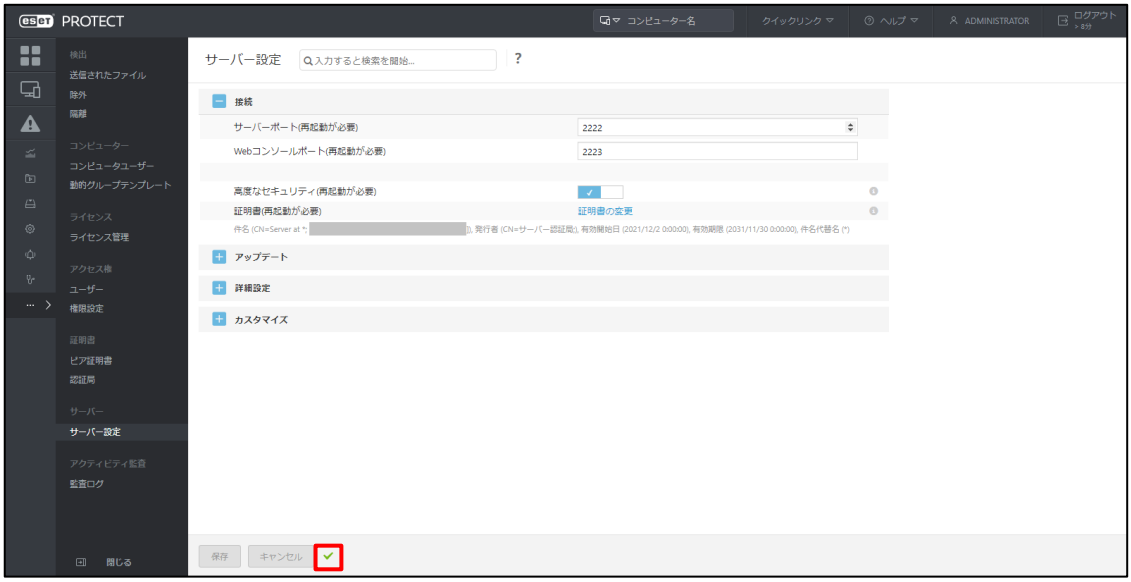
B-6-1. EP にログイン後、画面左側の「詳細」→「サーバー設定」をクリックします。

B-6-2. 「アップデート」→「アップデートサーバー」に「オンプレミス型セキュリティ管理ツールの検出エンジン」を「手順 B-2」で公開した Web サーバの URL を入力して、「保存」をクリックします。

※URL 例：http://"ミラーサーバーの IP アドレス":"ミラーサーバーの動作ポート"/era_upd

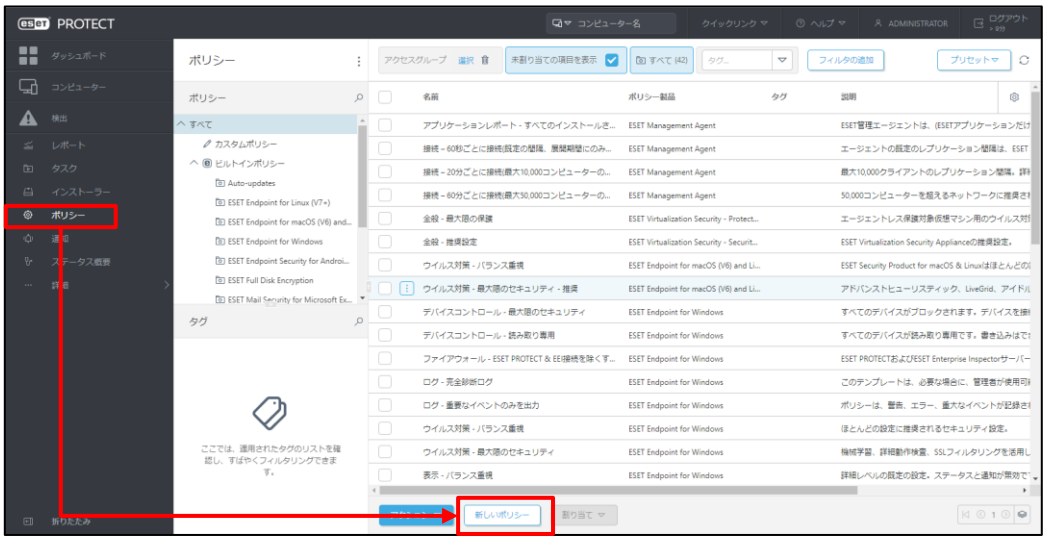


B-6-3. チェックが付き、設定が保存されていることを確認します。



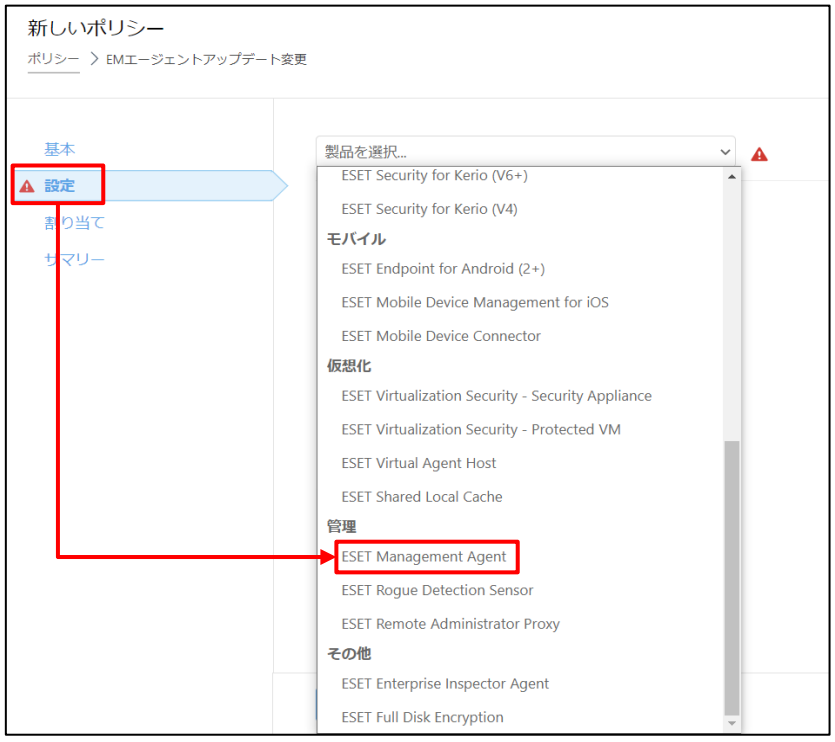
B-7. EM エージェントのアップデート先変更のポリシー作成

B-7-1. EP にログイン後、画面左側の「ポリシー」をクリックし、「新しいポリシー」をクリックします。



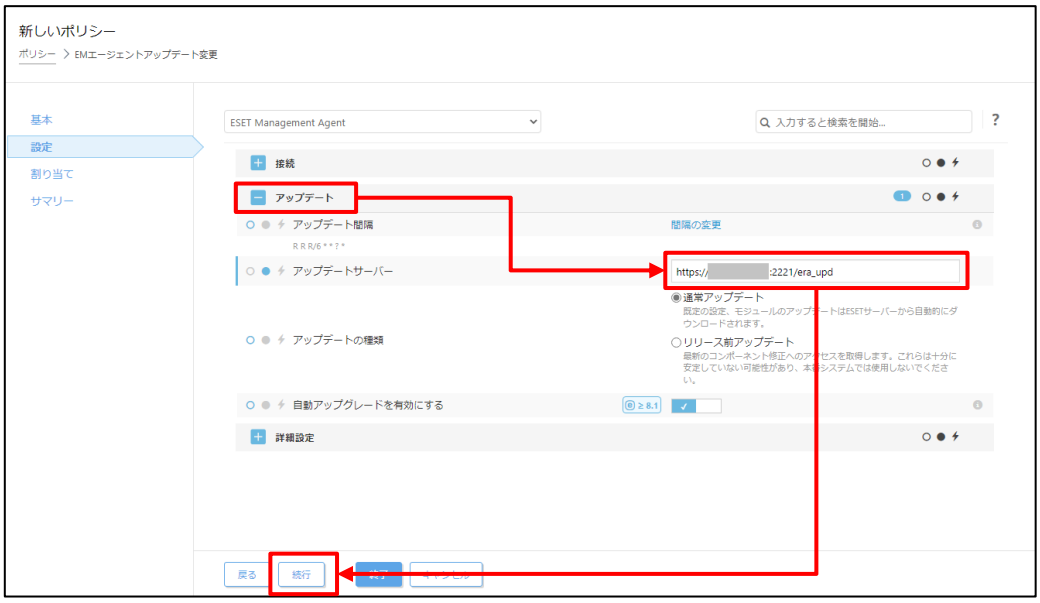
B-7-2. 「基本」を展開後、ポリシーの名前を任意に入力し、「続行」をクリックします。「説明」と「タグ」の設定は任意です。

B-7-3. 「設定」を展開後、「製品を選択...」欄にて[ESET Management Agent]を選択します

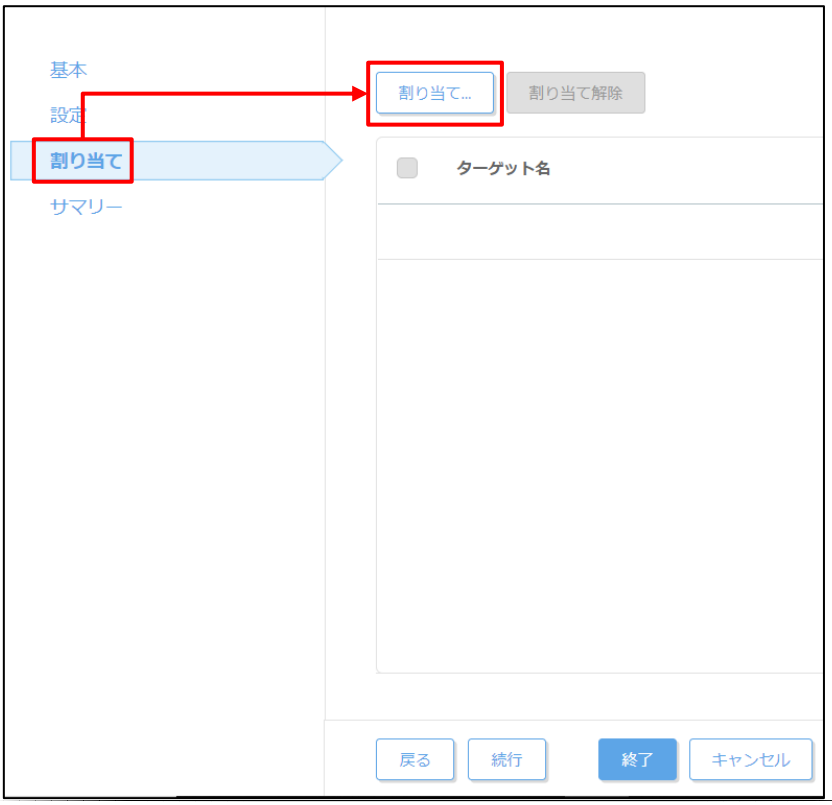


B-7-4.「アップデート」→「アップデートサーバー」に「オンプレミス型セキュリティ管理ツールの検出エンジン」を「手順 B-2」で公開している URL を入力して、「続行」をクリックします。

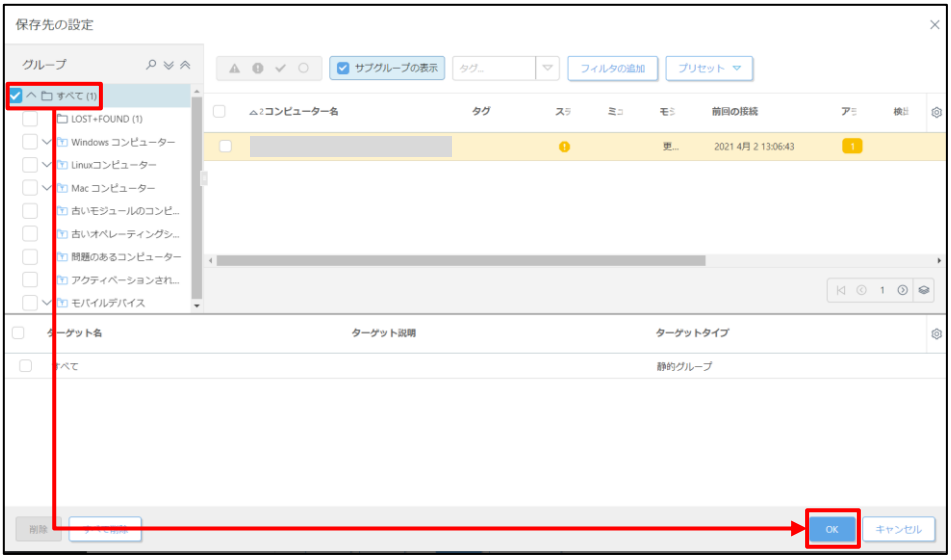
※URL 例：http://”ミラーサーバーの IP アドレス”:“ミラーサーバーの動作ポート”/era_upd



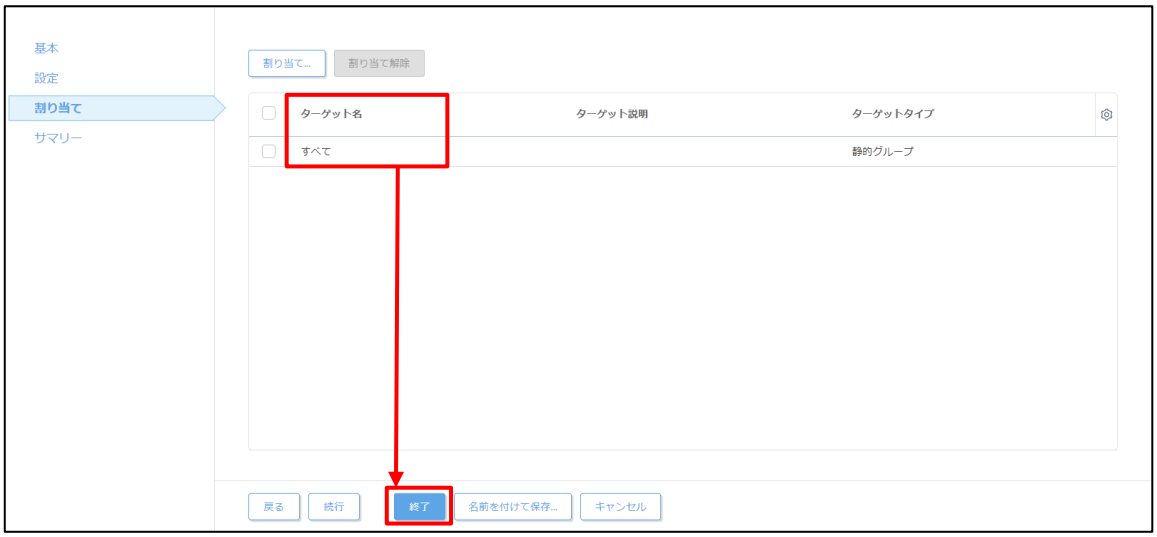
B-7-5.「割り当て」で、「割り当て...」をクリックします。



B-7-6. 「すべて」のグループにチェックを入れ、「OK」をクリックします。



B-7-7. 「すべて」のグループがターゲット名に表示されていることを確認し、「終了」をクリックします。



7．【STEP3】サーバーのバージョンアップ

サーバーにインストールされている EP と EFSW をバージョンアップします。

STEP3-1．動作要件の確認

バージョンアップの前に、EP V9.X と ESSW V9.X の動作要件を確認します。

＜ESET PROTECT 動作要件＞
https://eset-info.canon-its.jp/business/ep/#spec

＜ESET Server Security for Microsoft Windows Server 動作要件＞
・ESET PROTECT Entry オンプレミス(旧名称：ESET Endpoint Protection Advanced)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-entry-o/spec.html
・ESET PROTECT Essential オンプレミス(旧名称：ESET Endpoint Protection Standard)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-essential-o/spec.html

＜参考＞

EP V8.X 以降では、64bit 版の Java が必要です。
Oracle 社提供の Java Runtime Environment 8 は公式アップデートを終了しております。
公式アップデートが終了された後もセキュリティ管理ツールをご利用いただくことはできますが、新たなセキュリティパッチなどを含むアップデートは提供されないため、有償の JRE もしくは、無償のオープンソース JDK のご利用（移行）を推奨しています。

なお、EP V9.1 では Java17 のみ対象となりますのでご注意ください。
ご利用のソフトウェアが動作環境のバージョンを満たしているかご確認ください。バージョンアップが必要な場合は、Java17 を新規でインストールし、バージョンアップ完了後に不要になった古いバージョンの Java のアンインストールをお願いいたします。

＜参考＞

EP V8.X 以降では、Apache Tomcat 9(64bit)が必要です。
32bit 版を利用している場合は、32bit 版をアンインストール後、64bit 版をインストールしてからオンプレミス型セキュリティ管理ツールのバージョンアップを実施してください。
Apache Tomcat のバージョンアップ方法については、以下 URL をご参照ください。
＜Apache Tomcat のバージョンアップ方法＞
https://eset-support.canon-its.jp/faq/show/24431?site_domain=business

＜参考＞

Microsoft SQL Server 2008 R2 以前のデータベースをご利用の場合は、先に Microsoft SQL Server 2014 以降へアップグレードしたうえで、サーバーのバージョンアップを実施してください。

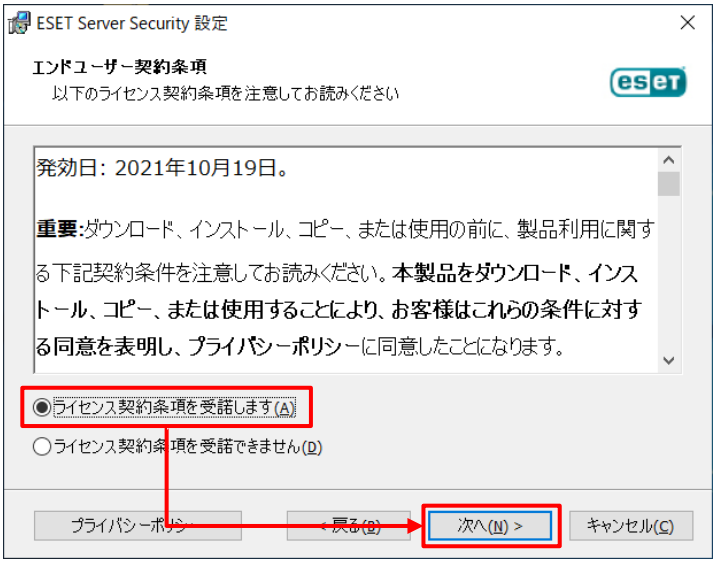
STEP3-2. ESET File Security for Microsoft Windows Server のバージョンアップ

以下の手順で ESET Server Security for Microsoft Windows Server V9.X へ上書きバージョンアップします。

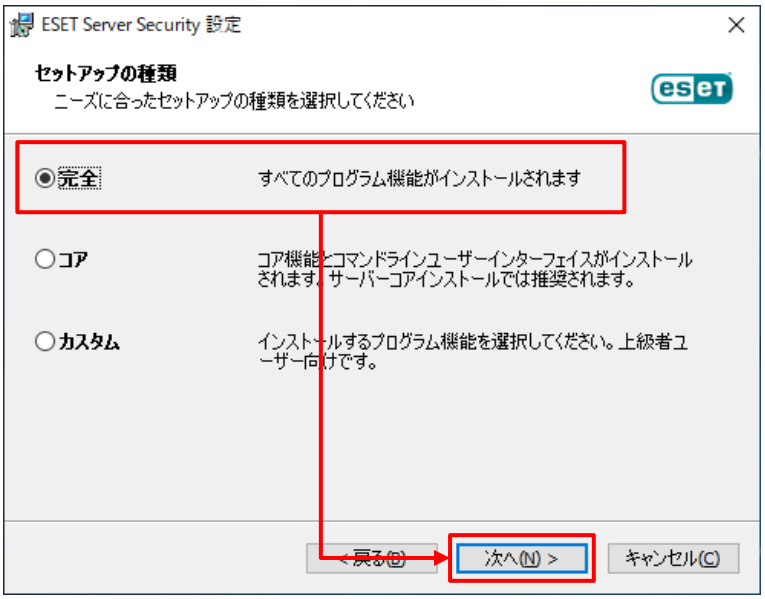
1. 【STEP0】事前準備でダウンロードした ESET Server Security for Microsoft Windows Server (V9)のインストーラーをサーバー上の任意の場所に移動し、ダブルクリックして実行します。

2. 「ESET Server Security セットアップウィザードへようこそ」画面が表示されます。[次へ]ボタンをクリックします。

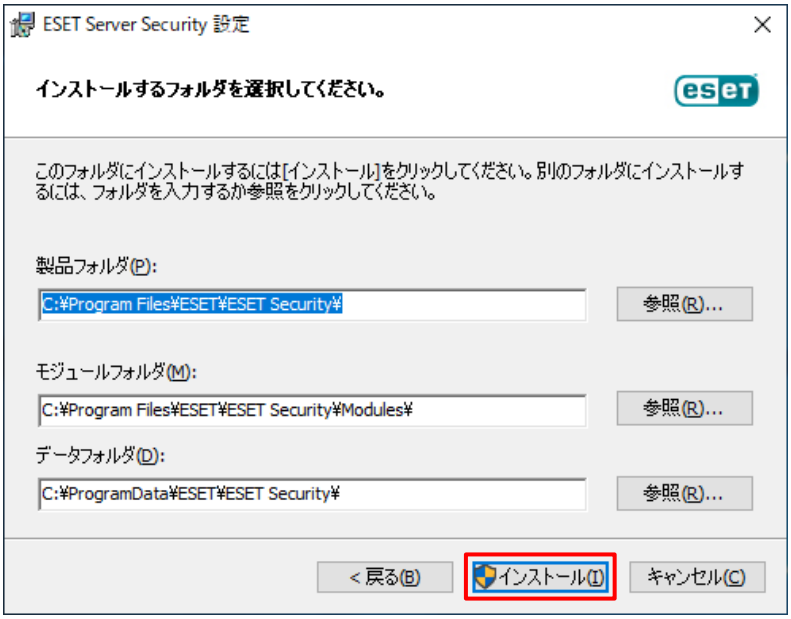
3. 「エンドユーザー契約条項」画面が表示されます。
「ライセンス契約条項」と「プライバシーポリシー」をご確認のうえ、「ライセンス契約条項を受諾します」のラジオボタンにチェックを入れ、[次へ]ボタンをクリックします。



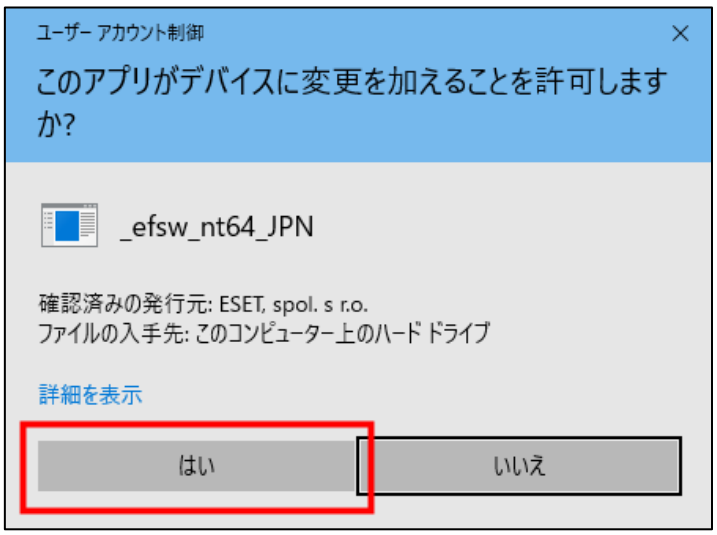
4. 「セットアップの種類」画面が表示されます。
[完全]のラジオボタンにチェックを入れ、[次へ]ボタンをクリックします。



5. 「インストールするフォルダを選択してください。」画面が表示されます。
[インストール]ボタンをクリックします。



6. 上書きインストールが開始します。インストールが完了するまでそのままお待ちください。
※ユーザーアカウント制御の画面が表示された場合は、[はい]ボタンをクリックします。



7. 上書きインストールが完了すると、「ESET Server Security セットアップウィザードを完了しています」画面が表示されます。
   [完了]ボタンをクリックし、画面を閉じてください。

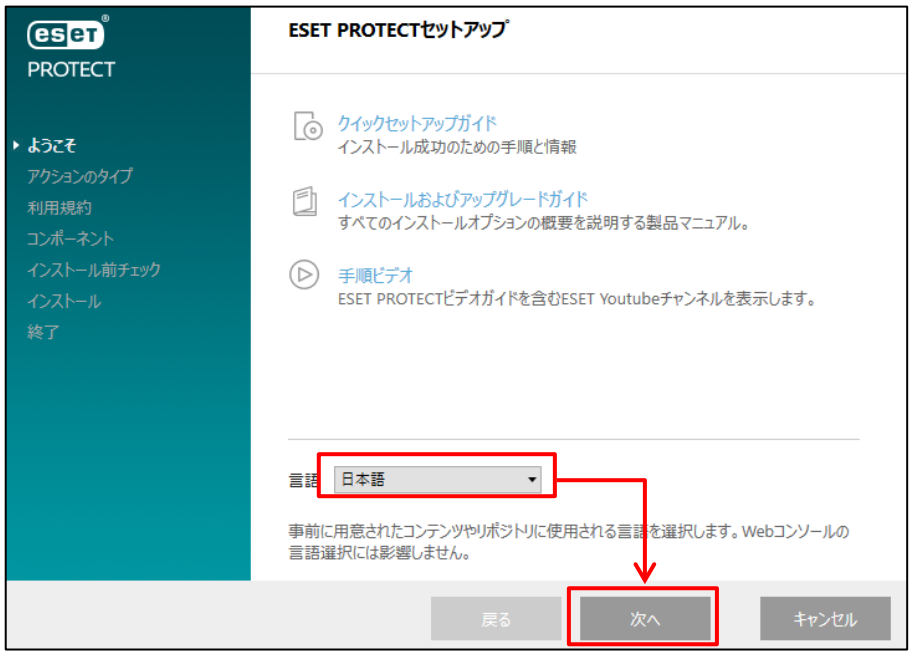
※「再起動」を促すアラートが表示されますが、次の【STEP3-3】を実行後に再起動いたします。

STEP3-3. ESET PROTECT のバージョンアップ

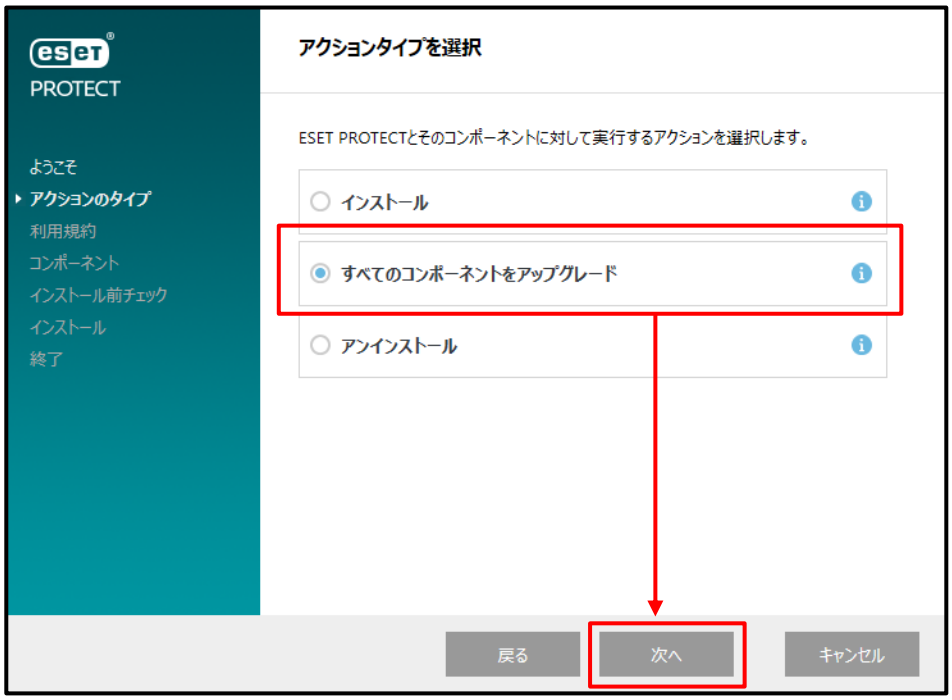
1. 【STEP0】事前準備でユーザーズサイトよりダウンロードした「ESET PROTECT(Ver 9.X.XX.X)」のオールインワンインストーラー「Setup_x64.zip」をサーバー上の任意の場所に配置します。

2. サーバーに配置した「Setup_x64.zip」を展開し、「Setup.exe」をダブルクリックで実行します。
   ※ユーザーアカウント制御の画面が表示された場合は、[はい]ボタンをクリックします。

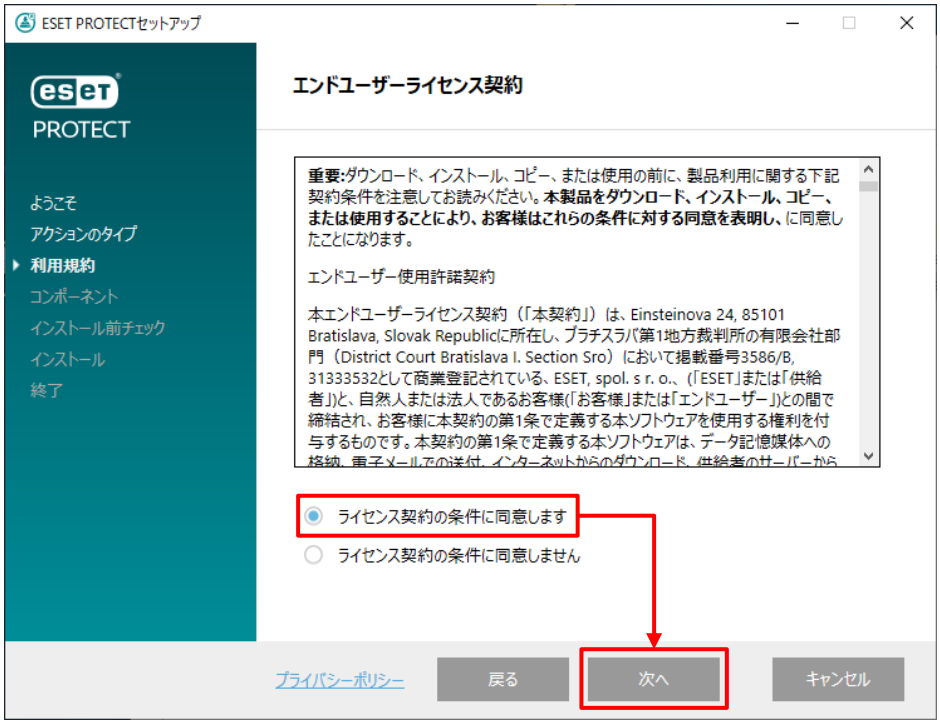
3. 言語で「日本語」を選択し、[次へ]ボタンをクリックします。



4. 「すべてのコンポーネントをアップグレード」を選択し、[次へ]ボタンをクリックします。

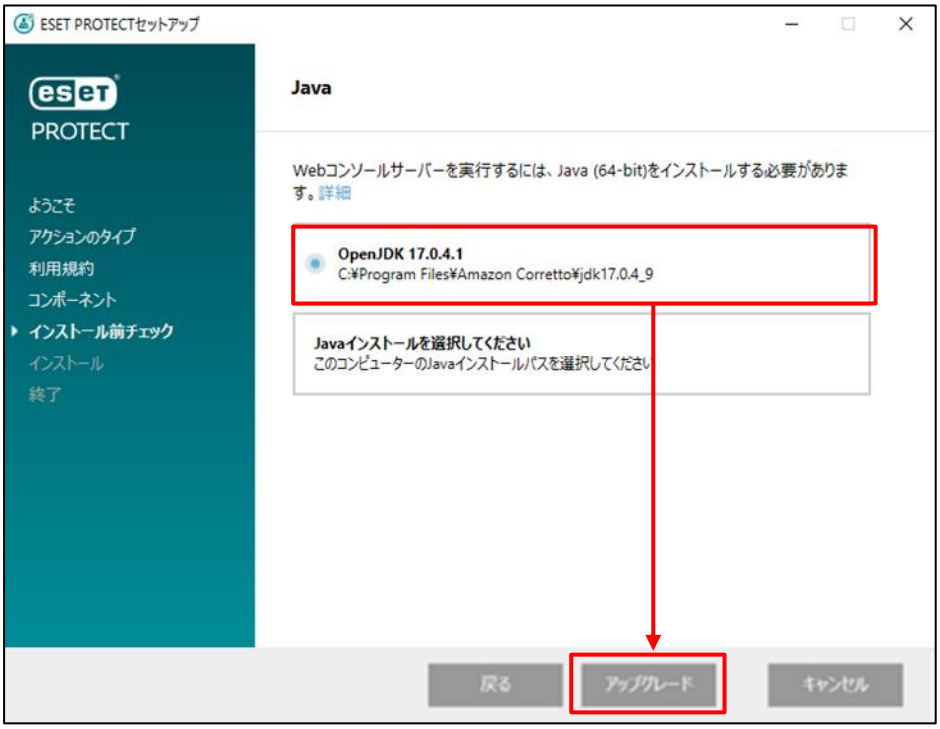


5. エンドユーザーライセンス契約に同意したら、「ラインセンス契約の条件に同意します」を選択し、[次へ]ボタンをクリックします。

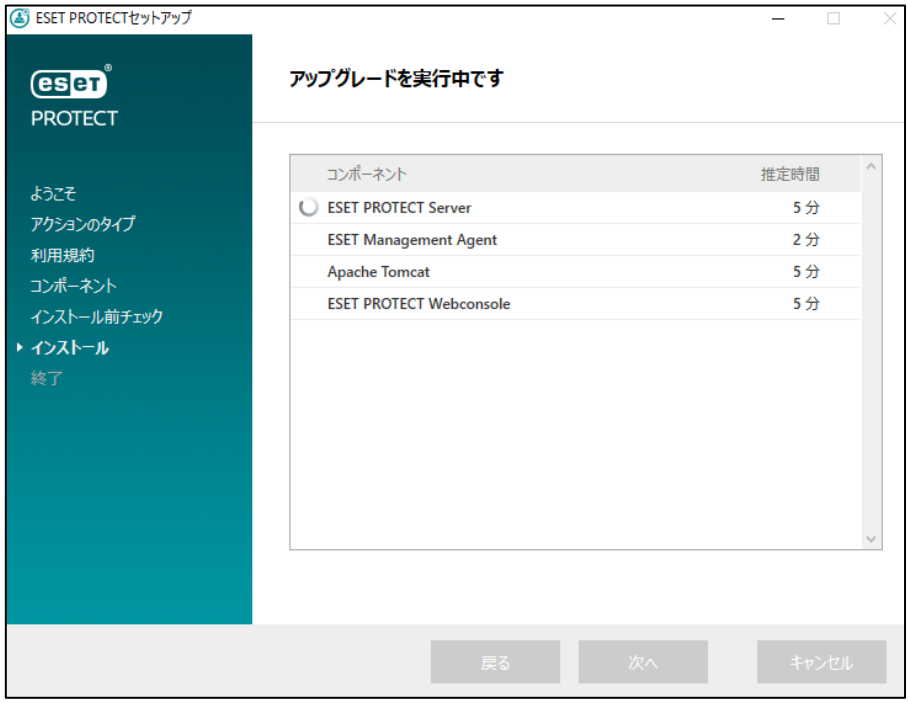


6. アップグレードするコンポーネントを確認し、[次へ]ボタンをクリックします。
※EP V8.X で利用しているコンポーネントがアップグレードされます。

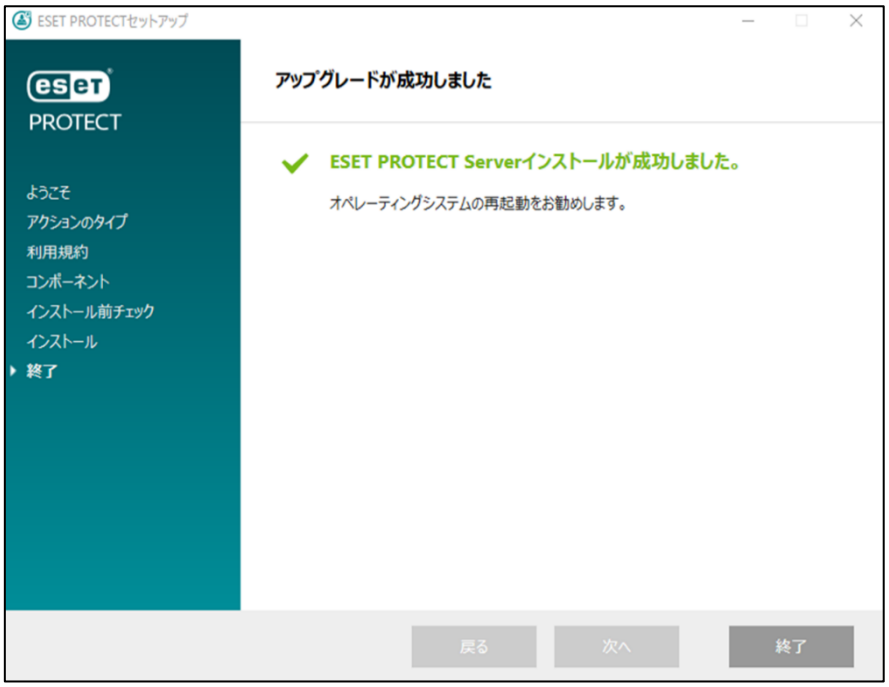
7. ご利用の Java を選択します。Amazon Corretto を利用している場合は、「OpenJDK」を選択し、[アップグレード]ボタンをクリックします。



8. アップグレードが実行されます。



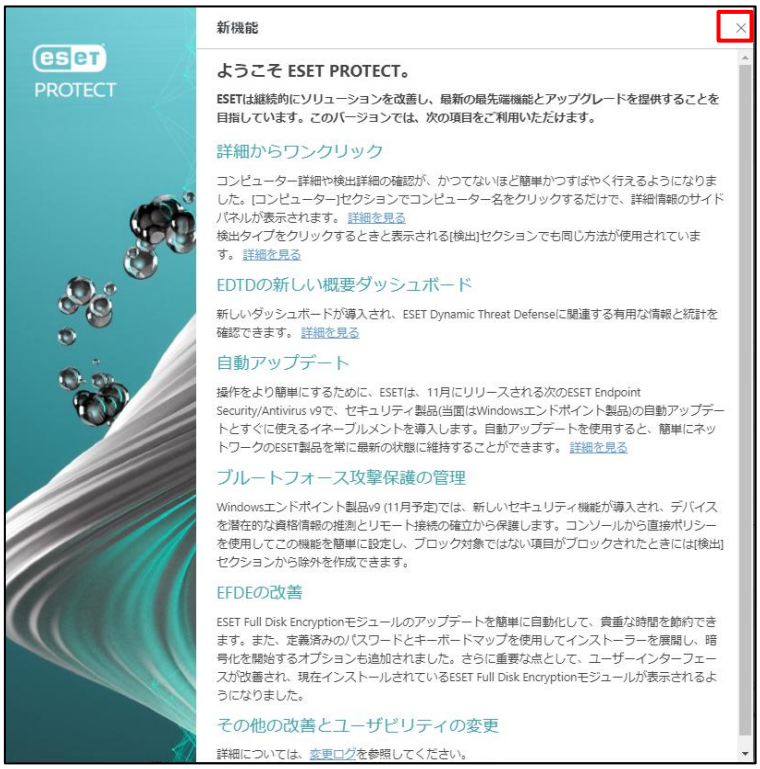
9. アップグレードが完了したら、以下の画面が表示されます。
[終了]ボタンをクリックします。



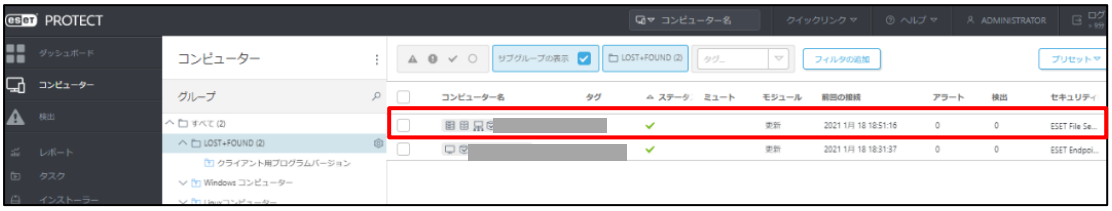
10. 再起動します。

11. EP Web コンソール を起動して、ESET PROTECT に接続します。
ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
※ EP Web コンソールには以下の URL よりアクセスできます。
https://＜管理サーバーのサーバー名、または、IP アドレス＞/era/

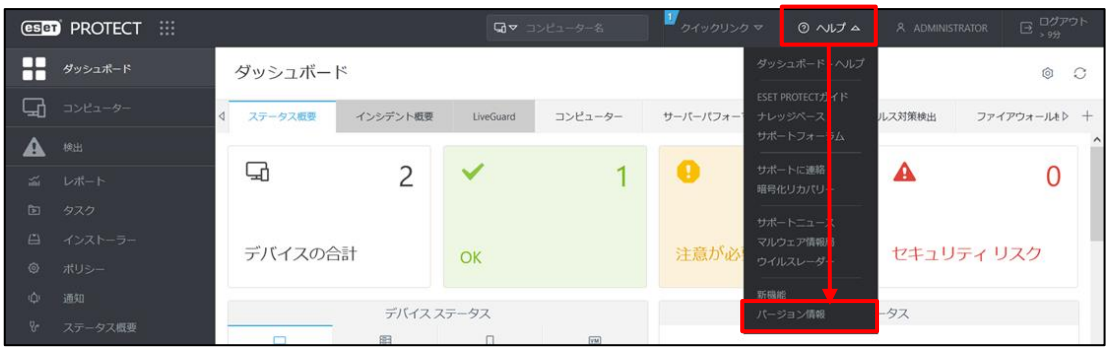
12. 以下の画面が表示されたら、「×」で閉じます。



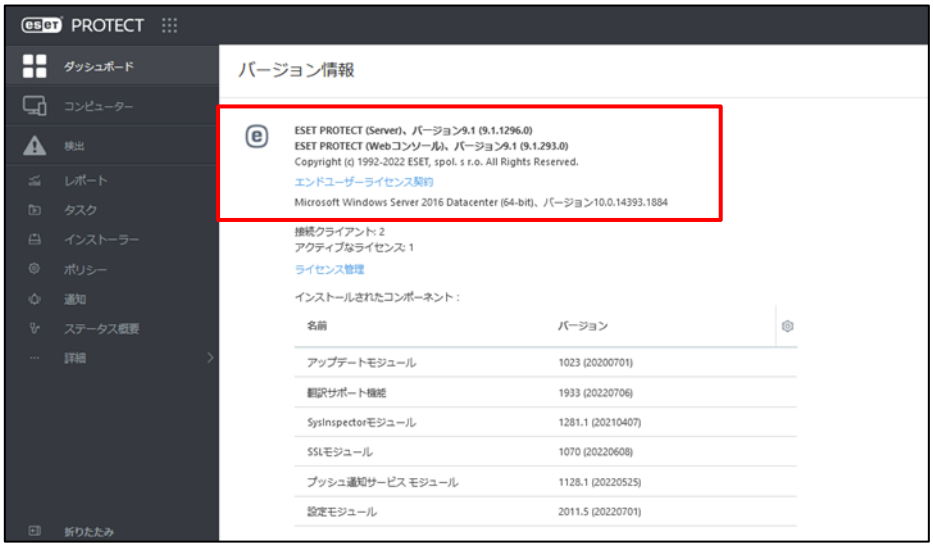
13. 「コンピューター」より、管理兼ミラーサーバーの再起動アラートが消えていることを確認します。
※他の原因でアラートが表示されている場合は、適宜ご対応ください。



14. 右上の[ヘルプ]-[バージョン情報]をクリックします。



15. 「ESET PROTECT(Server)」と「ESET PROTECT (Web コンソール)」バージョンが、「9.X」であることを確認します。



STEP3-4. データベースのバックアップ

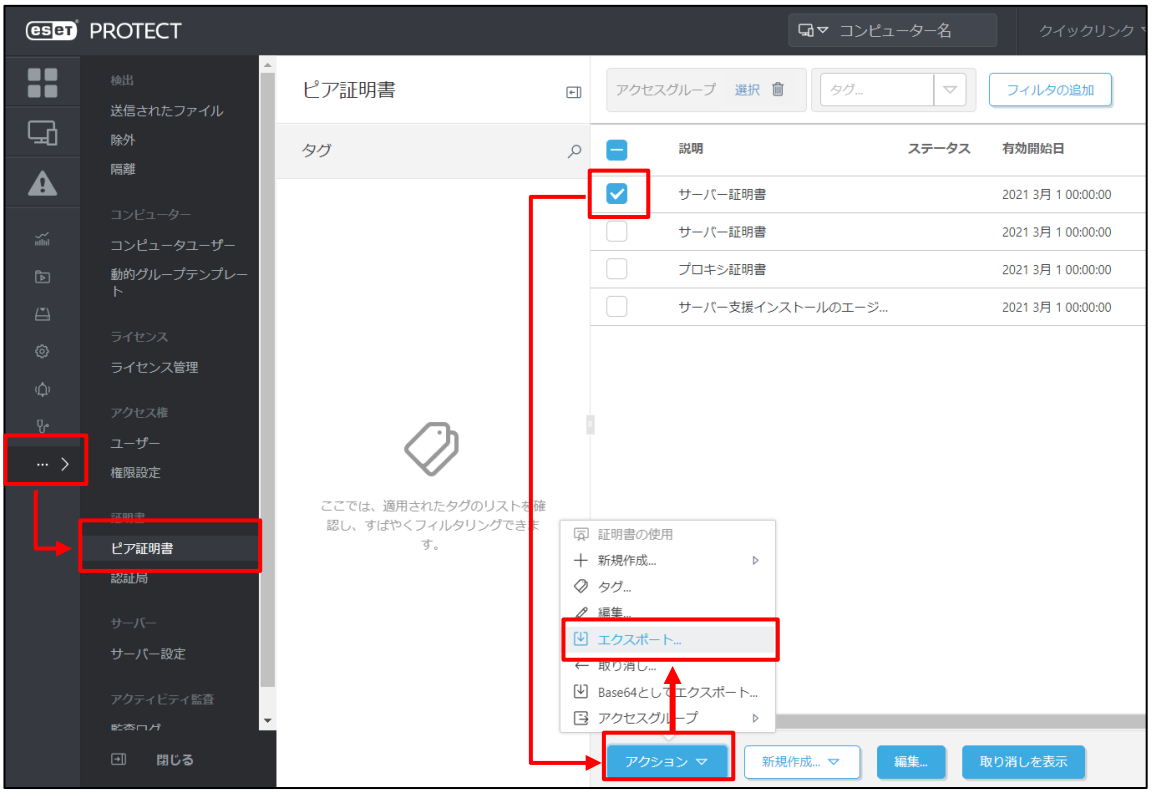
【STEP1】ESET PROTECT サーバーのバックアップと同様の方法で、再度 ESET PROTECT のデータベースとコンフィグレーションのバックアップを取得してください。

※バックアップ取得時には、「ESET PROTECT Sever」サービスを停止する必要がありますのでご注意ください。

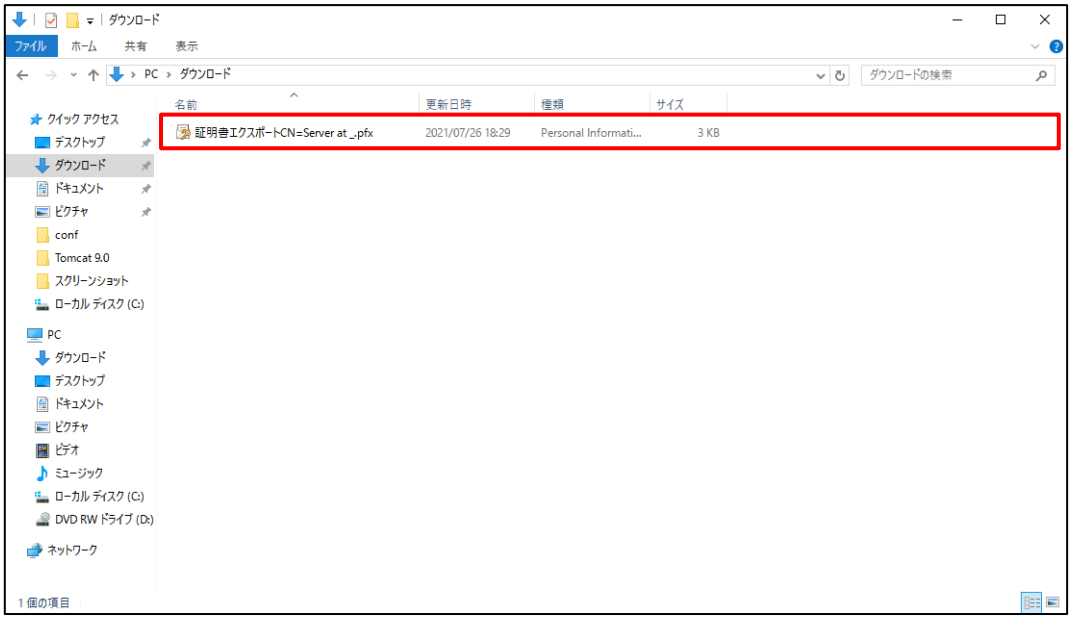
STEP3-5. ピア証明書と認証局のバックアップ

ESET PROTECT と EM エージェントの接続に使用しているピア証明書と認証局をエクスポートして、バックアップを取得します。

1. [詳細]-[ピア証明書]より、エクスポートを行う証明書を選択し、[アクション]より[エクスポート]をクリックします。

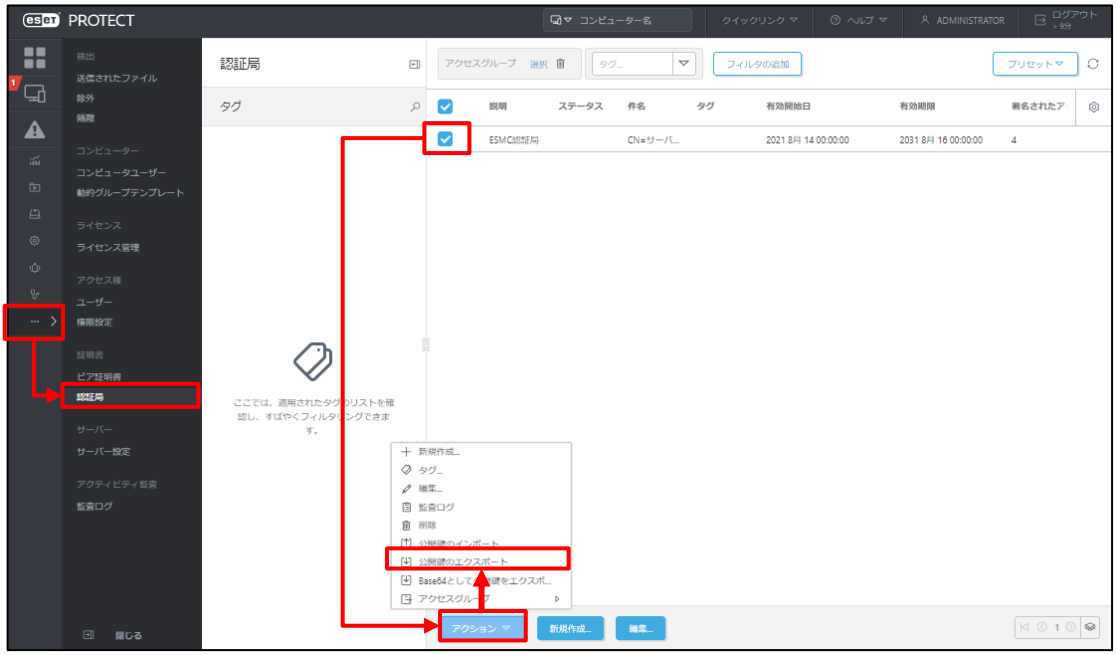


2. エクスポートした証明書を任意の保存先に保存します。

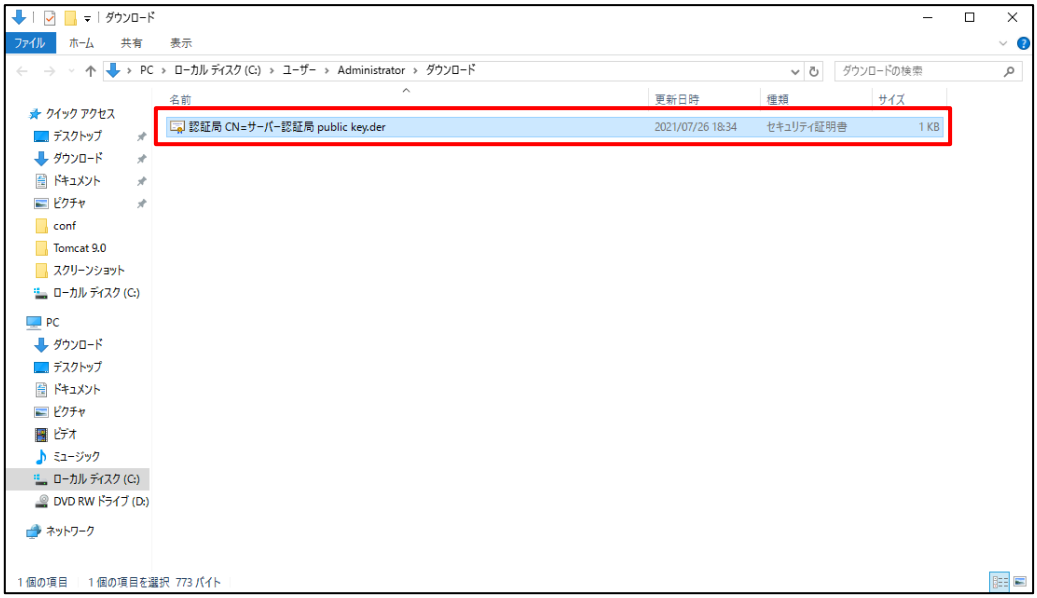


3. 手順 1～2 を繰り返し、各証明書のエクスポートを行います。

4. [詳細]-[認証局]より、エクスポートを行う認証局を選択し、[アクション]より[公開鍵のエクスポート]をクリックします。



5. エクスポートした公開鍵(認証局)を任意の保存先に保存します。



＜参考＞

不具合に伴うサーバーの再構築やリース切れに伴うサーバーのリプレースや増設をおこなう場合、クライアント端末の接続先を変更するため、旧サーバーのサーバー証明書や認証局を新サーバーにインポートする必要があります。
＜増設、または、新しく移行したセキュリティ管理ツールへ接続するには？＞
https://eset-support.canon-its.jp/faq/show/13248?site_domain=business

以上で、サーバーのバージョンアップは完了です。

8.【STEP4】 クライアントのバージョンアップ事前準備

STEP5 以降で、管理しているクライアント用プログラムとエージェントを V9.X にバージョンアップした後、自動で端末が振り分けられるバージョンアップ完了確認用のグループをそれぞれ作成します。また、STEP2 で作成したミラーサーバーからのアップデートに自動的に変更できるよう、作成した動的グループに STEP2 で作成したポリシーを配布します。

重要

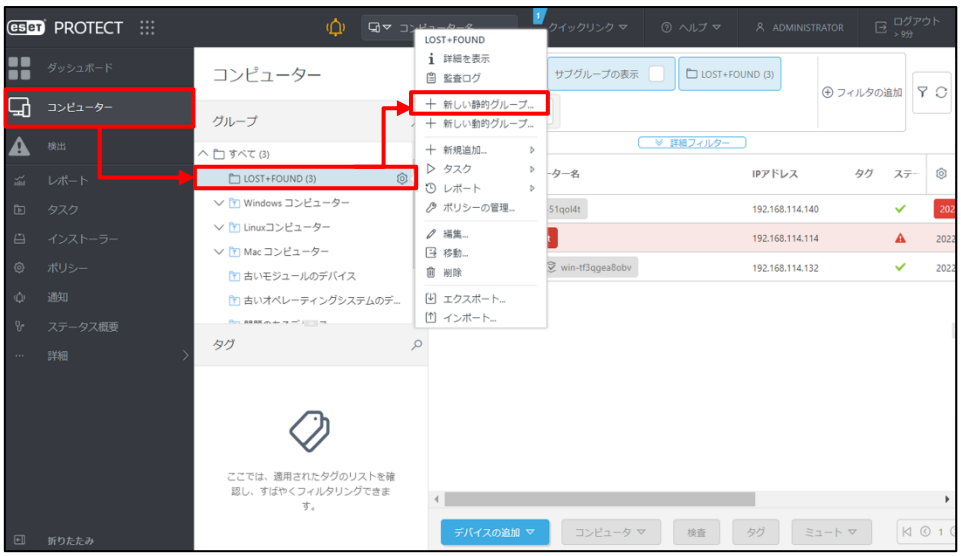
ユーザーズサイトから取得したファイルを IIS で公開している場合は、下記手順を参考に、バージョンアップ後に V9 用の検出エンジンの取得先を指定するポリシーも作成してください。
[STEP2]新ミラーサーバーの構築
-パターン B:EFSW V7.3 のミラー機能で公開している場合
-B-5. バージョンアップ前クライアントのアップデート先変更

STEP4-1. バージョンアップ完了確認用の動的グループ作成

※本資料では、EM エージェントのバージョンアップ完了確認用の動的グループを例に説明します。以下の手順を参考に、クライアント用プログラムのバージョンアップ完了確認用のグループも別途作成してください。

1. EP Web コンソール を起動して、ESET PROTECT に接続します。
   ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
   ※EP Web コンソールには以下の URL よりアクセスできます。
   https:// <管理サーバーのサーバー名、または、IP アドレス> /era/

2. 「コンピューター」より、バージョンアップを行うクライアント端末が所属する静的グループを選択し、[歯車]-[新しい動的グループ...]をクリックします。
※本手順では、既定でクライアントが所属する「LOST+FOUND」を選択します。



3. [基本]を展開し、任意の名前(例：EM エージェントバージョンアップ完了グループ)を入力します。
※クライアント用プログラムのバージョンアップ完了確認用の動的グループを作成する場合は、「例:クライアント用プログラムバージョンアップ完了グループ」と入力します。
※「説明」の入力は任意です。

4. [テンプレート]を展開し、[新規作成]ボタンをクリックします。

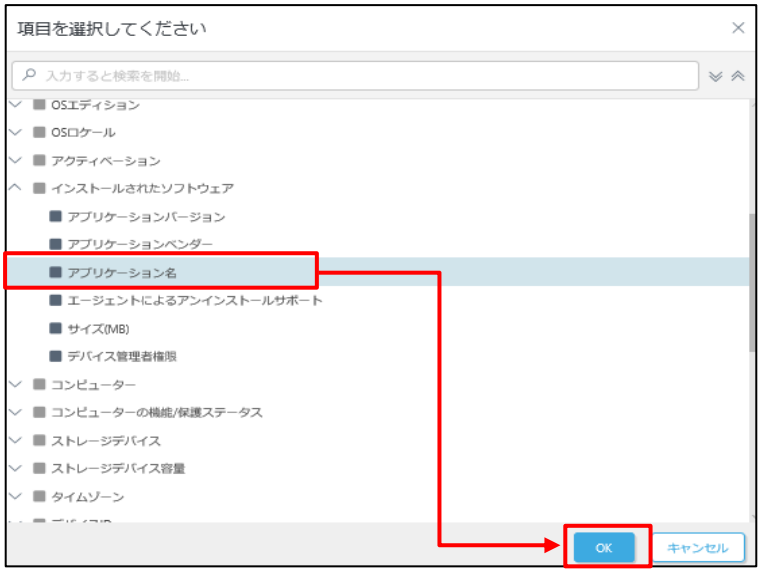
5. [基本]を展開し、任意の名前(例：EM エージェント自動振り分けテンプレート)を入力します。
※クライアント用プログラムバージョンアップ完了グループ作成の場合は、「例：クライアント用プログラムバージョンアップ完了自動振り分けテンプレート」を入力します。
※「説明」の入力は任意です。

6. [式]を展開し、処理に「AND(すべての条件が真であること)」を選択します。
「ルールの追加」をクリックします。

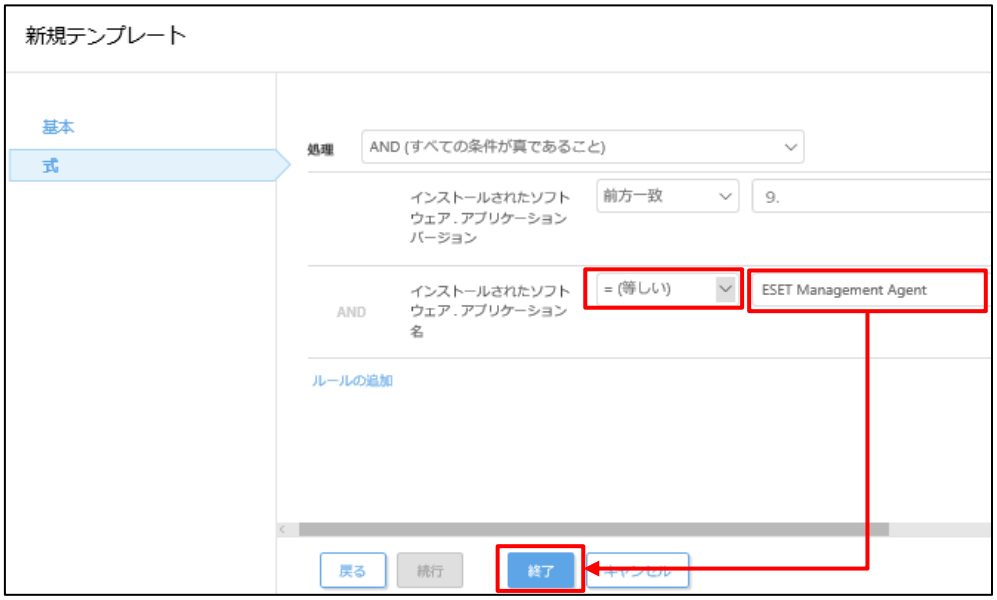
7. 「インストールされたソフトウェア」-「アプリケーションバージョン」を選択し、[OK]ボタンをクリックします。

8. 「前方一致」を選択し、条件に「9.」と入力します。
「ルールの追加」をクリックします。

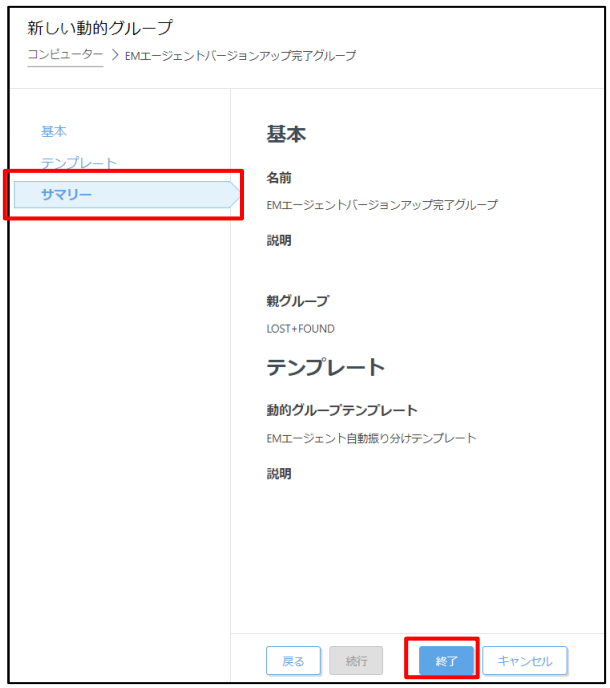
9. 「インストールされたソフトウェア」-「アプリケーション名」を選択し、[OK]ボタンをクリックします。



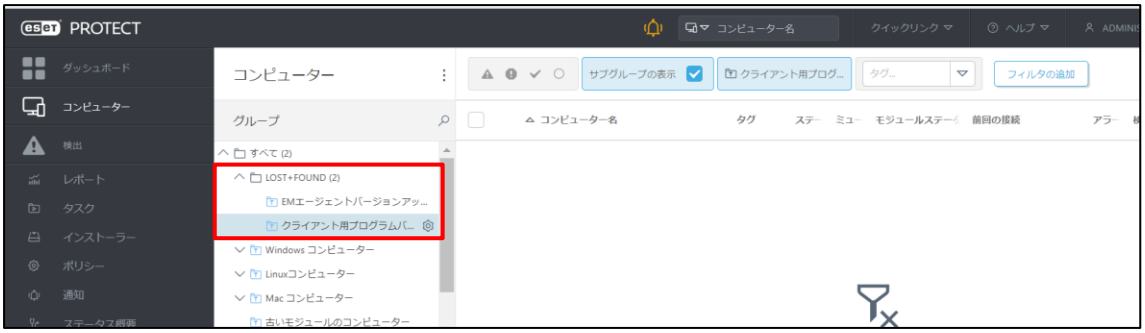
10. 「=(等しい)」を選択し、条件に「ESET Management Agent」を入力します。
「手順 8 で設定した条件」と「本手順 10 で設定した条件」の 2 つが指定されていることを確認し、[終了]ボタンをクリックします。
※クライアント用プログラムのバージョンアップ完了を確認する動的グループを作成する場合は、条件に「ESET Endpoint Security」または「ESET Endpoint Antivirus」を入力します。
※ESET Server Security for Microsoft Windows Server(管理ツール以外にインストールされている場合)のバージョンアップ完了を確認する動的グループを作成する場合は、「ESET Server Security」を入力します。



11. 「サマリー」の内容を確認し、問題がなければ[終了]ボタンをクリックします。



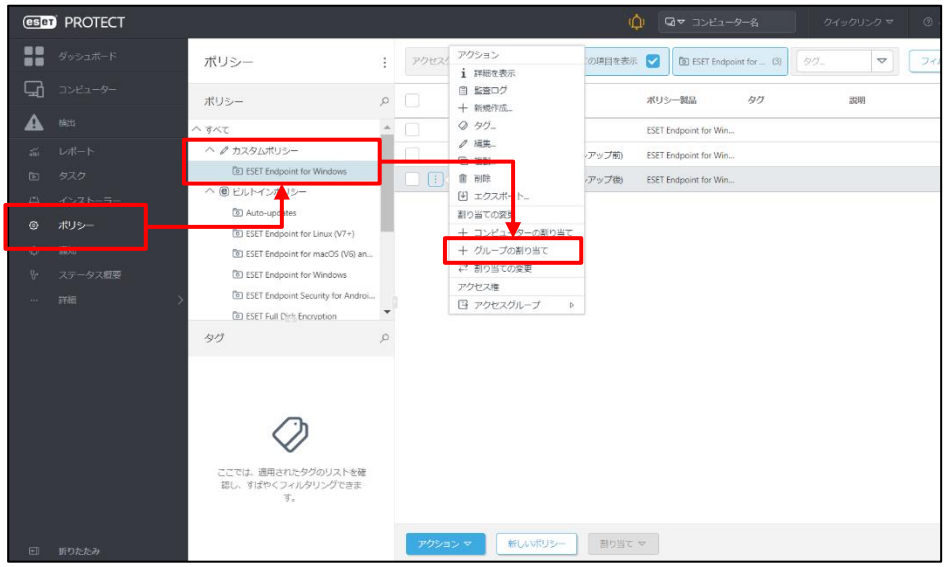
12. バージョンアップするクライアント端末が所属する静的グループ下に、作成した動的グループがあることを確認します。



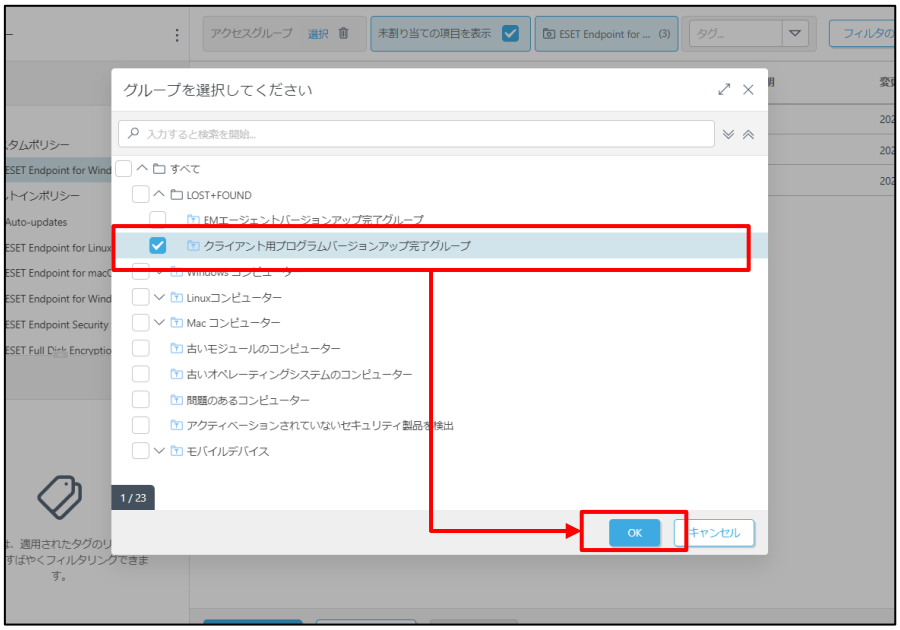
STEP4-2. 動的グループへのポリシー適用

バージョンアップが完了したクライアント用プログラムが、STEP2 で構築した新ミラーサーバーの新バージョン用フォルダー(例：ess9_upd)から自動で検出エンジンのアップデートができるように、STEP4-1 で作成した動的グループにポリシーを割り当てておきます。

1. [ポリシー]-[カスタムポリシー]より、STEP2 で作成した**「検出エンジン更新先変更(バージョンアップ後)」**を選択し、「＋グループの割り当て」をクリックします。



2. 「STEP4-1」で作成した動的グループ「クライアント用プログラムバージョンアップ完了グループ」を選択し、「OK」ボタンをクリックします。



9.【STEP5】エージェントおよびクライアント用プログラムのバージョンアップ

■バージョンアップ方法パターン分け■

重要

【STEP5】で行う「エージェントおよびクライアント用プログラムのバージョンアップ」作業は、お客様の環境によってバージョンアップ方法が異なります。
以下のパターン分けとお客様環境をご確認いただき、バージョンアップを行ってください。

パターン A:インストーラーをローカル実行してバージョンアップする場合(P53～P59)

パターン B:共有フォルダを使用してセキュリティ管理ツールからバージョンアップする場合(P60～P83)

パターン C:Web サーバーを使用してセキュリティ管理ツールからバージョンアップする場合 (P84～P95)

パターンD:AD 環境で GPO を使用してバージョンアップする場合(P96～P108)

パターン A：インストーラーをローカル実行してバージョンアップする場合

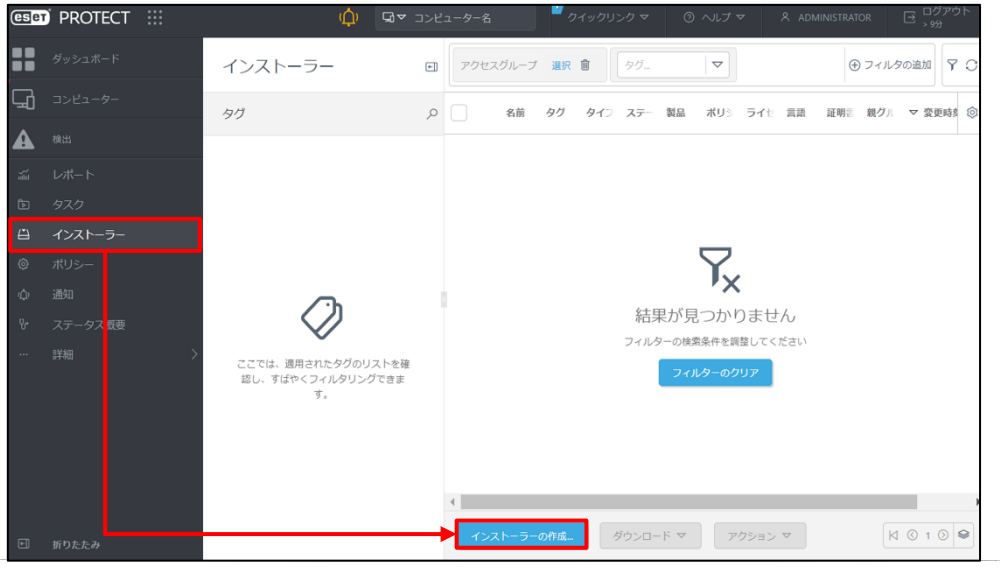
a. EM エージェントのバージョンアップ

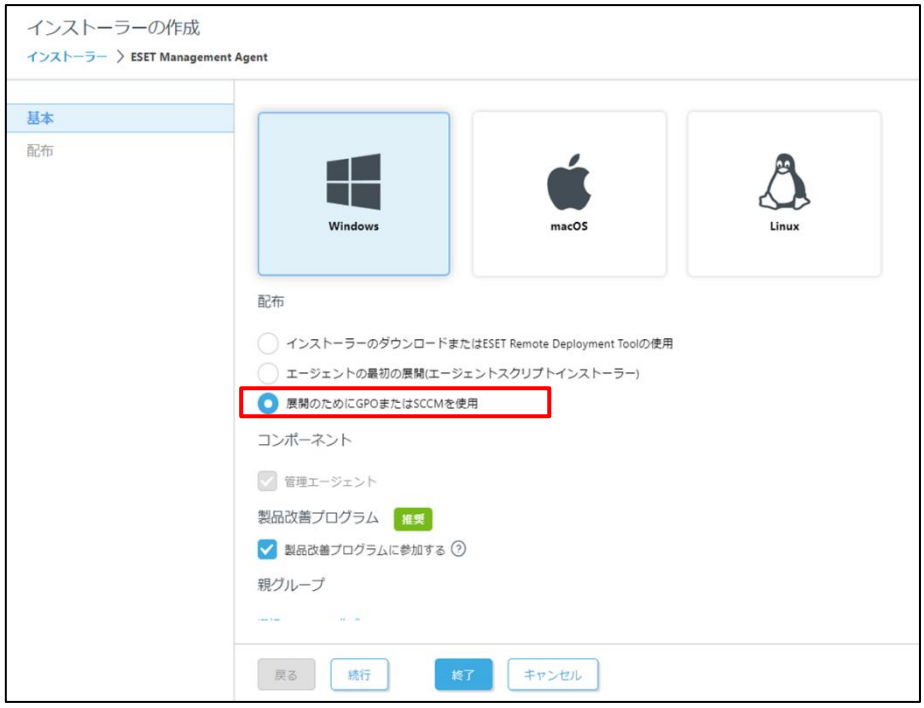
各クライアント端末にインストールされている EM エージェント V8.X を V9.X にバージョンアップします。

a-1. EM エージェントバージョンアップ用の GPO または SCCM スクリプトの準備

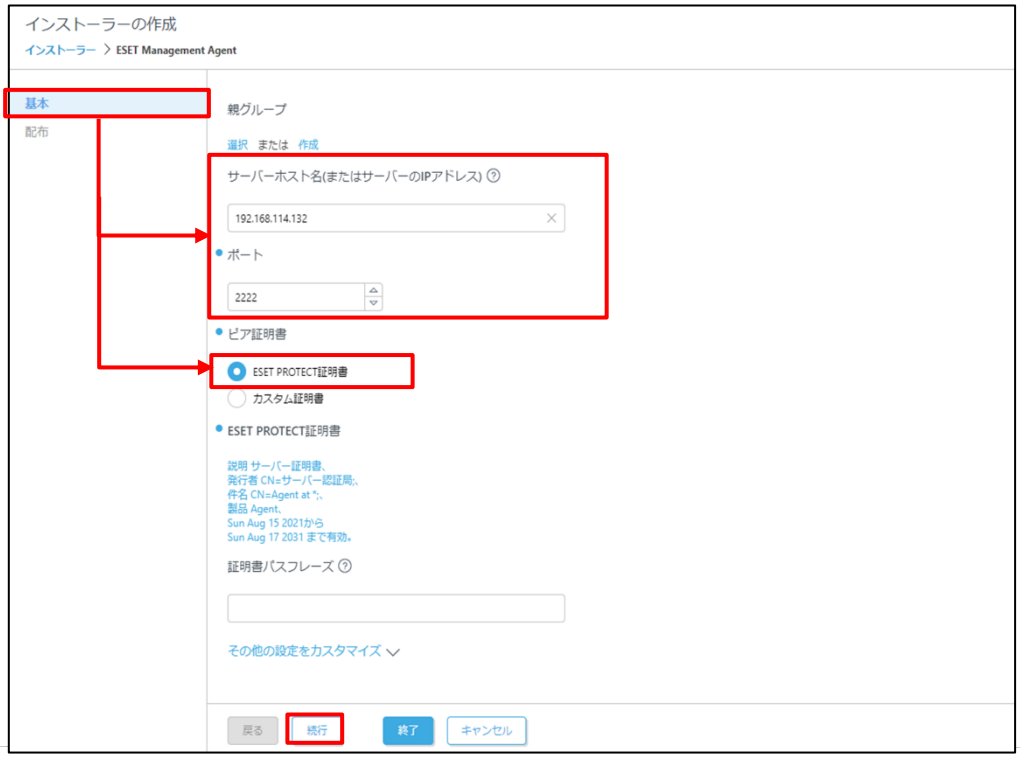
1. EP Web コンソール を起動して、ESET PROTECT に接続します。
   ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
   ※ EP Web コンソールには以下の URL よりアクセスできます。
   https://＜管理サーバーのサーバー名、または、IP アドレス＞/era/

2. [インストーラー]より、[インストーラーの作成]-[GPO または SCCM スクリプト]を選択します。

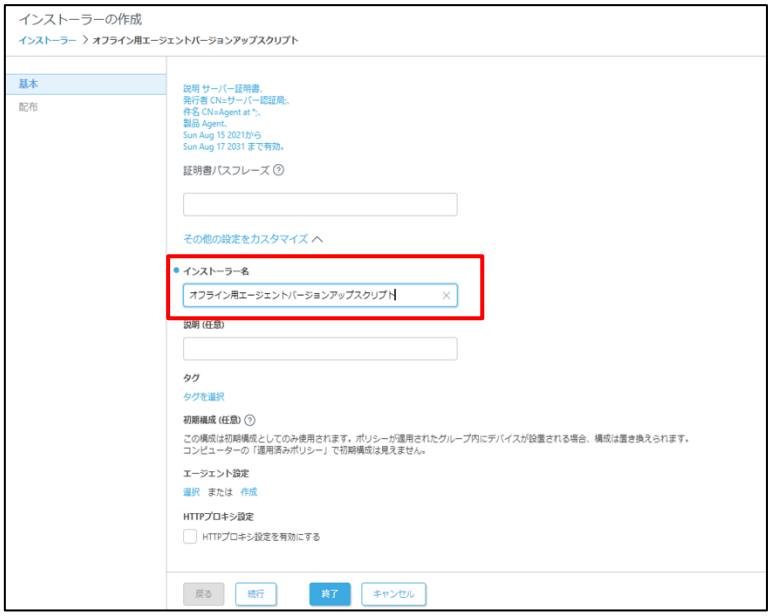




3. 「サーバーホスト名(またはサーバーの IP アドレス)」と「ポート」を確認します。
[ピア証明書]で「ESET PROTECT 証明書」を選択し、[続行]ボタンをクリックします。
※クライアント端末が所属する静的グループ情報は引き継がれるため、「親グループ」の設定は必要ありません。



4. インストーラー名に任意の名前を入力します。(例：オフライン用エージェントバージョンアップスクリプト)
   ※「説明」の入力は任意です。



5. [終了]ボタンをクリックします。
   「GPO または SCCM スクリプト(ファイル名例：install_config.ini)」がダウンロードされますので、任意の場所に保存します。

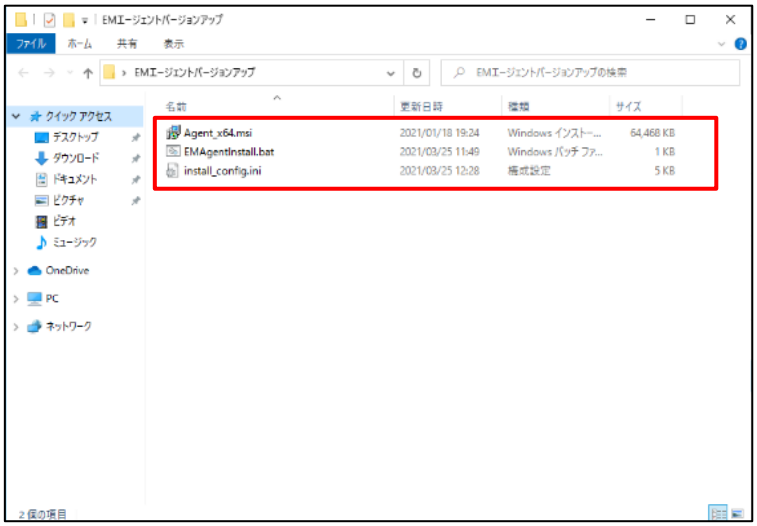
   以上で、Web コンソール上での操作は完了です。

a-2. EM エージェントバージョンアップ用のバッチファイルの準備

1. 端末でメモ帳などを開き、以下のコマンドを入力して、バッチファイルとして任意の名前を付けて保存します。(ファイル名例：EMAgentInstall.bat)
   ※「Agent_x64.msi」部分は、EM エージェントのインストーラー名を記入します。

```
@echo off
cd /d %~dp0
msiexec /i Agent_x64.msi /qb!
```

2. <a-1>で Web コンソールからダウンロードした**「GPO または SCCM スクリプト」の ini ファイル(ファイル名例：install_config.ini)**と手順 1 で作成した**「バッチファイル」**、【STEP0】事前準備でダウンロードした**「EM エージェント V9.X」**のインストーラーを同じフォルダに格納します。

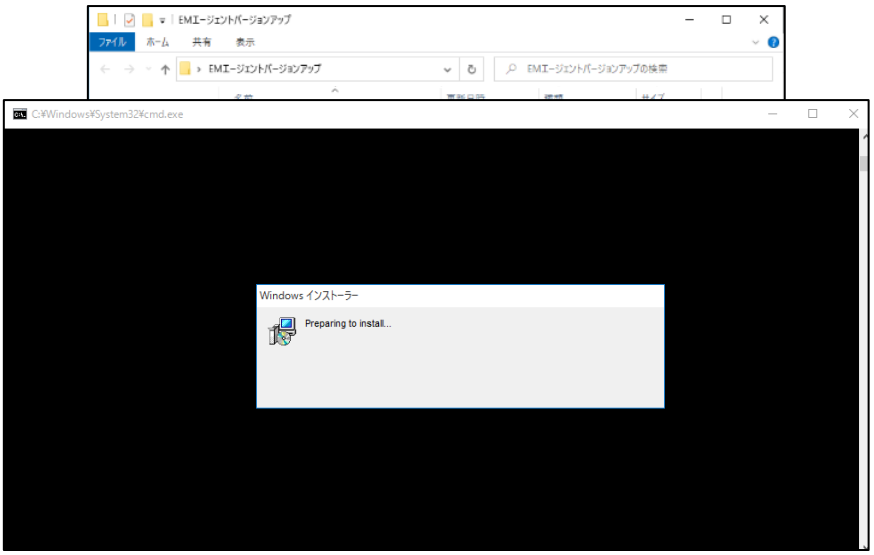


3. 手順 2 で作成したフォルダをお客様環境に合わせた方法で、バージョンアップを行うクライアント端末に配布します。(社内の共有フォルダなど)

a-3.EM エージェントのバージョンアップ

＜a-2＞で各クライアント端末に配布したフォルダ内のバッチファイルを使用し、クライアント端末の EM エージェントをバージョンアップしていきます。

1. 各クライアント端末上で、＜a-2＞で作成したフォルダ内のバッチファイル「EMAgentInstall.bat」を右クリックして、「管理者として実行」します。
   ※「ユーザーアカウント制御」画面が表示されたら、[はい]ボタンをクリックします。



2. EM エージェントのバージョンアップが始まります。Windows インストーラーの画面とコマンドプロンプト画面が消えたらバージョンアップ完了です。

以上で、EM エージェントのバージョンアップ作業は完了です。

b. クライアント用プログラムのバージョンアップ

b-1. 動作要件の確認

バージョンアップの前に、EES V9.X と EEA V9.X の動作要件を確認します。
＜ESET Endpoint Security / ESET Endpoint アンチウイルス 動作要件＞
・ESET PROTECT Entry オンプレミス(旧名称：ESET Endpoint Protection Advanced)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-entry-o/spec.html
・ESET PROTECT Essential オンプレミス(旧名称：ESET Endpoint Protection Standard)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-essential-o/spec.html

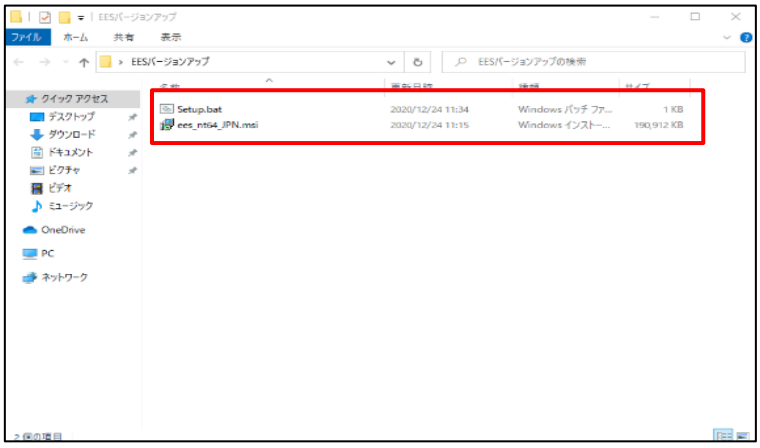
b-2. クライアント用プログラムのバージョンアップ用バッチファイルの準備

クライアント用プログラムをサイレントでバージョンアップするためのバッチファイルを作成します。

1. 任意の端末でメモ帳などを開き、以下のコマンドを入力して、バッチファイルとして任意の名前を付けて保存します。(ファイル名例：Setup.bat)
   ※「ees_nt64_JPN.msi」部分は、クライアント用プログラムのインストーラー名を記入します。

```
@echo off
msiexec /i ees_nt64_full.msi /qb! INSTALLED_BY_ERA=1
```

2. 手順 1 で作成した**「バッチファイル」**と、【STEP0】事前準備でダウンロードした**「EES V9.X または EEA V9.X のインストーラー」**を同じフォルダに格納します。



手順 2 で作成したフォルダをお客様環境に合わせた方法で、バージョンアップを行うクライアント端末に配布します。(社内の共有フォルダなど)

b-3. クライアント用プログラムのバージョンアップ

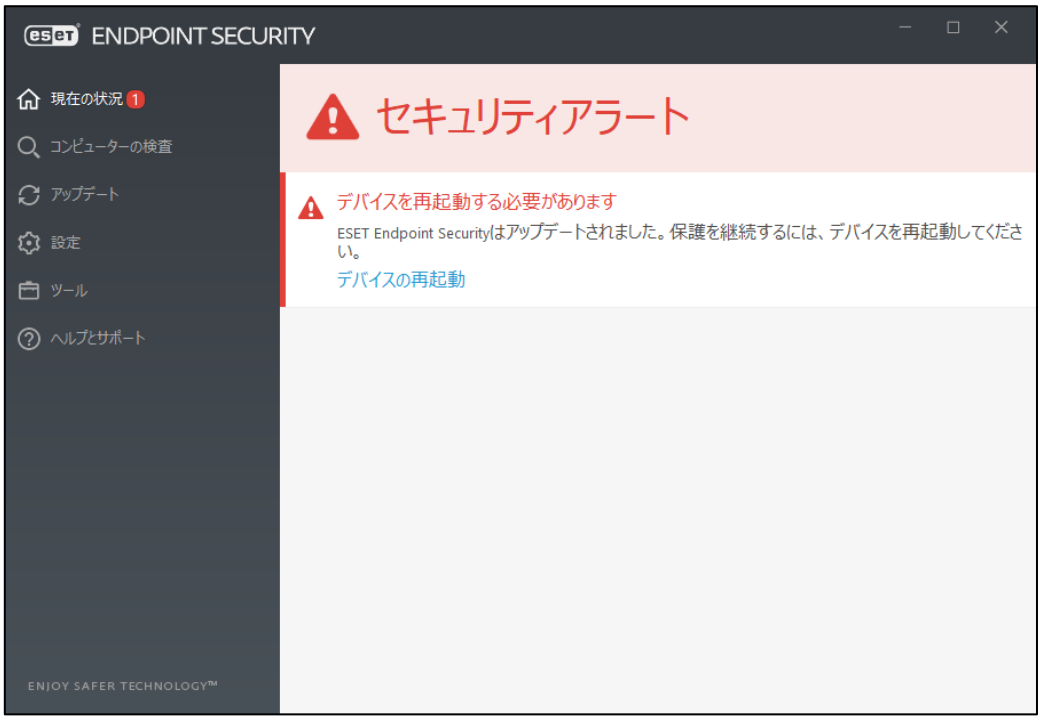
＜b-2＞で各クライアント端末に配布したフォルダ内のバッチファイルを使用して、クライアント用プログラムのバージョンアップを行います。

1. 各クライアント端末の配布されたフォルダ内のバッチファイルをダブルクリックして実行します。
   ※ユーザーアカウント制御の画面が表示された場合は、[はい]ボタンをクリックします。

2. 上書きバージョンアップが実行されます。

3. バージョンアップ完了後、必ず再起動を行います。

※「リアルタイムファイルシステム保護は機能していません」というアラートが表示される場合は、
再起動により解消されます。



再起動が終了したら、クライアント用プログラムのバージョンアップは完了です。

以上で、【パターン A：インストーラーをローカル実行してバージョンアップする場合】は完了です。
最後に【STEP6】で各プログラムのバージョンが完了したことを確認します。

パターン B:共有フォルダを使用してセキュリティ管理ツールからバージョンアップする場合

a. EM エージェントのバージョンアップ

各クライアント端末にインストールされている EM エージェント V9.X を V10.X にバージョンアップします。

※本手順は 64bit 端末を前提としています。32bit 端末が存在する場合は、端末ごとに分けて実施ください。

※各タスクを実行する際は端末のタスクの実行状況を確認したうえで、次のタスクの実行をお願いいたします。

a-1.共有フォルダの準備

1. クライアントからアクセス可能な端末にて共有フォルダの作成をお願いします。また、共有フォルダに Everyone フルコントロールにて公開をしてください
   ※本資料では C ドライブ直下の「test」フォルダを作成する前提としております。

a-2. EM エージェントのプログラムの準備

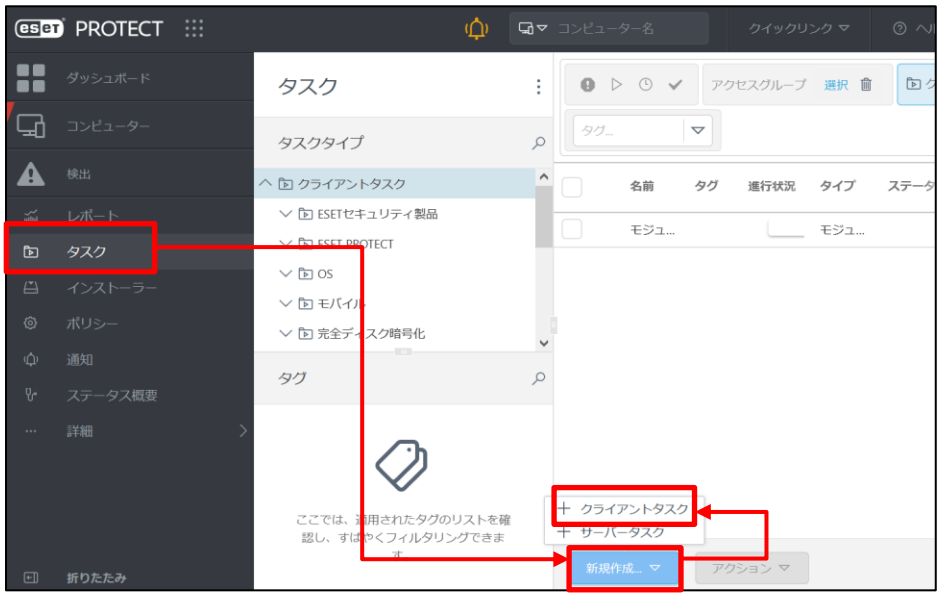
1. 【STEP0】にて用意した ESET Management エージェントを＜a-1＞で用意した共有フォルダに保存します。

a-3.EM エージェントのバージョンアップ

＜a-2＞で保存した共有フォルダ内の EM エージェントを使用して、クライアント端末の EM エージェントをバージョンアップしていきます。
バージョンアップ実施にあたり、コマンド実行タスクを 2 回実施いたしますのでご注意ください。

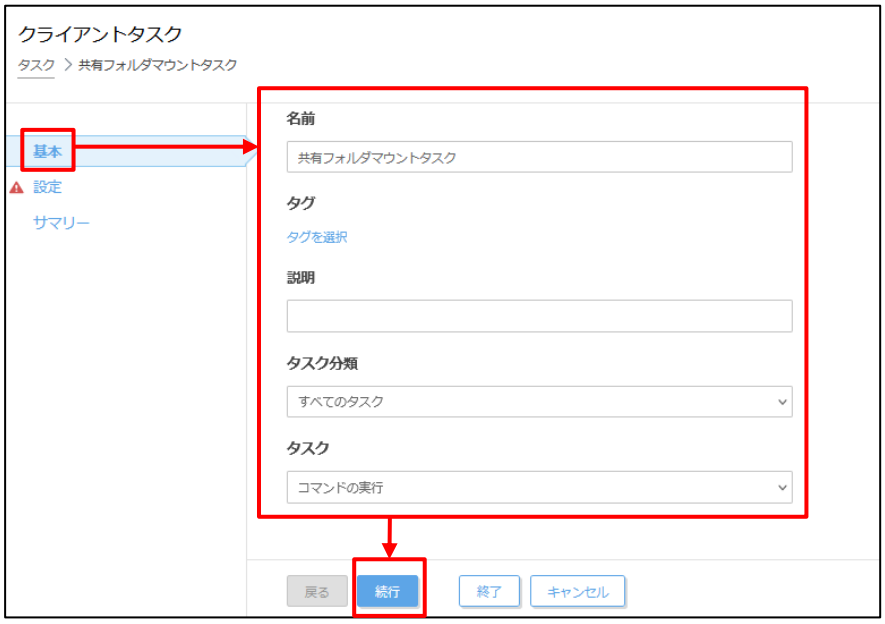
1. EP Web コンソール を起動して、ESET PROTECT に接続します。
   ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
   ※EP Web コンソールには以下の URL よりアクセスできます。
   https://＜管理サーバーのサーバー名、または、IP アドレス＞/era/

2. 共有フォルダをマウントするタスクを作成します。※実施する 1 つ目のタスクです。
「タスク」より、「新規作成」をクリックし「クライアントタスク」をクリックします。



3. 「基本」を展開し、以下の通り設定します。[続行]ボタンをクリックします。

名前	任意の名前(例：共有フォルダマウントタスク)
説明	任意の説明
タスク分類	すべてのタスク
タスク	コマンドの実行



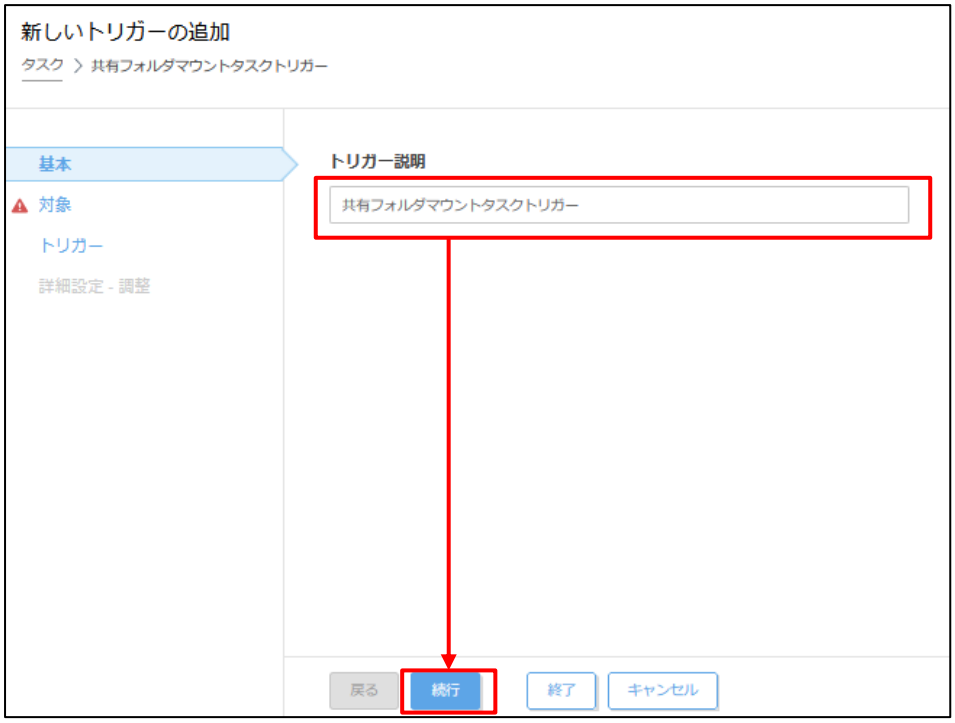
4. 「実行するコマンドライン」に以下のコマンドを入力し、[終了]ボタンをクリックします。
※「作業ディレクトリ」は空欄のままにします。

net use ¥¥共有フォルダ公開元 IP アドレス¥test パスワード(※1) /user:共有フォルダ公開元 IP アドレス or ホスト名¥ユーザー名(※2)

※1:共有フォルダを作成している端末の管理者権限のユーザーのログオンパスワードを入力ください。
※2:共有フォルダを作成しているをもったユーザー名を入力ください。
ドメイン環境にて上記で失敗する場合は /user: の後を以下に設定をし、お試しください。
「ドメイン名¥ユーザー名」

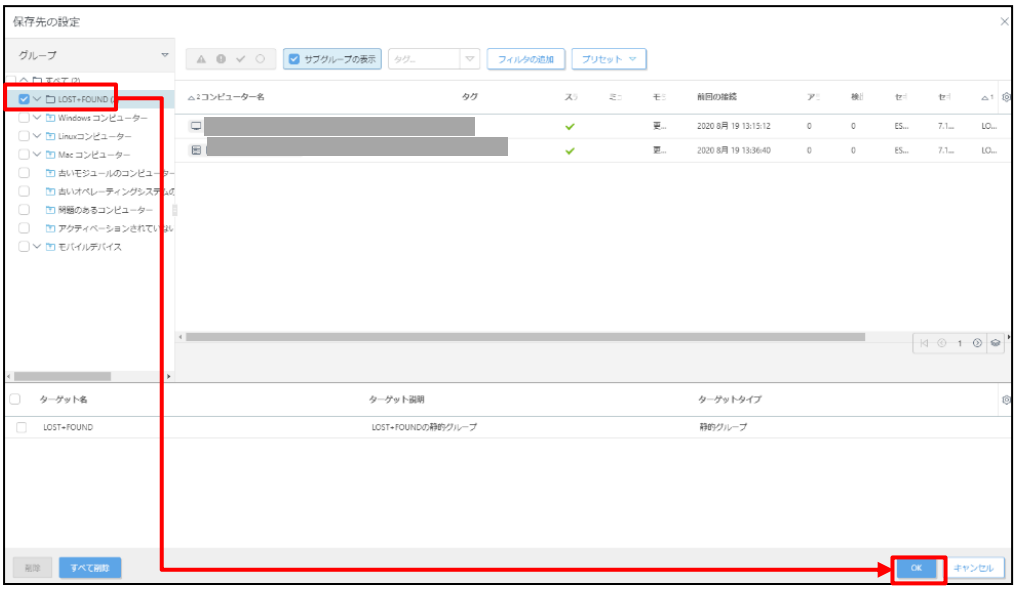
5. 以下の画面が表示されたら、[トリガーの作成]ボタンをクリックします。

6. 「基本」を展開し、任意のトリガー説明(例：エージェントのバージョンアップトリガー)を入力します。
[続行]ボタンをクリックします。

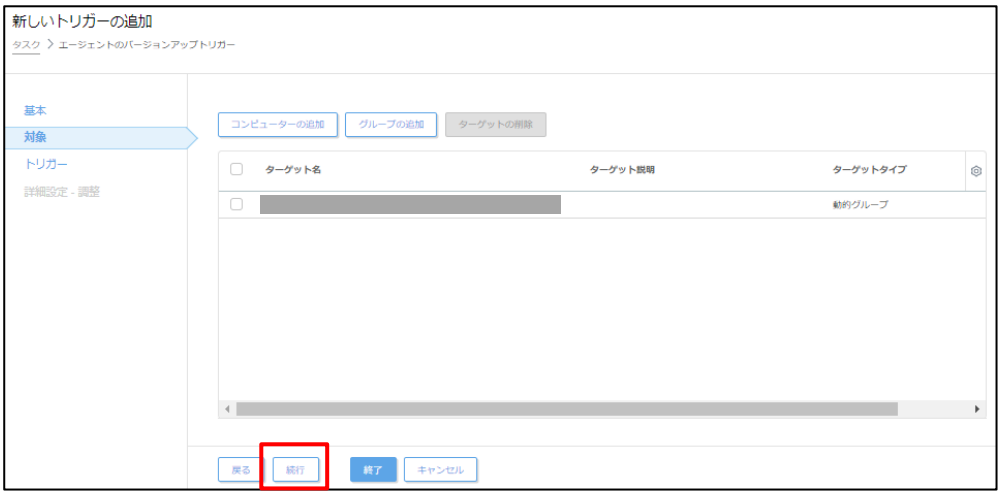


7. 「対象」を展開し、[ターゲットの追加]、[コンピューターの追加]、または[グループの追加]ボタンをクリックします。
※本手順では「ターゲットの追加」を選択します。

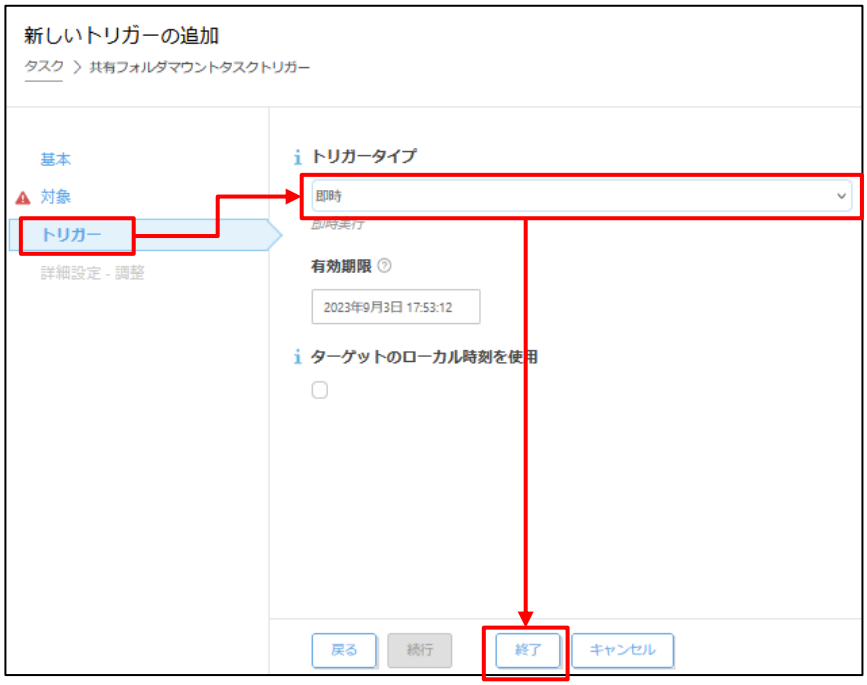
8. EM エージェントのバージョンアップを実施するコンピューター、または、グループを選択し、[OK]ボタンをクリックします。



9. [続行]ボタンをクリックします。

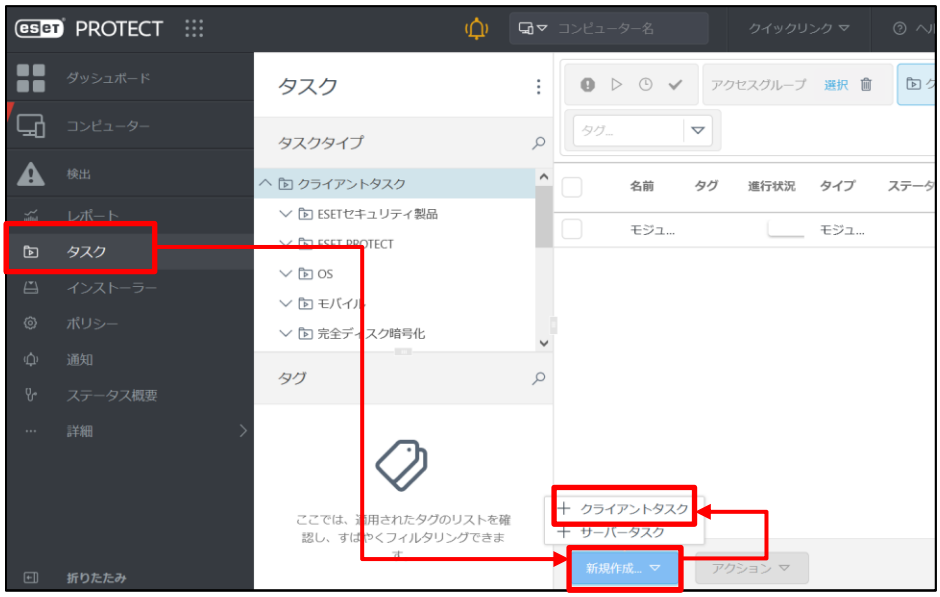


10. [トリガー]を展開し、「トリガータイプ」を選択します。
※本手順では「即時」を選択します。
[終了]ボタンをクリックします。



※以上で、実施する 1 つ目のタスクの作業は終了です。

11. エージェントをバージョンアップするためのタスクを作成します。※実施する 2 つ目のタスクです。
「タスク」より、「新規作成」をクリックし「クライアントタスク」をクリックします。

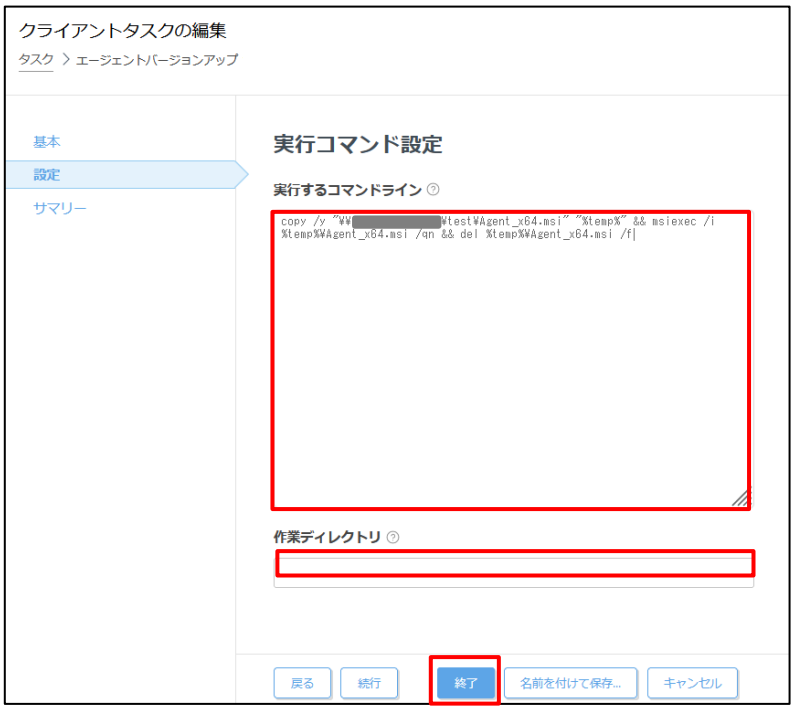


12.「基本」を展開し、以下の通り設定します。[続行]ボタンをクリックします。

名前	任意の名前(例：エージェントバージョンアップ)
説明	任意の説明
タスク分類	すべてのタスク
タスク	コマンドの実行

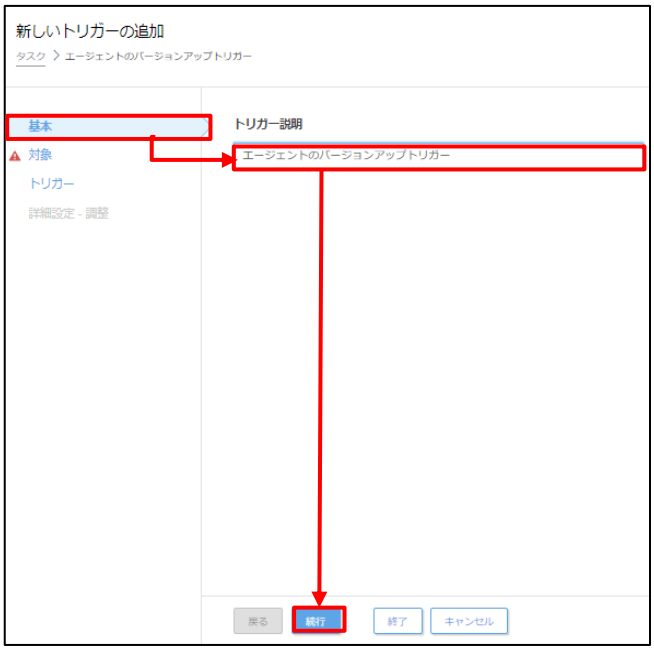
13.「実行するコマンドライン」に以下のコマンドを入力し、 [終了]ボタンをクリックします。
※「作業ディレクトリ」は空欄のままにします。

```
copy /y ¥¥共有フォルダ公開元 IP アドレス¥test¥ファイル名.msi "%temp%" &&
msiexec /i %temp%¥ファイル名.msi /qn && del %temp%¥ファイル名.msi /f
```

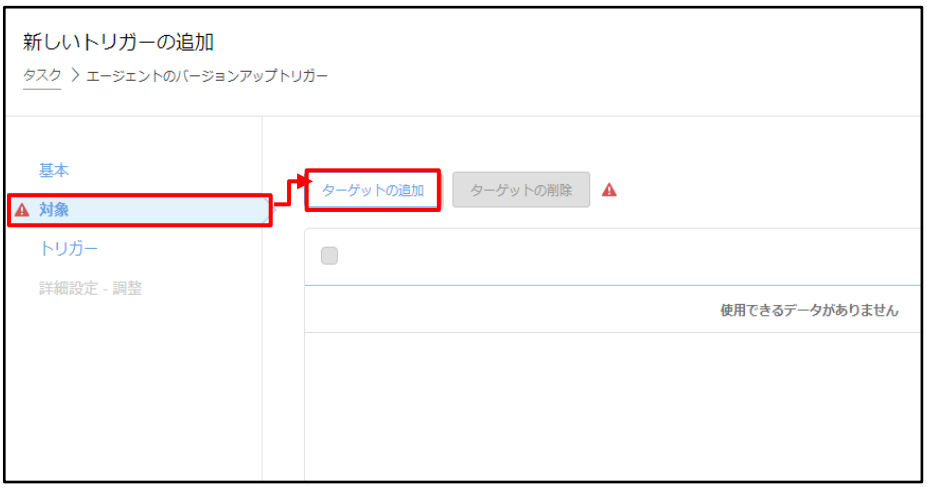


14. 以下の画面が表示されたら、[トリガーの作成]ボタンをクリックします。

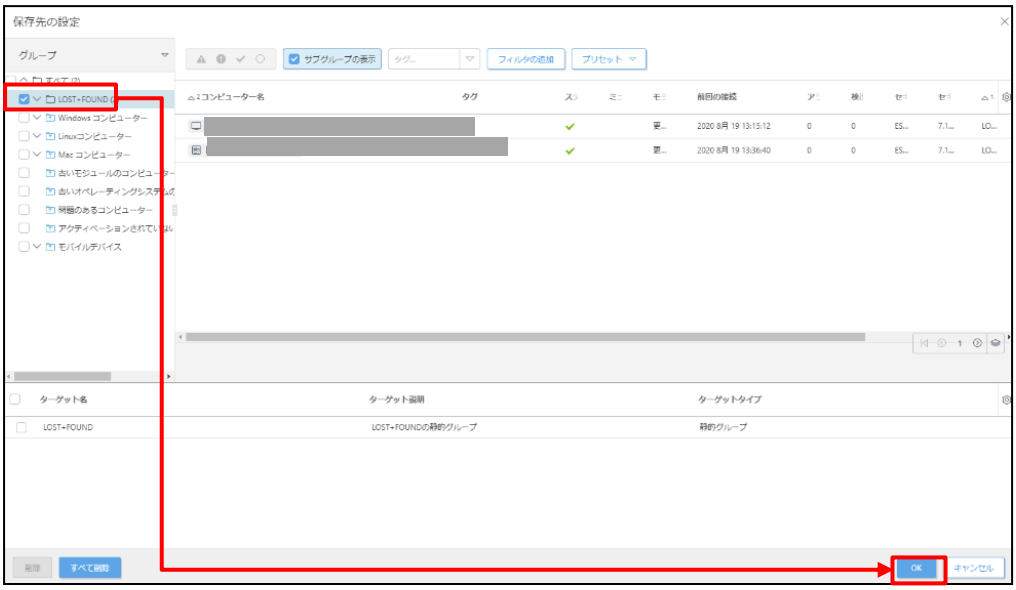
15. 「基本」を展開し、任意のトリガー説明(例：エージェントのバージョンアップトリガー)を入力します。
[続行]ボタンをクリックします。



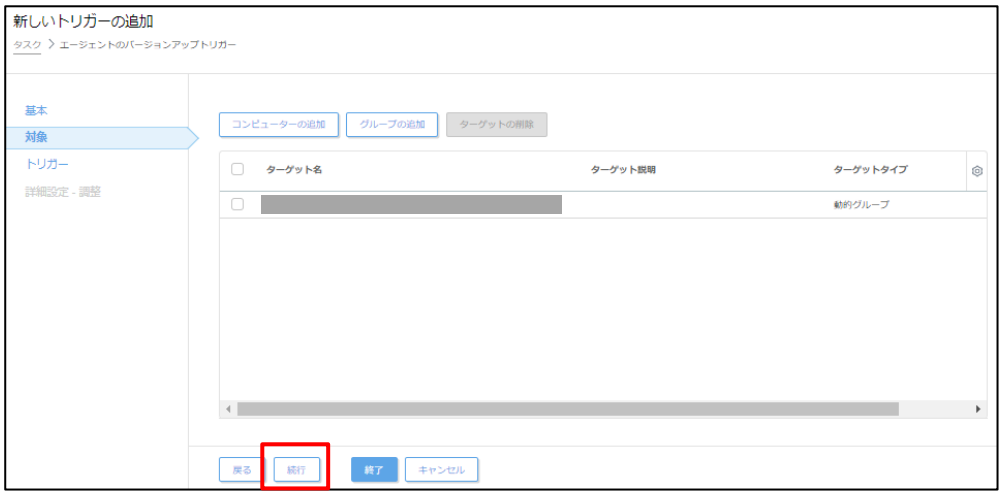
16. 「対象」を展開し、[ターゲットの追加]、[コンピューターの追加]、または[グループの追加]ボタンをクリックします。
※本手順では「ターゲットの追加」を選択します。



17. EM エージェントのバージョンアップを実施するコンピューター、または、グループを選択し、[OK]ボタンをクリックします。



18. [続行]ボタンをクリックします。



19. [トリガー]を展開し、「トリガータイプ」を選択します。
※本手順では「即時」を選択します。
[終了]ボタンをクリックします。

※以上で、実施する 2 つ目のタスクの作業は終了です。

以上で、EM エージェントのバージョンアップ作業は完了です。

b. クライアント用プログラムのバージョンアップ

各クライアント端末にインストールされているクライアント用プログラム V9.X を V10.X にバージョンアップします。

※本手順は 64bit 端末を前提としています。32bit 端末が存在する場合は端末ごとに分けて実施ください。

※各タスクを実行する際は端末のタスクの実行状況を確認したうえで、次のタスクの実行をお願いいたします。

※本手順は ESET Endpoint Security を利用する前提としております。ご利用プログラムが異なる場合は読み替えて実施ください。

b-1. 動作要件の確認

バージョンアップの前に、EES V9.X と EEA V9.X の動作要件を確認します。

＜ESET Endpoint Security / ESET Endpoint アンチウイルス 動作要件＞

・ESET PROTECT Entry オンプレミス(旧名称：ESET Endpoint Protection Advanced)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-entry-o/spec.html

・ESET PROTECT Essential オンプレミス(旧名称：ESET Endpoint Protection Standard)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-essential-o/spec.html

b-2. クライアント用プログラムの準備

1. 【STEP0】にて用意した Windows 向けクライアント用プログラムを＜a-1＞で用意した共有フォルダに保存します。

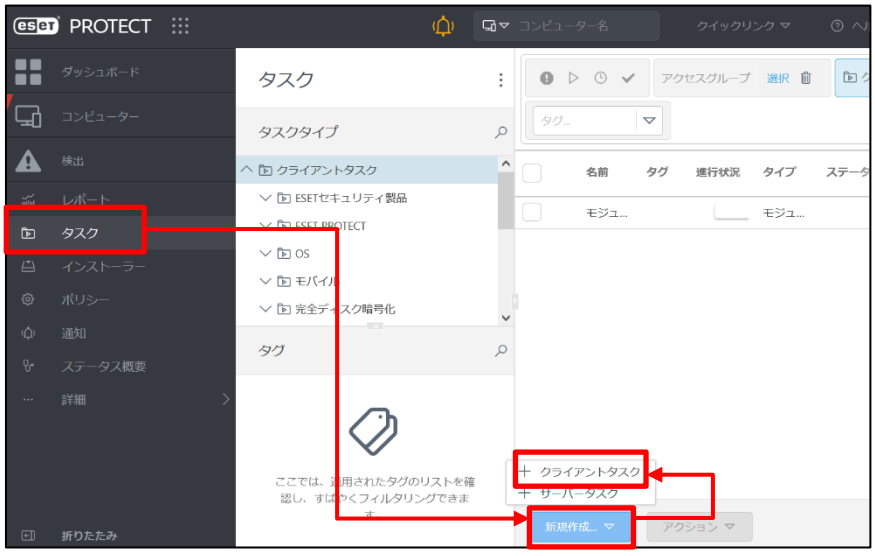
※＜a-1＞を実施し、共有フォルダがある前提です。
共有フォルダを作成していない場合は、＜a-3＞手順 1~10 の実施をお願いいたします。

b-3. クライアント用プログラムのバージョンアップ

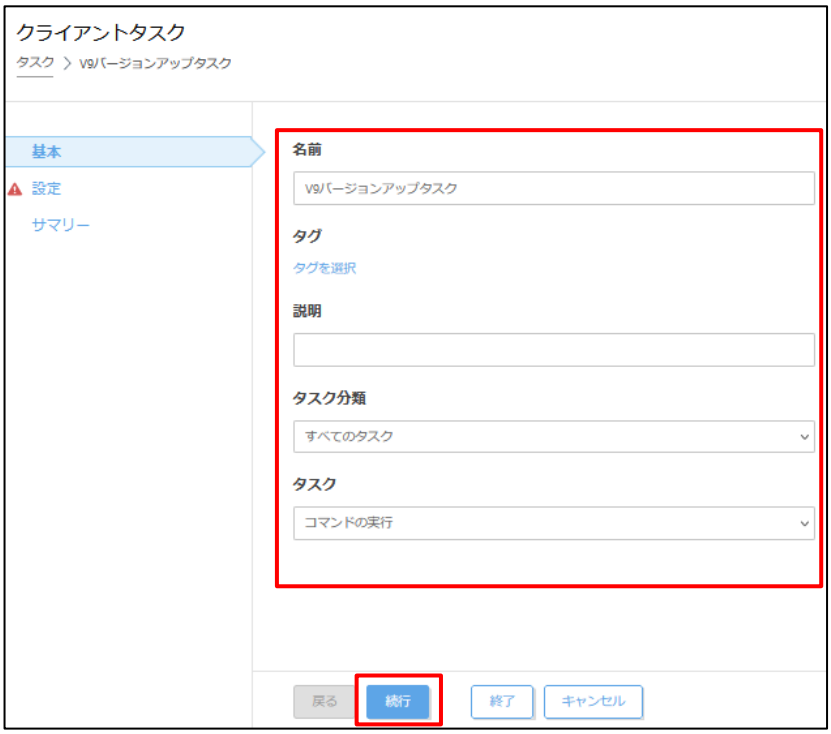
手順 <b-2> で保存した共有フォルダ内のクライアント用プログラムを使用して、クライアント端末のプログラムのバージョンアップを行います。

1. EP Web コンソール を起動して、ESET PROTECT に接続します。
   ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
   ※EP Web コンソールには以下の URL よりアクセスできます。
   https:// <管理サーバーのサーバー名、または、IP アドレス> /era/

2. クライアント用プログラムをバージョンアップするためのタスクを作成します。
   「タスク」をクリックして、「新規作成」をクリックします。
   ※すでに <a-3> の手順 1～10 を実施している前提です。
   実施していない場合は上記手順を実施のうえ、本手順を実施ください。



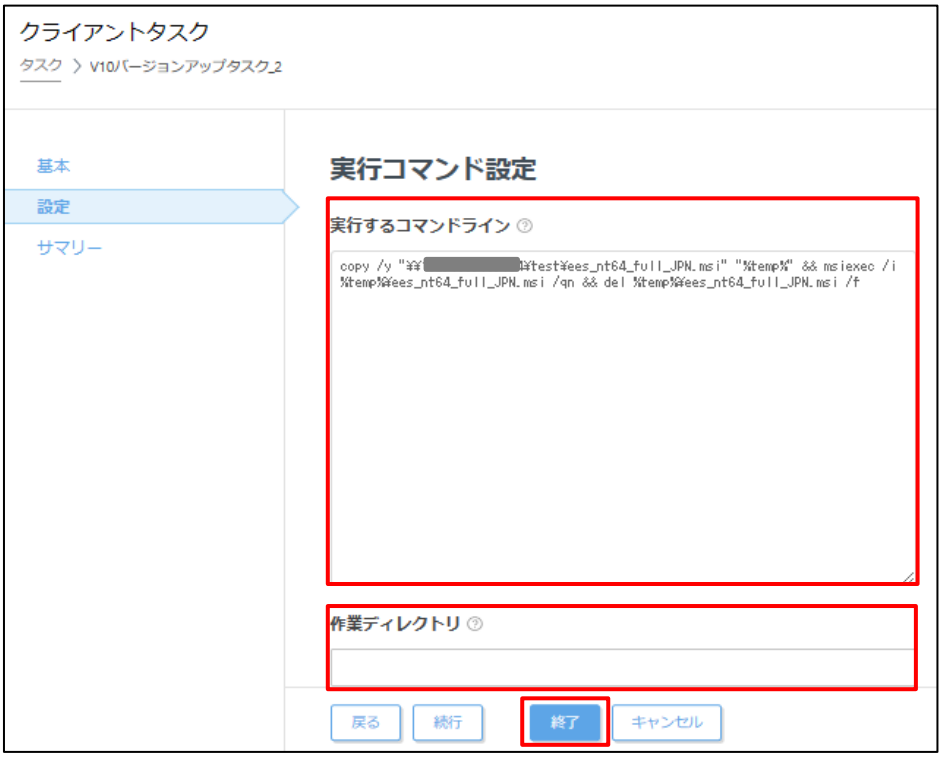
3. 「基本」を展開し、以下の通り設定し、[続行]ボタンをクリックします。



名前	任意の名前(例：V9 バージョンアップタスク)
説明	任意の説明
タスク分類	すべてのタスク
タスク	コマンドの実行

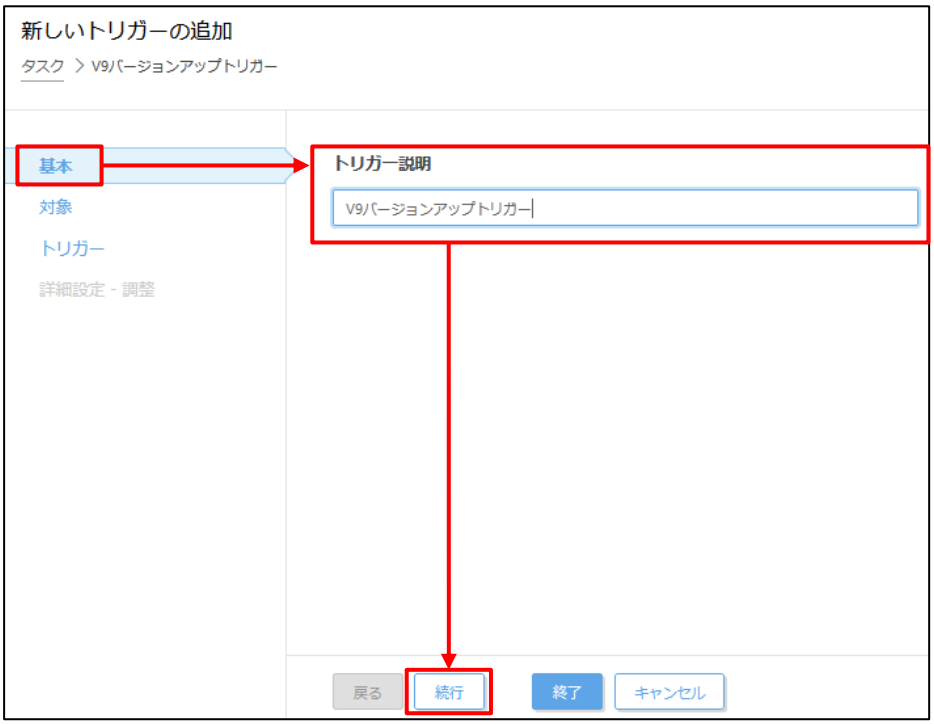
4. 「設定」を展開し、[実行するコマンドライン]に以下のコマンドを入力し、 [終了]ボタンをクリックします。
※「作業ディレクトリ」は空欄のままにします。

copy /y ¥¥共有フォルダ公開元 IP アドレス¥test¥ファイル名.msi "%temp%" && msiexec /i %temp%¥ファイル名.msi /qn && del %temp%¥ファイル名.msi /f

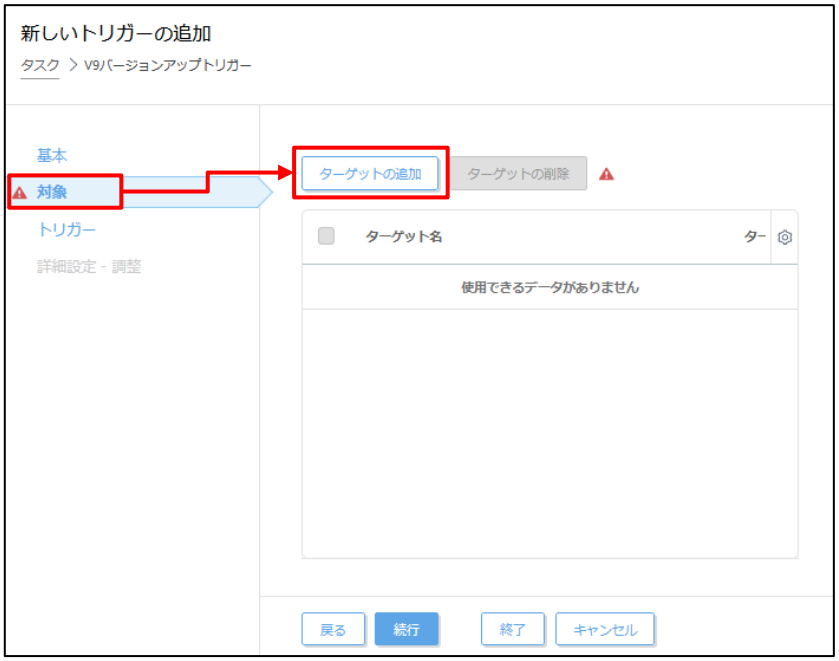


5. 以下の画面が表示されたら、[トリガーの作成]ボタンをクリックします。

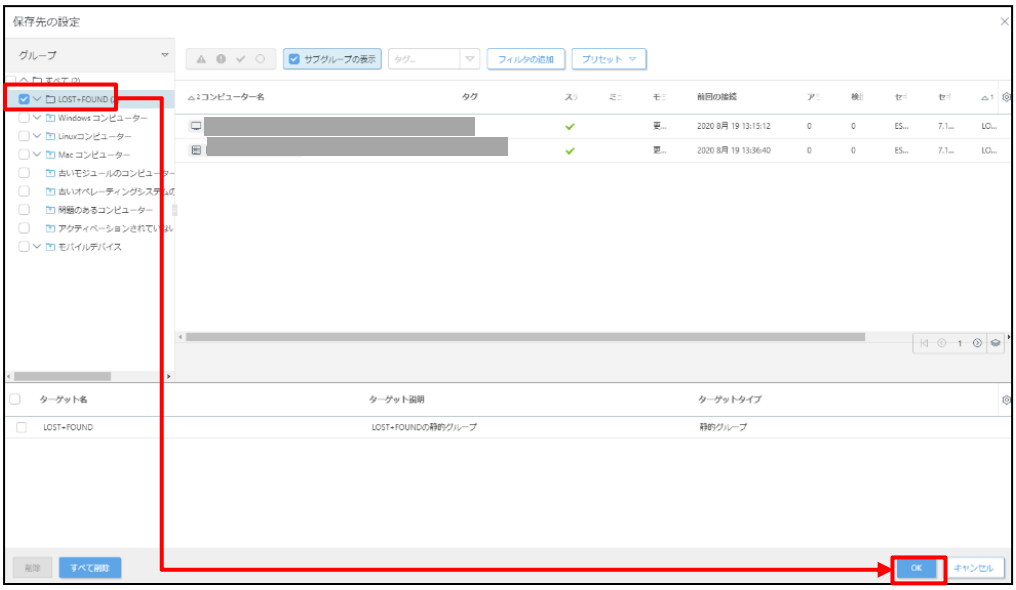
6. 「基本」を展開し、任意のトリガー説明(例：V9 バージョンアップトリガー)を入力します。
[続行]ボタンをクリックします。



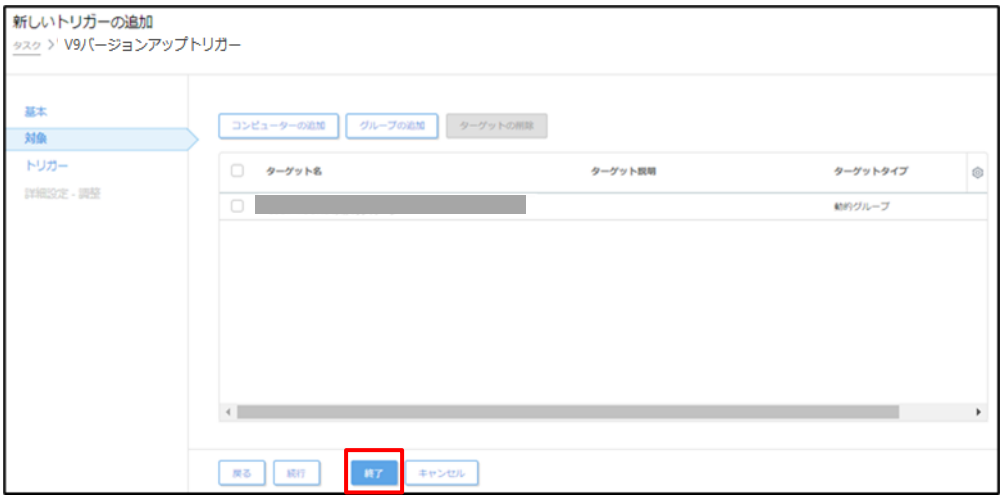
7. 「対象」を展開し、[ターゲットの追加]、[コンピューターの追加]、または[グループの追加]ボタンをクリックします。
※本手順では「ターゲットの追加」を選択します。



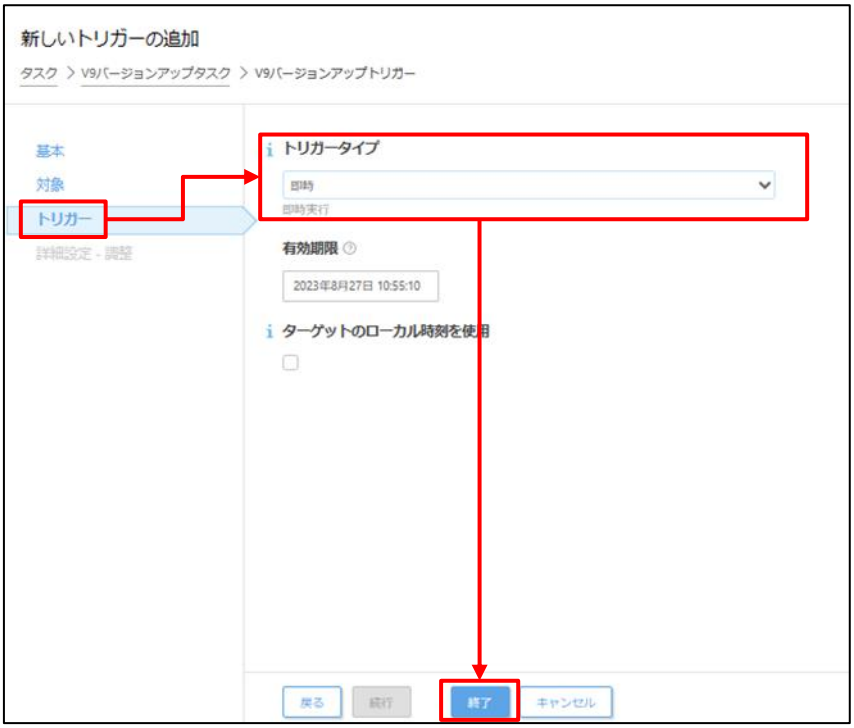
8. EM エージェントのバージョンアップを実施するコンピューター、または、グループを選択し、[OK]ボタンをクリックします。



9. [続行]ボタンをクリックします。



10. [トリガー]を展開し、「トリガータイプ」を選択します。
※本手順では「即時」を選択します。
[終了]ボタンをクリックします。



以上で、クライアント用プログラムのバージョンアップ作業は完了です。

以上で、【パターン B：ファイル共有を使用してバージョンアップする場合】は完了です。
最後に【STEP6】で各プログラムのバージョンが完了したことを確認します。

パターン C:Web サーバーを使用してセキュリティ管理ツールからバージョンアップする場合

※Web サーバーを使用してバージョンアップを行う場合、各インストーラーがクライアント端末からアクセス可能な Web サーバー上で公開してあることが前提です。

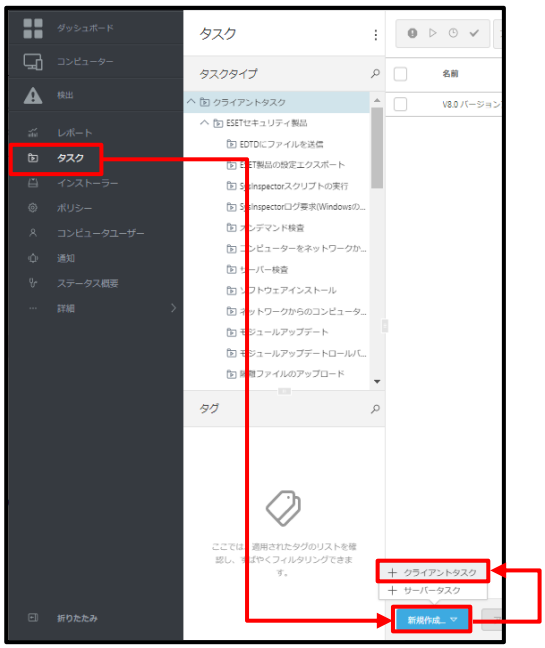
a. EM エージェントのバージョンアップ

クライアント端末の EM エージェント V8.X を V9.X にバージョンアップします。

a-1. クライアントの EM エージェントをバージョンアップ

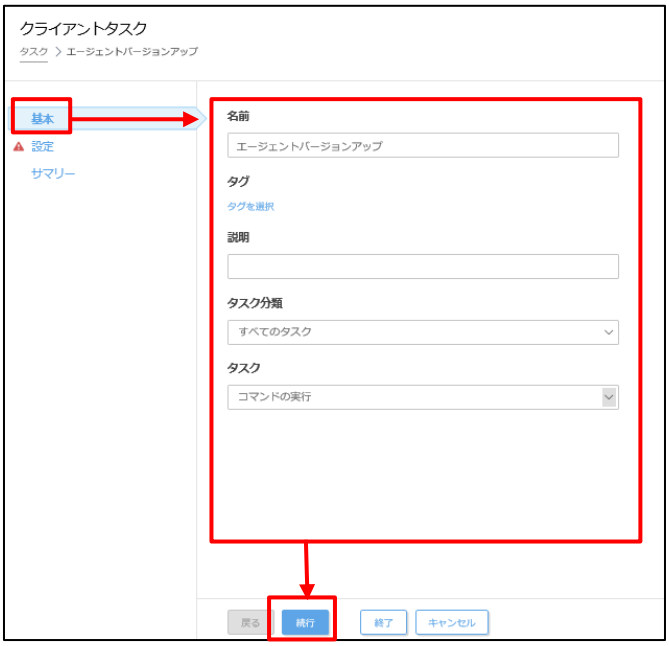
1. EP Web コンソール を起動して、ESET PROTECT に接続します。
   ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
   ※ EP Web コンソールには以下の URL よりアクセスできます。
   https:// <管理サーバーのサーバー名、または、IP アドレス> /era

2. [タスク]-[新規作成]-[クライアントタスク]をクリックします。



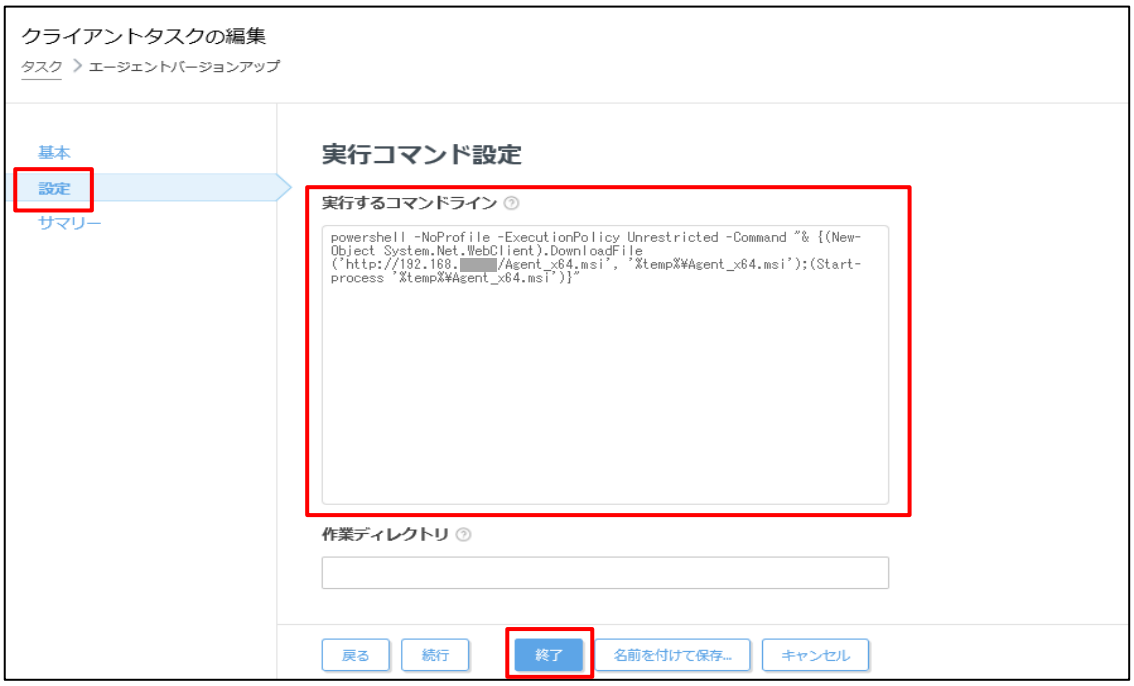
3. 「基本」を展開し、以下の通り設定します。[続行]ボタンをクリックします。

名前	任意の名前(例：エージェントバージョンアップ)
説明	任意の説明
タスク分類	すべてのタスク
タスク	コマンドの実行



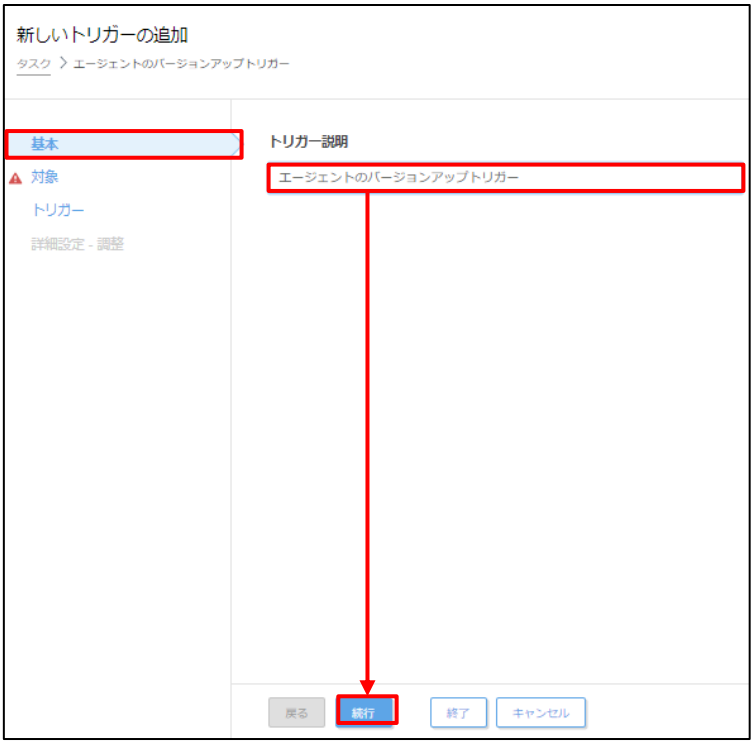
4. 「実行するコマンドライン」に以下のコマンドを入力し、[終了]ボタンをクリックします。

```
powershell -NoProfile -ExecutionPolicy Unrestricted -Command "& {(New-Object System.Net.WebClient).DownloadFile('http://Web サーバーの IP アドレス/EM エージェントのインストーラーパス', '%temp%¥インストーラー名');(Start-process '%temp%¥インストーラー名')}"
```

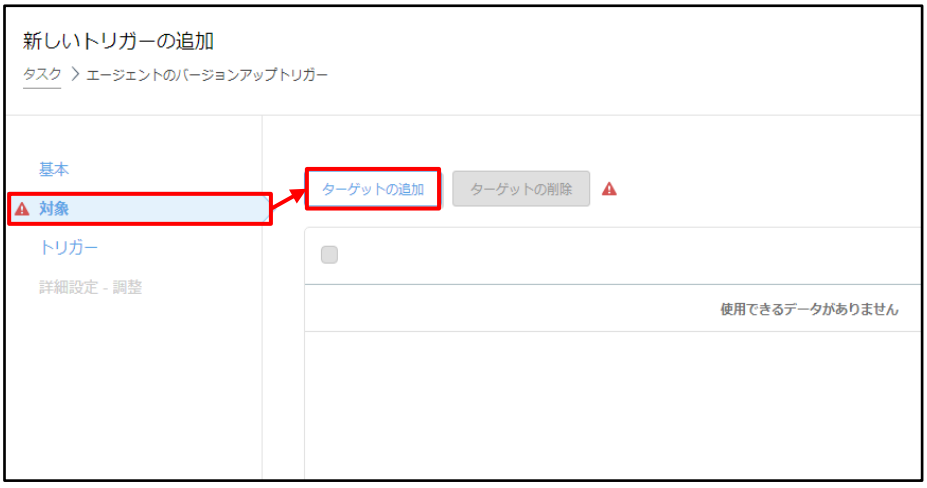


5. 以下の画面が表示されたら、[トリガーの作成]ボタンをクリックします。

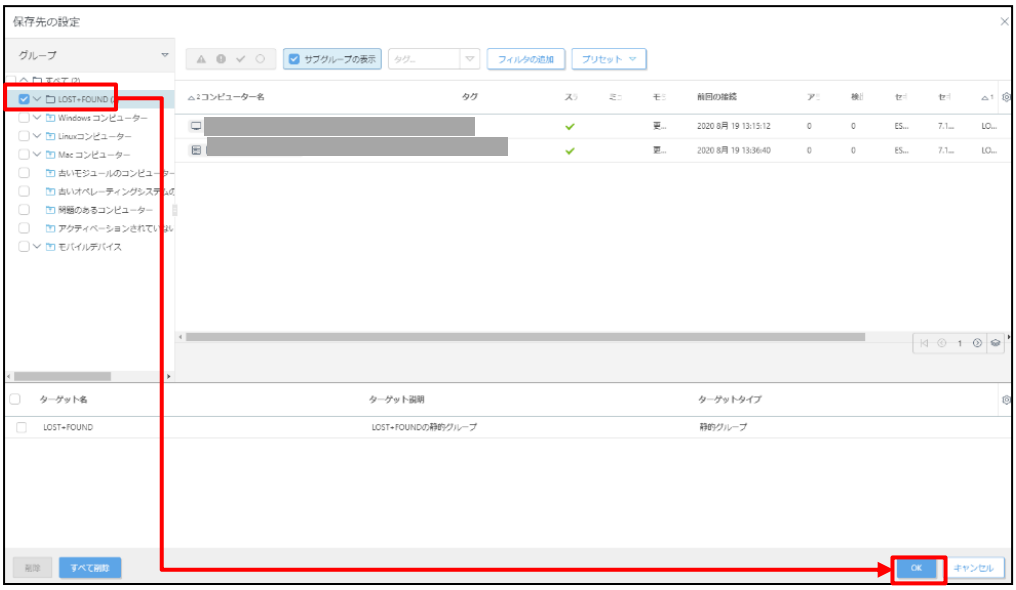
6. 「基本」を展開し、任意のトリガー説明(例：エージェントのバージョンアップトリガー)を入力します。
[続行]ボタンをクリックします。



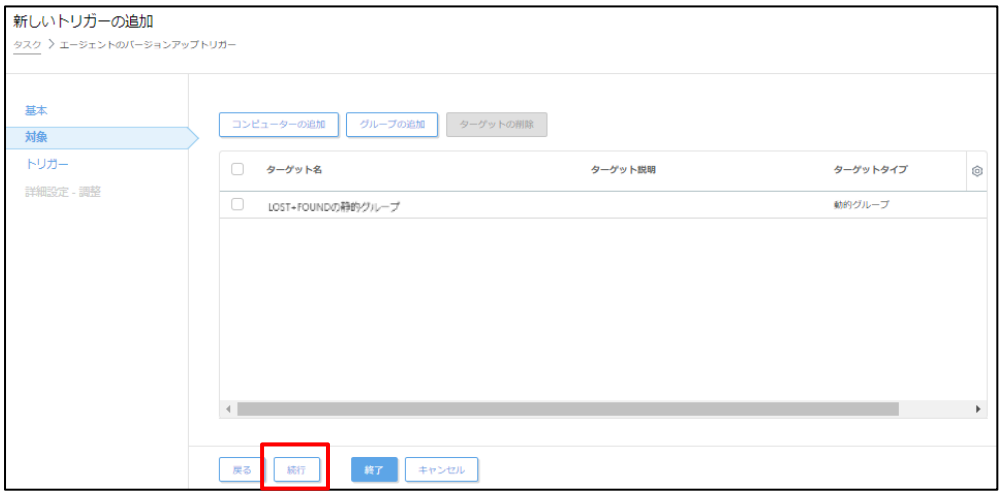
7. 「対象」を展開し、[ターゲットの追加]、[コンピューターの追加]、または[グループの追加]ボタンをクリックします。
※本手順では「ターゲットの追加」を選択します。



8. EM エージェントのバージョンアップを実施するコンピューター、または、グループを選択し、[OK]ボタンをクリックします。



9. [続行]ボタンをクリックします。



10. [トリガー]を展開し、「トリガータイプ」を選択します。
    ※本手順では「即時」を選択します。
    [終了]ボタンをクリックします。

以上で、EM エージェントのバージョンアップは完了です。

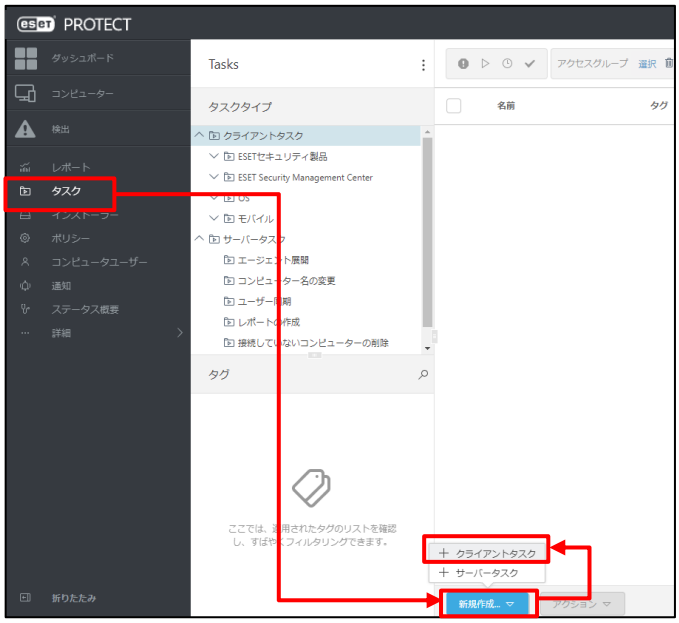
b. クライアント用プログラムのバージョンアップ

b-1. 動作要件の確認

バージョンアップの前に、EES V9.X と EEA V9.X の動作要件を確認します。
＜ESET Endpoint Security / ESET Endpoint アンチウイルス 動作要件＞
・ESET PROTECT Entry オンプレミス(旧名称：ESET Endpoint Protection Advanced)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-entry-o/spec.html
・ESET PROTECT Essential オンプレミス(旧名称：ESET Endpoint Protection Standard)をご利用のお客様
https://eset-info.canon-its.jp/business/ep-essential-o/spec.html

b-2. クライアント用プログラムのバージョンアップ

1. [タスク]より、[新規作成]をクリックし、[クライアントタスク]を選択します。

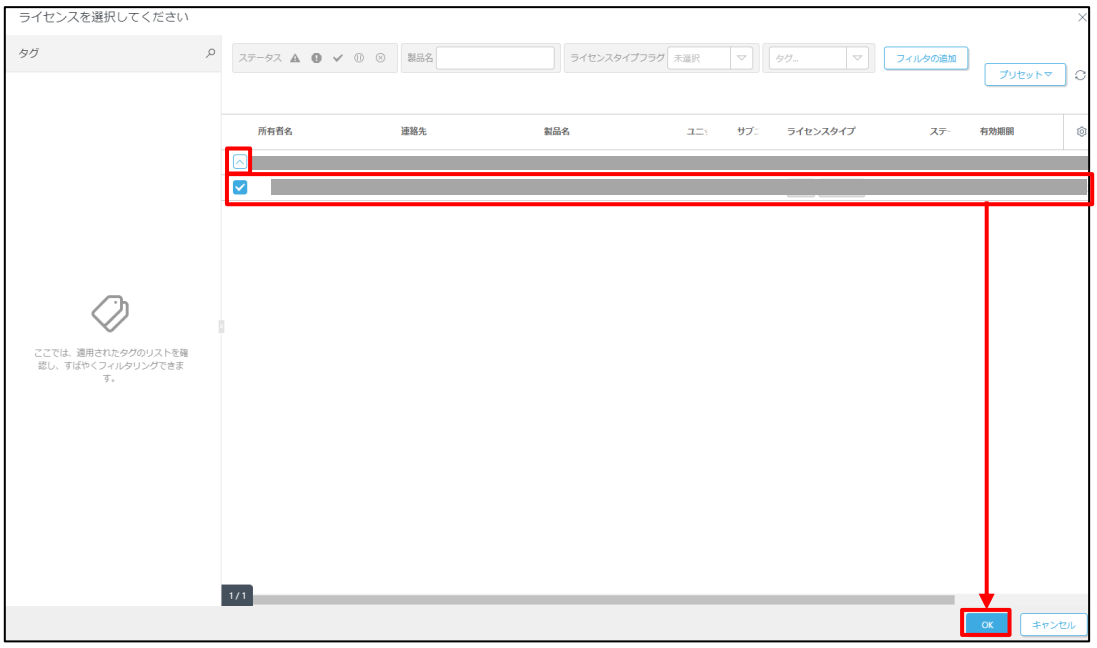


2. [基本]を展開し、以下の通り設定します。

名前	任意の名前(例：V9 バージョンアップタスク)
説明	任意で入力
タスク分類	すべてのタスク
タスク	ソフトウェアインストール

3. 「設定」を展開し、「ESET ライセンス」の＜選択＞をクリックします。

4. [^]を展開し、ご利用ライセンスを選択のうえ、[OK]ボタンをクリックします。



5. 「直接パッケージ URL でインストール」を選択し、Web サーバーに配置しているクライアント用プログラムのパスを記載します。
※以下は例です。

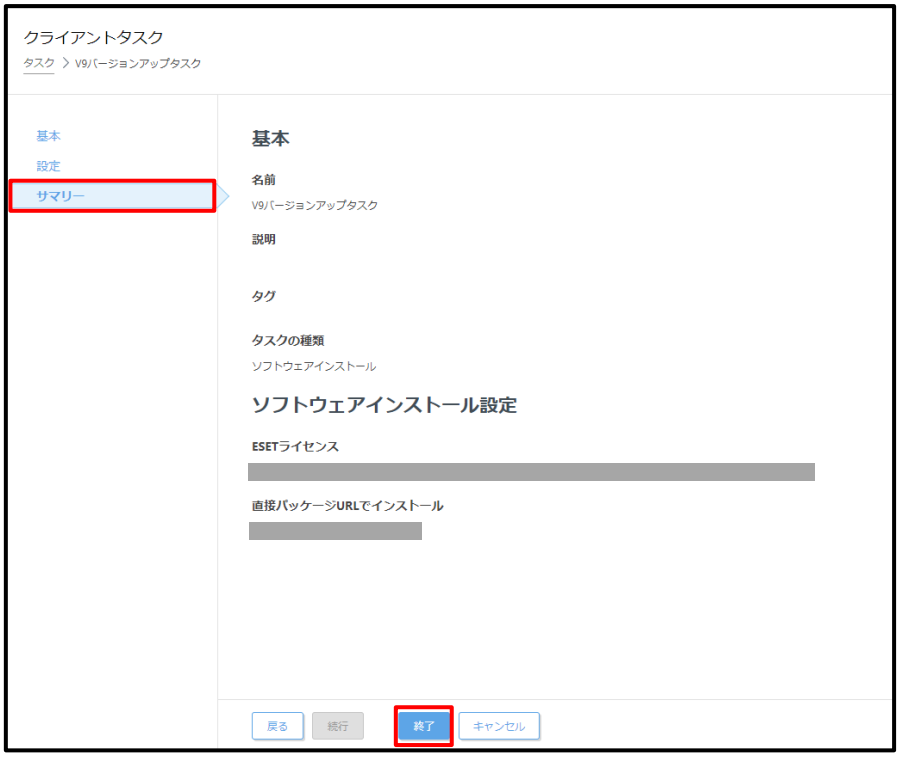
(例)http://192.168.XXX.XXX/ees_nt64.msi
http://Web サーバーの IP アドレス/インストーラーのパス

<参考>

サーバー用プログラムの EFSW(管理サーバーにインストールされている EFSW を除く)をバージョンアップする場合は、「ESET Server Security for Microsoft Windows Server」のインストーラーのパスを指定してください。

6. 「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。」または「エンドユーザーライセンス契約に同意する」にチェックを入れます。

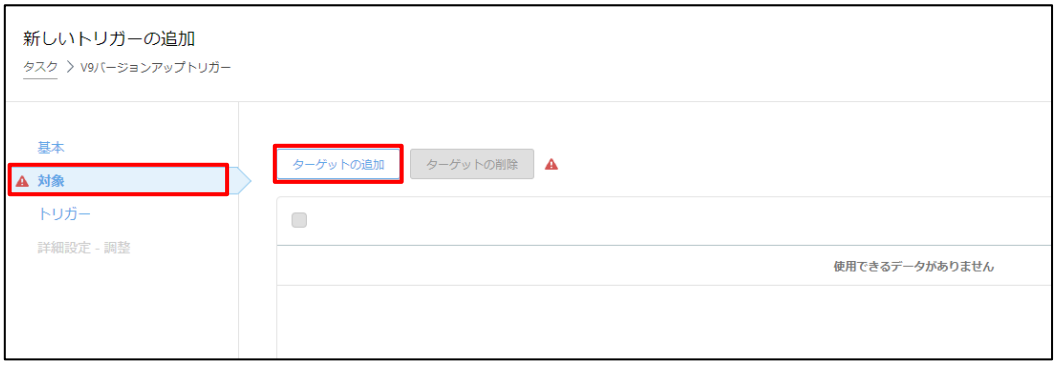
7. 「サマリー」の内容を確認し、問題なければ[終了]ボタンをクリックします。



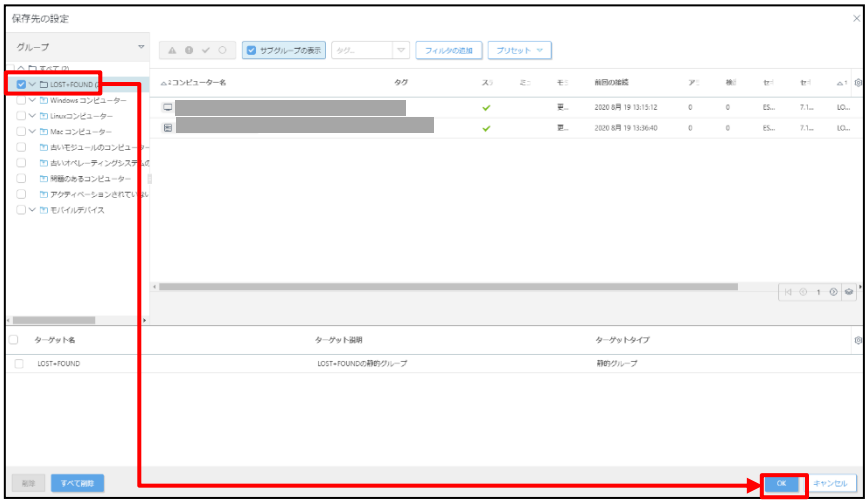
8. 以下の画面が表示されたら、[トリガーの作成]ボタンをクリックします。

9. 「基本」を展開し、任意のトリガーの説明(例：V9 バージョンアップトリガー)を入力します。

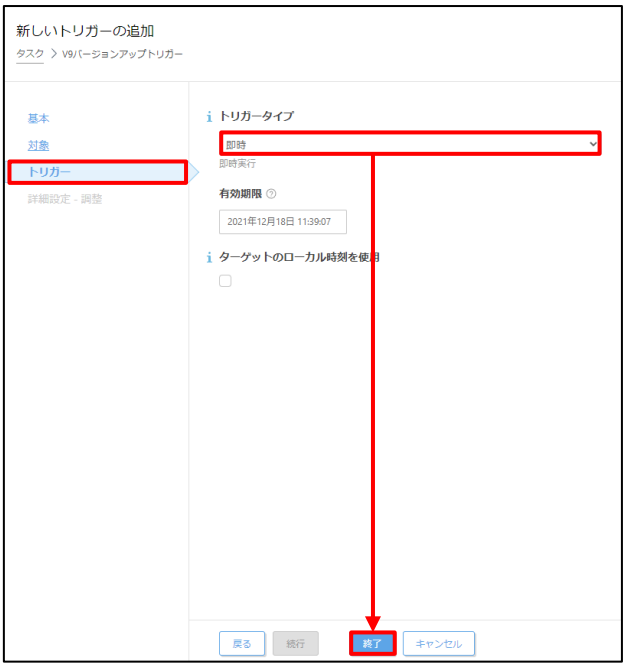
10. 「対象」を展開し、[ターゲットの追加] 、[コンピューターの追加]、または[グループの追加]ボタンをクリックします。
※本手順では「ターゲットの追加」を選択します。



11. バージョンアップするクライアントが所属するグループを選択し、[OK]ボタンをクリックします。



12. [トリガー]を展開し、「トリガータイプ」を選択します。
※本手順では「即時」を選択します。
[終了]ボタンをクリックします。



以上で、クライアント用プログラムのバージョンアップは完了です。

以上で、【パターン C：Web サーバーを使用してバージョンアップする場合】は完了です。
最後に【STEP6】で各プログラムのバージョンが完了したことを確認します。

パターン D：AD 環境で GPO を使用してバージョンアップする場合

※GPO を使用してバージョンアップを行う場合、GPO で配布を行う各インストーラーがクライアント端末からアクセス可能なネットワークパスの共有フォルダに格納してあること、また各クライアント端末は任意の OU に所属していることが前提です。

a. EM エージェントとクライアント用プログラムのバージョンアップ

GPO を使用してバージョンアップを行う場合は、EM エージェントとクライアント用プログラムを同時にバージョンアップします。

a-1. 動作要件の確認

バージョンアップの前に、EES V9.X と EEA V9.X の動作要件を確認します。

＜ESET Endpoint Security / ESET Endpoint アンチウイルス 動作要件＞

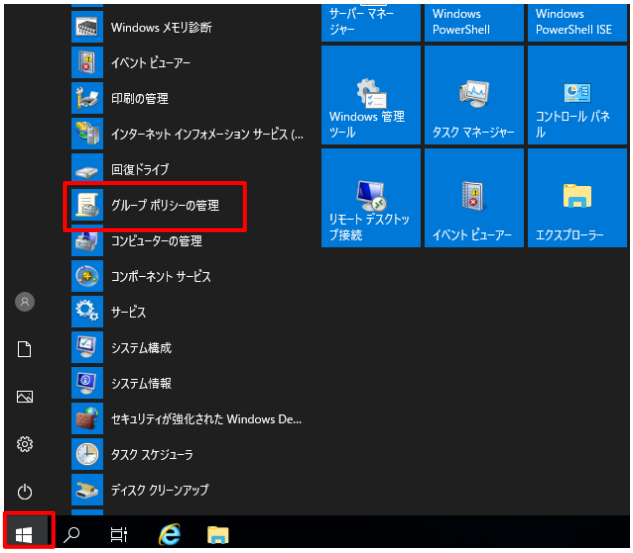
・ESET PROTECT Entry オンプレミス(旧名称：ESET Endpoint Protection Advanced)をご利用のお客さま
https://eset-info.canon-its.jp/business/ep-entry-o/spec.html

・ESET PROTECT Essential オンプレミス(旧名称：ESET Endpoint Protection Standard)をご利用のお客さま
https://eset-info.canon-its.jp/business/ep-essential-o/spec.html

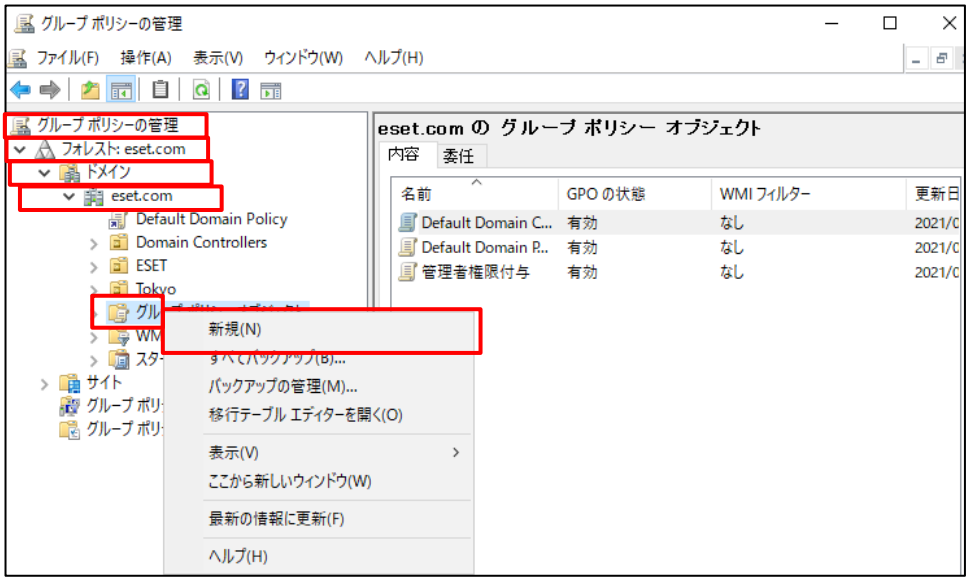
a-2-1. 各プログラムのバージョンアップ準備 ～GPO の作成～

クライアント用プログラムのバージョンアップを行うための GPO を作成します。

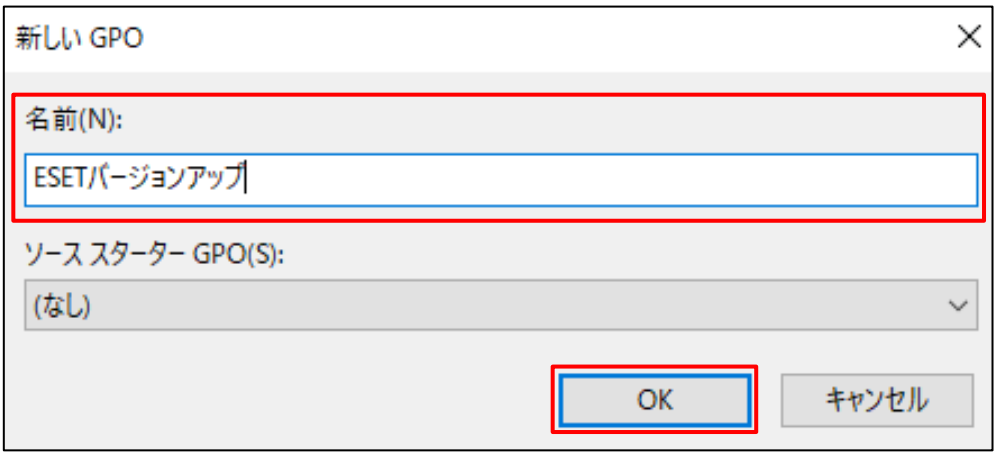
1. スタートボタンをクリックし、「Windows 管理ツール」より「グループポリシーの管理」を起動します。



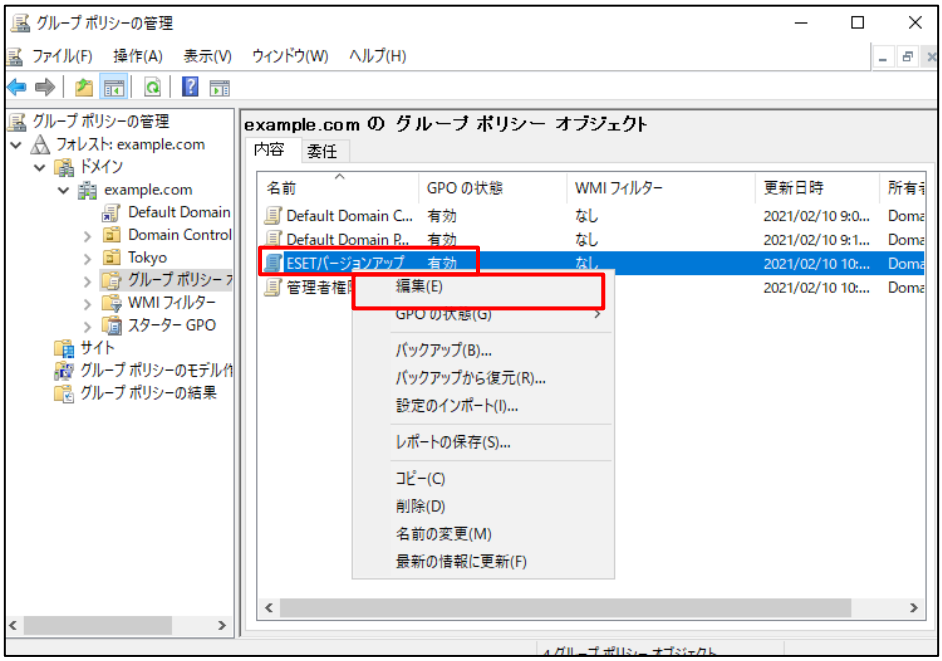
2. 「グループポリシーの管理」が起動したら、[グループポリシーの管理]-[フォレスト]-[ドメイン]-[任意のドメイン名]と展開して「グループポリシーオブジェクト」を右クリックし、[新規]をクリックします。



3. 「新しい GPO」が表示されたら、任意の名前を設定し、[OK]ボタンをクリックします。
※本手順では「ESET バージョンアップ」とします。

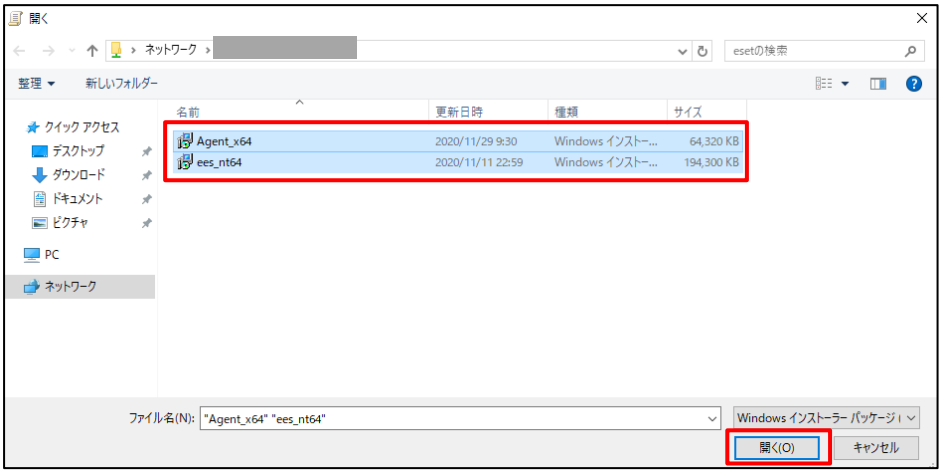


4. 新しく作成したグループポリシーオブジェクトを右クリックし、[編集]をクリックします。

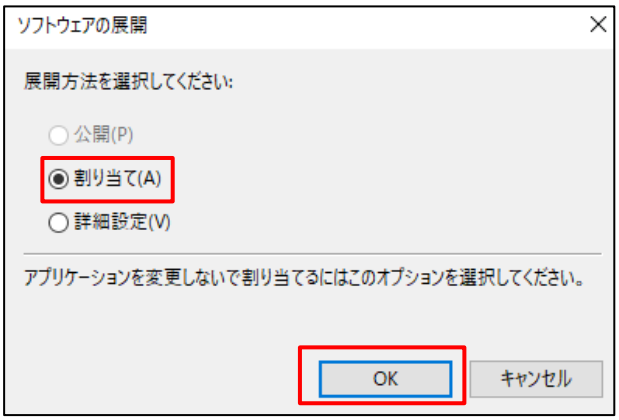


5. 「グループポリシー管理エディター」が起動したら、[コンピューターの構成]-[ポリシー]-[ソフトウェアの設定]と展開し、[ソフトウェアのインストール]を右クリックして[新規作成]-[パッケージ]をクリックします。

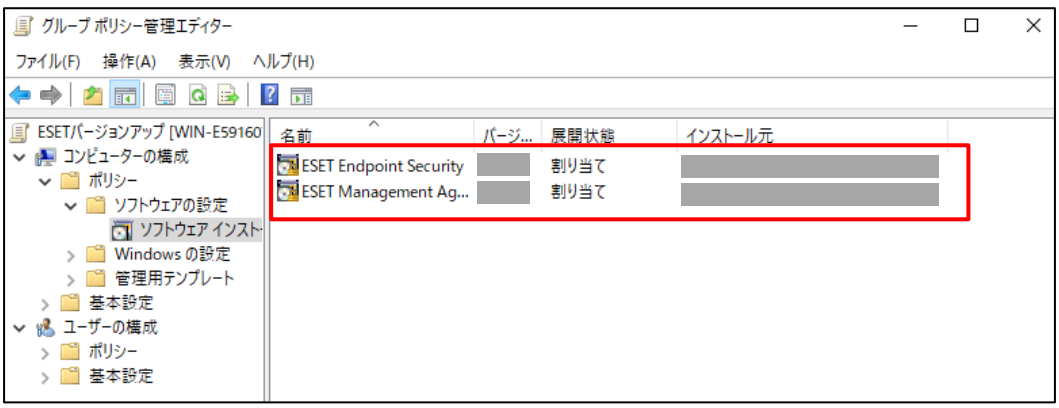
6. ネットワークパスの共有フォルダに公開してある EM エージェントとクライアント用プログラムのインストーラーを両方選択し、[開く]ボタンをクリックします。



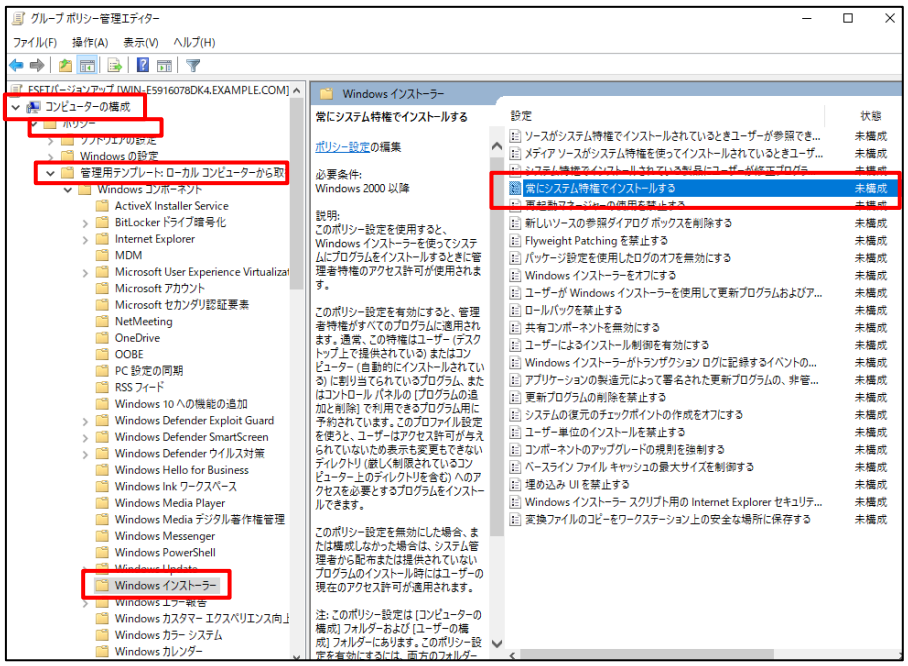
7. 「ソフトウェアの展開」画面が表示されたら、「割り当て」にチェックを入れ、[OK]ボタンをクリックします。
※本画面は 2 回表示されます。2 回とも「割り当て」にチェックを入れてください。



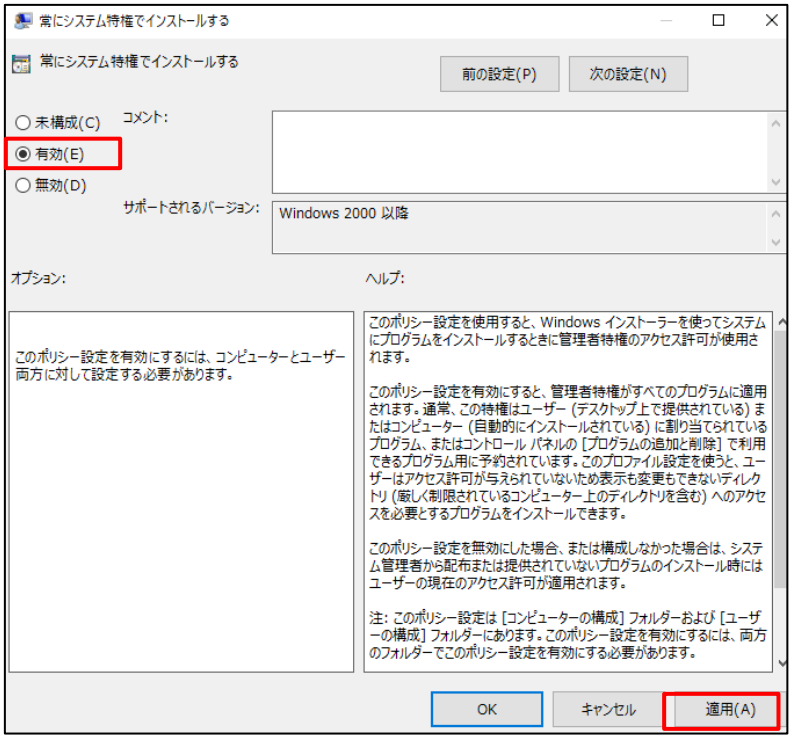
8. 手順 6 で選択したインストーラーが表示されたことを確認します。



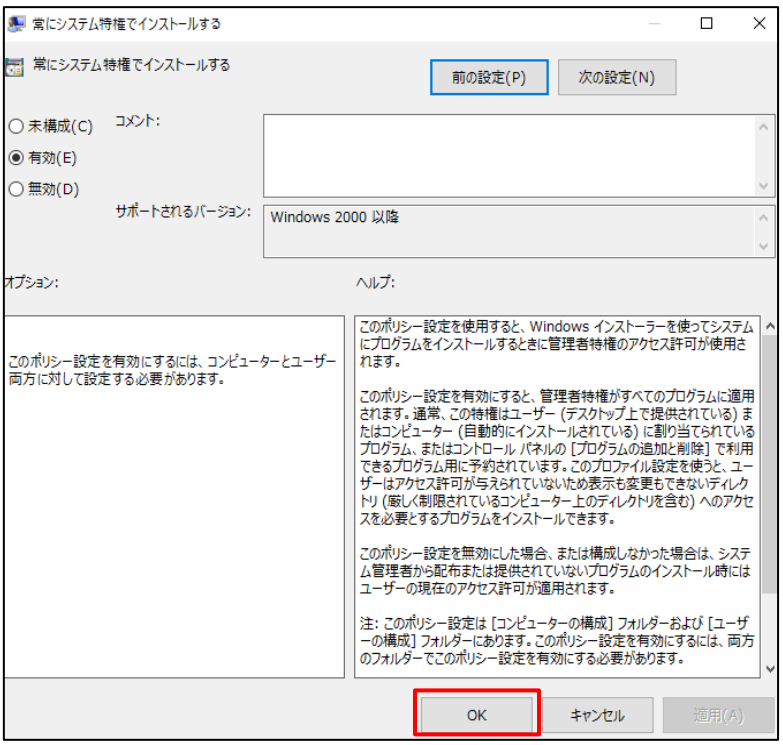
9. [コンピューターの構成]-[ポリシー]-[管理用テンプレート]-[Windows コンポーネント]-[Windows インストーラー]を展開し、画面右側の「常にシステム特権でインストールする」をダブルクリックします。



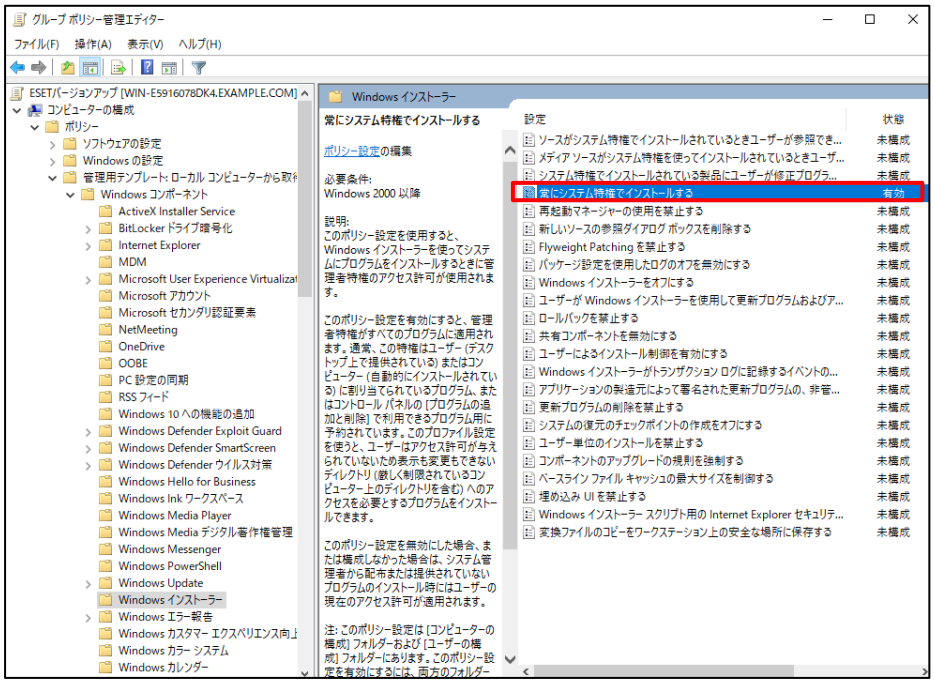
10. 「有効」にチェックを入れ、[適用]ボタンをクリックします。



11. [OK]ボタンをクリックします。



12. 「常にシステム特権でインストールする」の状態が、「有効」になっていることを確認します。

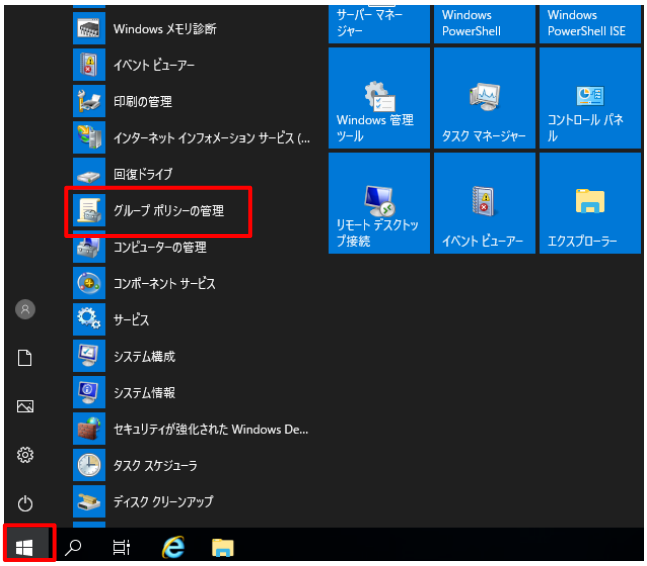


以上で、クライアント用プログラムと EM エージェントのバージョンアップ用の GPO の作成は終了です。

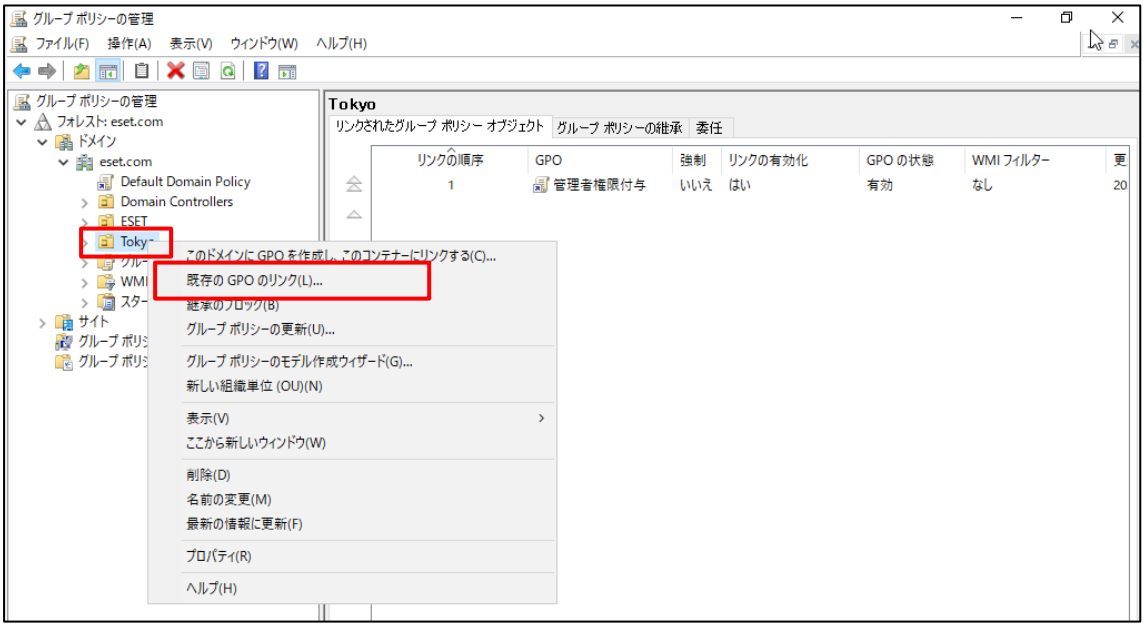
a-2-2. 各プログラムのバージョンアップ準備　～GPO の配布～

作成した GPO を、クライアント端末が所属している OU に割り当てます。

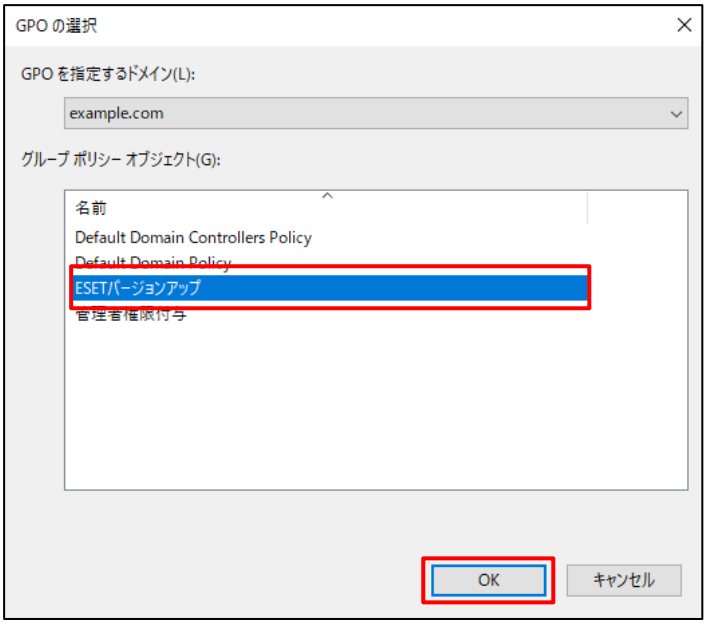
1. スタートボタンをクリックし、「Windows 管理ツール」より「グループポリシーの管理」を起動します。



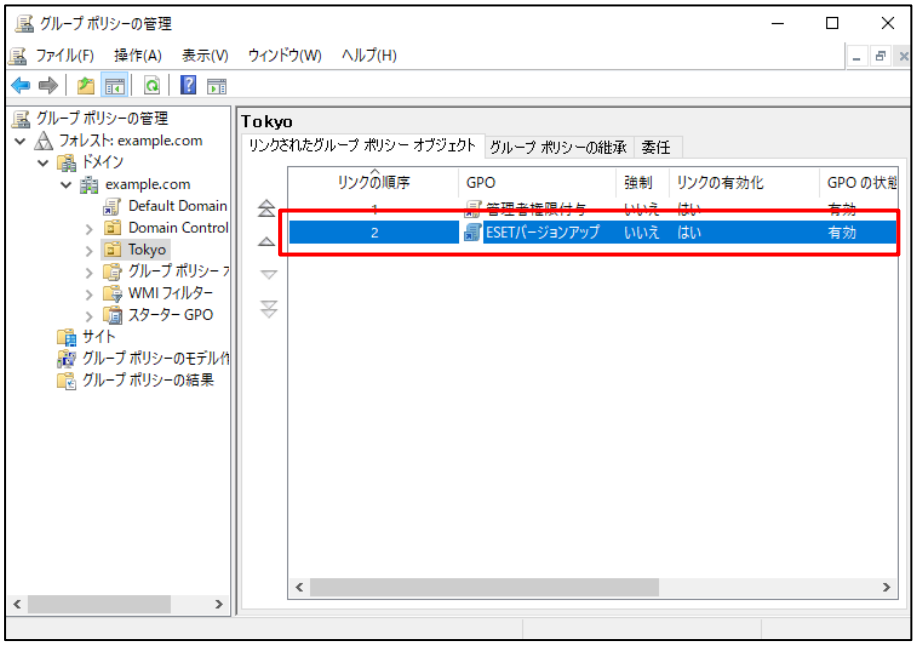
2. 「グループポリシーの管理」が起動したら、クライアント端末が所属している OU を右クリックし、「既存の GPO のリンク」をクリックします。



3. 「GPO を指定するドメイン」が正しく設定されていることを確認し＜a-2-1＞で作成した GPO を選択し、[OK]ボタンをクリックします。



4. 「リンクされたグループポリシーオブジェクト」の一覧に、手順 3 で選択した GPO が追加されていることを確認します。



以上で、EM エージェントとクライアント用プログラムのバージョンアップ用の GPO の配布は終了です。

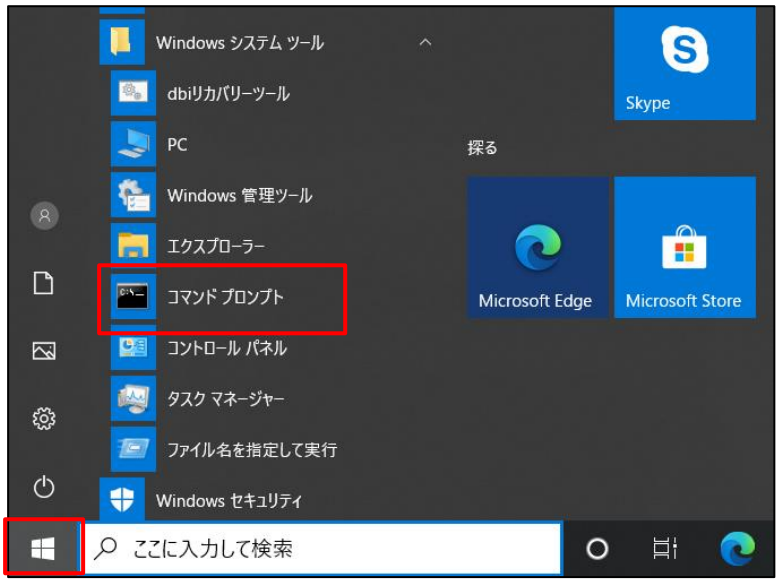
a-3. EM エージェントとクライアント用プログラムのバージョンアップ

GPO の配布が完了すると、クライアント端末の次回起動時にバージョンアップが実行されます。
バージョンアップ後は以下の画像のようにクライアント端末の再起動が必要になりますので、必ず再起動を行ってください。
※クライアント端末での GPO 適用には時間がかかる場合があります。
※「リアルタイムファイルシステム保護は機能していません」というアラートが表示される場合は、
再起動により解消されます。

再起動が終了したら、クライアント端末のバージョンアップは完了です。
【STEP6】で各プログラムのバージョンが完了したことを確認します。

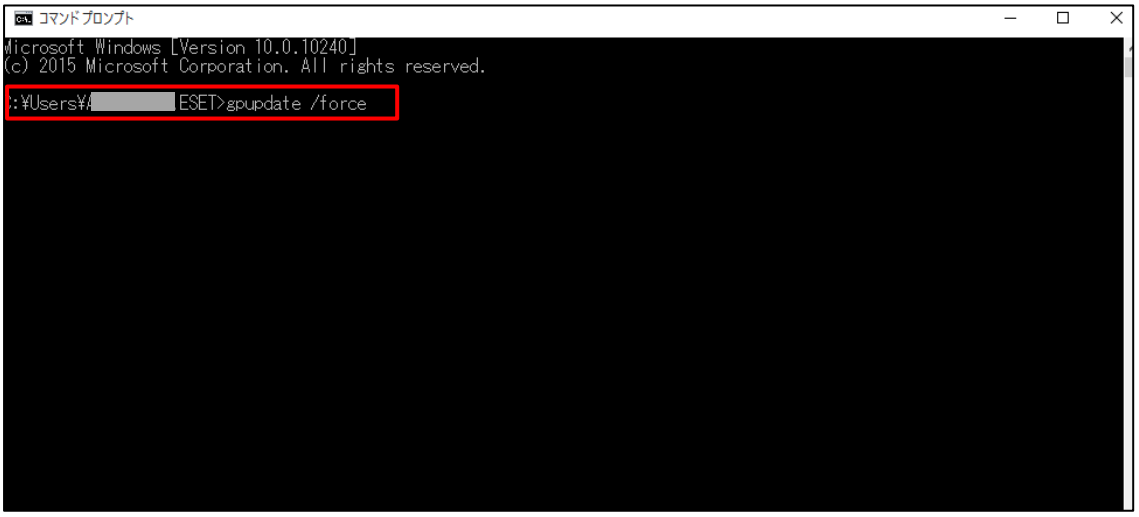
※次回起動時以降にバージョンアップが行われない場合は、クライアント端末で以下の操作を行ってください。

1. クライアント端末でスタートボタンをクリックし、「Windows システムツール」より、「コマンドプロンプト」を起動します。

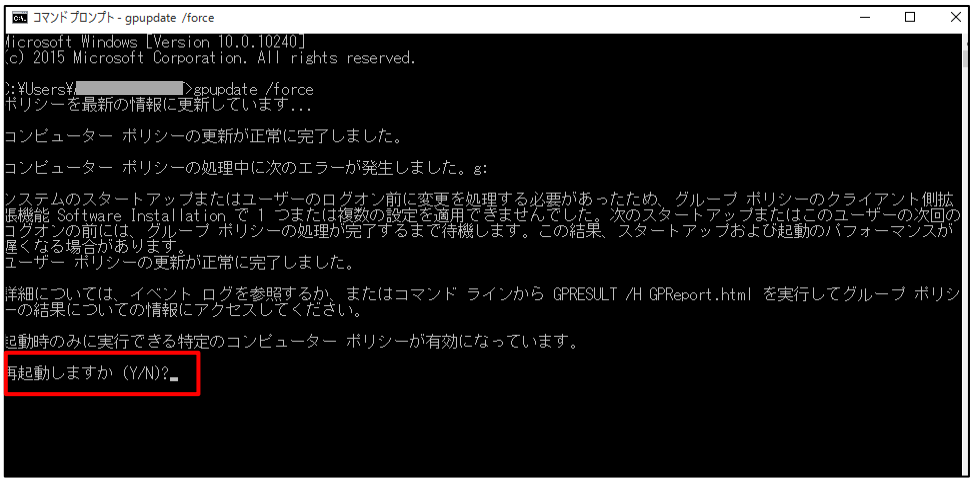


2. 「コマンドプロンプト」が起動したら、以下のコマンドを実行します。

コマンド：gpupdate /force



3. 「再起動しますか(Y/N)?」が表示されたら、「Y」を入力し再起動します。

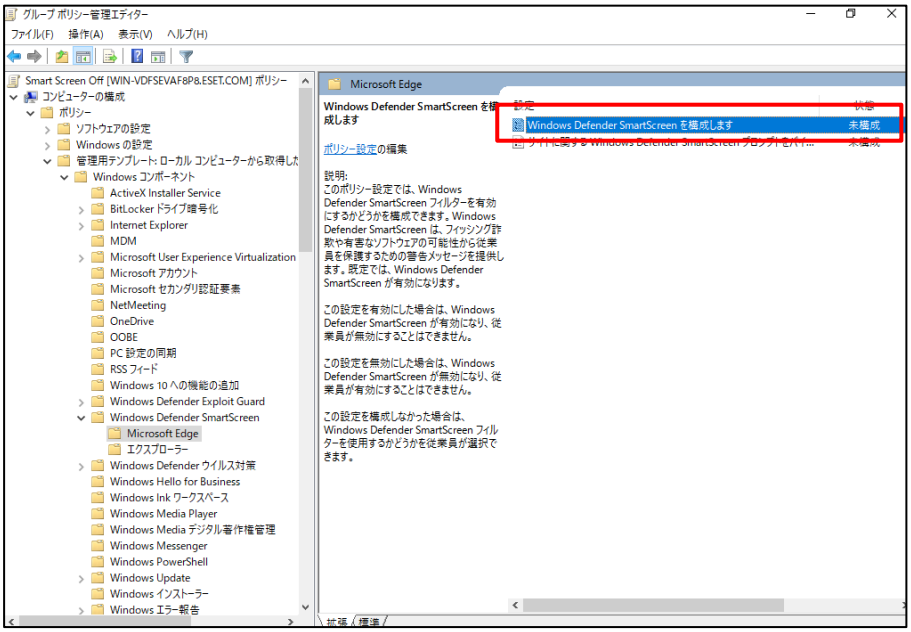


4. 再起動後、バージョンアップが行われたことを確認します。

<参考>

クライアント端末で、「SmartScreen」が有効になっている場合は、バージョンアップに失敗する場合があります。以下の画像を参考に、「グループポリシー管理エディター」で「SmartScreen」を無効にするGPO を作成・配布するなどして対応をお願いします。

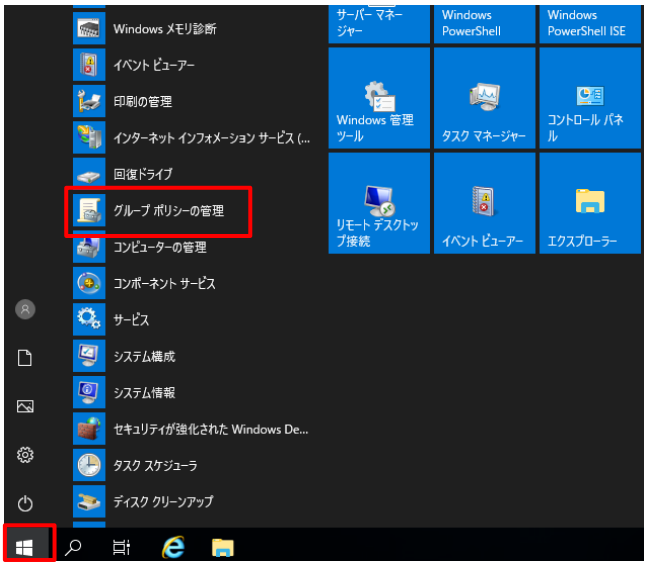
※[グループポリシー管理エディター]で[コンピューターの構成]-[ポリシー]-[管理用テンプレート]-[Windows コンポーネント]-[Windows Defender SmartScreen]-[Microsoft Edge]を展開し、「Windows Defender SmartScreen を構成します」をダブルクリックして設定を行います。



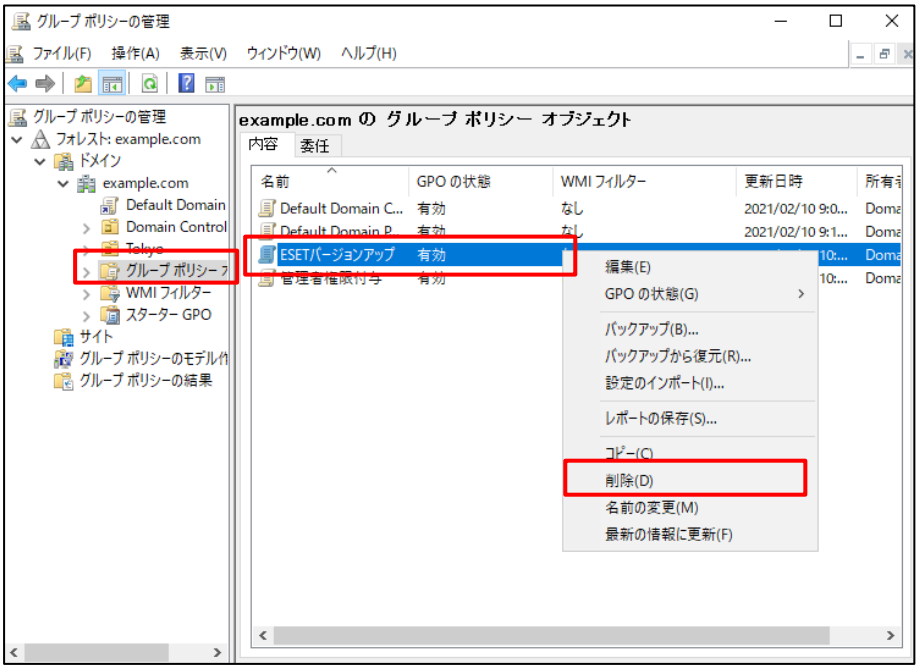
※以下の＜a-4＞は、【STEP6】でバージョンアップ完了が確認できた後に実施してください。

a-4. 配布した GPO の割り当て解除

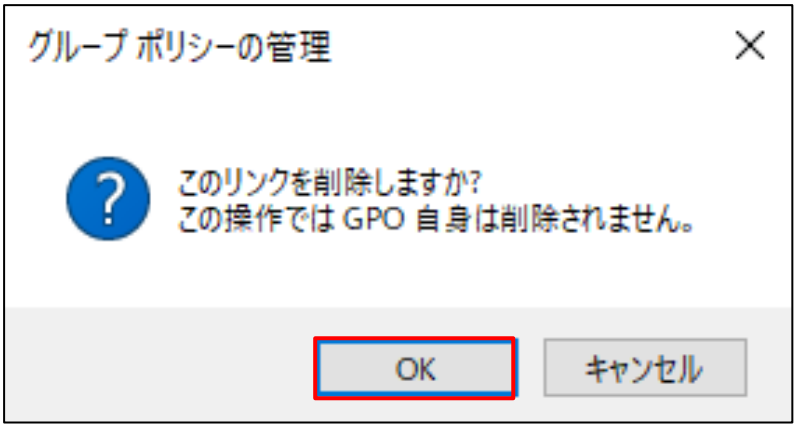
1. スタートボタンをクリックし、「Windows 管理ツール」より「グループポリシーの管理」を起動します。



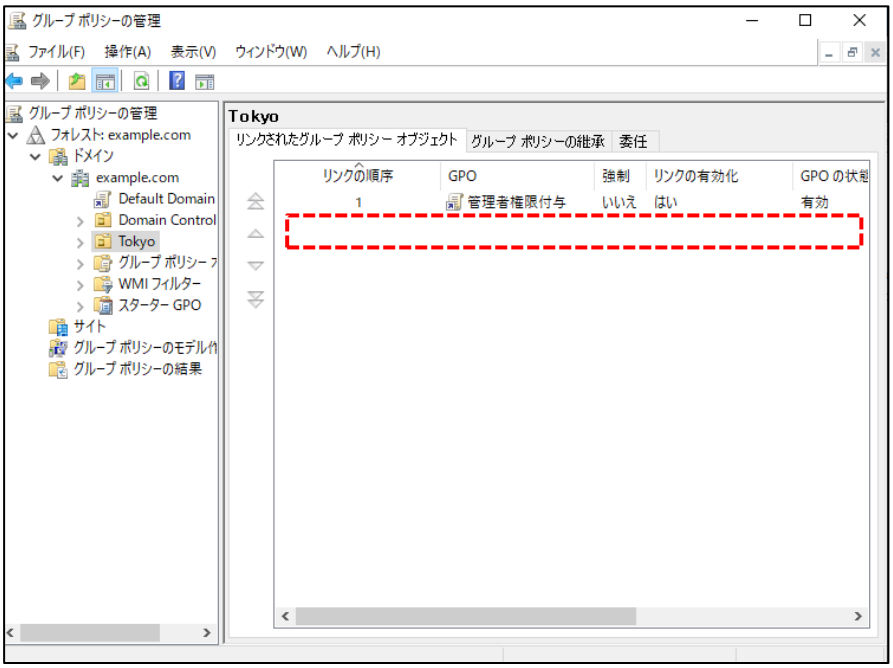
2. 「グループポリシーの管理」が起動したら、クライアント端末が所属している OU を選択し、クライアント用プログラムのバージョンアップ用に割り当てた GPO を右クリックして[削除]をクリックします。



3. 以下のポップアップが表示されたら、[OK]ボタンをクリックします。



4. クライアント端末のバージョンアップ用に割り当てた GPO が削除されていることを確認します。



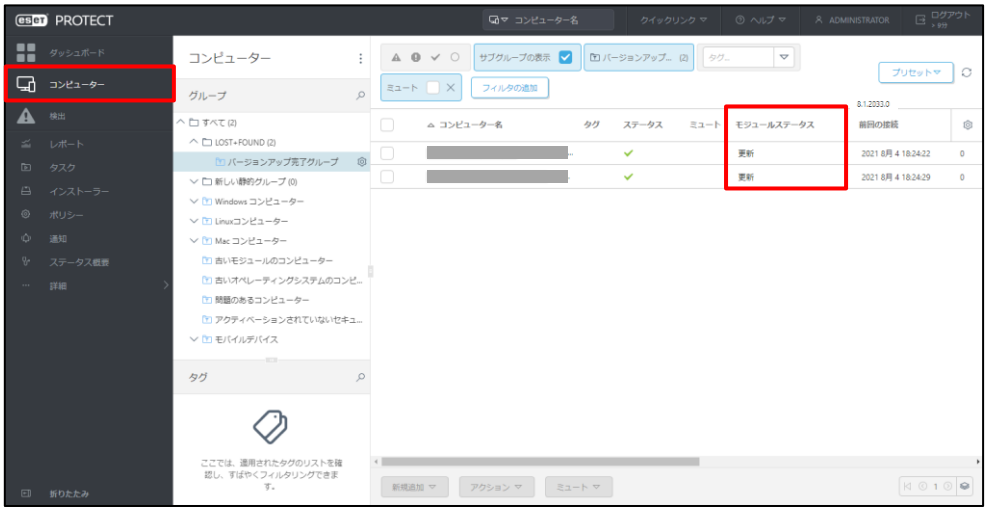
以上で、GPO の割り当て解除は完了です。

以上で、【パターン D：AD 環境で GPO を使用してバージョンアップする場合】は完了です。

10. 【STEP6】 バージョンアップ完了の確認

1. Web コンソール を起動して、ESET PROTECT に接続します。
   ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
   ※ EP Web コンソールには以下の URL よりアクセスできます。
   https://＜管理サーバーのサーバー名、または、IP アドレス＞/era

2. 「コンピューター」より、【STEP4】で作成した動的グループにバージョンアップしたクライアントが所属し、セキュリティ製品バージョンがクライアント用プログラム、サーバー用プログラムともに「9.X」であることが確認できれば、バージョンアップ完了です。
   また、モジュールステータスが「更新」になっていることもご確認ください。
   ※バージョンアップ後は再起動が必要なため、アラートが表示されます。
   その場合は、クライアントの再起動を行ってください。



以上でバージョンアップ作業は終了です。