クラウド型XDRコンポーネント

ESET Inspect 機能紹介資料

第9版

2025年5月26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のクラウド型XDRコンポーネントである**ESET Inspect**（以降、EI）の機能についてご説明いたします。

※ MDRサービスは「ESET PROTECT MDR Ultimate」をご契約いただいたお客様のみご利用可能です。
※ 「ESET PROTECT MDR Ultimate」でMDRサービスとプレミアムサポートを受ける場合、クラウドでのセキュリティ管理となります。

もくじ

Ⅰ. ESET Inspectとは

Ⅰ. ESET Inspectとは

- **XDR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

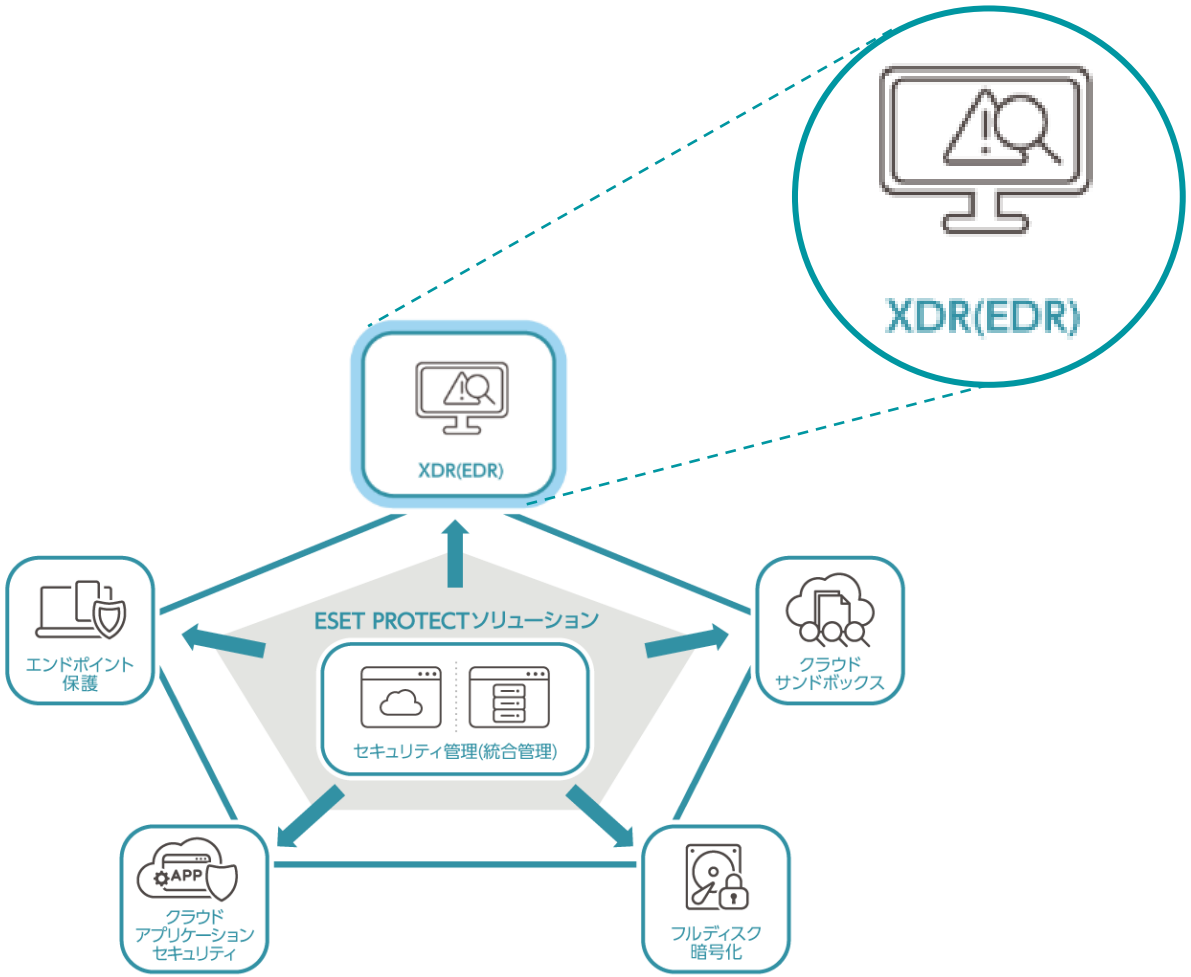
早期に攻撃を発見し
被害を抑えられる

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

Ⅰ. ESET Inspectとは

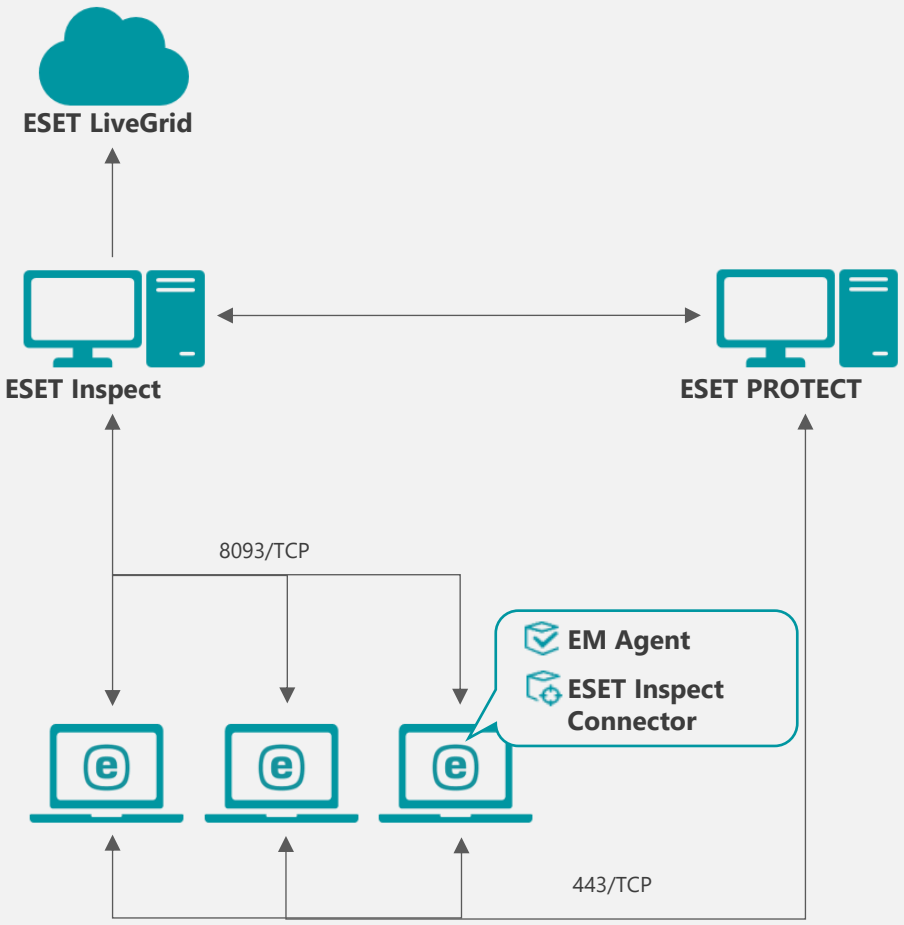


- ESET Inspect（以降、EI）とはクラウド型のXDRコンポーネントです。
- SaaSであるため、利用者によるサーバーのバージョンアップやメンテナンスの必要はございません。
- EIの利用には、クラウド型セキュリティ管理ツールである ESET PROTECT（以降、EP）が利用可能なバンドルライセンスと、ライセンス管理のWebシステムでありEIとEPのポータルとしても使用するESET Business Account（以降、EBA）/ ESET PROTECT HUB（以降、EPH）のアカウントが必要です。
- EIを利用するにはEPでのクライアント管理が必須となります。

Ⅱ. ESET Inspectの構成

Ⅱ. ESET Inspectの構成

ESET Inspect構成イメージ



ESET Inspect（EI）

EI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）

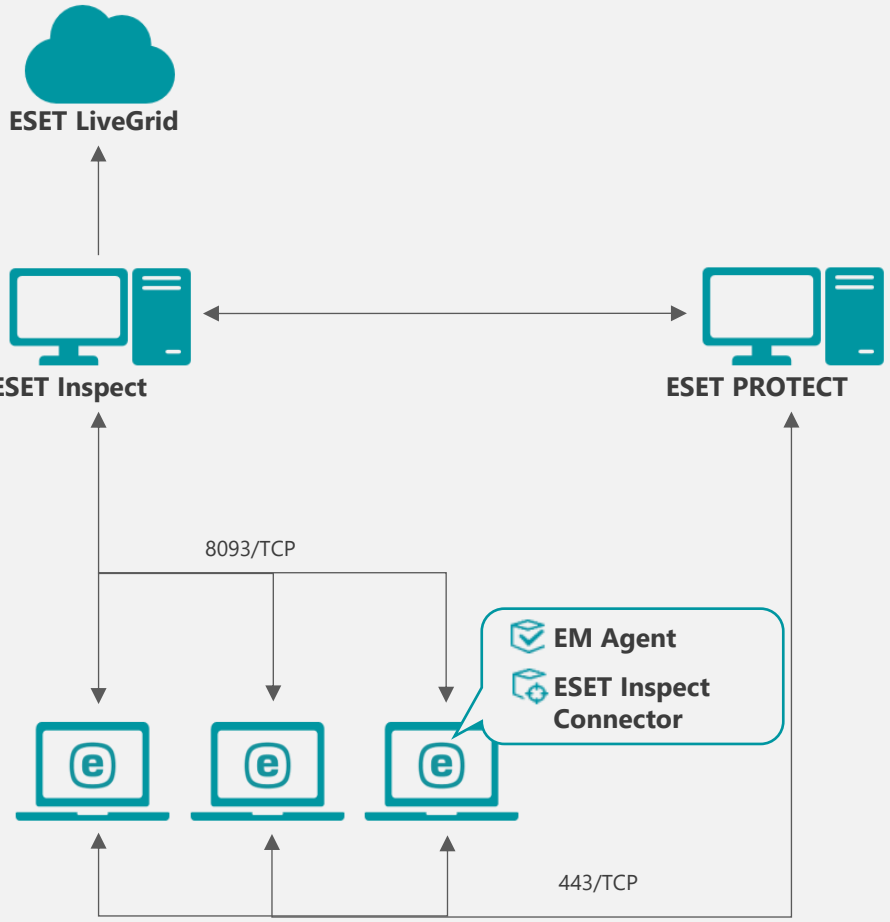
EI Connectorはクライアントのデータを収集し7分間隔でEIへデータを送信します。また、悪意のあるコンポーネントを削除し、これらのコンポーネントの実行をブロックします。

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。

Ⅱ. ESET Inspectの構成

ESET Inspect構成イメージ



ESET Inspectに関連する主な通信ポート

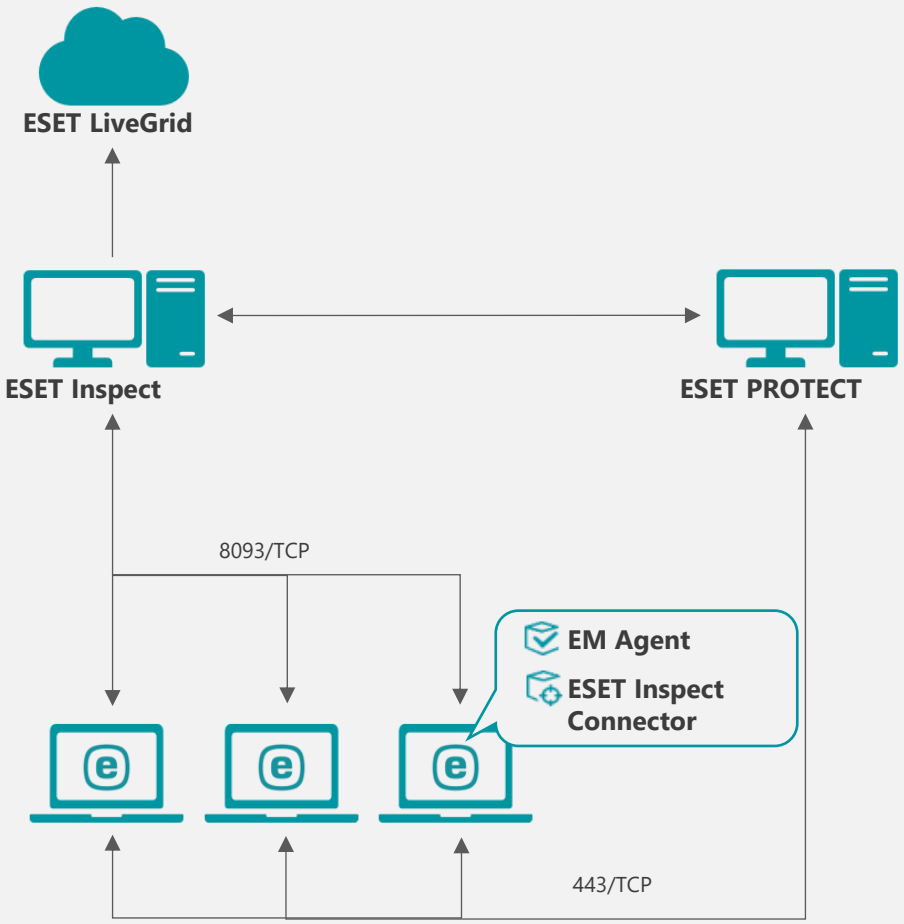
ポート	用途
443/TCP	EM AgentとESET PROTECT間の通信に使用
8093/TCP	ESET Inspect ConnectorとESET Inspect間の通信に使用

サポートされるプログラム

アプリケーション名
ESET Endpoint Security / アンチウイルス
ESET Endpoint Security for macOS / ESET Endpoint アンチウイルス for OS X
ESET Endpoint アンチウイルス for Linux
ESET Server Security for Microsoft Windows Server
ESET Server Security for Linux

Ⅱ. ESET Inspectの構成

ESET Inspect構成イメージ



サポートされるOS（ESET Inspect Connector）

OS名
Windows 10 ※1 ※2 / 11
Windows Server 2012 / 2012 R2 / 2016 / 2019 / 2022
Red Hat Enterprise Linux (RHEL) 7.9以降 / 8 / 9以降 (64bit)
Cent OS 7.9以降 (64bit)
SUSE Linux Enterprise Server (SLES) 15 (64bit)
Amazon Linux 2 (64bit)
Alma Linux 8 / 9 (64bit)
Rocky Linux 8 / 9 (64bit)
Ubuntu 18.04 / 20.04 / 22.04 Desktop (64bit)
macOS 10.15 Catalina / 11 Big Sur / 12 Monterey / 13 Ventura / 14 Sonoma / 15 Sequoia

※1 Windows10 21H1以前のOSはサポート対象外
※2 Azure Virtual Desktop / Microsoft Windows 10マルチセッションモードをサポート

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. ESET Inspectのメリット

Ⅲ. ESET Inspectのメリット

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

Ⅲ. ESET Inspect（旧ESET Inspect Cloud）のメリット

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。

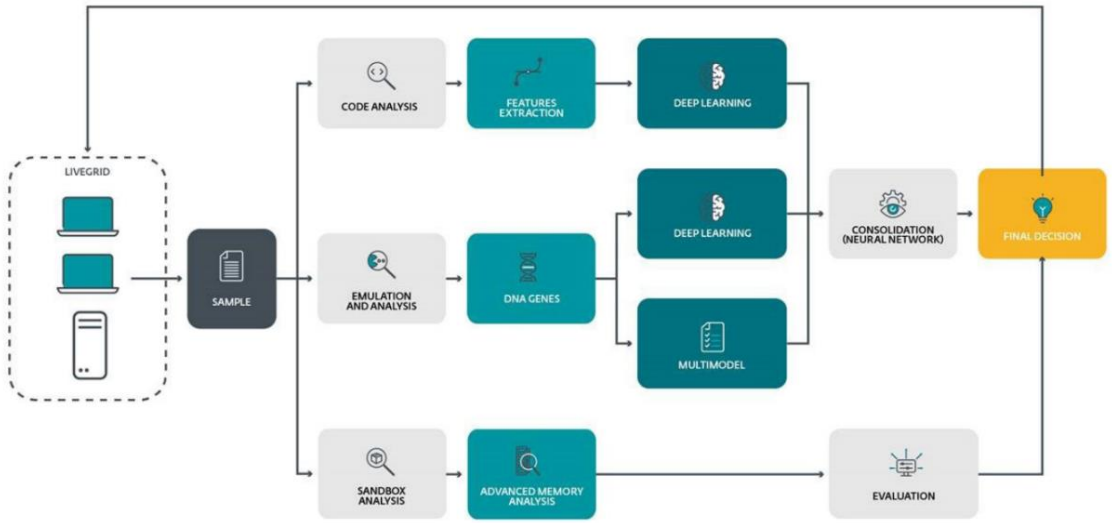
ESET LiveGrid®（Reputation & Feedback）

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。

Ⅲ. ESET Inspectのメリット

20年以上の機械学習への取り組みで得た知見をベースに開発

- ニューラルネットワーク（ディープラーニング, LSTM（長期短期記憶））
- 6つの厳選された分類アルゴリズム
- サンプルを「クリーン」,「潜在的に望ましくない」,「悪意があるもの」としてラベリング
- DNA分析, サンドボックス, メモリ分析など、他の保護テクノロジーや動作特性の抽出機能と連携



出力結果は**LiveGrid®**を介して様々なシーンで利用される

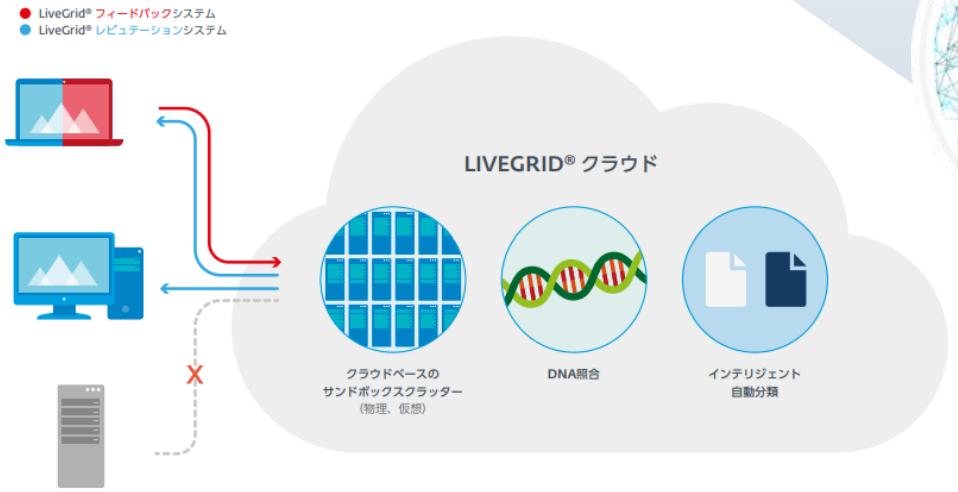
Ⅲ. ESET Inspectのメリット

LiveGrid®レピュテーションシステム

- 最新の分析結果をリアルタイムで提供
- 様々なオブジェクトを判定（ファイル, 証明書, URL, IPアドレスなど）

LiveGrid®フィードバックシステム

- 疑わしいサンプルをESETに送信し詳細な分析にかける
- 機械学習やセキュリティ専門家による分析結果も反映



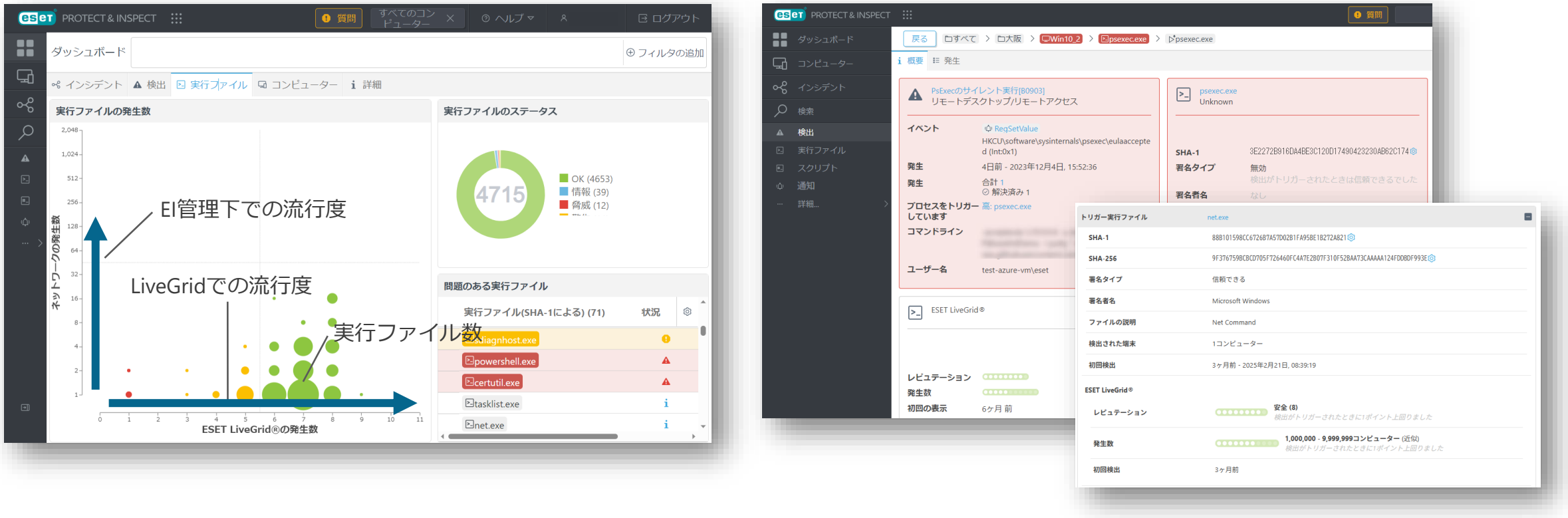
New **Cloud Malware Protection System**

世界１億１千万台以上の

センサーから集積されたデータを分析

検出エンジンの更新を待つことなく
常に最新の脅威情報を得られる

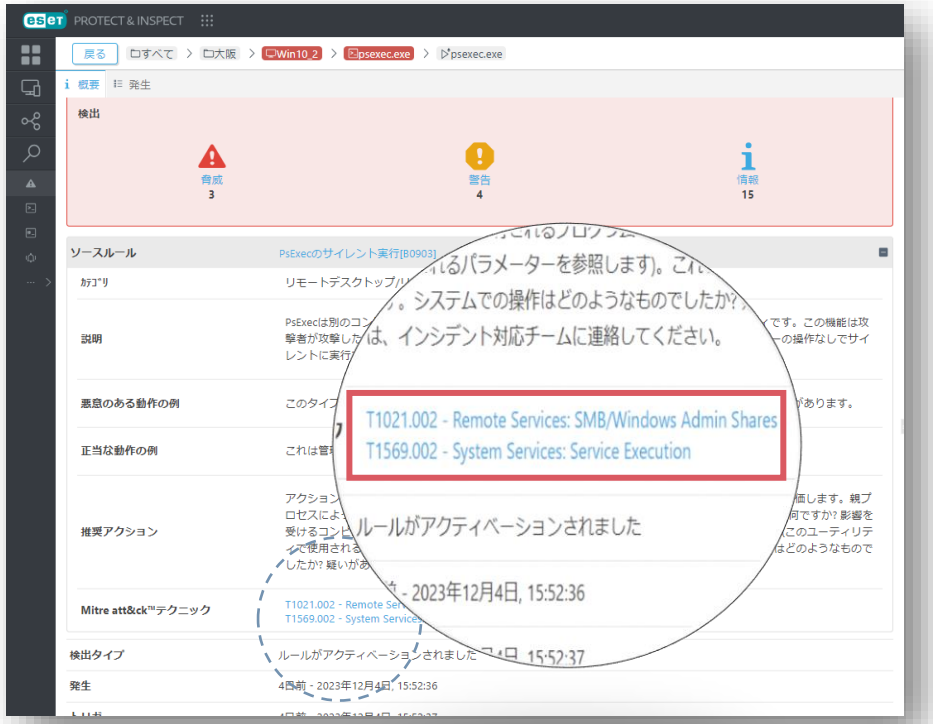
Ⅲ. ESET Inspectのメリット

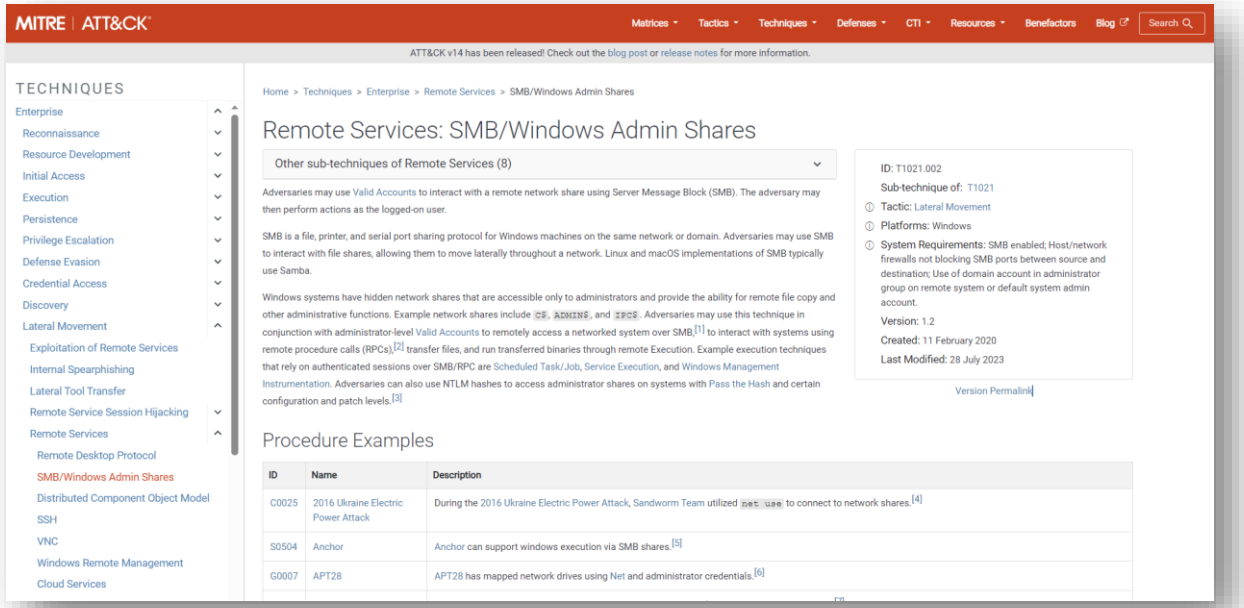


- **EI管理下とLiveGridの流行度（Popularity）を軸に、自組織とグローバルのギャップを可視化**
- **LiveGrid上の評判（Reputation）や流行度（Popularity）を確認し、トリアージの判断材料として活用**

Ⅲ. ESET Inspectのメリット

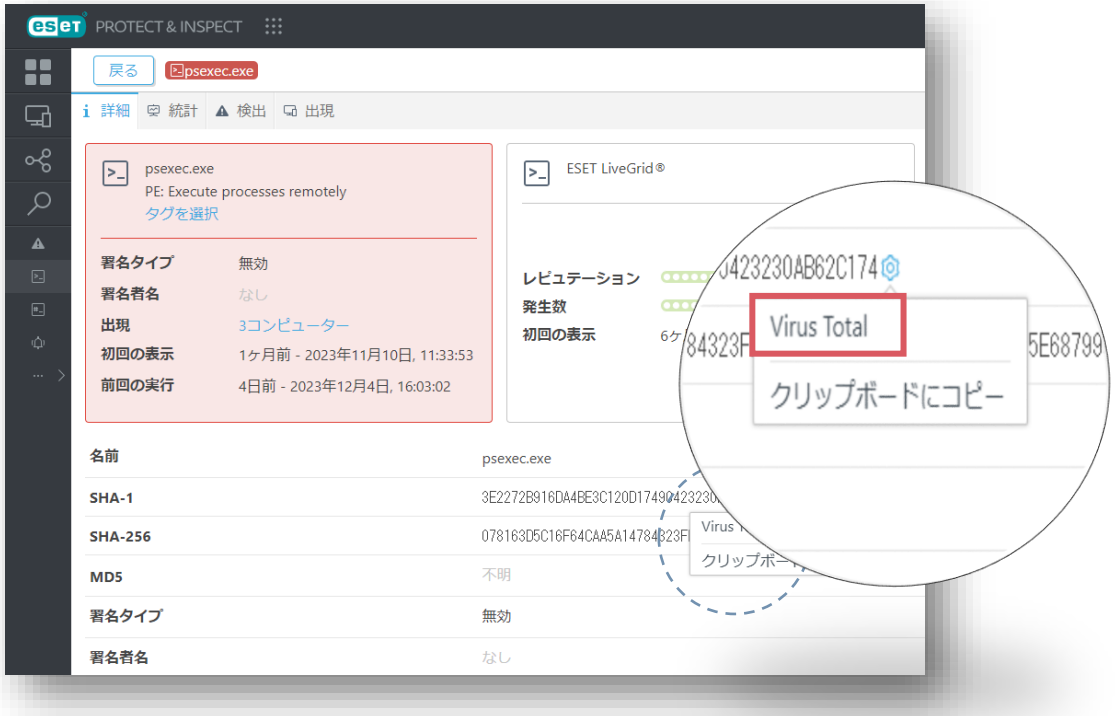
EIの検出アラートから、攻撃に使用されたテクニックの詳細を参照可能

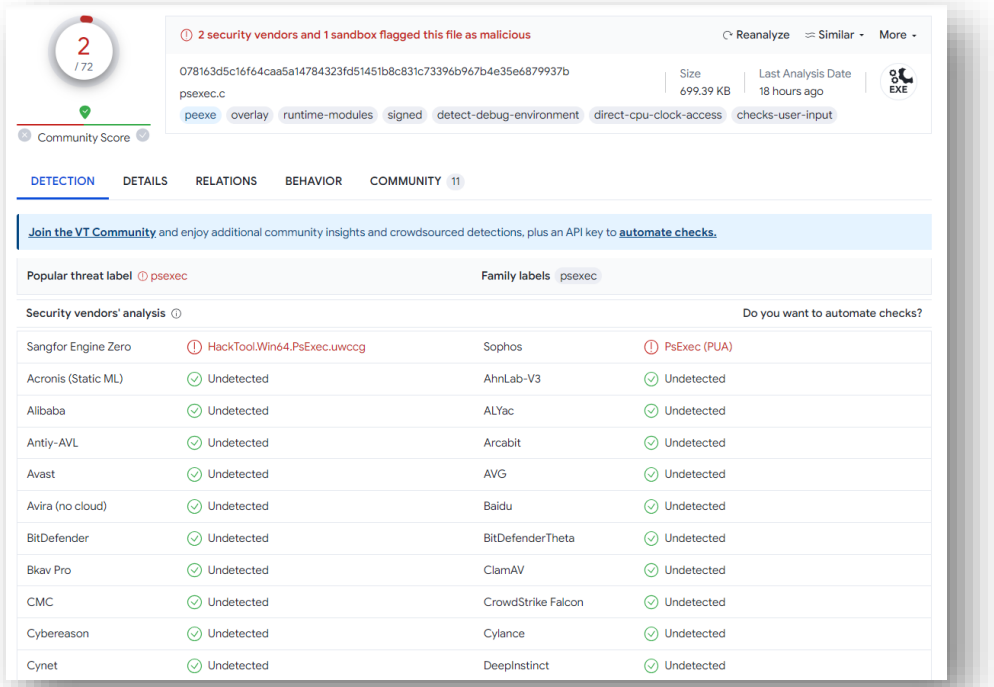




Ⅲ. ESET Inspectのメリット

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

VirusTotal

Ⅳ. WEBコンソールのご紹介

Ⅳ. WEBコンソールのご紹介

- **WEBコンソールへのログイン**

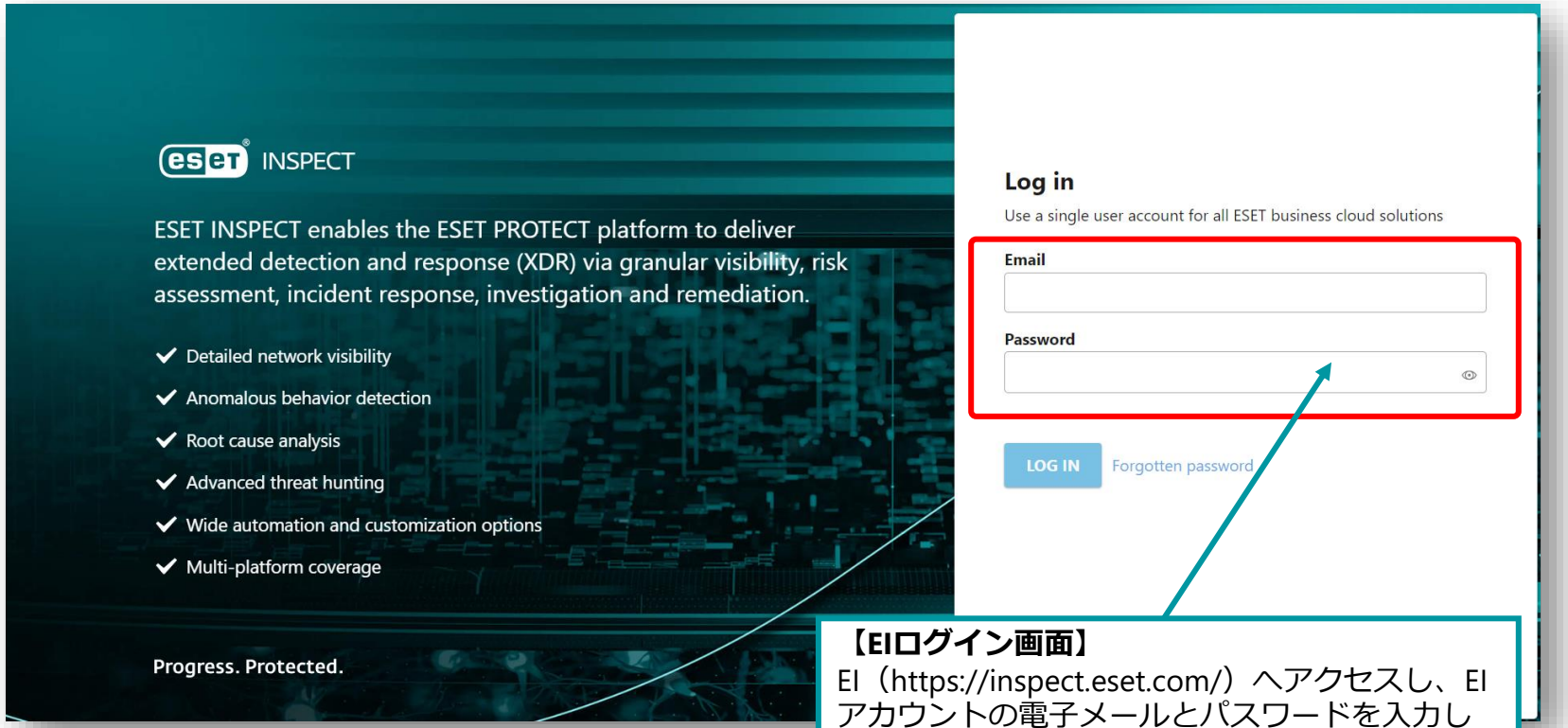
  EIのWEBコンソールへは、WEBブラウザを使用してログインします。WEBインターフェースのため、WEBブラウザからいつでもどこからでもログインできます。

ESET Inspect 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

※最新バージョンでの
ご利用をお勧めします

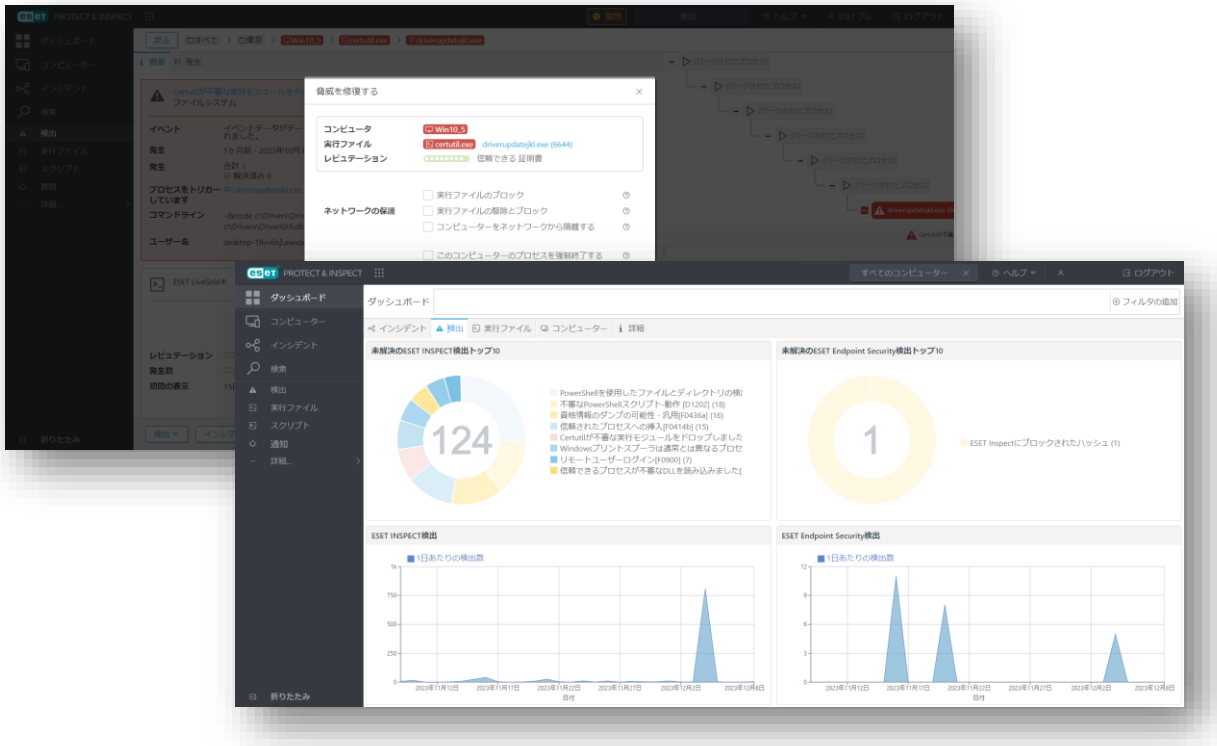
ESET Inspect Webコンソールへのログイン

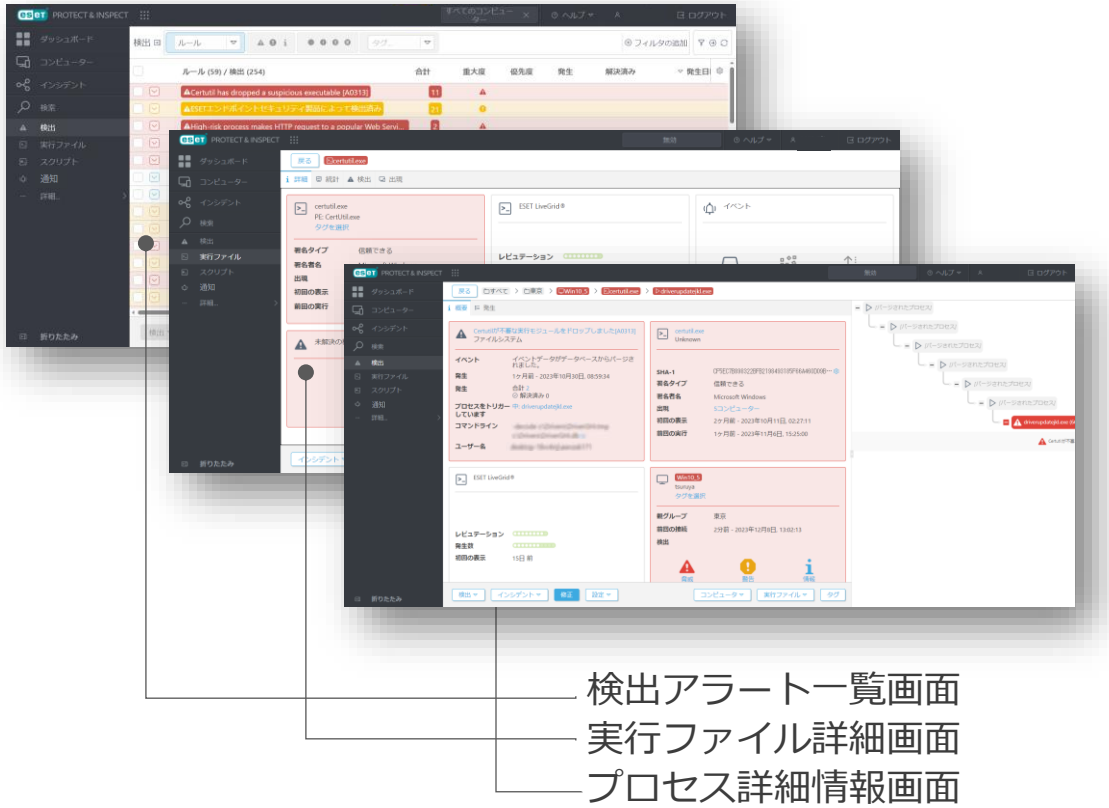


【EIログイン画面】
EI（https://inspect.eset.com/）へアクセスし、EIアカウントの電子メールとパスワードを入力してログインします。

Ⅳ. WEBコンソールのご紹介

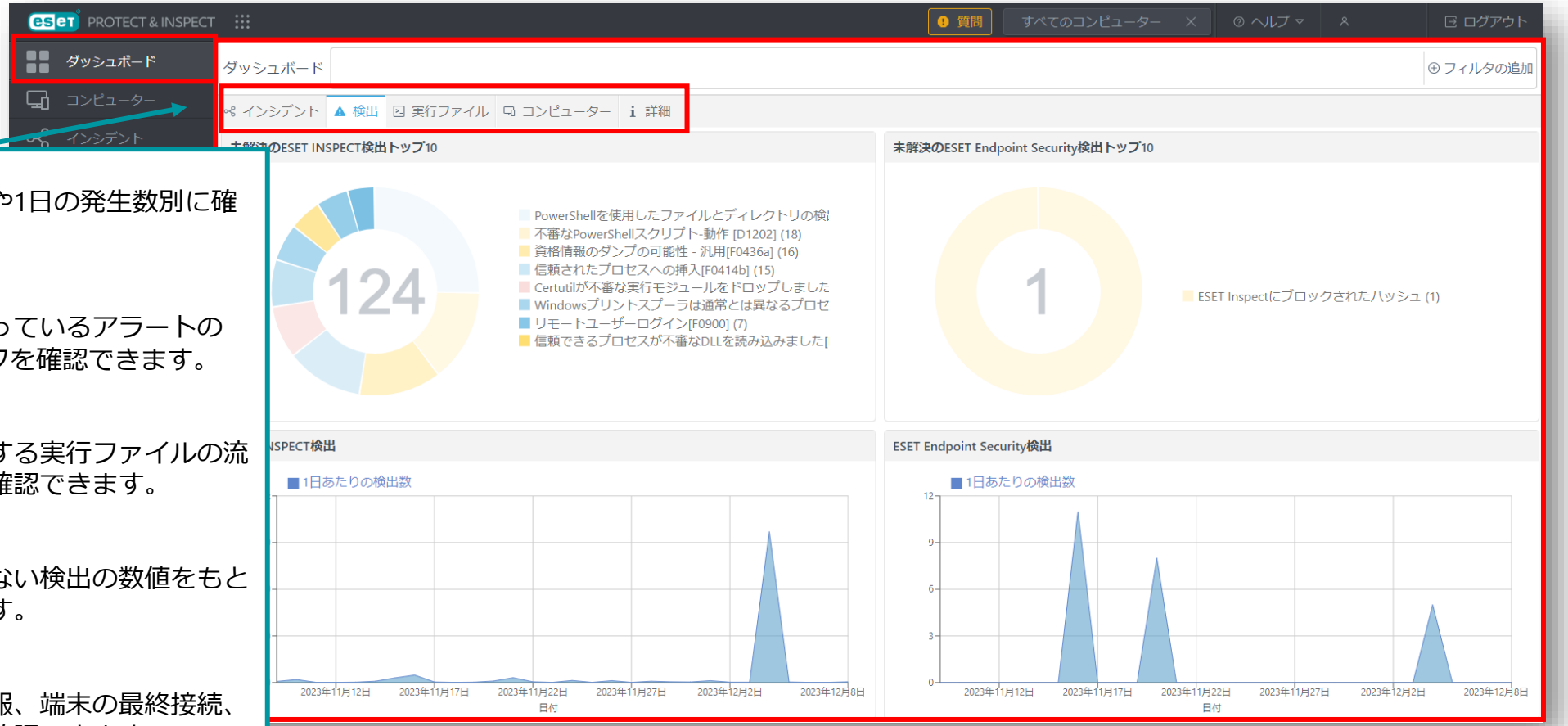
- **WEBコンソールについて**
  ダッシュボードを起点にあらゆる角度から調査を開始可能です。
  可視化機能や高度な検索機能が対応を強力にサポートしているため、１つのWebコンソールだけでミクロ・マクロ両方の視点から調査が可能です。脅威が発見された場合は、すぐにネットワークやコンピューターの保護を実行できます。





Ⅳ. WEBコンソールのご紹介

- **ダッシュボードについて**
  ダッシュボードではタブに応じて、様々な情報を表示することができます。EIユーザーはこれらの情報を利用することでトリアージを行うことができ、迅速な対応が可能となります。



【インシデントタブ】
インシデントをステータスや1日の発生数別に確認できます。

【検出タブ】
管理している端末内で起こっているアラートのTOP10や発生日時別のグラフを確認できます。

【実行ファイルタブ】
管理している端末内に存在する実行ファイルの流行度をグルーバルな観点で確認できます。

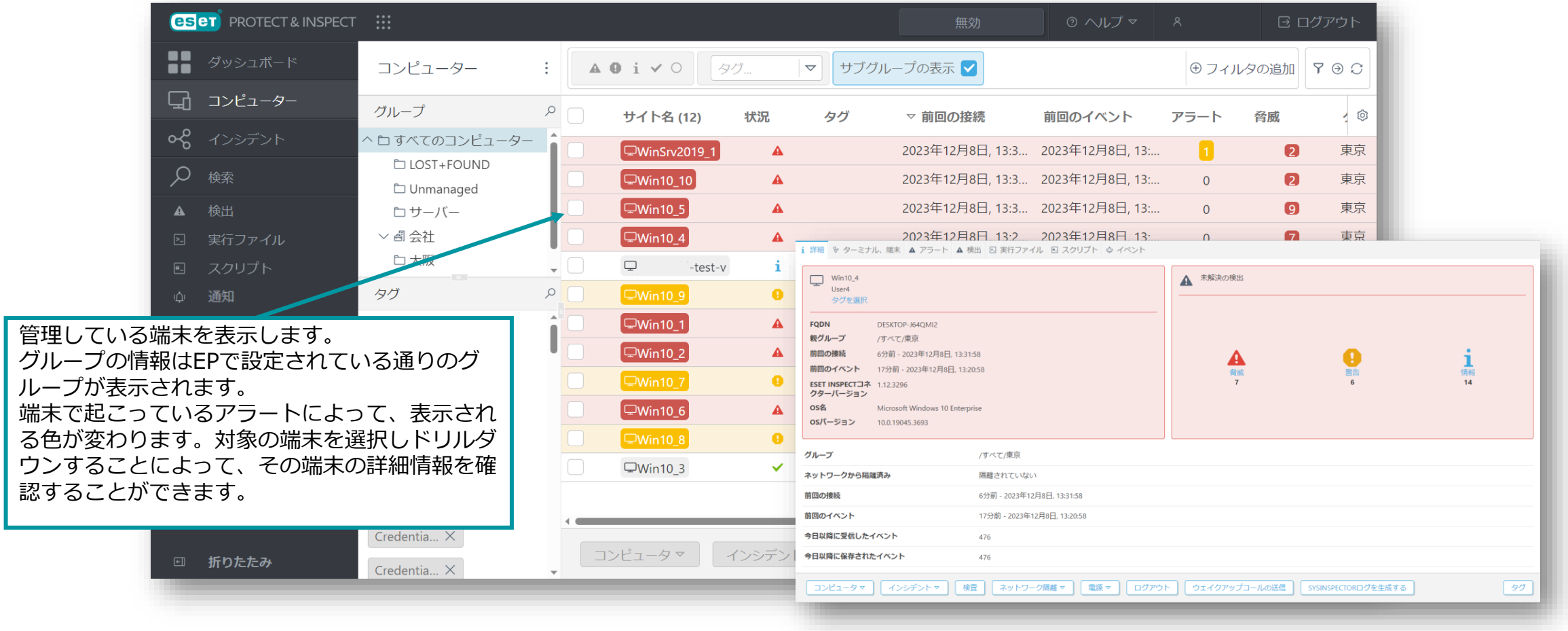
【コンピュータータブ】
解決した検出、解決していない検出の数値をもとに対象の端末を確認できます。

【詳細】
解決されていない検出の情報、端末の最終接続、本日起こったイベント等を確認できます。

Ⅳ. WEBコンソールのご紹介

- **コンピューターについて**

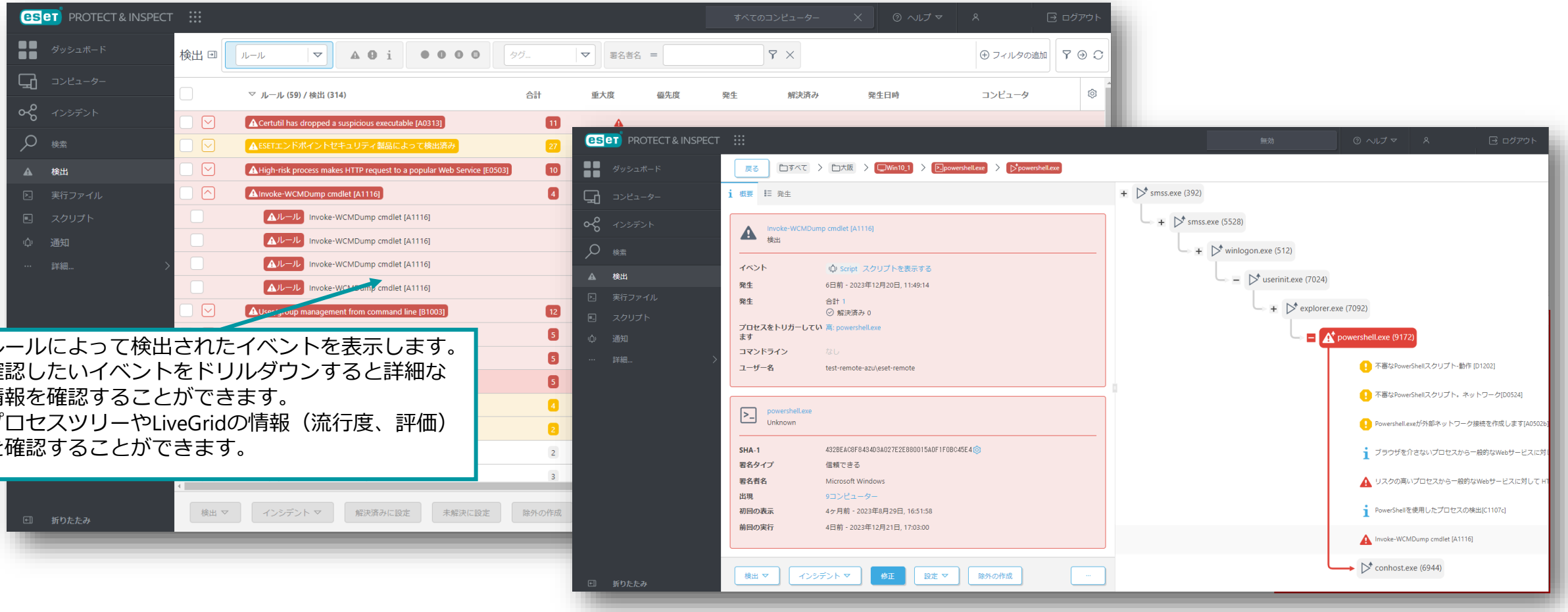
  コンピューターではESET PROTECTのグループ構成を表示することが可能です。
  この画面ではコンピューター毎に詳細情報を確認・調査していくことができます。



管理している端末を表示します。
グループの情報はEPで設定されている通りのグループが表示されます。
端末で起こっているアラートによって、表示される色が変わります。対象の端末を選択しドリルダウンすることによって、その端末の詳細情報を確認することができます。

Ⅳ. WEBコンソールのご紹介

- **検出について**
  検出ではルールに引っかかった検出を確認できます。フィルターや並び替えを利用することで確認したい検出を簡単に確認できます。
  またこの画面から検出の詳細画面に遷移することができます。

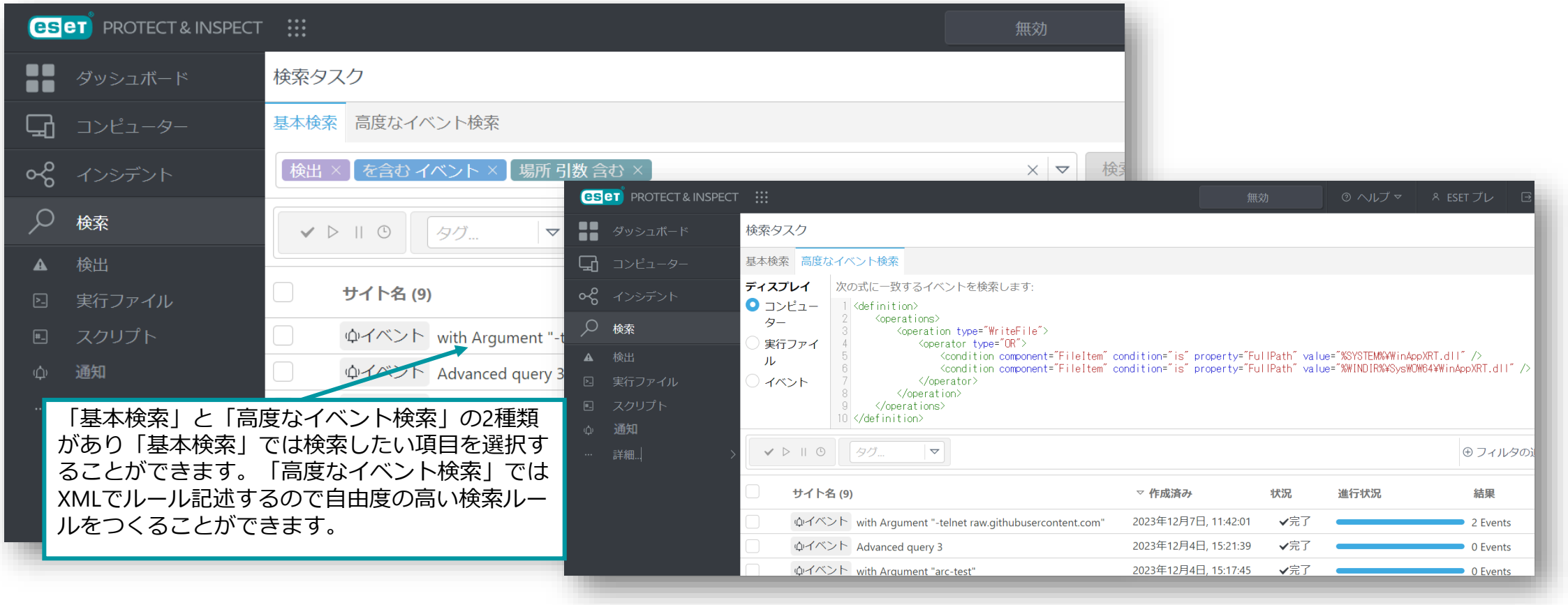


ルールによって検出されたイベントを表示します。
確認したいイベントをドリルダウンすると詳細な情報を確認することができます。
プロセスツリーやLiveGridの情報（流行度、評価）を確認することができます。

Ⅳ. WEBコンソールのご紹介

- **検索について**

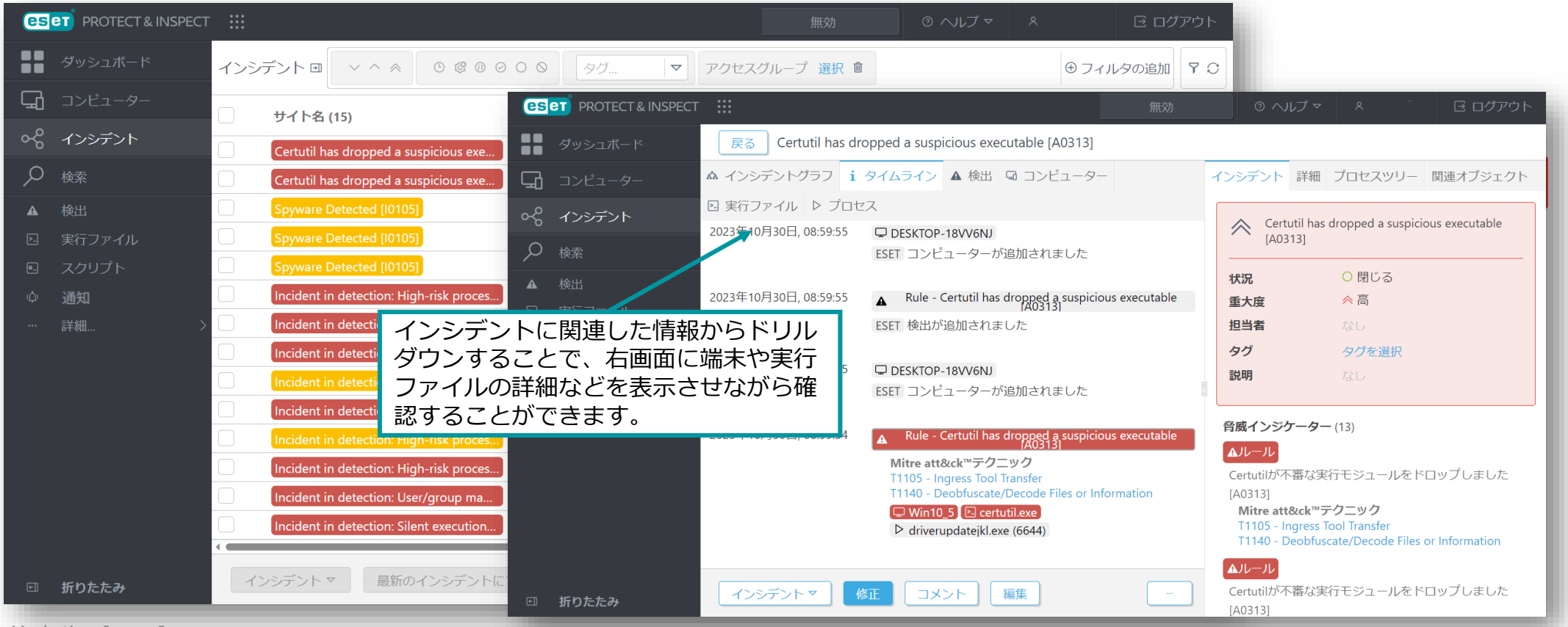
  検索はEIに集められた膨大なイベントの中から特定の情報を探しだすことができます。設定した検索方法は保存しておくことができるので、効率的に検索することができます。



Ⅳ. WEBコンソールのご紹介

- **インシデントについて**

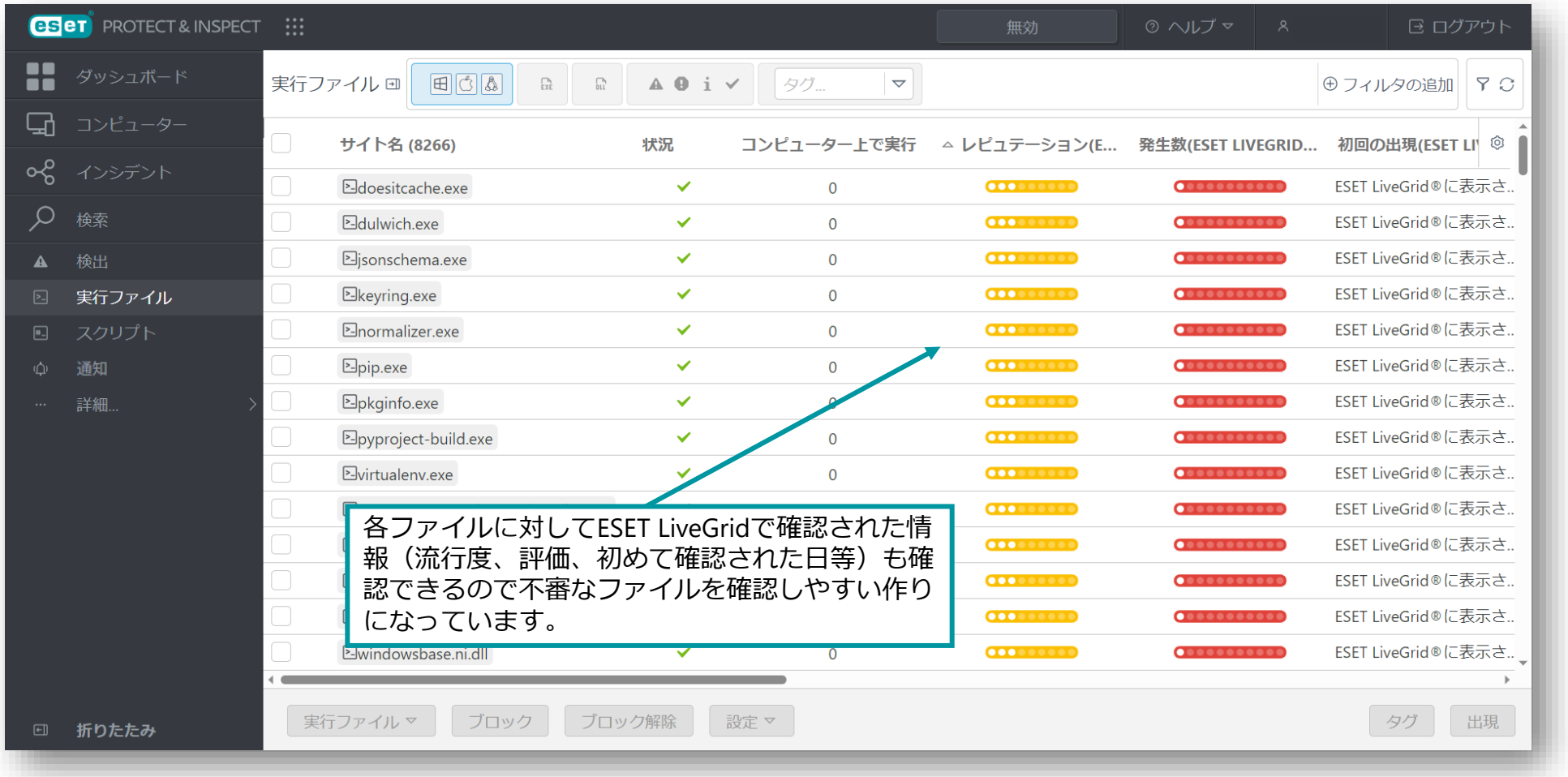
インシデントと疑われる検出があった場合、自動でEIにインシデントが作成されます。
作成されたインシデントの詳細では、検出やオペレーターの対応内容などのタイムラインに加えて、関連するプロセスや実行ファイルなどのオブジェクトを一元的に管理し、コンピューターのネットワーク隔離などの対応までをまとめて実施することができます。
また、オペレーター同士でコメントを残せるため、本機能をインシデントレスポンスチームで使用することも可能です。



Ⅳ. WEBコンソールのご紹介

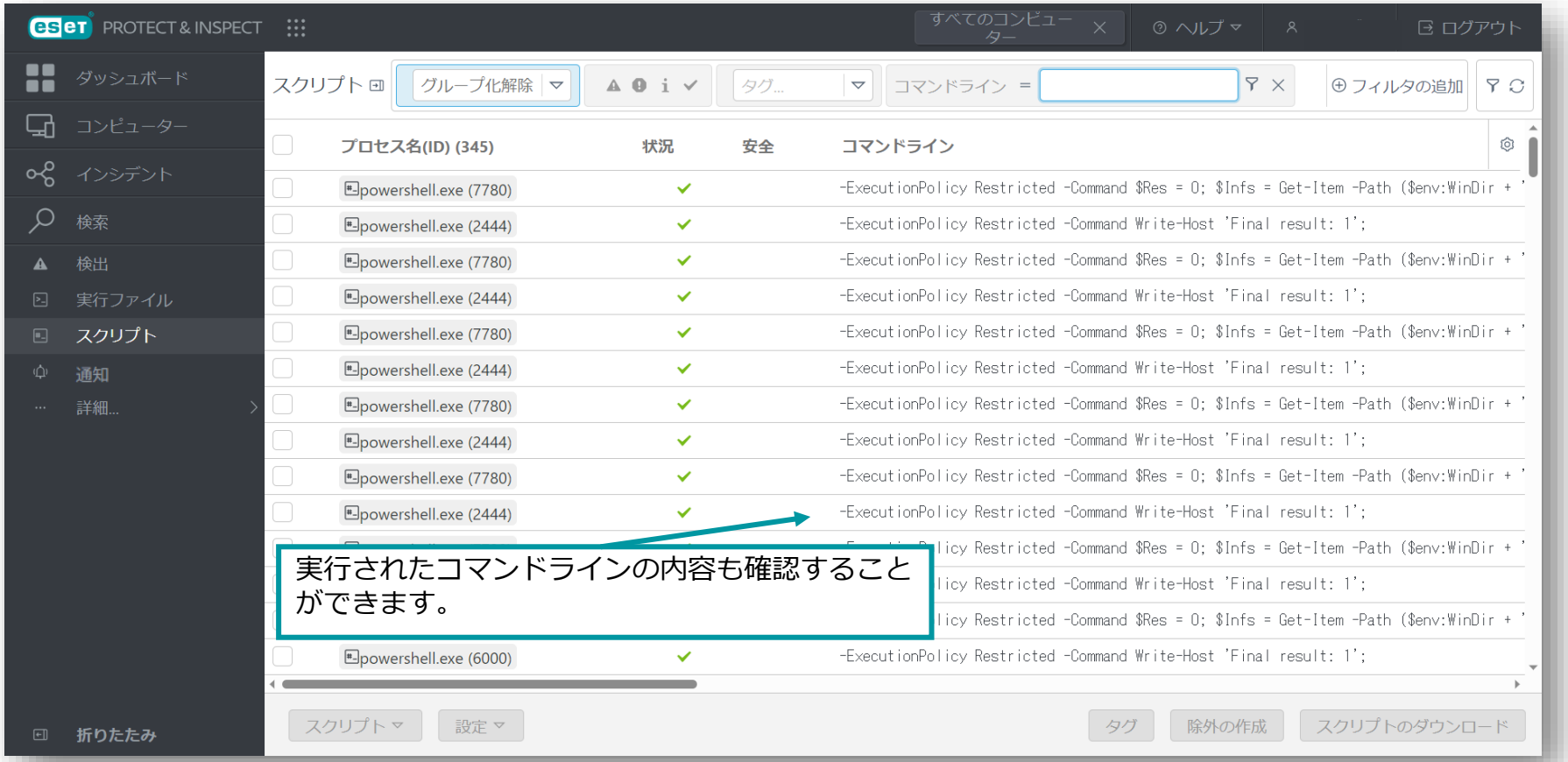
- **実行ファイルについて**

  実行ファイルは管理している端末内に存在する実行ファイル（Windows/macOS/Linux）を確認できます。
  プリセットのフィルタを利用することで、条件にマッチした実行ファイルのみを確認できます。



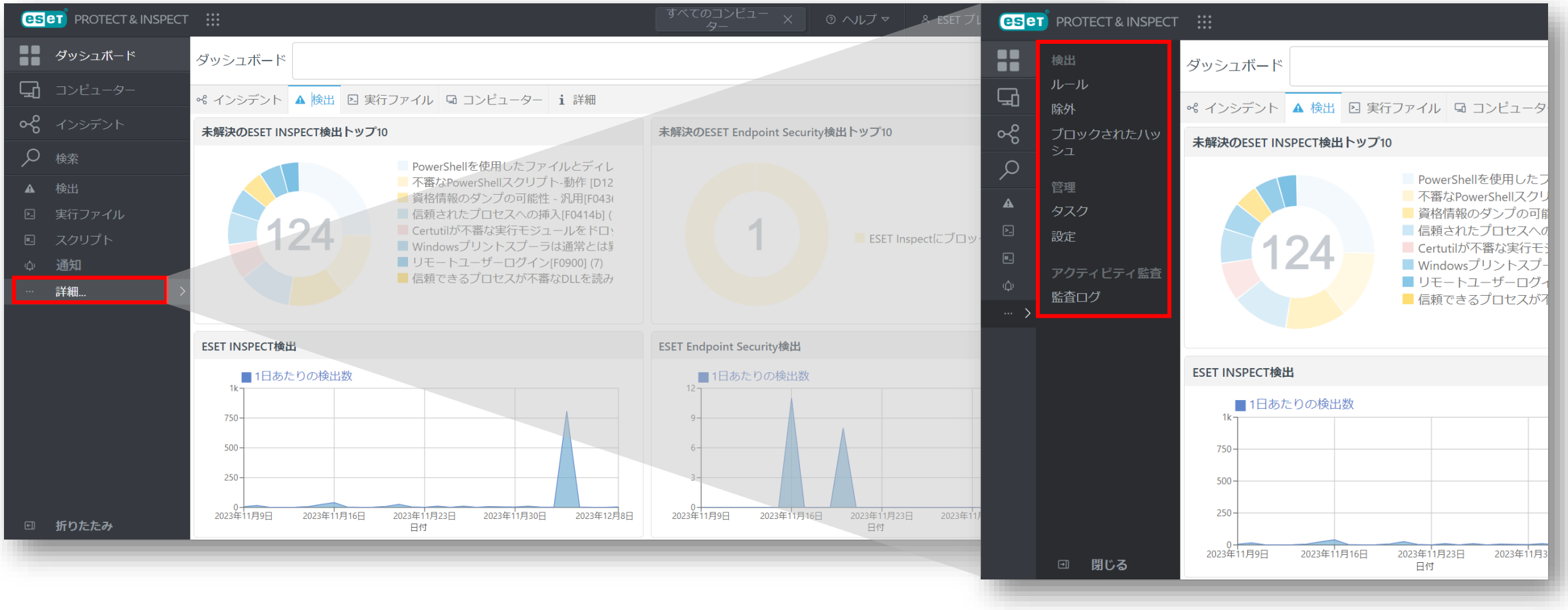
Ⅳ. WEBコンソールのご紹介

- **スクリプトについて**
  スクリプトは管理している端末内で実行された全てのスクリプトに関する情報を確認できます。
  Visual Basicスクリプト、PowerShell用スクリプト（WScriptとCScript）がサポートされます。



Ⅳ. WEBコンソールのご紹介

- **詳細について**
  詳細はルール作成、除外、ハッシュブロック、監査ログの確認、タスクの実行、サードパーティ製WEBサイトとの連携に関する設定を行うことができます。

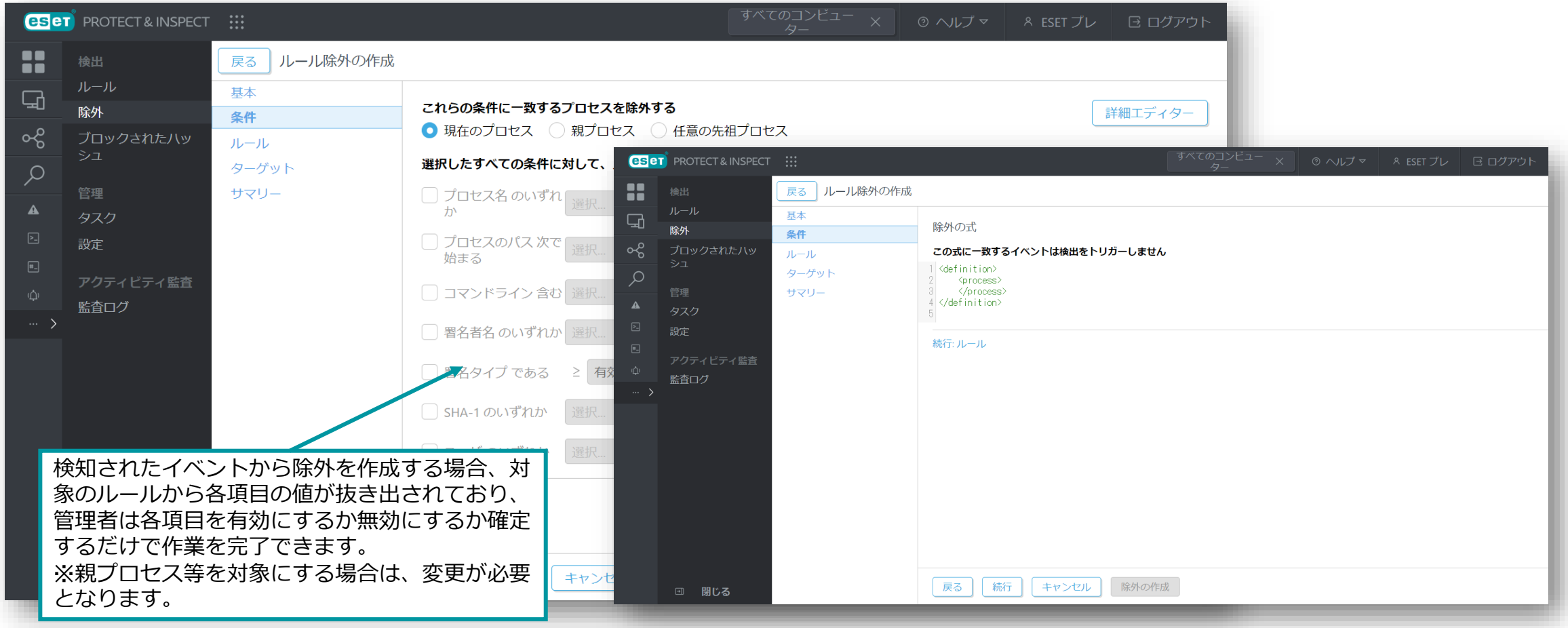


Ⅴ. 各機能のご紹介

V. 各機能のご紹介

- **除外について**

除外は各ルールからある一定の条件を満たした検出を除外することができる機能です。除外には2種類の方法があり、
プリセットされた項目を利用する方法とXMLで記述する自由度の高い詳細エディターがあります。

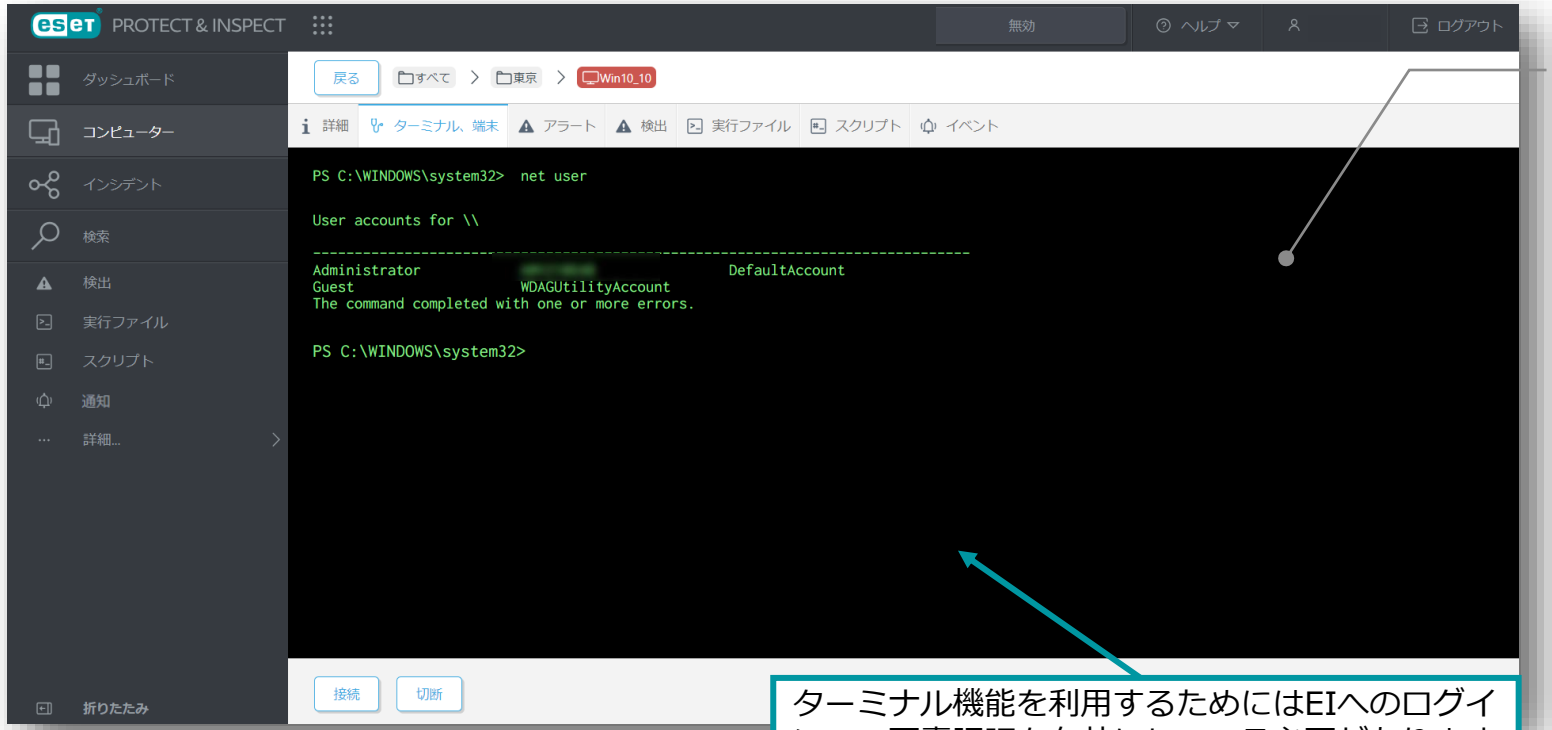


検知されたイベントから除外を作成する場合、対象のルールから各項目の値が抜き出されており、管理者は各項目を有効にするか無効にするか確定するだけで作業を完了できます。
※親プロセス等を対象にする場合は、変更が必要となります。

V. 各機能のご紹介

- **ライブレスポンスについて**

  ターミナル機能を利用することで管理者はエンドユーザーに負担をかけることなくバックグラウンドで調査できます。
  Active DirectoryのポリシーなどでPowerShellの使用が禁止されている環境では利用できないのでご注意ください。



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

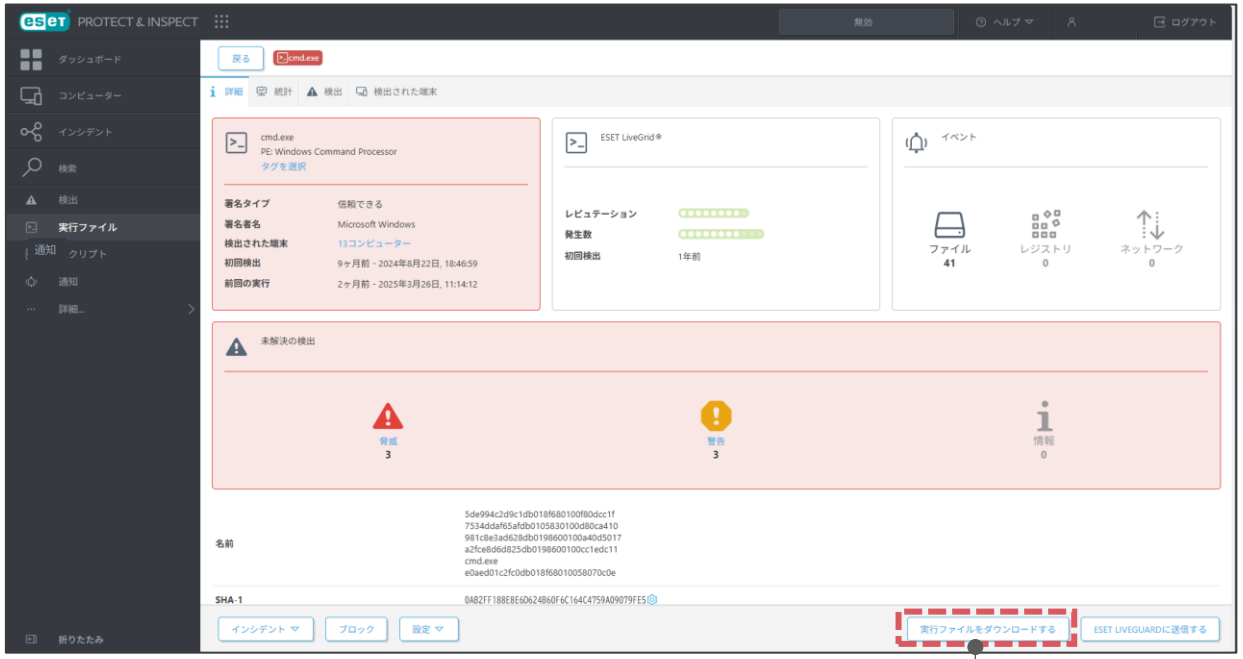
ライブレスポンスとは？

- 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

Ⅴ. 各機能のご紹介

- **ハッシュブロック、プロセスキルについて**

  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

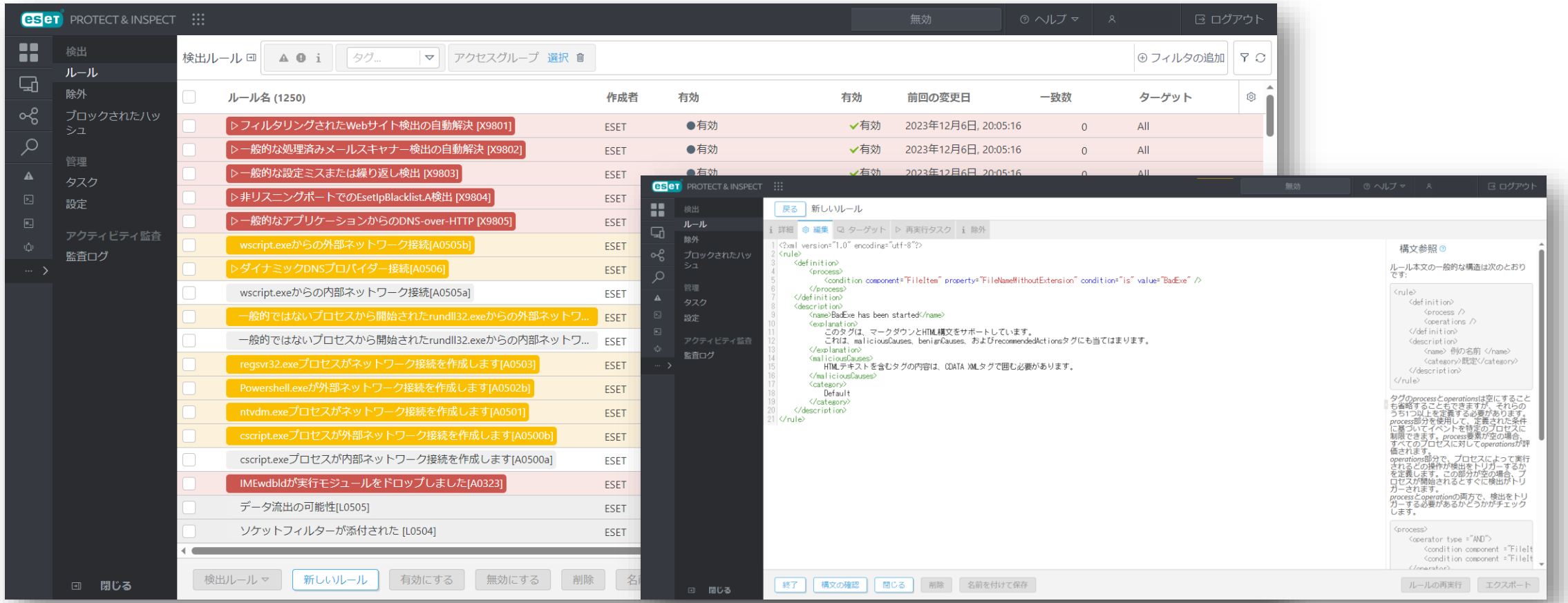
SHA1ハッシュ値を用いて
実行ファイルを即座にブロック

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

V. 各機能のご紹介

- **ルール作成について**

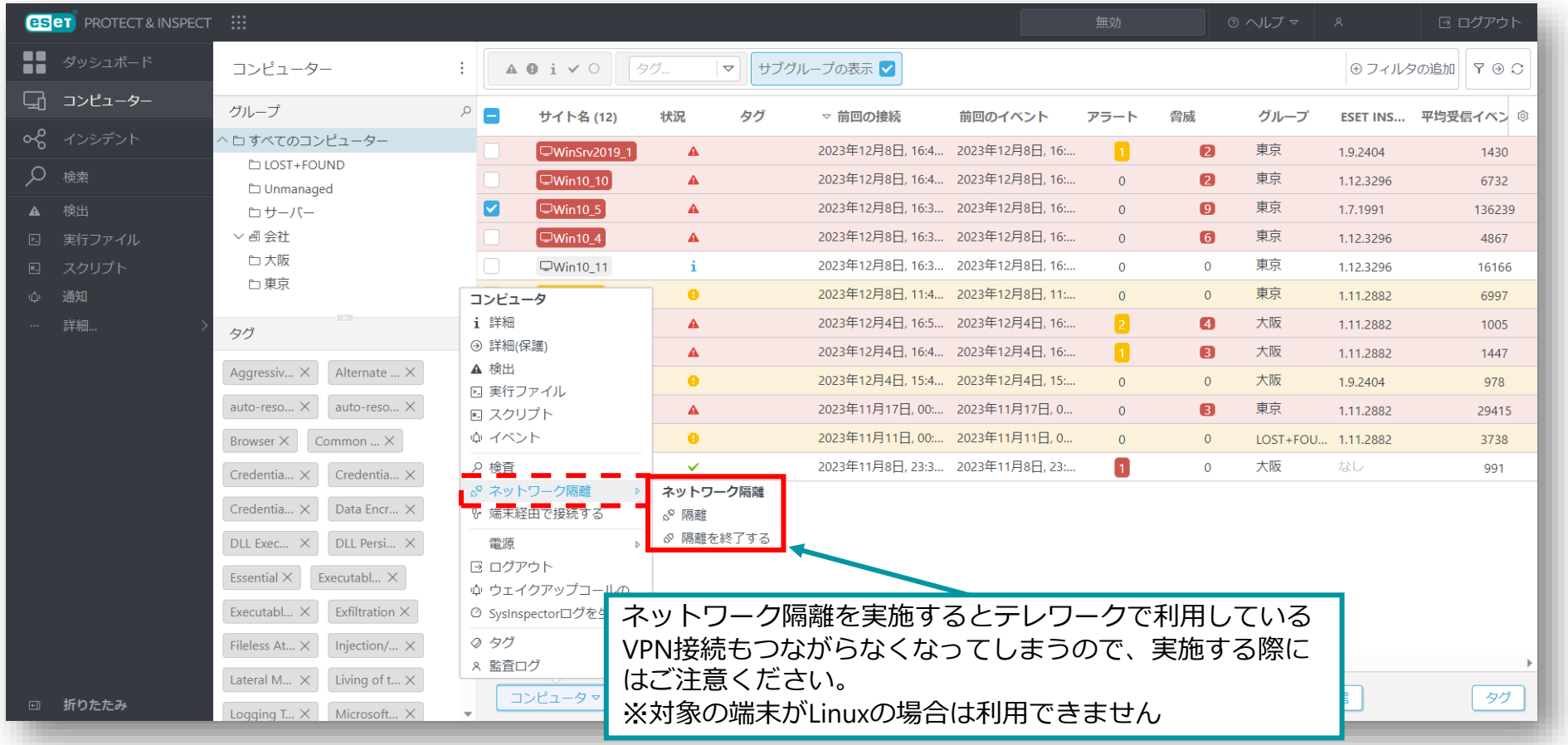
  EIにはデフォルトで1,200以上のルールが存在しますが、お客様環境に合わせてルールを追加することができます。
  ルールはXMLで記載することができ、自由度の高い柔軟なルールを作成することができます。



V. 各機能のご紹介

- **ネットワーク隔離について**

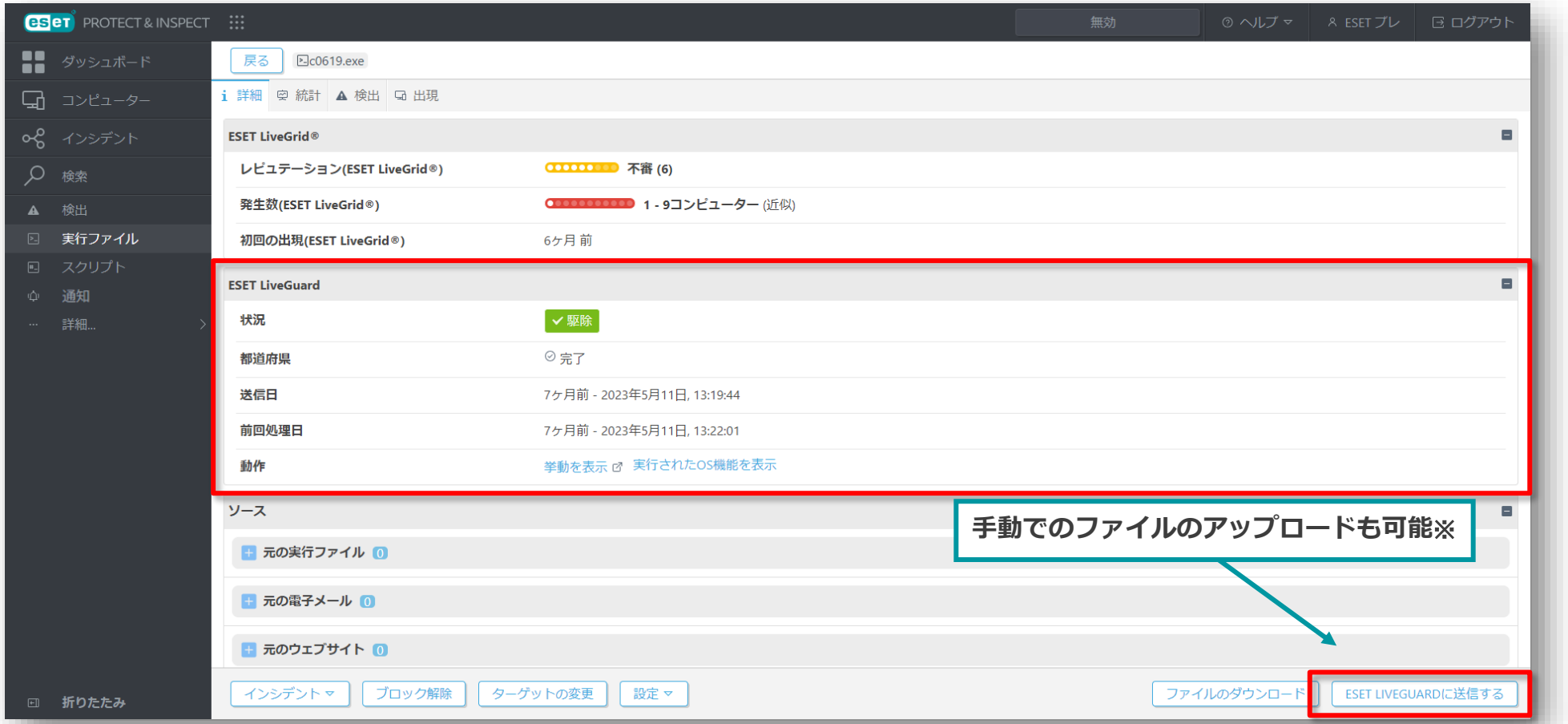
  調査の結果、疑わしい端末を発見した際はネットワークから隔離することができます。完全に隔離するわけではなくESETサーバとの通信は維持されるので継続して調査を行うことができます。



Ⅴ. 各機能のご紹介

- **ESET LiveGuard連携について**

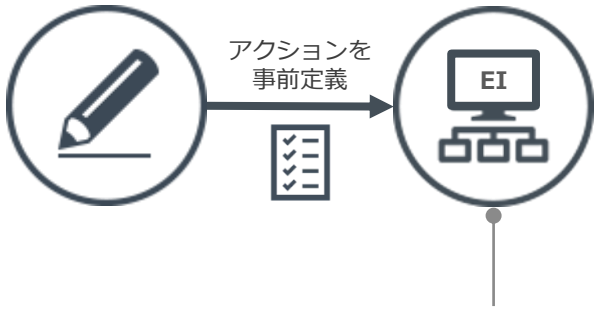
  クラウドサンドボックスであるLiveGuardに手動/自動で送信されたファイルの調査結果が表示されます。
  またXMLのルール内のactionsに記載することで、EIでの検出をトリガーとして実行ファイルをLiveGuardに送信することができます。
  ※実行された端末からファイルを提出するためには、端末側でのLiveGuardのアクティベーションと設定が必要です。



Ⅴ. 各機能のご紹介

- **アクションの自動化について**

  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。
  XDRによって、インシデントの影響が広範囲におよぶと判断された場合には、被害拡大を未然に防ぐために、
  XDRの自動アクション機能で端末全体に対して初動対応(プロセスの停止やDLLの実行ブロック)が行われることがあります。



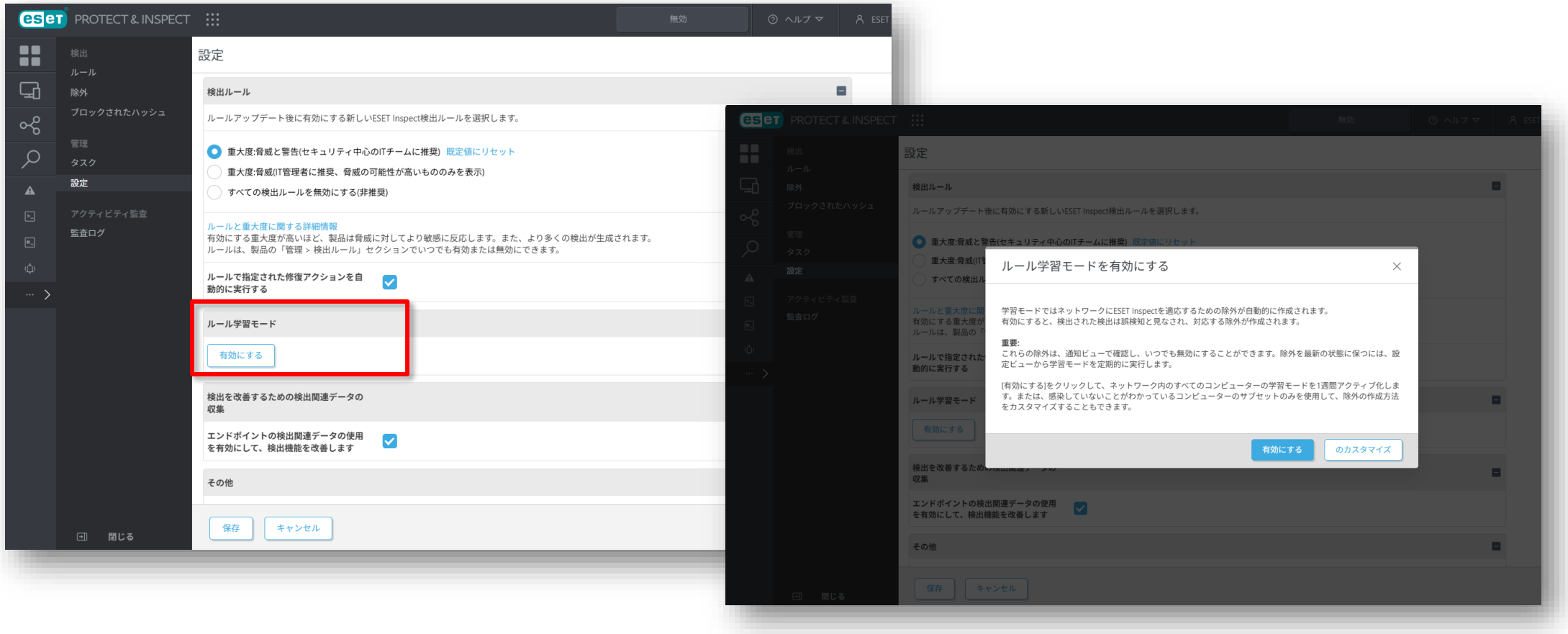
検出アラートがトリガーされたら
ルールに沿ってアクションを自動実行

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

V. 各機能のご紹介

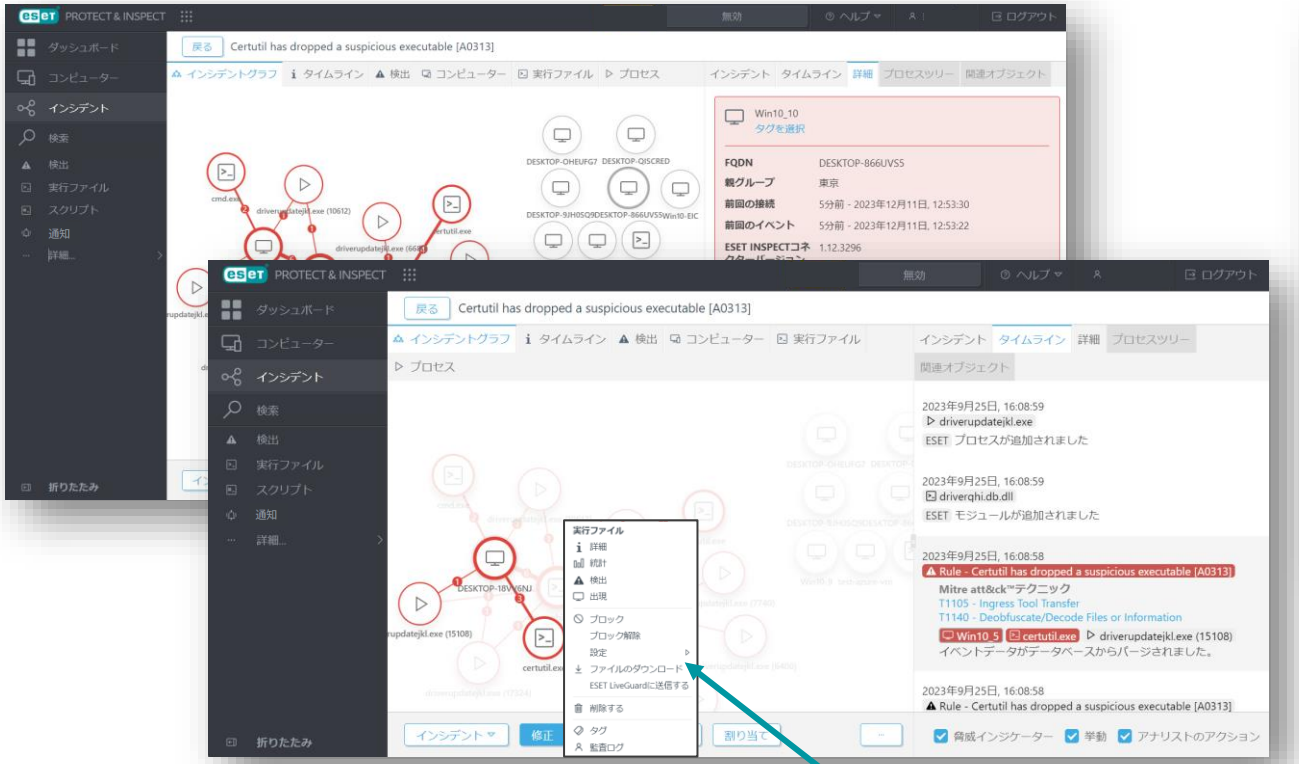
- **自動除外ルール作成機能について**
  「ルール学習モード」を有効にすることで、自動で除外ルールを作成することができるため、チューニング負荷を抑えた運用が可能になります。



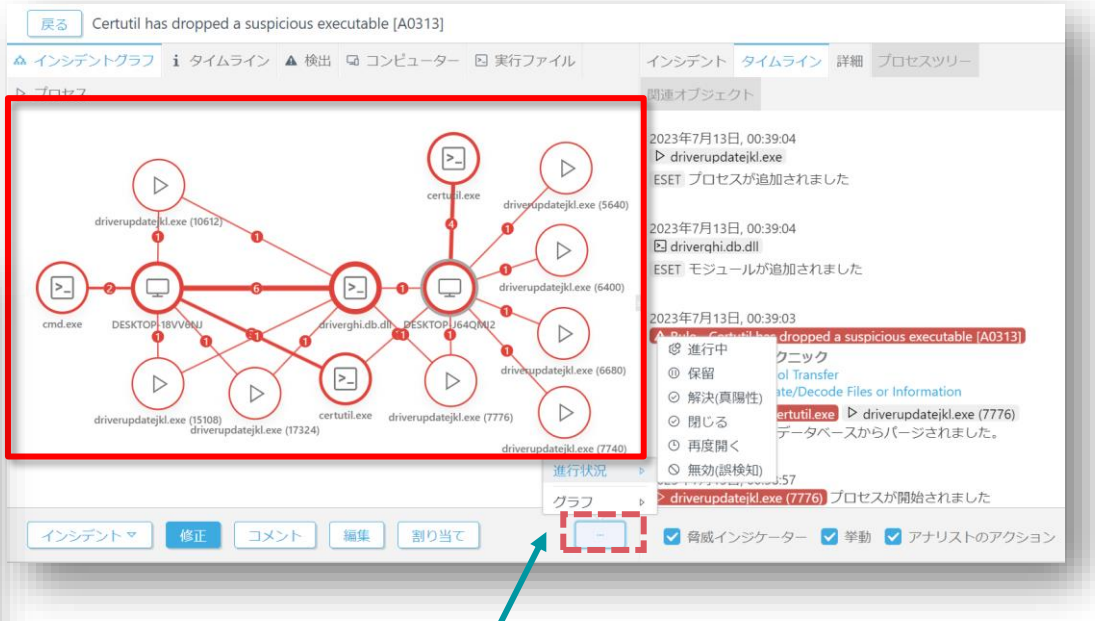
Ⅴ. 各機能のご紹介

- **インシデントグラフについて**

  選択したインシデントの相関グラフを確認でき、右側にはグラフ上で選択したオブジェクトに関連するインシデント、詳細、プロセスツリーを併せて表示できます。タイムラインでは、インシデントの変更に関するタイムスタンプを表示し、選択したイベントをグラフ内で協調表示します。また、任意のノードを移動および再配置することで目的に合ったグラフの作成ができます。



グラフ内の任意のノードを右クリックすると、選択したノードに関連するアクションのドロップダウンメニューを含むコンテキストメニューが開きます。



進行状況：確認中のインシデントの進行状況の変更が可能
グラフ　：移動させたノードのリセット等が可能

Ⅵ. オンプレミス型XDR製品との主な違い

Ⅵ. オンプレミス型XDR製品との主な違い

EIとEI on-premの違い（1）

クラウド型であるESET Inspectとオンプレミス型であるESET Inspect on-premの機能は同等です。違いに関しては以下の表をご確認ください。

	ESET Inspect	ESET Inspect on-prem	備考
ホスト	ESET社が管理するクラウド	お客様によるオンプレミス	
管理可能なデバイス数	25,000クライアントまで	ハードウェアスペック構成次第	
ターミナル接続	有り（2FAが必要）	有り	
API	有り	有り※	※サポート対象外
マルチOS対応	Windows / Linux / Mac	Windows	Windowsはネットワーク隔離可能
データ保存期間	検出：31日 イベント：7日	検出：１週間～3年で設定可能 イベント：1日~3カ月で設定可能	
イベントフィルター※	無し	有り	低レベルのイベントをDBに保存しないかEIに指示する特別なルール
ダッシュボード	サーバステータス：無し Event load：無し	サーバステータス：有り Event load：有り	EIにはインフラリソースに関連する項目は表示されない
接続間隔	7分間隔固定	5分～1440分間隔で設定可能	

Ⅵ. オンプレミス型XDR製品との主な違い

EIとEI on-premの違い（2）

クラウド型であるESET Inspectとオンプレミス型であるESET Inspect on-premの機能は同等です。違いに関しては以下の表をご確認ください。

	ESET Inspect	ESET Inspect on-prem	備考
証明書	設定項目なし（ESET社管理）	ユーザーによる設定・管理	
Agentのローカル展開	不可	可能	
インストーラー	EPでライブインストーラーが作成可能（設定やライセンスは組み込めるが製品プログラムは都度ダウンロード）※	EP on-premで製品のインストーラー込みのオールインワンインストーラーが作成可能	※WindowsのみEndpoint/EM Agent/EI Connector入りのインストーラーを作成可能 Linux/MacにEI Connectorをインストールする場合はEPの「ソフトウェアインストールタスク」を使用
ポリシー	一部作成不可※	すべて設定可能	※接続間隔や接続先設定（接続先IP、ポート、証明書）の設定変更不可