クラウドサンドボックス

ESET LiveGuard Advanced
機能紹介資料

第27版

2025年2月

Canon

キヤノンマーケティングジャパン株式会社

目次

1. はじめに(本資料について)

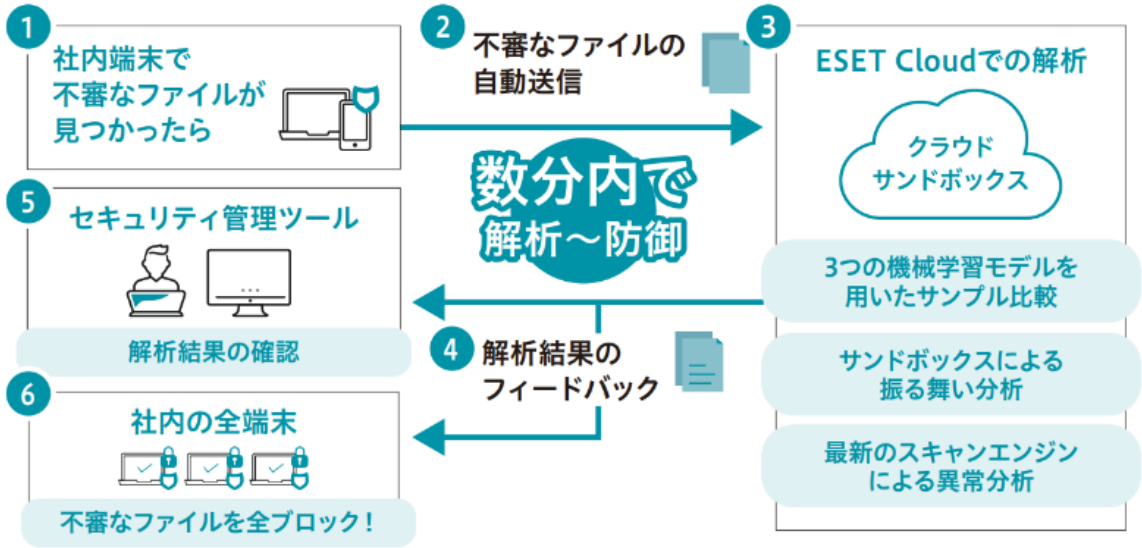
本資料はクラウドサンドボックス「ESET LiveGuard Advanced」の機能を紹介した資料です。

- ESET LiveGuard Advancedを利用いただくには、オンプレミス型セキュリティ管理ツールであるESET PROTECT on-prem V9以降、またはクラウド型セキュリティ管理ツールであるESET PROTECT(※EP)での管理が必要です。
- ESET LiveGuard Advancedにて作成できる動作レポートですが、XDRソリューション(ESET Inspect または ESET Inspect on-prem)の利用可否により、異なりますのでご注意ください。詳細は本資料のP12-13を確認ください。
- 本資料で使用している画面イメージは使用するOSにより異なる場合があります。また、今後画面イメージや文言が変更される可能性があります。
- ESET PROTECTソリューションではクライアントOSおよびサーバーOSの端末に導入する プログラムとしてWindows、Mac、Linux、Android OS向けプログラムをご使用いただけます。また、上記のプログラムを管理するセキュリティ管理ツール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は、米国Microsoft Corporationの、米国、日本およびその他の国における登録商標または商標です。
- ESET LiveGuard Advancedの導入方法は以下を参照ください。
  https://eset-info.canon-its.jp/files/user/pdf/manual/guide_edtd.pdf

2. ESET LiveGuard Advanced (ELGA) とは

(1) ELGAとは？

ゼロデイ攻撃に用いられるような未知の高度なマルウェアに対する検出・防御の即時性を高めるクラウドサンドボックスです。
エンドポイント(クライアント)プログラムが不審なファイル(サンプル)を発見すると、クラウド上の解析環境であるESET Cloudへ自動送信(手動も可)を行い、解析を依頼します。ESET CloudではESETの最新テクノロジーを用いた多段階での分析が行われます。解析結果はセキュリティ管理ツールより、レポートで確認できます。
悪質と判断されたファイルに対しては、エンドポイントで駆除、ブロックなどの防御処理を全社レベルで自動的に行います。



2. ESET LiveGuard Advanced (ELGA) とは

(2) 特長

①未知の脅威を自動解析、自動防御

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

②最新テクノロジーによる解析

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

③解析結果のレポート

サンプルの解析結果はセキュリティ管理ツールである「ESET PROTECT」または「ESET PROTECT on-prem」より閲覧可能です。悪質なものであるかどうかの判断や、サンドボックスシミュレーションで観察された挙動などを把握できます。

2. ESET LiveGuard Advanced (ELGA) とは

(3) 導入の効果

①ゼロデイ攻撃に速やかに対処したい

未知の脅威をクラウド上で自動解析し大半のサンプルは数分内に自動で駆除します。

②ESETの保護機能を手軽に強化したい

ESET PROTECTソリューションを既に使用しており、セキュリティ管理ツールでエンドポイントの管理を行っていれば、ライセンスを追加して機能を有効にすることで追加のエージェント不要で未知の脅威に対する対策を強化できます。

③サンドボックス機能を手軽に構築したい

セキュリティ管理ツールで管理を行っていれば、ハードウェアとエージェント不要で手軽かつ安価にサンドボックス環境を実装できます。

3. ESET LiveGuard Advancedの構成

(1) 動作環境

ESET LiveGuard Advancedの利用にあたっては、以下の環境が必要です。

①セキュリティ管理ツールが構築されていること

②セキュリティ管理ツールでエンドポイントの管理が行われていること

③セキュリティ管理ツールとエンドポイントがインターネットに接続されていること

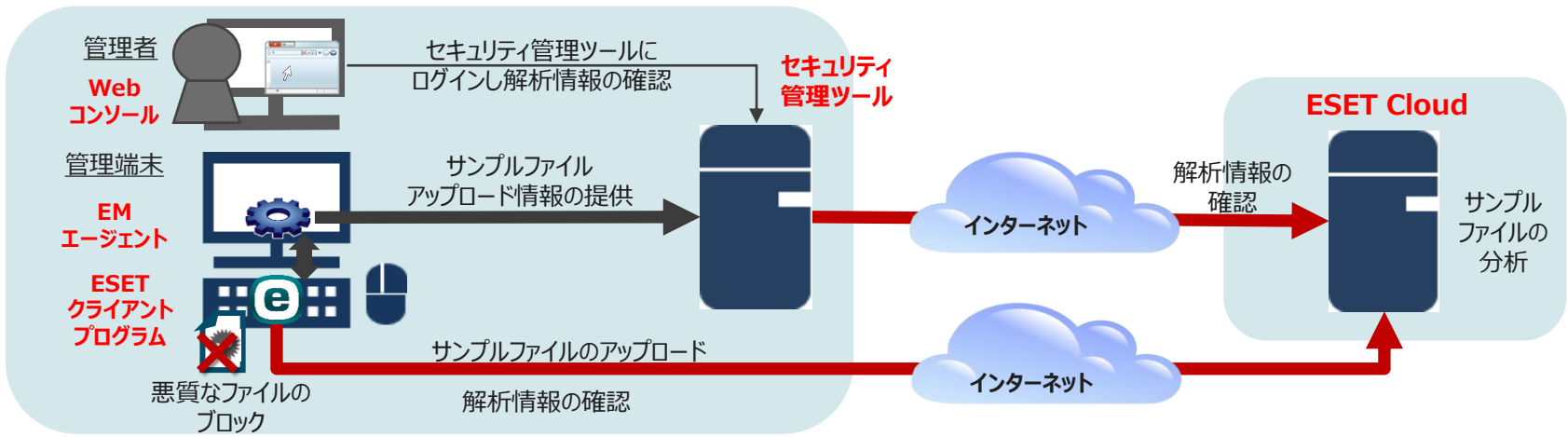
④エンドポイントにはELGAに対応したプログラムが導入されていること
対応プログラムは下記ページの[動作環境]よりご確認ください
https://canon.jp/business/solution/it-sec/lineup/eset/feature/cloud-sandbox

※EESM V8を管理される場合、クラウド型セキュリティ管理ツールをご利用ください。
オンプレミス型セキュリティ管理ツールでは、ELGAをご利用いただけません。(2024年12月現在)

3. ESET LiveGuard Advancedの構成

(2) コンポーネント

ESET LiveGuard Advancedは以下のコンポーネントから構成されています。



コンポーネント	
Webコンソール	管理者がセキュリティ管理ツールにログインして、分析情報やクライアントの情報を確認
EMエージェント	アップロードしたサンプルのリストをセキュリティ管理ツールに送信。Webコンソールから実施した設定変更やタスクの実行をESETクライアントプログラムに送信
ESETクライアントプログラム	サンプルのアップロード。分析情報の確認、悪質なファイルのブロック
セキュリティ管理ツール (ESET PROTECTまたはESET PROTECT on-prem)	分析結果の確認、管理端末へのタスクやポリシーの配布に使用
ESET Cloud	サンドボックス技術などでサンプルの分析(ライセンス毎に分離された環境)

4. ELGAの機能紹介

(1) エンドポイントプログラムの主な設定

サンプルの送信内容及び、分析で脅威と検出された場合の動作を指定します。

設定項目	内容
検出しきい値	分析結果に対して脅威として処理を行う際のしきい値を選択。 しきい値は「不審」、「非常に不審」、「悪意」の３段階より選択。
検出後のアクション	検出しきい値以上の脅威が検出された場合のアクションを選択。 「実行中の処理を停止して駆除」、「次回アクセス時に駆除」より選択。
不審なサンプルの自動送信	実行ファイル、アーカイブ、スクリプト、その他、考えられる迷惑メール、文書より選択。
サンプルの最大サイズ(MB)	1～64MBより指定。
ESETのサーバーから実行ファイル、アーカイブ、スクリプト、 他のサンプル、および可能性がある迷惑メールを削除	送信したサンプルをESETのサーバーから削除するタイミングを設定。 追加しない(※ESETのサーバーから削除しない)、30日後、分析後即時より選択。
除外	特定のファイルおよびフォルダをサンプルの送信対象から除外が可能。

エンドポイントプログラム(ESET Endpoint Security V11)の設定画面

非常に不審を選択した場合、
上位のしきい値である
・**悪意**
を含めて処理します

※本設定はエンドポイント毎に設定を行います。設定はセキュリティ管理ツールのポリシーを使用することでグループ毎または全台に一括で適用することができます。
※EEALはセキュリティ管理ツールのポリシーでのみ設定可能です。

4. ELGAの機能紹介

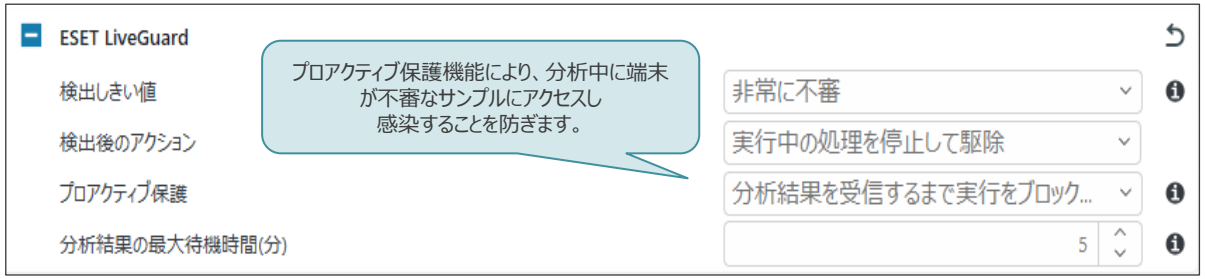
(2) プロアクティブ保護機能

メールまたはブラウザ経由でダウンロードされたファイルに関しては、分析結果が受信できるまで実行を保留させることができます。

設定項目	内容
分析結果の最大待機時間(分)	ESET Cloudの分析結果を受信するまでファイルの実行を待機させる最大待機時間を設定。 5分～60分より指定。
プロアクティブ保護	メールまたはブラウザ経由でダウンロードされたファイルの実行を、ESET Cloudの分析結果が 確認できるまで保留することが可能。 「実行をただちに許可する」、「分析結果を受信するまで実行をブロックする」より選択。

分析中のポップアップ画面

エンドポイントプログラム(ESET Endpoint Security V11)の設定画面

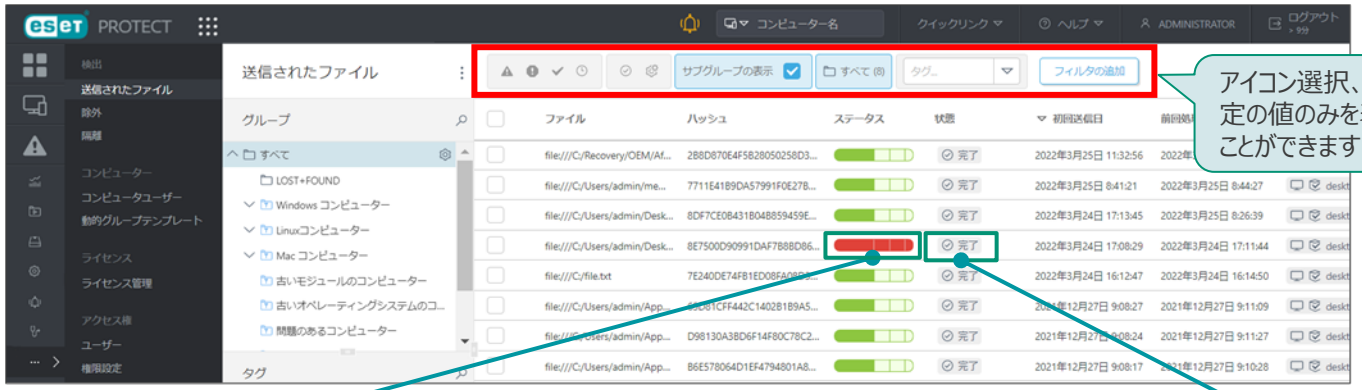


本機能の詳細は下記をご確認ください。
https://help.eset.com/elga/ja-JP/proactive_protection.html

4. ELGAの機能紹介

(3) 送信したサンプルファイルの一覧

セキュリティ管理ツールより、クライアントが送付したファイルの一覧及び分析情報を確認することができます。
並べ替え、ステータス・状態毎の表示、フィルタで特定の値のみを抽出して表示できます。



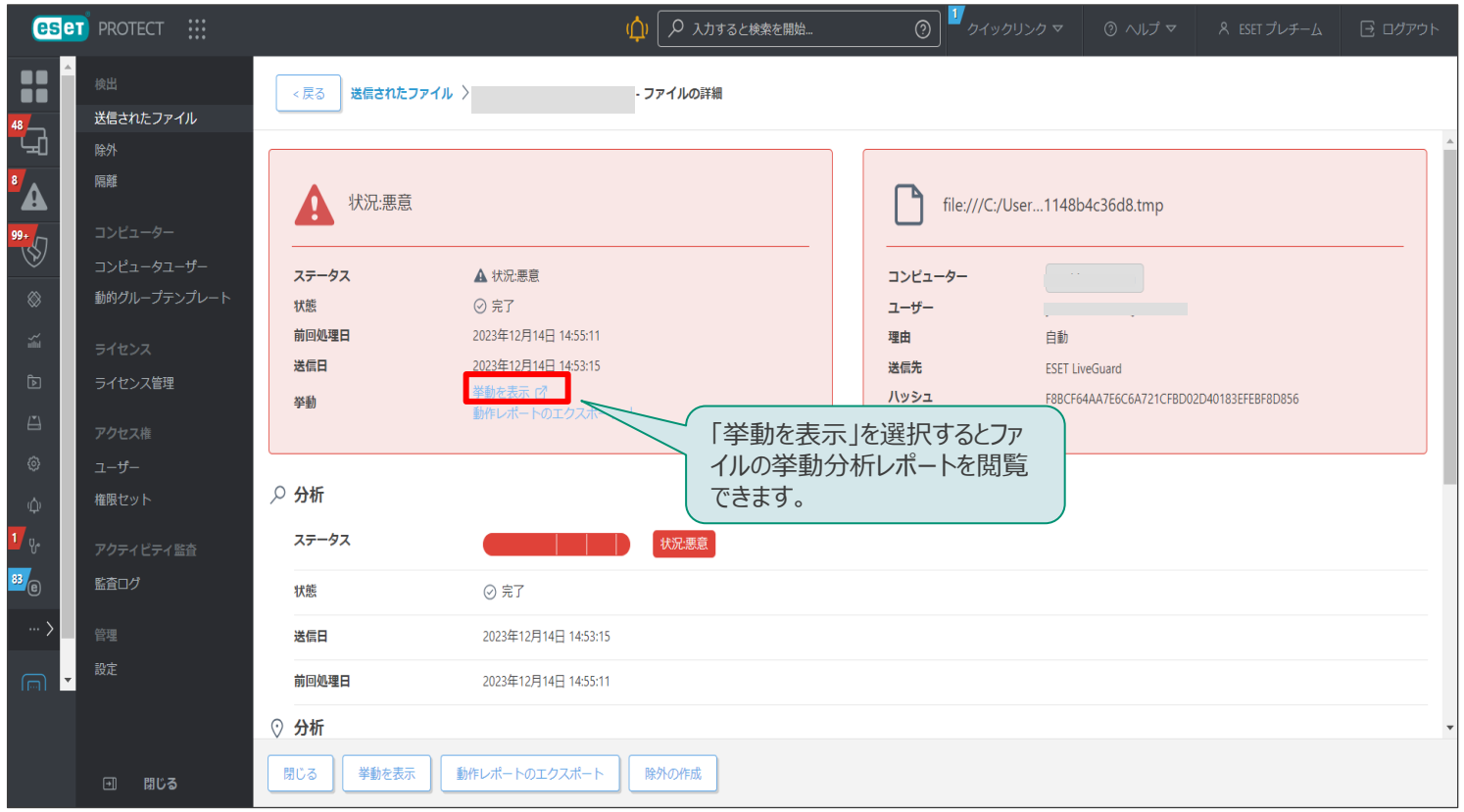
アイコン	ステータス	説明
	不明	ファイルは分析されませんでした。
	未感染	検出エンジンはサンプルを悪意があるものとして特定していません。
	不審 不審な可能性が高い	検出エンジンは不審であるとファイル動作を評価しましたが、明確に悪意があるわけではありません。
	悪意	ファイル動作は悪意があるとみなされます。

状態	説明
LiveGuard Advancedに送信	ファイルは分析のため ESET Cloudに送信されました。
分析中	分析を実行中です。
完了	ファイルが正常に分析されました。
再分析中	以前の結果がありますが、ファイルは再分析されています。

4. ELGAの機能紹介

(4) 送信したサンプルファイルの詳細

セキュリティ管理ツールよりクライアントが送付したサンプルファイルの詳細情報を確認することができます。



4. ELGAの機能紹介

(5) 解析結果のレポート(1/2)

セキュリティ管理ツールよりサンプルの解析結果のレポートを閲覧できます。状態より悪意があるかの判断、検出された挙動や特徴よりサンドボックスシミュレーションで観察された挙動などを把握できます。サンプルファイルによっては複数の挙動が含まれる場合があります。

※本画像はXDRソリューションが利用できない環境のレポート画面となります。XDRソリューションが利用できる環境は表示できるレポート画面異なります。詳細は次のページを確認ください。

ファイルの挙動分析レポート例 (ESET Inspect が利用できない環境の場合)

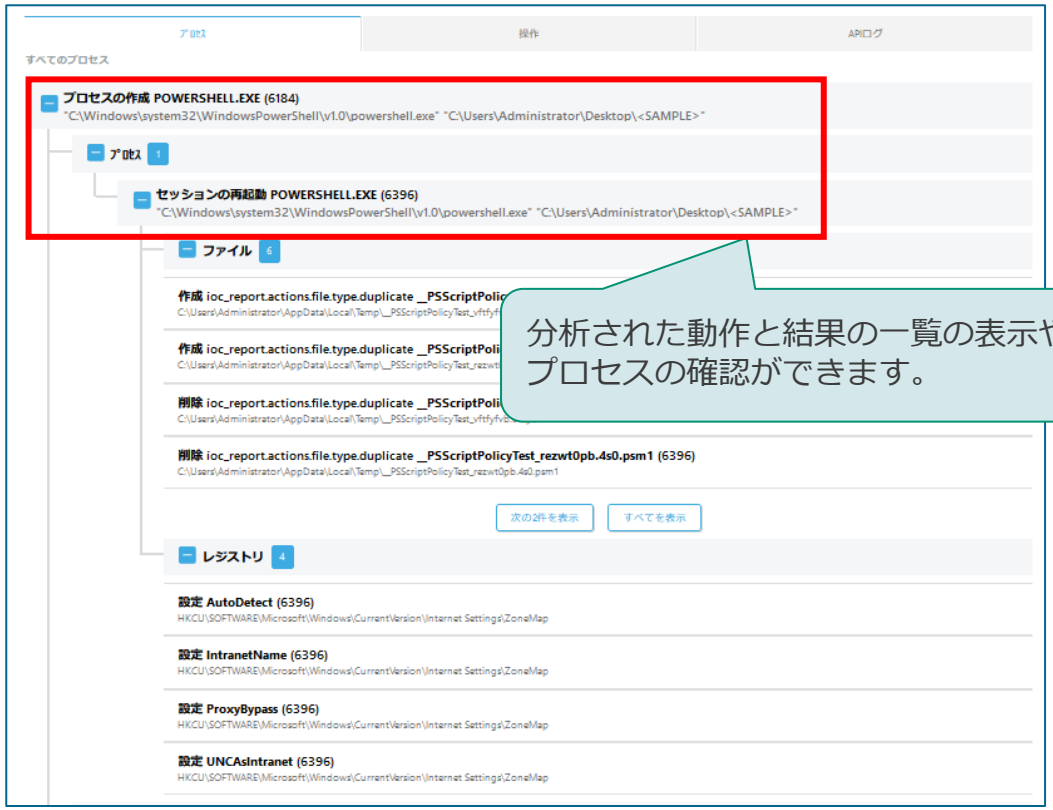
サンプルのハッシュ値などが確認できます。

4. ELGAの機能紹介

(5) 解析結果のレポート(2/2)

本画像はXDRソリューションが利用可能な環境のレポート画面となります。XDRソリューションが利用できない場合は表示できるレポート画面が異なります。詳細は前のページを確認ください。

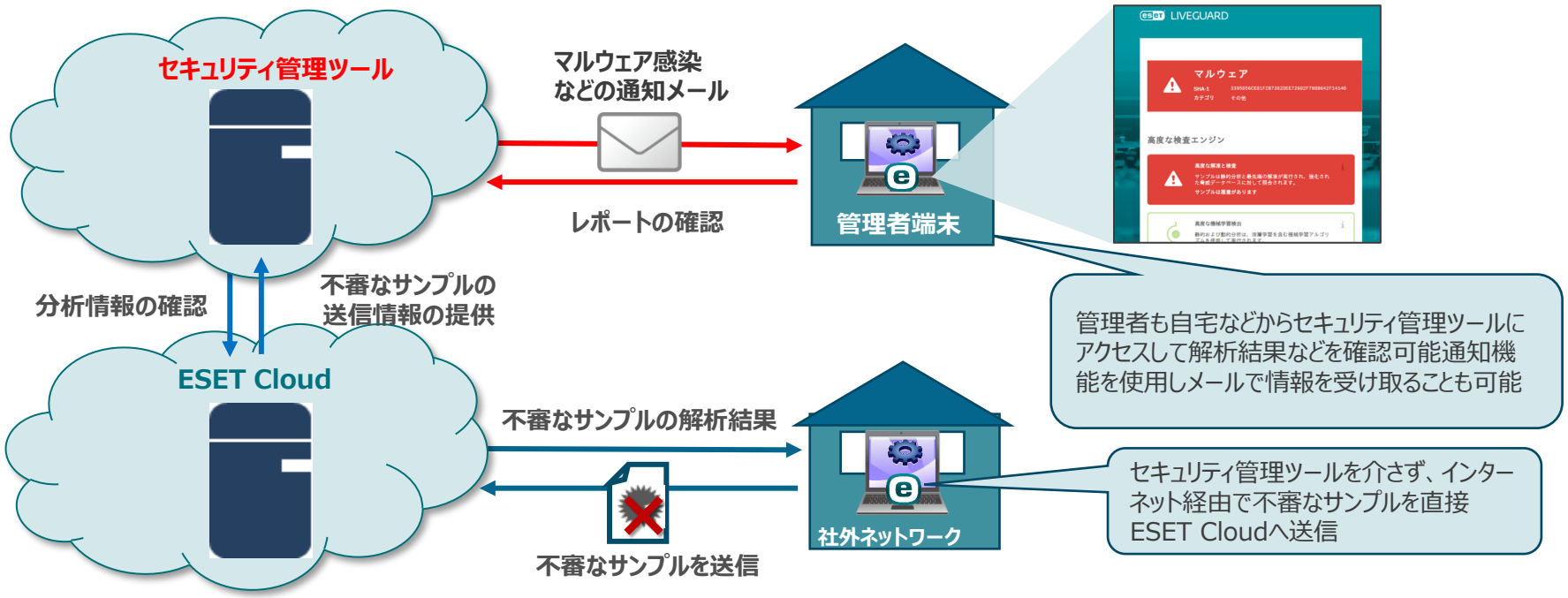
ファイルの挙動分析レポート例 (XDRソリューションが利用可能な環境の場合)



4. ELGAの機能紹介

(6) テレワークへの対応について

インターネットに接続できればESET Cloudへ不審なサンプルを送信できるため、外出時やテレワーク時も全社レベルで端末を保護することが可能です。クラウド型セキュリティ管理ツール「ESET PROTECT」を利用するなど、クライアント端末とセキュリティ管理ツールが通信できる場合は、管理者はESET Cloudに送信されたファイル情報や解析結果を社外からも確認することができます。

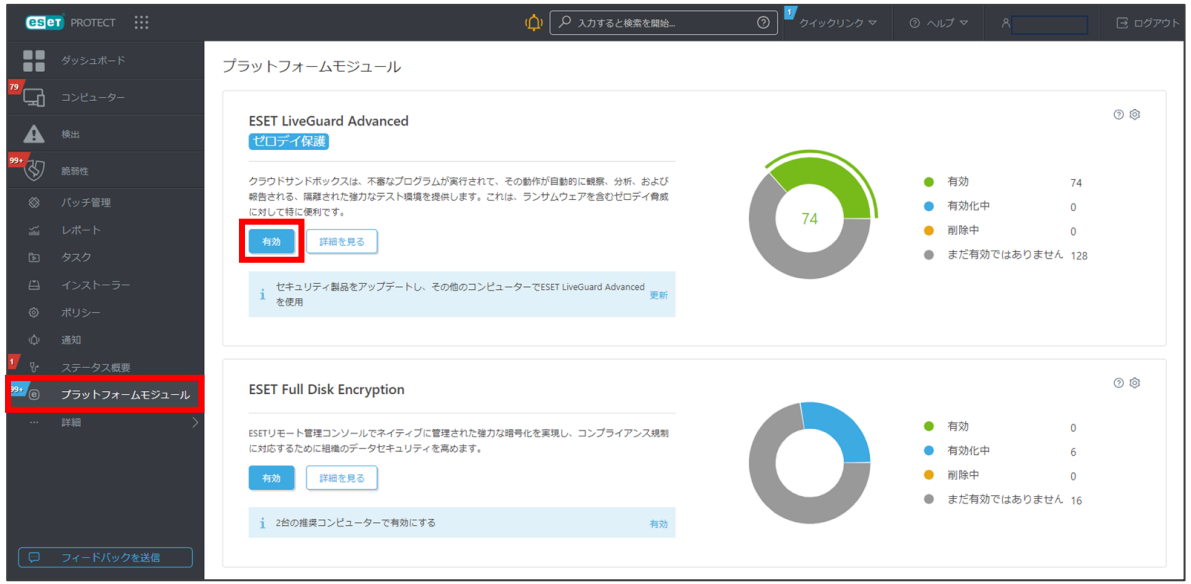


5. ELGAの有効化手順

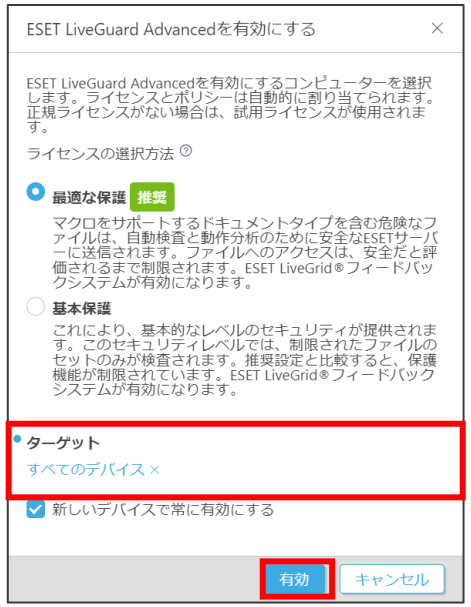
(1) アクティベーションタスクの実行 – プラットフォームモジュールから実行する場合 -

ELGAをご利用いただくためにアクティベーションの実施が必要です。以下のいずれかで実施ください。
・「プラットフォームモジュール」から実行する場合(本手順)
・タスクから実行する場合(p16~20)

① ESET PROTECTメインメニューの[プラットフォームモジュール]を選択し、ESET LiveGuard Advancedの[有効]をクリックします。



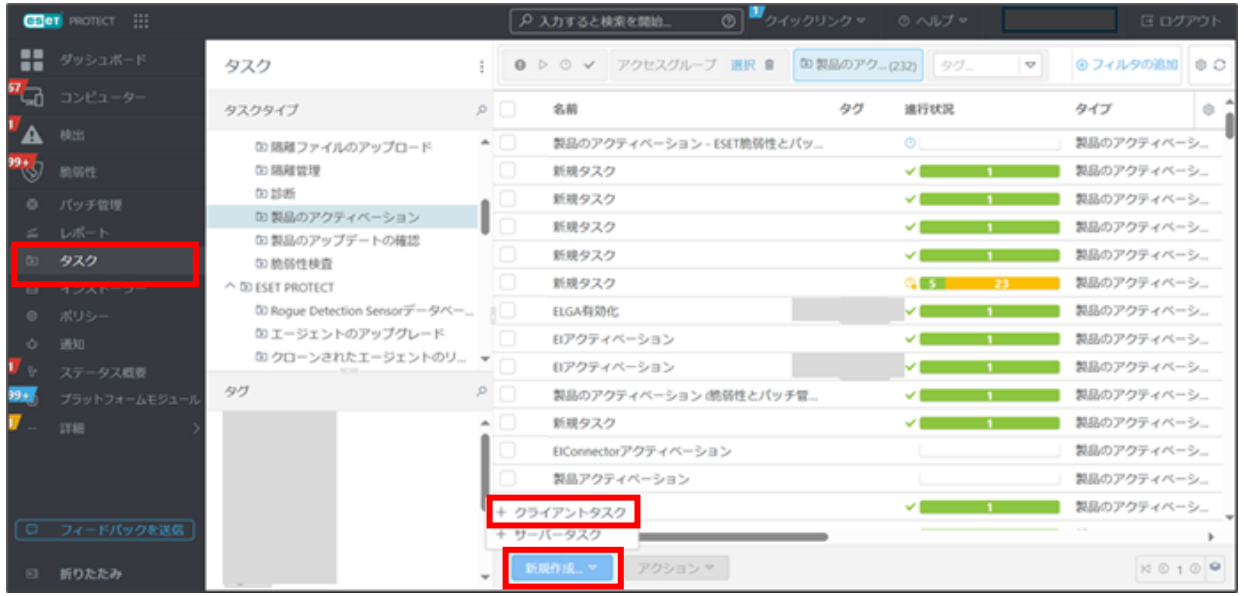
② 設定とターゲット(ELGAを有効化するデバイス)を選択し、[有効]をクリックします。



5. ELGAの有効化手順

(1) アクティベーションタスクの実行 – タスクから実行する場合 (1/5) -

① ESET PROTECTメインメニューの[タスク]-[新規作成]-[クライアントタスク]をクリックします。

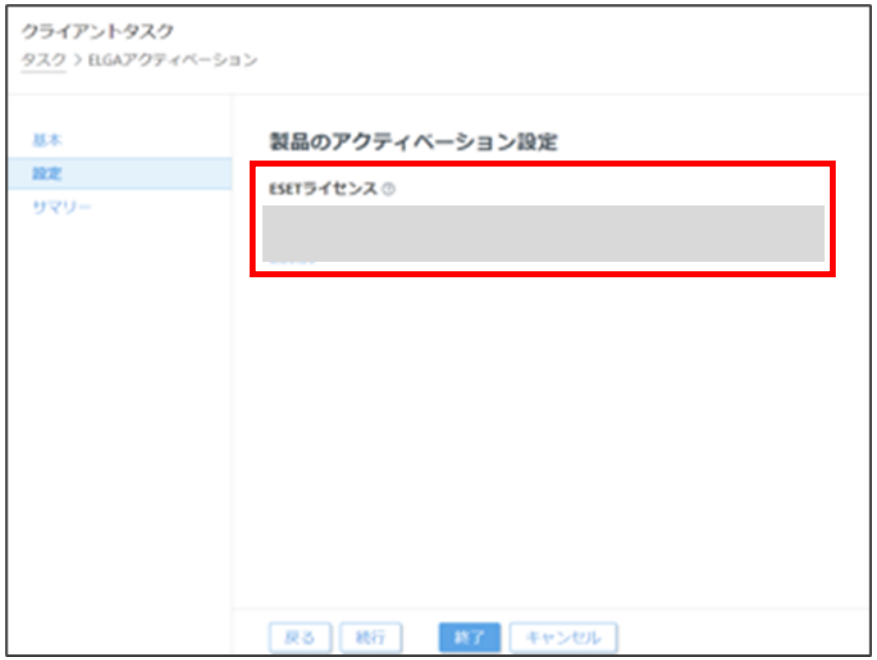


② [名前]欄に任意のタスク名を入力します。[タスク]欄では「製品のアクティベーション」を選択し、[続行]をクリックします。

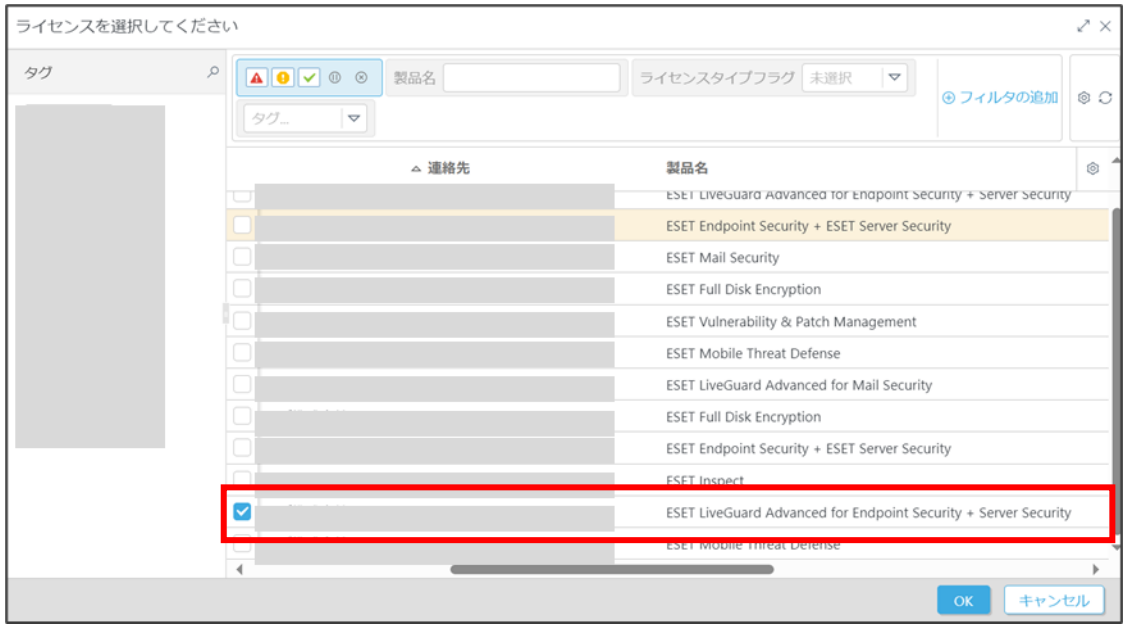
5. ELGAの有効化手順

(1) アクティベーションタスクの実行 – タスクから実行する場合 (2/5) -

③ [ESETライセンス]の下のライセンスをクリックします。



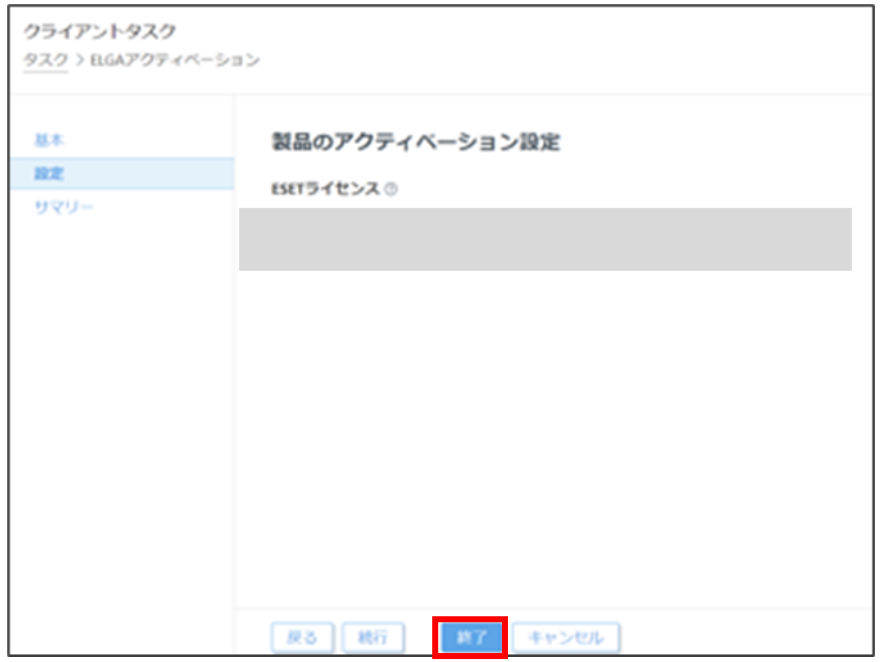
④ 「ESET LiveGuard Advanced for Endpoint Security + Server Security」を選択し、[OK]をクリックします。



5. ELGAの有効化手順

(1) アクティベーションタスクの実行 – タスクから実行する場合 (3/5) -

⑤ [終了]をクリックします。



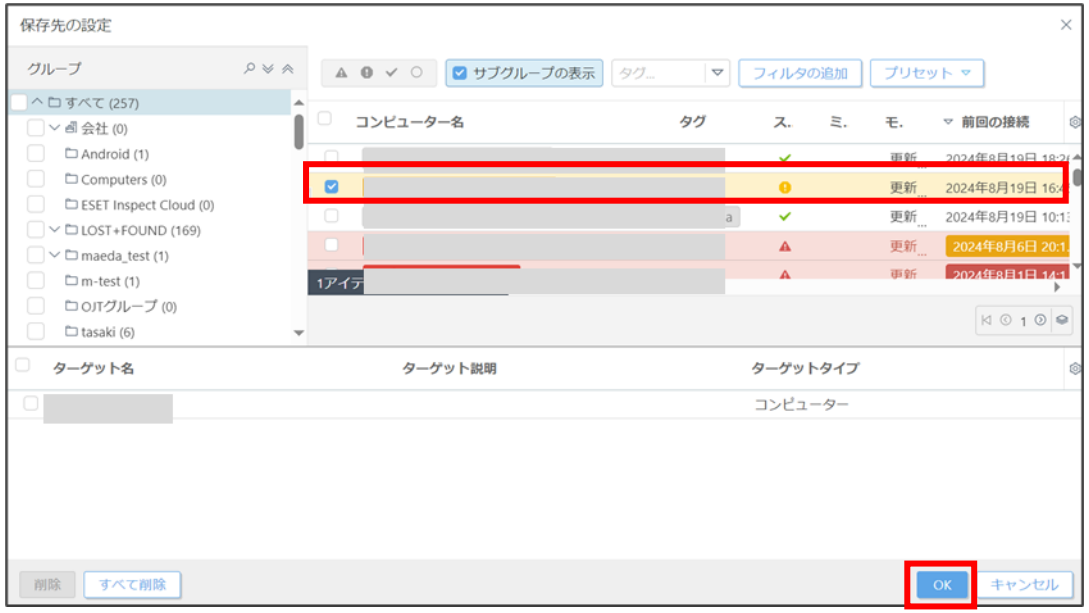
⑥ [トリガーの作成]をクリックします。

5. ELGAの有効化手順

(1) アクティベーションタスクの実行 – タスクから実行する場合 (4/5) -

⑦ [対象]-[ターゲットの追加]をクリックします。

⑧ アクティベーション対象のPC、またはグループを選択し、[OK]をクリックします。

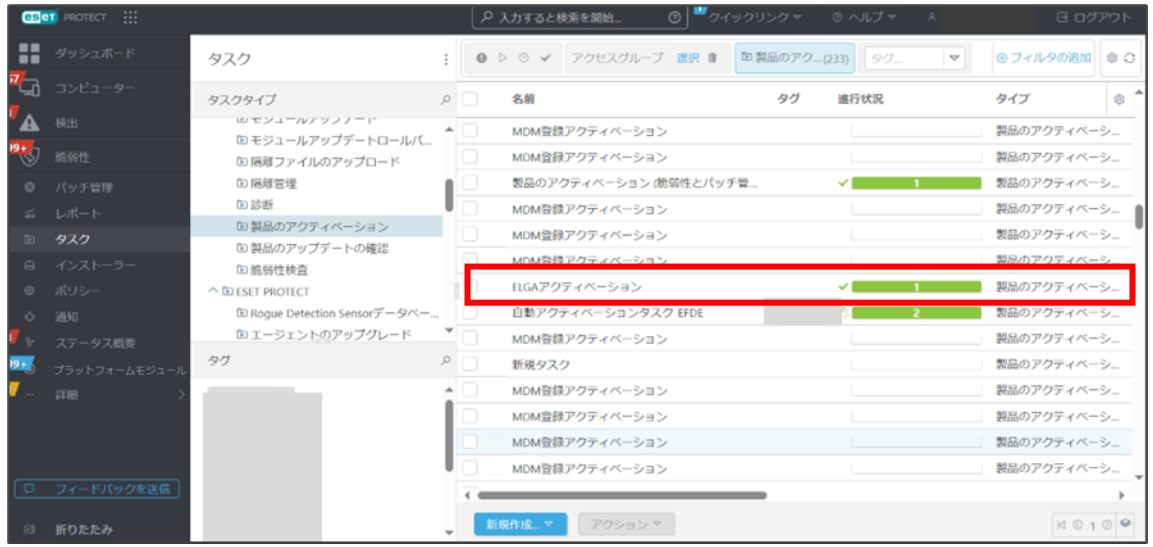


5. ELGAの有効化手順

(1) アクティベーションタスクの実行 – タスクから実行する場合 (5/5) -

⑨ [終了]をクリックします。

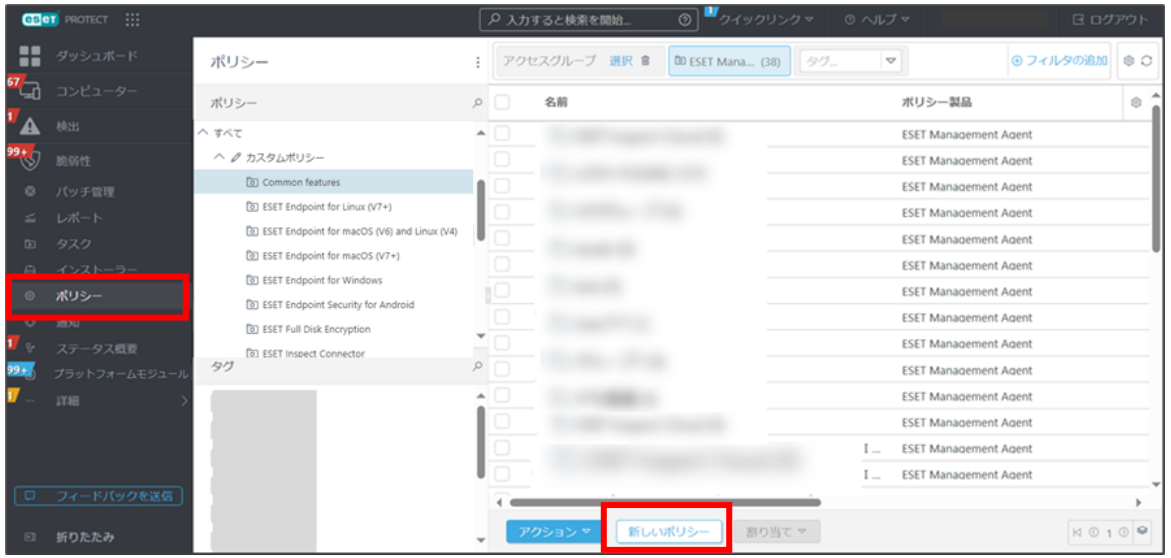
⑩ 該当タスクの進行状況が緑色に遷移したらタスク成功です。



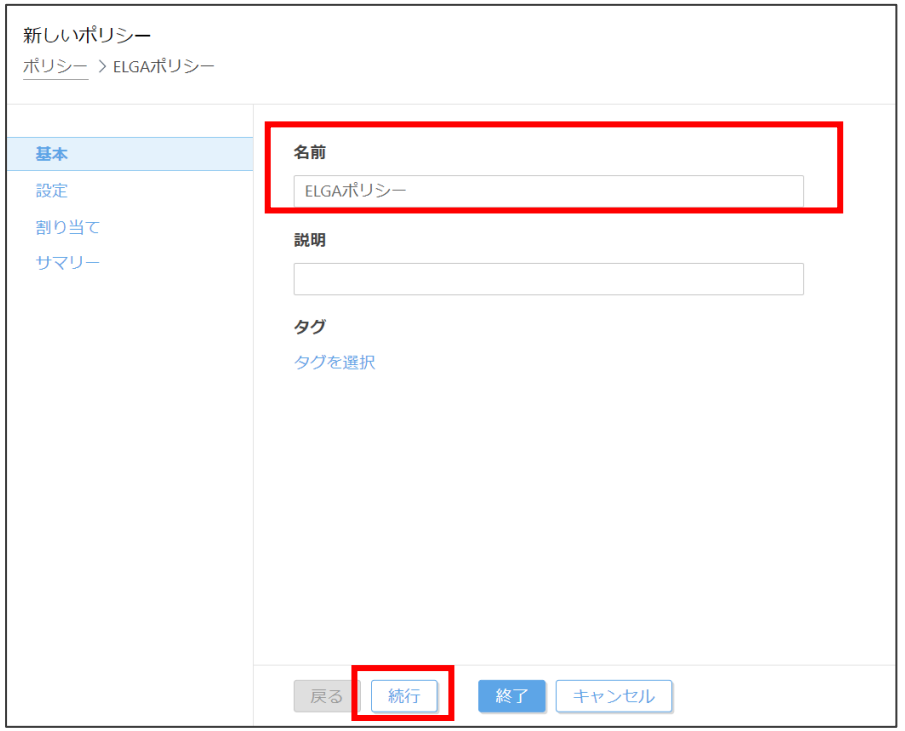
5. ELGAの有効化手順

(2) ELGA機能の有効化(1/4)

① ESET PROTECTメインメニューの[ポリシー]-[新しいポリシー]をクリックします。



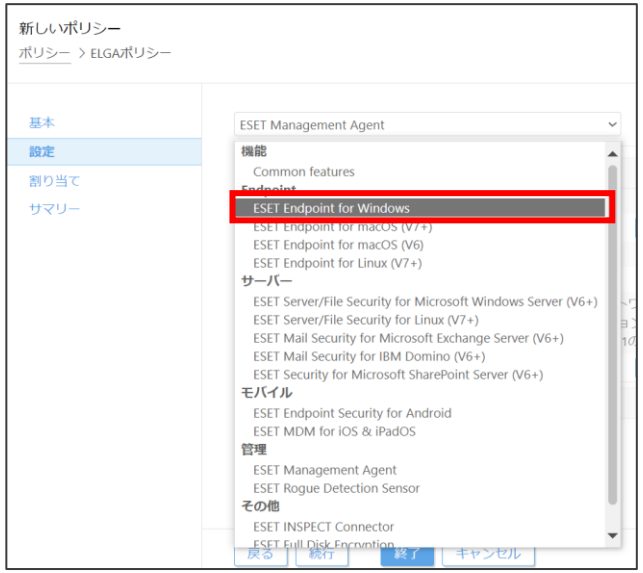
② [名前]欄に任意のタスク名を入力し、[続行]をクリックします。



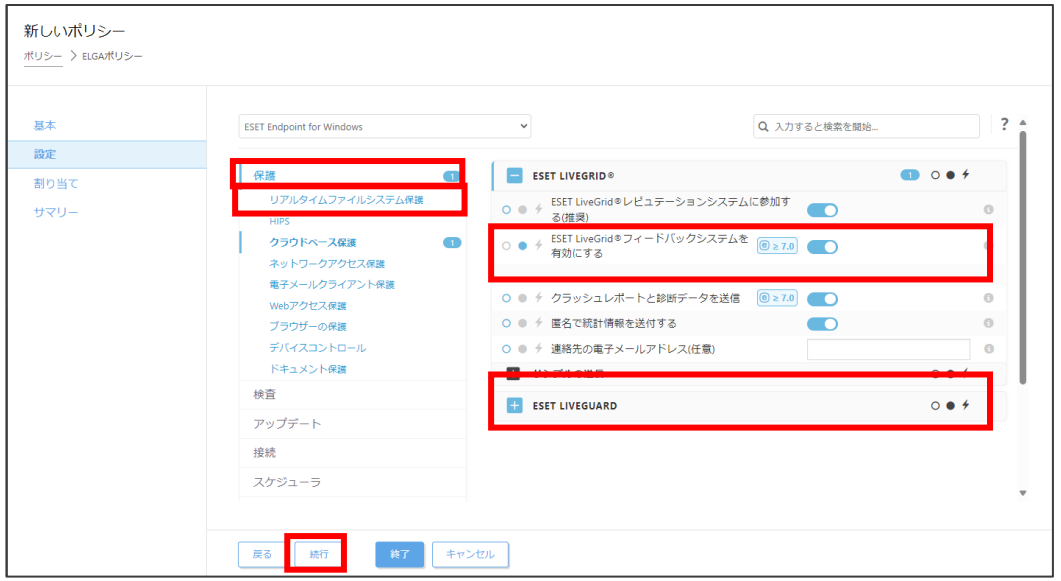
5. ELGAの有効化手順

(2) ELGA機能の有効化(2/4)

③ プルダウンメニューより、ご利用のプログラムを選択します。
※本手順では、[ESET Endpoint for Windows]を選択します。



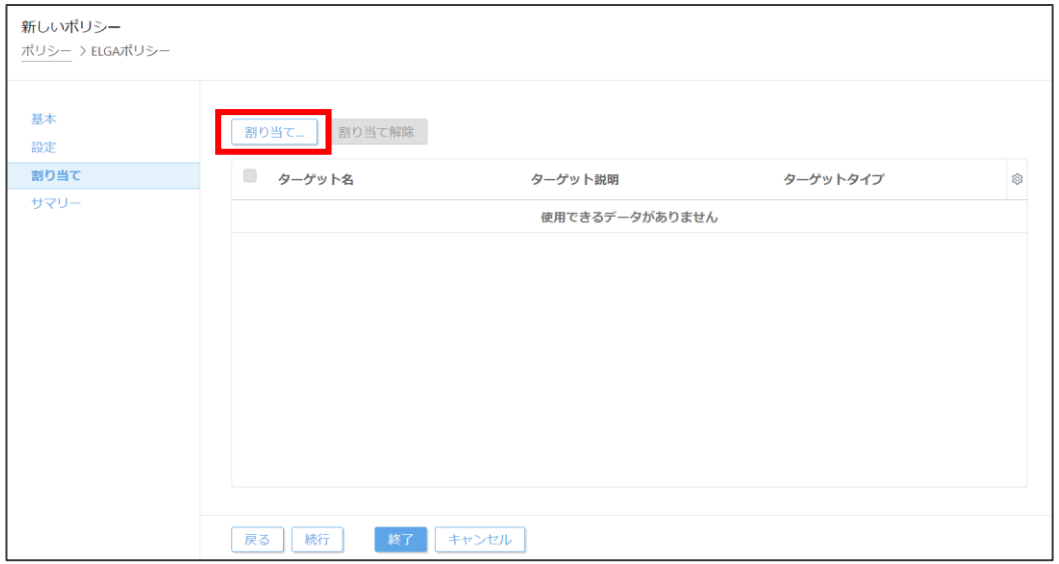
④ [保護]-[クラウドベース保護]を選択します。[ESET LiveGridフィードバックシステムを有効にする]を有効にし、「サンプルの送信」、「ESET LIVEGUARD」の各項目の設定を行います。設定が完了したら、[続行]をクリックします。



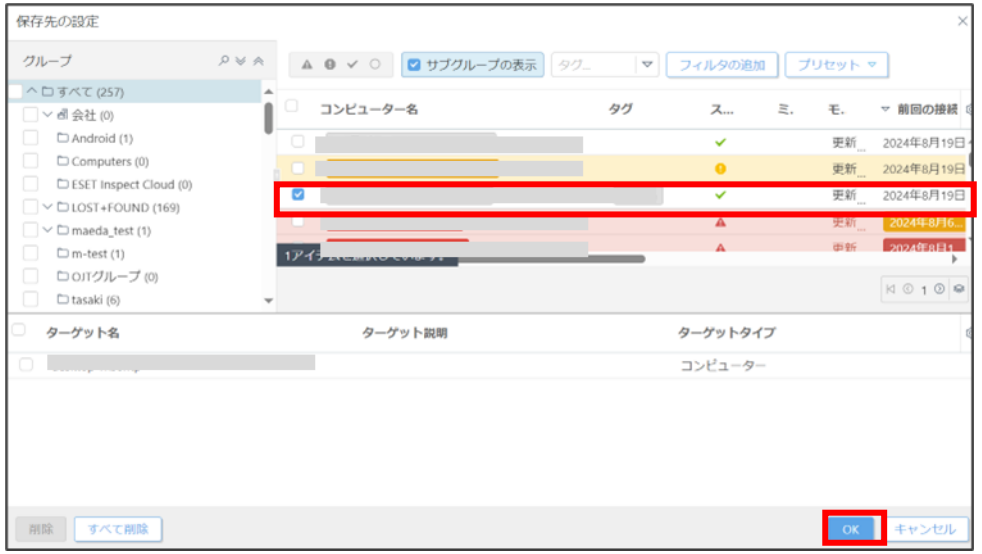
5. ELGAの有効化手順

(2) ELGA機能の有効化(3/4)

⑤ [割り当て]をクリックします。



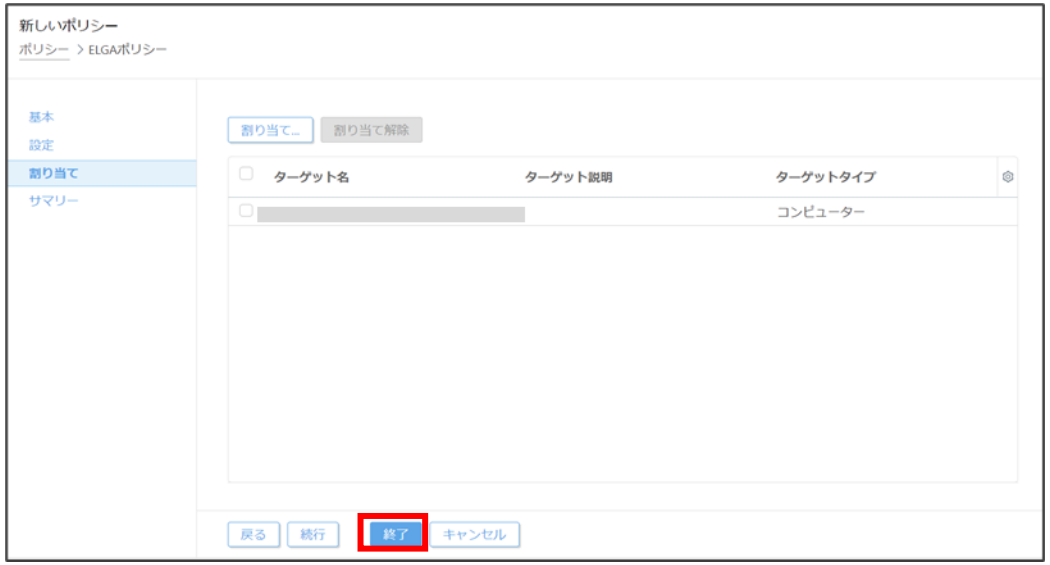
⑥ ポリシーを割り当てたいコンピューターを[グループ]もしくは[コンピューター名]から選択し、[OK]をクリックします。



5. ELGAの有効化手順

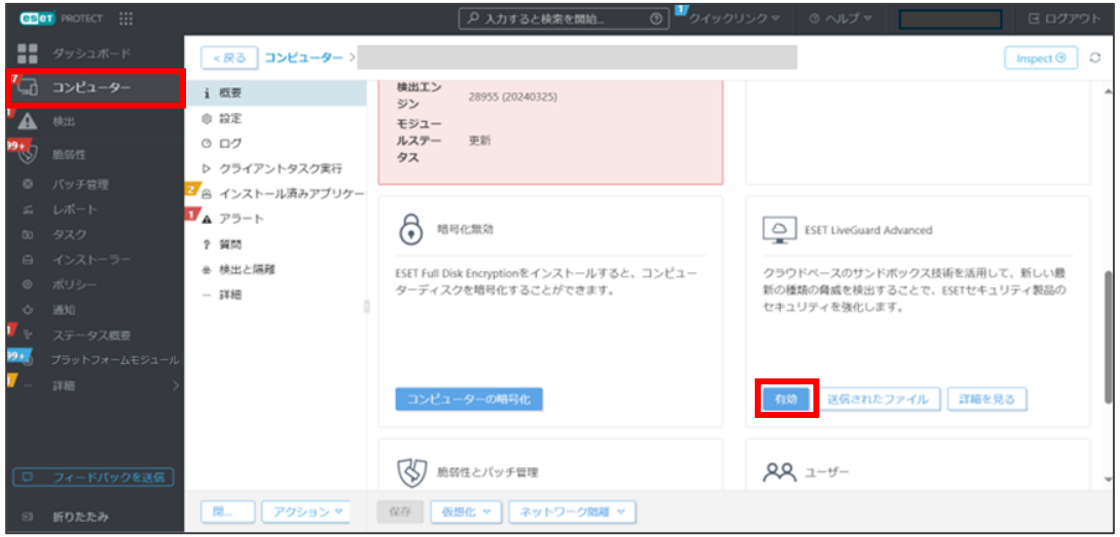
(2) ELGA機能の有効化(4/4)

⑦ [終了]をクリックします。



【参考】

メインメニューの[コンピューター]画面にて、各コンピューターの[詳細を表示]-[概要]-[ESET LiveGuard Advanced]の「有効」ボタンより、ELGA機能の有効化を行うことも可能です。



6. 参考情報

ESET LiveGridとの違い

ESET製品では以前よりESET LiveGridを使用してクラウド環境に不審なファイルの自動送信や手動による分析を依頼できました。
ELGAを使用することで分析結果の閲覧および、悪意があると判断された場合に自動保護を即時に実施することができるようになりました。

項目	ESET LiveGuard Advanced	ESET LiveGrid
ファイルの提出	自動/手動	自動/手動
分析結果	ESET PROTECT / ESET PROTECT on-prem のレポートで確認可能	分析結果は未公開
結果の種類	未感染、不審、非常に不審、悪意	なし
提供される情報	ファイルの動作結果と詳細な記述	なし
分析に使用される技術	サンドボックスを用いた高度な検出手法と 行動分析および機械学習を組み合わせた 多段分析を使用	DNA検出や様々な機械学習モデルを用いた ファジーハッシングを使用
サンプル分析の優先順位	高	低
インタフェース	EP Web Console / EP on-prem Web Console	なし
サポートされる ESET製品	下記ページの[動作環境]をご確認ください https://canon.jp/business/solution/it-sec/lineup/eset/feature/cloud-sandbox	すべてのESETセキュリティ製品
会社全体の自動保護	あり	なし

7. マルウェアの検出事例

(1) 解析の迅速性

弊社の検証環境で検出された「ステガノグラフィー」を用いた実際のマルウェアの検出事例をもとに
「ELGAの解析の迅速性と高度な解析技術」の2点をご紹介します。

(マルウェア検出までの流れ)
①「ばらまき型メール攻撃」でメールを受信
②メールに添付されたExcelファイルをESET Cloudに自動送信、解析を依頼
③解析の結果「悪意」と認定、各エンドポイントでブロックを実施。
※本マルウェアは弊社ELGA検証環境での検知3時間後に検出エンジンに追加。エンドポイント製品でも検知可能に。

ポイント
・メールに添付されていたExcelファイルを自動的に解析を依頼
・複数の高度な手法を用いて検出の回避を狙ったファイルを迅速に解析 (詳細は次ページ参照)

7. マルウェアの検出事例

(2) 高度な解析技術

検出されたマルウェア(DOC/Agent.DZ)には、高度に解析を妨害・回避する処理が複数存在

※マルウェア(DOC/Agent.DZ)の詳細な情報は、弊社マルウェアレポート2019年6月号を参照
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1906.html

【本マルウェア(DOC/Agent.DZ)に実施されていた主な解析の妨害・回避手法】

・ExcelファイルのVBAのコードにロックを掛け解析を妨害
・VBAが実行された環境が日本語環境でない場合、処理を終了させることで解析を回避
・PowerShellコマンドを多重に難読化し解析を妨害
・PowerShell v3.0以降がインストールされている環境のみで稼働、それ以外は処理を終了させることで解析を回避
・攻撃用データを画像ファイルに高度に隠蔽(ステガノグラフィー)し、検出と解析を回避

ポイント
エンドポイント製品やサンドボックス製品で検知が行われないように、高度で巧妙な解析の妨害・回避処理が複数実施されていたが、ELGAは「悪意」があるマルウェアとして検出を実施。

※ステガノグラフィーとは (詳細は2018年10月マルウェアレポートを参照)
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1810.html#anc_02