クラウド型セキュリティ管理ツール
ESET PROTECT 移行手順書

第 22 版

2025 年 7 月 2 日

キヤノンマーケティングジャパン株式会社

改訂履歴

版数	発行日	改訂履歴
第 1 版	2021 年 7 月 1 日	初版発行
第 2 版	2021 年 10 月 8 日	P4…ライセンス情報確認場所について追記 P21～P30…手順「EM エージェントのアップグレード」と手順「移行したポリシーを EPC へ適用」の入れ替え P31 以降…端末の再アクティベーション不要のため削除
第 3 版	2021 年 10 月 15 日	P8～P43…EPC 移行のための事前準備追加 P46～P48…移行後端末のグルーピング方法を追加
第 4 版	2021 年 10 月 29 日	P4…オンプレミスなどの既存環境からの移行にも本手順書が利用可能な旨を追記 P6…モバイル移行手順書の URL を追記 P7…移行イメージ図の追加 P14…EBA へのライセンス追加時に表示されるメッセージを追加
第 5 版	2021 年 11 月 11 日	P5…サポートしている OS(エージェント)に「macOS Monterey 12.x」を追記 P42…項番 4.3(7)内の「手順 4.2.6 でエクスポートした旧ポリシー」を「手順 4.2.4 でエクスポートした旧ポリシー」に修正 P44…項番 5.1 を「EPC からダウンロードした移行用ポリシーのインポート」から「EPC からダウンロードした移行用ポリシーの割り当て」に修正し、移行用ポリシーをインポートする手順を削除(4.1.5 でインポート済みのため)
第 6 版	2022 年 1 月 13 日	P22…画面変更に伴い(2)の画像差し替え

第 7 版	2022 年 2 月 15 日	P5…ユーザーズサイトへのログイン方法の説明を修正 P6…「管理可能な CET 製品」の表からサポート終了したプログラムを削除 「サポートしている OS(エージェント)」の表の内容を最新の情報に更新
第 8 版	2022 年 2 月 25 日	P8…移行イメージの項番の修正
第 9 版	2022 年 3 月 31 日	P6…ESET Dynamic Threat Defense を ESET LiveGuard Advanced へ名前を修正 P7…認証プロキシが利用不可の仕様を追記
第 10 版	2022 年 4 月 18 日	P8…移行イメージ画像の修正
第 11 版	2022 年 6 月 7 日	P6…デバイスオーナーモードの注釈を修正
第 12 版	2022 年 6 月 16 日	P40-42、P47-48、P50…EPC の画面変更に伴い画像差し替え P52…トリガー作成の手順を追記
第 13 版	2022 年 7 月 15 日	P38…各種レポートやグループ情報のエクスポートの手順修正
第 14 版	2022 年 10 月 27 日	P6…サポートしている Android OS のバージョンを更新
第 15 版	2022 年 12 月 20 日	P18…二要素認証未サポートの記載削除
第 16 版	2022 年 12 月 27 日	P9-56…セキュリティ管理ツールのバージョン変更、EBA の画面変更に伴う画像差し替えと手順を修正
第 17 版	2024 年 1 月 4 日	p1 以降…製品名称変更に伴い資料名の変更、画像差し替えと手順を修正 p5,8…クラウド対応オプション(通常/Lite)の販売終了に伴い記載の削除

第 18 版	2024 年 7 月 16 日	P5,51…手順 5.2 はセキュリティ管理ツール V11.1 以上では実施不要な旨を追記 P8…Mobile Device Connector 販売終了について追記 P43…手順 4.2.6 にバージョン毎の操作変更点を追記
第 19 版	2024 年 8 月 7 日	P5 以降…ESET PROTECT HUB(EPH)リリースに伴い手順の追加と一部手順を修正
第 20 版	2025 年 5 月 28 日	P52 以降…クラウド型セキュリティ管理ツールの画面構成変更（メインメニューの「ポリシー」が「コンフィグレーション」に変更）に伴う、手順修正と画像差し替え
第 21 版	2025 年 6 月 25 日	P47,48…クラウド型セキュリティ管理ツールの仕様変更に伴う、文言修正と画像差し替え
第 22 版	2025 年 7 月 2 日	P9…画像差し替え(EPH の記載追加) P52…既存セキュリティ管理ツールでの作業である旨、追記と画像差し替え

内容

※手順「5.2　移行後の再グルーピング」はオンプレミス型セキュリティ管理ツール V11.1 以上をご利用の場合は実施不要です。

1. はじめに

○ 本書は、「クラウド型セキュリティ管理ツール」をご利用になるお客さま向けで、既存の「オンプレミス型セキュリティ管理ツール」から「クラウド型セキュリティ管理ツール」へ移行するための手順書となります。

○ 本書は、オンプレミス型セキュリティ管理ツール V10.1 からの移行を例に作成しております。バージョンによっては、手順や画面が異なる場合がありますのでご注意ください。

○ 本書は、本書作成時のソフトウェア及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搭載されている機能及び名称が異なっている場合があります。また本書の内容は、将来予告なく変更することがあります。

○ 本書内における名称は以下の通りです

略称	正式名称
EP	クラウド型セキュリティ管理ツール ESET PROTECT
EBA	ESET Business Account
EPH	ESET PROTECT HUB
EP on-prem	オンプレミス型セキュリティ管理ツール ESET PROTECT on-prem
EM エージェント	ESET Management エージェント
EES	ESET Endpoint Security
EEA	ESET Endpoint アンチウイルス

○ 本手順書<4.1.2>で EBA/EPH に登録するライセンス情報は、以下ユーザーズサイトで確認が可能です。
ユーザーズサイトにつきましては、以下 URL をご確認ください。

https://eset-support.canon-its.jp/faq/show/82?site_domain=business

2. 本書における構成の前提

以下の動作環境を前提として、既存セキュリティ管理ツールからクラウド型セキュリティ管理ツールへの移行する際の注意事項やフローを記載しております。

クラウド型セキュリティ管理ツール EP 動作環境

クラウド型セキュリティ管理ツール EP で管理可能な ESET 製品、サポートしている OS につきましては、以下 URL をご確認ください。

https://eset-support.canon-its.jp/faq/show/143?site_domain=business

注意事項

移行作業を始める前に以下の要件を満たしていることを確認してください。満たしていない要件がある場合は、**必ず要件を満たす環境にしてから移行作業を開始してください**。

(1) 各管理している端末では EM エージェント V9.X 以降を利用している必要があります。利用しているバージョンが古い場合は EM エージェント V9.X 以降へバージョンアップを実施ください。

※EM エージェントのバージョンアップ方法は以下の URL をご確認ください。

■クライアント端末にインストールされたエージェントをバージョンアップする方法

https://eset-support.canon-its.jp/faq/show/19162?site_domain=business

(2) クライアント端末からクラウド型セキュリティ管理ツール(EP)への接続ポートは 2222/TCP から 443/TCP に変更になります。そのため、クライアント端末から直接、またはプロキシサーバー経由で 443/TCP を用いてインターネットへ接続できる必要があります。

また、プロキシサーバーでは認証は利用できません。変更前の接続ポート(2222/TCP)は不要になりますので、ファイアウォール等で閉じていただくことを推奨いたします。

(3) 移行前の環境のデータベースに格納されている情報（コンピューター名の編集やコメント情報、各種ログ、グループ情報）は移行されません。

(4) グループ情報が移行されないため、移行後のクライアント端末は「LOST+FOUND」に追加されます。移行後に再度グルーピングを行う必要があります。
※グループについては以下の URL をご確認ください。
https://help.eset.com/protect_cloud/ja-JP/?admin_groups.html

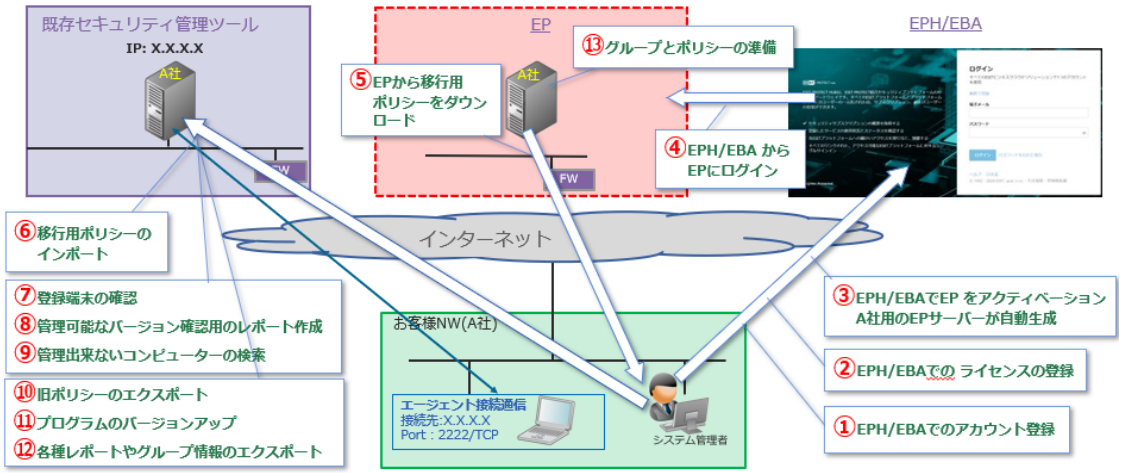
(5) モバイル端末は仕様上本手順では移行できないため、移行前の環境でモバイル管理を行っている場合は、クラウド型セキュリティ管理ツール(EP)への再登録が必要です。
移行手順につきましては、以下 EP モバイル移行手順書をご参照ください。
https://eset-info.canon-its.jp/files/user/pdf/support/cloud_conversion_mobile.pdf

(6) 移行前の環境でモバイル端末を管理している場合は、「手順 5-1」で移行用ポリシーを既存のセキュリティ管理ツールサーバー本体に適用しないでください。モバイル管理を行うコンポーネントである Mobile Device Connector がクラウド型セキュリティ管理ツール(EP)に移行されてしまうため、移行前の環境でモバイル端末を管理できなくなります。
「Mobile Device Connector」はサポート終了となっておりますのでご注意ください。
※Mobile Device Connector のサポート終了の詳細については以下の URL をご確認ください。
https://eset-support.canon-its.jp/faq/show/23588?site_domain=business

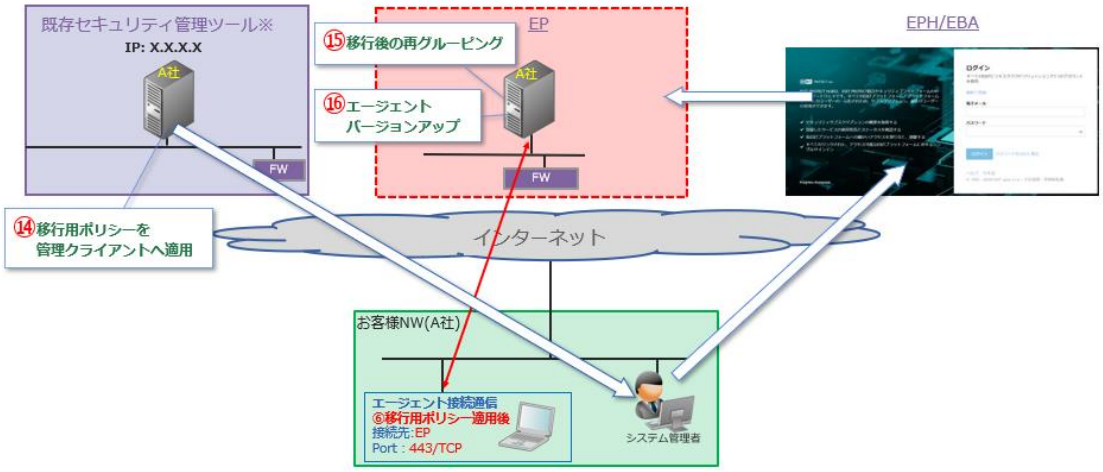
3. 既存セキュリティ管理ツールからクラウド型セキュリティ管理ツールへの移行イメージ

以下、クラウド型セキュリティ管理ツール ESET PROTECT (以降 EP)への移行イメージとなります。

既存セキュリティ管理ツールからの移行イメージ(移行準備)



既存セキュリティ管理ツールからの移行イメージ(移行)



※「⑮移行後の再グルーピング」はオンプレミス型セキュリティ管理ツール V11.1 以上をご利用の場合、実施不要です。

4. 移行前の事前準備

「既存セキュリティ管理ツール」からクラウド型セキュリティ管理ツールへの移行を実施するにあたり必要となる準備作業となります。

4.1. 事前準備 1 「EBA/EPH および EP での作業」

EPH でのアカウント作成および EBA/EPH でのライセンス登録、クラウド型セキュリティ管理ツール EP のアクティベーション等の事前作業を実施します。

※EBA アカウントをお持ちの場合は、EPH のアカウント作成は不要です。
手順 4.1.2 EBA/EPH でのライセンス登録より実施ください

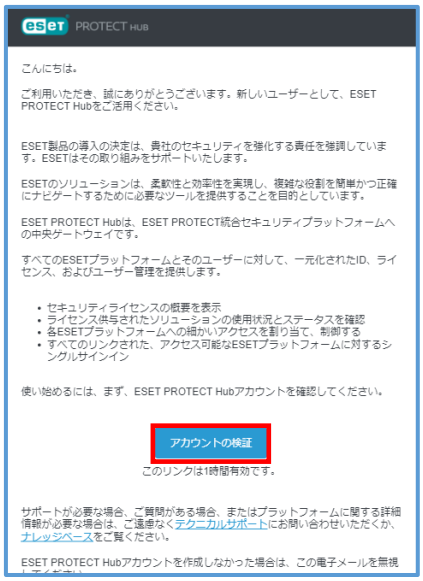
4.1.1. EPH でのアカウント登録

(1). “https://protecthub.eset.com”にアクセスします。

(2). 電子メールアドレス、会社名、会社国、captcya を入力し「アカウントの作成」をクリックします。

(3). 情報入力が完了すると以下の「確認電子メールが送信されました」の画面に遷移します。

(4). 登録したメールアドレス宛に以下のメールが受信出来ているか確認してください。受信したメール本文内の「アカウントの検証」のリンクをクリックします。なお、**リンクの有効期限は 1 時間となっておりますため、時間内にアカウントの検証を行ってください。**

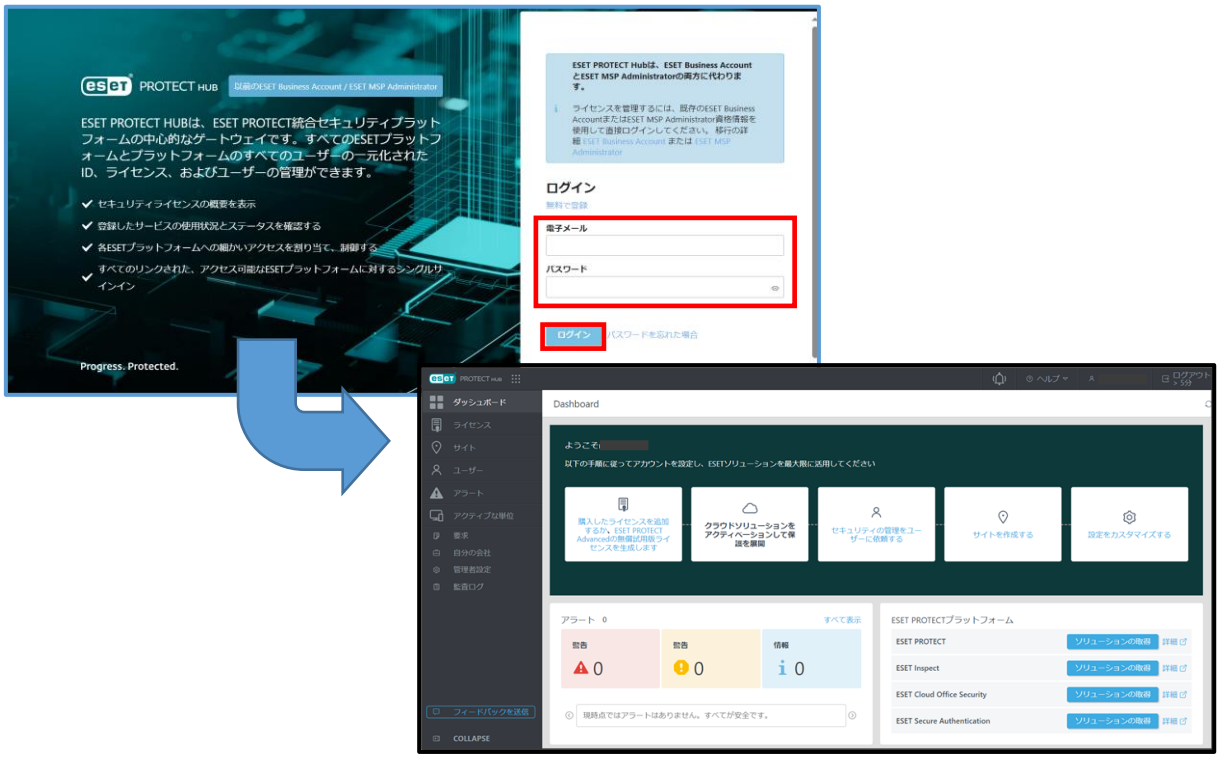


(5). (4)でアカウントの検証を行ったのち、ESET PROTECT HUB の以下の画面が出力されたら、名前(名)、名前(姓)、パスワードを入力し、「続行」をクリックしてください。

(6).ユーザーの国(国名)、言語、電話番号(任意)を入力し、「ESET に同意する」にチェックが入っていることを確認し、「アカウントをアクティベーションする」をクリックします。

(7).以下の画面が出力されるので、「ログインページに移動」をクリックします。

(8).ログイン画面が出力されたら、(2)で登録した電子メールアドレス、パスワードを入力し「ログイン」をクリックします。

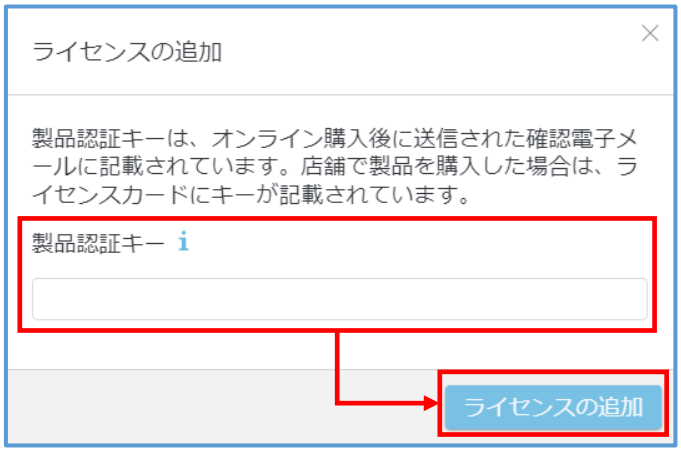


4.1.2. EBA/EPH でのライセンス登録

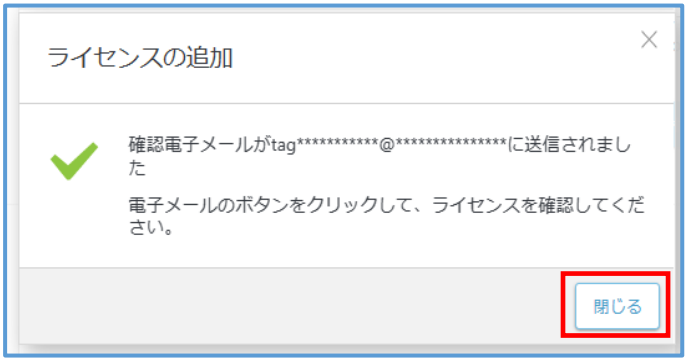
【EBA の場合】

(1).「ダッシュボード」->「最初のライセンスを追加する」をクリックします。

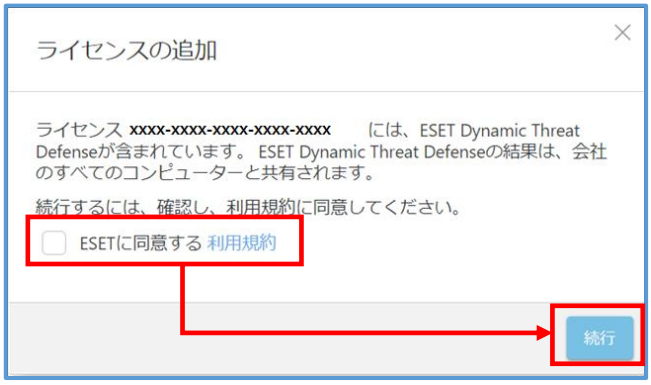
(2).製品認証キーを入力して「ライセンス追加」をクリックします。



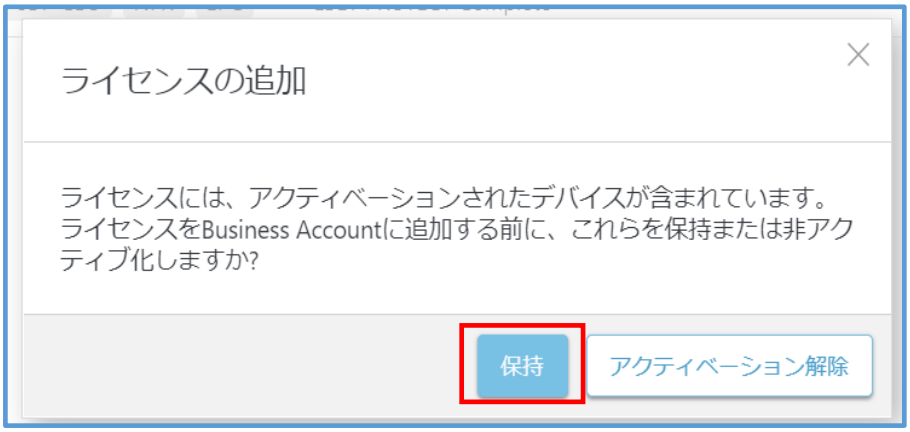
(3).「閉じる」をクリックします。



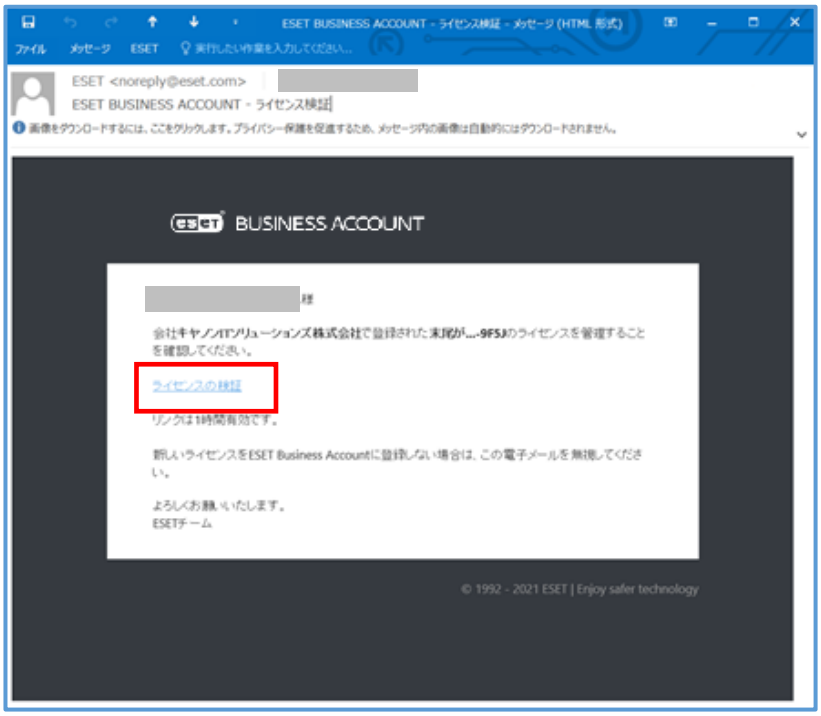
※以下のメッセージが表示された場合は「ESET に同意する」チェックをし「続行」をクリックします。同意いただかない場合ご利用いただけませんのでご注意ください。



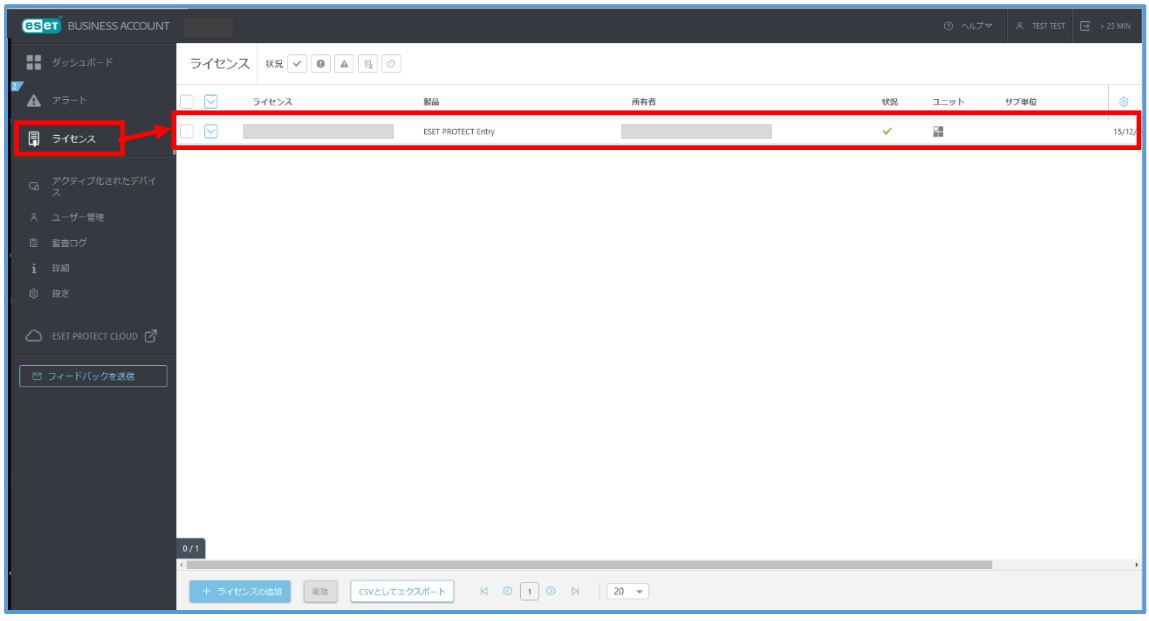
※以下のメッセージが表示された場合は**「保持」**をクリックしてください。



(4). ライセンス発行時に登録したメールアドレスに、「件名：BUSINESS ACCOUNT-ライセンス検証」が届きます。メール本文内にある、「ライセンス検証」のリンクをクリックしライセンスを有効化します。

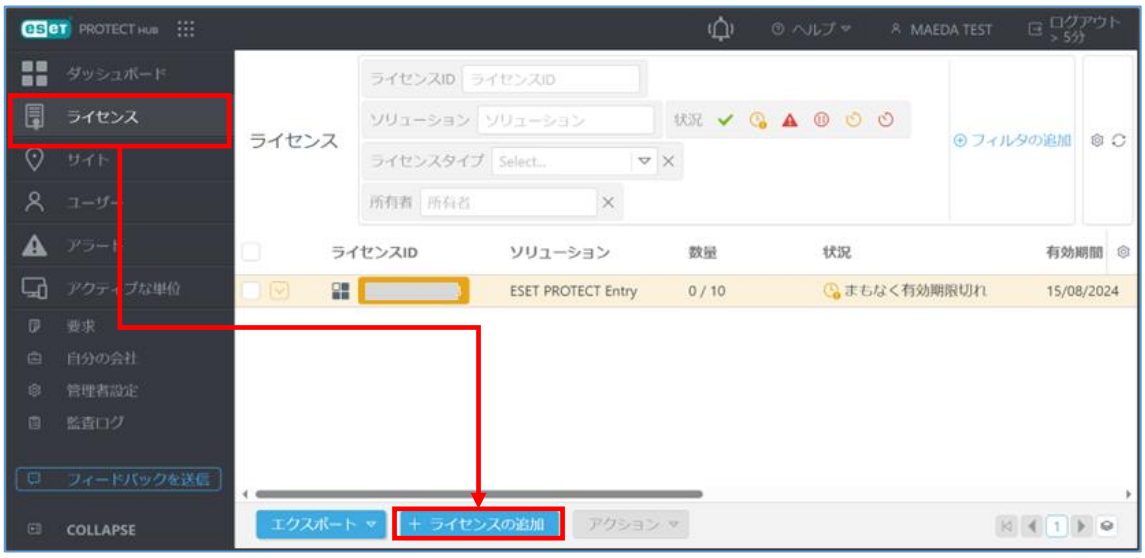


(6). (4)を実施後、EBA メインメニューの「ライセンス」をクリックします。ライセンスが追加されていれば EBA へのライセンス登録は完了です。

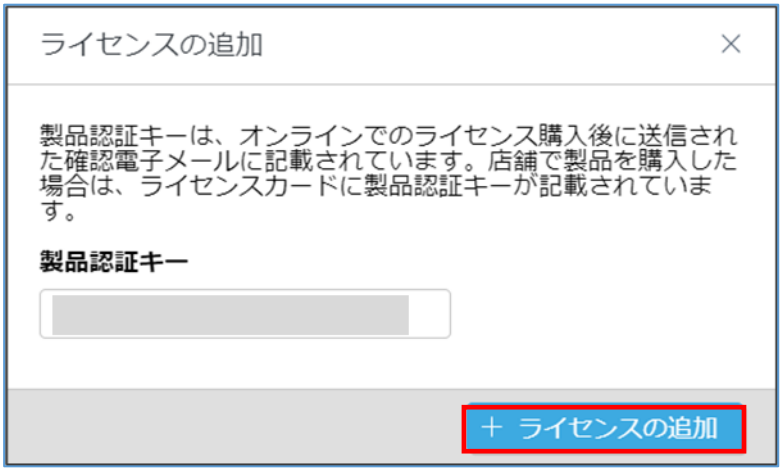


【EPH の場合】

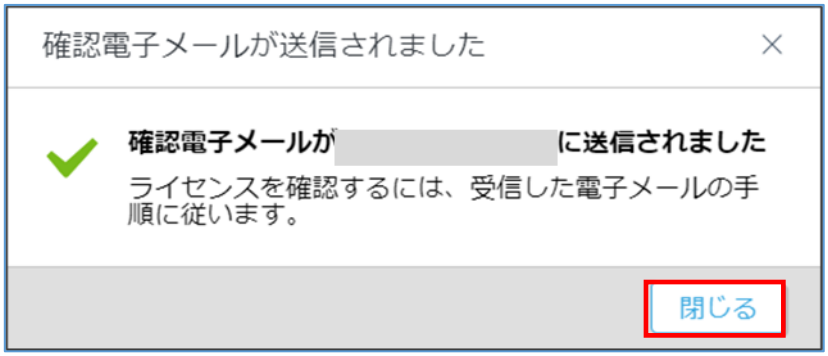
(1). 「ライセンス」->「+ライセンスの追加」をクリックします。



(2). 製品認証キーを入力して「ライセンス追加」をクリックします。

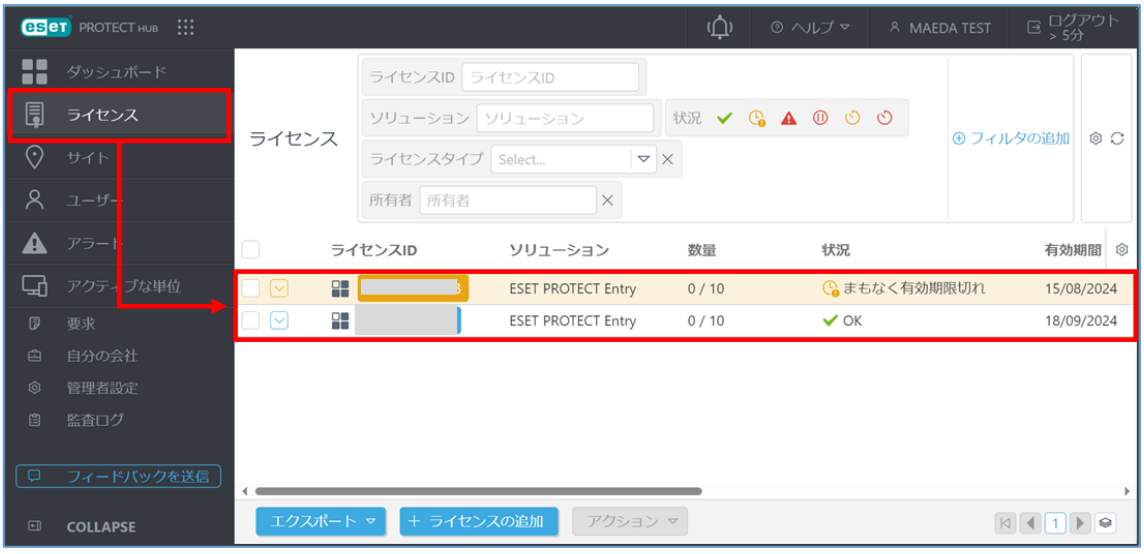


(3). 「閉じる」をクリックします。



(4).ライセンス発行時に登録したメールアドレスに、「件名：ライセンス管理の検証」が届きます。メール本文内にある、「ライセンスの検証」のリンクをクリックしライセンスを有効化します。

(5). (4)を実施後、EPH メインメニューの「ライセンス」をクリックします。ライセンスが追加されていれば EPH へのライセンス登録は完了です。

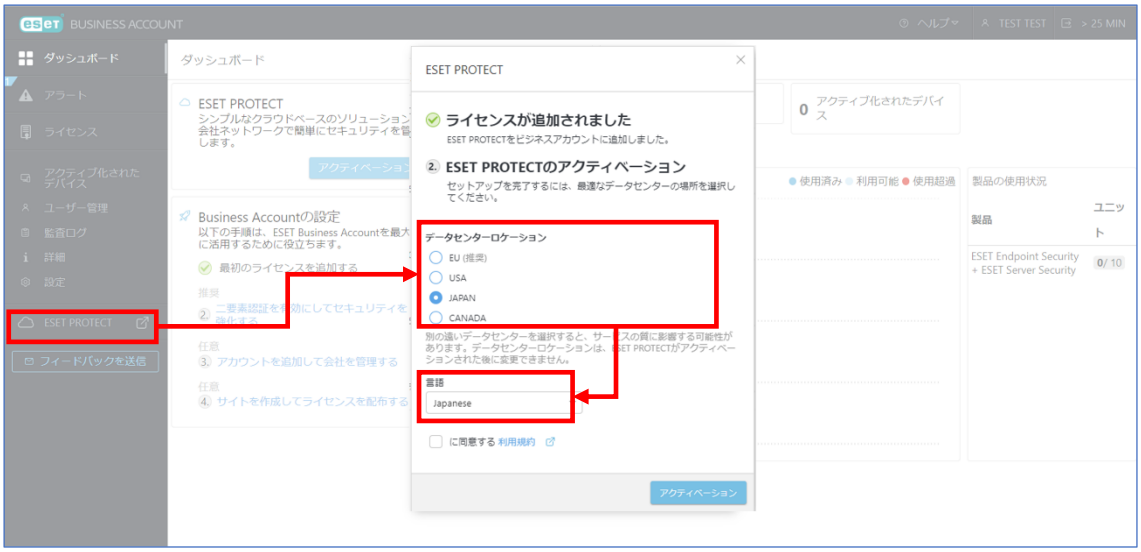


4.1.3. クラウド型セキュリティ管理ツールのアクティベーション

アクティベーションを実施し移行先であるクラウド型セキュリティ管理ツールを利用可能な状態にします。

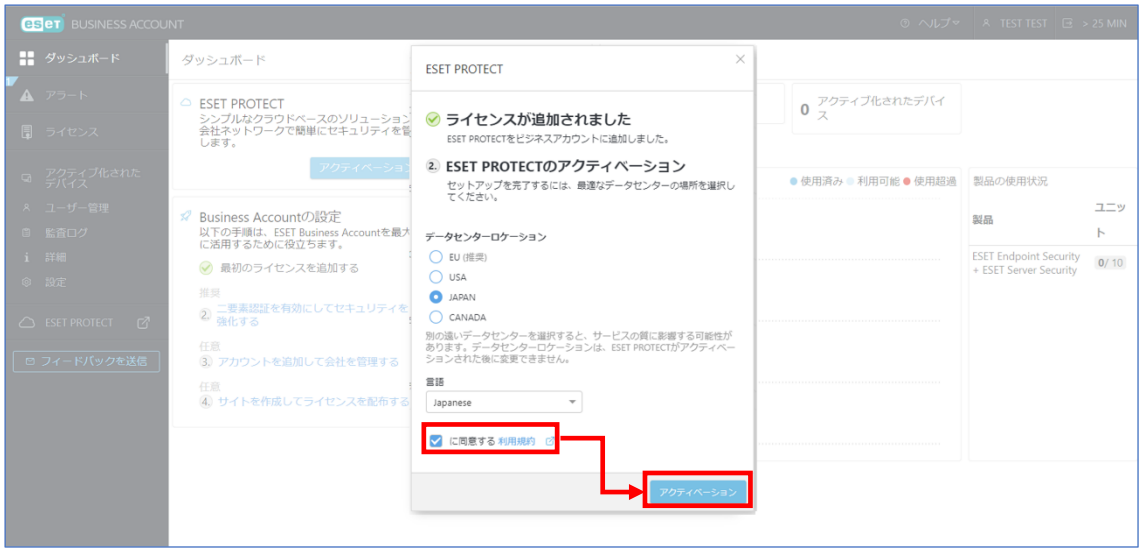
【EBA の場合】

(1). EBA のメインメニューの「ESET PROTECT」クリックします。ESET PROTECT のアクティベーション画面が表示されたら、データロケーションは**必ず「JAPAN」を選択**し、言語選択では**日本語**を選択します。

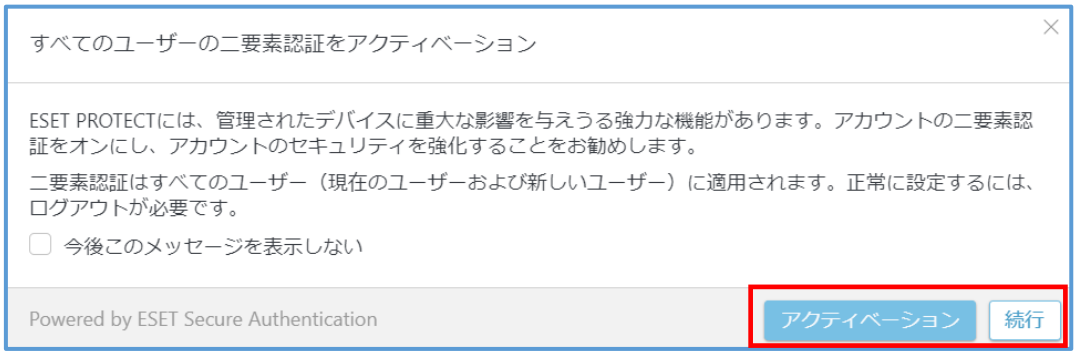


(2). 利用規約に同意して、「アクティベーション」をクリックします。

※同意いただけない場合ご利用いただけません。



(3).「すべてのユーザーの二要素認証アクティベーション」画面が出力されます。
二要素認証を利用する場合は「アクティベーション」、二要素認証を利用しない場合は「続行」をクリックします。



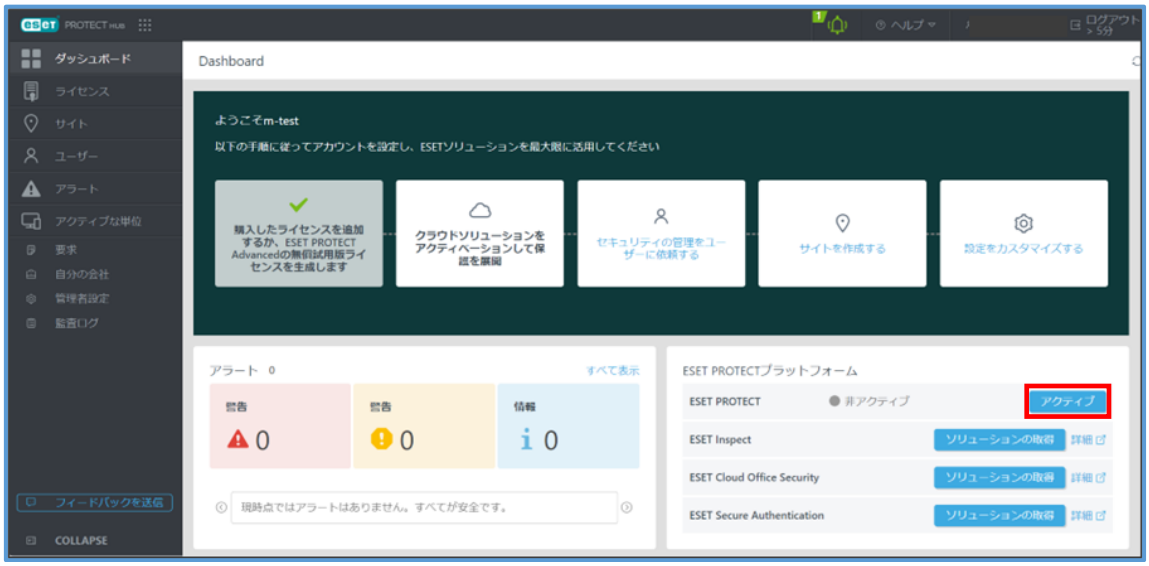
※二要素認証の詳細については以下をご確認ください。
https://help.eset.com/eba/ja-JP/two-factor-authentication.html

(4).「ESET PROTECT を設定しています…」画面が出力されます。数分間経過したのち「ESET PROTECT の準備が完了しました」画面が出力されたら、「続行」をクリックします。

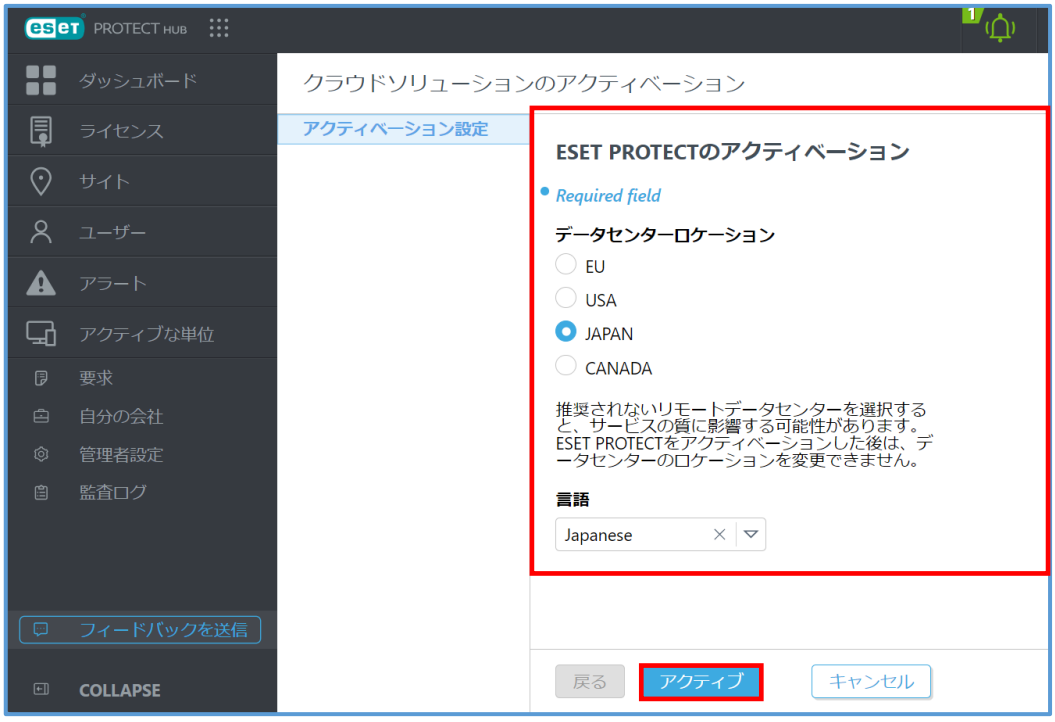
(5).「ESET PROTECT」に画面が遷移し、以下の画面が出力されましたらクラウド型セキュリティ管理ツールが利用できる状態となります。
「スキップ」をクリックすると、操作が行えます。

【EPH の場合】

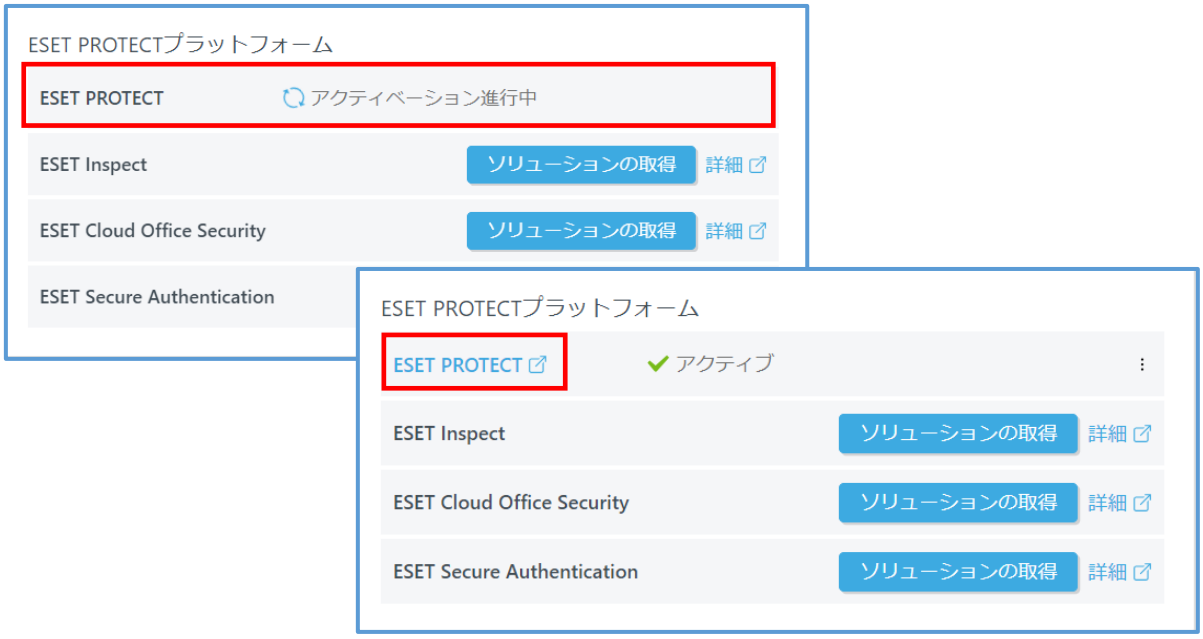
(1).EPH の画面右下の ESET PROTECT の「アクティブ」をクリックします。



(2). ESET PROTECT のアクティベーション画面が表示されたら、データロケーションは**必ず「JAPAN」を選択**し、言語選択では **JAPANESE** を選択します。



(3).「アクティベーション進行中」画面が出力されます。数分間経過したのち「アクティブ」画面が出力されたら、「ESET PROTECT」をクリックします。



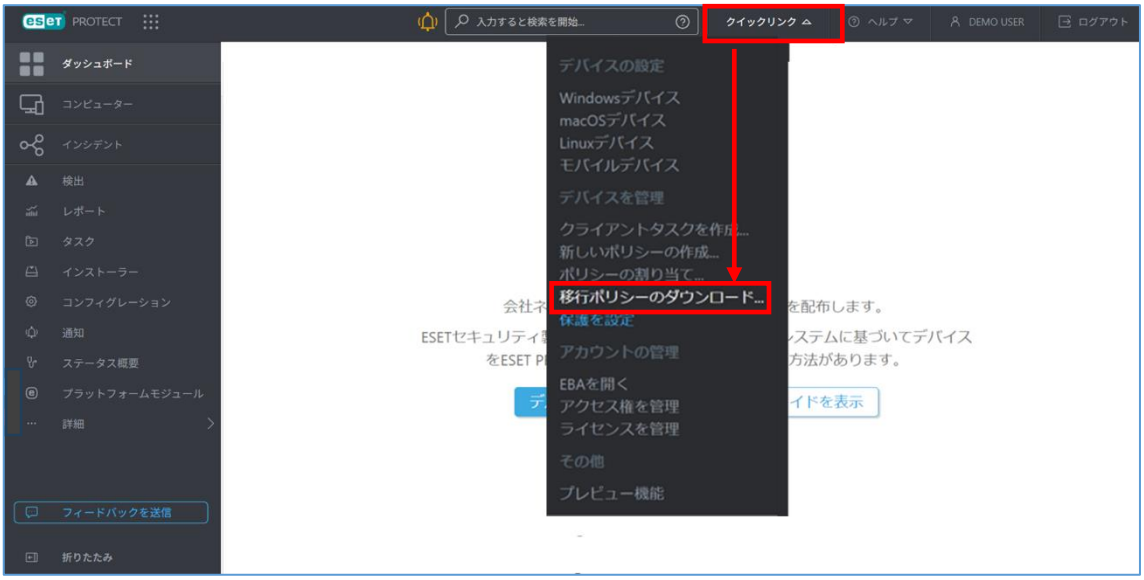
(4). 「ESET PROTECT」に画面が遷移し、以下の画面が出力されましたらクラウド型セキュリティ管理ツールが利用できる状態となります。「保護を設定」画面が表示されますが、「これ以上表示しない」または「後で確認」をクリックいただくか、設定を行い「今すぐに適用」をクリックします。

4.1.4. クラウド型セキュリティ管理ツールから移行用ポリシーをダウンロード

クラウド型セキュリティ管理ツールへの移行用ポリシーをダウンロードします。本ポリシーを既存セキュリティ管理ツールにインポートしてクライアント端末に配布することで移行が行えます。

(1). クラウド型セキュリティ管理ツールにログインします。

(2). 「クリックリンク」->「移行ポリシーのダウンロード」をクリックします。

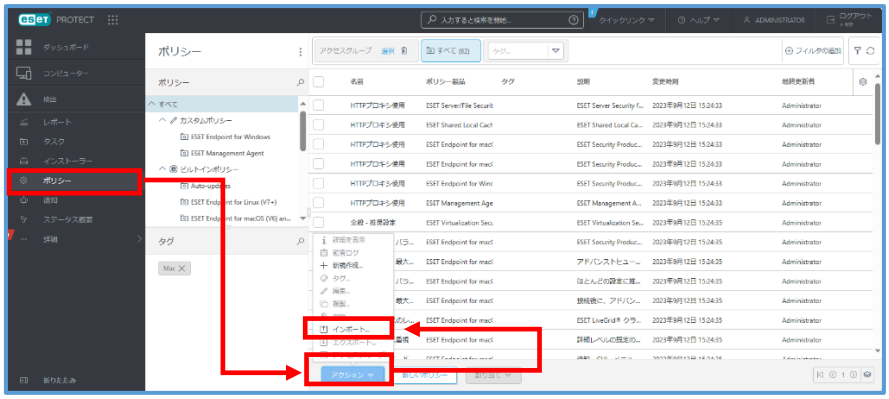


(3). ファイル名「CloudMigrationPolicy xxxx-xx-xx xx-xx-xx.dat」が作成されます。任意のフォルダに保存します。

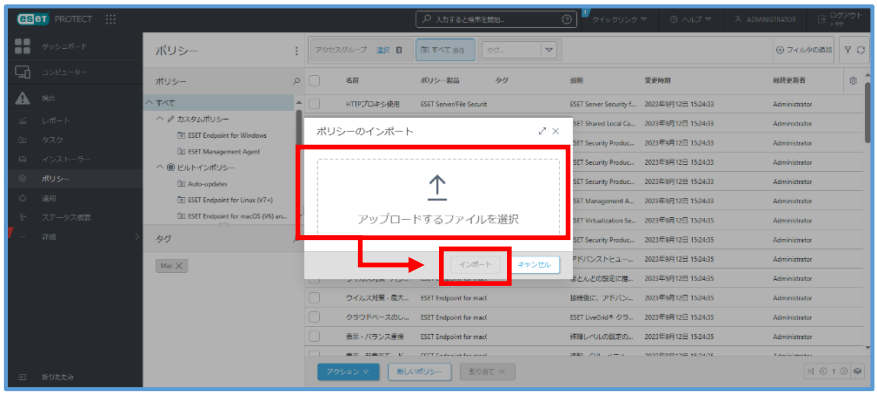
4.1.5. 移行用ポリシーのインポート

(1). 既存セキュリティ管理ツールにログインします。

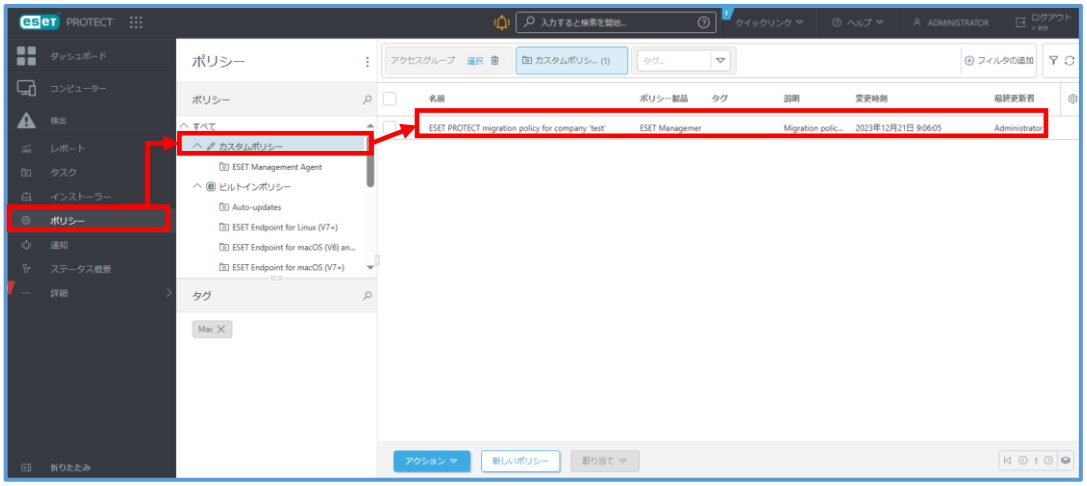
(2). メインメニューの「ポリシー」 ->「アクション」->「インポート」を選択します。



(3). ポリシーインポート画面「アップロードするファイルを選択」へ 4.1.4 でダウンロードした.dat ファイルをドラック＆ドロップし、「インポート」をクリックします。



(4). メインメニューの「ポリシー」->「カスタムポリシー」をクリックします。ポリシー一覧に、「ESET PROTECT migration policy for company “お客様名”」が追加されていることを確認してインポートは完了です。



4.2. 事前準備 2「既存セキュリティ管理ツールでの作業」

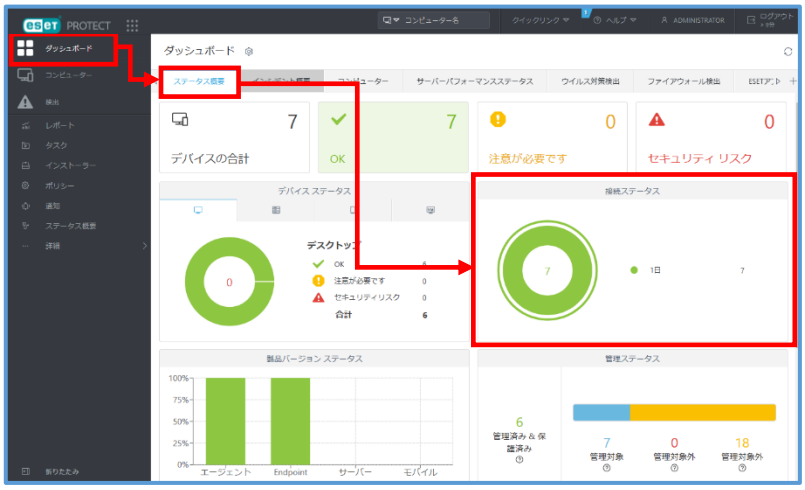
既存セキュリティ管理ツールに登録している端末数やプログラムバージョンの確認、ポリシーの設定情報確認をします。

4.2.1. 登録端末の確認

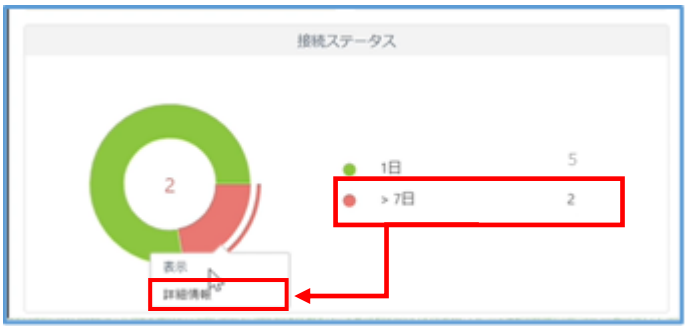
ダッシュボードの概要欄「前回の接続」で接続が無い端末の確認⇒詳細情報からレポート作成して確認⇒実際の管理数を確認

(1). 既存セキュリティ管理ツールにログインします。

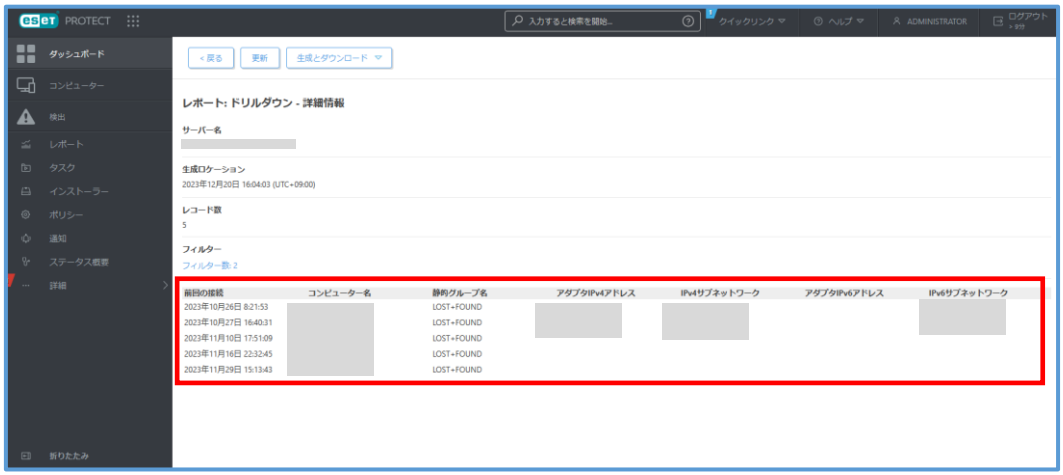
(2). メインメニュー「ダッシュボード」の「ステータス概要」タブより、「接続ステータス」を確認します。



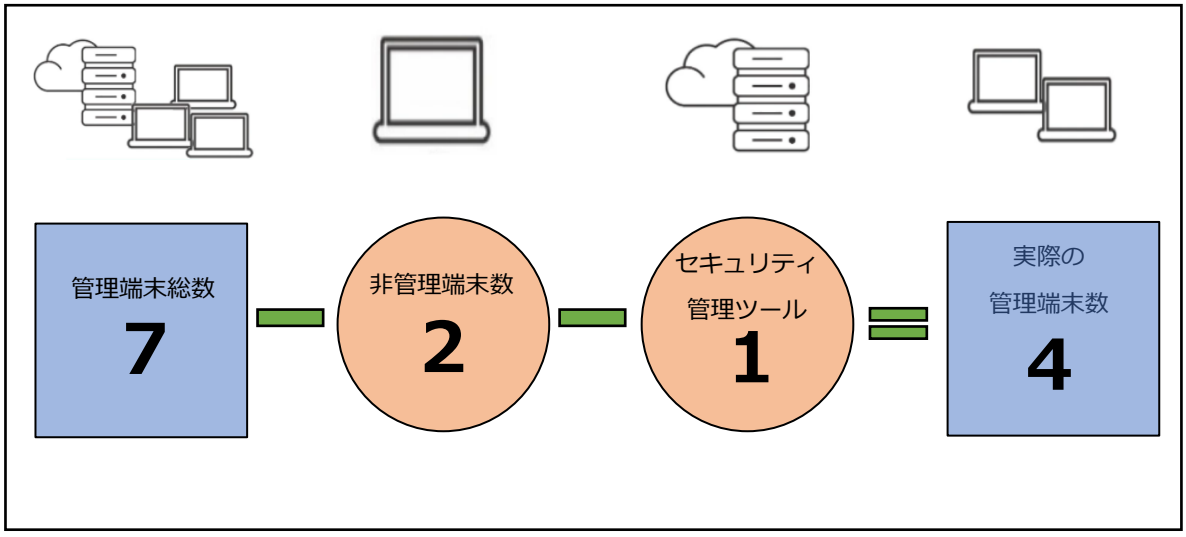
(3). 既定では 7 日間接続が無い場合赤く表示されますので、詳細情報を確認します。



(4). コンピューター名や静的グループ、IP アドレス情報などをもとに利用している PC なのか判別します。



(5). ダッシュボード「概要」で確認できるデバイスの合計と照らして実際に管理している台数を算出します。

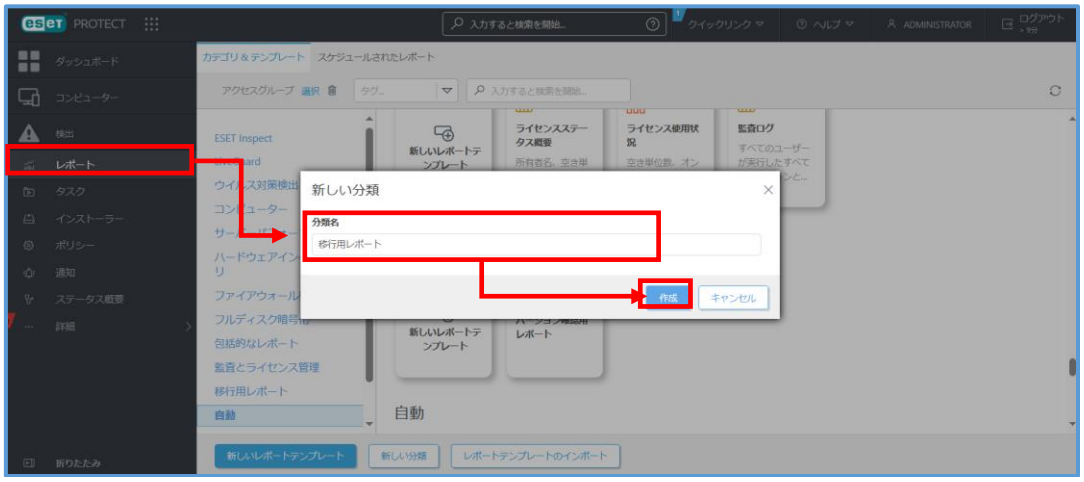


注意：もし、現在は管理していない端末のログが残っているだけの場合は、移行用ポリシーを適用してもクラウド型セキュリティ管理ツールには端末は移行されないため正確な管理数を把握しておく必要があります。ダッシュボード「概要」で確認できるデバイス数には「既存セキュリティ管理ツール本体」も含まれるためご注意ください。

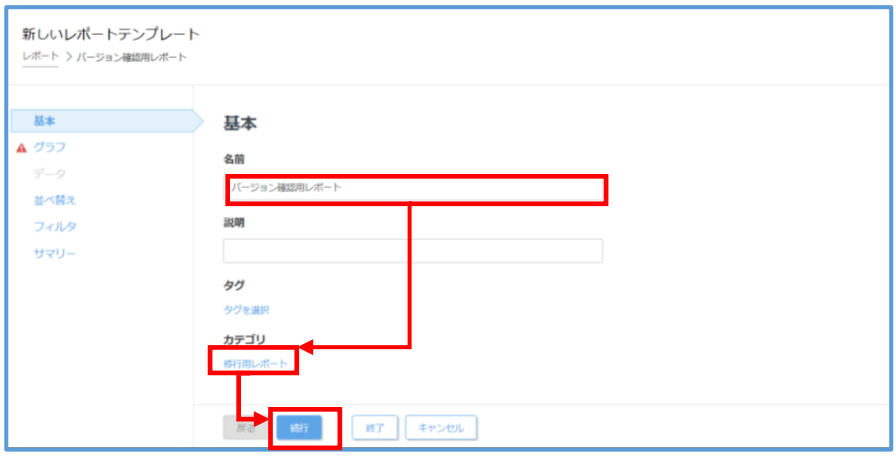
4.2.2. 管理可能なバージョン確認用のレポート作成

移行先のクラウド型セキュリティ管理ツールで管理可能なバージョンであるかを確認するために、クライアント用プログラムのバージョンを確認するレポートを作成します。

(1). メインメニュー「レポート」->「新しい分類」を任意の分類名を入力し「作成」をクリックします。

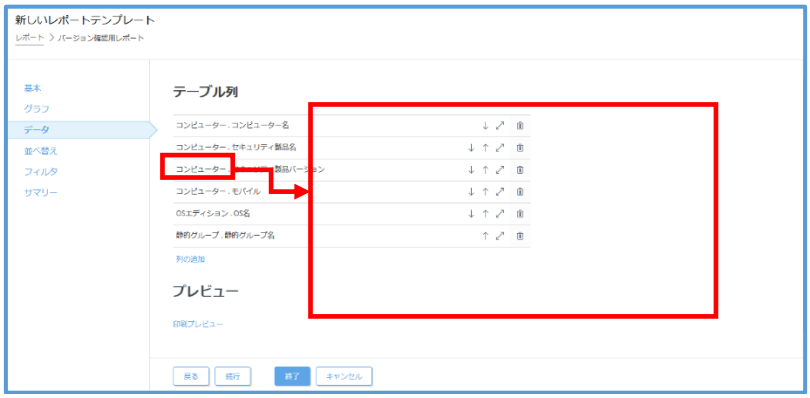


(2). 「新しいレポートテンプレート」をクリックし、「名前」にて任意の名前を入力し、(1)の「新しい分類」で作成した分類名を「カテゴリ」にて選択し、「続行」をクリックします。



(3).「グラフ」をクリックし、表示テーブルにチェックします。

(4).「データ」->「列の追加」をクリックします。以下の項目を追加して「終了」をクリックします。



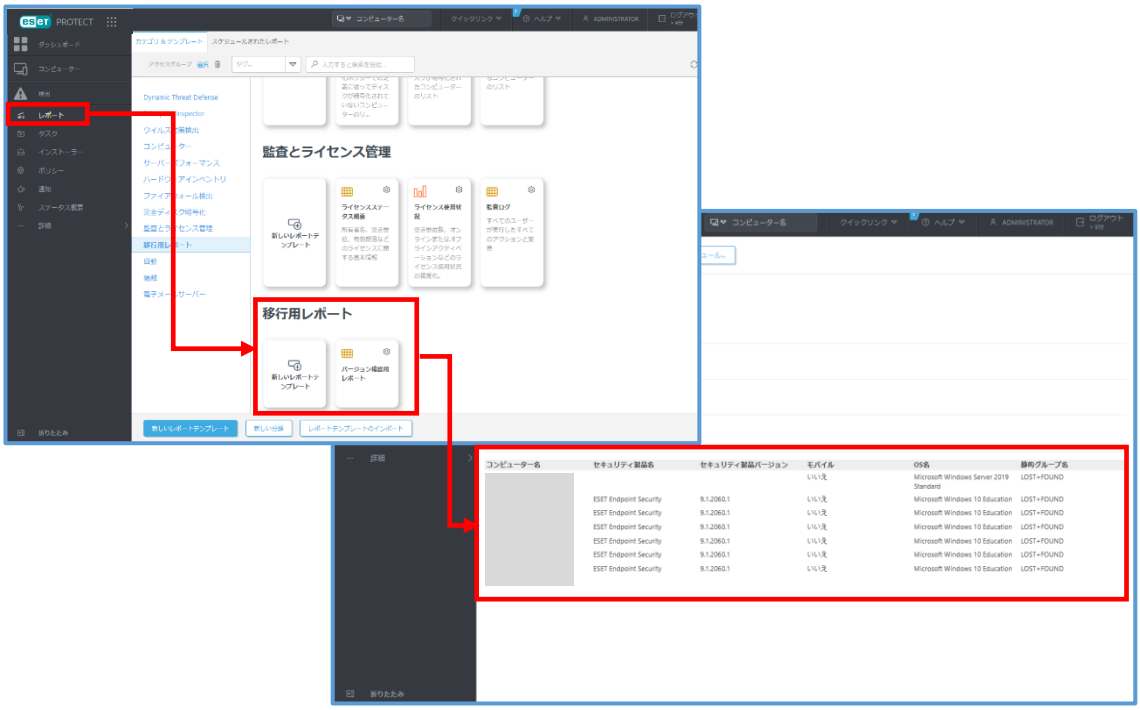
テーブル列

■コンピューター	コンピューター名
■コンピューター	セキュリティ製品名
■コンピューター	セキュリティ製品バージョン
■コンピューター	モバイル
■OS エディション	OS 名
■静的グループ	静的グループ名

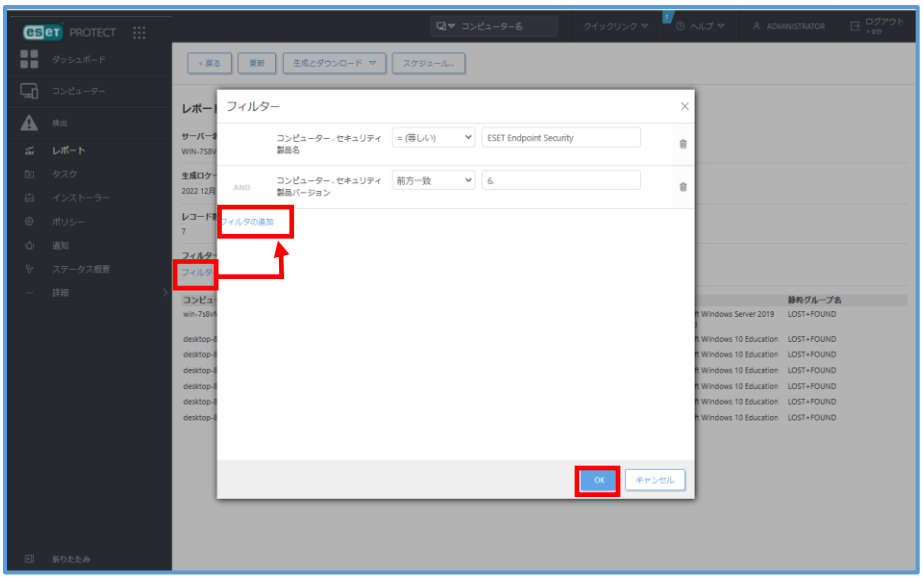
4.2.3. 管理できないコンピューターの検索

4.2.2 で作成したレポートを使用して、各プログラムがクラウド型セキュリティ管理ツールで管理可能なバージョンか確認します。

(1). まずクライアント用プログラムが管理可能かどうかを確認するため、「作成したレポート」をクリックし、移行用レポートを表示させます。



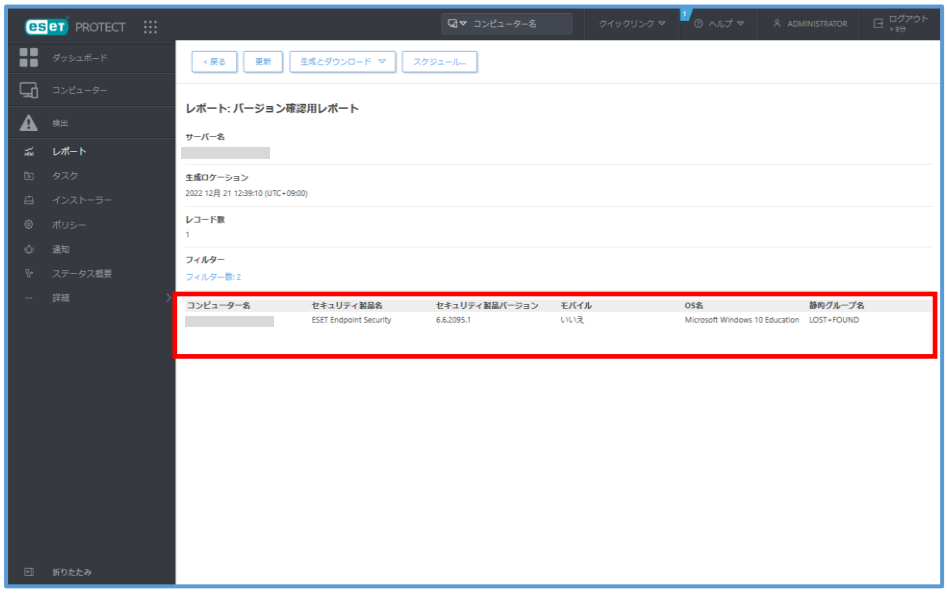
(2).「フィルターなし」->「フィルタの追加」をクリックします。以下、フィルタ項目を設定して「OK」をクリックします。



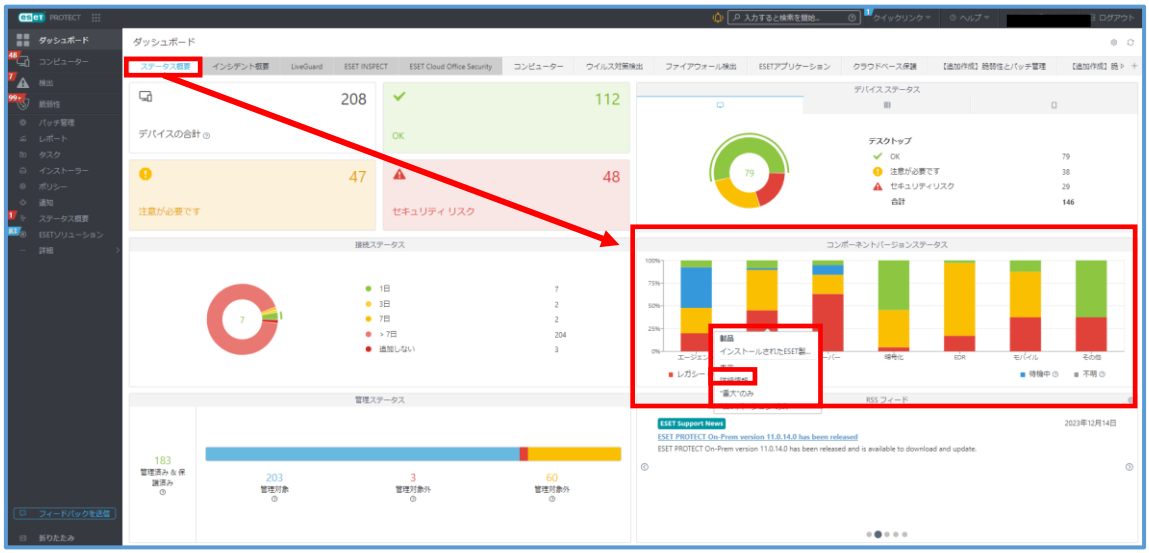
フィルタ値（例として ESET Endpoint Security V6 以下を検索します）

■コンピューター	セキュリティ製品名	=(等しい)	任意のプログラム名 例）**ESET Endpoint Security**
■コンピューター	セキュリティ製品バージョン	前方一致	プログラムのメジャーバージョン 例）**6.**

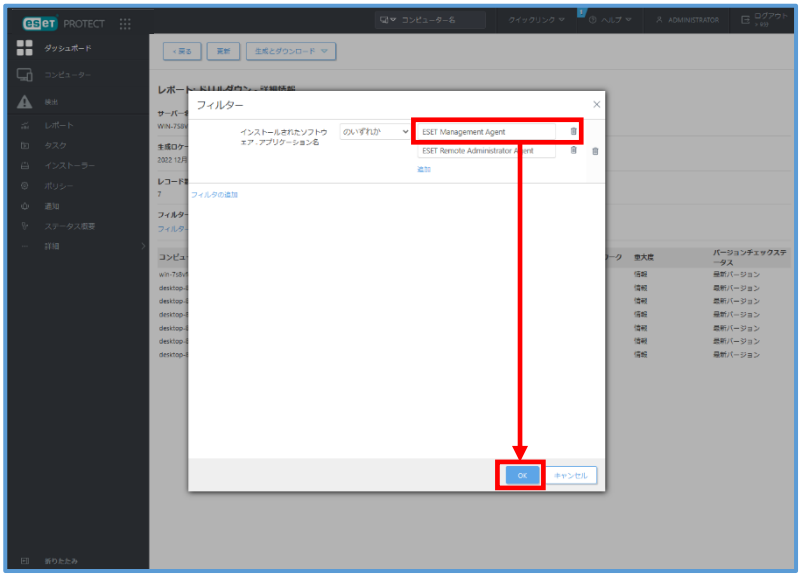
(3). 結果を確認します。



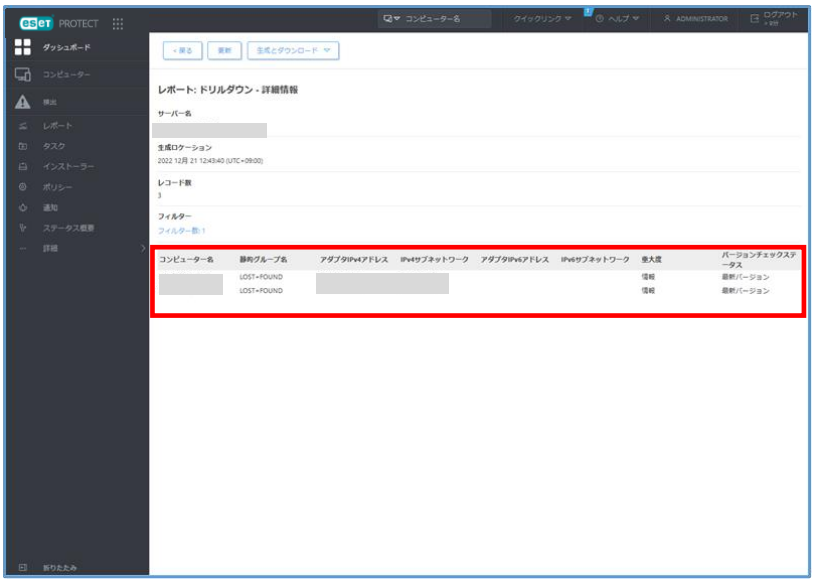
(4). 次に、エージェントがクラウド型セキュリティ管理ツールで管理可能なバージョンかどうか確認するため、ダッシュボード「ステータス概要」の「コンポーネントバージョンステータス」から「詳細情報」をクリックします。



(5). 「フィルタ」が表示されたら、「ESET Management Agent」を削除します。



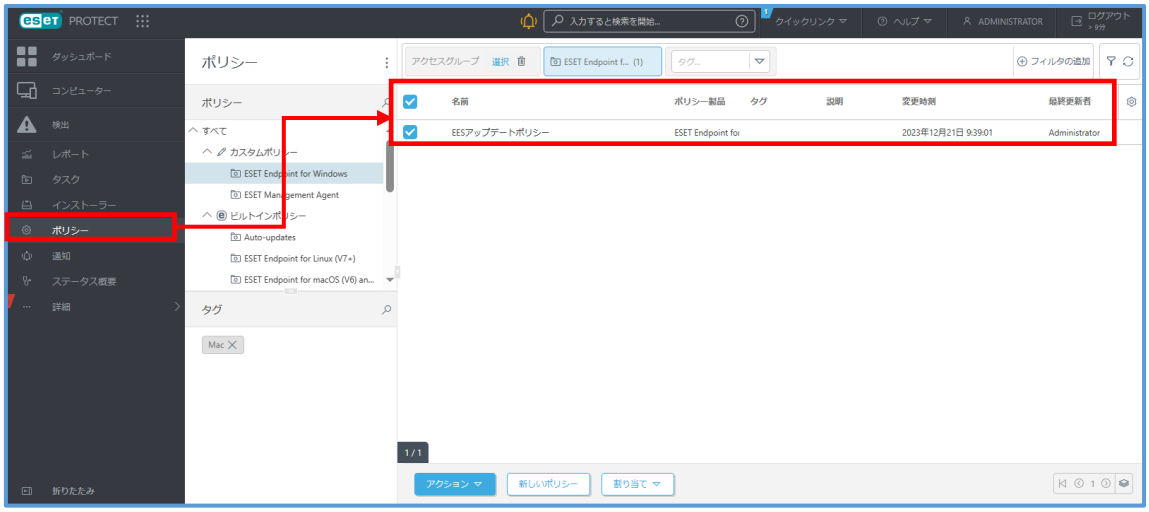
(6). 管理端末内にクラウド型セキュリティ管理ツールでは管理できない ESET Remote Administrator Agent V6 がインストールされている場合は、以下のように表示されます。



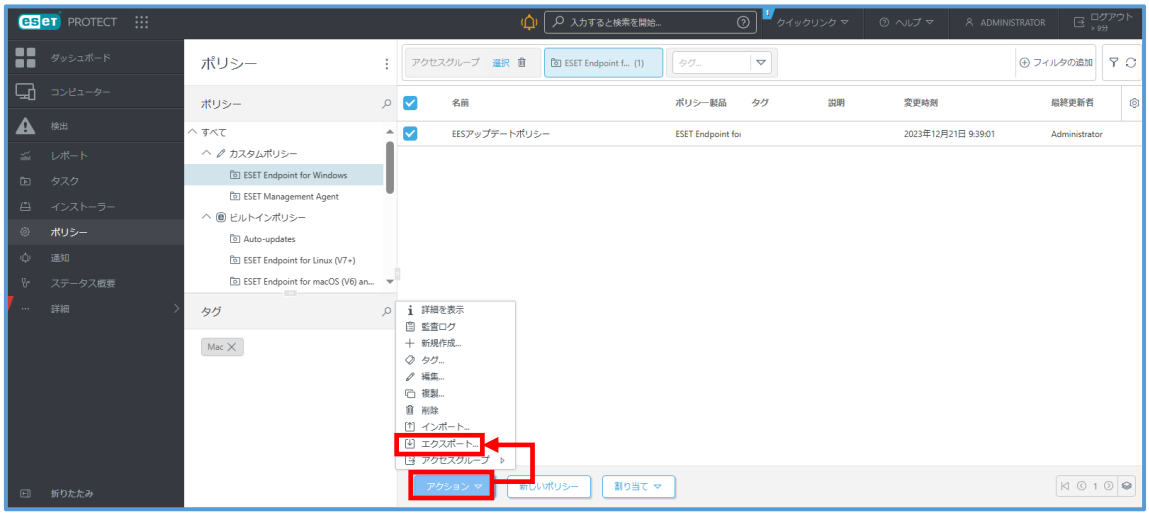
4.2.4. 旧ポリシーのエクスポート

既存セキュリティ管理ツールで使用していた旧ポリシーのエクスポートをします。本手順でエクスポートした旧ポリシーはクラウド型セキュリティ管理ツールにインポートすることで再利用可能です。

(1). メインメニュー「ポリシー」より既存セキュリティ管理ツールで利用していたポリシーのチェックボックスを選択します。



(2). 「アクション」->「エクスポート」をクリックします。



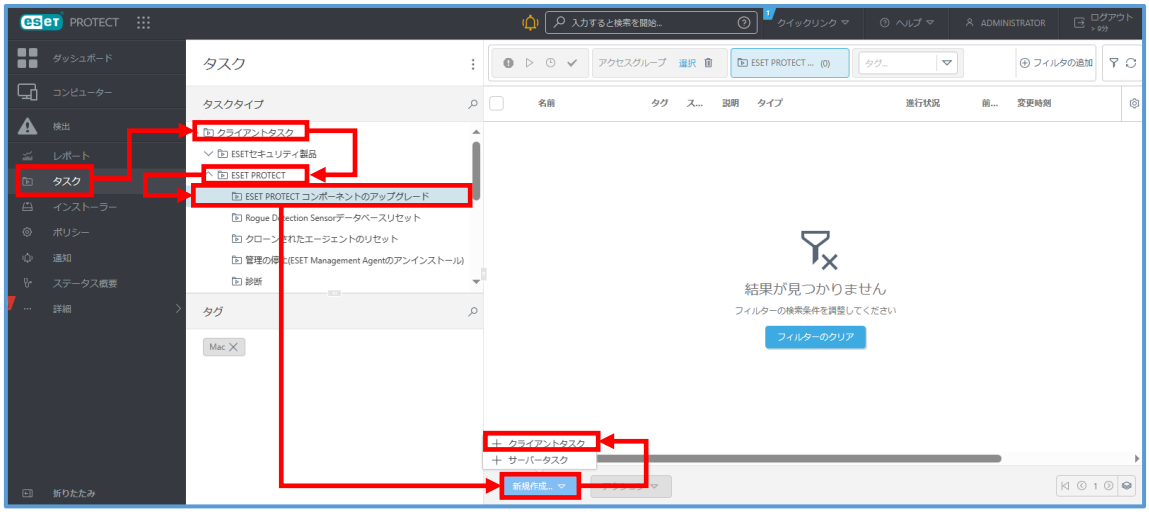
注意：クラウド型セキュリティ管理ツールでは EM エージェントのポリシーは異なるため、既存セキュリティ管理ツールからエクスポートする必要はありません。

4.2.5. プログラムのバージョンアップ

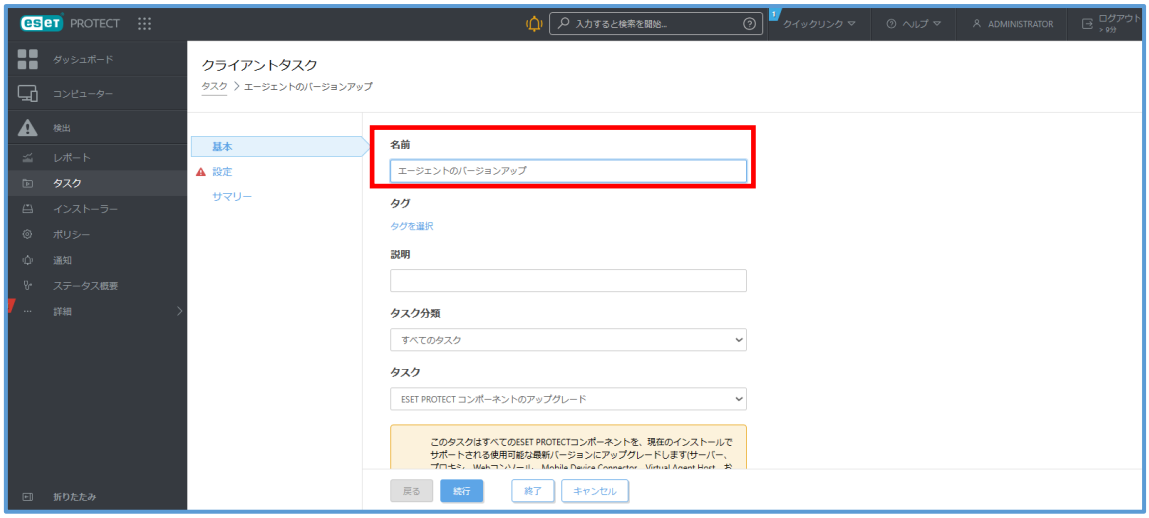
クラウド型セキュリティ管理ツールで管理出来ないプログラムが見つかった場合、プログラムのバージョンアップを行います。

(1). エージェントのバージョンアップを行う場合

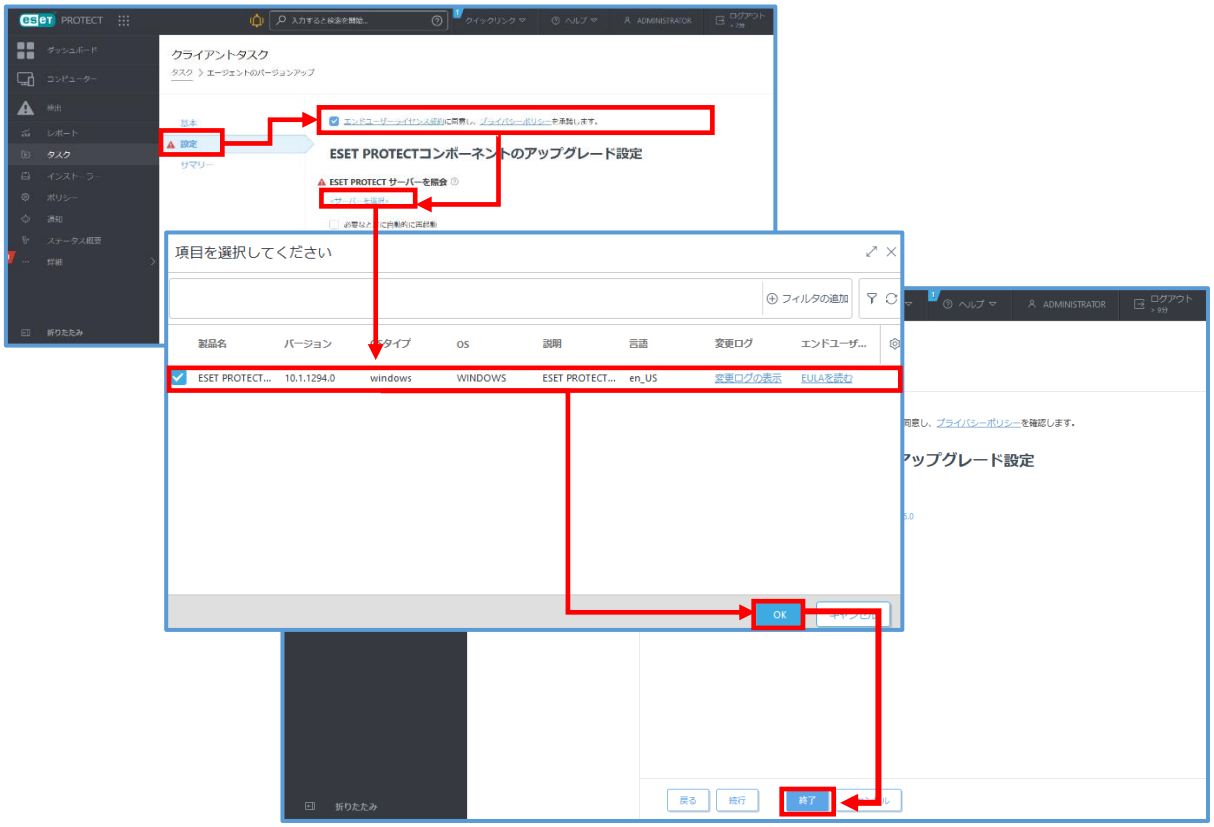
① メインメニュー「タスク」-> タスクタイプ「クライアントタスク」-> 「ESET PROTECT」-> 「ESET PROTECT コンポーネントのアップグレード」を選択し、「新規作成」-> 「クライアントタスク」をクリックします。



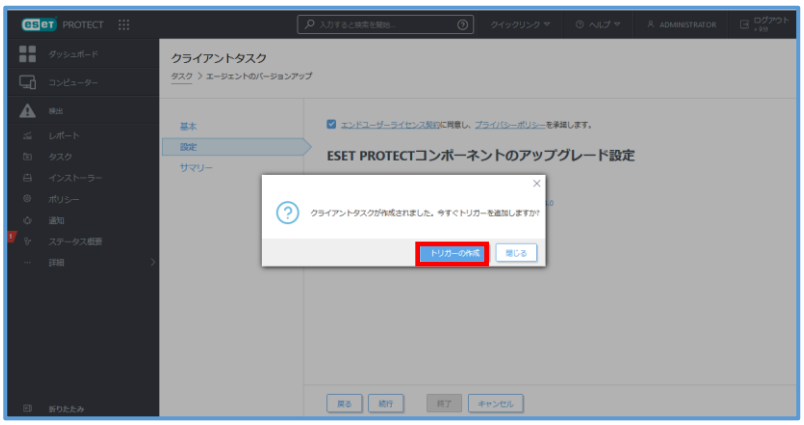
② クライアントタスクでは「名前」任意の名前を入力します。



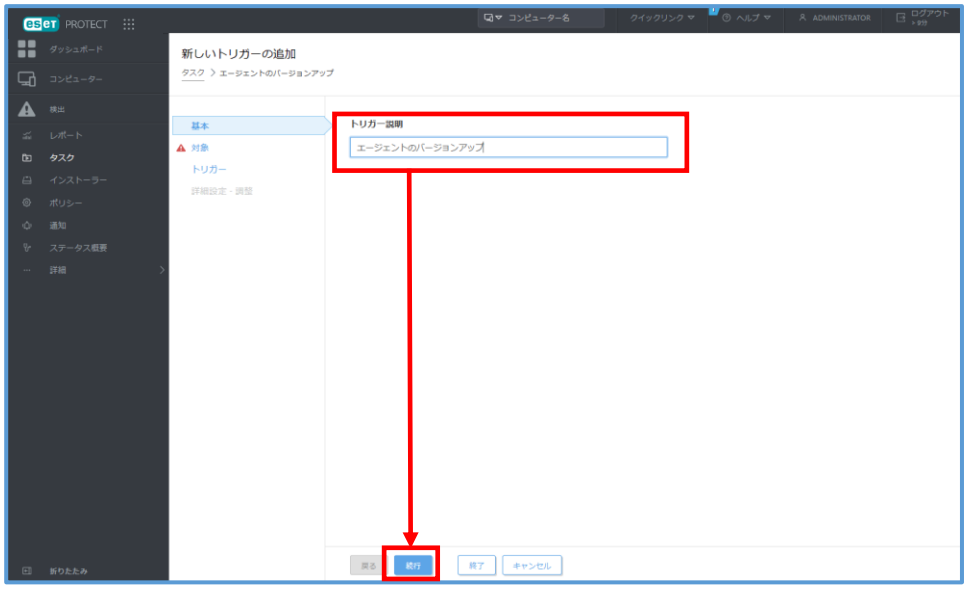
③　「設定」->「エンドユーザーライセンス契約に同意し、プライバシーポリシーを承諾します。」をチェックします。
「サーバー選択」をクリックし、既存セキュリティ管理ツールと同じバージョンを選択して「OK」->「終了」とクリックします。
※以下画像は例として V10.1 を選択しています。



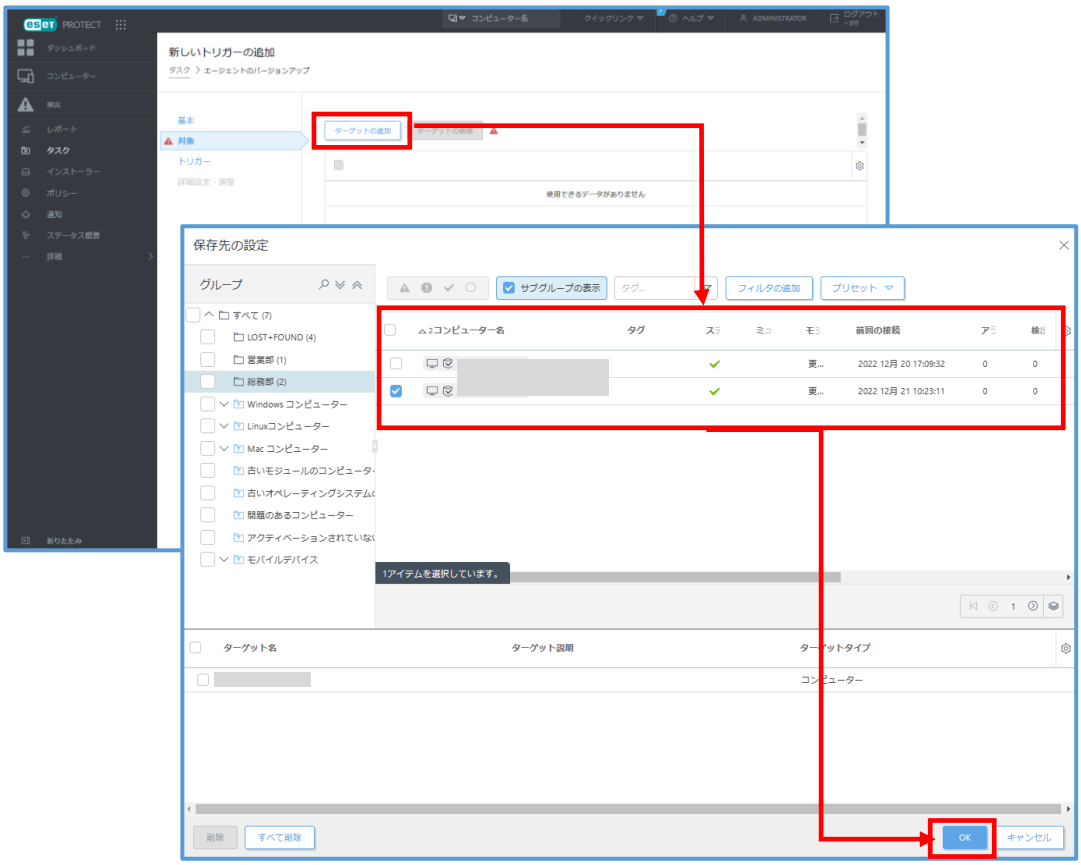
④　「トリガーの作成」をクリックします。



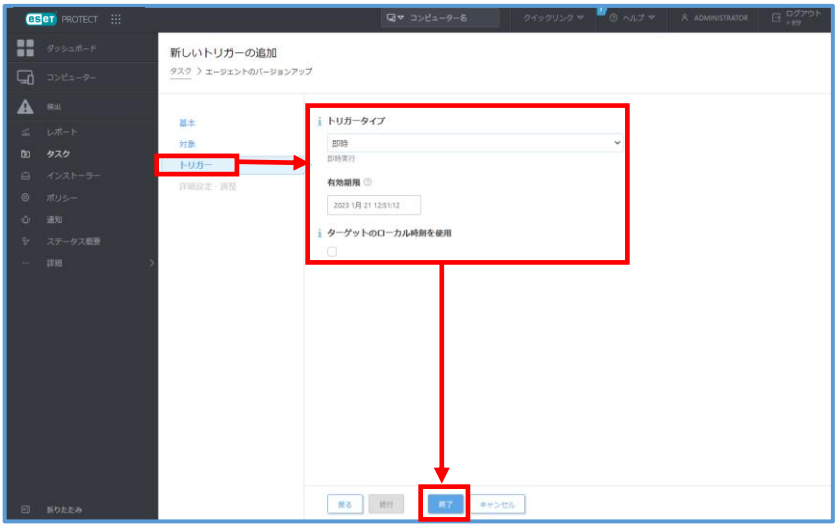
⑤　トリガー説明に任意の説明を入力し、「続行」をクリックします。



⑥　「コンピューターの追加」をクリックし、エージェントのバージョンアップを行うコンピューターを追加して「OK」をクリックします。



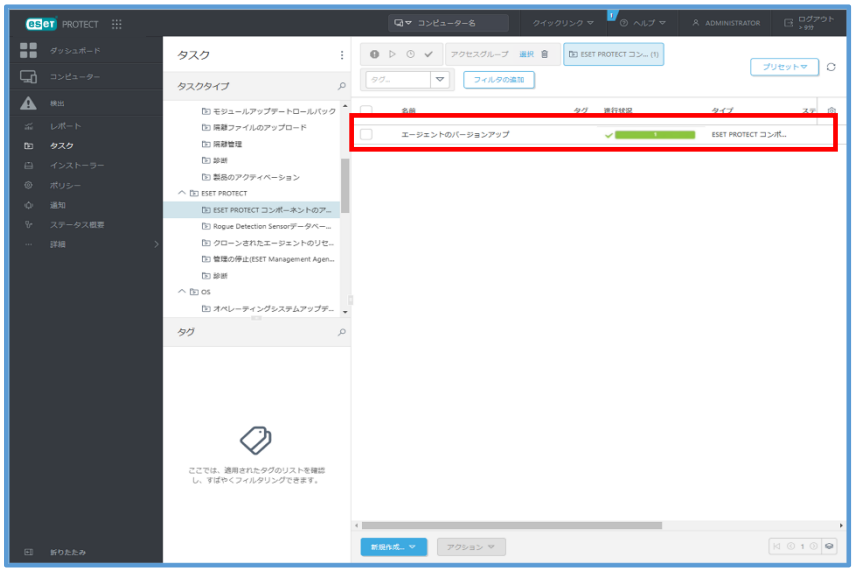
⑦　「トリガー」をクリックします。設定値(*1)は以下の通り設定し「終了」をクリックします。



設定値(*1)

トリガータイプ	デフォルトのまま（即時）
有効期限	デフォルトのまま
ローカル時刻を使用	デフォルトのまま

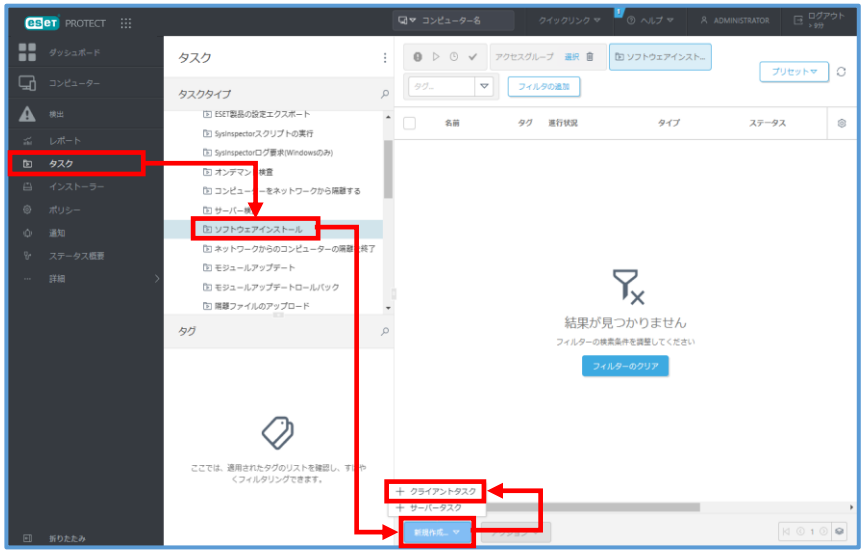
⑧　ステータスバーが緑（成功）になったことを確認します。



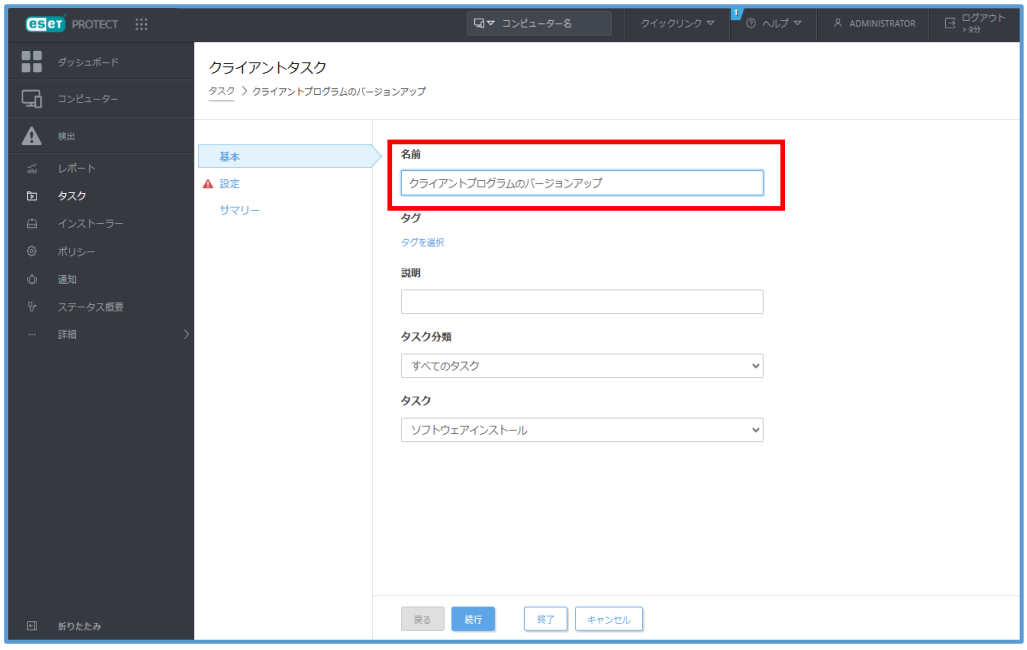
※クライアント端末が、既存セキュリティ管理ツールに接続してタスクが実行されるまで時間がかかる場合があります。

(2). クライアント用プログラムのバージョンアップの場合

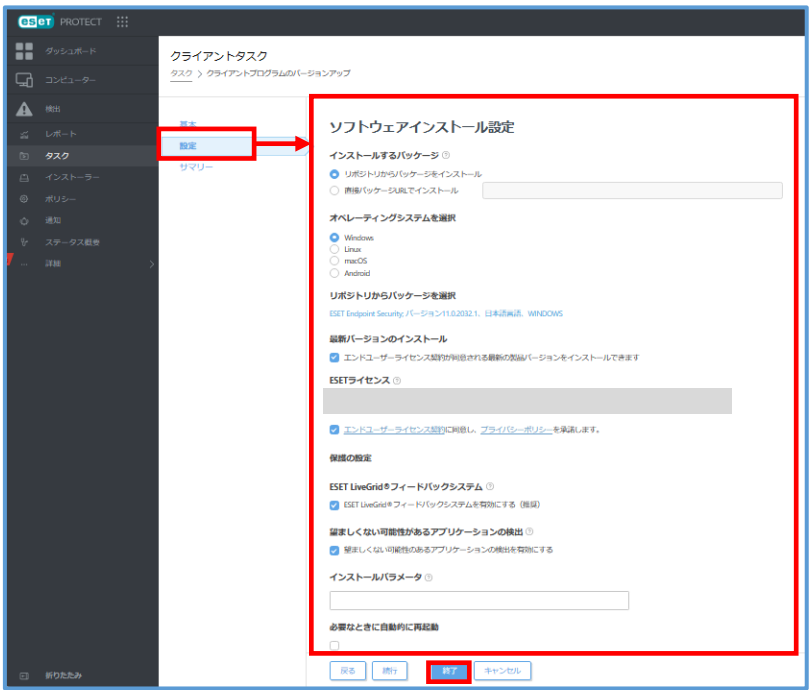
① メインメニュー「タスク」->タスクタイプ「クライアントタスク」->「ESET セキュリティ製品」->「ソフトウェアインストール」を選択し、「新規作成」->「クライアントタスク」をクリックします。



② 「基本」では任意の名前を設定します。



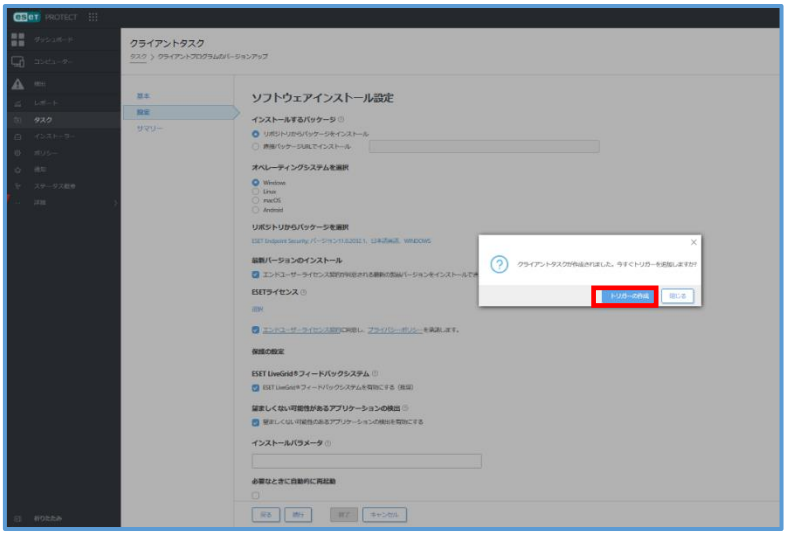
③ 「設定」をクリックします。以下の設定値(*1)を選択し「終了」をクリックします。



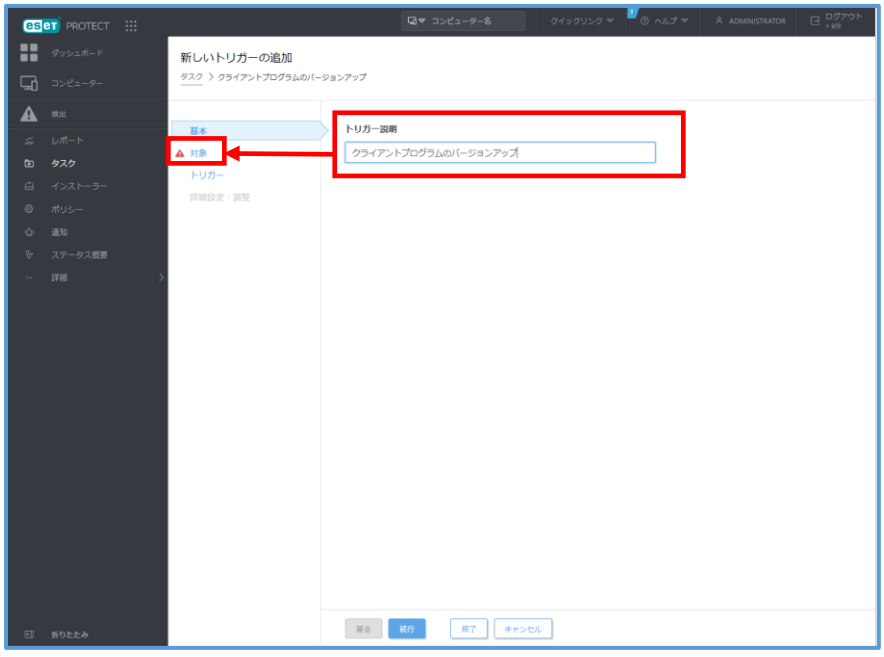
設定値(*1)

インストールするパッケージ	「リポジトリからパッケージをインストール」を選択
オペレーティングシステムを選択	バージョンアップを行うプログラムのオペレーティングシステムを選択
リポジトリからパッケージを選択	バージョンアップを行うプログラムとバージョンを選択 ※画像は EES V11.0 を選択した例です
ESET ライセンス	利用するライセンスを選択
エンドユーザー使用許諾の契約条項	ラジオボタンを ON にする
インストールパラメータ	デフォルトのまま
必要なときに自動的に再起動	デフォルトのまま ※クライアント用プログラムをバージョンアップした場合は端末で再起動が必要になるため、任意で設定してください

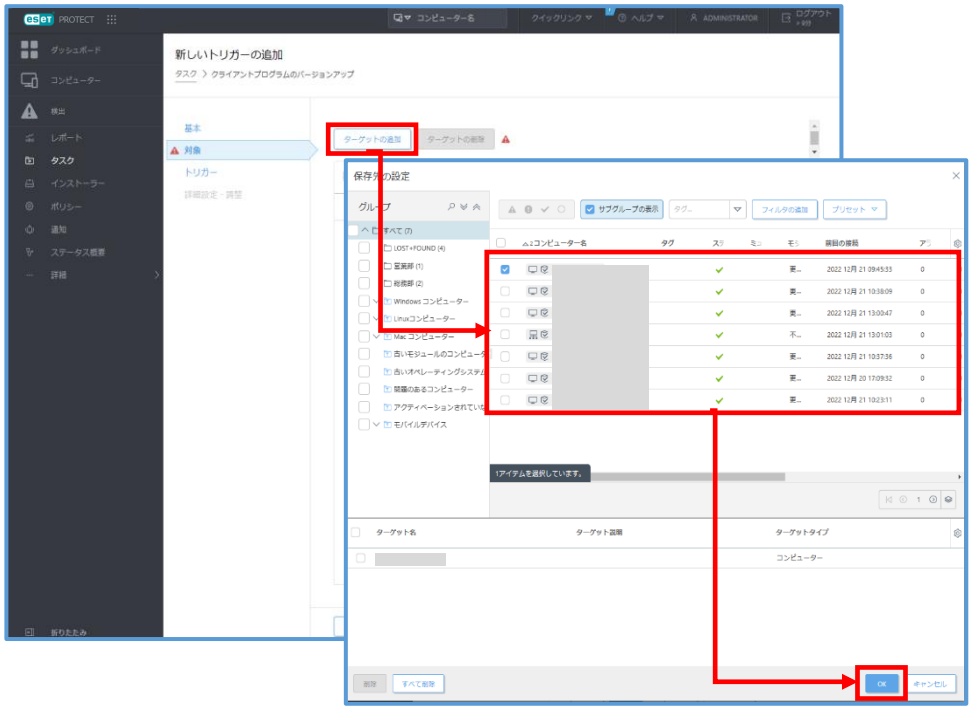
④　「トリガーの作成」をクリックします。



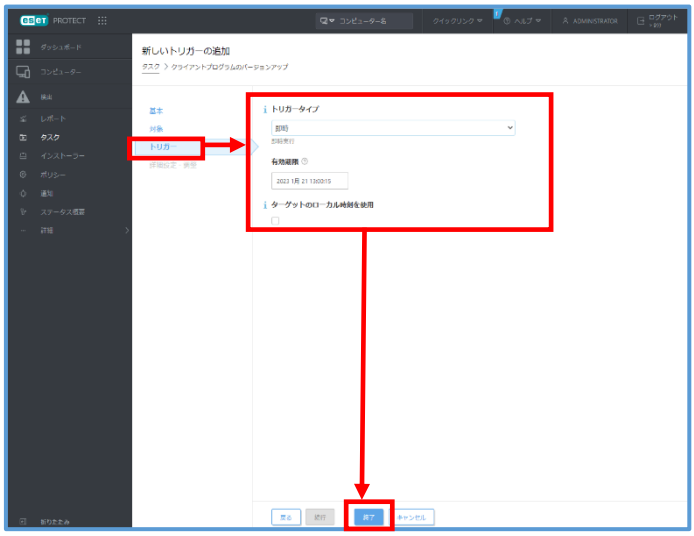
⑤　トリガー説明に任意の説明を入力し、「対象」をクリックします。



⑥　「ターゲットの追加」よりバージョンアップを行うコンピューターを選択して「OK」をクリックします。



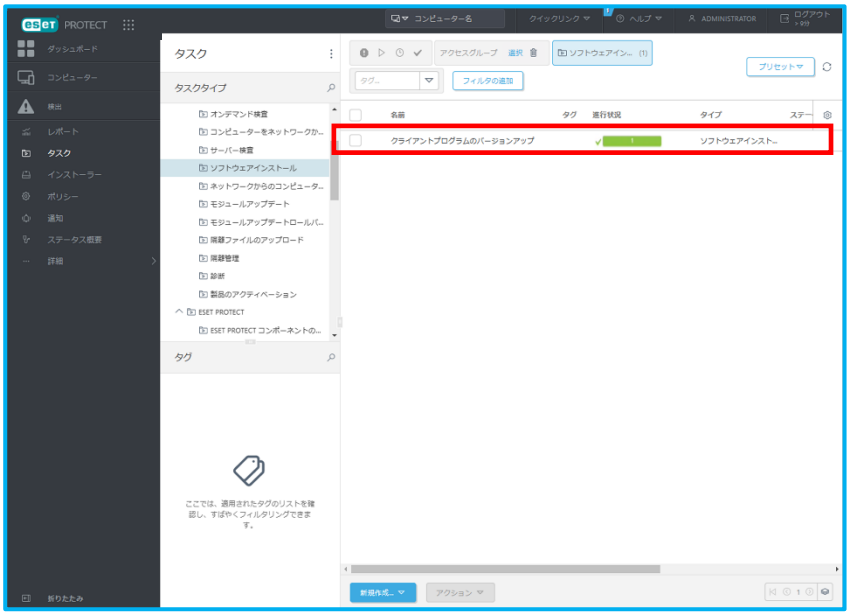
⑦　「トリガー」をクリックします。設定は以下の通り設定し「終了」をクリックします。



設定値(*1)

トリガータイプ	デフォルトのまま（即時）
有効期限	デフォルトのまま
ターゲットのローカル時刻を使用	デフォルトのまま

⑧　ステータスバーが緑（成功）になったことを確認します



注意：バージョンアップ後はクライアント端末での再起動が必要なため、再起動完了までセキュリティ管理ツールでアラートが表示されます。

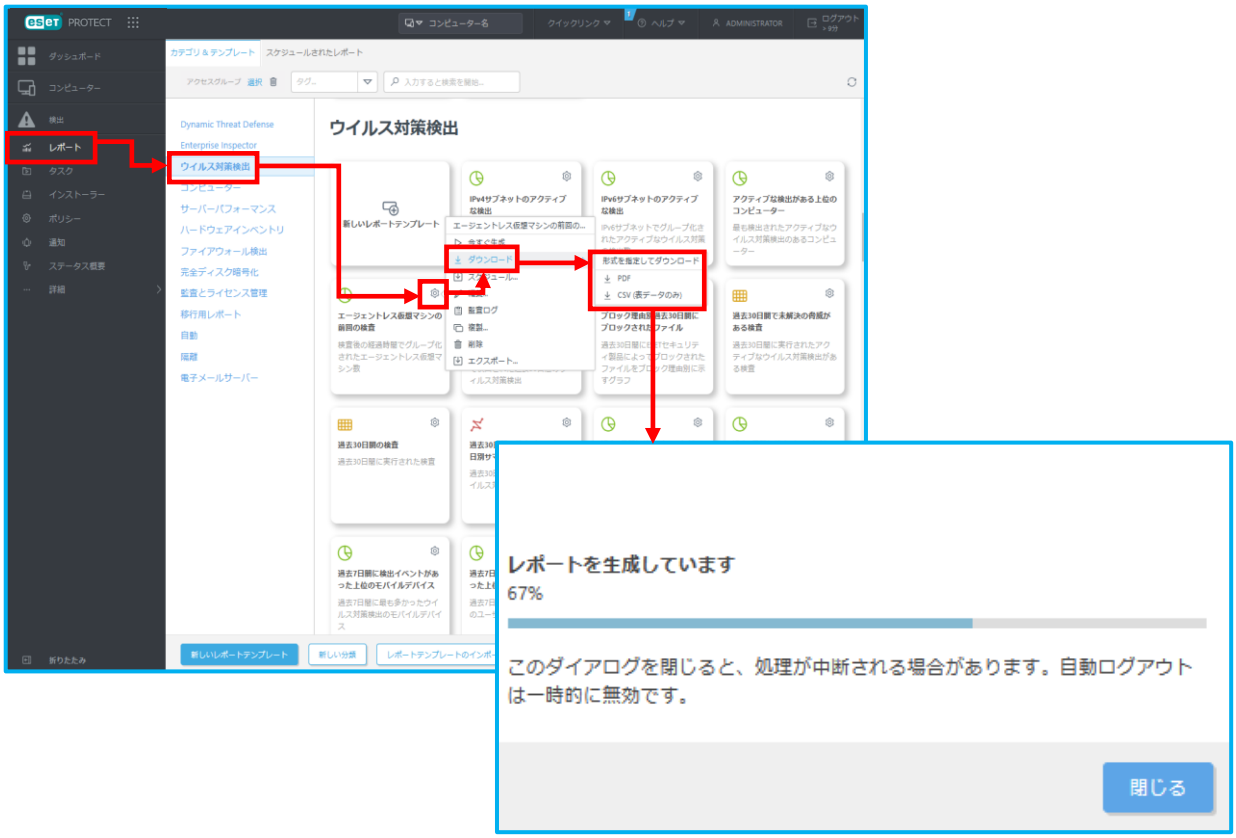
4.2.6. 各種レポートやグループ情報のエクスポート

メインメニュー「レポート」より、事前準備②の「1.登録端末、グループやポリシーの設定状況」で作成したレポートの「歯車マーク」->「エクスポート」->「形式を選択」して、ダウンロードします。

※クラウド型セキュリティ管理ツールへの移行後に、本レポートの内容を確認して
再グルーピングを行ってください。

(1). ウイルス対策検出やファイアウォール検出などの検出情報をエクスポート

① メインメニュー「レポート」->「ウイルス対策検出」->「該当するレポートの歯車マーク」->「ダウンロード」->「形式を選択してダウンロード」よりダウンロードします。



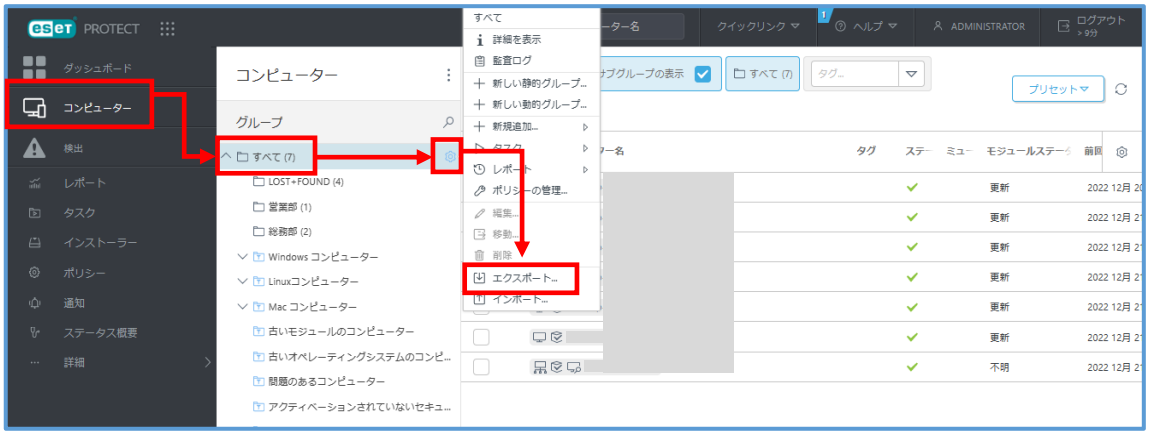
注意：必要に応じて各種レポートをダウンロードしてください。

(2). 静的グループと所属端末情報のエクスポート

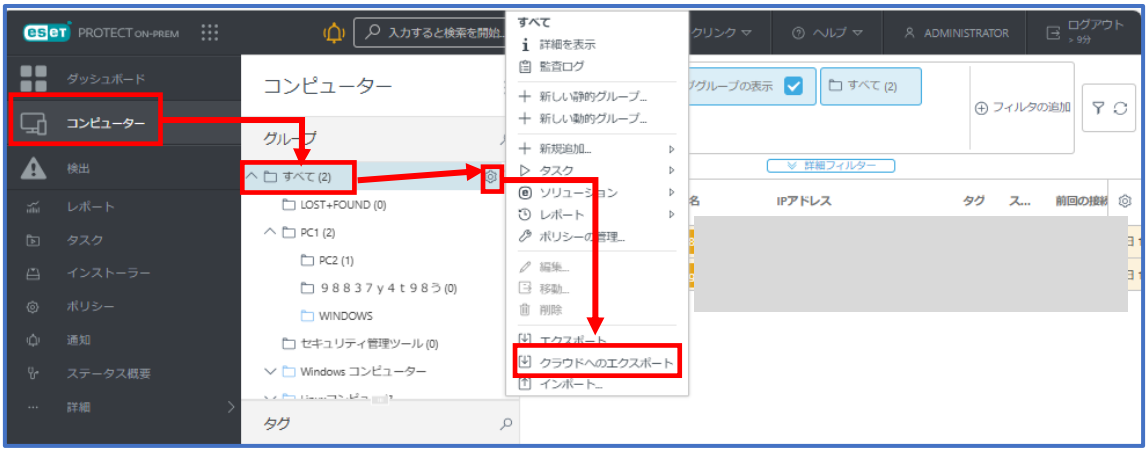
① メインメニュー「コンピューター」->「すべて」->「歯車マーク」->「エクスポート」または「クラウドへのエクスポート」をクリックします。

※オンプレミス型セキュリティ管理ツールのバージョンによって、選択する項目が異なりますのでご注意ください。

○オンプレミス型セキュリティ管理ツールＶ11.0 以下の場合



○オンプレミス型セキュリティ管理ツールＶ11.1 以上の場合



② 「サブグループからもコンピューターをエクスポートしますか？」->「はい」をクリックするとテキストファイルがダウンロードされます。

4.3. 事前準備 3「グループとポリシーの準備」

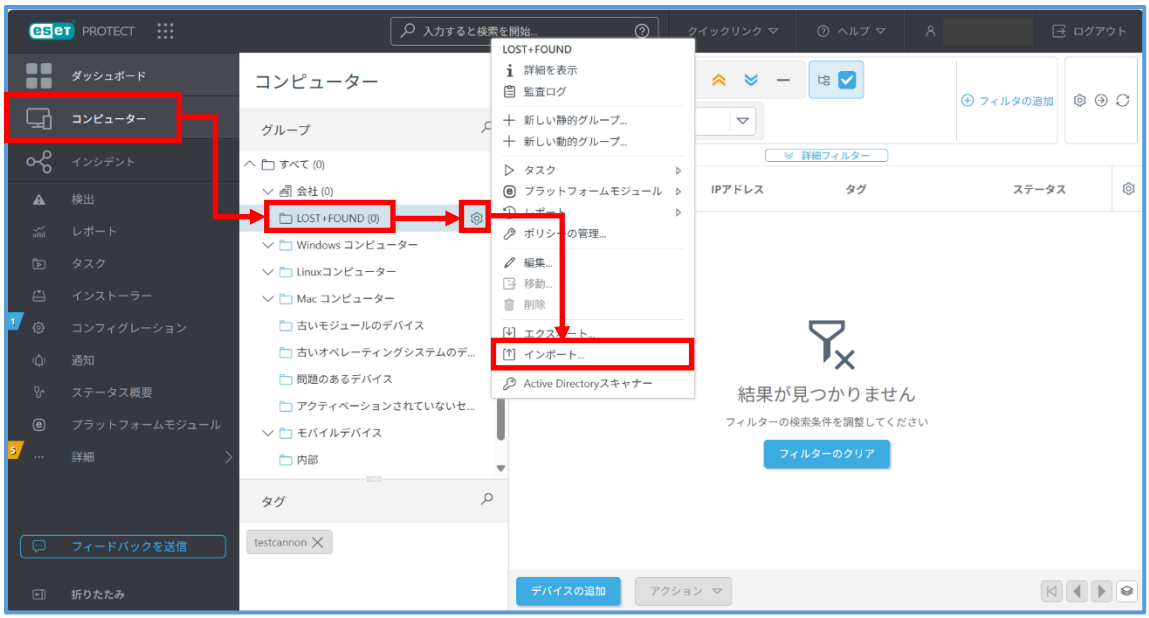
クラウド型セキュリティ管理ツールへの移行後、すぐにクライアント端末のグループを移行出来るように事前にグループを作成しポリシーの割り当てを行います。

(1). クラウド型セキュリティ管理ツール EP にログインします。

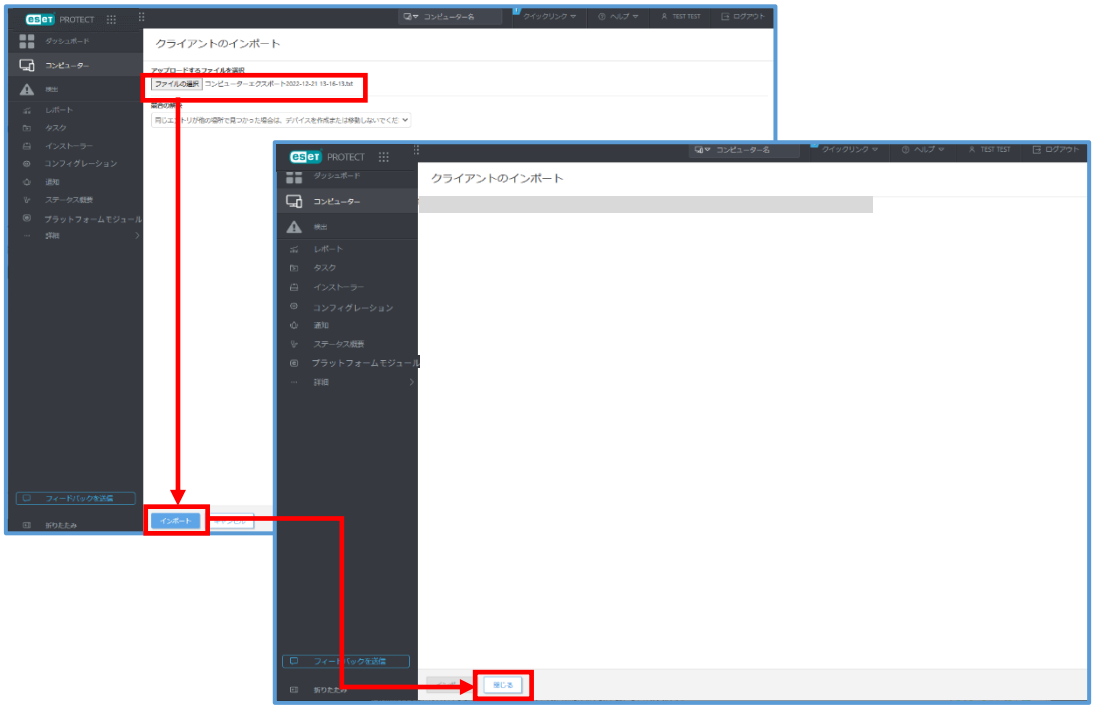
(2).「コンピューター」->「インポートしたいグループ※」->「歯車マーク」->「インポート」をクリックします。

※ここでは「LOST+FOUND」を選択します

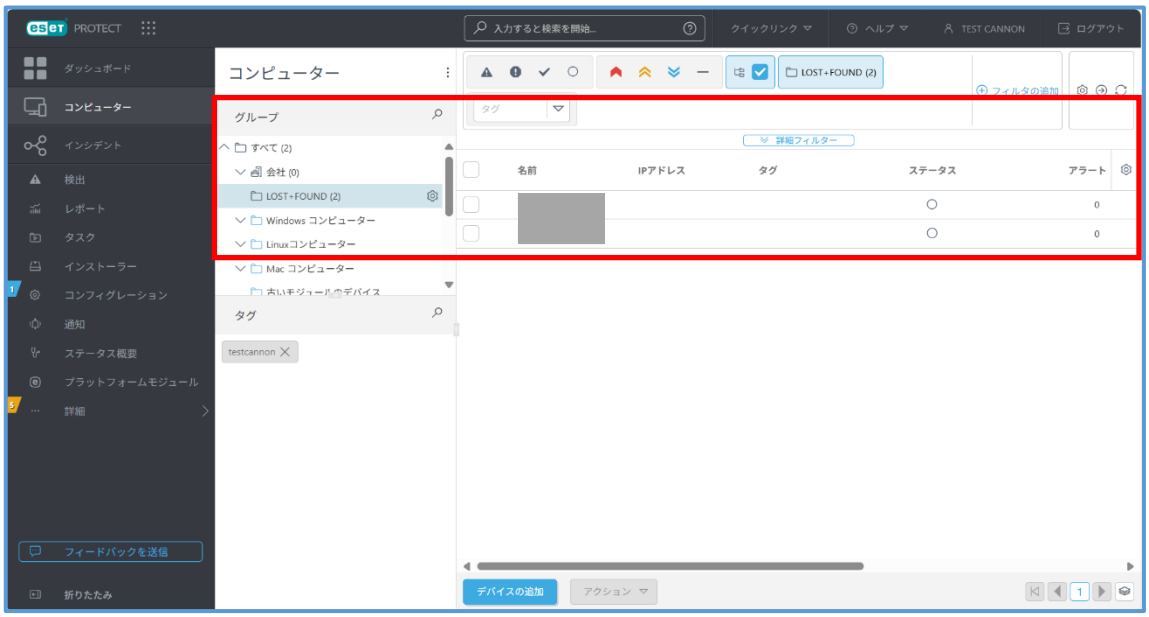
※別の静的グループから一度インポートした後は、「すべて」からもインポート可能になります



(3). 手順 4.2.6（2）で既存セキュリティ管理ツールからエクスポートしたテキストファイルを選択して、インポートをクリックし、インポートが完了したのを確認後、「閉じる」をクリックします。

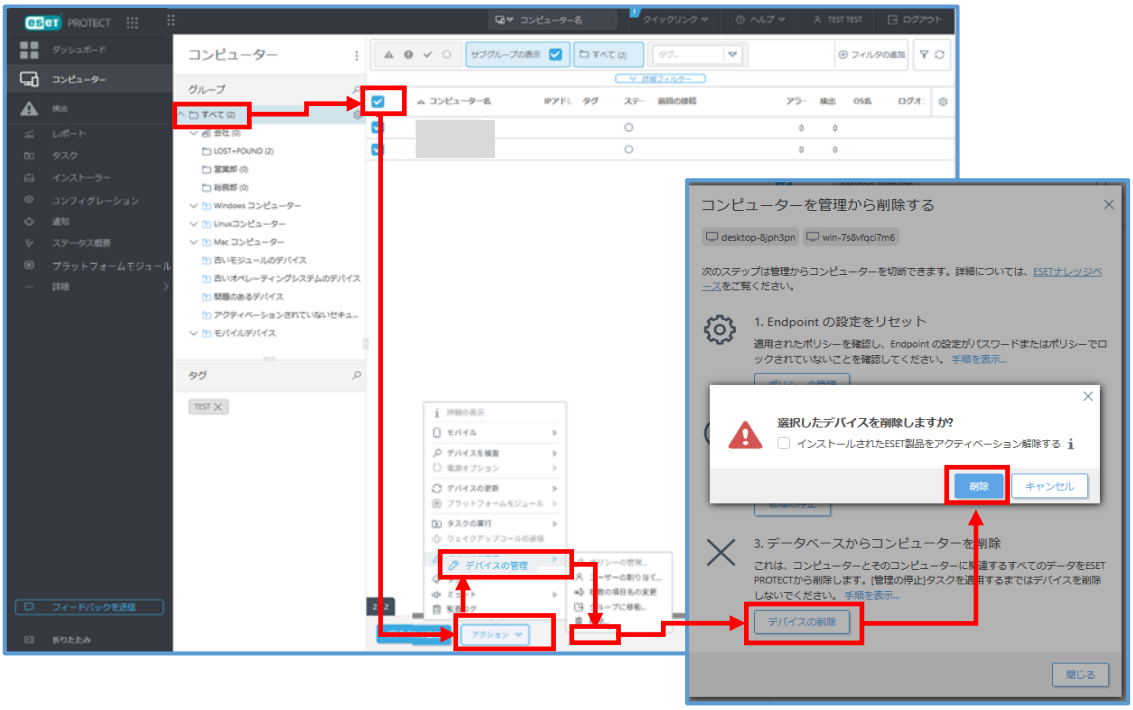


(4). 完了すると、静的グループと端末名が表示されます。



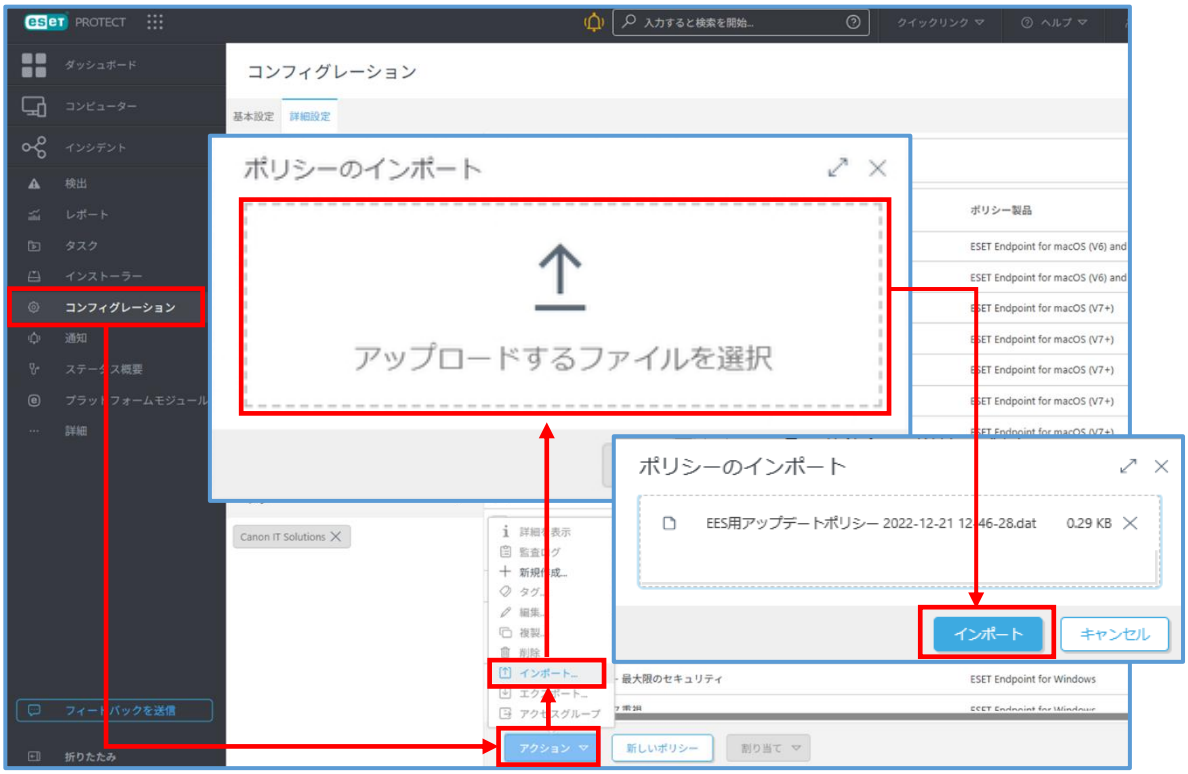
(5). **※本手順はオンプレミス型セキュリティ管理ツール V11.1 以上の場合は実施不要です。手順 4.3.7 へお進みください。**

「すべて」より全コンピューターを選択し、「アクション」->「デバイスの管理」->「削除」->「デバイスの削除」をクリックします。「インストールされた ESET 製品をアクティベーション解除する」の**チェックを外し**、「削除」をクリックします。

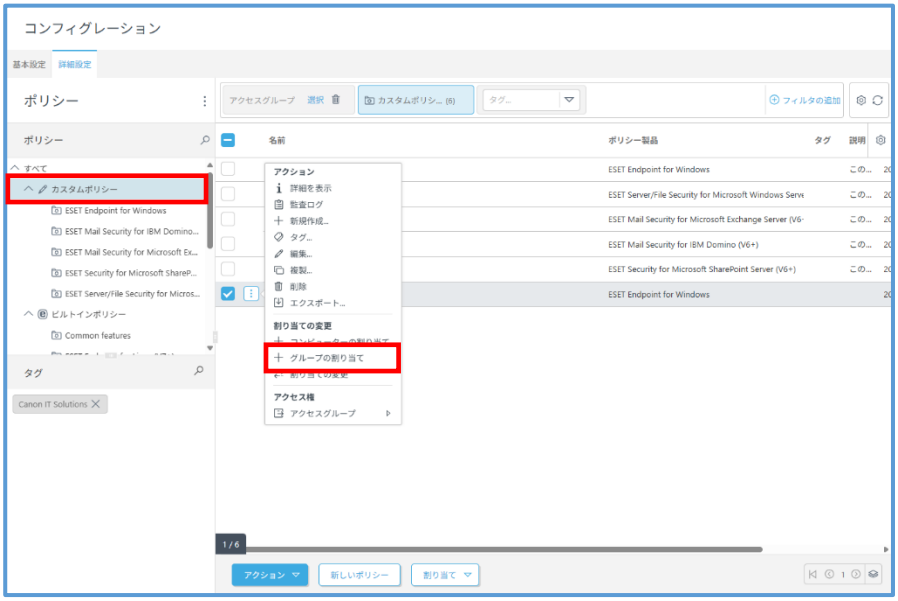


(6). 削除されたことを確認します。

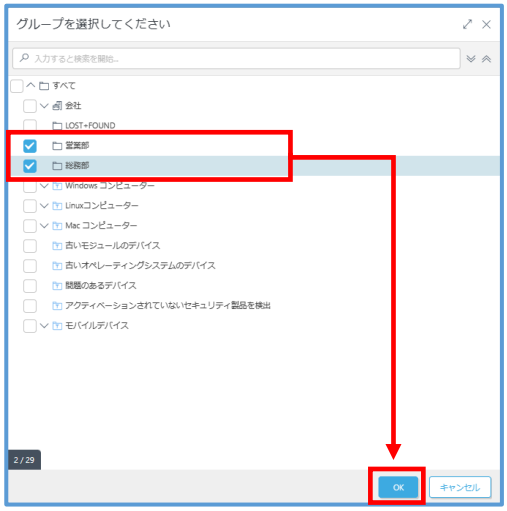
(7). メインメニュー「コンフィグレーション」->「詳細設定」->「アクション」->「インポート」をクリックし、手順 4.2.4 でエクスポートした旧ポリシーをインポートします。



(8). 「カスタムポリシー」よりインポートしたポリシーを選択し「グループの割り当て」をクリックします。



(9).「適用したいグループを選択」->「OK」をクリックします。



以上で事前準備はすべて終了です。

注意：クラウド型セキュリティ管理ツールへ移行後、クライアントは旧ポリシーが外れてしまうため設定がインストール時に戻ってしまいます。そのため、移行前にクラウド型セキュリティ管理ツール EP で新グループの作成と旧ポリシーの割り当てを行っておくことで、移行後すぐにお客様自身で再グルーピングを行い、少しでもポリシーが適用されていない時間を削減いただくようお願いします。（検出エンジンのアップデート設定もインストール時の状態に戻ります）

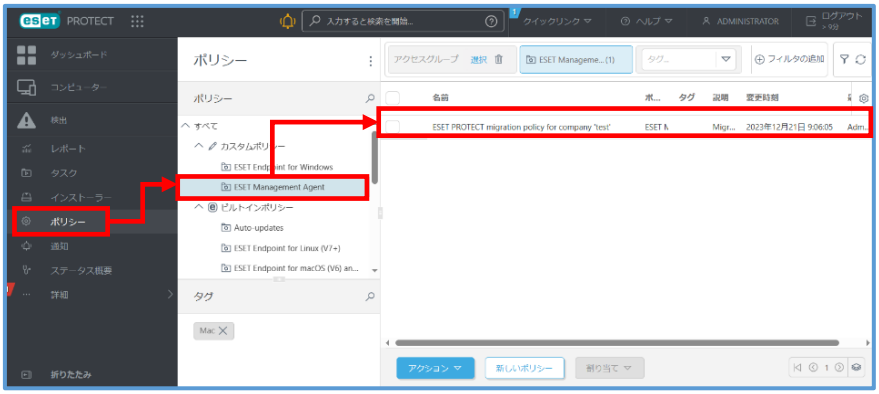
5. クラウド型セキュリティ管理ツールへの移行作業

事前作業で取得した**移行用ポリシー**を利用し移行作業を実施します。

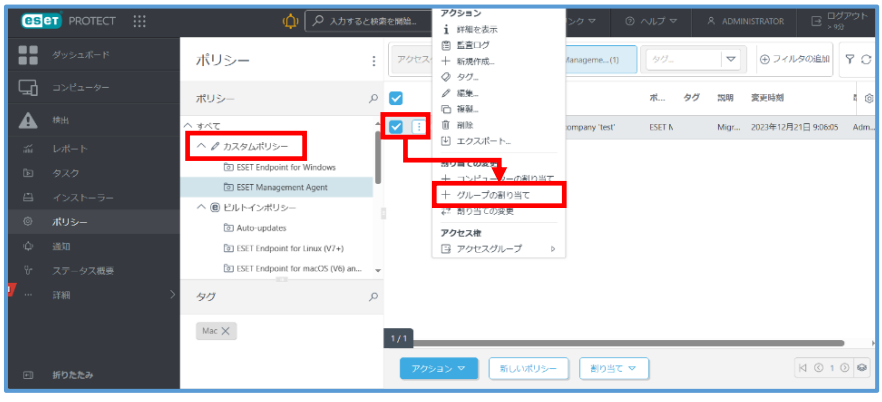
5.1. クラウド型セキュリティ管理ツールからダウンロードした移行用ポリシーの割り当て

(1). 既存セキュリティ管理ツールにログインします。

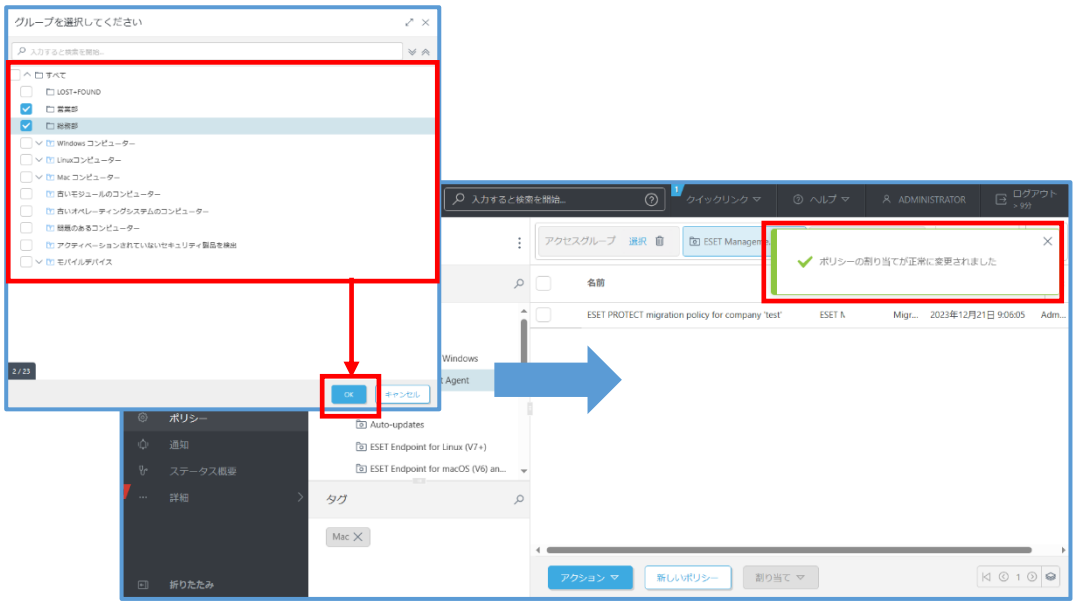
(2). メインメニュー「ポリシー」->「カスタムポリシー」-「ESET Management Agent」をクリックします。手順 4.1.5 でインポートした移行用ポリシーが追加されていることを確認してください。



(3). 「カスタムポリシー」->「(1)で確認した移行用ポリシー」->「グループの割り当て」をクリックします。



(4).移行を行うグループを選択し、「OK」をクリックします。



注意 1：既存セキュリティ管理ツールには移行用ポリシーを適用する必要がないため、すべてを選択しないようにご注意ください。また、モバイル端末を管理されている場合は、併せてモバイル端末も選択しないようにしてください。

注意 2：万が一失敗した時の影響範囲を考え、事前に数台の端末にポリシー適用をし、移行できることを確認してから順次ポリシーの適用をしてください。

注意 3：EM エージェントの通信にプロキシを使用している場合でも移行が可能です。

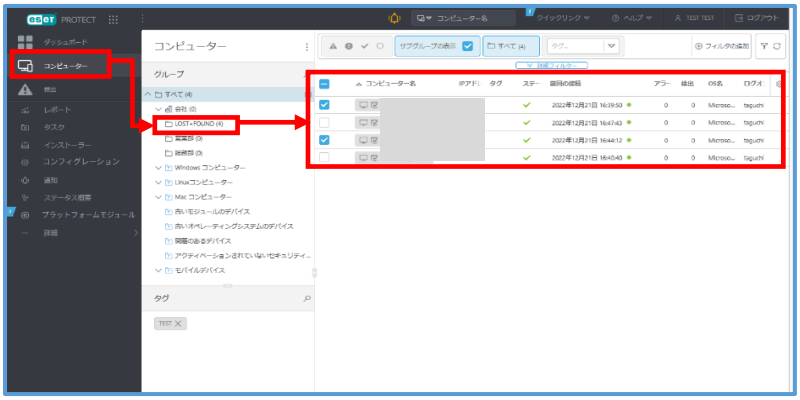
5.2. 移行後の再グルーピング

本手順はオンプレミス型セキュリティ管理ツール V11.1 以降の場合は実施不要です。
手順 5.3 へお進みください。

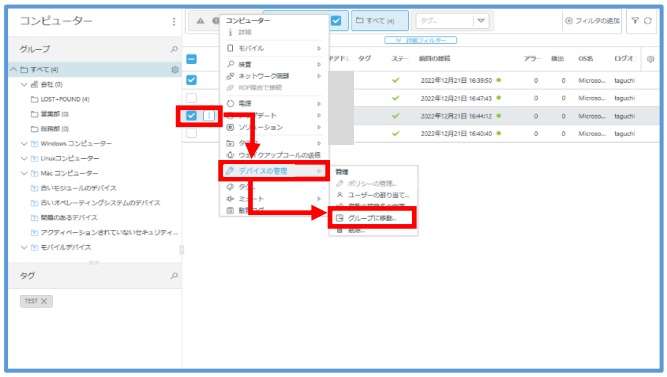
移行してきたクライアントを事前準備②で作成したレポートをもとに再グルーピングをします。クラウド型セキュリティ管理ツールへ移行してきたクライアントは LOST+FOUND に振り分けられておりますので、該当する静的グループに移動してください。

(1). クラウド型セキュリティ管理ツール EP へログインします。

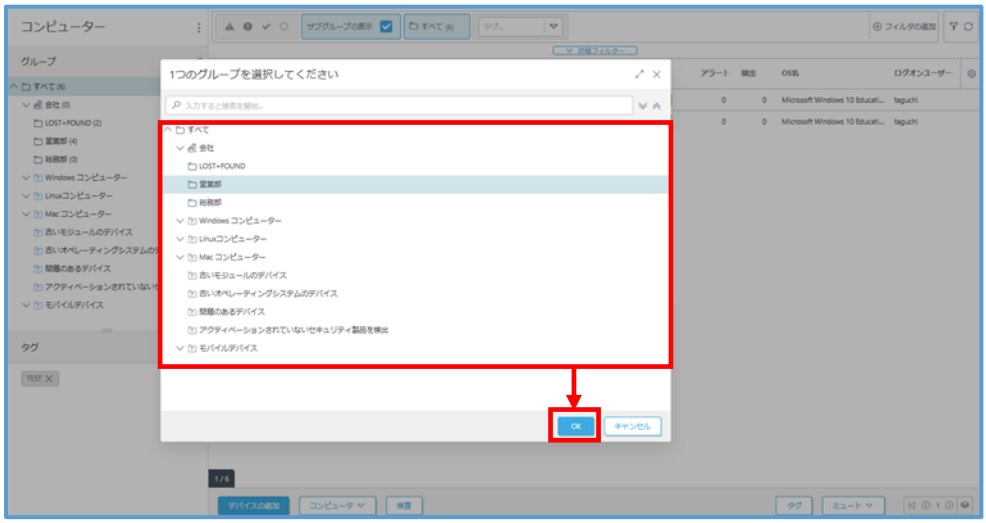
(2).「コンピューター」->「LOST+FOUND」->「移動するコンピューター」をクリックします。



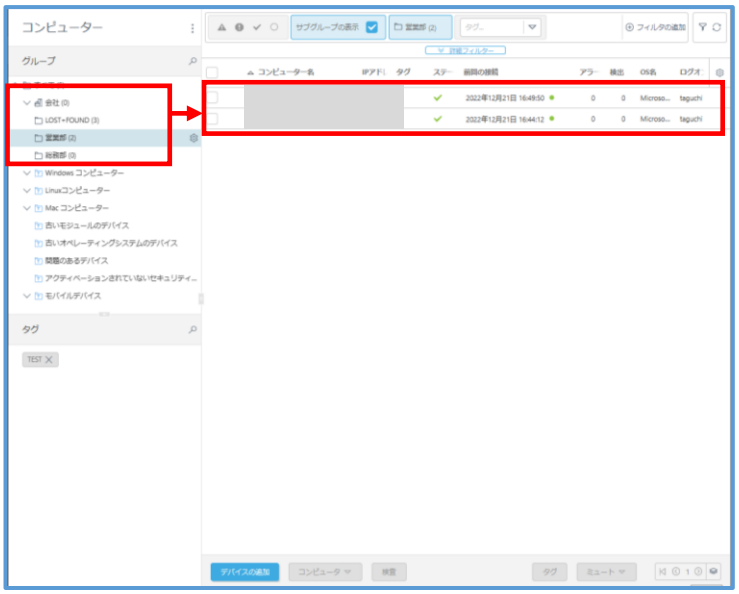
(3).「コンピュータ」->「デバイスの管理」->「グループに移動…」をクリックします。



(4).「移動先の静的グループ」選択し、「OK」をクリックします。



(5).選択した静的グループにコンピューターが移動したことを確認してください。



※ドラック&ドロップで移動させることもできます。

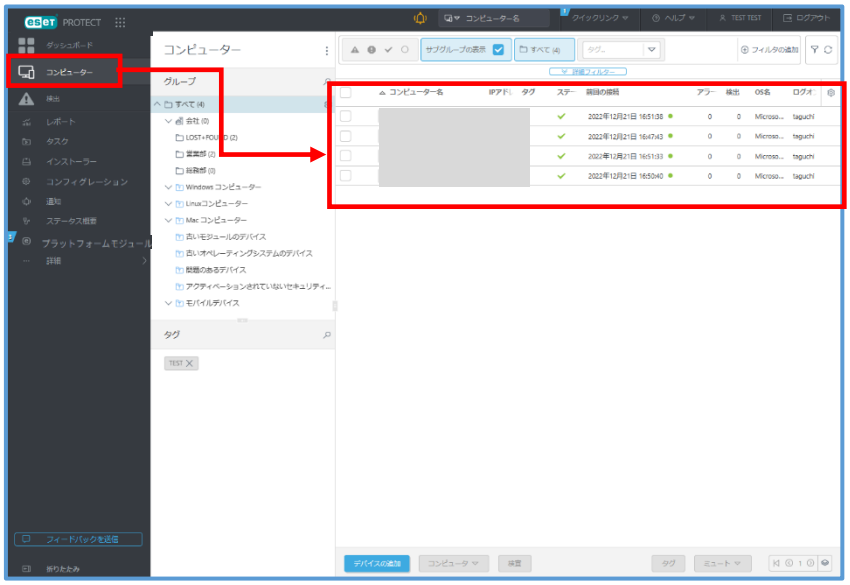
(6).「ダッシュボード」から事前に確認した既存セキュリティ管理ツールでの管理端末数と、クラウド型セキュリティ管理ツールへ移行した管理端末数が同じであることを「コンピューターの接続状態」よりご確認ください。

5.3. エージェントバージョンアップ

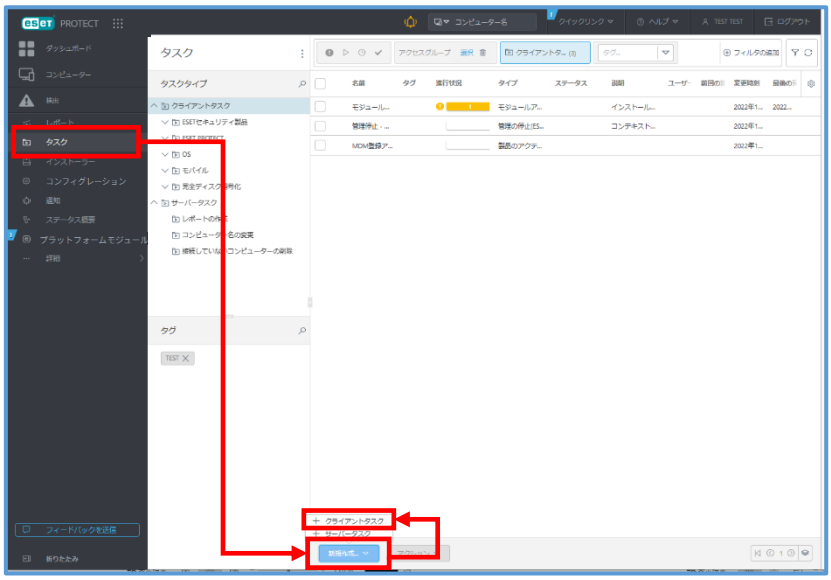
クラウド型セキュリティ管理ツールへ移行済みのクライアントに対する EM エージェントのバージョンアップを行います。

(1). クラウド型セキュリティ管理ツール EP へログインします。

(2). メインメニューの「コンピューター」をクリックします。移行前の環境からクラウド型セキュリティ管理ツールへクライアントが接続変更出来ていることを確認します。
移行対象となるクライアントが一覧で確認出来れば正常に移行出来ています。
※既存セキュリティ管理ツールからの移行漏れのクライアント端末がないことを確認ください。



(3). メインメニューの「新規作成」->「クライアントタスク」をクリックします。

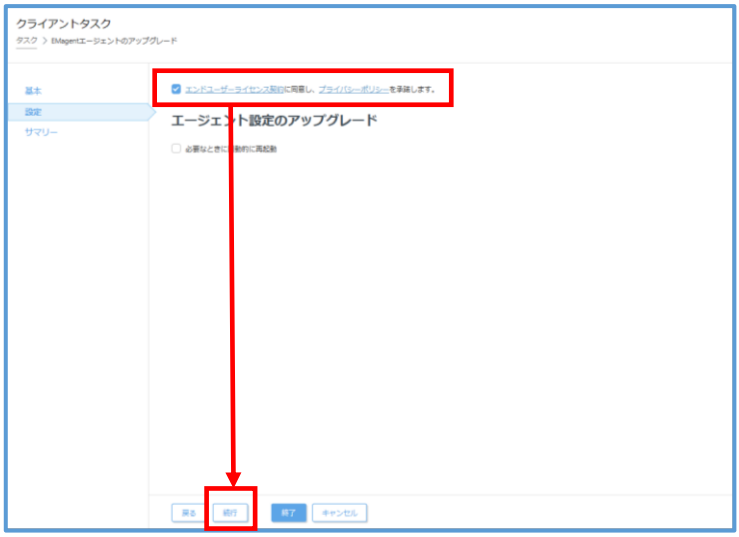


(4). 新規タスクで以下の情報を入力し「続行」をクリックします。

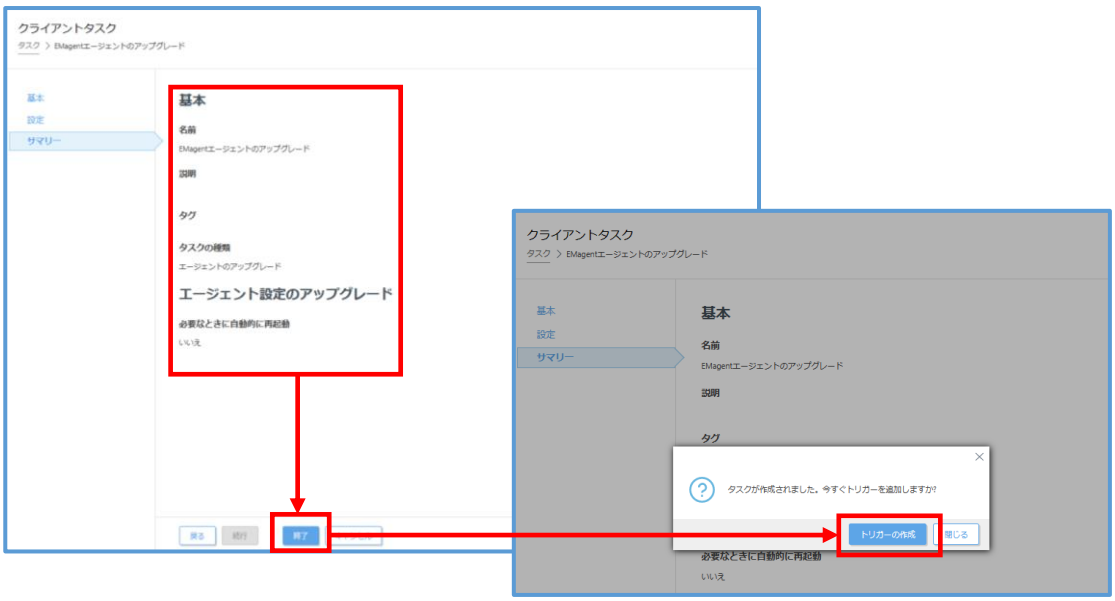
名前	任意の値を入力してください
タグ	任意の値を入力してください。(未入力でも可)
説明	任意の値を入力してください。(未入力でも可)
タスク分類	「ESET PROTECT」を選択してください。
タスク	「エージェントのアップグレード」を選択してください

(5). エンドユーザー使用許諾契約の条項に同意し、「続行」をクリックします。

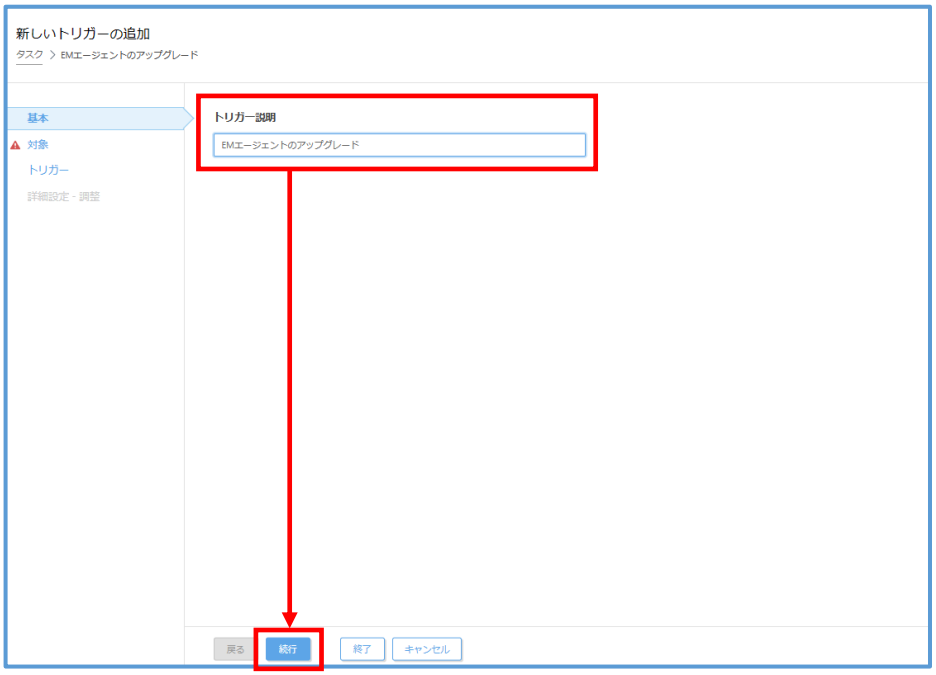
※同意いただけない場合ご利用いただけません。



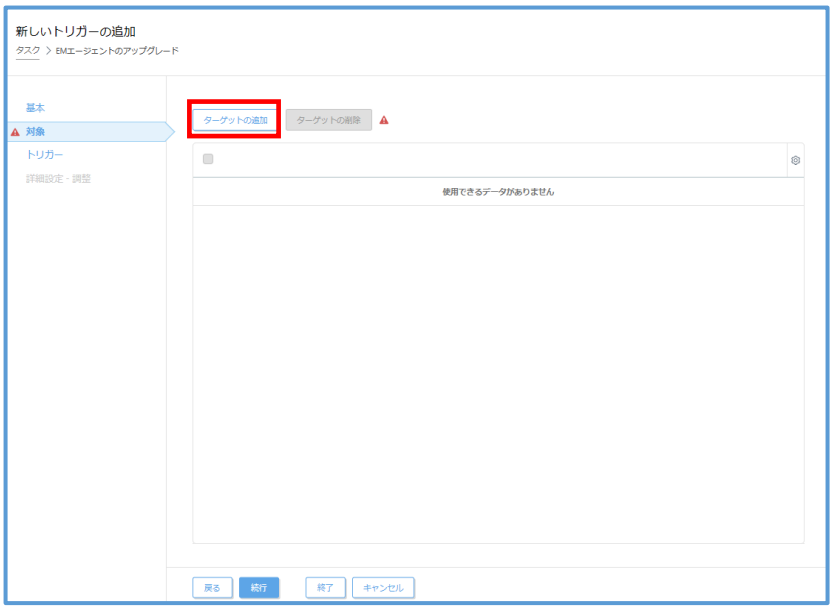
(6). 設定した内容が正しいことを確認し、「終了」->「トリガーの作成」をクリックします。
※「終了」をクリック後、トリガー作成のポップアップが表示されます。



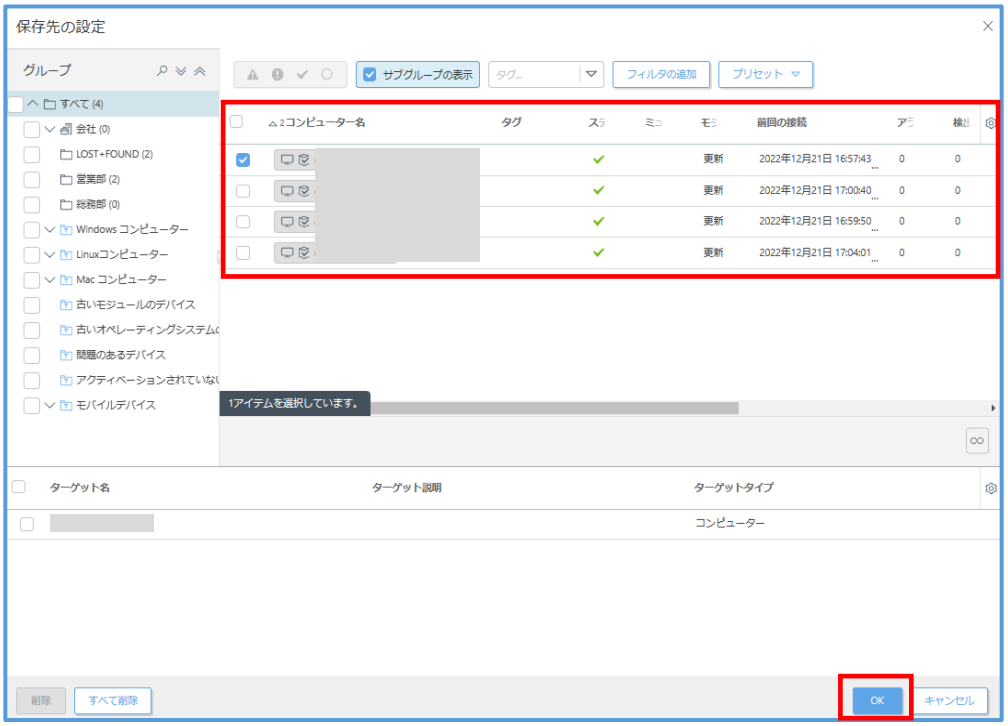
(7). 新しいトリガーの追加で「トリガー説明」に任意の値を入力し、「続行」をクリックします。



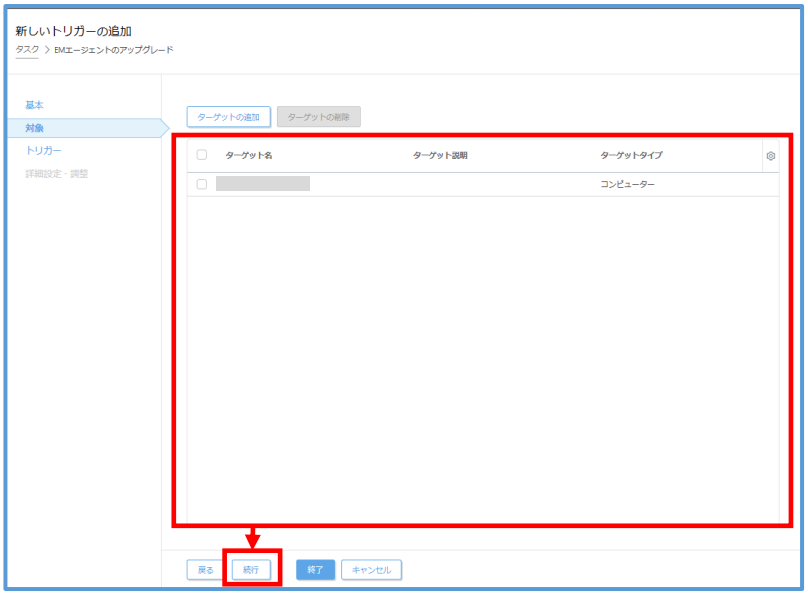
(8).「ターゲットの追加」をクリックします。



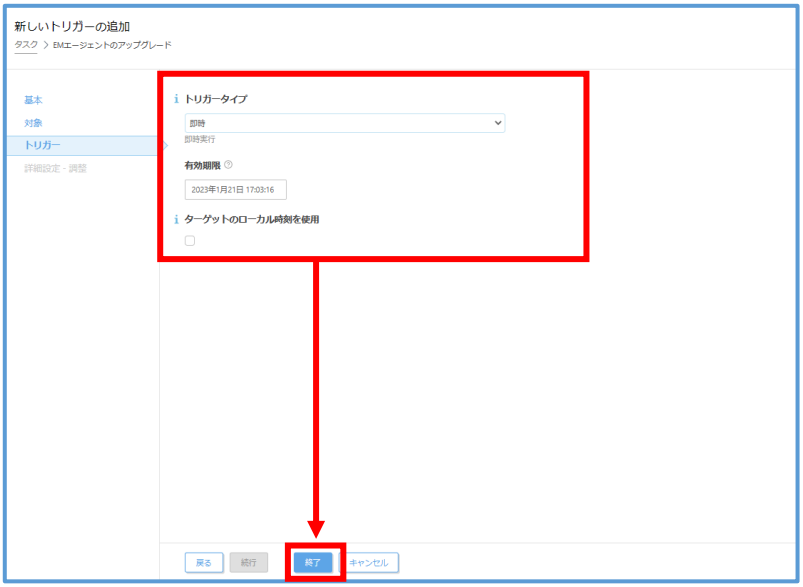
(9).アップグレード対象となるクライアントを選択し、「OK」をクリックします。



(10). アップグレード対象となるクライアントが選択されていることを確認し「続行」をクリックします。

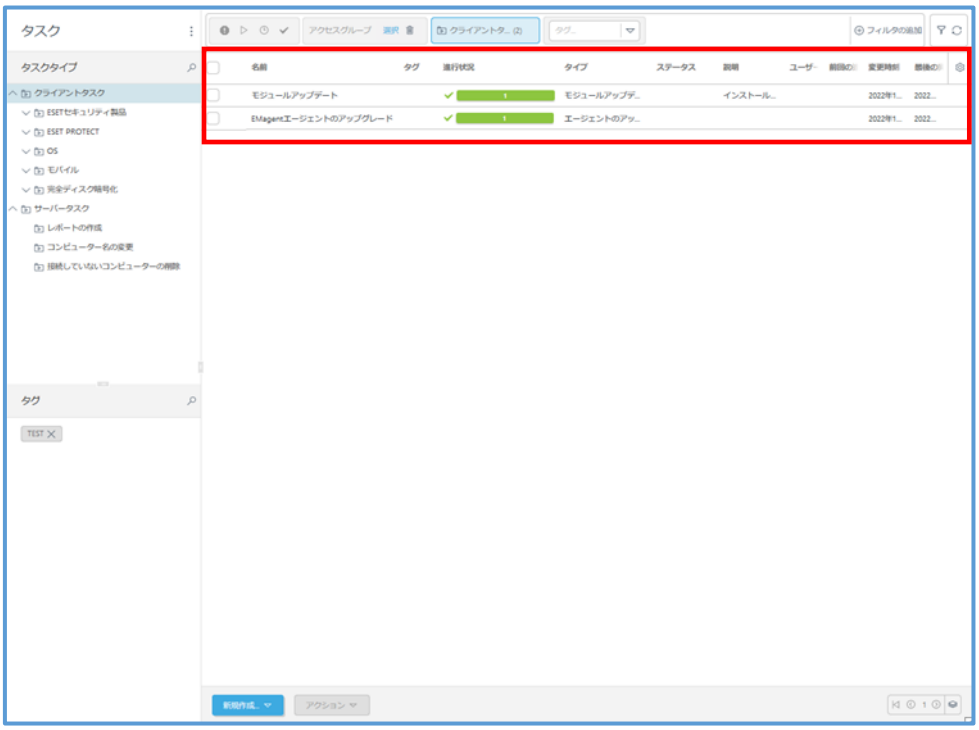


(11). 以下の情報を入力し、「終了」をクリックします。



トリガータイプ	運用方法にあったタスクの実行方法を選択してください
有効期限	デフォルトの状態のまま
ターゲットのローカル時間を使用	デフォルトの状態のまま

(12). 作成したクライアントタスクが正常終了したことを確認します。進行状況のステータスバーが「緑」の状態になれば正常終了となります。それ以外の場合は、ステータスバーをクリックし状態を確認してください。



以上でクラウド型セキュリティ管理ツールへの移行作業はすべて終了です。