

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

Canon

キヤノンマーケティングジャパン株式会社

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。

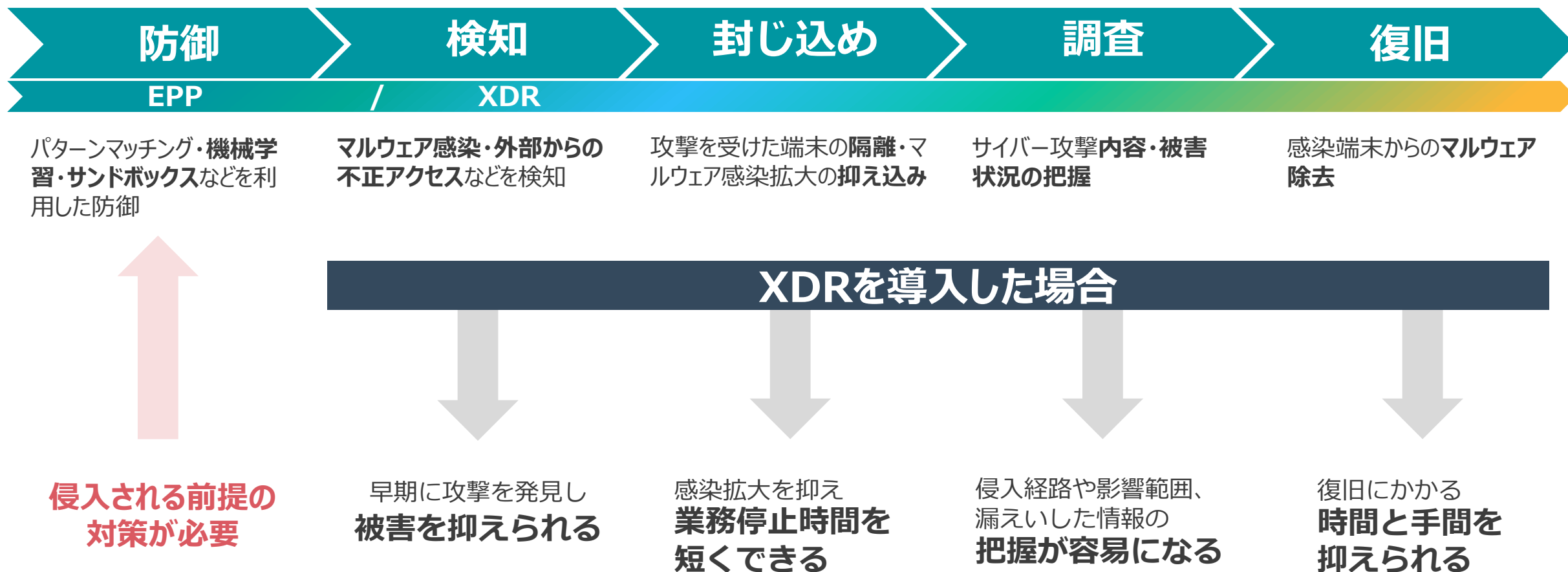
※ 「ESET PROTECT MDR Ultimate」でMDRサービスとプレミアムサポートを受ける場合、クラウドでのセキュリティ管理となります。

- I. ESET Inspectとは
- II. ESET Inspectの構成
- III. ESET Inspectのメリット
- IV. WEBコンソールのご紹介
- V. 各機能のご紹介
- VI. オンプレミス型XDR製品との主な違い

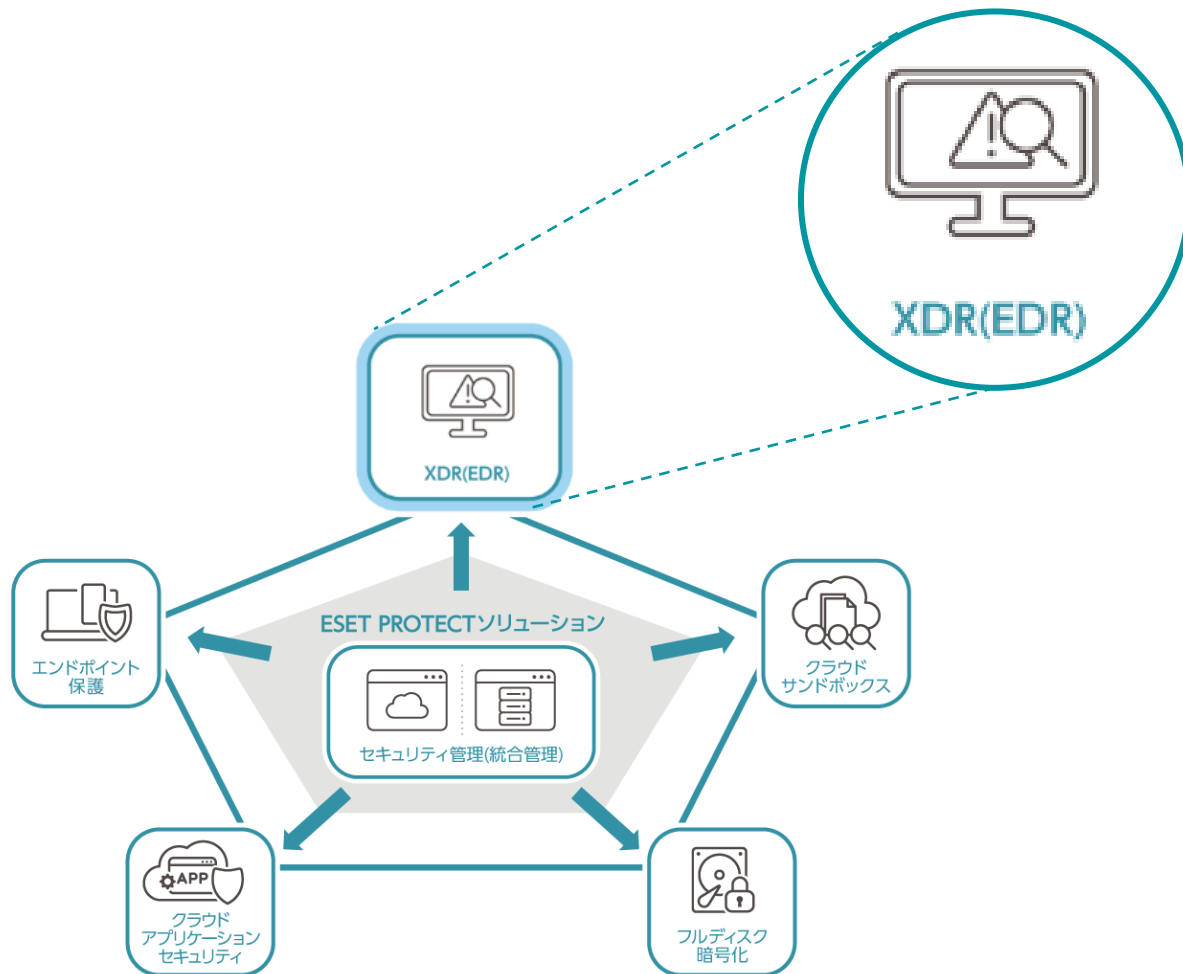
I . ESET Inspectとは

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！



I . ESET Inspectとは

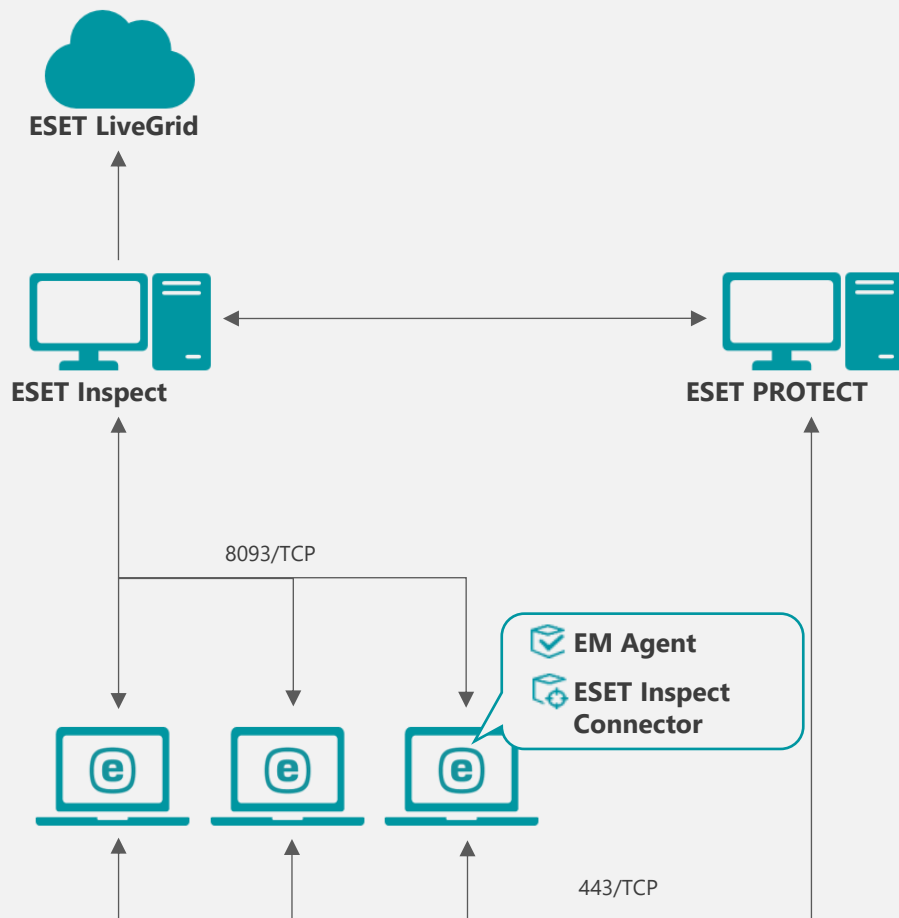


- ESET Inspect（以降、EI）とはクラウド型のXDRコンポーネントです。
- SaaSであるため、利用者によるサーバーのバージョンアップやメンテナンスの必要はありません。
- EIの利用には、クラウド型セキュリティ管理ツールであるESET PROTECT（以降、EP）が利用可能なバンドルライセンスと、ライセンス管理のWebシステムでありEIとEPのポータルとしても使用するESET Business Account（以降、EBA） / ESET PROTECT HUB（以降、EPH）のアカウントが必要です。
- EIを利用するにはEPでのクライアント管理が必須となります。

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)

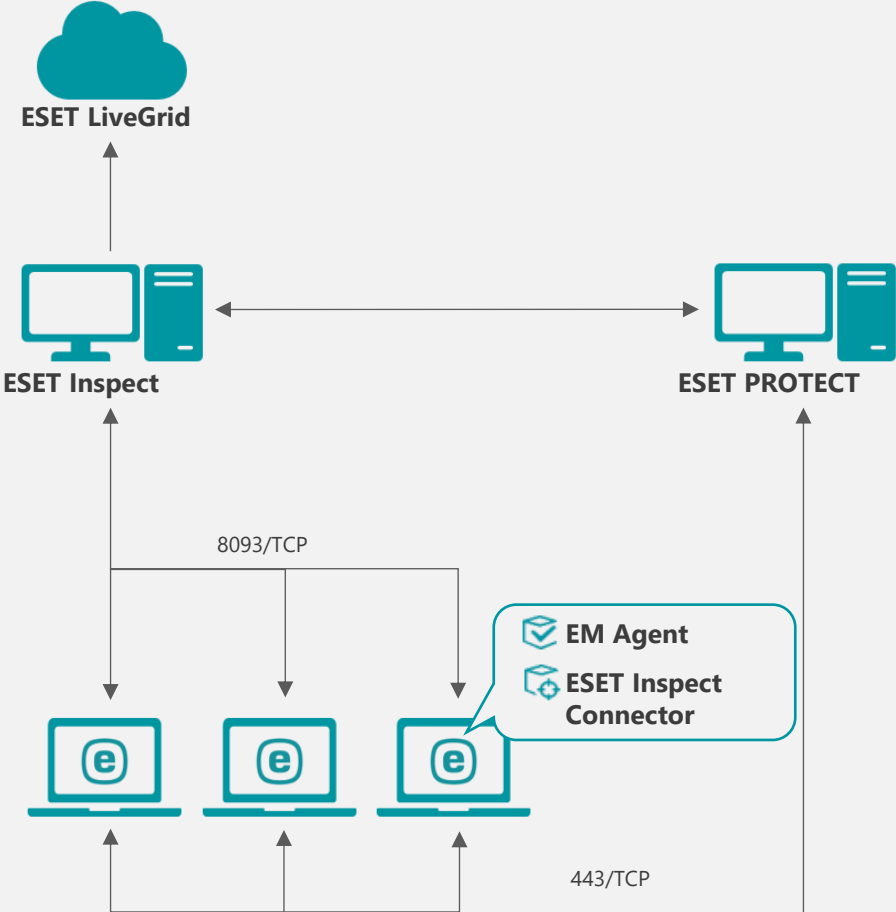
EI Connectorはクライアントのデータを収集し7分間隔でEIへデータを送信します。また、悪意のあるコンポーネントを削除し、これらのコンポーネントの実行をブロックします。

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

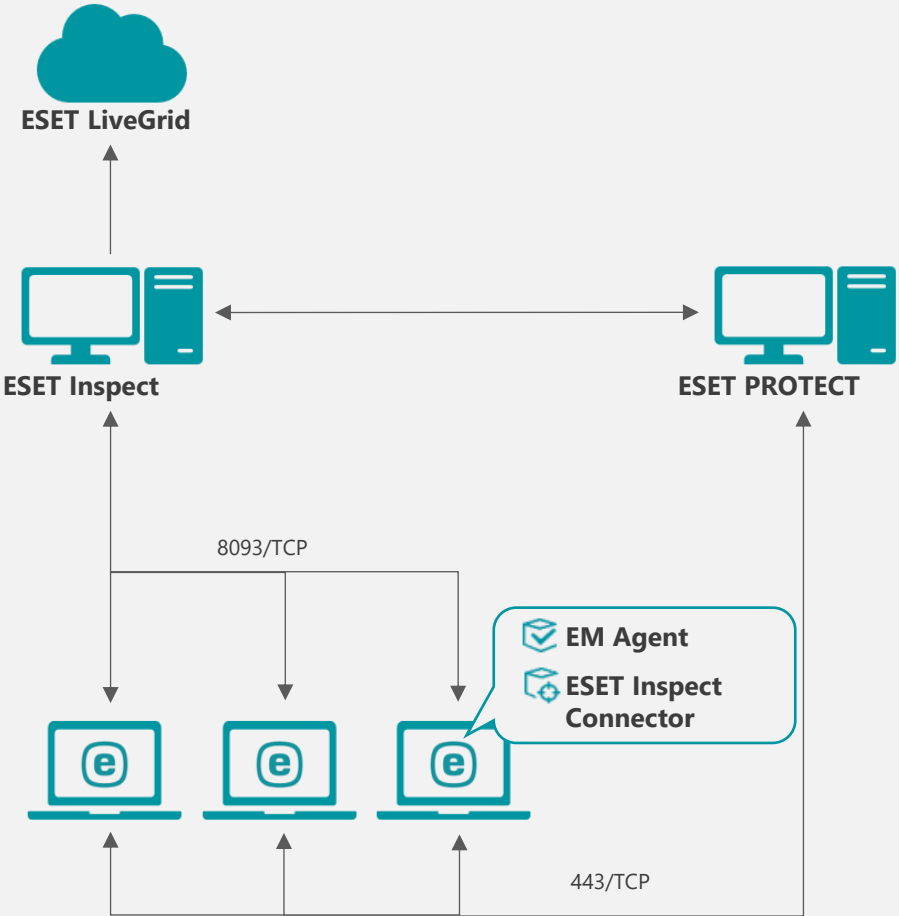
ポート	用途
443/TCP	EM AgentとESET PROTECT間の通信に使用
8093/TCP	ESET Inspect ConnectorとESET Inspect間の通信に使用

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。

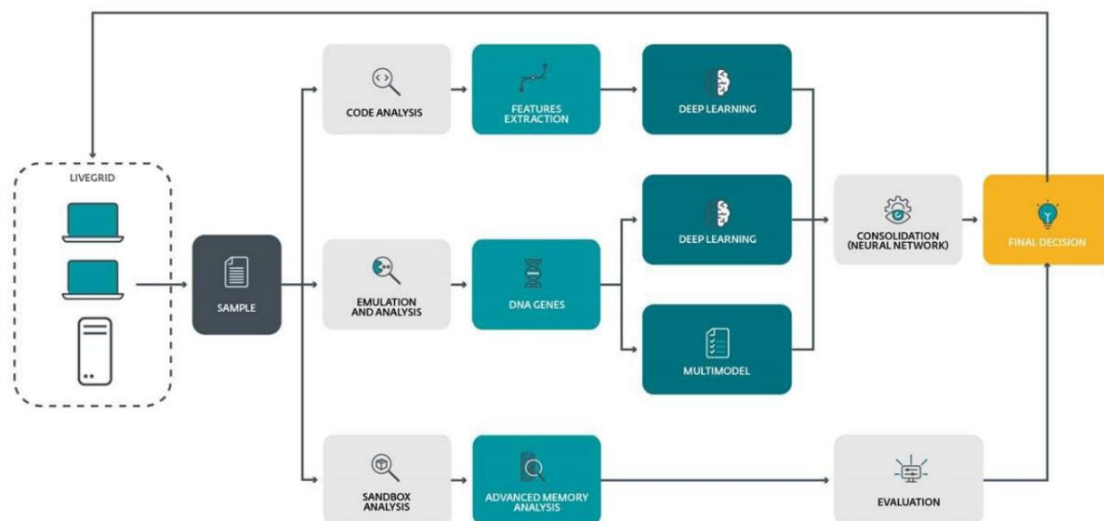


ESET LiveGrid® (Reputation & Feedback)

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。

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

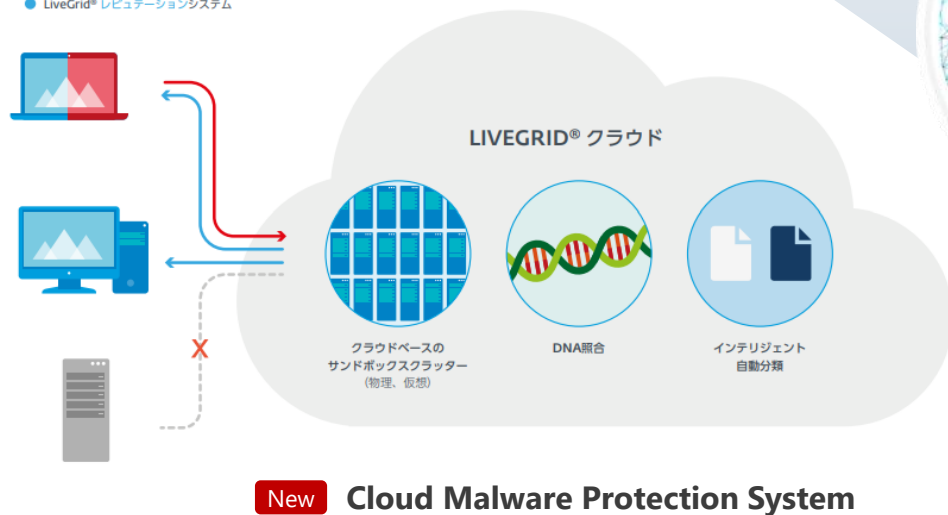
LiveGrid® レピュテーションシステム

- 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

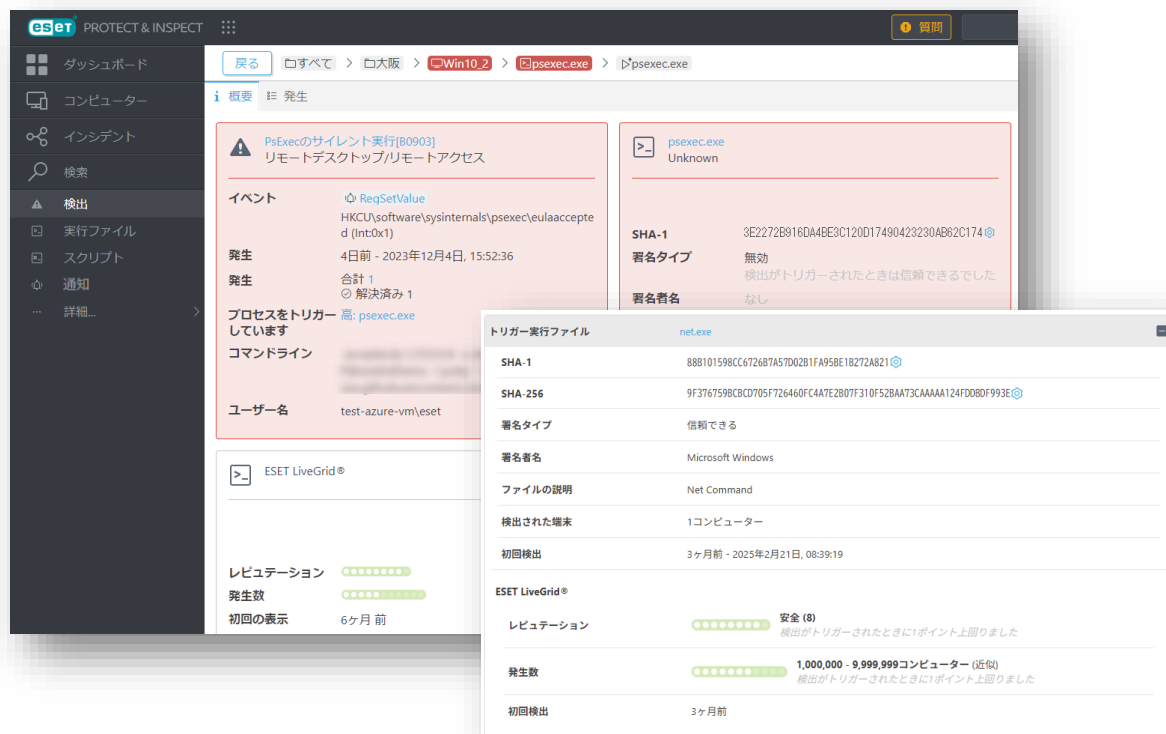
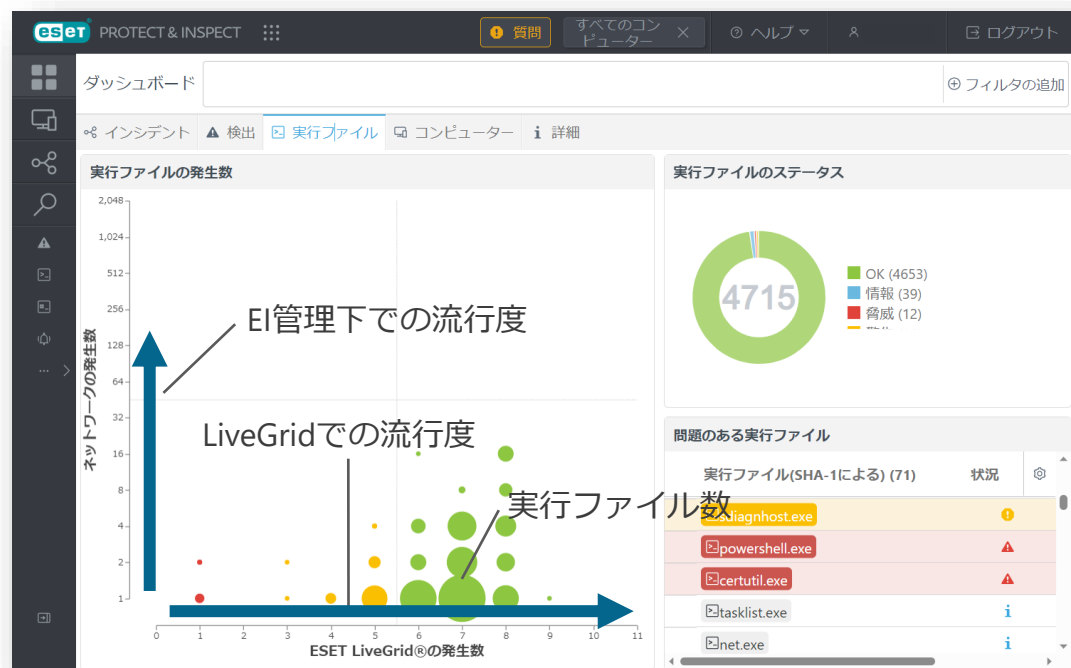
● LiveGrid® フィードバックシステム
● LiveGrid® レピュテーションシステム



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

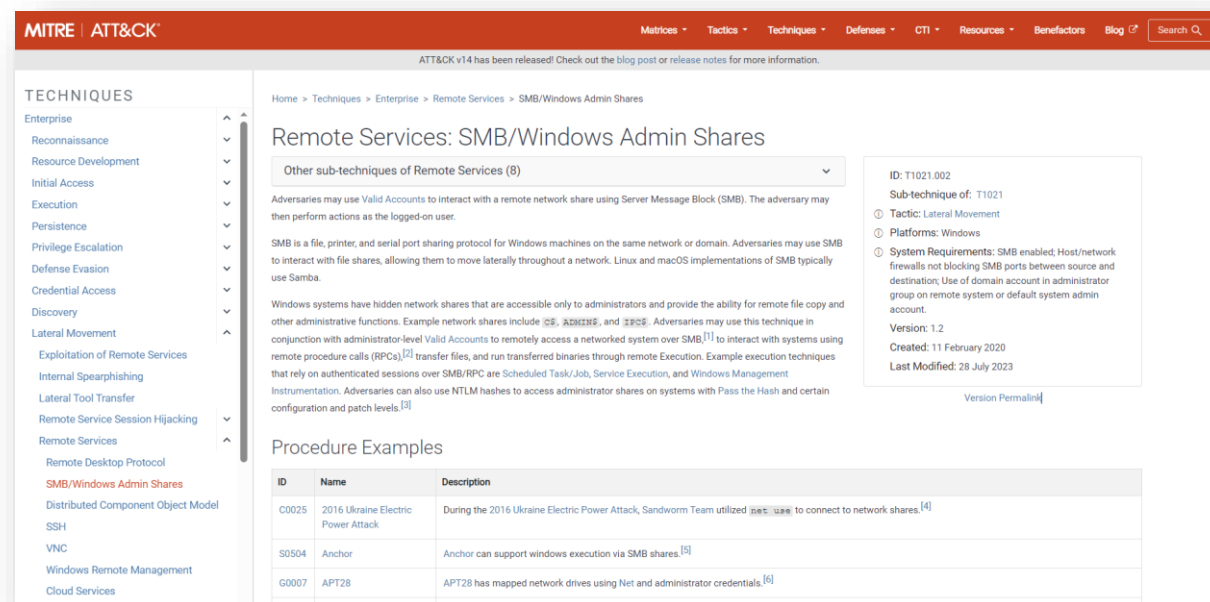
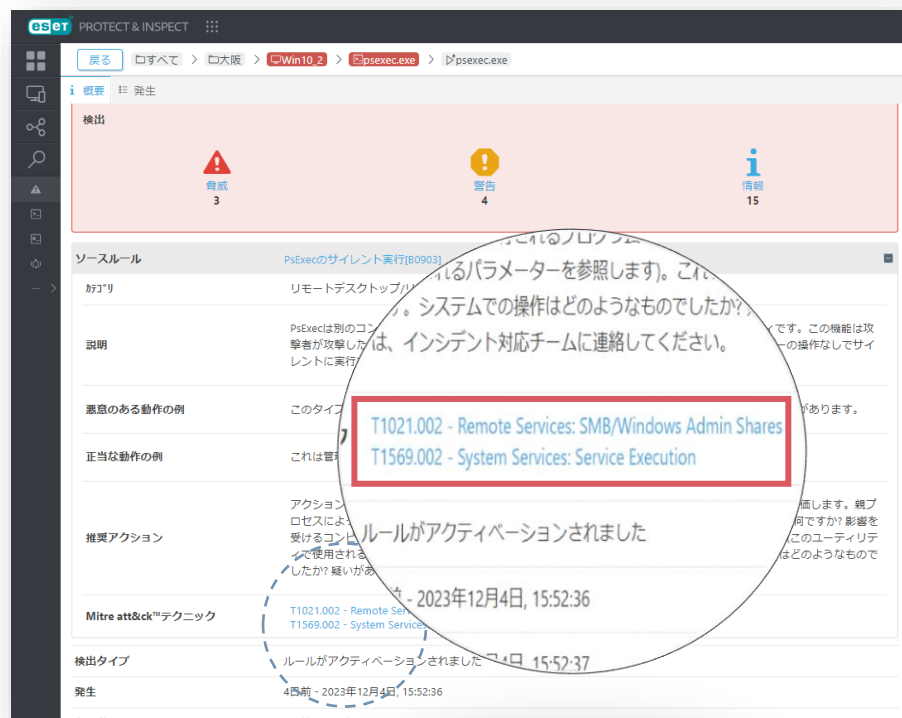
Ⅲ. ESET Inspectのメリット



- **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**

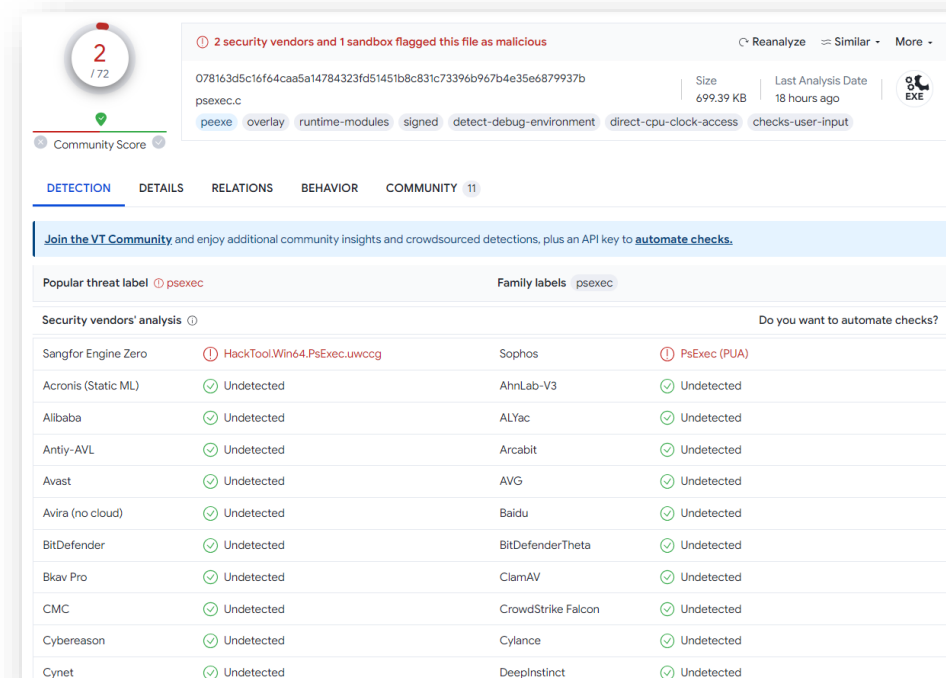
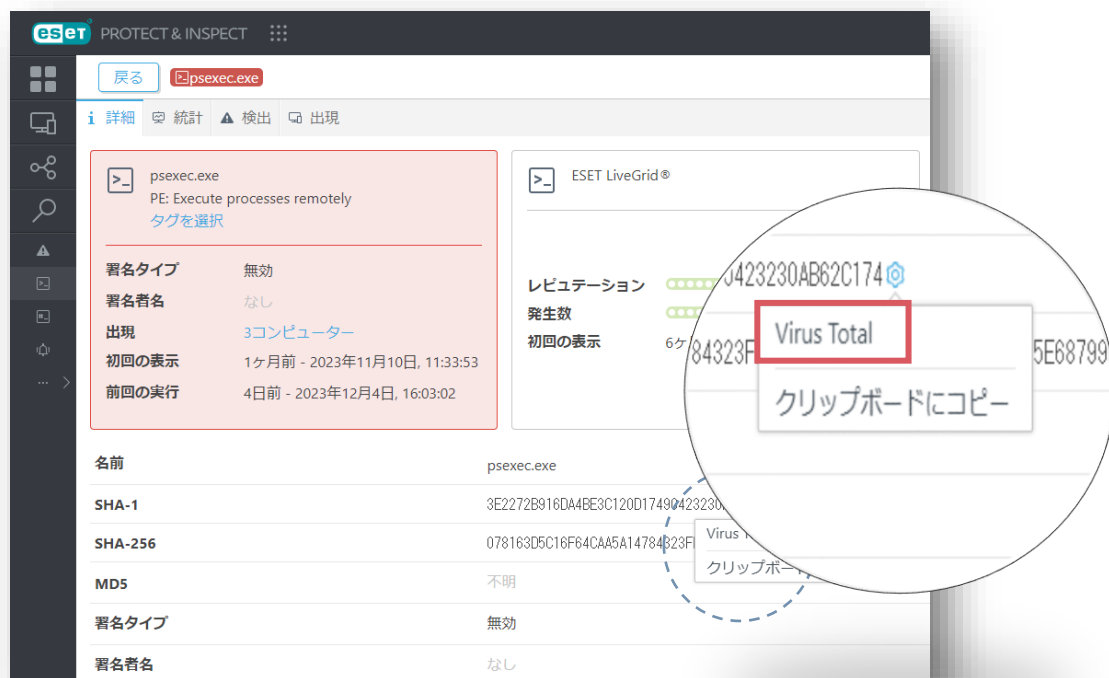
Ⅲ. ESET Inspectのメリット

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



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

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

Log in
Use a single user account for all ESET business cloud solutions

Email

Password

LOG IN [Forgotten password](#)

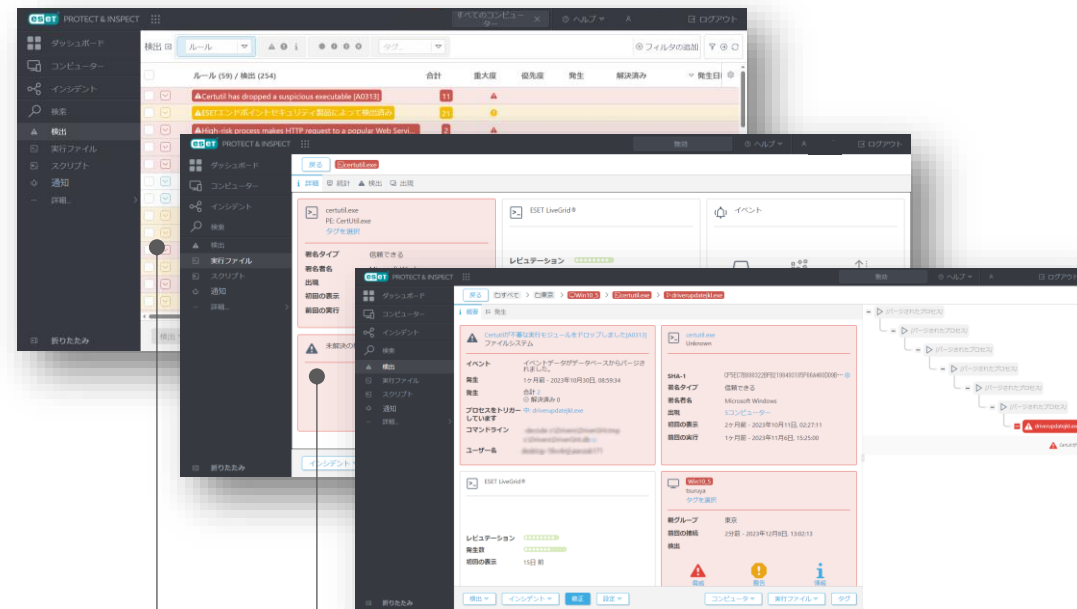
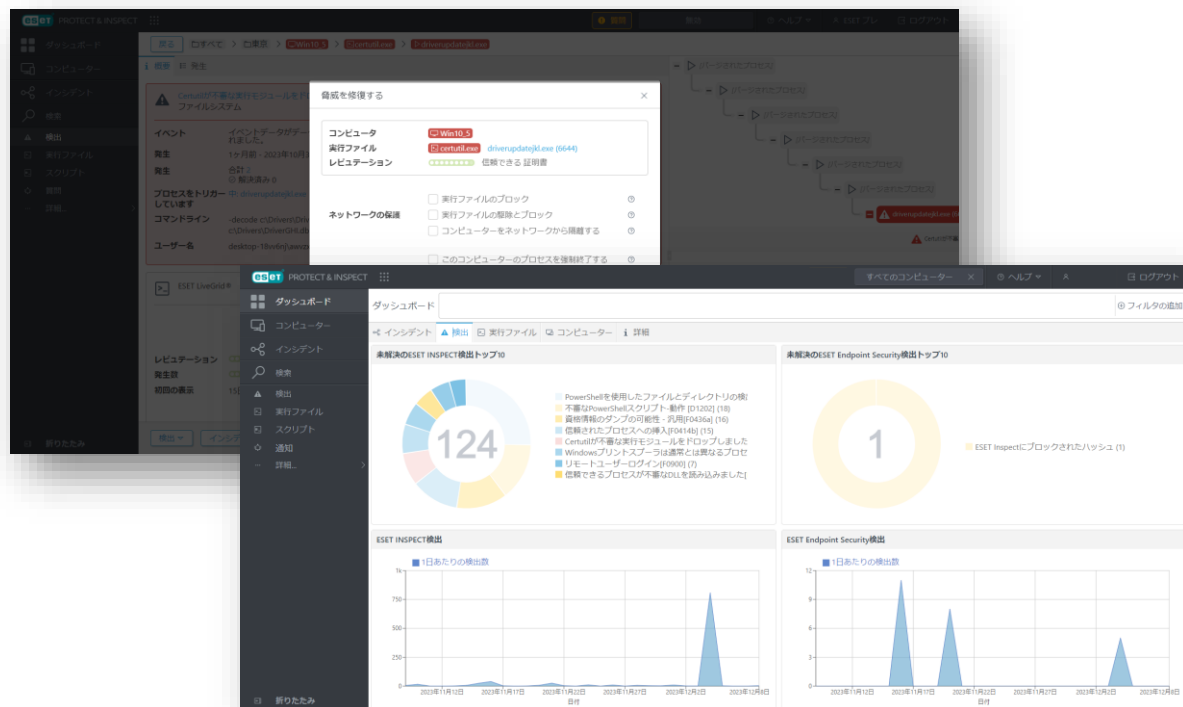
【EIログイン画面】
EI (<https://inspect.eset.com/>) へアクセスし、EI アカウントの電子メールとパスワードを入力してログインします。

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に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の保護を実行できます。

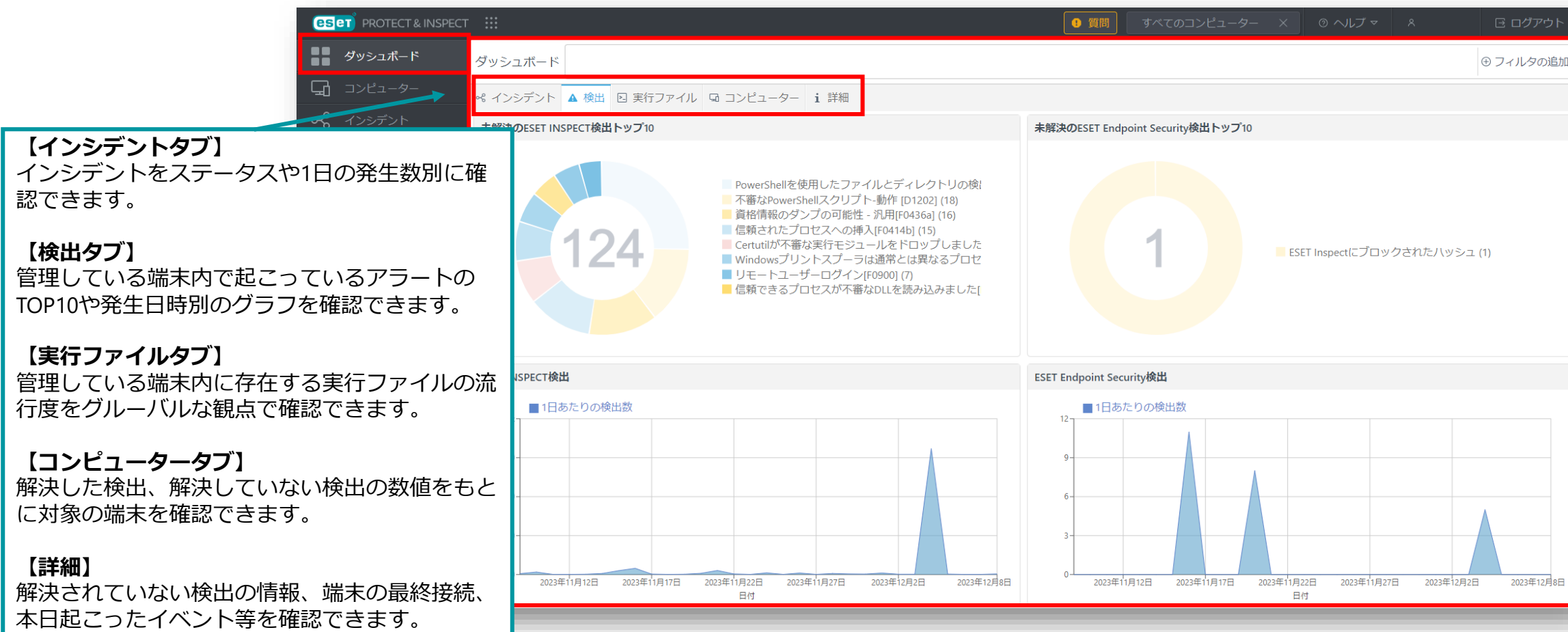


検出アラート一覧画面
実行ファイル詳細画面
プロセス詳細情報画面

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。E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。



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。

サイト名 (12)	状況	タグ	前回の接続	前回のイベント	アラート	脅威	情報
WinSrv2019_1	△		2023年12月8日, 13:3...	2023年12月8日, 13:...	1	2	東京
Win10_10	△		2023年12月8日, 13:3...	2023年12月8日, 13:...	0	2	東京
Win10_5	△		2023年12月8日, 13:3...	2023年12月8日, 13:...	0	9	東京
Win10_4	△		2023年12月8日, 13:2...	2023年12月8日, 13:...	0	7	東京
-test-v	i						
Win10_9	!						
Win10_1	△						
Win10_2	△						
Win10_7	!						
Win10_6	△						
Win10_8	!						
Win10_3	✓						

Win10_4 詳細

Win10_4
User4
タグを選択

FQDN: DESKTOP-J64QM12
親グループ: /すべて/東京
前回の接続: 6分前 - 2023年12月8日, 13:31:58
前回のイベント: 17分前 - 2023年12月8日, 13:20:58
ESET INSPECTコネクタバージョン: 1.12.3296
OS名: Microsoft Windows 10 Enterprise
OSバージョン: 10.0.19045.3693

グループ: /すべて/東京
ネットワークから隔離済み: 隔離されていない
前回の接続: 6分前 - 2023年12月8日, 13:31:58
前回のイベント: 17分前 - 2023年12月8日, 13:20:58
今日以降に受信したイベント: 476
今日以降に保存されたイベント: 476

未解決の検出

脅威 7
警告 6
情報 14

コンピュータ インシデント 検査 ネットワーク隔離 電源 ログアウト ウェイクアップコールの送信 SYSINSPECTORログを生成する

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。

The screenshot displays the ESET Protect & Inspect web console interface. On the left, a sidebar menu includes options like 'ダッシュボード' (Dashboard), 'コンピュータ' (Computer), 'インシデント' (Incidents), '検出' (Detections), '実行ファイル' (Executable Files), 'スクリプト' (Scripts), '通知' (Notifications), and '詳細...' (Details...). The main area shows a list of detection rules under the '検出' (Detections) tab. The list includes rules such as 'Certutil has dropped a suspicious executable [A0313]', 'ESETエンドポイントセキュリティ製品によって検出済み' (Detected by ESET endpoint security product), 'High-risk process makes HTTP request to a popular Web Service [E0503]', and 'Invoke-WCMDump cmdlet [A1116]'. A red arrow points from a text box to the 'Invoke-WCMDump cmdlet [A1116]' rule. Below the list, there are buttons for '検出' (Detections), 'インシデント' (Incidents), '解決済みに設定' (Set to resolved), '未解決に設定' (Set to unresolved), and '除外の作成' (Create exclusion). On the right, a detailed view of the 'Invoke-WCMDump cmdlet [A1116]' event is shown, including event details, process information, and a process tree diagram. The process tree shows the execution flow from 'powershell.exe' to 'explorer.exe' and 'conhost.exe'. A red arrow points from the 'powershell.exe' process in the tree to the 'Invoke-WCMDump cmdlet [A1116]' rule in the list.

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。

「基本検索」と「高度なイベント検索」の2種類があり「基本検索」では検索したい項目を選択することができます。「高度なイベント検索」ではXMLでルール記述するので自由度の高い検索ルールをつくることができます。

検索タスク

基本検索 高度なイベント検索

検出 × を含む イベント × 場所 引数 含む ×

タグ...

サイト名 (9)

イベント with Argument "-telnet raw.githubusercontent.com"

イベント Advanced query 3

イベント with Argument "arc-test"

検索タスク

基本検索 高度なイベント検索

ディスプレイ

次の式に一致するイベントを検索します:

```
<definition>
  <operations>
    <operation type="WriteFile">
      <operator type="OR">
        <condition component="FileItem" condition="is" property="FullPath" value="%SYSTEM%\WinAppXRT.dll" />
        <condition component="FileItem" condition="is" property="FullPath" value="%WINDIR%\SysWow64\WinAppXRT.dll" />
      </operator>
    </operation>
  </operations>
</definition>
```

作成済み	状況	進行状況	結果
2023年12月7日, 11:42:01	完了	2 Events	
2023年12月4日, 15:21:39	完了	0 Events	
2023年12月4日, 15:17:45	完了	0 Events	

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。

The screenshot displays the ESET Protect & Inspect web interface. On the left is a sidebar with navigation options: ダッシュボード, コンピューター, インシデント, 検出, 実行ファイル, スクリプト, 通知, and 詳細... The main area shows a list of incidents under the 'インシデント' tab. A callout box with a blue border and arrow points to the 'インシデント' link in the left sidebar, containing the text: 「インシデントに関連した情報からドリルダウンすることで、右画面に端末や実行ファイルの詳細などを表示させながら確認することができます。」 The right pane shows the details of an incident titled 'Certutil has dropped a suspicious executable [A0313]'. It includes a timeline of events, a list of related processes (e.g., DESKTOP-18VV6NJ, ESET コンピューターが追加されました), and a list of related objects (e.g., Win10_5, certutil.exe, driverupdatejkl.exe (6644)). At the bottom right, there is a section for '脅威インジケーター (13)' with a rule entry: 「Certutilが不審な実行モジュールをドロップしました [A0313]」.

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。

各ファイルに対してESET LiveGridで確認された情報（流行度、評価、初めて確認された日等）も確認できるので不審なファイルを確認しやすい作りになっています。

サイト名 (8266)	状況	コンピューター上で実行	レピュテーション(E...	発生数(ESET LIVEGRID...	初回の出現(ESET LI
doesitcache.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
dulwich.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
jsonschema.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
keyring.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
normalizer.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
pip.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
pkginfo.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
pyproject-build.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
virtualenv.exe	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..
windowsbase.ni.dll	✓	0	●●●●●●●●	●●●●●●●●	ESET LiveGrid®に表示さ..

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。

eset PROTECT & INSPECT

すべてのコンピューター ター × ヘルプ ログアウト

ダッシュボード
コンピューター
インシデント
検索
検出
実行ファイル
スクリプト
通知
詳細...

スクリプト グループ化解除 警告 情報 設定 タグ... コマンドライン = フィルタの追加

プロセス名(ID) (345)	状況	安全	コマンドライン
powershell.exe (7780)	✓		-ExecutionPolicy Restricted -Command \$Res = 0; \$Infs = Get-Item -Path (\$env:WinDir +
powershell.exe (2444)	✓		-ExecutionPolicy Restricted -Command Write-Host 'Final result: 1';
powershell.exe (7780)	✓		-ExecutionPolicy Restricted -Command \$Res = 0; \$Infs = Get-Item -Path (\$env:WinDir +
powershell.exe (2444)	✓		-ExecutionPolicy Restricted -Command Write-Host 'Final result: 1';
powershell.exe (7780)	✓		-ExecutionPolicy Restricted -Command \$Res = 0; \$Infs = Get-Item -Path (\$env:WinDir +
powershell.exe (2444)	✓		-ExecutionPolicy Restricted -Command Write-Host 'Final result: 1';
powershell.exe (7780)	✓		-ExecutionPolicy Restricted -Command \$Res = 0; \$Infs = Get-Item -Path (\$env:WinDir +
powershell.exe (2444)	✓		-ExecutionPolicy Restricted -Command Write-Host 'Final result: 1';
powershell.exe (7780)	✓		-ExecutionPolicy Restricted -Command \$Res = 0; \$Infs = Get-Item -Path (\$env:WinDir +
powershell.exe (2444)	✓		-ExecutionPolicy Restricted -Command Write-Host 'Final result: 1';
powershell.exe (6000)	✓		-ExecutionPolicy Restricted -Command Write-Host 'Final result: 1';

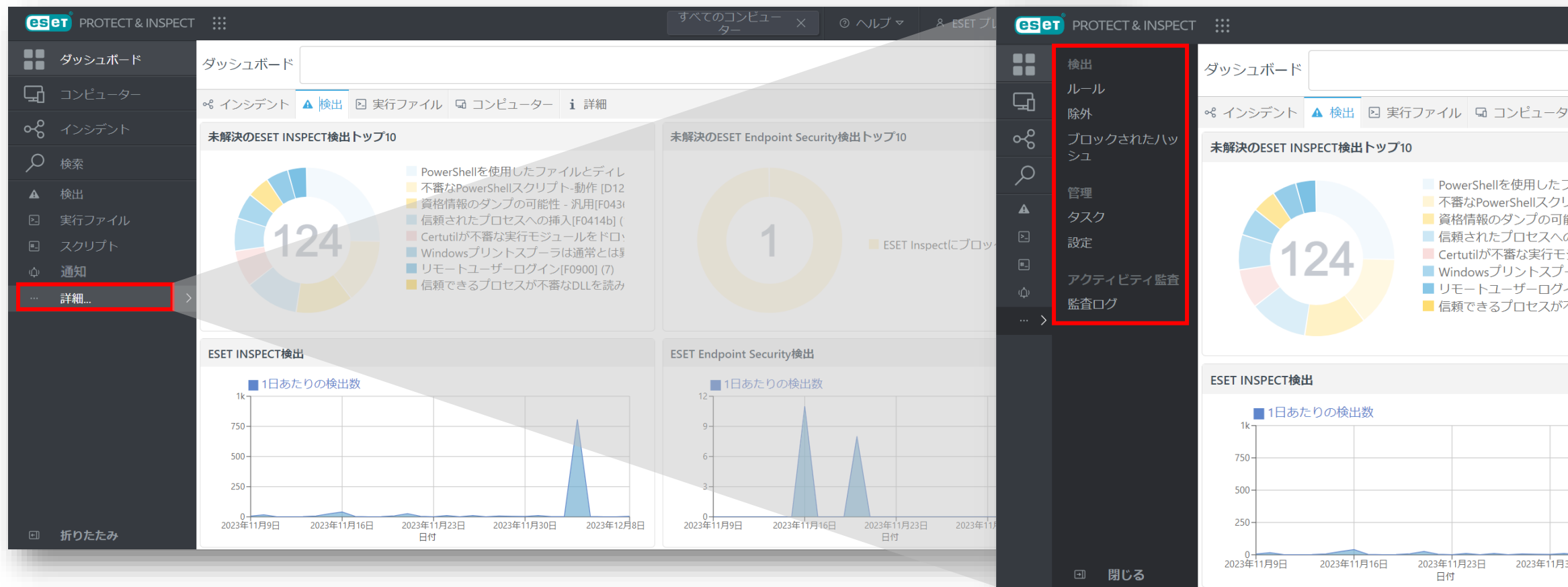
実行されたコマンドラインの内容も確認することができます。

折りたたみ スクリプト 設定 タグ 除外の作成 スクリプトのダウンロード

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

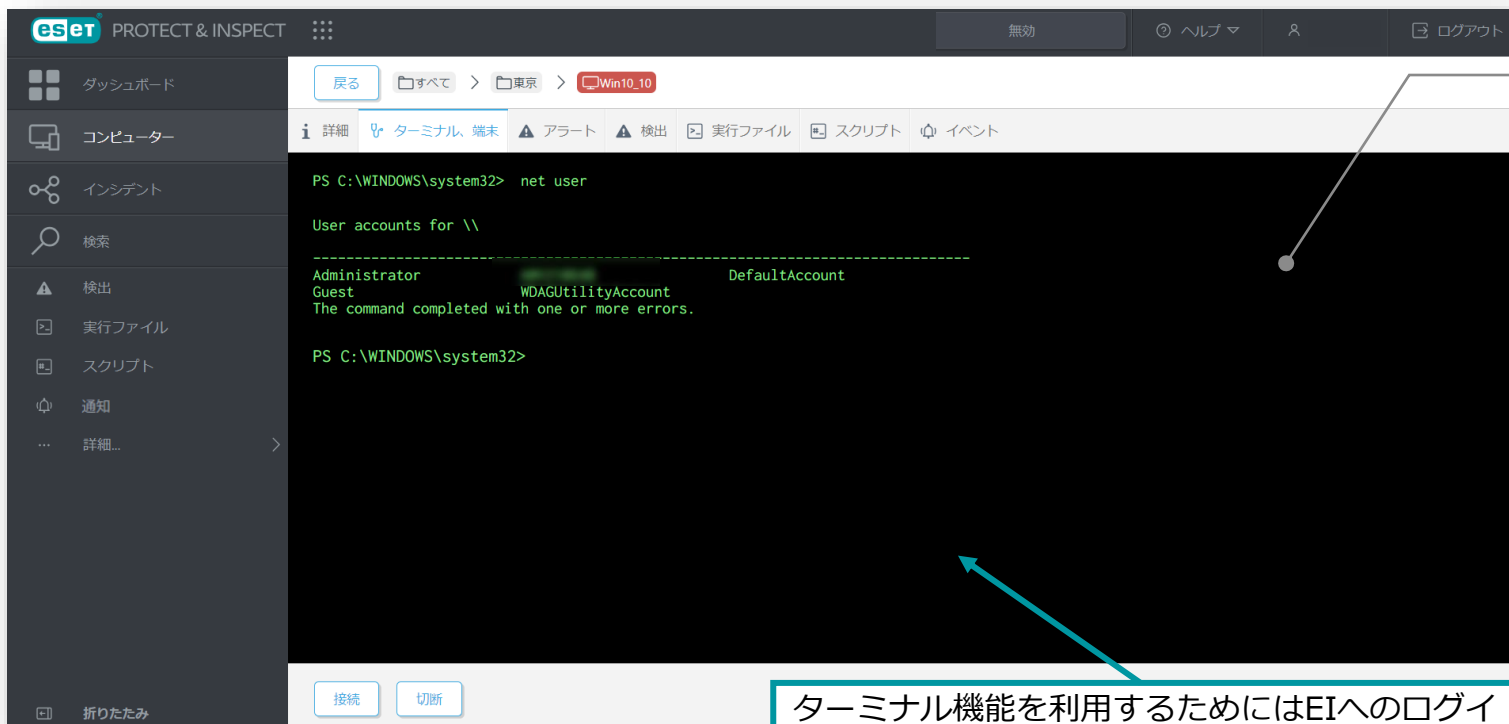
除外は各ルールからある一定の条件を満たした検出を除外することができる機能です。除外には2種類の方法があり、プリセットされた項目を利用する方法とXMLで記述する自由度の高い詳細エディターがあります。

検出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

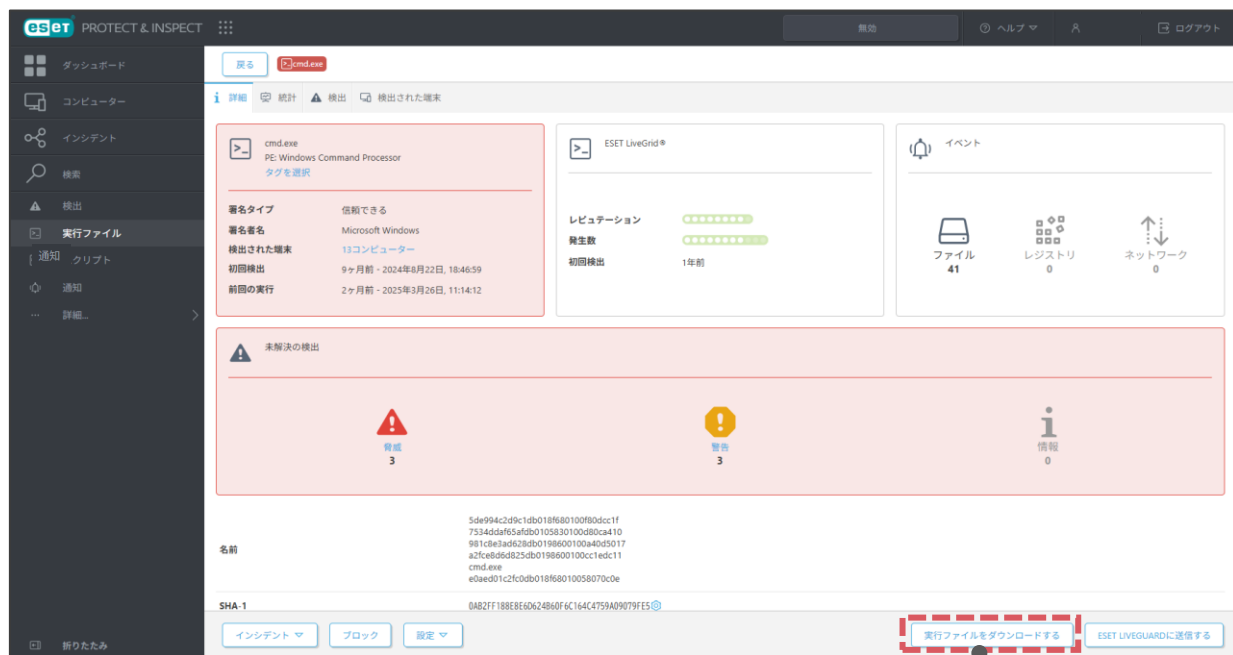
ライブレスポンスとは？

- 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。

The screenshot displays the ESET Protect & Inspect web interface. On the left, a sidebar contains navigation icons for '検出' (Detection), 'ルール' (Rules), '除外' (Exclusions), 'ブロックされたハッシュ' (Blocked hashes), '管理' (Management), 'タスク' (Tasks), '設定' (Settings), 'アクティビティ監査' (Activity audit), and '監査ログ' (Audit log). The main area is titled '検出ルール' (Detection rules) and shows a table of 1250 rules. The table columns are: 'ルール名' (Rule name), '作成者' (Author), '有効' (Enabled), '有効' (Valid), '前回の变更日期' (Last update date), '一致数' (Match count), and 'ターゲット' (Target). The rules are listed with their names, authors (mostly ESET), and status (有効/有効). Below the table, there are buttons for '検出ルール' (Detection rules), '新しいルール' (New rule), '有効にする' (Enable), '無効にする' (Disable), '削除' (Delete), and '名前' (Name). An inset window shows the '新しいルール' (New rule) creation process. It includes a '戻る' (Back) button, a '新しいルール' (New rule) title, and a '戻る' (Back) button. The main content area shows the XML definition of a rule, with a '戻る' (Back) button and a '終了' (End) button. The XML is a rule definition for detecting malicious files. The right sidebar contains a '構文参照' (Syntax reference) section, which provides a detailed explanation of the XML syntax used in the rule definition, including the structure of the rule, definition, process, condition, and operation elements.

ルール名 (1250)	作成者	有効	有効	前回の变更日期	一致数	ターゲット
フィルタリングされたWebサイト検出の自動解決 [X9801]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
一般的な処理済みメーラ検出の自動解決 [X9802]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
一般的な設定ミスまたは繰り返し検出 [X9803]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
非リスニングポートでのEsetpBlacklist.A検出 [X9804]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
一般的なアプリケーションからのDNS-over-HTTP [X9805]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
wscript.exeからの外部ネットワーク接続[A0505b]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
動的DNSプロバイダ接続[A0506]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
wscript.exeからの内部ネットワーク接続[A0505a]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
一般的ではないプロセスから開始されたrundll32.exeからの外部ネットワ...	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
一般的ではないプロセスから開始されたrundll32.exeからの内部ネットワ...	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
regsvr32.exeプロセスがネットワーク接続を作成します[A0503]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
Powershell.exeが外部ネットワーク接続を作成します[A0502b]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
ntvdm.exeプロセスがネットワーク接続を作成します[A0501]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
cscript.exeプロセスが外部ネットワーク接続を作成します[A0500b]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
cscript.exeプロセスが内部ネットワーク接続を作成します[A0500a]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
IMEWdbldが実行モジュールをドロップしました[A0323]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
データ流出の可能性[L0505]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All
ソケットフィルタが添付された [L0504]	ESET	有効	有効	2023年12月6日, 20:05:16	0	All

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。

The screenshot shows the ESET Protect & Inspect interface. On the left, the 'Computer' section is selected. The main area displays a table of devices. The 'Win10_5' device is highlighted, and a context menu is open over it. The 'Network Isolation' option is selected in the menu. A callout box points to this option with the following text:

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。
※対象の端末がLinuxの場合は利用できません

サイト名 (12)	状況	タグ	前回の接続	前回のイベント	アラート	脅威	グループ	ESET INS...	平均受信イベン
WinSrv2019_1	▲		2023年12月8日, 16:4...	2023年12月8日, 16:...	1	2	東京	1.9.2404	1430
Win10_10	▲		2023年12月8日, 16:4...	2023年12月8日, 16:...	0	2	東京	1.12.3296	6732
Win10_5	▲		2023年12月8日, 16:3...	2023年12月8日, 16:...	0	9	東京	1.7.1991	136239
Win10_4	▲		2023年12月8日, 16:3...	2023年12月8日, 16:...	0	6	東京	1.12.3296	4867
Win10_11	i		2023年12月8日, 16:3...	2023年12月8日, 16:...	0	0	東京	1.12.3296	16166
	i		2023年12月8日, 11:4...	2023年12月8日, 11:...	0	0	東京	1.11.2882	6997
	▲		2023年12月4日, 16:5...	2023年12月4日, 16:...	2	4	大阪	1.11.2882	1005
	▲		2023年12月4日, 16:4...	2023年12月4日, 16:...	1	3	大阪	1.11.2882	1447
	i		2023年12月4日, 15:4...	2023年12月4日, 15:...	0	0	大阪	1.9.2404	978
	▲		2023年11月17日, 00:...	2023年11月17日, 0:...	0	3	東京	1.11.2882	29415
	i		2023年11月11日, 00:...	2023年11月11日, 0:...	0	0	LOST+FOU...	1.11.2882	3738
	✓		2023年11月8日, 23:3...	2023年11月8日, 23:...	1	0	大阪	なし	991

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。

The screenshot displays the ESET Protect & Inspect web interface. The left sidebar contains navigation links: ダッシュボード, コンピューター, インシデント, 検索, 検出, 実行ファイル, スクリプト, 通知, and 詳細... The main content area shows the details for a file named 'c0619.exe'. It includes tabs for 詳細, 統計, 検出, and 出現. The 'ESET LiveGrid®' section shows a 'レビュー' (Review) status of '不審 (6)' (Suspicious (6)). The 'ESET LiveGuard' section is highlighted with a red box and contains the following information:

ESET LiveGuard	
状況	✓ 駆除
都道府県	完了
送信日	7ヶ月前 - 2023年5月11日, 13:19:44
前回処理日	7ヶ月前 - 2023年5月11日, 13:22:01
動作	挙動を表示 実行されたOS機能を表示

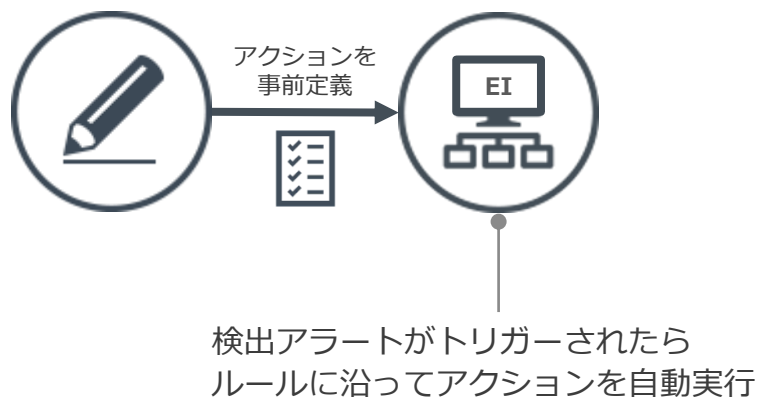
Below this, the 'ソース' (Source) section lists upload methods: 元の実行ファイル (0), 元の電子メール (0), and 元のウェブサイト (0). A red box highlights the 'ESET LIVEGUARDに送信する' (Send to ESET LIVEGUARD) button at the bottom right. A callout box with the text '手動でのファイルのアップロードも可能※' (Manual file upload is also possible※) has an arrow pointing to this button.

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

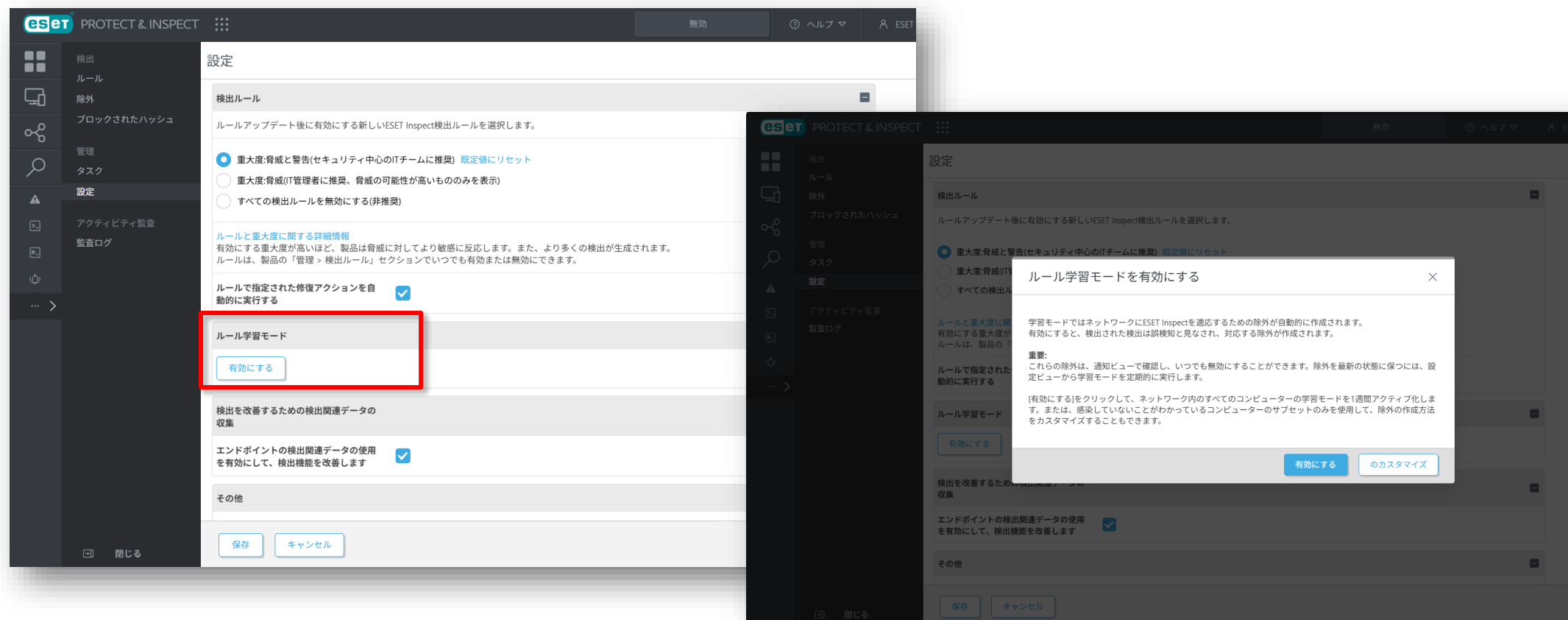
- ・ ネットワーク隔離
- ・ ハッシュ値によるブロック
- ・ 各種マーカーの付与
- ・ イベントのドロップ
- ・ 検出アラートのトリガー など



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関連グラフを確認でき、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。

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

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。

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