ESET PROTECT ソリューション

データベースを移行しないサーバーのリプレイスに伴う ESET PROTECT on-prem V11.1 の移行手順

(サーバーの IP アドレスやコンピューター名を変更する場合)

第 2 版

2024 年 7 月 31 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. 新サーバーへの EP on-prem 移行フロー 5

4. 作業をはじめる前に 6

5. ［STEP1］ 新サーバーにて ESSW のインストール 7

6. ［STEP2］ 新サーバーにてミラーサーバーの構築 13

7. ［STEP3］ 新サーバーにて EP on-prem のインストールとセットアップ 16

8. ［STEP4］ 旧サーバーにてクライアントの接続先変更 35

9. ［STEP5］ 新サーバーにてリプレイス完了の確認 48

1. はじめに

○ 本資料は、ESET PROTECT ソリューションをご利用中のお客さまがサーバーのリプレイス時にデータベースを移行せずに ESET PROTECT on-prem V11.1 のリプレイスを行う際、必要となる作業や注意事項について記載しております。

○ オンプレミス型セキュリティ管理ツールの名称が V11.0 より ESET PROTECT on-prem になりました。
※V10.1 以下のオンプレミス型セキュリティ管理ツールの名称は ESET PROTECT です。

○ 本資料は、本資料作成時のソフトウェア、並びに、ハードウェアの情報に基づき作成されております。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搭載されている機能、及び、名称が異なっている場合がございます。また本資料の内容は、将来予告なく変更を行うことがございます。

○ 本資料の画面イメージは、Windows Server 2016、及び、Windows Server 2019 をベースに作成しております。そのため、OS によっては記載内容と名称が異なっている場合がございます。

○ 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問わず、禁じます。

○ Microsoft, Windows, Windows Server は、米国 Microsoft Corporation の米国及びその他の国における商標または、登録商標です。ESET、ESET Endpoint Security, ESET PROTECT on-prem はスロバキア共和国 ESET,LLC ならびに ESET,spol. s r. o.に帰属します。本資料の著作権は、キヤノンマーケティングジャパン株式会社に帰属します。その他の製品名及び社名などは、各社の商標または登録商標です。

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、**データベースを移行しない場合**のサーバーリプレイス時に ESET PROTECT on-prem V11.1 を移行するためのフローや注意点を記載しております。

移行前

		旧サーバー
全体構成		・一台のサーバーで管理とミラーを運用 ・専用サーバーで運用 ・Apache HTTP プロキシの利用なし ・モバイル管理なし ・オンライン環境
OS		・Windows Server 2016
ESET 製品	オンプレミス型セキュリティ管理ツール	・ESET PROTECT on-prem V11.1.0.15.0 (略称 EP on-prem)
	ウイルス・スパイウェア対策	・ESET Server Security for Microsoft Windows Server V11.0.12011.1 (略称 ESSW)
	ミラー	・2022 年 1 月 27 日公開のミラーツール
利用データベース		・Microsoft SQL Server 2019 Express Edition (略称 MSSQL)

移行後

		新サーバー
全体構成		・一台のサーバーで管理とミラーを運用 ・専用サーバーで運用 ・Apache HTTP プロキシの利用なし ・モバイル管理なし ・オンライン環境 ・旧サーバーと異なる IP アドレスとコンピューター名
OS		・Windows Server 2019
ESET 製品	オンプレミス型セキュリティ管理ツール	・ESET PROTECT on-prem V 11.1.15.0 (略称 EP on-prem)※
	ウイルス・スパイウェア対策	・ESET Server Security for Microsoft Windows Server V11.0.12011.1 (略称 ESSW)
	ミラー	・2022 年 5 月 31 日公開のミラーツール
利用データベース		・Microsoft SQL Server 2019 Express Edition **(新規インストール)**

※移行前と移行後の ESET PROTECT on-prem は完全に同一のバージョンである必要があります。
※データベースの移行を行わないため、グループ情報は移行できません。リプレイス後、再度クライアント端末のグルーピングをお願いします。(リプレイス後、クライアントは静的グループ[LOST+FOUND]に所属します。)

3. 新サーバーへの EP on-prem 移行フロー

サーバーリプレイスに伴う、EP on-prem と ESSW の移行に必要なステップは以下の通りです。

作業をはじめる前に

- 事前準備

↓

［STEP1］ 新サーバーにて ESSW のインストール

STEP1-1. ESSW のインストール

↓

［STEP2］ 新サーバーにてミラーサーバーの構築

STEP2-1. ミラーサーバーの構築

↓

［STEP3］ 新サーバーにて EP on-prem のインストールとセットアップ

STEP3-1. EP on-prem のインストール

STEP3-2. クライアントのアップデート先変更ポリシーの作成

STEP3-3. EM エージェントの証明書と認証局のエクスポート

↓

［STEP4］旧サーバーにてクライアントの接続先変更

STEP4-1. 旧 EP on-prem サーバーへ認証局のインポート

STEP4-2. EM エージェントの接続先変更

↓

［STEP5］ 新サーバーにてリプレイス完了の確認

STEP5-1. クライアントのアップデート状況と EP on-prem への接続確認

＜参考＞

インターネットから直接検出エンジンのアップデートを行っている場合は、【STEP2-1. ミラーサーバーの構築】、【STEP3-2. クライアントのアップデート先変更ポリシーの作成】は必要ありません。
また、【STEP5-1. クライアントのアップデート状況と EP on-prem への接続確認】の手順 4、および手順 5 もご確認いただく必要はありません。

4. 作業をはじめる前に

事前準備

移行作業を始める前に、以下について事前にご用意いただきますようお願いいたします。

以下のプログラムは**新サーバー**で使用します。ユーザーズサイトより、ダウンロードをお願いいたします。(インストールは手順書内で行います。)
[ユーザーズサイト]
URL：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。

・ESSW のインストーラー
※ユーザーズサイトで[プログラム/マニュアル]-[クライアント用プログラム]-[基本的な/総合的なエンドポイント保護]-[Windows Server 向けプログラム]と進むとインストーラーがございます。

・EP on-prem のオールインワンインストーラー
※ユーザーズサイトで[プログラム/マニュアル]-[オンプレミス型セキュリティ管理ツール（ESET PROTECT on-prem）]-[ESET PROTECT on-prem]と進むとインストーラーがございます。

・2022 年 5 月 31 日公開のミラーツール
※ユーザーズサイトで[プログラム/マニュアル]-[クライアント用プログラム]-[基本的な/総合的なエンドポイント保護]-[オプション（各種ツール）]-[ミラーツール]-[Windows Server 向けミラーツール]と進むとございます。

また、ESSW のアクティベーション時に使用する以下の情報をご確認ください。
・「製品認証キー」を使用する場合
本資料では製品認証キーを使用したアクティベーション方法でご案内しております
※ユーザーズサイトの[ライセンス情報/申込書作成]-[アクティベーション情報(プログラムの利用に必要な情報)]にある[製品認証キー]をお控えいただきますようお願いいたします。

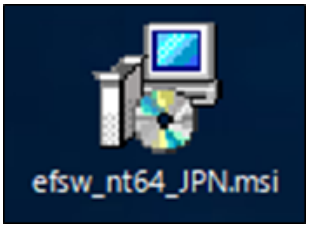
・「ESET Business Account」、「ESET PROTECT HUB」を使用する場合
上記を利用したアクティベーション方法は下記よりご確認ください。
◇クライアント用プログラムの製品のアクティベーションをおこなうには？
https://eset-support.canon-its.jp/faq/show/48?site_domain=business
※詳細や開設方法につきましては下記サポートサイトをご参照ください。
◇ ESET Business Account について
https://eset-support.canon-its.jp/faq/show/19554?site_domain=business
◇ESET PROTECT HUB について
https://eset-support.canon-its.jp/faq/show/29662?site_domain=business

5. ［STEP1］ 新サーバーにて ESSW のインストール

新サーバーに ESSW をインストールします。
※旧サーバーの ESSW で設定しているミラー機能以外の設定については新サーバーで再度設定してください。なお、旧サーバーの設定を読み込ませながらインストールを行う、設定読み込み型インストールもございます。詳細は以下の Web ページをご参照ください。
URL：https://eset-support.canon-its.jp/faq/show/20?site_domain=business

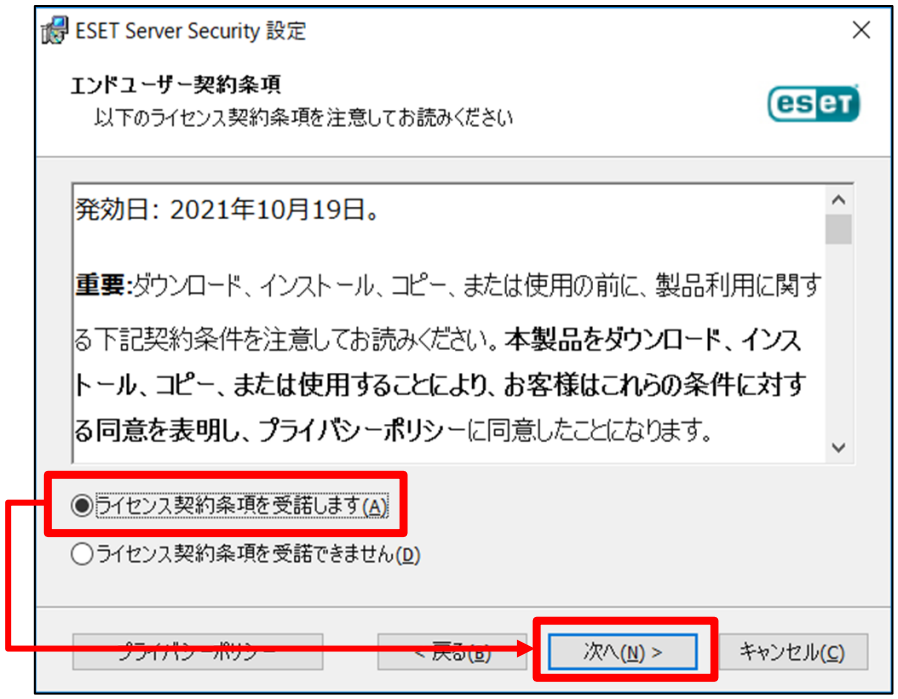
STEP1-1. ESSW のインストール

1. 事前準備で用意した ESSW のインストーラー[efsw_nt64_JPN.msi]をダブルクリックします。

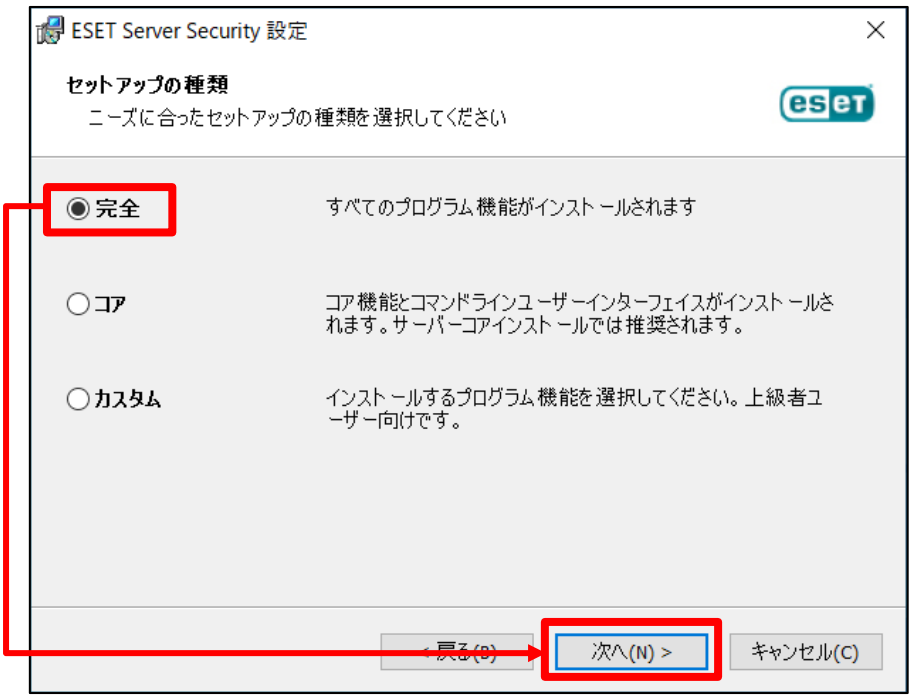


2. ESET Server Security セットアップウィザードが表示されましたら、[次へ]をクリックします。

3. エンドユーザー契約条項を受諾し、[次へ]をクリックします。

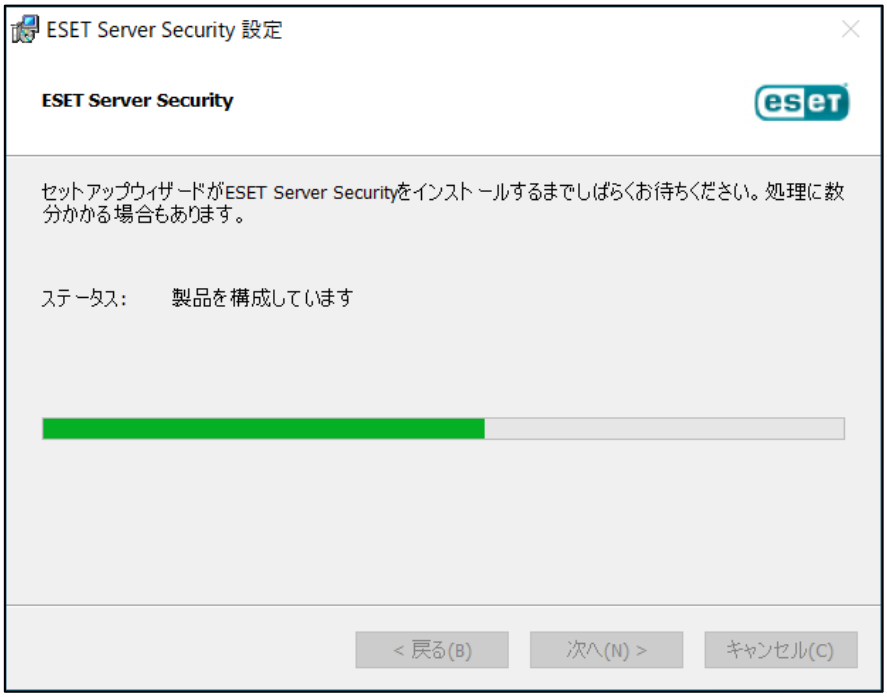


4. [完全]を選択し、[次へ]をクリックします。



5. インストールするフォルダを選択し、[インストール]をクリックします。
※既定では下の画像の赤枠のフォルダにそれぞれインストールされます。

6. インストールが開始されます。

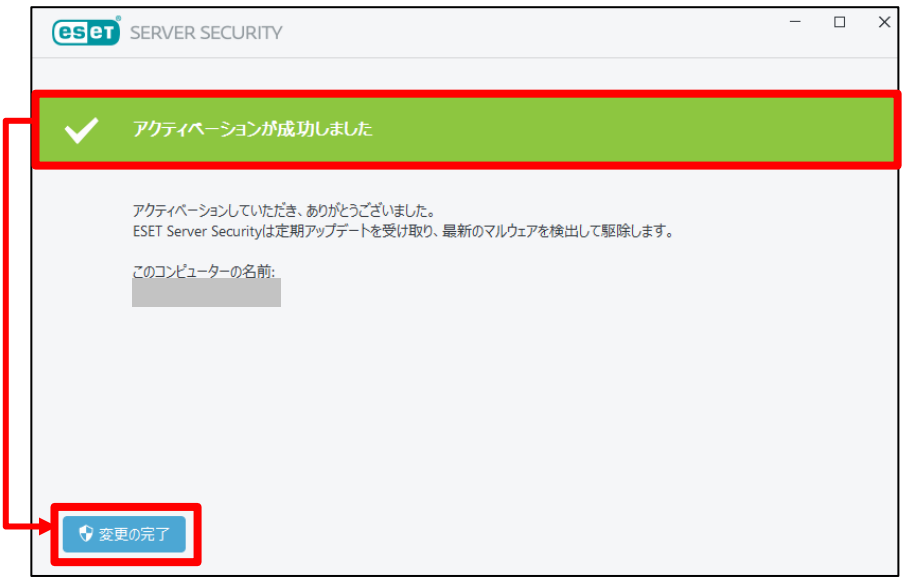


7. [ESET Server Security セットアップウィザードを完了しています]と表示されましたら、[完了]をクリックします。

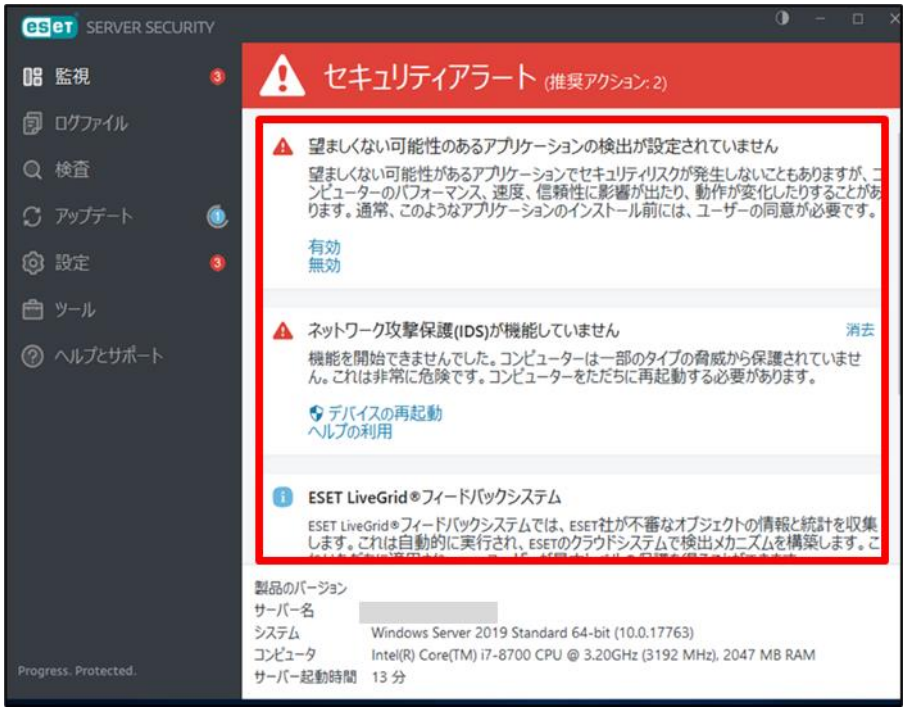
8. 以下の画面が表示されましたら、アクティベーション方法を選択します。
本手順では、[購入した製品認証キーを使用]をクリックしてアクティベーションをおこないます。
※その他のアクティベーション方法については P7 の事前準備をご確認ください。

9. 製品のアクティベーション画面が表示されますので、製品認証キーを入力して、[続行]をクリックします。
※製品認証キーについては、P7 の事前準備をご確認ください。

10. [アクティベーションが成功しました]と表示されましたら、[完了]をクリックします。



11. 以下のような画面が表示されましたら、お客様のご利用条件に合わせて、不審なアプリケーションの検出有無、ESET LiveGrid®フィードバックシステム参加有無を選択し、それぞれ[OK]をクリックします。



以上で、ESSW のインストールは終了です。

6. ［STEP2］ 新サーバーにてミラーサーバーの構築

STEP2-1. ミラーサーバーの構築

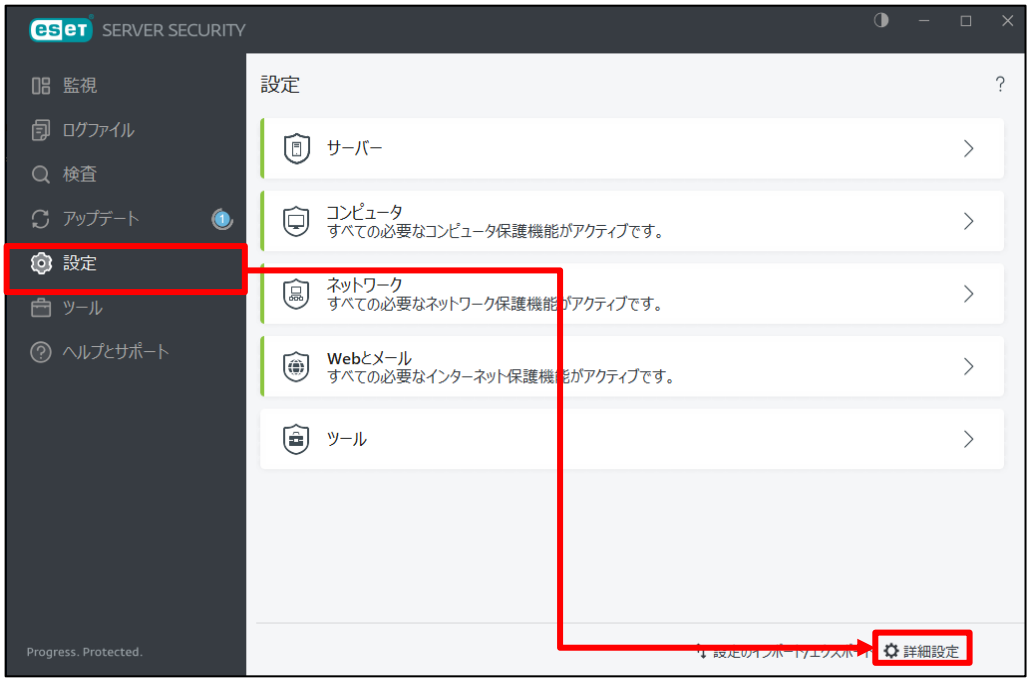
1. 以下のサポート情報を確認し、ミラーツールを使用してミラーサーバーを構築してください。

   ■Windows Server 環境でミラーツールを使用してミラーサーバーを構築するには？
   https://eset-support.canon-its.jp/faq/show/4341?site_domain=business

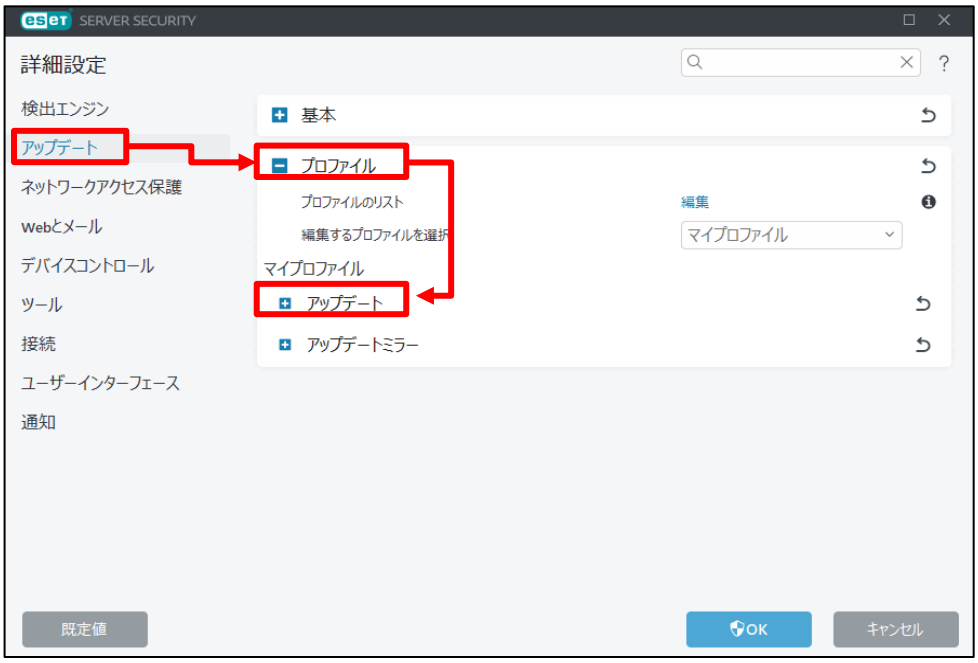
   ■IIS を利用して検出エンジンを公開する手順
   https://eset-support.canon-its.jp/faq/show/9499?site_domain=business

2. ESSW のアップデート先を設定します。

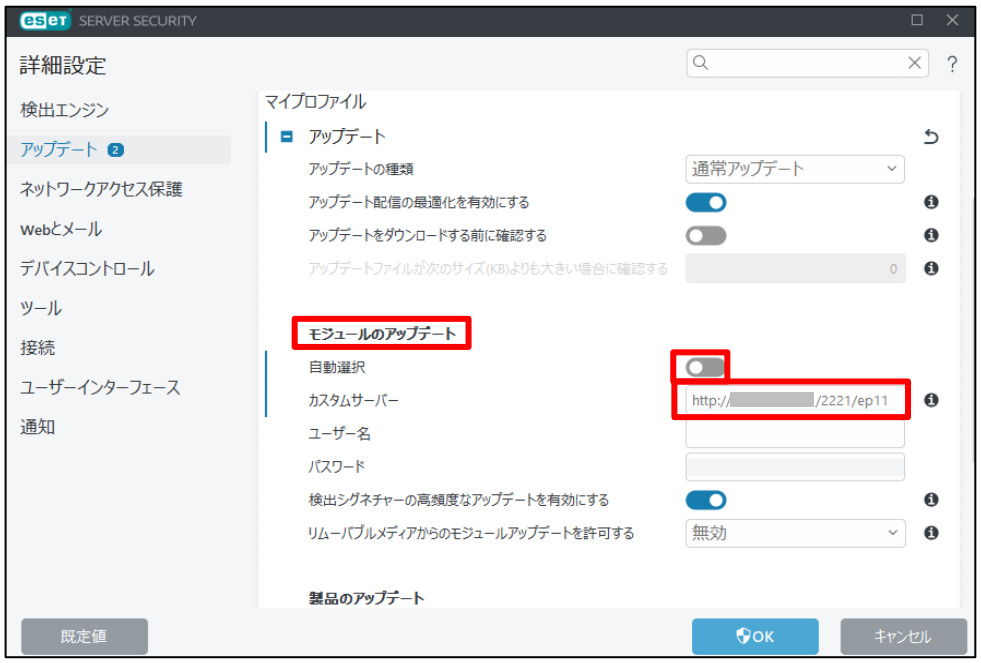
   ESET の基本画面より、[設定]-[詳細設定]をクリックします。



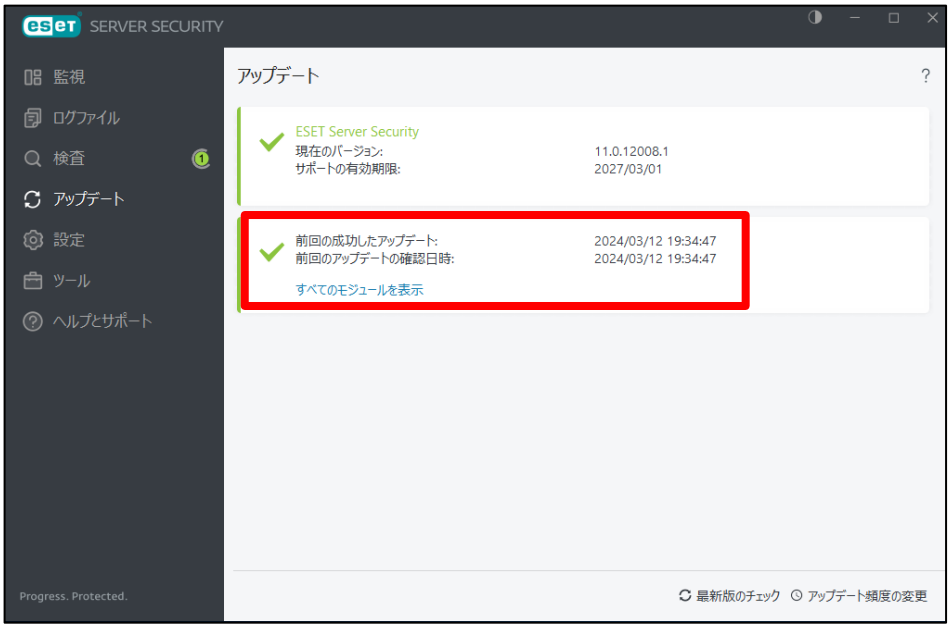
3. [アップデート]-[プロファイル]-[アップデート]をクリックします。



4. [モジュールアップデート]下の「自動選択」の項目を無効にし、カスタムサーバーに「ミラーサーバー（新サーバー）の URL を入力して、「OK」をクリックします。
   例）http://localhost:2221/ep11
   ※ミラーサーバーの既定ポート番号：2221



5. 自動的にアップデートが開始されますので、ESET の基本画面の「アップデート」に移動し、[前回のアップデートの確認日時]が更新されていることを確認します。



以上で、ミラーサーバーの構築は終了です。

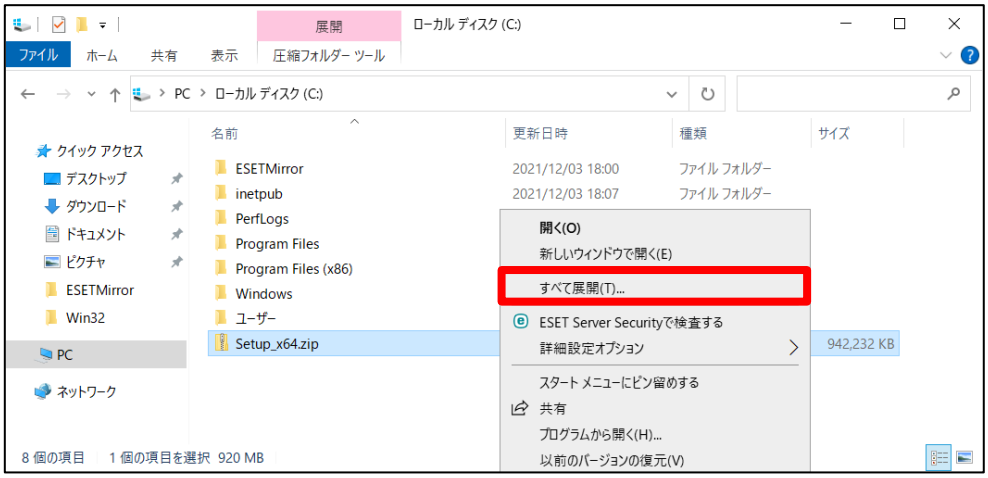
続いて、EP on-prem のインストールを行います。

7. ［STEP3］ 新サーバーにて EP on-prem のインストールとセットアップ

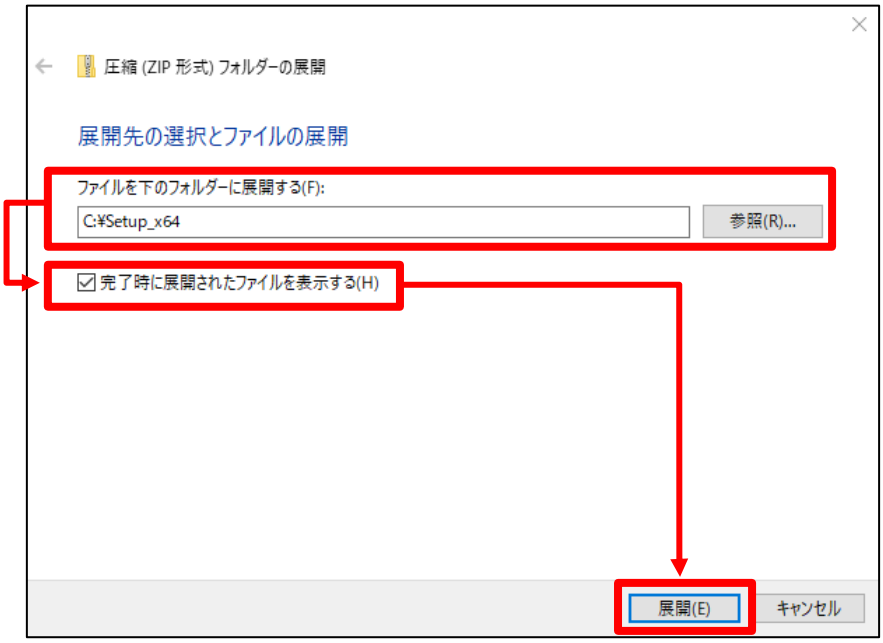
STEP3-1. EP on-prem のインストール

EP のオールインワンインストーラーを使用して、EP on-prem をインストールします。

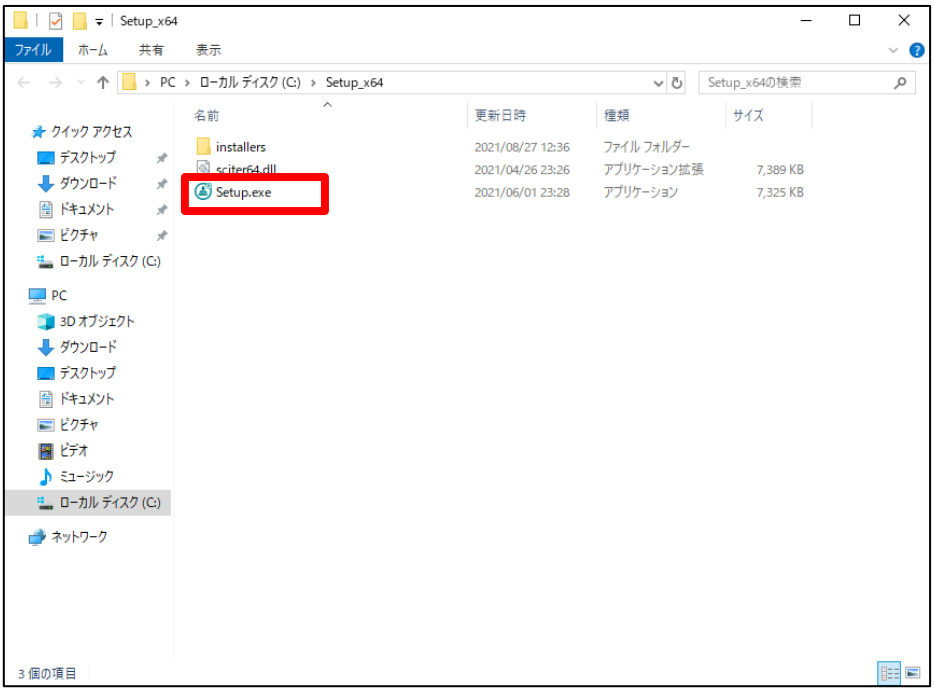
1. 事前準備で用意した EP on-prem のオールインワンインストーラー [Setup_x64.zip]を右クリックし、[すべて展開]をクリックします。



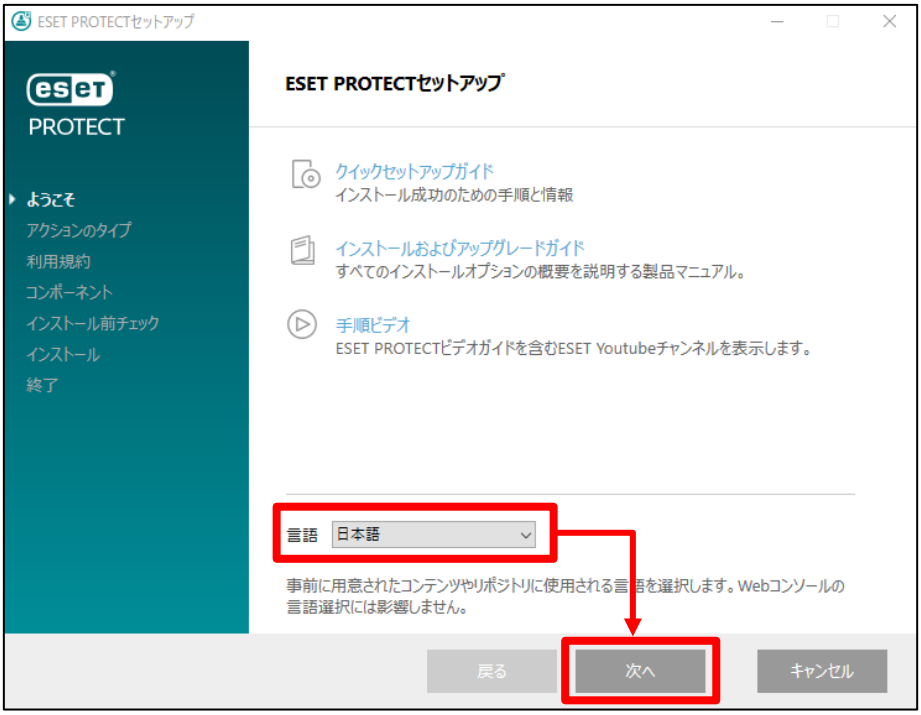
2. ファイルを展開させるフォルダを選択し、以下の項目がチェックされていることを確認して、[展開]をクリックします。
   ☑完了時に展開されたファイルを表示する



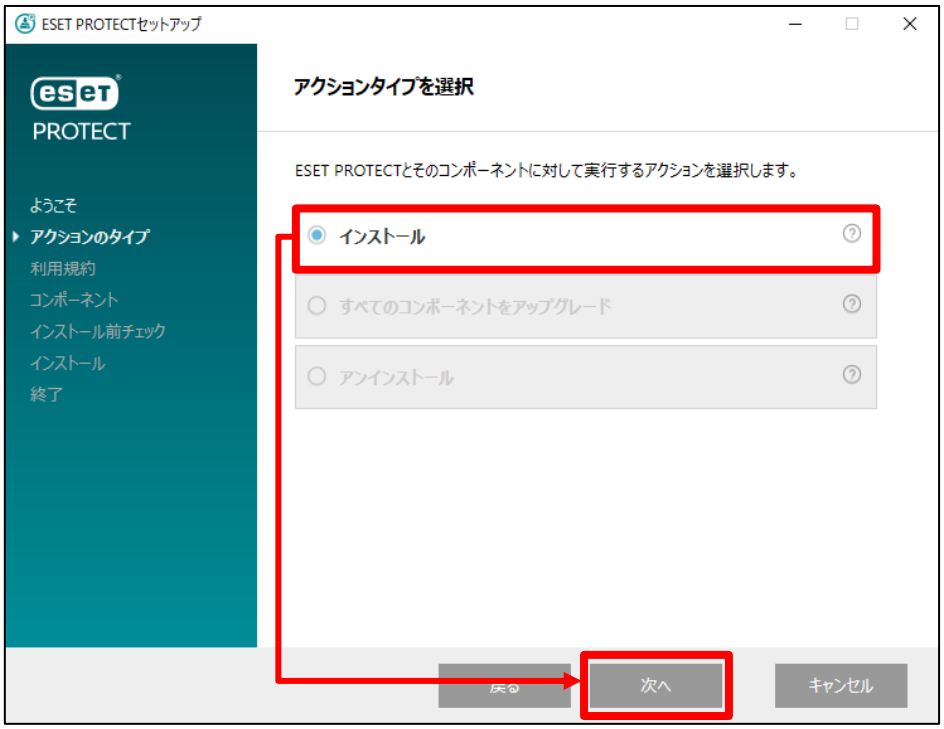
3. 展開されたファイルが表示されましたら、[Setup.exe]をダブルクリックしてオールインワンインストーラーを起動します。



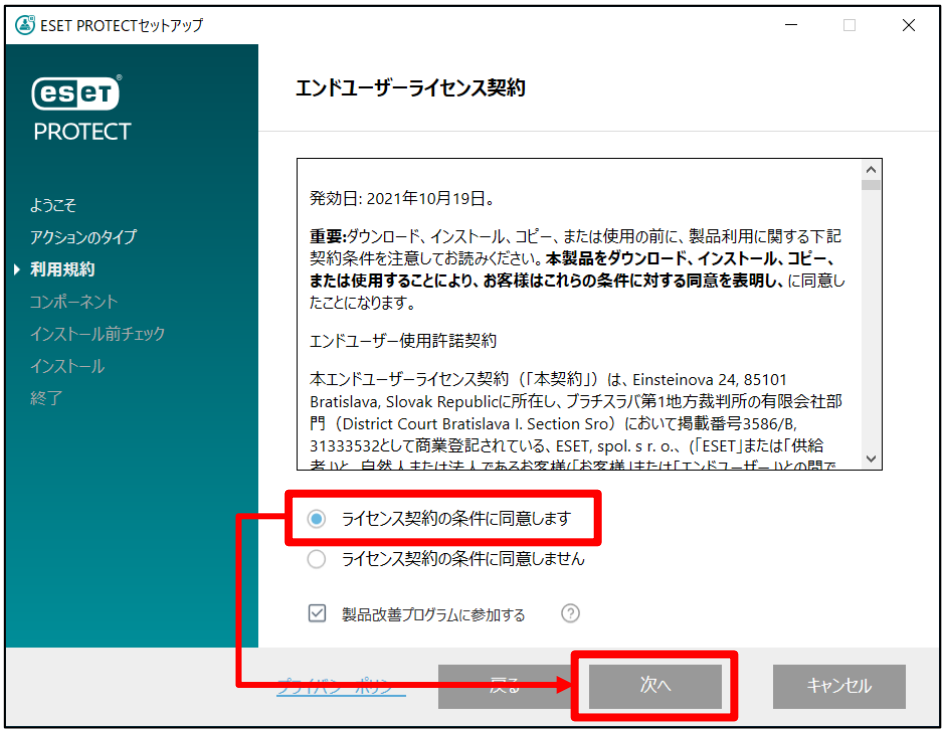
4. 言語は日本語を選択し、[次へ]をクリックします。



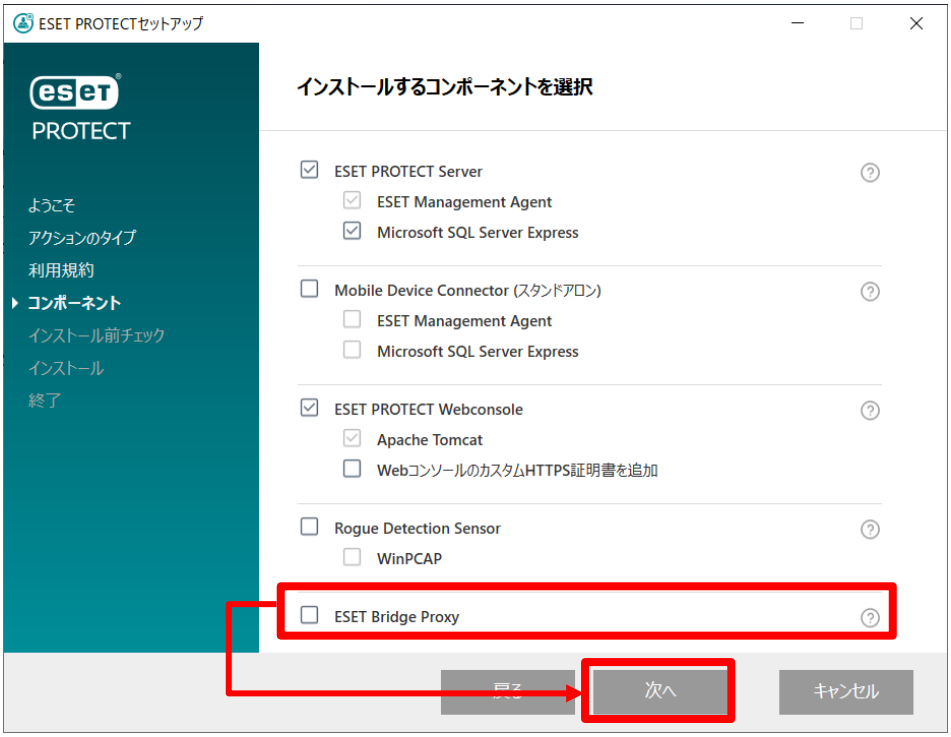
5. [インストール]を選択して、[次へ]をクリックします。



6. [ライセンス契約の条件に同意します]に同意して[次へ]をクリックします。



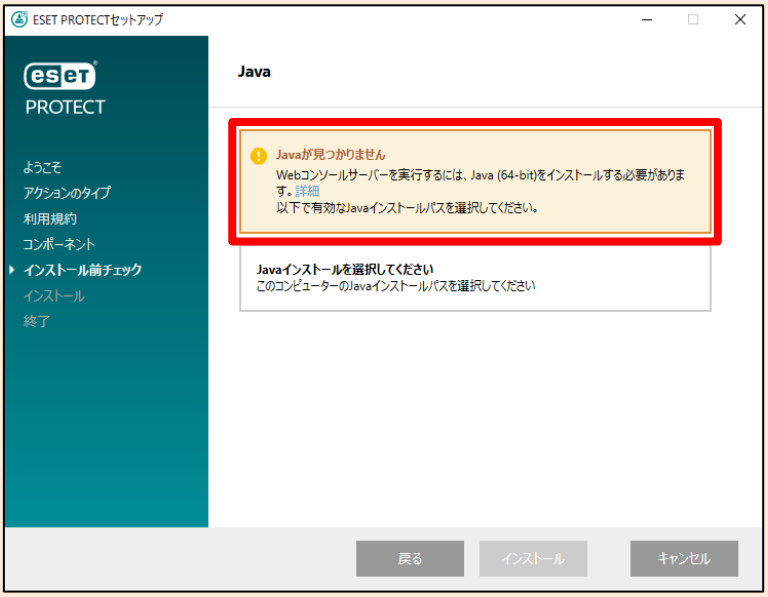
7. **[ESET Bridge Proxy]のチェックを外し、**[次へ]をクリックします。
   ※Rogue Detection Sensor は任意でインストールしてください。
   ※ [Mobile Device Connector(スタンドアロン)]にチェックを入れないようご注意ください。



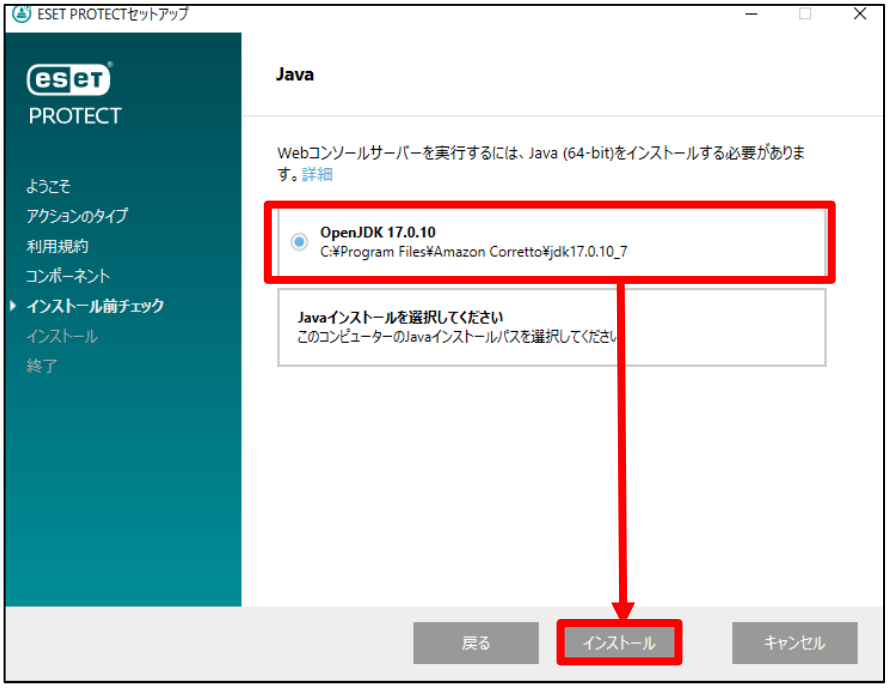
＜参考＞

以下のようなエラーが表示されましたら、[Microsoft .NET Framework 4]をインストールし、その後、[再試行]をクリックしてください。

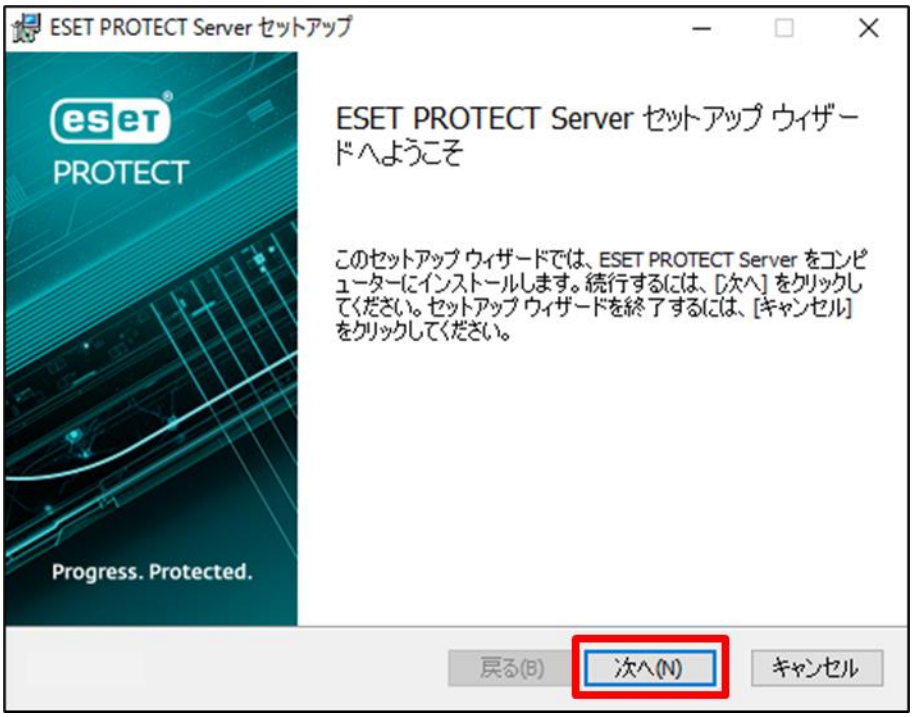
さらに、以下のようなエラーが表示されましたら、64bit 版の Java をインストールする必要があります。Java をインストールして、[インストール]をクリックしてください。
なお、オープンソース JDK を利用して構築される場合は以下のサイトを参照してインストールを行ってください。
URL：https://eset-support.canon-its.jp/faq/show/13029?site_domain=business



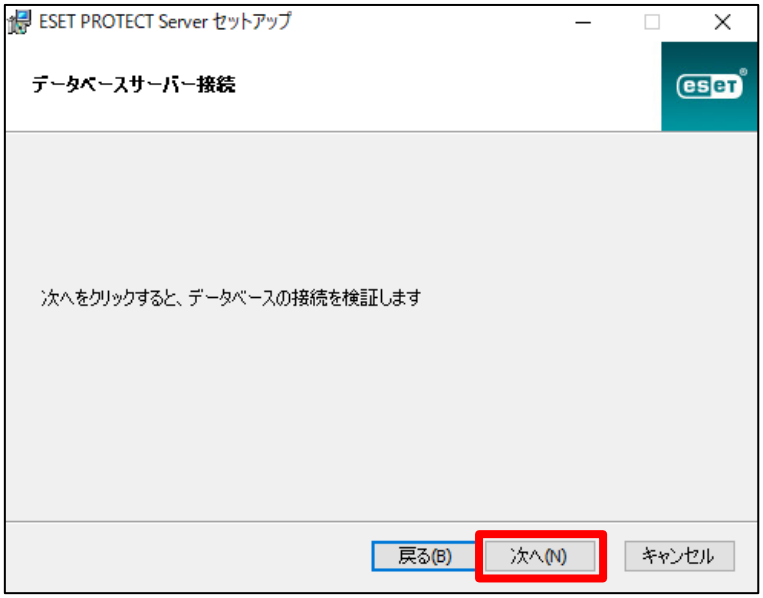
8. Web コンソールで使用する 64bit 版の Java を選択し、[インストール]をクリックします。
   ※本手順書では、オープンソース JDK を利用します。



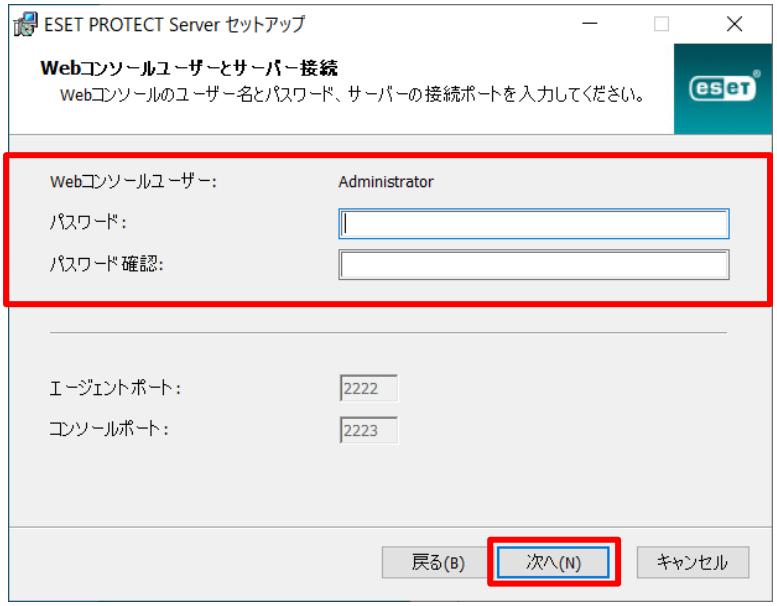
9. ESET PROTECT on-prem Server セットアップウィザードが表示されましたら、[次へ]をクリックします。



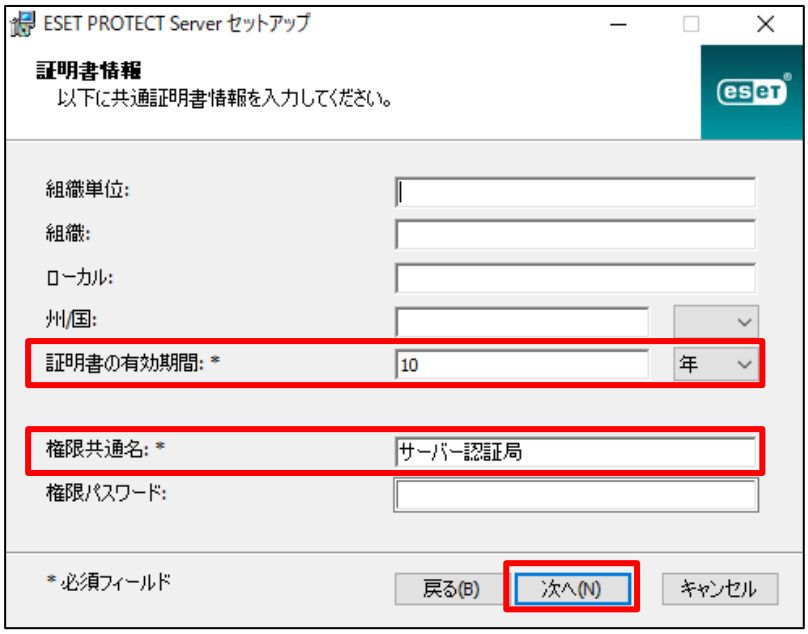
10. 以下の画面が表示されましたら、[次へ]をクリックします。



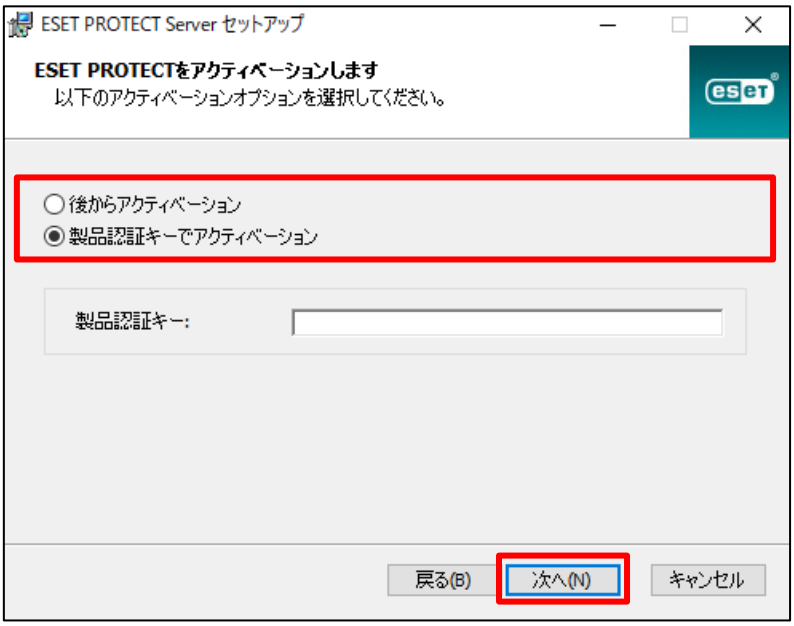
11. Web コンソールへ Administrator でログインするためのパスワードを設定して、［次へ］をクリックします。



12. 必須フィールドに入力があることを確認し、［次へ］をクリックします。



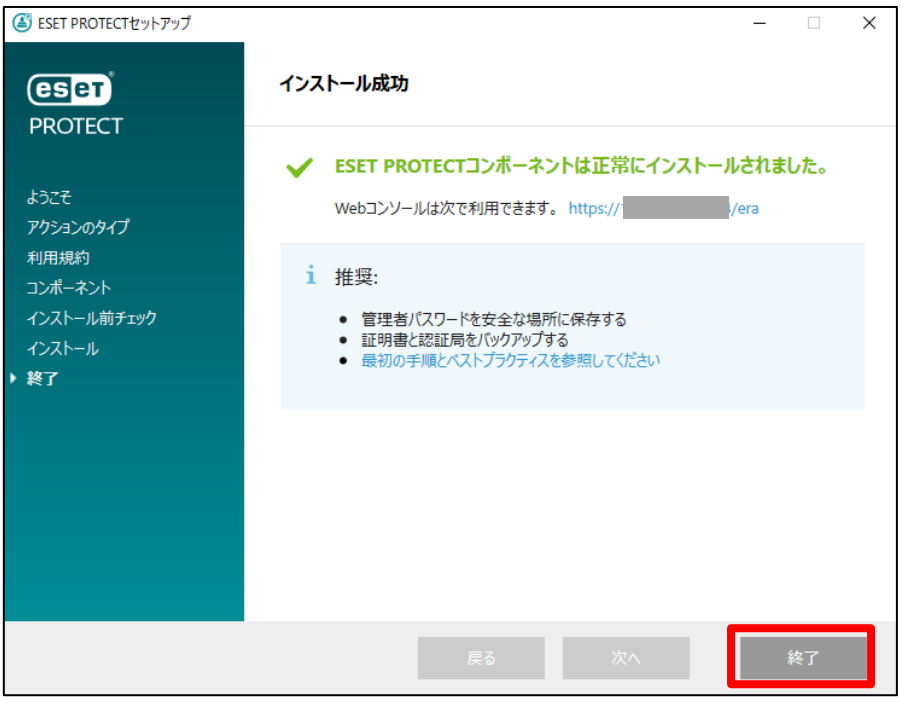
13. [製品認証キーでアクティベーション]にチェックをいれ、[製品認証キー]を入力して[次へ]をクリックします。
※プロキシサーバー経由でインターネットに接続する環境の場合は、「後からアクティベーション」を選択のうえインストールを行い、以下を参考にプロキシ設定を行ってからアクティベーションを実施ください。
【プロキシサーバーの設定方法について】
https://eset-support.canon-its.jp/faq/show/158?site_domain=business
【オンプレミス型セキュリティ管理ツールの製品のアクティベーションをおこなうには？】
https://eset-support.canon-its.jp/faq/show/17938?site_domain=business



14. [インストール]をクリックして、EP on-prem サーバーのインストールを開始します。

15. 以下の画面が表示されましたら[完了]をクリックします。

16. インストールが成功すると、以下の画面が表示されます。Web コンソールのアドレスが表示されますのでご確認ください。最後に［終了］をクリックしてインストール完了です。



<参考>

EP on-prem では、クライアントから収集したログや設定ファイルを、既定でインストールされる Microsoft SQL Server に保存します。管理するクライアントの台数が多い場合やログを長期間保存する場合は、容量制限のないデータベースをご利用ください。
詳細は、下記 Web ページをご参照ください。
【セキュリティ管理ツールのサポート対象データベースについて】
https://eset-support.canon-its.jp/faq/show/91?site_domain=business

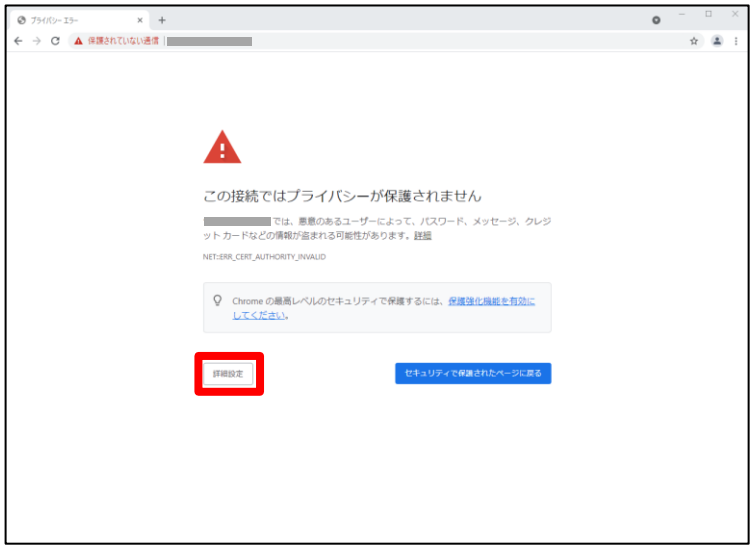
<参考>

EP on-prem で使用するポート番号は、下記 Web ページをご参照ください。
【セキュリティ管理ツールで使用するポート番号について】
https://eset-support.canon-its.jp/faq/show/94?site_domain=business

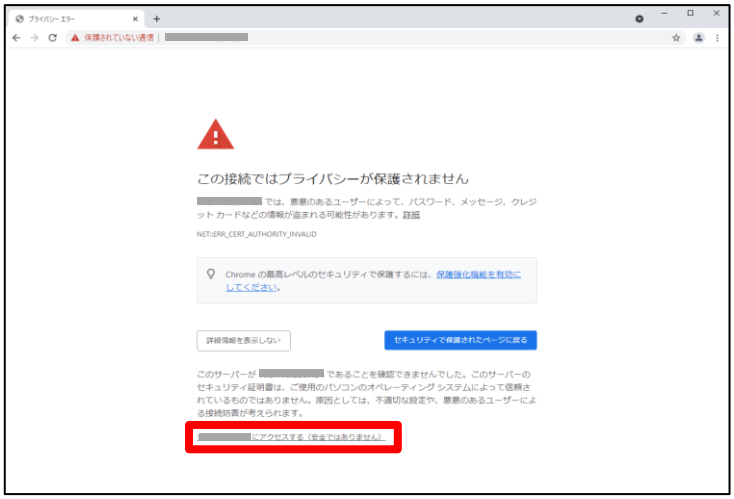
STEP3-2. クライアントのアップデート先変更ポリシーの作成

クライアントのアップデート先を新サーバーに変更するポリシーを作成します。
以下の手順でクライアントのアップデート先を変更してください。

1. 新サーバーの EP on-prem にアクセスし、EP on-prem の Web コンソールを開きます。[詳細設定]をクリックします。
   ※本手順書では、Google Chrome を利用します。
   ※ EP on-prem 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/

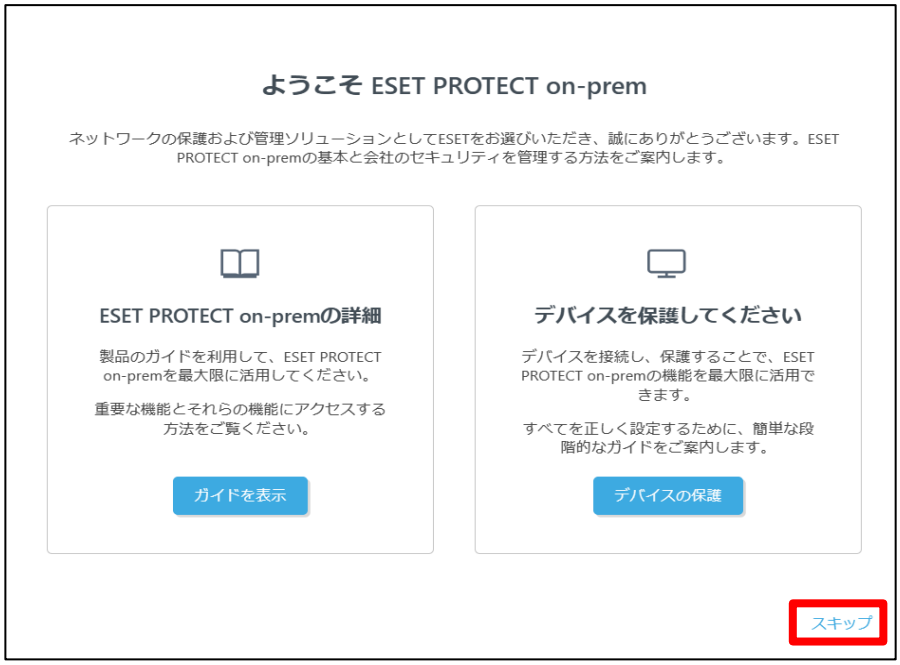


2. [<EP on-prem の IP アドレス>にアクセスする(安全ではありません)]をクリックします。
   ※ここでは、EP on-prem のインストール時に独自に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。
   ※お使いのブラウザにより表示内容が異なります。

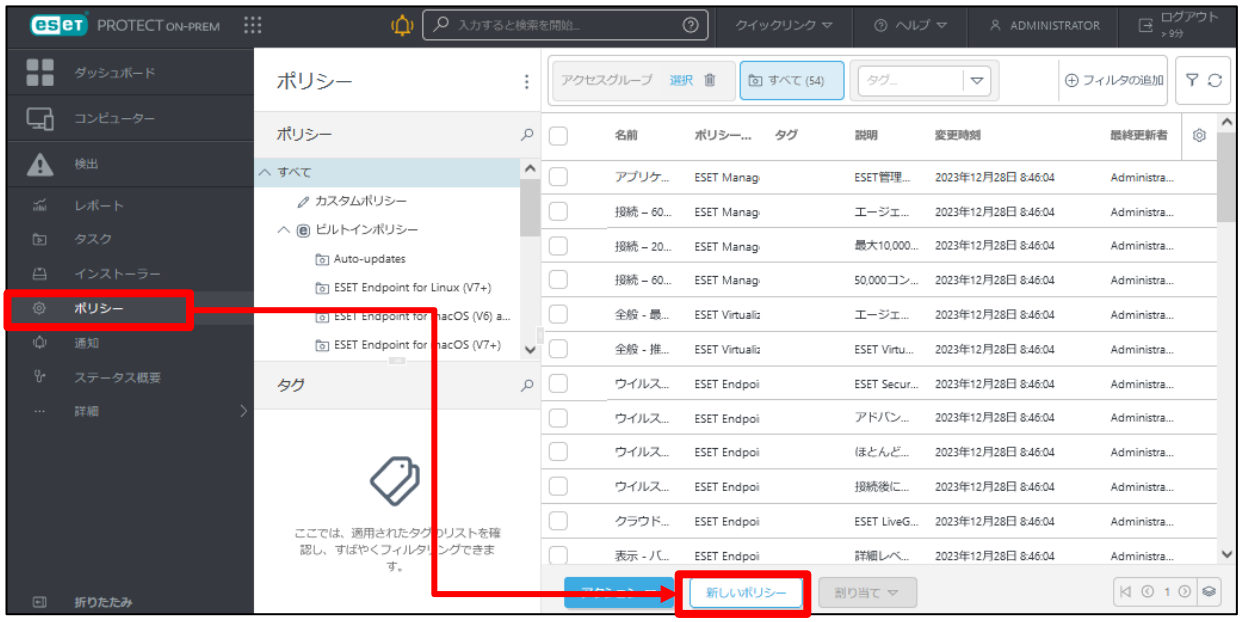


3. 言語を日本語に設定し、ユーザー名とパスワードを入力し、[ログイン]をクリックします。

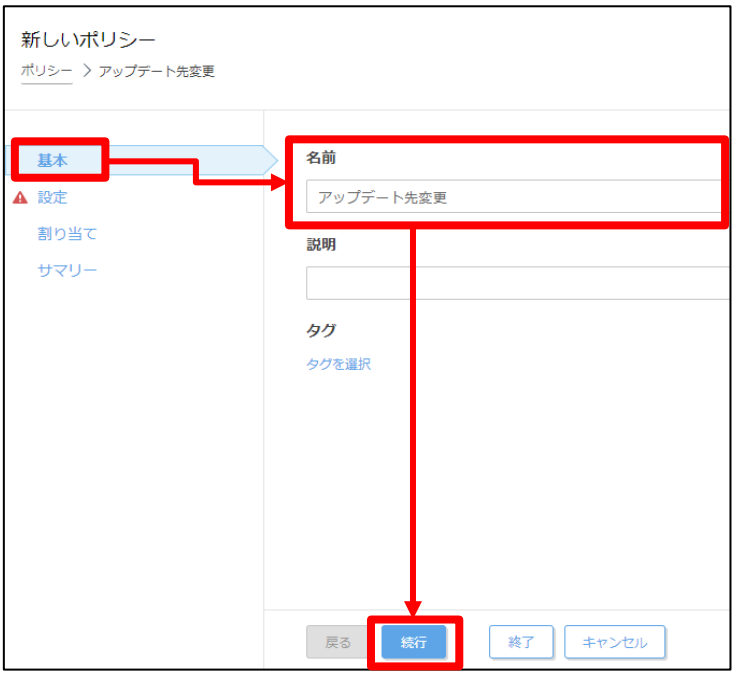
4. 以下のような画面が表示されたら[スキップ]をクリックして閉じます。



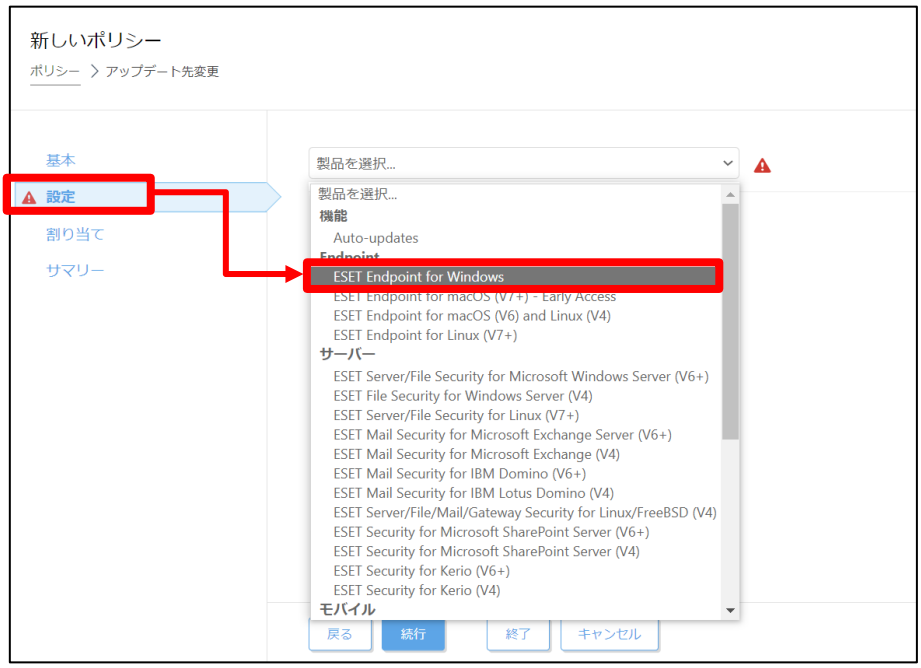
5. 画面左メニューから、[ポリシー]-[新しいポリシー]をクリックします。



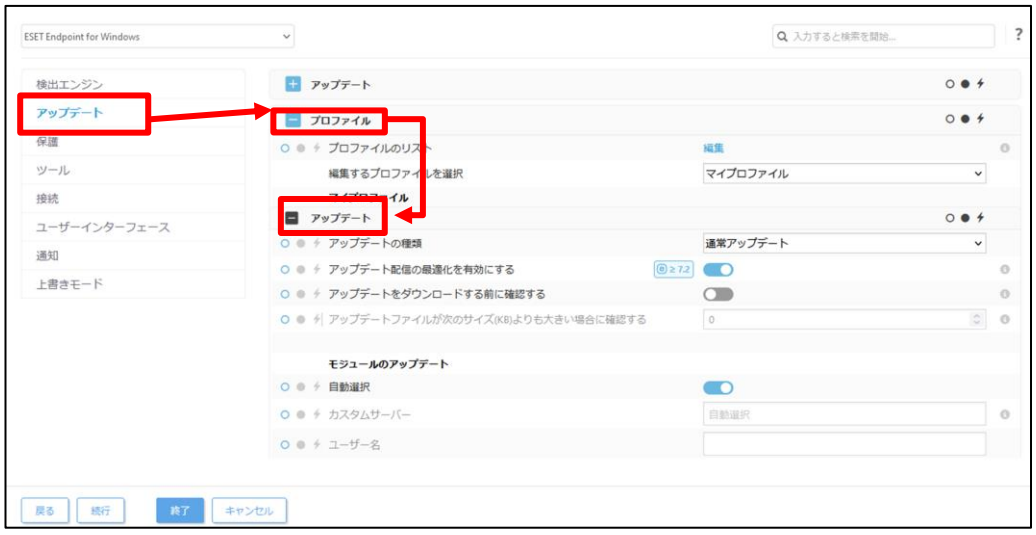
6. [基本]では、ポリシーの[名前]を入力し、[続行]をクリックします。
※[説明]と[タグ]の設定は任意です。



7. [設定]の[製品を選択...]欄にて、管理しているクライアントのプログラムに合わせて製品を選択します。
※ここでは例として、Windows クライアント用プログラムの[ESET Endpoint for Windows]を選択します。



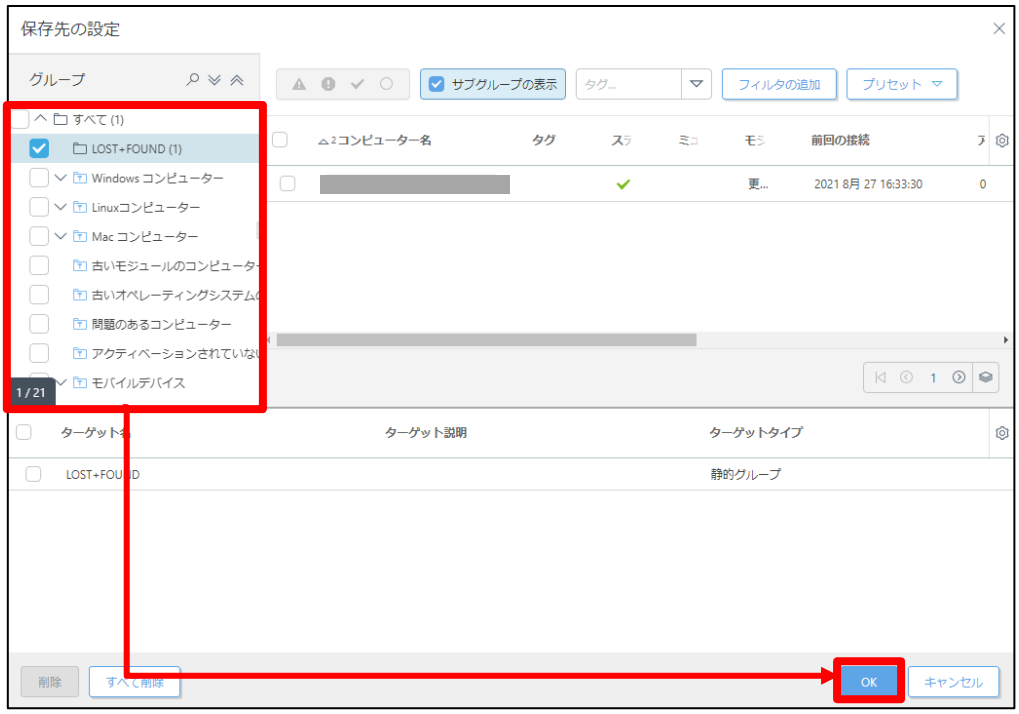
8. [アップデート]-[プロファイル]-[アップデート]をクリックします。



9. [モジュールアップデート]-[自動選択]のチェックを外して、[カスタムサーバー]に「ミラーサーバー（新サーバー）の URL を入力し、[続行]をクリックします。
例）http://<新サーバーの IP アドレス>:<ポート番号>/ep11
※ミラーサーバーの既定ポート番号：2221

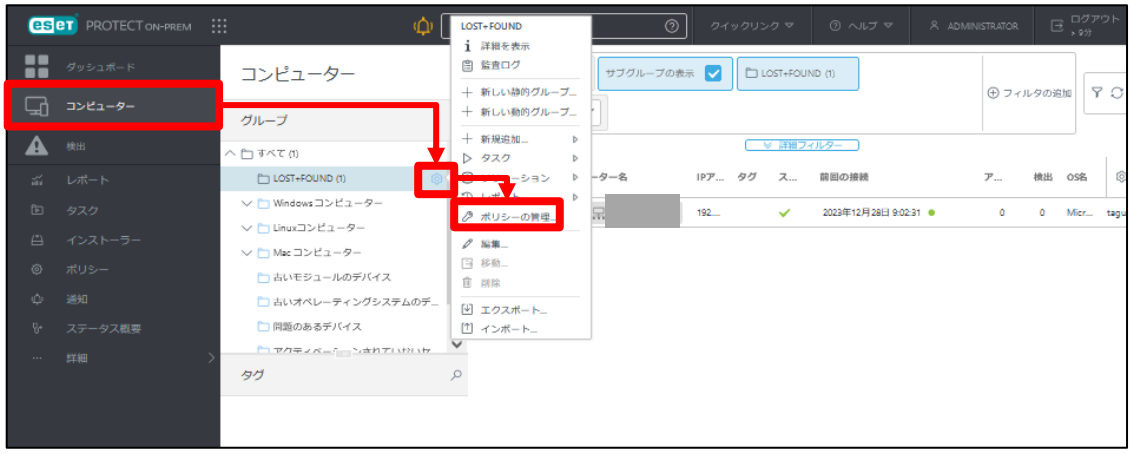
10. [割り当て]で、[割り当て...]をクリックします。

11. ポリシーを割り当てたいグループにチェックをいれ、[OK]をクリックします。
※本手順で[ESET Server/File Security for Windows Server (V6+)]用のポリシーを作成し新サーバーに割り当てた場合、[STEP2]で設定したアップデート先の設定が上書きされてしまいます。ご注意ください。

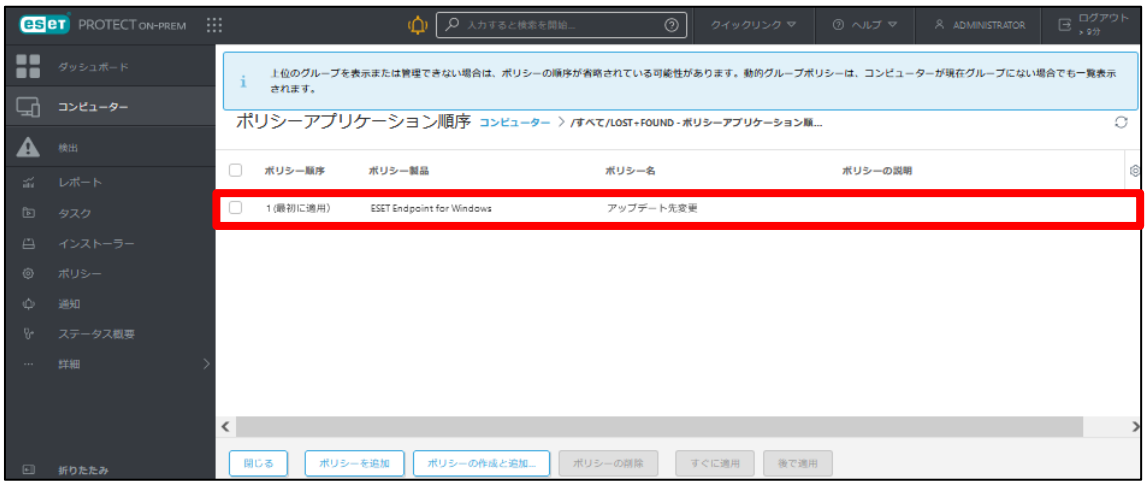


12. 手順 11 でチェックしたグループが[ターゲット名]に追加されていることを確認して、[終了]をクリックします。

13. 画面左メニューから、[コンピューター]へ移動し、手順 11 でチェックしたグループを選択し、歯車マークから[ポリシーの管理]をクリックします。



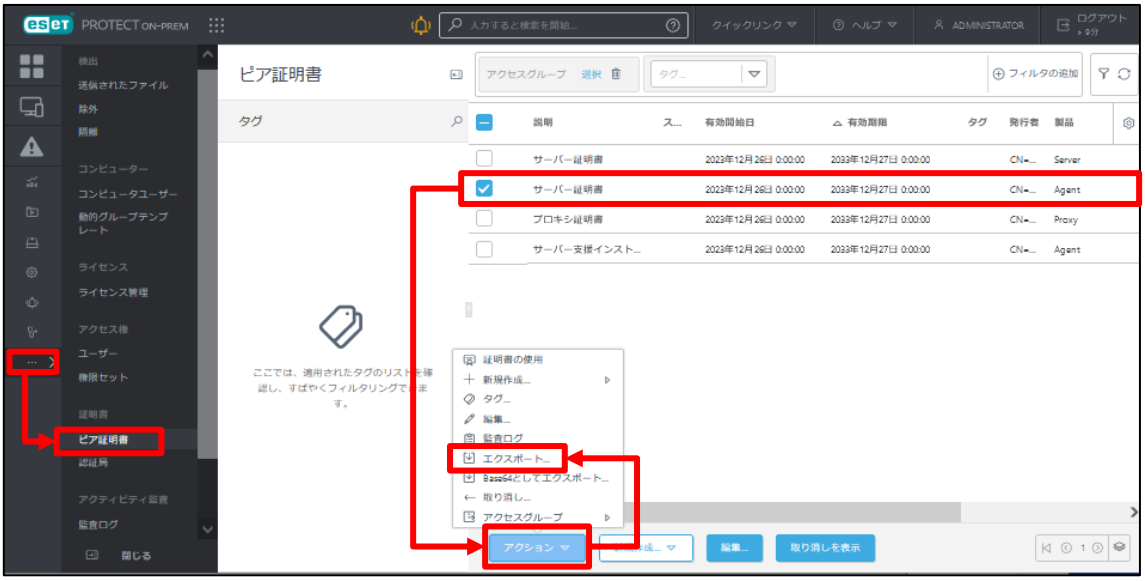
14. 割り当てたポリシーが表示されることを確認します。



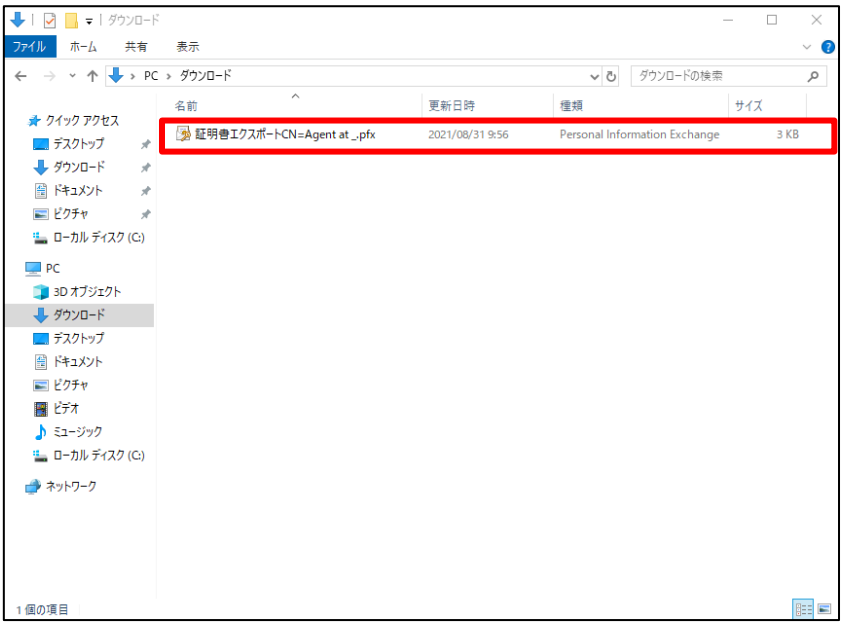
STEP3-3. EM エージェントの証明書と認証局のエクスポート

新サーバーの EP on-prem と EM エージェントの接続に使用しているエージェントの証明書をエクスポートします。

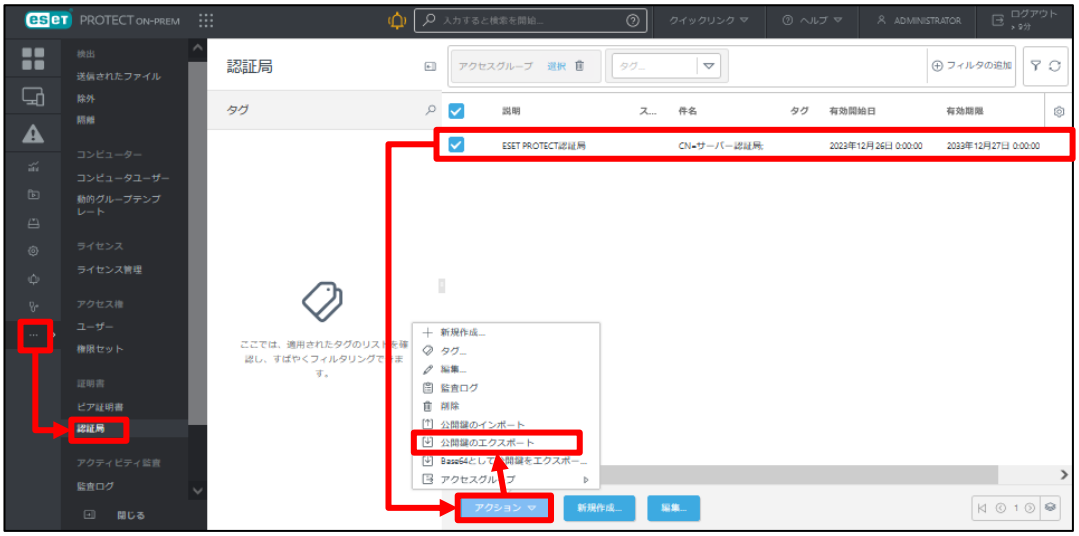
1. [詳細]-[ピア証明書]より、エクスポートを行う[サーバー証明書(製品：Agent)]を選択し、「アクション」より「エクスポート」をクリックします。



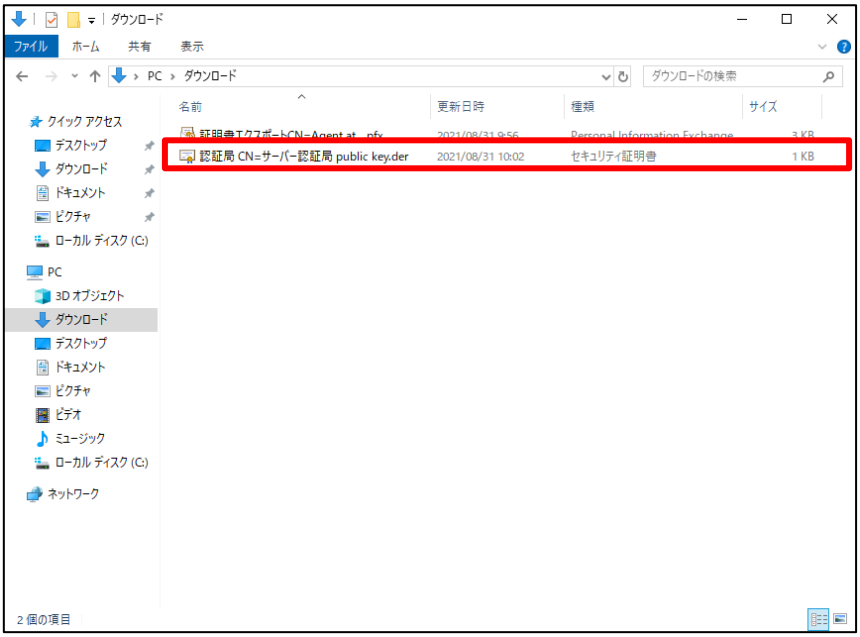
2. エクスポートした証明書を任意の保存先に保存します。
   ※保存した証明書は、旧サーバーで使用します。



3. [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。



4. 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。
※保存した公開鍵(認証局)は、旧サーバーで使用します。



以上で、新サーバーでの EP on-prem のインストールとセットアップは完了です。

ここまでが、新サーバー側での作業です。

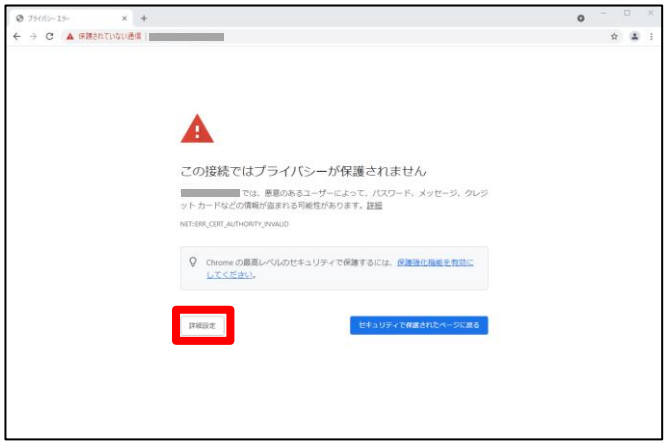
ここからは、旧サーバー側での作業です。

8. ［STEP4］ 旧サーバーにてクライアントの接続先変更

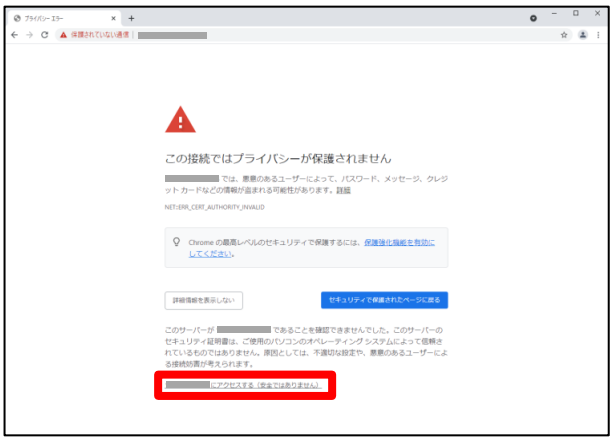
STEP4-1. 旧 EP on-prem サーバーへ認証局のインポート

クライアントの接続先を新サーバーに変更するために、<STEP3-3> でエクスポートした新サーバーの EP on-prem の認証局を旧サーバーにインポートします。

1. 旧サーバーの EP on-prem にアクセスし、EP on-prem の Web コンソールを開きます。
   [詳細設定]をクリックします。
   ※本手順書では、Google Chrome を利用します。
   ※ EP on-prem 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/

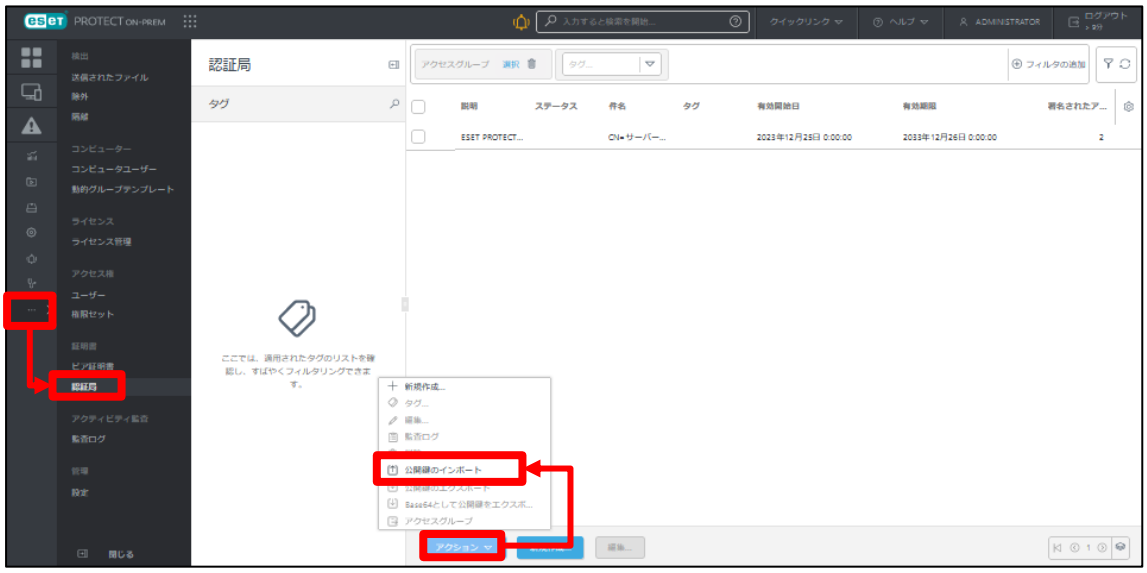


2. [<EP の IP アドレス>にアクセスする(安全ではありません)]をクリックします。
   ※ここでは、EP on-prem のインストール時に独自に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。
   ※お使いのブラウザにより表示内容が異なります。

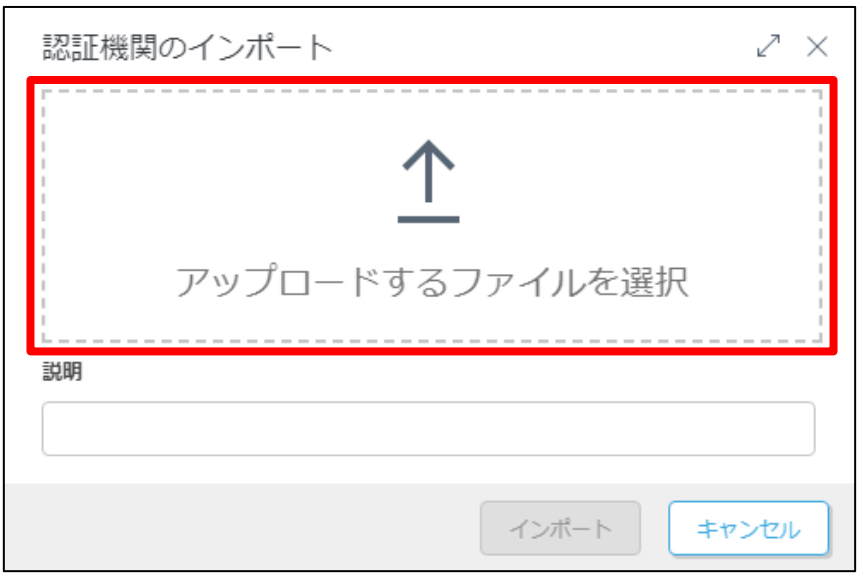


3. ユーザー名とパスワードを入力し、[ログイン]をクリックします。

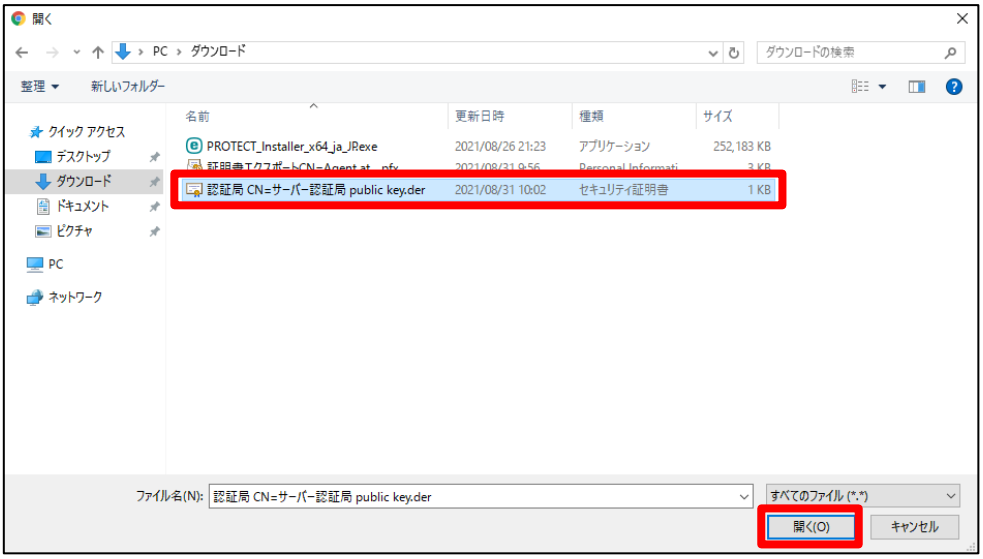
4. [詳細]-[認証局]より、[アクション]-[公開鍵のインポート]をクリックします。



5. [アップロードするファイルを選択]をクリックします。

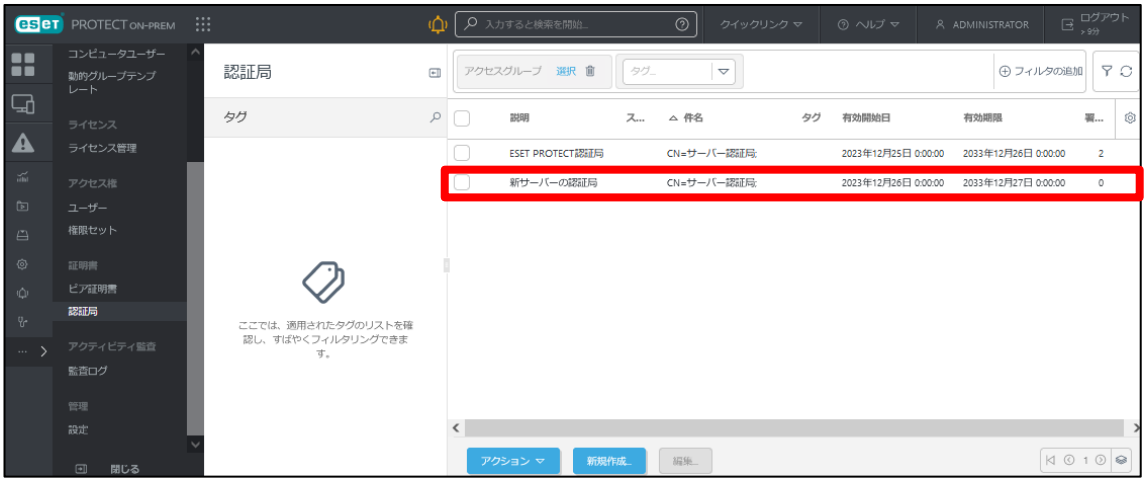


6. [STEP3-3]でエクスポートした新サーバーの公開鍵(認証局)を選択し、[開く]をクリックします。



7. 認証局が追加されたことを確認して[インポート]ボタンをクリックします。
※説明の入力は任意です。

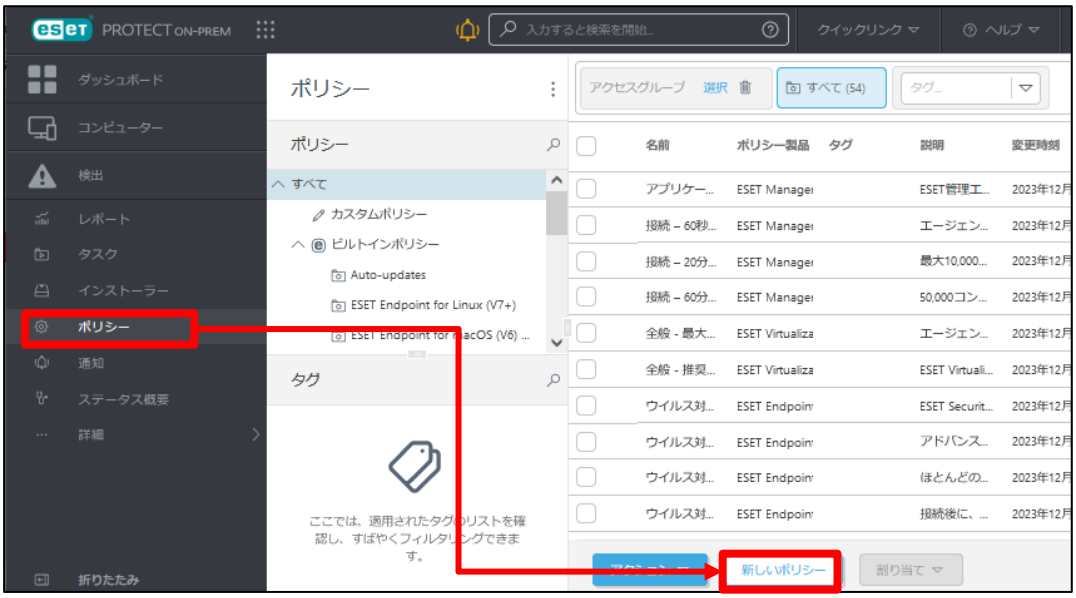
8. 新サーバーの認証局が追加されたことを確認します。



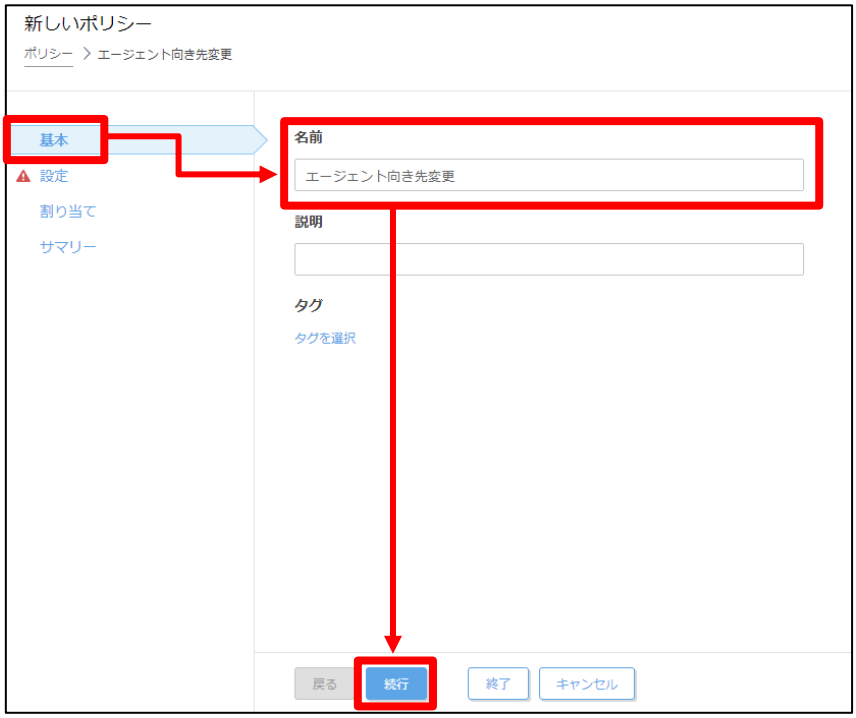
STEP4-2. EM エージェントの接続先変更

クライアントの接続先を新サーバーに構築した EP on-prem に変更するため、ポリシー機能を使用し、接続先 EP サーバーの変更と[STEP3-3]でエクスポートした証明書の配布を行います。

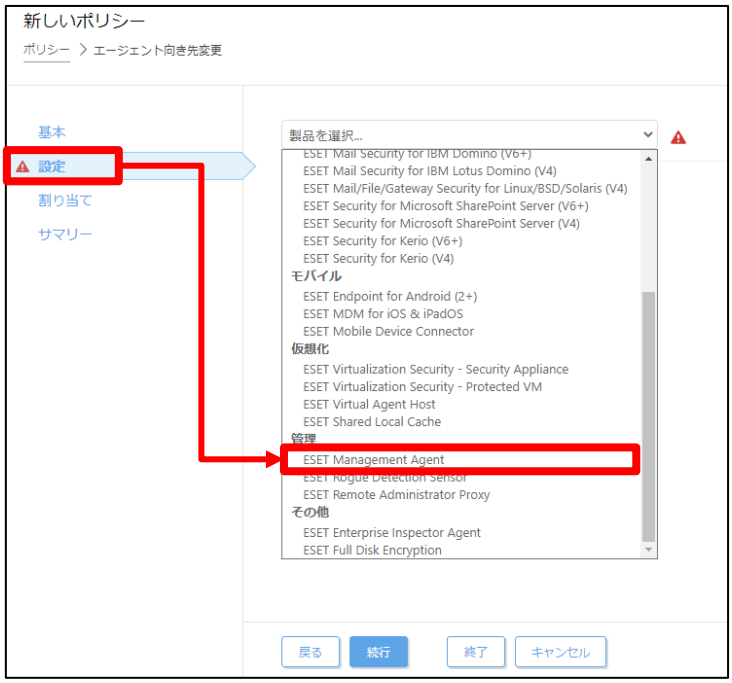
1. [ポリシー]-[新しいポリシー]をクリックします。



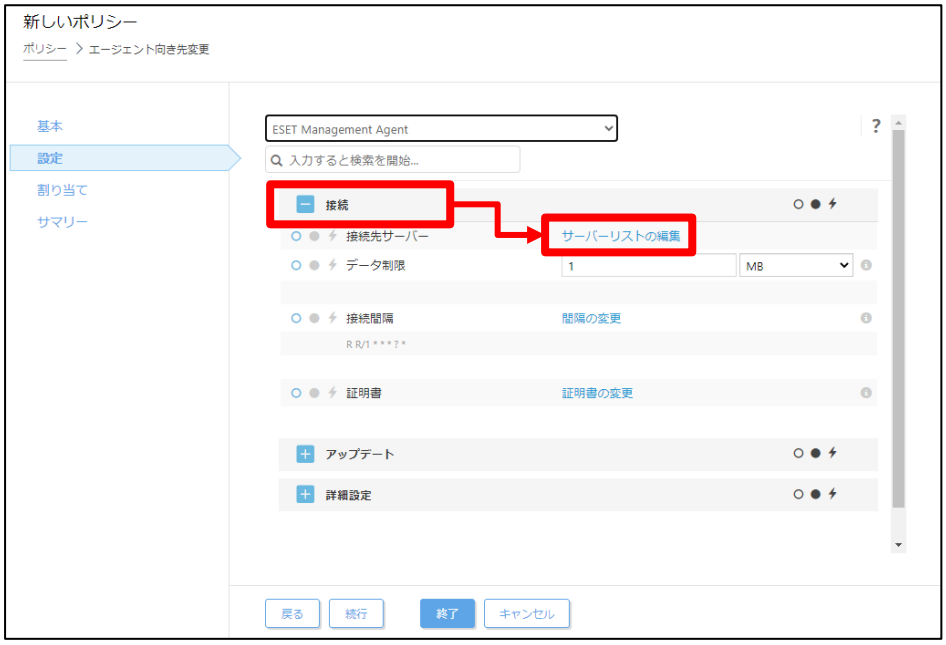
2. [基本]では、ポリシーの[名前]を入力し、[続行]をクリックします。
※[説明]と[タグ]の設定は任意です。



3. [設定]の[製品を選択...]欄にて[ESET Management Agent]を選択します。

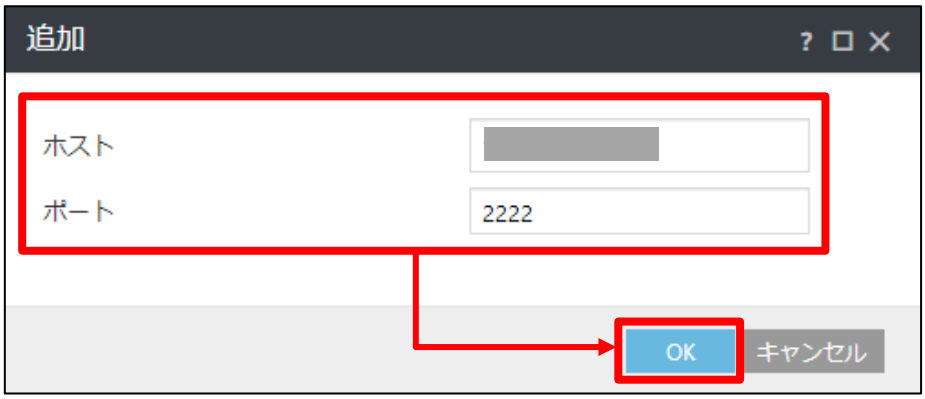


4. [接続]-[サーバーリストの編集]をクリックします。



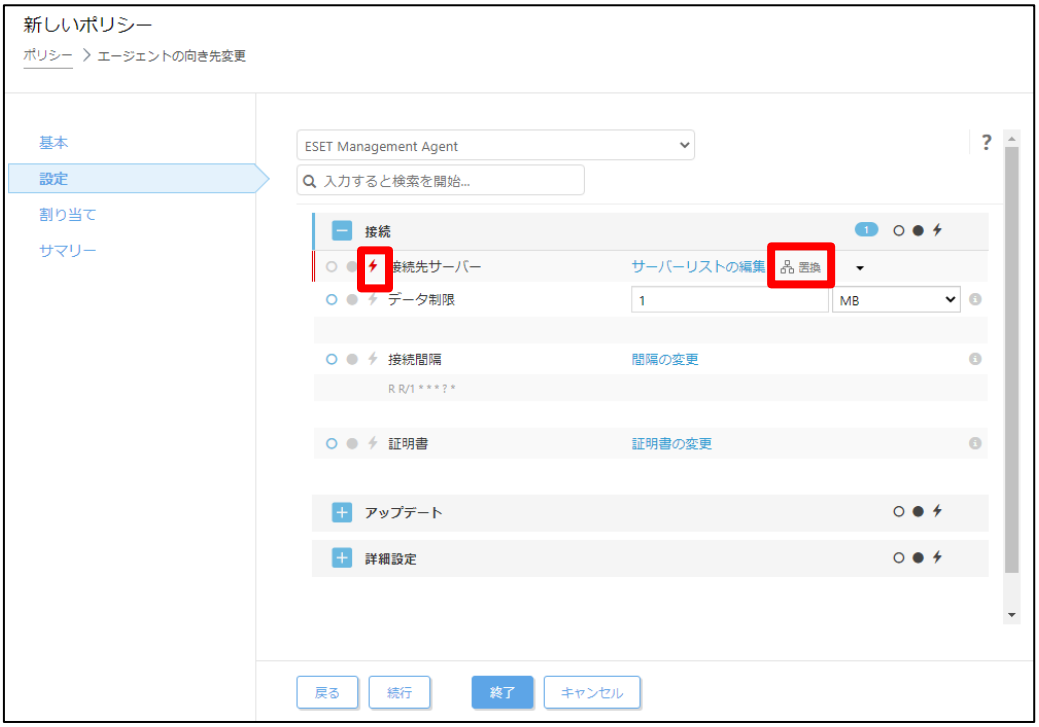
5. [サーバー]画面で[追加]をクリックします。

6. 以下の通り入力し、[OK]をクリックします。
ホスト：新サーバーの IP アドレスまたはコンピューター名
ポート：2222 (既定：2222)

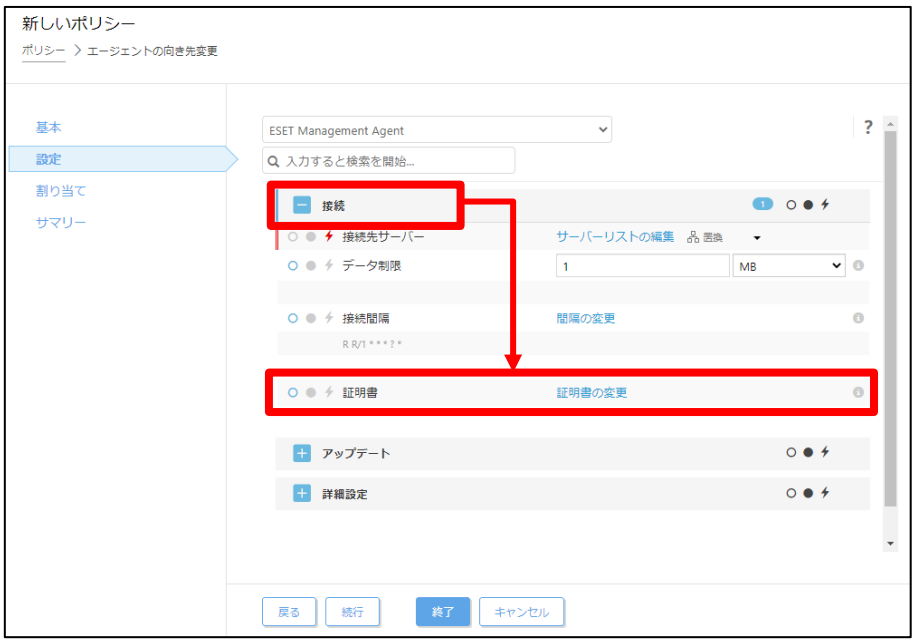


7. 手順 6 で入力した値が追加されていることを確認して[保存]をクリックします。

8. 適用方法が[置換]になっていることを確認し、[接続先サーバー]-[ ]マークを選択します。

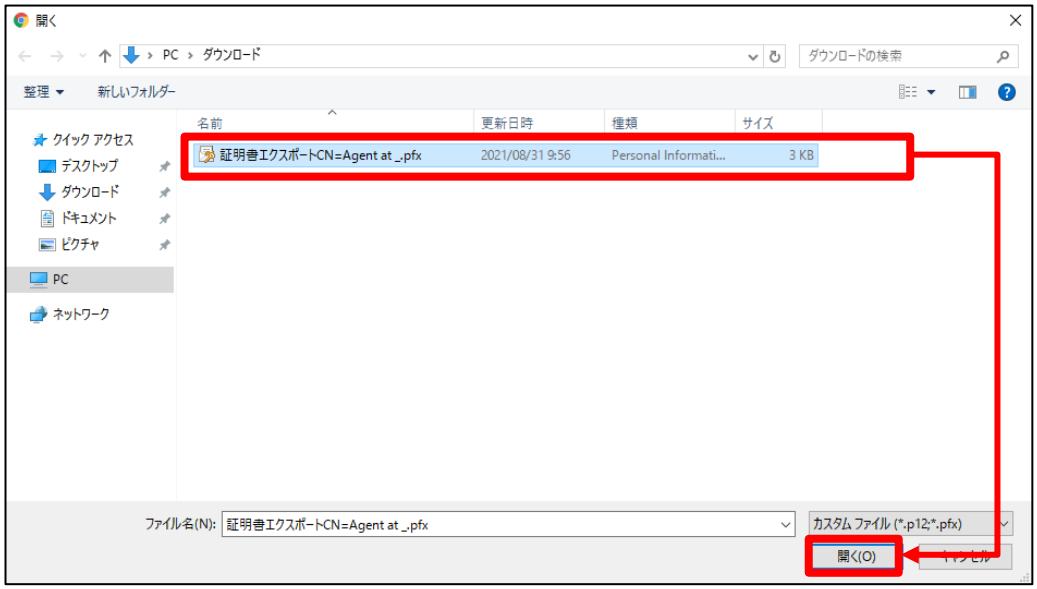


9. [接続]-[証明書の変更]をクリックします。



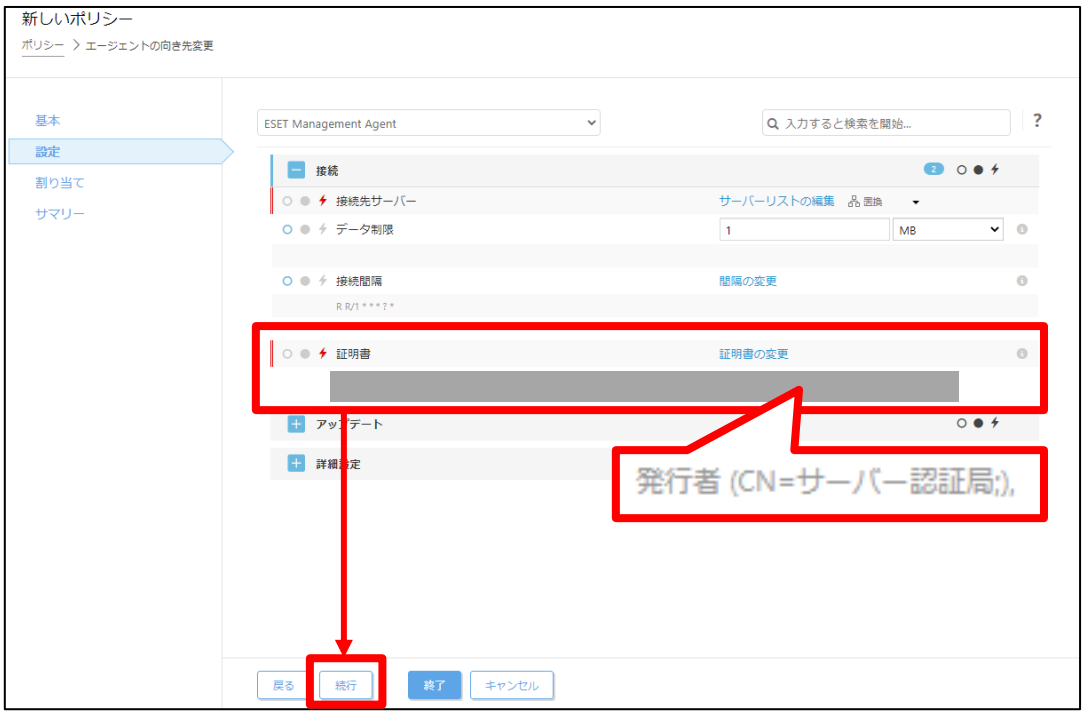
10. [ピア証明書]-[カスタム証明書]が選択されていることを確認して[カスタム証明書]横の[ ]マークをクリックします。

11. **新サーバーで使用していたサーバー証明書(製品：Agent)**を選択して、[開く]をクリックします。

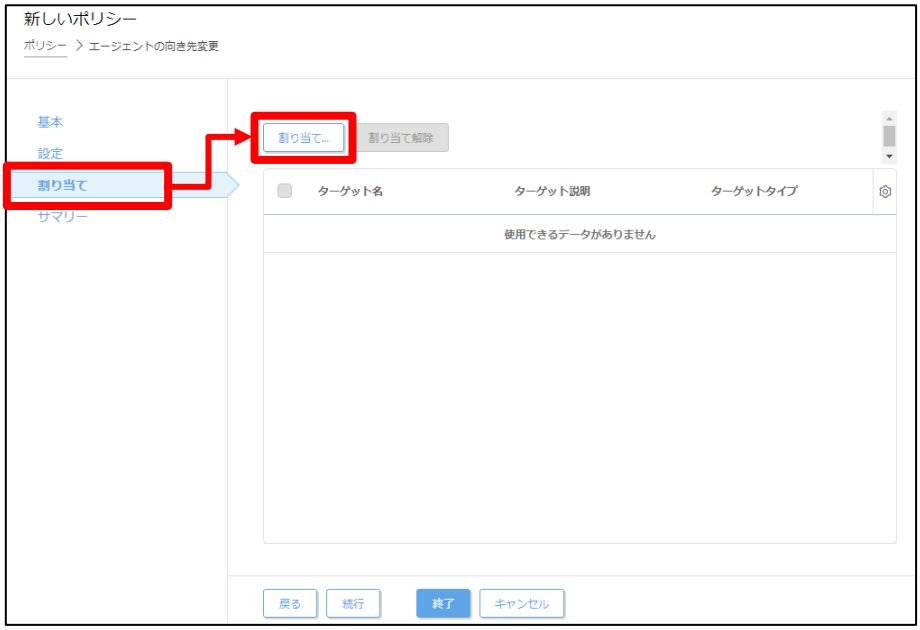


12. 新サーバーのサーバー証明書(製品：Agent)にパスワードを設定している場合は、[証明書パスワード]を入力してから、[OK]をクリックします。

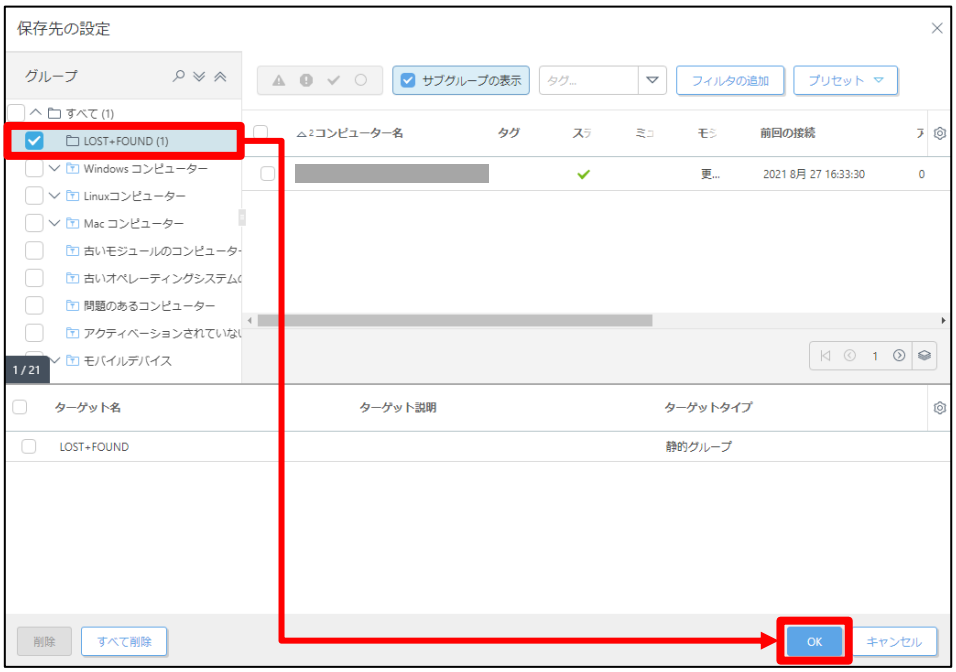
13. 手順 11 で選択した証明書に変更されていることを確認し、[証明書]-[ ]マークを選択し、[続行]をクリックします。



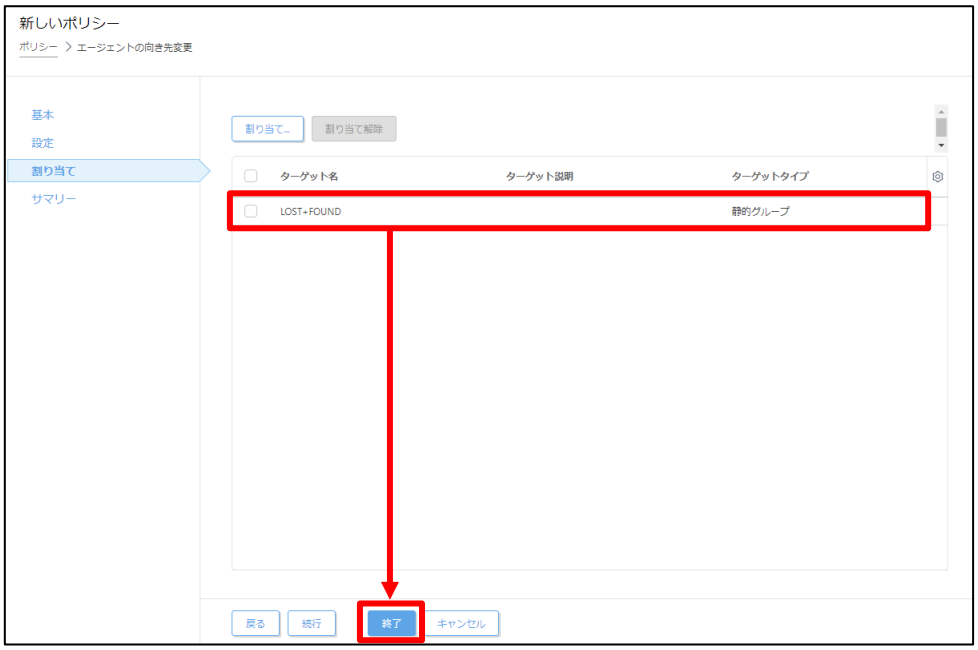
14. [割り当て]で、[割り当て...]をクリックします。



15. クライアント端末が所属するグループを選択し、[OK]をクリックします。



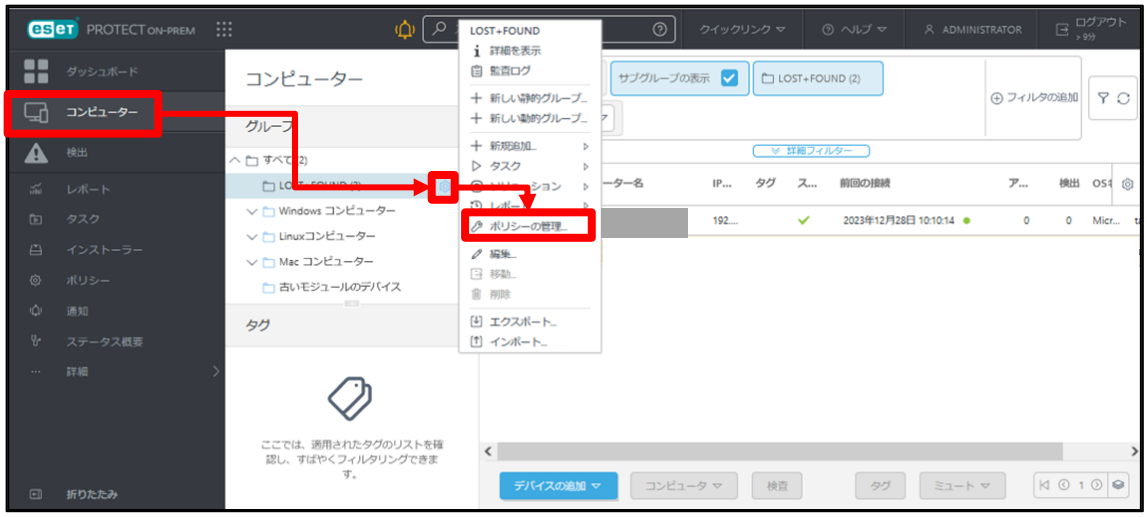
16. [ターゲット名]にクライアント端末が所属するグループが追加されていることを確認して、[終了]をクリックします。



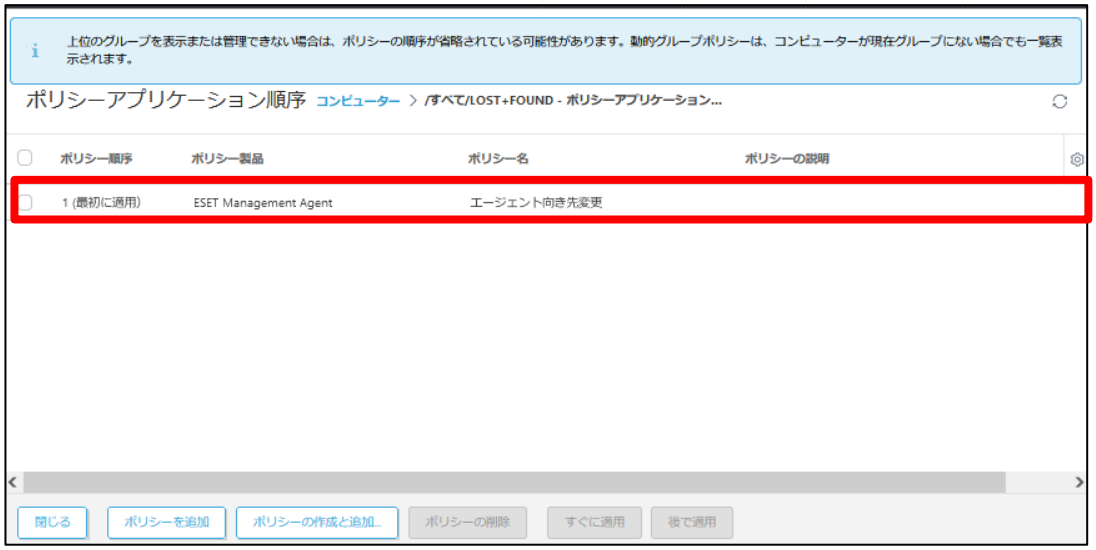
<注意>

本手順書ではグループに対して一括で接続先変更のポリシーを割り当てていますが、1 台で移行できることを確認してから、全台に展開するようにお願いいたします。

17. 画面左メニューから、[コンピューター]へ移動し、手順 15 でチェックしたグループを選択し、歯車マークから[ポリシーの管理]をクリックします。



18. ポリシーが適用されていることを確認します。



ここまでが、旧サーバー側での作業です。

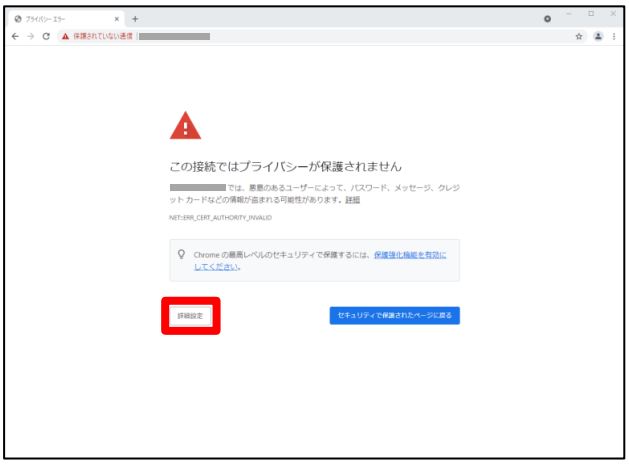
ここからは、新サーバー側での作業です。

9. ［STEP5］ 新サーバーにてリプレイス完了の確認

STEP5-1. クライアントのアップデート状況と EP on-prem への接続確認

旧サーバーで管理していたクライアントが正常に新サーバーに接続できているかを確認します。

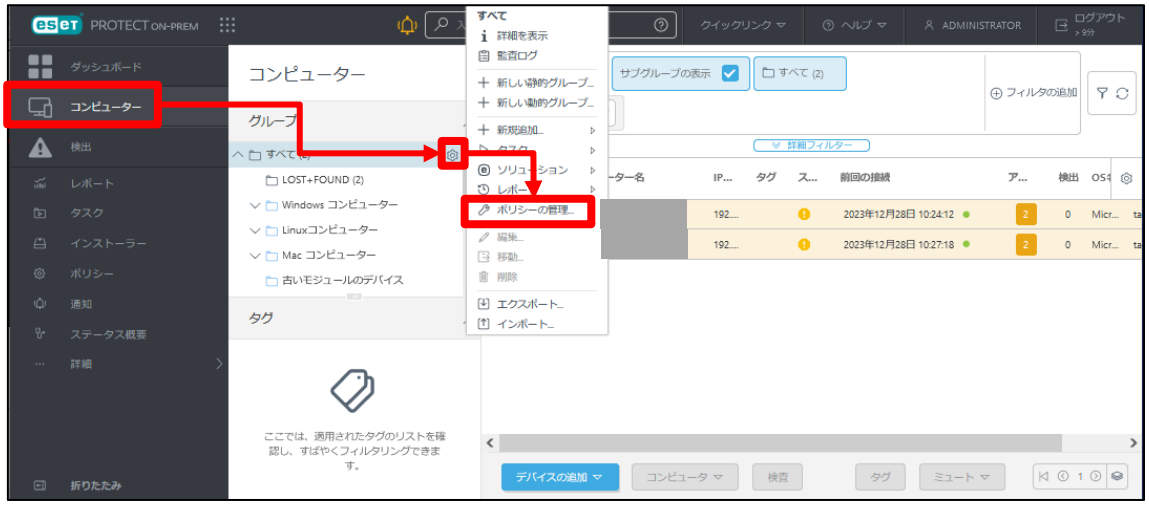
1. 新サーバーの EP on-prem にアクセスし、EP on-prem の Web コンソールを開きます。[詳細設定]をクリックします。
   ※本手順書では、Google Chrome を利用します。
   ※ EP on-prem Web コンソールには以下の URL よりアクセスできます。
   https://＜管理サーバーのサーバー名、または、IP アドレス＞/era/



2. [<EP on-prem の IP アドレス>にアクセスする(安全ではありません)]をクリックします。
   ※ここでは、EP on-prem のインストール時に独自に作成したセキュリティ証明書を利用しているため、管理画面アクセス時に上記の注意画面が表示されます。
   ※お使いのブラウザにより表示内容が異なります。

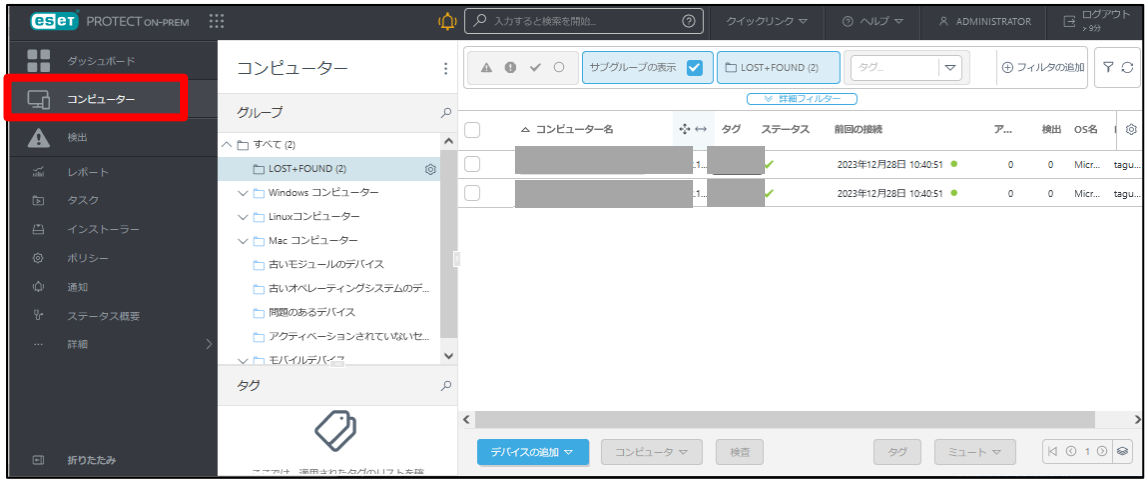
3. ユーザー名とパスワードを入力し、[ログイン]をクリックします。

4. 画面左メニューの[コンピューター]へ移動し、STEP3-2 の手順 15 でチェックしたグループを選択し、歯車マークから[ポリシーの管理]をクリックします。

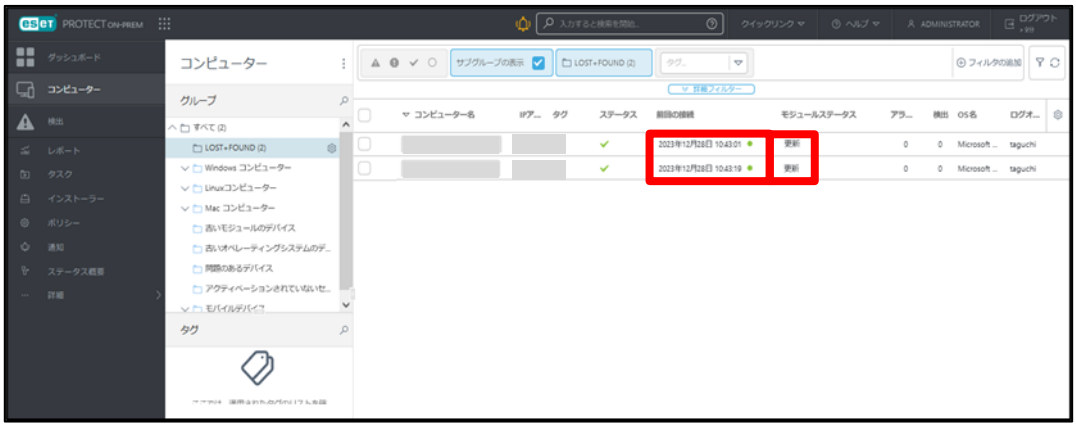


5. STEP3-2 で設定したアップデート先変更のポリシーが適用されていることを確認します。

6. 画面左メニューの[コンピューター]をクリックします。



7. コンピューターの一覧にて[モジュールステータス]が更新されていること、また、[前回の接続]の日時が更新されていることを確認します。
モジュールステータスが確認できない場合は、画面右側の歯車マークより「列を編集」をクリックし、「モジュールステータス」を表示させてください。



<参考>

サーバーリプレイスに伴い、旧サーバーの ESSW が不要になった場合は、アクティベーションを解除すると新サーバーや他の端末でライセンスを使用することができます。通常は、ESSW のアンインストールでアクティベーションを解除することが可能です。アクティベーション解除についての詳細は以下をご参照してください。

URL： https://eset-support.canon-its.jp/faq/show/4304?site_domain=business

旧サーバーで管理を行っていた全てのクライアントが新サーバーに接続できていることが確認できれば、サーバーリプレイスに伴う、ESET PROTECT on-prem 移行作業は終了です。

弊社 ESET サポートサイト情報ページにて、製品機能・仕様・操作手順などの情報を公開していますので、ご利用ください。

■ESET サポート情報　法人向けサーバー・クライアント用製品
https://eset-support.canon-its.jp/?site_domain=business

ご不明な点などがございましたら、上記の Web ページをご確認いただくか下記 Web ページより弊社の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