

# ESET PROTECT MDR Lite ～インシデント発生時のオペレーション～

## I. 概要

1. ESET MDR Lite とは
2. インシデント発生時の対応フロー

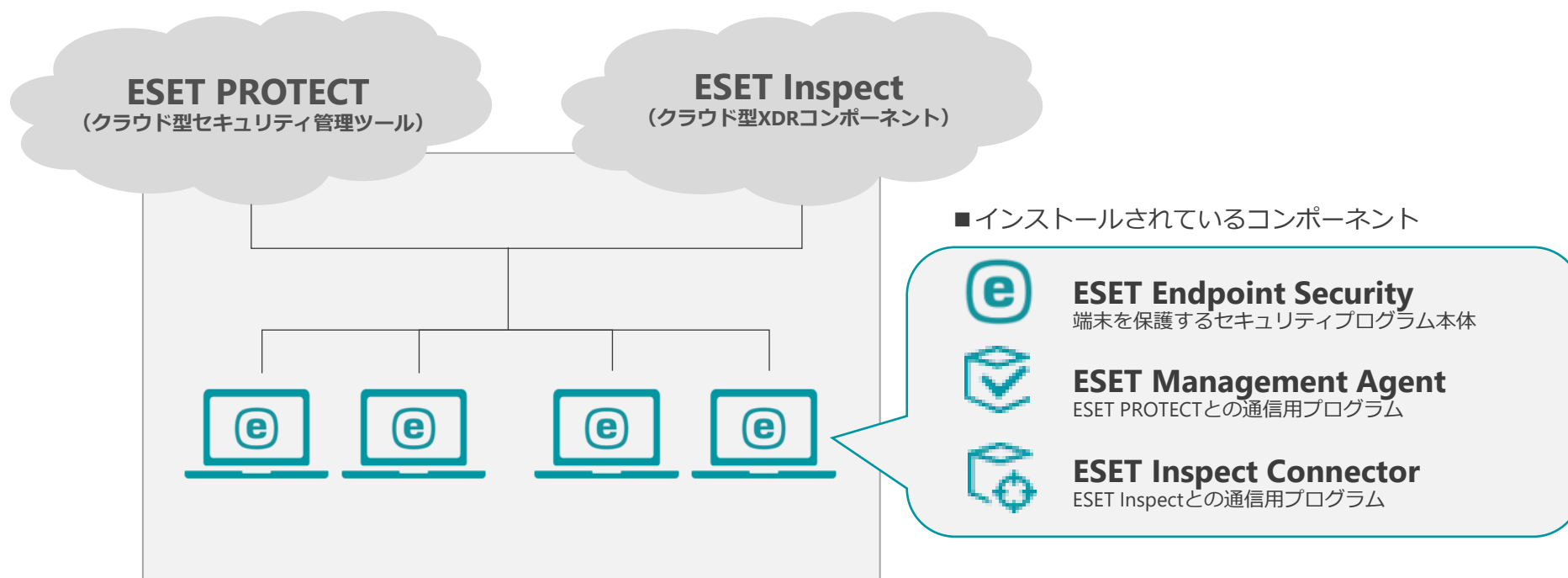
## II. インシデント発生時のオペレーション

1. インシデント発生とメール通知
2. インシデント対応状況の確認
3. NW隔離からの復旧【補足】

## III. まとめ

# 本資料について

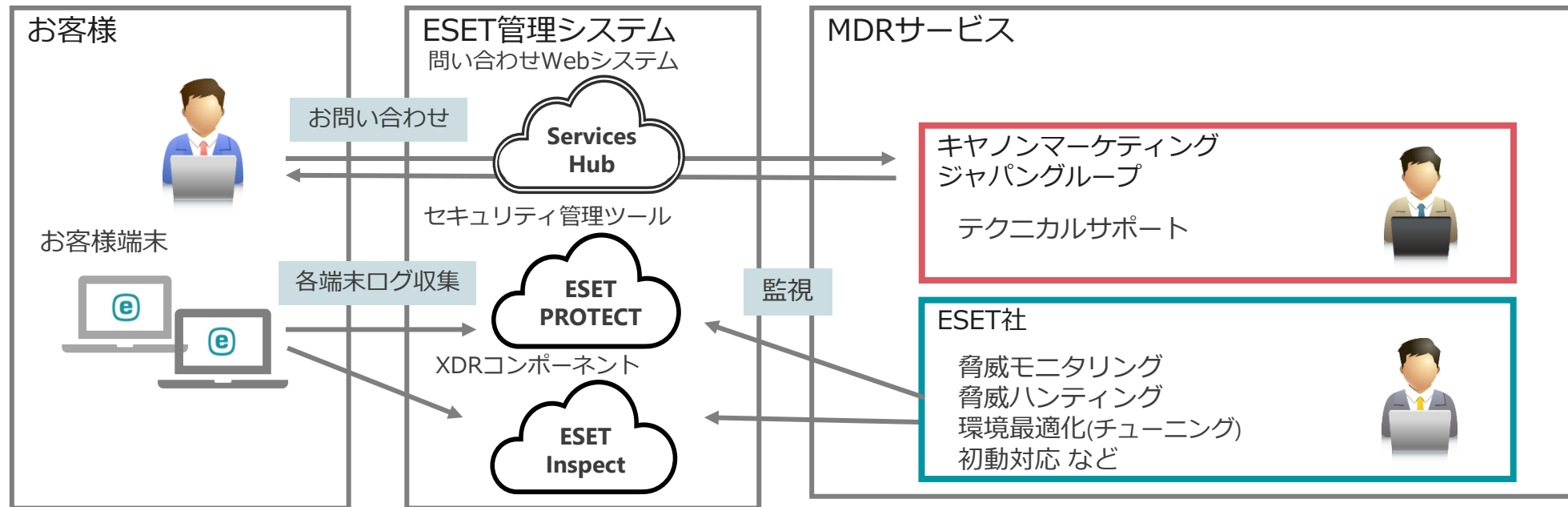
- 本資料は「ESET PROTECT MDR Lite」ご契約のお客様がインシデント発生した場合のオペレーションについてまとめた資料になります。
- 本資料はEPPをすり抜けてしまった場合を前提としています。



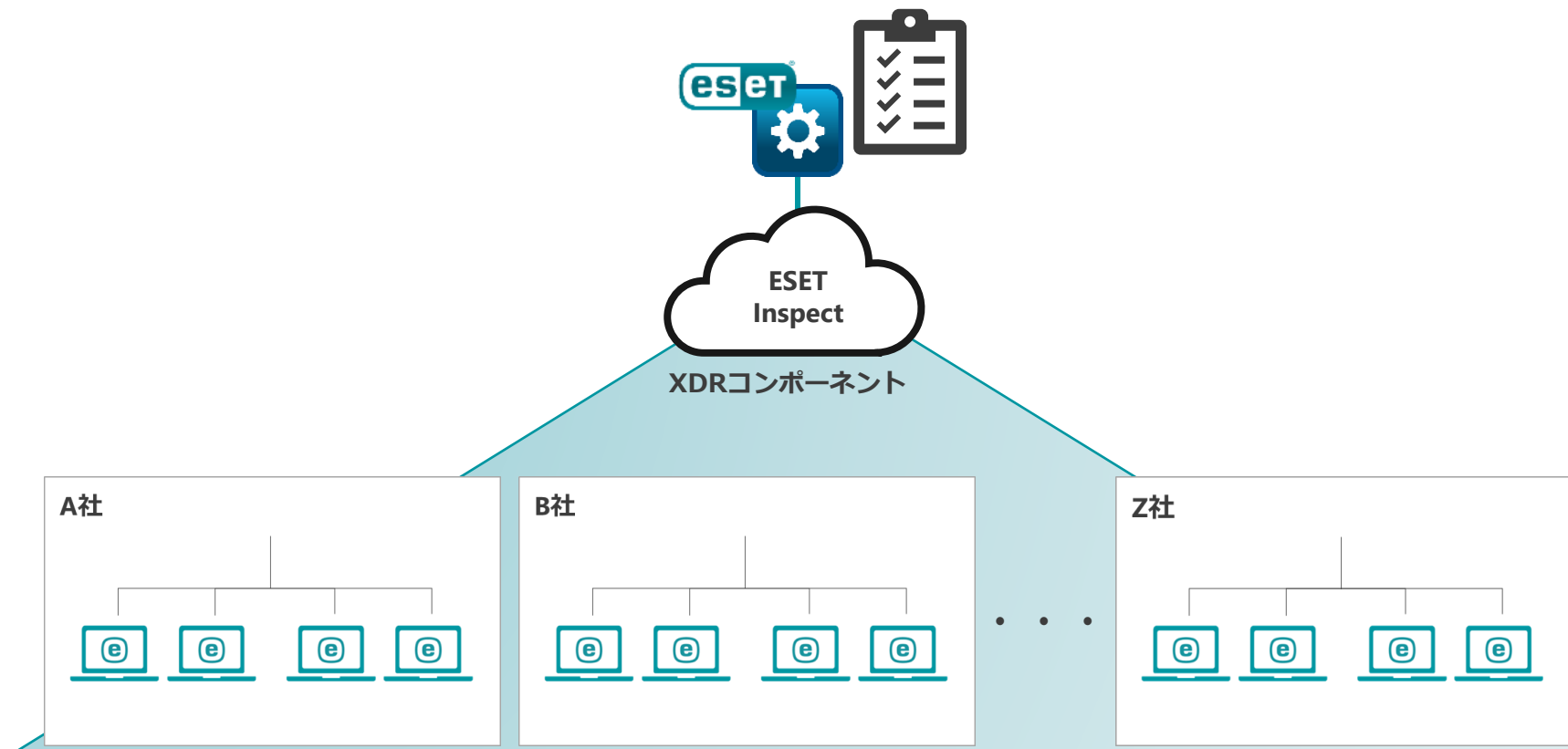
# I. 概要

# ESET PROTECT MDR Liteとは

「ESET PROTECT MDR Lite」は、ESET社運用のもと提供されるMDR（Managed Detection and Response）サービス。低コストですぐに運用開始でき、万が一の初動対応もESET社が自動で実施。問い合わせはキャノンマーケティング ジャパングループのエンジニアより日本語で対応・サポートいたします。



# ESET PROTECT MDR Liteとは



**ESET社オリジナルルール**により脅威を検出！  
24時間365日継続的に脅威モニタリングを行い、お客様環境の監視・保護・分析を行う。

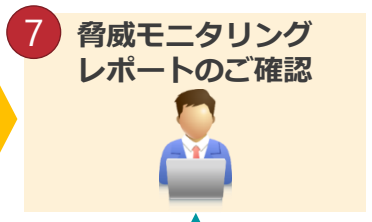
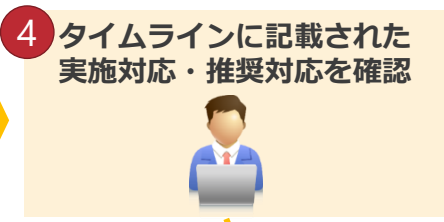
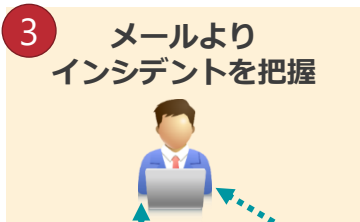


# インシデント発生時の対応フロー

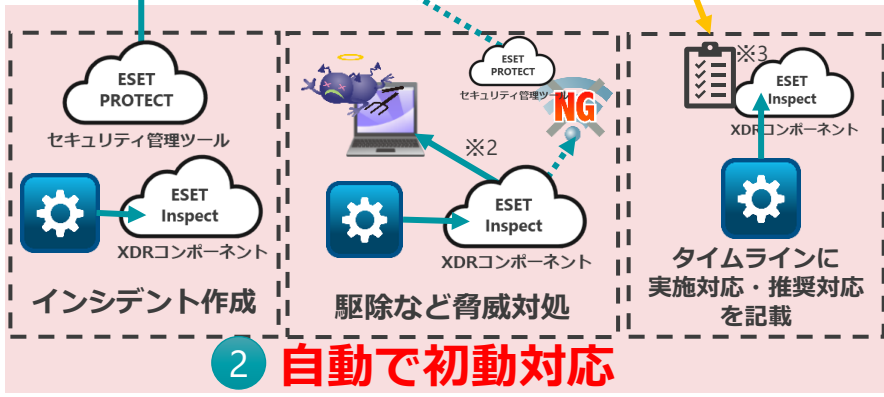
お客様側

ESET

キヤノン



3 4 5 7 ... お客様側作業



- ※1: インシデント作成とネットワーク隔離実行時のメール通知はESET PROTECTの設定が必須です。設定手順はスターターガイドに記載しています。
- ※2: 実施される脅威対処は実行ファイルの駆除が基本です。ネットワーク隔離は横展開防止のためにまれに実行されることがあります。
- ※3: タイムラインの推奨対応は英語で記載されます。



脅威未検出の場合



Webシステムより24時間365日問い合わせ可能



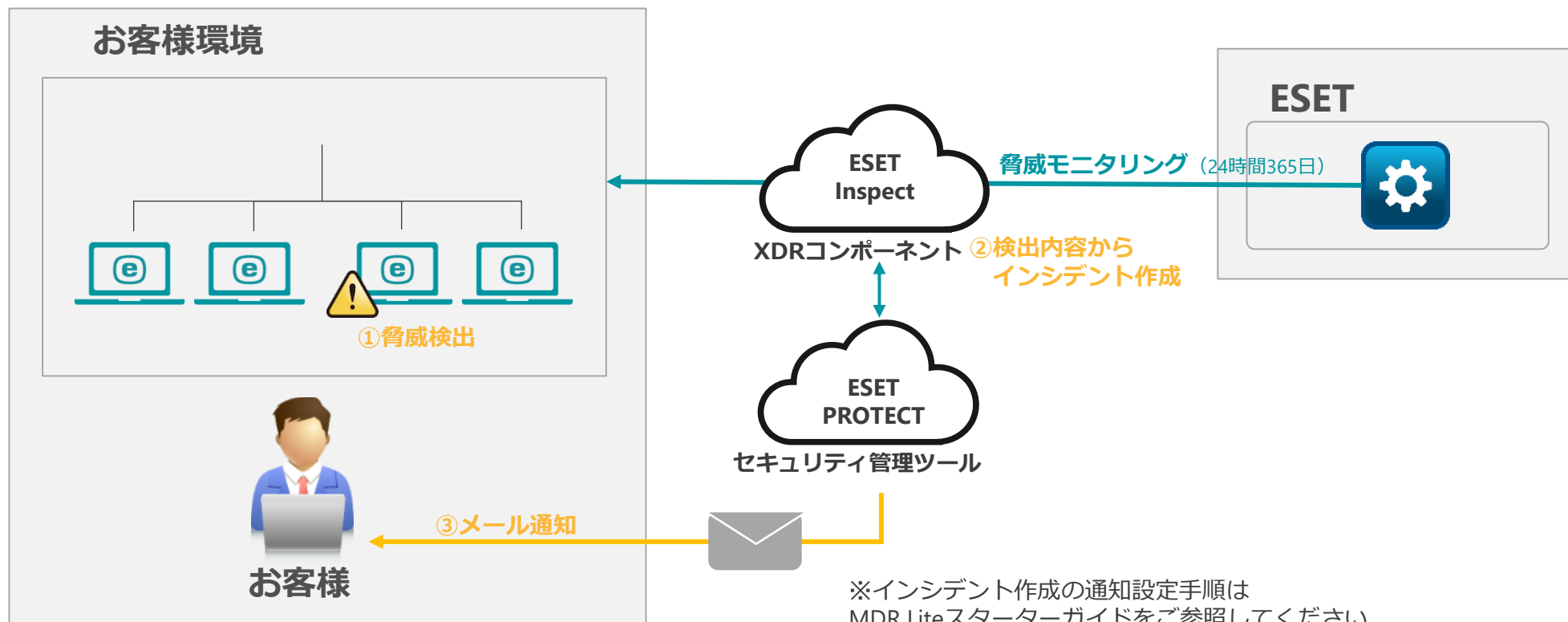
## III. インシデント発生時のオペレーション

## II. インシデント発生時のオペレーション

# 1. インシデント発生とメール通知

### ①、② 脅威監視と初動対応

通常、ESET社よりお客様環境を24時間365日脅威監視を行います。※お客様端末にインストールされたESETのログを元に監視します。お客様環境でESETの検知ルールに引っかかる脅威の疑いがあるものが検出された場合、インシデント作成が自動で実行されます。本サービスはそのまま初動対応まで自動で実行されますが、インシデント作成のメール通知設定を行うことでインシデントの疑いがあるものの検知をお客様が迅速に把握することが可能です。



## II. インシデント発生時のオペレーション

# 1. インシデント発生とメール通知

### ③ メールによるインシデント把握

インシデント作成時のメール通知設定よりインシデントの疑いがあるものの検知を把握し「ESET Inspect」にログインします。  
 ※通知メールにある「インシデントの概要を開く」をクリックいただければ「ESET Inspect」のログイン画面が表示されます。  
 ログイン情報を入力してログインいただければ、そのままインシデントのタイムライン画面に移動できます。

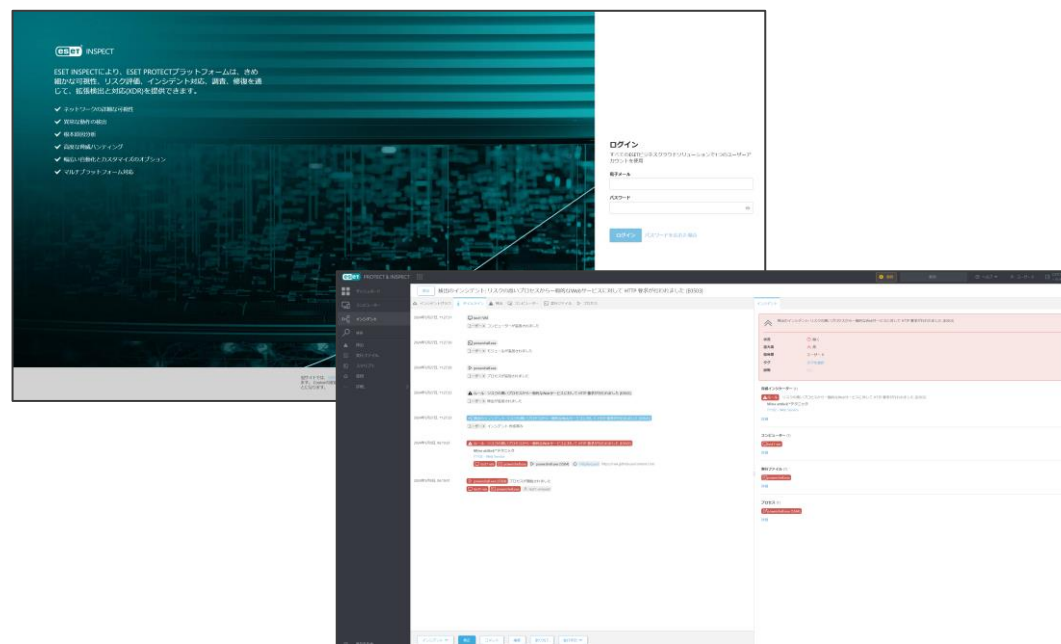
#### ■ インシデント作成通知メールサンプル



このメッセージはESET PROTECTによって送信されました

ESET PROTECT  
© 1992-2024 ESET, spol. s r.o. All Rights Reserved.

#### ■ ESET Inspectログイン画面



お客様

# 2. インシデント対応状況の確認

## ④-1 タイムラインに記載された実施対応・推奨対応を確認

発生したインシデントに対するESET社の対応状況をESET Inspectのタイムライン上で確認することができます。

2024年5月24日, 17:03:09  
Closed by ESET MDR.  
ESET MDR コメントしました

2024年5月24日, 17:03:08  
Certutil has dropped a suspicious executable  
ESET MDR ステータスが変更されました 閉じる

2024年5月24日, 17:02:49  
Certutil dropped a suspicious executable, which was subsequently blocked. No actions needed  
ESET MDR コメントしました

2024年5月24日, 16:59:41  
certutil.exe  
ESET MDR プロセスが追加されました

2024年5月24日, 16:59:39  
test1-VM  
ESET MDR コンピューターが追加されました

2024年5月24日, 16:59:39  
ルール - Certutilが不審な実行モジュールをドロップしました[A0313]  
ESET MDR 検出が追加されました

2024年5月24日, 16:59:38  
certutil.exe  
ESET MDR モジュールが追加されました

2024年5月24日, 16:59:37  
Certutil has dropped a suspicious executable  
ESET MDR インシデント 作成済み

2024年5月24日, 16:50:51  
ルール - Certutilが不審な実行モジュールをドロップしました[A0313]  
Mitre att&ck™ テクニク  
T1105 - Ingress Tool Transfer  
T1140 - Deobfuscate/Decode Files or Information  
test1-vm certutil.exe certutil.exe (7488) Exe

2024年5月24日, 16:49:32  
certutil.exe (7488) プロセスが開始されました  
test1-vm certutil.exe test1-vm\eset

ESET社の対応が完了した場合、クローズのコメントが入ります。

対応状況に応じてESET社がステータスを設定します。こちらの「状況」を確認いただくことでインシデント対応ステータスを確認することができます。

■ 設定されるステータス一覧

- ・ 進行中
- ・ 保留
- ・ 解決
- ・ 閉じる
- ・ 再度開く
- ・ 無効
- ・ ・ ・ インシデント対応中
- ・ ・ ・ インシデント対応保留
- ・ ・ ・ インシデント対応完了
- ・ ・ ・ ユーザー影響がないと判断された場合
- ・ ・ ・ 再度インシデント作成された場合
- ・ ・ ・ 調査によりインシデントではなかった場合

### ■ ESET Inspectタイムライン画面

■ ESET Inspectタイムライン画面

このタイムラインよりプロセススキルなど実施された初動対応やESET社の対応状況やESET社のコメントなど確認することができます。

# 2. インシデント対応状況の確認

## ④-2タイムライン上に記載されたESET社のコメントを確認

インシデント対応を進める中でESET社のセキュリティエンジニアから発生したインシデントに対する、分析結果と推奨対応に関するコメントがタイムライン上に記載されます。**ESET社のコメントを確認して推奨対応を実施してください。※ESET社のコメントは英語で記載されます。**

インシデントグラフ **タイムライン** 検出 コンピューター 実行ファイル プロセス

攻撃の内容や状態、推奨事項などについてコメントが追加されます。

2024年4月26日, 15:06:15

ESET MDR Staff Comment: MDR has detected successful SQL server exploitation. Adversary has created a new account mediaadminmCC1\$ on the server and added it into several groups such as administrators and remote management users. Adversary has performed basic enumeration on the server with standard utilities such as systeminfo, net, hostname and wmic.

Adversary has created persistence by adding following command to modify registry reg add "hkml\software\microsoft\windows nt\currentversion\image file execution options\ex.exe" /v debugger /t reg\_sz /d svchost.exe /f

For further execution adversary utilized srv.exe which we suspect is a Meterpreter attempted to clear multiple system logs and install AnyDesk for remote access or further persistence.

Adversary performed several defense evasion techniques as disabling the firewall and enabling RDP.

We believe this activity was a precursor to ransomware deployment which seems to have been unsuccessful as the host was isolated before the adversary managed to deploy it.

We strongly recommend starting the Incident Response process on customers side.

ESET MDR コメントしました

ESETによってコメントされたことが分かります。

※対応お困りの場合

不明点等ございましたらお問い合わせWebシステム「ESET Services Hub」にてお問い合わせ下さい。キャノンマーケティングジャパングループのエンジニアがサポートいたします。**※ESET社のコメントは全文記載した上でお問い合わせください。**

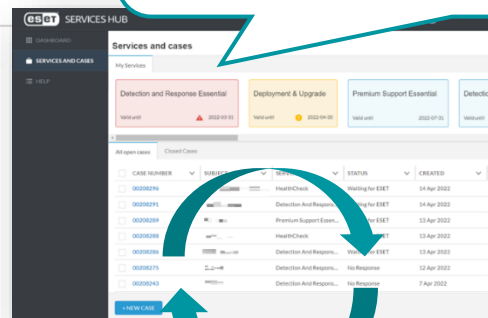
2024年4月26日, 14:58:45

Resolved by

ESET MDR コメントしました



お客様



テクニカルサポート

※翻訳のみの依頼は対象外になります。

## 2. インシデント対応状況の確認

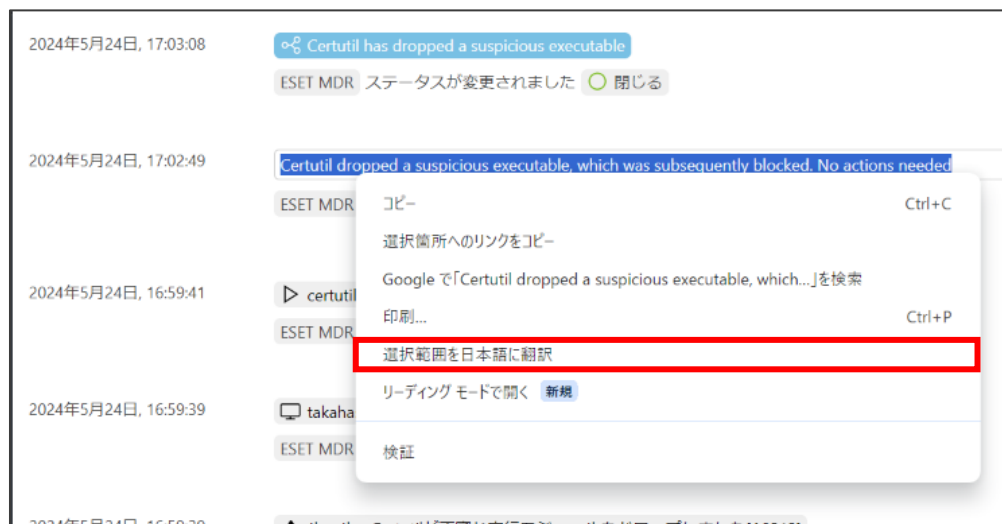
### 【参考】ESET社のコメント翻訳

ESET社のコメントは英語での記載になりますがブラウザ標準の翻訳機能などで簡単に日本語訳可能です。

### 例：「Google chrome」ご利用の場合

コメントを範囲選択して右クリックし、「選択範囲を日本語に翻訳」をクリック

※「Microsoft edge」なども同様に右クリックから翻訳することが可能。



# 3. NW隔離からの復旧【補足】

## ⑤NW隔離実行の把握とその対応

インシデントの初動対応は基本的に脅威駆除などが実行されますが、NW隔離が実施される場合もございます。NW隔離からの復旧作業はお客様作業になりますので、ESET社からの推奨対応を実施したのちにNW復旧作業を実施してください。

※NW隔離の通知設定を実施いただければ、迅速に隔離された端末を把握することが可能です。設定手順はMDR Liteスターターガイドをご参照ください。

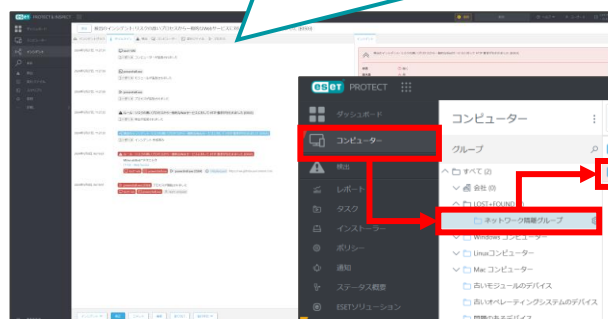
### ■ ネットワーク隔離通知メールサンプル



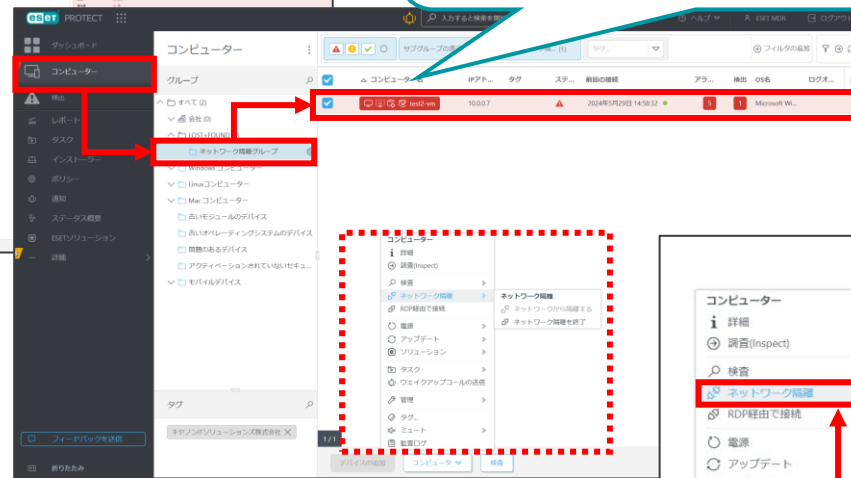
お客様

ESET社  
初動対応完了後

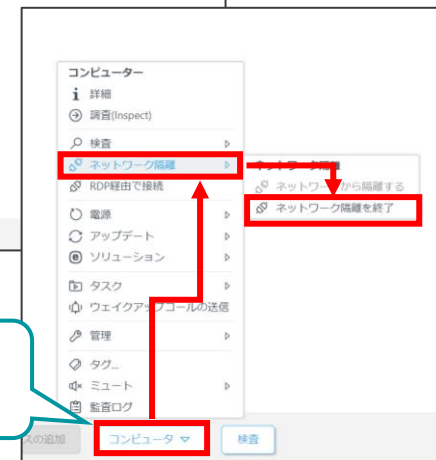
① 「ESET Inspect」のタイムラインより ESET社の推奨対応を確認・実施



② 「ESET PROTECT」にログインし、メインメニューの「コンピューター」より NW隔離用動的グループにある端末を選択 ※NW隔離用の動的グループはデフォルトではございません。設定手順はMDR Liteスターターガイドをご参照ください。



③ 「コンピュータ」-「ネットワーク隔離」 - 「NW隔離を終了」よりNW復旧





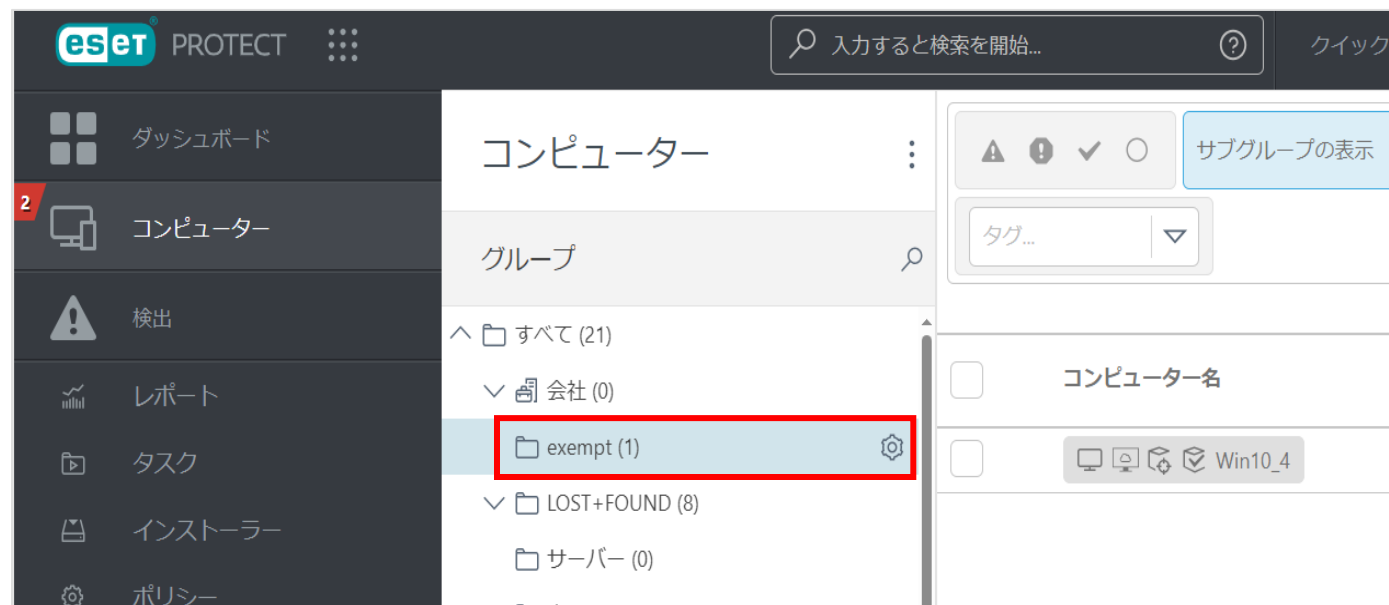
# 参考：初動対応から除外している場合 1/2

クリティカルなサーバーなどESET社による初動対応を希望しないクライアントがある場合、「exempt」という名前で静的グループを作成して該当クライアントを所属させることで、そのクライアントはESET社によるプロセス停止やネットワーク隔離などの初動対応から除外されます。

初動対応からの除外については、いつでも除外グループへの登録や解除が可能ですので、一定期間除外し問題がなさそうであればグループから外して初動対応の対象にするといった運用も可能です。

※初動対応から除外するグループの作成方法については、スターターガイドをご参照ください。

※初動対応から除外したクライアントについては、インシデント発生時の対応をお客様にて対処いただく必要がありますので、初動対応から除外するかどうかは慎重にご判断ください。





## II. インシデント発生時のオペレーション

# 参考：初動対応から除外している場合 2/2

### 対応例：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ESET Inspect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



The screenshot shows the ESET Inspect interface with an incident selected. A text box highlights the 'ネットワーク隔離' (Network Isolation) button in the bottom toolbar. A callout box explains that network isolation also disconnects VPN connections, so users should be notified. Another callout points to the 'ネットワーク隔離' button in the detailed incident view, indicating it can be clicked directly from there.

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、実施するにはご注意ください。

ネットワーク隔離

ネットワーク隔離

インシデント対応の一例として、インシデントレスポンスのデモ動画がございますので対応の際の参考としてご参照ください。

▼ 【ESET Inspect】インシデントレスポンス デモ動画①

<https://youtu.be/KMlcfBqjYZU>

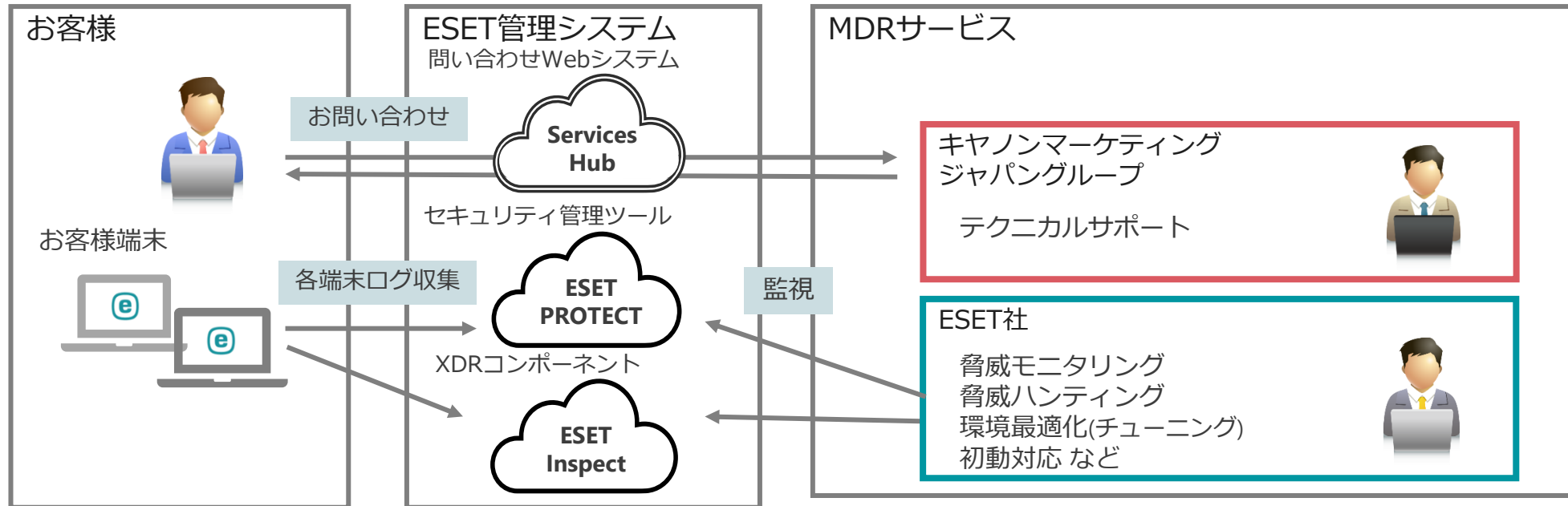
▼ 【ESET Inspect】インシデントレスポンス デモ動画②

<https://youtu.be/SGWKGa65v3o>

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

## III.まとめ

# まとめ



**本資料はインシデント発生時のお客様対応を中心にお伝えした内容となっておりますが、  
負荷の高い常時監視やインシデント発生時の初動対応などはESET社で対応いたしますのでご安心ください。**