オンプレミス型セキュリティ管理ツール
ESET PROTECT V10
機能紹介資料

第13版

2024年1月4日

Canon

キヤノンマーケティングジャパン株式会社

もくじ

1. はじめに(本資料について)

・本資料はオンプレミス型セキュリティ管理ツール(ESET PROTECT V10)の機能を紹介している資料です。

種別	新プログラム名(V8/9/10)	旧プログラム名(V7)
オンプレミス型セキュリティ管理ツール	ESET PROTECT(Windows版)	ESET Security Management Center(Windows版)
	ESET PROTECT(Linux版)	ESET Security Management Center(Linux版)

・本資料で使用している画面イメージは使用するOS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あります。

・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。

・ESET File Security for Linuxは、V8よりESET Server Security for Linuxに名称が変更になりました。

・ESET Dynamic Threat Defenseは、ESET LiveGuard Advancedに名称が変更になりました。

2. ESET PROTECT(EP)とは

2. ESET PROTECT(EP)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をネットワーク経由で統合管理するプログラムです。Windows、Mac OS X、Linux向けプログラムを管理できます。

ESET PROTECT V10 で管理可能なプログラム(2024年1月時点)

管理可能なプログラム	種別	バージョン
ESET Endpoint Security	Windows クライアントOS向け総合セキュリティプログラム	11.X /10.X /9.1/8.1
ESET Endpoint アンチウイルス	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	11.X /10.X /9.1/8.1
ESET Server Security for Microsoft Windows Server	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	10.X /9.0/8.0/7.3
ESET Endpoint Security for OS X	Mac クライアントOS向け総合セキュリティプログラム	6.11
ESET Endpoint アンチウイルス for OS X	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	7.4 / 6.11
ESET Endpoint アンチウイルス for Linux	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	10.X / 9.X / 8.1
ESET Server Security for Linux	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	10.X /9.X/ 8.1/7.2
ESET Endpoint Security for Android(※2)	Android OS向け総合セキュリティプログラム	3.3以降 / 4.X

※セキュリティ管理ツールのバージョンによって管理できるクライアント用プログラムに差異があります。詳細は以下サポートページをご参照ください。
https://eset-support.canon-its.jp/faq/show/143?site_domain=business

2. ESET PROTECT(EP)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をネットワーク経由で統合管理することができます。EPは主に以下の３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
- インストーラー
- グループ
- 通知
- ポリシー
- タスク

サーバー運用管理機能
- ユーザー管理
- 監視・監査

5.ログ監視機能のご紹介を参照

6.クライアント管理機能のご紹介を参照

7.サーバー運用管理機能のご紹介を参照

3. ESET PROTECTの構成

3. 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。

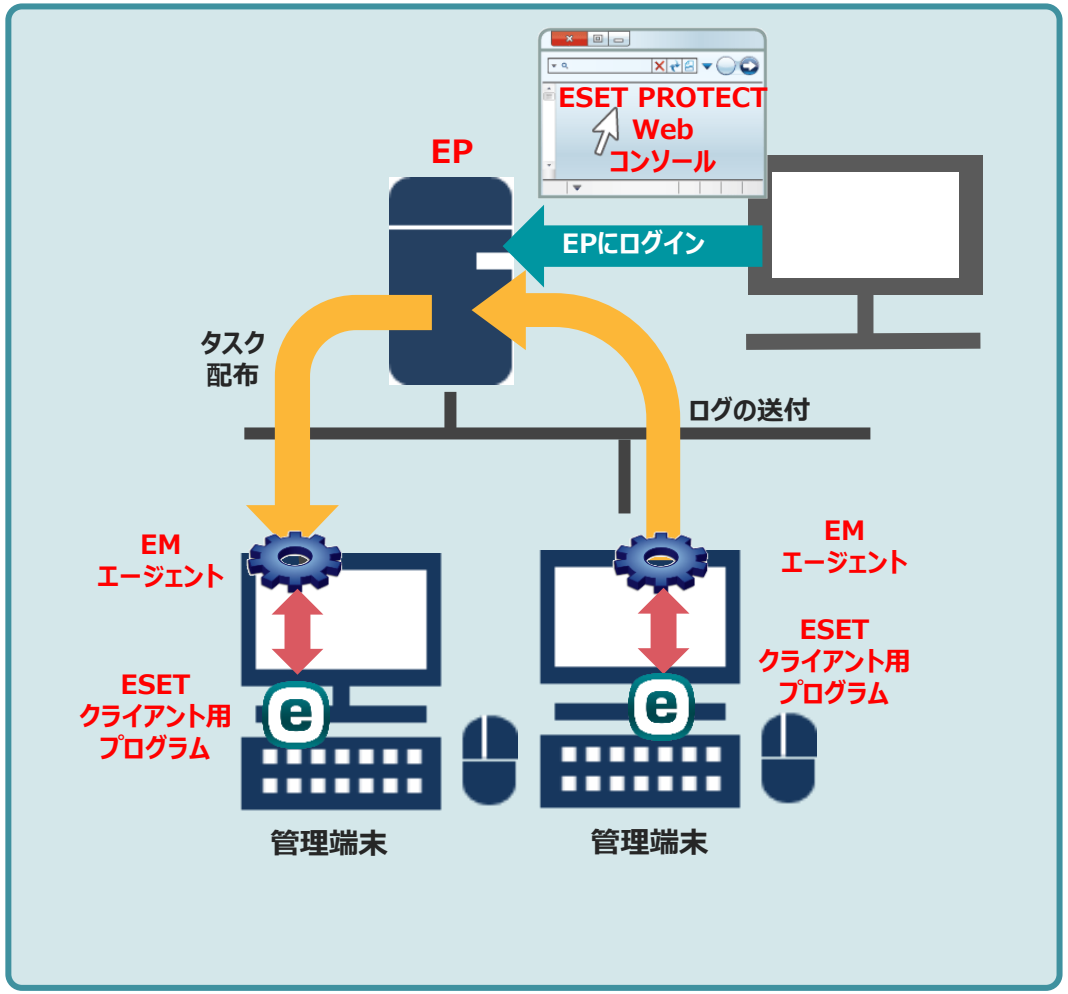
ESET PROTECT Webコンソール

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EPの設定変更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)

EMエージェントは、クライアントから情報を収集し一定の間隔毎で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エージェントへ送信されたのち、EMエージェントがクライアントへ送信します。また、EMエージェントは自動アップグレードに対応しています。

※ 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。



3. ESET PROTECTの構成

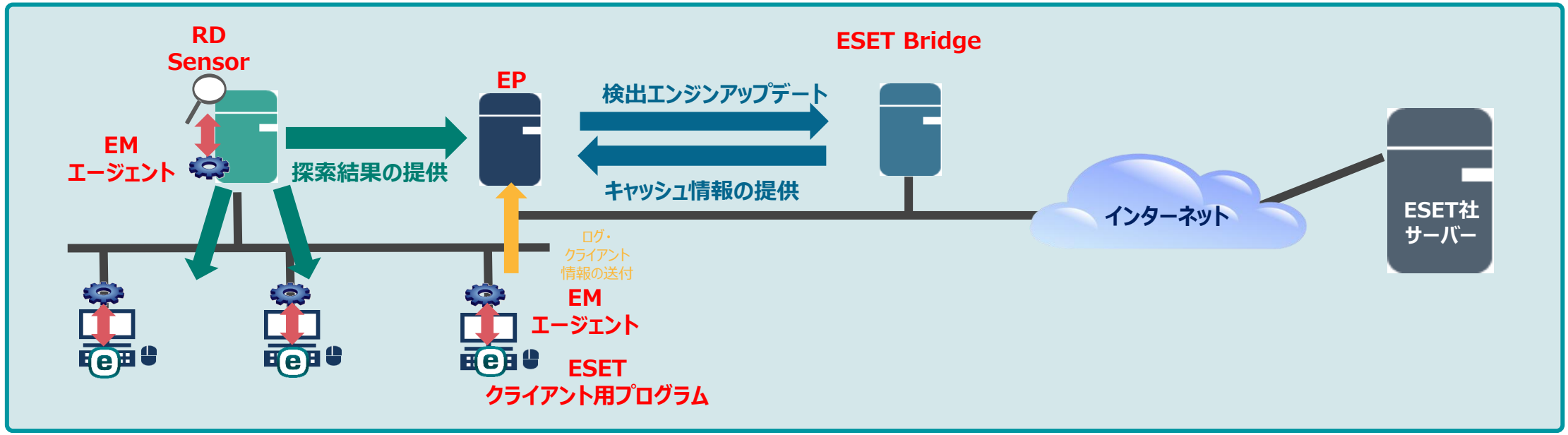
以下のコンポーネントは任意で構成します。

Rogue Detection Sensor(RD Sensor)

RD Sensorはネットワーク上のコンピューターを探索し、EPに追加するツールです。追加したコンピューターに対してEPよりEM エージェントの展開ができます。なお本機能はEPに含めることができます。

ESET Bridge

ESET Bridgeはクライアントに検出エンジンなどのアップデート配布に利用するプロキシです。ESET Bridgeのプロキシを利用すると検出エンジンやアクティベーションなど、ESETの通信をキャッシュすることで、ネットワーク通信トラフィックを軽減することができます。



3. ESET PROTECTの構成 (動作要件：利用可能なデータベース)

利用可能なデータベースは以下の通りです。Microsoft SQL Serverは2014、2016、2017、2019の利用が可能です。エディションの指定はございません。以下には主要なエディションを記載しています。

利用可能なデータベース

プログラム	利用可能なデータベース	データベースの最大サイズ
EP V10 (Windows版)	Microsoft SQL Server 2014 Standard Edition	制限なし
	Microsoft SQL Server 2014 Express Edition(既定)※1	10GBまで
	Microsoft SQL Server 2016 Standard Edition	制限なし
	Microsoft SQL Server 2016 Express Edition	10GBまで
	Microsoft SQL Server 2017 Standard Edition	制限なし
	Microsoft SQL Server 2017 Express Edition	10GBまで
	Microsoft SQL Server 2019 Standard Edition	制限なし
	Microsoft SQL Server 2019 Express Edition(既定)※2	10GBまで
	Microsoft SQL Server 2022 Standard Edition	制限なし
	Microsoft SQL Server 2022 Express Edition	10GBまで
EP V10 (Linux版)	MySQL(※3) 5.6、5.7、8.0	制限なし

※1　Windows Server 2012/2012 R2の場合
※2　Windows Server 2016/2019/2022の場合
※3　Windows ServerでもMySQLの利用は可能です。Microsoft SQL Serverではドメインコントローラーを同居させることはできないため、ドメインコントローラーにEPを構築する場合はMySQLの利用をお願いいたします。

3. ESET PROTECTの構成 (動作要件：サポートOS)

インストール可能なサポートOSは以下の通りです。Windows版またはLinux版の以下OSでご利用いただくことが可能です。

EPのサポートOS

プログラム	オペレーティングシステム名
EP V10 (Windows版)	Windows Server 2012 Standard (64bit)
	Windows Server 2012 R2 Standard (64bit)
	Windows Server 2016 Standard (64bit) / Datacenter (64bit)
	Windows Server 2019 Standard (64bit) / Datacenter (64bit)
	Windows Server 2022 Standard (64bit) / Datacenter (64bit)
EP V10 (Linux版)	Red Hat Enterprise Linux 7 (64bit)
	CentOS 7 (64bit)

※ ESET BridgeのサポートOSは上表とは異なります。詳細は下記ページをご確認ください。
https://help.eset.com/ebe/2/ja-JP/welcome.html?requirements_and_supported_products.html

4. Webコンソールのご紹介

4-1. 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ログインします。Webベースのインターフェイスのため、EPに接続可能なデバイスのブラウザからいつ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
ログイン画面

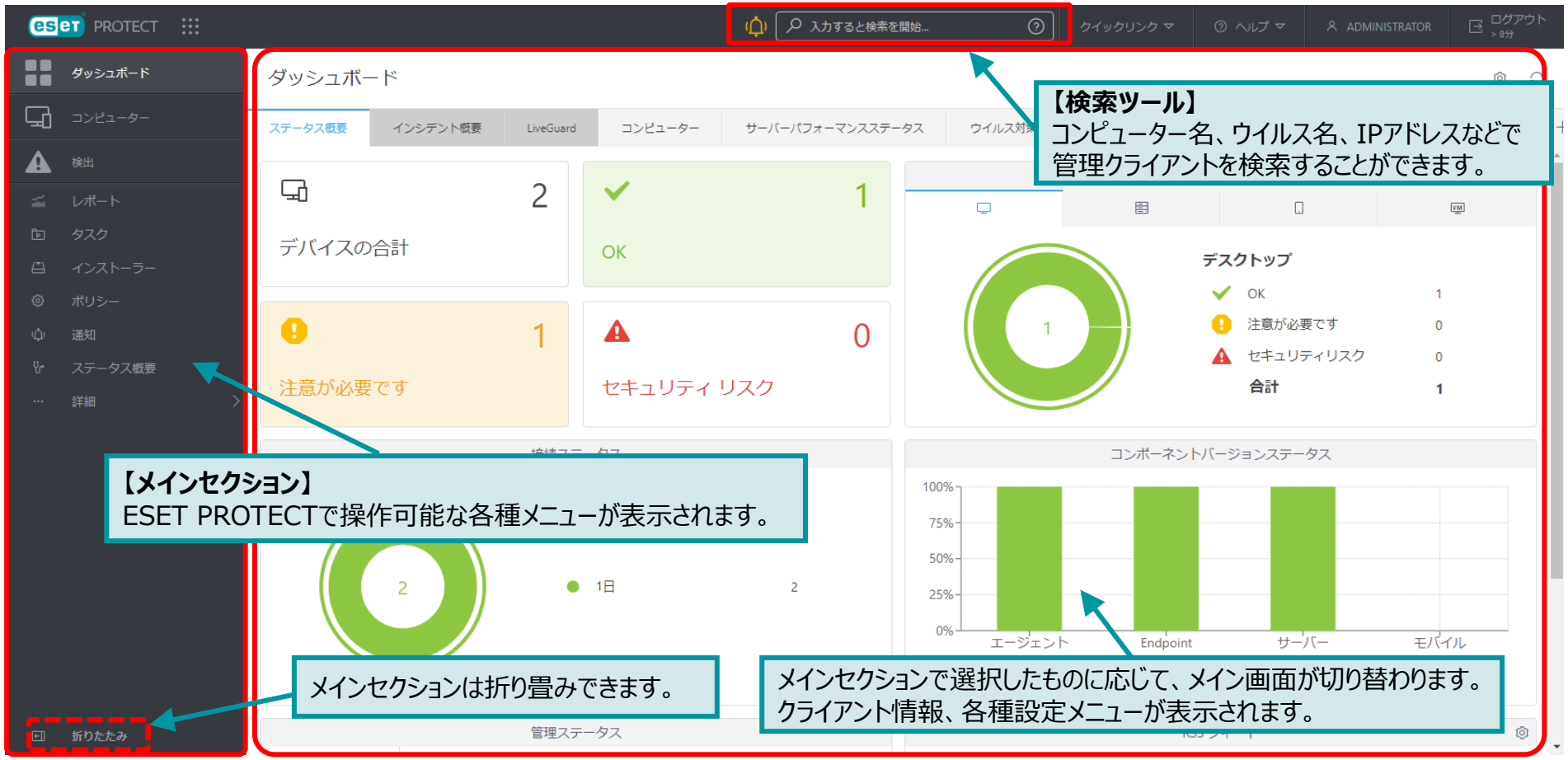
【ログイン画面】
ユーザー名・パスワードを入力して、ログインします。

【マルチ言語対応】
EPの表示言語を選択することができます。
設定やログの中身を選択した言語で表示させることができます。

※ただし日本語で入力した設定やコメントは、英語などを選択してログインしても日本語のまま表示されます。

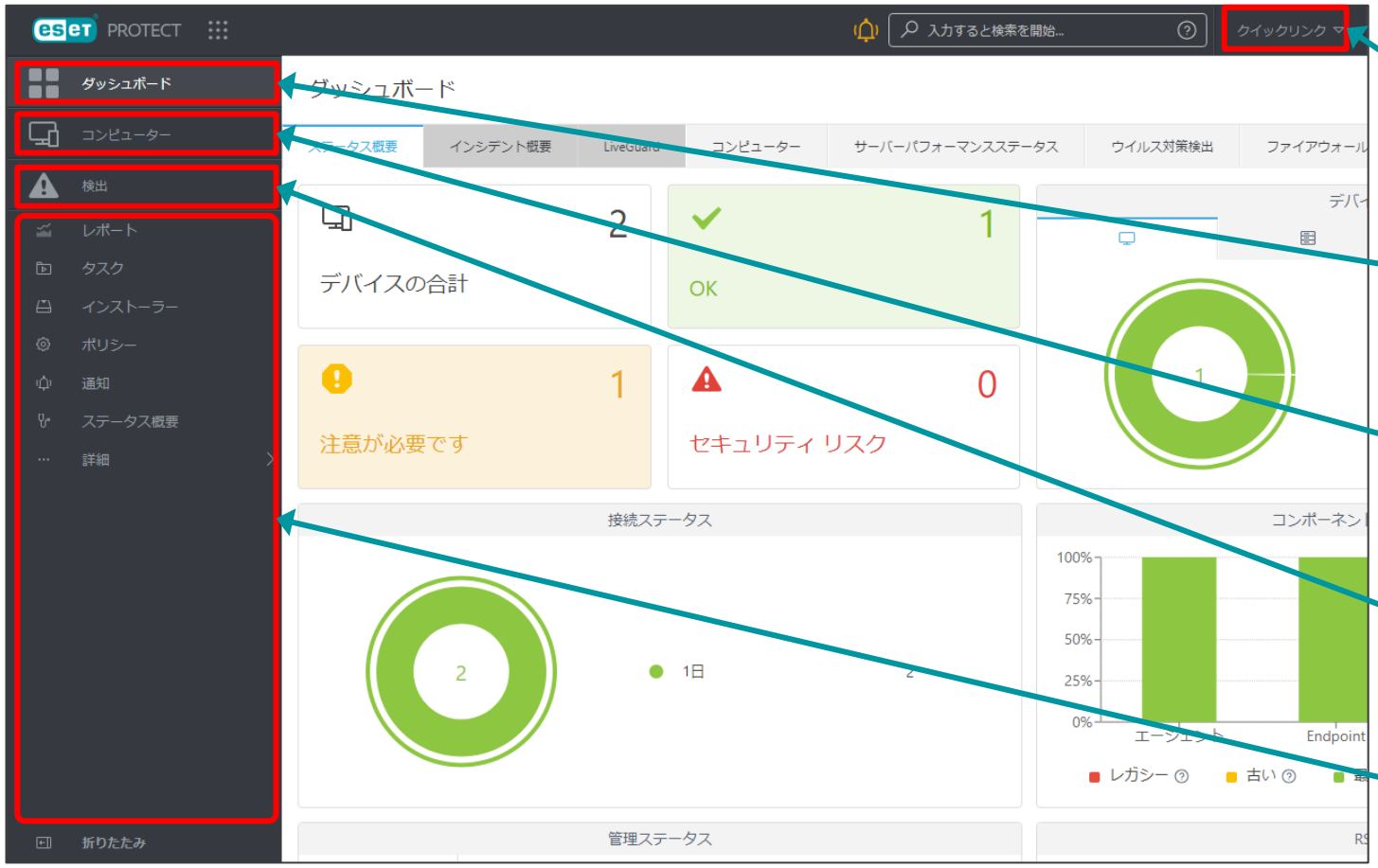
4-2. Webコンソールの画面構成

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、画面左のメインセクションより、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。



4-2. 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セクションでは 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。



【クイックリンク】
よく使用される機能がショートカットとして登録されています。セットアップ・管理・状態に分かれており、すぐに機能を使うことが可能です。

【ダッシュボード】
EPにログインすると最初に表示される画面です。コンピューターや脅威情報、EPのネットワーク情報が表示されます。

【コンピューター】
EPで管理するクライアントの一覧と、クライアントの詳細な情報がグループに分かれて表示されます。

【検出】
EPで管理するクライアントで検出された脅威の概要が表示されます。

EPで円滑にクライアント管理を行うための様々なメニューが集約されています。

4-2. Webコンソールの画面構成 (メインセクション)

メインセクションの後半には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ます。詳細は各機能のご紹介をご確認ください。

【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。

【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。

【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。

【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。

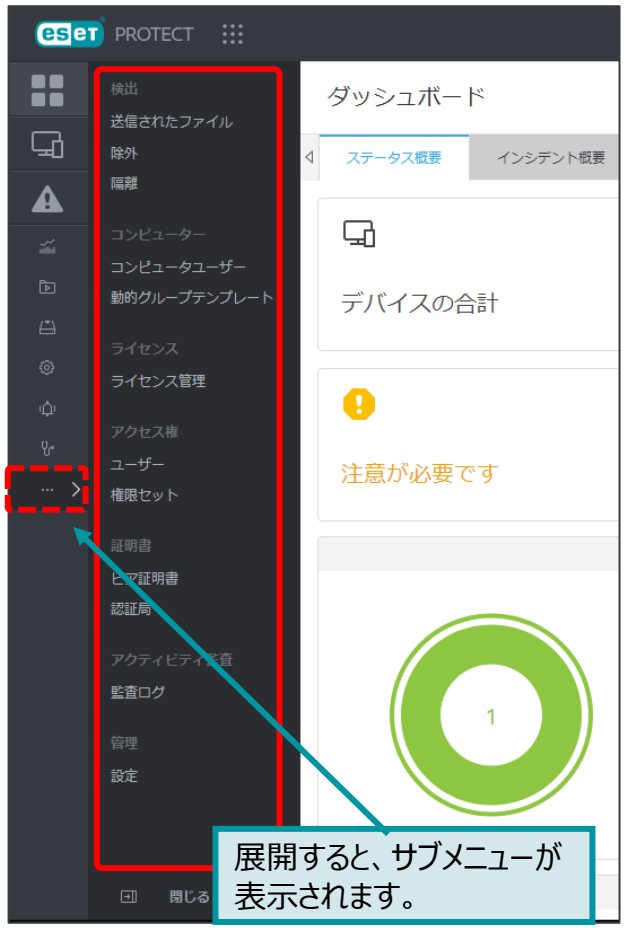
【インストーラー】
EMエージェントを展開するためのインストーラーパッケージを作成できます。

【詳細】
EPに関するさらに詳細なメニューが開きます。

【ポリシー】
クライアントの設定変更や設定の制御に利用します。

4-2. 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おこなうための、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(旧名称：ESET Threat Dynamic Defense)」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 を利用するためには、別途ライセンスを購入・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】
ユーザーとコンピューターの結びつけを行います。

【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】
EPで管理しているライセンスが登録されます。オフライン環境用のライセンスもこちらで管理できます。

【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。

【証明書】
EPの各コンポーネントがEPと通信するために必要なピア証明書の作成や認証局の作成ができます。

【アクティビティ監査】
ログインユーザーがおこなった操作内容を確認します。

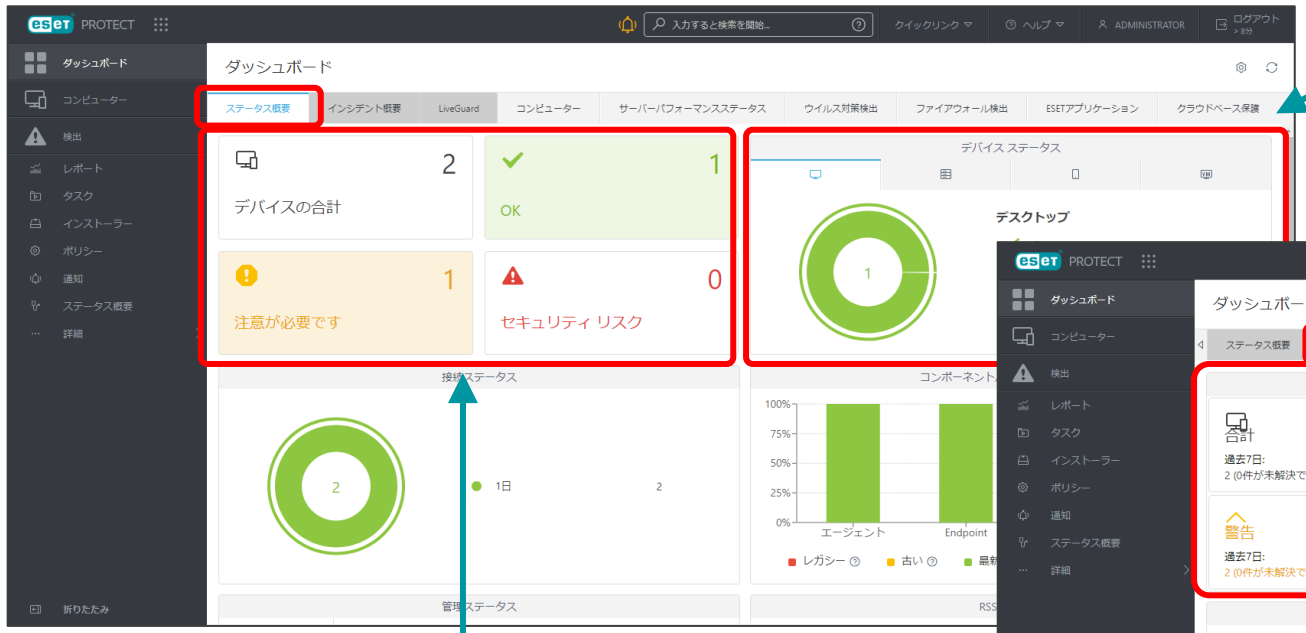
【管理】
EPサーバーのアップデート間隔や、EPサーバー本体の設定ができます。

5. ログ監視機能のご紹介

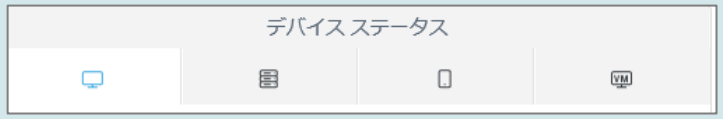
5-1. ダッシュボード

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。「概要」や「インシデント概要」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)



デバイスごとのステータスを表示します。
上部タブを切り替えるとその他デバイスのステータス統計情報も円グラフで確認できます。



正常な端末や注意が必要な端末、問題のある端末を色別でカウントします。

ダッシュボード - インシデント概要(既定テンプレート)

重大な脅威を検出した端末数もすぐさま確認できます。

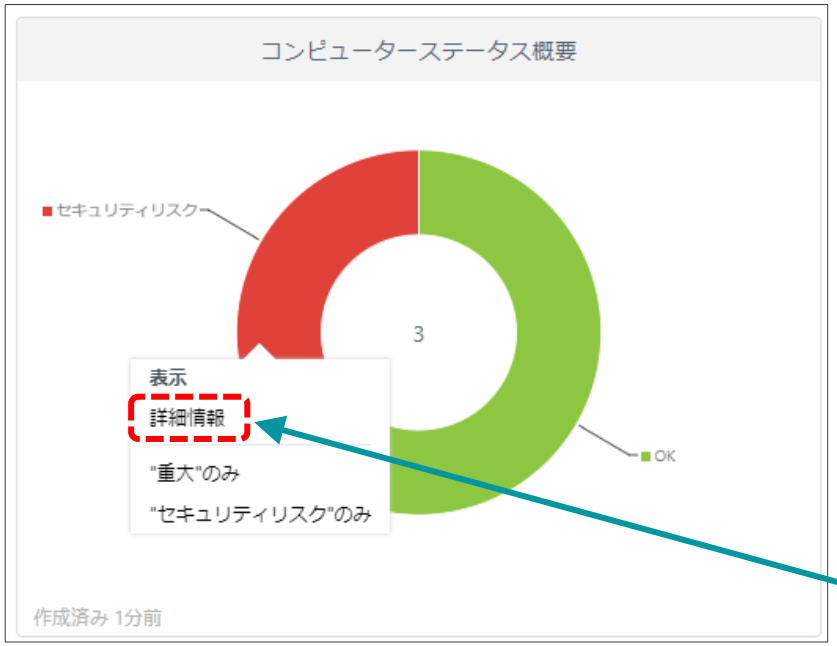
5-1. ダッシュボード

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や、ESET PROTECTのパフォーマンス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)

5-1. 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。

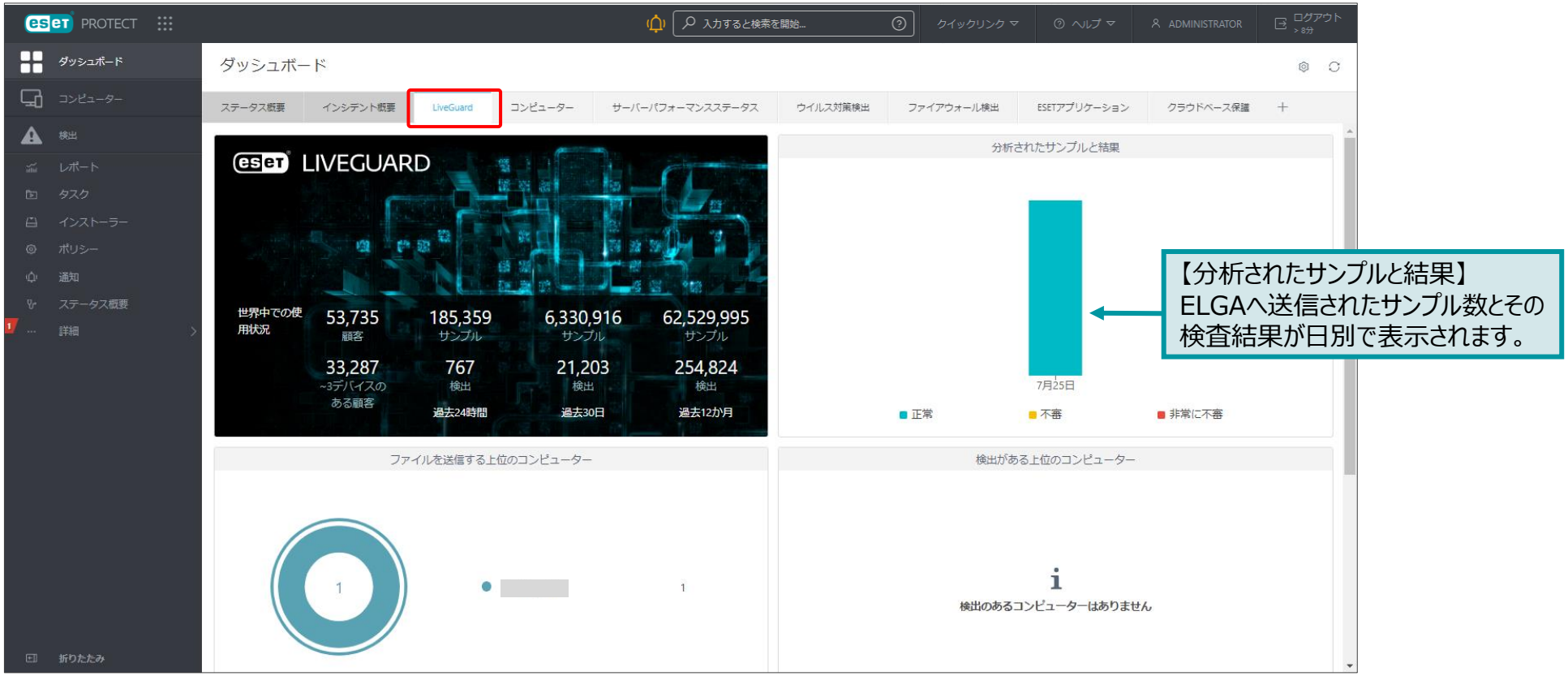
③セキュリティ通知
内容が表示されます。

【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。

5-1. ダッシュボード (LiveGuard Advanced)

クラウドサンドボックスであるESET LiveGuard Advanced (ELGA)の世界中での使用状況が確認できます。また、その他レポートでは送信されたサンプル数や検出数、検出数が多いコンピューター、検出されたファイルタイプなどの情報が確認できます。

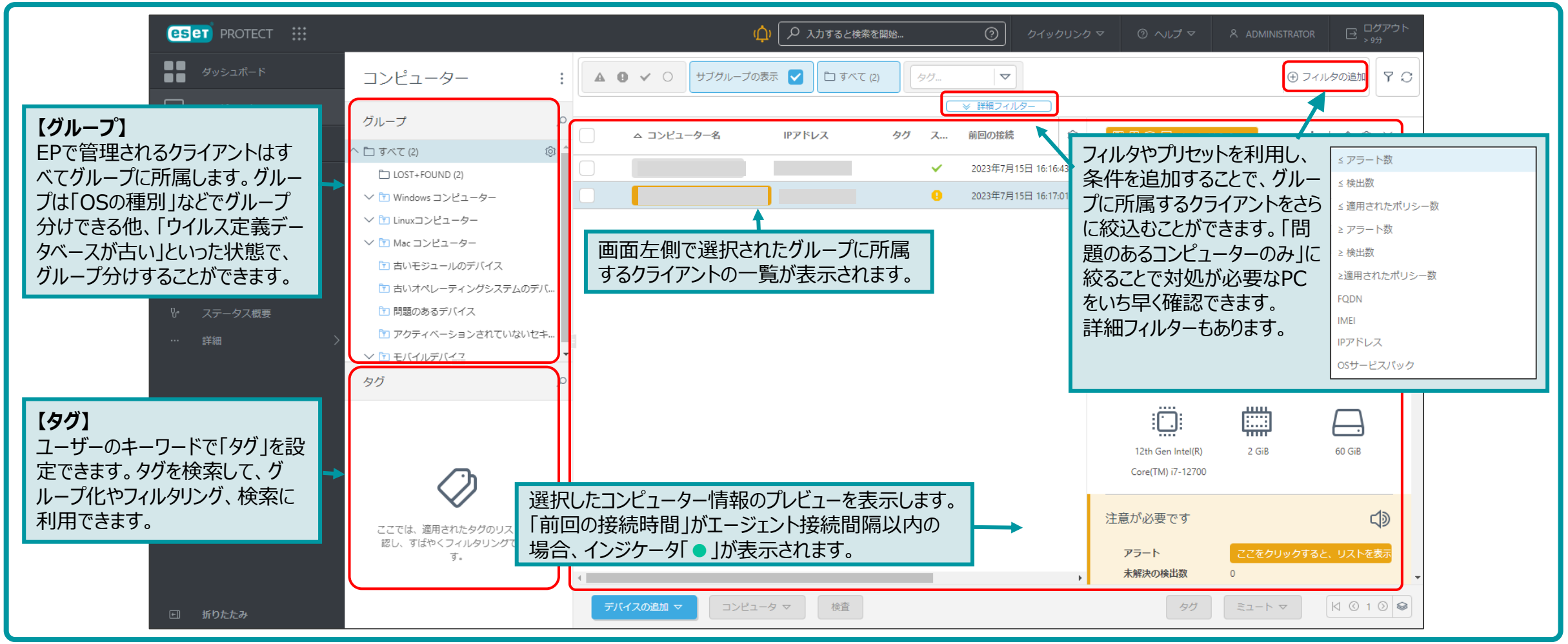
※ELGAは以下のオンプレミスソリューションでご利用可能です。
ESET PROTECT Essential Plus オンプレミス 、ESET PROTECT Advanced オンプレミス



【分析されたサンプルと結果】
ELGAへ送信されたサンプル数とその検査結果が日別で表示されます。

5-2. 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。



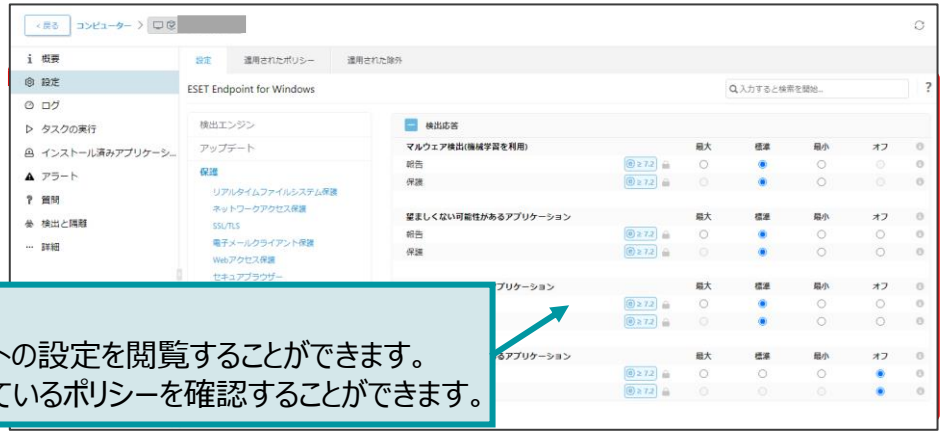
5-2. コンピューター (詳細情報)

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

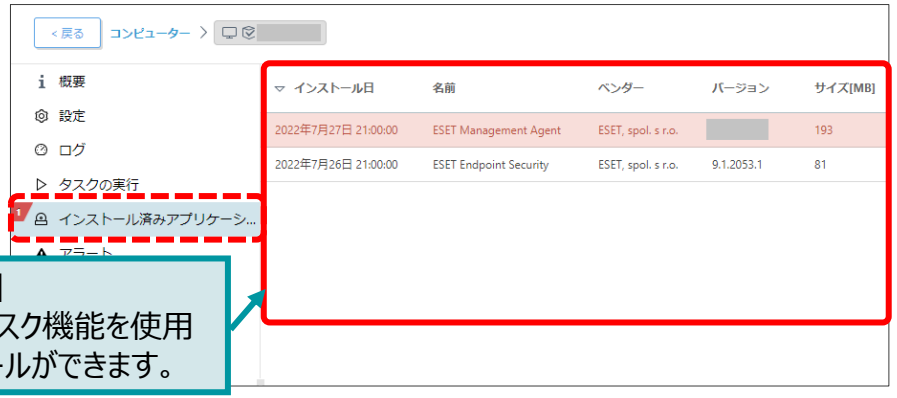
【詳細】-【ハードウェア】
コンピューターの情報やESETの情報について、概要がまとめられています。ハードウェアでは、デバイスのRAM、ストレージ、プロセッサーなどハードウェアの詳細情報を確認できます。

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。

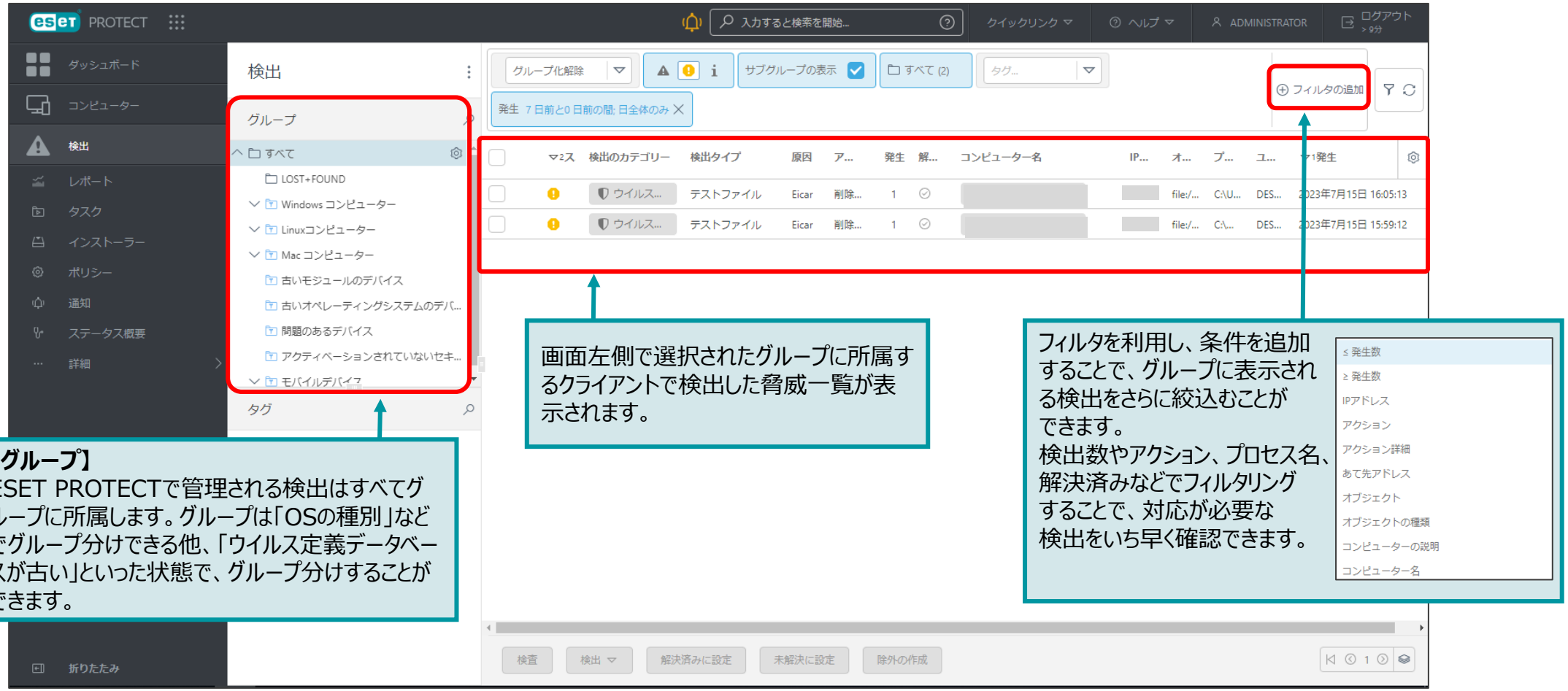
コンピューター - 詳細画面 - インストール済みアプリケーション



【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。

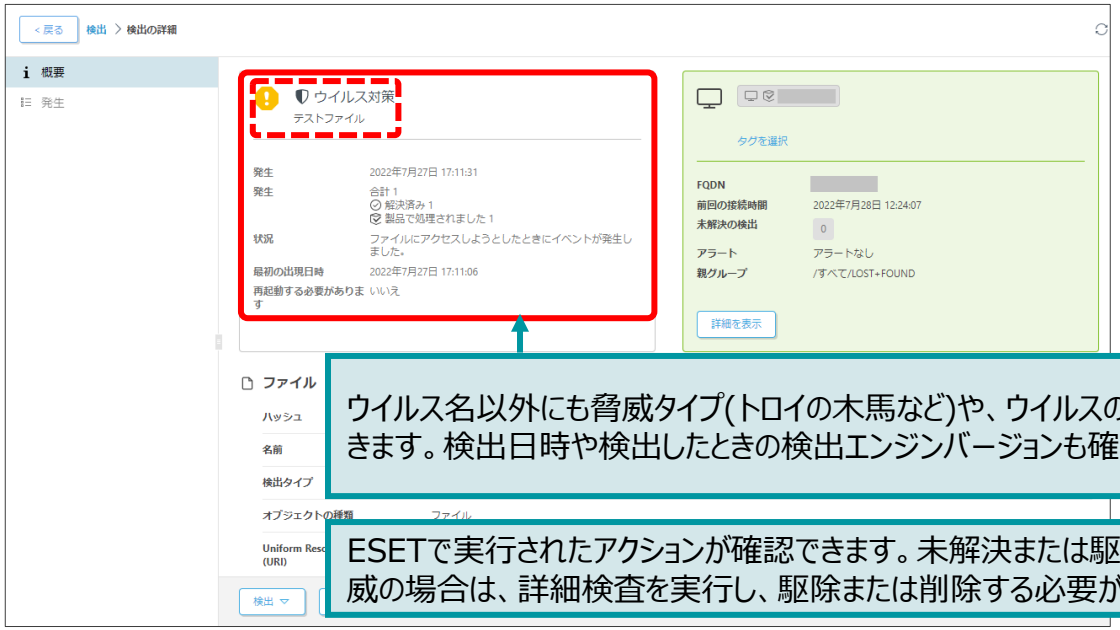
5-3. 検出

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ログなどの概要が表示されます。



5-3. 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。

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アカウントで検出されたか確認することができます。

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。

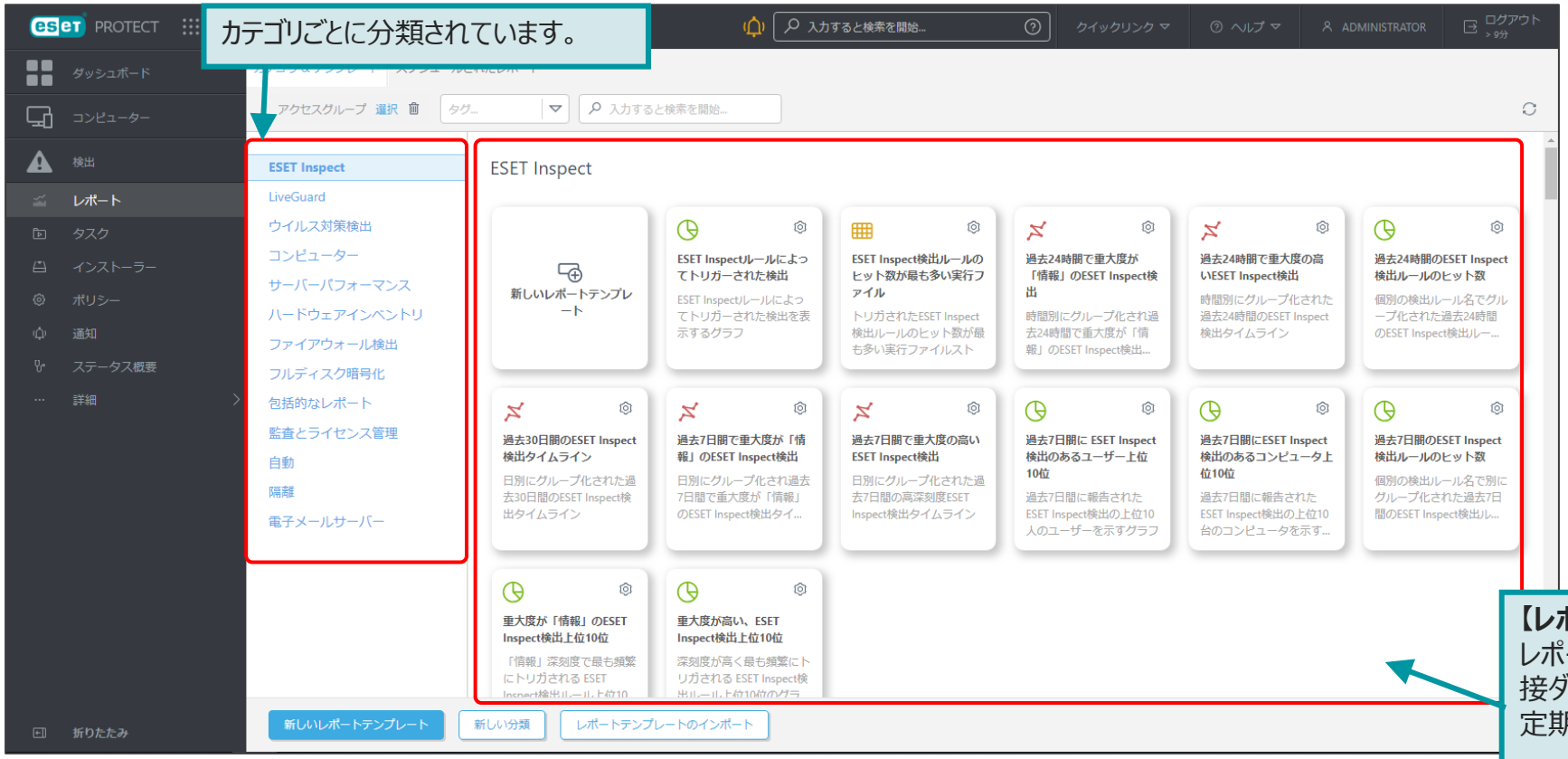
[世界での観測]
ESET LiveGrid®で収集した情報から脅威を評価します。
LiveGridでの評価や発生数、初回に確認された時期が確認できます。評価は色別に脅威レベルが分かれており、[赤：悪意] [黄：不審] で表示されます。

[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。

6. クライアント管理機能のご紹介

6-1. レポート

クライアントから収集した情報や管理サーバー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120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。

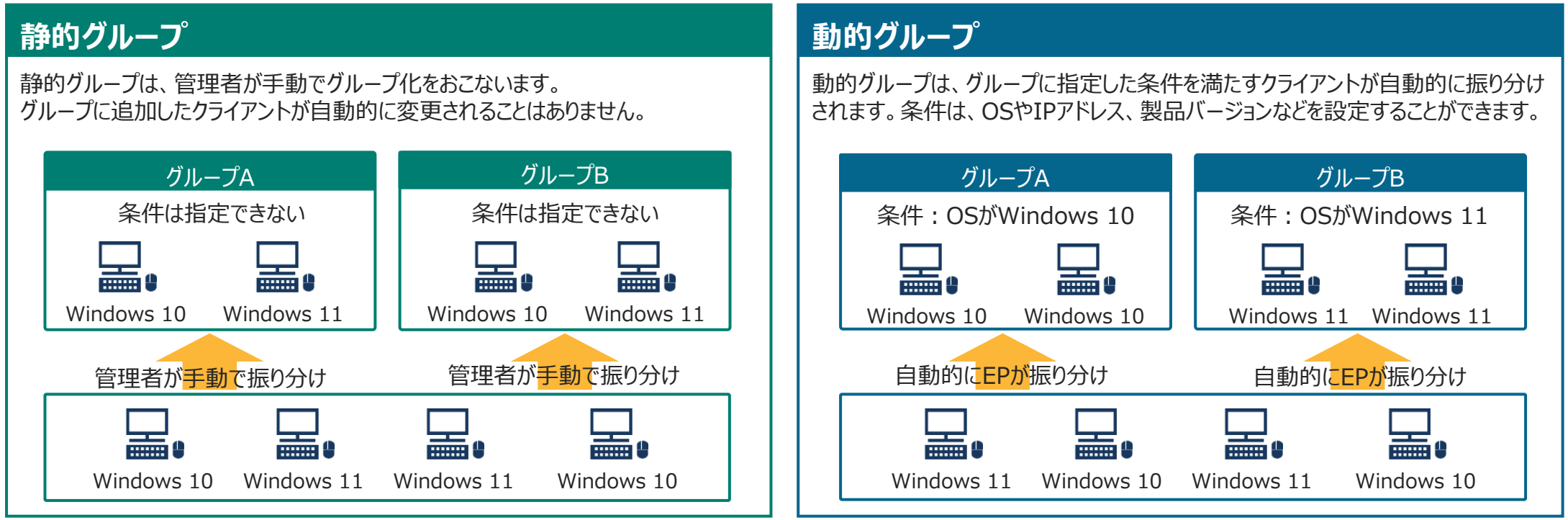


【レポート】
レポートはCSVやPS、PDF形式でブラウザから直接ダウンロードすることが可能です。また、レポートを定期的に自動作成することも可能です。

用途に応じて柔軟に作成することができます。

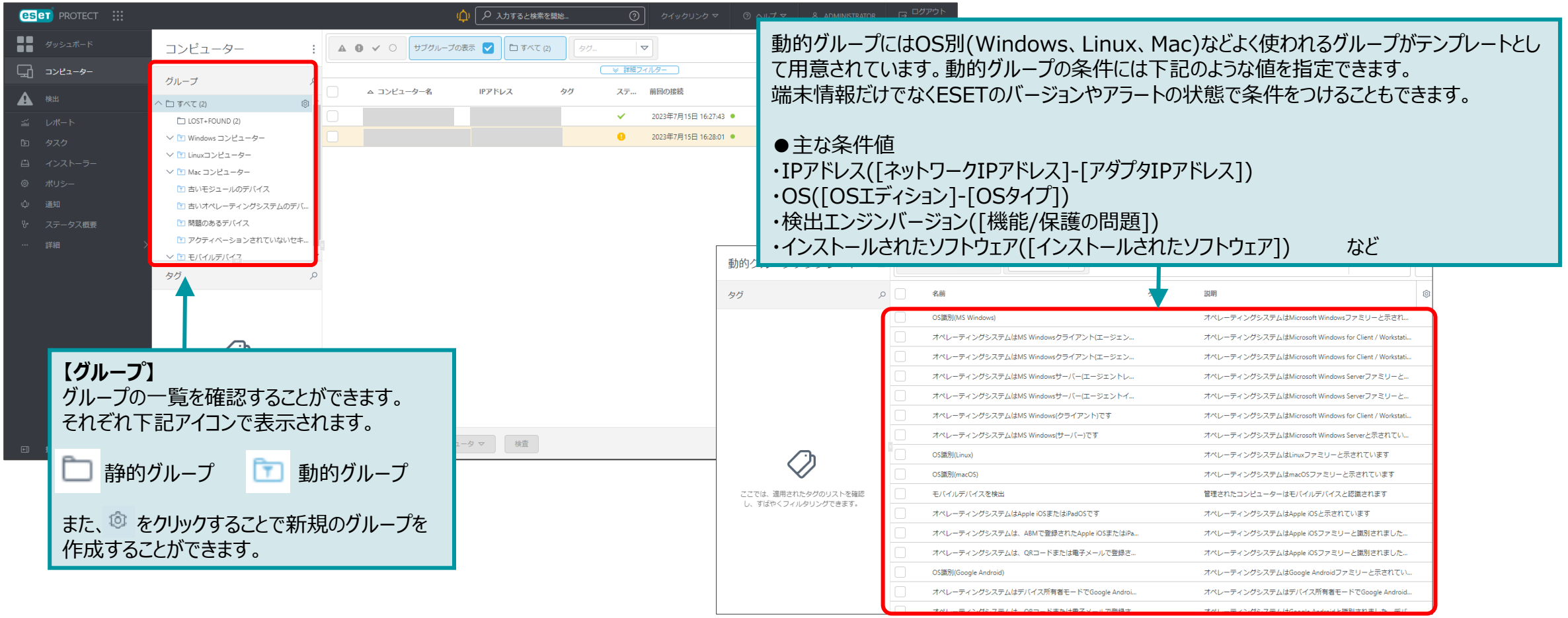
6-2. グループ

ESET PROTECT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。



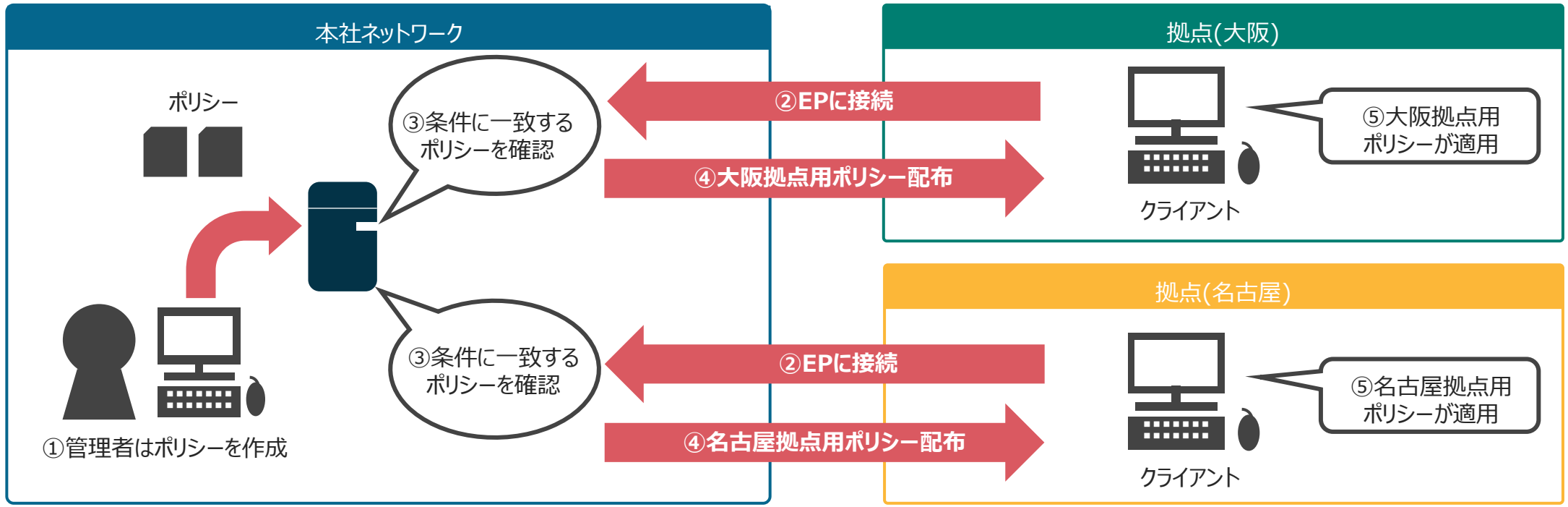
6-2. グループ

コンピューターより、「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。



6-3. ポリシー

ポリシーを利用して、クライアントのESET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(ポリシー)を自動で適用することもできます。



6-3. ポリシー

ポリシーにはあらかじめテンプレートが用意されています。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ができます。設定を行う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るため、簡単に設定を行うことができます。

設定したポリシーをグループまたはクライアントに割り当てることができます。

現在、ポリシーを適用中の端末を確認できます。

【ポリシー】
ポリシーには、デバイスコントロール、ファイアウォール、ログ、画面表示、ウイルス対策など様々なテンプレートが用意されています。設定内容は設定をクリックすると表示されます。テンプレートはビルトインポリシーに分類され、新しく作成するポリシーは、カスタムポリシーに保存されます。

6-4. 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から配布できる主なタスクは以下の通りです。

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ーの検査を実行します。
- **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

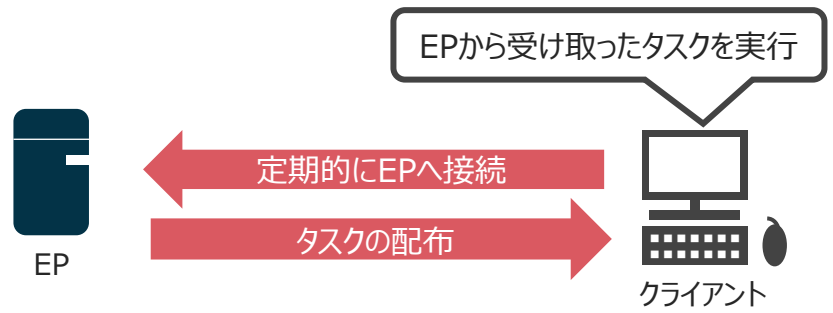
- **ESET PROTECT コンポーネントのアップグレード**
  EPやEMエージェントのアップグレードを実行します。
- **管理の停止**
  クライアントのEM エージェントをアンインストールします。

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。

モバイル

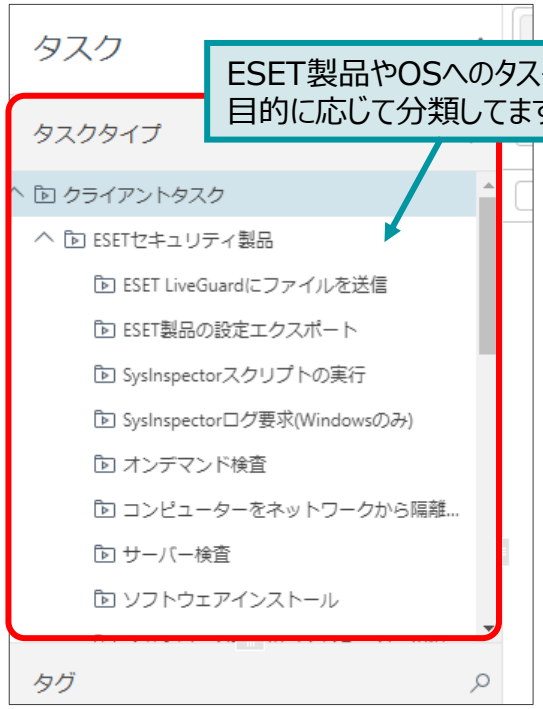
- **アンチセフトアクション**
  AndroidデバイスやiOSバイスの盗難や紛失時に、検索、ロック、警報、ワイプ、拡張初期設定リセットを実行します。



6-4. タスク

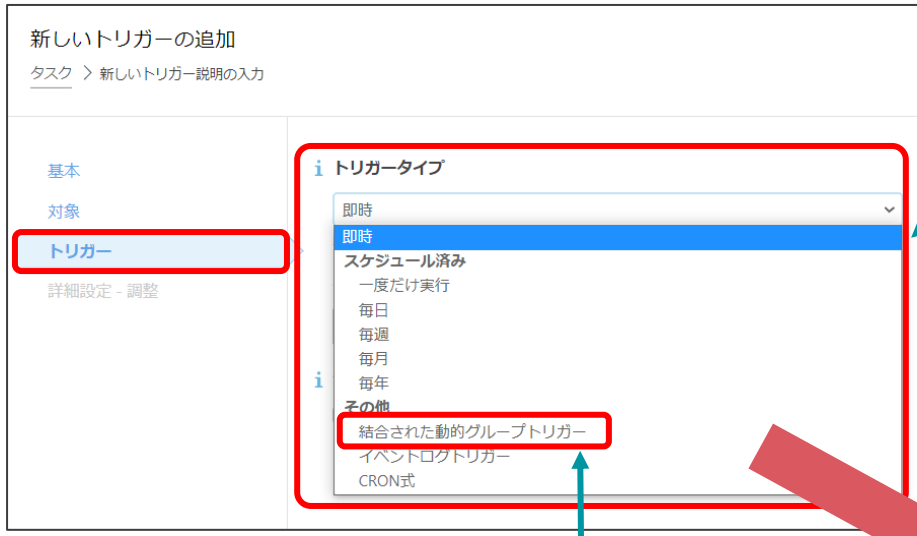
タスクでは、実行するターゲットを「コンピューター」単体で指定する以外に、「静的グループ」「動的グループ」を指定することで複数のコンピューターに対して指定できます。タスクを実行するタイミングはトリガーで設定します。

タスク画面



ESET製品やOSへのタスクなど、目的に応じて分類してます。

タスク - トリガータイプ画面



【トリガータイプ】
タスクを実行させる日にちや時間の指定を行います。負荷を分散するために指定した時間の範囲内でランダムにタスクを実行させる「ランダム遅延間隔」の指定もできます。

タスク - 詳細設定画面

【結合された動的グループトリガー】
動的グループトリガーに指定することにより、動的グループにクライアントが加わったタイミングでタスクを実行することができます。
「古いモジュールのコンピューター」や「アクティベーションされていないセキュリティ製品を検出」などの動的グループを設定しておくことで、問題が発生したクライアントに対してタスクを自動的に適用させることができます。

6-5. インストーラー

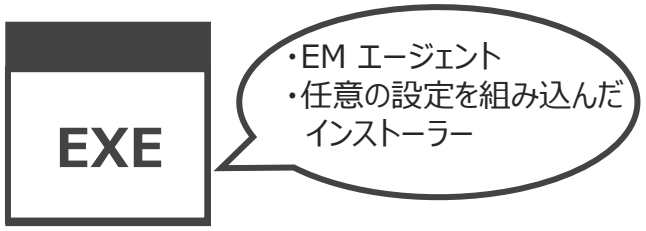
クライアントにEMエージェントとESET製品を展開するためのインストーラーパッケージを作成することができます。インストーラー機能では、以下3種類のインストーラーを作成することができます。

オールインワンインストーラー

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。(Windows製品のみ)

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。

コアコンポーネントのみの軽量版インストーラーか、fullインストーラー（従来版）かの選択が可能です。(EES/EEA V9.1以降、ESSW V10.0以降の場合)



エージェントスクリプトインストーラー

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

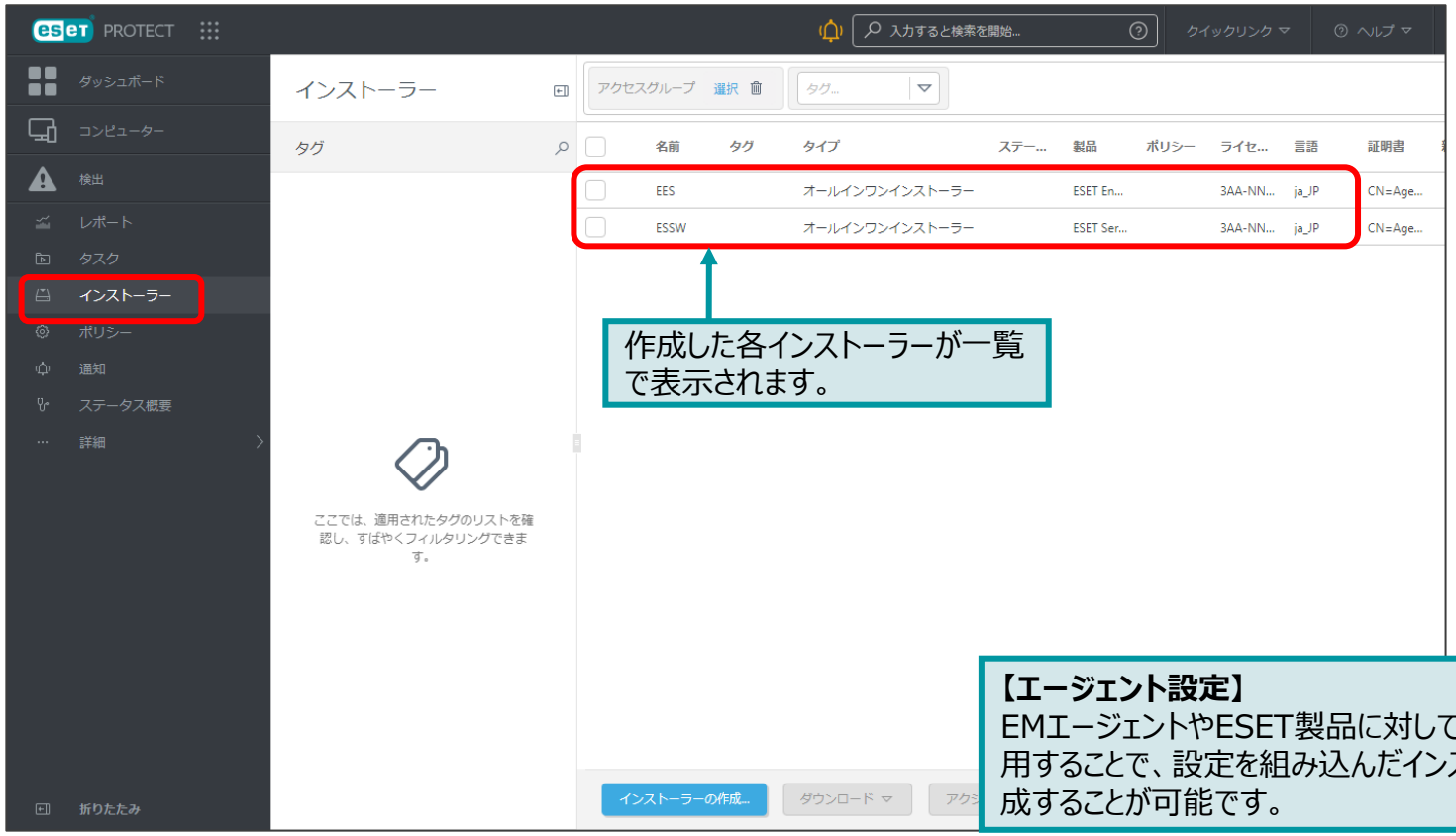
GPOまたはSCCMを使用したEMエージェント展開用スクリプトファイル。
本スクリプトファイルを弊社ユーザーズサイトよりダウンロードしたEMエージェントのインストーラーと同ディレクトリに配置してインストーラーを実行します。

ESET製品のインストールは、別途行う必要があります。

6-5. インストーラー

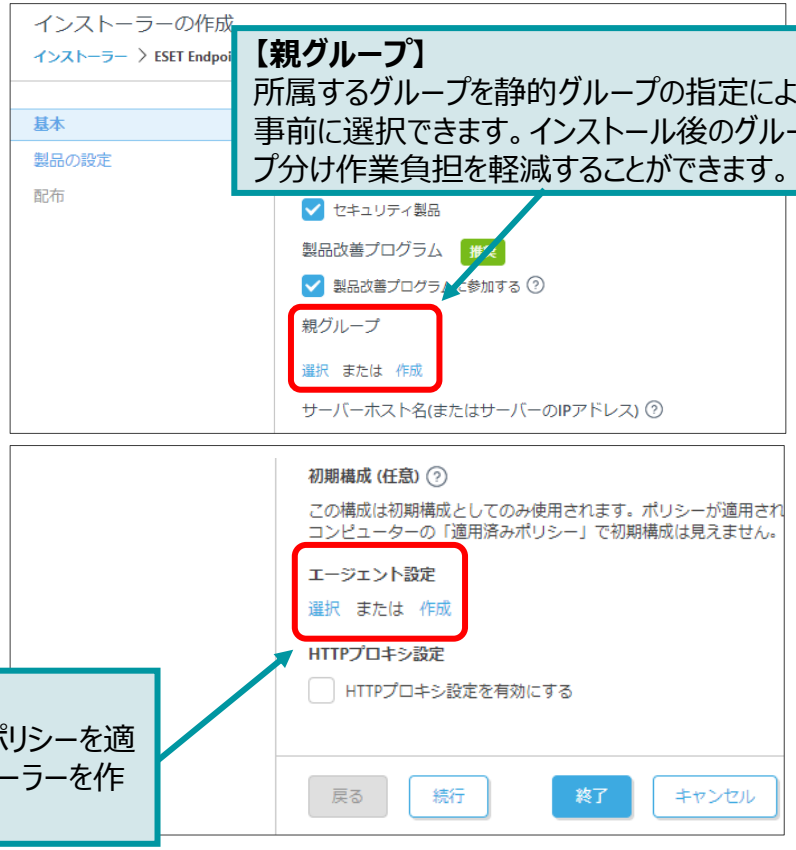
一度作成したインストーラーは、一覧で表示されます。作成時にポリシーをEM エージェントやESET製品に組み込むことができます。また、所属する「静的グループ」を事前に指定することができ、展開時のグループ管理がおこないやすくなっております。

インストーラー画面



作成した各インストーラーが一覧で表示されます。

オールインワンインストーラー - 作成画面

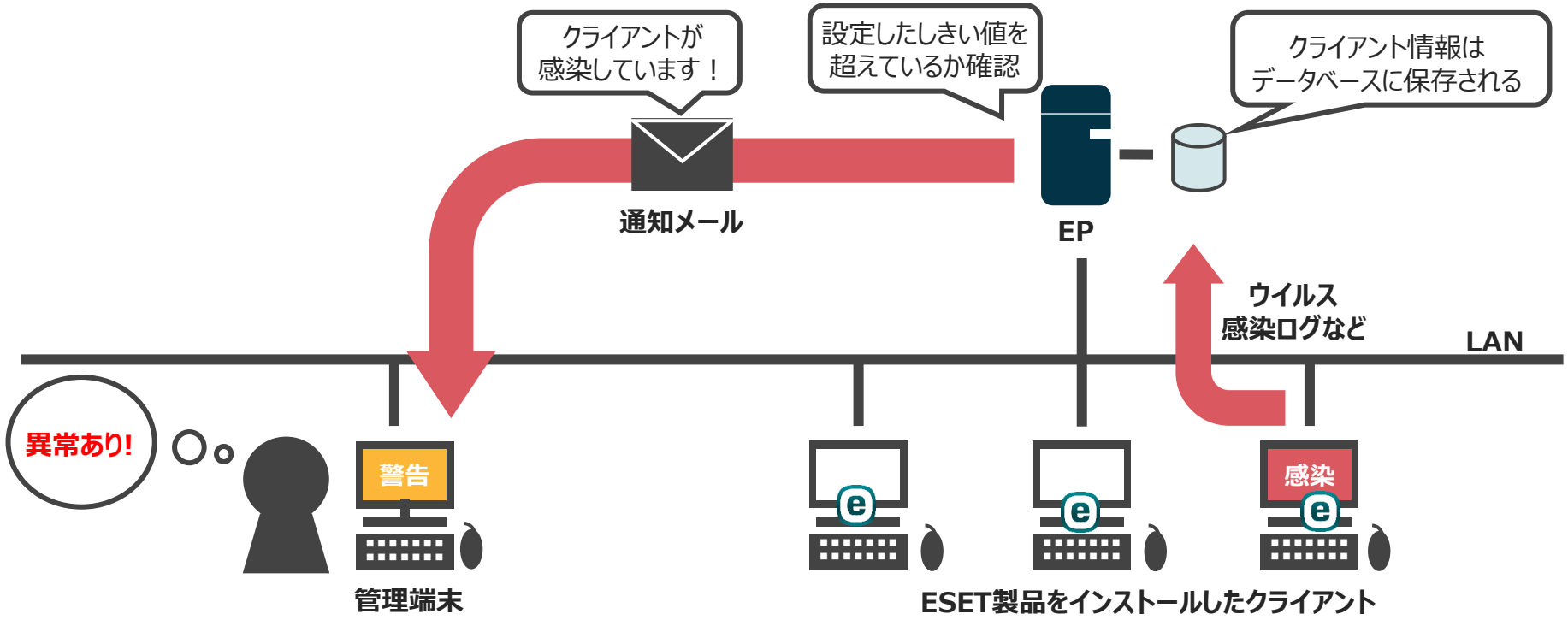


【親グループ】
所属するグループを静的グループの指定により事前に選択できます。インストール後のグループ分け作業負担を軽減することができます。

【エージェント設定】
EMエージェントやESET製品に対して、ポリシーを適用することで、設定を組み込んだインストーラーを作成することが可能です。

6-6. 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おこなうことができます。
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。

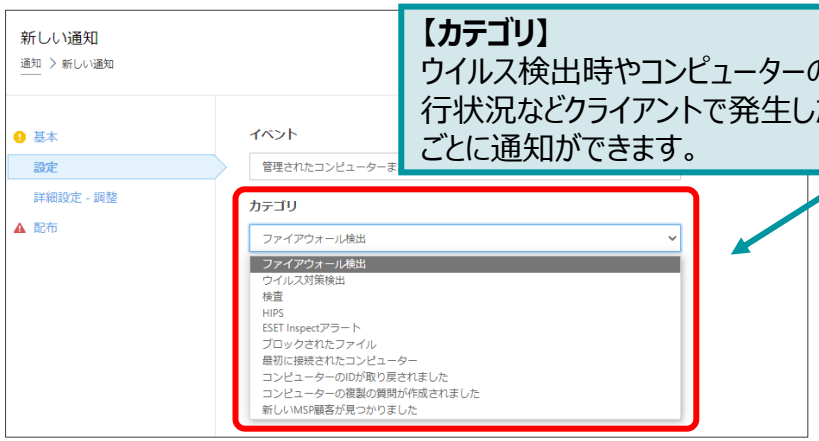


6-6. 通知

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SNMPトラップ、電子メール、Syslogへの送信でおこないます。

通知画面

通知 - 設定画面



通知 - 配布画面

【カテゴリ】
ウイルス検出時やコンピューター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。

【通知ルール】
マルウェアの発生状況など、既定で28種類のルールが用意されています。

【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。

7. サーバー運用管理機能のご紹介

7-1. 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。

本社

ユーザー名：Administrator

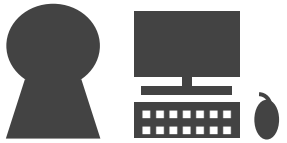
本社管理者
※本社および拠点(大阪)を管理

機能アクセス
全ての機能に対して書き込み権限を付与

グループアクセス
全てのグループに対してアクセスを許可

拠点(大阪)

ユーザー名：osaka



拠点(大阪)管理者
※拠点(大阪)を管理

機能アクセス
タスクのみ書き込み権限を付与
それ以外の機能に対する権限は付与しない

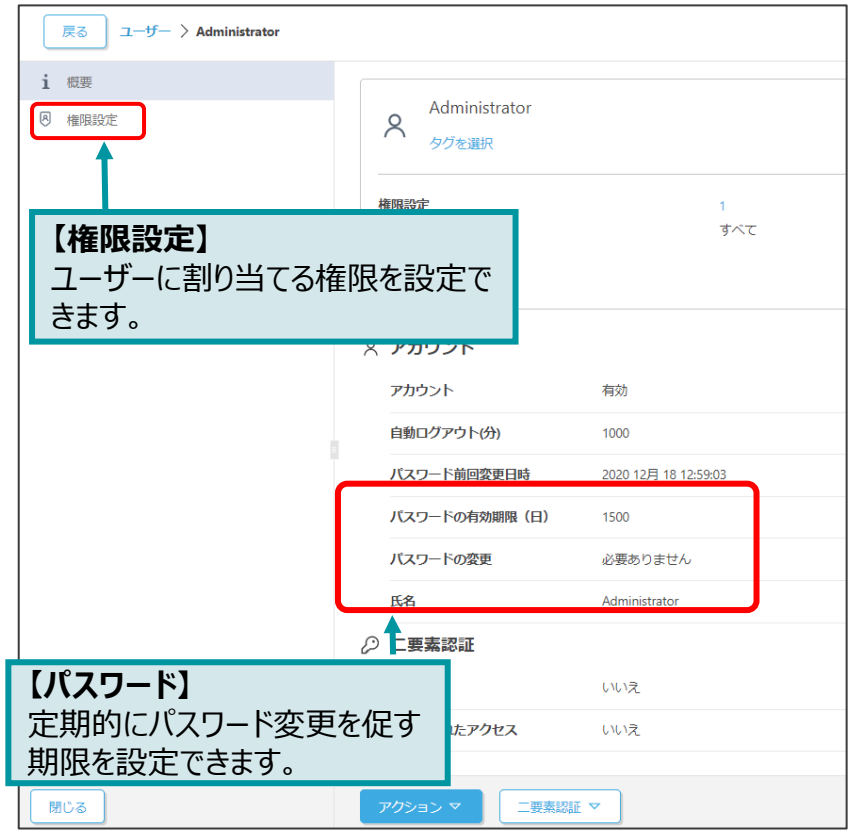
グループアクセス
自拠点(大阪)のグループに対してのみ
アクセスを許可

・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。

7-1. 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。

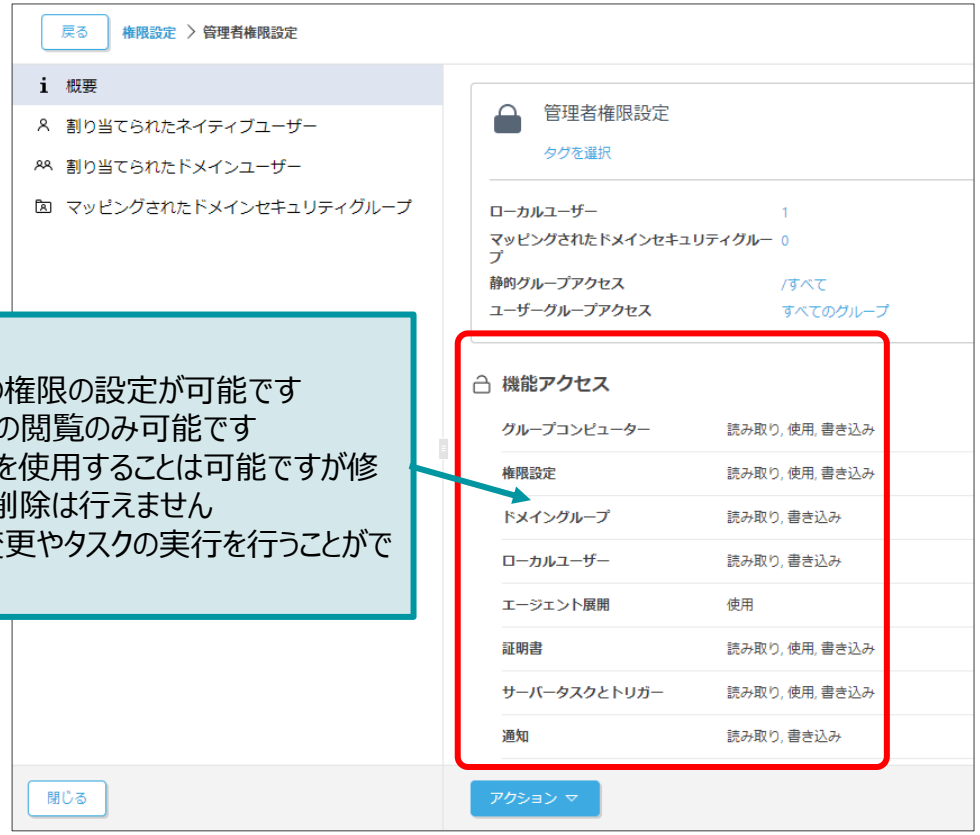
ユーザー画面



【権限設定】
ユーザーに割り当てる権限を設定できます。

【パスワード】
定期的にパスワード変更を促す期限を設定できます。

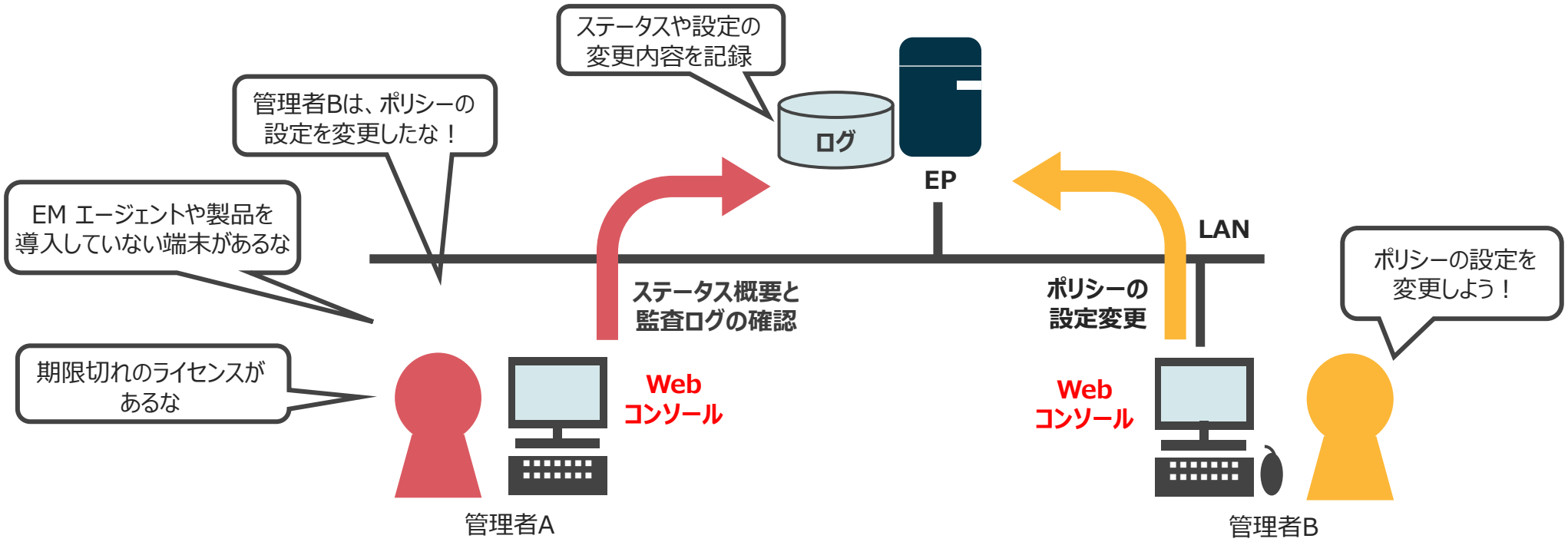
権限設定画面



【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

7-2. 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おこな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。



7-2. 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

EPのステータスがセクションごとに色別で表示されます。

色の意味は以下の通りです。
・緑 (OK) - 問題ありません。
・黄色 (警告) - １つ以上の警告があります。
・赤 (エラー) - １つ以上のエラーがあります。
・灰色 (コンテンツは利用できません) - アクセス権不足のため表示できません。
・青 (情報) - ハードウェアに関する質問があります。

7-2. 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」などを確認することができます。

監査ログ画面

「Administrator」がポリシーを設定

「Administrator」がライセンスを追加

「Administrator」がEPにログインを試行