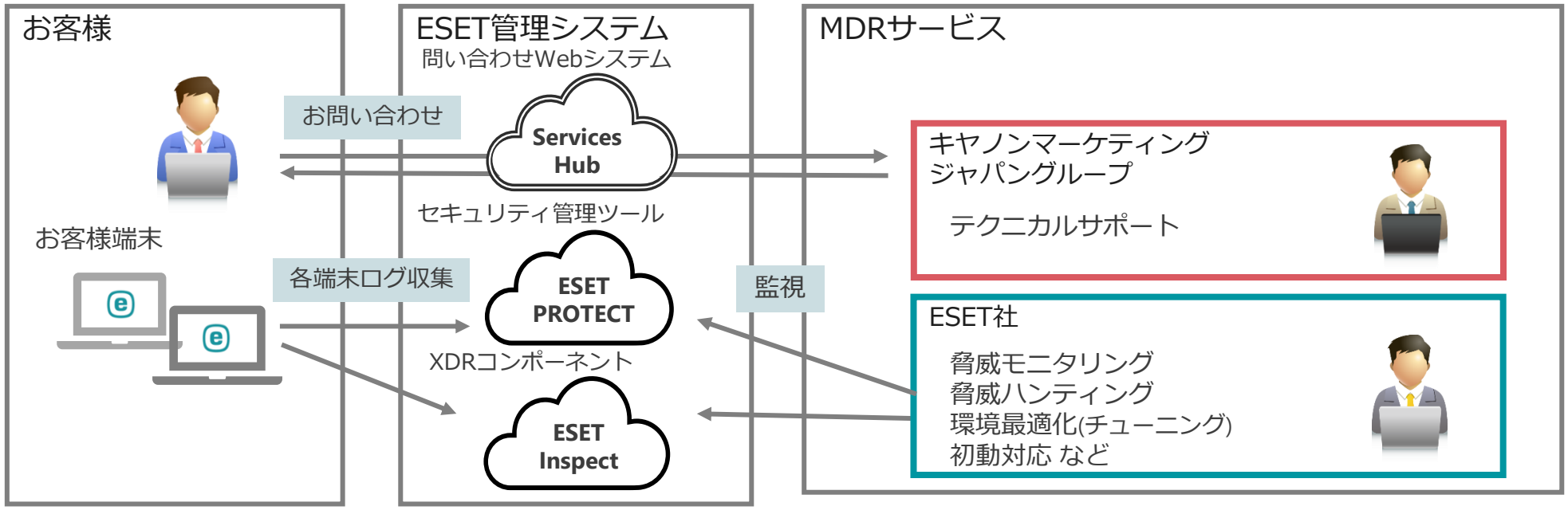
ESET PROTECT MDR Lite
スターターガイド

キヤノンマーケティングジャパン株式会社

第4版 2024年6月14日

はじめに

本資料は、ESETが提供しているMDR（Managed Detection and Response）である、
「ESET PROTECT MDR Lite」のスターターガイドです。
本サービスを導入いただくお客様が必要となる作業内容を記載しています。



もくじ

Ⅰ.導入の流れについて

	納品月	納品月 ~1ケ月後~	納品月 ~2ケ月後~	…	納品月 ~9ケ月後~	…	納品月 ~11ケ月後~	納品月 ~12ケ月後~
発注～納品フェーズ								
	初期フェーズ							
		運用フェーズ						

ご発注～製品ライセンス納品

ご発注書のほか本サービス所定の申込書(Sales Order Form)をご提出ください。
Sales Order Formのご提出をもってESET所定のサービス規約(Terms)に
ご同意いただいたものとみなします。
ライセンス納品時から本ソリューションの利用が開始されます。
お客様には「利用開始案内付き納品メール」「パスワード案内メール」の2通が送信されます。

EP/EI利用開始

ESET PROTECTとESET Inspect のアクティベーションしていただきます。

ESETプログラム導入

お客様環境にESETプログラムをインストールしていただきます。

脅威モニタリング

ESET社によるモニタリングが開始されます。
※ プログラムが導入され次第、モニタリングは開始されます。

ESET Services Hub 利用開始

お問い合わせにご利用いただくServices Hubのアカウントを開設していただきます。

脅威発生時
脅威に検出した場合、脅威内容によっては自動で端末のネットワーク隔離などの初動対応を行います。

2年目以降 サービス継続

ESET PROTECT MDR Lite 有効期限（製品・サービスのご契約期間）

Ⅱ.お客様必須作業

1. ESET Services Hubについて

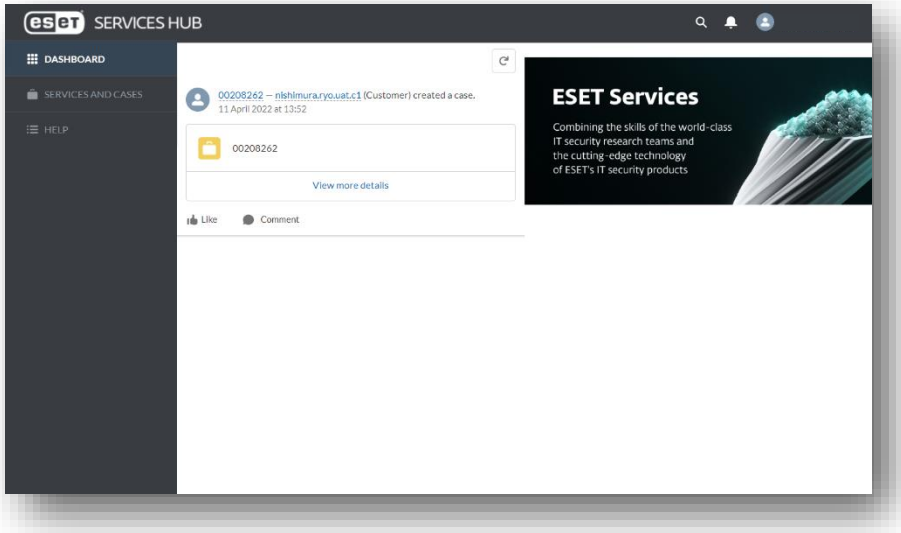
ESET Services Hubの概要

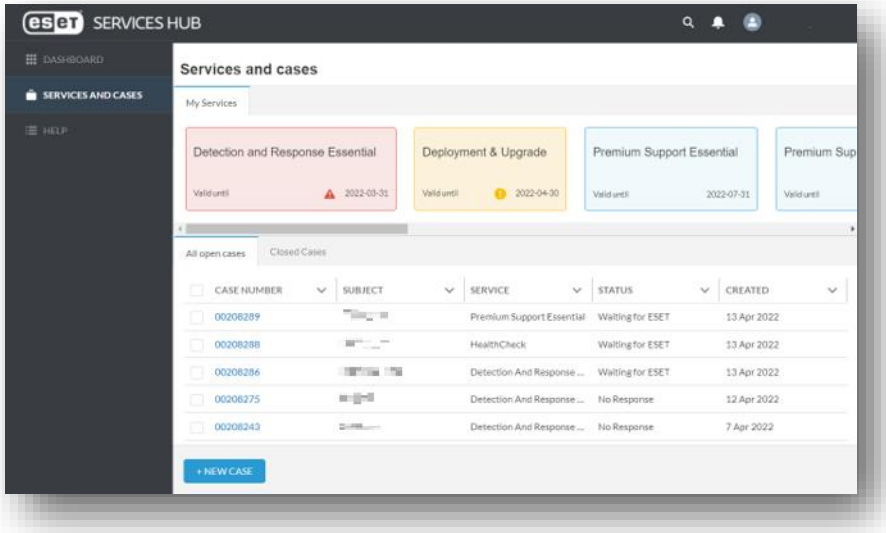
ESET Services Hubとは

「ESET Services Hub」とは、お客様のお問い合わせチケットを作成および管理するESET社が提供するWebサービスです。
セキュリティサービスに関するお問い合わせについては、本Webサービスをご利用ください。

ESET Services Hubで実施できること

- セキュリティサービスに関するお問い合わせチケットの作成
- お問い合わせチケットの継続のご対応
- お問い合わせチケットの管理





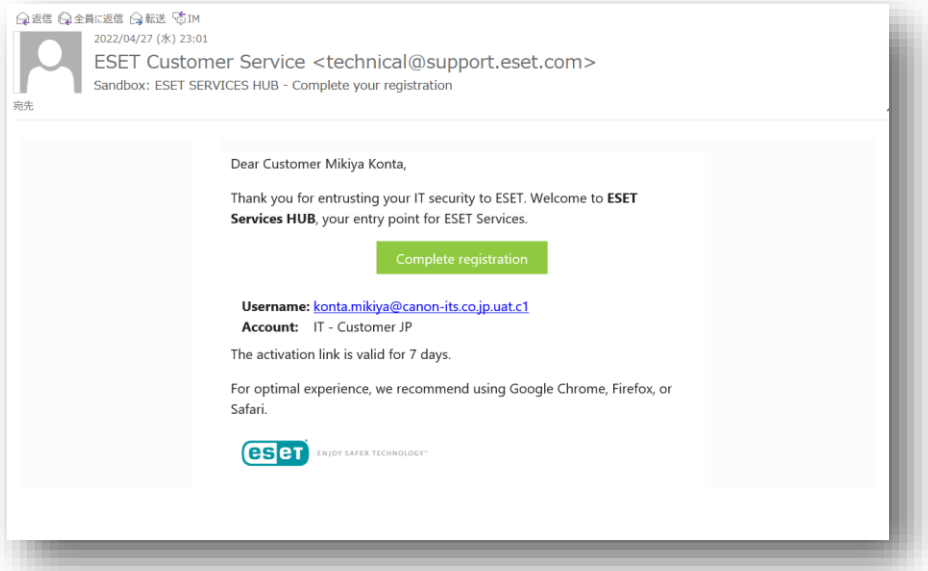
1. ESET Services Hubについて

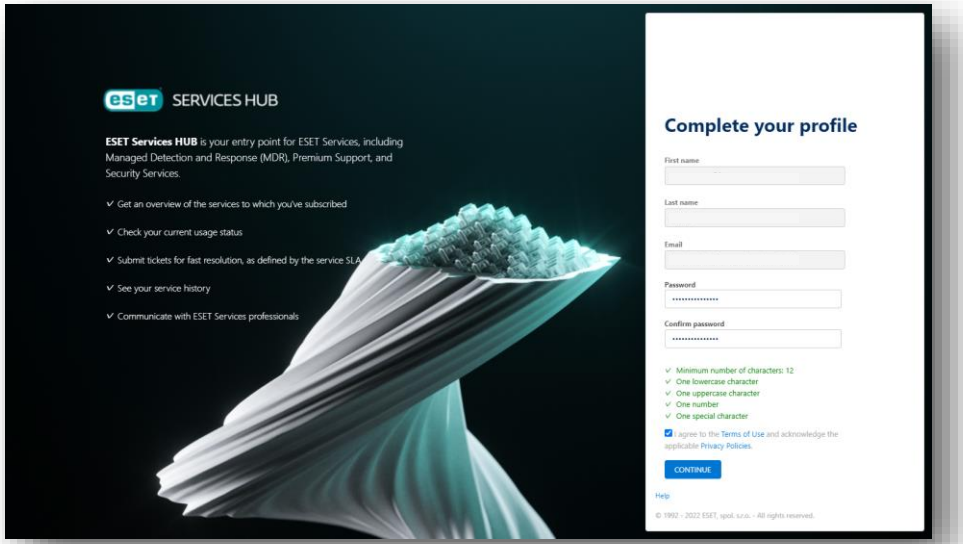
ESET Services Hubの利用方法

アカウント開設方法

1. 件名「ESET Services HUB – Complete your registration」の招待メールを開き、
   メール内に記載されている「Complete Registration」をクリックします。

2. Webブラウザに表示された「Complete your profile」画面で、パスワードの設定および利用規約に同意します。
   ※次回以降のログインでは2要素認証の設定が必要となります。
   　再ログイン時に表示される、画面「Connect Salesforce Authenticator」の手順に従って設定します。



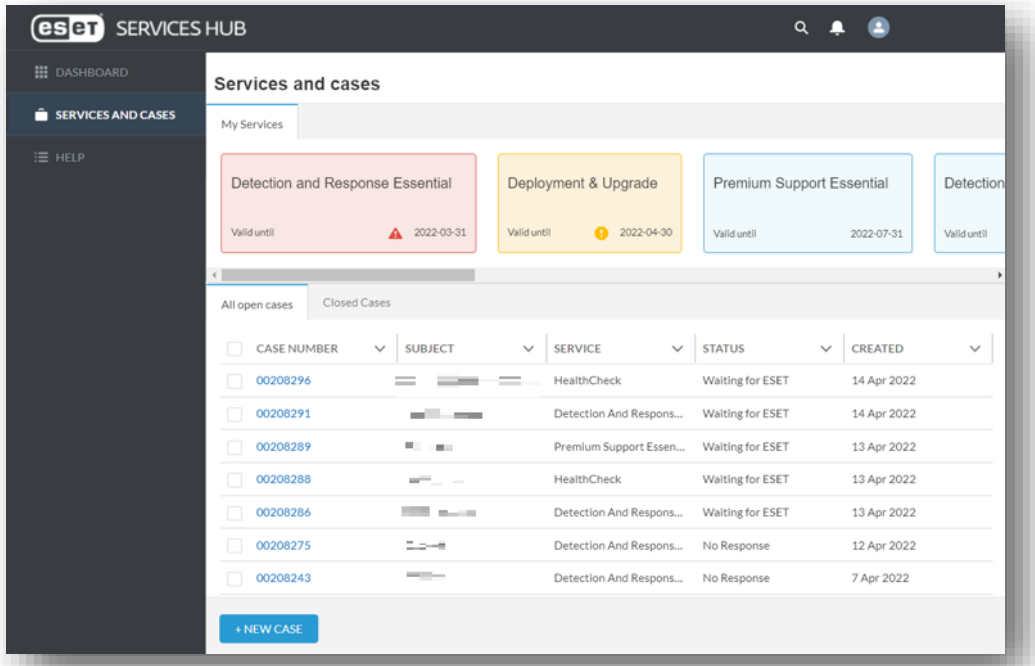


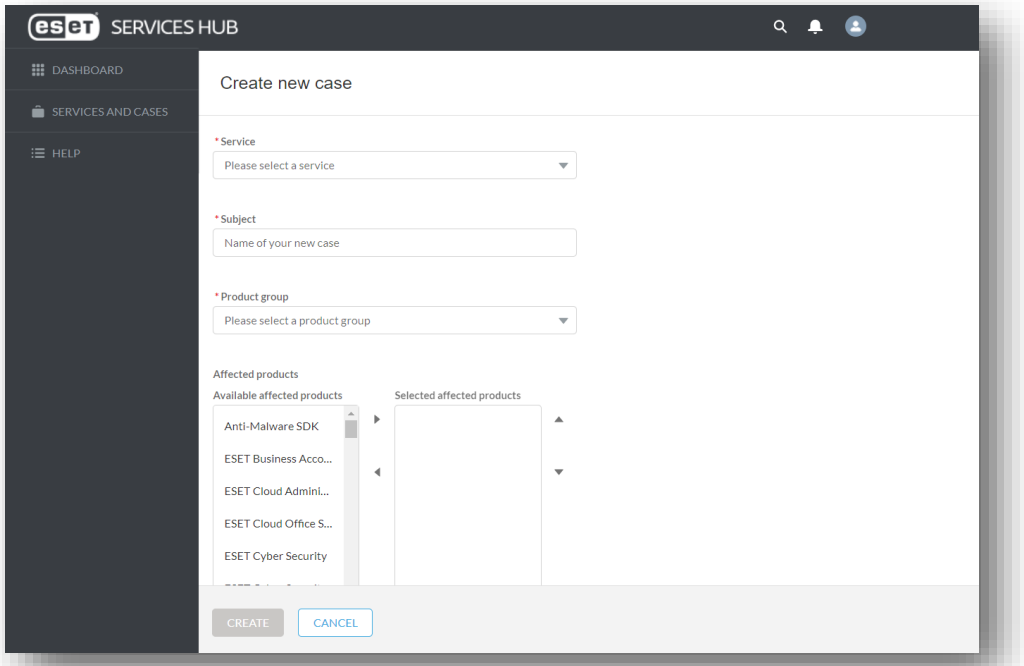
1. ESET Services Hubについて

ESET Services Hubの利用方法

お問い合わせチケットの作成方法

1. 画面「SERVICES AND CASES」を開き、画面下部の[+NEW CASE]をクリックしてお問い合わせチケットを作成します。
2. 必要項目をすべて入力し、[CREATE]をクリックしチケット作成を完了します。
   ※添付ファイルはチケット作成後に別途添付可能です。



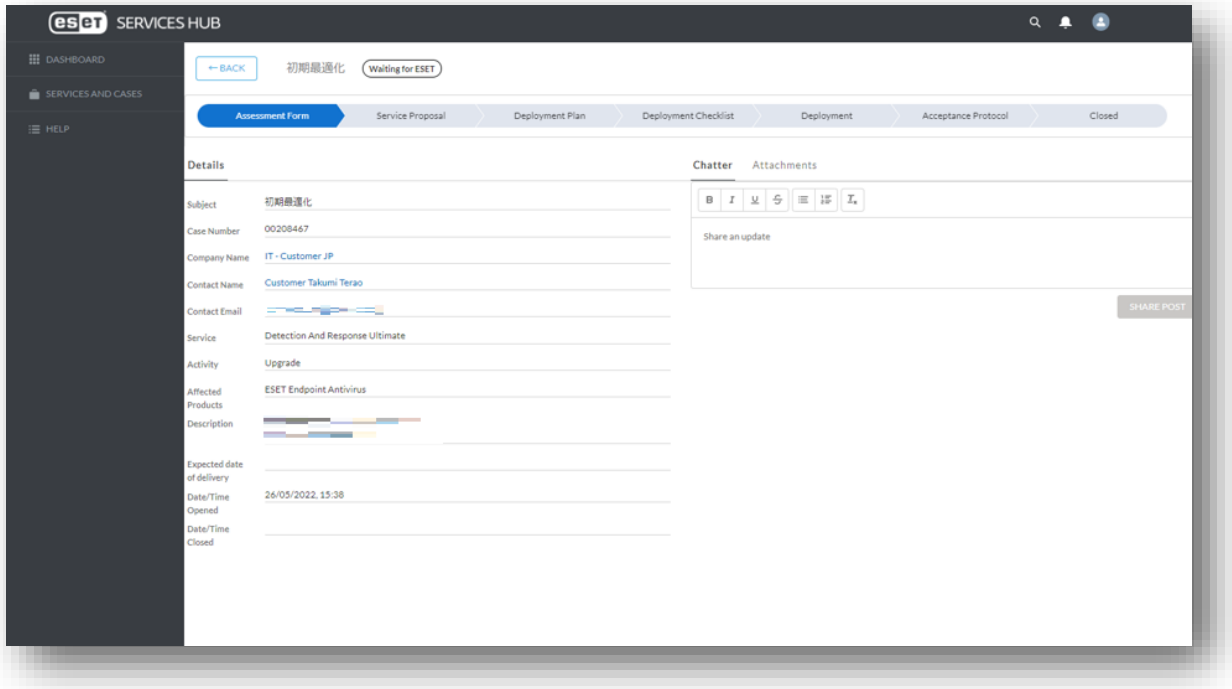


1. ESET Services Hubについて

ESET Services Hubの利用方法

オープン中のお問い合わせチケットの対応方法

1. 画面「SERVICES AND CASES」を開き、表示されたお問い合わせチケットから対応を行いたいものをクリックします。
2. お問い合わせチケットについて各種対応を行います。



Chatter

お問い合わせチケットに対してのオペレーターからの連絡に返信することができます。

Attachment

お問い合わせチケット作成後に、問い合わせに関連するファイルを添付することができます。

2. プログラムの導入

- ESET PROTECT MDR Liteの利用には、ESETプログラムの最新バージョンの利用が必要です。
  ▼利用条件
  https://canon.jp/business/solution/it-sec/lineup/eset/product/eset-protect-mdr
  ※ページ下部の「動作環境」をご参照ください。

- プログラムの導入に伴うお客様の作業は以下のパターンに分かれます。
  - **ESET PROTECT（クラウド版）で端末を管理済みの場合**
    →10ページへ
  - **ESET PROTECT on-premで端末を管理済みの場合**
    →11ページへ
  - **ESET製品を新規導入の場合**
    →15ページへ

2. プログラムの導入 ~ ESET PROTECT（クラウド版）で端末を管理済みの場合~

ESET PROTECT（クラウド版）で端末を管理済みの場合、追加でXDRと接続するためのESET Inspect Connectorのインストールが必要です。

作業手順については、別資料「ESET PROTECT MDR環境構築ガイド 」をご参照ください。

2. プログラムの導入 ~ ESET PROTECT on-premで端末を管理済みの場合~

ESET PROTECT on-premで端末を管理済みの場合、必要なステップは以下の通りです。

2. プログラムの導入~ ESET PROTECT on-premで端末を管理済みの場合~

STEP1. ESET PROTECT (クラウド版)への移行

本サービスはクラウド版の管理ツールを利用いただくことが条件となりますので、ご利用のオンプレミス版管理ツールからクライアントを移行します。
移行手順については、以下の手順書やサポートページの移行動画をご参照ください。

▼移行手順書
https://eset-info.canon-its.jp/files/user/pdf/support/cloud_conversion.pdf

▼参考情報(動画)：ESET PROTECT（クラウド版）移行手順について
①Overview編
https://www.youtube.com/watch?v=xODeNT2410g
①Overview編
https://www.youtube.com/watch?v=96znMK9go1s

2. プログラムの導入 ~ ESET PROTECT on-premで端末を管理済みの場合~

2. プログラムの導入~ ESET PROTECT on-premで端末を管理済みの場合~

STEP2. EI Connectorのインストール

XDRと接続するためのESET Inspect Connectorをインストールします。

作業手順については、別資料「ESET PROTECT MDR環境構築ガイド 」をご参照ください。

2. プログラムの導入 ~ ESET製品を新規導入の場合~

ESET製品を新規で導入いただく場合、必要なステップは以下の通りです。

2. プログラムの導入 ~ ESET製品を新規導入の場合~

STEP1. ESET Business Accountの解説

1. https://eba.eset.com/にアクセスし、ログイン画面で「無料で登録」をクリックしアカウント作成を開始
2. 画面に表示される説明に沿ってお客様情報を入力
   ※ 電子メールアドレスやパスワード、名前、電話番号、お客様企業名などを入力します
   ※ 本手順で設定した電子メールアドレスとパスワードはEBAログイン時に使用します

■ログイン画面

■Business Accountを作成

2. プログラムの導入 ~ ESET製品を新規導入の場合~

3. 利用規約をご確認いただき「ESETに同意」にチェックし「登録ボタン」をクリック
4. アカウントのアクティベーション
   ※ 登録した電子メールアドレスに「@eset.com」からメールが届きます

■利用規約への同意画面

■アクティベーション用メール

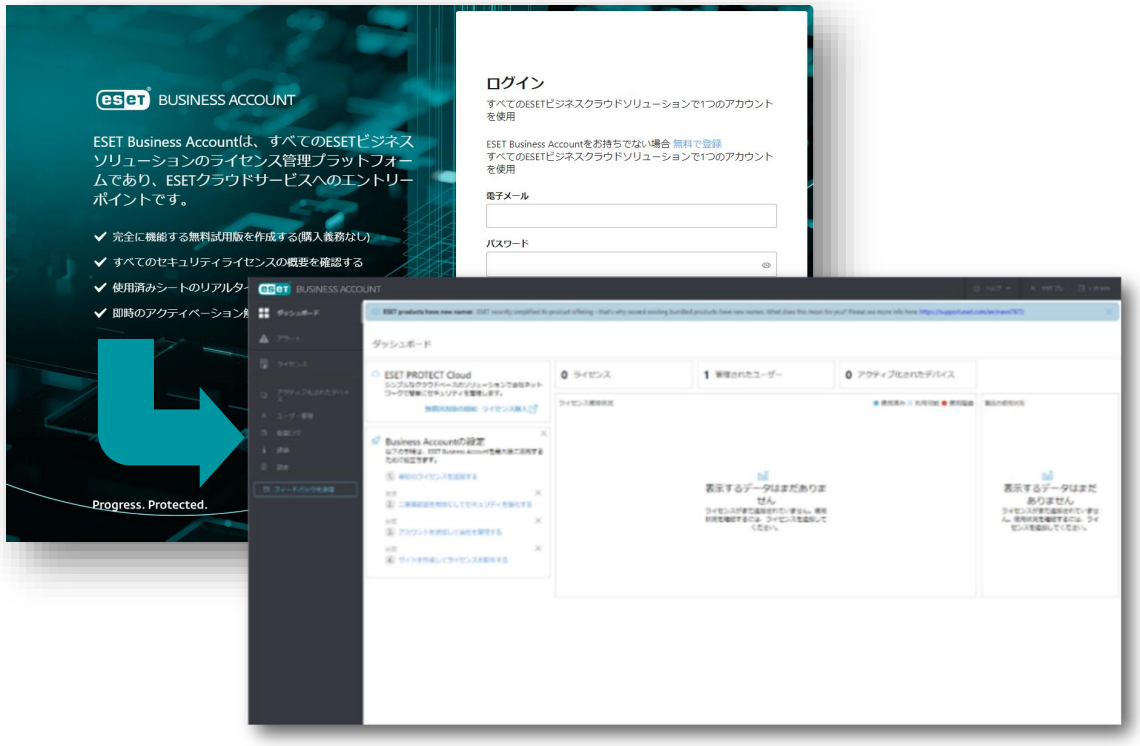
2. プログラムの導入 ~ ESET製品を新規導入の場合~

5. アカウントがアクティベーションされたことの確認
   ※ 登録した電子メールアドレスに「@eset.com」からメールが届きます

6. EBAにログインできることの確認
   ※ 登録した電子メールアドレスとパスワードを使用します

■アクティベーション完了確認用メール

■EBAにログインできることの確認



2. プログラムの導入 ~ ESET製品を新規導入の場合~

2. プログラムの導入 ~ ESET製品を新規導入の場合~

STEP2. ライセンスの登録

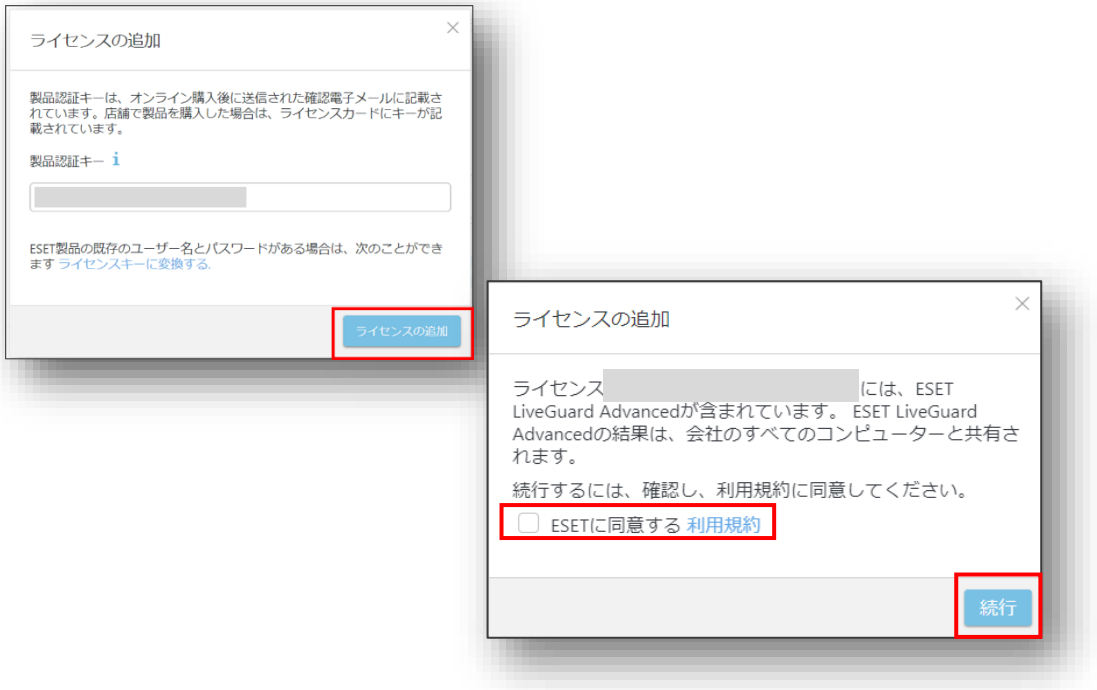
1. EBAへのライセンスの登録

※ 弊社ユーザーズサイトで確認できる以下の情報をご用意ください。
- 製品認証キー

※ 「ライセンスの追加」画面ではESETの利用規約へご同意いただく必要がございます。
※ ユーザーズサイトでのライセンス情報確認の方法は以下をご参照ください。
https://eset-support.canon-its.jp/faq/show/82?site_domain=business

①[ダッシュボード]内の[最初のライセンスを追加する]

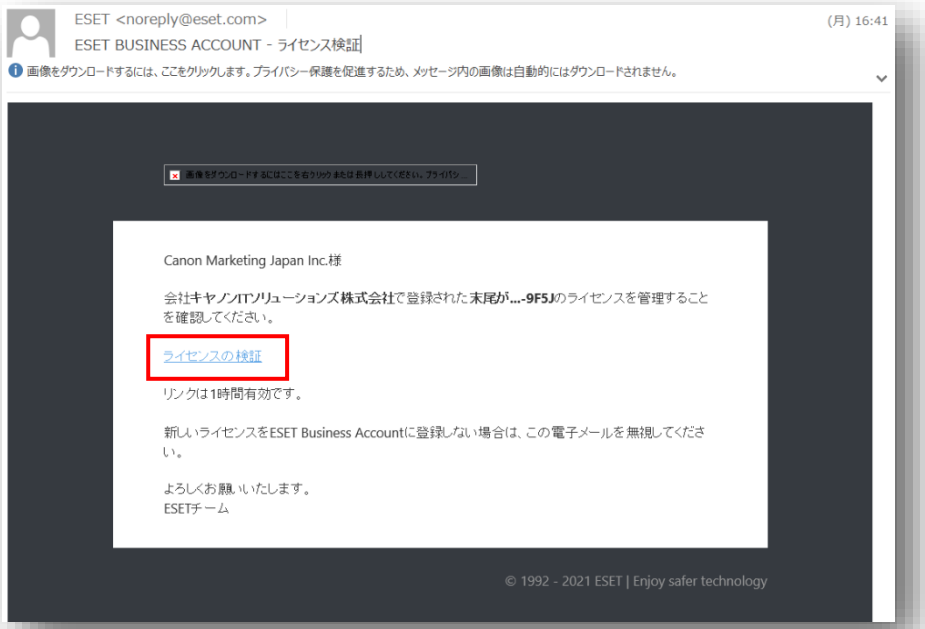
②[ライセンスの追加]画面



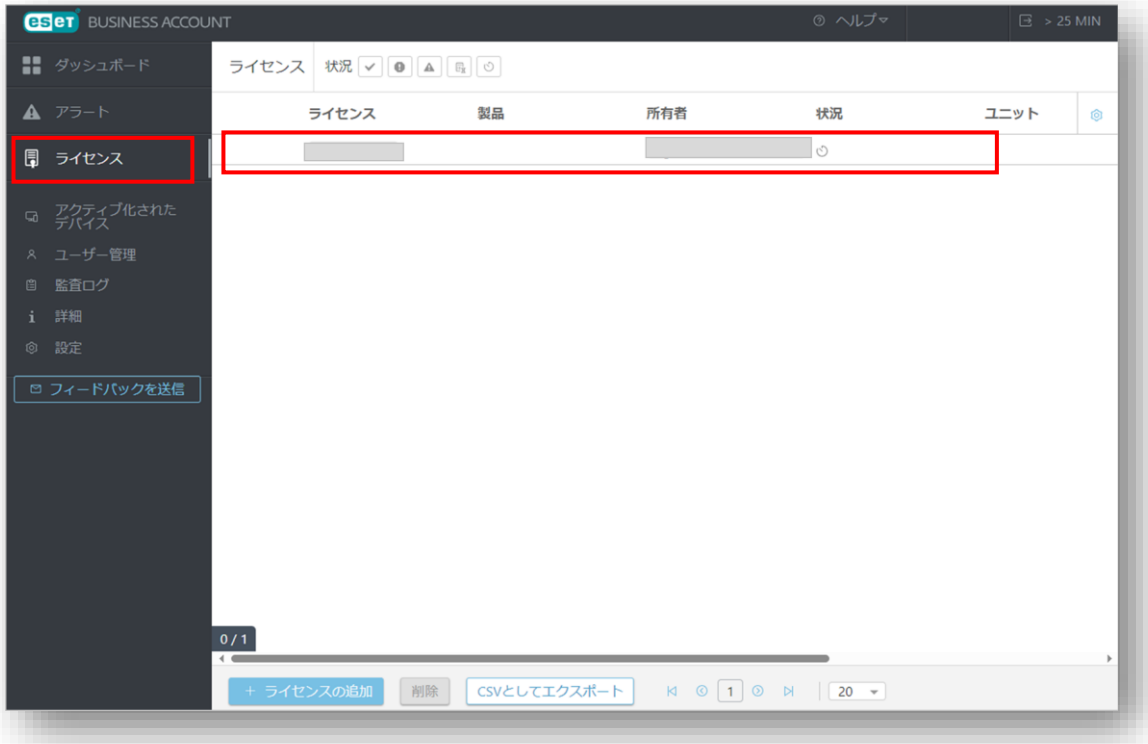
2. プログラムの導入 ~ ESET製品を新規導入の場合~

2. ライセンスのアクティベーション
   ※ ライセンス契約時の電子メールアドレスにアクティベーションメールが送信されます。
3. ライセンスが追加されたことの確認

■ライセンスアクティベーション時のメール例



■ライセンスが登録されたことの確認画面例



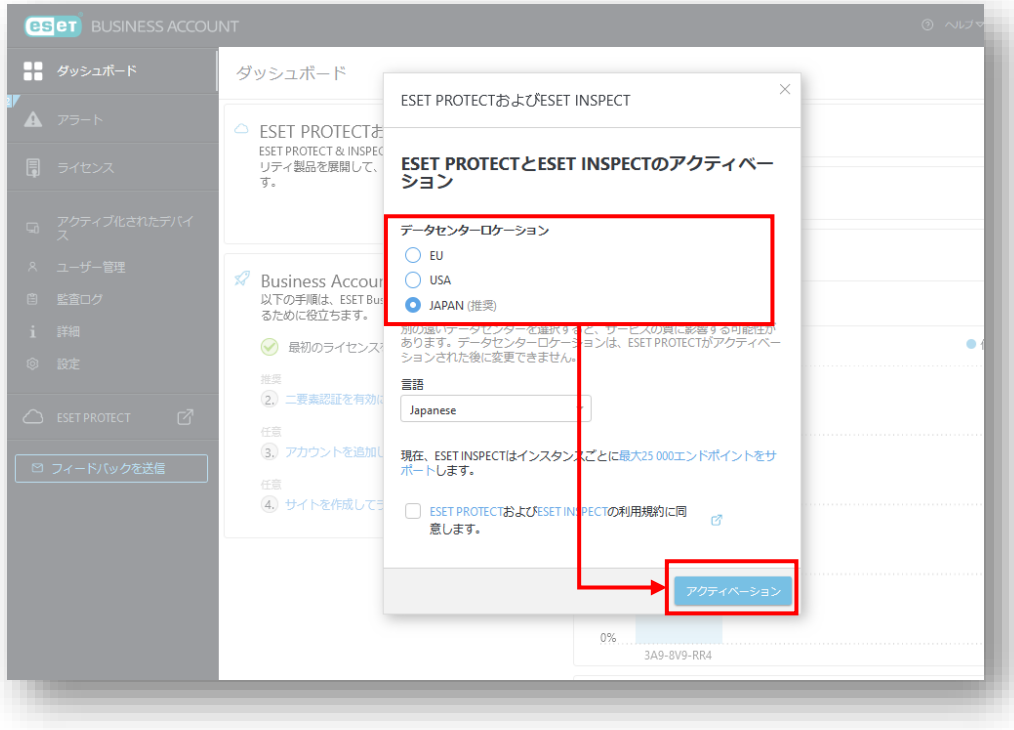
2. プログラムの導入 ~ ESET製品を新規導入の場合~

2. プログラムの導入 ~ ESET製品を新規導入の場合~

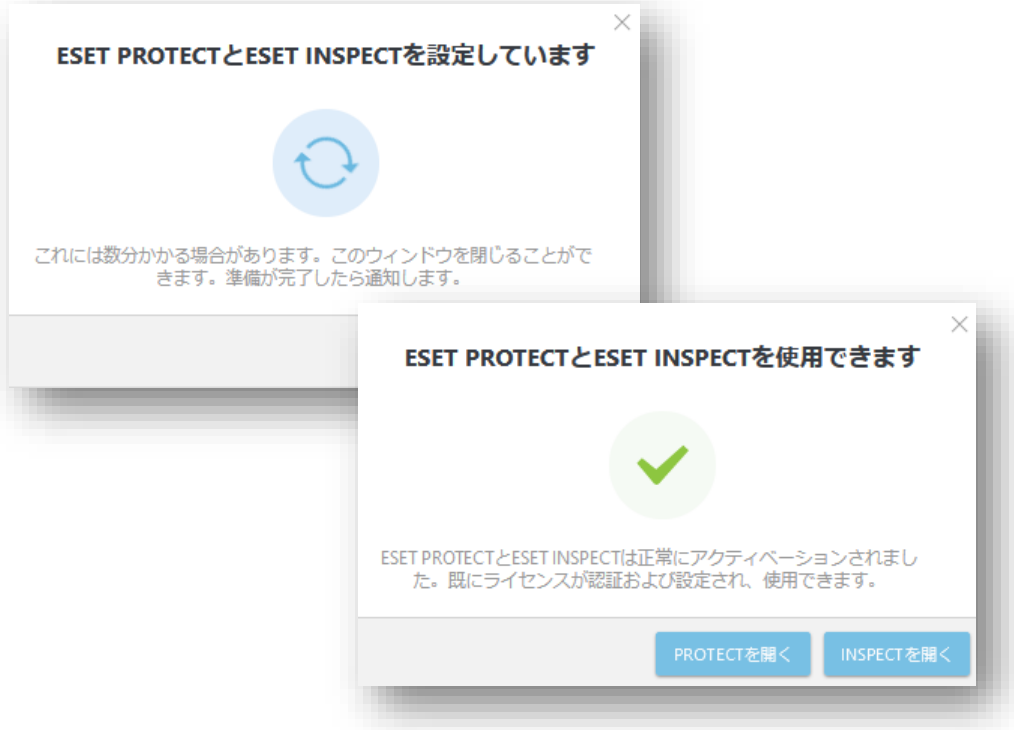
STEP3. EP/EIのアクティベーション

1. EPとEIのアクティベーション（左側メインメニューの「ESET PROTECT 」をクリックして開始します）
2. 10分～15分でアクティベーション完了
   ※ データセンターのロケーション選択画面では必ずJAPANを選択してください。
   ※ ESET PROTECT とESET Inspect が同時にアクティベーションされます。

■データセンターのロケーション選択画面



■ESET PROTECT アクティベーション画面



2. プログラムの導入 ~ ESET製品を新規導入の場合~

2. プログラムの導入 ~ ESET製品を新規導入の場合~

STEP4. プログラムの展開

- プログラムの展開の流れは以下になります。
  ※ EPとEIをご利用いただくにはクライアント用プログラムの他に以下のプログラムのインストールが必要です。
  - EMエージェント（クライアントとEPの接続に使用）
  - EI Connector（クライアントとEIの接続に使用）

1.静的グループの作成（任意）

- クライアントが所属するグループを作成します。
  事前に静的グループを作成し、インストーラーに静的グループ情報を組み込むことで、管理後のグルーピング負荷を軽減できます。

2.ポリシーの作成（任意）

- クライアントの各種設定を行うポリシーを作成します。ポリシーはインストーラーに組み込んでインストール時の初期設定値を変更することが可能です。
  ※ グループやクライアントに配布することで一括での設定変更も可能です。

3.インストーラーによる展開
または
ソフトウェアインストールタスクによる展開

- **新規インストールする場合（EMエージェント未インストール）**
  - **Windowsの場合**
    EMエージェント/EI Connector/クライアント用プログラムを一括インストールするためのライブインストーラーを作成します。
  - **macOSの場合**
    EMエージェント/クライアント用プログラムを一括インストールするためのライブインストーラーを作成します。インストール後、EI Connectorをソフトウェアインストールタスクでインストールします。
  - **Linuxの場合**
    EMエージェントインストールするためのライブインストーラーを作成します。インストール後、EI Connector/クライアント用プログラムをそれぞれソフトウェアインストールタスクでインストールします。
- **追加インストールする場合（EMエージェントインストール済）**
  ソフトウェアインストールタスクでクライアントにEI Connectorをインストールします。
  EI Connector/クライアント用プログラムのバージョンアップもソフトウェアインストールタスクを使用した本手順で対応が可能です。

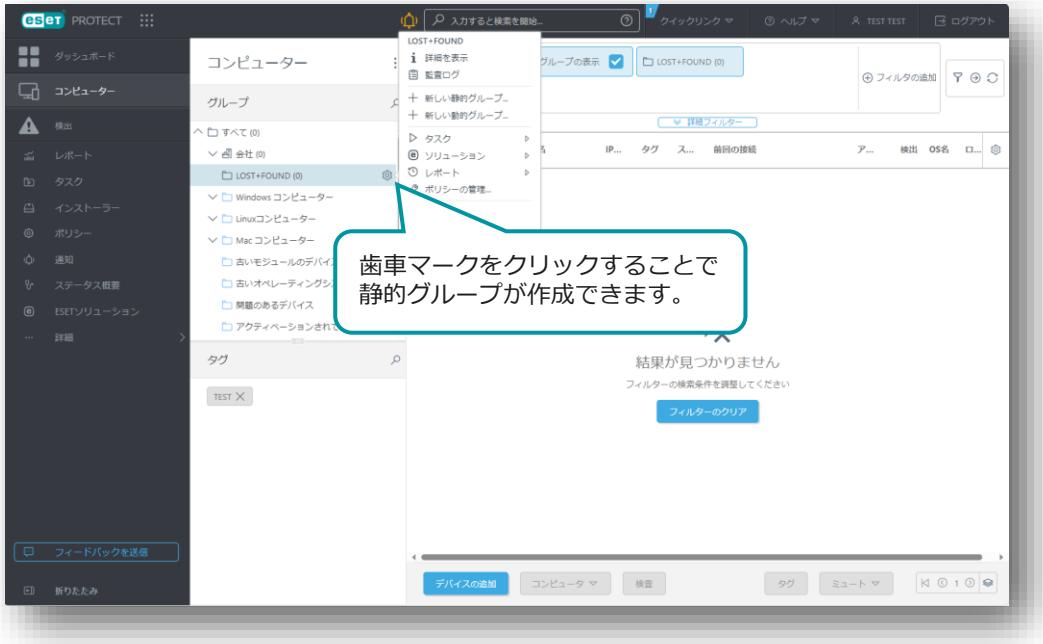
2. プログラムの導入 ~ ESET製品を新規導入の場合~

1. 静的グループの作成

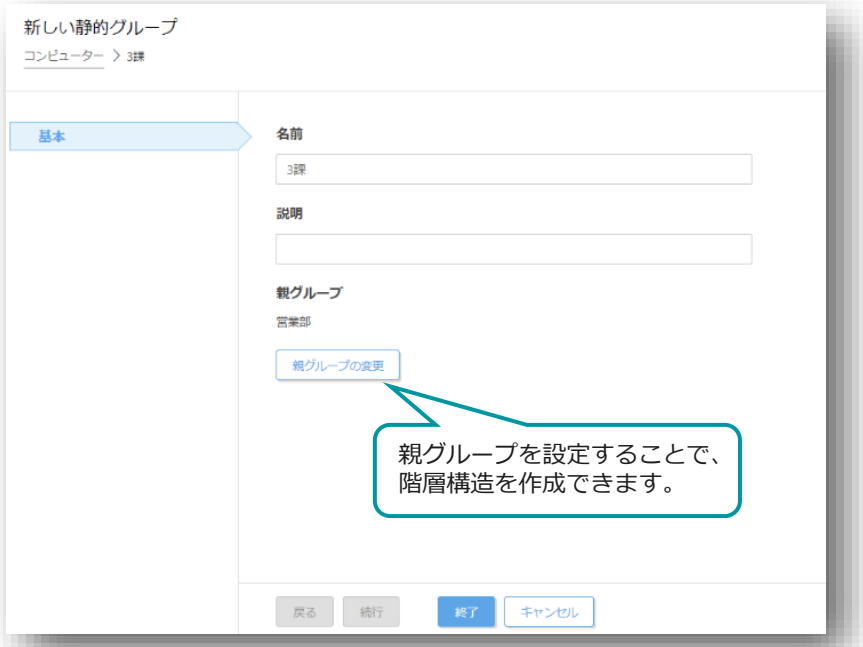
静的グループはメインメニュー「コンピューター」から作成可能です。
グループは階層構造も可能なため、柔軟に組織構造的を作成することができます。

1. メインメニューの「コンピューター」画面より、静的グループを作成する親グループの歯車マークを選択し、「新しい静的グループ」をクリックします。
2. 作成する静的グループの「名前」(必須)と「説明」(任意)を入力し、「終了」をクリックします。

■メインメニュー「コンピューター」画面



■静的グループ作成画面



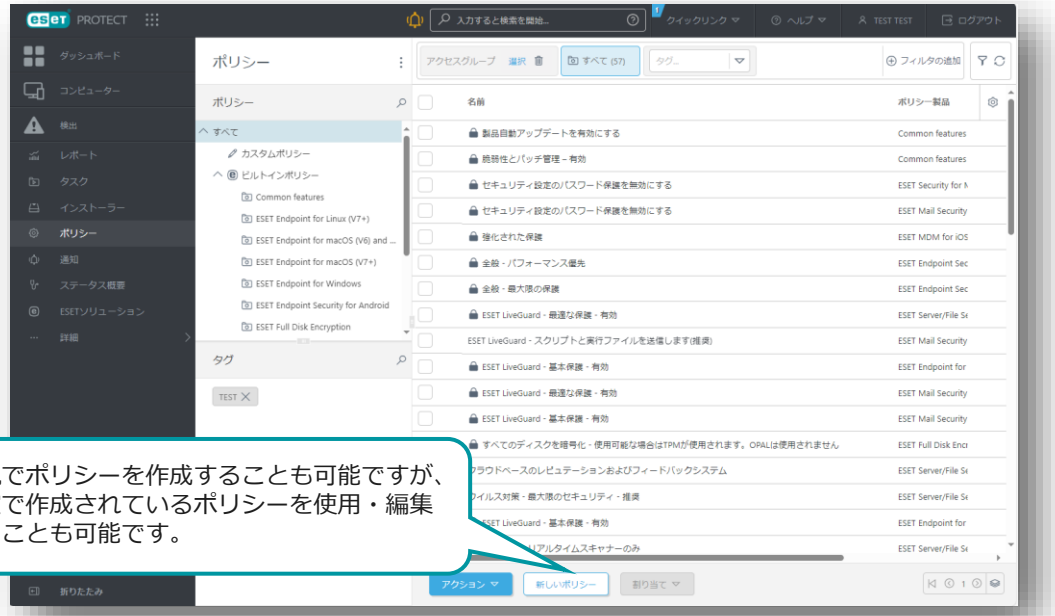
2. プログラムの導入 ~ ESET製品を新規導入の場合~

2. ポリシーの作成

クライアント用プログラムやEM Agent、EI Connectorに対して、検査の除外設定、
検出エンジンのアップデート先の設定、プロキシ設定など各種プログラムの設定を行います。

1. メインメニューの「ポリシー」画面より、「新しいポリシー」をクリックします。
2. 「基本」画面にて、ポリシーの「名前」を入力します。
3. 「設定」画面にて、ポリシーを作成するプログラムを選択し、各種設定を行います。
   （例:クライアント用プログラムの検査の除外設定やアップデート先の変更、プロキシの設定など）

■メインメニュー「ポリシー」画面



■ポリシー作成画面

2. プログラムの導入 ~ ESET製品を新規導入の場合~

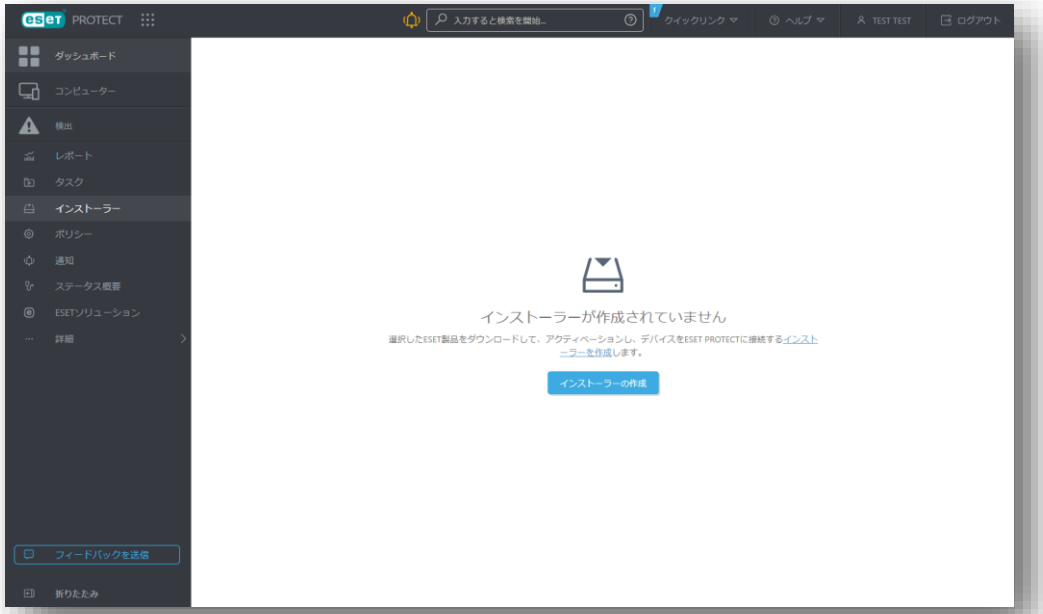
3. インストーラーの作成を行う場合(1/3)

EPメインメニュー「インストーラー」より、ライブインストーラーを作成します。

1. メインメニューの「インストーラー」画面より、「インストーラーの作成」をクリックします。
2. インストーラーの作成画面が表示されたら、「インストーラーのカスタマイズ」をクリックします。

※「インストーラーのカスタマイズ」を選択し、インストールにEI Connectorを含めたり、
クライアントが所属する親グループや事前に作成したポリシーを設定に含めることが可能です。

■メインメニュー「インストーラー」画面



■インストーラー作成画面(1/4)

※複数の静的グループがある場合は、静的グループごとにインストーラーを分けて作成する必要があります。

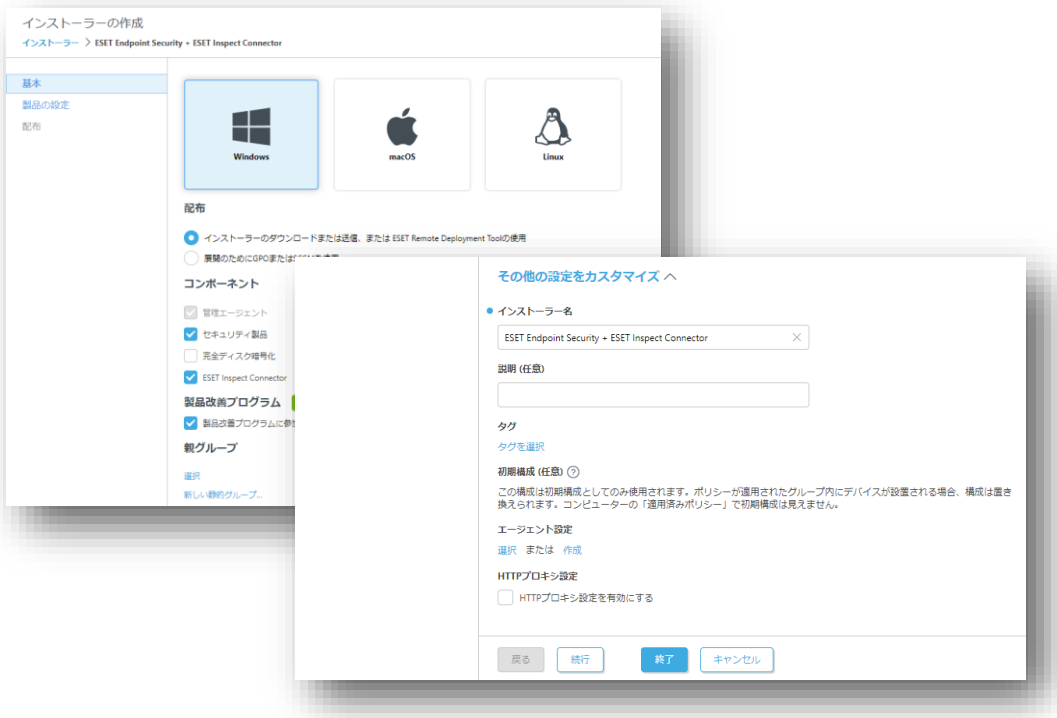
2. プログラムの導入 ~ ESET製品を新規導入の場合~

3. インストーラーの作成を行う場合(2/3)

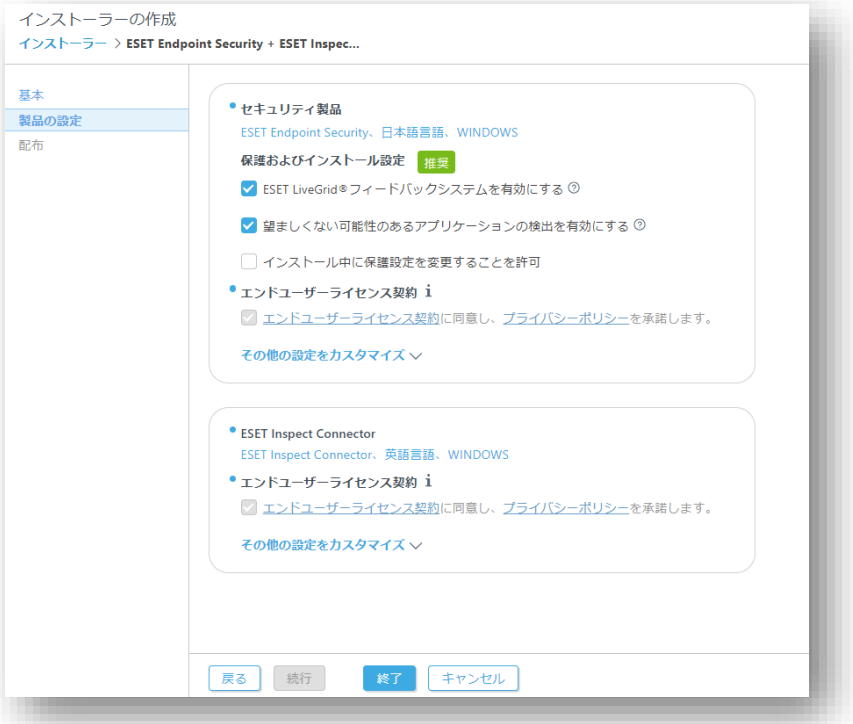
インストーラーに含めるコンポーネントやポリシー、親グループなどの各種設定を行います。

3. 「基本」画面では、インストーラーに含めるコンポーネントや親グループ、インストーラー名、ESET Management Agentに関する設定を行います。
4. 「製品の設定」画面では、インストーラー含めるセキュリティ製品のバージョンやポリシーの組み込みなどを行います。

■インストーラー作成画面(2/4)



■インストーラー作成画面(3/4)



2. プログラムの導入 ~ ESET製品を新規導入の場合~

3. インストーラーの作成を行う場合(3/3)

「配布」画面では作成したインストーラーの配布方法を検討します。

- インストーラーのダウンロードリンクが表示されるため、ダウンロードリンクのコピーやブラウザから直接ダウンロードが可能です。
- 電子メールアドレスを登録してメールでURLを配布することも可能です。（CSVで一括で電子メールアドレスを登録することも可能です。）

■インストーラー作成画面(4/4)

■電子メールプレビュー画面

2. プログラムの導入 ~ ESET製品を新規導入の場合~

Digital Security
Progress. Protected.

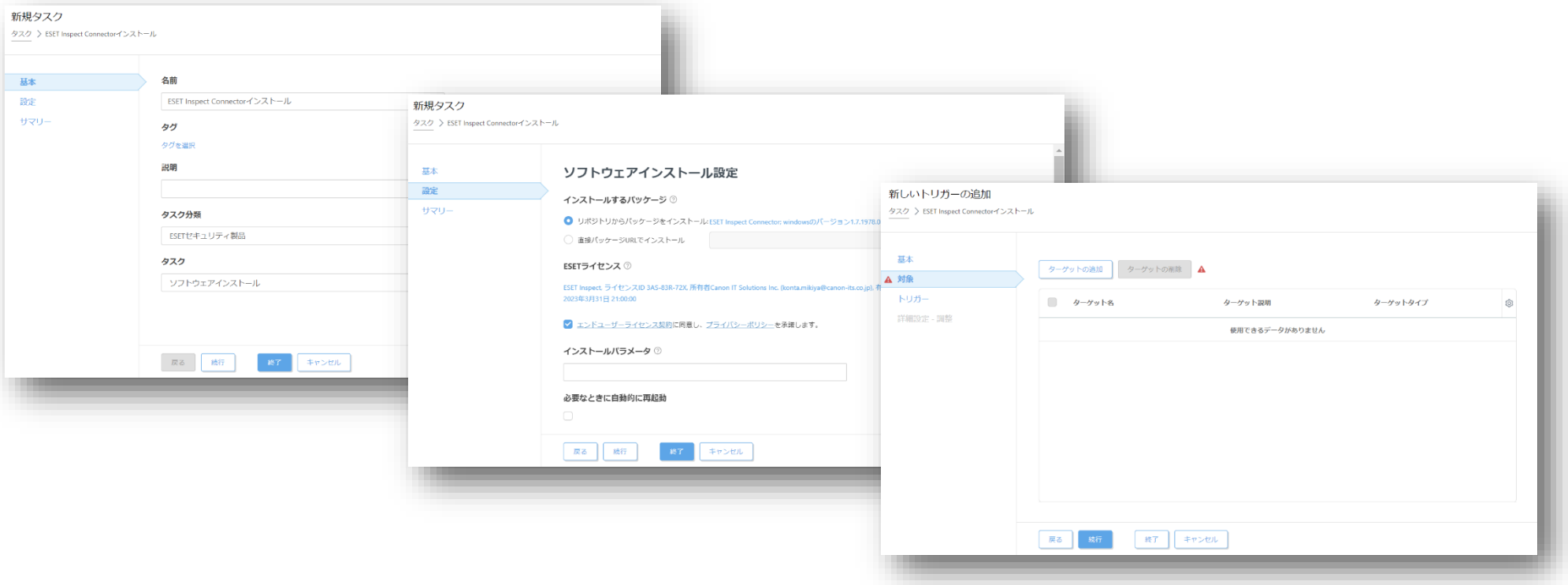
3. ソフトウェアインストールタスクを利用する場合

EPメインメニュー「タスク」より、「新規作成」-「クライアントタスク」を作成します。

メインメニューの「タスク」画面より、「新規作成」-「クライアントタスク」をクリックします。

1. 基本画面でタスク分類を「すべてのタスク」または「ESETセキュリティ製品」、タスクを「ソフトウェアインストールタスク」を選択します。
2. 設定画面でインストールするパッケージから「ESET Inspect Connector」を選択し、ESETライセンスで「ESET Inspect」が選択されていることを確認します。
3. トリガー作成では、EI Connectorをインストールするクライアントまたはグループを選択し、タスク実行のタイミングであるトリガーを設定します。

■ソフトウェアインストールタスク画面



Ⅲ.メール通知の設定作業について

通知メール設定

ESET PROTECT MDR Liteでは、お客様環境でインシデントと疑われる検出が発生すると、ESET Inspect上にインシデントが作成されます。必要に応じて、ESET社のセキュリティエンジニアによりインシデントに対するコメント(英語)が追加されます。また、検出の内容によっては、自動で端末のネットワーク隔離が実施されるため、これらが発生した場合に即座に管理者の方へ通知するための設定を必ず行ってください。これらの通知を受け取ることで、迅速に状況を把握することができます。

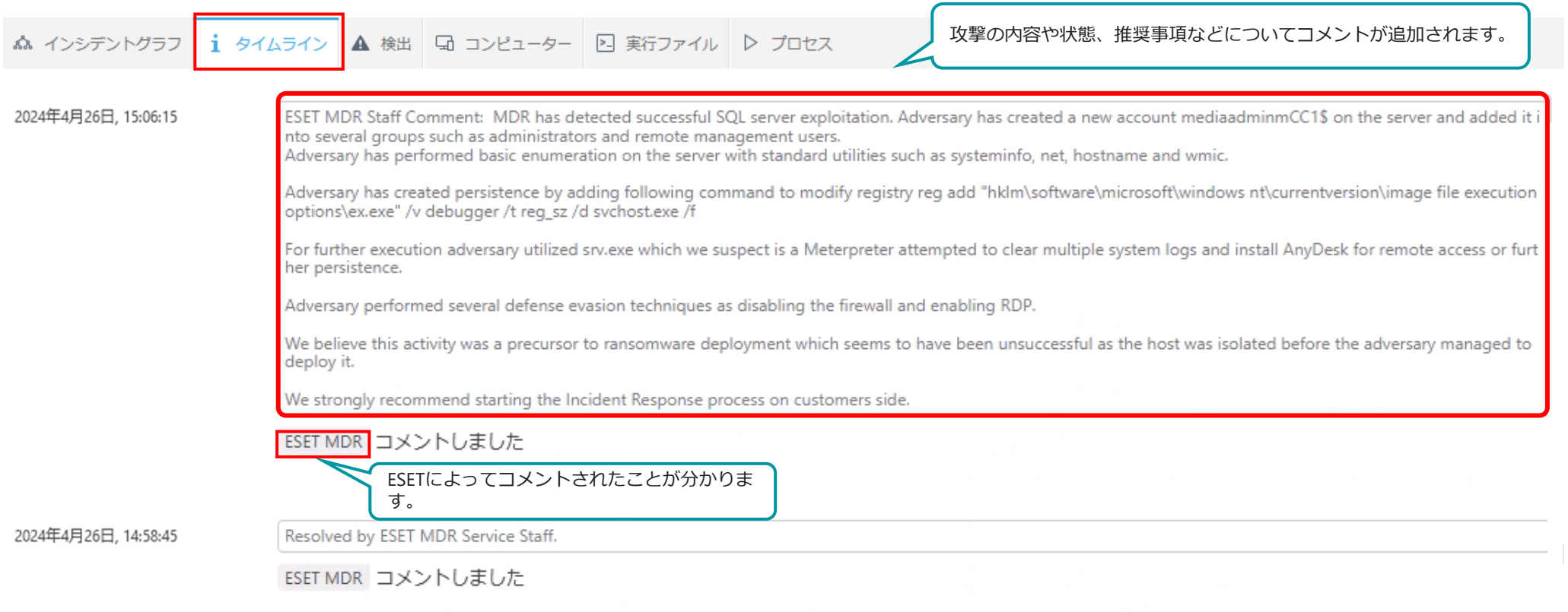
■インシデント作成レポート メールサンプル

■インシデント作成通知メールサンプル

■ネットワーク隔離通知メールサンプル

通知メール設定

ESET社のセキュリティエンジニアからのコメントは作成されたインシデントのタイムライン上で確認可能です。
英語でインシデントの詳細や対処などについて記載されます。

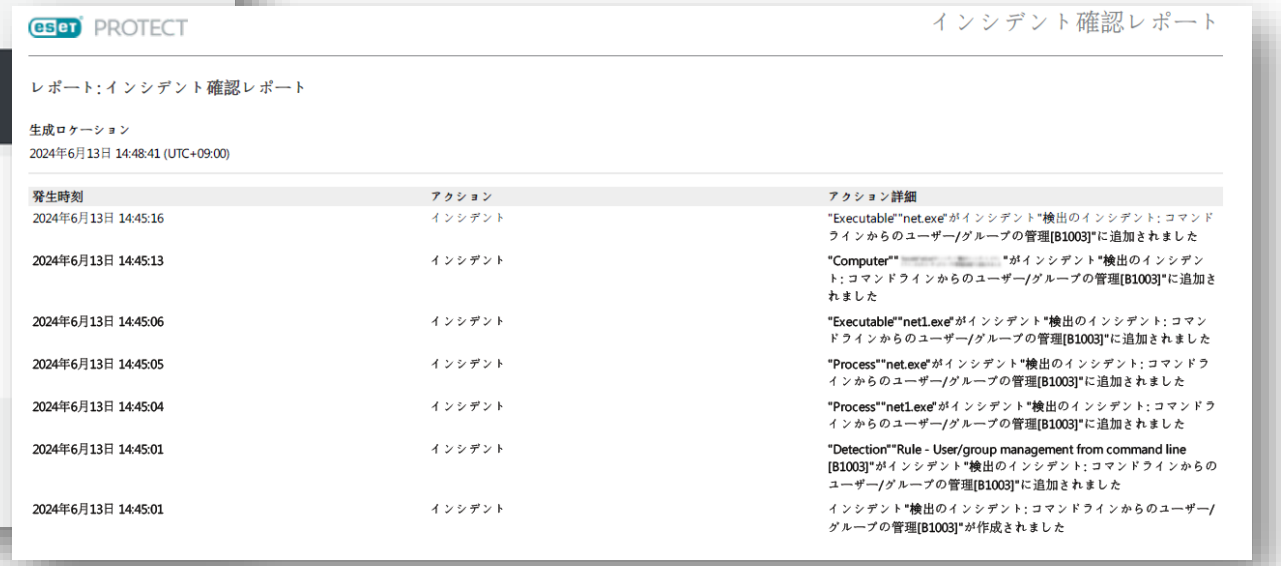


通知メール設定 1. インシデント作成レポートの作成方法

お客様のESET Inspectでインシデントが作成された際に、メールでレポートを送付する設定ができます。
本設定を行うことで過去1時間以内のインシデント発生を確認することができ、インシデントの把握漏れを防ぐことが可能です。

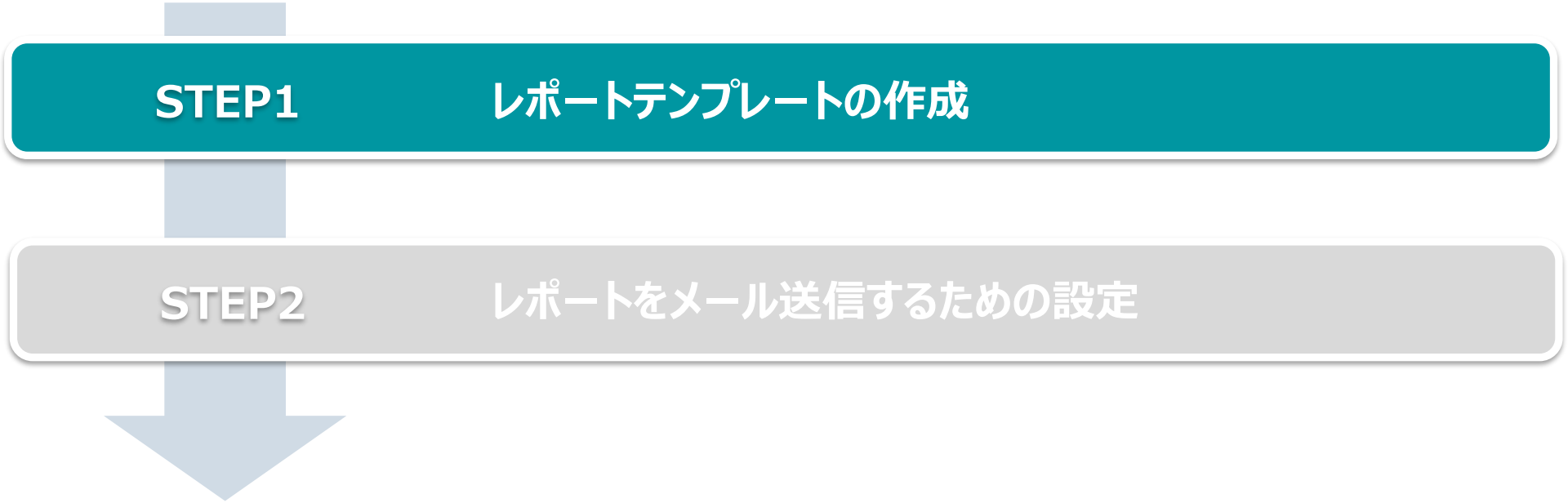
■インシデント作成レポート メールサンプル

■インシデント確認レポート メールサンプル



通知メール設定 1. インシデント作成レポートの作成方法

インシデント作成レポートを受け取るための作成手順として、必要なステップは以下の通りです。

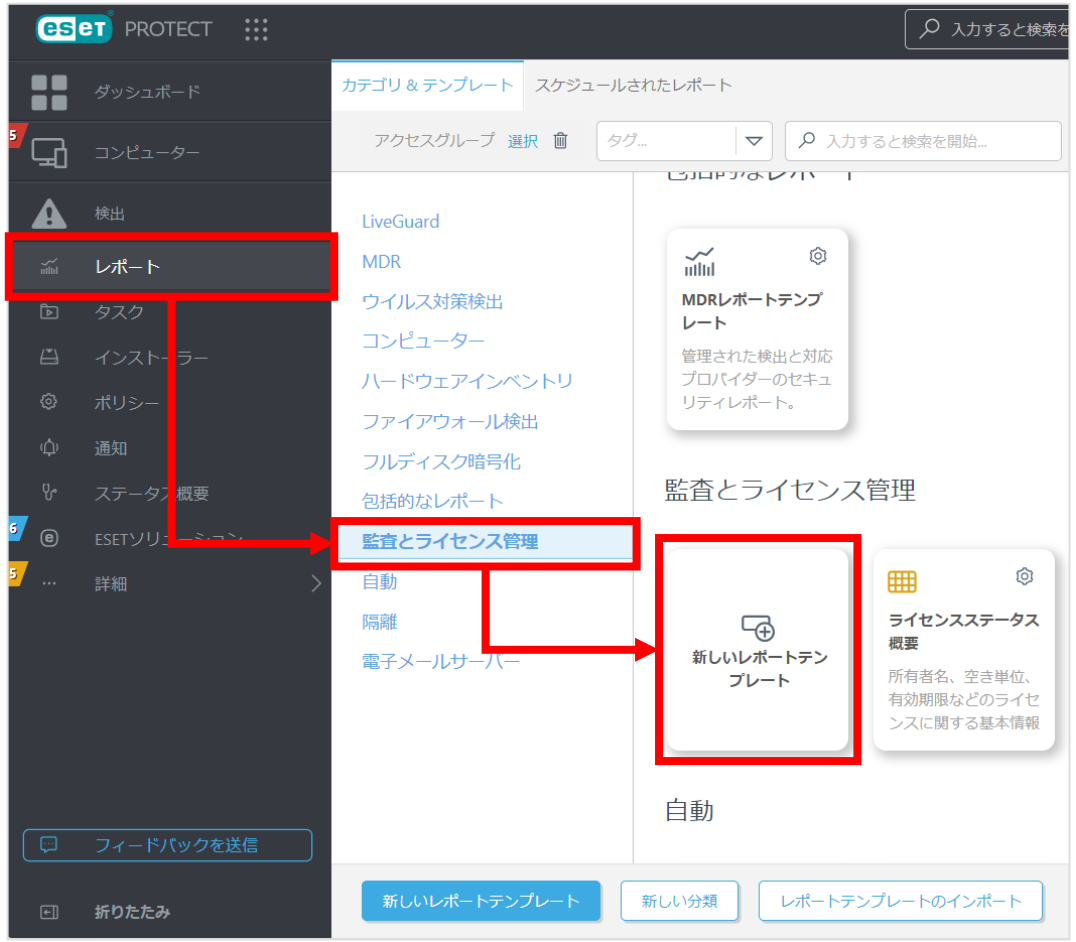


通知メール設定 1. インシデント作成レポートの作成方法

STEP1.レポートテンプレートの作成

監査ログから1時間以内のインシデントを抽出するレポートのテンプレートを作成します。

1.ESET PROTECTログイン後、［レポート］→
　[監査とライセンス管理] →
　[新しいレポートテンプレート]をクリックします。



通知メール設定 1. インシデント作成レポートの作成方法

2. ［基本］をクリックし、任意の名前（例：インシデント確認レポート）を入力します。
※ ［説明］の入力は任意です。

通知メール設定 1. インシデント作成レポートの作成方法

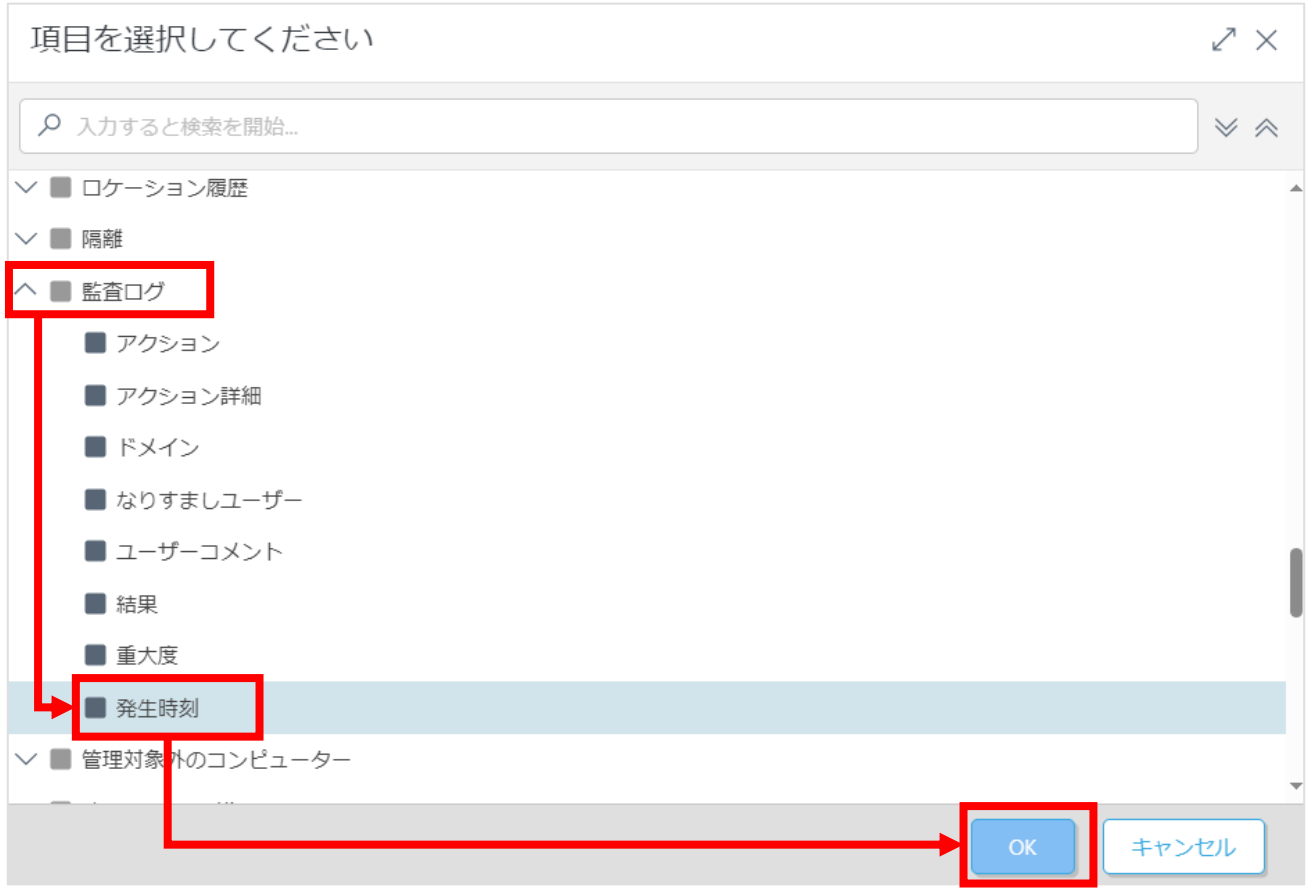
3. [グラフ] をクリックし、[表示テーブル]のチェックボックスにチェックを入れます。

通知メール設定 1. インシデント作成レポートの作成方法

4. [データ] をクリックし、[列の追加]をクリックします。

通知メール設定 1. インシデント作成レポートの作成方法

5.項目一覧より[監査ログ]を展開し、[発生時刻]を選択し[OK]をクリックします。



通知メール設定 1. インシデント作成レポートの作成方法

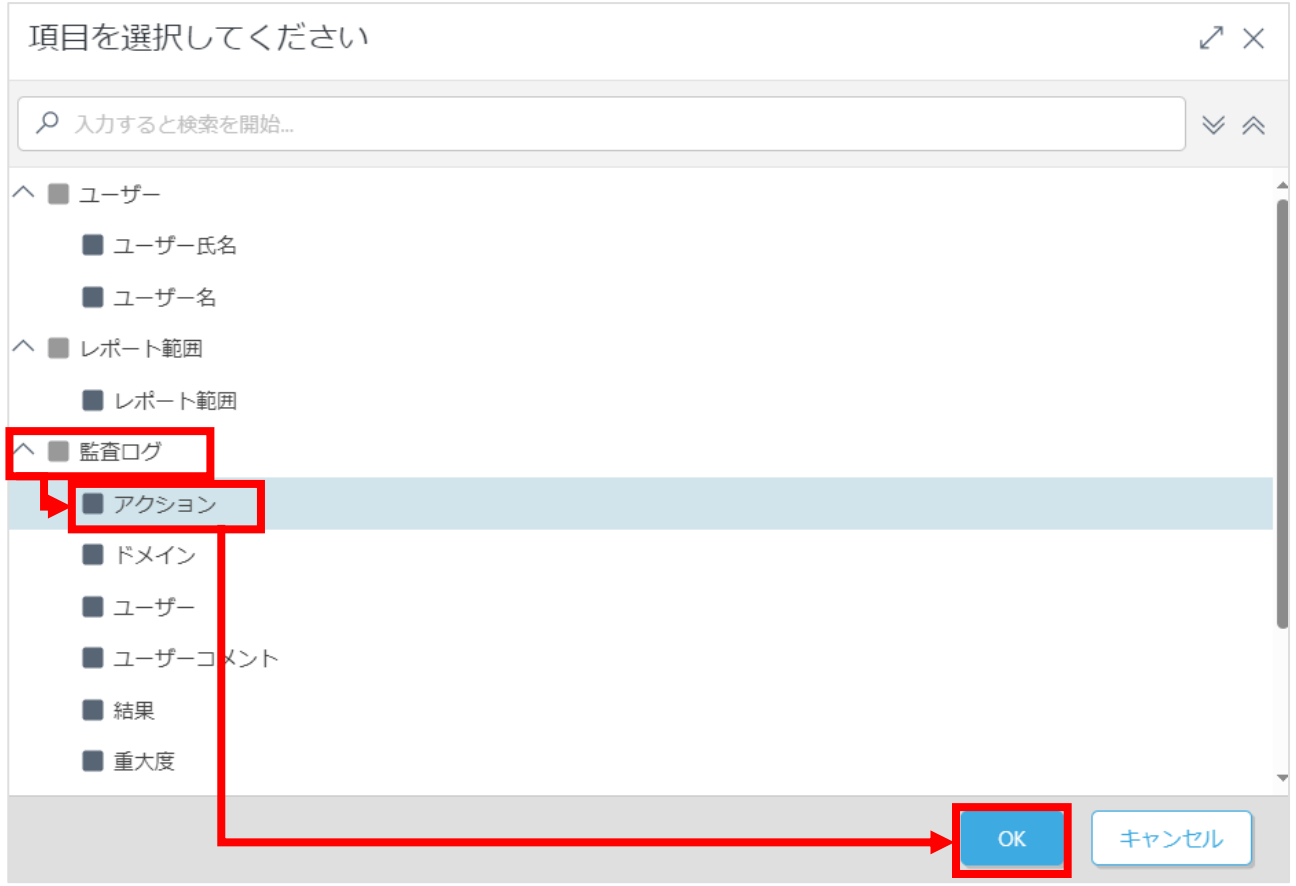
6.手順5の作業を繰り返し、続けてテーブル列に[監査ログ.アクション]と[監査ログ.アクション詳細]を追加します。

通知メール設定 1. インシデント作成レポートの作成方法

7. [フィルタ] を展開し、[フィルタの追加]をクリックします。

通知メール設定 1. インシデント作成レポートの作成方法

8.項目一覧より[監査ログ]を展開し、[アクション]を選択し[OK]をクリックします。



通知メール設定 1. インシデント作成レポートの作成方法

9.フィルタの条件を画像のように「=(等しい)」「インシデント」に変更します。

通知メール設定 1. インシデント作成レポートの作成方法

10.再度[フィルタの]追加をクリックし、項目一覧より[監査ログ]を展開し、[発生時刻]→[相対的な時間間隔(発生時間)]を選択して[OK]をクリックします。

通知メール設定 1. インシデント作成レポートの作成方法

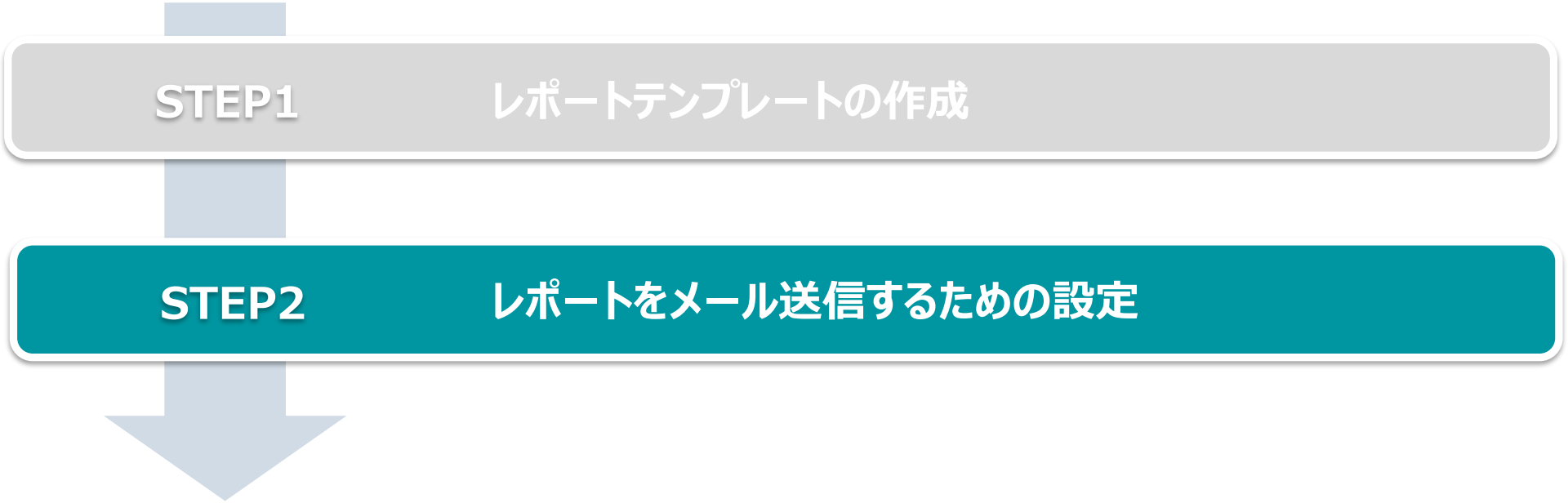
11.フィルタの条件を画像のように「=(等しい)」「1時間前と現在の間」に変更します。

通知メール設定 1. インシデント作成レポートの作成方法

12.[サマリー]をクリックし、内容に問題がなければ[終了]をクリックし作成を完了します。

通知メール設定

1. インシデント作成レポートの作成方法

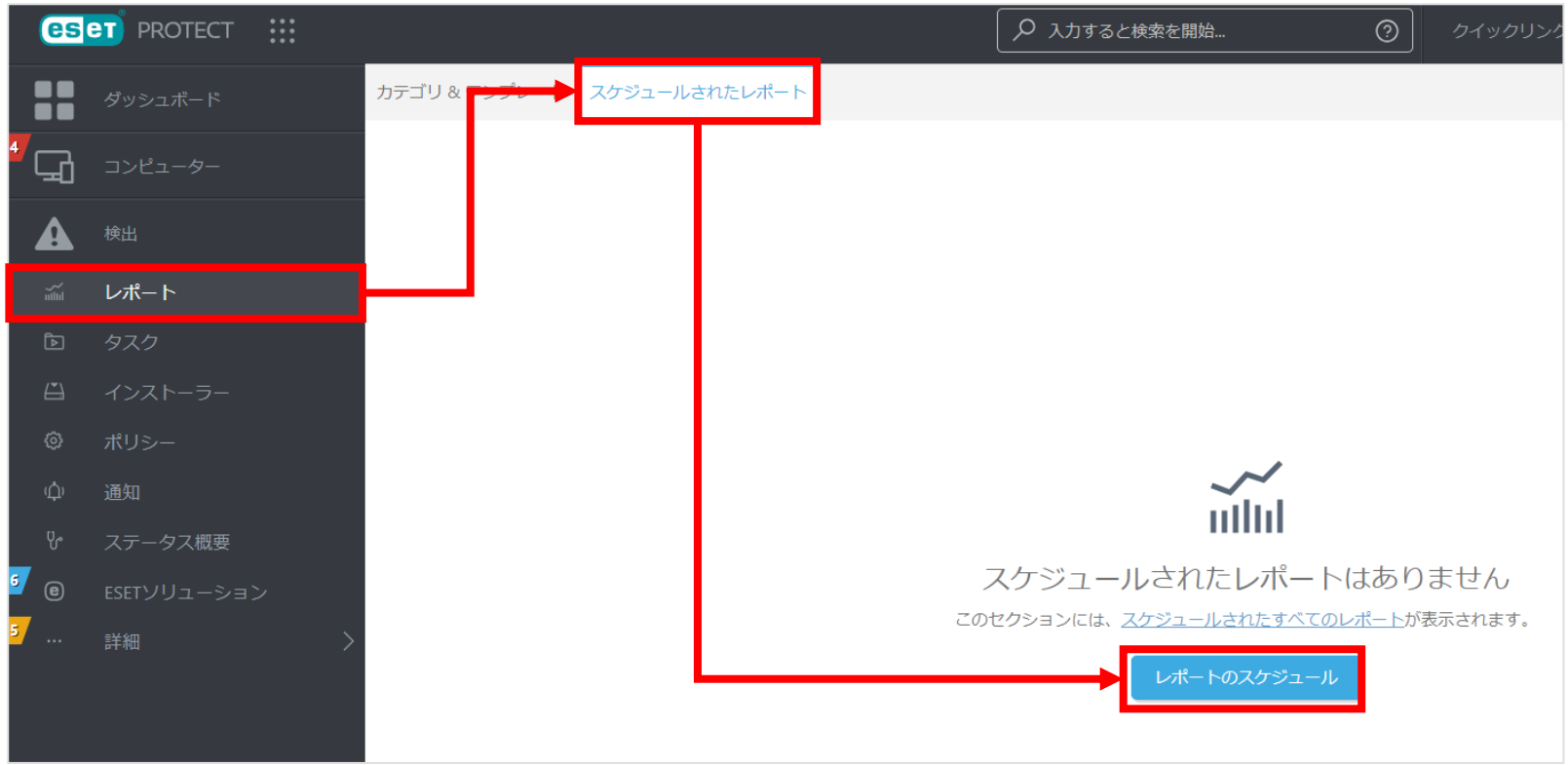


通知メール設定 1. インシデント作成レポートの作成方法

STEP2.レポートをメール送信するための設定

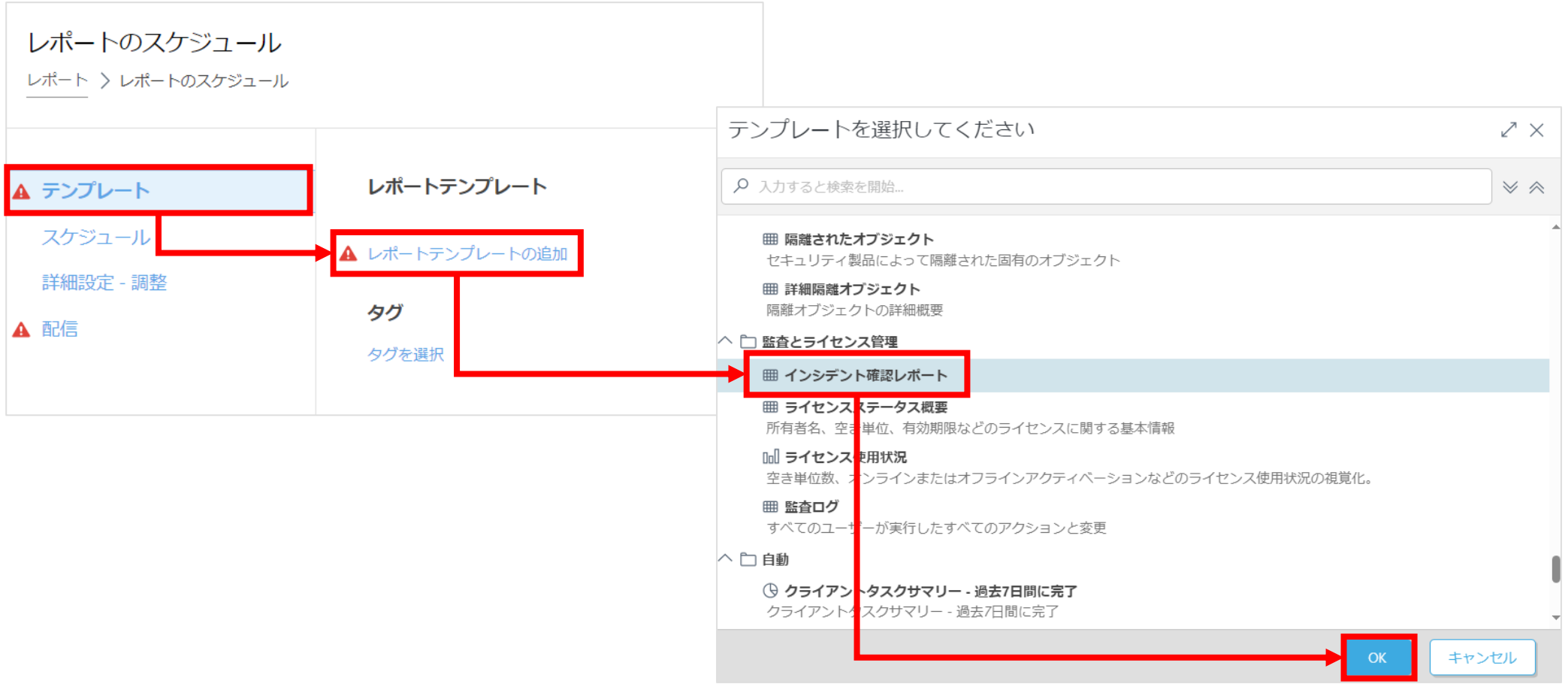
STEP1で作成したテンプレートを1時間に1回メール送信するためのスケジュールを作成します。

1.ESET PROTECTログイン後、［レポート］→[スケジュールされたレポート]→[レポートのスケジュール]をクリックします。



通知メール設定 1. インシデント作成レポートの作成方法

2.［テンプレート］→ ［レポートテンプレート］クリックし、テンプレート一覧よりSTEP1で作成した
［インシデント確認レポート］を選択して［ OK ］をクリックします。



通知メール設定 1. インシデント作成レポートの作成方法

3.［スケジュール］をクリックし、トリガータイプから［CRON式］を選択し、［CRON式］のテキスト欄には［0 0 * * * ? * ］と入力します。※CRON式の文字間には半角スペースを入力してください。

通知メール設定 1. インシデント作成レポートの作成方法

4.［配信］をクリックし、各項目を設定します。

■**送信先**

→任意のメールアドレスを入力します。
複数の場合はカンマで区切ります。

■**メッセージをカスタマイズ**

→チェックを入れます。

■**件名、メッセージ**

→それぞれ任意の内容を入力します。

■**レポートが空の場合にメールを送信**

→チェックを外します。

※チェックを外さないとインシデントが発生していない場合もメールが送信されますので、必ずチェックを外してください。

5.［終了］をクリックします。

通知メール設定 2.インシデント作成通知メール作成方法

お客様のESET Inspectでインシデントが作成された際に、メールで通知する設定ができます。
本設定を行うことで、インシデントの疑いがあるものを検知したことを迅速に把握し、素早い内容確認と影響を受ける可能性があるコンピュータの詳細を確認することができます。

■インシデント作成通知メールサンプル

通知メール設定 2.インシデント作成通知メール作成方法

1.ESET PROTECTログイン後、［通知］→[新しい通知]をクリックします。

通知メール設定 2.インシデント作成通知メール作成方法

2.[基本]を開き、[名前]に任意の名前を入力し、有効にします。

通知メール設定 2.インシデント作成通知メール作成方法

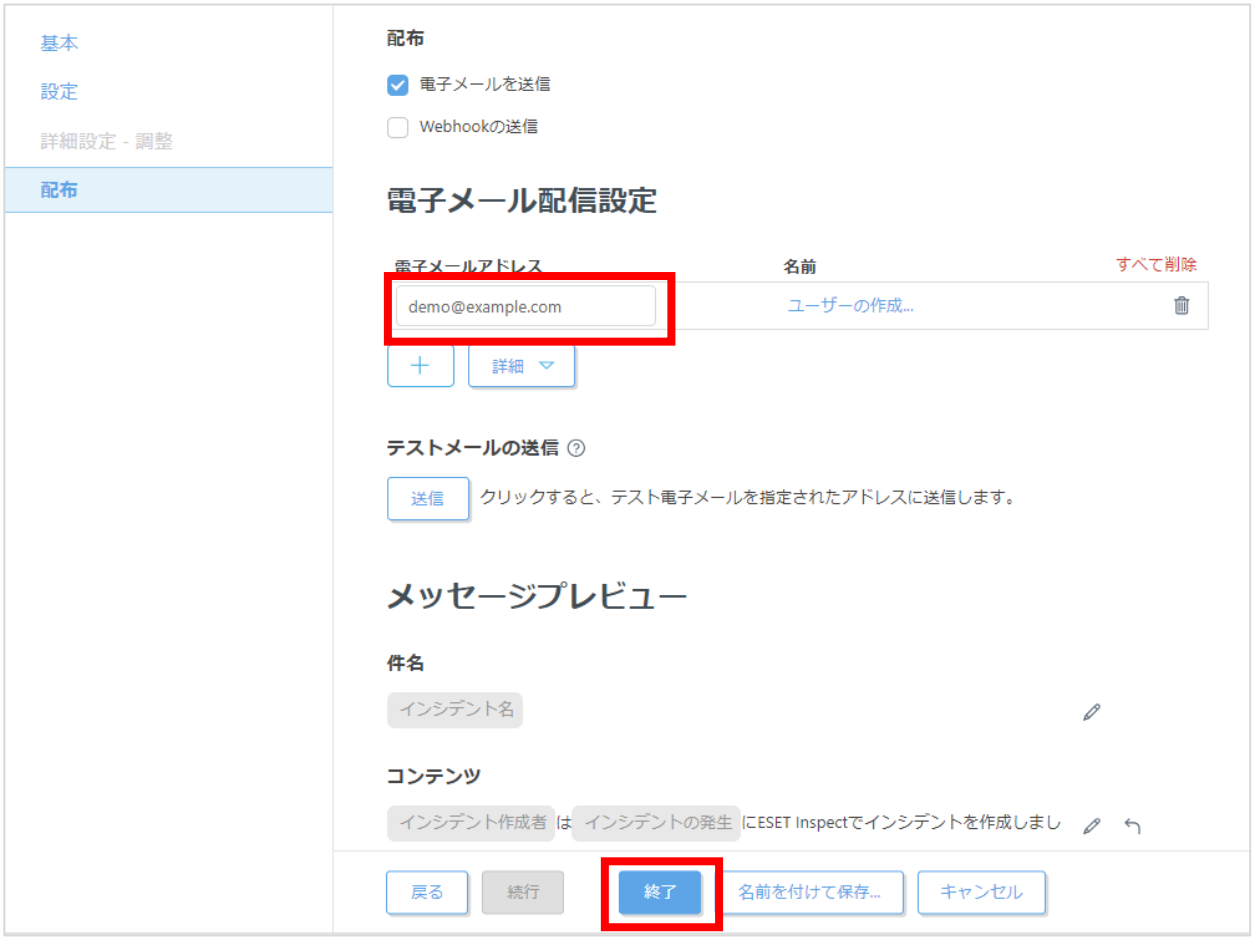
3.[設定]の各項目は以下のように設定します。

- [イベント]：[管理されたコンピューターまたはグループのイベント]を選択します。
- [カテゴリ]：[ESET Inspectインシデント]を選択します。
- 監視された静的グループ：任意のグループを選択します。

通知メール設定 2.インシデント作成通知メール作成方法

4. [配布]を開き、任意のメールアドレスを指定して[終了]をクリックします。

※[+]をクリックし複数の宛先を指定可能です。



通知メール設定

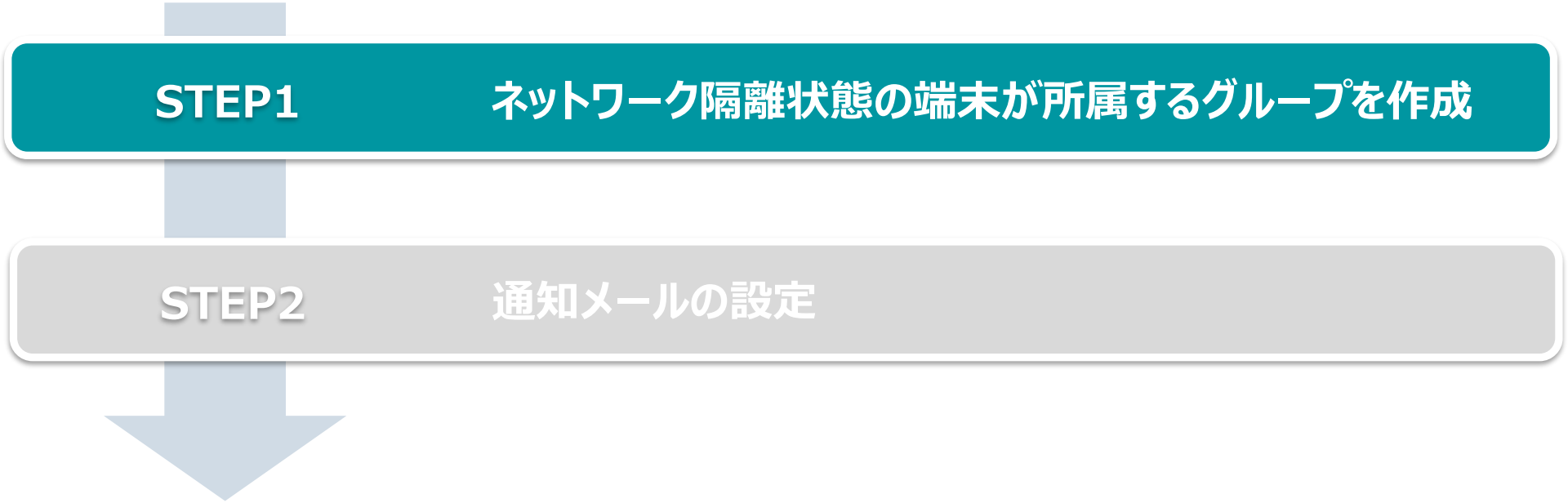
3.ネットワーク隔離通知メール作成方法

ESET PROTECTで管理されている端末でネットワーク隔離が動作した際に、通知メールでお知らせします。
本設定を行うことで、迅速に隔離された端末を把握することが可能です。。

■ネットワーク隔離通知メールサンプル

通知メール設定 3.ネットワーク隔離通知メール作成方法

ネットワーク隔離隔離通知メールを受け取るための作成手順として、必要なステップは以下の通りです。

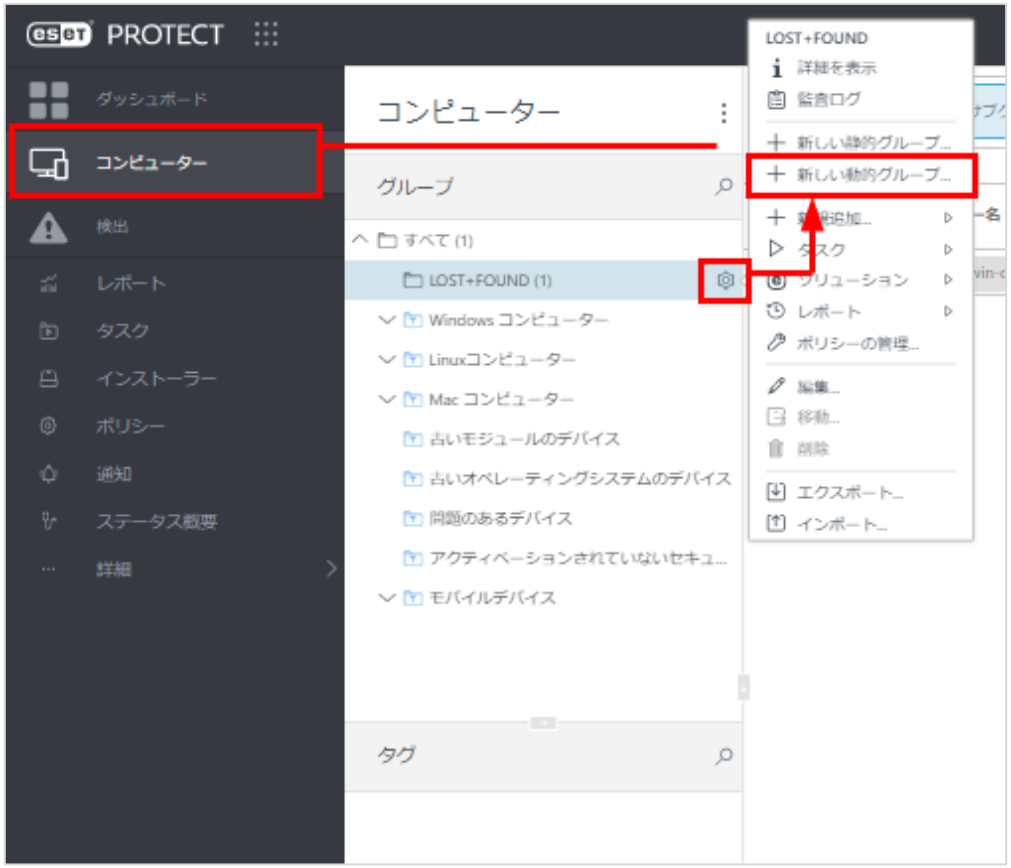


通知メール設定 3.ネットワーク隔離通知メール作成方法

STEP1.ネットワーク隔離状態の端末が所属するグループを作成

1.ネットワーク隔離状態の端末が所属するグループを作成します。

［コンピューター］→親グループに指定するグループの右横にある歯車アイコンをクリックして、［新しい動的グループ］をクリックします。



通知メール設定 3.ネットワーク隔離通知メール作成方法

2.［基本］を展開し、任意の名前（例：ネットワーク隔離グループ）を入力します。
※ ［説明］の入力は任意です。

通知メール設定 3.ネットワーク隔離通知メール作成方法

3.［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。

通知メール設定 3.ネットワーク隔離通知メール作成方法

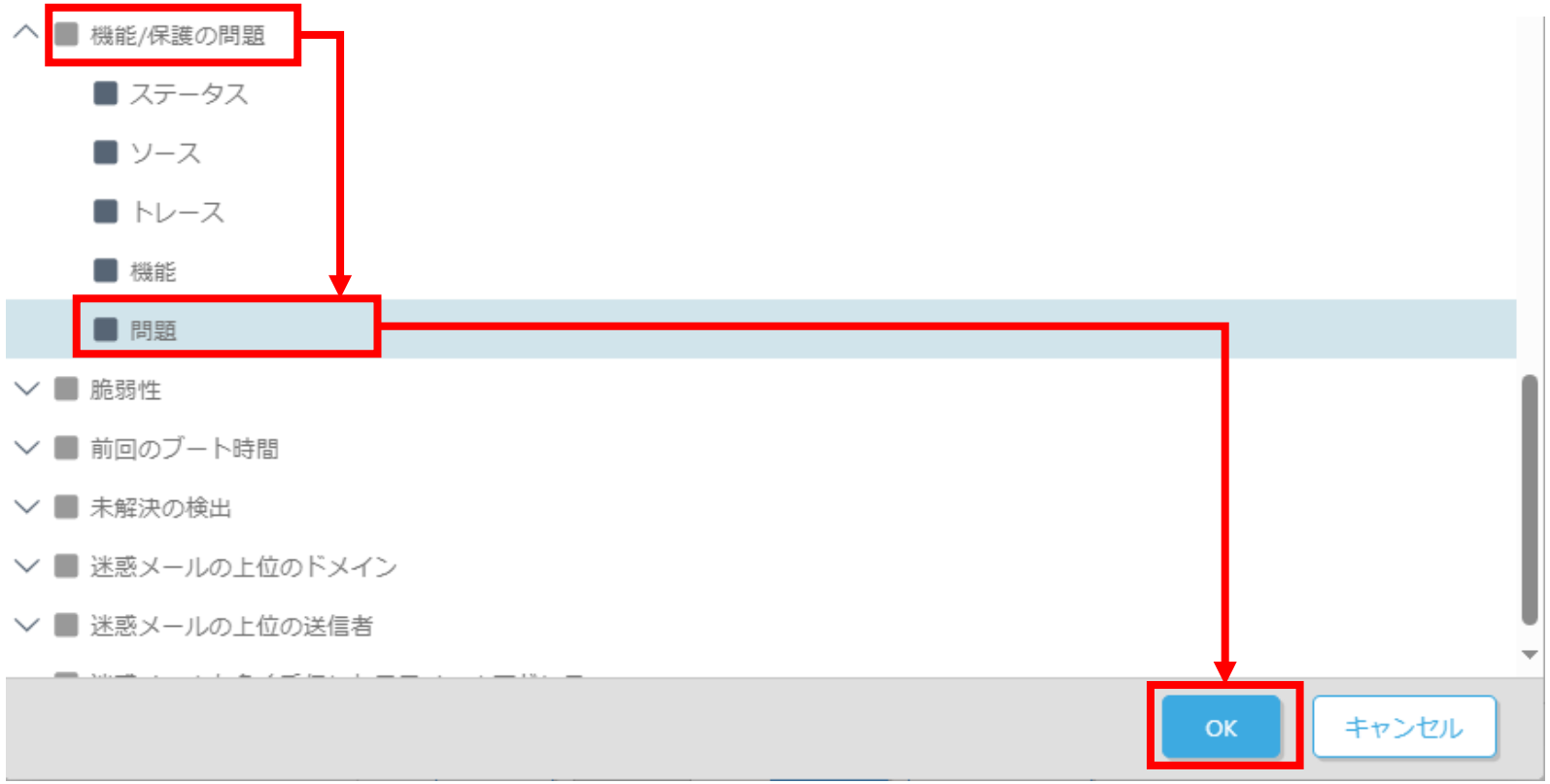
4.［基本］を展開し、任意の名前（例：ネットワーク隔離）を入力します。
※ ［説明］の入力は任意です。

通知メール設定 3.ネットワーク隔離通知メール作成方法

5. ［式］を展開し、［処理］のプルダウンリストから［AND（すべての条件が真であること）］を選択し、［ルールの追加］をクリックします。

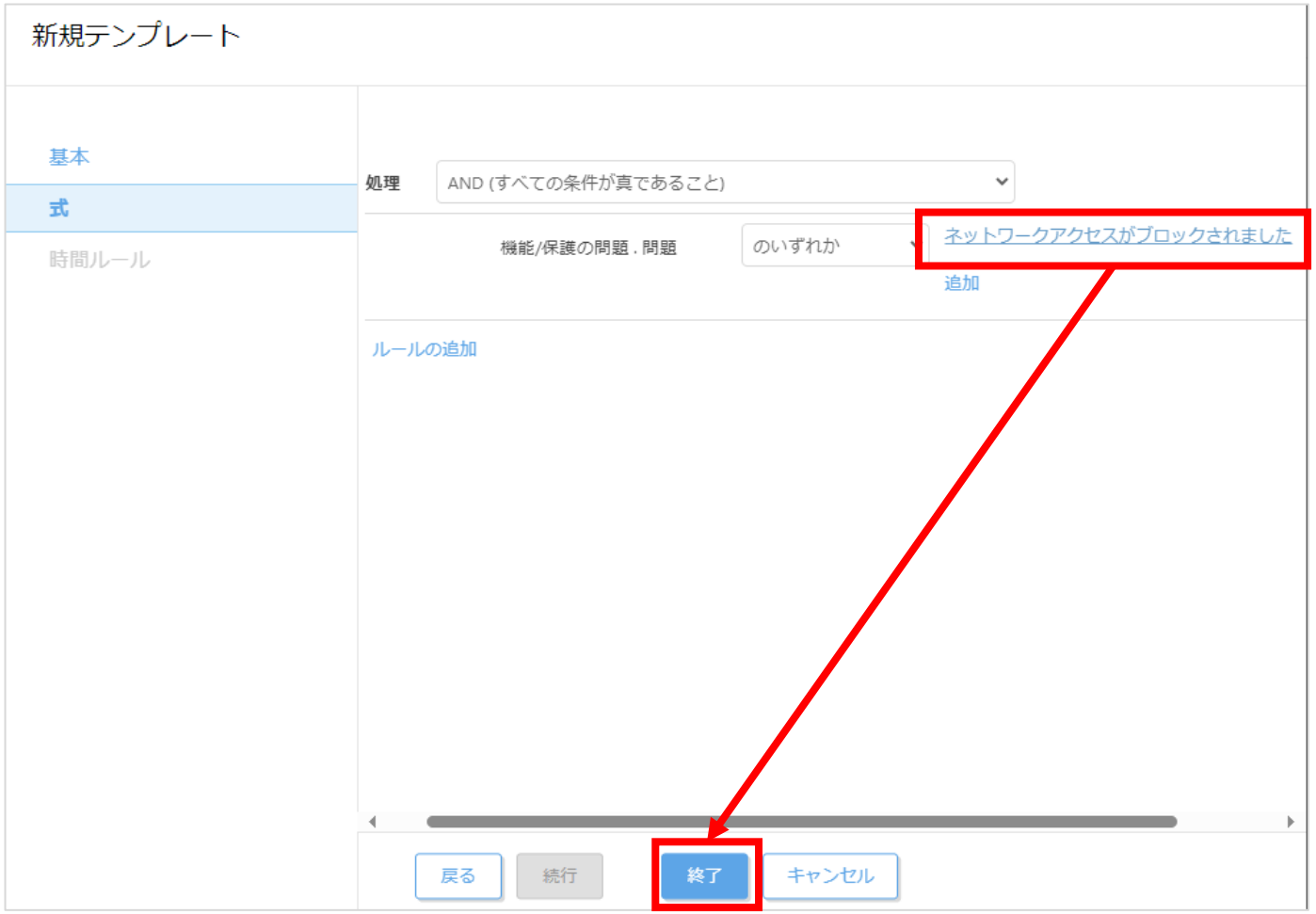
通知メール設定 3.ネットワーク隔離通知メール作成方法

6.［機能/保護の問題］→［問題］をクリックし、［OK］ボタンをクリックします。



通知メール設定 3.ネットワーク隔離通知メール作成方法

7.値の選択欄で[ネットワークアクセスがブロックされました]を選択して[終了]をクリックします。



通知メール設定

3.ネットワーク隔離通知メール作成方法

STEP1 ネットワーク隔離状態の端末が所属するグループを作成

STEP2 通知メールの設定

通知メール設定 3.ネットワーク隔離通知メール作成方法

STEP2.通知メールの設定

1. ［通知］→[新しい通知]をクリックします。

通知メール設定 3.ネットワーク隔離通知メール作成方法

2.[基本]を開き、[名前]に任意の名前を入力し、有効にします。

通知メール設定 3.ネットワーク隔離通知メール作成方法

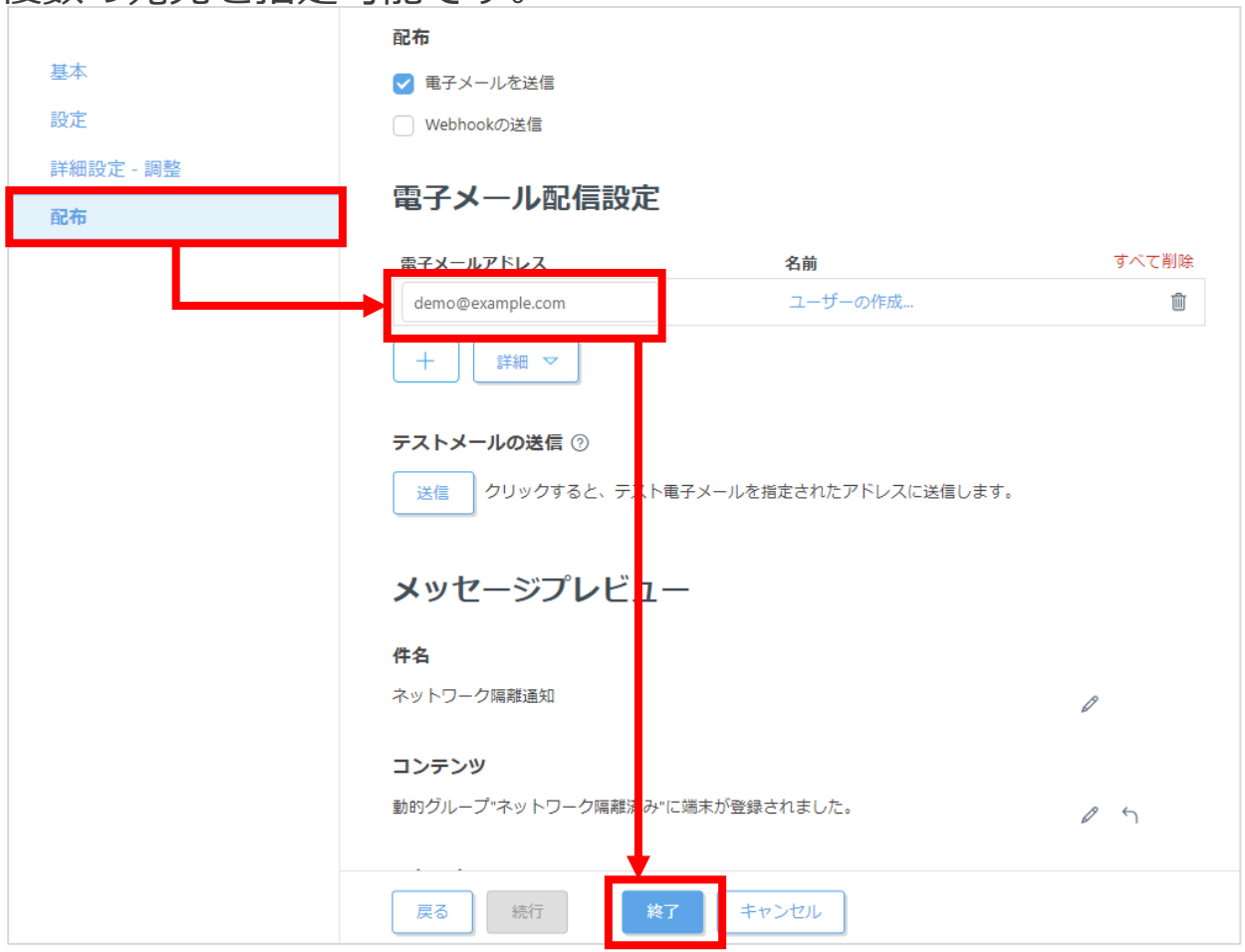
3.[設定]の各項目は以下のように設定します。

・[イベント]　　：[動的グループ変更]を選択します。
・[動的グループ]：[選択]クリックし、作成したネットワーク隔離の動的グループを選択します。
・[条件]　　：[動的グループコンテンツが変更されるたびに通知]を選択します。

通知メール設定 3.ネットワーク隔離通知メール作成方法

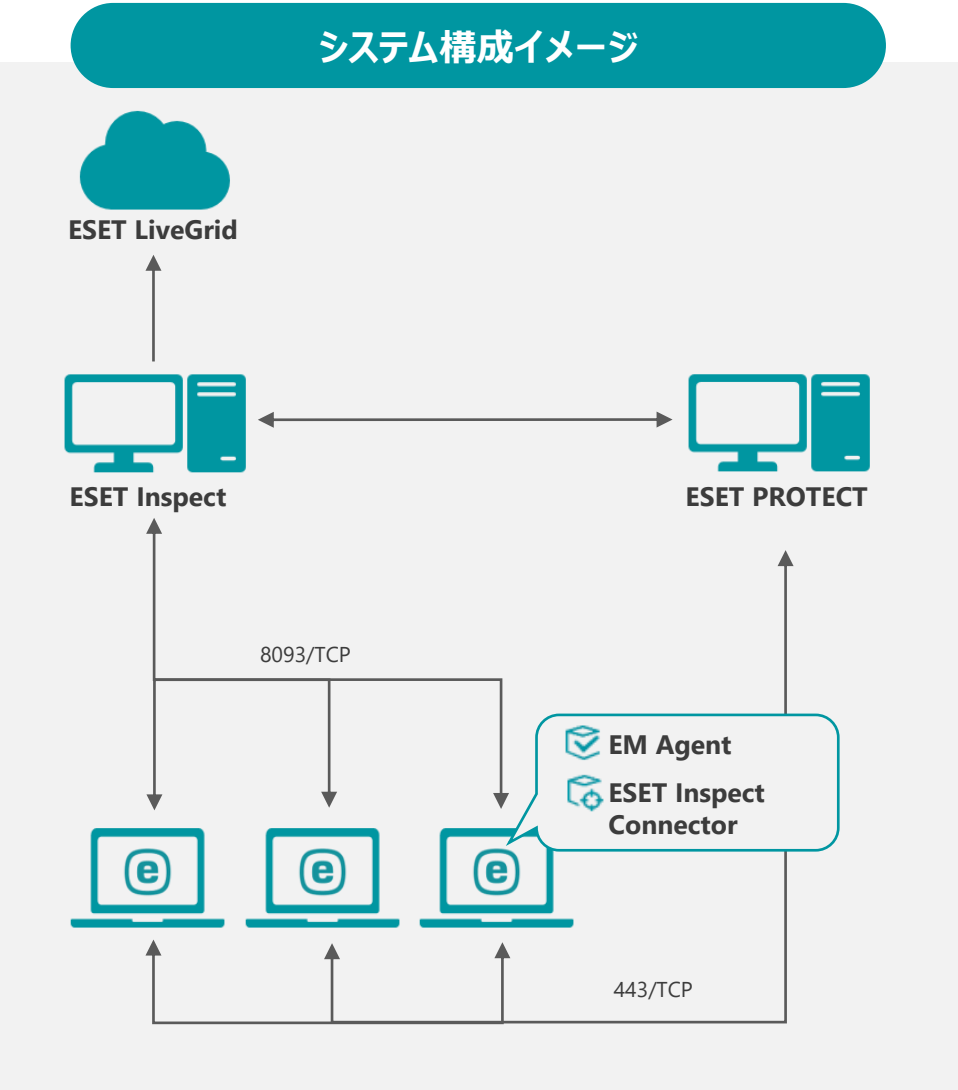
4. [配布]を開き、任意のメールアドレスを指定して[終了]をクリックします。

※[+]をクリックし複数の宛先を指定可能です。



Ⅳ. その他の情報

1. システム構成(1/2)



ESET Inspect (EI)

EIはEI Connectorを使用してエンドポイントデバイスでリアルタイムにデータを収集します。データは一連のEI内のルールと照合され、疑わしいアクティビティが自動的に検出されます。この集約されたデータにより、異常で疑わしいアクティビティをより効率的に検索し、正確なインシデント対応、管理、およびレポートの作成ができます。

ESET PROTECT (EP)

EPはクライアントプログラムの情報収集や設定の変更、インストーラーの作成、タスク配布などを行います。クライアントとの通信はEM Agentを経由して行います。

ESET Inspect Connector (EI Connector)

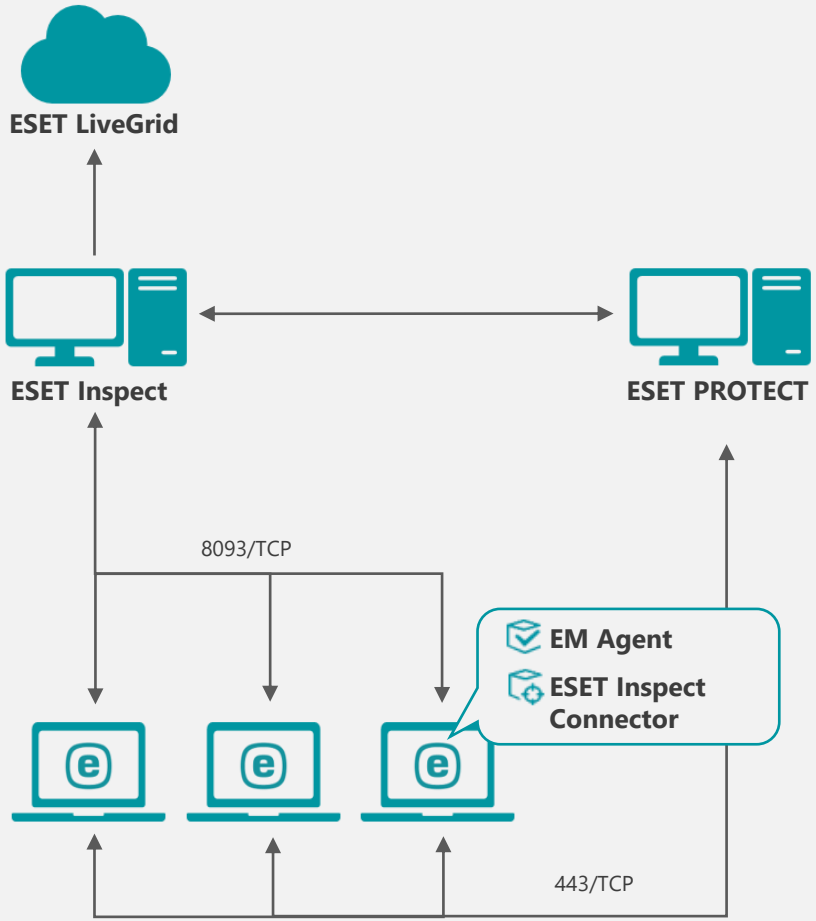
EI Connectorはクライアントのデータを収集し7分間隔でEIへデータを送信します。また、悪意のあるコンポーネントを削除し、これらのコンポーネントの実行をブロックします。

ESET Managementエージェント (EM Agent)

EM Agentは、クライアントから情報を収集し、10分間隔でEPへデータを送信します。また、EPからのタスク配布などはEM Agentへ送信されたのち、EM Agentがクライアントへ送信します。

1. システム構成(2/2)

システム構成イメージ



システム構成に関連する主な通信ポート

ポート	用途
443/TCP	EM AgentとESET PROTECT 間の通信に使用
8093/TCP	ESET Inspect ConnectorとESET Inspect 間の通信に使用

サポートされるアプリケーションバージョン

MDR関連でご利用いただく各プログラムは最新バージョンでのご利用を推奨しております。
（サポートより最新版へバージョンアップのお願いをする場合もございます。）

アプリケーション名	EPによる管理	EIによる管理
ESET Endpoint Security / アンチウイルス	8.1以降	11.0.2032.1以降
ESET Endpoint Security / アンチウイルス for OS X	6.11以降	6.11.606.0以降 /7.3.3600.0以降
ESET Endpoint アンチウイルス for Linux	8.1以降	10.2.2.0以降
ESET Endpoint Security for Android	3.5以降	-
ESET Server Security for Microsoft Windows Server	7.3以降	10.0.12014.1以降
ESET Server Security for Linux	8.1以降	10.2.41.0以降

ログの格納期間

ログの種類	データ保持期間
生ログ（検知の有無に関係なくEIに集められたすべてのログ）	7日間
検出ログ（EIの検知ルールによって検出されたログ）	31日間

2. EPとEIのバージョンアップについて

- **ESET PROTECT とESET Inspect のバージョンアップ**
  EPとEIのバージョンアップはESET社にて実施されるためお客様による作業は不要です。
  ※ バージョンアップの個別対応は不可となります。
- **ESET PROTECT のバージョンアップ作業に関して**
  EPのバージョンアップはESET社により段階的に行われ、バージョンアップ中は2~3分程度
  EPにアクセスできなくなります。
  EM Agentはログを溜め込む機能があるため、EPバージョンアップ後にEPにログ転送を再開します。
- **ESET Inspect のバージョンアップ作業に関して**
  EIのバージョンアップはESET社により段階的に行われ、バージョンアップ中は2~5分程度
  EIにアクセスできなくなります。
  EI Connectorはログを溜め込む機能があるため、EIバージョンアップ後にEIにログ転送を再開します。
- **ESET Management Agentのバージョンアップ**
  EM Agentは自動バージョンアップに対応しています。
  新しいバージョンのEM Agentがリリースされると、その2週間後から自動アップグレードがトリガーされます。
- **ESET Inspect Connectorのバージョンアップ**
  EI Connectorのバージョンアップはお客様自身で実施いただく必要がございます。
  EPのソフトウェアインストールタスクを利用してバージョンアップをお願いいたします。

3. サポート情報

- **弊社Webページにてサポート情報を記載しております。**
  ESET PROTECTソリューションシリーズ サポート情報(Q&A)
  https://eset-support.canon-its.jp/?site_domain=business
- **ESET PROTECTソリューションシリーズの**
  プログラムおよびマニュアルはユーザーズサイトにてご提供しております。
  ESET PROTECTソリューション ユーザーズサイト
  https://canon-its.jp/product/eset/users/index.html
- **以下の各種オンラインヘルプもご確認ください。**
  ESET PROTECT のオンラインヘルプ
  https://help.eset.com/protect_cloud/ja-JP/

  ESET Inspect のオンラインヘルプ
  https://help.eset.com/ei_cloud/ja-JP/