

**オンプレミス型セキュリティ管理ツール
ESET PROTECT on-prem V13
機能紹介資料**

第1版
2026年1月13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)
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 V13)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 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 V13.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	12.X / 11.X / 10.X / 9.X
ESET Endpoint Security for macOS	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 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
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	12.X / 11.X / 10.2 / 10.3 / 9.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	12.X / 11.X / 10.X / 9.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 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などウィルス・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

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 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。

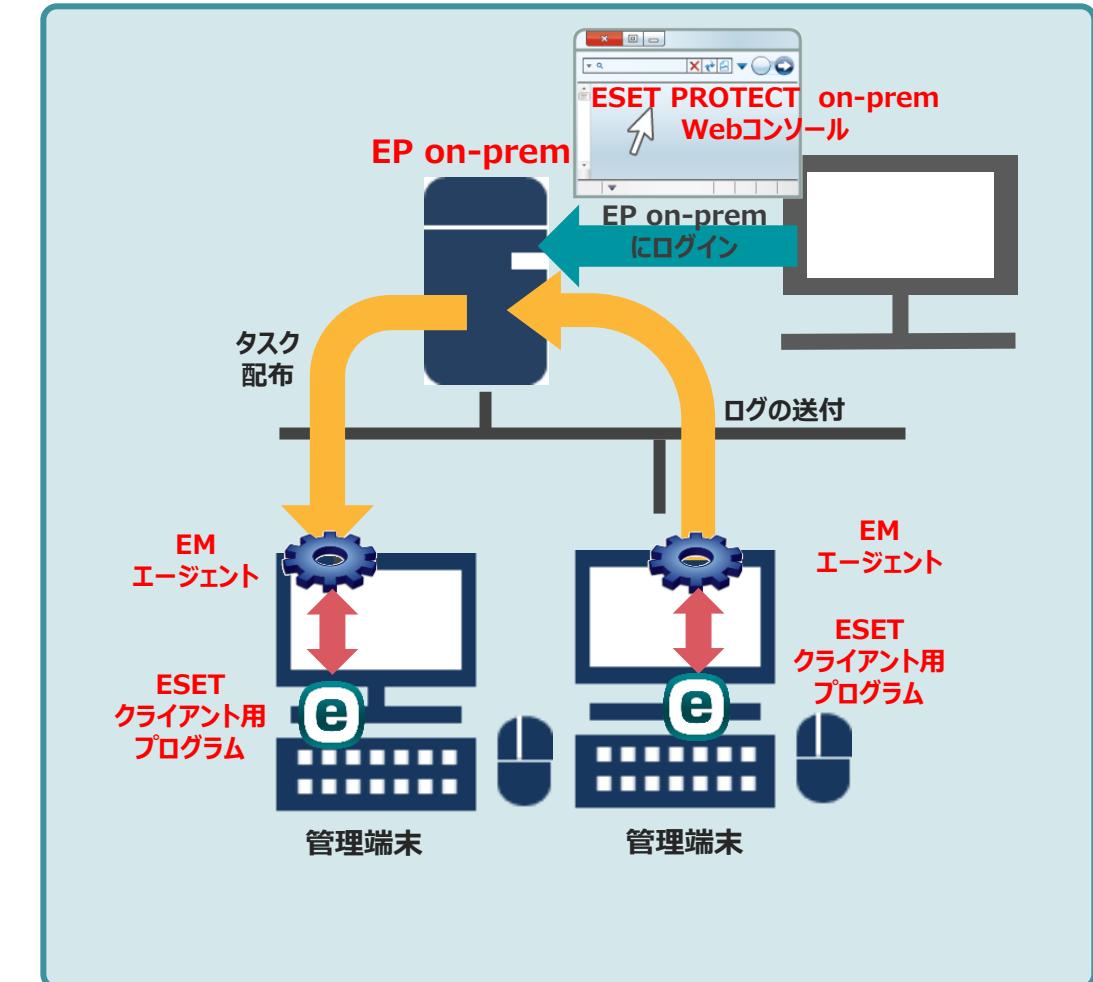
ESET PROTECT on-prem Webコンソール

WebコンソールはWebベースのインターフェースであり、ブラウザーを使用してEP on-prem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 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

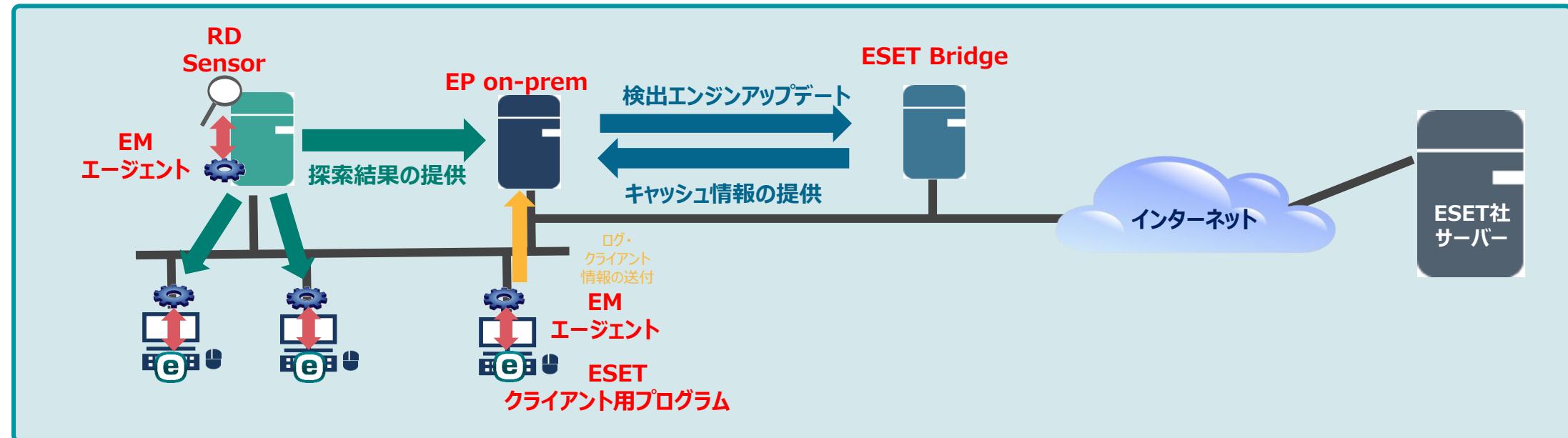
以下のコンポーネントは任意で構成します。

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を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2016、2017、2019、2022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 ※1	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 V13 (Windows版)	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 V13 (Linux版)	MySQL(※3) 8.0 / 8.1 / 8.4 / 9	制限なし

※ 1 ここではESET on-prem V13.0をご利用の場合に利用可能なデータベースをご案内しております。他のバージョンをご利用の際は下記をご参照ください。

https://eset-support.canon-its.jp/faq/show/91?site_domain=business

※ 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 ※1	オペレーティングシステム名
EP on-prem V13 (Windows版)	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 V13 (Linux版)	Rocky Linux 9 (64bit)
	Ubuntu 20.04, 22.04, 24.04 (64bit)
	Debian 11, 12, 13 (64bit)
	RHEL Server 9, 10(64bit)

※ 1 ここではESET on-prem V13.0をご利用の場合のサポートOSをご案内しております。他のバージョンをご利用の際は下記をご参照ください。
https://eset-support.canon-its.jp/faq/show/4926?site_domain=business

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/4/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 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。



[検索ツール]
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。

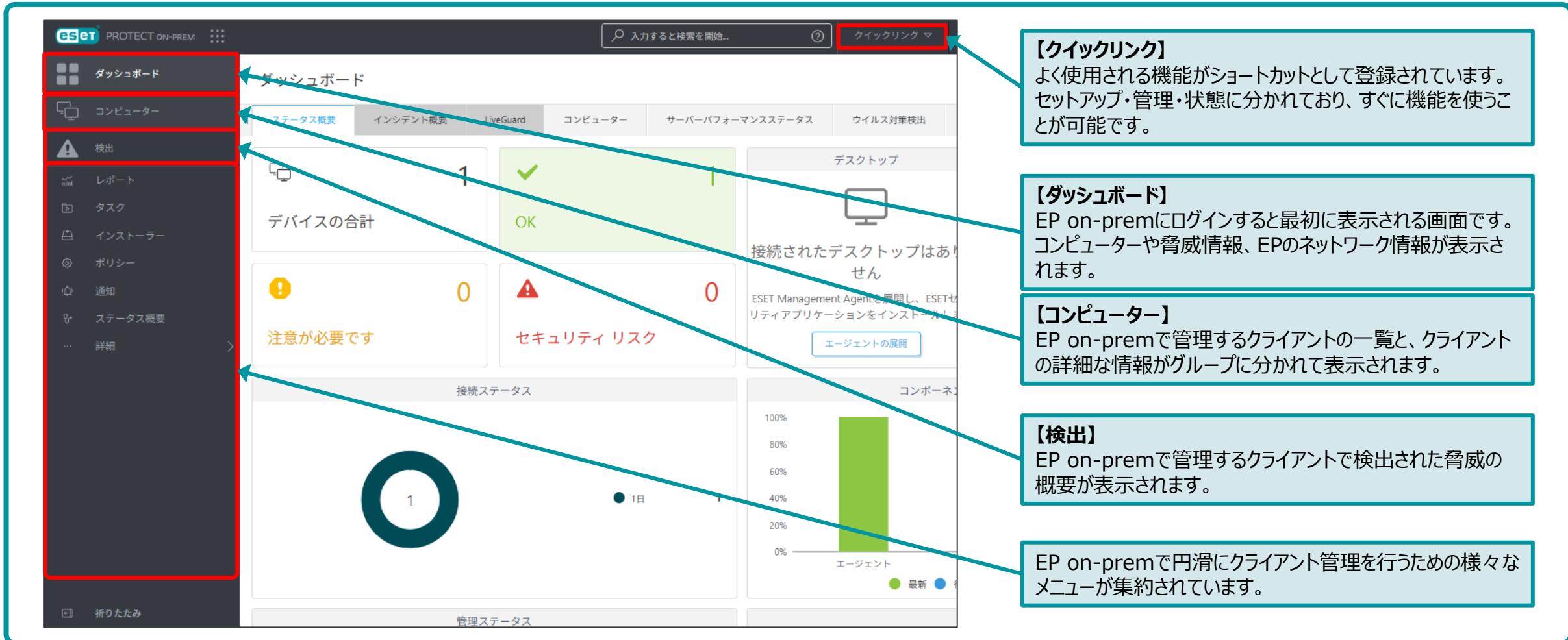
[メインセクション]
ESET PROTECT on-premで操作可能な各種メニューが表示されます。

メインセクションは折り畳みできます。

メインセクションで選択したものに応じて、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。

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・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います。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】
 ウィ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イメージを開くためのインストーラーパッケージを作成できます。

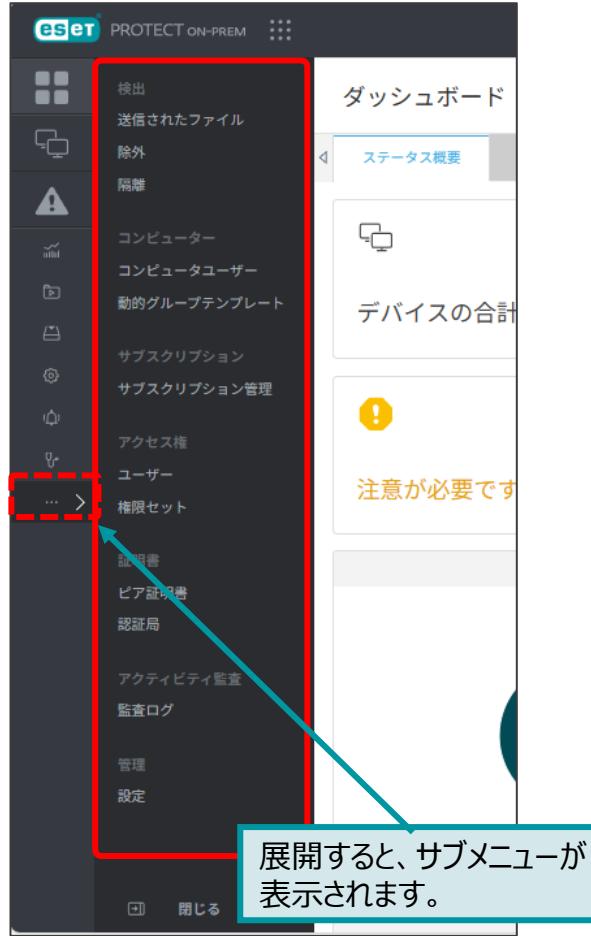
【詳細】
 EP on-premに関するさらに詳細なメニューが開きます。

【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。

【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。

【サブスクリプション】

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】

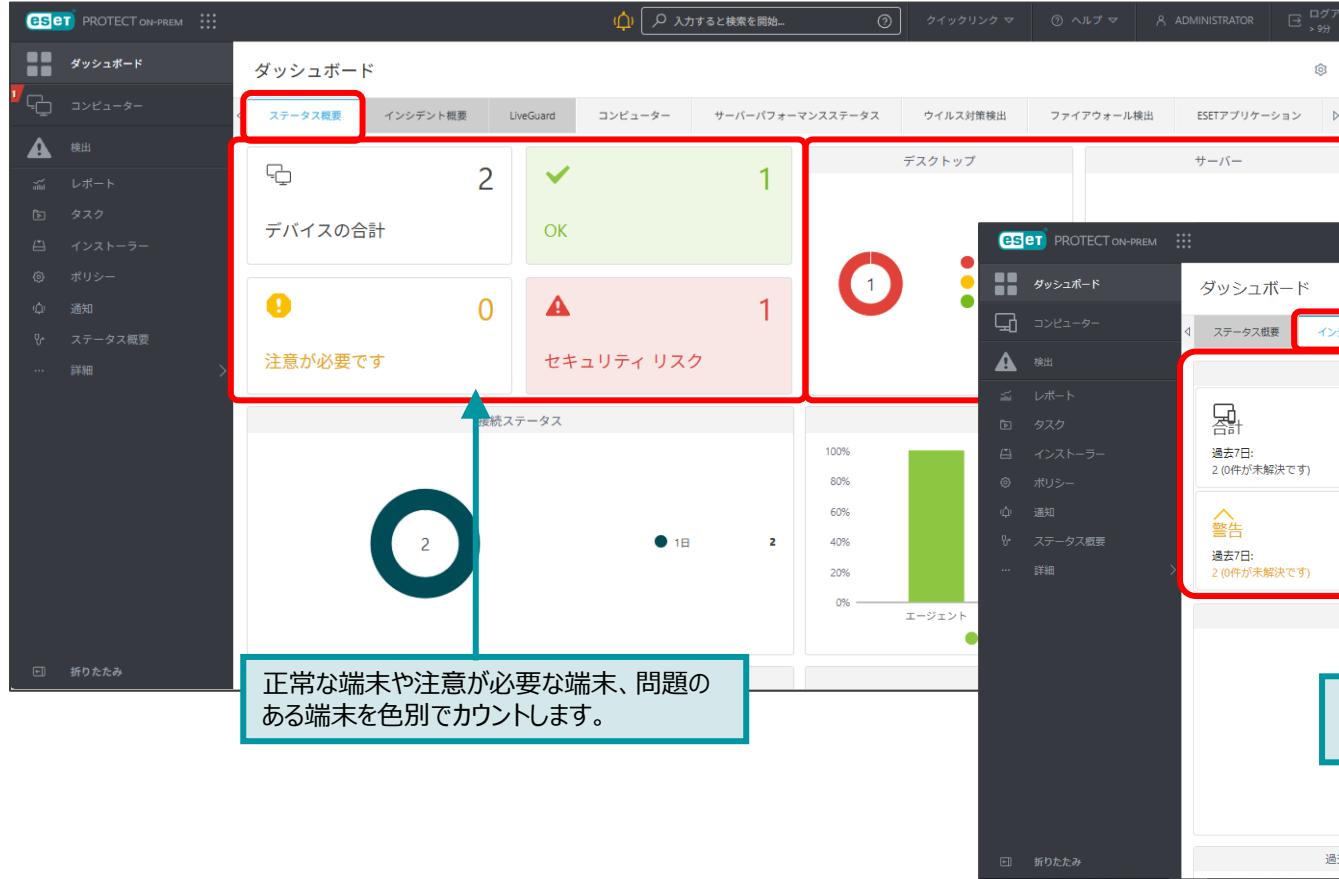
EP on-premサーバーのアップデート間隔や、EP on-premサーバー本体の設定ができます。

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)



デバイスの合計	
2	OK

セキュリティ リスク	
0	注意が必要です

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)



重大度別未解決の検出	
合計	0
過去7日:	2 (件が未解決です)

警告	
0	重大
過去7日:	2 (件が未解決です)

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

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)

eset PROTECT ON-PREM

ダッシュボード

コンピューター

検出

レポート

タスク

インストーラー

ポリシー

通知

ステータス概要

詳細

折りたたみ

ダッシュボード

入力すると検索を開始...

クイックリンク

ヘルプ

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。

コンピューターステータス概要

セキュリティリスク

OK 2

作成済み 0分前

上位のコンピューターの問題

保護設定が失...

1

作成済み 0分前

前回のコンピューター接続

1日 2

作成済み 0分前

前回の更新

ウイルス対策検出

新しいレポートテンプレート

IP4リファネットのアラートが発生

IP4リファネットのアラートが発生

アラートが発生する上位のユーザー

エージェントレス監視マシンの回復

スキャナーバージョンが既に最新

過去7日間に検出イベントがなかった場合

過去7日間で未解決の内蔵

過去7日間に実行された接続

過去7日間に検出イベントがなかった場合

過去7日間に実行された接続

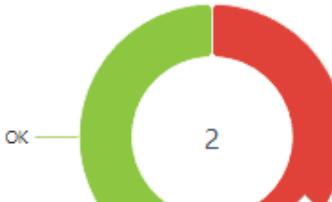
過去7日間に検出イベントがなかった場合

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。

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

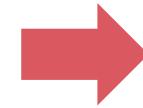


OK セキュリティリスク 2

作成済み 0分前

表示 詳細情報

“重大”のみ “セキュリティリスク”のみ



レポート: ドリルダウン - 詳細情報

サーバー名 [REDACTED]

生成ロケーション
2025年12月19日 16:35:21 (UTC+09:00)

レコード数
1

フィルター
フィルター数: 3

重大度	発生時刻	コンピューターの一覧	静的グループ名	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	2025年12月19日 16:26:37	セキュリティリスク	1名				



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 ここをクリックすると、リストを表示します
未解決の検出数 0

前回の接続時間 2022年7月28日 10:13:11

前回の検査時刻 n/a

検出エンジン 25374 (20220603)

モジュールステータス 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。

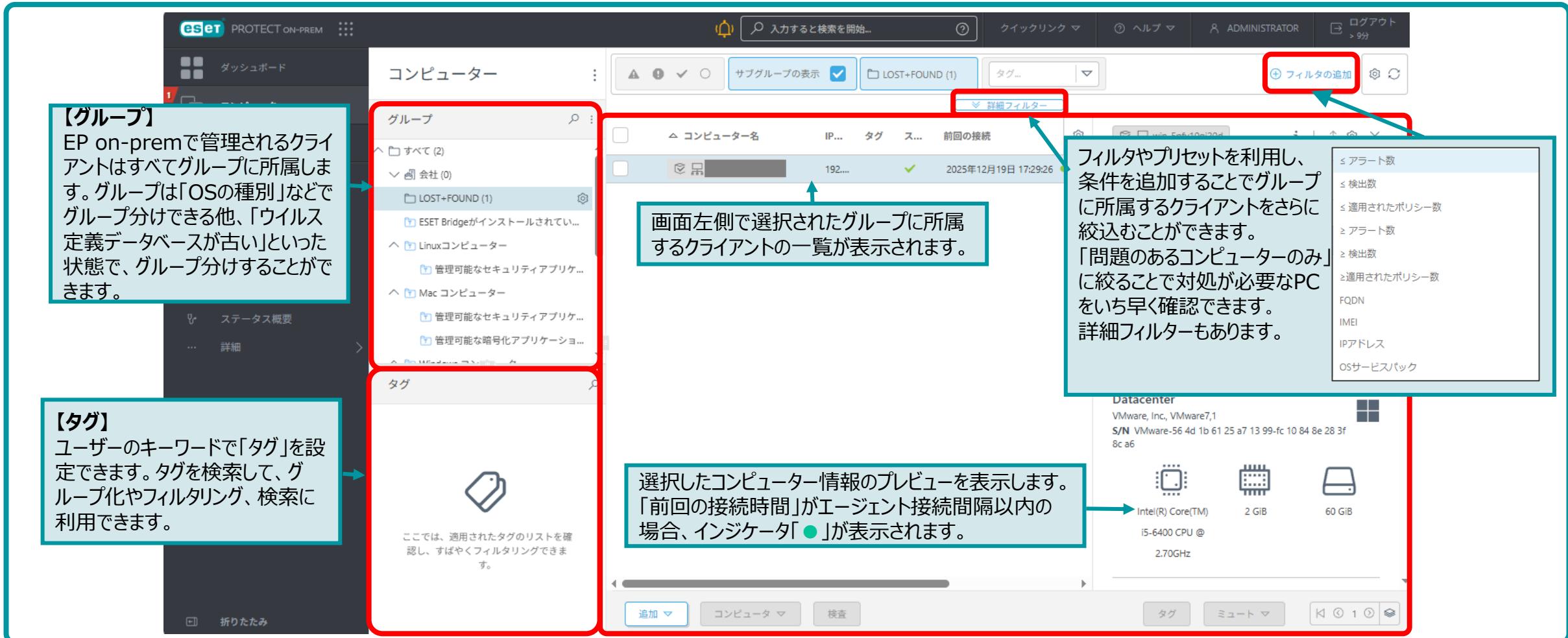
※通常、ドリルダウンは複数の階層で表示されます。

©Canon Marketing Japan Inc.

20

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。

グループ

- すべて (2)
 - 会社 (0)
 - LOST+FOUND (1)
 - ESET Bridgeがインストールされてい...
- Linuxコンピューター
- Macコンピューター

タグ

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。

△コンピューター名 IP... タグ ス... 前回の接続

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。

追加 ▾ コンピュータ ▾ 検査

詳細フィルター
+ フィルタの追加

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。

Datacenter

VMware, Inc., VMware7.1
S/N VMware-56 4d 1b 61 25 a7 13 99-fc 10 84 8e 28 3f
8c a6

Intel(R) Core(TM)
i5-6400 CPU @
2.70GHz
2 GB
60 GB

©Canon Marketing Japan Inc.

21

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。

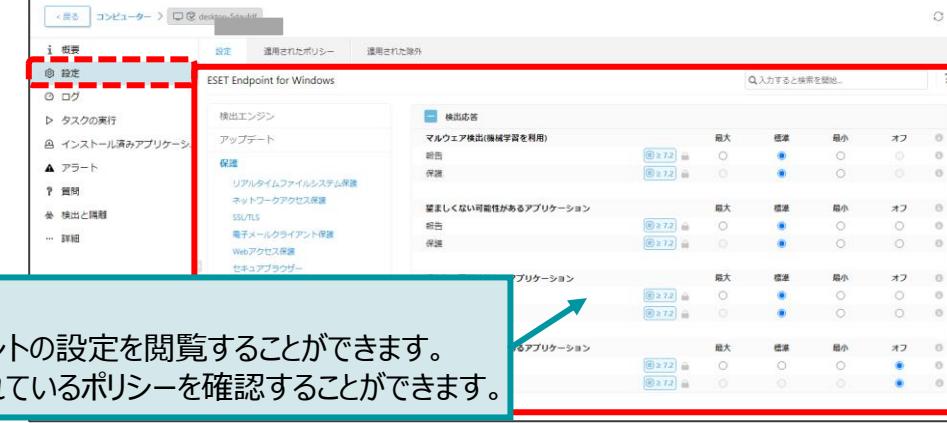
コンピューター - 詳細画面 - 概要



【詳細】-[ハードウェア]

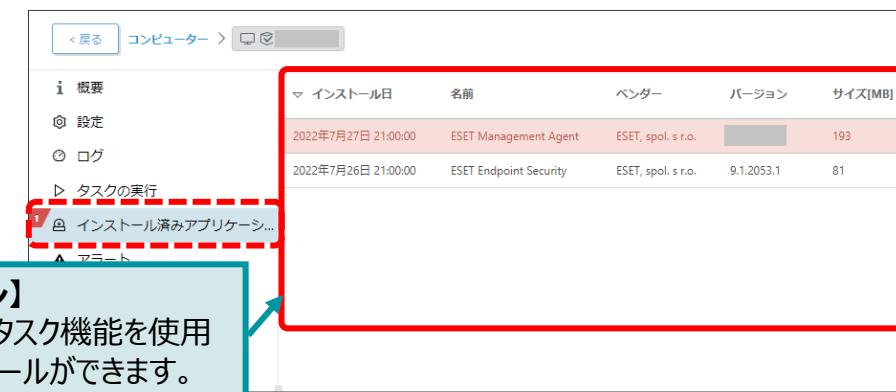
コンピューターの情報やESETの情報について、概要がまとめられています。ハードウェアでは、デバイスのRAM、ストレージ、プロセッサーなどハードウェアの詳細情報を確認できます。

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。

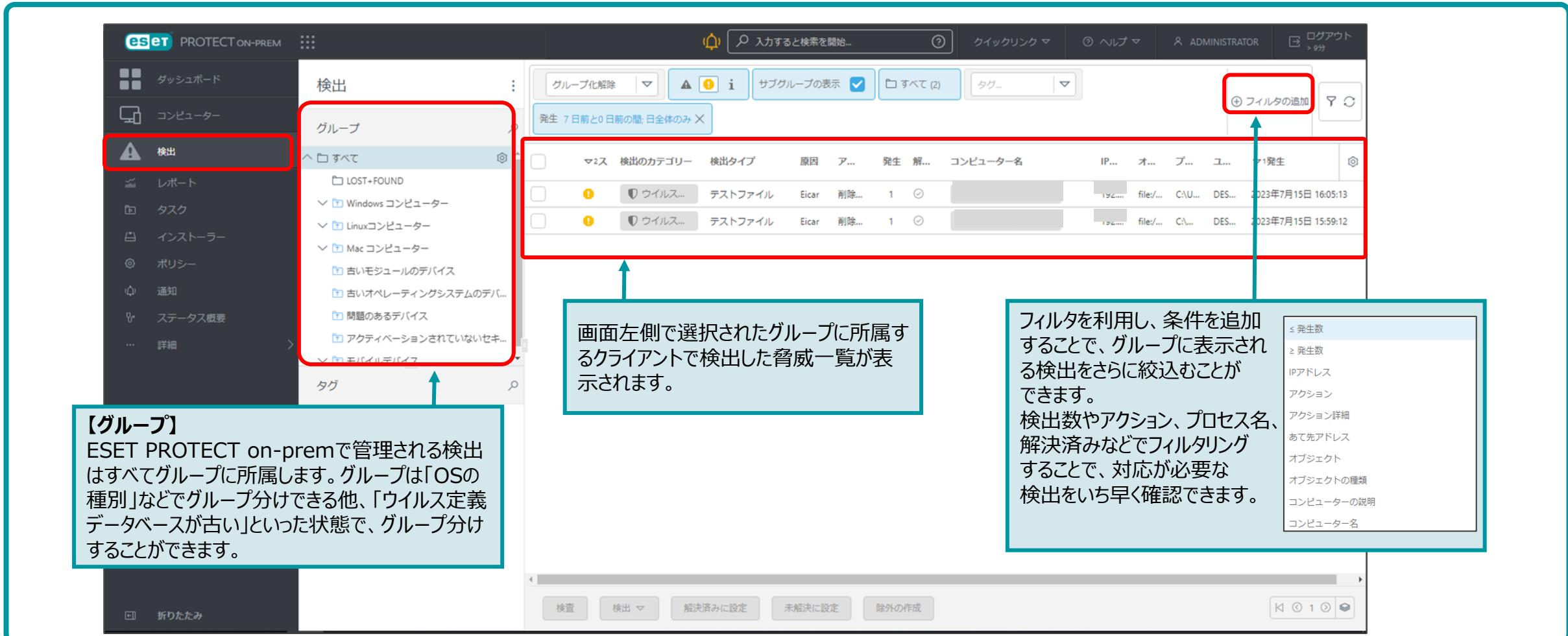
コンピューター - 詳細画面 - インストール済みアプリケーション



【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。



【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。

5-3. 検出 (脅威の詳細)

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

概要

ウイルス対策
テストファイル

発生
発生
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 17:11:31

再起動する必要がありま
す
す

詳細を表示

タグを選択

FQDN
前回の検出時間
未解決の検出
アラート
親グループ

2022年7月28日 12:24:07
0
アラートなし
すべて/LOST+FOUND

ファイル

ハッシュ
名前
検出タイプ
オブジェクトの種類
Uniform Res
(URI)

検出

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
初回
前回

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

ファイル

ハッシュ
名前
検出タイプ
オブジェクトの種類
Uniform Resource Identifier (URI)
プロセス名
ユーザー

339586C81F287382DE72602F7968642F14140
Eicar
テストファイル
ファイル
file:///C:/Users/taguchi/AppData/Local/Microsoft/Windows/NetCache/Low/E/GZ320CV/G/eicar[1].com
C:\Program Files (x86)\Internet Explorer\explorer.exe
WIN-F3JQEQMV9taguchi

検索
スキヤナ
リアルタイムファイルシステム保護

完了時間
アクション
アクションエラー

削除によって駆除されました

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。

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。

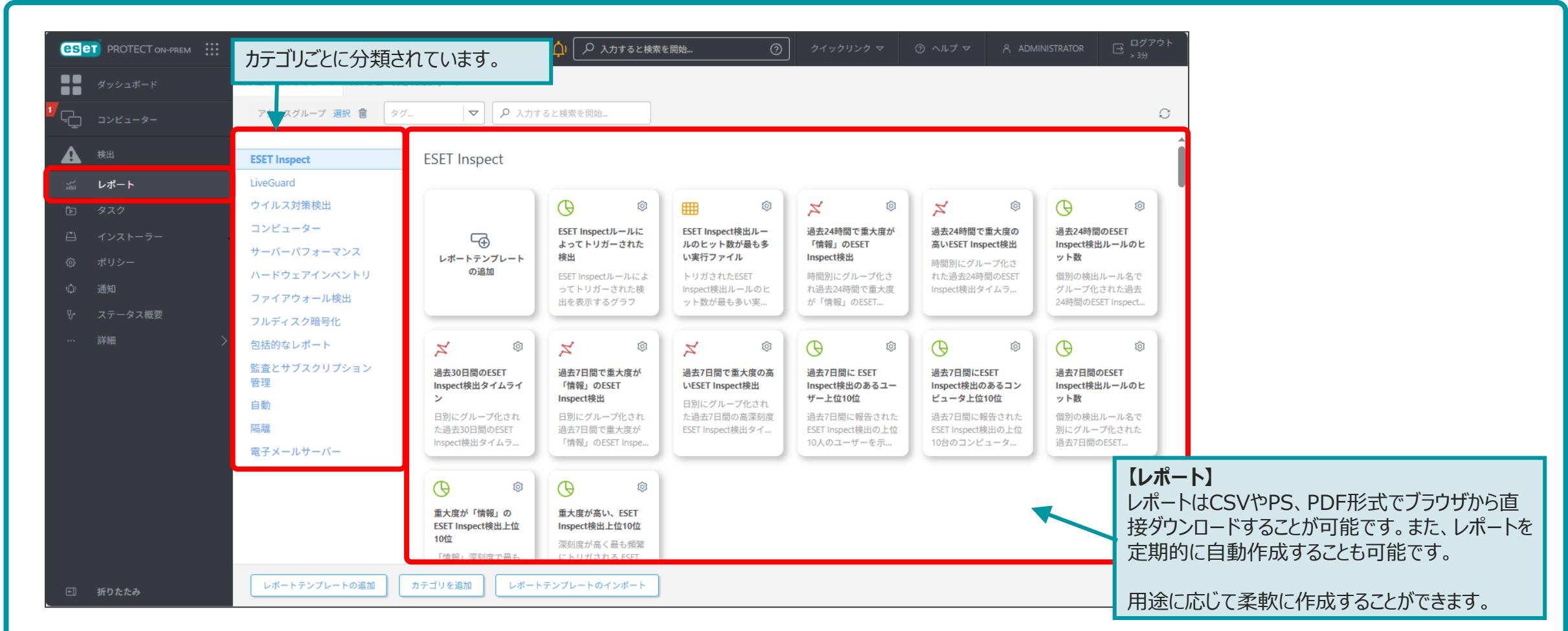
[世界での観測]
ESET LiveGrid®で収集した情報から脅威を評価します。
LiveGridでの評価や発生数、初回に確認された時期が確認できます。評価は色別に脅威レベルが分かれています。[赤 : 悪意] [黄 : 不審] で表示されます。

[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。



The screenshot shows the ESET PROTECT ON-PREM interface. On the left, the navigation menu is visible, with the 'Report' item highlighted. A red box surrounds the 'Report' section, which contains a list of report templates. One template, 'ESET Inspect', is expanded, showing various report cards. A blue box highlights the message 'カテゴリごとに分類されています。' (Categorized by category). A blue arrow points from this message to the 'Report' section in the navigation menu. Another blue arrow points from the 'Report' section in the navigation menu to the expanded 'ESET Inspect' section.

【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。

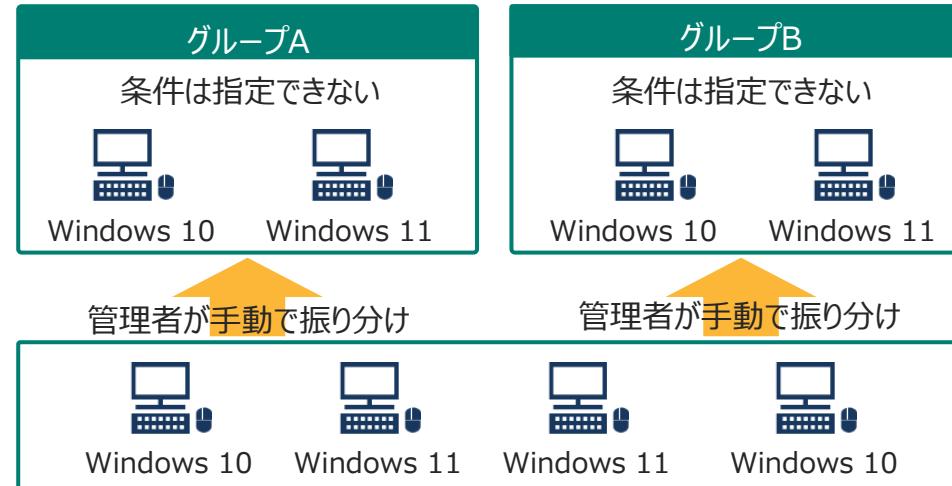
用途に応じて柔軟に作成することができます。

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。

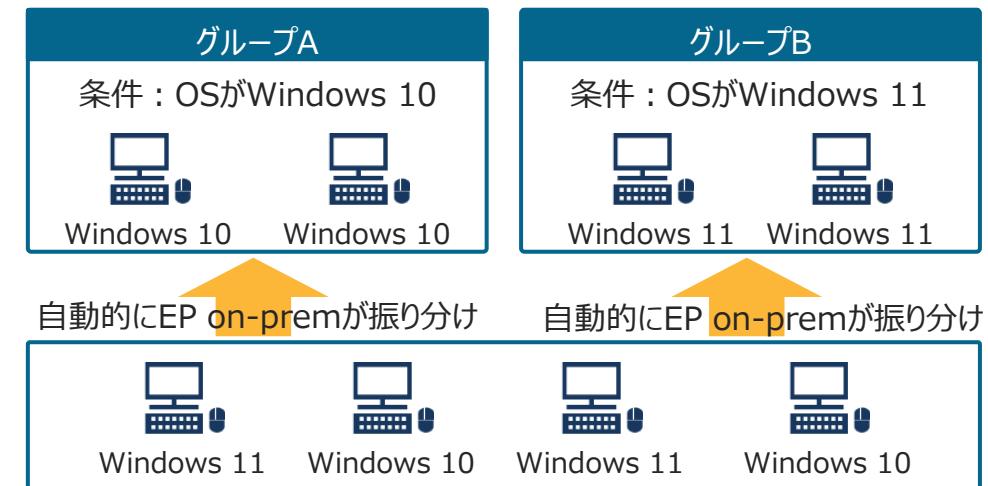
静的グループ

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。



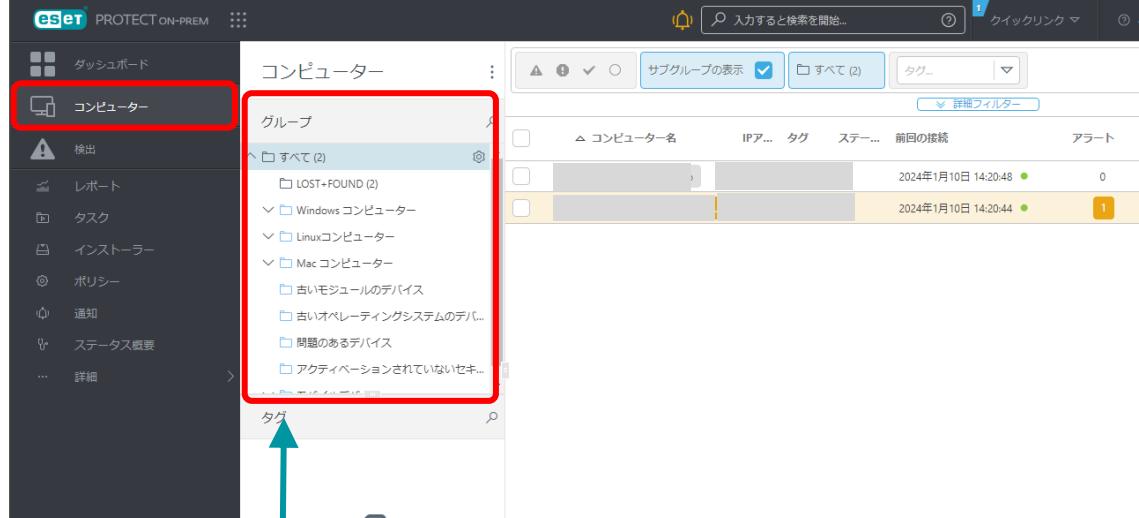
動的グループ

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。



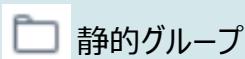
6-2. グループ

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。



【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。





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])

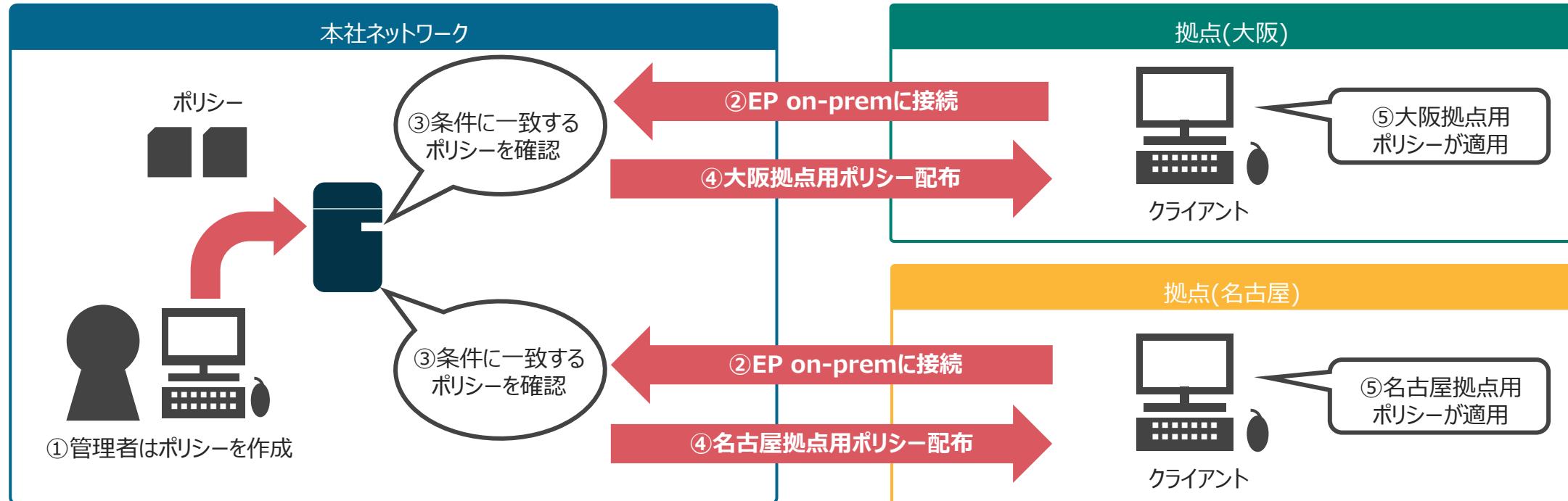
など



テンプレート名	テンプレート説明	タグ
OS識別(MS Windows)	オペレーティングシステムはMicrosoft Windowsファミリーと示されています。	
オペレーティングシステムはMS Windowsクライアント(エージェント)	オペレーティングシステムはMicrosoft Windows for Client / Workstation。	
オペレーティングシステムはMS Windowsクライアント(エージェント)	オペレーティングシステムはMicrosoft Windows for Client / Workstation。	
オペレーティングシステムはMS Windowsサーバー(エージェント)	オペレーティングシステムはMicrosoft Windows Serverファミリーと特定されています。	
オペレーティングシステムはMS Windowsサーバー(クライアント)	オペレーティングシステムはMicrosoft Windows for Client / Workstation。	
オペレーティングシステムはMS Windows(サーバー)	オペレーティングシステムはMicrosoft Windows Serverと示されています。	
OS識別(Linux)	オペレーティングシステムはLinuxファミリーと示されています。	
OS識別(macOS)	オペレーティングシステムはmacOSファミリーと示されています。	
古いオペレーティングシステムを検出	オペレーティングシステムは、より最新の更新が使用可能ですがまだ古い。	
アプリケーションモジュールが最新ではありません	セキュリティアプリケーションは、そのモジュールが最近アップデートされました。	
コンピューターのアイドル状態を検出	エージェントは、コンピュータがアイドル状態にあることを示しています。	
デバイスが問題を報告しました	ESET Management Agentは、オペレーティングシステムまたは管理対象デバイスが問題を報告しました。	
アクティベーションされていないプラットフォームモジュール	プラットフォームモジュールは、アクティベーションされていません。	

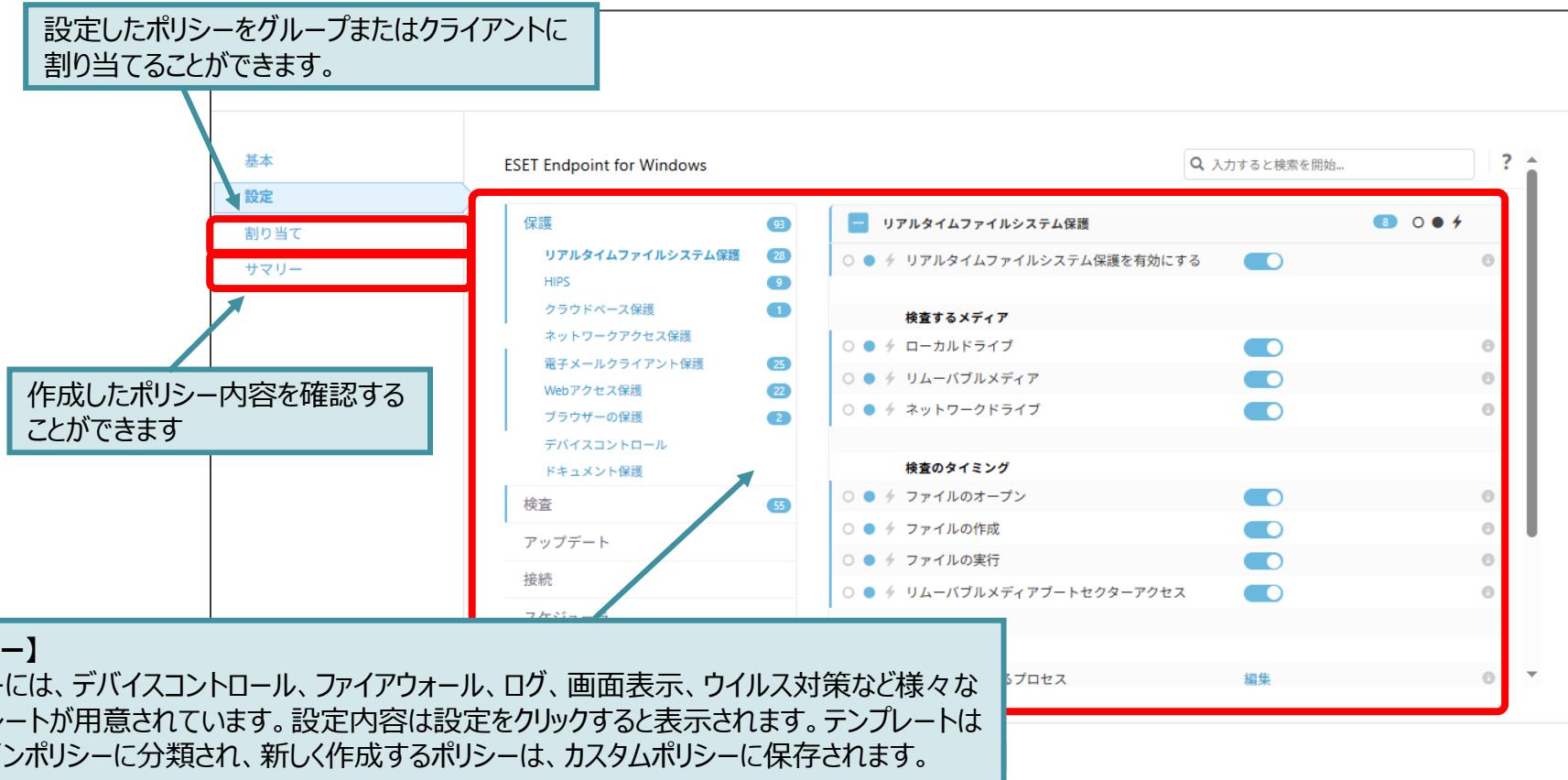
6-3. ポリシー

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。



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。
- ・モジュール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



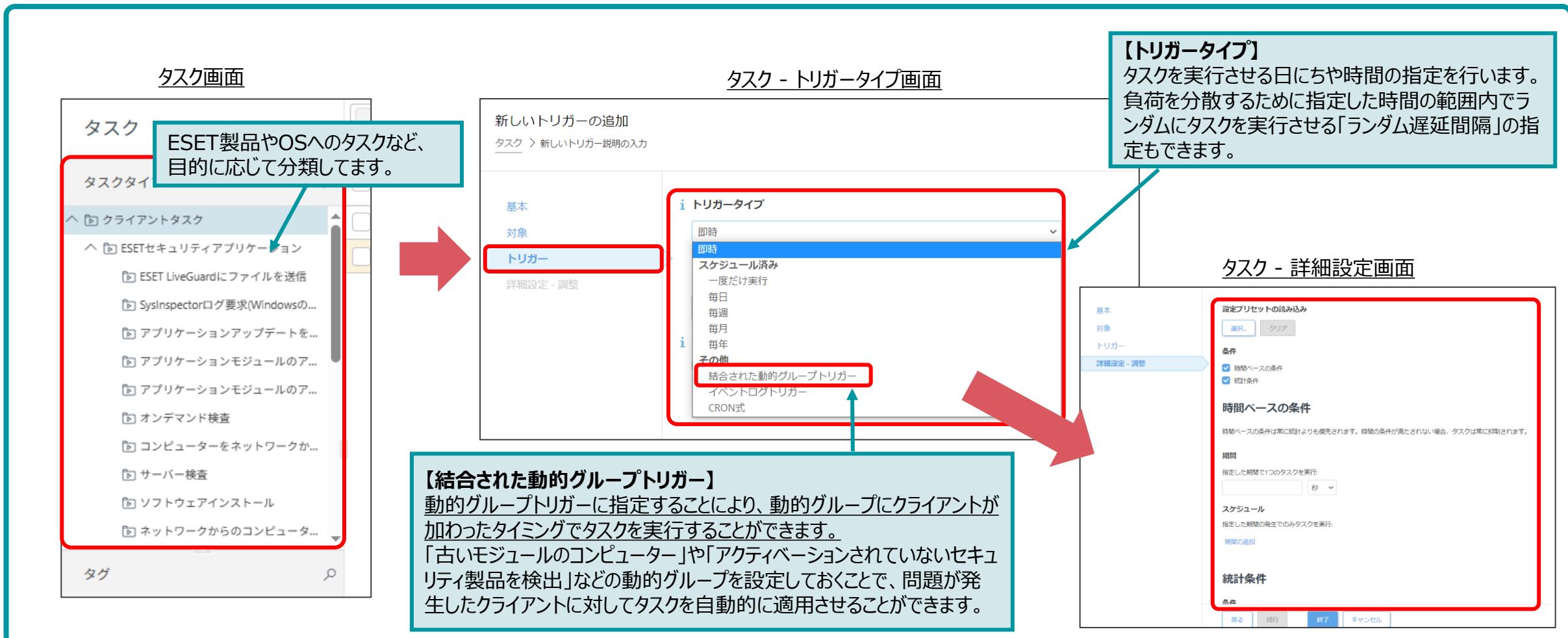
クライアント

EP on-premから受け取った
タスクを実行

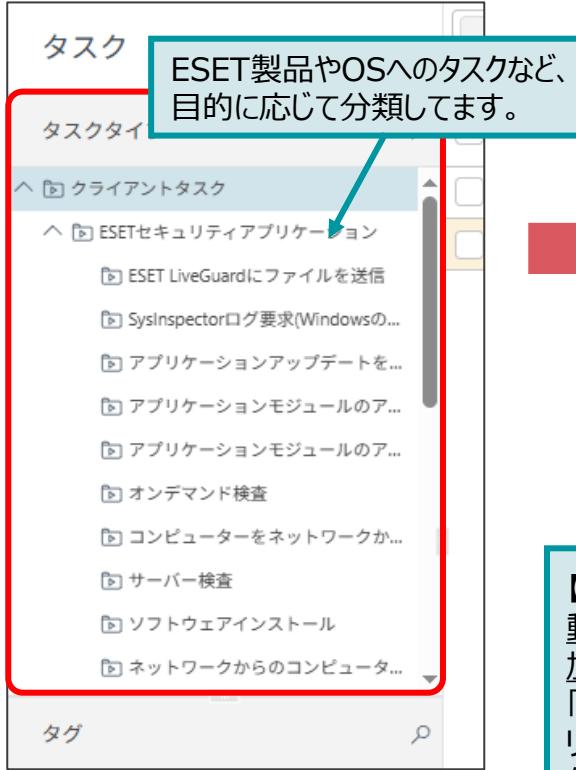


6-4. タスク

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。

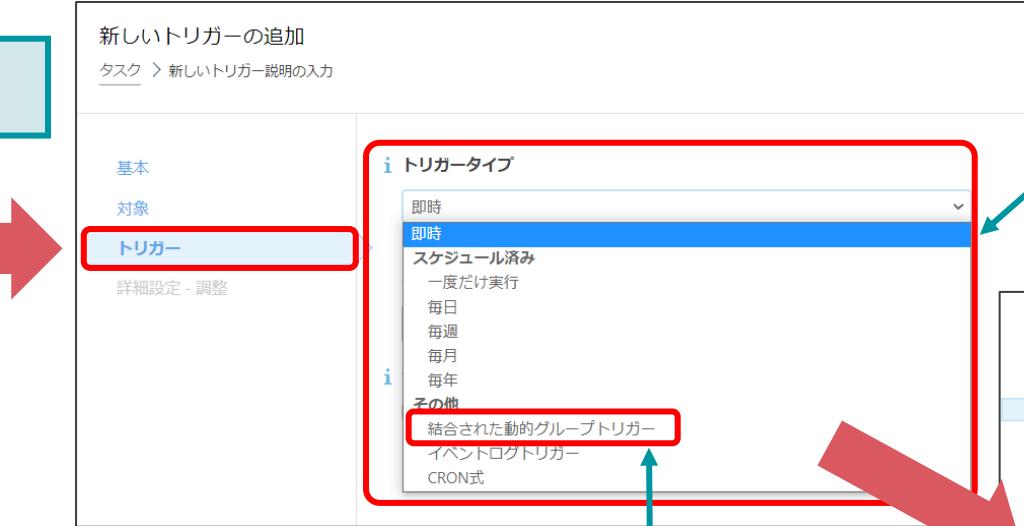


タスク画面



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



【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。

【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。

タスク - 詳細設定画面



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。



- 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。

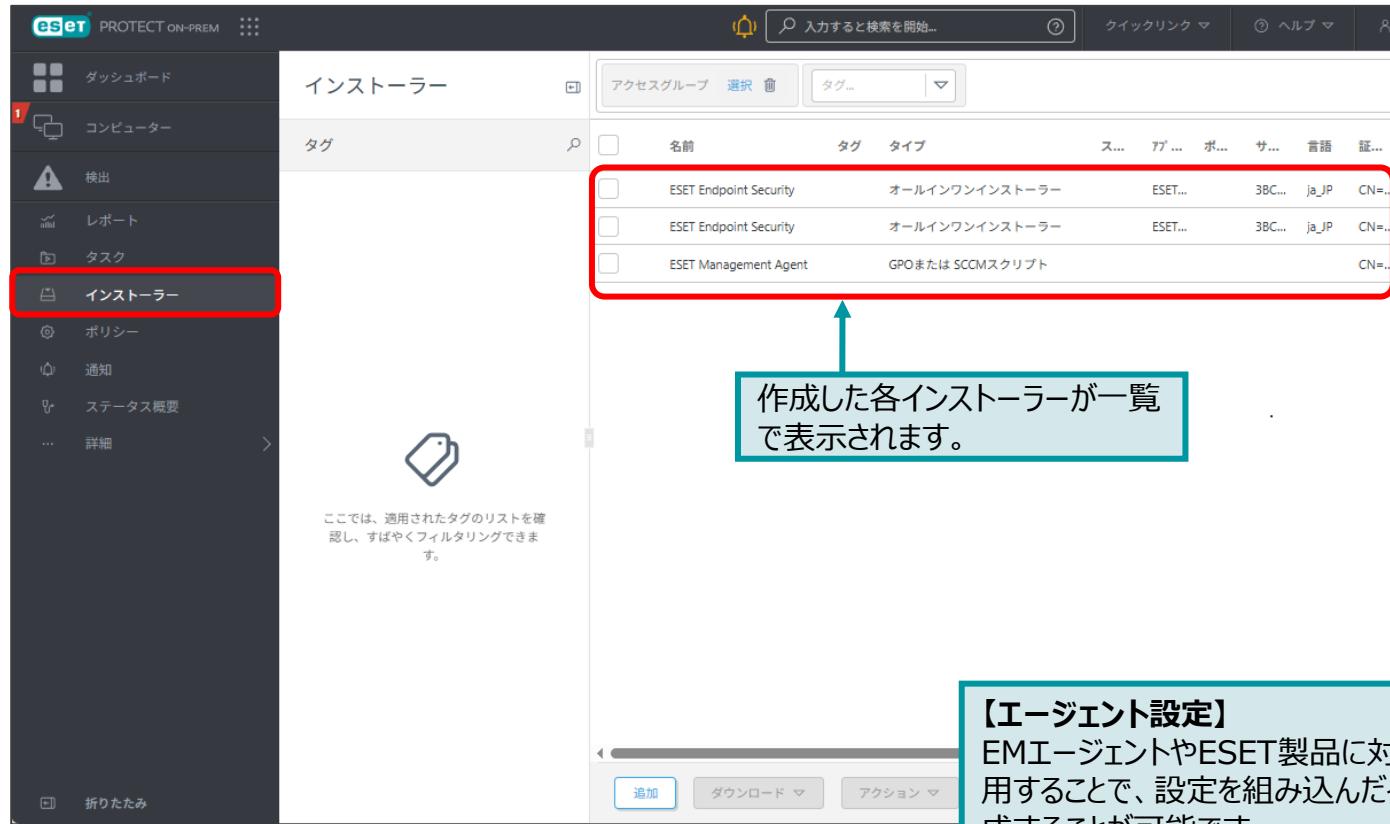


- EM エージェント展開用ファイル

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います。

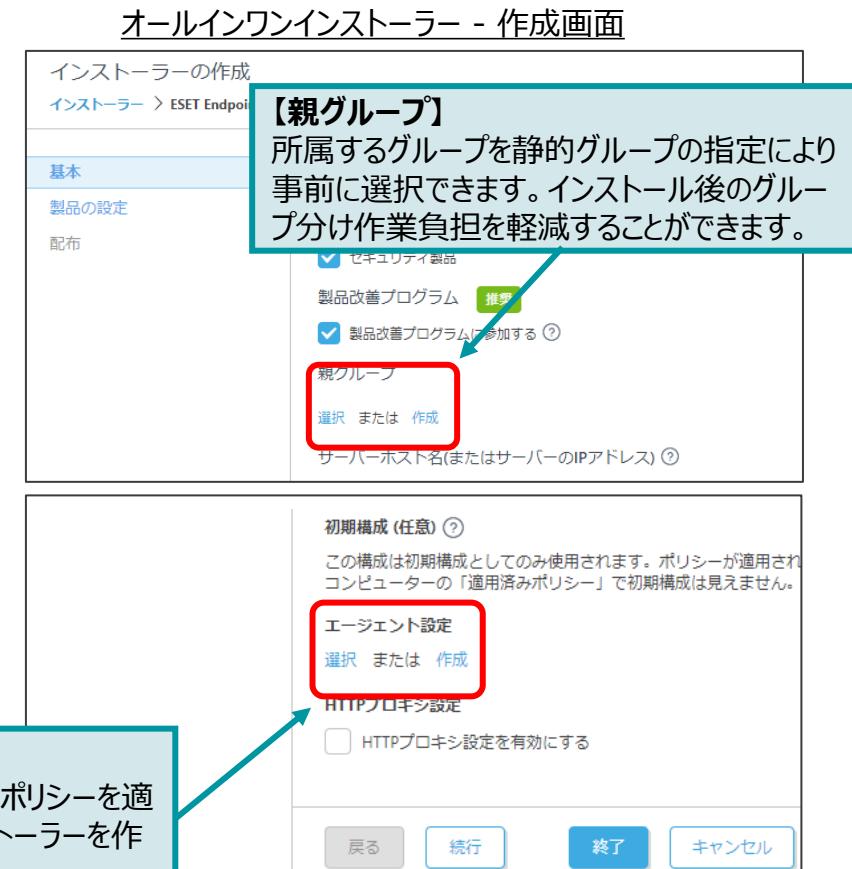
インストーラー画面



名前	タイプ	ス...	ア...	ボ...	サ...	言語	証...
ESET Endpoint Security	オールインワンインストーラー	ESET...	3BC...	ja_JP	CN=..		
ESET Endpoint Security	オールインワンインストーラー	ESET...	3BC...	ja_JP	CN=..		
ESET Management Agent	GPOまたはSCCMスクリプト				CN=..		

【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できます。

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。

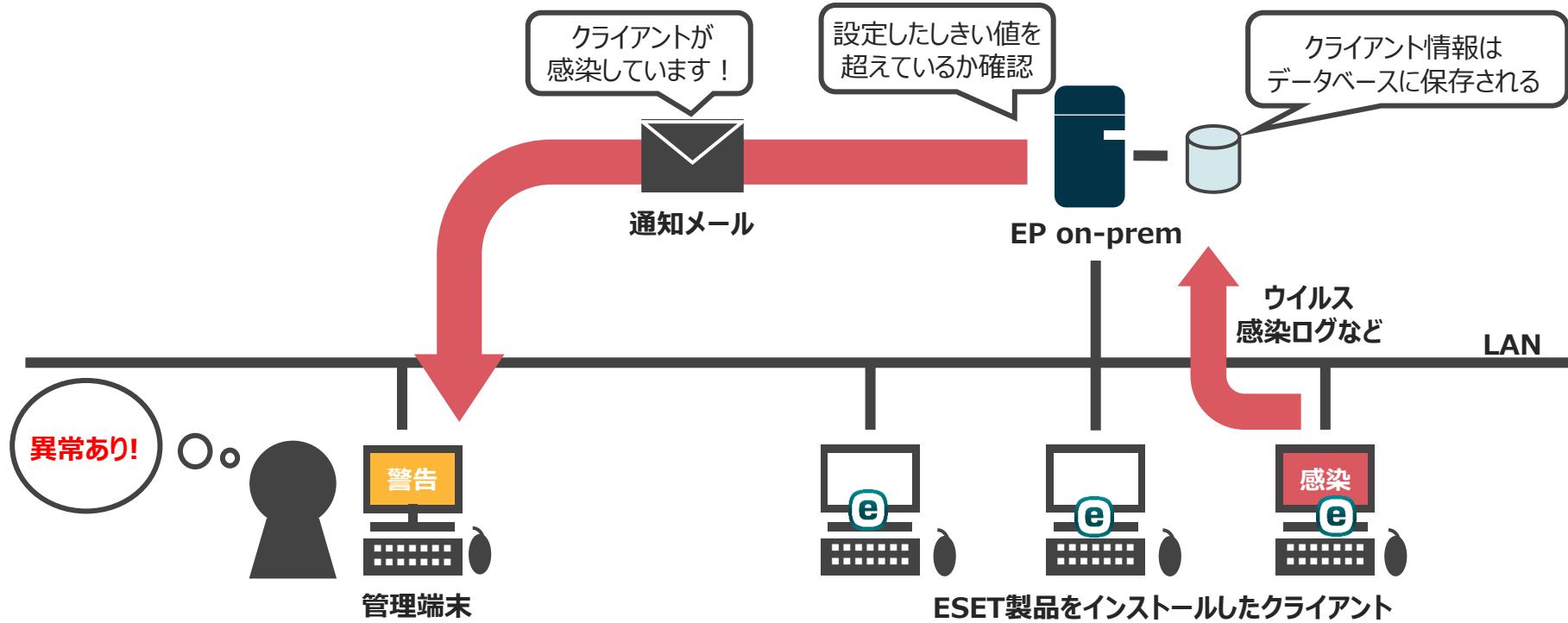
初期構成 (任意) ②
この構成は初期構成としてのみ使用されます。ポリシーが適用されコンピューターの「適用済みポリシー」で初期構成は見えません。

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

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

【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 - 配布画面

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

ユーザー名 : Administrator



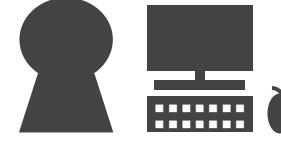
本社管理者
※本社および拠点(大阪)を管理

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

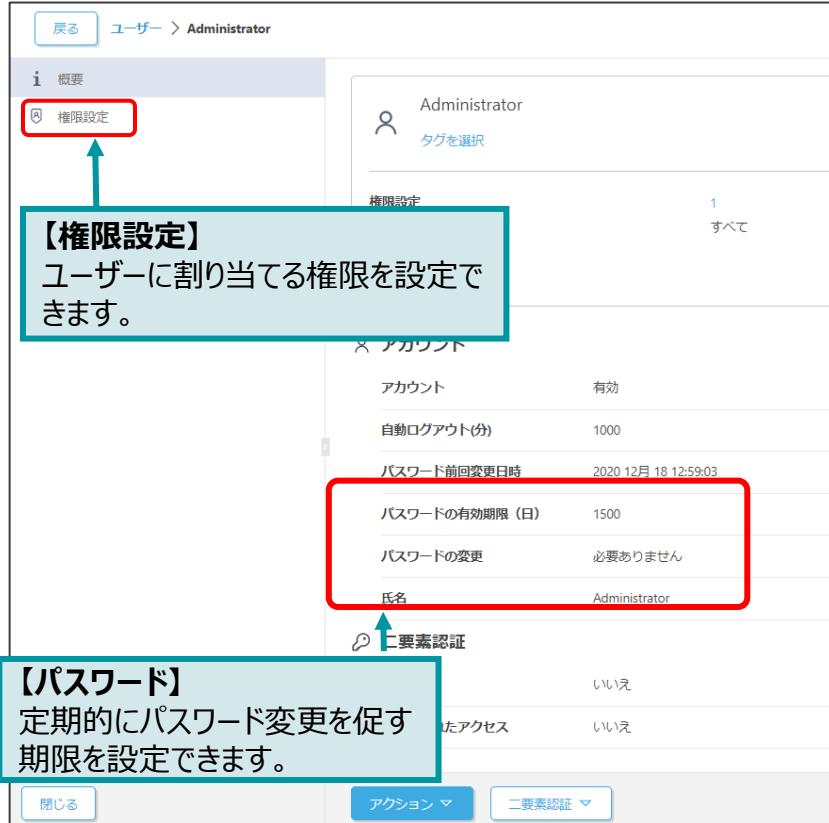
グループアクセス
自拠点(大阪)のグループに対してのみ
アクセスを許可

- ・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。

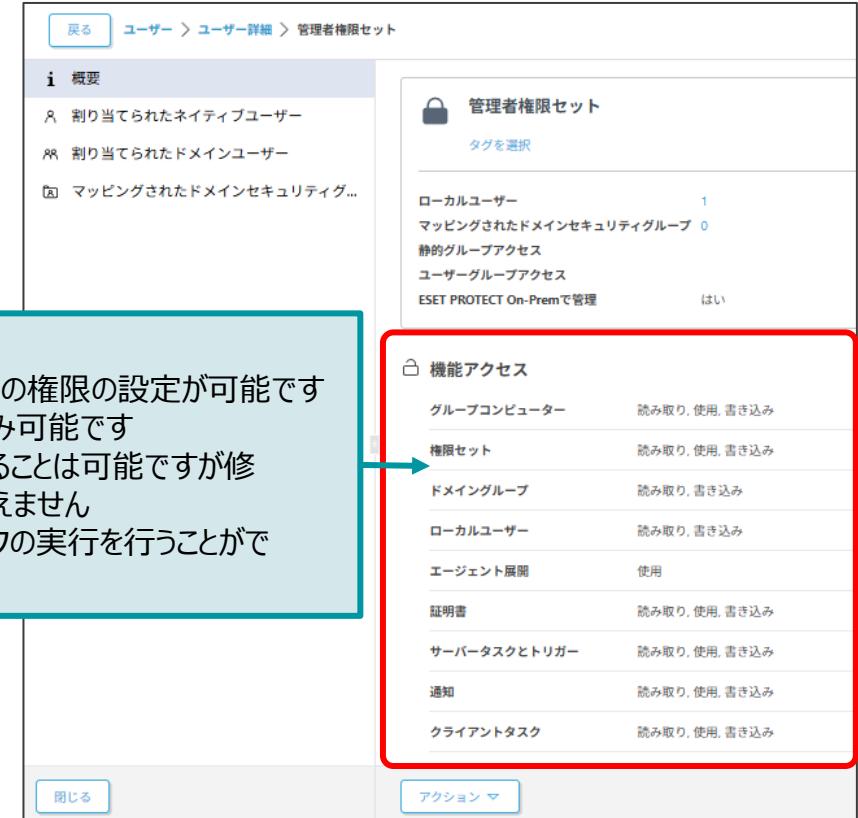
ユーザー画面



【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

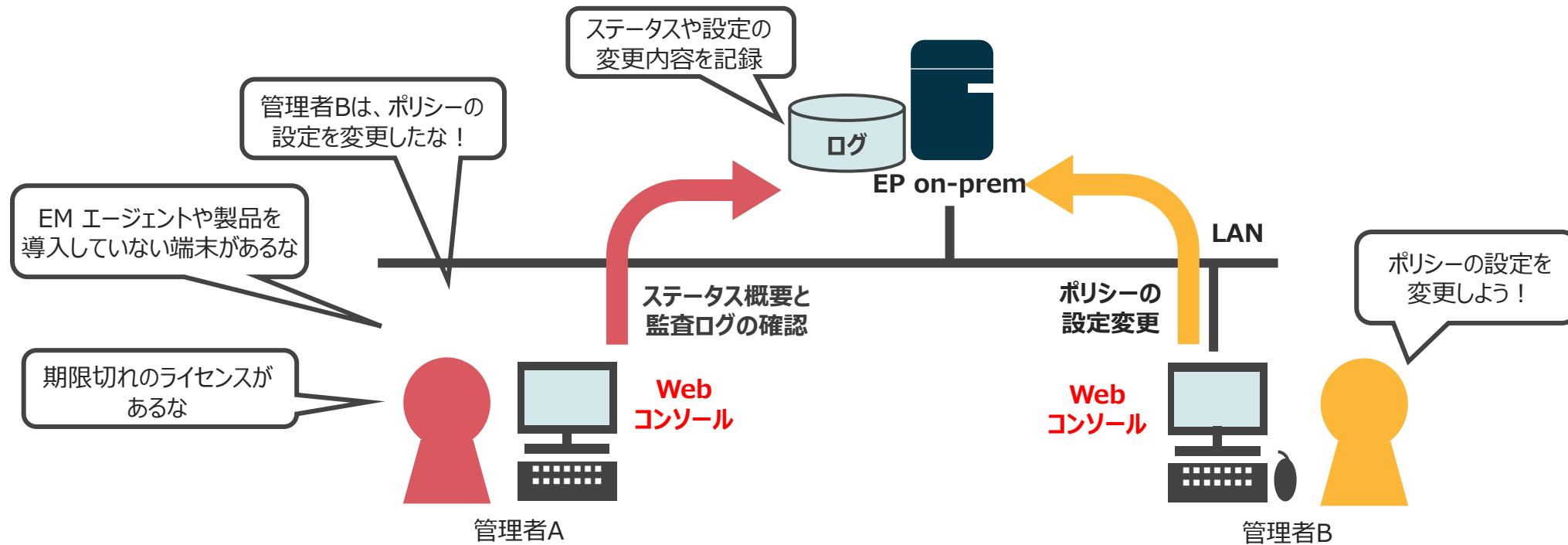


【機能アクセス】
EP on-premの各機能に対して下記の権限の設定が可能です

- ・**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

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



ステータス概要

ユーザー
ネイティブユーザーを作成し、権限を設定して、さまざまなレベルのリモート管理アクセス権を許可します。二要素認証(2FA)は、ESET PROTECT Webコンソールにログインしてアクセスするためのより安全な方法を提供します。

2FAが有効ではないユーザー: 1

コンピューター
使用可能な展開方法のいずれかを使用して、コンピューターを追加し、リモートで管理します。

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。

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。

無効なオブジェクト
タスクと通知の実行は内部および外部パラメーター(コンピューター、グループ、リポジトリからのインストーラーなど)によって異なります。オブジェクトにアクセスできない場合は、タスクと通知は動作しません。

⚠ アクセスできないオブジェクトを含むクライアントタスク: 1
✓ アクセスできないオブジェクトを含むサーバータスク: 0

外部サービス
ESET PROTECT On-PremはEPNS、SMTPサーバーなどの外部サービスに接続します。外部サービスは特定のタスクの実行をサポートします。

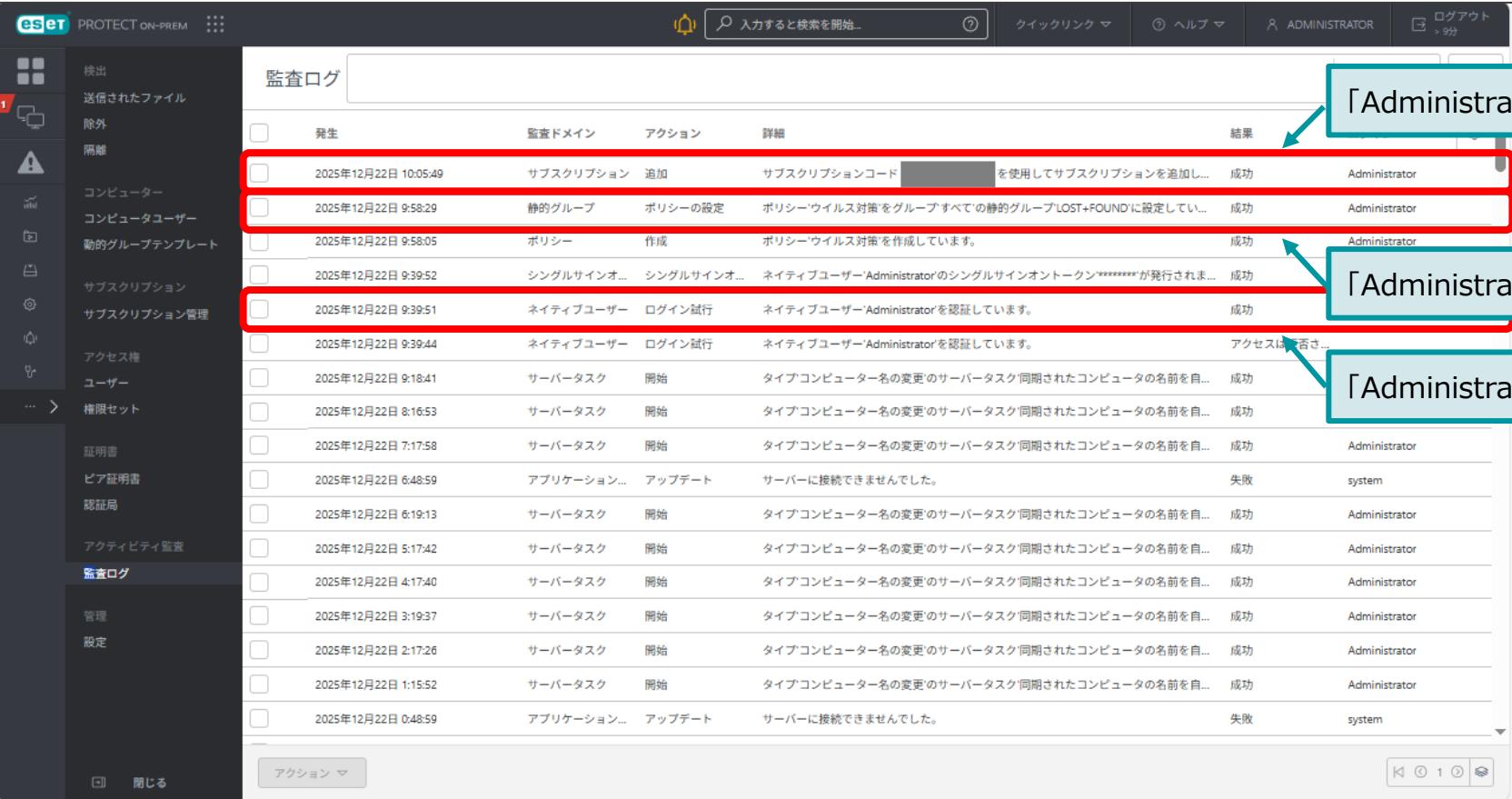
⚠ サーバー モジュール アップデートの失敗。詳細は監査ログをご覧ください。
⚠ SMTPサーバーが設定されていません
✓ ESET LiveGuardサーバーが接続されています

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	監査ドメイン	アクション	詳細	結果	ユーザー名
2025年12月22日 10:05:49	サブスクリプション	追加	サブスクリプションコード [REDACTED] を使用してサブスクリプションを追加しました。	成功	Administrator
2025年12月22日 9:58:29	静的グループ	ポリシーの設定	ポリシー「ウイルス対策」をグループ「すべて」の静的グループ「LOST+FOUND」に設定しています。	成功	Administrator
2025年12月22日 9:58:05	ポリシー	作成	ポリシー「ウイルス対策」を作成しています。	成功	Administrator
2025年12月22日 9:39:52	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
2025年12月22日 9:39:51	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
2025年12月22日 9:39:44	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。	アクセスに拒否されました	
2025年12月22日 9:18:41	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 8:16:53	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 7:17:58	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 6:48:59	アプリケーション	アップデート	サーバーに接続できませんでした。	失敗	system
2025年12月22日 6:19:13	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 5:17:42	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 4:17:40	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 3:19:37	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 2:17:26	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 1:15:52	サーバータスク	開始	タイプ「コンピューター名の変更」のサーバータスク「同期されたコンピュータの名前を自...」を開始しました。	成功	Administrator
2025年12月22日 0:48:59	アプリケーション	アップデート	サーバーに接続できませんでした。	失敗	system