

オンプレミス型セキュリティ管理ツール ESET PROTECT on-prem V12 機能紹介資料

第1版

2025年1月9日

Canon

もくじ

1. はじめに(本資料について)
2. ESET PROTECT on-premとは
3. ESET PROTECT on-premの構成
4. Webコンソールのご紹介
5. ログ監視機能のご紹介
6. クライアント管理機能のご紹介
7. サーバー運用管理機能のご紹介

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 on-prem V12)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をご用意しています。
- 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 Dynamic Threat Defenseは、ESET LiveGuard Advancedに名称が変更になりました。

2. ESET PROTECT on-premとは

2. ESET PROTECT on-premとは

ESET PROTECT on-prem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、Linux向けプログラムを管理できます。

※オンプレミス型セキュリティ管理ツールではAndroid、iOSなどのモバイル端末の管理はできませんので、ご注意ください。

モバイル端末を管理される場合はクラウド型セキュリティ管理ツールのご利用をご検討ください。

ESET PROTECT on-prem V12.X で管理可能なプログラム

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	12.X / 11.X / 10.1 / 9.1
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	12.X / 11.X / 10.1 / 9.1
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	11.X / 10.X / 9.X / 8.X
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	8.X
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.X
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

※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 on-premとは

ESET PROTECT on-premの主な機能

ESET PROTECT on-prem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。ESET PROTECT on-prem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



5.ログ監視機能の
ご紹介を参照

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



6.クライアント管理機能の
ご紹介を参照

サーバー運用管理機能

- ・ユーザー管理
- ・監視・監査



7.サーバー運用管理機能の
ご紹介を参照

3. ESET PROTECT on-premの構成

3. ESET PROTECT on-premの構成

ESET PROTECT on-premは以下のコンポーネントから構成されています。

ESET PROTECT on-prem

EP on-prem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。

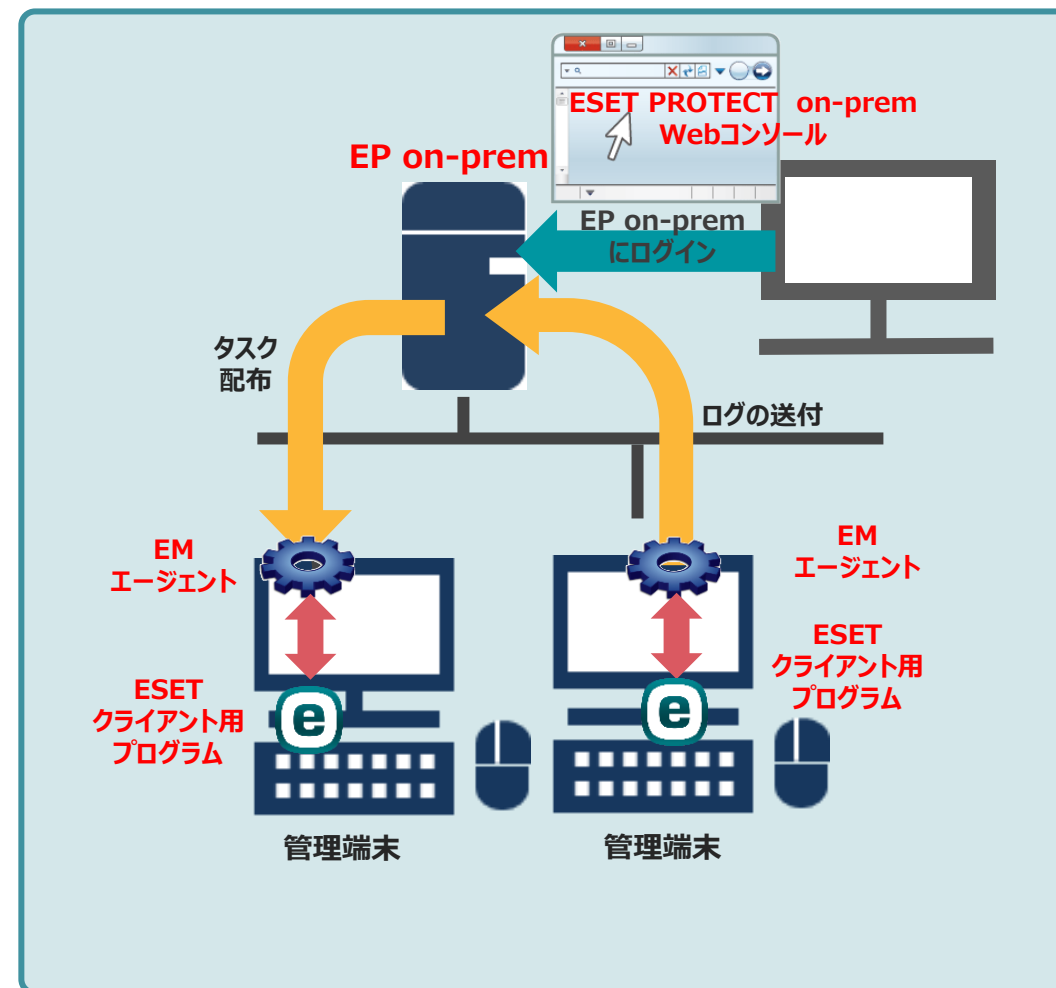
ESET PROTECT on-prem Webコンソール

WebコンソールはWebベースのインターフェースであり、ブラウザを使用してEP on-premへアクセスします。ブラウザ経由でクライアント情報の閲覧やEP on-prem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 on-premへデータを送信します。また、EP on-prem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 on-premの構成

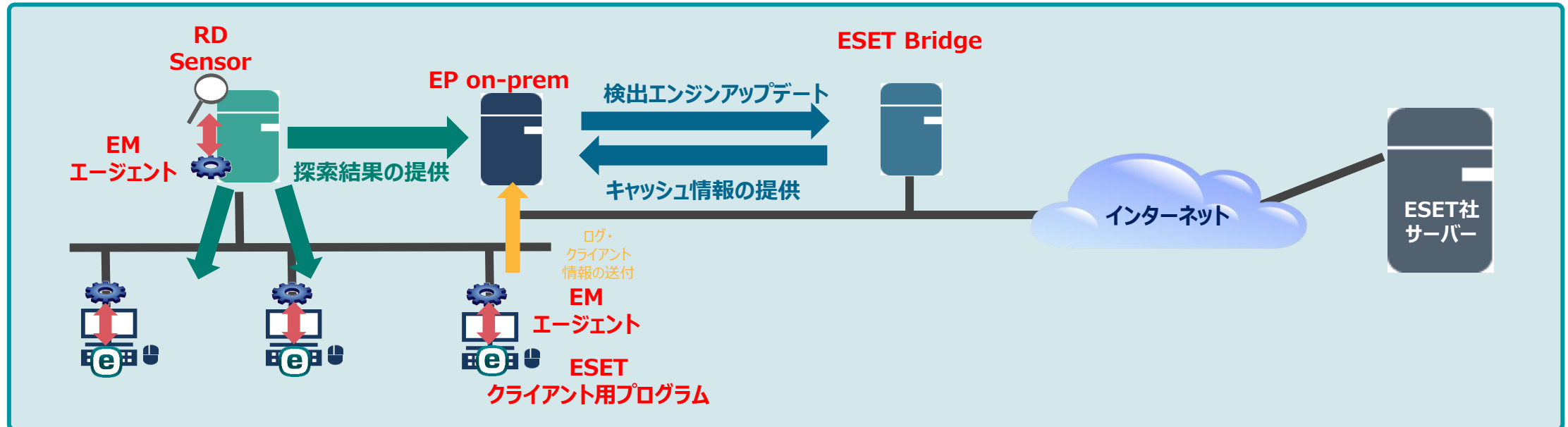
以下のコンポーネントは任意で構成します。

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 on-prem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 on-prem V12 (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	10GBまで
	Microsoft SQL Server 2022 Standard Edition	制限なし
	Microsoft SQL Server 2022 Express Edition(既定) ※2	10GBまで
EP on-prem V12 (Linux版)	MySQL(※3) 5.7、8.0、8.1	制限なし

※1 Windows Server 2012/2012 R2の場合。

※2 Windows Server 2016/2019/2022の場合。MSSQL2022では「.NET Framework 4.7.2以降」のご利用が必要です。

※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 on-prem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 on-prem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 on-prem V12 (Windows版)	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)
	Windows Server 2025 Standard (64bit) / Datacenter (64bit)
EP on-prem V12 (Linux版)	Rocky Linux 9(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 on-prem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 on-prem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 on-prem Webコンソール サポート対象ブラウザ

サポート対象ブラウザ
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 on-prem 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。

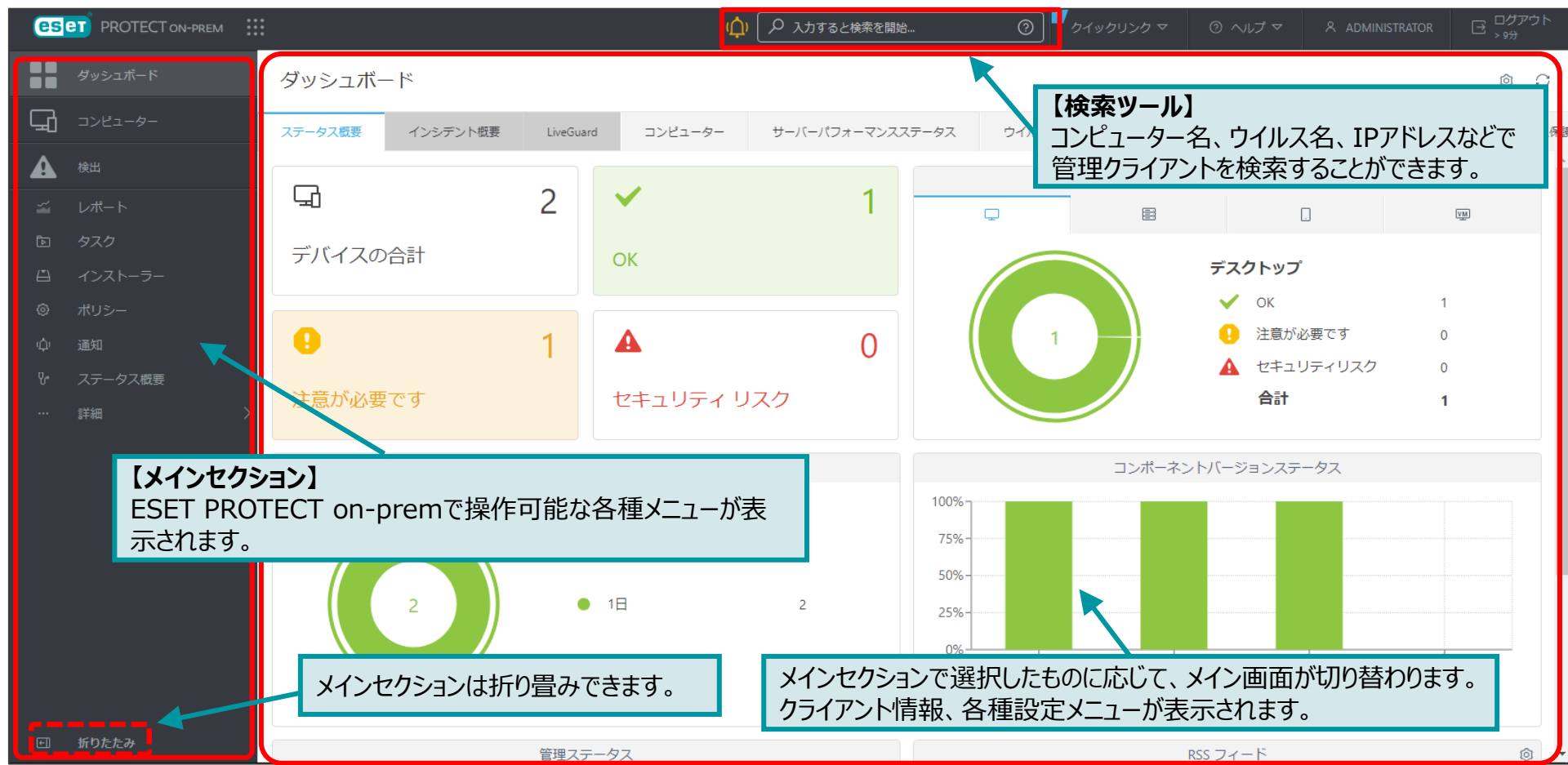
【マルチ言語対応】

EP on-prem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。



The screenshot shows the ESET PROTECT ON-PREM Web Console interface. The interface is divided into three main sections:

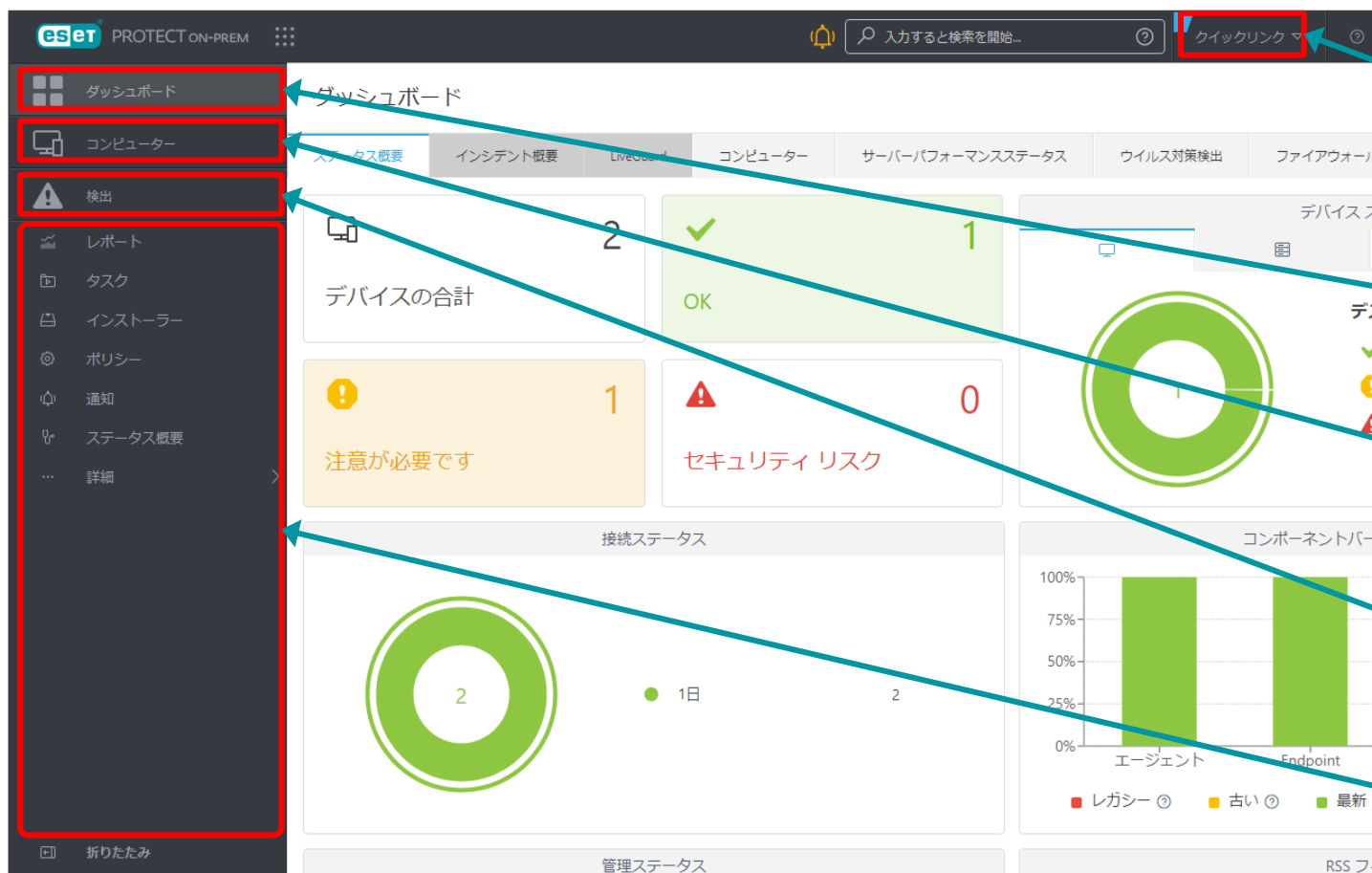
- Left Section (Main Section):** A dark sidebar containing a menu with items like 'ダッシュボード' (Dashboard), 'コンピューター' (Computer), '検出' (Detection), 'レポート' (Report), 'タスク' (Task), 'インストーラー' (Installer), 'ポリシー' (Policy), '通知' (Notification), 'ステータス概要' (Status Overview), and '詳細' (Details). A callout box labeled **【メインセクション】** states: "ESET PROTECT on-premで操作可能な各種メニューが表示されます。" (Various menus operable in ESET PROTECT on-prem are displayed). At the bottom of this sidebar, a button labeled '折りたたみ' (Collapse) is highlighted with a dashed red box. A callout box below it states: "メインセクションは折り畳みできます。" (The main section can be collapsed).
- Top Section (Search Tool):** A search bar at the top center with the placeholder text '入力すると検索を開始...' (Start search when input...). A callout box labeled **【検索ツール】** states: "コンピューター名、ウイルス名、IPアドレスなどで管理クライアントを検索することができます。" (You can search for managed clients by computer name, virus name, IP address, etc.).
- Right Section (Main Content Area):** The main dashboard area showing various metrics and charts. It includes a 'ダッシュボード' (Dashboard) header, tabs for 'ステータス概要' (Status Overview), 'インシデント概要' (Incident Overview), 'LiveGuard', 'コンピューター' (Computer), 'サーバーパフォーマンスステータス' (Server Performance Status), and 'ウイルス' (Virus). Key metrics include:
 - デバイスの合計 (Total Devices): 2
 - OK: 1
 - 注意が必要です (Needs Attention): 1
 - セキュリティ リスク (Security Risk): 0
 A donut chart shows 1 OK and 1 Needs Attention. A table titled 'デスクトップ' (Desktop) shows:

ステータス	数
OK	1
注意が必要です	0
セキュリティリスク	0
合計	1

 Below this is a bar chart titled 'コンポーネントバージョンステータス' (Component Version Status) showing 100% completion for three components. A callout box at the bottom right states: "メインセクションで選択したものに依じて、メイン画面が切り替わります。クライアント情報、各種設定メニューが表示されます。" (Depending on what is selected in the main section, the main screen switches. Client information and various setting menus are displayed).

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 on-prem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 on-prem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 on-prem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 on-prem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 on-prem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 on-prem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 on-prem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 on-prem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。

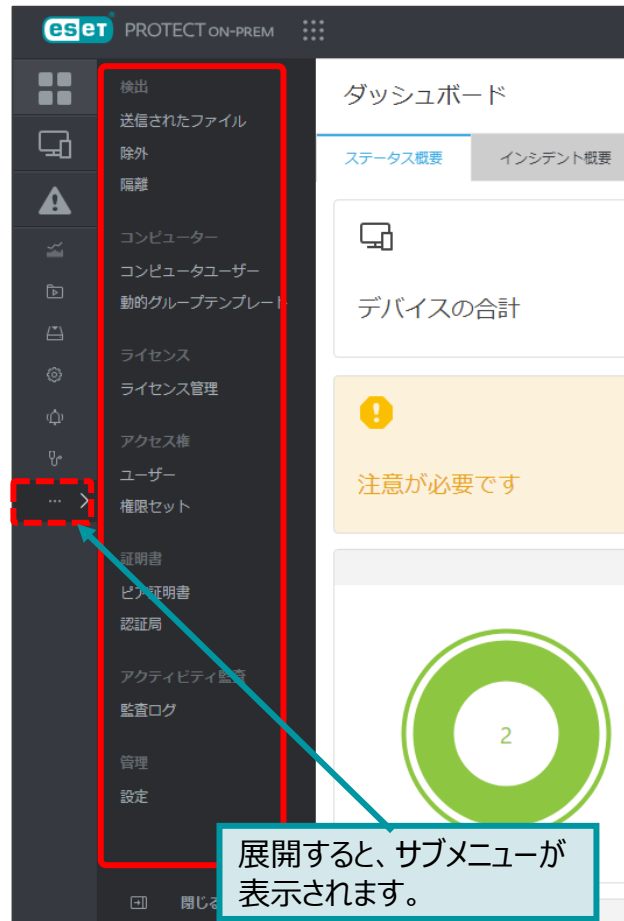
【詳細】
EP on-premに関するさらに詳細なメニューが開きます。

【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】

クラウドサンドボックス製品である「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のご利用には、「ESET PROTECT Advanced」以上のライセンスが必要です。

【ライセンス】

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

【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。

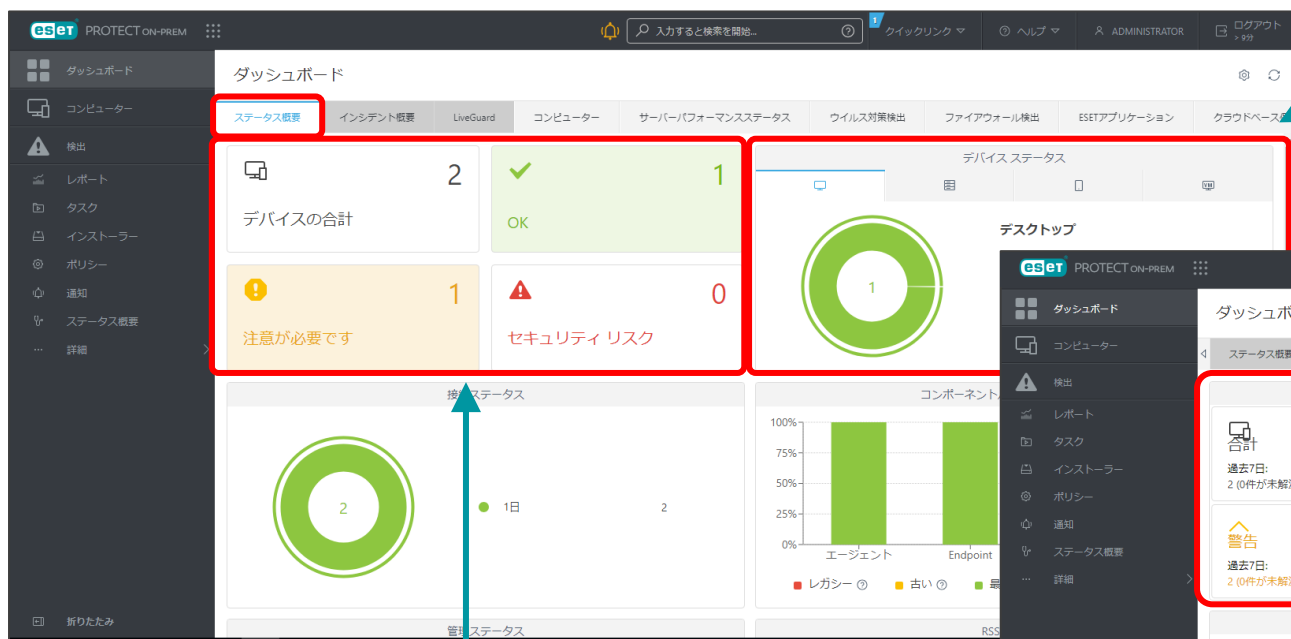
展開すると、サブメニューが表示されます。

5. ログ監視機能のご紹介

5-1. ダッシュボード

EP on-prem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。



ダッシュボード - インシデント概要(既定テンプレート)



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。

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 on-prem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)

ダッシュボード上部のタブをクリックすることで、表示する画面を切り替えることができます。

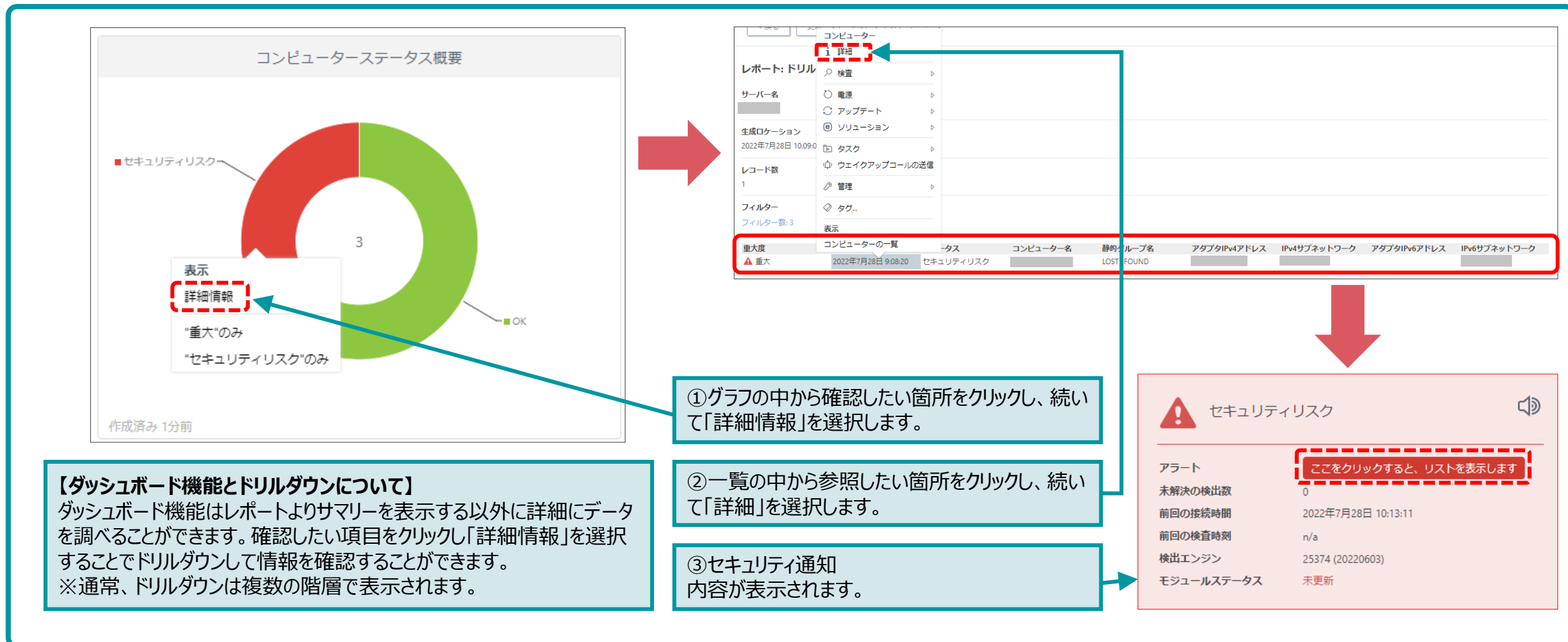
ダッシュボードに表示するレポートは、追加することもできます。また、位置や大きさなどをカスタマイズすることができます。

ウイルス対策検出

コンピュータ名	発生時刻	重大度	ソース	機能
██████████	2024年1月10日 13:...	警告	セキュリティ製品	その他

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。



コンピューターステータス概要

■ セキュリティリスク

3

■ OK

表示

詳細情報

"重大"のみ

"セキュリティリスク"のみ

作成済み 1分前

コンピューターステータス概要

レポート: ドリル

サーバー名

生成ロケーション

レコード数

フィルター

重大度	コンピューターステータス概要	タス	コンピューターステータス概要	静黙グループ名	アダプタIPv4アドレス	IPv4サブネットワーク	アダプタIPv6アドレス	IPv6サブネットワーク
▲ 重大	2022年7月28日 9:08:20	セキュリティリスク		LOST FOUND				

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。

セキュリティリスク

アラート

未解決の検出数

前回の接続時間

前回の検査時刻

検出エンジン

モジュールステータス

ここをクリックすると、リストを表示します

0

2022年7月28日 10:13:11

n/a

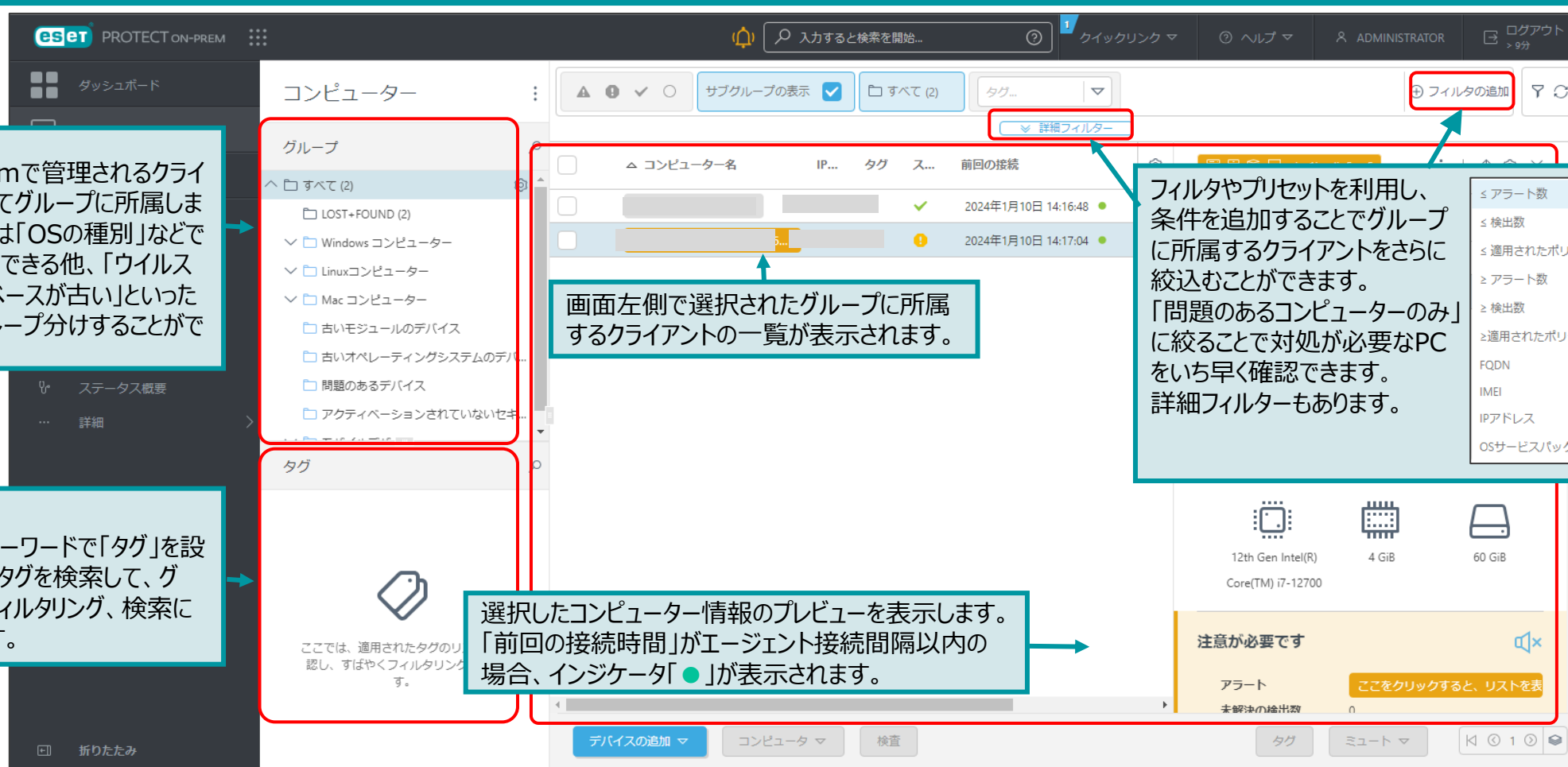
25374 (20220603)

未更新

【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。

5-2. コンピューター

EP on-prem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 on-prem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、「ウイルス定義データベースが古い」といった状態で、グループ分けすることができます。

【タグ】
ユーザーのキーワードで「タグ」を設定できます。タグを検索して、グループ化やフィルタリング、検索に利用できます。

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。

選択したコンピューター情報のプレビューを表示します。「前回の接続時間」がエージェント接続間隔以内の場合、インジケータ●が表示されます。

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ーのみ」に絞ることで対処が必要なPCをいち早く確認できます。詳細フィルターもあります。

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



ハードウェア

デバイス

メーカー: VMware, Inc.
 モデル: VMware7,1
 シリアル番号: VMware-56 4d 13 cf f7 31 5c 1f-8b 83 b5 8a c4 29 8f 86
 トラステッドプラットフォームモジュール(TPM)のバージョン: n/a
 ファームウェアタイプ: UEFI
 ファームウェアバージョン: INTEL - 6040000, VMW71.00V.18452719.B64.2108091906, VMware, Inc., VMware, Inc. c4 29 8f 86

CPU

説明: Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz
 クロックスピード: 2904 MHz
 コア数: 2
 論理コア数: 2
 アーキテクチャタイプ: x64
 メーカー: GenuineIntel

RAM

容量: 2 GiB
 クロックスピード: n/a
 メーカー: VMware Virtual RAM
 説明: 物理メモリ
 アーキテクチャタイプ: DRAM

【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

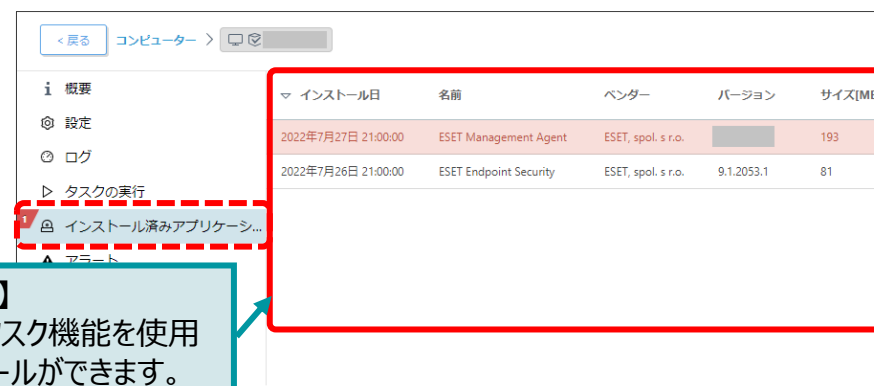


設定

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。

アプリケーション	最大	標準	最小	オフ
マルウェア検出(後継学習器を利用)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
警告	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
保護	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
疑わしくない可能性のあるアプリケーション	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
警告	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
保護	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
アプリケーション	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
アプリケーション	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

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



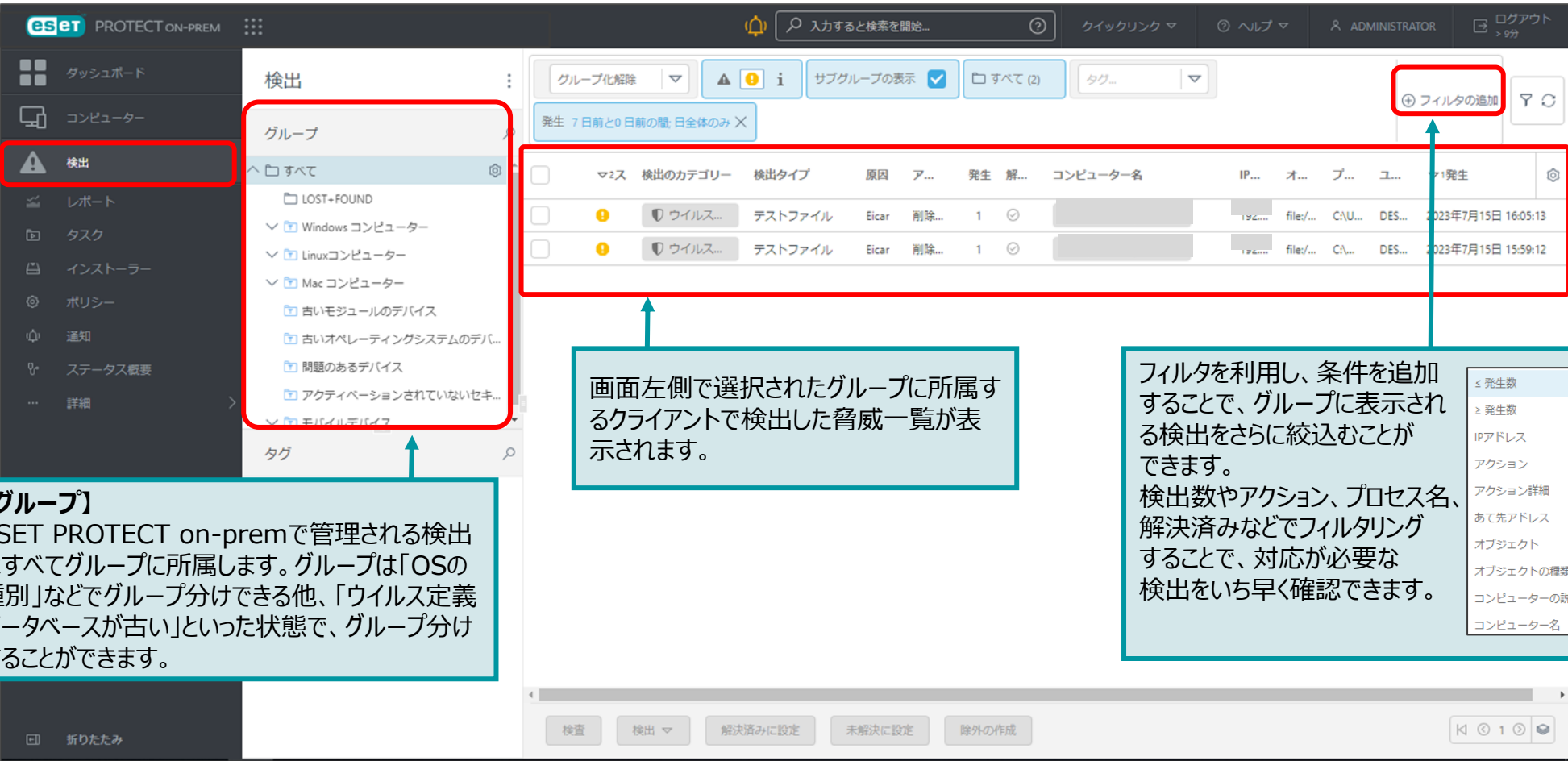
インストール日	名前	ベンダー	バージョン	サイズ[MB]
2022年7月27日 21:00:00	ESET Management Agent	ESET, spol. s r.o.		193
2022年7月26日 21:00:00	ESET Endpoint Security	ESET, spol. s r.o.	9.1.2053.1	81

【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。



【グループ】
ESET PROTECT on-premで管理される検出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、「ウイルス定義データベースが古い」といった状態で、グループ分けすることができます。

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で検出した脅威一覧が表示されます。

フィルタを利用し、条件を追加することで、グループに表示される検出をさらに絞込むことができます。検出数やアクション、プロセス名、解決済みなどでフィルタリングすることで、対応が必要な検出をいち早く確認できます。

フィルタ	値
発生数	≤ 発生数
発生数	≥ 発生数
IPアドレス	
アクション	
アクション詳細	
あて先アドレス	
オブジェクト	
オブジェクトの種類	
コンピューターの説明	
コンピューター名	

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。

ウイルス対策
テストファイル

発生 2022年7月27日 17:11:31
 合計 1
 ○ 解決済み 1
 ⊗ 製品で処理されました 1

状況 ファイルにアクセスしようとしたときにイベントが発生しました。

最初の出現日時 2022年7月27日 17:11:06
 再起動する必要がありません

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。

[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。

ファイル

ハッシュ 3395856C81F2B7382D8E72602F7968842F14140

名前 Eicar

検出タイプ テストファイル

オブジェクトの種類 ファイル

Uniform Resource Identifier file:///C:/Users/taquchi/AppData/Local/Microsoft/Windows/NetCache/low/E-QE323CVQ/eicar[1].com (URI)

プロセス名 C:\Program Files (x86)\Internet Explorer\iexplore.exe

ユーザー WIN-F3IQE4QM\9taquchi

検出

スキャナ リアルタイムファイルシステム監視

アクション 削除によって駆除されました

アクションエラー

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ー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®)

評価 ●●●●●●●●

発生数 ●●●●●●●●

初回の表示 7年前


組織内で観測された検出

数	4
初回	2021年12月10日 10:16:33
前回	2022年1月21日 15:39:39

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。



カテゴリごとに分類されています。

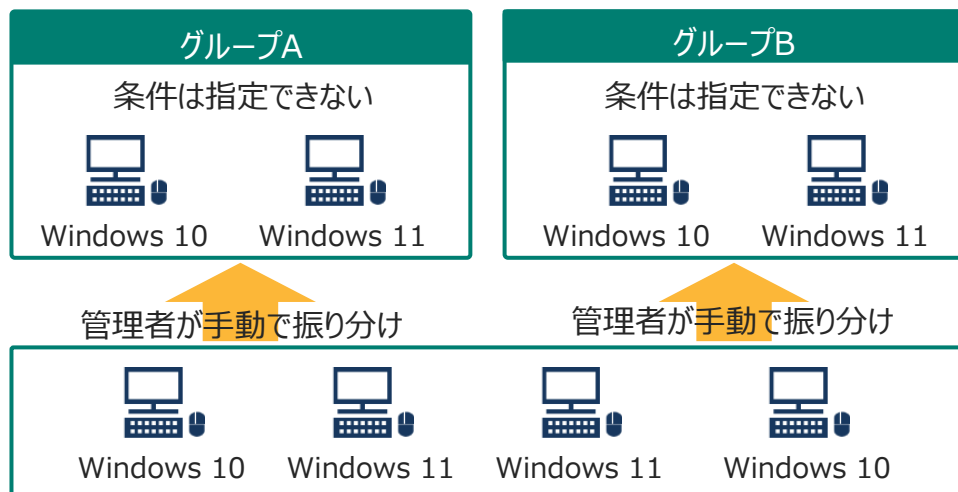
【レポート】
 レポートはCSVやPS、PDF形式でブラウザから直接ダウンロードすることが可能です。また、レポートを定期的に自動作成することも可能です。
 用途に応じて柔軟に作成することができます。

6-2. グループ

ESET PROTECT on-prem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。

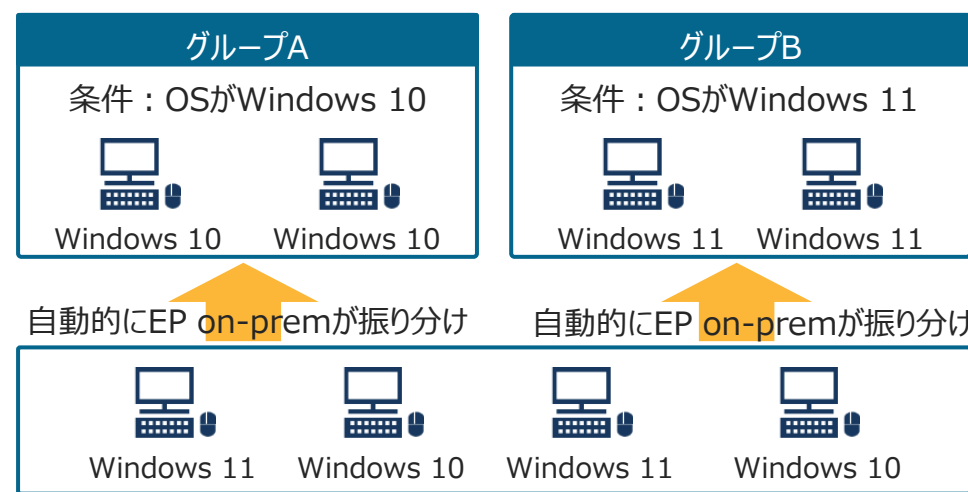
静的グループ

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。



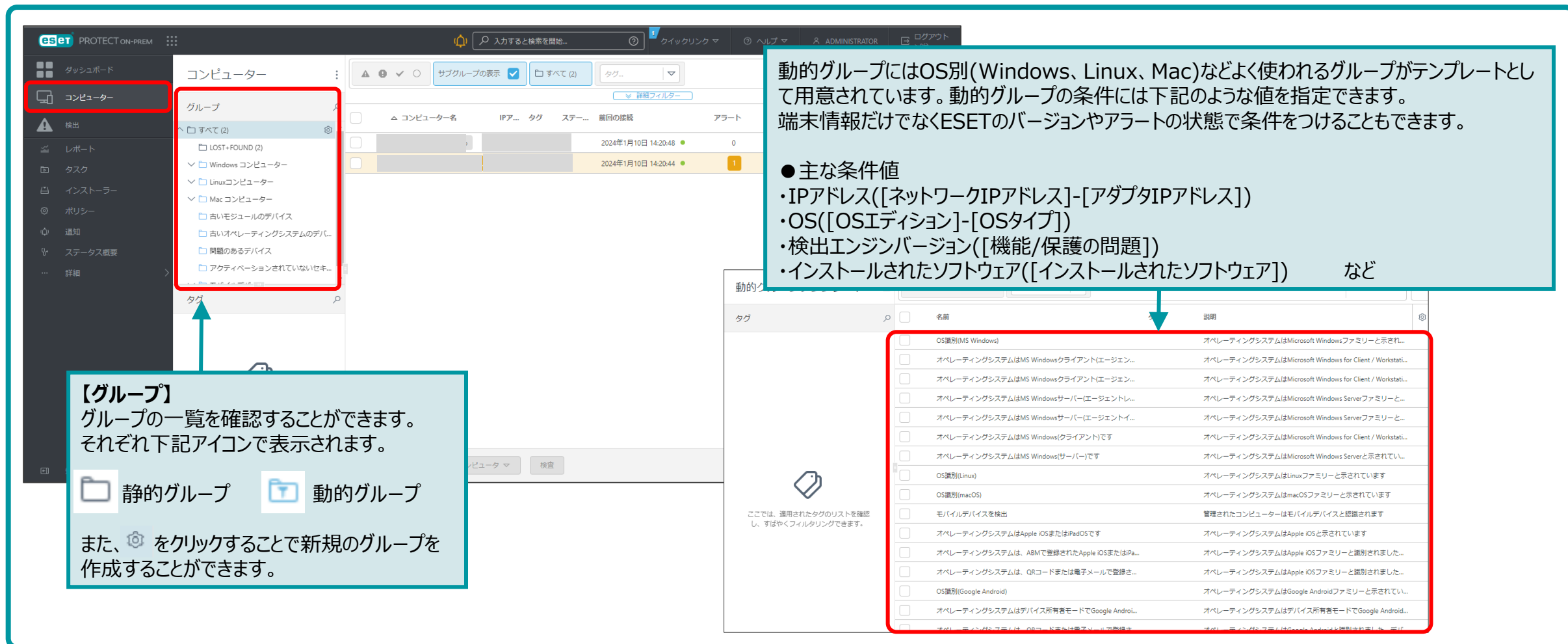
動的グループ

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。



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。



The screenshot shows the ESET Protect On-Prem interface. On the left, the 'コンピューター' (Computers) menu is highlighted. The main area displays a list of computer groups, including 'Windows コンピューター', 'Linux コンピューター', and 'Mac コンピューター'. A red box highlights the '動的グループ' (Dynamic Groups) section, which lists various OS-based and device-based conditions. A callout box explains that dynamic groups use templates and can be configured with specific conditions. Another callout box provides a list of these conditions, such as IP address, OS, and installed software. A third callout box explains how to create new groups using static or dynamic group icons.

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

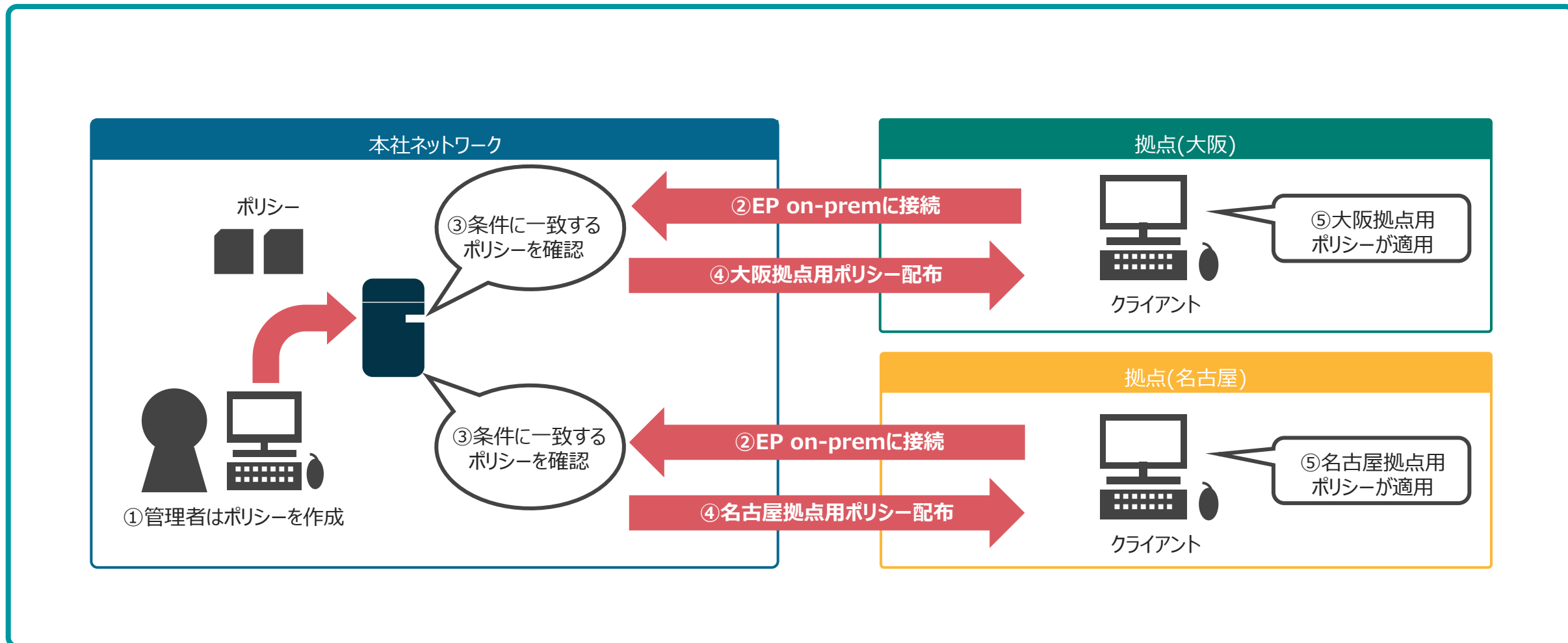
【グループ】
グループの一覧を確認することができます。それぞれ下記アイコンで表示されます。

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。

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 on-prem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。

概要

設定

割り当て先

適用中

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。

ESET Endpoint for Windows

検出エンジン

65

保護

79

リアルタイムファイルシステム保護

27

SSL/TLS

2

電子メールクライアント保護

24

Webアクセス保護

22

Q 入力すると検索を開始...

リアルタイムファイルシステム保護

8

リアルタイムファイルシステム保護を有効にする



検査するメディア

ローカルドライブ



リムーバブルメディア



ネットワークドライブ



検査のタイミング

ファイルのオープン



ファイルの作成



ファイルの実行



リムーバブルメディアブートセクターアクセス



13

パラメータ

6

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 on-prem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

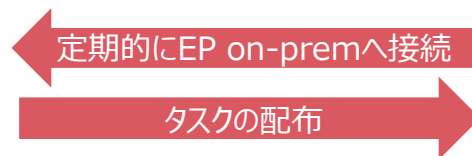
- **ESET製品の設定エクスポート**
クライアントの設定をエクスポートします。
- **オンデマンド検査**
クライアントでコンピューターの検査を実行します。
- **ソフトウェアインストール / ソフトウェアアンインストール**
ESET製品のインストール/アンインストールを実行します。
- **モジュールアップデート**
クライアントの検出エンジンをアップデートします。
- **製品のアクティベーション**
クライアントのアクティベーションを実行します。
- **コンピューターをネットワークから隔離する**
エージェント等の通信以外を遮断しクライアントを隔離します。

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。

ESET PROTECT on-prem

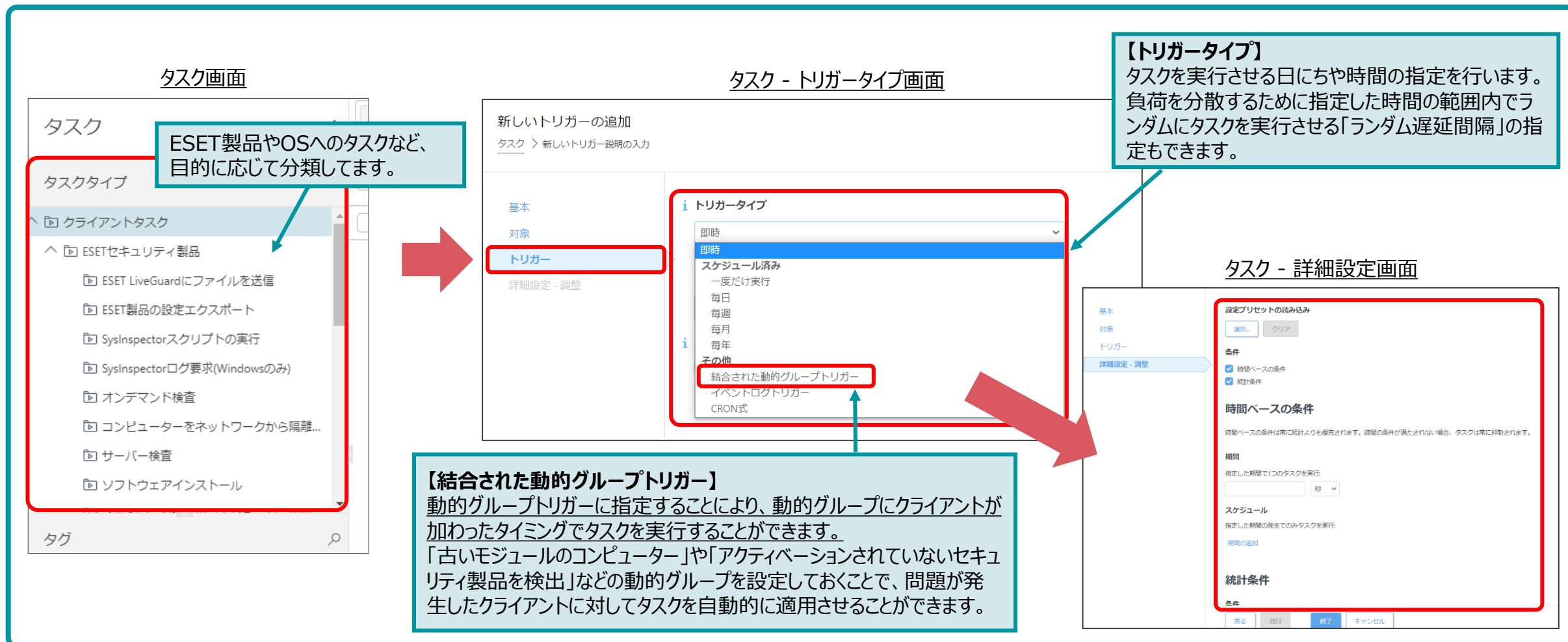
- **ESET PROTECT on-prem コンポーネントのアップグレード**
EP on-premやEMエージェントのアップグレードを実行します。
- **管理の停止**
クライアントのEM エージェントをアンインストールします。



EP on-premから受け取った
タスクを実行

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

タスクタイプ

- クライアントタスク
 - ESETセキュリティ製品
 - ESET LiveGuardにファイルを送信
 - ESET製品の設定エクスポート
 - SysInspectorスクリプトの実行
 - SysInspectorログ要求(Windowsのみ)
 - オンデマンド検査
 - コンピューターをネットワークから隔離...
 - サーバー検査
 - ソフトウェアインストール

ESET製品やOSへのタスクなど、目的に応じて分類しています。

タスク - トリガータイプ画面

新しいトリガーの追加
タスク > 新しいトリガー説明の入力

基本
対象
トリガー
詳細設定 - 調整

トリガータイプ

- 即時
- スケジュール済み
 - 一度だけ実行
 - 毎日
 - 毎週
 - 毎月
 - 毎年
- 結合された動的グループトリガー
- イベントログトリガー
- CRON式

【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

基本
対象
トリガー
詳細設定 - 調整

設定プリセットの読み込み
選択... クリア

条件
 時間ベースの条件
 統計条件

時間ベースの条件
時間ベースの条件は常に既定よりも優先されます。時間の条件が満たされない場合、タスクは常に抑制されます。

期間
指定した期間で1つのタスクを実行
[] 秒

スケジュール
指定した期間の発生でのみタスクを実行
期間の追加

統計条件
色

戻る 実行 終了 キャンセル

【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または、fullインストーラー（従来版）の選択が可能です。(EES/EEA V9.1以降、ESSW V10.0以降の場合)



•EM エージェント
•任意の設定を組み込んだ
インストーラー

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 on-prem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。



•EM エージェント
展開用ファイル

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。




•EM エージェント
展開用ファイル

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

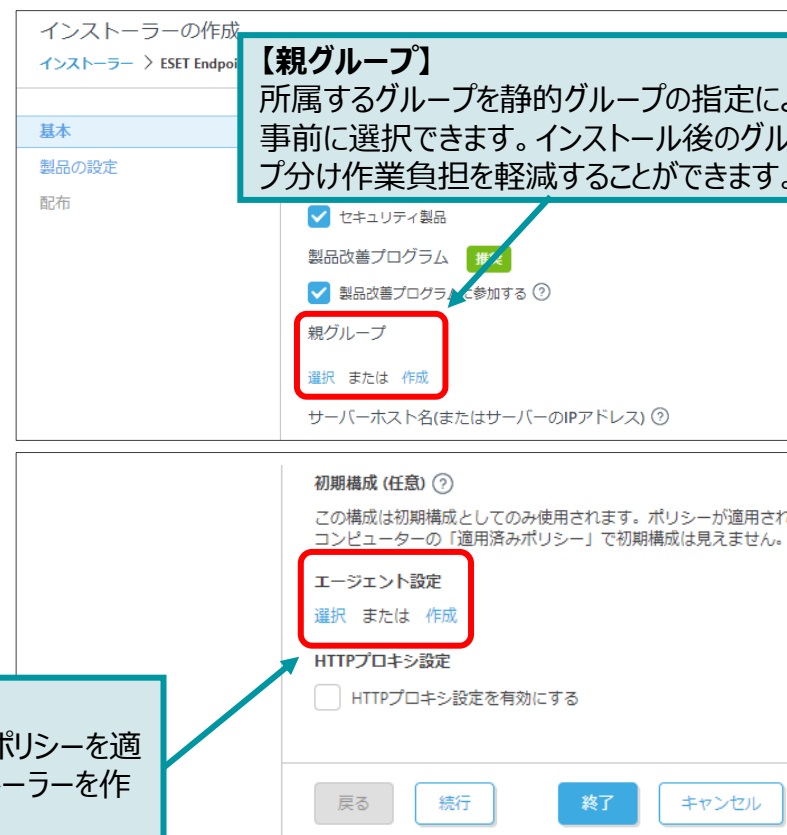


インストール画面

タグ	名前	タグ	タイプ	ステ...	製品	ポリ...	ライ...	言語	証明書
	ESET Server Security for Mi...		オールインワンインストーラー	ESET ...	3AA-...	ja_JP	CN=...		
	ESET Endpoint Security		オールインワンインストーラー	ESET ...	3AA-...	ja_JP	CN=...		

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



インストールの作成
インストーラー > ESET Endpoi

【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。

基本
製品の設定
配布

セキュリティ製品
製品改善プログラム 推奨
 製品改善プログラムに参加する ?

親グループ
選択 または 作成

サーバーホスト名(またはサーバーのIPアドレス) ?

初期構成 (任意) ?
この構成は初期構成としてのみ使用されます。ポリシーが適用されたコンピューターの「適用済みポリシー」で初期構成は見えません。

エージェント設定
選択 または 作成

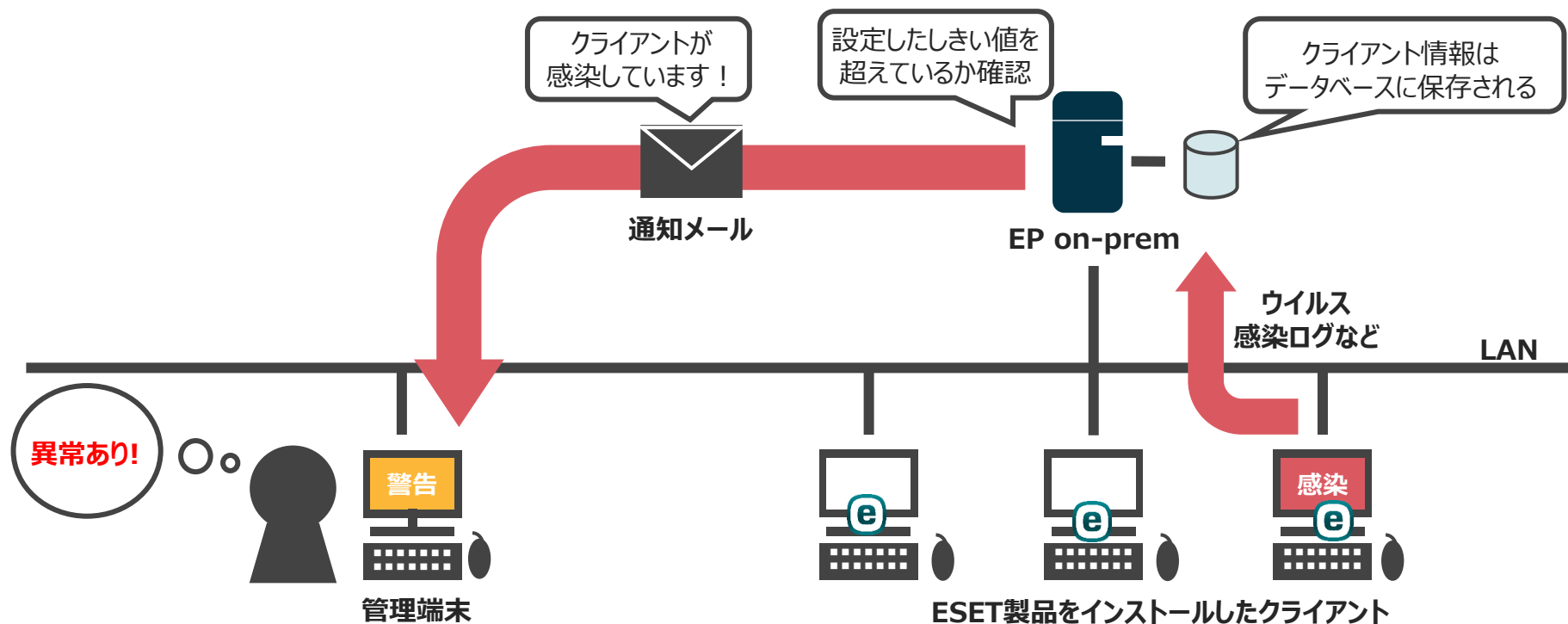
HTTPプロキシ設定
 HTTPプロキシ設定を有効にする

戻る 続行 終了 キャンセル

【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 on-prem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



通知画面のスクリーンショット。左側のナビゲーションメニューで「通知」が選択されています。中央には「通知」タブがあり、アクセスグループとタグのフィルターが設定されています。右側には通知ルールの一覧が表示されています。

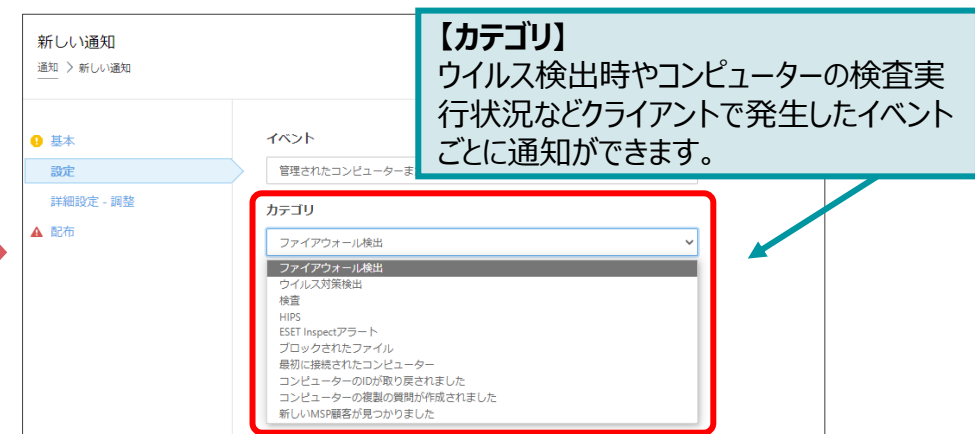
名前	タグ	有効
<input type="checkbox"/>	マルウェア発生アラート...	<input type="radio"/> 無効
<input type="checkbox"/>	ネットワーク攻撃アラ...	<input type="radio"/> 無効
<input type="checkbox"/>	コンピューターの問題ア...	<input type="radio"/> 無効
<input type="checkbox"/>	モジュールが古すぎます	<input type="radio"/> 無効
<input type="checkbox"/>	CA証明書期限切れアラ...	<input type="radio"/> 無効
<input type="checkbox"/>	ピア証明書期限切れアラ...	<input type="radio"/> 無効
<input type="checkbox"/>	ライセンス期限切れアラ...	<input type="radio"/> 無効
<input type="checkbox"/>	ライセンス使用超過アラ...	<input type="radio"/> 無効
<input type="checkbox"/>	ライセンス上限アラート	<input type="radio"/> 無効
<input type="checkbox"/>	ESET PROTECT過負荷に...	<input type="radio"/> 無効
<input type="checkbox"/>	管理クライアント未接続...	<input type="radio"/> 無効
<input type="checkbox"/>	古いESET製品のアラート	<input type="radio"/> 無効
<input type="checkbox"/>	サーバタスク失敗アラ...	<input type="radio"/> 無効
<input type="checkbox"/>	悪意のあるファイルが...	<input type="radio"/> 無効
<input type="checkbox"/>	通知の構成が無効であ...	<input type="radio"/> 無効
<input type="checkbox"/>	新しいバージョンのES...	<input type="radio"/> 無効

ここでは、適用されたタグのリストを確認し、すばやくフィルタリングできます。

【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。

通知 - 設定画面



通知設定画面のスクリーンショット。左側のメニューで「設定」が選択されています。右側には「新しい通知」の設定項目が表示されています。

【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。

カテゴリ:
ファイアウォール検出
ファイアウォール検出
ウイルス対策検出
検査
HIPS
ESET Inspectアラート
ブロックされたファイル
最初に接続されたコンピューター
コンピューターのIDが取り戻されました
コンピューターの複製の異動が作成されました
新しいMSP顧客が見つかりました

通知 - 配布画面



通知配布画面のスクリーンショット。左側のメニューで「配布」が選択されています。右側には「配布」の設定項目が表示されています。

配布:
 SNMPトラップの送信
 電子メールを送信
 Syslogの送信

受信者

電子メールアドレス	名前	すべて削除
eset@example.com	ユーザーの作成...	<input type="button" value="削除"/>

メッセージプレビュー


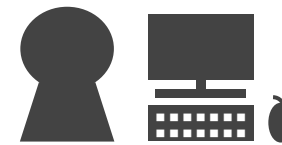
7. サーバー運用管理機能のご紹介

7-1. ユーザー管理

EP on-premのアクセス権をもつユーザーを複数作成できます。EP on-prem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 on-prem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	拠点(大阪)
<p>ユーザー名 : Administrator</p>  <p>本社管理者 ※本社および拠点(大阪)を管理</p>	<p>ユーザー名 : osaka</p>  <p>拠点(大阪)管理者 ※拠点(大阪)を管理</p>
<p>機能アクセス</p> <p>全ての機能に対して書き込み権限を付与</p>	<p>機能アクセス</p> <p>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</p>
<p>グループアクセス</p> <p>全てのグループに対してアクセスを許可</p>	<p>グループアクセス</p> <p>自拠点(大阪)のグループに対してのみ アクセスを許可</p>

- ・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	すべて
ローカルユーザー	1
マッピングされたドメインセキュリティグループ	0
静的グループアクセス	すべて
ユーザーグループアクセス	すべてのグループ

アカウント	有効
自動ログアウト(分)	1000
パスワード前回変更日時	2020 12月 18 12:59:03
パスワードの有効期限(日)	1500
パスワードの変更	必要ありません
氏名	Administrator

権限設定画面

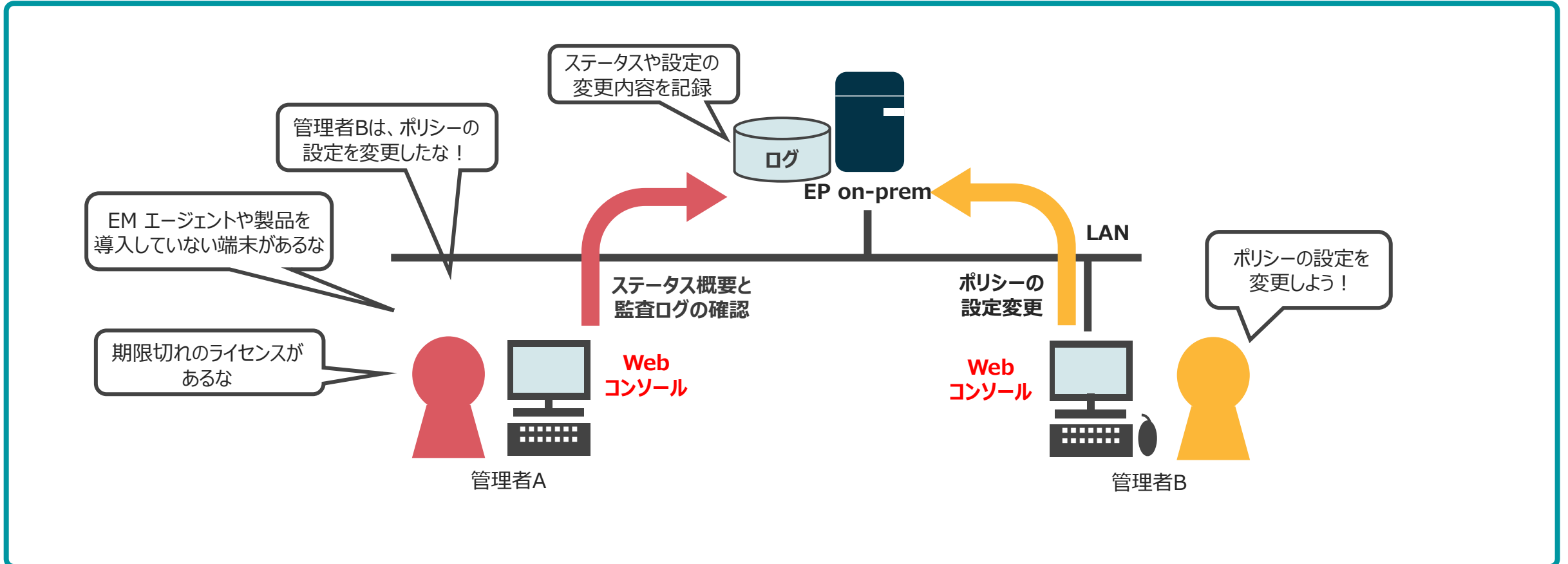
【機能アクセス】
EP on-premの各機能に対して下記の権限の設定が可能です

- 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

機能アクセス	
グループコンピューター	読み取り, 使用, 書き込み
権限設定	読み取り, 使用, 書き込み
ドメイングループ	読み取り, 書き込み
ローカルユーザー	読み取り, 書き込み
エージェント展開	使用
証明書	読み取り, 使用, 書き込み
サーバータスクとトリガー	読み取り, 使用, 書き込み
通知	読み取り, 書き込み

7-2. 監視・監査

「ステータス概要」では、EP on-prem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 on-prem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 on-premに関する詳細なステータスを確認できます。
各セクションタイトルは、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 on-prem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



発生時刻	監査ドメイン	アクション	詳細	結果	ログイン
2023年7月15日 16:35:37	コンピューター	ポリシーの設定	ポリシー「ウイルス対策・最大限のセキュリティ」をグループ「すべて」のコンピューターに適用しています。	成功	Administrator
2023年7月15日 16:17:38	サーバタスク	開始	タイプコンピューター名の変更のサーバタスク同期されたコンピューターの名前を自動的にFQDNに更新しています。	成功	Administrator
2023年7月15日 15:54:04	ライセンス	追加	公開ID '3AS-83R-72X'でライセンスを追加しています。	失敗	Administrator
2023年7月15日 15:38:32	シングルサインオン	シングルサインオン	ネイティブユーザー「Administrator」のシングルサインオントークン「*****」が発行されました。	成功	Administrator
2023年7月15日 15:38:32	ネイティブユーザー	ログイン試行	ネイティブユーザー「Administrator」を認証しています。	成功	Administrator
2023年7月15日 15:27:35	ネイティブユーザー	ログアウト	ネイティブユーザー「Administrator」をログアウトしています。	成功	Administrator
2023年7月15日 15:18:12	サーバタスク	開始	タイプコンピューター名の変更のサーバタスク同期されたコンピューターの名前を自動的にFQDNに更新しています。	成功	Administrator
2023年7月15日 15:03:35	コンピューター	作成	紛失と検出グループに検出されたコンピューター「desktop-5daudfd」を作成しています。	成功	Administrator
2023年7月15日 14:57:46	保存されたインストーラー	読み取り	オールインワンインストーラー「EES」を生成しています。	成功	Administrator
2023年7月15日 14:57:41	保存されたインストーラー	作成	保存されたインストーラー「EES」を作成しています。	成功	Administrator
2023年7月15日 14:50:37	保存されたインストーラー	読み取り	オールインワンインストーラー「ESSW」を生成しています。	成功	Administrator
2023年7月15日 14:50:32	保存されたインストーラー	作成	保存されたインストーラー「ESSW」を作成しています。	成功	Administrator
2023年7月15日 14:40:08	シングルサインオン	シングルサインオン	ネイティブユーザー「Administrator」のシングルサインオントークン「*****」が発行されました。	成功	Administrator
2023年7月15日 14:40:08	ネイティブユーザー	ログイン試行	ネイティブユーザー「Administrator」を認証しています。	成功	Administrator
2023年7月15日 14:28:16	エンドユーザー使用	承認	グループ「すべて」のエンドユーザー使用許諾契約書「EULA-PRODUCT-AGENT」バージョン「3537.0.0」を承認しています。	成功	system
2023年7月15日 14:28:15	静的グループ	ポリシーの設定	ポリシー「EULA」をグループ「\」の静的グループ「すべて」に設定しています。	成功	system

「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