



# ESET Endpoint Protection シリーズ クライアント管理用プログラム ESET PROTECT V8 機能紹介資料



ENDPOINT  
PROTECTION  
ADVANCED

イーセツ エンドポイント プロテクション アドバンスド



ENDPOINT  
PROTECTION  
STANDARD

イーセツ エンドポイント プロテクション スタンダード

第2版

2021年3月15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(EP)とは
3. ESET PROTECTの構成
4. Webコンソールのご紹介
  - ・ログイン画面
  - ・Webコンソールの画面構成
  - ・Webコンソールの画面構成（メインセクション）
5. ログ監視機能のご紹介
  - ・ダッシュボード
  - ・コンピューター
  - ・検出
6. クライアント管理機能のご紹介
  - ・レポート
  - ・グループ
  - ・ポリシー
  - ・タスク
  - ・インストーラー
  - ・通知
7. サーバー運用管理機能のご紹介
  - ・ユーザー管理
  - ・監視・監査
8. モバイルデバイス管理機能（iOSデバイスの管理）
9. ESETクライアント管理 クラウド対応オプション

# 1. はじめに（本資料について）

本資料は2021年2月10日より、「ESET Endpoint Protection シリーズ」で新たに提供を開始した、クライアント管理用プログラム (ESET PROTECT V8)の機能を紹介している資料です。本プログラムは、旧バージョンのクライアント管理用プログラム（ESET Security Management Center V7）の後継プログラムです。

旧プログラム名	新プログラム名	種別
ESET Security Management Center (Windows版)	ESET PROTECT (Windows版)	クライアント管理用プログラム
ESET Security Management Center (Linux版)	ESET PROTECT (Linux版)	クライアント管理用プログラム

- 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 Endpoint Protection シリーズではクライアント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。

## 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、Android向けプログラムを管理できます。また、iOSデバイスを管理することも可能です。（※）

ESET PROTECT V8 で管理可能なプログラム(2021年3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	8.0 / 7.X
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	8.0 / 7.X
ESET File 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	7.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	6.8 以降
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	6.8 以降
ESET NOD32アンチウイルス for Linux Desktop	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	管理不可
ESET File 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	7.2
ESET Endpoint Security for Android	Android OS向け 総合セキュリティプログラム	2.x

※EPでは、iOSデバイスの管理が可能ですが、iOS向けのウイルス対策機能はございません。  
 ※クライアント管理用プログラム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](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



**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
- ・グループ
- ・ポリシー
- ・タスク
- ・インストーラー
- ・通知



**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)

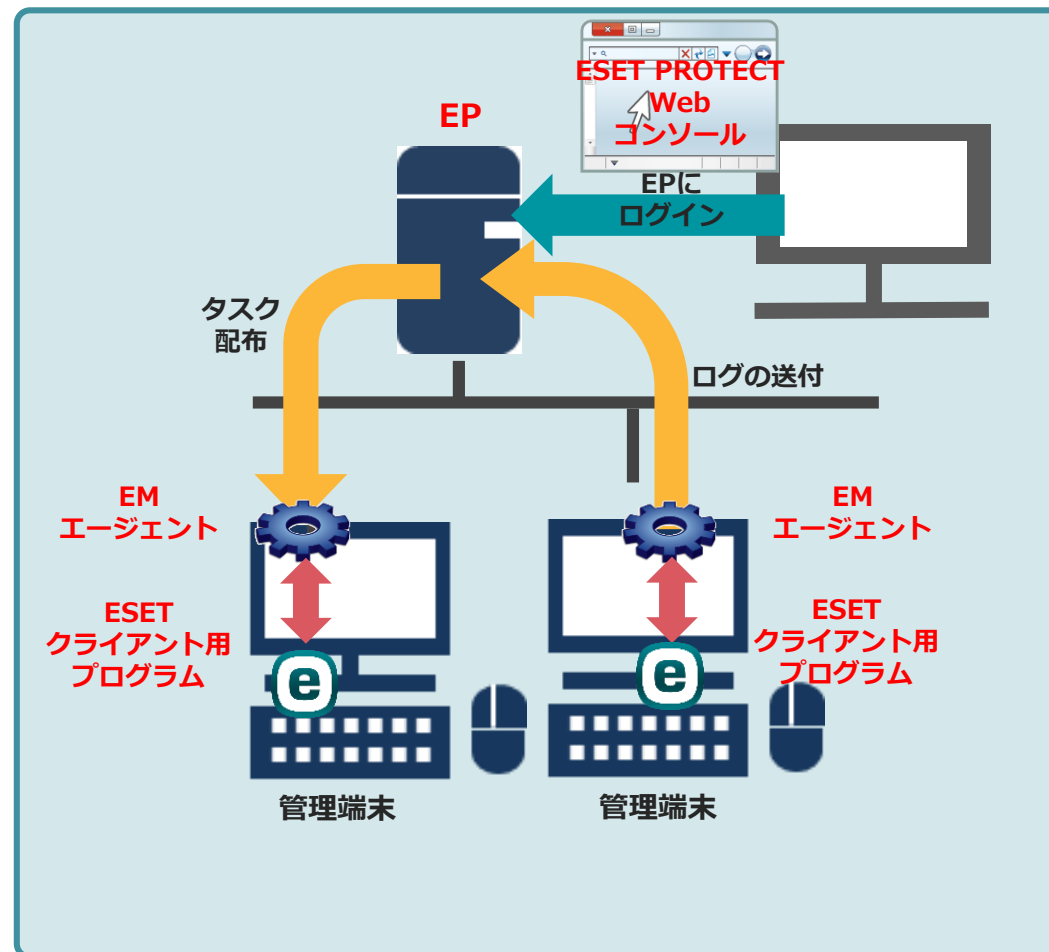
EPはクライアントプログラムの情報収集やタスク配布などを行います。クライアントとの通信はエージェントを経由して行います。

#### 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、ブラウザを使用してEP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)

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。



### 3. ESET PROTECTの構成

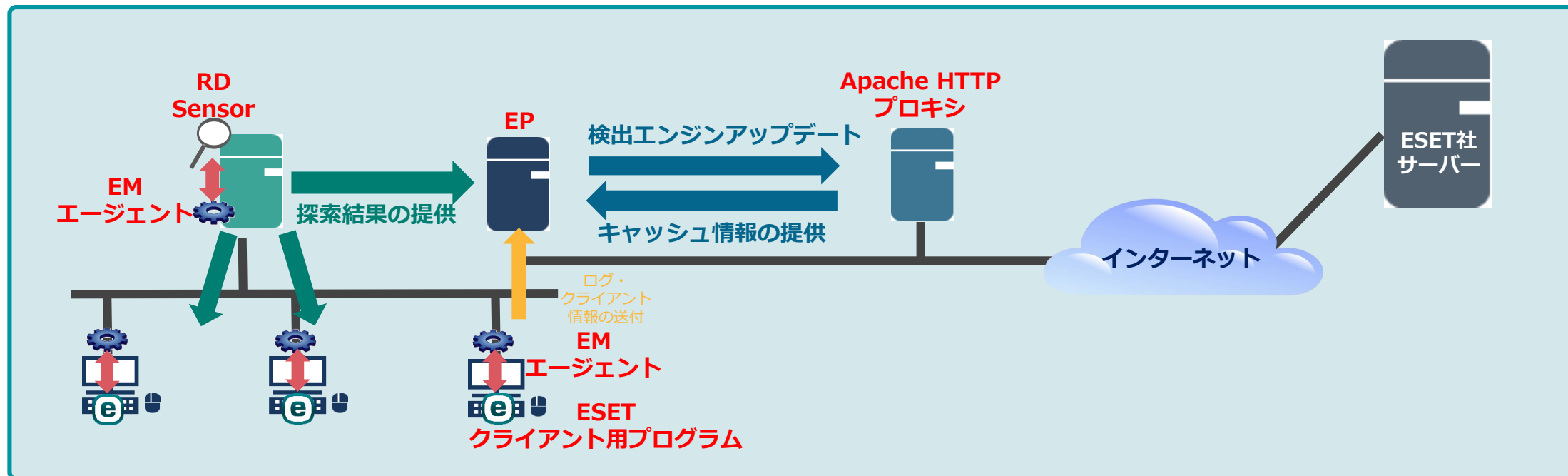
以下のコンポーネントは任意で構成します。

#### 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。

#### Apache HTTPプロキシ

Apache HTTPプロキシ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。Apache HTTP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。



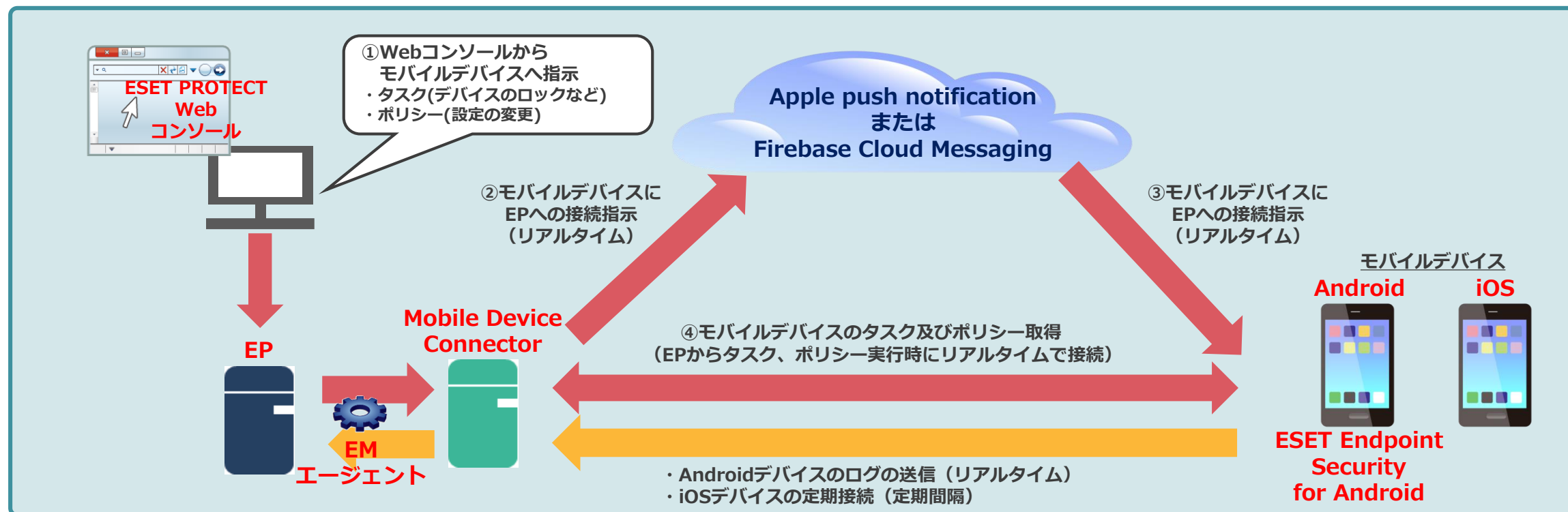
※本機能は、「ESETクライアント管理 クラウド対応オプション」および「ESETクライアント管理 クラウド対応オプション Lite」ではご使用いただけません。

### 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。

#### Mobile Device Connector

EPでAndroid端末やiOSのモバイルデバイスを管理するために必要なコンポーネントとなります。  
モバイルデバイスの登録および、モバイルデバイスとの通信を行う際に使用します。なお本機能はEPに含めることができます。



※本機能は「ESETクライアント管理 クラウド対応オプション Lite」ではご使用いただけません。



### 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 V8 (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)
EP V8 (Linux版)	Red Hat Enterprise Linux 7 (64bit)
	CentOS 7 (64bit)
	Suse Linux Enterprise Server 11 (64bit)
	Suse Linux Enterprise Server 12 (64bit)
	Suse Linux Enterprise Server 15 (64bit)

### 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、2012、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 V8 (Windows版)	Microsoft SQL Server 2012 Standard Edition	制限なし
	Microsoft SQL Server 2012 Express Edition	10GBまで
	Microsoft SQL Server 2014 Standard Edition	制限なし
	Microsoft SQL Server 2014 Express Edition (既定) ※	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) ※	10GBまで
EP V8 (Linux版)	MySQL 5.6、5.7、8.0	制限なし



## 4. Webコンソールのご紹介

**Canon**

キヤノンマーケティングジャパン株式会社

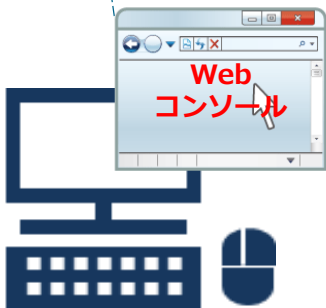
## 4. ログイン画面

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

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 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. 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。



### 【メインセクション】

ESET PROTECT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。

### 【簡易検索ツール】

検索はコンピューター名、ウイルス名、IPアドレスなどをキーに管理クライアントを検索することができます。

メインセクションで選択したものにに応じて、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. 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。

The screenshot shows the ESET PROTECT Web Console interface. The left sidebar contains a menu with icons for Dashboard, Computers, Detection, Reports, Tasks, Installer, Policies, Notifications, Status Overview, and Details. The main content area displays a dashboard with a donut chart showing 2 devices, a table of device status, and a bar chart showing product version status for Agents, Endpoints, Servers, and Mobile devices.

**【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。

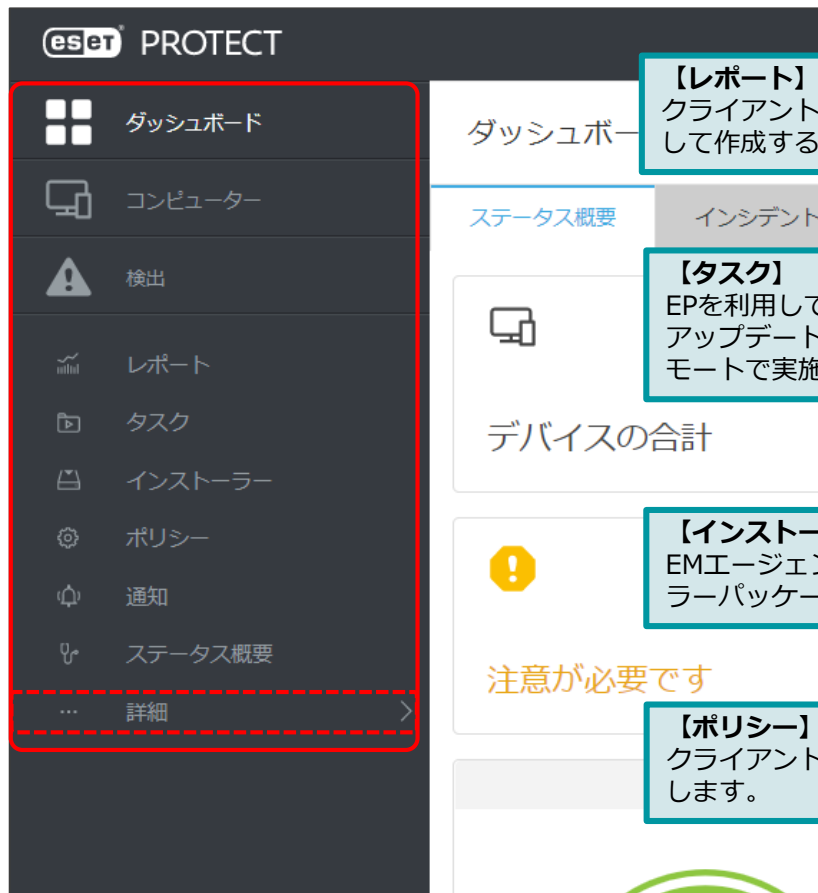
**【検出】**  
EPで管理するクライアントで検出された脅威の概要が表示されます。

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。

**【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。

## 4. 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. 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。

The screenshot shows the ESET PROTECT Web Console interface. The left sidebar contains a menu with various options. A red box highlights the '詳細' (Details) section, which includes options like '検出' (Detection), '送信されたファイル' (Transmitted files), '除外' (Exclusions), '隔離' (Isolation), 'コンピューター' (Computer), 'コンピューターユーザー' (Computer user), '動的グループテンプレート' (Dynamic group template), 'ライセンス' (License), 'ライセンス管理' (License management), 'アクセス権' (Access rights), 'ユーザー' (User), '権限設定' (Permission settings), '証明書' (Certificate), 'ピア証明書' (Peer certificate), '認証局' (CA), 'サーバー' (Server), 'サーバー設定' (Server settings), 'アクティビティ監査' (Activity audit), and '監査ログ' (Audit log). A callout points to the '...' icon in the sidebar, stating: 「展開すると、サブメニューが表示されます。」 (When expanded, the sub-menu is displayed).

**【送信されたファイル】**  
別製品「ESET Dynamic Threat 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 Dynamic Threat Defenseを利用するためには、別途ライセンスを購入・登録する必要があります。

**【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。

**【コンピューターユーザー】**  
iOSデバイスの管理に利用します。ユーザーとデバイス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。

**【ライセンス管理】**  
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。

**【サーバー】**  
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。

**【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。





## 5. ログ監視機能のご紹介

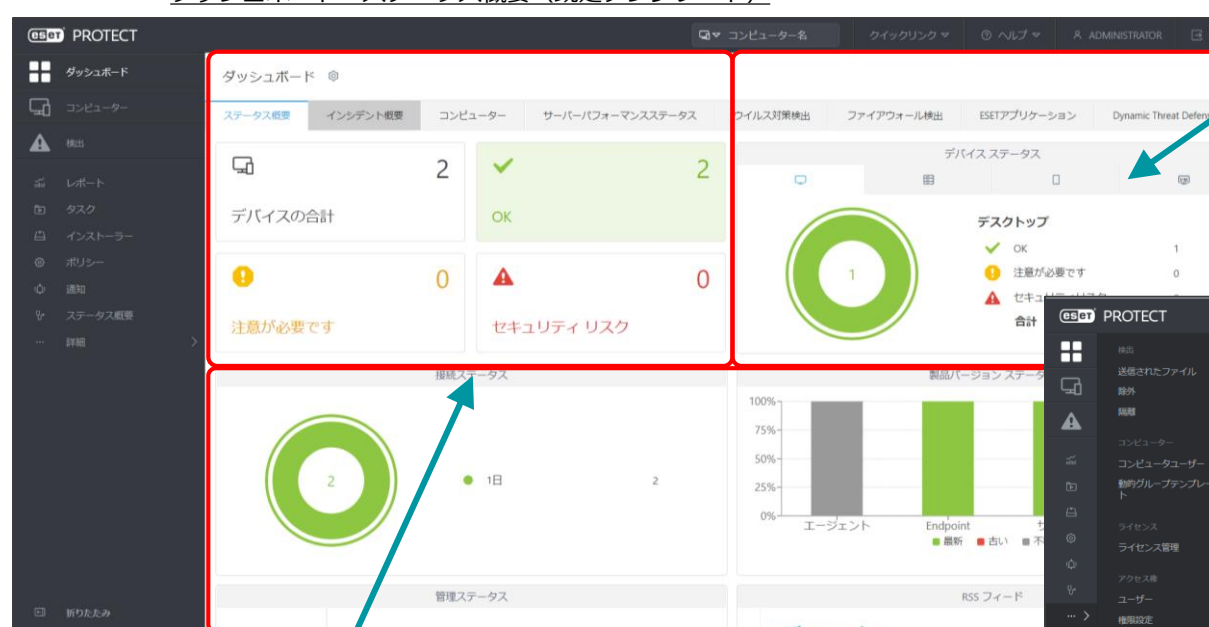
**Canon**

キヤノンマーケティングジャパン株式会社

## 5. ダッシュボード

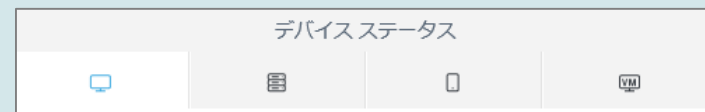
EPにログインするとはじめに表示されるのがダッシュボードです。「概要」や「インシデント概要」では、簡易的なクライアントの情報や脅威検出情報など管理しているクライアント全台の状態を確認できます。

ダッシュボード－ステータス概要（既定テンプレート）

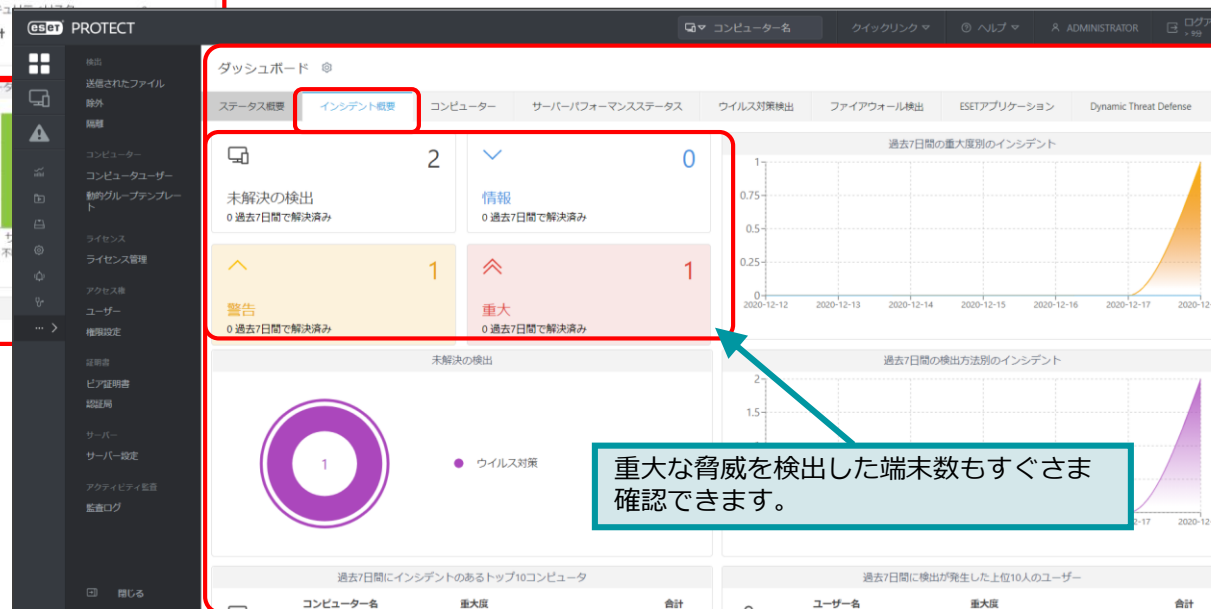


正常な端末や注意が必要な端末、問題のある端末を色別でカウントします。

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）



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. 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. 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。

コンピュターステータス概要

2

OK

セキュリティ通知

表示

詳細情報

"警告"のみ

"セキュリティ通知"のみ

作成済み 0分前

②一覧の中から参照したい箇所をクリックし、続いて「詳細を表示」を選択します。

レポート: ドリルダウン - 詳細情報

サーバー名  
WIN-PE6EUS0FF.localdomain

生成ロケーション  
2020 12月 18 14:34:04 (UTC+09:00)

レコード数  
1

フィルター  
フィルター数: 4

重大度	発生時刻	ステータス	コンピューター名	群組グループ名	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
警告	2020 12月 18 14:13:08	セキュリティ通知	desktop-dm9jha	LOST+FOUND	192.168.231.131	192.168.231.0		

詳細を表示

検索

モジュールの更新

再起動

タスクの実行...

新規タスク...

最後に使用されたタスク

ユーザーの割り当て...

ポリシーの管理...

③セキュリティ通知内容が表示されます。

注意が必要です

アラート

未解決の検出数  
0

前回の接続時間  
2020 12月 18 14:21:47

前回の検査時刻  
2020 12月 18 13:20:37

検出エンジン  
22501 (20201218)

更新  
更新

ここをクリックすると、リストを表示します

【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. 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、「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。

コンピュータ

サブグループの表示 ☒ すべて (2) タグ... ミュート ☐ × **フィルタの追加**

グループ	コンピュータ名	タグ	ステータス	ミュート	モジュール	前回の接続	アラート	検出	セキュリティ
すべて (2)									
LOST+FOUND (2)									
Windows コンピューター									
Linux コンピューター									
Mac コンピューター									
古いモジュールのコンピューター									
古いオペレーティングシステムのコンピューター									
問題のあるコンピューター									
アクティベーションされていないセキュリティ									
モバイルデバイス									
	desktop-dnmj3ha	192.16...	!		更新	2020 12月 18 14:23:47	1	0	ESET
	win-pe6ieu68iff	1...	✓		更新	2020 12月 18 14:23:54	0	0	ESET

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。

アラート数  
検出数  
適用されたポリシー数  
アラート数  
検出数  
適用されたポリシー数  
IPアドレス  
OSサービスパック  
OSタイプ  
OSバージョン

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。

# 5. 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 設定 ログ タスクの実行 インストール済みアプリケーション アラート 質問 検出と隔離 ... 詳細

基本 ハードウェア 製品およびライセンス

デバイス

メーカー VMware, Inc.  
モデル VMware7,1  
シリアル番号 VMware-56 4d 31 8a 09 b6 67 4e-e6 fd 37 dd 6d 22 2b bb  
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,14410784.B64,1908150010, VMware, Inc., VMware, Inc.

CPU

説明 Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz  
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

能力 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

【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 - 設定

概要 設定 ログ タスクの実行 インストール済みアプリケーション アラート 質問 検出と隔離 ... 詳細

ESET Endpoint for Windows

検出エンジン

リアルタイムファイルシステム保護  
マルウェア  
クラウドベース保護  
マルウェア検出  
HIPS

更新

リアルタイム保護  
マルウェア  
クラウドベース保護  
マルウェア検出  
HIPS

検出エンジン

リアルタイムファイルシステム保護  
マルウェア  
クラウドベース保護  
マルウェア検出  
HIPS

更新

リアルタイム保護  
マルウェア  
クラウドベース保護  
マルウェア検出  
HIPS

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

概要 設定 ログ タスクの実行 インストール済みアプリケーション アラート 質問 検出と隔離 ... 詳細

名前	ベンダー	バージョン	サイズ[MB]	エージェントによる
ESET Management Ag...	ESET, spol. s r.o.	8.0.1239.0	167	はい
ESET Endpoint Secur...	ESET, spol. s r.o.	8.0.2028.1	222	はい
Microsoft Update Heal...	Microsoft Corporation	2.70.0.0	1	はい
VMware Tools	VMware, Inc.	11.0.0.14549434	90	はい
Microsoft Visual C++ ...	Microsoft Corporation	14.20.27508.1	23	いいえ
Microsoft Visual C++ ...	Microsoft Corporation	14.20.27508.1	20	いいえ

【詳細】 - 【ハードウェア】  
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。

【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. 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ログの概要が表示されます。

**【グループ】**  
ESET PROTECT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。

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り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。

グループ	ステータス	検出タイプ	原因	アクション	発生	解決済み	コンピューター名
LOST+FOUND	未解決	ウイルス対策	テストファイル	Eicar	保持	1	0/1
Windows コンピューター	未解決	ウイルス対策	テストファイル	Eicar	削除によっ...	1	0/1

## 5. 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。

ウイルス対策	
発生	2020 12月 18 14:10:07
発生	合計 1 ① 解決済み 1 ② 製品で処理されました 1 新規作成されたファイルでイベントが発生しました。
状況	最新の出現日時
最初の出現日時	2020 12月 18 14:10:05

ファイル	
ハッシュ	3395856CE81F2B7382DEE72602F798B642F14140
名前	Eicar
Uniform Resource Identifier (URI)	file:///C:/Users/ESET/AppData/Local/Temp/vmware-ESET/VMwareDnD/171c7c3b/eicar.com
プロセス名	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe

検出	
スキャナ	リアルタイムファイルシステム保護
検出エンジンバージョン	22501 (20201218)
現在の検出エンジンバージョン	22501 (20201218)
検査対象	
検査された項目数	
感染	
駆除済み	
完了時間	
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	





## 6. クライアント管理機能のご紹介

**Canon**

キヤノンマーケティングジャパン株式会社

カテゴリごとに分類されています。



過去7日間の検出イベント  
過去7日間に最も多かった  
すべてのウイルス対策検出

用途に応じて柔軟に作成することができます。

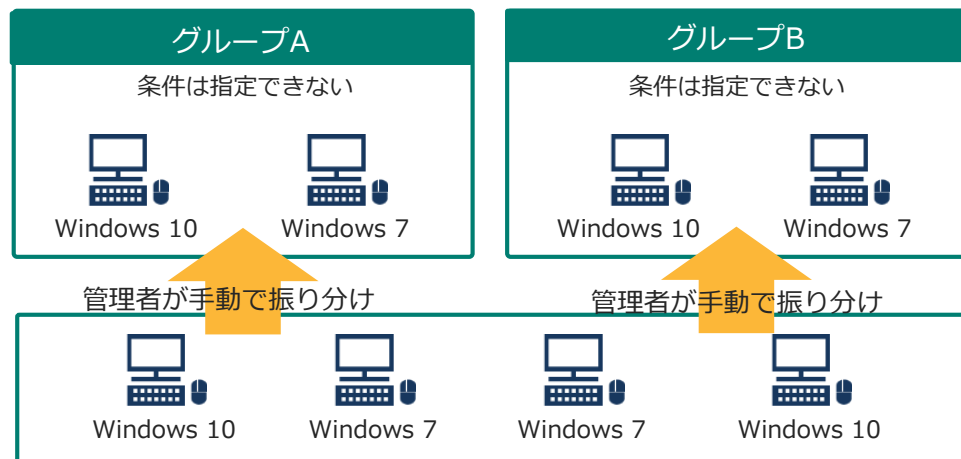
25

## 6. 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。

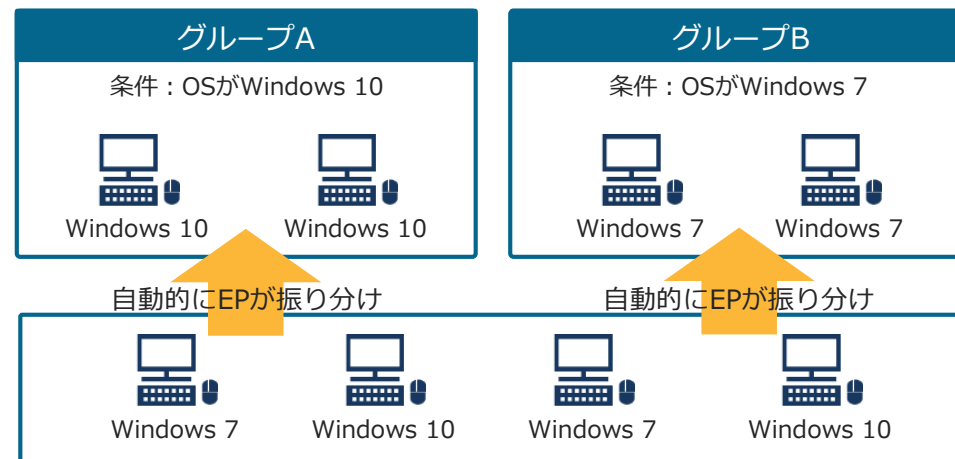
### 静的グループ

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。



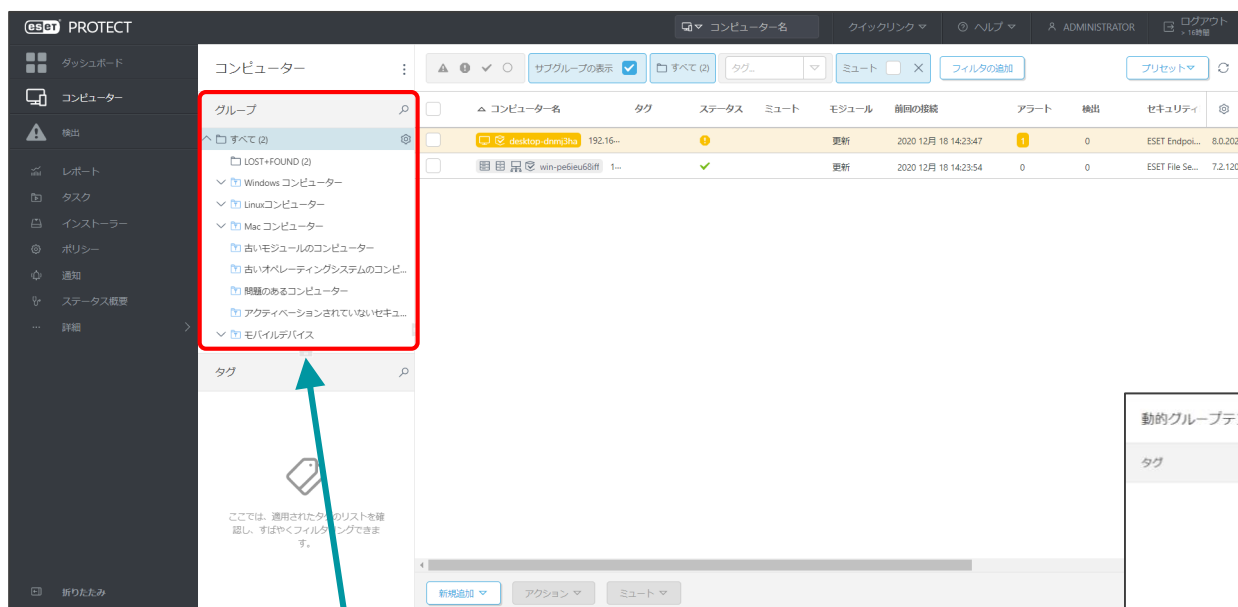
### 動的グループ

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. 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。

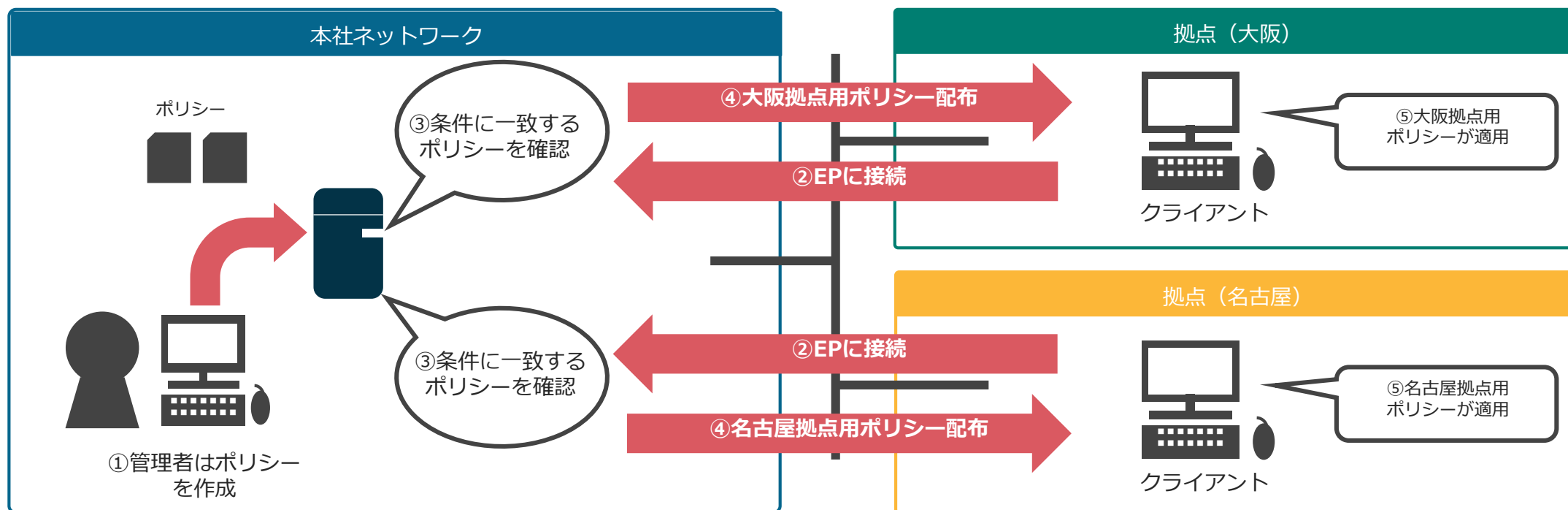
### ●主な条件値

- ・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



## 6. 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. ポリシー

ポリシーには予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。

<戻る ポリシー

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。

ESET Endpoint for Windows

検出エンジン

- リアルタイムファイルシステム保護
- クラウドベース保護
- マルウェア検査
- HIPS
- WEBとメール

基本

- 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

【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. 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。
- ・ **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

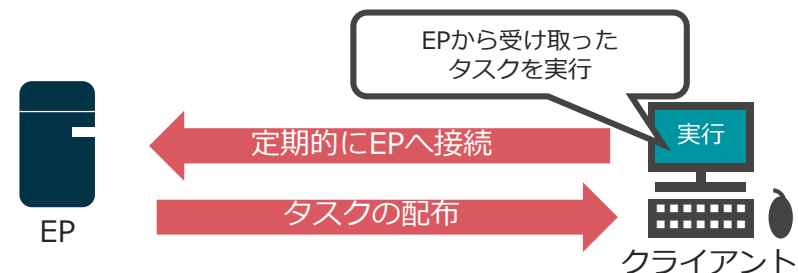
- ・ **ESET PROTECT コンポーネントのアップグレード**  
EPやEMエージェントのアップグレードを実行します。
- ・ **管理の停止**  
クライアントのEM エージェントをアンインストールします。

#### 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. 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。

The screenshot shows the ESET task configuration interface, divided into three main sections: **タスク画面** (Task Screen), **タスクトリガータイプ画面** (Task Trigger Type Screen), and **タスク詳細設定画面** (Task Detailed Settings Screen).

**タスク画面 (Task Screen):** Displays a list of tasks under the category **クライアントタスク** (Client Tasks). A red box highlights the list, and a blue callout box explains: **ESET製品やOSへのタスクなど、ターゲットに応じて分類しています。** (Tasks for ESET products or OS are classified according to the target).

**タスクトリガータイプ画面 (Task Trigger Type Screen):** Shows the selection of a trigger type. A red dashed box highlights the **トリガー** (Trigger) section. A blue callout box explains: **【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。 (Trigger Type: Specify the day or time to execute the task. To disperse the load, you can also specify a 'Random delay interval' to execute the task randomly within the specified time range).

**タスク詳細設定画面 (Task Detailed Settings Screen):** Shows the detailed configuration for the selected trigger. A red dashed box highlights the **結合された動的グループトリガー** (Combined dynamic group trigger) option. A blue callout box explains: **【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。 (Combined dynamic group trigger: By specifying a dynamic group trigger, you can execute the task at the timing when a client is added to the dynamic group. By setting dynamic groups such as 'Old module computer' or 'Detect security products that are not activated', you can automatically apply the task to clients where a problem occurs).



## 6. 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。

### インストーラー

#### 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。



- 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

#### エージェントライブインストーラー

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。



- 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。

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. 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。

eset PROTECT

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

インストーラー画面

インストーラー

アクセスグループ 選択

タグ...

フィルタの追加

タグ	名前	タイプ	ステータス	製品
	ESET Endpoint Security (ja_JP)	オールインワンインストーラー		ESET Endpoi...

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。

オールインワンインストーラー

エージェントライブインストー...

GPOまたは SCCMスクリプト

インストーラーの作成...

ダウンロード

作成した各インストーラーが一覧で表示されます。

作成するインストーラーの種類を選択します。

【設定テンプレート】  
EM エージェントやESET製品に対して、あらかじめ作成したポリシー適用することで、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。

オールインワンインストーラー作成画面

オールインワンインストーラーの作成

インストーラー > ESET Endpoint Antivirus (ja\_JP)

基本

セキュリティ製品

証明書

詳細

ダウンロード

名前

ESET Endpoint Antivirus (ja\_JP)

説明

タグ

タグを選択

親グループ(任意)

選択 または 新規グループの作成

ESET AV Removerを有効にする

インストールの初期設定

組み込んだ初期設定は静的グループに適用されたポリシーで置換されます。

設定テンプレート

設定しない

ポリシーのリストから設定を選択

サーバーホスト名(またはサーバーのIPアドレス)

戻る

続行

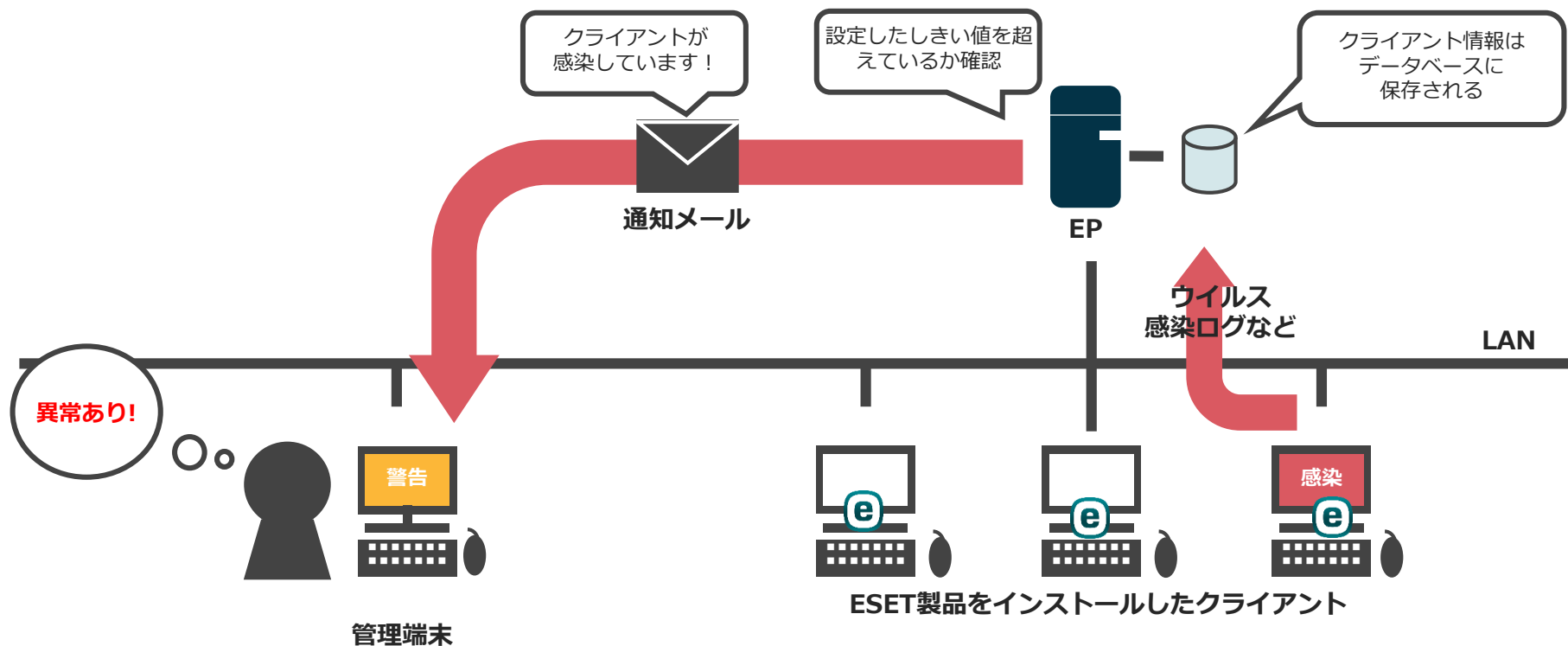
終了

キャンセル

【親グループ(任意)】  
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。

## 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。



※本機能は、「ESETクライアント管理 クラウド対応オプション Lite」ではご使用いただけません。

## 6. 通知

通知は予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。

タグ	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ート		<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ート		<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ート		<input type="radio"/> 無効
<input type="checkbox"/>	悪意のあるファイルが検...		<input type="radio"/> 無効
<input type="checkbox"/>	通知の構成が無効であり...		<input type="radio"/> 無効
<input type="checkbox"/>	新しいバージョンのESET ...		<input type="radio"/> 無効
<input type="checkbox"/>	古いバージョンのESET En...		<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。

新しい通知... アクション ▼

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。

新しい通知  
通知 > 新しい通知

基本  
設定  
詳細設定 - 調整  
配布

イベント  
管理されたコン...

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  
Enterprise Inspector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質問が作成されました  
新しいVMS顧客が見つかりました

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。

基本  
設定  
詳細設定 - 調整  
配布

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  
eset@example.com  
名前  
ユーザーの作成...  
すべて削除  
+ 詳細 ▼

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

**Canon**

キヤノンマーケティングジャパン株式会社

## 7. ユーザー管理


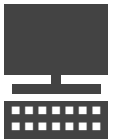

EPのアクセス権をもつユーザーを複数作成できます。EPではユーザーに対して設定可能なアクセス権が2種類あります。

- 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。

※本機能は、「ESETクライアント管理 クラウド対応オプション」および「ESETクライアント管理 クラウド対応オプション Lite」ではご使用いただけません。

# 7. 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

戻る ユーザー > Administrator

i 概要

権限設定

Administrator

タグを選択

権限設定 1 すべて

ホームグループ

電子メールアドレス

電話番号

アカウント

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

いいえ

ロックされたアクセス いいえ

閉じる アクション ▼ 二要素認証 ▼

**【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】**  
ユーザーに割り当てる権限を設定できます。

権限設定画面

戻る 権限設定 > 管理者権限設定

i 概要

割り当てられたネイティブユーザー

割り当てられたドメインユーザー

マッピングされたドメインセキュリティグ...

管理者権限設定

タグを選択

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

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, 使用, 書き込み

ローカルユーザー 読み取り, 使用, 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

クライアントタスク 読み取り, 使用, 書き込み

動的グループテンプレート 読み取り, 使用, 書き込み

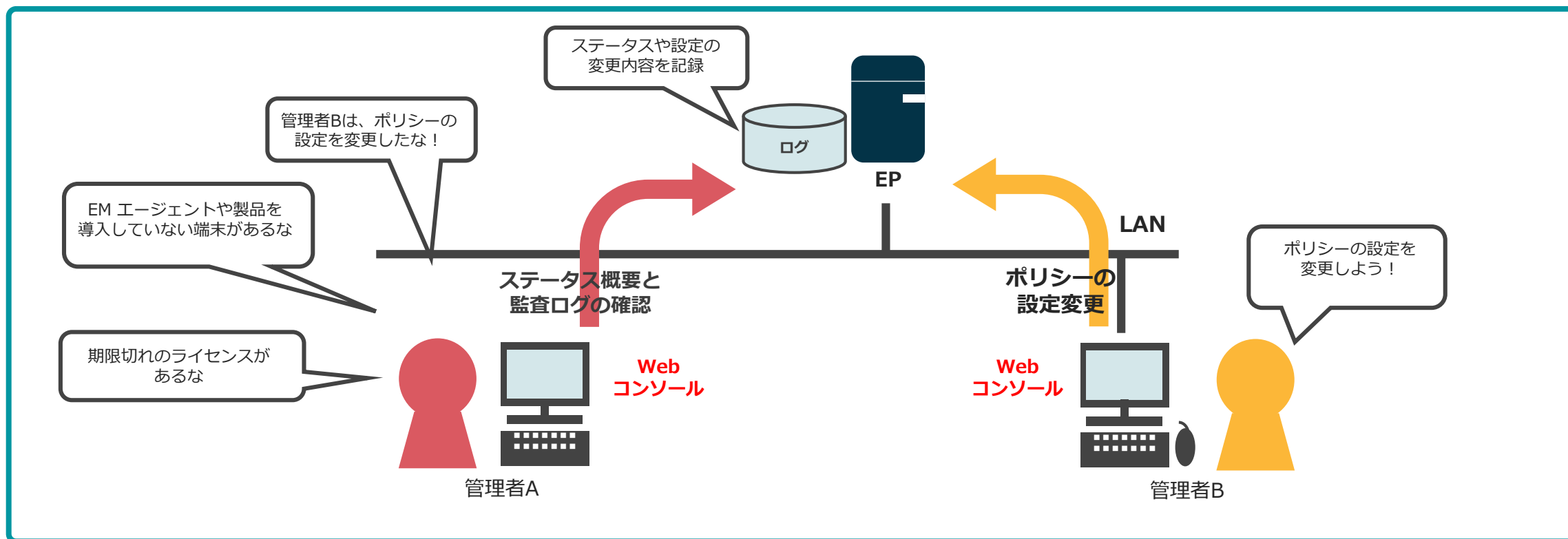
閉じる アクション ▼

**【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. 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。



※本機能は、「ESETクライアント管理 クラウド対応オプション」および「ESETクライアント管理 クラウド対応オプション Lite」ではご使用いただけません。



## 7. 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 (ℹ 情報) - ハードウェアに関する質問があります。

## 7. 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

eset PROTECT

コンピュータ名 クイックリンク ヘルプ ADMINISTRATOR ログアウト 16時間

監査ログ フィルタの追加 プリセット

	発生	監査ドメイン	アクション	詳細	結果	ログイン
<input type="checkbox"/>	2020 12月 18 14:54:53	保存されたインストーラー	削除	保存されたインストーラー-エー...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:53:22	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-エー...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:52:51	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-ESET ...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:43:02	クライアントタスク	作成	タイプオンデマンド検査のクラ...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:32:30	シングルサインオントークン	シングルサインオントークンの...	ネイティブユーザー'Administrat...	成功	
<input type="checkbox"/>	2020 12月 18 14:32:30	ネイティブユーザー	ログイン試行	ネイティブユーザー'Administrat...	成功	
<input type="checkbox"/>	2020 12月 18 14:31:44	コンピューター	ポリシーの設定	ポリシー'アプリケーションレポ...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:27:35	クライアントトリガー	割り当て	クライアントタスクESET製品の...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:27:03	クライアントトリガー	割り当て	クライアントタスクESET製品の...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:27:03	クライアントトリガー	割り当て	クライアントタスクESET製品の...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:26:58	クライアントトリガー	作成	説明'即時実行のタスクESET製品...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:26:56	クライアントトリガー	作成	説明'即時実行のタスクESET製品...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:26:26	クライアントトリガー	作成	説明'即時実行のタスクESET製品...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:26:20	クライアントタスク	作成	タイプESET製品の設定エクスボ...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:26:20	クライアントタスク	作成	タイプESET製品の設定エクスボ...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:26:19	クライアントタスク	作成	タイプESET製品の設定エクスボ...	成功	Administrator
<input type="checkbox"/>	2020 12月 18 14:19:43	シングルサインオントークン	シングルサインオントークンの...	ネイティブユーザー'Administrat...	成功	

②「Administrator」がタスクを割り当て。

①「Administrator」がタスクを作成。



## 8. モバイルデバイス管理機能(iOSデバイスの管理)

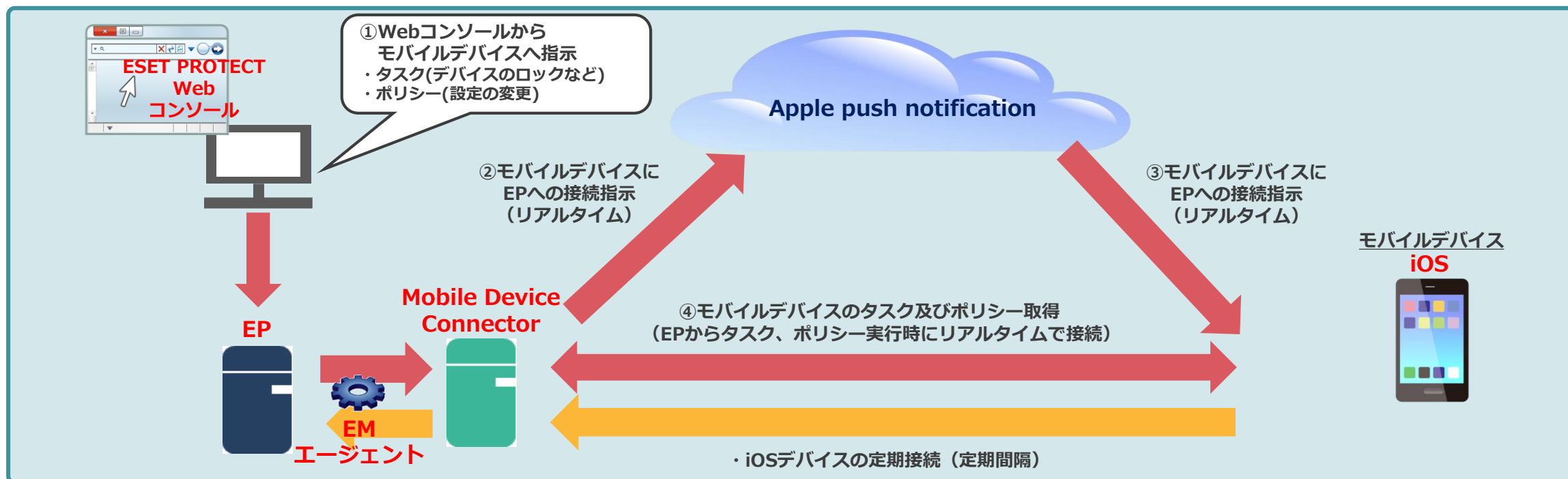
**Canon**

キヤノンマーケティングジャパン株式会社

## 8. 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。

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。



※本機能は、「ESETクライアント管理 クラウド対応オプション」および「ESETクライアント管理 クラウド対応オプション Lite」ではご使用いただけません。

## 8. 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 ・ESETライセンス情報

### iOSデバイス情報の閲覧



## 8. 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5種類の アクションの選択が行えます。 ・発見(ロストモードのオン) ※ ・ロストモードのオフ ※ ・ロック ・ロック解除 ・ワイプ ※DEPをご利用の場合のみ
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）



## 8. 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の管理機能一覧

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
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
その他	証明書、AirPrintプリンタ、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 Mobile Device Management for iOS)



ESET Mobile Device Management for iOS

Q 入力すると検索を開始...

パスコード

制限

その他

パスコード

○ ● ⚡ シンプルな値を許可 ☒

シンプルな値は昇順、降順、または繰り返し文字シーケンスです

○ ● ⚡ パスコードが必要 ☒

○ ● ⚡ 英数字の値が必要 ☒

○ ● ⚡ 最低パスコード長 5

○ ● ⚡ 複雑な文字の最低数 1

○ ● ⚡ 最大パスコード経過時間(1-730日、またはなし) 90

○ ● ⚡ 最大自動ロック時間(分) 1

○ ● ⚡ パスコード履歴(1-50パスコード、またはなし) 3

○ ● ⚡ デバイスロックの最大猶予期間 1分



## 9. ESETクライアント管理 クラウド対応オプション

**Canon**

キヤノンマーケティングジャパン株式会社



## 9. ESETクライアント管理 クラウド対応オプション



管理用プログラム(※)をクラウド上で提供するオプション製品を以下の2つのラインナップで提供しております。

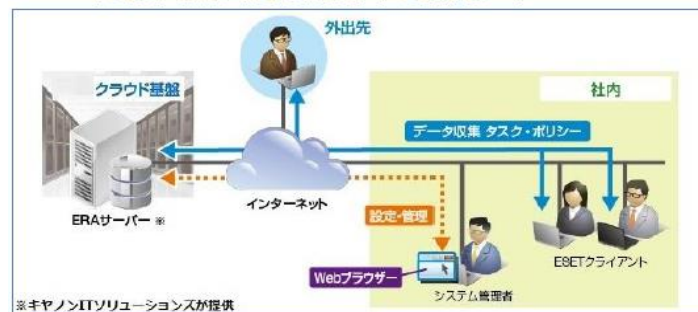
- ・「ESETクライアント管理 クラウド対応オプション」
- ・「ESETクライアント管理 クラウド対応オプション Lite」

クラウド対応オプション製品では、クラウド上の管理サーバーを使用するので、社内にサーバーを設置することなくクライアント管理を行うことができます。

### 製品特長

- ・お客様のサーバー機器購入および定期的なメンテナンスによる手間とコストの削減ができます。
- ・サーバー機器調達や構築期間を気にすることなく、すぐにESMCをご利用いただけます。
- ・サーバーの構築作業がなく、簡単にセットアップが完了できます。
- ・WEBブラウザでいつでもどこでもクライアント端末を簡単に管理できます。
- ・マルチプラットフォーム（Windows/Mac/Linux/Android）対応で、あらゆる機器を一括管理できます。  
※ 「ESETクライアント管理 クラウド対応オプション Lite」では、モバイル端末の管理はできません。

<ESET クライアント管理 クラウド対応オプション利用イメージ>



※クライアント管理用プログラムは、ESET Security Management Center V7.2でご提供しています。（2021年2月現在）

## 9. ESETクライアント管理 クラウド対応オプション



クラウド対応オプションは、サーバーの使用方法や機能制限に以下の違いがございます。

### 「ESETクライアント管理 クラウド対応オプション」

お客さまの専用サーバーで、25ライセンス以上のお客さまがご利用いただけます。

### 「ESETクライアント管理 クラウド対応オプション Lite」

他のお客さまとの共用サーバーで6～249ライセンスのお客さまがご利用いただけます。

	ESETクライアント管理 クラウド対応オプション	ESETクライアント管理 クラウド対応オプション Lite
動作サーバー	専用サーバー	共用サーバー
管理可能なクライアント 端末数	25ライセンス～	6～249ライセンス
ログ管理機能	○	○
クライアント管理機能	○	△（モバイルデバイスを除く）
お客さまごとの データバックアップ	○	×（共用サーバー全体でのバックアップは 実施）
メール通知	○	×
レポートのダウンロード	○	○

※機能制限について、詳細は以下のWEBページをご参照ください。

[https://eset-support.canon-its.jp/faq/show/4497?site\\_domain=business](https://eset-support.canon-its.jp/faq/show/4497?site_domain=business)

## 9. ESETクライアント管理 クラウド対応オプション



### 接続環境

クラウドオプションまたはクラウドオプションLiteでクライアント管理するためには、以下の接続環境が必要です。

①クライアントをクラウドオプションのESMCで管理するためには、クライアント用プログラム、および、管理画面利用端末からESMCの以下のポートへ接続できる必要がありますので、ご注意ください。

- ・ 2222/TCP : ESET Managementエージェント（EMエージェント）がESMCと通信する際に利用
- ・ 443/TCP : ESMCが管理画面利用端末からのWebコンソールアクセスを受ける際に利用
- ・ 80/TCP、443/TCP : 検出エンジンのアップデート用サーバーがクライアント用プログラムからのアクセスを受ける際に必要

【HTTPプロキシ経由する場合】

- ✓ HTTPプロキシがESMCで利用するTLS/SSL通信（2222/TCP）を転送できること
- ✓ HTTP CONNECTメソッドをサポートしていること
- ✓ プロキシ認証を必要としないこと（ユーザー名/パスワード設定不可）
- ✓ プロキシサーバーから上記ポートへ通信できること

クラウドオプションでモバイルデバイスを管理するためには、以下の接続環境が必要です。

※クラウドオプションLiteでは、モバイルデバイスの管理を行うことはできません。

【Android OSのモバイルデバイスを管理する場合】

- ✓ 9980/TCP : モバイルデバイスをESMCに登録する際に利用
- ✓ 9981/TCP : モバイルデバイスがESMCと通信する際に利用
- ✓ 5228/TCP、5229/TCP、5230/TCP : モバイルデバイス（Android OS）がFirebase Cloud Messagingへ接続する際に利用

## 9. ESETクライアント管理 クラウド対応オプション



### 禁止事項

クラウドオプション、もしくはクラウドオプションLiteをご利用いただく場合、以下の事項を禁止しております。

- ① EMエージェントの接続間隔を20分未満へ変更
- ② 一日に合計30MB以上のレポートファイルをダウンロード
- ③ 一日に合計1,000通以上を通知させる送信設定（クラウドオプションのみ）
- ④ 存在しない電子メールアドレスや不要な電子メールアドレスの設定（クラウドオプションのみ）
- ⑤ モバイルデバイスを管理するために表示されるESMCへの操作（クラウドオプションのみ）

クラウドオプションの場合、ESMCの管理画面のコンピューター一覧に、管理対象の端末としてサーバー自体が表示されています。ESMCサーバーに対する下記の操作は、クラウドオプションの運用管理に支障をきたしますので行わないでください。

1. コンピューターのシャットダウンタスクによるESMCサーバーのシャットダウンおよび再起動
2. オペレーティングシステムのアップグレードタスクによるESMCサーバーのOSのパッチ等のアップデート
3. 管理の停止タスクやアンインストールタスクによるESMCサーバー自身のEMエージェントのアンインストール
4. ESMCコンポーネントアップグレードによるESMCサーバー自体のアップグレード
5. コマンドの実行タスクによるESMCサーバー自身に対する任意のコマンド実行
6. 初期設定されているESMCサーバーのポリシーの変更及び削除
7. ESMCサーバーの削除
8. ESMCサーバーが所属する静的グループの変更