ESET PROTECTソリューション

ESET PROTECT Eliteスターターガイド

第11版

2024年4月22日

キヤノンマーケティングジャパン株式会社

はじめに

近年のサイバー攻撃は、非常に複雑かつ巧妙化されているため、
従来のセキュリティ対策だけでは防ぎきれないケースも多く見られるようになってきました。

そこで注目されているのが **XDR(eXtended Detection & Response)**です。
XDR は、「攻撃を防ぐこと」を目的とした従来のアンチウイルスソフト等のセキュリティ対策製品とは違い、異なるセキュリティ製品・レイヤーで収集された様々な種類のイベントデータを統合して、エンドポイントでの調査、対応、ハンティングを適切かつ迅速に行うことを目的としています。

したがって、近年のサイバー攻撃への対策では、従来の「事前対策」に加え、XDR による「事後対策」を合わせる方策が必要とされています。

XDRは様々なレイヤーで常時データを収集し、それらを分析して怪しい挙動を発見するため、日々の監視や運用が重要です。
そこで、XDRを導入する企業は、その運用負荷を軽減するため、セキュリティ会社が提供する **MDR(Managed Detection & Response)**を利用して、XDRの監視や運用をアウトソーシングすることが求められています。

本資料では、ESETのXDRである**「ESET Inspect/ESET Inspect on-prem」** がご利用いただける**「ESET PROTECT Elite」**についてご紹介します。

※ 「 ESET Inspect Cloud （旧名称）」から「ESET Inspect（新名称）」へ名称を変更いたしました。
※ 「 ESET Inspect （旧名称）」から「ESET Inspect on-prem （新名称）」へ名称を変更いたしました。
※ 本資料はクラウド型XDRである「ESET Inspect 」をメインに記載してあります。
※ ESETが提供するMDRをご利用いただくには、 「ESET PROTECT MDR Ultimate」または「 ESET PROTECT MDR Lite」をご契約いただく必要があります。

はじめに

本資料は、 ESET PROTECTソリューションのうち、 ESET PROTECT Eliteをご検討いただいているお客様に、本ソリューションで利用可能なプログラムやサービス、製品の利用開始方法などをご理解いただくことを目的としております。

- 対象ソリューション： **ESET PROTECT Elite**
- 対象プログラムとサービス (2024年4月時点)

プログラム名/サービス名	プログラム/サービス概要	最新バージョン	XDRによる管理
ESET Endpoint Security (EES)	Windowsクライアント用	V11.0	●
ESET Endpoint アンチウイルス (EEA)			
ESET Endpoint Security for OS X (EESM)	Macクライアント用	V6.11	●
ESET Endpoint アンチウイルスfor OS X (EEAM)		V7.4	
ESET Endpoint アンチウイルス for Linux (EEAL)	Linuxデスクトップ用	V10.2	●
ESET Endpoint Security for Android (EESA)	Android用	V4.2	×
ESET Server Security for Microsoft Windows Server (ESSW)	Windowsサーバー用	V10.0	●
ESET Server Security for Linux (ESSL)	Linuxサーバー用	V10.2	●
ESET LiveGuard Advanced (ELGA)	クラウドサンドボックス	常に最新版を提供	-
ESET Full Disk Encryption (EFDE)	フルディスク暗号化	V1.4	-
ESET Cloud Office Security (ECOS)	クラウドアプリケーションセキュリティ	常に最新版を提供	-
ESET Vulnerability & Patch Management (VAPM)	脆弱性とパッチ管理	常に最新版を提供	-
ESET Inspect (EI)	クラウド型XDR	常に最新版を提供	-
ESET Inspec on-prem (EI on-prem)	オンプレミス型XDR	V2.0	-
ESET PROTECT (EP)	クラウド型セキュリティ管理ツール	常に最新版を提供	-
ESET PROTECT on-prem (EP on-prem)	オンプレミス型セキュリティ管理ツール	V11.0	-

もくじ

※ オンプレミス型のセキュリティ管理ツールとXDRコンポーネントをご利用いただく場合は、
ユーザーズサイトに掲載されているプログラムをダウンロードいただき、それぞれの構築資料をご参照ください。

Ⅰ．セキュリティの考え方について

1. eXtended Detection & Responseとは

EPPの防御をすり抜けた攻撃を検知して封じ込め、調査から復旧までを行うソリューション！

パターンマッチング・**機械学習・サンドボックス**などを利用した防御

マルウェア感染・外部からの不正アクセスなどを検知

攻撃を受けた端末の**隔離**・マルウェア感染拡大の**抑え込み**

サイバー攻撃**内容・被害状況の把握**

感染端末からの**マルウェア除去**

侵入される前提の対策が必要

XDRを導入した場合

早期に攻撃を発見し
被害を抑えられる

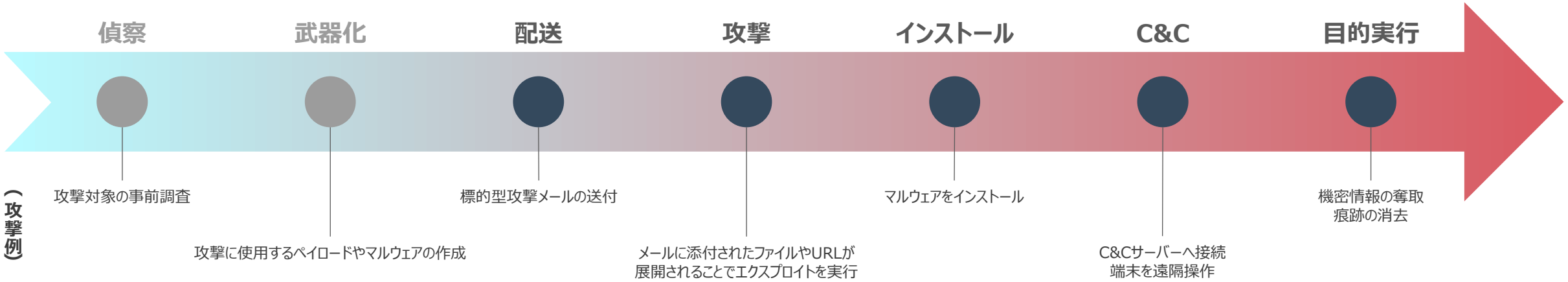
感染拡大を抑え
業務停止時間を短くできる

侵入経路や影響範囲、漏えいした情報の
把握が容易になる

復旧にかかる
時間と手間を抑えられる

2. サイバー攻撃の流れについて

発見が遅れると命取りに！早期対処にはXDRの活用が効果的！



サイバー攻撃は侵害が進むにつれて
対応が難しくなるため、
前半部分で検知できる仕組みが必要！

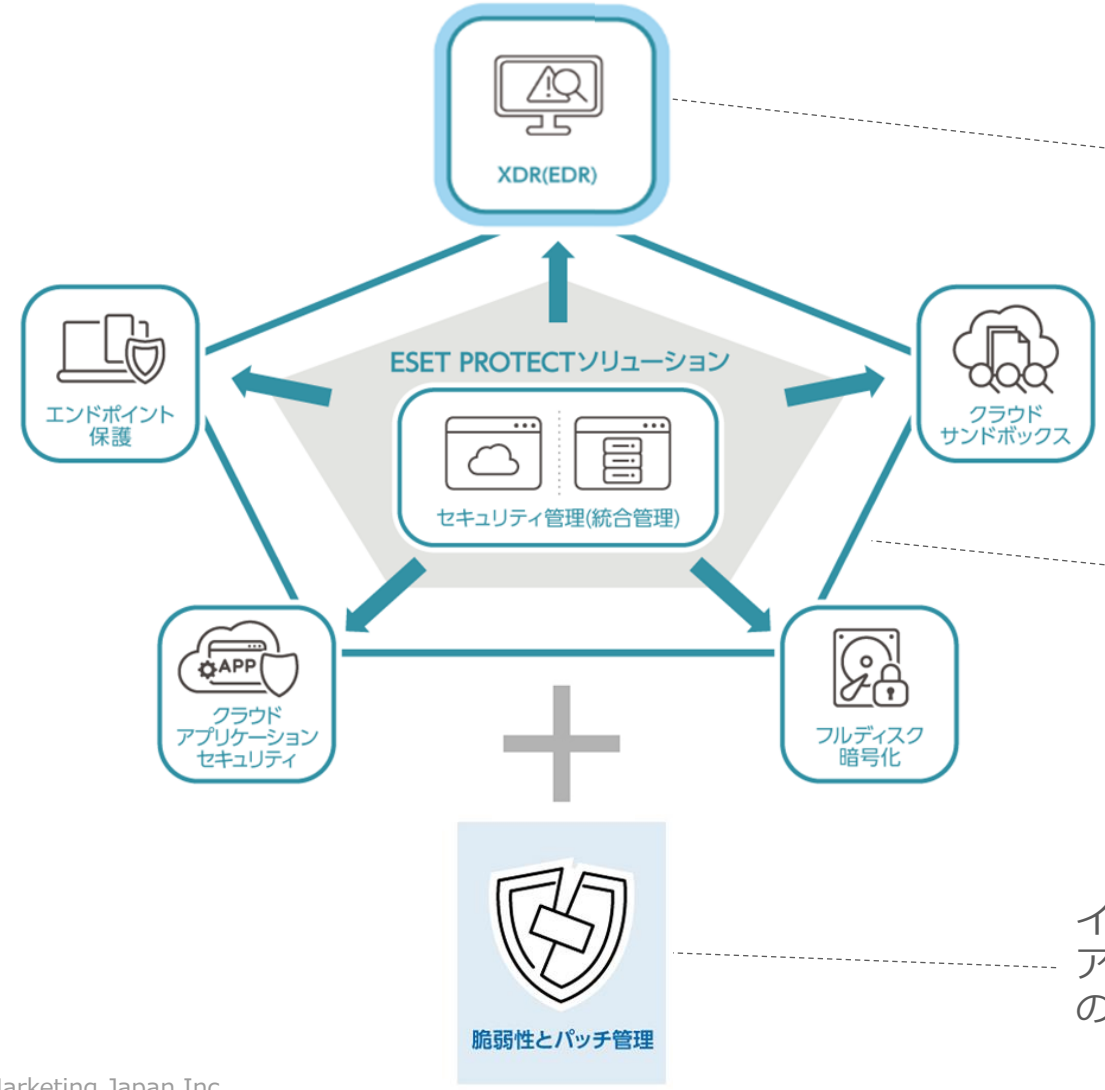
⚠ サイバー攻撃による実被害の例

- Webサイトの改ざん
- システム破壊
- ボットネットによるDDoS攻撃
- 機密情報窃取　etc…

大切な資産に脅威が及ぶ前に対処できれば、攻撃の成立を阻止できる

3. ESETが提供するXDRソリューション

ESETなら各種対策をパッケージ化した包括的なエンドポイントセキュリティソリューションをご提供！



異なるセキュリティ製品・レイヤーで収集された様々な種類のイベントデータを統合して、エンドポイントでの調査、対応、ハンティングを適切かつ迅速に行うXDR

エンドポイント対策から高度サイバー攻撃に対応するクラウドサンドボックス、端末持ち出し時の情報漏洩対策、Microsoft365へのクラウドアプリケーションセキュリティをワンストップでご提供

インストールしているアプリケーションを自動スキャンし、アプリケーションとデバイスの脆弱性を検出、修正パッチの適用を実施

Ⅱ．主な機能の紹介

1. ソリューションの概要

Digital Security
Progress. Protected.

ESETが提供するXDRソリューションについて

事後対策のニーズ

- 社内に潜む潜在的な**脅威を早期に発見**したい
- 社内ネットワークで何が起きているかを**リアルタイムで可視化**したい
- セキュリティ**インシデント対応**(影響調査や原因調査)を**高速化・効率化**したい
- 万が一侵害が発生した際の**被害の抑制**(封じ込めや除去)を短時間で行いたい
- ランサムウェアによるデータ**流出の防止や早期発見**ができる仕組みを備えたい
- 事前対策(EPP)から事後対策(XDR)まで、**ワンベンダー**でまとめて効率的に運用したい

XDR運用のニーズ

専門家へのアウトソース

- **24/365の運用**を委託したい
- XDRのアラート**分析を専門家に**任せたい
- インシデント対応や復旧、調査分析に**専門家の協力**を得たい

自社運用

- **自社ポリシーに沿って**運用したい
- **自社のSOCやCSIRT**で運用したい

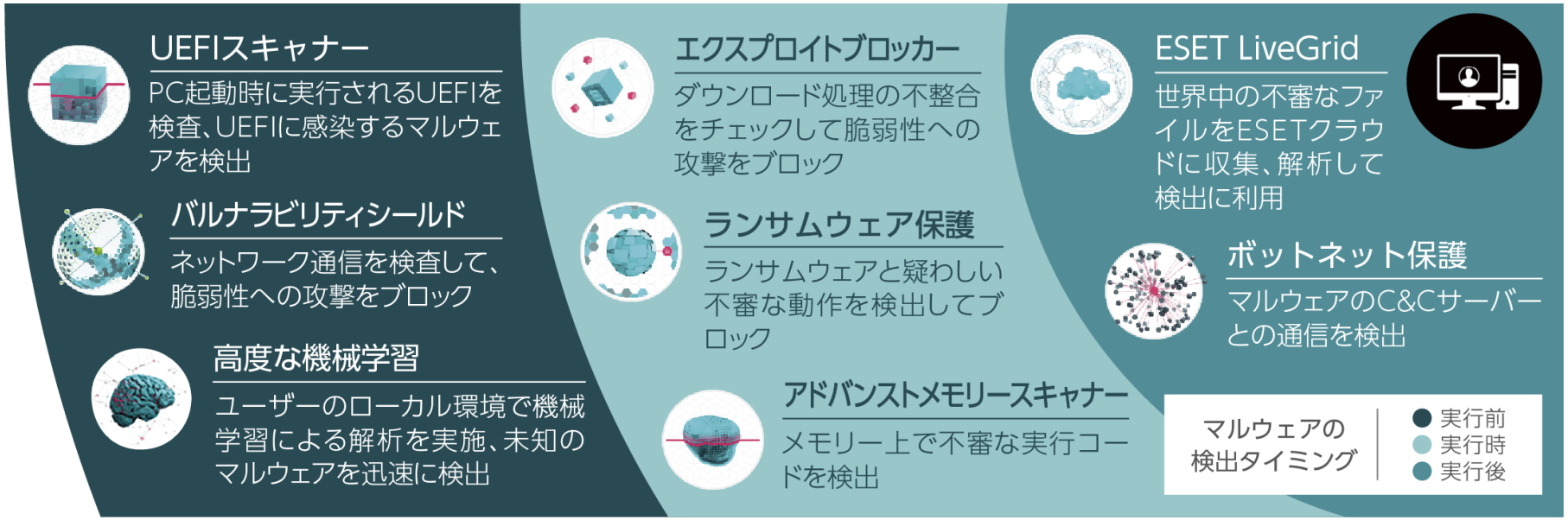
	クラウド型セキュリティ管理ツール	オンプレミス型セキュリティ管理ツール	基本的なエンドポイント保護	総合的なエンドポイント保護	クラウドサンドボックス	フルディスク暗号化	クラウドアプリケーションセキュリティ	脆弱性とパッチ管理	XDR	MDRサービス	プレミアムサポートサービス
ESET PROTECT MDR 専門家へのアウトソース	●	●	●	●	●	●	-	-	●	●	●
ESET PROTECT ELITE 自社運用	●	●	●	●	●	●	●	●	●	-	-

* MDRサービスおよびプレミアムサポートサービスを利用される際はセキュリティ管理ツールおよびXDRともクラウド利用が前提となります。
* XDRはクラウド/オンプレミスどちらも利用できます。XDRの利用環境(クラウド/オンプレミス)とセキュリティ管理ツールの利用環境(クラウド/オンプレミス)は同一が前提となります。

2. 製品概要 -Endpoint Protection Platform- (1/2)

エンドポイント保護の特徴

多層防御で新種の脅威に対する保護を強化

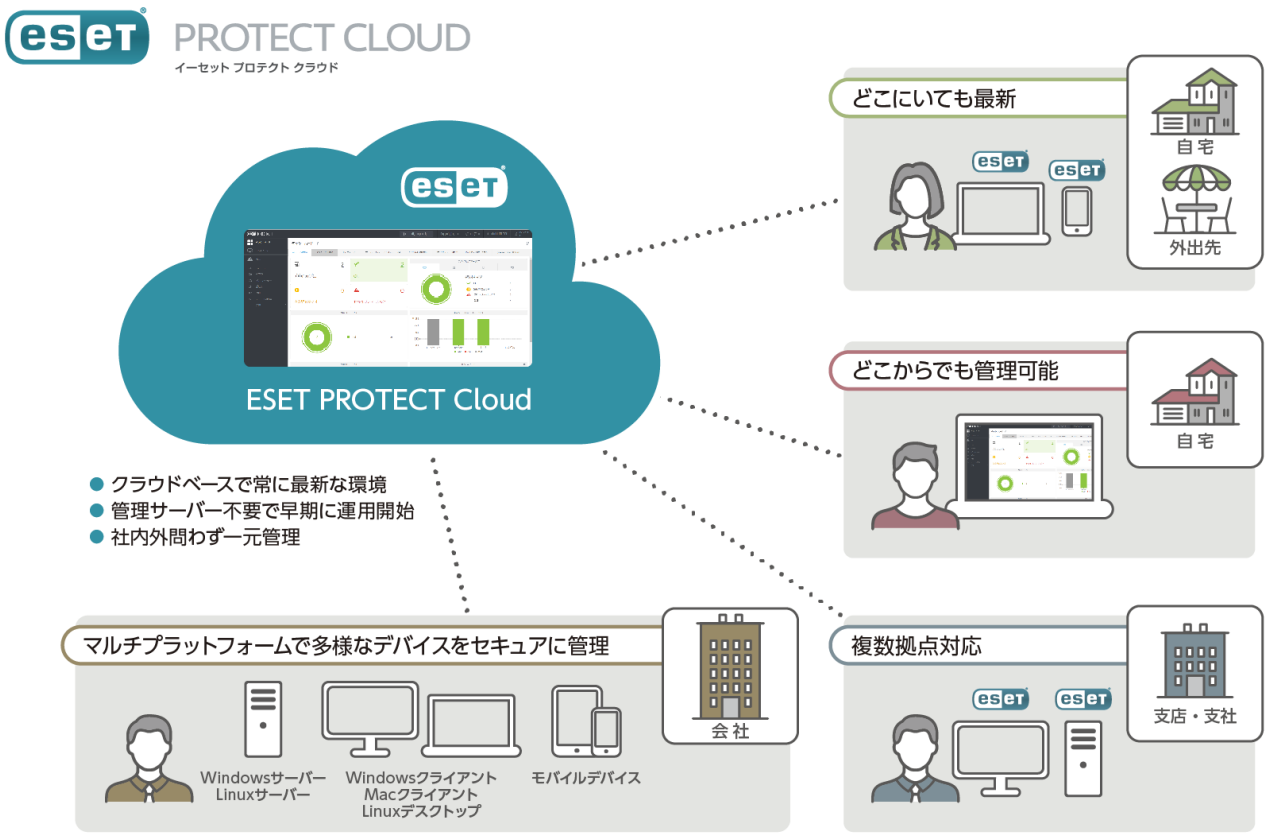


高度化・巧妙化する脅威に対抗するため、マルウェアの起動時だけではなく、その前後も含めた複数のタイミングで攻撃の手法に合わせた方法で検査を行います。新バージョンで新たに加わった高度な機械学習機能は、従来ESET社のクラウド環境でおこなっていた機械学習による解析をユーザーのローカル環境で実施し、より迅速にマルウェアかどうか判定できるようになりました。

※ Windowsクライアント用/Windowsサーバー用プログラムの最新バージョンではすべての機能が搭載されています。
ただし、その他のプログラムや旧バージョンにおいては一部の機能が搭載されていない場合があります。

2. 製品概要 -Endpoint Protection Platform- (2/2)

ESET PROTECT の特徴



※ESET PROTECT Cloud はクラウド型セキュリティ管理ツールESET PROTECT の旧名称です。

管理サーバー不要で早期に運用開始

EPはSaaS型であるため、サーバーの機器の購入や定期的なメンテナンスによる手間とコストを削減することができます。また、セットアップもWebブラウザ経由で10分程度で実施することが可能なため、すぐに運用を開始させることができます。

社内外問わず一元管理

インターネットに接続できるクライアント端末であれば社内外問わずに一元管理することができます。また、管理者はWebブラウザ経由でいつでもどこでもEPへアクセスでき、クライアント端末を管理することができます。

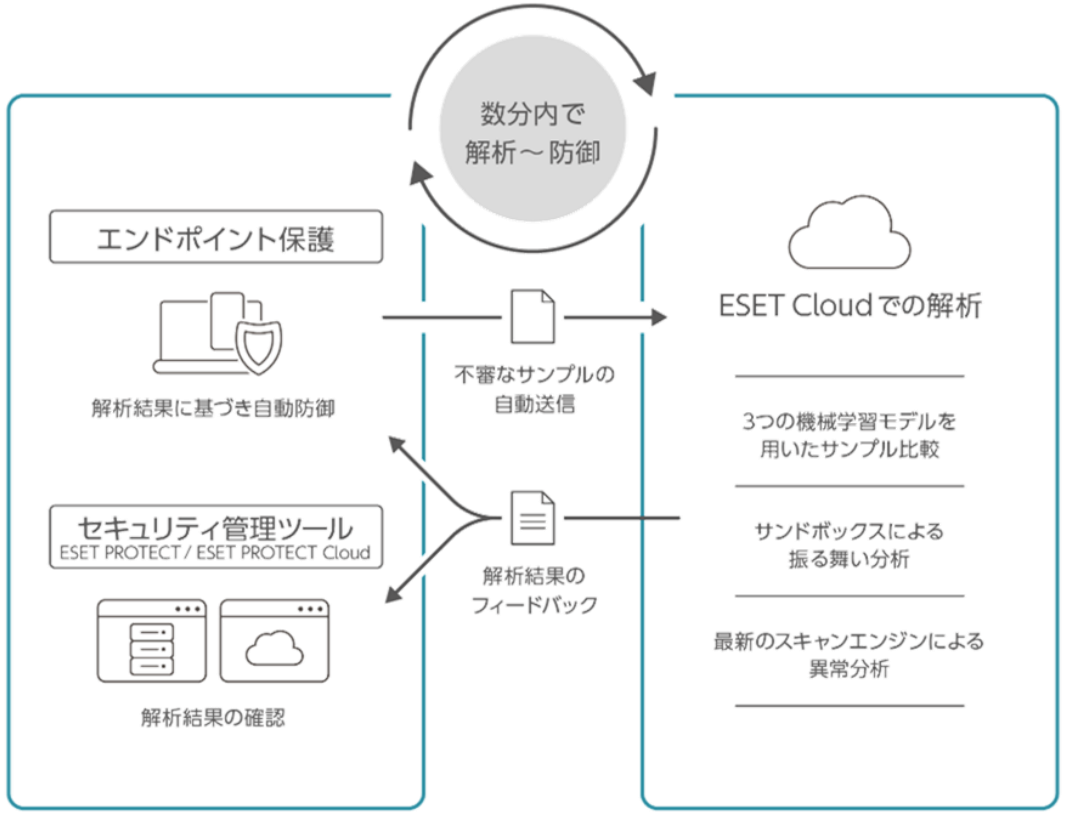
クラウドベースで常に最新な環境

EPのバージョン管理はESET社にて行われるため、お客様によるバージョンアップ作業は不要で常に最新の状態で利用することができます。また、EMエージェントも自動でバージョンアップされるため、お客様の運用やメンテナンスの負荷を減らすことができます。

2. 製品概要 -クラウドサンドボックス-

ESET LiveGuard Advancedの特徴

ESET LiveGuard Advanced（旧名称：ESET Dynamic Threat Defense）は、未知の高度なマルウェアに対する検出力・防御力をさらに高めるクラウドサービスです。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、
ユーザーは、端末への新規プログラムインストールをする必要がなく、手軽に多層防御の強化を行うことが可能です。

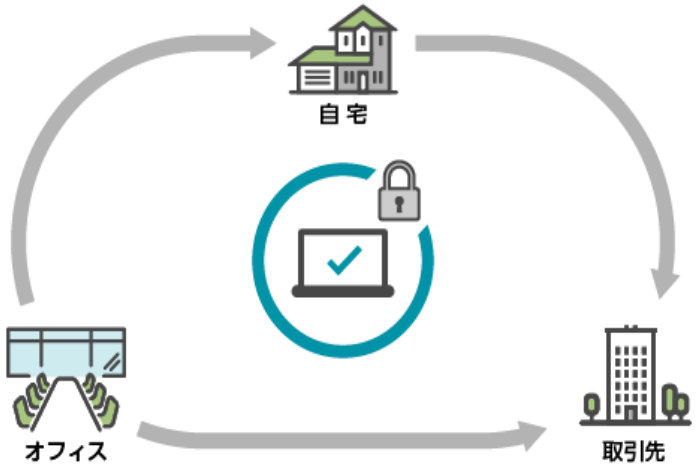


2. 製品概要 -フルディスク暗号化-

ESET Full Disk Encryptionの特徴

ESET Full Disk Encryptionは、リモート勤務や社内で利用するクライアントPCのディスク全体、またはブートディスク(※)を暗号化するディスク暗号化ソフトウェアです。
暗号化実施後、クライアント端末にはプリブート認証が付与されるため、
端末の紛失・盗難時の情報漏洩対策を行うことができます。
また、ESET PROTECTソリューションシリーズのセキュリティ管理ツールであるESET PROTECT /ESET PROTECT on-premを使用して、各クライアント端末の暗号化状況の確認や復号、プリブート認証パスワードの回復などを行うことができます。

持ち出し端末の情報漏洩対策



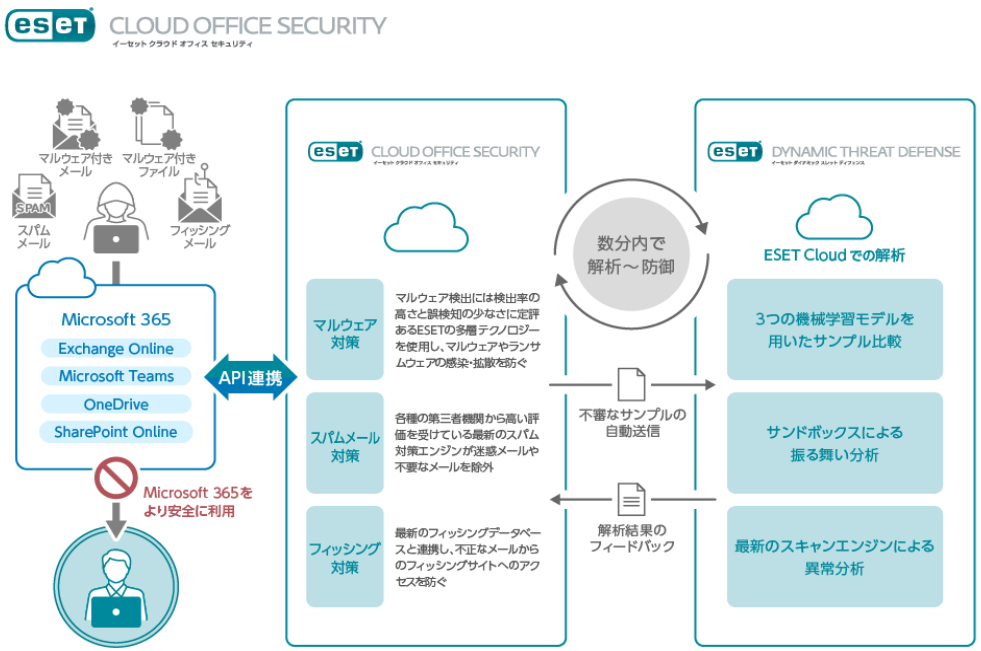
EPによる一括管理

※ブートディスク…Windowsのブートドライブとして使用される物理ディスクです。同一ディスク内にWindowsのブートドライブとその他のドライブが存在する場合は、そのディスク全体が暗号化されます。

2. 製品概要 -クラウドアプリケーションセキュリティ-

ESET Cloud Office Securityの特徴

ESET Cloud Office Securityは、お客様がご利用のMicrosoft 365サービスまたはGoogle WorkSpaceと連携させてすぐに、マルウェア対策、スパムメール対策、フィッシング対策を行うことができるクラウドサービスです。企業の通信とクラウドストレージを保護し、検出したメールやファイルの確認だけではなく、検出が発生するとすぐに管理者に通知することができます。



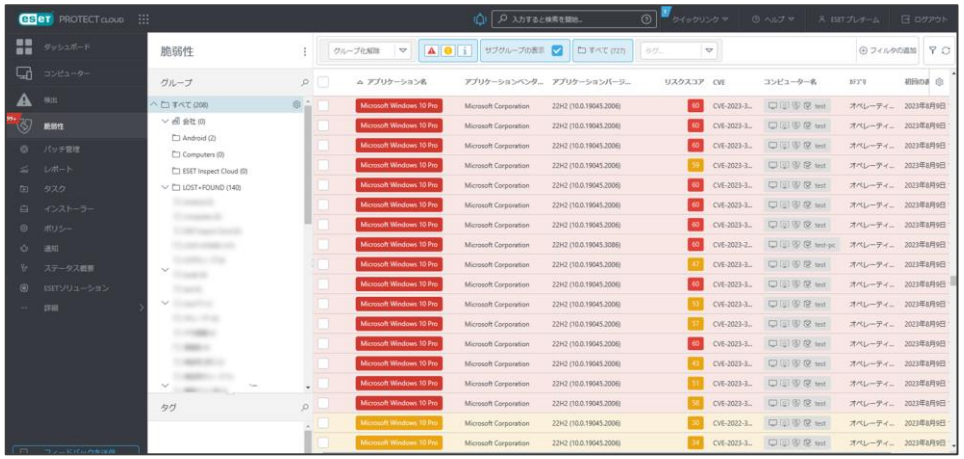
- **導入が簡単**
  - ✓ Microsoft 365とAPI連携を行うため、お客様のサービスに影響を与えることなく利用可能
  - ✓ API連携型のサービスであるため、お客様環境のMXレコードやDNSの書き換えが不要
  - ✓ ポリシー設定を行うだけで、ESET LiveGuard Advancedが利用可能
- **運用が容易**
  - ✓ Microsoft 365からユーザ/グループ情報を自動取得
  - ✓ ESET Cloud Office Securityの保対象を絞ることができるため、スモールスタートが可能
  - ✓ ESETが管理するクラウドサービスであるため、お客様によるECOSのバージョンアップが不要

2. 製品概要 -脆弱性とパッチ管理-

ESET Vulnerability ＆ Patch Managementの特徴

ESET Vulnerability & Patch Managementは、OSとアプリケーションの脆弱性※1とパッチ※2適用状況を管理するソリューションです。
古いオペレーティングシステムやアプリケーションを狙った脅威からクライアントを守ります。
クライアントの脆弱性情報は重大度（リスクスコア）が付与されるため、重大度の高いものから脆弱性対応するといった運用ができます。
また、パッチ管理につきましては手動またはスケジューリングして自動で適用させることもできます。

セキュリティ管理ツールでの「脆弱性とパッチ管理」のイメージ



- ESET Vulnerability & Patch Managementの主な機能

✓ クライアントの脆弱性情報を自動で収集
✓ 自動および手動でのパッチ適用
✓ 脆弱性の重大度のレベルづけ
✓ 対象のクライアントのリストの表示　など

※1 脆弱性…コンピュータ関連のプログラムに潜む欠点や盲点、弱点のことで、「セキュリティ・ホール」とも呼ばれます。
※2 パッチ… OSやソフトウェアに存在する脆弱性やバグを修正するプログラムを指します。「修正プログラム」「更新プログラム」「アップデート」などと呼ばれることもあります。

2. 製品概要 -eXtended Detection & Response- (1/4)

ESET Inspect の特徴

同一ベンダーだからこそできる、未然対策と事後対策のシームレスな統合

競合リスクやリソース消費量を抑えて多層防御をさらに強化

2. 製品概要 -eXtended Detection & Response- (2/4)

ESET Inspect の特徴

ESETのクラウドベースシステムとの連携

ESET Augur(機械学習エンジン)

ESET内部の機械学習エンジンでは、ニューラルネットワーク(ディープラーニングおよびLSTM)と
厳選されたアルゴリズムを組み合わせ、統合されたアウトプットを生成し、受信したサンプルを
「クリーン」、「望ましくない可能性がある」または「悪意がある」ものとして正確にラベル付けを行います。

ESET LiveGrid® (Reputation & Feedback)

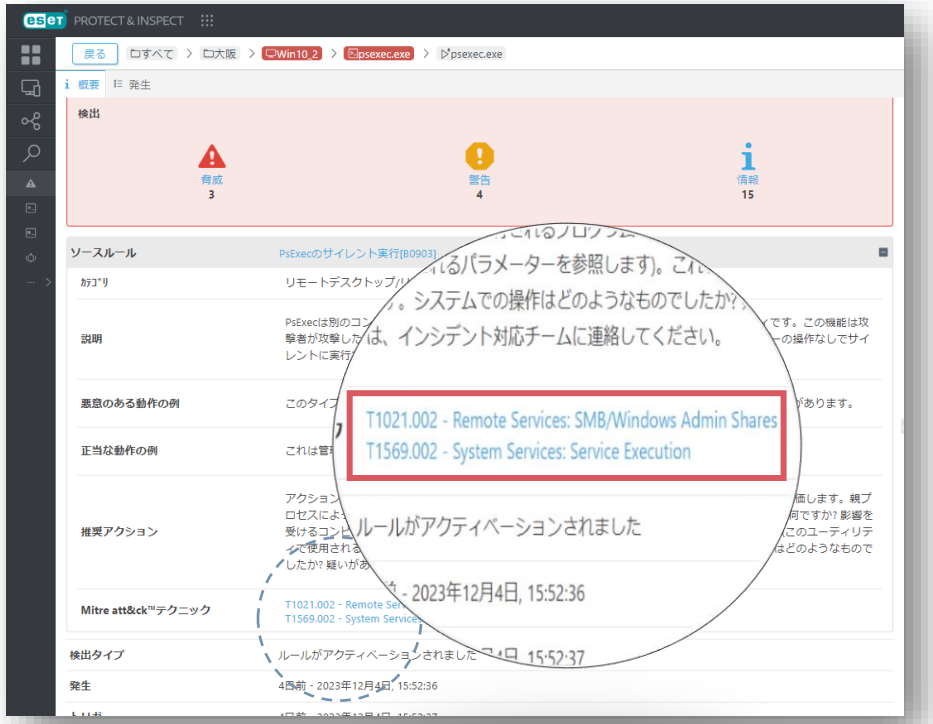
ESET LiveGrid®は、世界中のESETユーザーから脅威に関する情報を収集するための予防システムです。
LiveGrid®のデータベースには、潜在的な脅威に関する評価情報が含まれており、
最新の脅威を検知しブロックするので、急速に変化する脅威に対してきわめて効果的です。

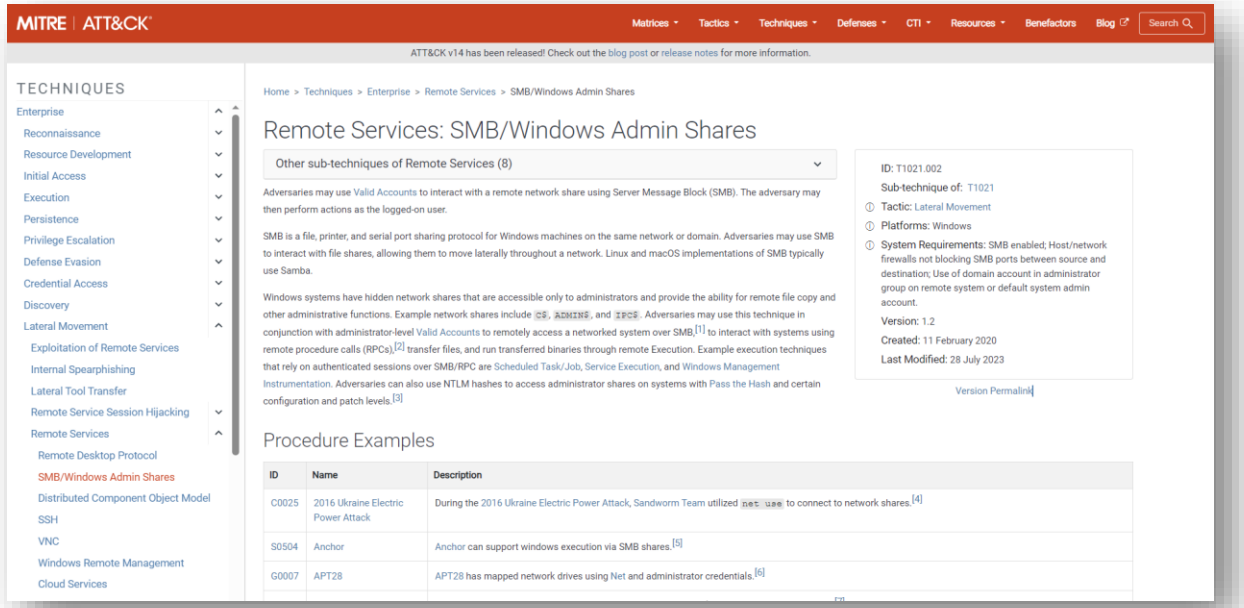
2. 製品概要 -eXtended Detection & Response- (3/4)

Digital Security
Progress. Protected.

ESET Inspect の特徴

EIの検出アラートから、攻撃に使用されたテクニックの詳細を参照可能



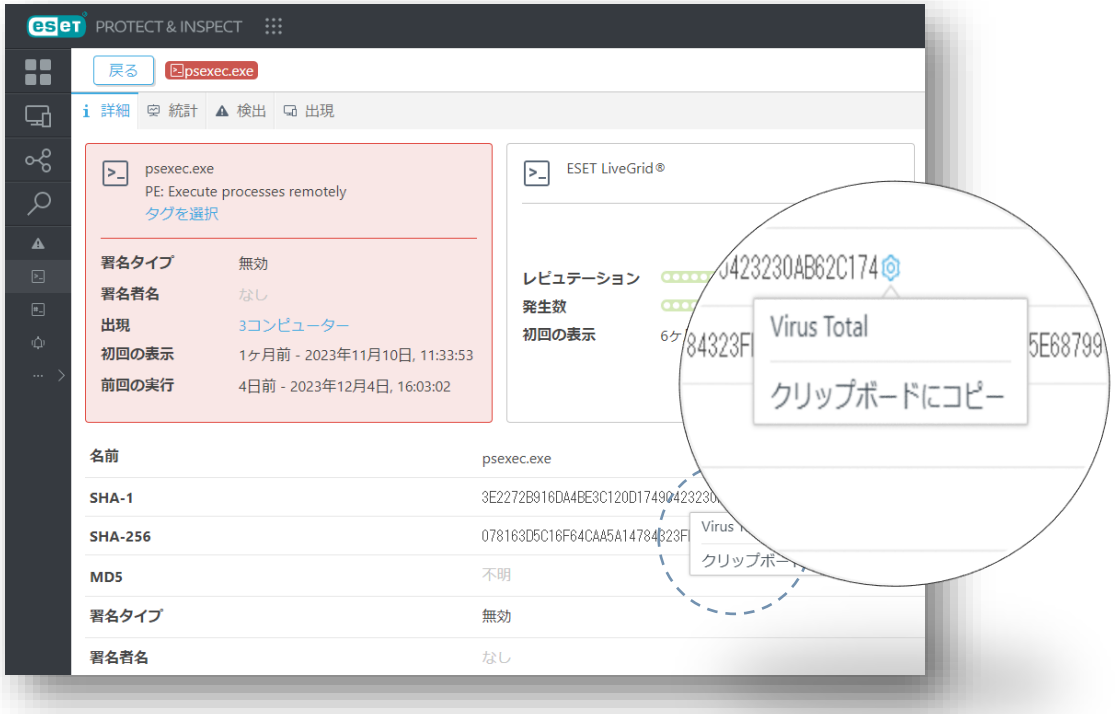


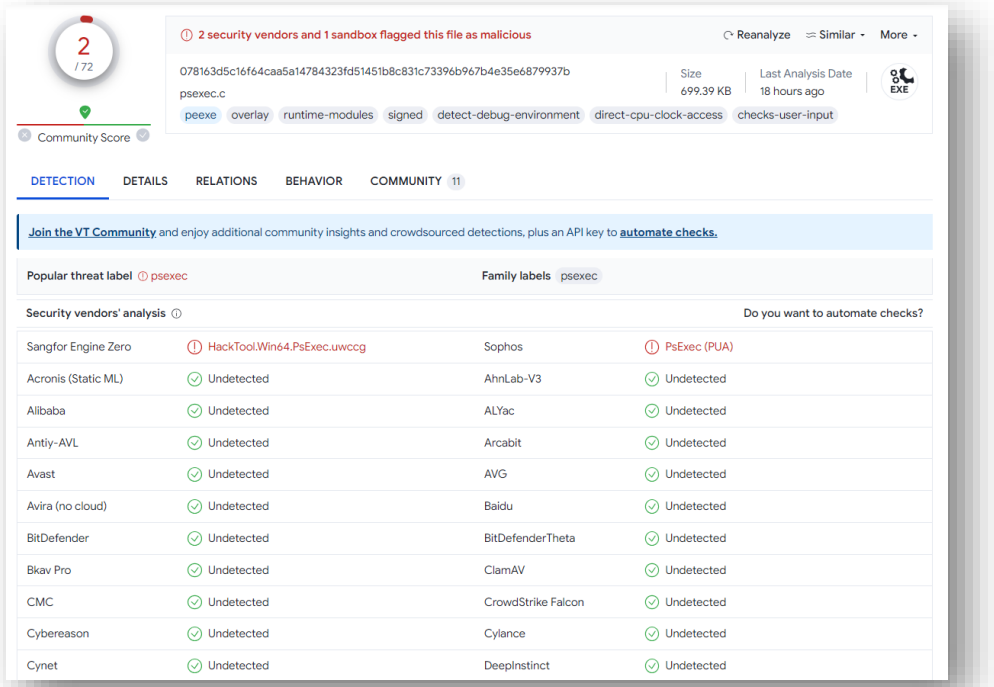
2. 製品概要 -eXtended Detection & Response- (4/4)

Digital Security
Progress. Protected.

ESET Inspect の特徴

VirusTotalにハッシュ値を用いたカスタムリンクを設定可能





ESET INSPECT

3. 主な機能 -クライアント用プログラム(1/4)-

① リアルタイム保護

EES EEA ESSW

- ファイル検査：ファイルを作成時や実行時に検査し、悪意のあるファイルを検出します。
- メモリー検査：メモリー内で展開されたデータを検査し、悪意のあるデータを検出します。
- 電子メールクライアント保護：メール受信時に検査し、悪意のあるメールや添付ファイルを検出します。
- Webアクセス保護：HTTP/HTTPSプロトコルに対応しており、Webアクセス時にダウンロードされるコンテンツやファイルを検査します。
- ドキュメント保護：Microsoft Office 形式ファイルに含まれる不正プログラムの有無を検査します。

② 新種・亜種のマルウェアの検出（ヒューリスティック技術）

EES EEA ESSW

ヒューリスティック技術は、遺伝子技術を応用したマルウェア検出方法です。従来の検出エンジンを使用したパターンマッチングなどでは検出できない新種や亜種のマルウェアも、「静的解析（プログラムコード解析）」、「動的解析（エミュレータ）」、「遺伝子工学的解析（ジェネリックシグネチャ）」の3つの機能により、詳細な分析の実行と悪意のある振る舞いの特性を識別することができます。

③ 機械学習保護

EES EEA ESSW

機械学習保護は、リアルタイムスキャンやオンデマンドスキャンでの検出に利用できます。
ESET独自の機械学習アルゴリズムにより、クラウド環境に接続できないオフライン環境でも、定義データベースにない未知のマルウェアを検出できます。

3. 主な機能 -クライアント用プログラム(2/4)-

④ HIPS

EES EEA ESSW

コンピューターのセキュリティに悪影響を与えようとする望ましくない活動およびマルウェアからシステムを保護します。
また、高度な動作分析とネットワークフィルタリングの検出機能を連携し、実行中のプロセスやファイル、レジストリキーを監視します。

⑤ エクスプロイトブロック

EES EEA ESSW

ブラウザー、メールソフトウェア、PDFリーダー、JAVAなどの
アプリケーションの脆弱性を悪用する動作を監視しブロックします。
これにより脆弱性を悪用して個人情報やFTPアカウントなどを盗もうとするウイルスを検知することが可能です。

⑥ アドバンストメモリスキャナー

EES EEA ESSW

実行中のメモリの詳細な検査を実施し、難読化や巧妙な手法で偽装されたウィルスの検出が可能です。
これにより、ヒューリスティック検査でも検出が難しい難読化・暗号化されたウイルスについての検出します。

⑦ ESET LiveGrid

EES EEA ESSW

クラウドを利用してより速くより正確にマルウェアを検出します。
また、使用しているプログラムの安全性を評価します。

⑧ ランサムウェア保護

EES EEA ESSW

データを修正しようとするアプリケーションとプロセスの動作を監視し、
悪意のあるアプリケーションからデータを保護します。

3. 主な機能 -クライアント用プログラム(3/4)-

⑨ フィッシング対策

EES EEA ESSW

フィッシングサイトのリスト、シグネチャと照合・検査を行います。
電子メールなどに埋め込まれているフィッシングサイトへのアクセスを抑止します。

⑩ デバイスコントロール

EES EEA ESSW

CD/DVDドライブ、USB接続のストレージデバイスなどの利用を制御できます。
CD/DVDの挿入時や外部ストレージデバイスの接続時に、自動的に中身を検査することも可能です。

⑪ 不正侵入対策/パーソナルファイアウォール

EES

IPv6対応のファイアウォール機能により、ワーム、RPC/DCOM攻撃、DNS Poisoning攻撃、
ポートスキャン攻撃、SMB Relay攻撃、TCP非同期攻撃、リバースTCP非同期攻撃、ICMP攻撃などを検出します。
また、社内LAN、公衆無線LANなど、接続するネットワークごとに
異なるファイアウォールポリシーのプロファイルを作成できます。
WindowsのV6以降のプログラムではボットなどによる外部の通信を検出・防御する「ボットネット保護」機能や、
IDS機能を強化して、各種攻撃と脆弱性を検出する「バルナラビリティシールド」機能が追加されました。
MacのV6のプログラムはパーソナルファイアウォール機能のみが実装されており、
指定したフィルタリングルールに基づいたネットワーク接続の可否の設定が可能です。

3. 主な機能 -クライアント用プログラム(4/4)-

⑫ 迷惑メール対策

EES

迷惑メール対策エンジンによる検出とブラックリスト・ホワイトリストの設定が可能です。
スパム判定された電子メールを指定のフォルダへ振り分けます。

⑬ Webコントロール

EES

ユーザーがアクセスできるWebサイトをカテゴリ指定またはURL指定で制限できます。
制限されているサイトにアクセスした場合、ブロック用ページを表示してユーザーに通知します。

⑭ セキュアブラウザー

EES

コンピューターで実行中の他のプロセスからWebブラウザーを保護します。
ゼロトラストアプローチであり、コンピューターまたはその保護機能が危険にさらされている、または不十分である
という前提でブラウザーのメモリ空間や結果的にブラウザーウィンドウの内容が改ざんされることを防止します。

⑮ 自動アップデート機能

EES EEA ESSW

随時公開される最新バージョンへのバージョンアップ負荷を軽減するため、これまでセキュリティ管理ツールや
ユーザー自身が手動で行っていたバージョンアップ作業を実施することなく、プログラムが自動でバージョンアップされる
機能です。本機能により、管理者やユーザーに負荷をかけることなく、常に最新のプログラムを使用したウイルス対策が可
能になります。

3. 主な機能 -セキュリティ管理ツール-

① ログ管理機能

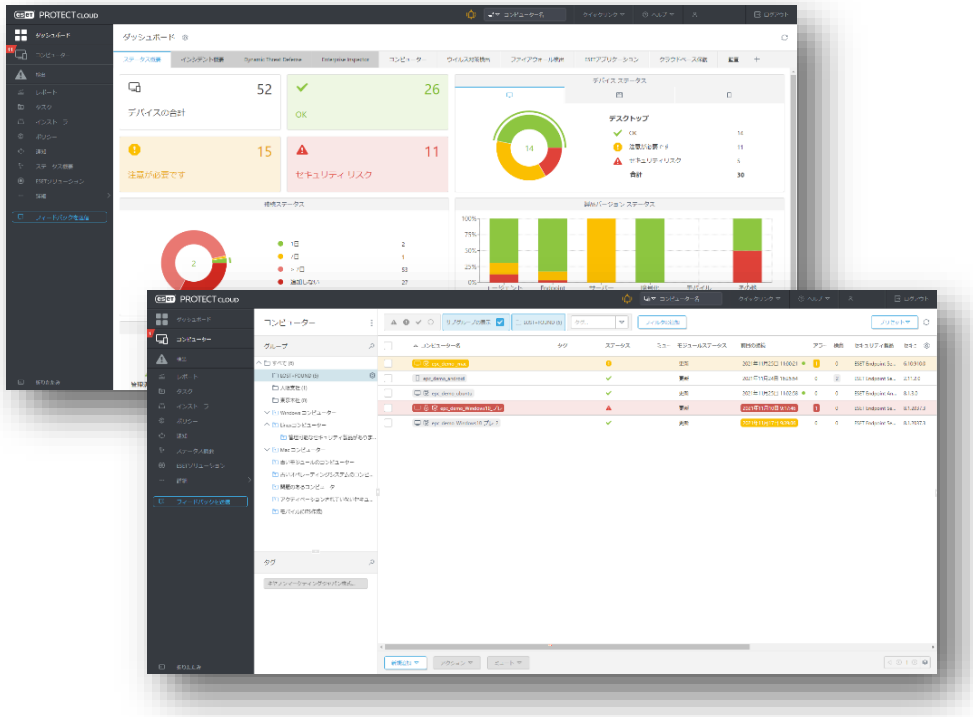
ログ管理機能はセキュリティ管理ツールの最も重要な機能の１つで、
クライアントから収集したログや設定情報の表示、
レポートの作成などを行うことができます。

② クライアント管理機能

クライアント管理機能を使用すると、端末にインストールした
クライアント用プログラムの設定をリモートで変更することが可能です。
また、クライアントをグループ化することや管理している
クライアントを指定してタスクを実行することもできます。

③ 運用管理機能

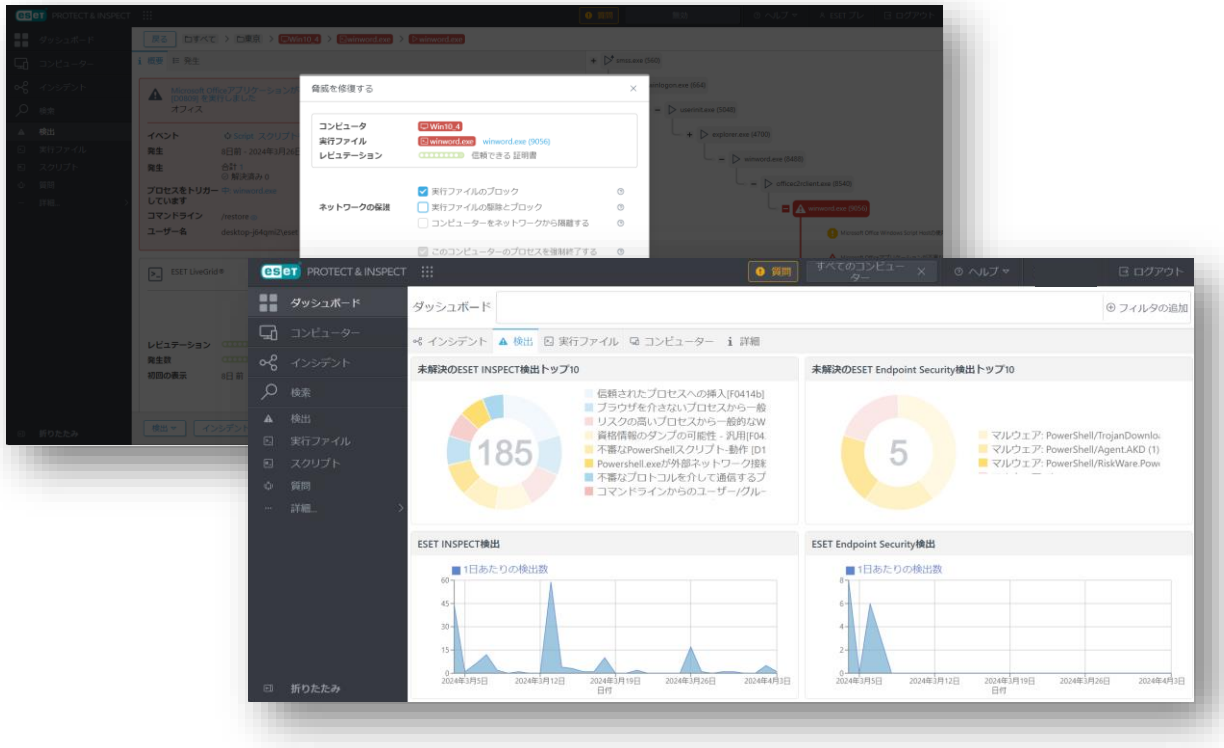
運用管理機能は、セキュリティ管理ツールが
円滑に運用できるように保守を行う機能です。
セキュリティ管理ツールへのログインユーザーの管理を行ったり、
管理者によって実施されたセキュリティ管理ツールの
操作内容の確認をすることが可能です。



3. 主な機能 -eXtended Detection and Response(1/5)-

①Webコンソール

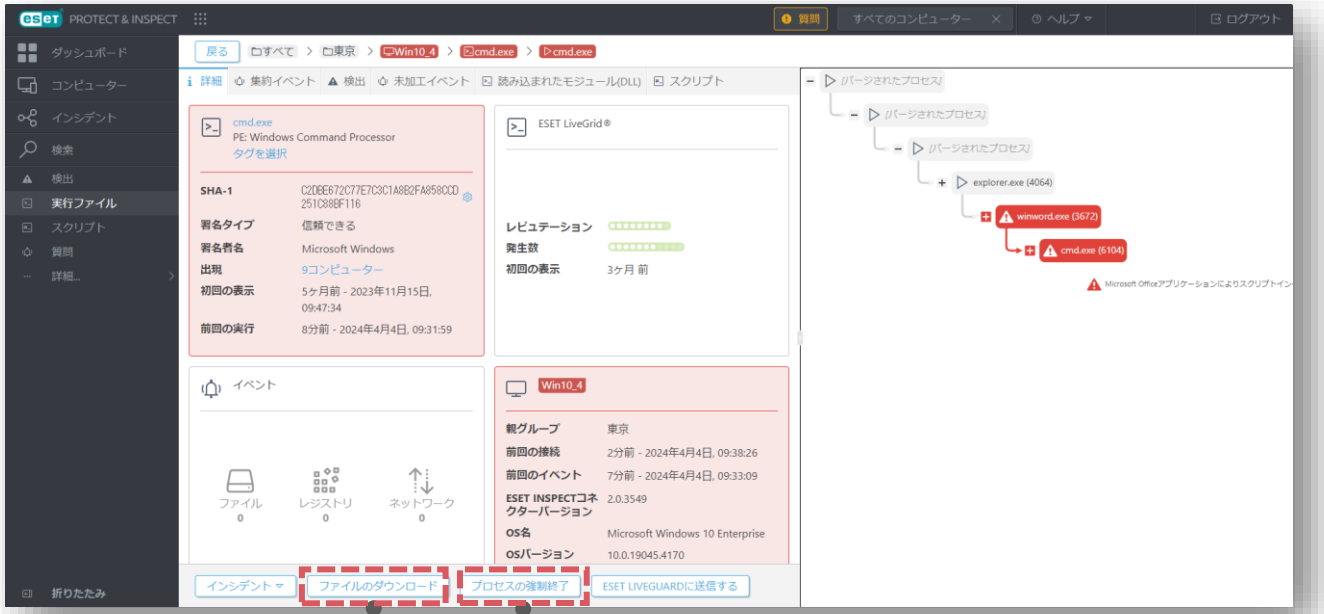
ダッシュボードを起点にあらゆる角度から調査を開始可能です。
可視化機能や高度な検索機能が対応を強力にサポートしているため、
１つのWebコンソールだけでミクロ・マクロ両方の視点から調査が可能です。
脅威が発見された場合は、すぐにネットワークやコンピューターの保護を実行できます。



3. 主な機能 -eXtended Detection and Response(2/5)-

②ハッシュ値によるブロック, プロセスの強制停止

ハッシュブロックでは端末/グループにハッシュ値(SHA-1)を利用して特定のファイルの利用を禁止することができます。
またブロックされたファイルが作成・修正したレジストリを削除でき、プロセスキルはプロセスを強制終了させることが可能です。



調査に必要なファイルを
パスワード付きZIP形式でダウンロード

1クリックで
プロセスを強制停止

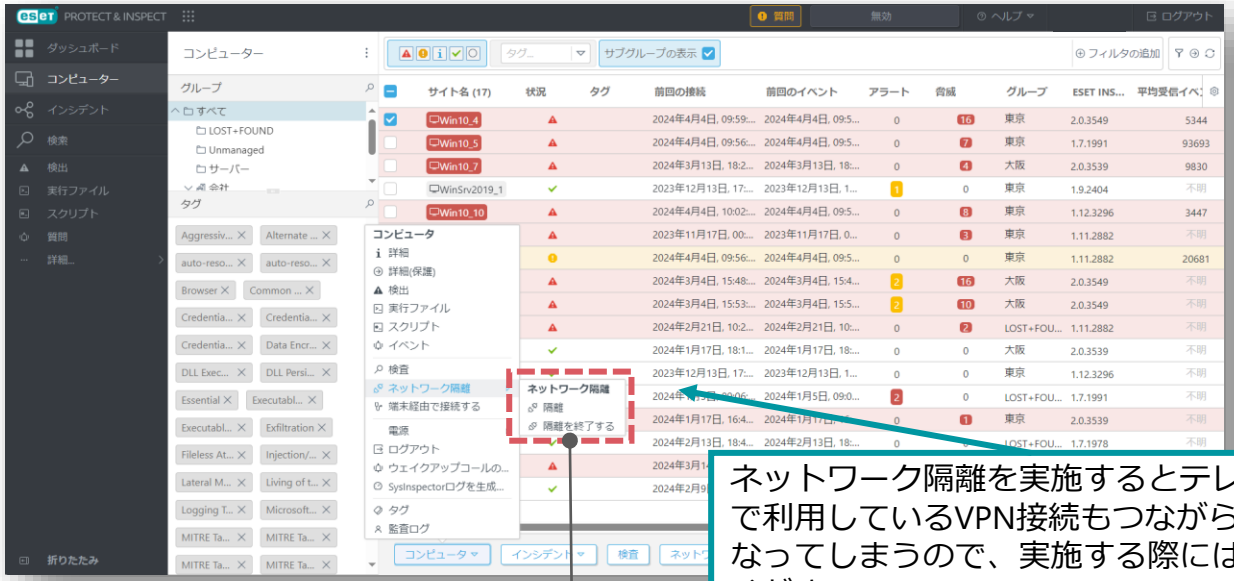
SHA1ハッシュ値を用いて
実行ファイルを即座にブロック

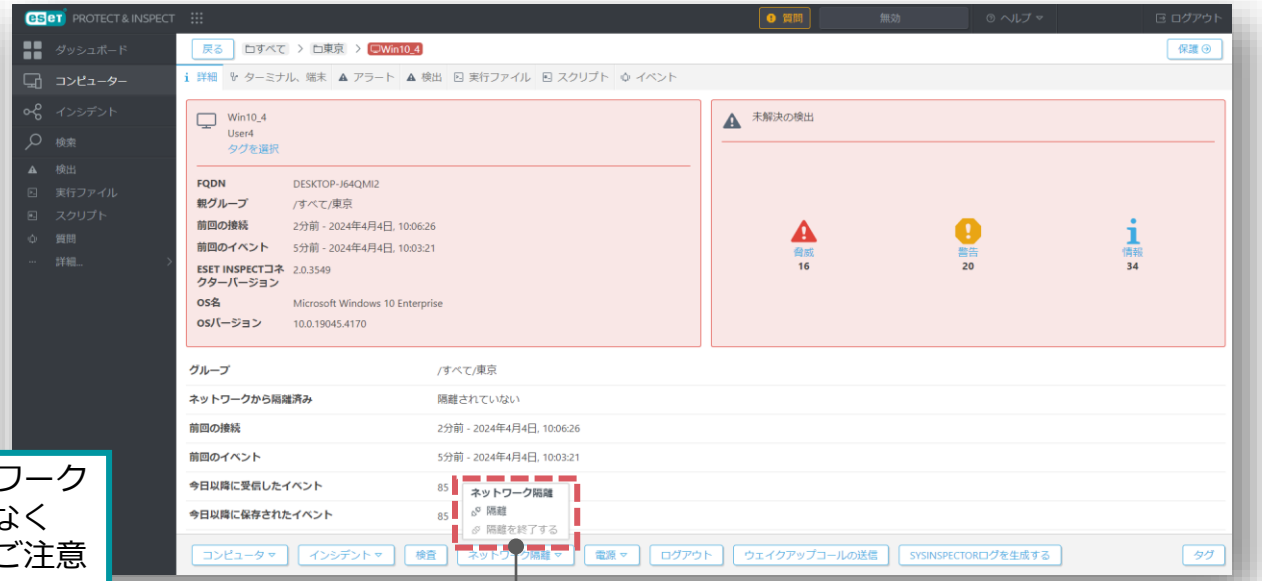
不正に書き込まれた
レジストリキーの削除や
ファイル駆除も合わせて実施

3. 主な機能 -eXtended Detection and Response(3/5)-

③ネットワーク隔離

侵害端末を素早くネットワークから隔離し、被害の拡大を抑制することができます。
隔離中でもWebコンソールからのリモート調査が可能であるため、
Remote PowerShellと組み合わせることで、より柔軟な対応を実施可能です。
※ESET関連の通信のみ可能





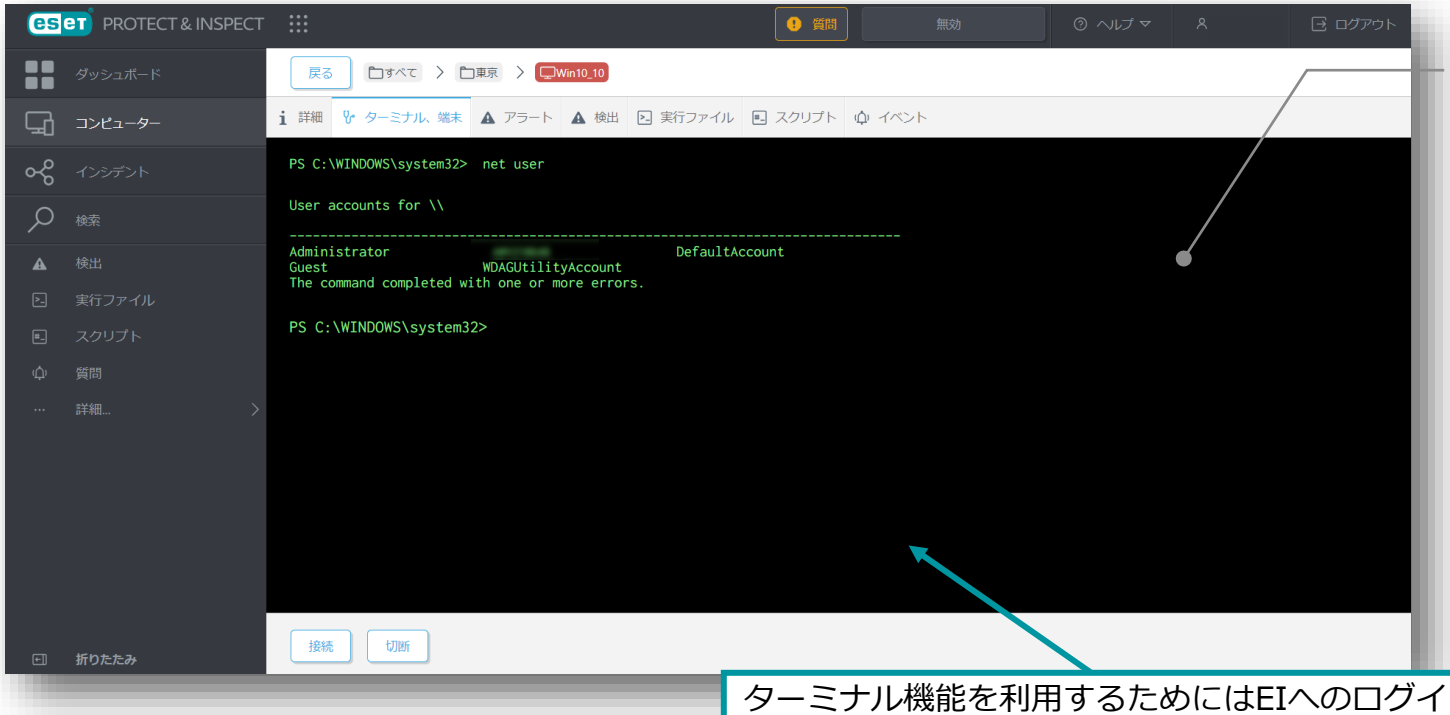
ネットワーク隔離を実施するとテレワークで利用しているVPN接続もつながらなくなってしまうので、実施する際にはご注意ください。

一覧画面や詳細画面から
1クリックでネットワーク隔離を実施

3. 主な機能 -eXtended Detection and Response(4/5)-

④Remote PowerShell Interface

リモートからエンドポイントへ直接接続してインシデントレスポンスが可能です。
同一の管理コンソールからリアルタイムでユーザーのワークフローを止めることなく、
侵害端末へのきめ細かな調査・対応・修復などが実施できます。



ターミナル機能を利用するためにはEIへのログインで二要素認証を有効にしている必要があります。
また対象の端末がLinux、Macの場合は利用できません。端末側のPowerShellのバージョンが5.1以上であることも利用条件になります。

リモートからのライブレスポンスをサポート

- 詳細調査のための情報取得
- システムのイベントログ取得
- 重要ファイルのバックアップ
- 攻撃者が生成したファイル等の削除
- 攻撃者が変更したレジストリキーの復旧　など

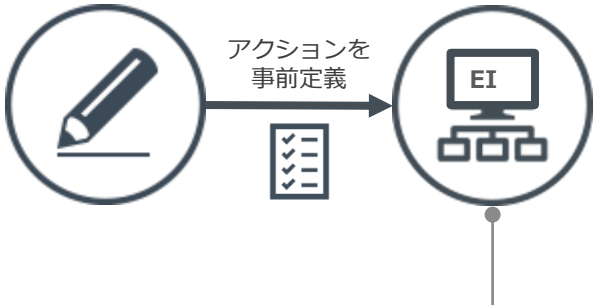
ライブレスポンスとは？

- コンソールへ直接接続してコマンドやツールを実行し、システムを稼働させたまま情報収集を行う手法
- 主にメモリ上に展開されているプロセス、ファイル、レジストリ、ネットワークなどの揮発性の情報取得に使用する

3. 主な機能 -eXtended Detection and Response(5/5)-

⑤アクションの自動化

検知ルールに事前にアクションを定義しておくことで、
検出アラートがトリガーされたタイミングで任意のアクションを自動実行可能です。

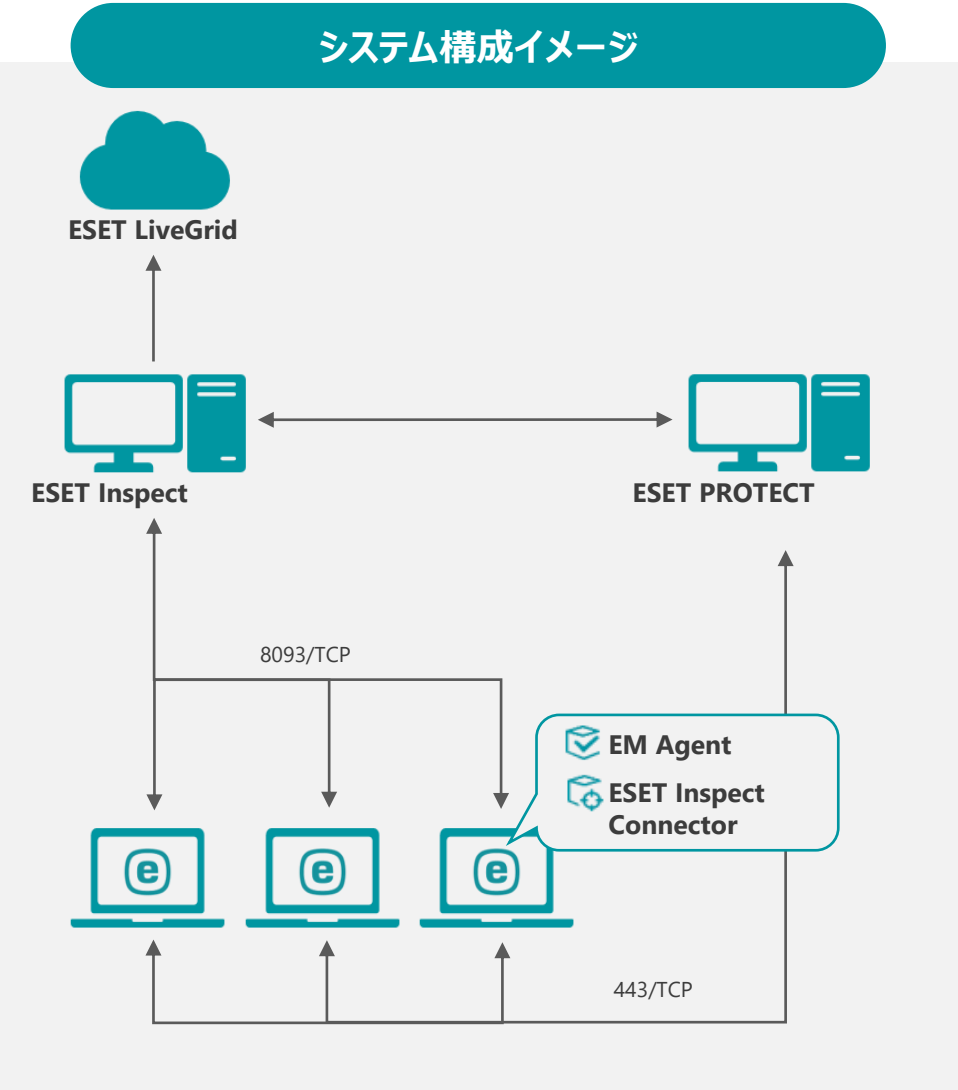


検出アラートがトリガーされたら
ルールに沿ってアクションを自動実行

検出時には定義済みアクションを自動実行

- ネットワーク隔離
- ハッシュ値によるブロック
- 各種マーカーの付与
- イベントのドロップ
- 検出アラートのトリガー　など

4. システム構成(1/2)



ESET Inspect（EI)

EI/EI on-premはEI Connectorを使用してエンドポイントデバイスでリアルタイムにデータを収集します。データは一連のEI/EI on-prem内のルールと照合され、疑わしいアクティビティが自動的に検出されます。この集約されたデータにより、異常で疑わしいアクティビティをより効率的に検索し、正確なインシデント対応、管理、およびレポートの作成ができます。

ESET PROTECT（EP)

EP/EP on-premはクライアントプログラムの情報収集や設定の変更、インストーラーの作成、タスク配布などを行います。クライアントとの通信はEM Agentを経由して行います。

ESET Inspect Connector (EI Connector)

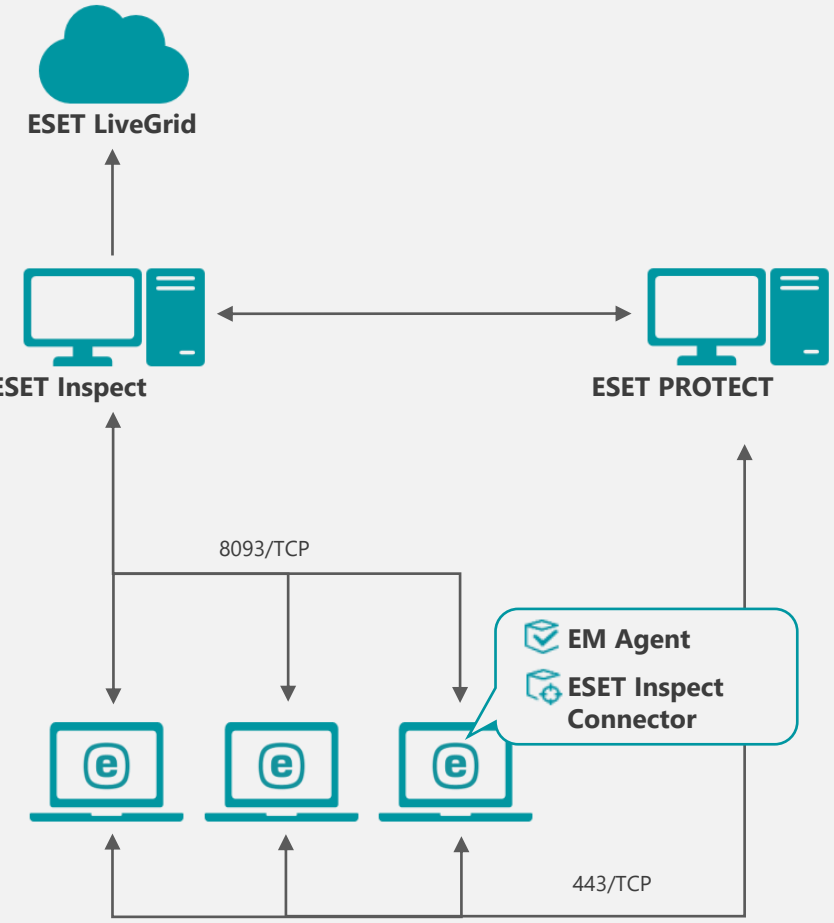
EI Connectorはクライアントのデータを収集し7分間隔でEIへデータを送信します。また、悪意のあるコンポーネントを削除し、これらのコンポーネントの実行をブロックします。

ESET Managementエージェント (EM Agent)

EM Agentは、クライアントから情報を収集し、10分間隔でEPへデータを送信します。また、EPからのタスク配布などはEM Agentへ送信されたのち、EM Agentがクライアントへ送信します。

4. システム構成(2/2)

システム構成イメージ



システム構成に関連する主な通信ポート

ポート	用途
443/TCP	EM AgentとESET PROTECT 間の通信に使用
8093/TCP	ESET Inspect ConnectorとESET Inspect 間の通信に使用

サポートされるアプリケーションバージョン※

アプリケーション名	EPによる管理	EIによる管理
ESET Endpoint Security / アンチウイルス	8.1以降	11.0.2032以降
ESET Endpoint Security / アンチウイルス for OS X	6.11以降	6.11.606.0以降 /7.3.3600.0以降
ESET Endpoint アンチウイルス for Linux	8.1以降	10.2.2.0以降
ESET Endpoint Security for Android	3.3以降	-
ESET Server Security for Microsoft Windows Server	7.3以降	10.0.12014以降
ESET Server Security for Linux	7.2以降	10.2.41.0以降

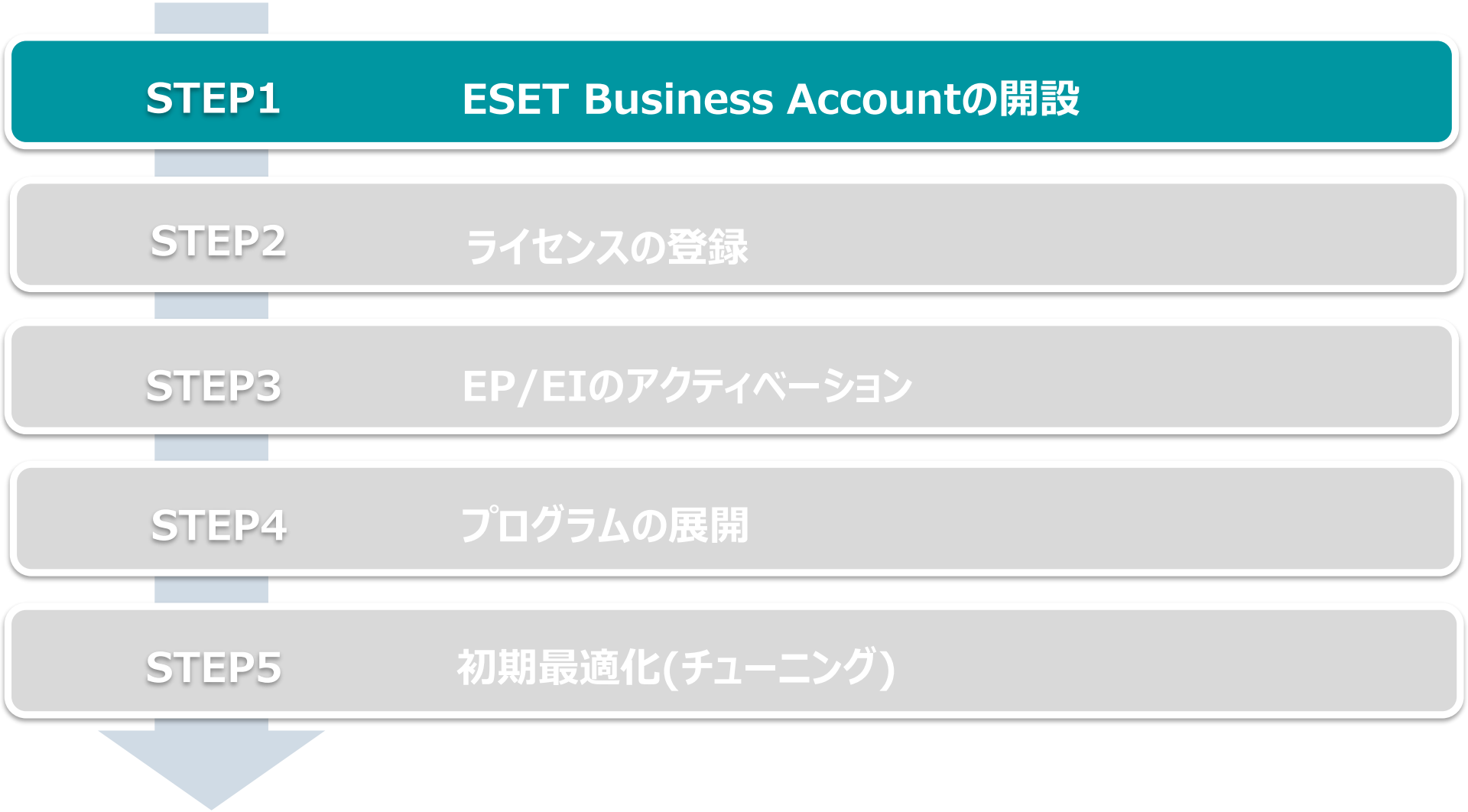
※VAPMの対象プログラムは、ESET Endpoint Security / アンチウイルス V10.1以降です。

ログの格納期間

ログの種類	データ保持期間
生ログ（検知の有無に関係なくEIに集められたすべてのログ）	7日間
検出ログ（EIの検知ルールによって検出されたログ）	31日間

Ⅲ. ご利用の流れ

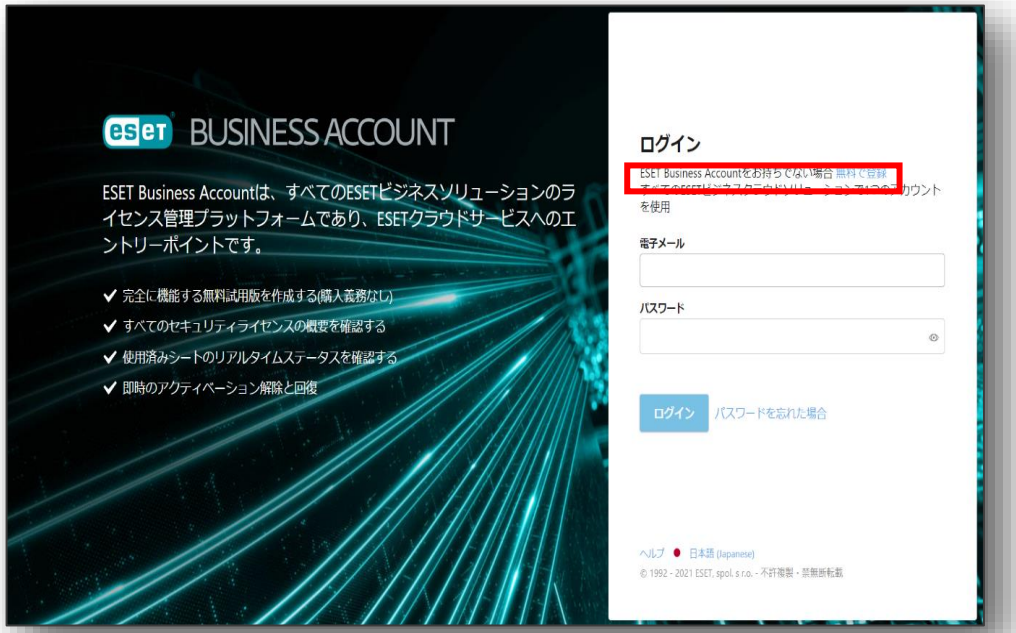
1. ESET Business Accountの開設



1. ESET Business Accountの開設

1. https://eba.eset.com/にアクセスし、ログイン画面で「無料で登録」をクリックしアカウント作成を開始
2. 画面に表示される説明に沿ってお客様情報を入力
   ※ 電子メールアドレスやパスワード、名前、電話番号、お客様企業名などを入力します
   ※ 本手順で設定した電子メールアドレスとパスワードはEBAログイン時に使用します

■ログイン画面

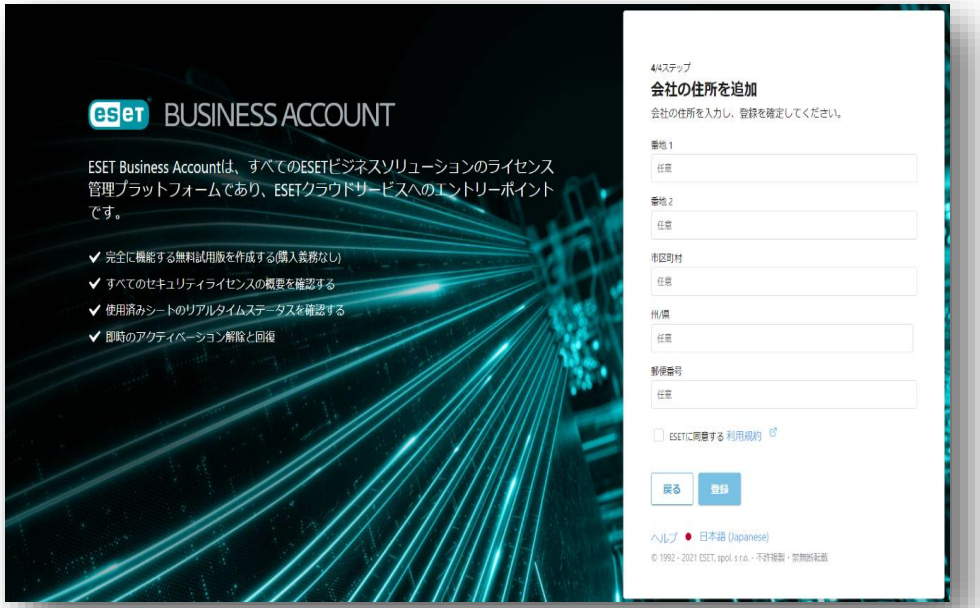


■Business Accountを作成

1. ESET Business Accountの開設

3. 利用規約をご確認いただき「ESETに同意」にチェックし「登録ボタン」をクリック
4. アカウントのアクティベーション
   ※ 登録した電子メールアドレスに「@eset.com」からメールが届きます

■利用規約への同意画面



■アクティベーション用メール

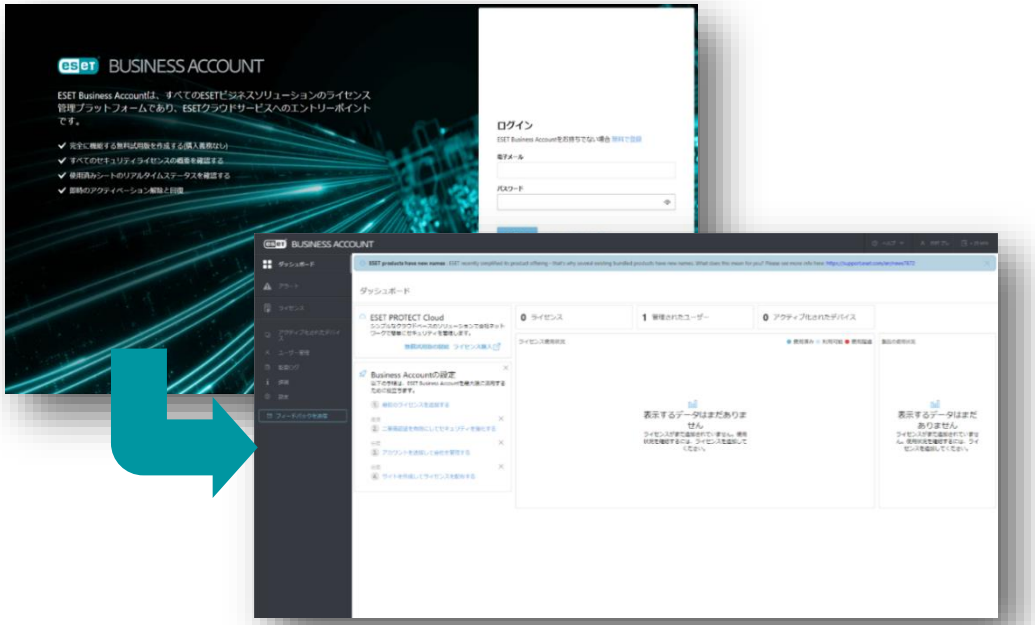
1. ESET Business Accountの開設

5. アカウントがアクティベーションされたことの確認
※ 登録した電子メールアドレスに「@eset.com」からメールが届きます

6. EBAにログインできることの確認
※ 登録した電子メールアドレスとパスワードを使用します

■アクティベーション完了確認用メール

■EBAにログインできることの確認



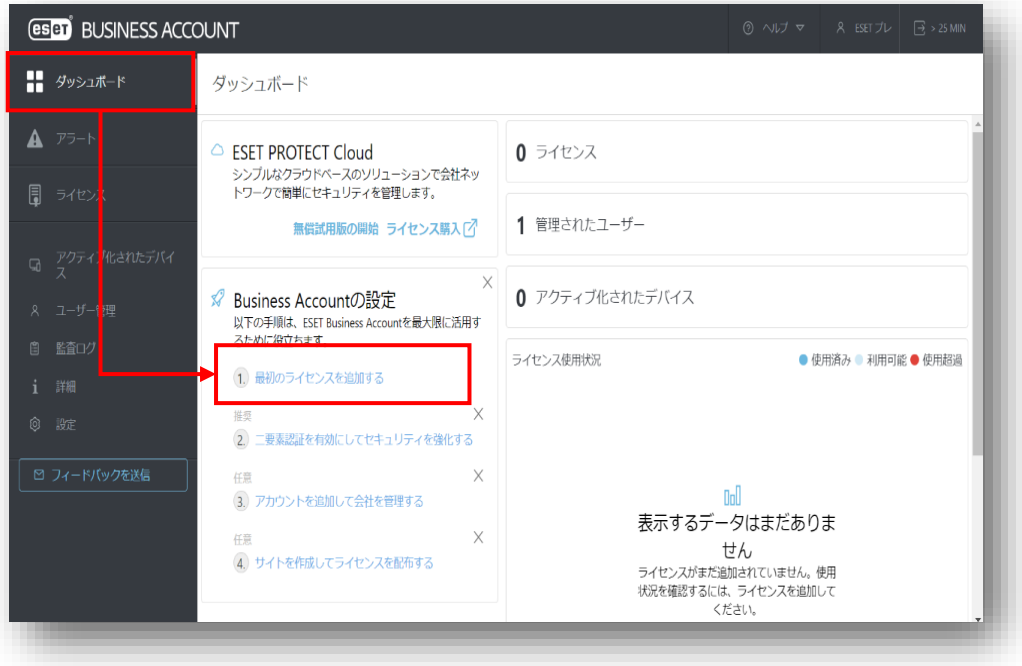
2. ライセンスの登録


STEP1
ESET Business Accountの開設
STEP2
ライセンスの登録
STEP3
EP/EIのアクティベーション
STEP4
プログラムの展開
STEP5
初期最適化(チューニング)

2. ライセンスの登録

1. EBAへのライセンスの登録
   ※ 弊社ユーザーズサイトで確認できる以下の情報をご用意ください。
   - 製品認証キー

①[ダッシュボード]内の[最初のライセンスを追加する]



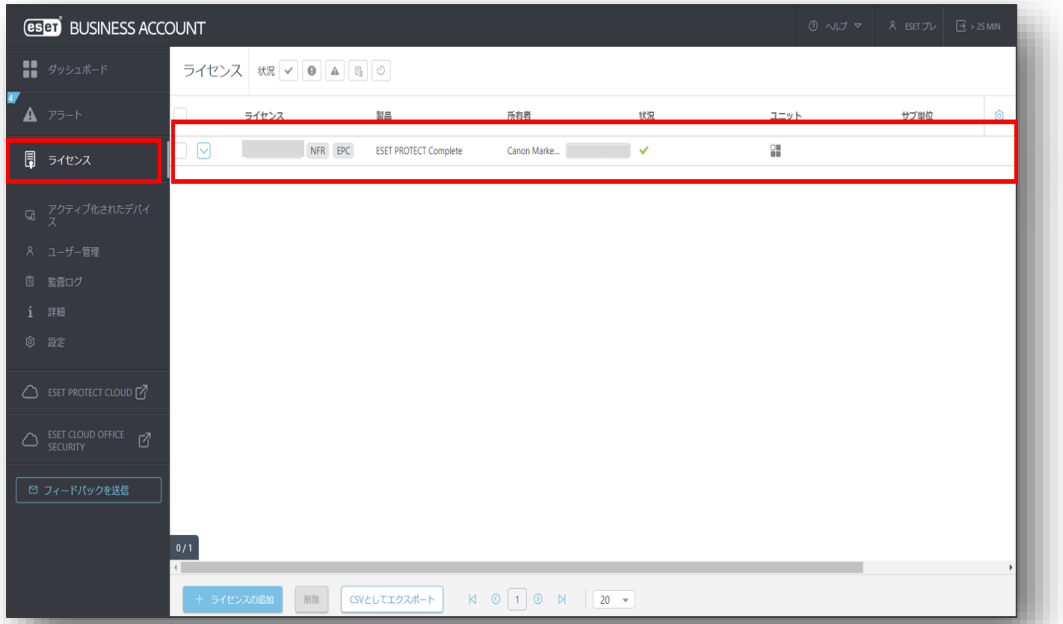
②[ライセンスの追加]画面

2. ライセンスの登録

2. ライセンスのアクティベーション
   ※ ライセンス契約時の電子メールアドレスにアクティベーションメールが送信されます
3. ライセンスが追加されたことの確認

■ライセンスアクティベーション時のメール例

■ライセンスが登録されたことの確認画面例

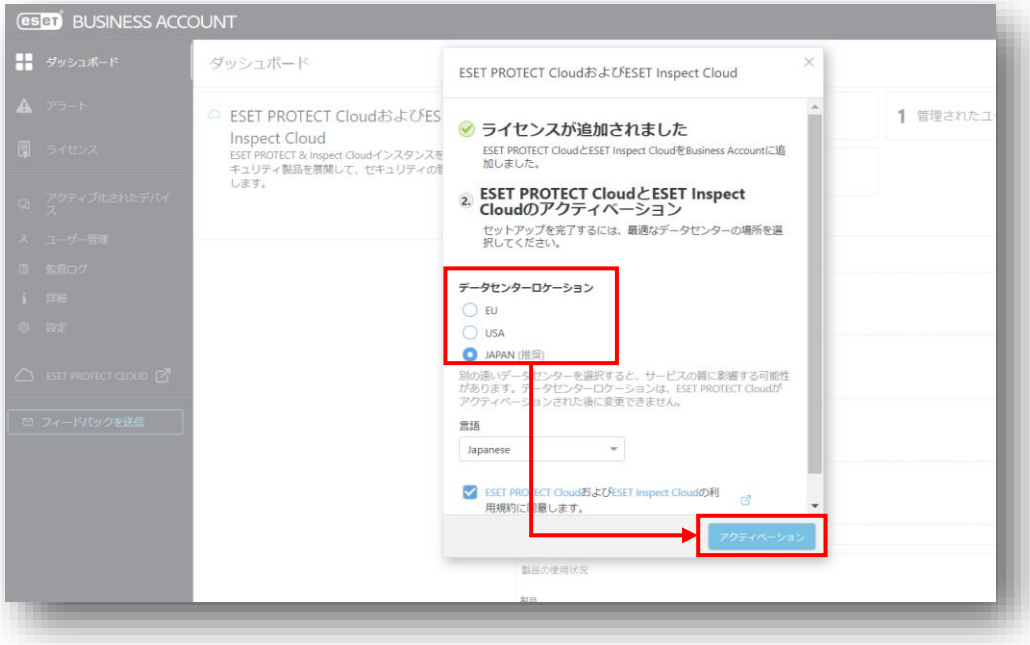


3. EP/EIのアクティベーション

3. EP/EIのアクティベーション

1. EPとEIのアクティベーション（左側メインメニューの「ESET PROTECT 」をクリックして開始します）
2. 10分～15分でアクティベーション完了
   ※ データセンターのロケーション選択画面では必ずJAPANを選択してください。
   ※ ESET PROTECT とESET Inspect が同時にアクティベーションされます。

■データセンターのロケーション選択画面



■ESET PROTECT Cloudアクティベーション画面

4. プログラムの展開


STEP1
ESET Business Accountの開設
STEP2
ライセンスの登録
STEP3
EP/EIのアクティベーション
STEP4
プログラムの展開
STEP5
初期最適化(チューニング)

4. プログラムの展開

- プログラムの展開の流れは以下になります。
  ※ EPとEIをご利用いただくにはクライアント用プログラムの他に以下のプログラムのインストールが必要です。
  - EMエージェント（クライアントとEPの接続に使用）
  - EI Connector（クライアントとEIの接続に使用）

1.静的グループの作成（任意）

2.ポリシーの作成（任意）

3.インストーラーによる展開
または
ソフトウェアインストールタスクによる展開

- クライアントが所属するグループを作成します。
  事前に静的グループを作成し、インストーラーに静的グループ情報を組み込むことで、管理後のグルーピング負荷を軽減できます。
- クライアントの各種設定を行うポリシーを作成します。ポリシーはインストーラーに組み込んでインストール時の初期設定値を変更することが可能です。
  ※ グループやクライアントに配布することで一括での設定変更も可能です。
- **新規インストールする場合（EMエージェント未インストール）**
  - **Windowsの場合**
    EMエージェント/EI Connector/クライアント用プログラムを一括インストールするための
    ライブインストーラーを作成します。
  - **macOSの場合**
    EMエージェント/クライアント用プログラムを一括インストールするためのライブインストーラーを作成します。インストール後、EI Connectorをソフトウェアインストールタスクでインストールします。
  - **Linuxの場合**
    EMエージェントインストールするためのライブインストーラーを作成します。インストール後、
    EI Connector/クライアント用プログラムをそれぞれソフトウェアインストールタスクでインストールします。
- **追加インストールする場合（EMエージェントインストール済）**
  ソフトウェアインストールタスクでクライアントにEI Connectorをインストールします。
  EI Connector/クライアント用プログラムのバージョンアップもソフトウェアインストールタスクを使用した
  本手順で対応が可能です。

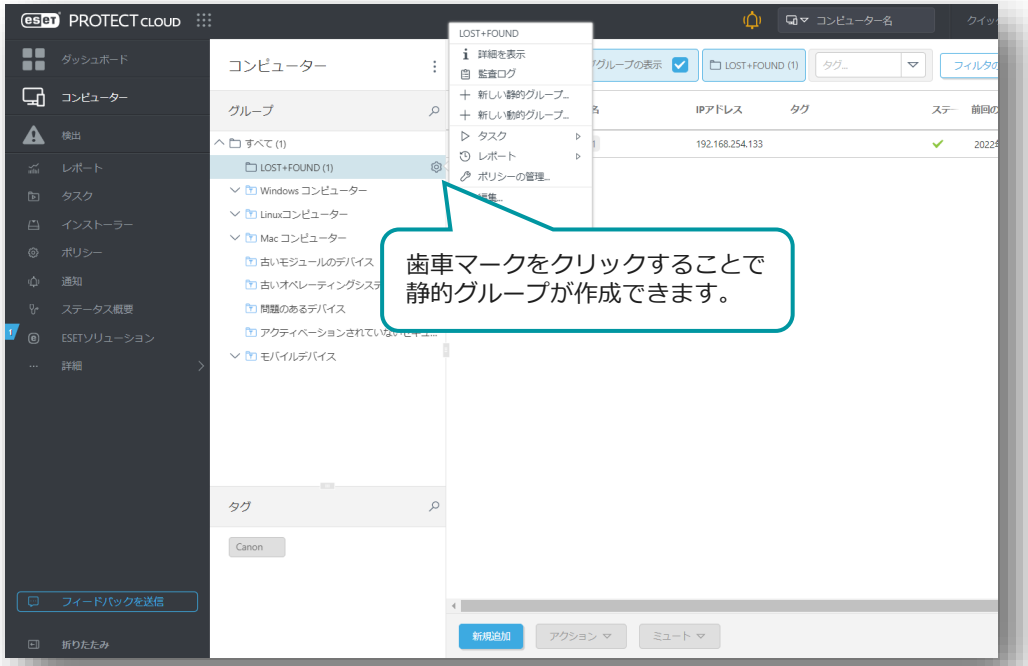
4. プログラムの展開

1. 静的グループの作成

静的グループはメインメニュー「コンピューター」から作成可能です。
グループは階層構造も可能なため、柔軟に組織構造的を作成することができます。

1. メインメニューの「コンピューター」画面より、静的グループを作成する親グループの歯車マークを選択し、「新しい静的グループ」をクリックします。
2. 作成する静的グループの「名前」(必須)と「説明」(任意)を入力し、「終了」をクリックします。

■メインメニュー「コンピューター」画面



■静的グループ作成画面

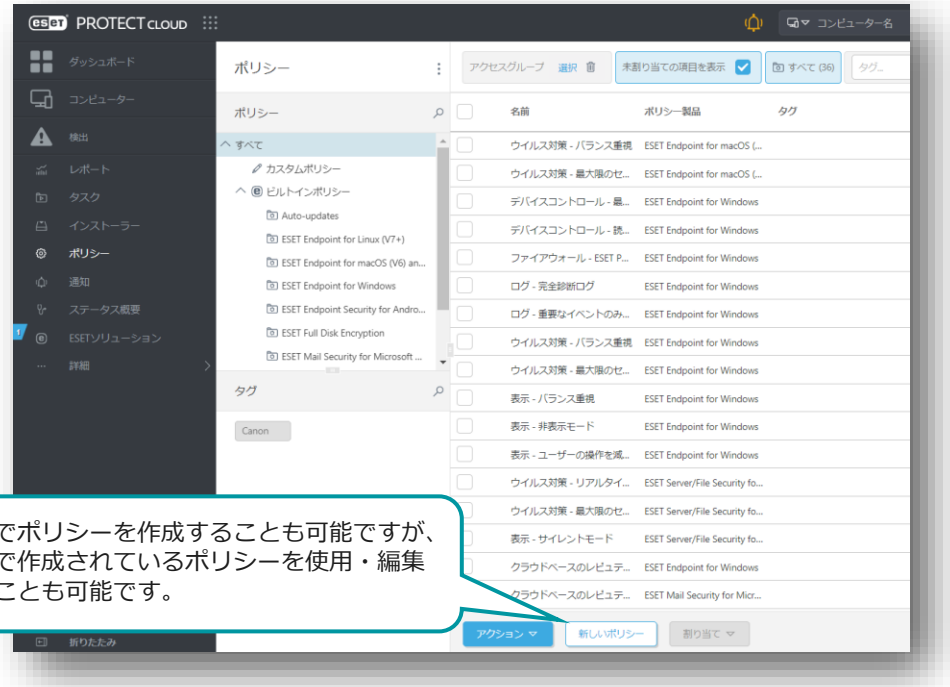
4. プログラムの展開

2. ポリシーの作成

クライアント用プログラムやEM Agent、EI Connectorに対して、検査の除外設定、
検出エンジンのアップデート先の設定、プロキシ設定など各種プログラムの設定を行います。

1. メインメニューの「ポリシー」画面より、「新しいポリシー」をクリックします。
2. 「基本」画面にて、ポリシーの「名前」を入力します。
3. 「設定」画面にて、ポリシーを作成するプログラムを選択し、各種設定を行います。
   （例:クライアント用プログラムの検査の除外設定やアップデート先の変更、プロキシの設定など）

■メインメニュー「ポリシー」画面



■ポリシー作成画面

4. プログラムの展開

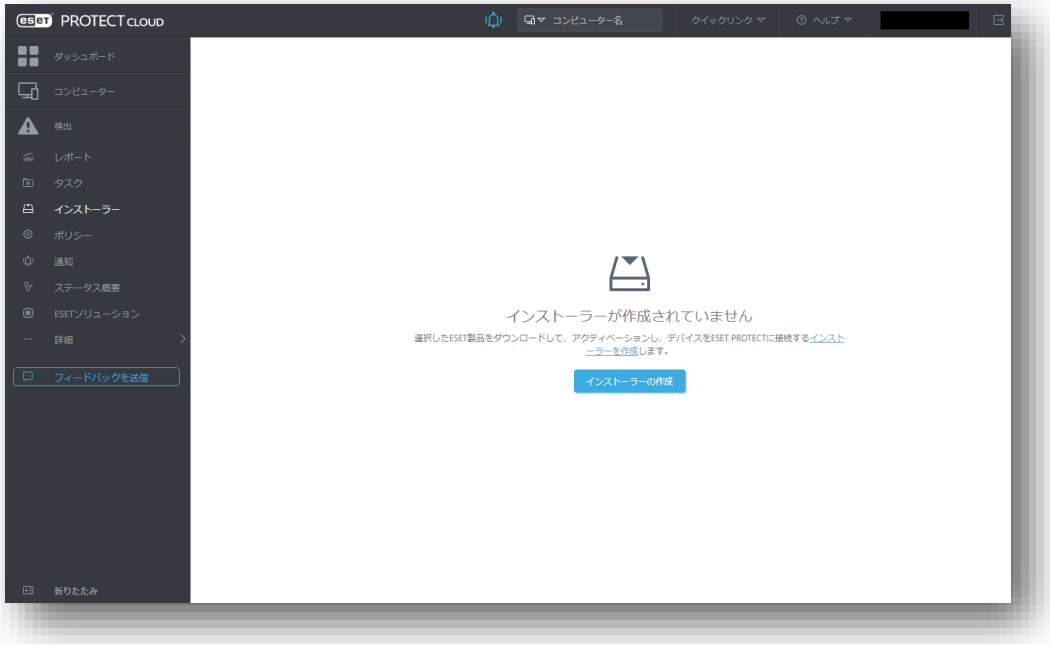
3. インストーラーの作成を行う場合(1/3)

EPメインメニュー「インストーラー」より、ライブインストーラーを作成します。

1. メインメニューの「インストーラー」画面より、「インストーラーの作成」をクリックします。
2. インストーラーの作成画面が表示されたら、「インストーラーのカスタマイズ」をクリックします。

※「インストーラーのカスタマイズ」を選択し、インストールにEI Connectorを含めたり、
クライアントが所属する親グループや事前に作成したポリシーを設定に含めることが可能です。

■メインメニュー「インストーラー」画面



■インストーラー作成画面(1/4)

※複数の静的グループがある場合は、静的グループごとにインストーラーを分けて作成する必要があります。

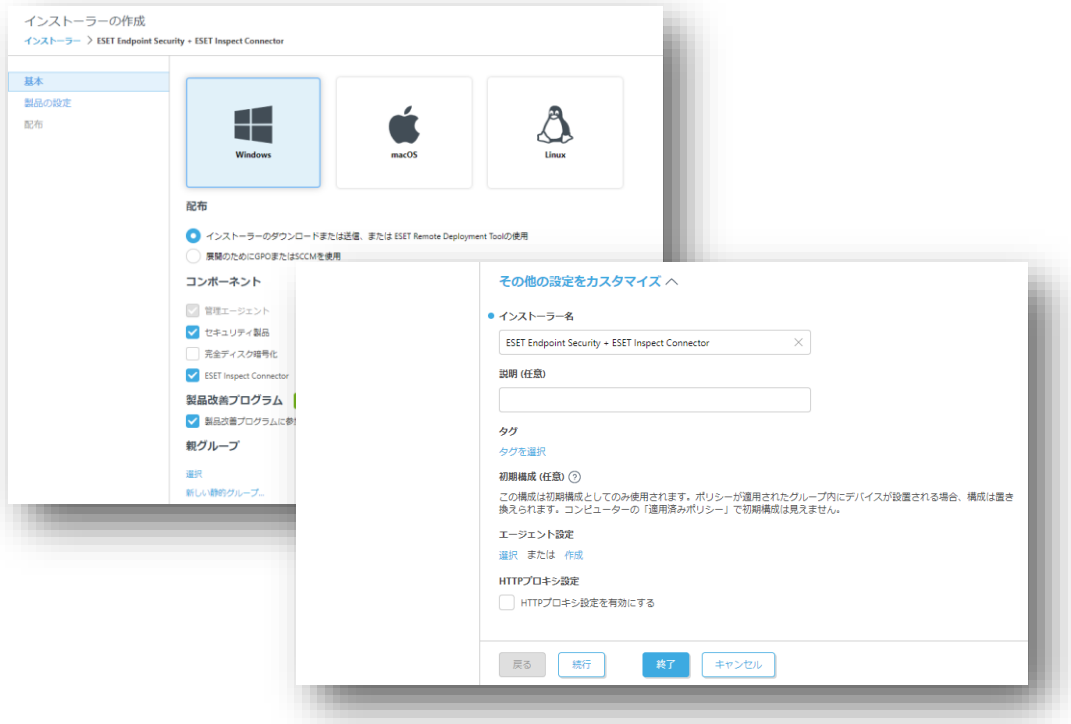
4. プログラムの展開

3. インストーラーの作成を行う場合(2/3)

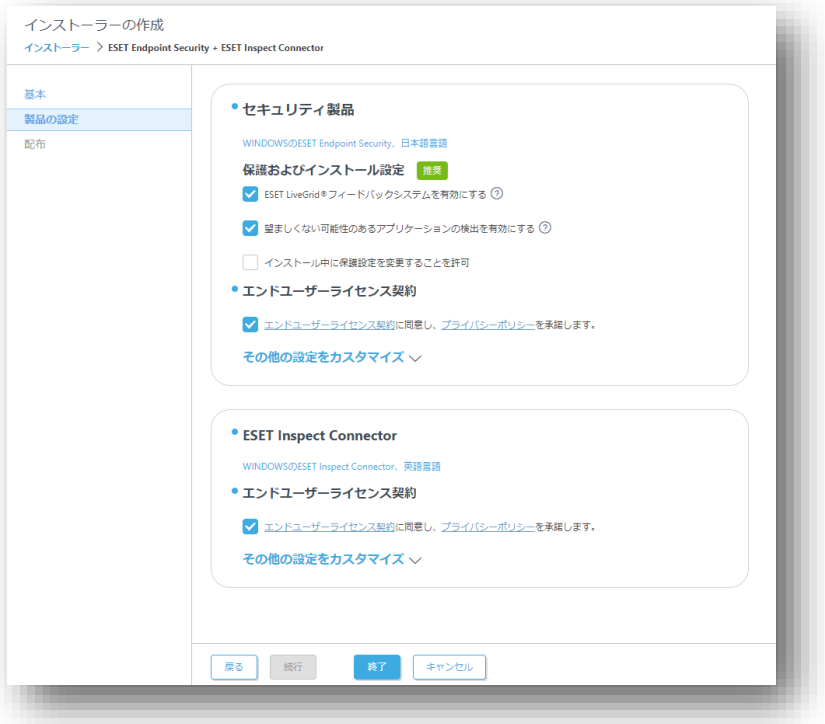
インストーラーに含めるコンポーネントやポリシー、親グループなどの各種設定を行います。

3. 「基本」画面では、インストーラーに含めるコンポーネントや親グループ、インストーラー名、ESET Management Agentに関する設定を行います。
4. 「製品の設定」画面では、インストーラー含めるセキュリティ製品のバージョンやポリシーの組み込みなどを行います。

■インストーラー作成画面(2/4)



■インストーラー作成画面(3/4)



4. プログラムの展開

3. インストーラーの作成を行う場合(3/3)

「配布」画面では作成したインストーラーの配布方法を検討します。

- インストーラーのダウンロードリンクが表示されるため、ダウンロードリンクのコピーやブラウザから直接ダウンロードが可能です。
- 電子メールアドレスを登録してメールでURLを配布することも可能です。（CSVで一括で電子メールアドレスを登録することも可能です。）

■インストーラー作成画面(4/4)

■電子メールプレビュー画面

4. プログラムの展開

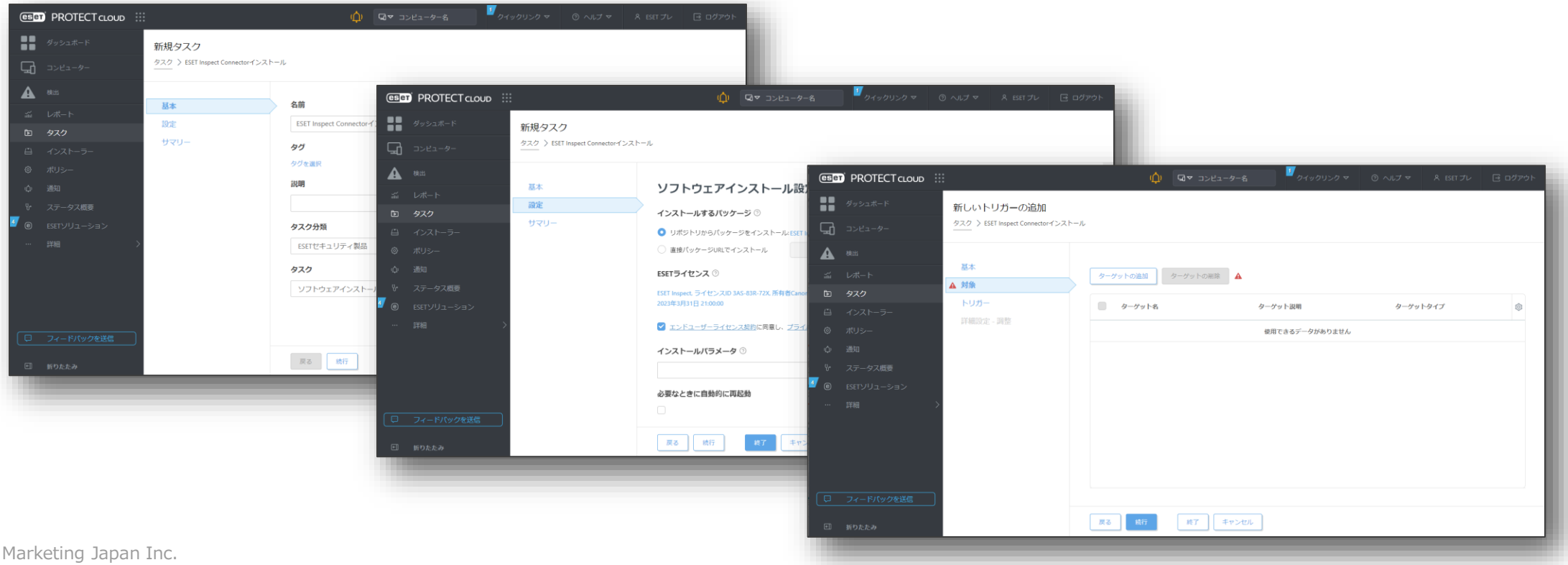
3. ソフトウェアインストールタスクを利用する場合

EPメインメニュー「タスク」より、「新規作成」-「クライアントタスク」を作成します。

メインメニューの「ポリシー」画面より、「新しいポリシー」をクリックします。

1. 基本画面でタスク分類を「すべてのタスク」または「ESETセキュリティ製品」、タスクを「ソフトウェアインストールタスク」を選択します。
2. 設定画面でインストールするパッケージから「ESET Inspect Connector」を選択し、ESETライセンスで「ESET Inspect」が選択されていることを確認します。
3. トリガー作成では、EI Connectorをインストールするクライアントまたはグループを選択し、タスク実行のタイミングであるトリガーを設定します。

■ソフトウェアインストールタスク画面



5. 初期最適化(チューニング)

5. 初期最適化(チューニング)

- 初期最適化は以下の流れで行います。

※ 初期最適化とはお客様業務により発生するアラートをEIの各検出ルールから除外することで、脅威により発生したアラートを見つけやすくする作業です。
※ 一度きりの検出を除外するのではなく、何度も繰り返し発生しているアラートを中心に除外を作成します。
※ 初期最適化完了後も脅威モニタリング時の継続したチューニングが必要です。

1.「ルール学習モード」によるチューニング

- EIには、自動で除外を作成できる「ルール学習モード」が搭載されています。
初期チューニング時には、本機能を有効化し、お客様業務により発生する
アラートを一定期間EIに認識させることで自動で除外を作成できます。
「ルール学習モード」の期間が終了したら、EIが作成した除外を
有効化するかを選択します。

2.手動による初期チューニング

- EIで発生したアラートを確認し、お客様業務により発生している
アラートであることが確認できた場合は除外を作成します。
※ LiveGridによるReputationやPopularity、親プロセスなどの情報を除外ルール含めることで、
よりセキュアな除外が作成できます。

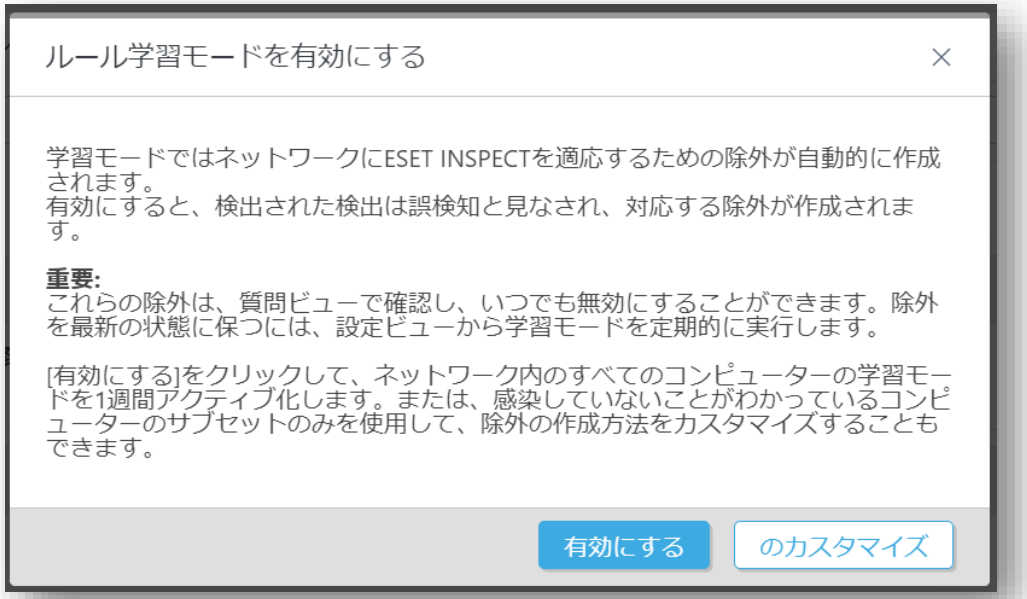
5. 初期最適化(チューニング)

1. 「ルール学習モード」によるチューニング(1/2)

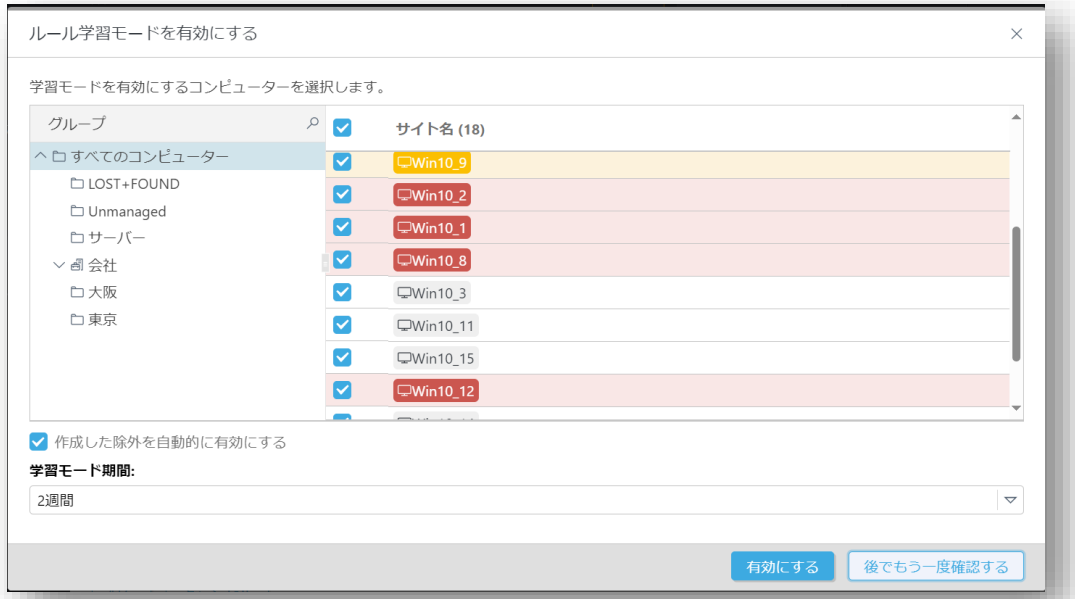
EIには自動で除外を作成できる「ルール学習モード」が搭載されています。

1. EIにログイン時に表示される「ルール学習モードを有効にする」から、「カスタマイズ」をクリックします。
2. 除外作成の対象とするグループとその期間を設定し、「有効にする」をクリックします。

■ 「ルール学習モード」設定画面



■ 「ルール学習モード」設定画面



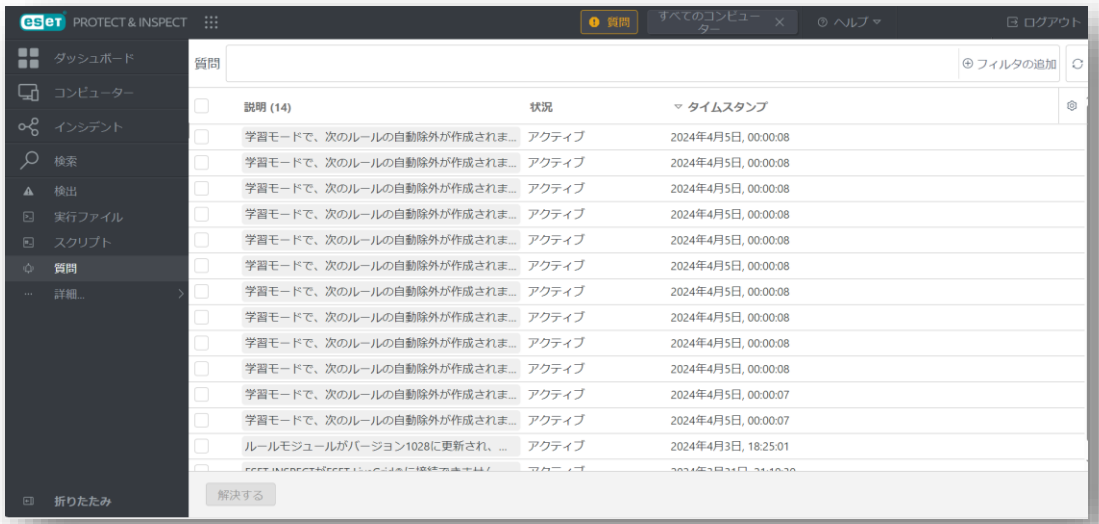
5. 初期最適化(チューニング)

1. 「ルール学習モード」によるチューニング(2/2)

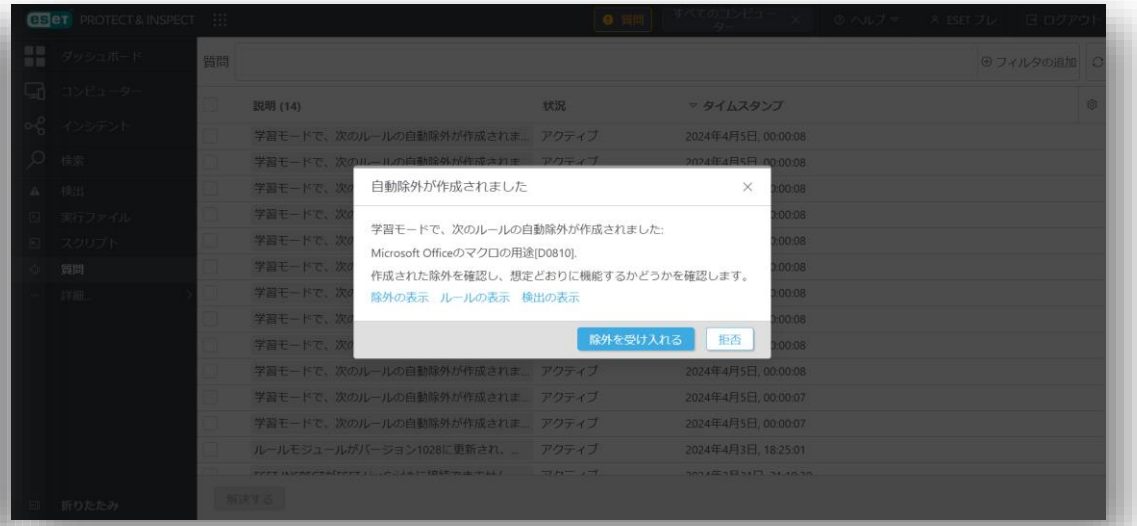
「ルール学習モード」の期間が終了したら、メインメニューの「質問」より有効化する除外を選択します。

3. メインメニューの「質問」より、「ルール学習モード」により作成された除外を確認します。
4. 作成された除外を有効化する場合は「除外を受け入れる」をクリックします。

■メインメニュー「Questions」画面



■除外ルール有効化画面



5. 初期最適化(チューニング)

2. 手動によるチューニング(2/3)

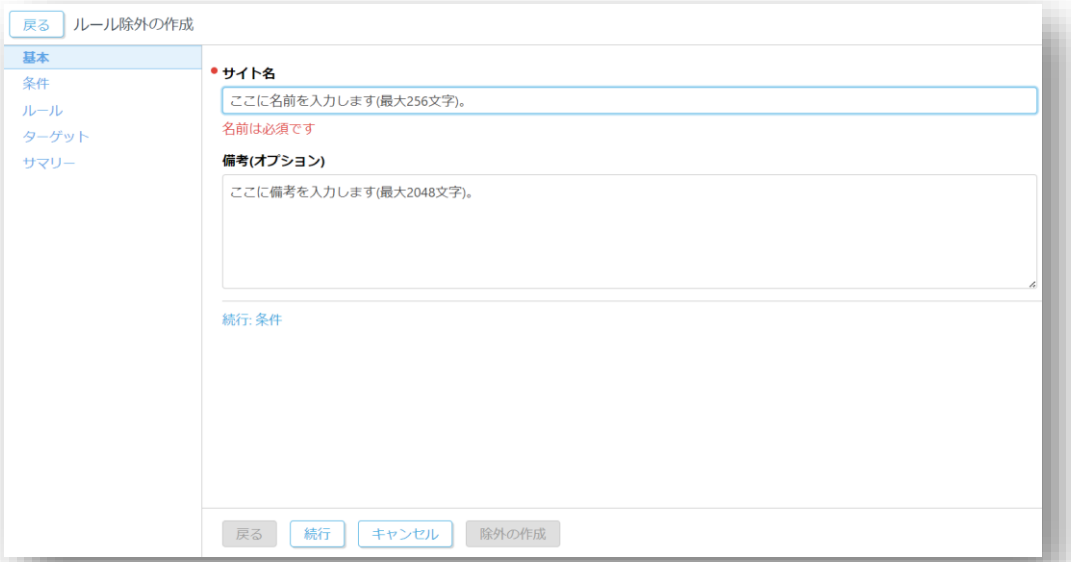
検出を除外しても問題ないことを十分確認してから作成します。

※ プロセスツリーやESET LiveGridによるレピュテーションの評価、検出されたファイルのシグネチャーの有無などをもとに判断します。

2. 除外を作成するアラートを選択し、「除外の作成」をクリックします。
   (複数の検出を選択して「除外の作成」をクリックすることで、検出情報をマージした除外が作成できます。)
3. 「基本」画面では、作成する除外の名前や説明を入力します。

■メインメニュー「DETECTIONS 」画面

■メインメニュー「DETECTIONS」画面



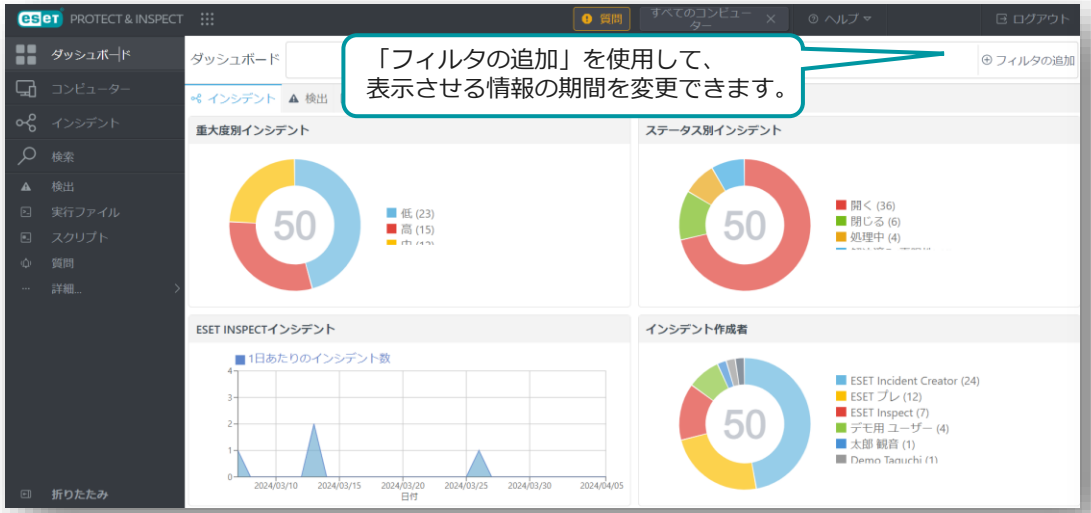
5. 初期最適化(チューニング)

2. 手動によるチューニング(1/3)

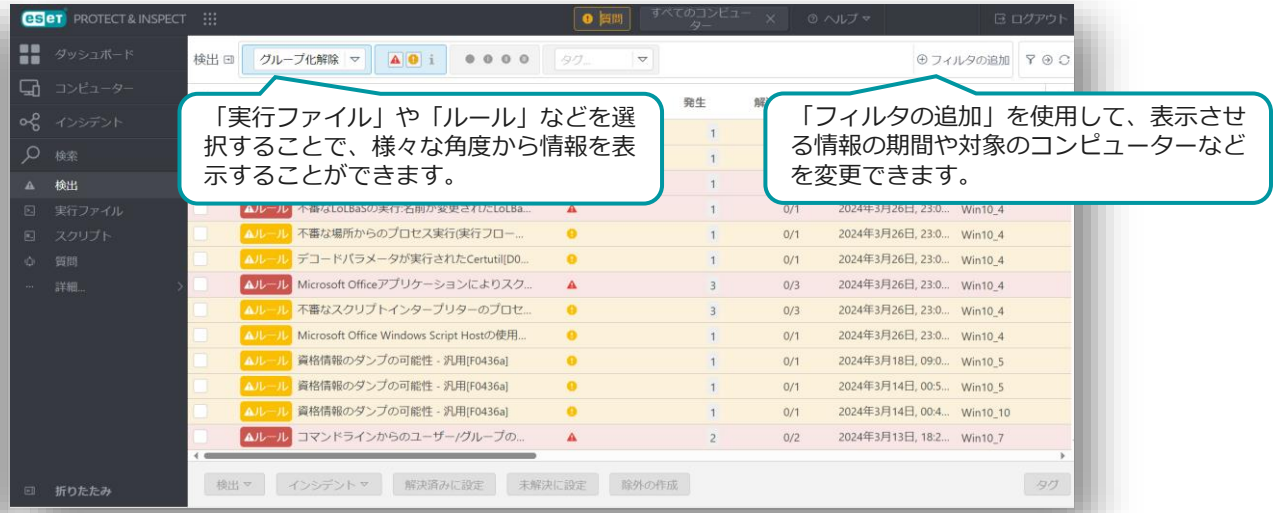
EIで表示されているアラートを確認し、お客様の業務により発生しているアラートである場合は手動で除外を作成します。
アラートは「ダッシュボード」や「検出」から確認できます。

1. 「ダッシュボード」からアラートを確認する場合は、発生しているアラートTOP10の円グラフ、または画面下部のタイムラインをクリックします。
   「検出」からアラートを確認する場合は、画面上部のフィルターを使用し、「ルール」や「実行ファイル」などでアラートを確認します。

■メインメニュー「ダッシュボード」画面



■メインメニュー「検出」画面



5. 初期最適化(チューニング)

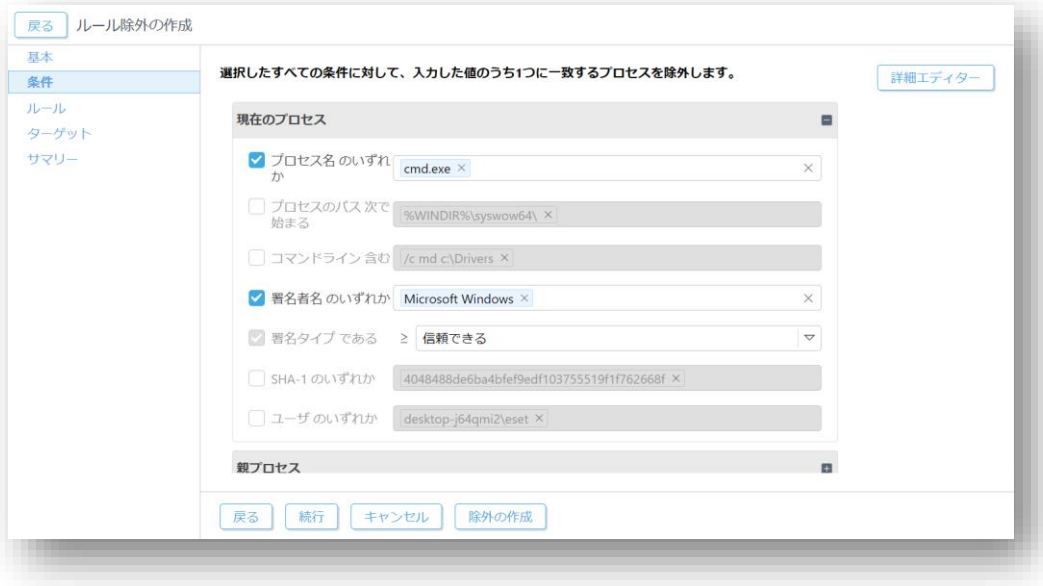
2. 手動によるチューニング(3/3)

除外のルールを設定します。

※ プロセスツリーやESET LiveGridによるレピュテーションの評価、検出されたファイルの署名の有無などをもとに判断します。

4. 「条件」画面では、除外のルールを作成します。
   ※ 除外はプリセットされた項目からチェックボックスで条件を選択して作成する方法とXMLで記述する自由度の高い「詳細エディター」の2種類があります。
5. 除外のルールを作成したら「ルール」画面にて、「一致する検出を解決する」にチェックが入っていることを確認して、「除外の作成」をクリックします。
   ※データベースからパージされたイベント(31日)によってトリガーされた検出は自動的に解決できません。

■基本除外画面



■詳細除外画面

※詳細エディターでの除外の記述方法に関しては以下のヘルプサイトをご参照ください。
https://help.eset.com/ei_rules/2.0/ja-JP/?rule_syntax.html

Ⅳ. その他の情報

EPとEIのバージョンアップについて

- **ESET PROTECT とESET Inspectのバージョンアップ**
  EPとEIのバージョンアップはESET社にて実施されるためお客様による作業は不要です。
  ※ バージョンアップの個別対応は不可となります。

- **ESET PROTECT のバージョンアップ作業に関して**
  EPのバージョンアップはESET社により段階的に行われ、バージョンアップ中は2~3分程度
  EPにアクセスできなくなります。
  EM Agentはログを溜め込む機能があるため、EPバージョンアップ後にEPにログ転送を再開します。

- **ESET Inspect のバージョンアップ作業に関して**
  EIのバージョンアップはESET社により段階的に行われ、バージョンアップ中は2~5分程度
  EIにアクセスできなくなります。
  EI Connectorはログを溜め込む機能があるため、EIバージョンアップ後にEIにログ転送を再開します。

- **ESET Management Agentのバージョンアップ**
  EM Agentは自動バージョンアップに対応しています。
  新しいバージョンのEM Agentがリリースされると、その2週間後から自動アップグレードがトリガーされます。

- **ESET Inspect Connectorのバージョンアップ**
  EI Connectorのバージョンアップはお客様自身で実施いただく必要がございます。
  EPのソフトウェアインストールタスクを利用してバージョンアップをお願いいたします。

サポート情報

- **弊社Webページにてサポート情報を記載しております。**
  ESET PROTECTソリューションシリーズ サポート情報(Q&A)
  https://eset-support.canon-its.jp/?site_domain=business
- **ESET PROTECTソリューションシリーズの**
  プラグラムおよびマニュアルはユーザーズサイトにてご提供しております。
  ESET PROTECTソリューション ユーザーズサイト
  https://canon-its.jp/product/eset/users/index.html
- **以下の各種オンラインヘルプもご確認ください。**
  ESET PROTECT のオンラインヘルプ
  https://help.eset.com/protect_cloud/ja-JP/

  ESET Inspect のオンラインヘルプ
  https://help.eset.com/ei_cloud/ja-JP/