クラウド型セキュリティ管理ツール
ESET PROTECT
機能紹介資料

第46版

2025年7月1日

Canon

キヤノンマーケティングジャパン株式会社

はじめに（本資料について）

本資料は、クラウド型セキュリティ管理ツール ESET PROTECT（以降、EP）の機能を紹介している資料です。

- 本資料で使用している画面イメージは使用するOSやライセンスにより異なる場合があります。
  また、今後画面イメージや文言が変更される可能性がございます。
- ESET PROTECT ソリューションではクライアントOSおよびサーバーOSの端末に導入するプログラムとしてWindows、Mac、Linux、Android OS向けのプログラムをご使用いただけます。 各プログラムの機能紹介は別資料でご用意しています。
- Windows、Windows Server、Microsoft Edge および Internet Explorerは、米国 Microsoft Corporation の米国、日本およびその他の国における商標登録または商標です。macOS、OS X および iPhoneは、米国およびその他の国で登録されている Apple Inc. の商標です。
- ESET File Security for Microsoft Windows ServerはV8よりESET Server Security for Microsoft Windows Serverに名称が変更になりました。

もくじ

Ⅰ. ESET PROTECTとは

Ⅰ. ESET PROTECTとは

ESET PROTECT（EP）とは、ESET Endpoint Securityなどのウイルス・スパイウェア対策プログラムやクラウドサンドボックス製品、暗号化製品をインターネット経由で統合管理するクラウド型の管理ツールです。ウイルス・スパイウェア対策プログラムはWindows、Mac、Linux、Android向けプログラムを管理できます。
EPではiOSデバイスの管理も可能ですが、iOS向けのウイルス・スパイウェア対策プログラムはございません。※1

ESET PROTECTで管理可能なプログラムとサービス（2025年7月時点）

管理可能なプログラム	種別	バージョン
ESET Endpoint Security（EES）	Windows クライアントOS向け総合セキュリティプログラム	12.X / 11.X / 10.1 / 9.1
ESET Endpoint アンチウイルス（EEA）	Windows クライアントOS向けウイルス・スパイウェア対策プログラム	12.X / 11.X / 10.1 / 9.1
ESET Server Security for Microsoft Windows Server（ESSW）	WindowsサーバーOS向けウイルス・スパイウェア対策プログラム	12.X /11.X / 10.X / 9.X
ESET Endpoint Security for macOS（EESM）※2	Mac クライアントOS向けウイルス･スパイウェア対策プログラム	8.X / 7.4
ESET Endpoint アンチウイルス for Linux（EEAL）	Linux クライアントOS向けウイルス・スパイウェア対策プログラム	11.X / 10.3 / 10.2 / 9.1
ESET Server Security for Linux（ESSL）	LinuxサーバーOS向けウイルス・スパイウェア対策プログラム	11.X / 10.X / 9.1
ESET Endpoint Security for Android（EESA）	Android OS向け総合セキュリティプログラム	6.X / 5.X / 4.4 / 4.3
ESET LiveGuard Advanced（ELGA）	クラウドサンドボックス製品	-
ESET Full Disk Encryption（EFDE）	暗号化製品	2.X
ESET Vulnerability & Patch Management（VAPM）	脆弱性とパッチ管理	-

※1 EPではiOS 9.X / 10.X / 11.X / 12.0.X / 13.X / 14.X / 15.X / 16.X / 17.X / 18.X が管理可能です。
▼iOS端末の管理について https://eset-support.canon-its.jp/faq/show/4921?site_domain=business
※2 Macクライアント用プログラムはV8より、ESET Endpoint Security for OS X (EESM)とESET Endpoint アンチウイルス for OS X (EEAM)の表記による区別はなくなり、ESET Endpoint Security for macOS の表記に統一されました。ただし、機能はこれまでと同様にEESMとEEAMでは異なり保有ライセンス種別により区別されます。

Ⅰ. ESET PROTECTとは

EPの主な機能

EPを使用することにより、ESET Endpoint Securityなどウイルス・スパイウェア対策プログラムだけではなく、クラウドサンドボックス製品である**ESET LiveGuard Advanced** やフルディスク暗号化製品である**ESET Full Disk Encryption**、脆弱性とパッチ管理製品である**ESET Vulnerability & Patch Management**もインターネット経由で統合管理することができます。EPは主に以下の4つの機能で構成されています。

ログ監視機能
- ダッシュボード
- コンピューター
- 検出

クライアント管理機能
- レポート
- グループ
- ポリシー
- タスク
- インストーラー
- 通知

サーバー運用管理機能
- ユーザー管理
- 監視・監査

各ソリューションの統合管理機能
- ELGA
- EFDE
- VAPM

Ⅴ.ログ監視機能のご紹介を参照

Ⅵ.クライアント管理機能のご紹介を参照

Ⅶ.サーバー運用管理機能のご紹介を参照

Ⅷ.各ソリューションの統合管理機能のご紹介を参照

Ⅱ. ESET PROTECTの構成

Ⅱ. ESET PROTECTの構成

ESET PROTECTは以下のコンポーネントから構成されています。

ESET PROTECT（EP）

EPはクライアントプログラムの情報収集やタスク配布などを行います。クライアントとの通信はエージェントを経由して行います。

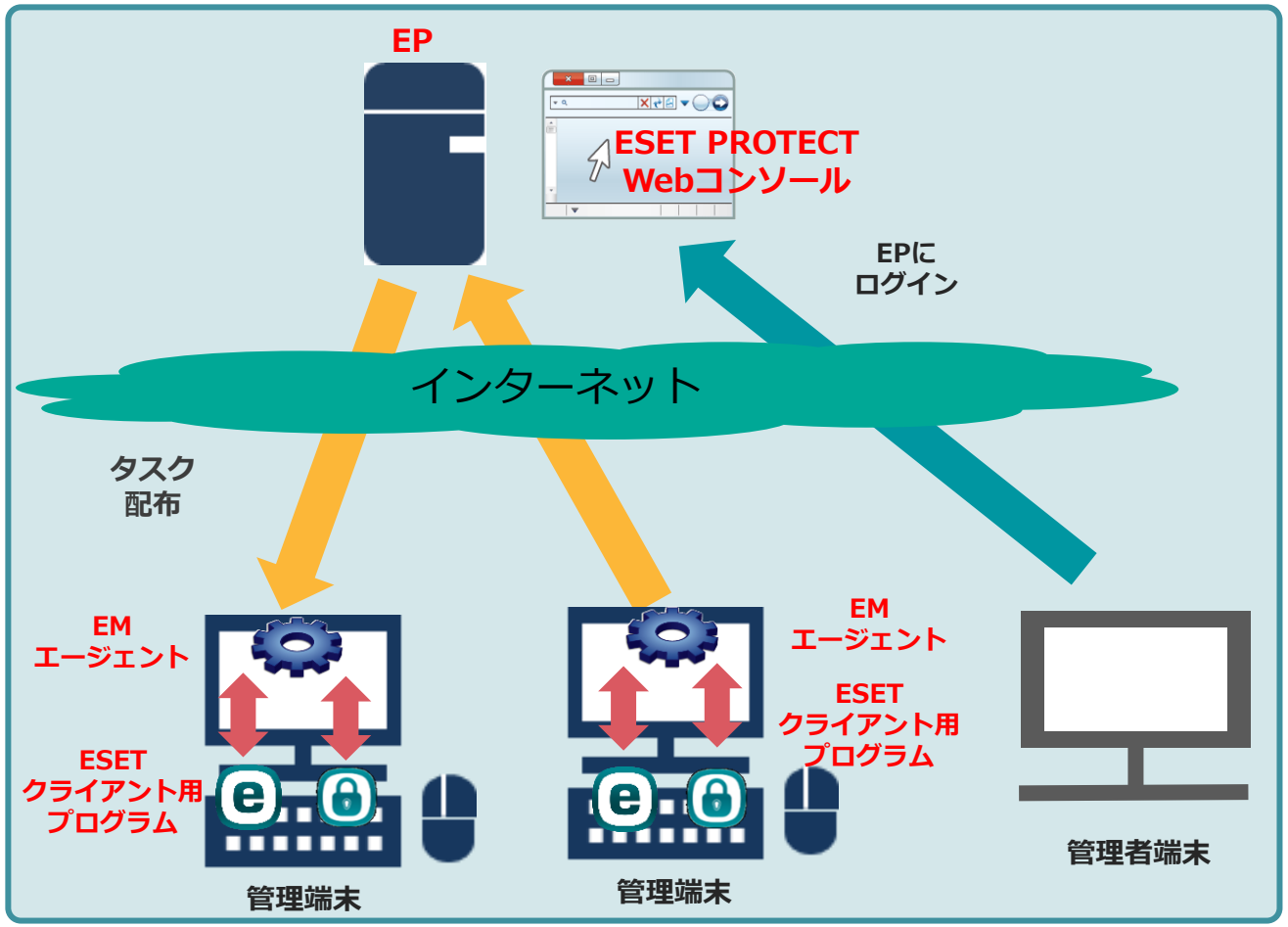
ESET PROTECT Webコンソール

WebコンソールはWebベースのインターフェースであり、ブラウザーを使用してEPへアクセスします。ブラウザー経由でクライアント情報の閲覧やタスクの実行などを行うことができます。

ESET Managementエージェント（EM エージェント）

エージェントは、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エージェントへ送信されたのち、エージェントがクライアントへ送信します。

※エージェントは自動バージョンアップに対応しています。

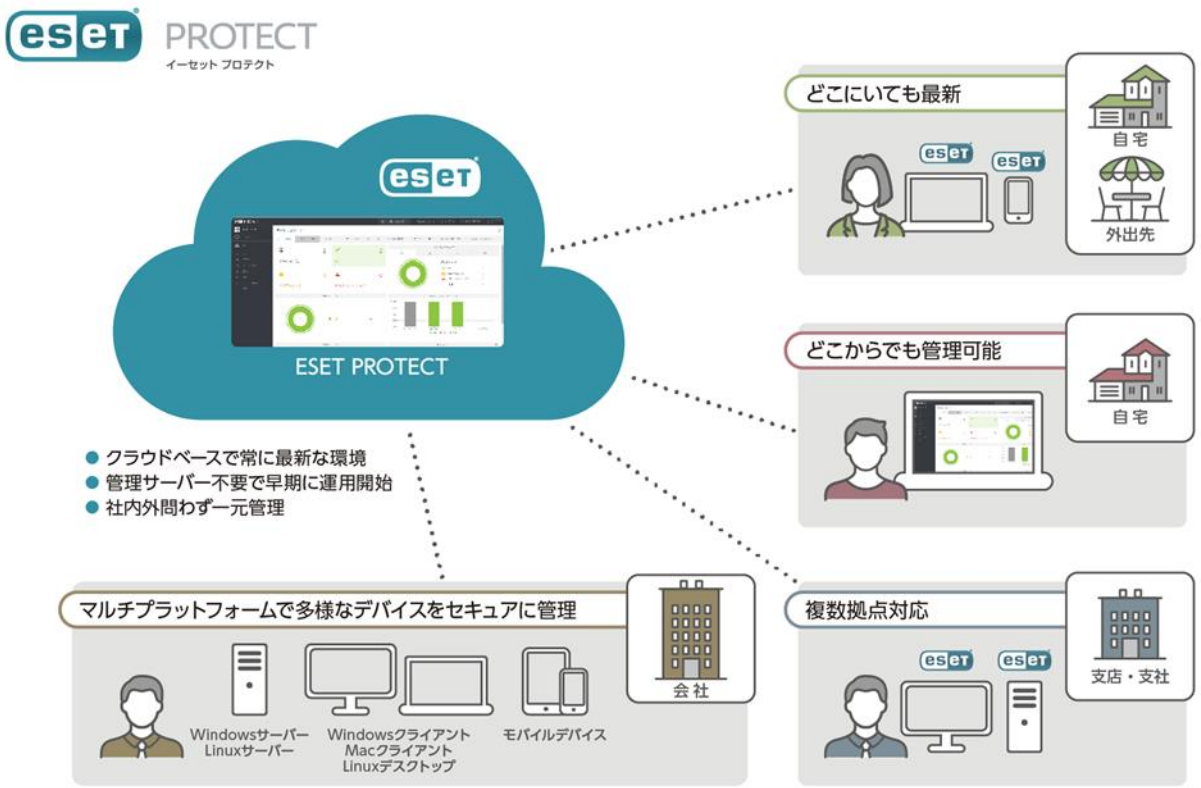


※EPとEMエージェント間の通信には認証プロキシはご利用いただけません。

Ⅲ. ESET PROTECTのメリット

Ⅲ. ESET PROTECTのメリット

EPを利用することで以下のメリットがあります。



① **管理サーバー不要で早期に運用開始**

EPはSaaS型であるため、サーバーの機器の購入や定期的なメンテナンスによる手間とコストを削減することができます。また、セットアップもWebブラウザ経由で10分程度で実施することが可能なため、すぐに運用を開始させることができます。

② **社内外問わず一元管理**

インターネットに接続できるクライアント端末であれば、社内外問わずに一元管理することができます。また、管理者はWebブラウザ経由でいつでもどこでもEPへアクセスでき、クライアント端末を管理することができます。

③ **クラウドベースで常に最新な環境**

EPのバージョン管理はESET社にて行われるため、お客様によるバージョンアップ作業は不要で常に最新の状態で利用することができます。また、EMエージェントも自動でバージョンアップされるため、お客様の運用やメンテナンスの負荷を減らすことができます。

Ⅳ. Webコンソールのご紹介

Ⅳ-Ⅰ.ログイン画面

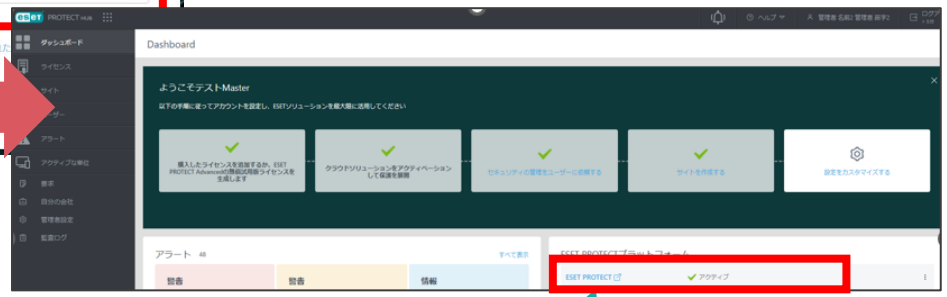
EPのWebコンソールへは、Webブラウザを使用して、ESET PROTECT HUB（EPH）を経由してログインします。Webベースのインターフェイスのため、Webブラウザからいつでもどこでもログインできます。

ESET PROTECT Webコンソール
サポート対象ブラウザー

サポート対象ブラウザー
Microsoft Edge
Mozilla Firefox
Google Chrome
Safari
Opera

※最新バージョンでご利用をお勧めします。

ESET PROTECT Webコンソールへのログイン



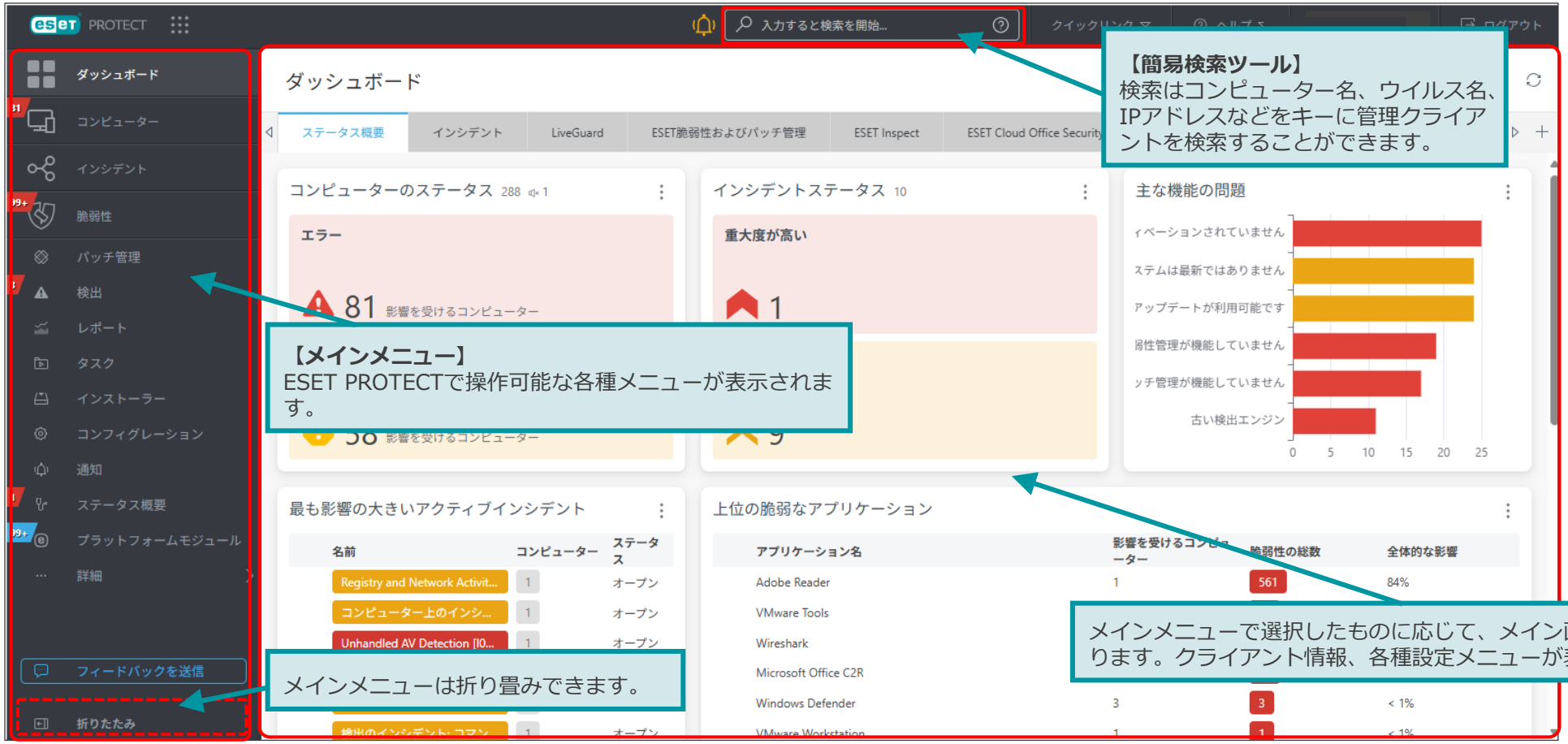
【EPHログイン画面】
EPH(https://protecthub.eset.com)へアクセスし、EPHアカウントの電子メールとパスワードを入力してログインします。

EPHにログイン後、画面右下の【ESET PROTECT】からログインします。

※ESET PROTECT HUB(EPH)とは、EPのログインの他、EPで利用するライセンスの管理を行うために使用します。
EPHアカウントの登録や使用方法についてはWebページをご確認ください
https://help.eset.com/protect_hub/public/ja-JP/

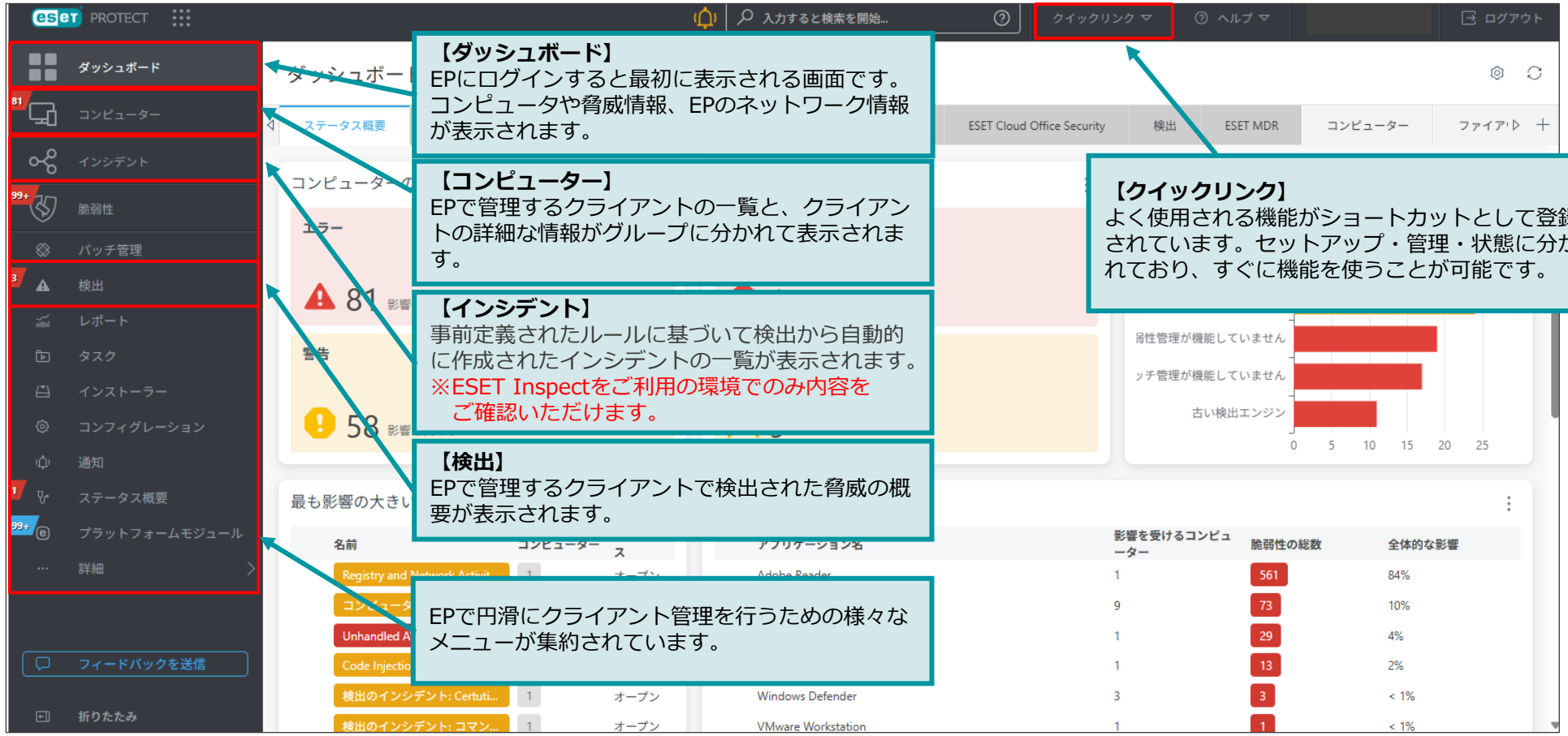
Ⅳ-Ⅱ. Webコンソールの画面構成

Webコンソールにログインすると以下の画面が表示されます。Webコンソールは３つのセクションより構成されており、画面左のメインメニューより、各種メニューを選択することで、レポートの閲覧や管理を行うための設定ができます。



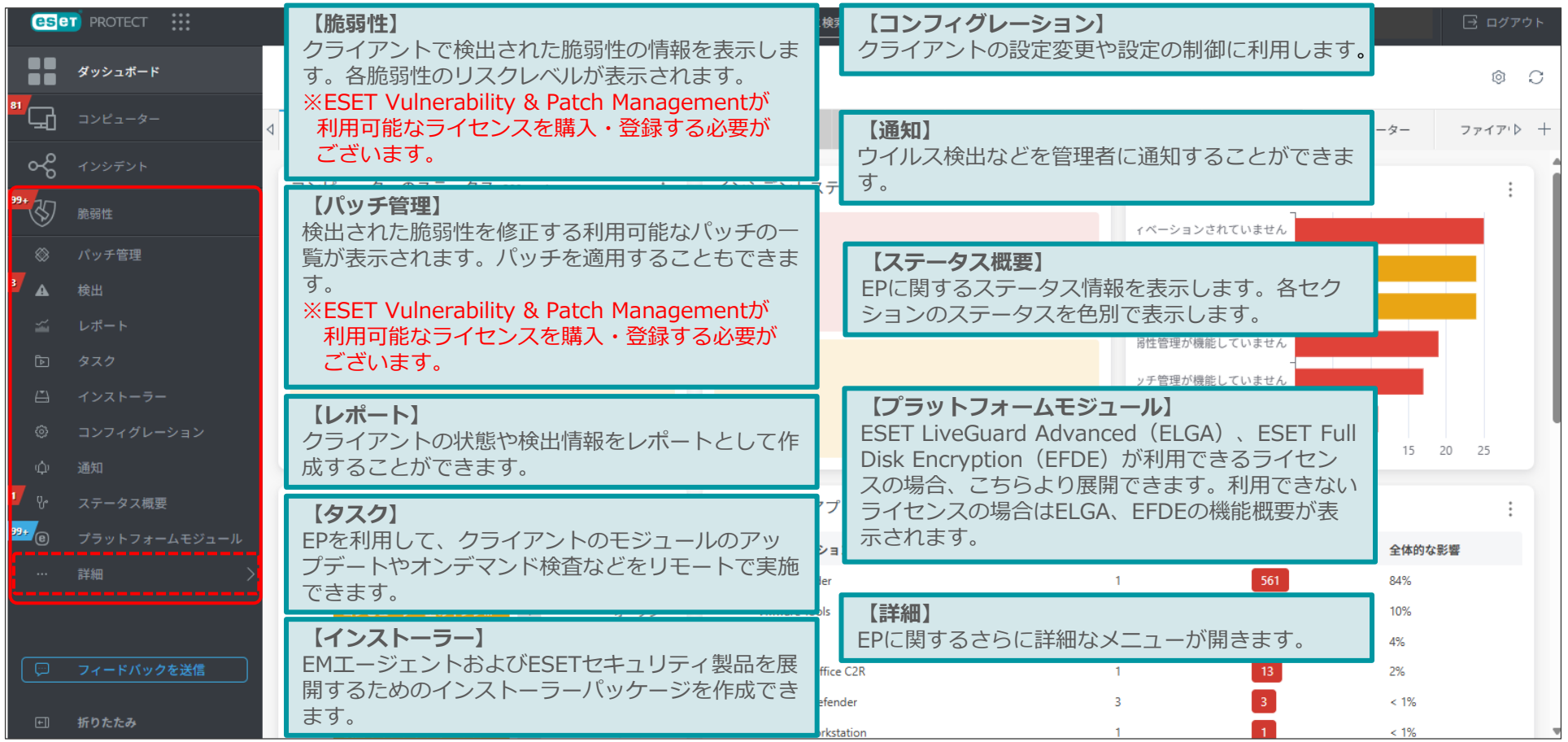
Ⅳ-Ⅲ. Webコンソールの画面構成（メインセクション）

Webコンソールのメインメニューではepの各メニューを選択することができます。
各メニューの詳細については、各機能のご紹介をご確認ください。



Ⅳ-Ⅲ. Webコンソールの画面構成（メインセクション）

メインメニューの後半にはEPの各メニューを選択することができます。
主にクライアント管理機能やログ監視機能が集約されています。詳細は各機能のご紹介をご確認ください。



【脆弱性】
クライアントで検出された脆弱性の情報を表示します。各脆弱性のリスクレベルが表示されます。
※ESET Vulnerability & Patch Managementが利用可能なライセンスを購入・登録する必要がございます。

【パッチ管理】
検出された脆弱性を修正する利用可能なパッチの一覧が表示されます。パッチを適用することもできます。
※ESET Vulnerability & Patch Managementが利用可能なライセンスを購入・登録する必要がございます。

【レポート】
クライアントの状態や検出情報をレポートとして作成することができます。

【タスク】
EPを利用して、クライアントのモジュールのアップデートやオンデマンド検査などをリモートで実施できます。

【インストーラー】
EMエージェントおよびESETセキュリティ製品を展開するためのインストーラーパッケージを作成できます。

【コンフィグレーション】
クライアントの設定変更や設定の制御に利用します。

【通知】
ウイルス検出などを管理者に通知することができます。

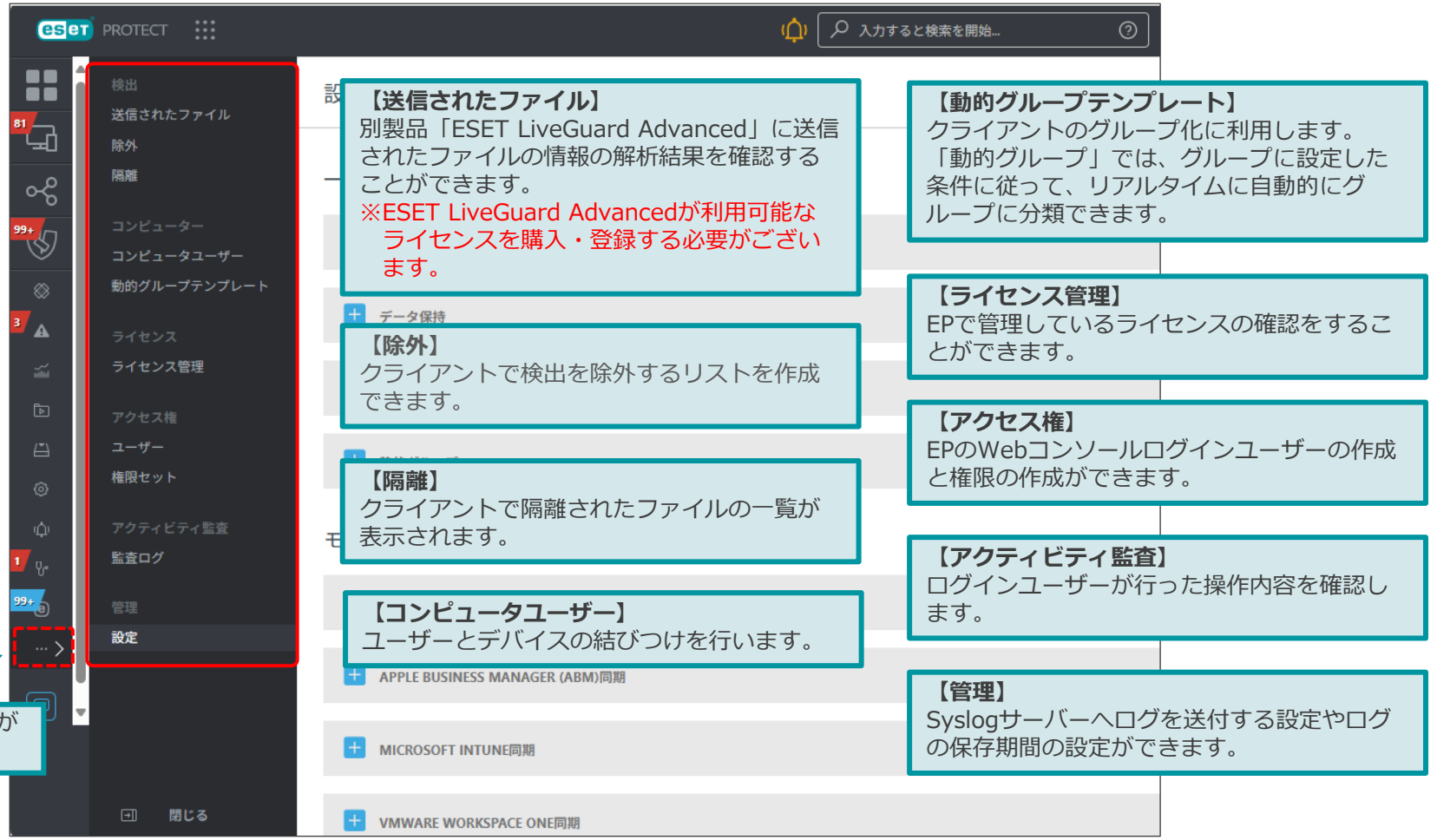
【ステータス概要】
EPに関するステータス情報を表示します。各セクションのステータスを色別で表示します。

【プラットフォームモジュール】
ESET LiveGuard Advanced（ELGA）、ESET Full Disk Encryption（EFDE）が利用できるライセンスの場合、こちらより展開できます。利用できないライセンスの場合はELGA、EFDEの機能概要が表示されます。

【詳細】
EPに関するさらに詳細なメニューが開きます。

Ⅳ-Ⅲ. Webコンソールの画面構成（メインセクション）

「詳細」を選択するとサブメニューが表示されます。
クライアント管理を行うための、さらに詳細な各種設定がございます。



【送信されたファイル】
別製品「ESET LiveGuard Advanced」に送信されたファイルの情報の解析結果を確認することができます。
※ESET LiveGuard Advancedが利用可能なライセンスを購入・登録する必要がございます。

【除外】
クライアントで検出を除外するリストを作成できます。

【隔離】
クライアントで隔離されたファイルの一覧が表示されます。

【コンピュータユーザー】
ユーザーとデバイスの結びつけを行います。

展開すると、サブメニューが表示されます。

【動的グループテンプレート】
クライアントのグループ化に利用します。
「動的グループ」では、グループに設定した条件に従って、リアルタイムに自動的にグループに分類できます。

【ライセンス管理】
EPで管理しているライセンスの確認をすることができます。

【アクセス権】
EPのWebコンソールログインユーザーの作成と権限の作成ができます。

【アクティビティ監査】
ログインユーザーが行った操作内容を確認します。

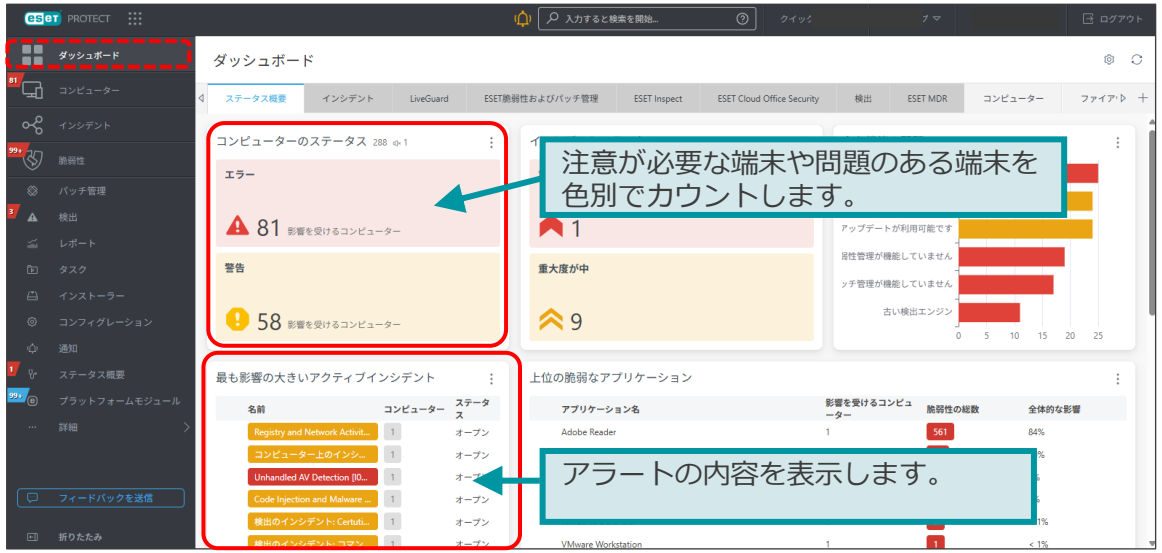
【管理】
Syslogサーバーへログを送付する設定やログの保存期間の設定ができます。

Ⅴ. ログ監視機能のご紹介

V-Ⅰ.ダッシュボード

EPにログインするとはじめに表示されるのがダッシュボードです。「ステータス概要」や「検出」では、
簡易的なクライアントの情報や脅威検出情報など管理しているクライアント全台の状態を確認できます。

ダッシュボード－ステータス概要（既定テンプレート）

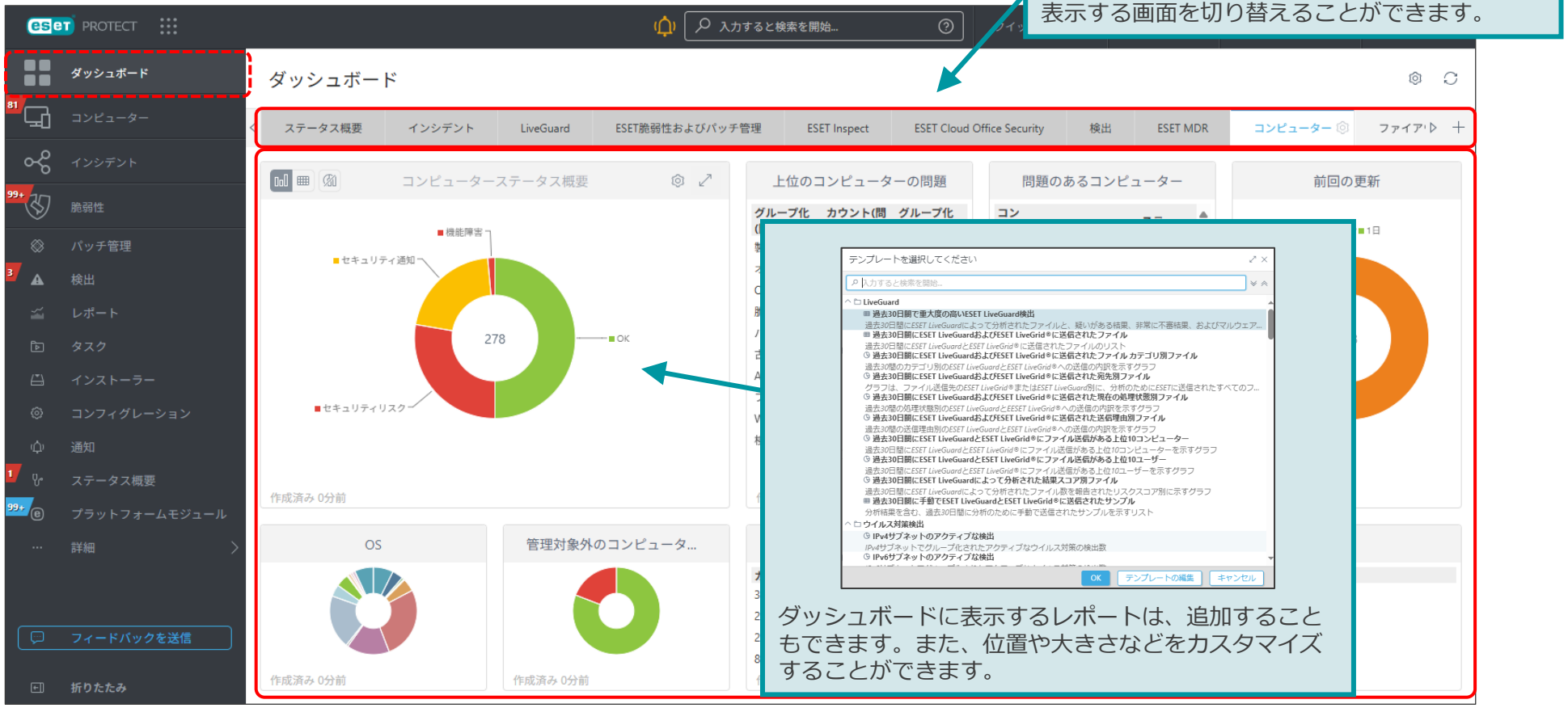


ダッシュボード－検出（既定テンプレート）

V-I.ダッシュボード

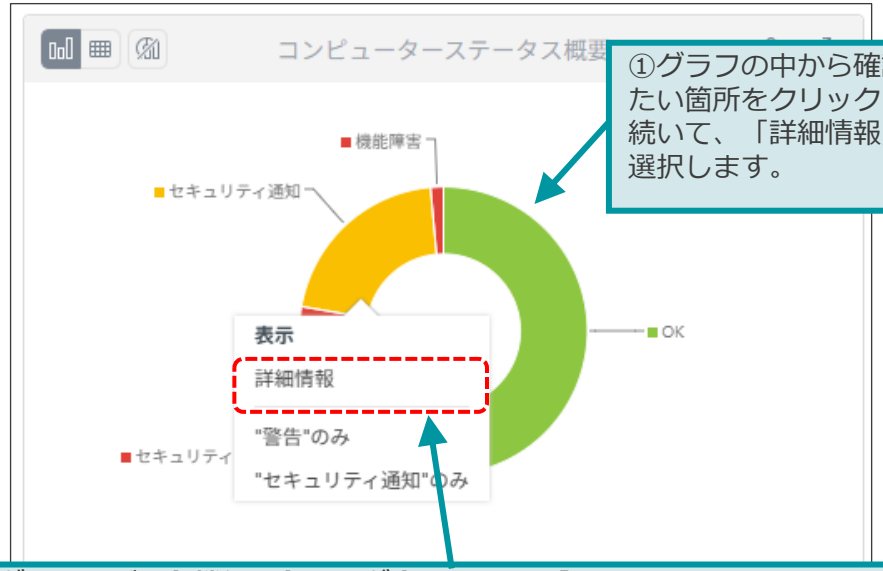
その他のダッシュボード画面はクライアントから収集した情報などをレポート化して閲覧できます。表示するレポートは、種類、大きさ、数を自由に変更することができます。

ダッシュボード－コンピューター（既定テンプレート）



V-I.ダッシュボード（詳細情報）

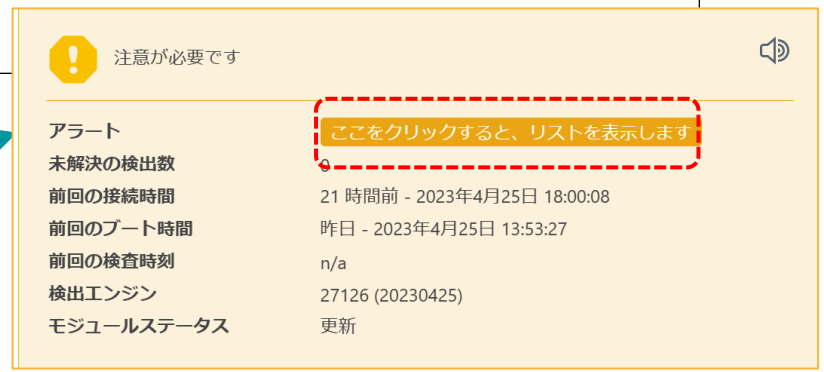
ダッシュボードに表示されているレポートから、詳細な情報を確認することができます。レポート上の確認したい箇所をクリックし「詳細情報」を選択することで、「ドリルダウン」して、さらに詳細な情報を確認することができます。



①グラフの中から確認したい箇所をクリックし、続いて、「詳細情報」を選択します。

②一覧の中から参照したい箇所をクリックし、続いて「詳細」を選択します。

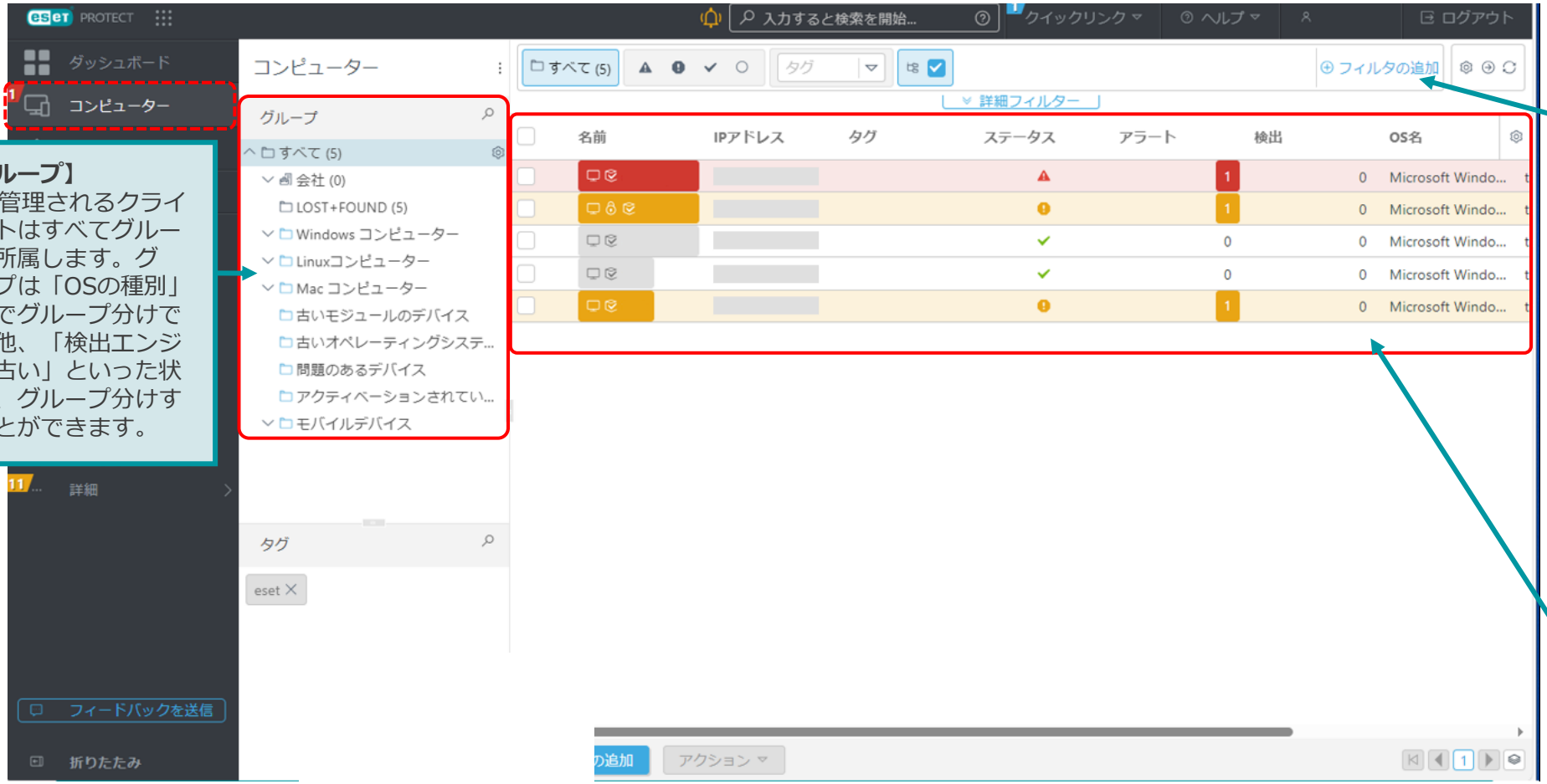
③セキュリティ通知内容が表示されます。



【ダッシュボード機能とドリルダウンについて】
ダッシュボード機能はレポートよりサマリーを表示する以外に詳細にデータを調べることができます。
確認したい項目をクリックし「詳細情報」を選択することでドリルダウンして情報を確認することができます。
※通常、ドリルダウンは複数の階層で表示されます。

Ⅴ-Ⅱ.コンピューター

EPで管理しているクライアントの情報を確認することができます。ウイルスの検出状況以外にもインストールが行われているOS情報やアプリケーションの名前、バージョンなども確認できます。



【グループ】
EPで管理されるクライアントはすべてグループに所属します。グループは「OSの種別」などでグループ分けできる他、「検出エンジンが古い」といった状態で、グループ分けすることができます。

フィルタやプリセットを利用し、条件を追加することで、グループに所属するクライアントをさらに絞込むことができます。「問題のあるコンピュータのみ」に絞ることで対処が必要なPCをいち早く確認できます。

- FQDN
- IMEI
- IPアドレス
- OSタイプ
- OSバージョン
- OSバージョンパック
- OSプラットフォーム
- OS名
- アラート数
- ｸﾞﾙｰﾌﾟ

画面左側で選択されたグループに所属するクライアントの一覧が表示されます。

V-Ⅱ.コンピューター（詳細情報）

コンピューターの詳細情報では、ウイルス対策製品の情報以外にもデバイスの情報や導入されているアプリケーションの情報、ハードウェア情報の閲覧ができます。

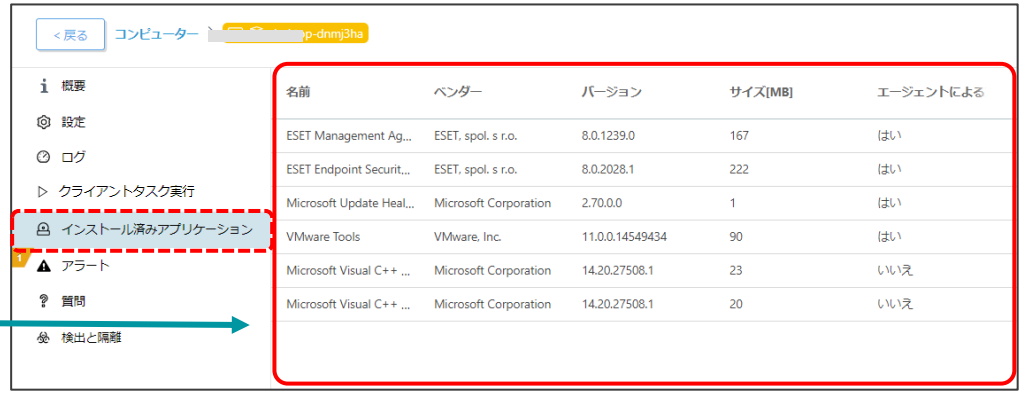
コンピューター詳細画面－概要

【 概要 】
コンピュータの情報やESETの情報について、概要をまとめています。
またデバイスのRAM、ストレージ、プロセッサーなどハードウェアの詳細情報についても確認できます。

コンピューター詳細画面－設定

【 設定 】
クライアントの設定を閲覧することができます。適用されているポリシーを確認することができます。

コンピューター詳細画面－インストール済みアプリケーション



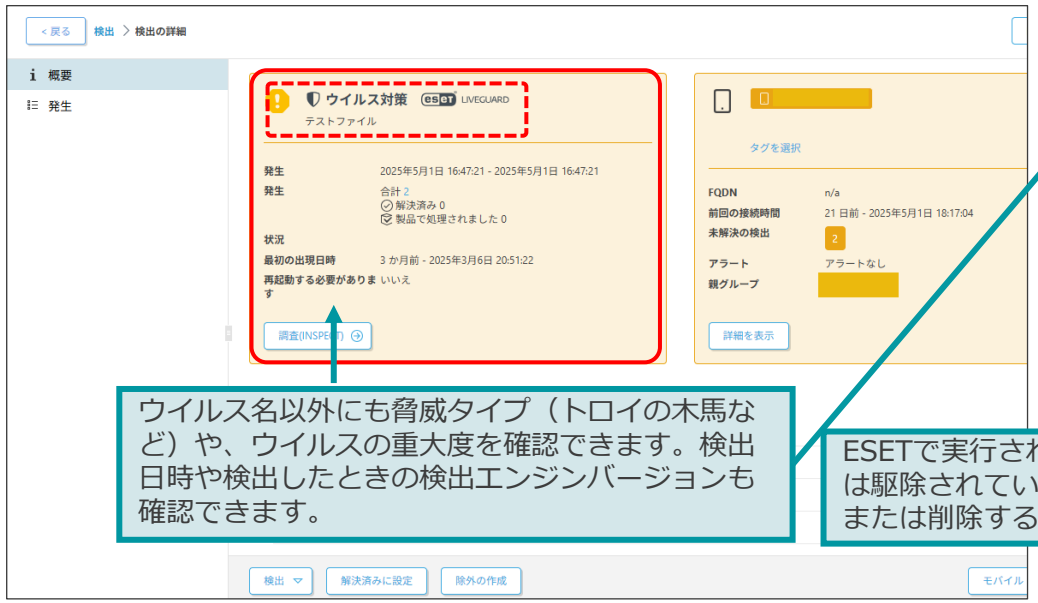
【 インストール済みアプリケーション 】
一覧を表示させることができます。タスク機能を使用して、アプリケーションのアンインストールができます。

Ⅴ-Ⅲ. 検出

コンピューターで検出された脅威の概要を確認できます。検出された脅威は、「未解決の脅威」と「解決済みの脅威」に分類され、すべてのウイルスログやファイアウォール、HIPSログの概要が表示されます。

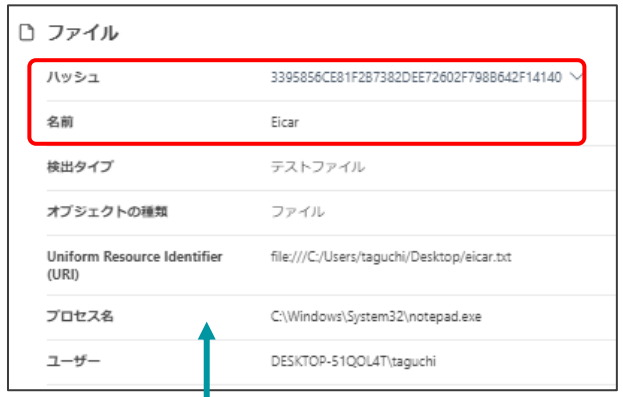
Ⅴ-Ⅲ. 検出（脅威の詳細）

脅威の詳細では、ウイルス名以外にも、脅威が検出された方法（スキャナ）やプロセス名などを閲覧することができます。



ウイルス名以外にも脅威タイプ（トロイの木馬など）や、ウイルスの重大度を確認できます。検出日時や検出したときの検出エンジンバージョンも確認できます。

ESETで実行されたアクションが確認できます。未解決または駆除されていない脅威の場合は、詳細検査を実行し、駆除または削除する必要があります。



ウイルスが検出されたプロセスが表示されます。また、検出時のユーザー名が表示されるため、共有端末などでユーザアカウントを切替えて使用する場合もどのユーザーアカウントで検出されたか確認することができます。

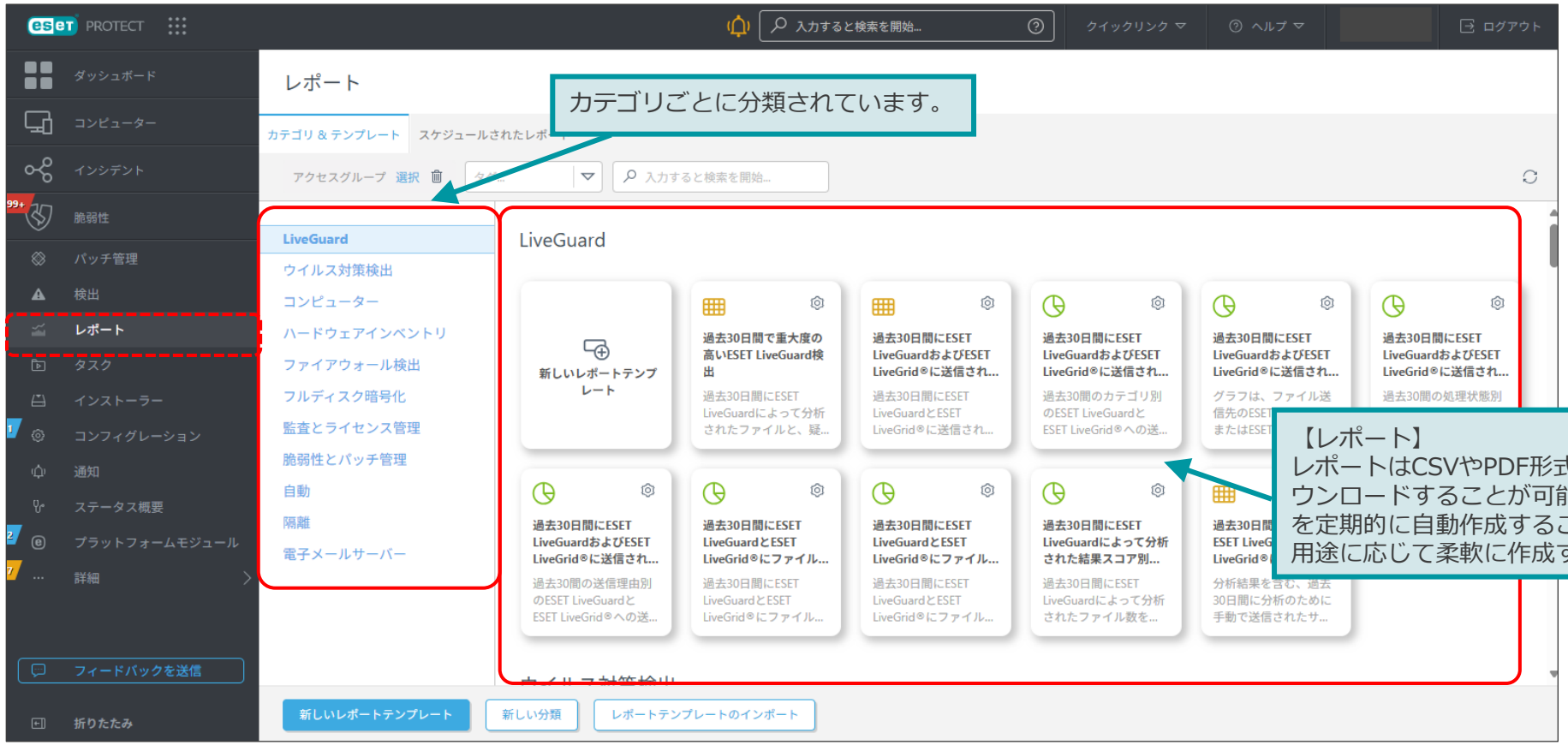
[世界での観測]
ESET LiveGrid®で収集した情報から脅威を評価します。LiveGridでの評価や発生数、初回に確認された時期が確認できます。評価は色別に脅威レベルが分かれており、[赤：悪意] [黄：不審] で表示されます。

[組織内で観測された検出]
管理しているクライアントの中で検出された回数や初回検出日時、前回の検出日時を確認できます。

Ⅵ. クライアント管理機能のご紹介

Ⅵ-Ⅰ. レポート

クライアントから収集したウイルス対策やハードウェアなどの情報をもとにレポートを作成することができます。テンプレートとして既に定義されているレポートは約100種類あり、テンプレートをもとに独自にレポートを作成することもできます。

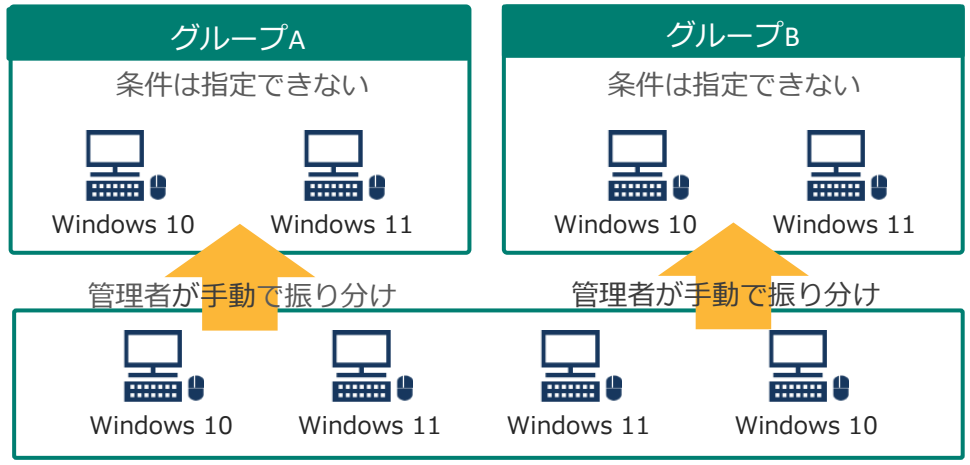


Ⅵ-Ⅱ. グループ

EPで管理しているクライアントをグループ分けすることができます。「静的グループ」と「動的グループ」の2種類のグループを作成することができます。

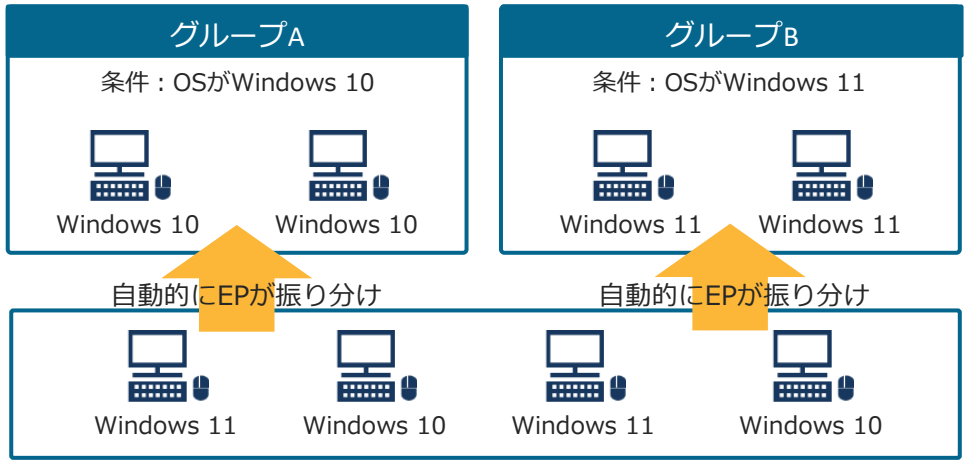
静的グループ

静的グループは、管理者が手動でグループ化をおこないます。
グループに追加したクライアントが自動的に変更されることはありません。



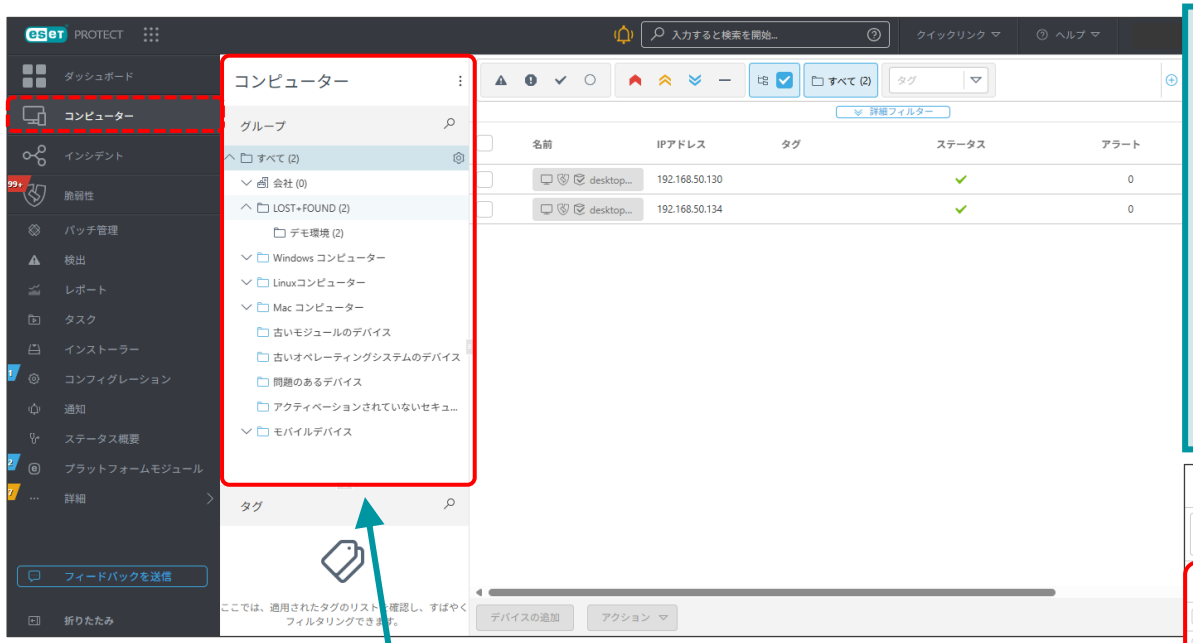
動的グループ

動的グループは、グループに指定した条件を満たすクライアントが自動的に振り分けされます。条件は、OSやIPアドレス、製品バージョンなどを設定することができます。



Ⅵ-Ⅱ. グループ

コンピュータより、「動的グループ」と「静的グループ」でグループ分けしたコンピューターの情報確認と、グループの設定ができます。



【グループ】
グループの一覧を確認することができます。
それぞれ下記アイコンで表示されます。

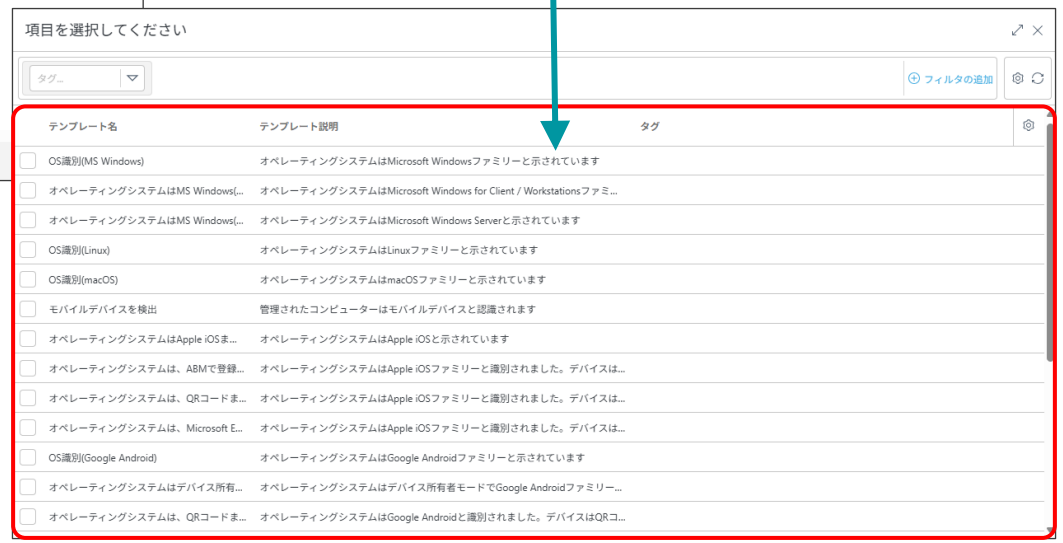
静的グループ、 動的グループ

また、 をクリックすることで新規のグループを作成することができます。

動的グループにはOS別（Windows、Linux、Mac）など
よく使われるグループがテンプレートとして用意されています。
動的グループの条件には下記のような値を指定できます。
端末情報だけでなくESETのバージョンやアラートの状態で条件をつけることもできます。

●主な条件値
・IPアドレス（[ネットワークIPアドレス]-[アダプタIPアドレス]）
・OS（[OSエディション]-[OSタイプ]）
・検出エンジンバージョン（[機能/保護の問題]）
・インストールされたソフトウェア（[インストールされたソフトウェア]）

など

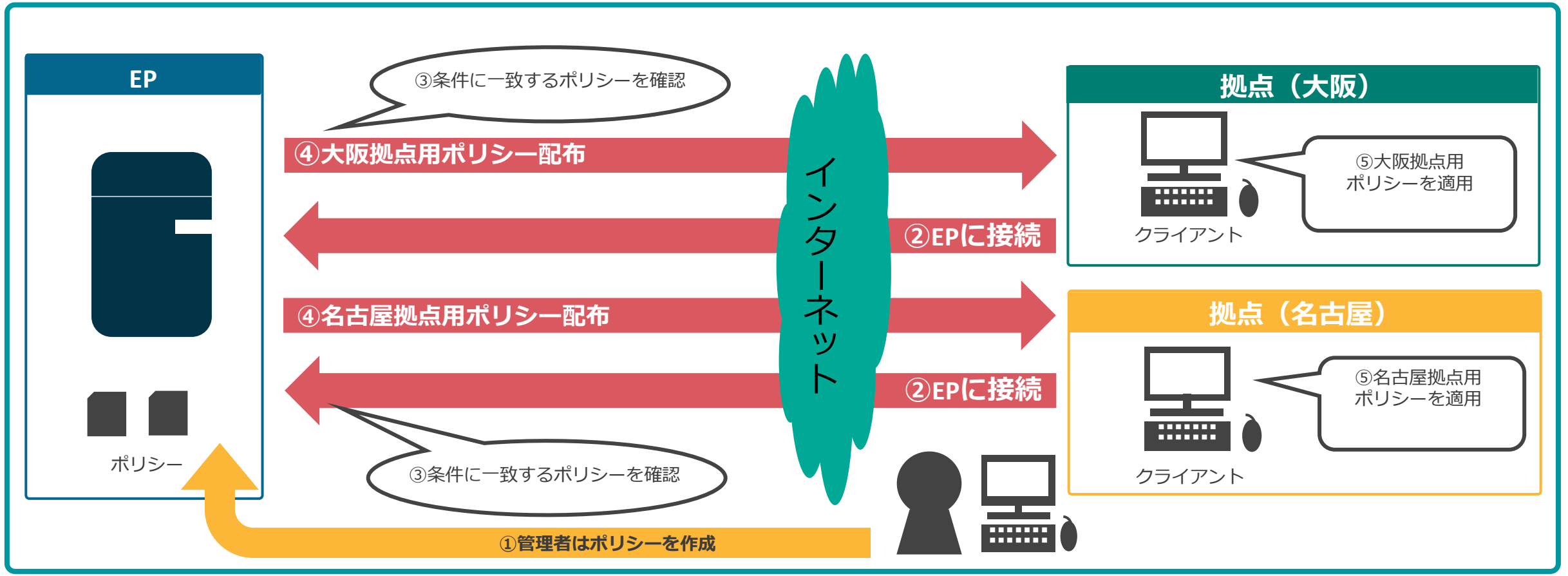


Ⅵ-Ⅲ. コンフィグレーション

コンフィグレーションには、セキュリティ製品などの設定をおこなう「基本設定」とポリシー設定をおこなう「詳細設定」があります。
基本設定タブでは、セキュリティ製品やESET LiveGuardの設定が可能です。設定可能な内容としては、パスワードによるセキュリティ設定のロックや、ESET LiveGuardの有効化などがあります。

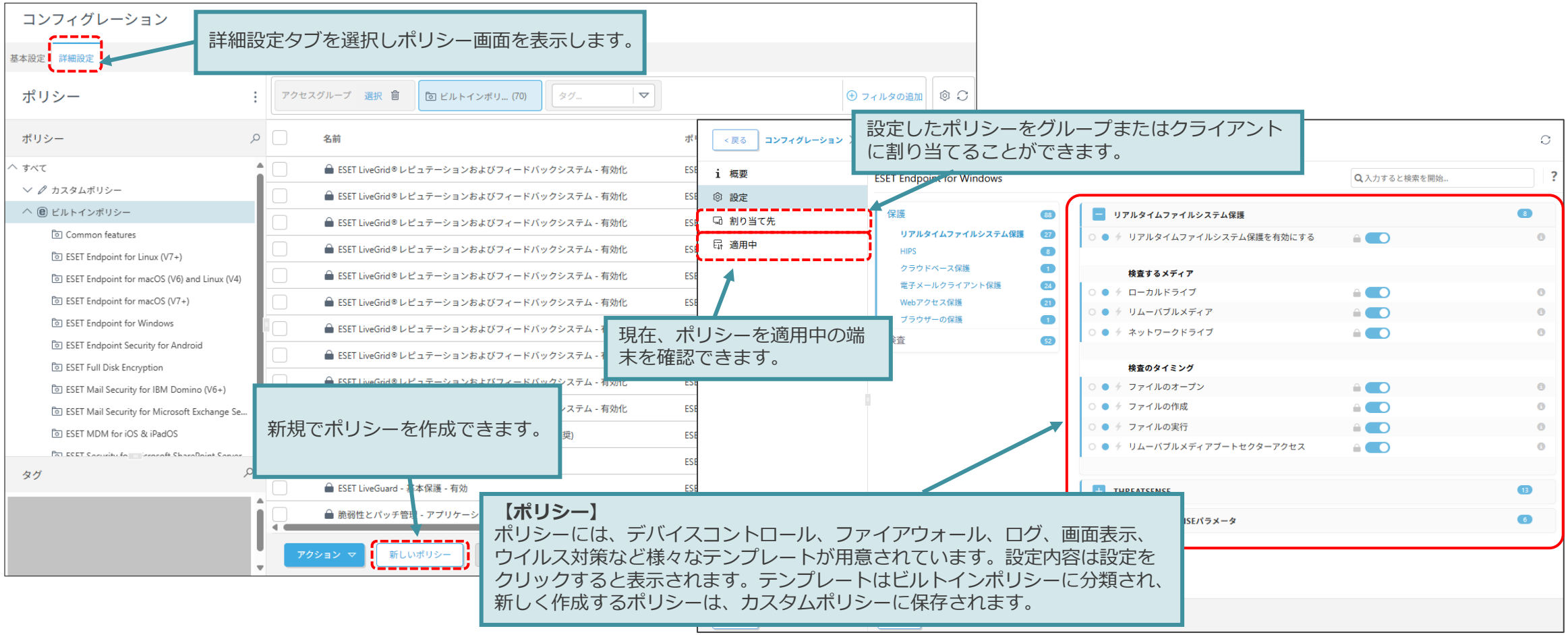
Ⅵ-Ⅲ. コンフィグレーション

詳細設定タブでは、「ポリシー」が利用できクライアントのESETの設定変更が可能です。
ポリシーは、クライアントがEPに接続した際に適用されます。「グループ」に適用するとあらかじめ設定した条件に従って、任意の設定を自動で適用することもできます。



Ⅵ-Ⅲ. コンフィグレーション

詳細設定タブでは、ポリシーの作成や編集をおこなうことも可能です。ポリシーにはテンプレートが用意されていますが、テンプレートをもとにして独自にポリシーを作成することも可能です。設定画面はクライアント側で表示される画面と同じ画面となり、簡単に設定をおこなうことができます。



Ⅵ-Ⅳ. タスク

タスク機能を使用すると、ウイルス検査や、検出エンジンのアップデートをリモートで実行することができます。製品別に分類されており、約40種類のタスクを用意しています。
EPから配布できるタスクは以下の通りです。

主要なタスク

ESETセキュリティ製品

- **ESET製品の設定エクスポート**
  クライアントの設定をエクスポートします。
- **オンデマンド検査**
  クライアントでコンピュータの検査を実行します。。
- **モジュールアップデート**
  クライアントの検出エンジンをアップデートします。
- **製品のアクティベーション**
  クライアントのアクティベーションを実行します。
- **コンピューターをネットワークから隔離する**
  エージェント等の通信以外を遮断しクライアントを隔離します。

ESET PROTECT

- **エージェントのアップグレード**
  EMエージェントのアップグレードを実行します。
- **管理の停止（ESET Management Agentのアンインストール）**
  クライアントのEM エージェントをアンインストールします。

OS

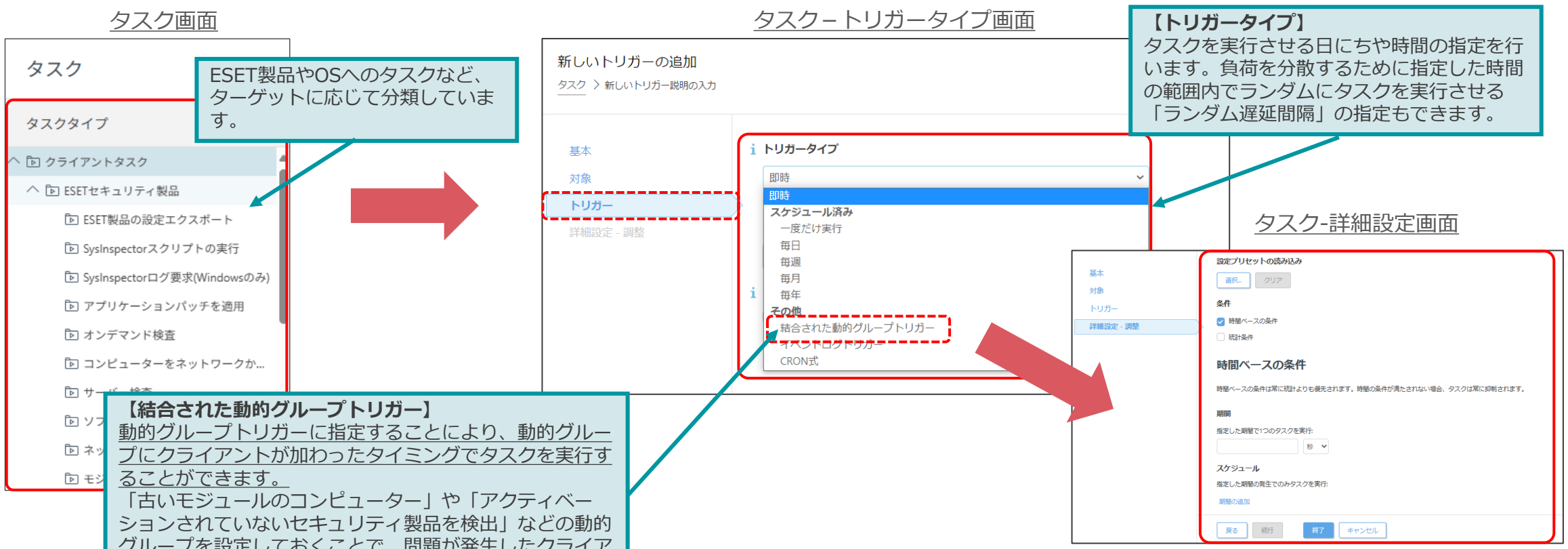
- **オペレーティングシステムアップデート**
  クライアントのOSのアップデートを実行します。
- **メッセージの表示**
  クライアントの画面上に任意の文字列を表示させます。
- **ソフトウェアインストール / ソフトウェアアンインストール**
  ESET製品のインストール/アンインストールを実行します

モバイル

- **Anti-Theftアクション**
  Androidデバイスの盗難や紛失時に、検索、ロック、警報、ワイプ拡張初期設定リセットを実行します。

Ⅵ-Ⅳ. タスク

タスクでは、実行するターゲットを「コンピューター」単体で指定する以外に「静的グループ」「動的グループ」を指定することで複数のコンピューターに対して指定できます。タスクを実行するタイミングはトリガーで設定します。



Ⅵ-Ⅴ. インストーラー

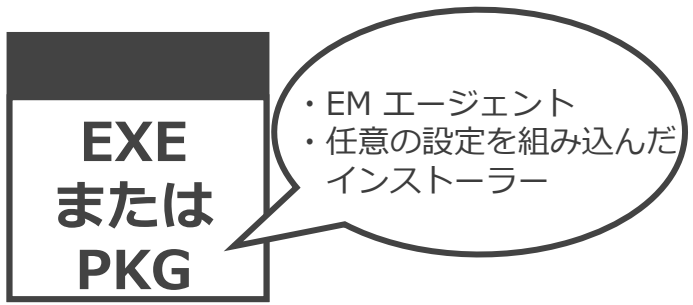
クライアントにEM エージェントとESET製品を展開するためのインストーラーパッケージを作成することができます。インストーラー機能では、以下3種類のインストーラーを作成することができます。
作成したインストーラーはダウンロードリンクを作成してブラウザからダウンロード、または電子メールでユーザーにダウンロードリンクを送信することもできます。

インストーラー

ライブインストーラー（Windows/Mac）

EM エージェントとESET製品を含むインストーラーパッケージ、またはEMエージェントのインストーラーパッケージ。

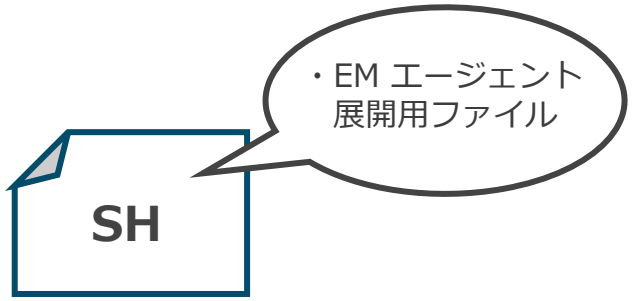
ESET製品の設定を組み込んだり、所属するグループを事前に指定できます。



エージェントスクリプトインストーラー（Mac/Linux）

EM エージェントにEPへ接続するための設定を組み込んだスクリプトファイル。

ESET製品のインストールは、別途行う必要があります。



GPOまたはSCCMスクリプト

GPOまたはSCCMを使用したEMエージェント展開用スクリプトファイルとEMエージェントのインストーラー。

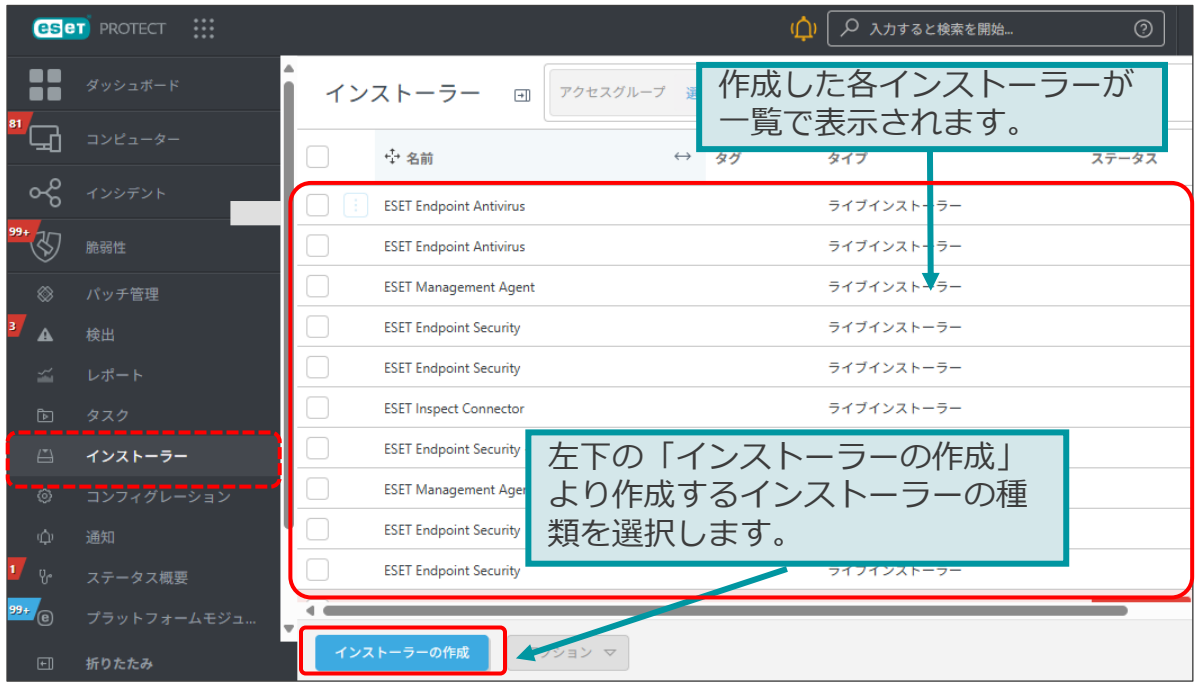
ESET製品のインストールは、別途行う必要があります。

展開用スクリプトファイルとEMエージェントのインストーラーを同一ファイルに配置して実行する必要があります。

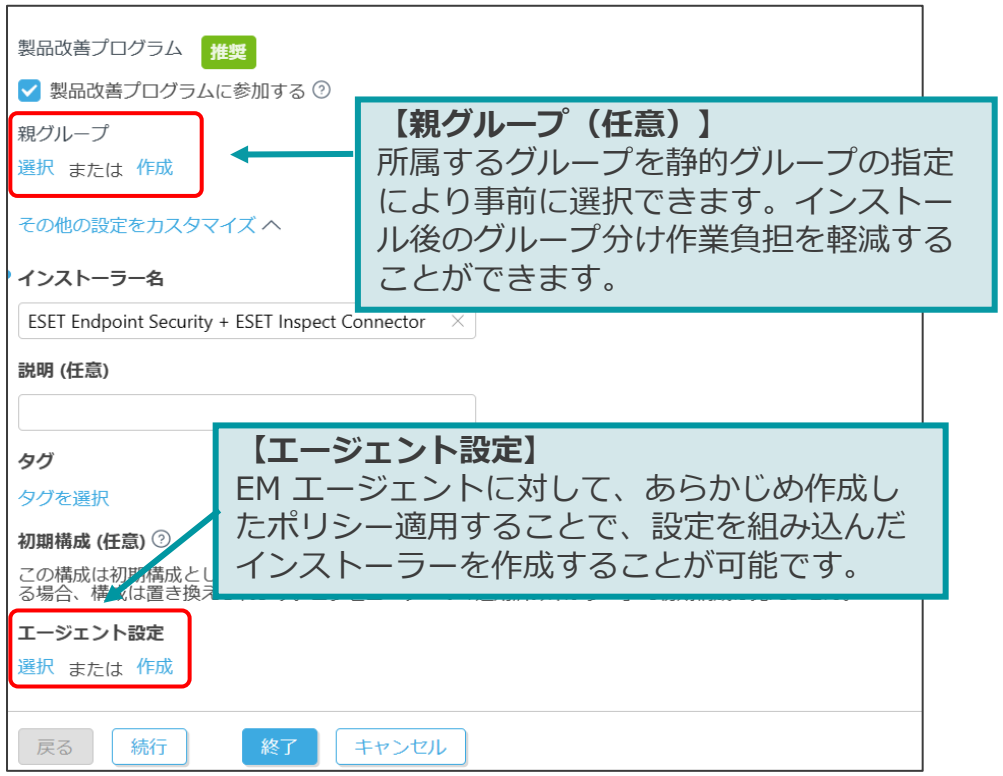
Ⅵ-Ⅴ. インストーラー

一度作成したインストーラーは、一覧で表示されます。作成時にポリシーをEM エージェントやESET製品に組み込むことができます。また、所属する「静的グループ」を事前に指定することができ、展開時のグループ管理がおこないやすくなっております。

インストーラー画面

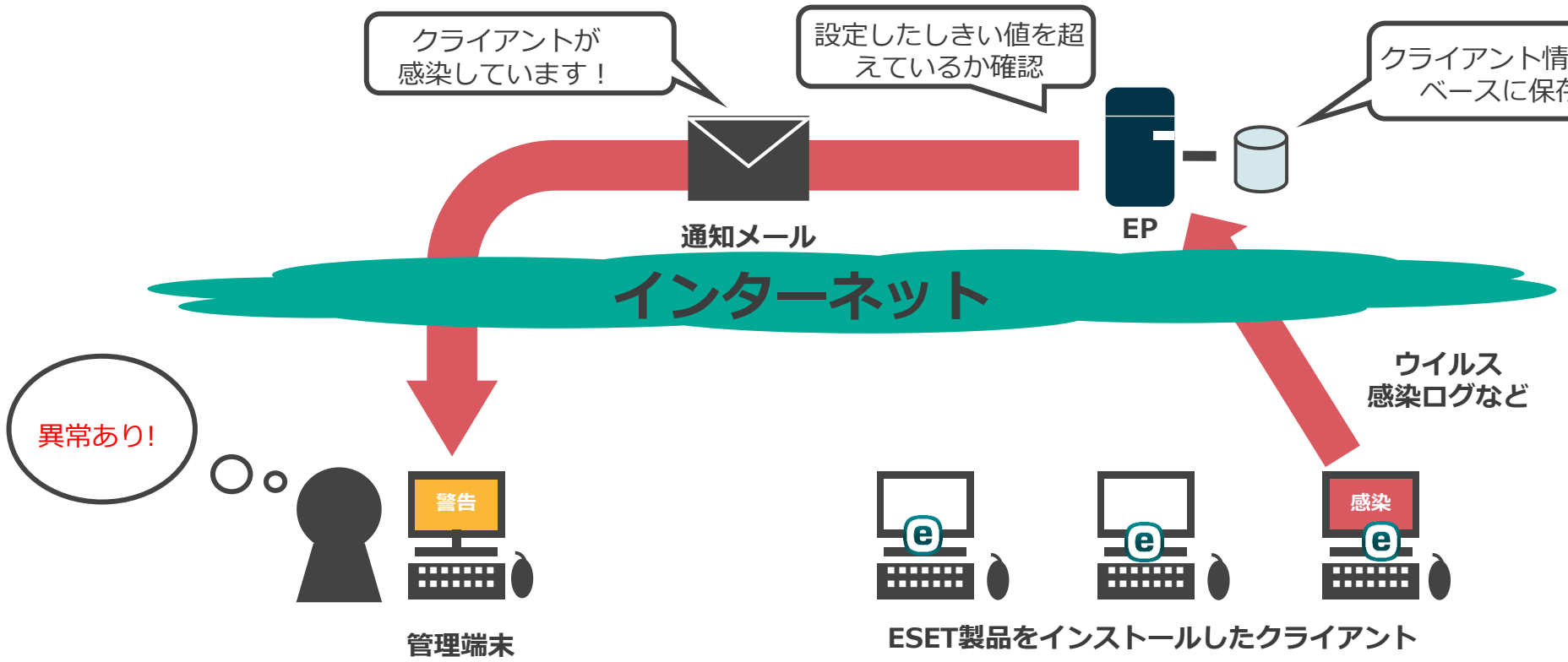


ライブインストーラー(カスタマイズ)画面



VI-VI. 通知

通知メニューで設定したルールのしきい値を超えた場合、 EPから管理者に通知を行うことができます。
これにより、ウイルスを検出したクライアントが発見された場合やクライアントで問題があった場合、管理者に通知することができます。

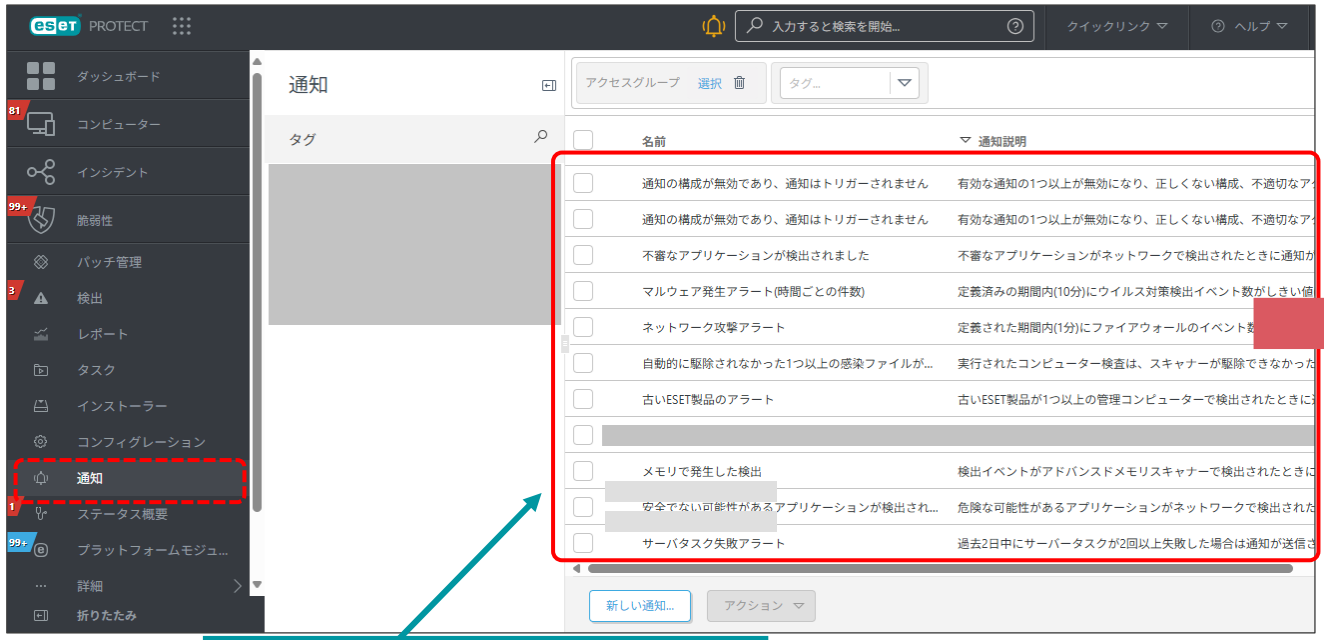


※通知メールがスパム判定されないように以下のアドレスを除外してください。
report@protect.eset.com

VI-VI. 通知

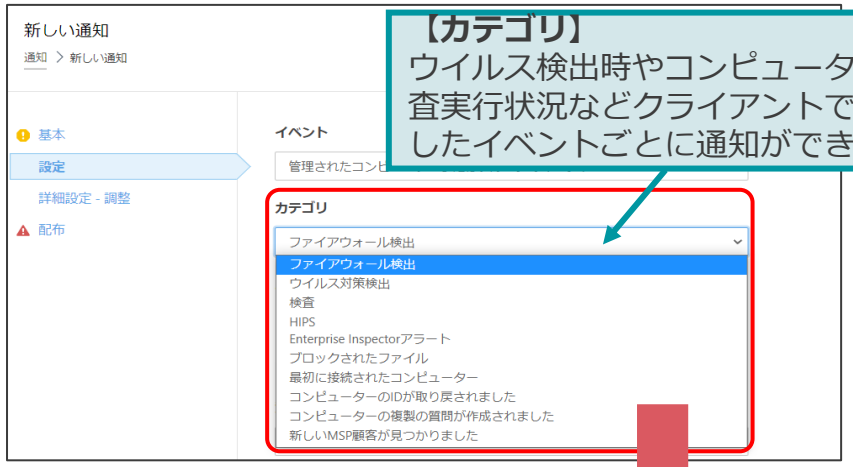
通知はあらかじめテンプレートが用意されています。通知は電子メールまたはWebhookでおこないます。

通知画面



【通知ルール】
マルウェアの発生状況など、既定で24種類のルールが用意されています。

通知–設定画面



【カテゴリ】
ウイルス検出時やコンピュータの検査実行状況などクライアントで発生したイベントごとに通知ができます。

通知–配布画面

【配布】
通知先を設定します。複数の管理者に通知する場合は、CSVのインポートでアドレスを登録することができます。

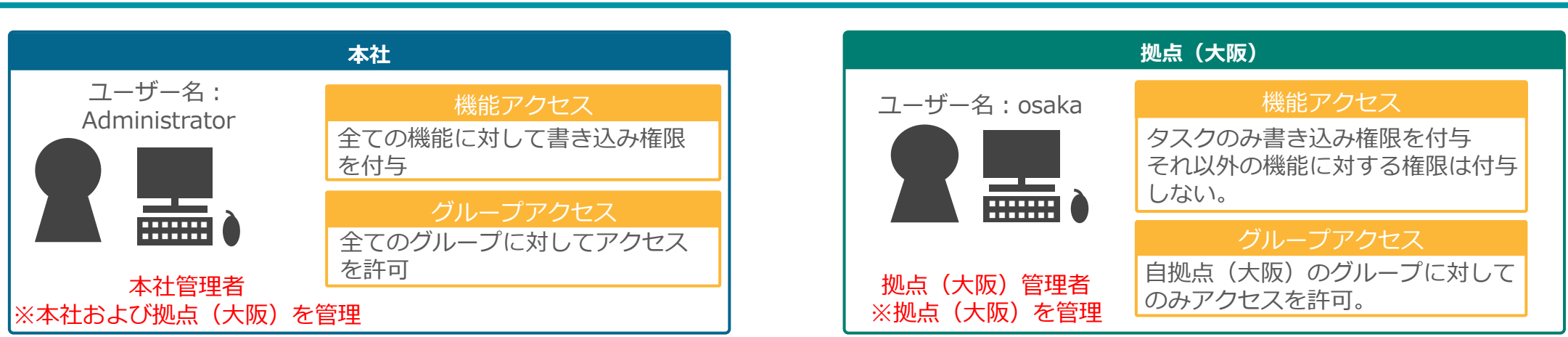
Ⅷ. サーバー運用管理機能のご紹介

Ⅷ-Ⅰ.ユーザー管理

EPのアクセス権をもつユーザーを複数作成できます。EPではユーザーに対して設定可能なアクセス権が2種類あります。

① 機能アクセス　　：EPの各機能に対して読み取り/使用/書き込みの指定ができます
② グループアクセス：静的グループの指定により対象の指定ができます

２種類のアクセス権を組み合わせることで、特定のグループに所属するクライアントに対して管理を行うといった柔軟なアクセス設定ができます。

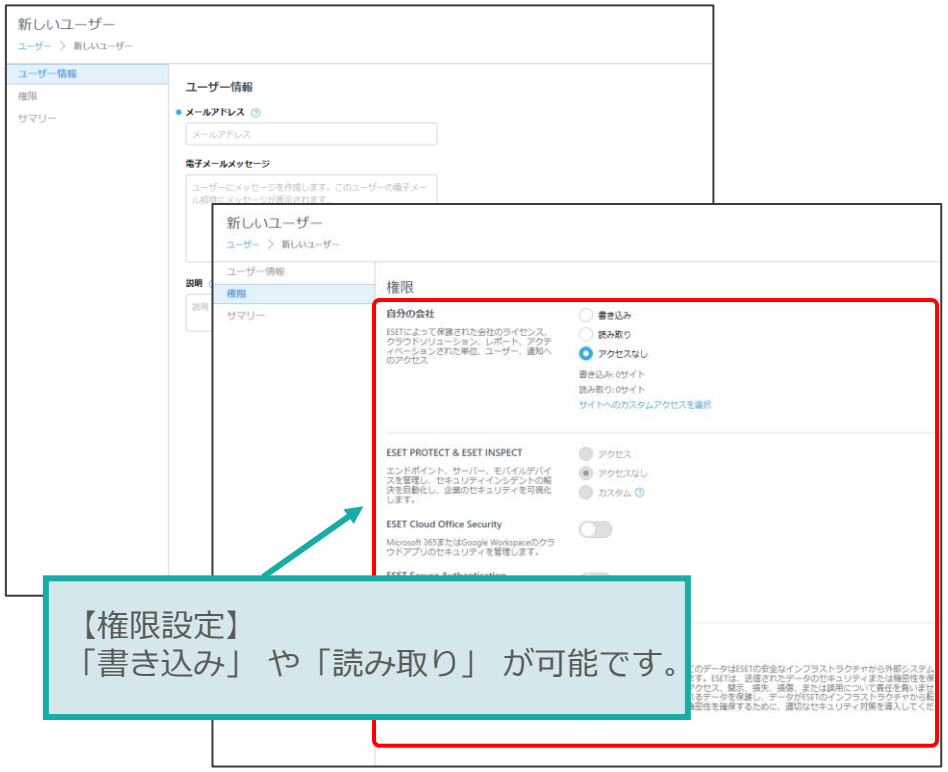


・読み取り　：設定などの閲覧は可能ですが変更は行えません。
・使用　　：設定などを使用することは可能ですが修正または削除は行えません。
・書き込み　：設定の変更やタスクの実行を行うことができます。

Ⅷ-Ⅰ.ユーザー管理

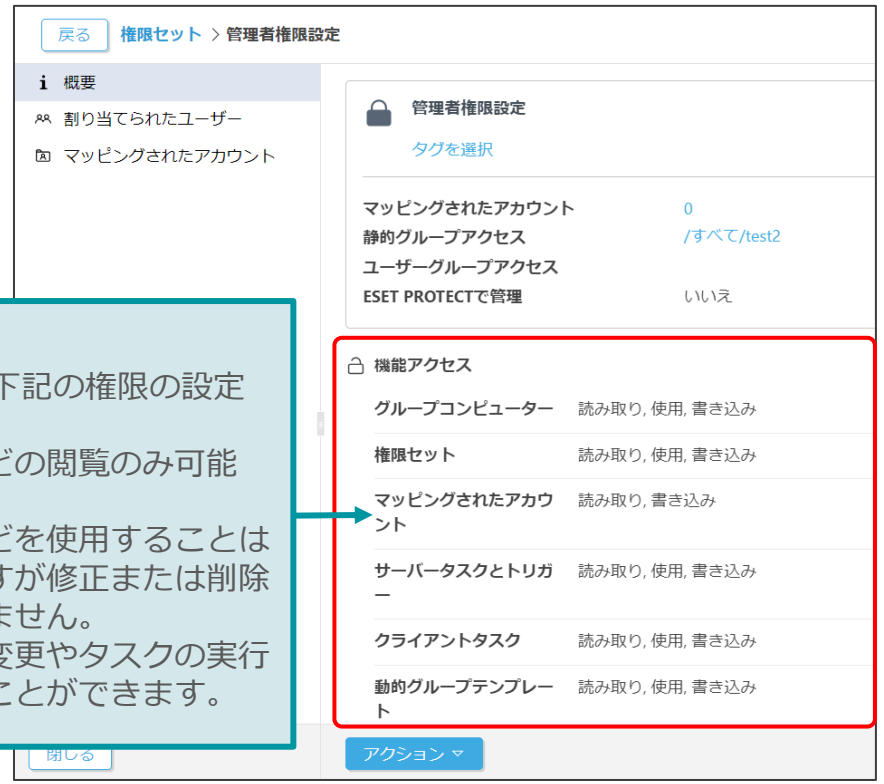
各ユーザーには、所属する静的グループと権限設定を割り当てます。アクセス権には既定で全ての機能が実行できる「管理者権限設定」に加えて、設定の表示は行えるが変更は行えない「レビューア権限設定」などがあります。※ESET PROTECT HUB（EPH）で作成したユーザーに対し、EPで詳細な権限設定を行います。

EPHのユーザー作成画面



【権限設定】
「書き込み」 や「読み取り」 が可能です。

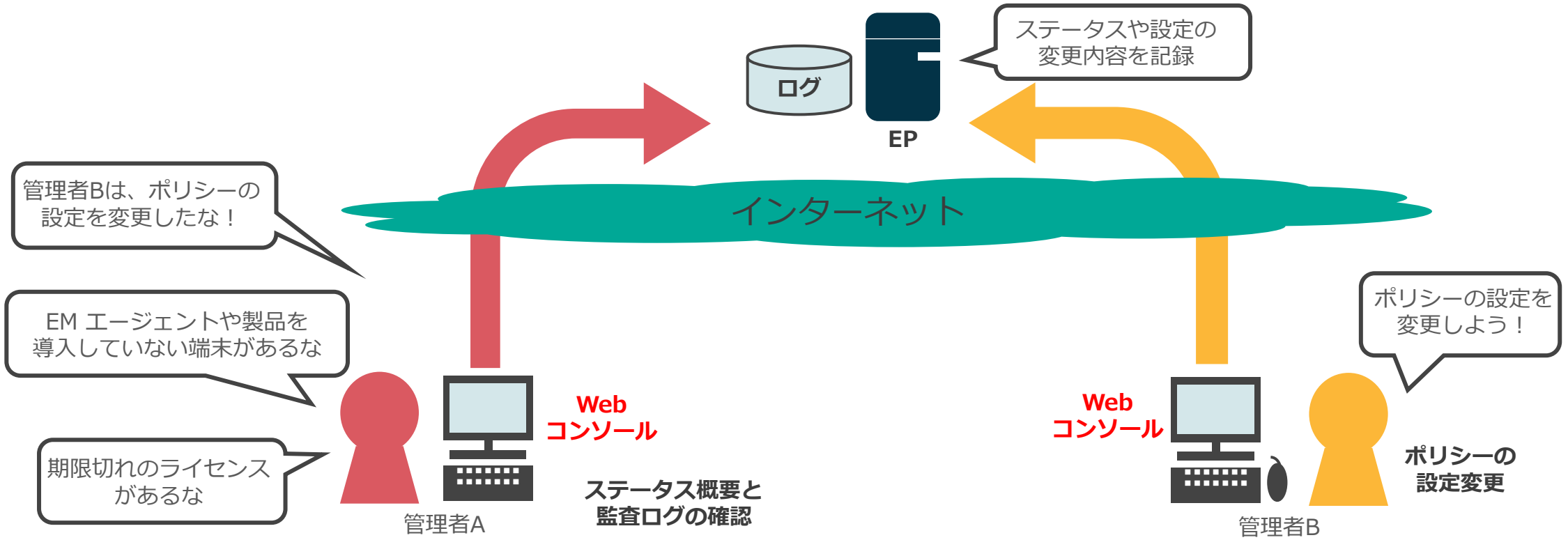
権限設定画面



【機能アクセス】
EPの各機能に対して下記の権限の設定が可能です。
・読み取り：設定などの閲覧のみ可能です。
・使用　　：設定などを使用することは可能ですが修正または削除は行えません。
・書き込み：設定の変更やタスクの実行を行うことができます。

Ⅶ-Ⅱ. 監視・監査

「ステータス概要」では、EPの統計的な使用情報やステータスを表示します。また「監査レポート」を利用すると、ログインユーザーが行った操作内容を記録します。これらにより、EP上の問題をただちに発見でき、管理者は「いつ」「だれが」「なにを」「どのように」設定を変更したか確認することができます。



Ⅶ-Ⅱ. 監視・監査

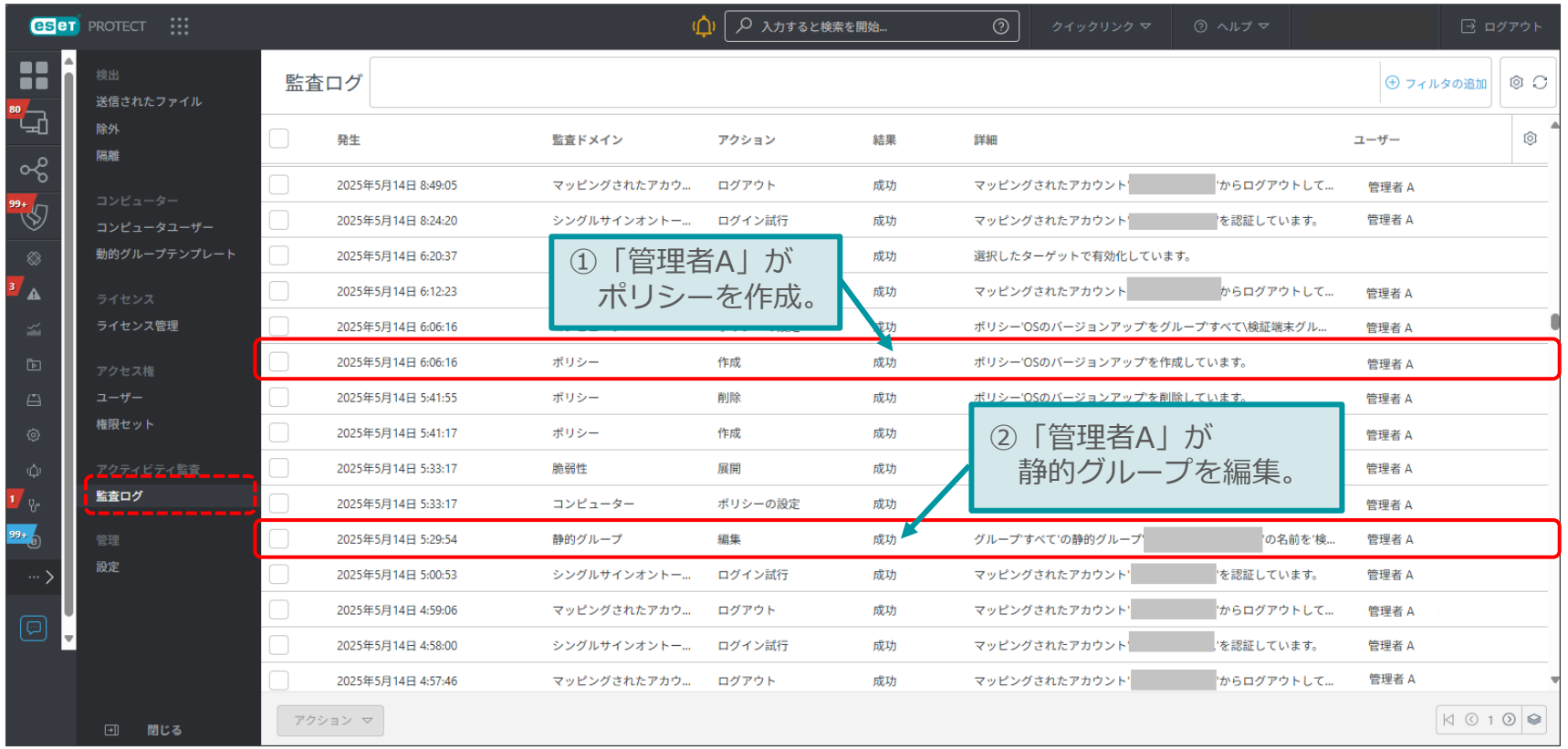
ステータス概要では、EPに関する詳細なステータスを確認できます。
各セクションタイルは、項目の状態に応じて色別でステータスを表示します。

ステータス概要画面

Ⅶ-Ⅱ. 監視・監査

監査ログはレポートまたはダッシュボードより閲覧することができます。
監査ログは、「発生時刻」「アクション」「アクションの詳細」「結果」「ユーザー名」「ポリシーの変更箇所」などを確認することができます。

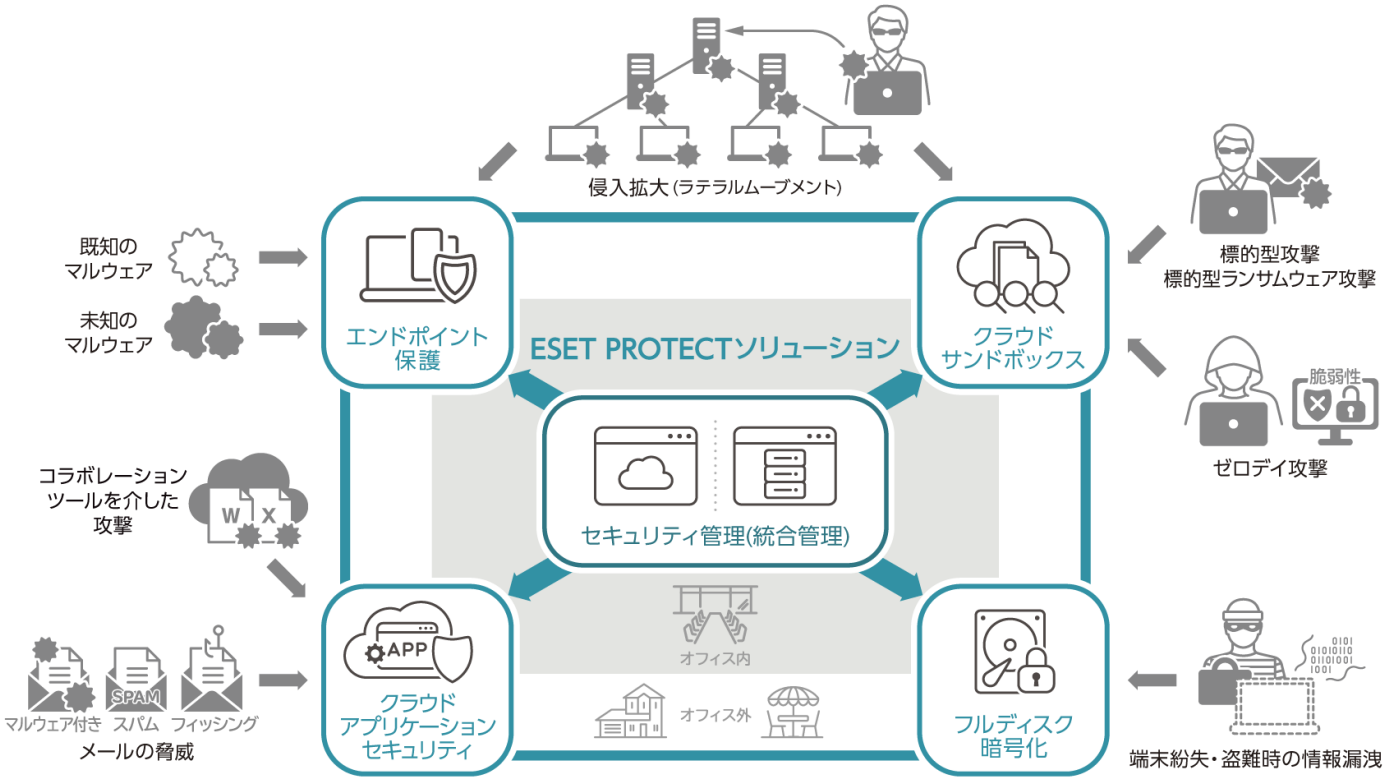
監査ログ画面



Ⅷ. 各ソリューションの統合管理機能のご紹介

Ⅷ. 各ソリューションの統合管理機能のご紹介

ESET PROTECTソリューションは、マルウェア対策などの基本的な対策に加え、クラウドサンドボックス、デバイス紛失・盗難時の情報漏洩対策、Microsoft 365向け対策など、保護する対象や規模のニーズに合わせて多重防御を行い、包括的にエンドポイントを守ります。クラウド型セキュリティ管理ツールである「ESET PROTECT」は、エンドポイント保護だけではなく、クラウドサンドボックスとフルディスク暗号化の統合管理を行うことができる管理ツールです。
※クラウドアプリケーションセキュリティ「ESET Cloud Office Security」は、専用の管理コンソールが用意されています。

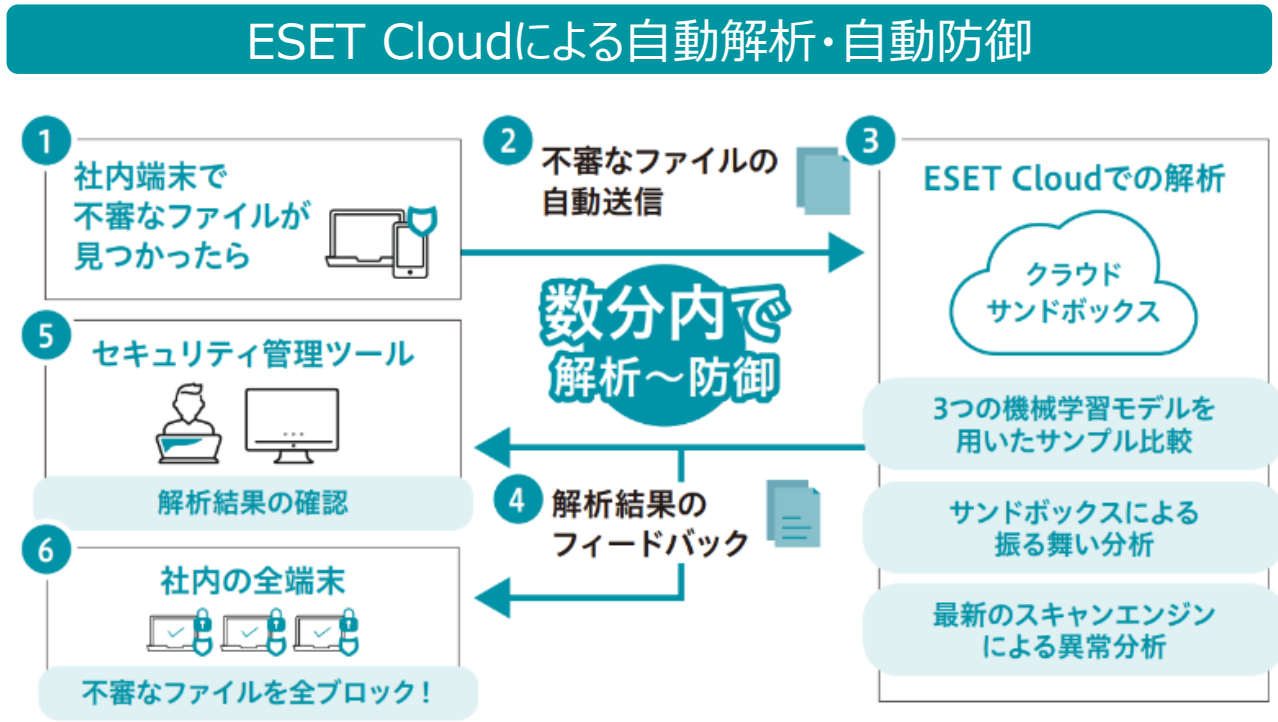


ESET PROTECTソリューション概要図

Ⅷ-Ⅰ. ESET LiveGuard Advanced

クラウドサンドボックスの機能

ESET LiveGuard Advancedは、未知の脅威に対する検出力・防御力をさらに高めるクラウドサンドボックスです。検出から解析、防御までの処理をすべて自動で行います。ゼロデイ攻撃に用いられるような未知の高度なマルウェアに対する検出・防御の即時性を高め、また、ユーザーは端末へ新規プログラムをインストールをする必要がなく、手軽に多層防御の強化を行うことが可能です。



Ⅷ-Ⅰ. ESET LiveGuard Advanced

①未知の脅威を自動解析、自動防御

不審なサンプルをクラウドベースの解析環境「ESET Cloud」へ自動で送信、大半のサンプルは数分内で解析でき、悪質と判断したファイルは全社レベルで自動的にブロックします。

②最新テクノロジーによる解析

「ESET Cloud」での分析には、3つの機械学習モデルを用いたサンプル比較、サンドボックスによるシミュレーション、最新の検出エンジンによる異常分析など、ESETの最新テクノロジーが用いられています。

③プロアクティブ保護機能により解析完了まで不審なファイルの実行をブロック

不審なファイルを「ESET Cloud」で分析している間はプロアクティブ保護によってファイルの実行がブロックされ、万が一の感染リスクを低減できます。

④解析結果のレポート

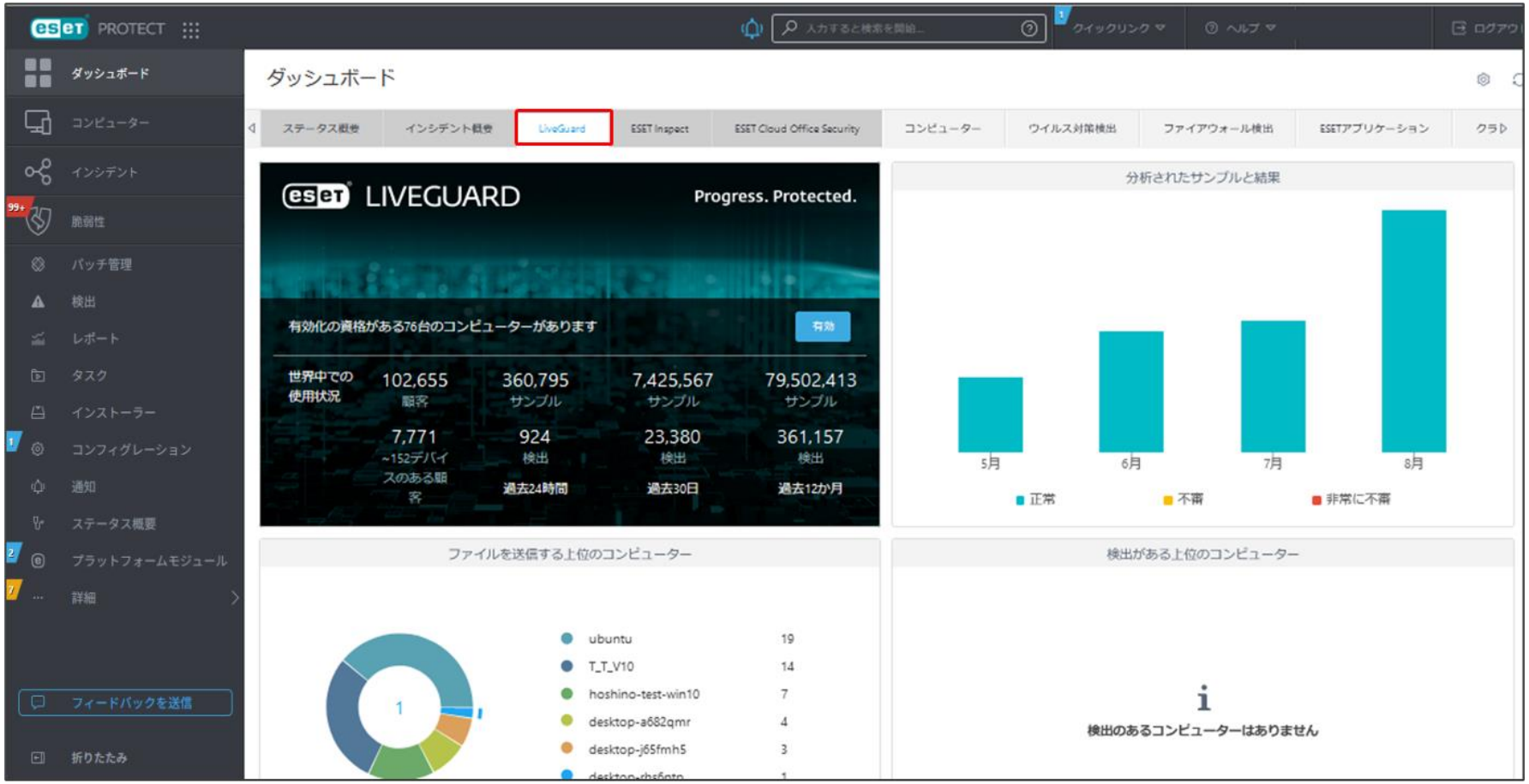
サンプルの解析結果は「ESET PROTECT」より閲覧可能です。

悪質なものであるかどうかの判断や、サンドボックスシミュレーションで観察された挙動などを把握できます。

Ⅷ-Ⅰ. ESET LiveGuard Advanced

世界でのELGAによる検知状況確認

EPのダッシュボードでは、ELGAを使用した世界中での検知状況を確認することができます。

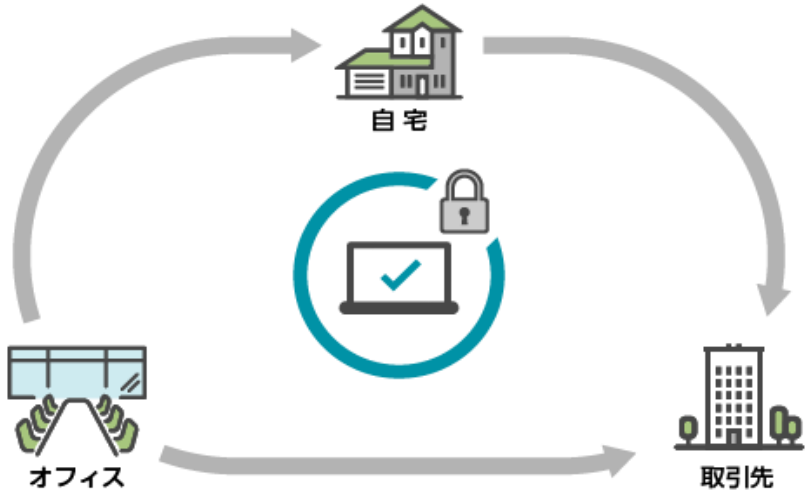


Ⅷ-Ⅱ. ESET Full Disk Encryption

フルディスク暗号化プログラムの機能

ESET Full Disk Encryptionは、リモート勤務や社内で利用するクライアントPCのディスク全体、またはブートディスク（※）を暗号化するディスク暗号化ソフトウェアです。暗号化実施後、クライアント端末にはプリブート認証が付与されるため、端末の紛失・盗難時の情報漏洩対策を行うことができます。また、EPを使用して、各クライアント端末の暗号化状況の確認や復号、プリブート認証パスワードの回復などを行うことができます。

持ち出し端末の情報漏洩対策



EPによる一括管理

※ブートディスク…Windowsのブートドライブとして使用される物理ディスクです。同一ディスク内にWindowsのブートドライブとその他のドライブが存在する場合は、そのディスク全体が暗号化されます。

Ⅷ-Ⅱ. ESET Full Disk Encryption

①ESET Full Disk Encryptionの強固な暗号化

EFDEはAES256を使用したソフトウェアでの暗号化、または、OPAL2.0準拠の自己暗号化ドライブを使用したハードウェアでの暗号化が可能なため、高い暗号化強度を実現しています。さらに、暗号化キー保護に対するセキュリティ強化として、Trusted Platform Module 2.0（TPM2.0）の使用も可能です。

②ESET PROTECTを使用した一元管理

EFDEはESET PROTECTソリューションシリーズによるウイルス・スパイウェア対策プログラムと同一のセキュリティ管理ツールで一元管理が可能です。EFDEの展開や暗号化状況の確認だけではなく、ポリシーやタスク、レポート機能を使用した柔軟な管理が可能です。

③ESET PROTECTを使用したリカバリー対応

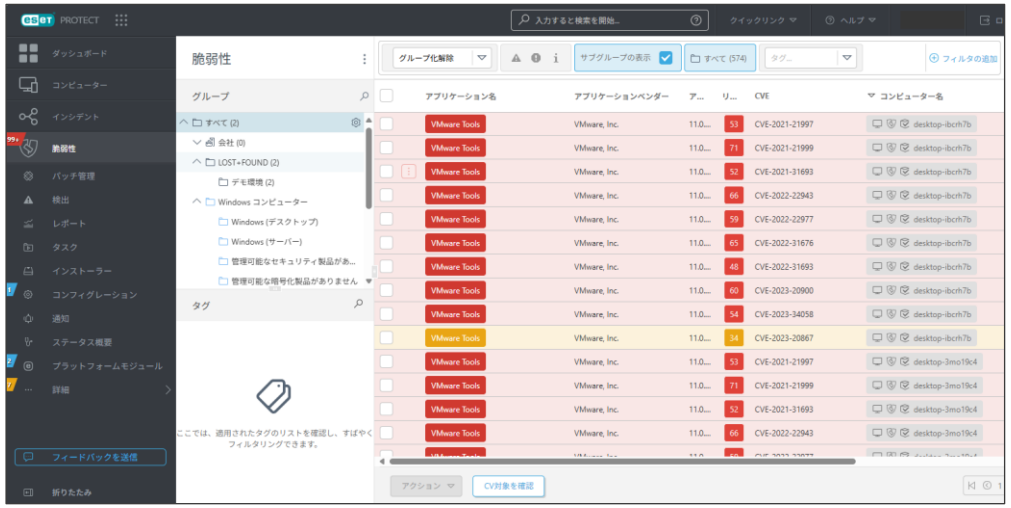
ユーザーがEFDEのプリブート認証パスワードを忘れてしまった場合や、Windowsが起動しなくなった場合は、EPを使用した迅速なプリブート認証パスワードの回復や、EPで作成したリカバリーデータを元に用意した復号USBドライブを使用することで、ディスクの復号を行うことができます。

Ⅷ-Ⅲ. ESET Vulnerability & Patch Management

脆弱性とパッチ管理の機能

ESET Vulnerability & Patch Managementは、OSとアプリケーションの脆弱性※1とパッチ※2の適用状況を管理するソリューションです。古いオペレーティングシステムやアプリケーションを狙った脅威からクライアントを守ります。
クライアントの脆弱性情報は重大度（リスクスコア）が付与されるため、重大度の高いものから脆弱性対応するといった運用ができます。
また、パッチ管理につきましては手動またはスケジューリングして自動で適用させることもできます。

EPによる脆弱性とパッチの一括管理



- ESET Vulnerability & Patch Management の主な機能

  - クライアントの情報を自動で収集
  - 自動および手動でのパッチ適用
  - 脆弱性の重大度のレベルづけ
  - 対象のクライアントのリストの表示　　など

※1　脆弱性… コンピュータ関連のプログラムに潜む欠点や盲点、弱点のことで、「セキュリティ・ホール」とも呼ばれます。
※2　パッチ… OSやソフトウェアに存在する脆弱性やバグを修正するプログラムを指します。「修正プログラム」「更新プログラム」「アップデート」などと呼ばれることもあります。

Ⅷ-Ⅲ. ESET Vulnerability & Patch Management

①組織全体の状況の可視化

組織全体の脆弱性やパッチの適用状況を可視化します。

可視化することにより、組織全体の一元管理を行うことができ、管理者の脆弱性とパッチ管理の負担を軽減することができます。

②脆弱性のリスクレベルによる対応の優先順位づけ

Adobe Acrobat、Mozilla Firefox、Zoom Client などの数百ものアプリケーションをスキャンすることにより、35,000を超える一般的な脆弱性とCVE※を検出します。

検出した脆弱性はリスクレベルが付与され、リスクレベルを参考に対応する脆弱性の優先順位づけを行うことができます。

※CVE…脆弱性のデータベースのことを指し。共通脆弱性識別子とも呼ばれます。

③パッチの手動または自動での適用

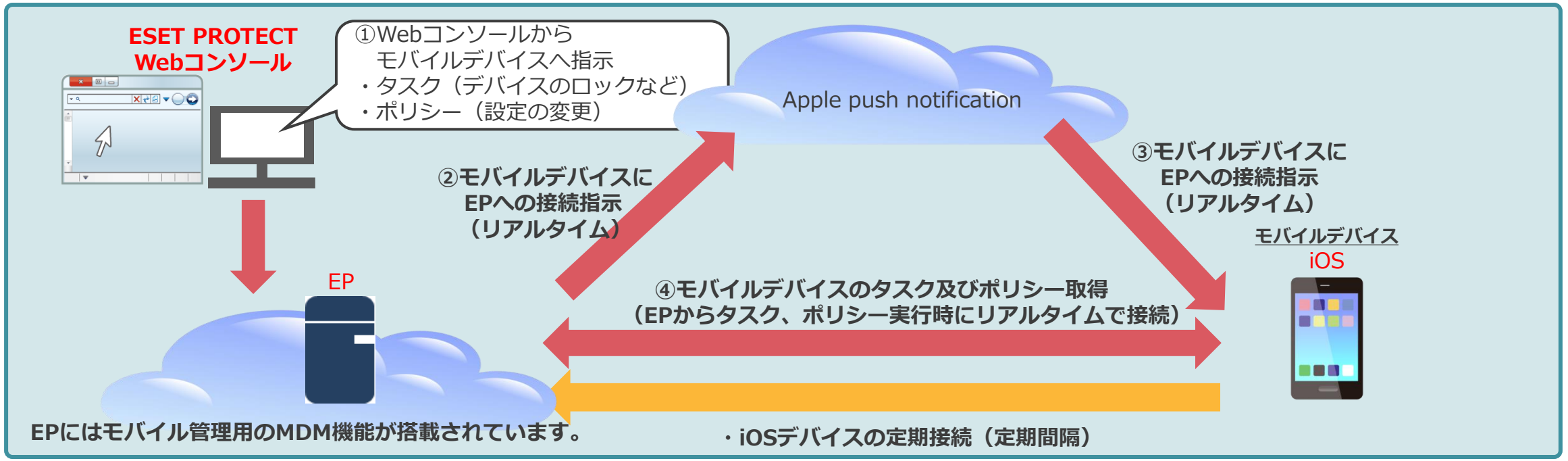
パッチは手動または自動で適用することができます。

パッチの自動適用はアプリケーション毎に個別に設定することができ、パッチの自動適用するタイミングをスケジュールすることもできます。

Ⅸ. モバイルデバイス管理機能（iOSデバイスの管理）

Ⅸ. モバイルデバイス管理機能（iOSデバイスの管理）

EPではiOSデバイスを管理することができます。EPにiOSデバイスの登録、iOSデバイスにプロファイルをインストールすることでiOSデバイスを管理することができます。標準またはABM（※）登録モードで登録が可能です。iOSの管理ではEPからiOSデバイスへタスクを実行することで、iOSデバイス情報の取得、 iOSデバイスを紛失した場合にデバイスのロックなどのアンチセフトを行うことができます。また、ポリシー機能を使用することでEPからiOSデバイスの設定変更やアプリケーションの制御を行うことができます。



※ABM（Apple Business Manager）…Apple Inc.が法人向けに提供しているMDMによるモバイル管理をサポートするサービスです。

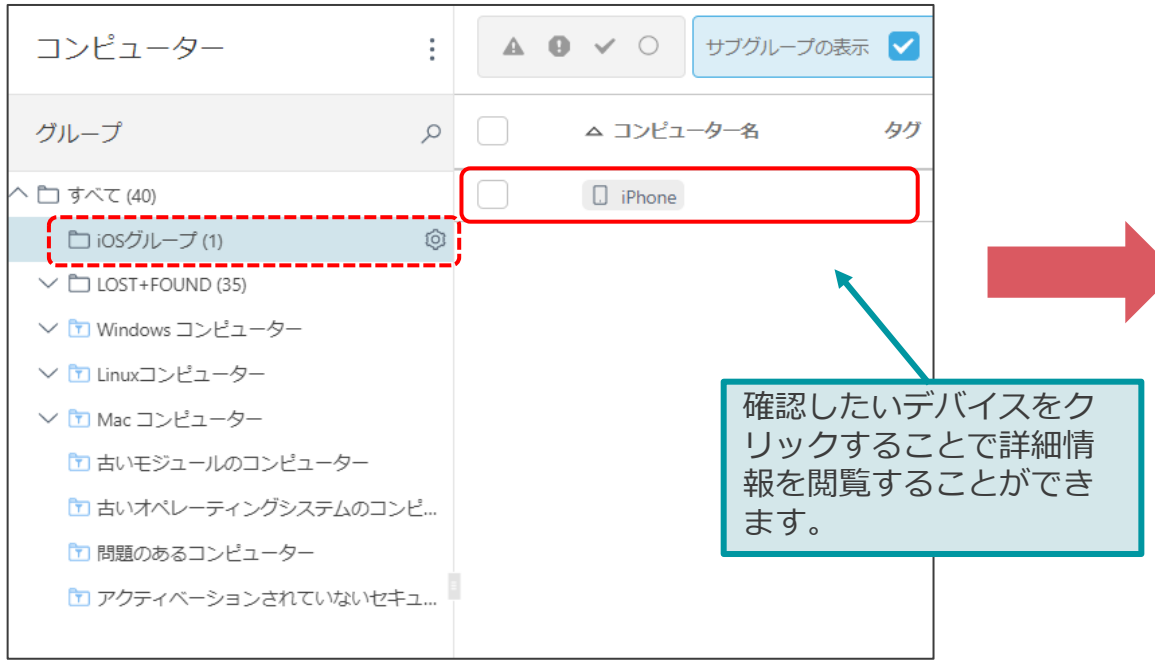
Ⅸ. モバイルデバイス管理機能（iOSデバイスの管理）

EPのコンピューター一覧よりiOSデバイスの一覧および、デバイスの詳細情報を確認することができます。詳細情報ではiOSデバイスの以下情報が確認できます。

・メーカー　・モデル　・OS情報　・IMEI

iOSデバイス情報の閲覧

コンピューター - 一覧画面



コンピューター - 詳細画面

Ⅸ. モバイルデバイス管理機能（iOSデバイスの管理）

EPからiOSデバイスに以下のタスクを配信することができます。アンチセフトアクションを使用することで、iOSデバイスを紛失した場合にEPから、iOSデバイスのロックやワイプをさせることができます。

iOSに実行可能なタスク

タスク名	説明
ESET製品の設定のエクスポート	iOSに適用されたポリシーをエクスポートしてEPで表示します。
アンチセフトアクション	iOSでは以下のアクションが行えます。 ・紛失モードをオンにして検索※ ・ロストモードのオフ※ ・検索※ ・警報/紛失モードサウンド※ ・ロック ・パスコードをクリア ・初期設定リセット ※ABM登録モードで管理の場合のみ
製品のアクティベーション	アクティベーションを実行します。
管理の停止	アクティベーションを解除して、iOS端末の管理を停止します。

タスク設定画面（アンチセフトアクション）

Ⅸ. モバイルデバイス管理機能（iOSデバイスの管理）

EPからiOSデバイスのポリシーで管理できる項目は以下の通りです。
iOSデバイスに対して設定の変更や、デバイス、アプリケーションの使用を制限することができます。

iOSの管理機能

項目	詳細
パスコード	パスワード文字ルール、変更日数、ロック時間、失敗回数など
デバイス機能	アプリインストール、カメラ使用、FaceTime使用、Siri使用、ロック画面の表示内容、スクリーンショット使用、アプリ内購入など
AIRPRINT	AirPrintの使用の許可、AirPrintの資格情報の保存などのAirPrintに関する制御
ICLOUD	バックアップ、データ同期、写真共有などの使用制限など
セキュリティとプライバシー	診断データの送信、証明書、ドキュメント、TouchIDデバイスロックなどの使用制限
アプリケーション	iTunes Store、ゲーム、Safari、メディア再生などの使用制限
アップデート	ソフトウェアアップデートを延期に関する設定など
その他	証明書、プロキシ、アクセスポイント、Wi-Fi、VPN、各アカウントなどの設定

ポリシー - 設定画面
（ESET MDM for iOS/iPadOS）

X. オンプレミス型セキュリティ管理ツールとの主な違い

X. オンプレミス型セキュリティ管理ツールとの主な違い

オンプレミス型セキュリティ管理ツールである「ESET PROTECT on-prem」と本資料でご紹介の「ESET PROTECT」の主な違いは以下になります。

	ESET PROTECT	ESET PROTECT on-prem	備考
管理可能なデバイス数	50,000クライアントまで	ハードウェアスペック構成次第	
ESET Inspectとの連携	可能	可能	
Active Directoryとの連携	可能 ※1	可能	※1 別途ツールを利用します ユーザー同期は利用できません
エージェントの接続間隔	10分	任意	
製品パッケージ型のインストーラー	ライブインストーラー	オールインワンインストーラー	インストーラーの違いについては次ページを参照
サーバーへのレポートの保存	不可	可能	
通知機能	可能 ※2	可能 ※3	※2 電子メール、Webhookによる通知が可能 ※3 電子メール、Syslogへの送信、SNMPトラップによる通知が可能

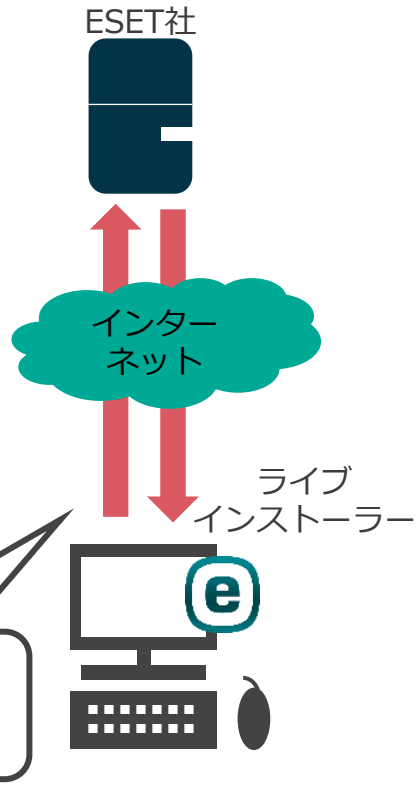
X.（参考） 製品パッケージ型インストーラーの違い

製品パッケージ型インストーラーの「ライブインストーラー」と「オールインワンインストーラー」には以下のような違いがあります。

ライブインストーラー

ライブインストーラーを実行すると、ESET社と通信を行い、インストールに必要なウイルス・スパイウェア対策プログラム 本体とEMエージェントをダウンロードします。

インターネット接続	必須
インストーラーのサイズ	約12MB
対応OS	Windows Mac



オールインワンインストーラー

オールインワンインストーラーはESETプログラム本体とEMエージェントがパッケージ化されたインストーラーです。ESET社と通信することなく、EMエージェントとESET製品をインストールすることができます。

※製品認証キーでのアクティベーションにはインターネット接続が必要です。

インターネット接続	任意
インストーラーのサイズ	約250MB
対応OS	Windows