ESET PROTECT ソリューション

V7 から V8 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 9 版
2022 年 2 月 15 日
キヤノンマーケティングジャパン株式会社

目次

※上記手順 9～11(P35~P66)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 P34 をご確認ください。

1. はじめに

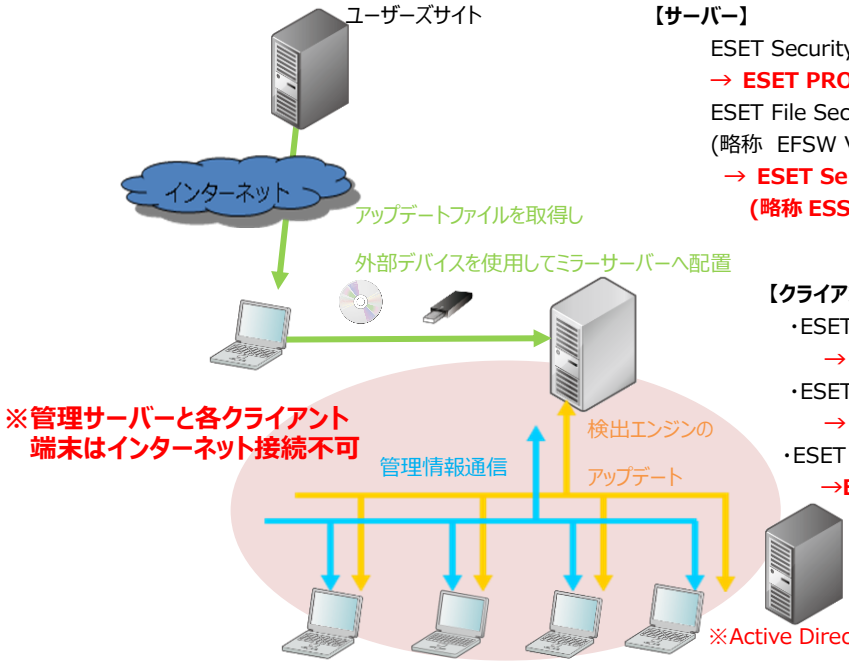
○本資料は、ESET PROTECT ソリューションをご利用のお客さまが旧バージョンからバージョン 8 へバージョンアップする際に必要となる作業や注意事項について記載しています。

○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。

2. 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 プログラムから V8 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 ・管理サーバー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 ・管理サーバー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 Security Management Center V7.X	・ESET PROTECT V8.X 以降
	ミラー	・ユーザーズサイトから取得したファイルを IIS または EFSW V7.X 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 または ESSW V8.0 以降のミラー機能で公開
	ウイルス・スパイウェア対策	・ESET File Security for Microsoft Windows Server V7.X	・ESET Server Security for Microsoft Windows Server V8.X 以降
クライアント用 (Windows10)	管理	・ESET Management エージェント V7.X	・ESET Management エージェント V8.X
	ウイルス・スパイウェア対策	・ESET Endpoint Security V7.X または ESET Endpoint アンチウイルス V7.X	・ESET Endpoint Security V8.X ・ESET Endpoint アンチウイルス V8.X



【サーバー】

ESET Security Management Center V7.X (略称 ESMC V7.X)
→ ESET PROTECT V8.X (略称 EP V8.X)
ESET File Security for Microsoft Windows Server V7.X
(略称 EFSW V7.X)
→ ESET Server Security for Microsoft Windows Server V8.0 (略称 ESSW V8.X 以降)

【クライアント】

・ESET Endpoint Security V7.X (略称 EES V7.X)
→ ESET Endpoint Security V8.X (略称 EES V8.X)
・ESET Endpoint アンチウイルス V7.X (略称 EEA V7.X)
→ ESET Endpoint アンチウイルス V8.X (略称 EEA V8.X)
・ESET Management エージェント V7.X (略称 EM エージェント V7.X)
→ESET Management エージェント V8.X (略称 EM エージェント V8.X)

3. 新バージョンへのバージョンアップフロー

V7.X から V8.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】ESET Security Management Center サーバーのバックアップ

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

STEP1-2. ESET Security Management Center 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】サーバーのバージョンアップ

STEP2-1. 動作要件の確認

STEP2-2. ESET File Security for Microsoft Windows Server のバージョンアップ

STEP2-3. ESET Security Management Center のバージョンアップ

STEP2-4. データベースのバックアップ

STEP2-5. ピア証明書と認証局のバックアップ

【STEP3】バージョンアップ確認のための動的グループの作成

【STEP4】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～C 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:Web サーバー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 C: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

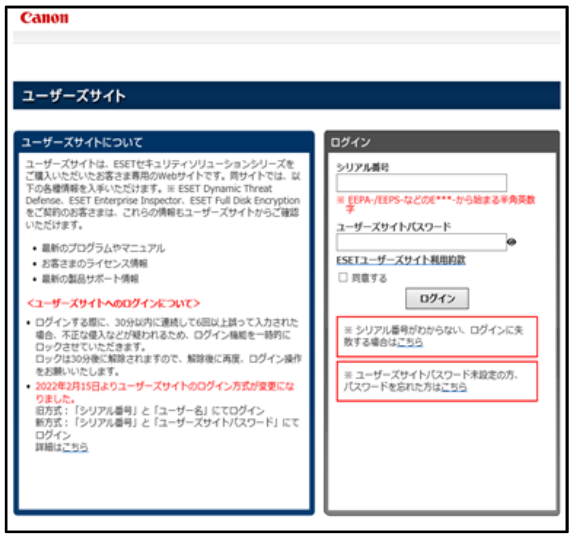
以降は共通の確認作業

【STEP5】バージョンアップ完了の確認

4.【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]と進みます。
   それぞれのプログラムの※に記載の[旧バージョンプログラムについて]をクリックし、[旧バージョンプログラムダウンロード]ページより以下のインストーラーをダウンロードします。
   ※ESET Server Security for Microsoft Windows Server については[最新版プログラム／マニュアル ダウンロード]より、最新版プログラムをダウンロードします。

・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.8.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.8.X.XXX.X)
※ESET PROTECT のオールインワンインストーラーの下にあります。

・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.8.X.XXX.X)

・Windows Server 向けクライアント用プログラム
ESET Server Security for Microsoft Windows Server(Ver. 8.X.XXXX.X)
※ESET Server Security for Microsoft Windows Server は最新版プログラムをダウンロードします。

5.【STEP1】ESET Security Management Center サーバーのバックアップ

ESET Security Management Center のバージョンアップをする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。

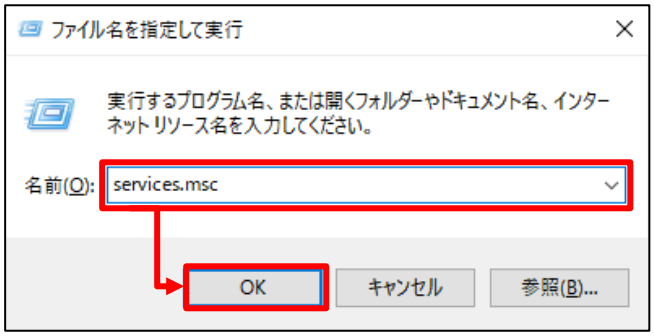
STEP1-2. ESET Security Management Center のサービス停止

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 ESMC のサービスを停止させます。

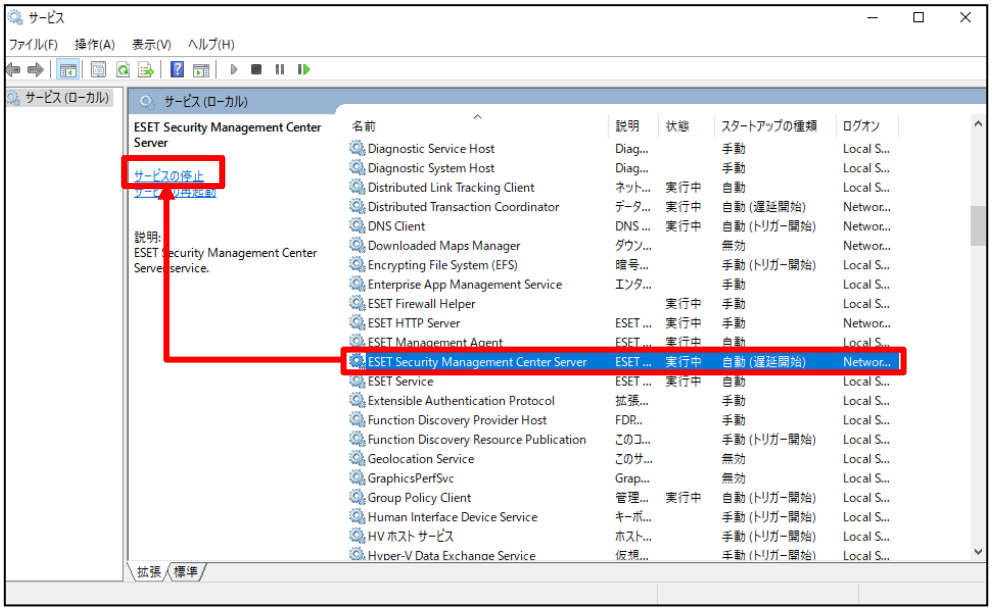
<注意>

ESMC のサービスを一時的に停止するため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 ESMC にログが送付されます。

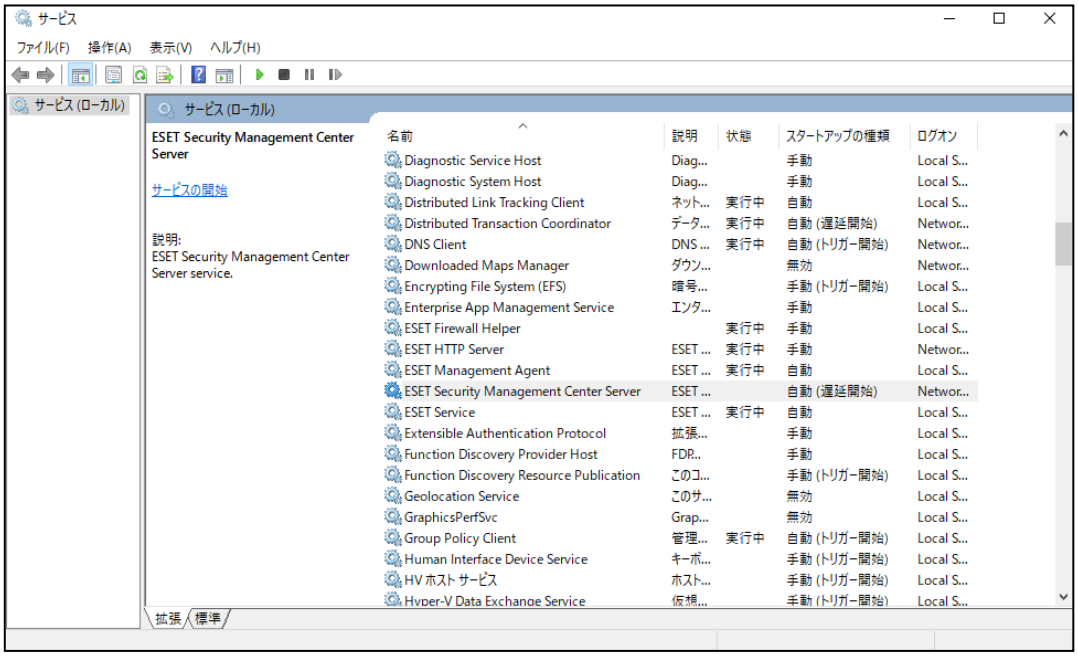
1. 「Windows キー」+「R」でファイル名を指定して実行させるウィンドウを開き「services.msc」と入力し、[OK]ボタンをクリックします。



2. 「ESET 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。



3. 「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。



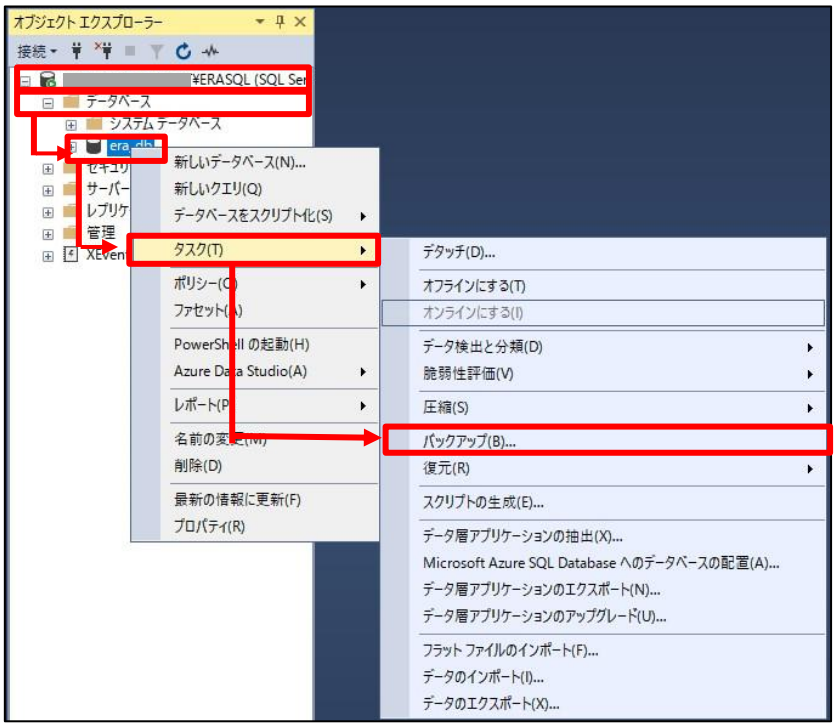
STEP1-3. データベースのバックアップ

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。

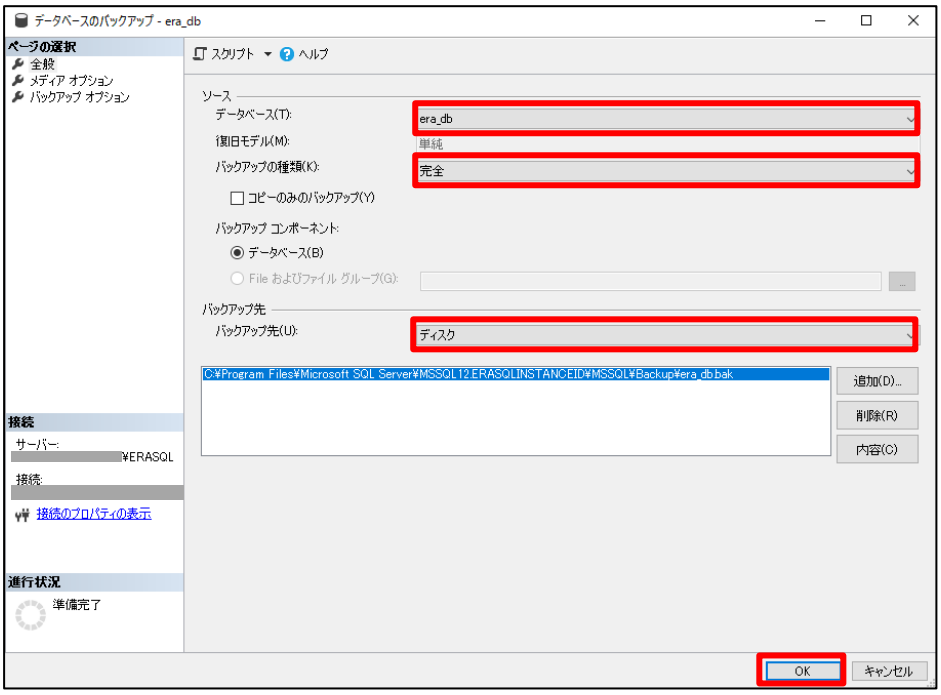
サーバーの種類	データベースエンジン
サーバー名	ESMC のサーバーで使用しているインスタンス名 ※既定は「コンピューター名¥ERASQL」
認証	Windows 認証

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。

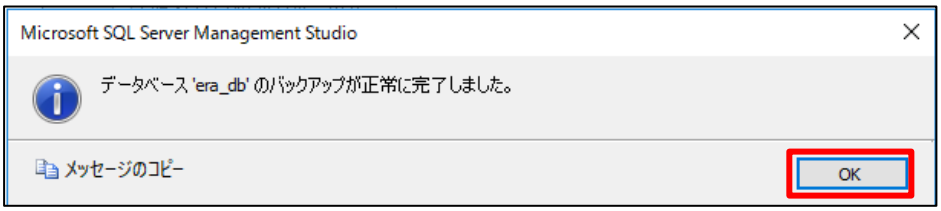


4. データベースのバックアップ画面で、以下の通り設定し、[OK]ボタンをクリックします。

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 Server 2008/ Window Server 2012/ Window Server 2016/ Window Server 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 Server 2008/ Window Server 2012/ Window Server 2016/ Window Server 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 Security Management Center Server」サービスを起動してください。

<注意>

EP V8.X 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>

ESET Security Management Center 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

6.【STEP2】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 ESMC と EFSW をバージョンアップします。

STEP2-1. 動作要件の確認

バージョンアップの前に、EP V8.X と ESSW V8.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 File 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。
なお、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。
＜Java Runtime Environment 8 のサポート終了に伴う今後の対応について＞
https://eset-support.canon-its.jp/faq/show/13127?site_domain=business

そのため、有償の JRE もしくは以下の URL を参照し、無償のオープンソース JDK の移行を実施してください。
＜【移行手順】Windows Server 環境に構築済みのセキュリティ管理ツールで、オープンソース JDK を利用するには？＞
https://eset-support.canon-its.jp/faq/show/13052?site_domain=business

＜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。
64bit 版のインストールにつきましては、以下 URL 内の「事前準備-3. Java と Apache Tomcat のバージョンアップ、または、64bit 版のダウンロード(項番 4 除く)」を参照してください。
＜Windows Server 環境でコンポーネントプログラムのインストーラーを利用して、セキュリティ管理ツールをバージョンアップする手順＞
https://eset-support.canon-its.jp/faq/show/4773?site_domain=business
※既に 64bit 版を利用している場合は、Apache Tomcat の事前バージョンアップは必要ありません。

＜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。

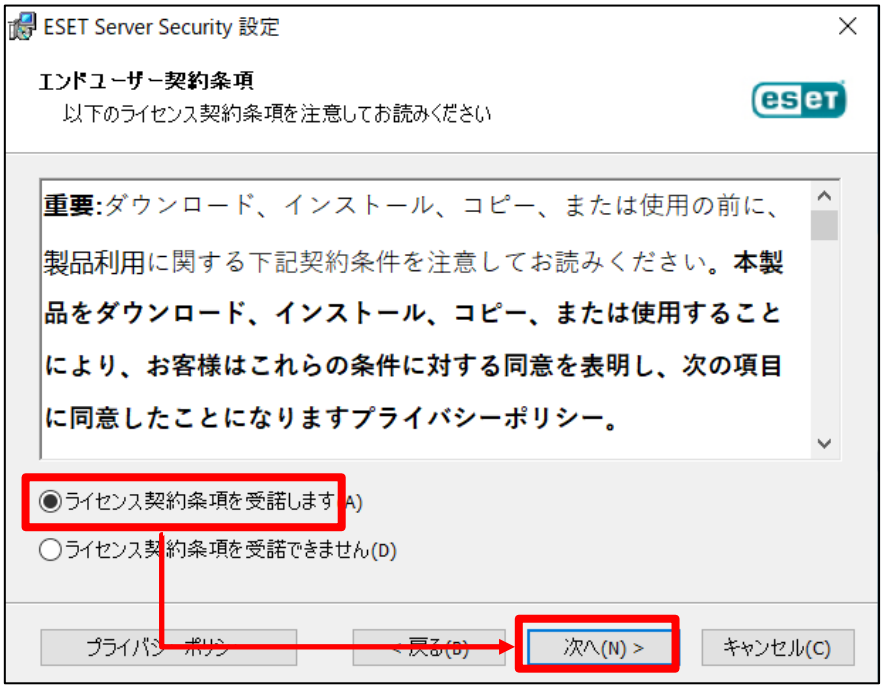
STEP2-2. ESET File Security for Microsoft Windows Server のバージョンアップ

以下の手順で ESET Server Security for Microsoft Windows Server V8.0 以降へ上書きバージョンアップします。

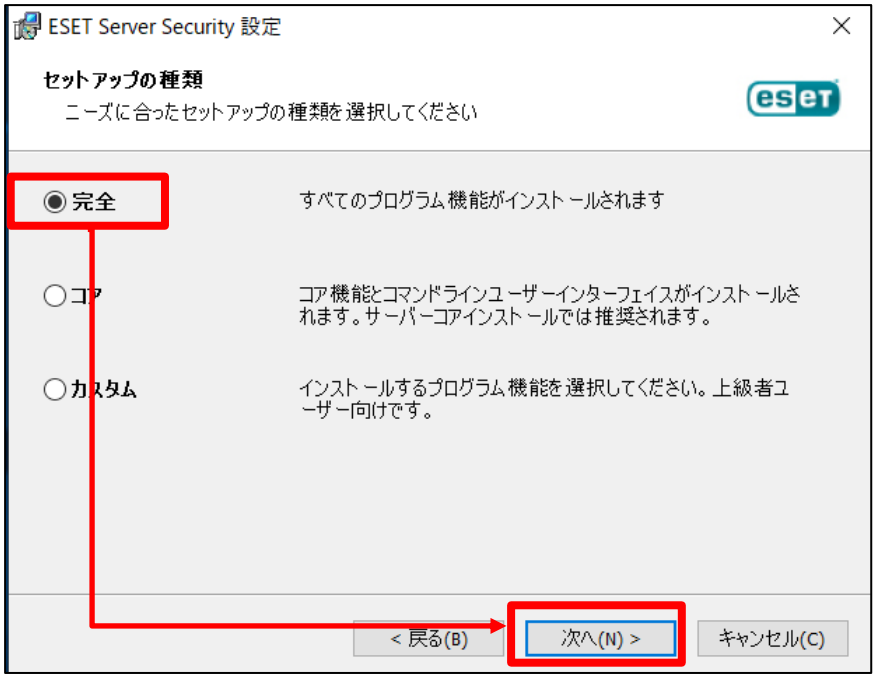
1. 【STEP0】事前準備でダウンロードした ESET Server Security for Microsoft Windows Server のインストーラーをサーバー上の任意の場所に移動し、ダブルクリックして実行します。

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。

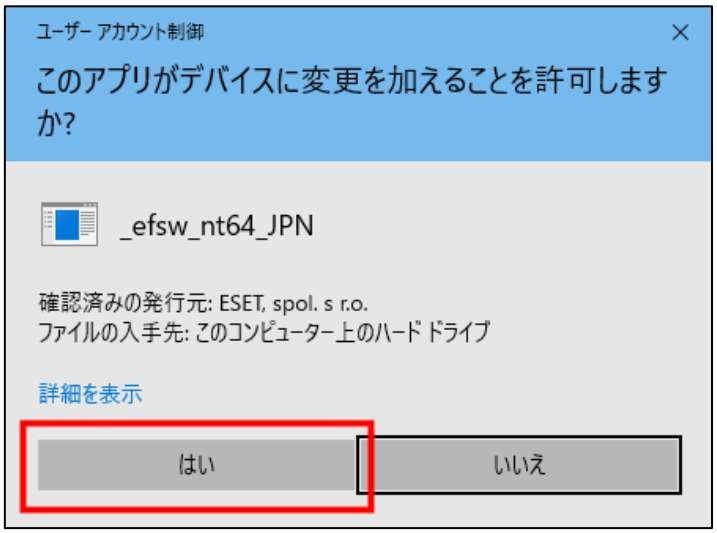


4. 「セットアップの種類」画面が表示されます。
[完全]のラジオボタンにチェックを入れ、[次へ]ボタンをクリックします。



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。

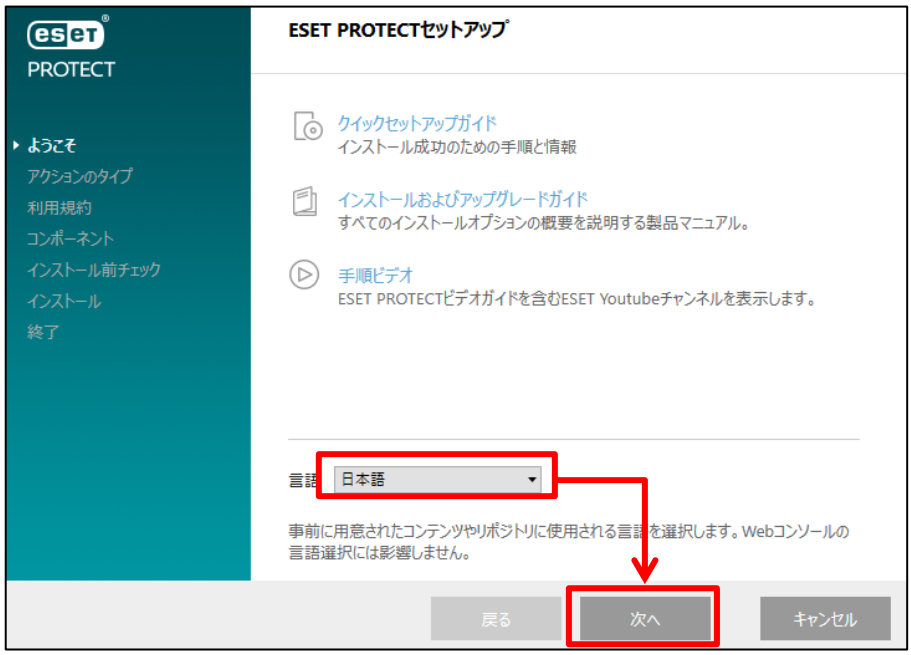
※「再起動」を促すアラートが表示されますが、次の【STEP2-3】を実行後に再起動いたします。

STEP2-3. ESET Security Management Center のバージョンアップ

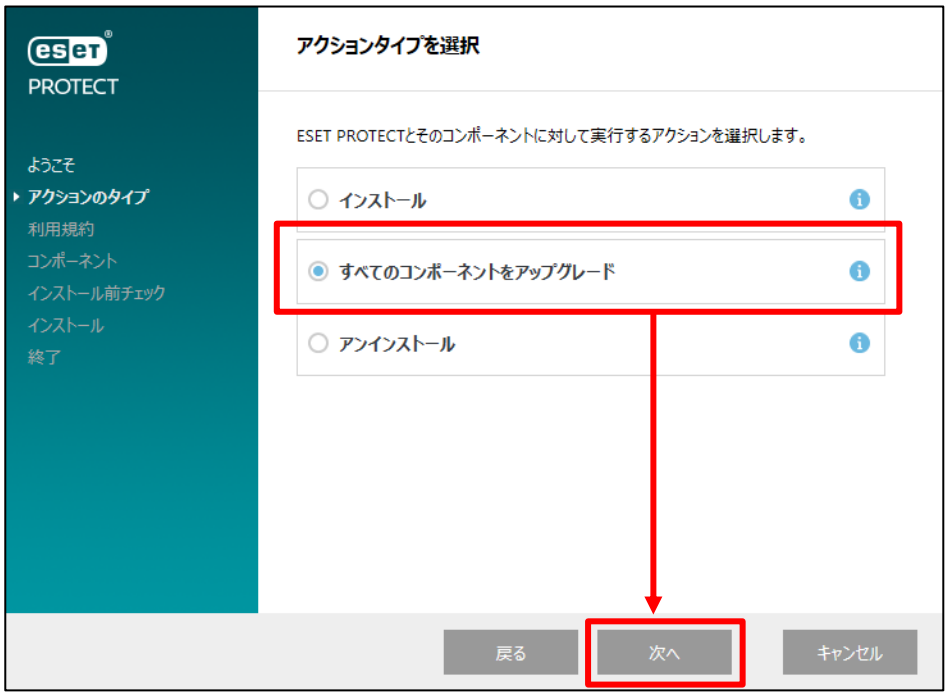
1. 【STEP0】事前準備でユーザーズサイトよりダウンロードした「ESET PROTECT(Ver 8.X.XX.X)」のオールインワンインストーラー「Setup_x64.zip」をサーバー上の任意の場所に配置します。

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。

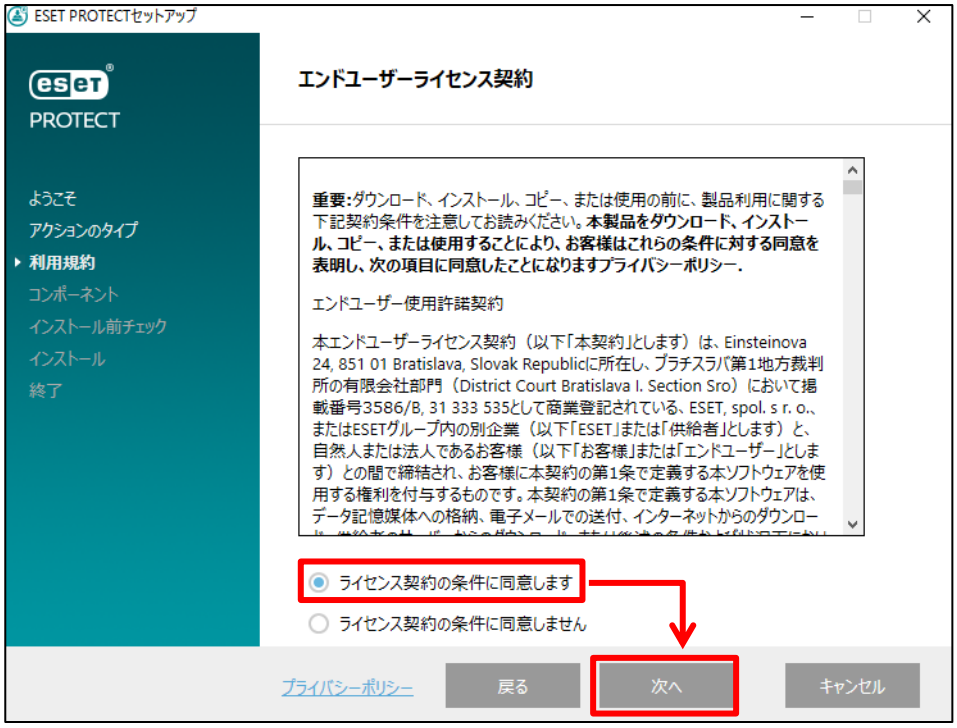
3. 言語で「日本語」を選択し、[次へ]ボタンをクリックします。



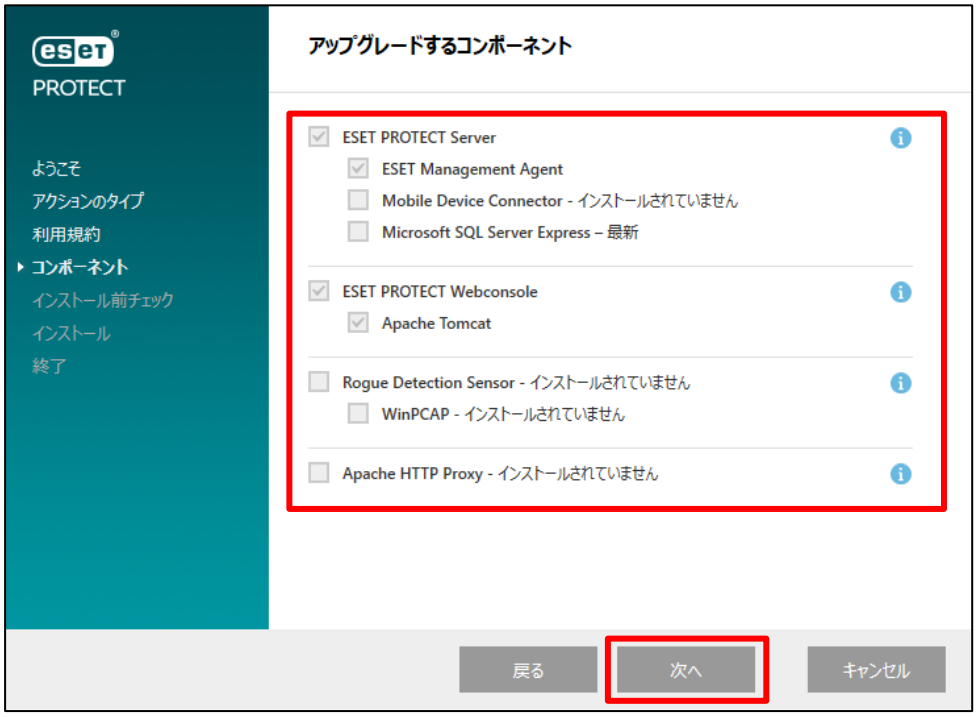
4. 「すべてのコンポーネントをアップグレード」を選択し、[次へ]ボタンをクリックします。



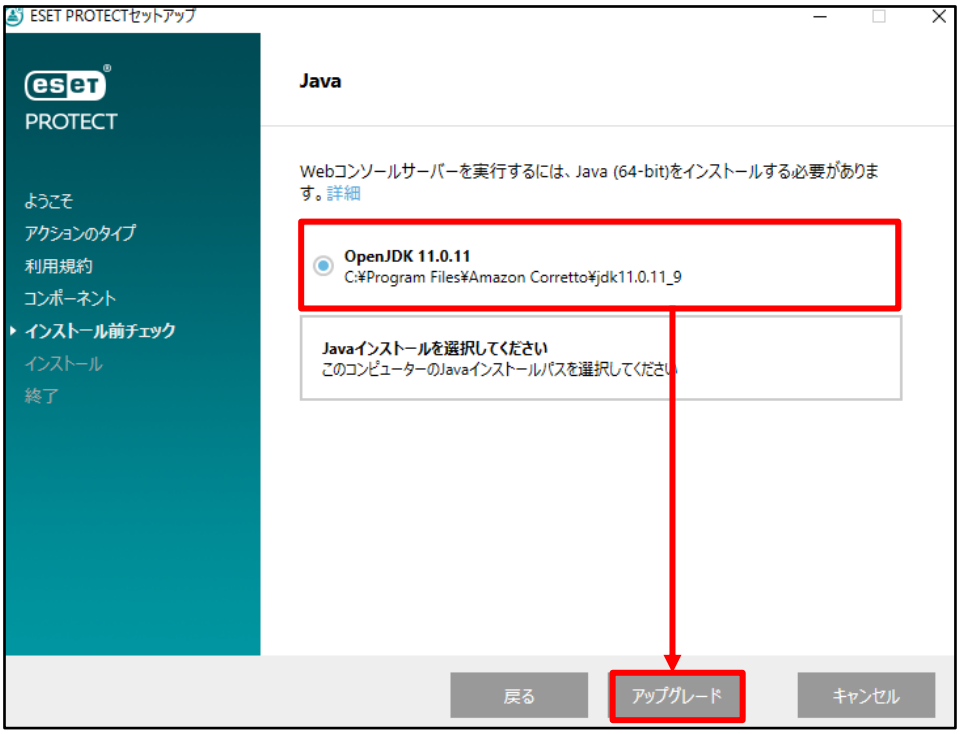
5. エンドユーザーライセンス契約に同意したら、「ラインセンス契約の条件に同意します」を選択し、[次へ]ボタンをクリックします。



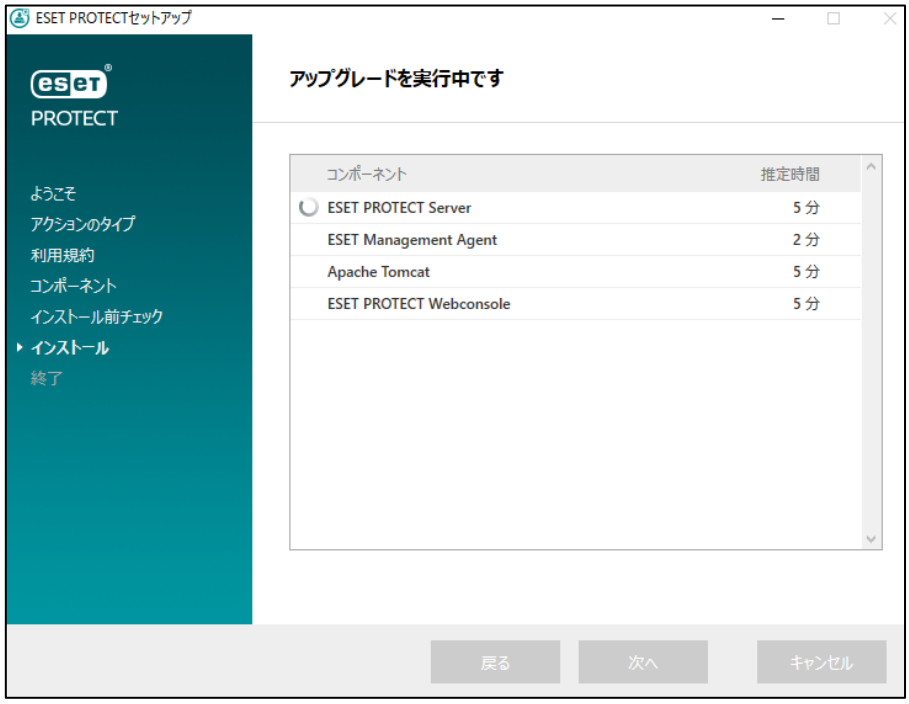
6. アップグレードするコンポーネントを確認し、[次へ]ボタンをクリックします。
※ESMC V7.X で利用しているコンポーネントがアップグレードされます。



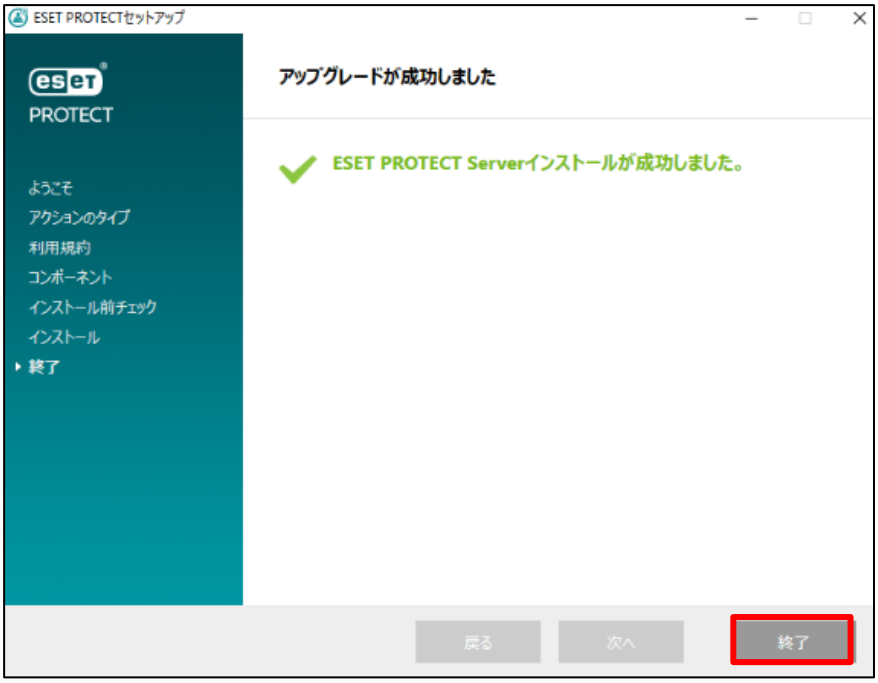
7. ご利用の Java を選択します。Amazon Corretto を利用している場合は、「OpenJDK」を選択し、[アップグレード]ボタンをクリックします。



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。

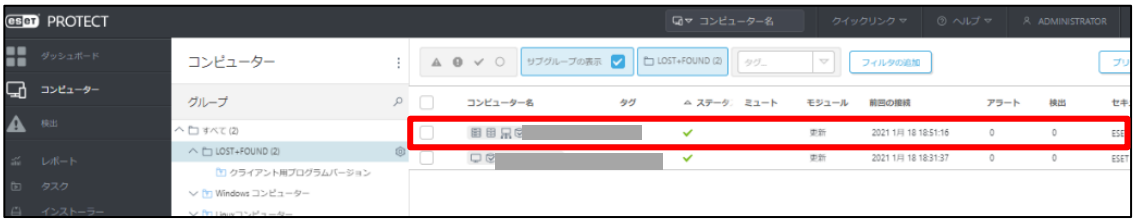


10. 再起動します。

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、「8.X」であることを確認します。

STEP2-4. データベースのバックアップ

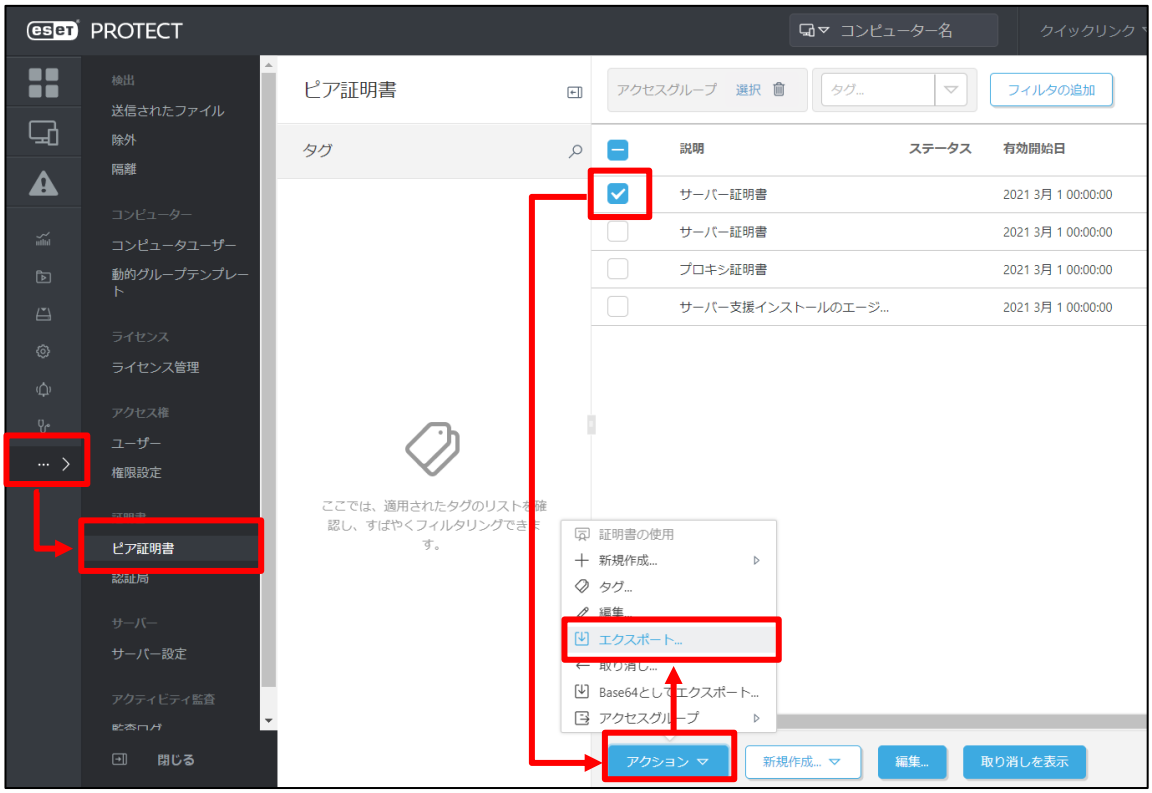
【STEP1】ESET Security Management Center サーバーのバックアップと同様の方法で、再度 ESET PROTECT のデータベースとコンフィグレーションのバックアップを取得してください。

※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。

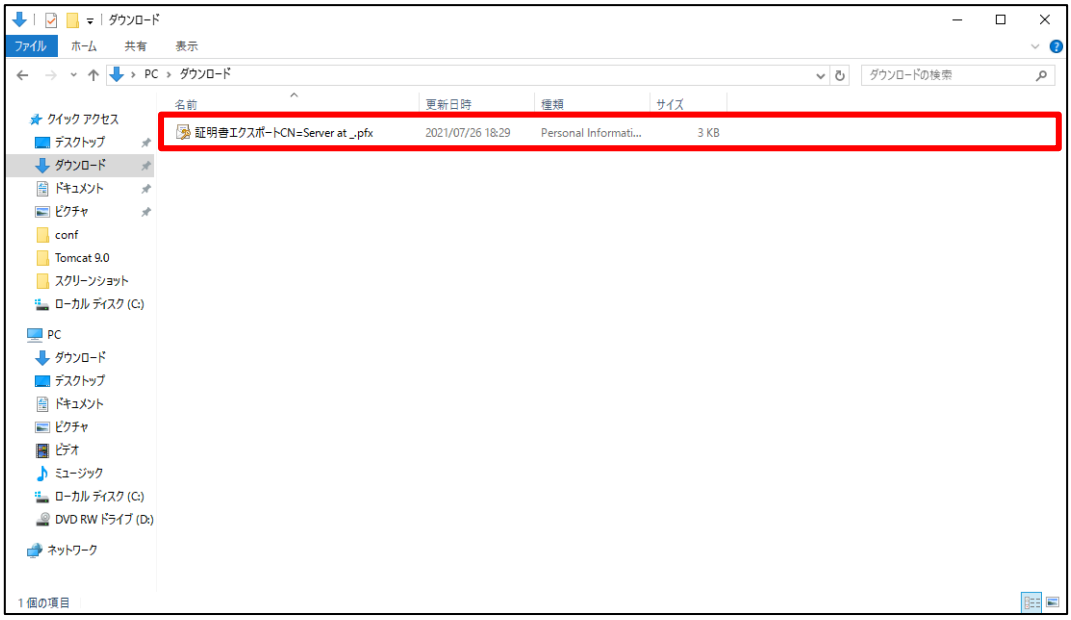
STEP2-5. ピア証明書と認証局のバックアップ

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。

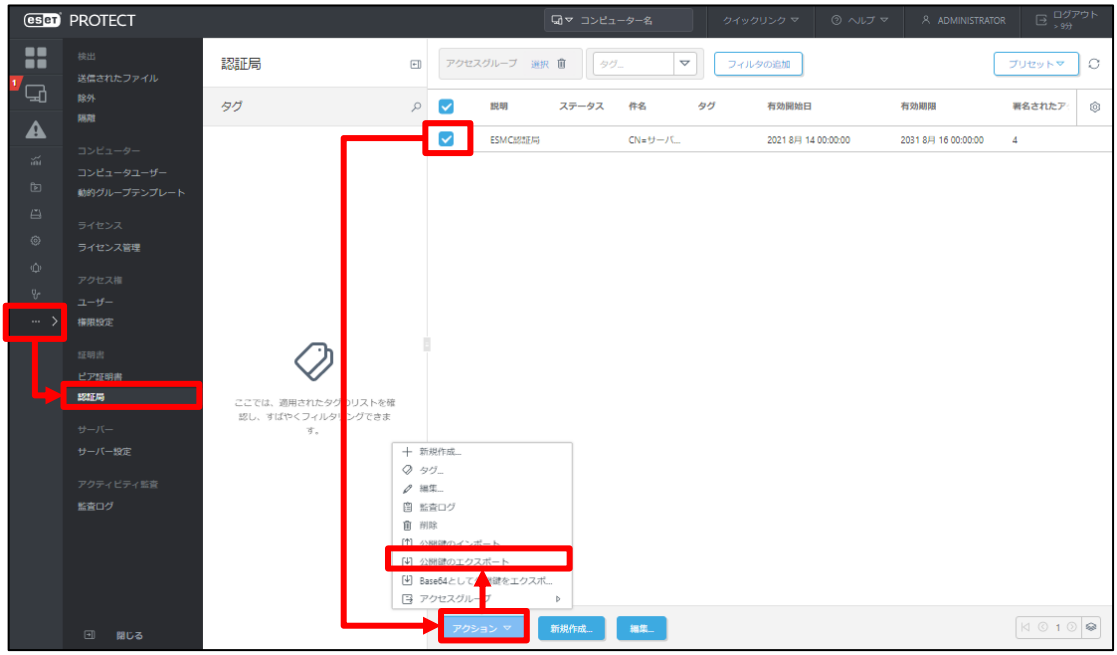


2. エクスポートした証明書を任意の保存先に保存します。

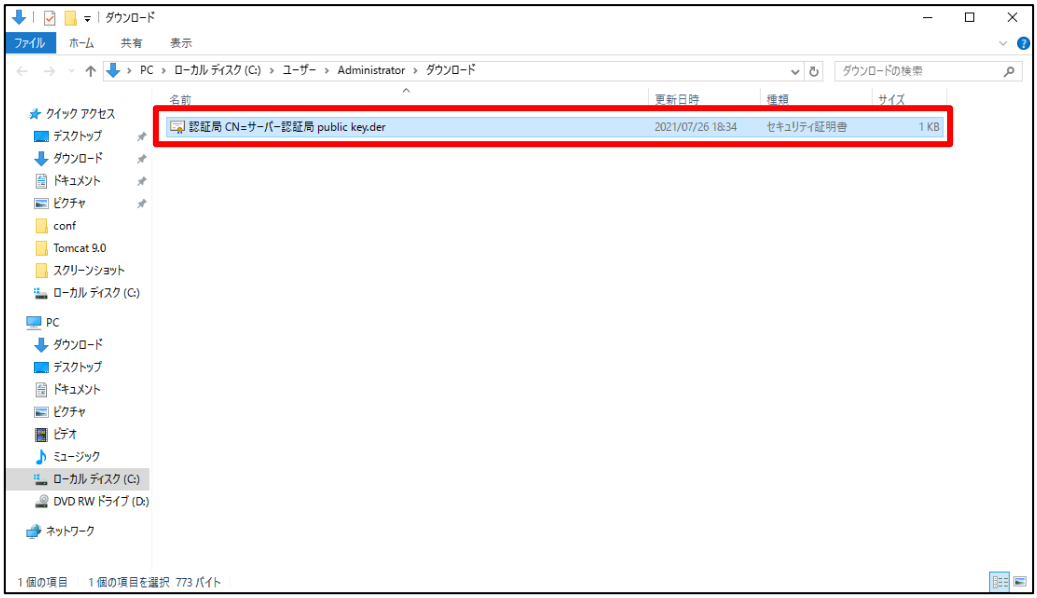


3. 手順 1～2 を繰り返し、各証明書のエクスポートを行います。

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

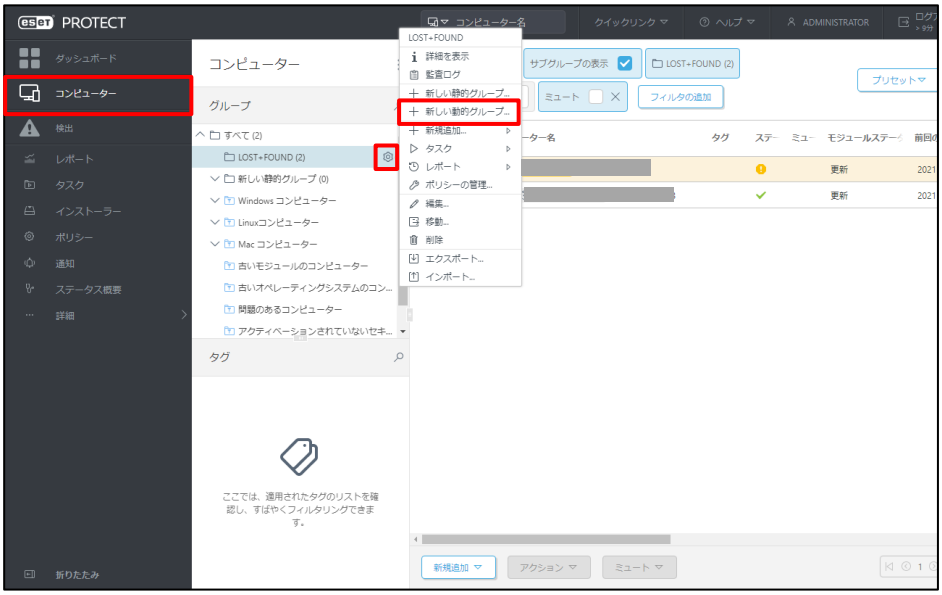
以上で、サーバーのバージョンアップは完了です。

7.【STEP3】バージョンアップ確認のための動的グループの作成

バージョンアップが完了したクライアント端末が振り分けられる動的グループを作成します。親グループに割り当てられているポリシーは引き継がれるため、アップデート先の設定などを新たに行う必要はありません。

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。



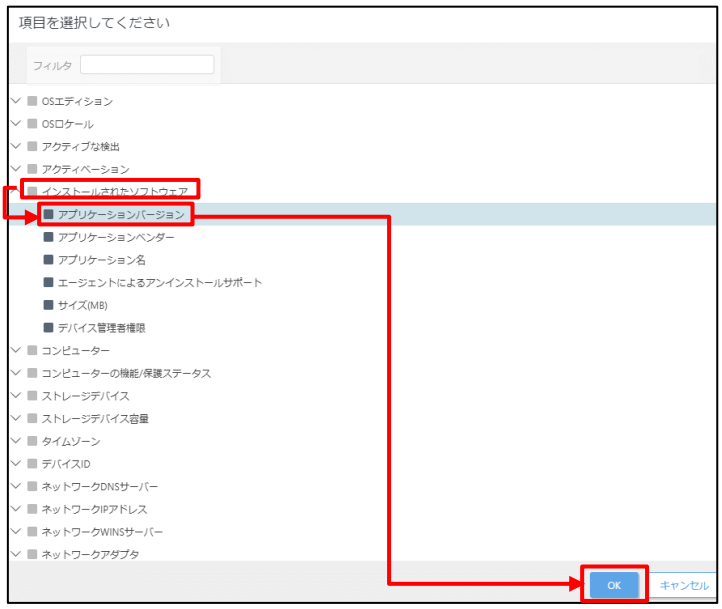
3. [基本]を展開し、任意の名前(例：バージョンアップ完了グループ)を入力します。
※「説明」の入力は任意です。

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：V8 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。

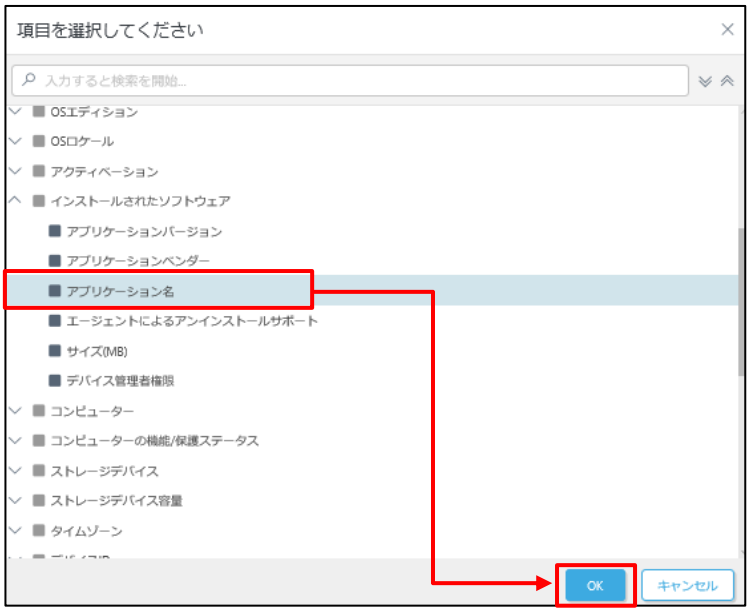
6. [式]を展開し、処理に「AND(すべての条件が真であること)」を選択します。
「ルールの追加」をクリックします。

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。

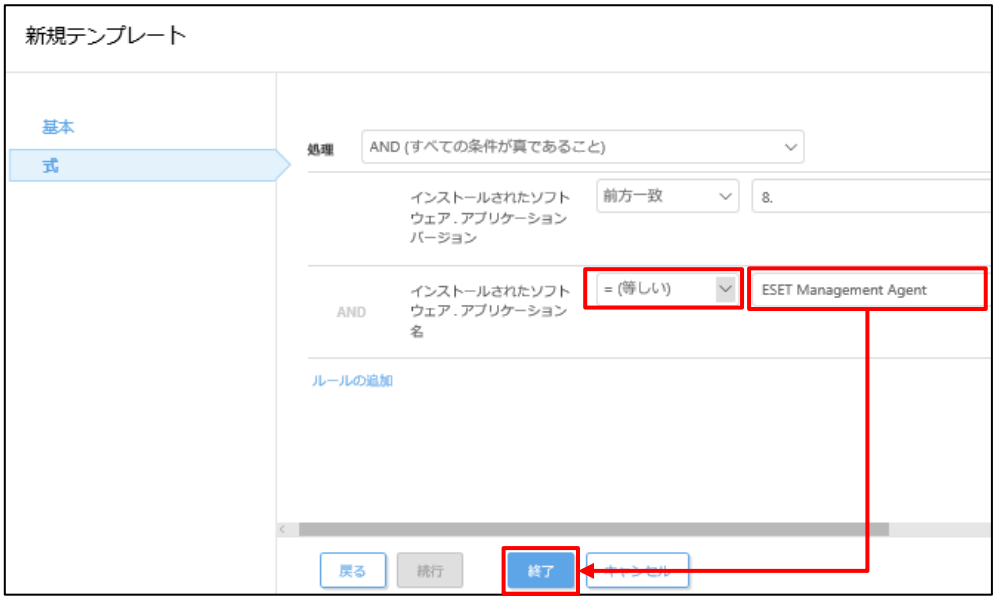


8. 「前方一致」を選択し、条件に「8.」と入力します。
「ルールの追加」をクリックします。

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。

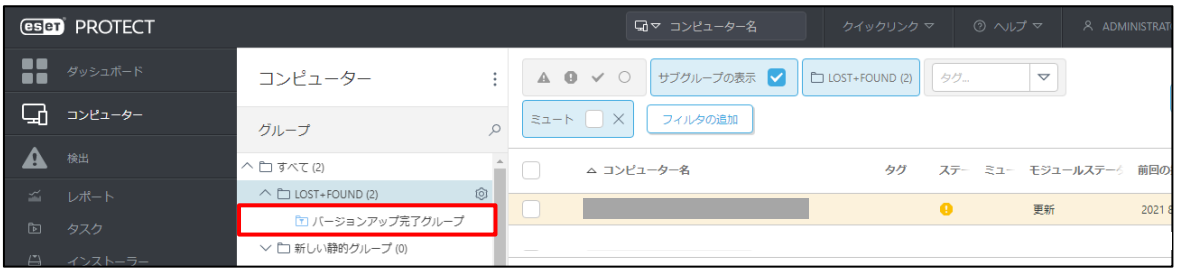


10. 「=(等しい)」を選択し、条件に「ESET Management Agent」を入力します。
手順 8 で設定した条件と、本手順 10 で設定した 2 つが指定されていることを確認し、[終了]ボタンをクリックします。



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。



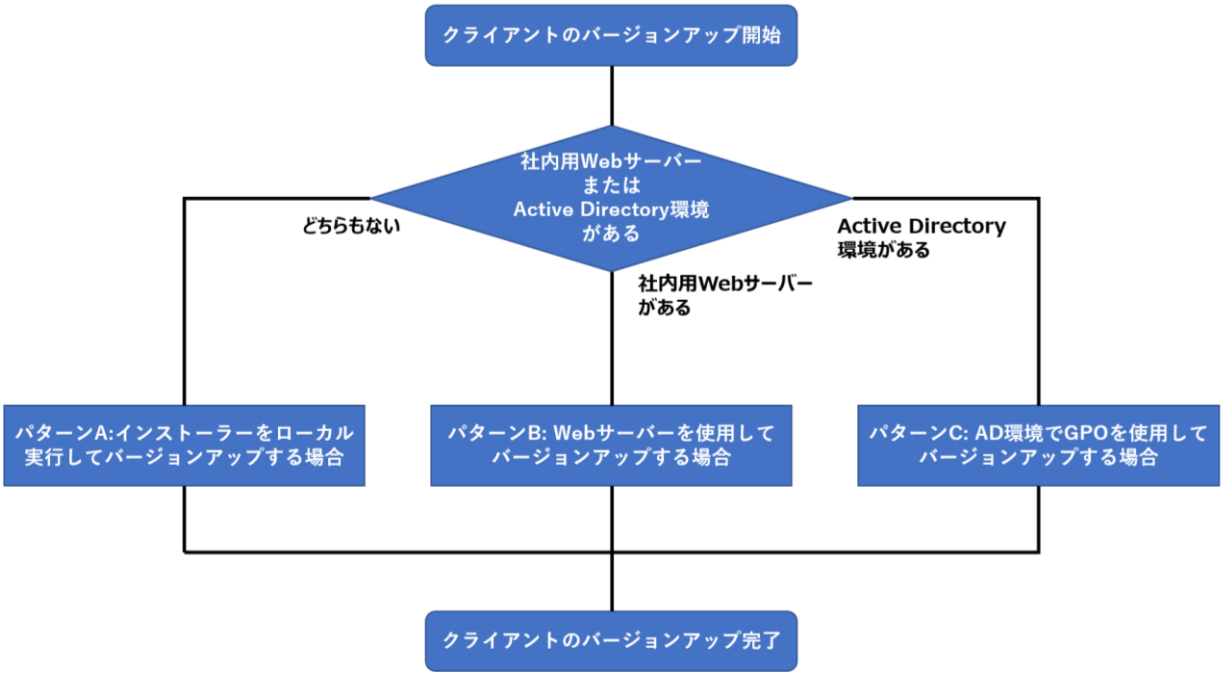
以上で、バージョンアップ確認のための動的グループの作成の作成は完了です。

8.【STEP4】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

【STEP4】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(P35～P41)

パターン B:Web サーバーを使用してバージョンアップする場合(P42～P53)

パターン C:AD 環境で GPO を使用してバージョンアップする場合(P54～P66)

9. 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

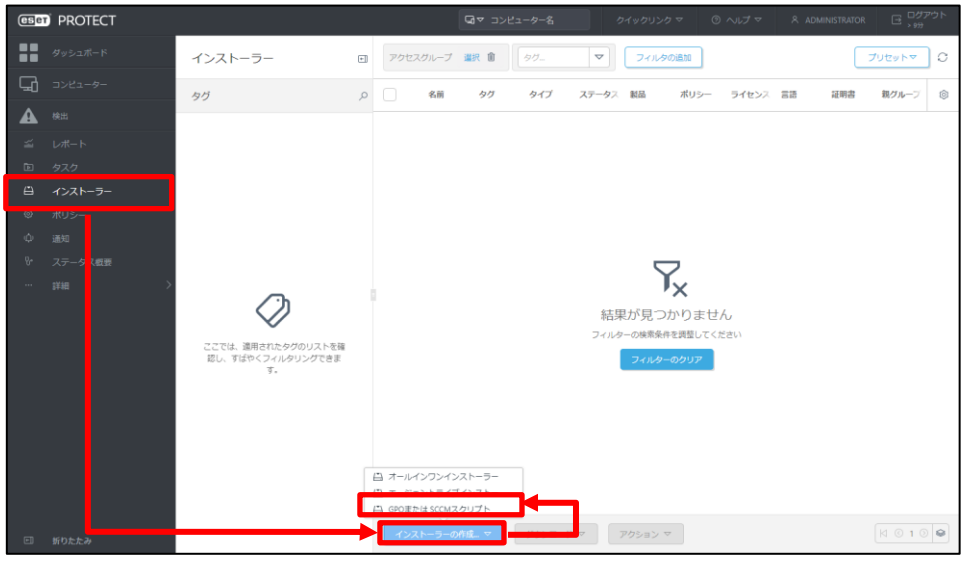
a. EM エージェントのバージョンアップ

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 V7.X を V8.X にバージョンアップします。

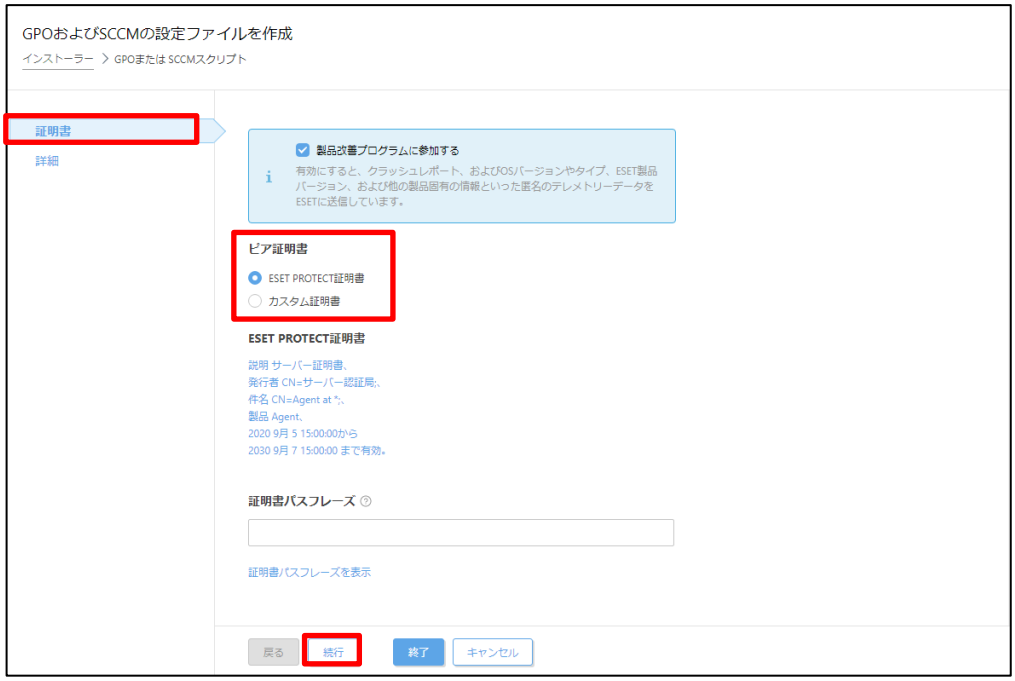
a-1. EM エージェントバージョンアップ用の GPO または SCCM スクリプトの準備

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。

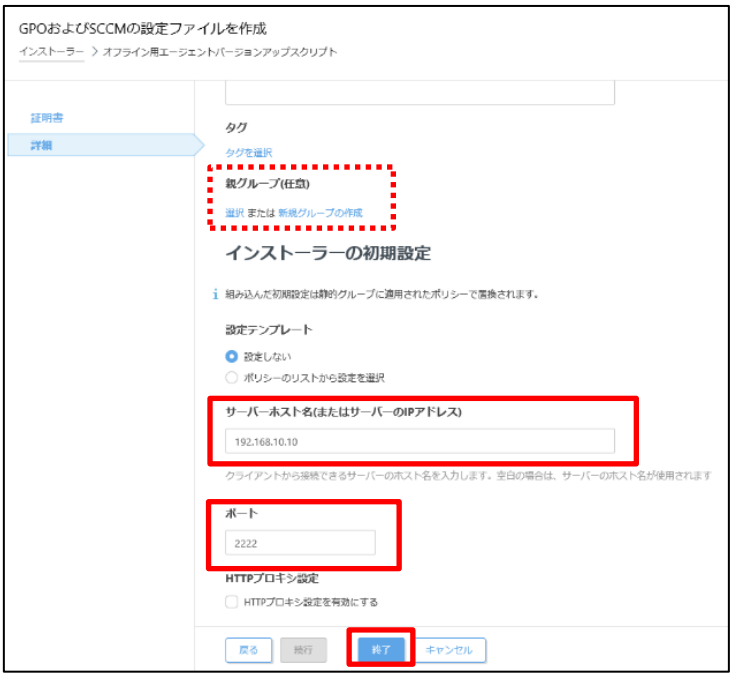


3. [証明書]を展開し、[ピア証明書]で「ESET PROTECT 証明書」を選択し、[続行]ボタンをクリックします。



4. [詳細]を展開し、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. 「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、[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。
   ※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。



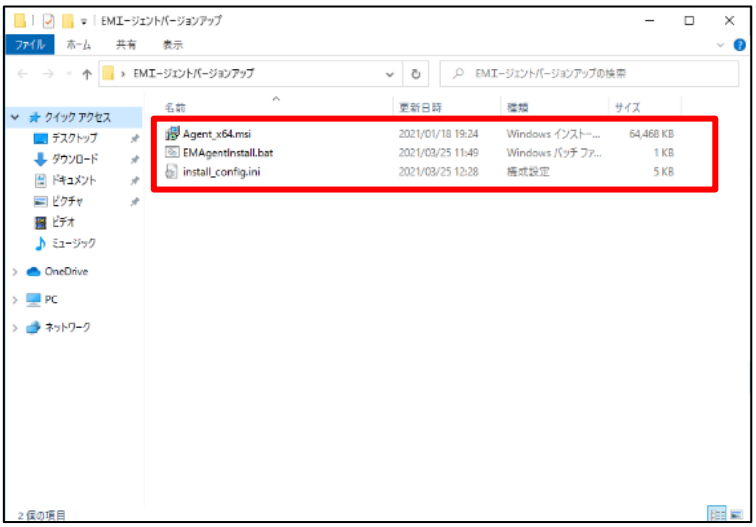
以上で、Web コンソール上での操作は完了です。

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 V8.X」**のインストーラーを同じフォルダに格納します。

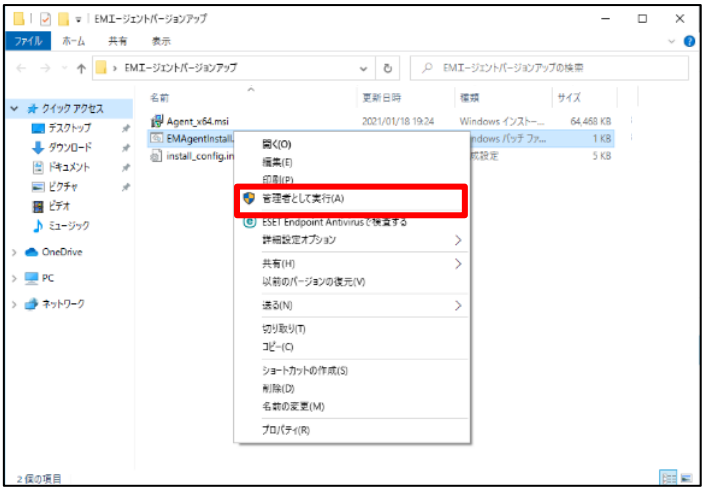


3. 手順 2 で作成したフォルダをお客様環境に合わせた方法で、バージョンアップを行うクライアント端末に配布します。(社内の共有フォルダなど)

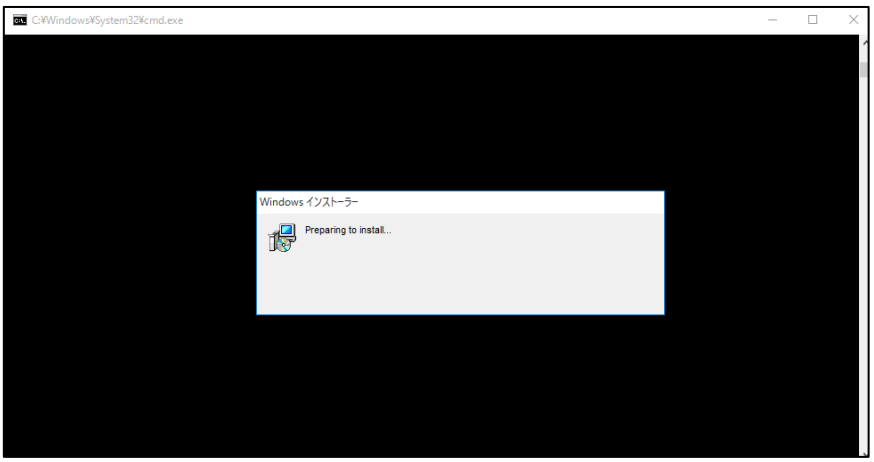
a-3.EM エージェントのバージョンアップ

<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 V8.X と EEA V8.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

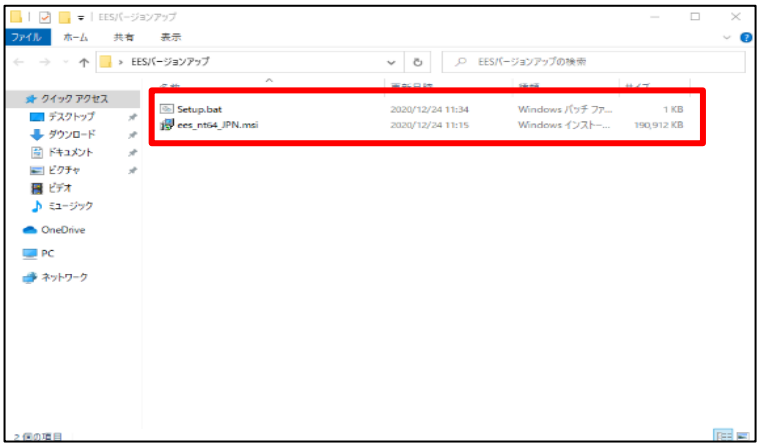
b-2. クライアント用プログラムのバージョンアップ用バッチファイルの準備

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_JPN.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 V8.X または EEA V8.X のインストーラー」**を同じフォルダに格納します。

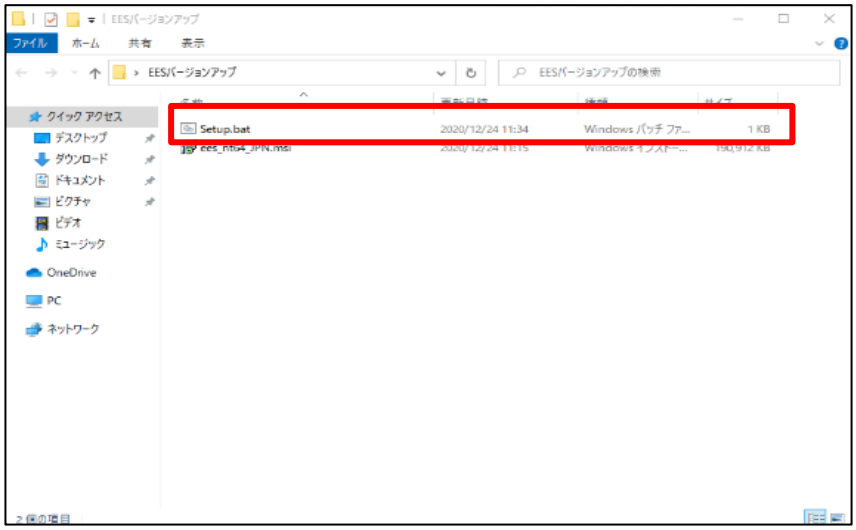


手順 2 で作成したフォルダをお客様環境に合わせた方法で、バージョンアップを行うクライアント端末に配布します。(社内の共有フォルダなど)

b-3. クライアント用プログラムのバージョンアップ

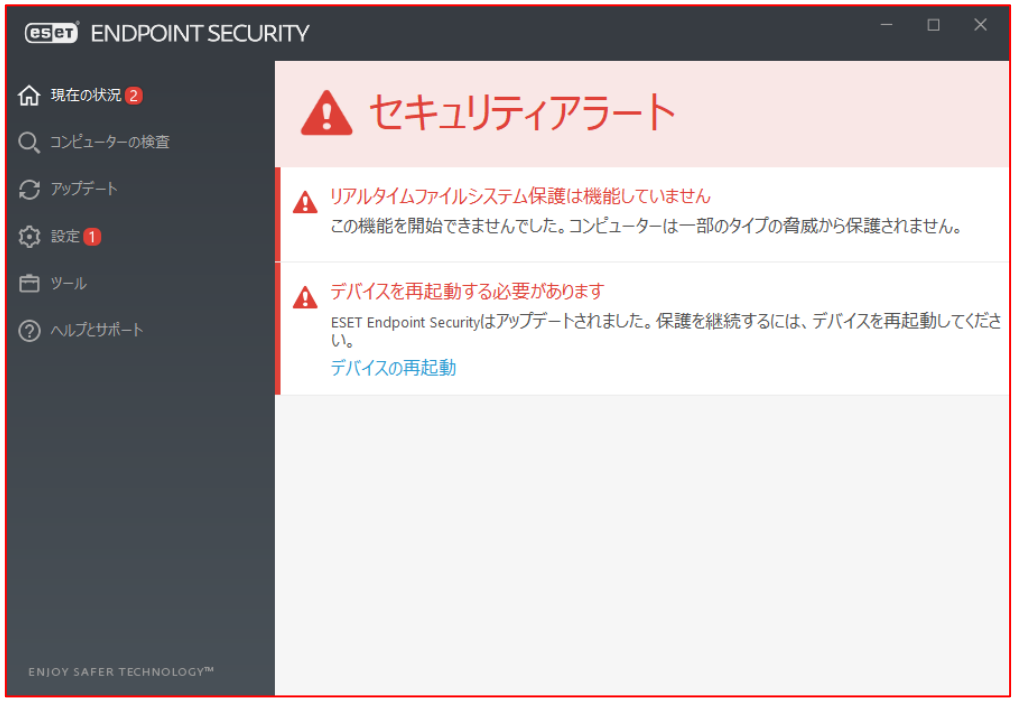
＜b-2＞で各クライアント端末に配布したフォルダ内のバッチファイルを使用して、クライアント用プログラムのバージョンアップを行います。

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【STEP5】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。

10. パターン B：Web サーバーを使用して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。

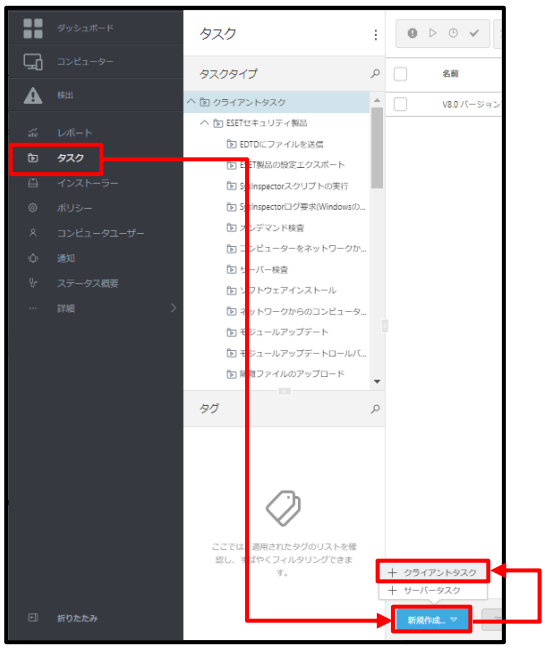
a. EM エージェントのバージョンアップ

クライアント端末の EM エージェント V7.X を V8.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

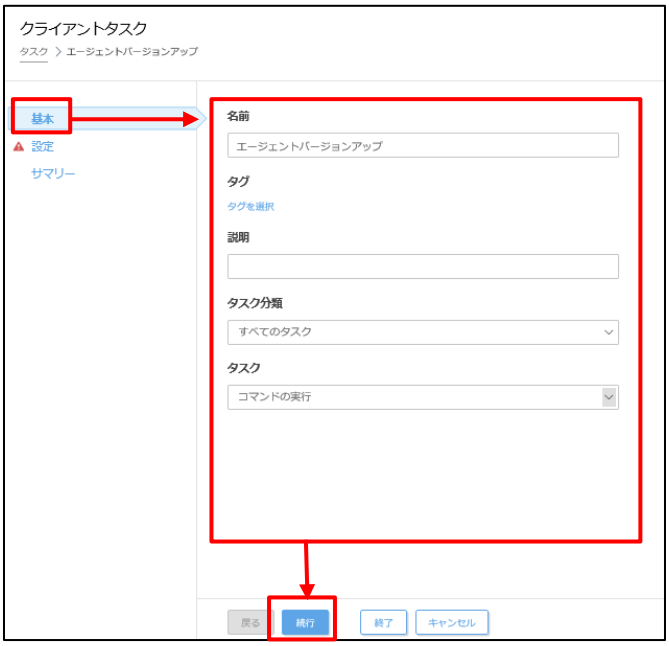
1. EP Web コンソール を起動して、ESET PROTECT に接続します。
   ユーザー名とパスワードを入力し、[ログイン]ボタンをクリックします。
   ※ EP Web コンソールには以下の URL よりアクセスできます。
   https:// <管理サーバーのサーバー名、または、IP アドレス> /era

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

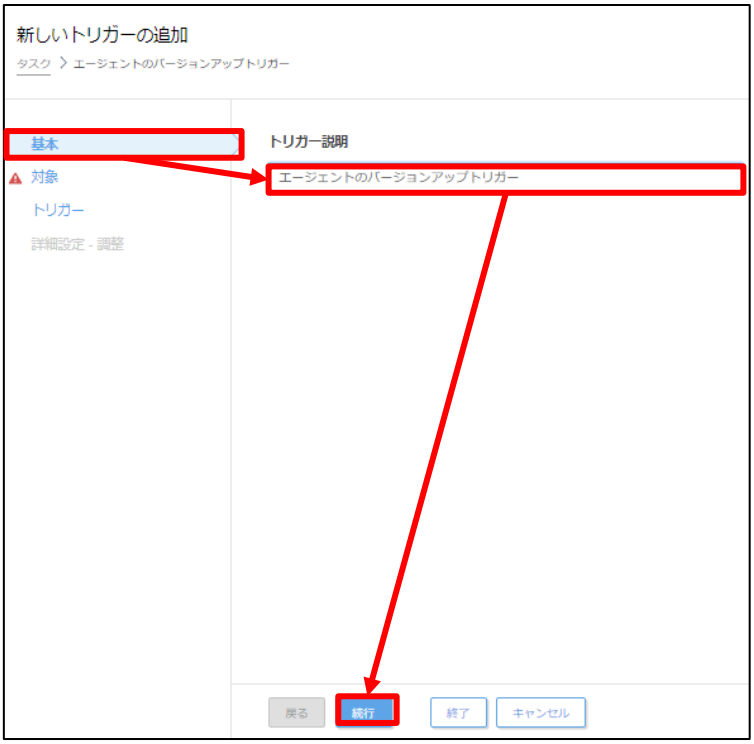


4. 「実行するコマンドライン」に以下のコマンドを入力し、[終了]ボタンをクリックします。

```
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')}"
```

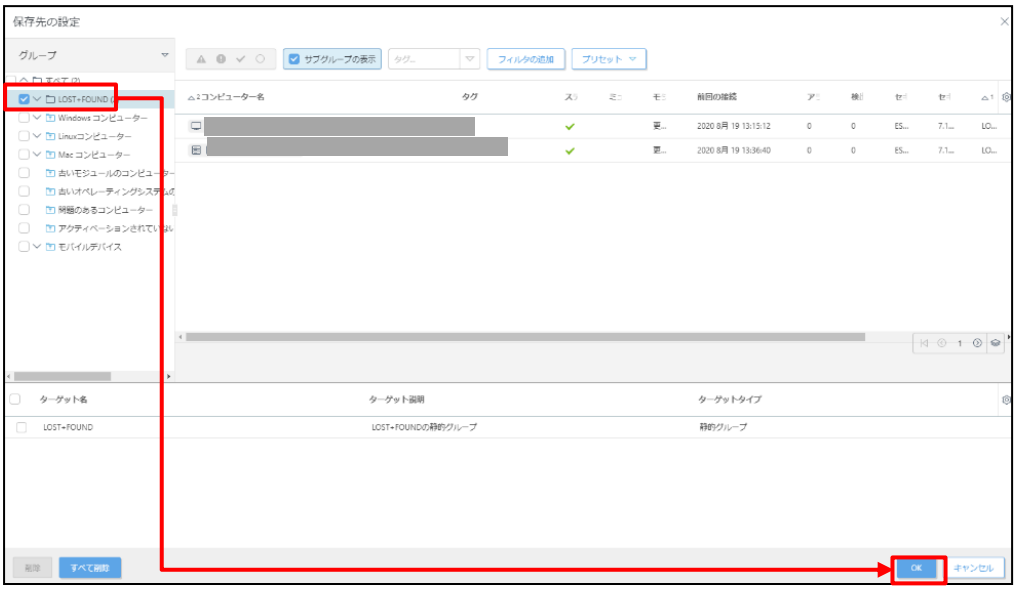
5. 以下の画面が表示されたら、[トリガーの作成]ボタンをクリックします。

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。

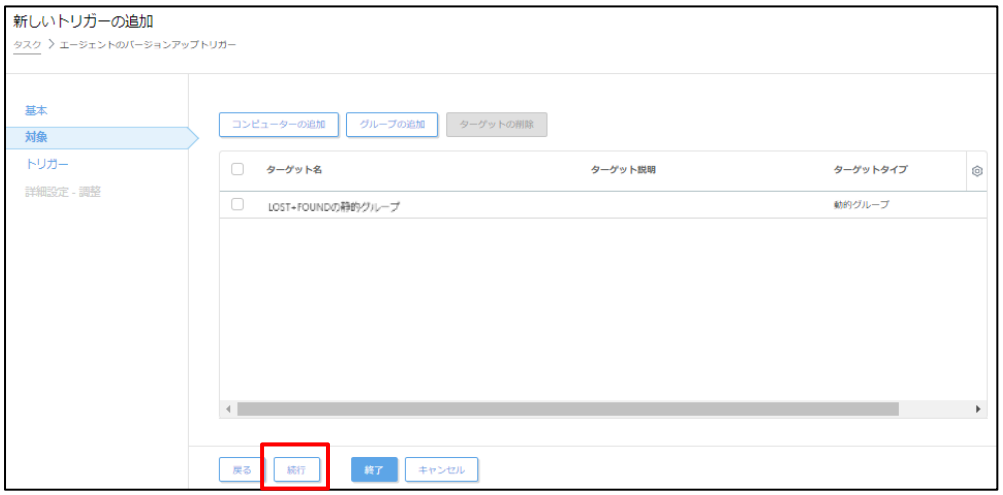


7. 「対象」を展開し、[ターゲットの追加]、[コンピューターの追加]、または[グループの追加]ボタンをクリックします。
※本手順では「ターゲットの追加」を選択します。

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 V8.X と EEA V8.X の動作要件を確認します。

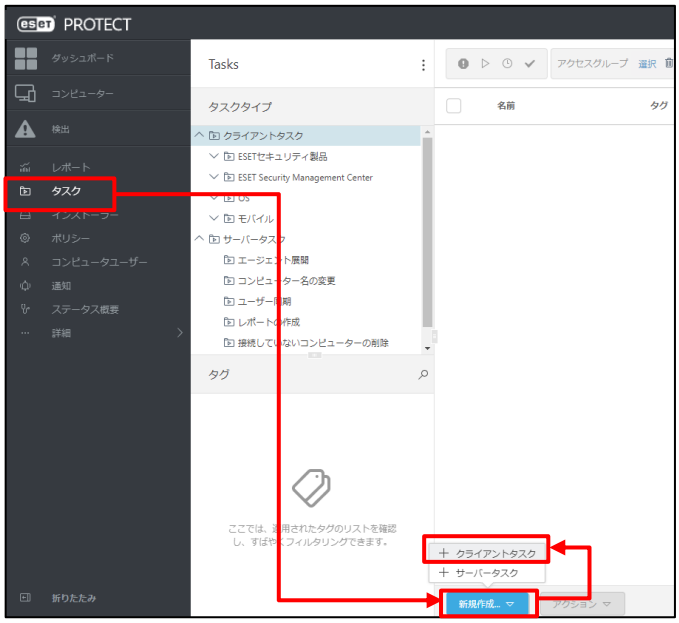
＜ESET Endpoint Security / ESET Endpoint アンチウイルス 動作要件＞

・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。

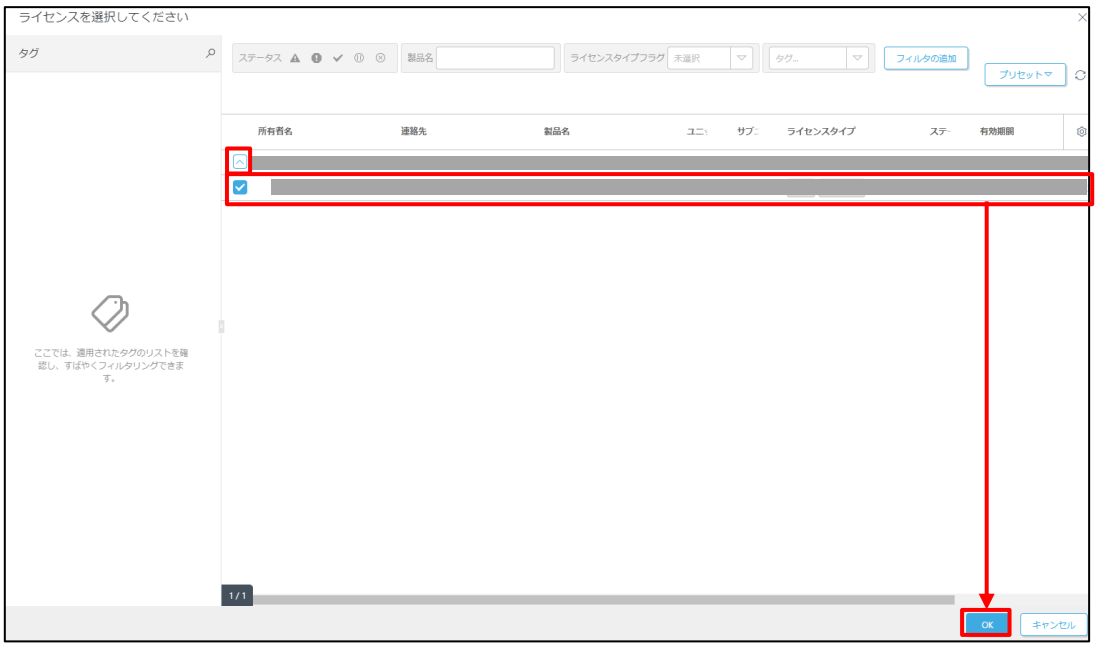


2. [基本]を展開し、以下の通り設定します。

名前	任意の名前(例：V8.1 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。

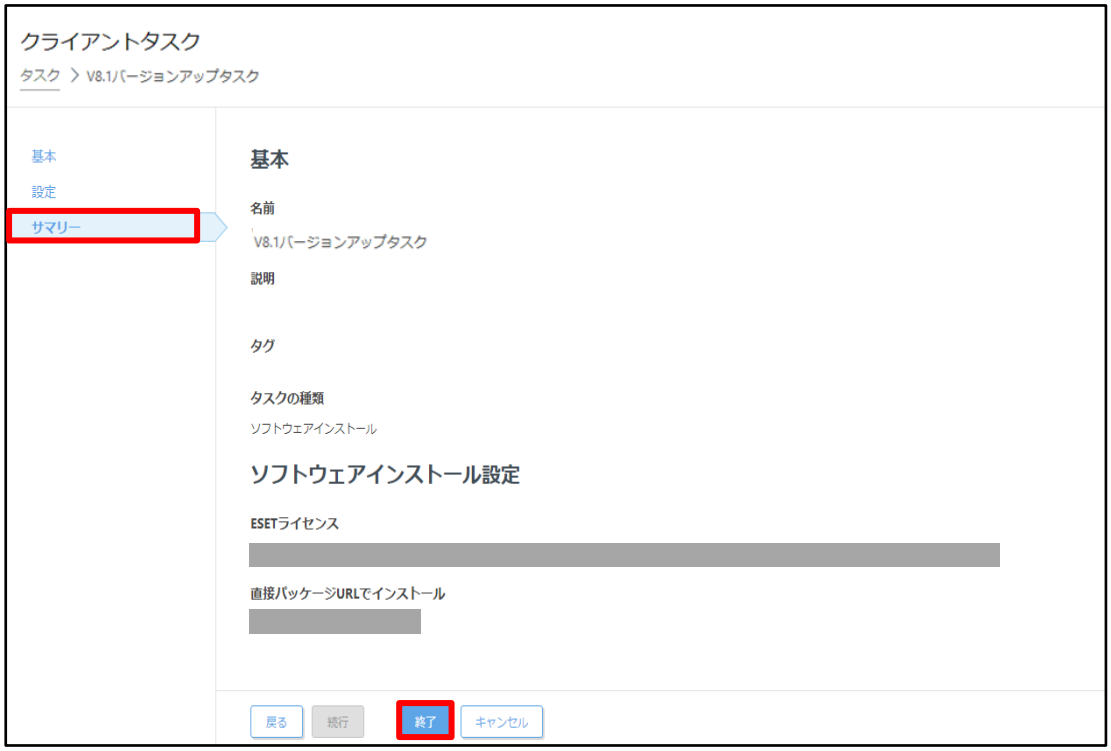
(例)http://192.168.XXX.XXX/ees_nt64.msi
http://Web サーバーの IP アドレス/インストーラーのパス

<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 File 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。

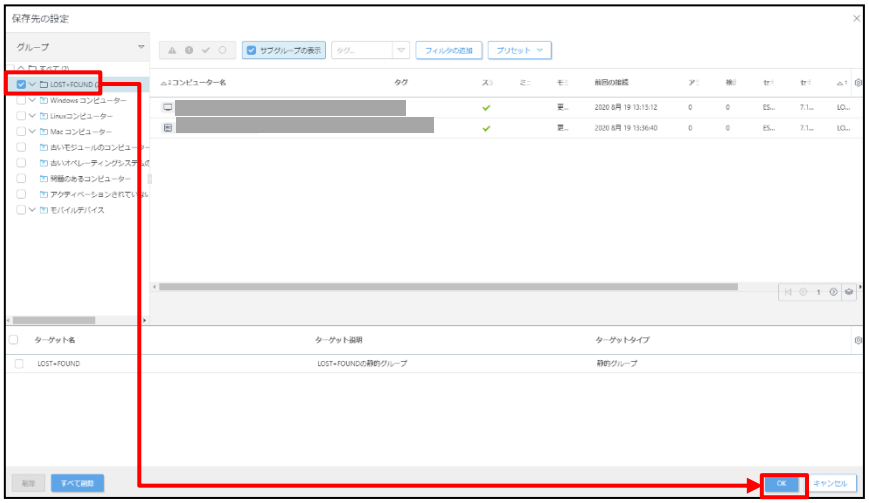


8. 以下の画面が表示されたら、[トリガーの作成]ボタンをクリックします。

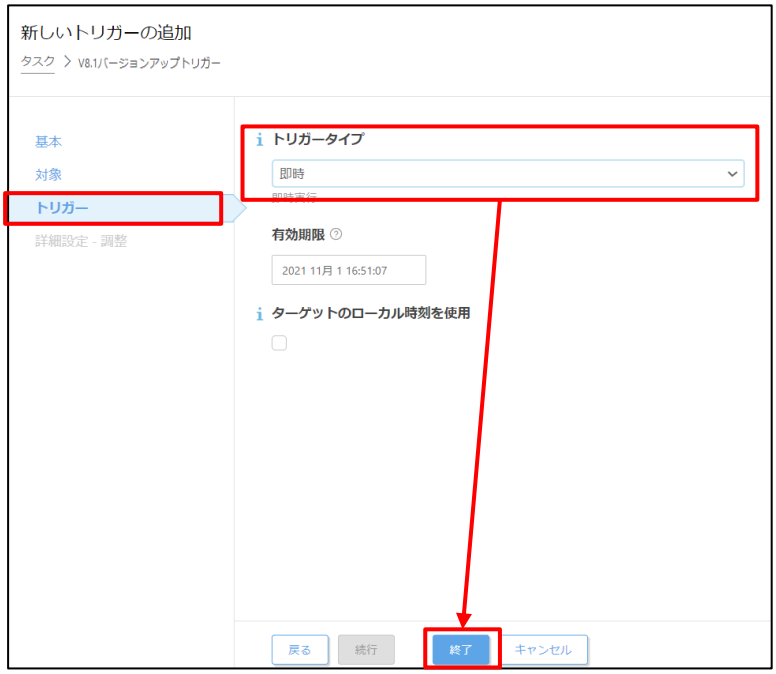
9. 「基本」を展開し、任意のトリガーの説明(例：V8.1 バージョンアップトリガー)を入力します。

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 B：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【STEP5】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。

11.　パターン C：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

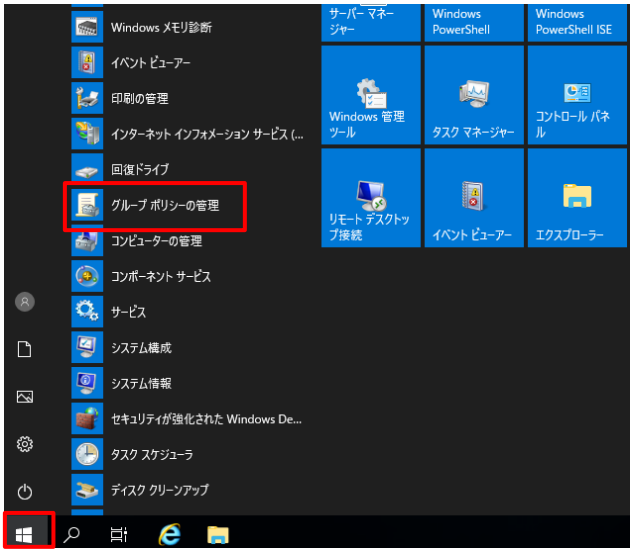
GPO を使用してバージョンアップを行う場合は、EM エージェントとクライアント用プログラムを同時にバージョンアップします。

a-1.　動作要件の確認

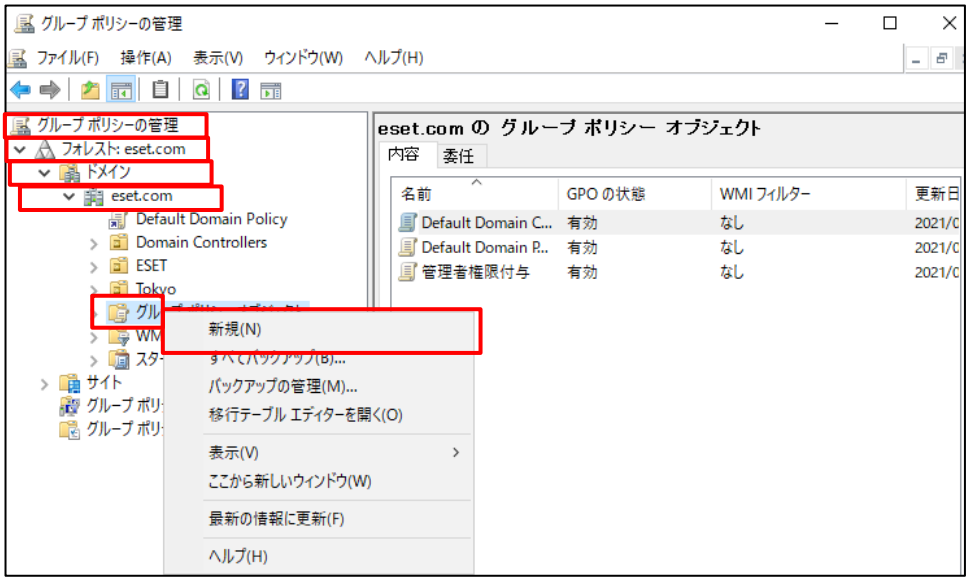
バージョンアップの前に、EES V8.X と EEA V8.X の動作要件を確認します。
＜ESET Endpoint Security　/ ESET Endpoint アンチウイルス 動作要件＞
・ESET PROTECT Entry オンプレミス(旧名称：ESET Endpoint Protection Advanced)をご利用のお客さま
https://eset-info.canon-its.jp/business/ep-entry-o/spec.html
・ESET PROTECT Essential オンプレミス(旧名称：ESET Endpoint Protection Standard)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～

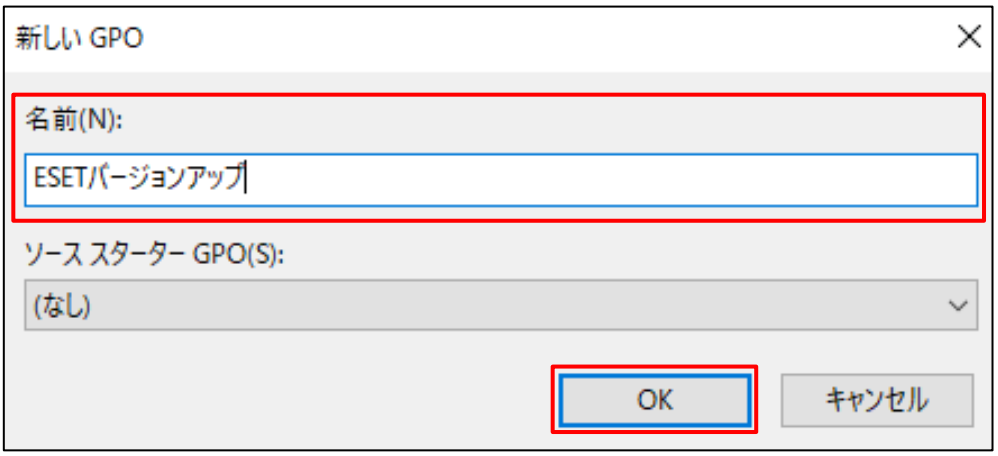
クライアント用プログラムのバージョンアップを行うための GPO を作成します。
1.　スタートボタンをクリックし、「Windows 管理ツール」より「グループポリシーの管理」を起動します。



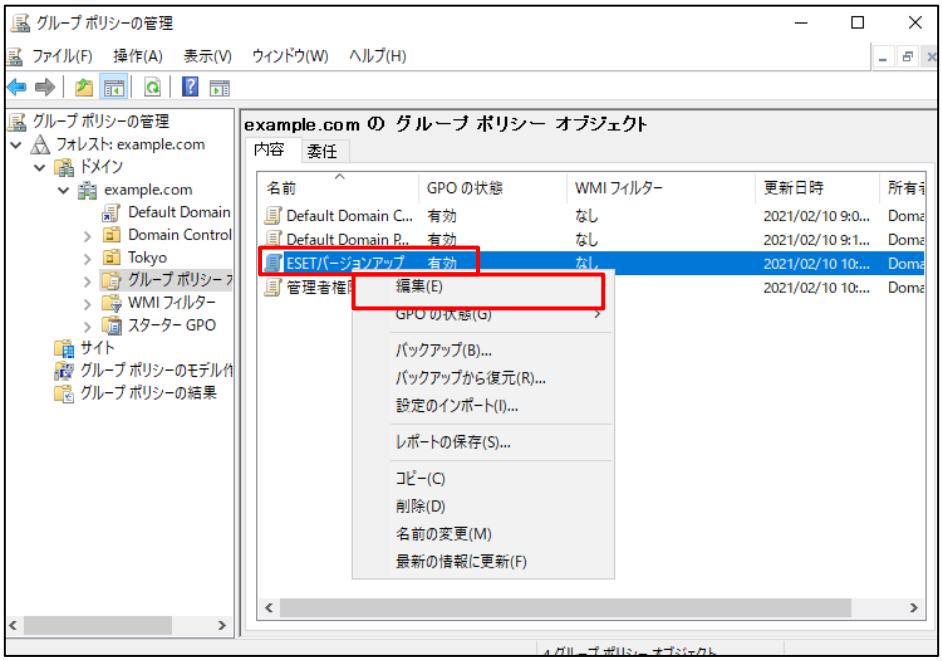
2. 「グループポリシーの管理」が起動したら、[グループポリシーの管理]-[フォレスト]-[ドメイン]-[任意のドメイン名]と展開して「グループポリシーオブジェクト」を右クリックし、[新規]をクリックします。



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。

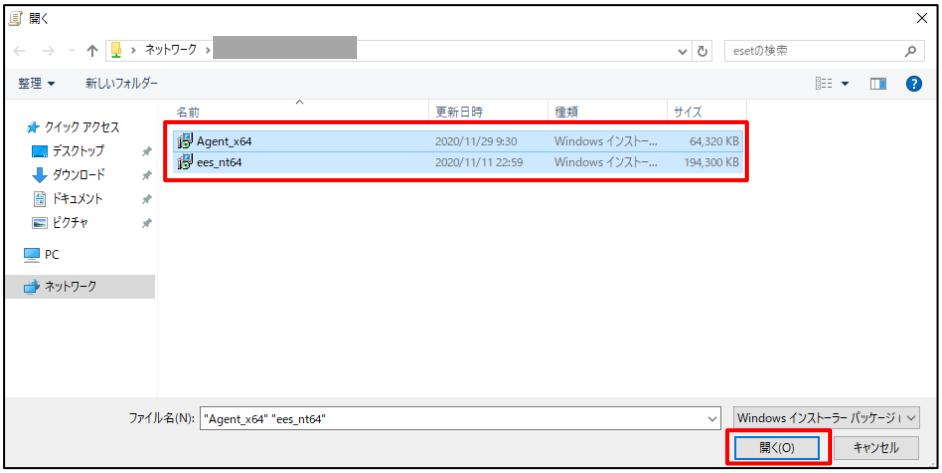


4. 新しく作成したグループポリシーオブジェクトを右クリックし、[編集]をクリックします。

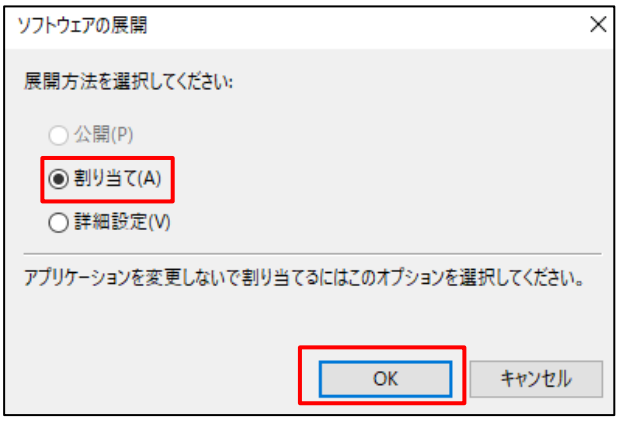


5. 「グループポリシー管理エディター」が起動したら、[コンピューターの構成]-[ポリシー]-[ソフトウェアの設定]と展開し、[ソフトウェアのインストール]を右クリックして[新規作成]-[パッケージ]をクリックします。

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。

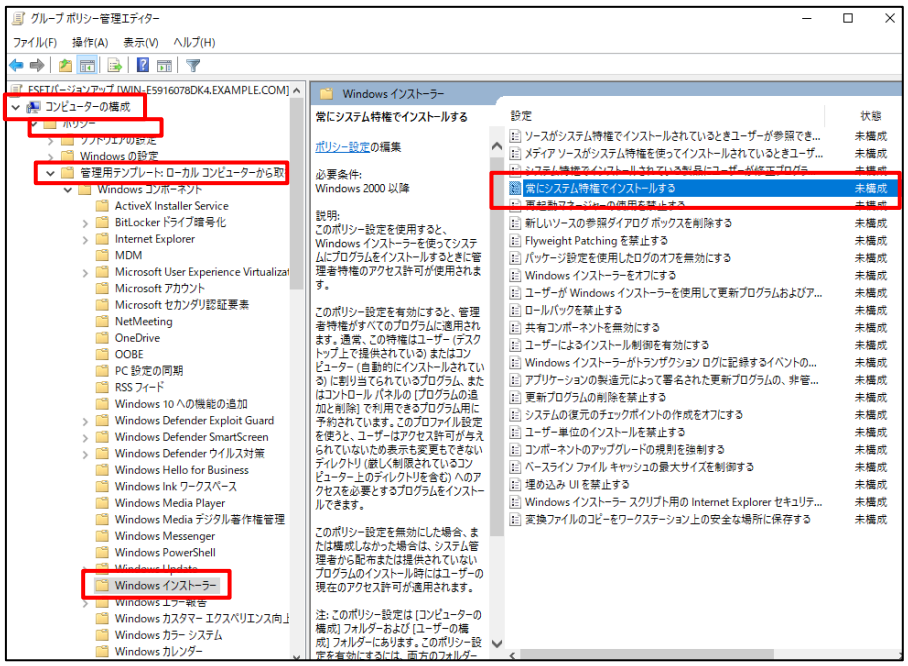


7. 「ソフトウェアの展開」画面が表示されたら、「割り当て」にチェックを入れ、[OK]ボタンをクリックします。
※本画面は 2 回表示されます。2 回とも「割り当て」にチェックを入れてください。

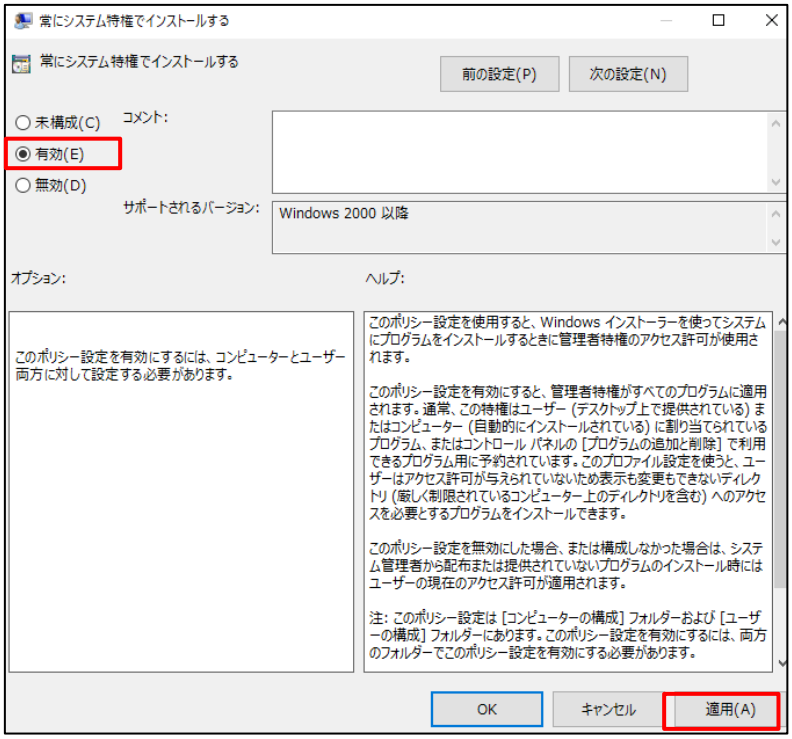


8. 手順 6 で選択したインストーラーが表示されたことを確認します。

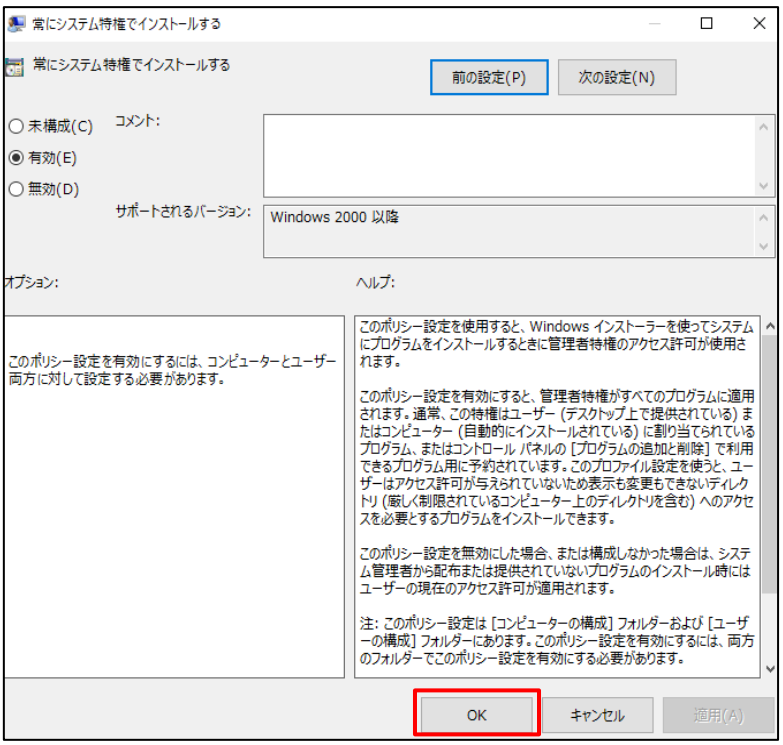
9. [コンピューターの構成]-[ポリシー]-[管理用テンプレート]-[Windows コンポーネント]-[Windows インストーラー]を展開し、画面右側の「常にシステム特権でインストールする」をダブルクリックします。



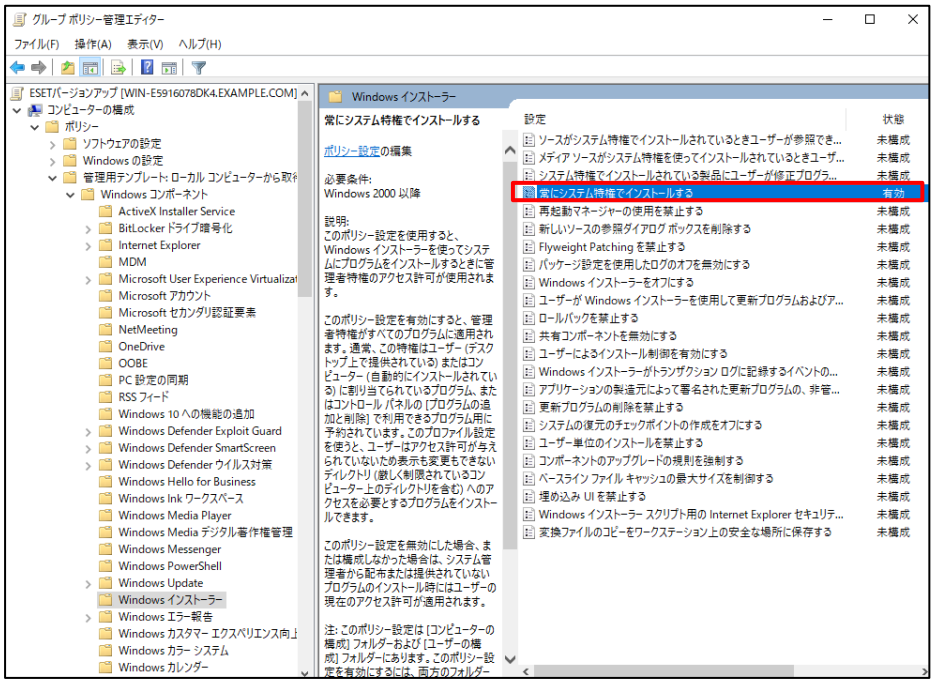
10. 「有効」にチェックを入れ、[適用]ボタンをクリックします。



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。

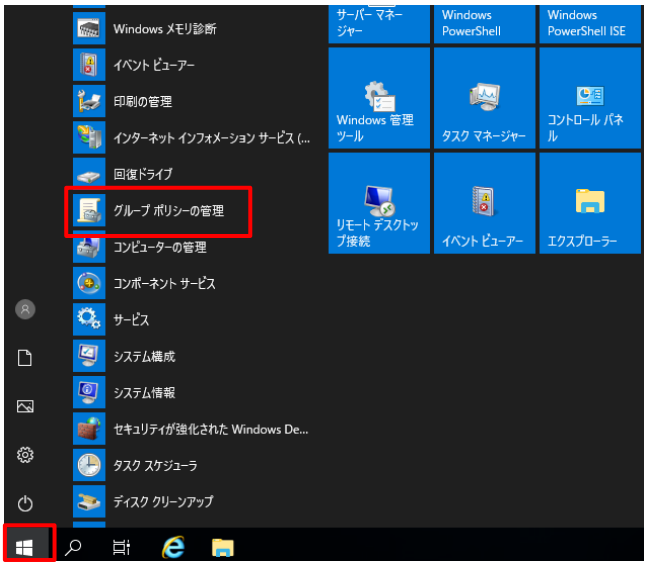


以上で、クライアント用プログラムと EM エージェントのバージョンアップ用の GPO の作成は終了です。

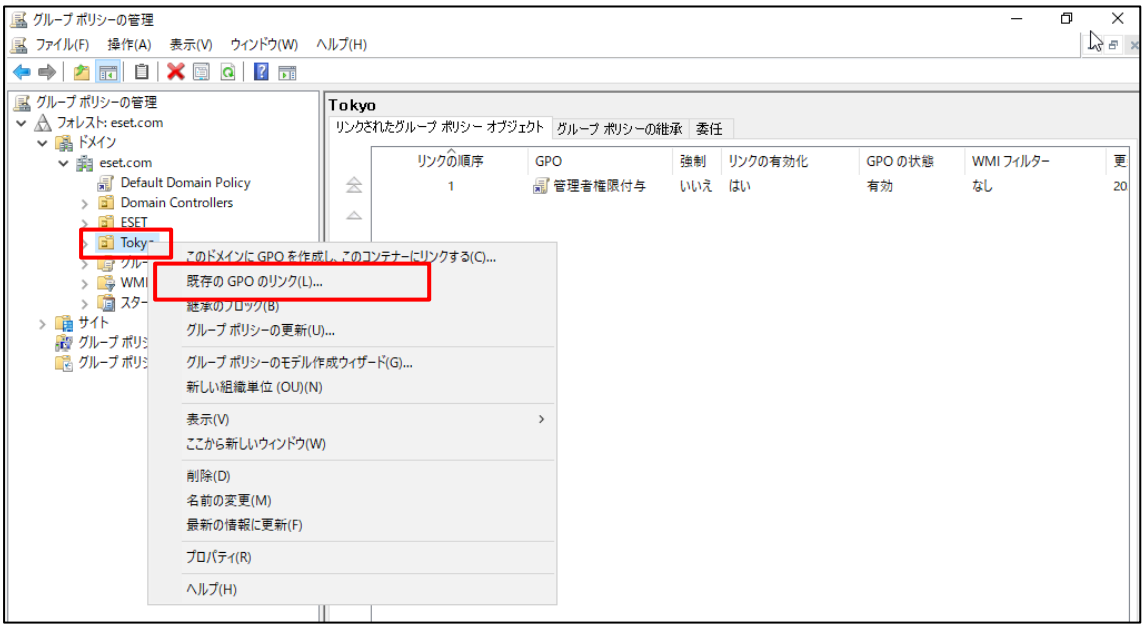
a-2-2. 各プログラムのバージョンアップ準備　～GPO の配布～

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。

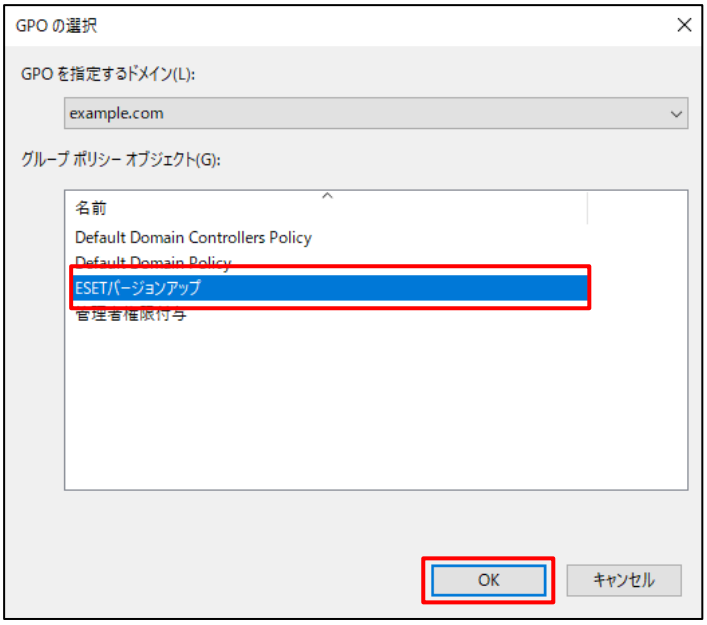
1. スタートボタンをクリックし、「Windows 管理ツール」より「グループポリシーの管理」を起動します。



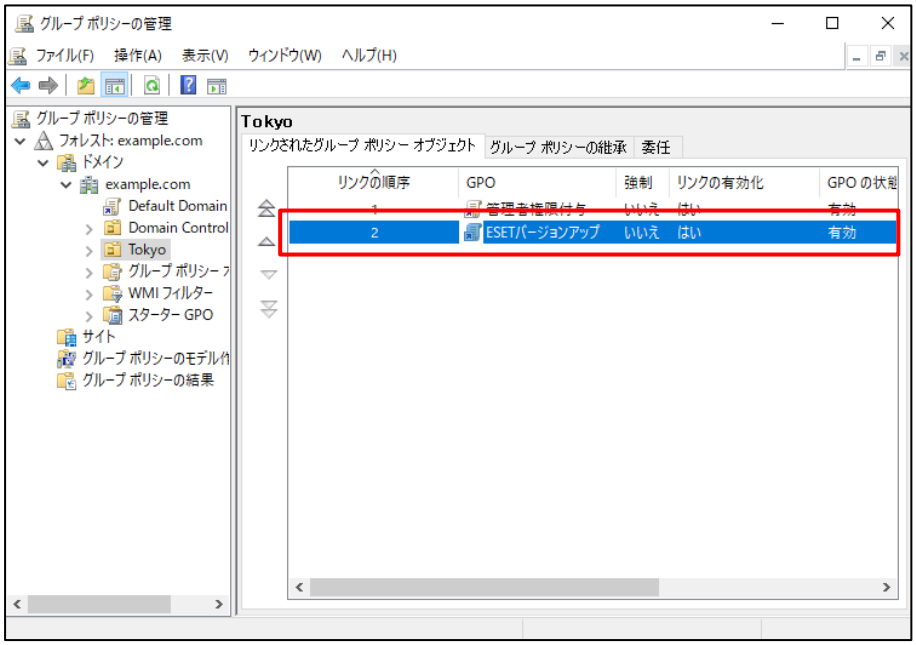
2. 「グループポリシーの管理」が起動したら、クライアント端末が所属している OU を右クリックし、「既存の GPO のリンク」をクリックします。



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。

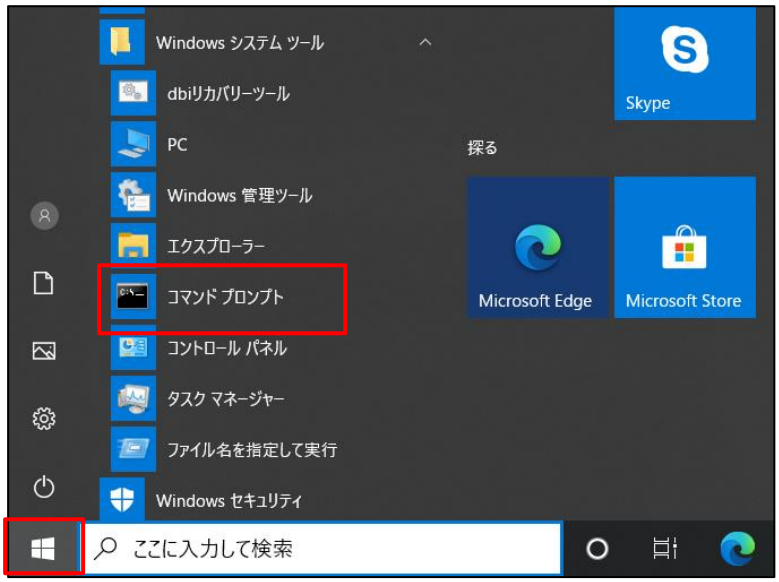
a-3. EM エージェントとクライアント用プログラムのバージョンアップ

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。
【STEP5】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。

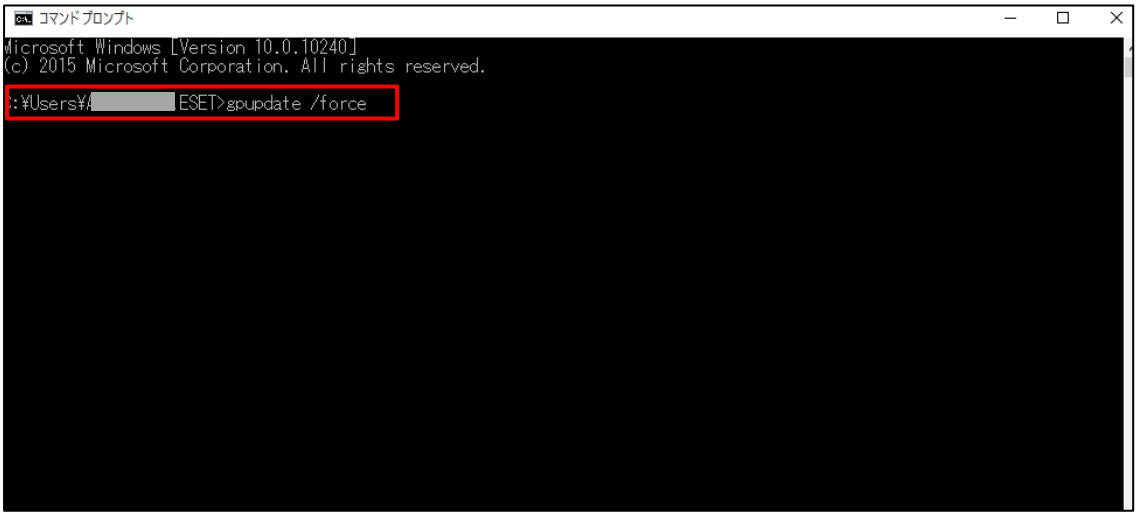
※次回起動時以降にバージョンアップが行われない場合は、クライアント端末で以下の操作を行ってください。

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。

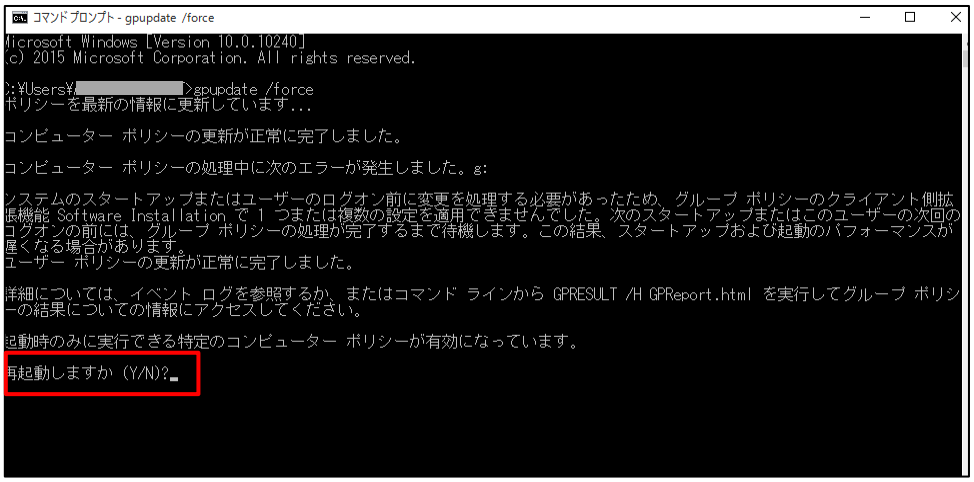


2. 「コマンドプロンプト」が起動したら、以下のコマンドを実行します。

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。

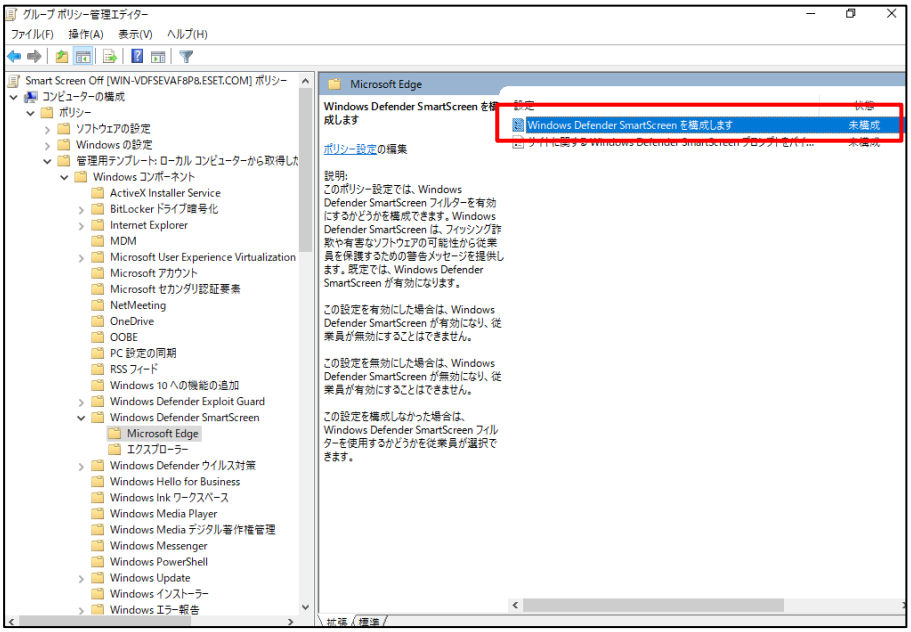


4. 再起動後、バージョンアップが行われたことを確認します。

<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。

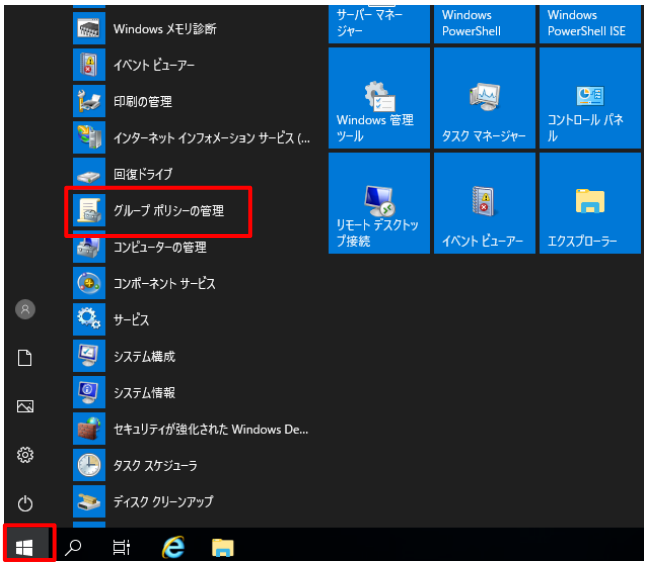
※[グループポリシー管理エディター]で[コンピューターの構成]-[ポリシー]-[管理用テンプレート]-[Windows コンポーネント]-[Windows Defender SmartScreen]-[Microsoft Edge]を展開し、「Windows Defender SmartScreen を構成します」をダブルクリックして設定を行います。



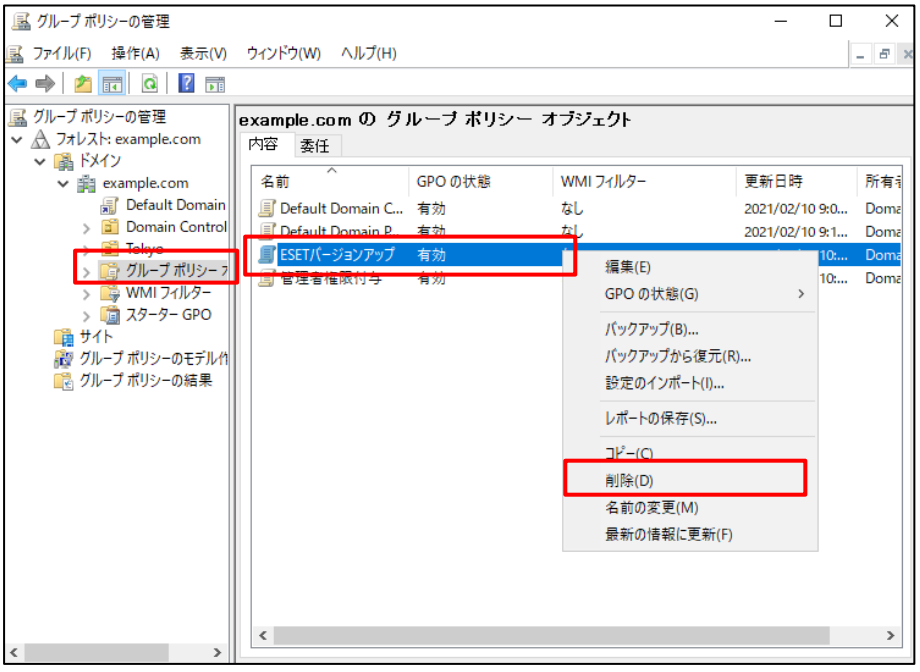
※以下の＜a-4＞は、【STEP5】でバージョンアップ完了が確認できた後に実施してください。

a-4. 配布した GPO の割り当て解除

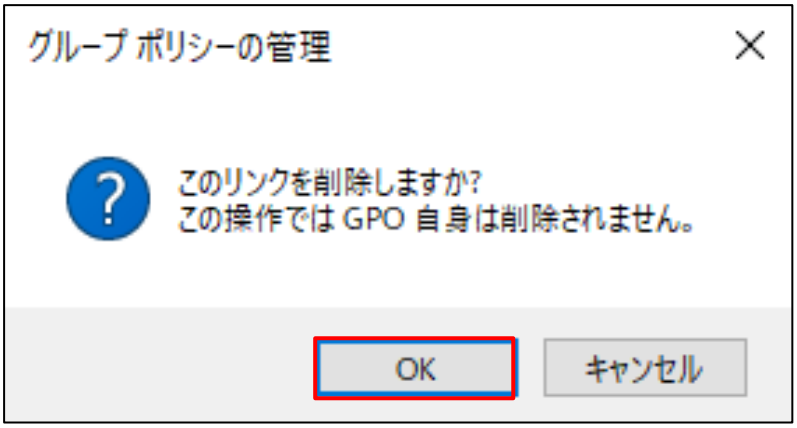
1. スタートボタンをクリックし、「Windows 管理ツール」より「グループポリシーの管理」を起動します。



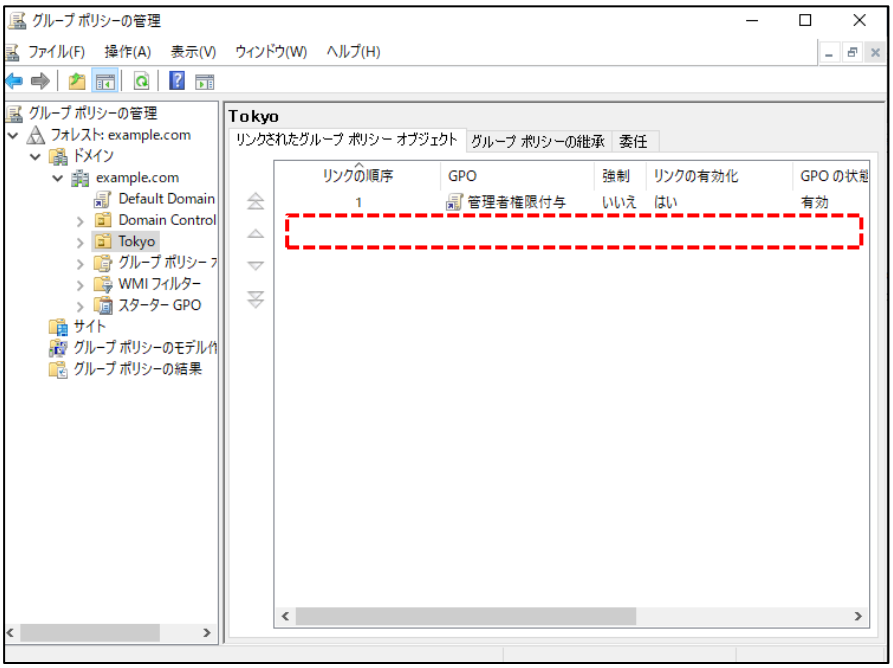
2. 「グループポリシーの管理」が起動したら、クライアント端末が所属している OU を選択し、クライアント用プログラムのバージョンアップ用に割り当てた GPO を右クリックして[削除]をクリックします。



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。



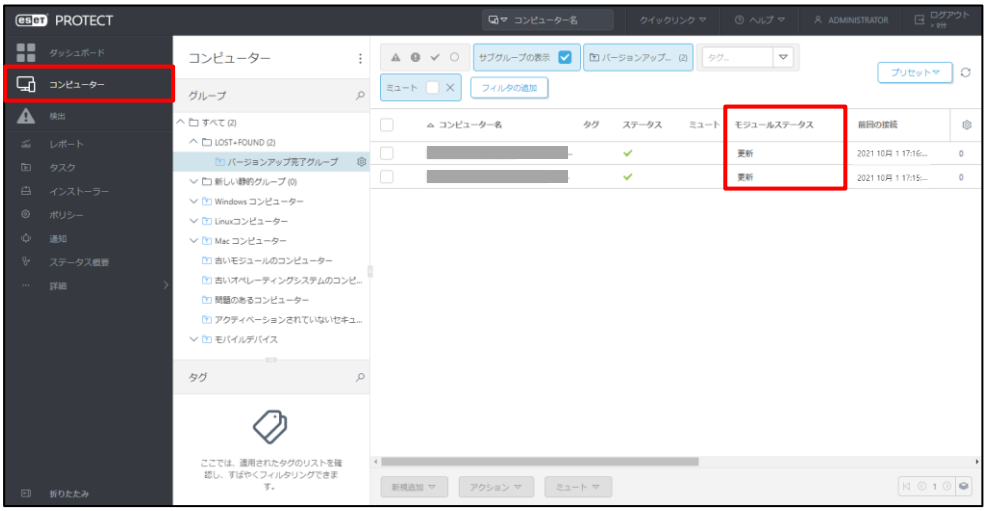
以上で、GPO の割り当て解除は完了です。

以上で、【パターン C：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。

12. 【STEP5】 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、【STEP3】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「8.X」以上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。