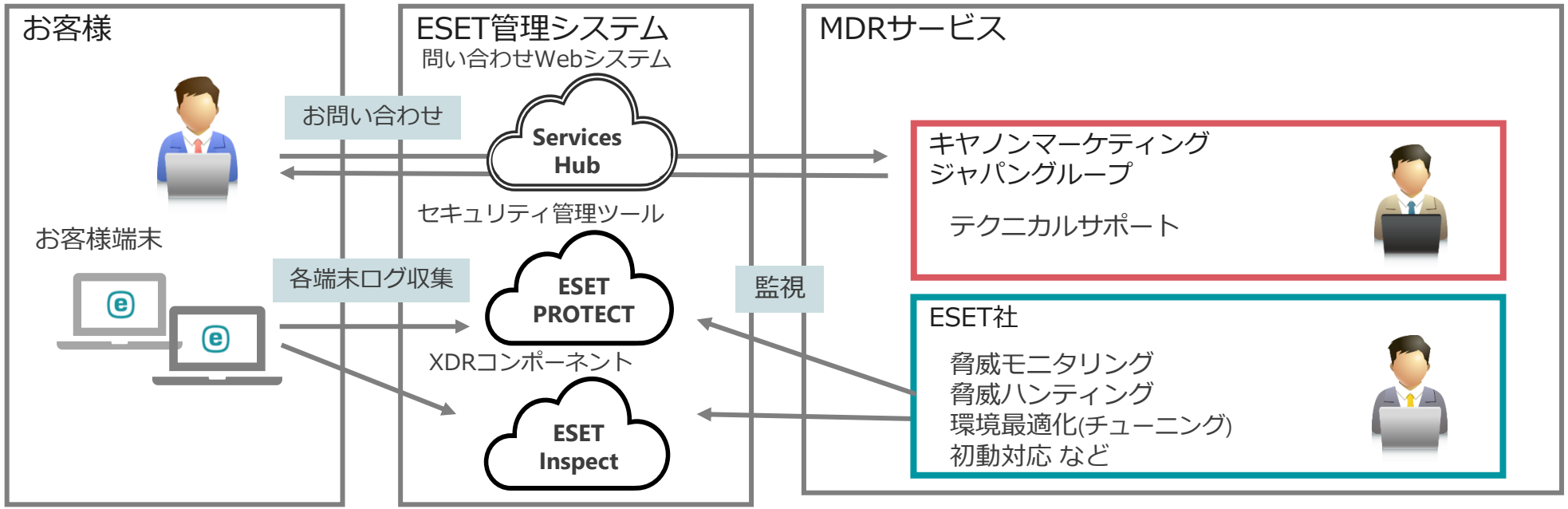
ESET PROTECT MDR Lite
スターターガイド

キヤノンマーケティングジャパン株式会社

第11版 2025年5月30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「利用開始案内メール」「納品完了メール」など3通のメールが送信されます。

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。

メール通知設定作業

インシデントと疑われる検出が発生した際の通知を受け取るための設定をESET PROTECT上で実施いただきます。

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）

Ⅰ.導入の流れについて（補足）

納品時ご送付のメール概要

納品時に以下3通のメールを申込書に記載のお客さま宛てにお送りいたします。

- **「ESET PROTECT MDR Liteの加入に伴う各種ご案内について」メール**
  サービスのお問い合わせ窓口およびサービス加入時の諸手続き等、以下4点についてのご案内メールです

  - お問い合わせ窓口情報のご案内について（緊急度が高い場合の連絡先を含む）
  - ESETセキュリティサービスセンターからの確認事項について
  - サービス加入時の諸手続きについて
  - その他のご注意事項について

- **「ESETセキュリティソリューションシリーズ 納品完了のご案内」メール**
  ライセンス情報が記載されたpdfをお送りします。本PDFをご覧いただき、ライセンスの登録を実施ください。
  手順は後述のスライドにてご案内しております。

- **ESET Services Hub登録メール ※ESET社より届きます**
  MDRユーザーさま専用のお問い合わせ窓口であるESET Services Hubへ登録するためのメールです。
  本メールよりESET Services Hubの開設が可能です。詳細については後述のスライドをご確認ください。

Ⅱ.お客様必須作業

1. ESET Services Hubについて

ESET Services Hubの概要

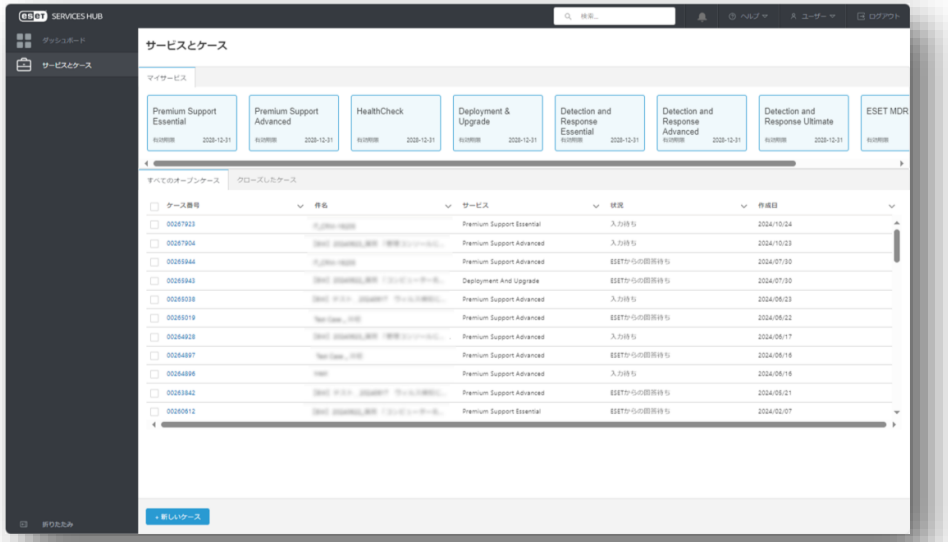
ESET Services Hubとは

「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

ESET Services Hubの操作方法などの詳細については、オンラインヘルプをご参照ください。
https://help.eset.com/eset_services_hub/ja-JP/



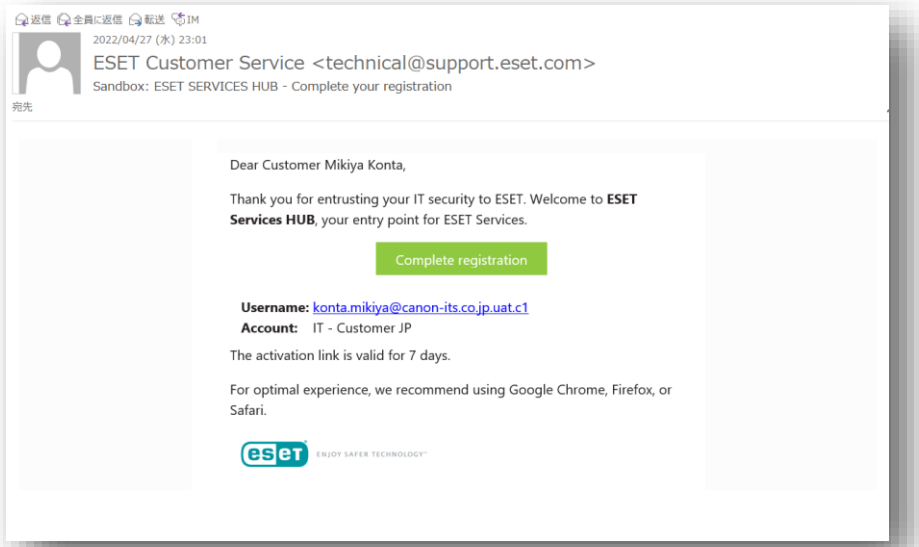
1. ESET Services Hubについて

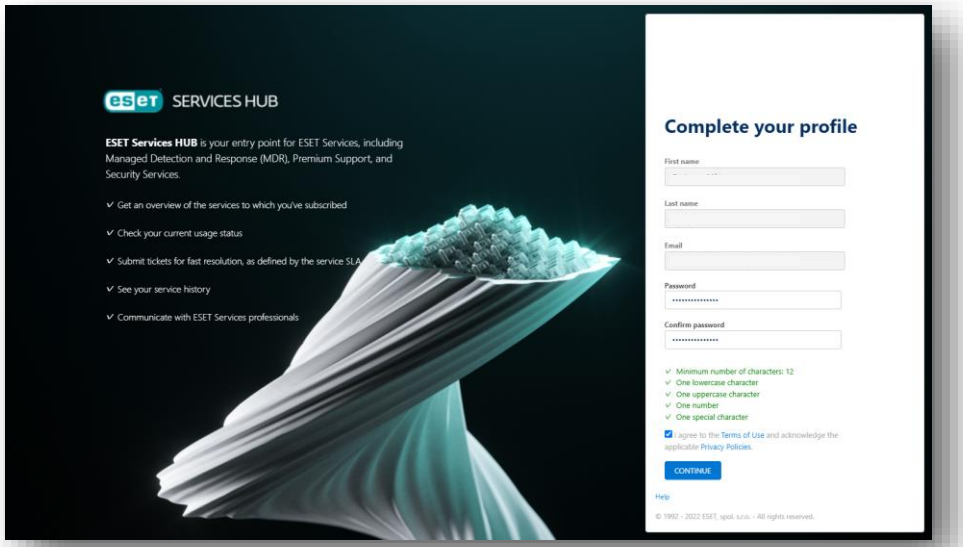
ESET Services Hubの利用方法

アカウント開設方法

1. 件名「ESET Services HUB - 登録を完了してください」の招待メールを開き、
   メール内に記載されている「登録の完了」ボタンをクリックします。

2. プロファイルの入力画面がWebブラウザーに表示されますので、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。

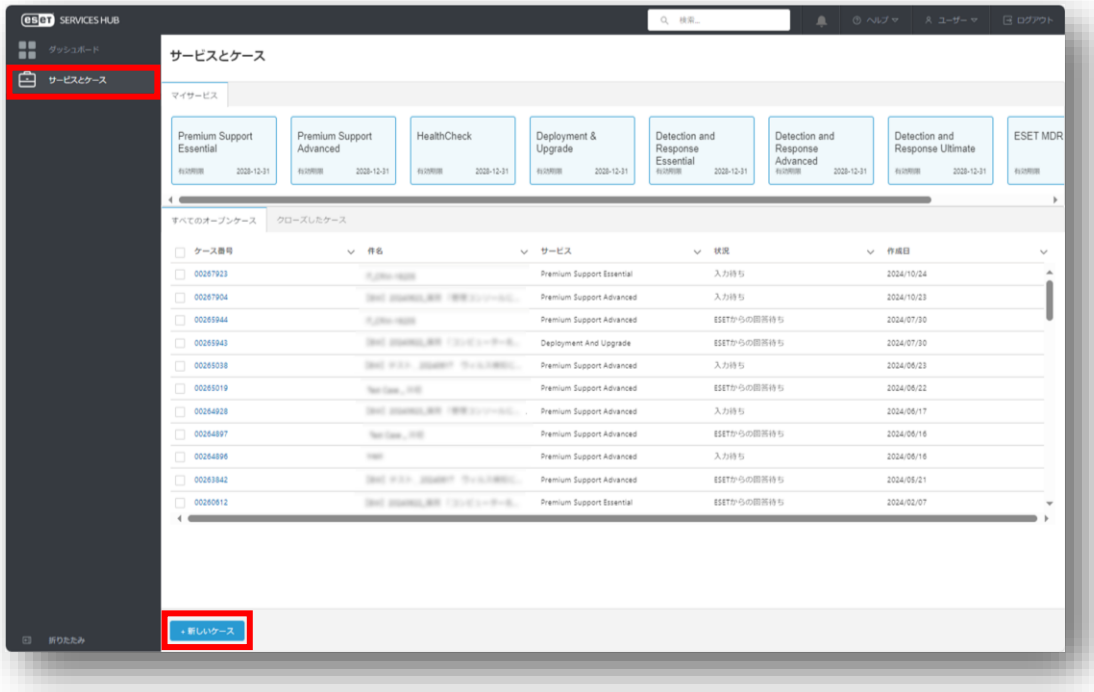


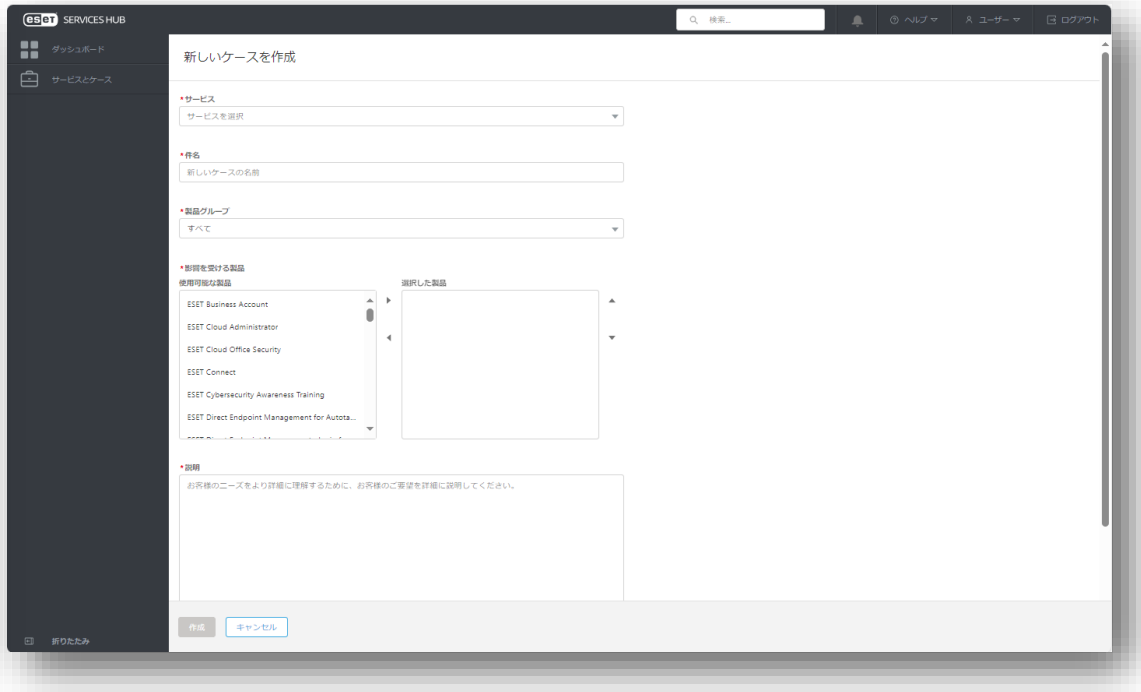


参考情報：問い合わせが発生した場合

ESET Services Hubで問い合わせをする方法

1. 画面「サービスとケース」を開き、画面下部の[+新しいケース]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、[作成]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。





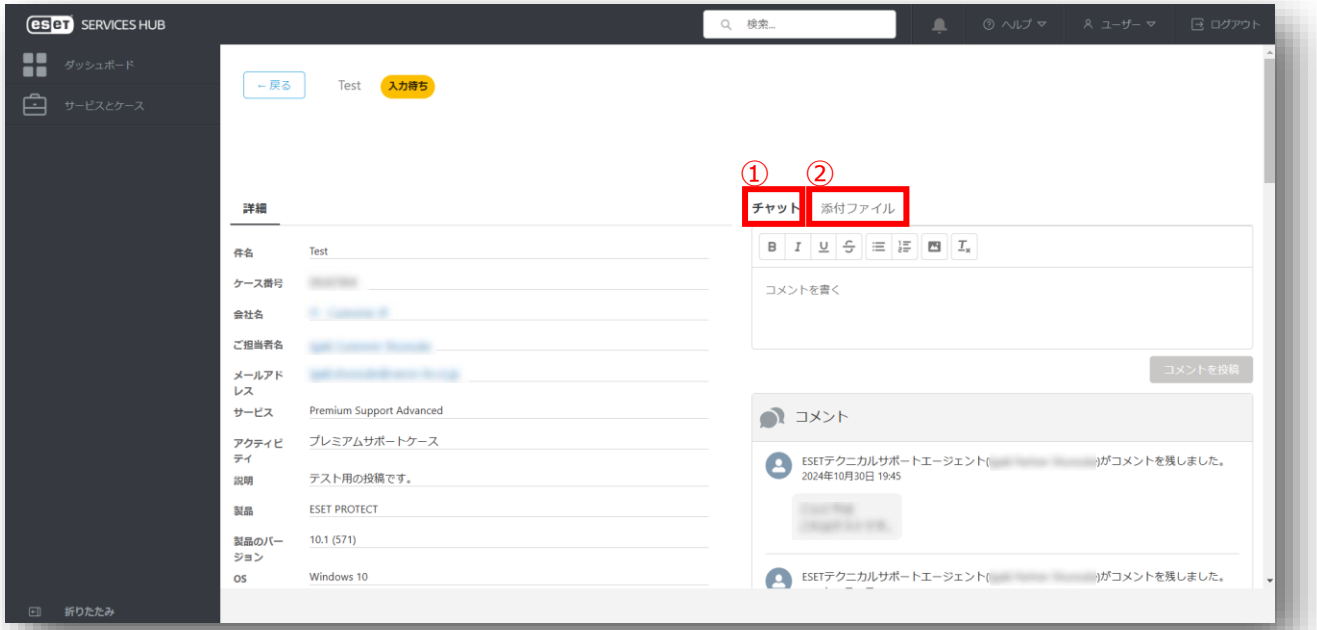
参考情報：問い合わせが発生した場合

オープン中のお問い合わせチケットの対応方法

1. 画面「サービスとケース」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。

ESET Services Hubの問い合わせ方法ついては、別資料「Services HUBお問い合わせ手順」をご参照ください。

▼ESET Services Hubお問い合わせ手順
https://eset-info.canon-its.jp/files/user/pdf/support/ep-mdr_sh.pdf



①チャット

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。

②添付ファイル

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。

参考情報：プレミアムサポートサービスについて

プレミアムサポートサービス概要

ESETプログラムに関する問合せ対応を行うサービスです。
サービス専用の窓口で、ESET社の教育を受けたメンバーが管理する窓口として対応を実施します。

項目	内容
24時間365日対応	24時間365日で対応します。
重大度レベルに応じた対応	対応までの人的初期レスポンス時間は重大度レベルに応じて定義されます。 重大度A：2時間　重大度B：4時間　重大度C：1稼働日 ※ 重大度は最終的にESET社によって定義されます。
優先度を上げた対応	本サービスの問合せは、ESET社によって優先的に対応されます。
登録者制サポート	サービス窓口では、登録いただいたご担当者の方からの問合せのみ受け付けます。
サポート対象製品とプログラム	ESET PROTECT MDR製品で利用可能なプログラムが対象となります。 また、各プログラムのサポートポリシーはライフサイクルポリシーに準拠します。 https://eset-info.canon-its.jp/business/info/lifecycle-eol/

Severity Response Timeにおける重大度
・重大度A（重大）…本製品またはその主要機能が動作しないか、または本製品の使用に重大な影響を与える定期的/断続的な問題が発生している場合
・重大度B（深刻）…製品の機能に欠陥があるか、欠落しているか、または製品の使用を困難にする問題が発生しているが、使用できないわけではない場合
・重大度C（一般）…わずかなパフォーマンスの低下や、製品やドキュメントの修正を必要とするマイナーな問題がお客様に発生している場合

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**
    →12ページへ
  - **ESET PROTECT on-premで端末を管理済みの場合**
    →13ページへ
  - **ESET製品を新規導入の場合**
    →17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ESET Inspectのアクティベーションや ESET Inspect Connectorのインストールなどが必要です。
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。

▼【既存ユーザーさま向け】MDR環境構築ガイド
https://eset-info.canon-its.jp/files/user/pdf/support/ep-mdr_kg.pdf

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、以下のサポートページや移行動画をご参照ください。

▼ESET PROTECT（クラウド版）について
https://eset-support.canon-its.jp/faq/show/19302?site_domain=business

▼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
②Migration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

ESET InspectのアクティベーションやESET Inspect Connectorのインストールなどが必要です。
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。

▼【既存ユーザーさま向け】MDR環境構築ガイド
https://eset-info.canon-its.jp/files/user/pdf/support/ep-mdr_kg.pdf

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 PROTECT Hubの開設

1. https://protecthub.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します。
2. 画面に表示される説明に沿って必要事項を入力し[アカウントの作成]をクリックします。
   確認用メールが送信されたページが表示されます。
   ※ 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EPHログイン時に使用します

■ログイン画面

■アカウントを作成

2. プログラムの導入 ~ ESET製品を新規導入の場合~

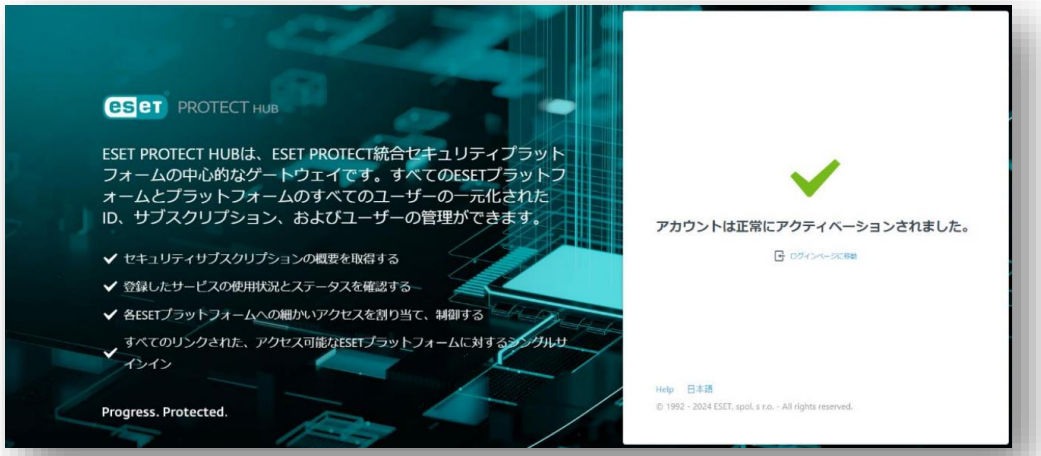
3. 登録したメールアドレス宛に電子メール確認のメールが届きますので、リンクをクリックするとブラウザで入力画面が開きます。
4. 必要事項を入力し、[続行]をクリックします。
5. 次画面でも必要事項を入力し、[アカウントをアクティベーションする]をクリックします。

■アカウントのアクティベーション画面

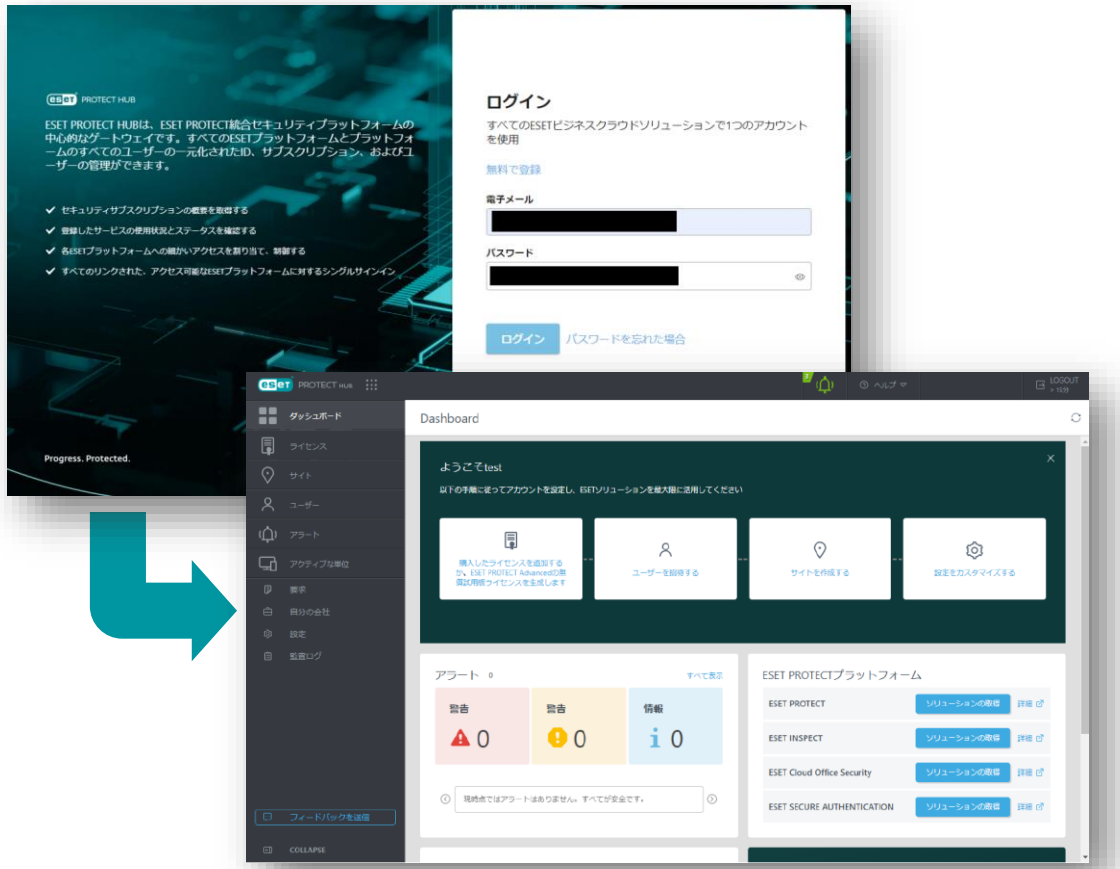
2. プログラムの導入 ~ ESET製品を新規導入の場合~

6. 以下の画面が表示され、アクティベーションは完了となります。
[ログインページに移動]をクリックするとログイン画面が表示されます。

■アクティベーション完了画面



■EPH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

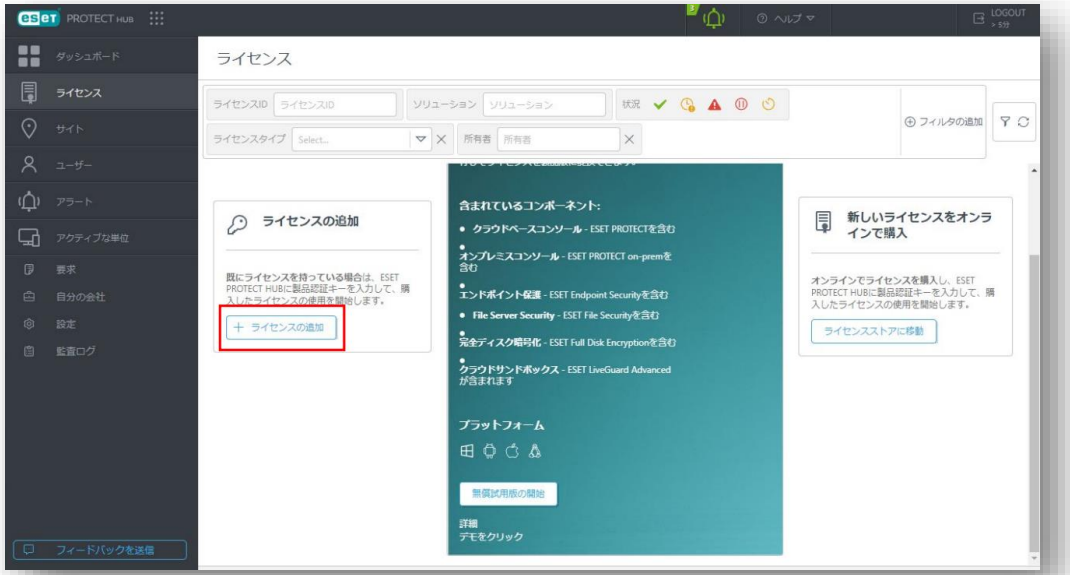
1. EPHへのライセンスの登録

※ 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

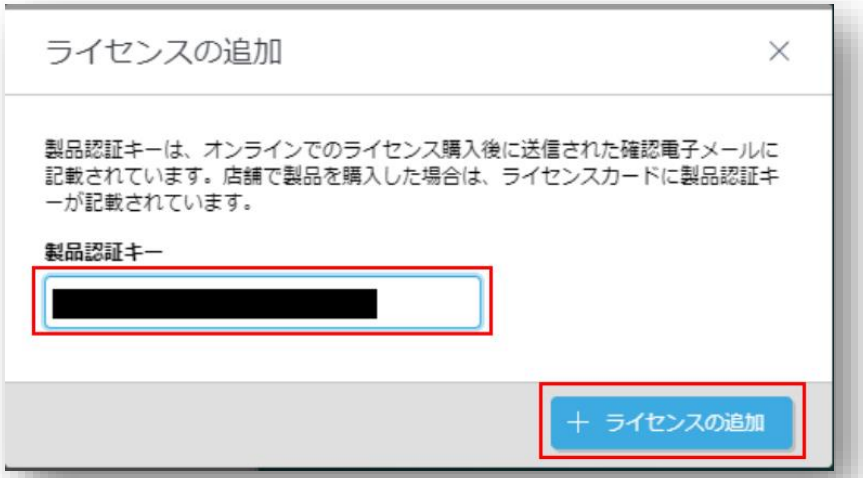
※ 「ライセンスの追加」画面ではESETの利用規約へご同意いただく必要がございます。

※ 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[ライセンス]内の[ライセンスの追加]をクリック



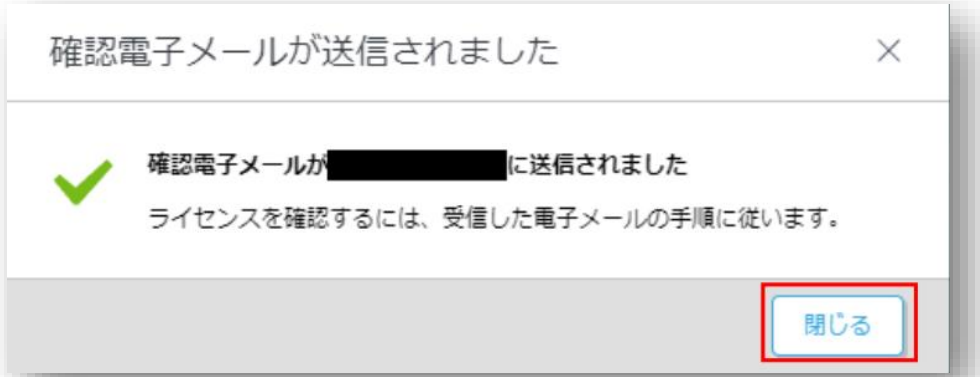
②[ライセンスの追加]画面



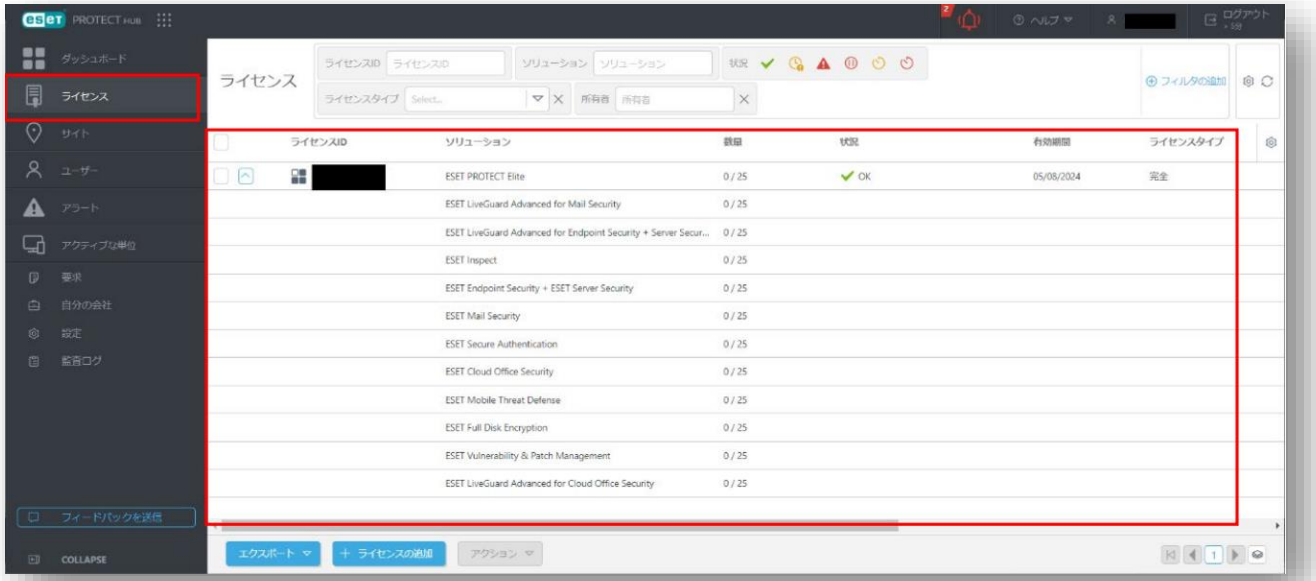
2. プログラムの導入 ~ ESET製品を新規導入の場合~

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

■ライセンス確認メール



■ライセンスが登録されたことの確認画面例



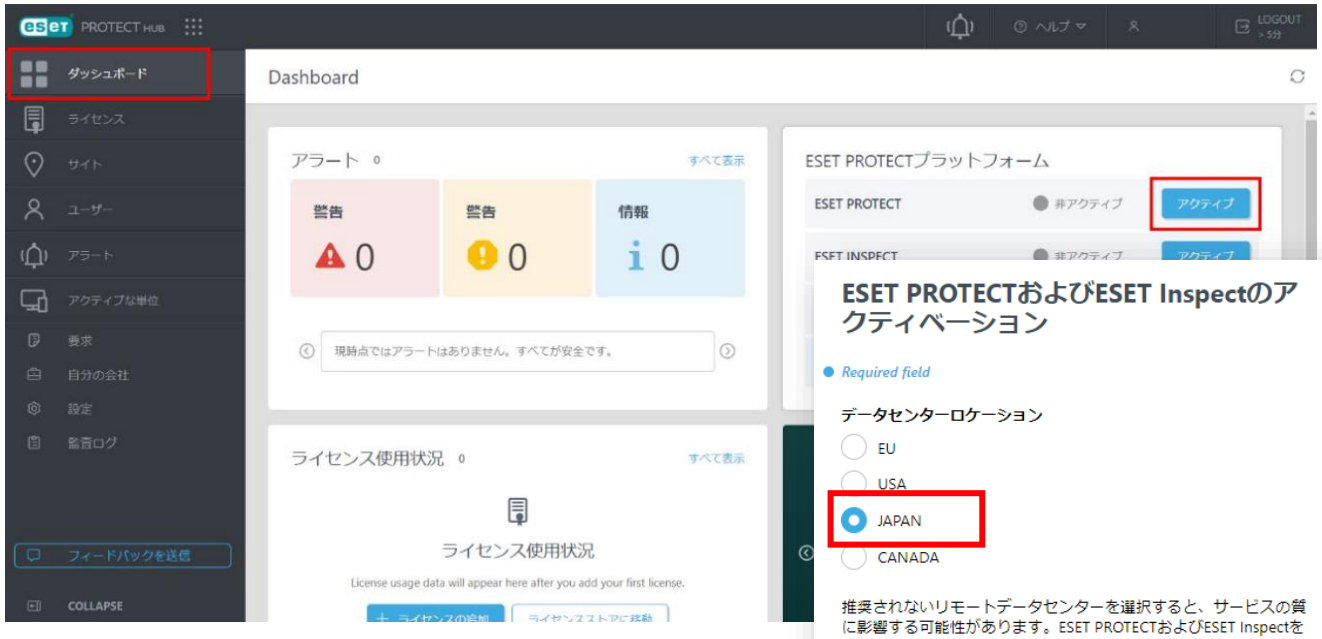
2. プログラムの導入 ~ ESET製品を新規導入の場合~

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「ダッシュボード」からESET PROTECTの[アクティブ]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）

2.ポリシーの作成（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。
- 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. インストーラーの作成と展開

- **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。

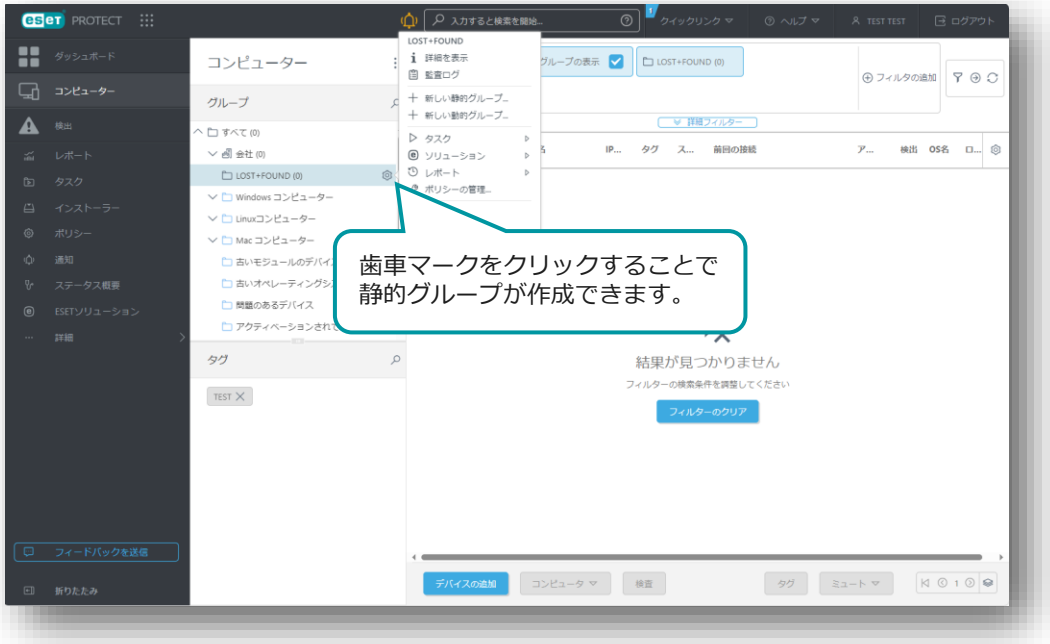
2. プログラムの導入 ~ ESET製品を新規導入の場合~

1. 静的グループの作成

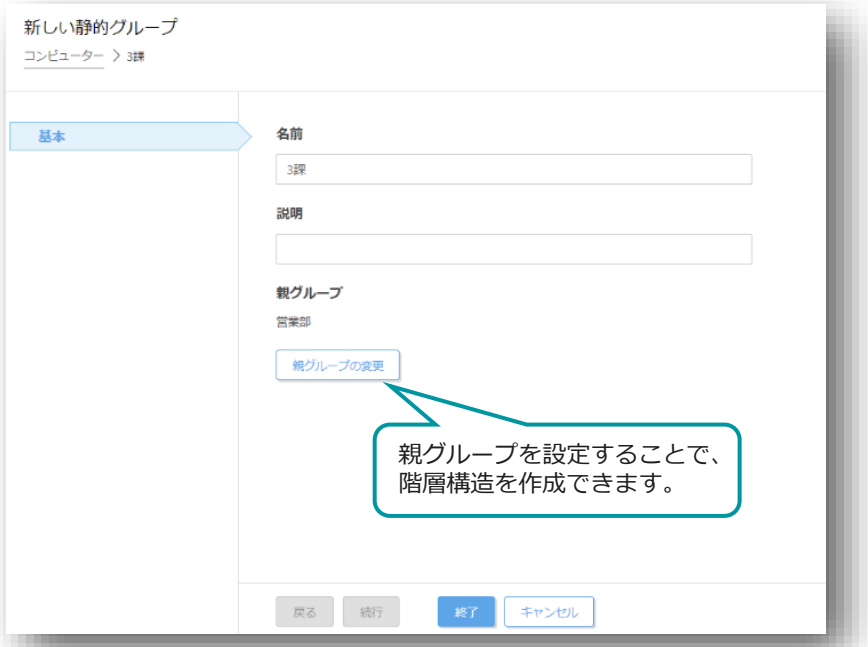
静的グループはメインメニュー「コンピューター」から作成可能です。
グループは階層構造も可能なため、柔軟に組織構造を作成することができます。

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



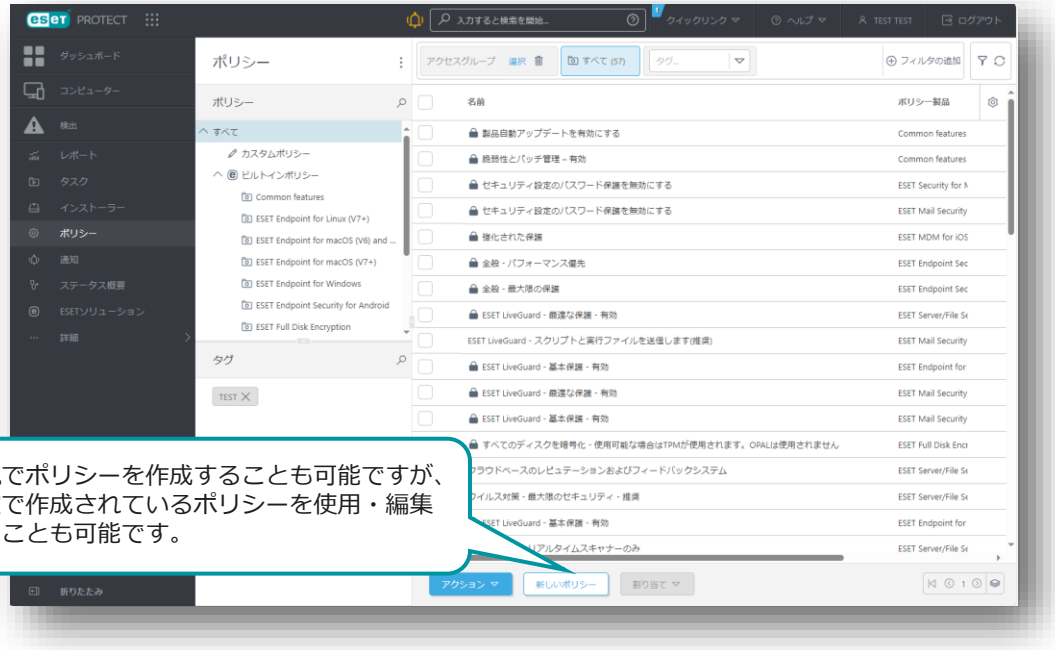
2. プログラムの導入 ~ ESET製品を新規導入の場合~

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と展開(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、ライブインストーラーに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。

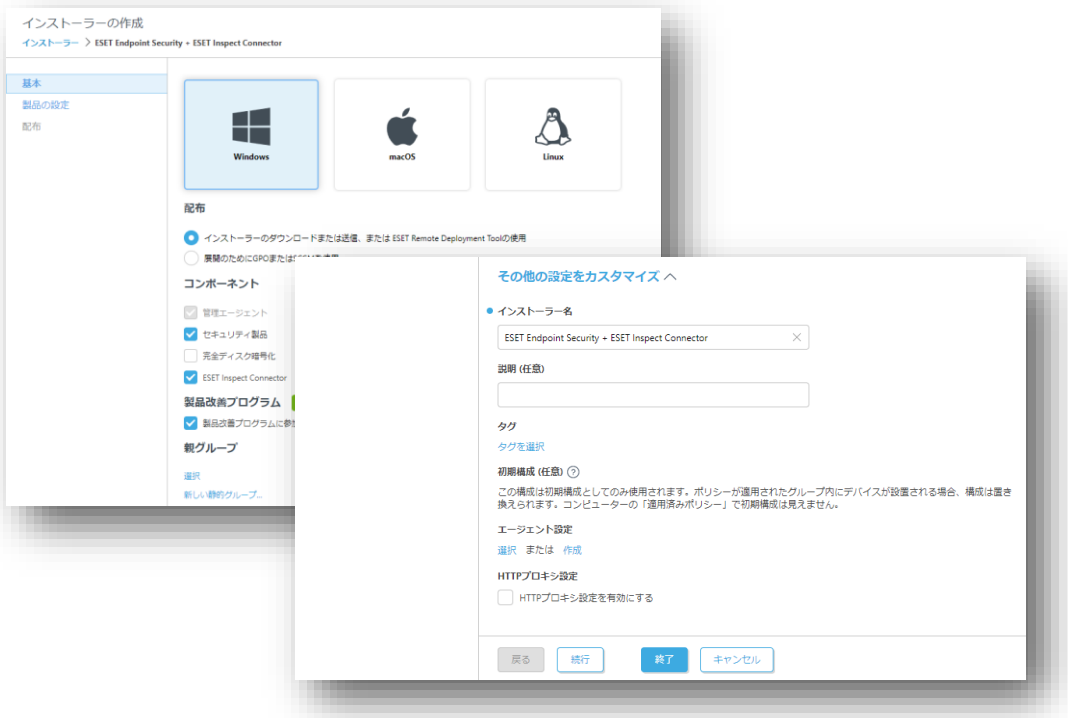
2. プログラムの導入 ~ ESET製品を新規導入の場合~

3. インストーラーの作成と展開(2/3)

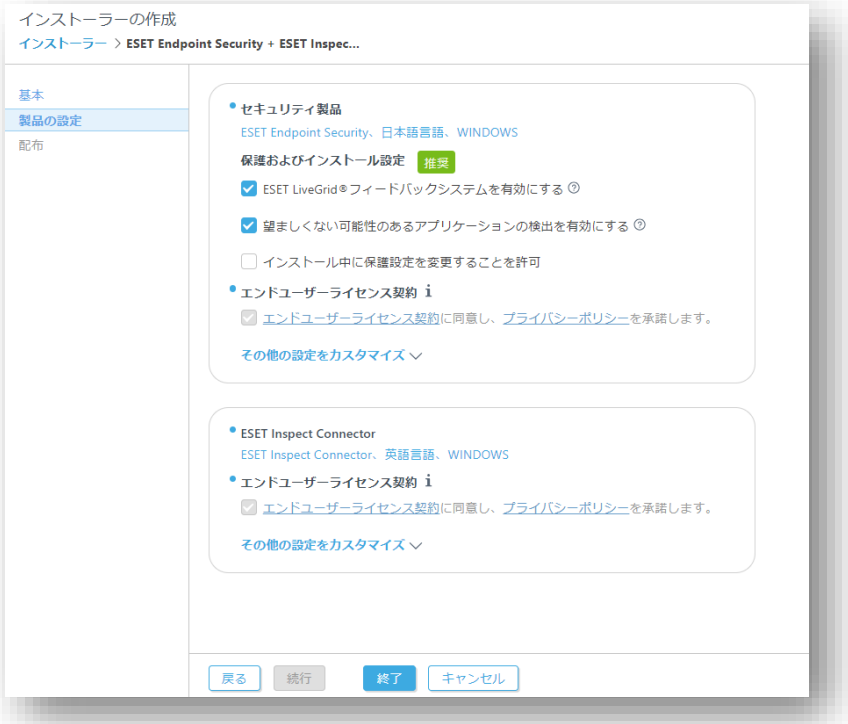
インストーラーに含めるコンポーネントやポリシー、親グループなどの各種設定を行います。

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、インストーラーに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と展開(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~

3. インストーラーの作成と展開(※Windows以外のOSの場合のみ実施)

Windows以外のOSの場合、以下の手順でタスク機能を利用し残りの必要なプログラムをリモートインストールします。

1. EP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。
2. 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。
3. 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。
4. 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。
※Linuxクライアントの場合、手順1～４を再度実施しクライアント用プログラムもインストールします。

■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ご確認ください。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。

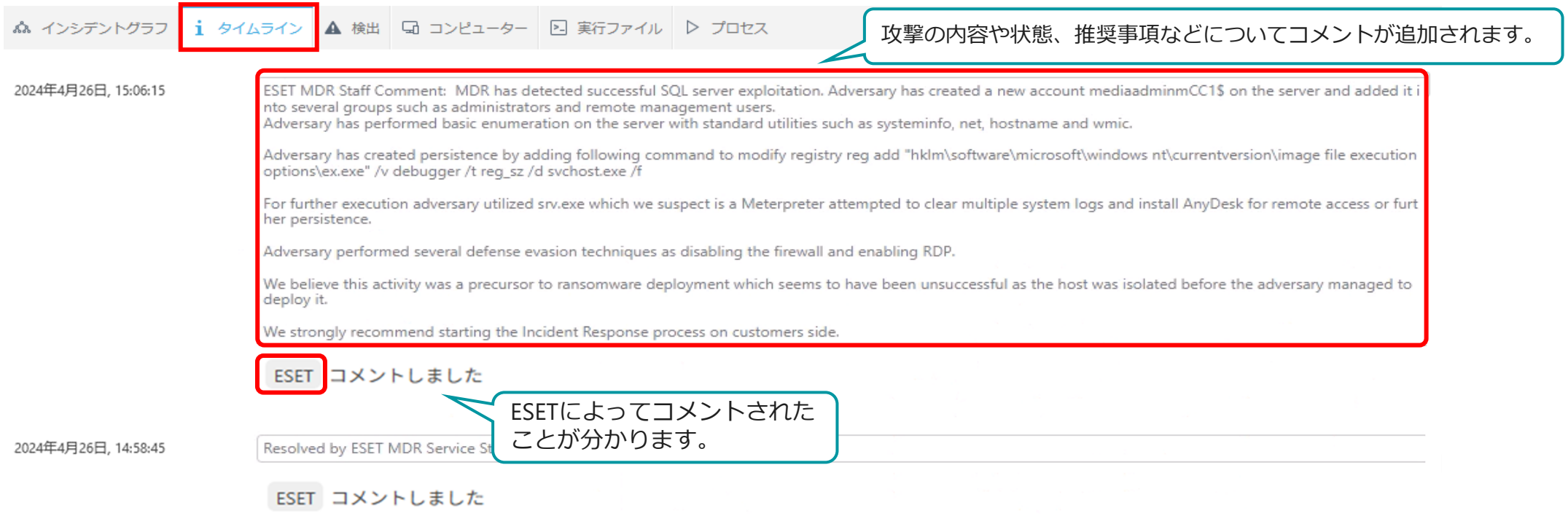
※設定した通知メールが正常に受信できないなど発生しましたら、サポートセンターまでお問い合わせください。

■インシデント発生時の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。



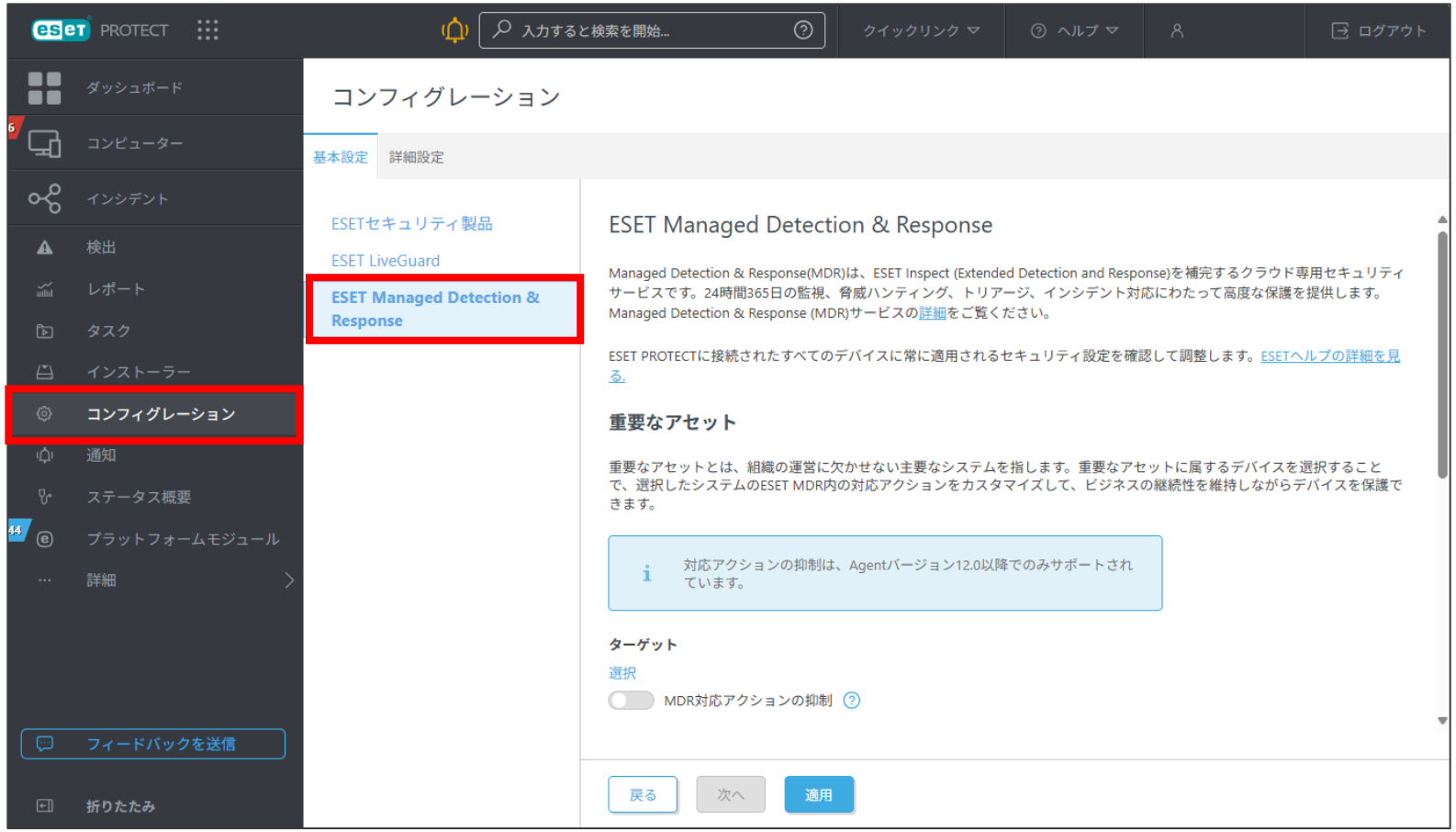
通知メール設定 1.インシデント発生通知メール設定

お客様のESET Inspectでインシデント発生時に、メールで通知されます。
本設定により、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。

■インシデント発生時の通知メールサンプル

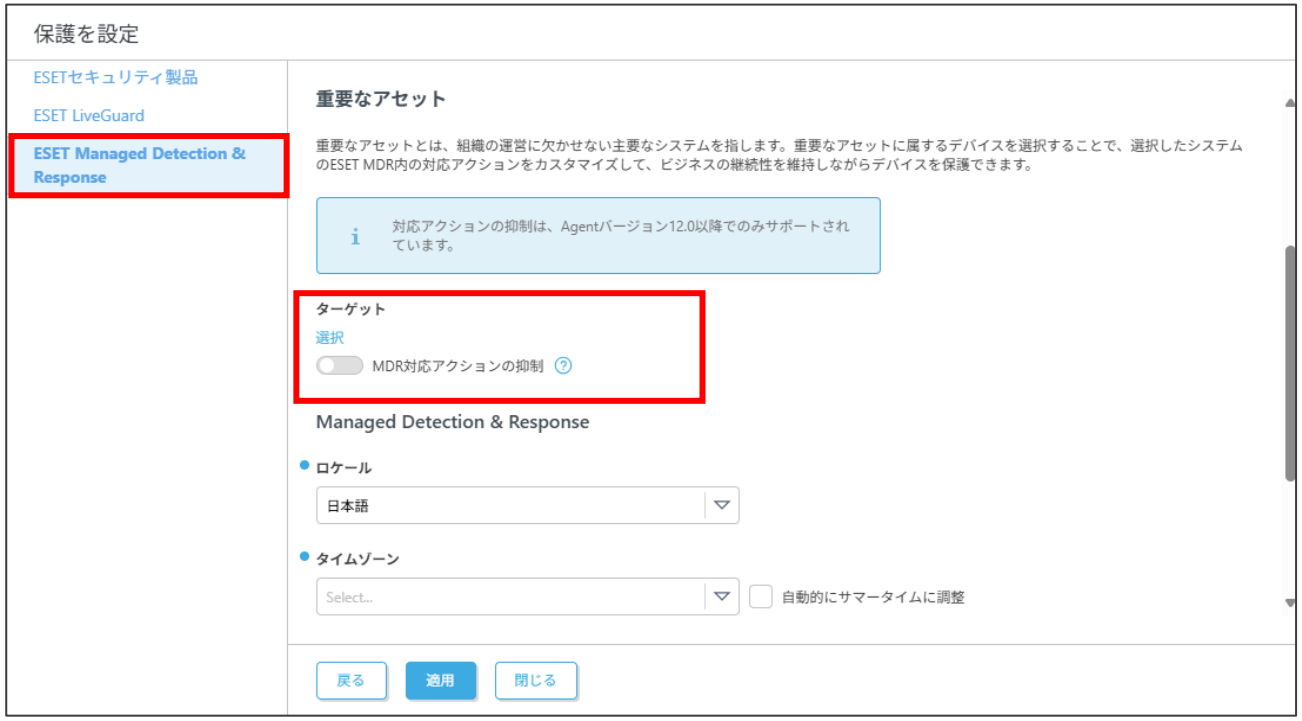
通知メール設定 1.インシデント発生通知メール設定

1. ESET PROTECTログイン後、[コンフィグレーション]→[ESET Managed Detection & Response]をクリックします。



通知メール設定 1.インシデント発生通知メール設定

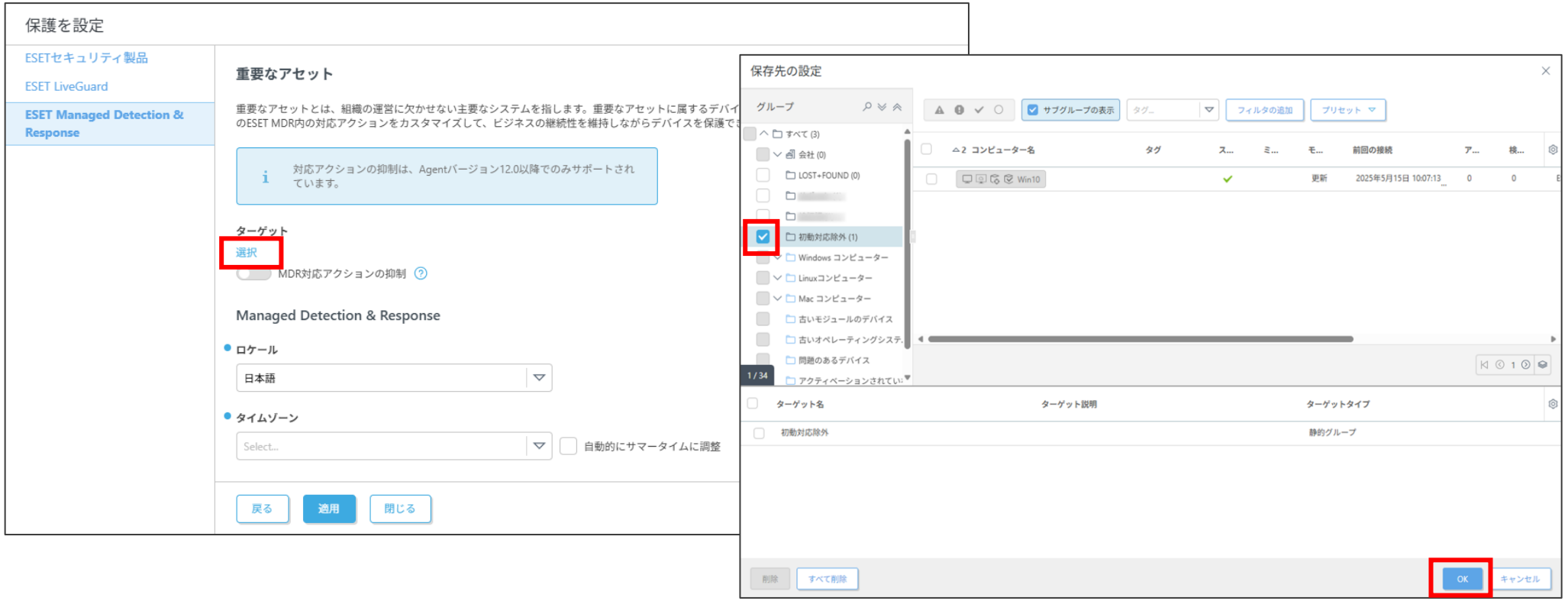
2. クリティカルなサーバーなどESET社による初動対応を希望しないクライアントがある場合、 「MDR対応アクションの抑制」の設定を行います。この設定を行っておくことで、該当のターゲット（静的グループまたはクライアント）はプロセス停止やネットワーク隔離などの初動対応から除外されます。



※初動対応からの除外については、いつでも登録や解除が可能ですので、一定期間除外し問題がなさそうであれば設定から外して初動対応の対象にするといった運用も可能です。

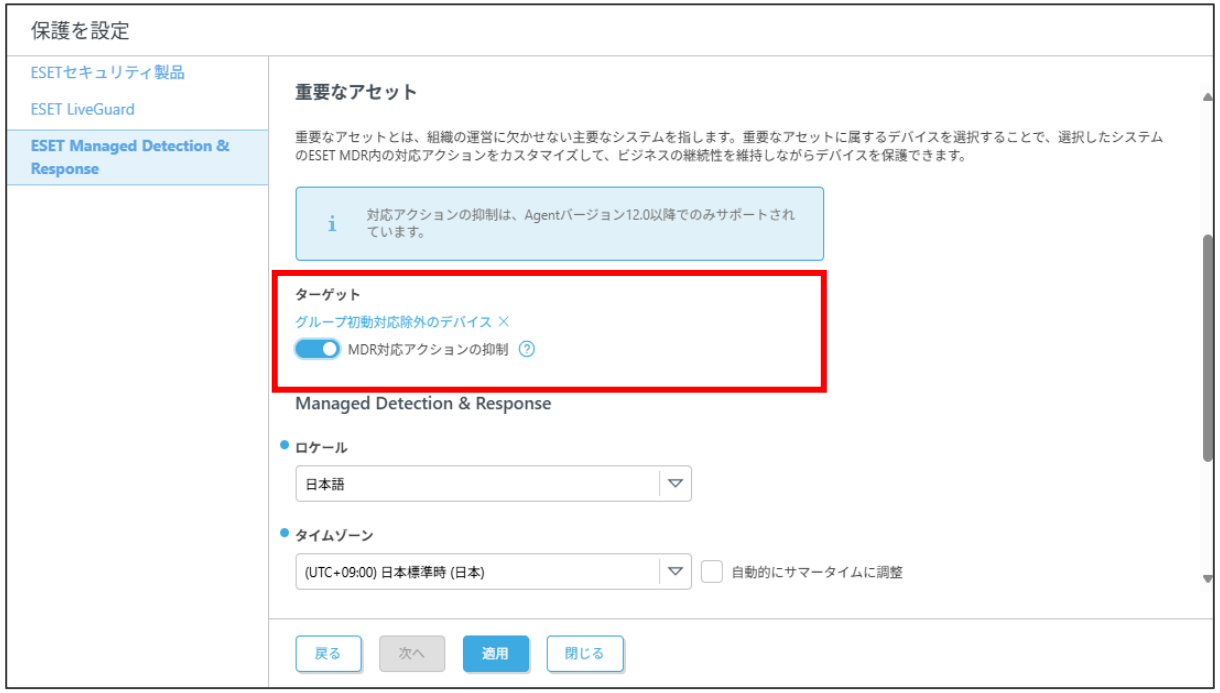
通知メール設定 1.インシデント発生通知メール設定

3. [ターゲット]より「選択」をクリックし、初動対応から除外したい静的グループもしくはクライアントを選択し、「OK」をクリックします。
※本例では、事前に「初動対応除外」グループを作成しています。



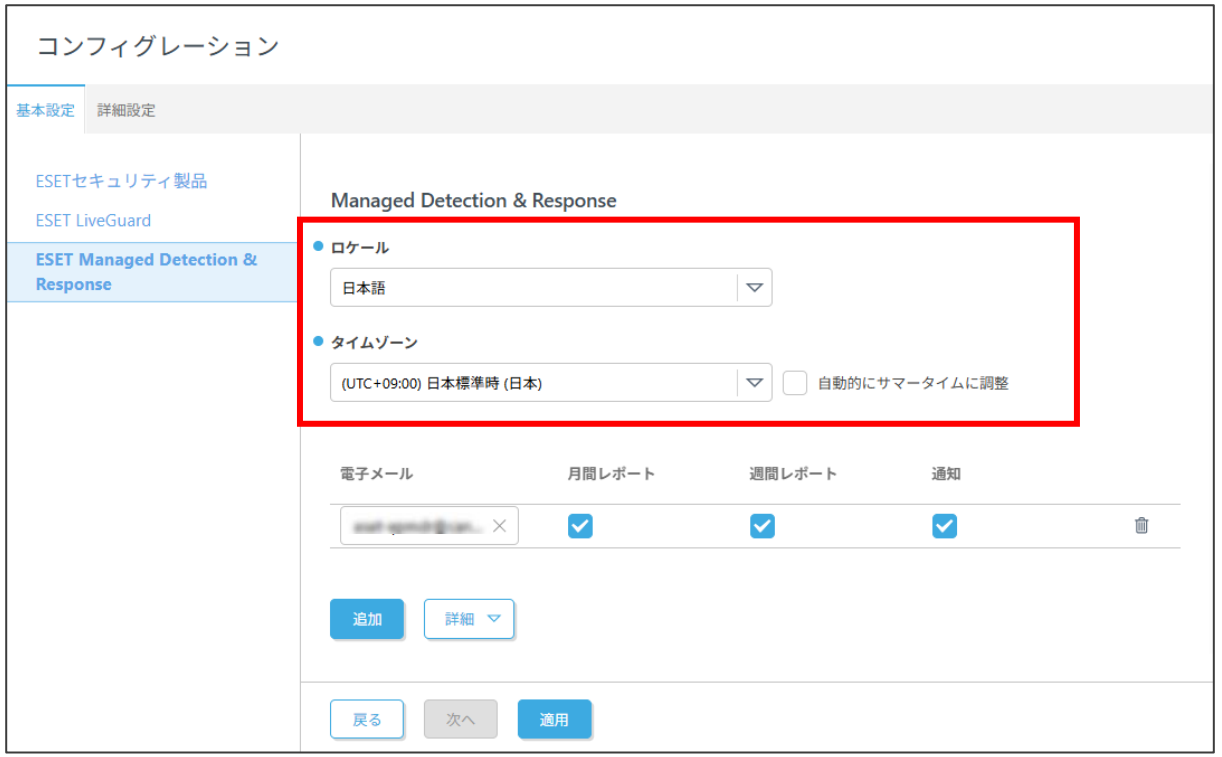
通知メール設定 1.インシデント発生通知メール設定

4. [ターゲット]に設定した静的グループもしくはクライアントが選択されていることを確認し、[MDRアクションの抑制]を有効にします。



通知メール設定 1.インシデント発生通知メール設定

5. <Managed Detection & Response>では以下設定になっていることを確認します。
   ・ロケール：日本語
   ・タイムゾーン：日本



通知メール設定 1.インシデント発生通知メール設定

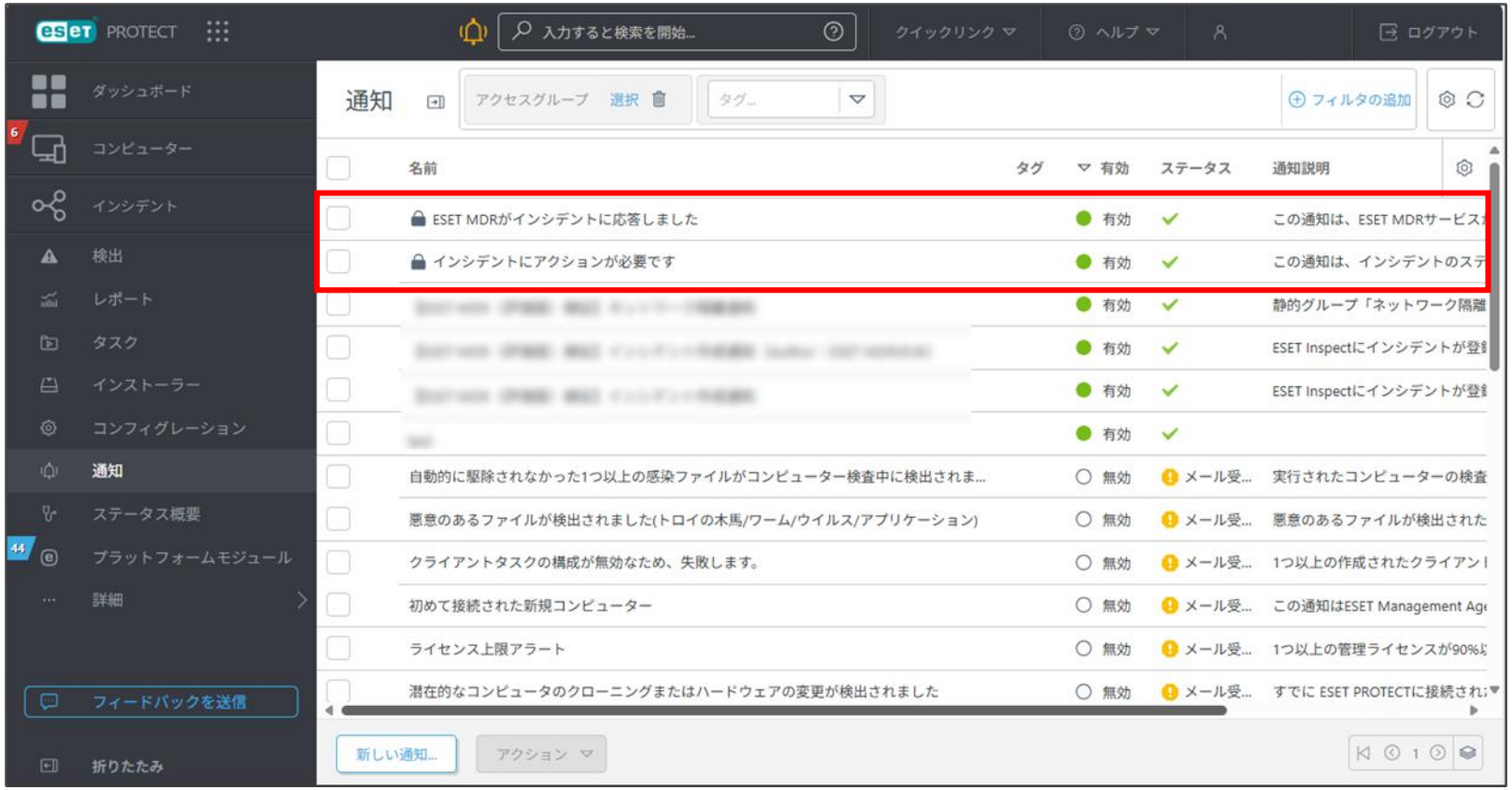
6. 下図の赤枠内の電子メール設定では必要に応じて設定変更を行い、「適用」をクリックします。
※[レポート] (月間/週間) 、[通知] いずれもデフォルトで有効です。
※[通知]の内容は以下の通りです。迅速にインシデントに気付くため、必ず有効になっていることをご確認ください。
・ESET MDRがインシデントに応答しました ：インシデントに自動対応し、ユーザーアクションが不要な場合の通知
・インシデントにアクションが必要です ：インシデントが作成され、ユーザーアクションが必要な場合の通知

※通知先は「追加」をクリックし設定することで複数の宛先を指定可能です

通知メール設定 1.インシデント発生通知メール設定 （参考）

<参考>

インシデント発生時の通知が有効になっているかはメインメニューの「通知」より確認することも可能です。



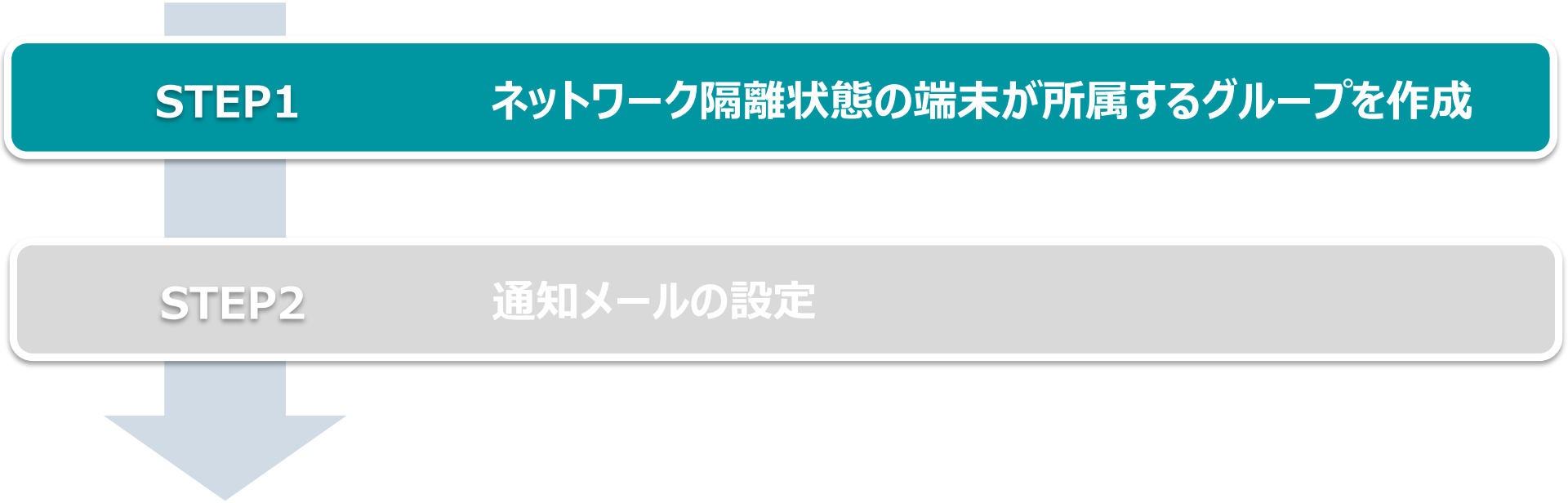
通知メール設定 2.ネットワーク隔離通知メール作成方法

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 2.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。

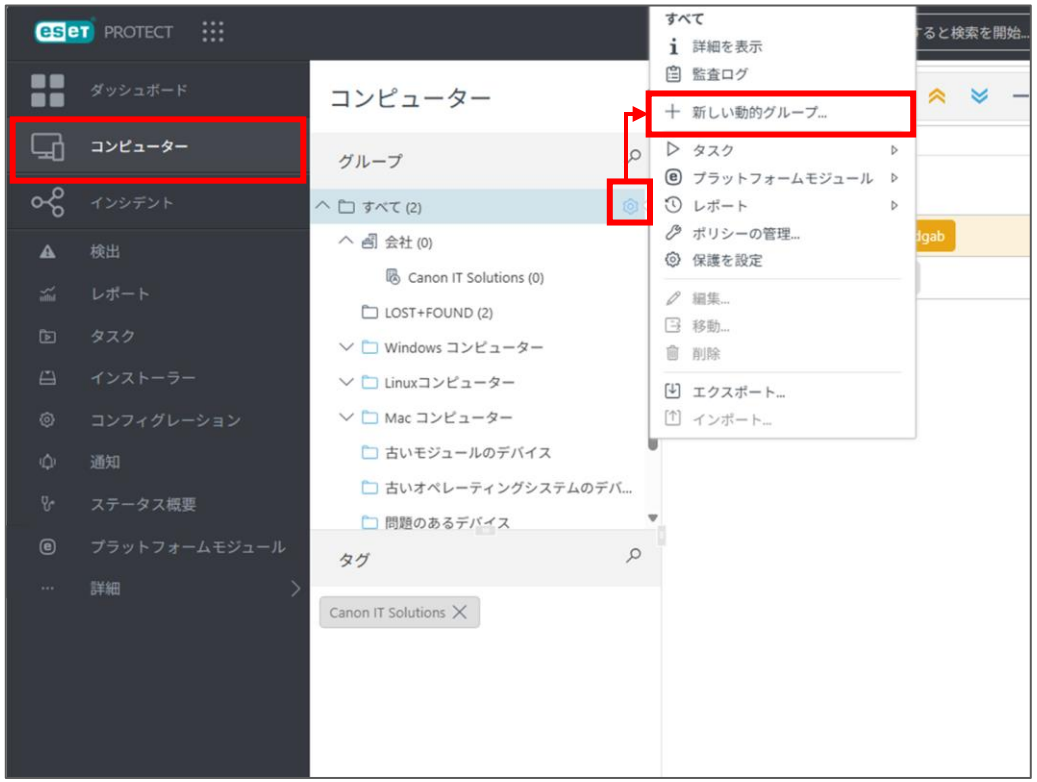


通知メール設定 2.ネットワーク隔離通知メール作成方法

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 2.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 2.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 2.ネットワーク隔離通知メール作成方法

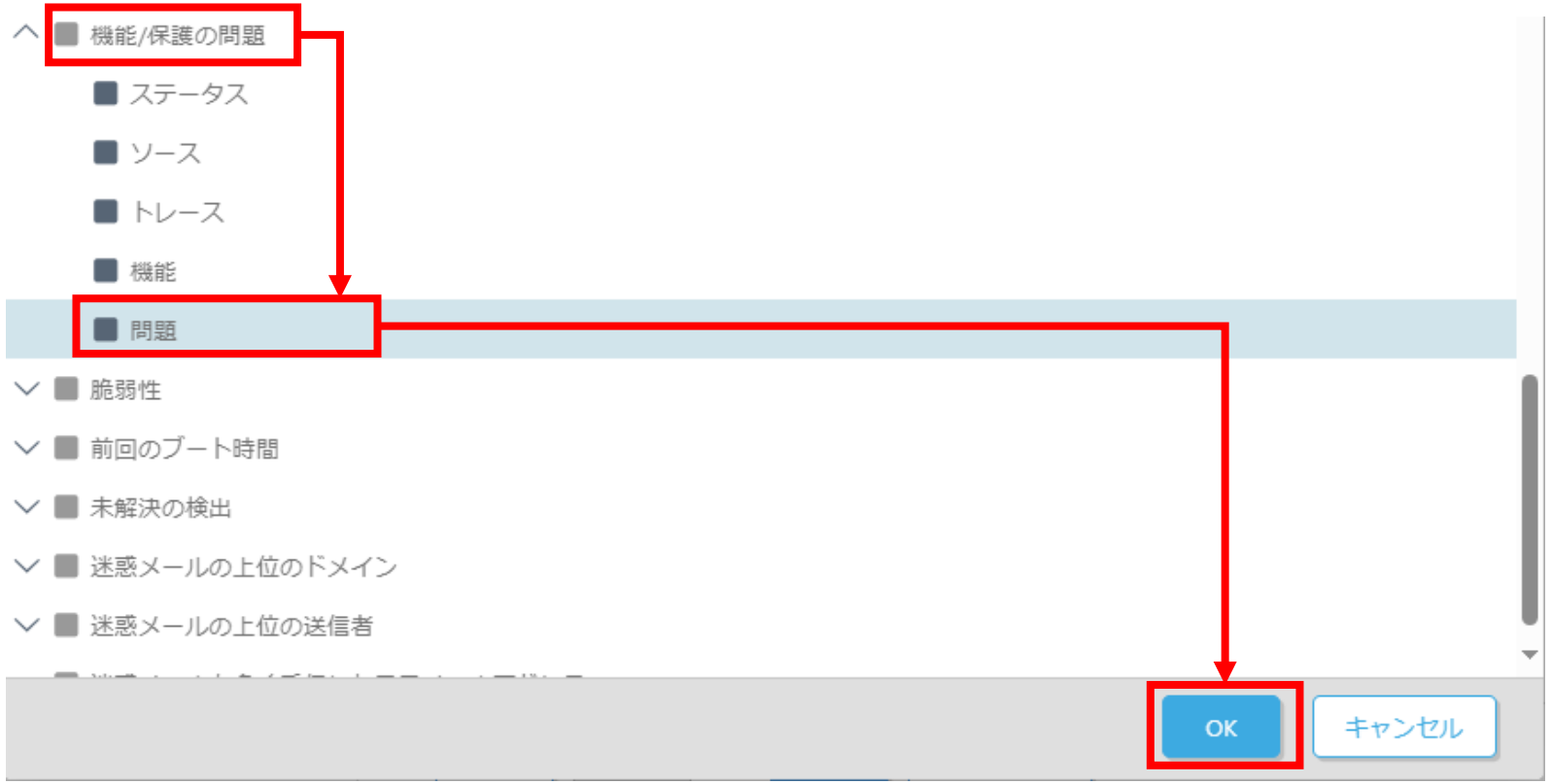
4. ［基本］を展開し、任意の名前（例：ネットワーク隔離）を入力します。
※ ［説明］の入力は任意です。

通知メール設定 2.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。

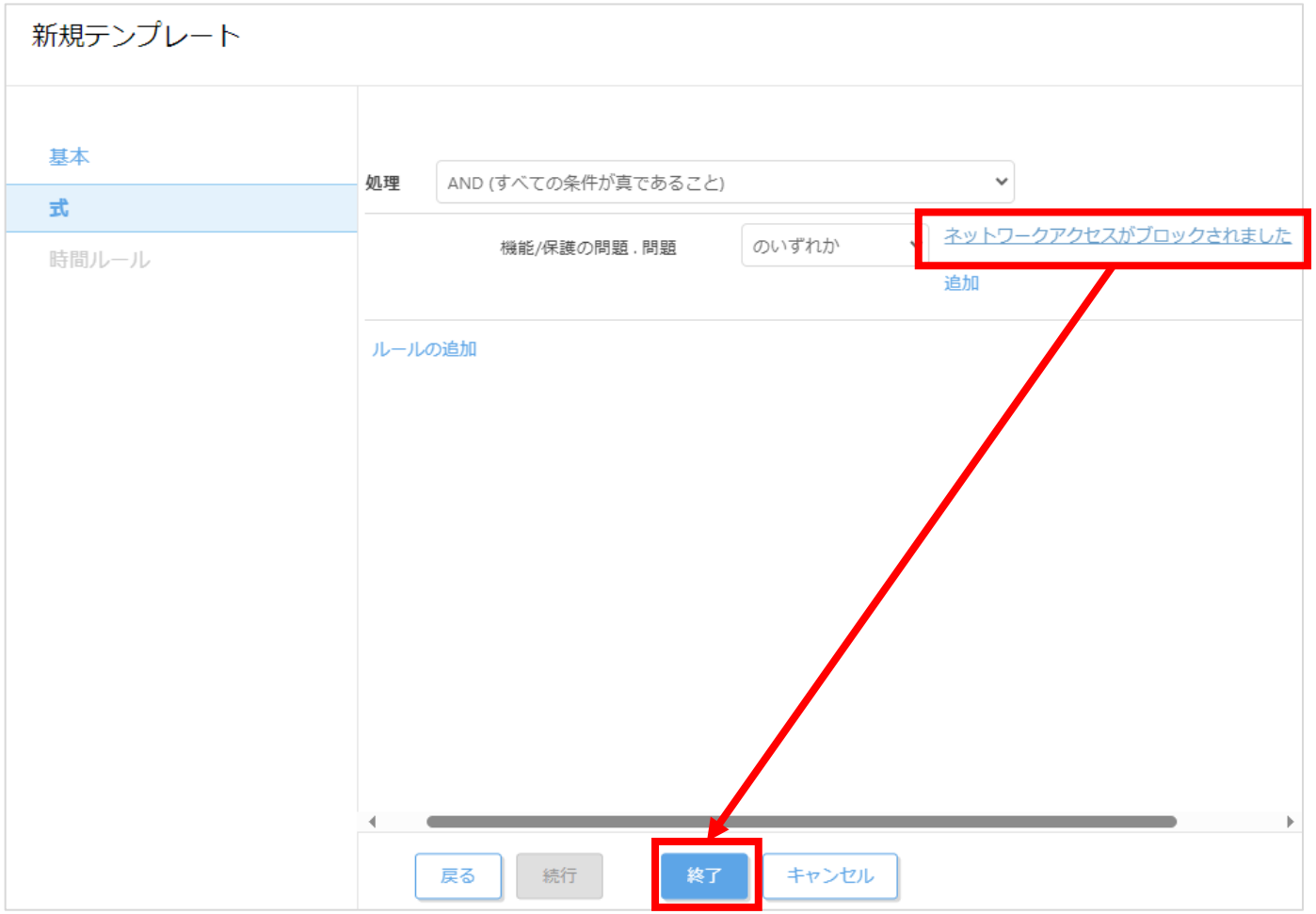
通知メール設定 2.ネットワーク隔離通知メール作成方法

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。



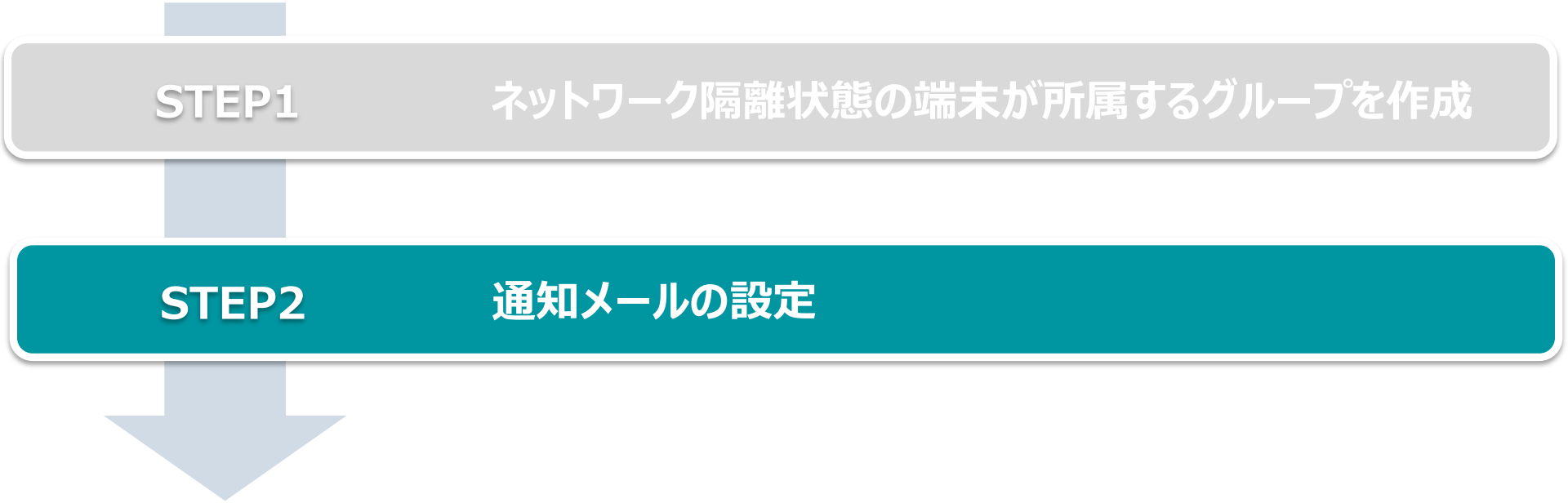
通知メール設定 2.ネットワーク隔離通知メール作成方法

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

2.ネットワーク隔離通知メール作成方法



通知メール設定 2.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 2.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 2.ネットワーク隔離通知メール作成方法

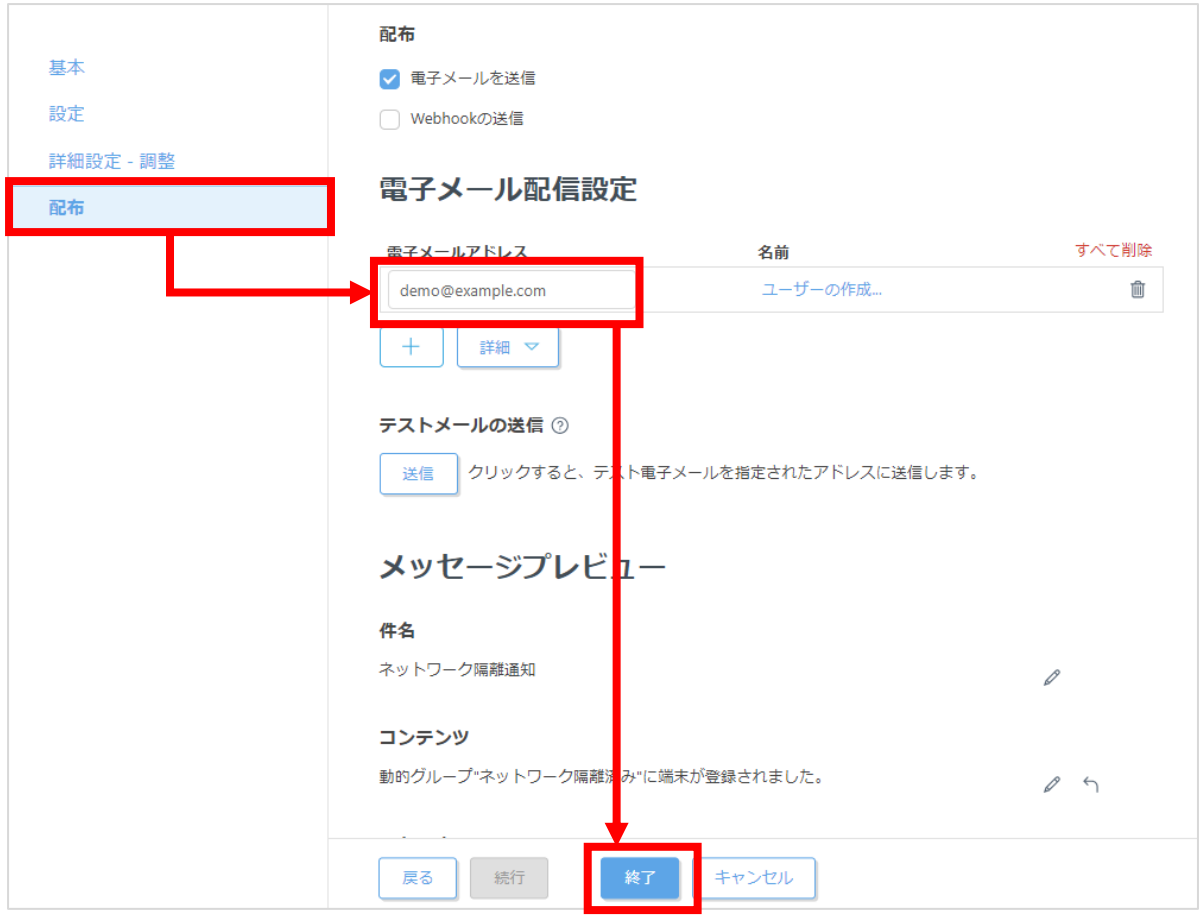
3. [設定]の各項目は以下のように設定します。

・[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 2.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。



参考：ESET Inspect ご確認時の注意事項

ESET Inspectをご確認いただく際、ご注意いただきたい点をご案内いたします。
※ESET社で脅威監視を実施しておりますので基本的にはお客さま側でESET Inspectの検知状況の確認は不要です。

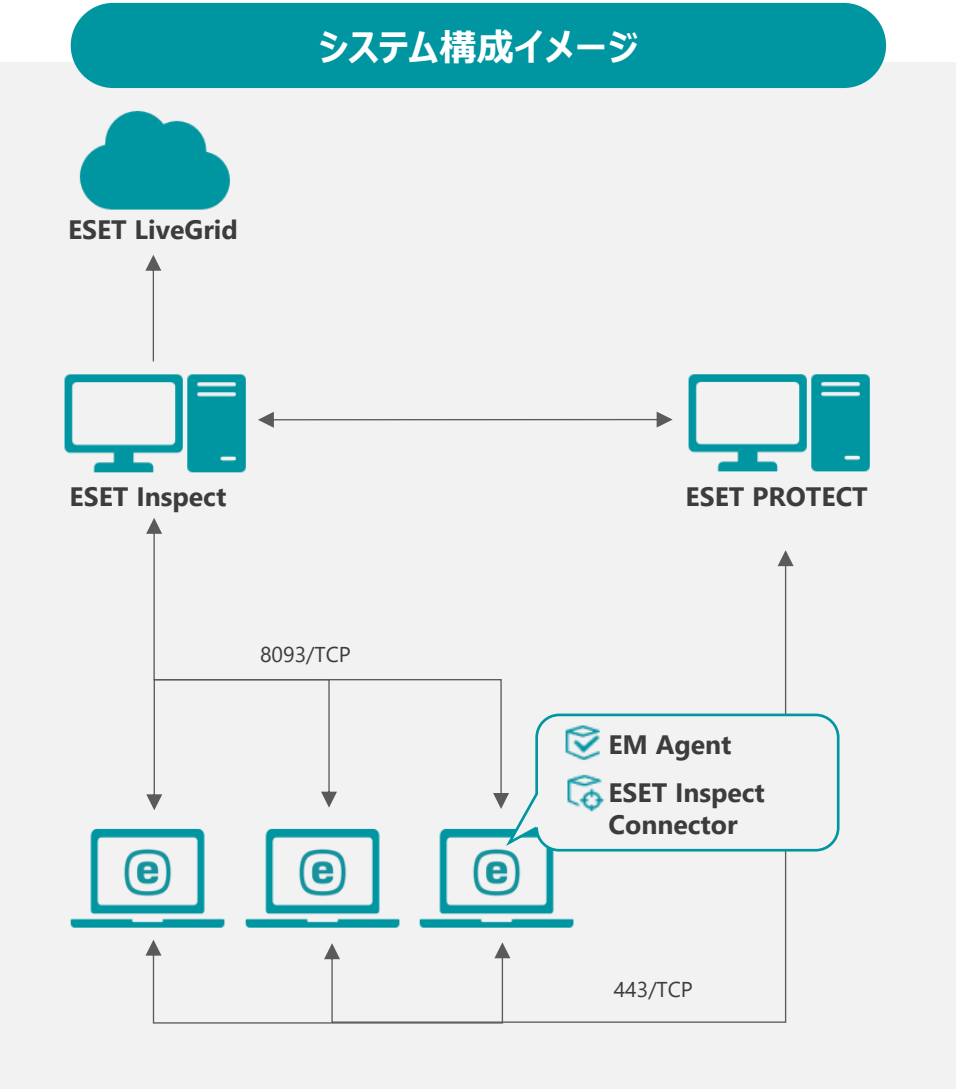
- **「検出」アラート**
  一定のルールに基づいて、PCのイベントが検出されます。
  検出内容はESET社で確認しているため、**アラートが上がっていてもユーザーさま側で何か対処いただく必要はありません。**
  対処が必要なアラートが発生した場合は「インシデント」として作成されます。

- **「インシデント」について**
  対応が必要なものは、「インシデントにユーザーのアクションが必要です」という通知が届いたインシデントのみです。
  ツール(EI)上で上記以外のインシデントも自動処理により作成されますが、ESET社による確認を行っているため
  対応不要です。

インシデントが発生した場合のオペレーションについてまとめた資料をご用意しております。
詳細は下記をご参照ください。
▼ESET PROTECT MDR Lite ~インシデント発生時のオペレーション~
https://eset-info.canon-its.jp/files/user/pdf/support/ep-mdr-lite_op.pdf

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)

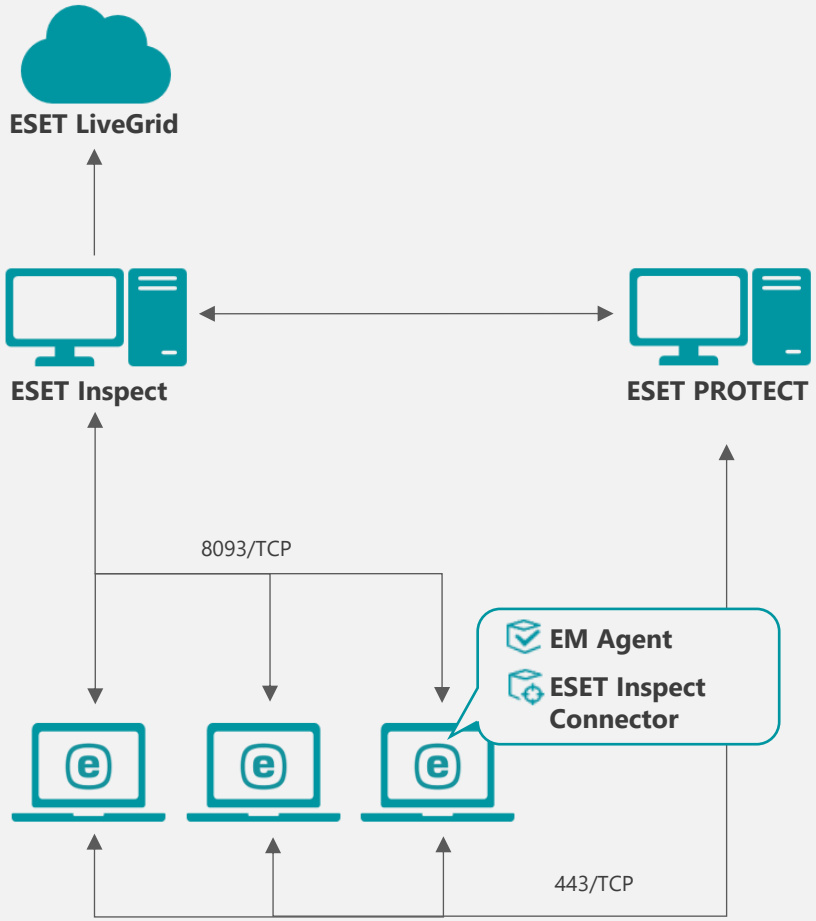
EI Connectorはクライアントのデータを収集し7分間隔でEIへデータを送信します。また、悪意のあるコンポーネントを削除し、これらのコンポーネントの実行をブロックします。

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

サポートされるプログラム

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
ESET Endpoint Security / アンチウイルス
ESET Endpoint Security / アンチウイルス for mac OS
ESET Endpoint アンチウイルス for Linux
ESET Server Security for Microsoft Windows Server
ESET Server Security for Linux

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は自動バージョンアップに対応しています。

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/