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

キヤノンマーケティングジャパン株式会社

第7版 2026年10月14日

目次

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

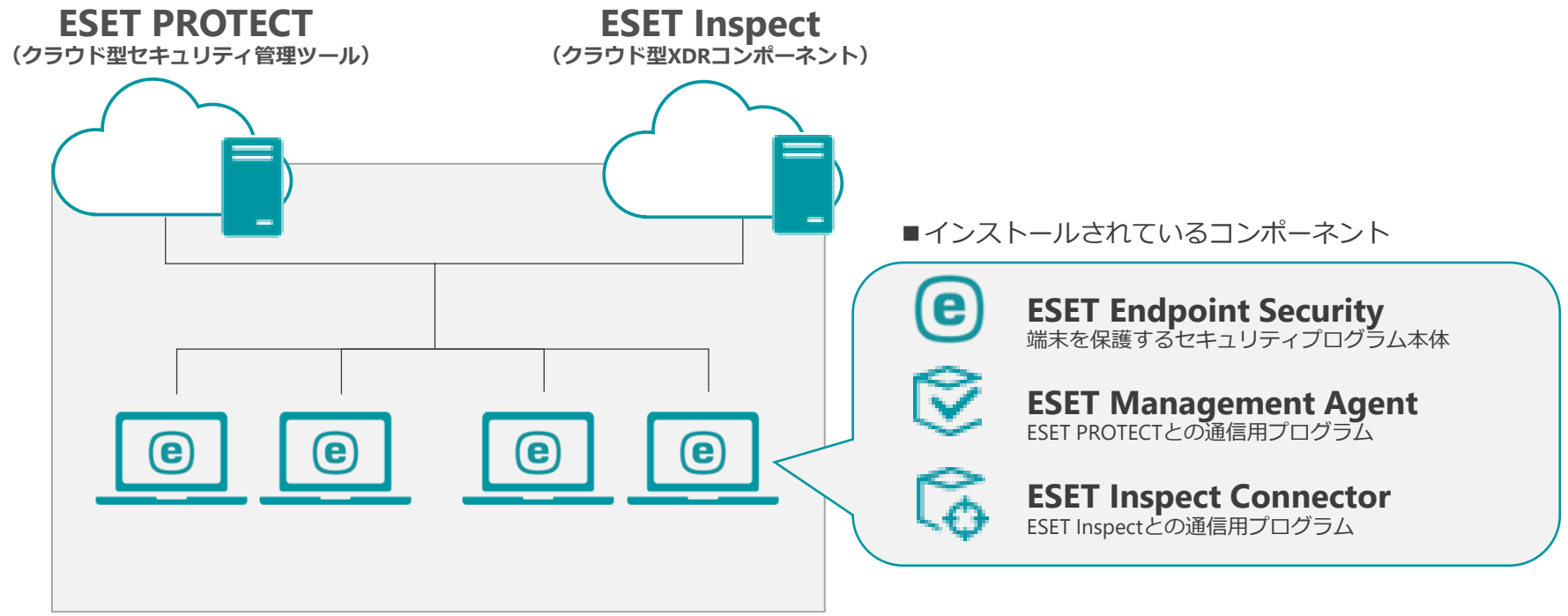
II. インシデント発生時のオペレーション

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】
4. インシデントクローズ

III. まとめ

本資料について

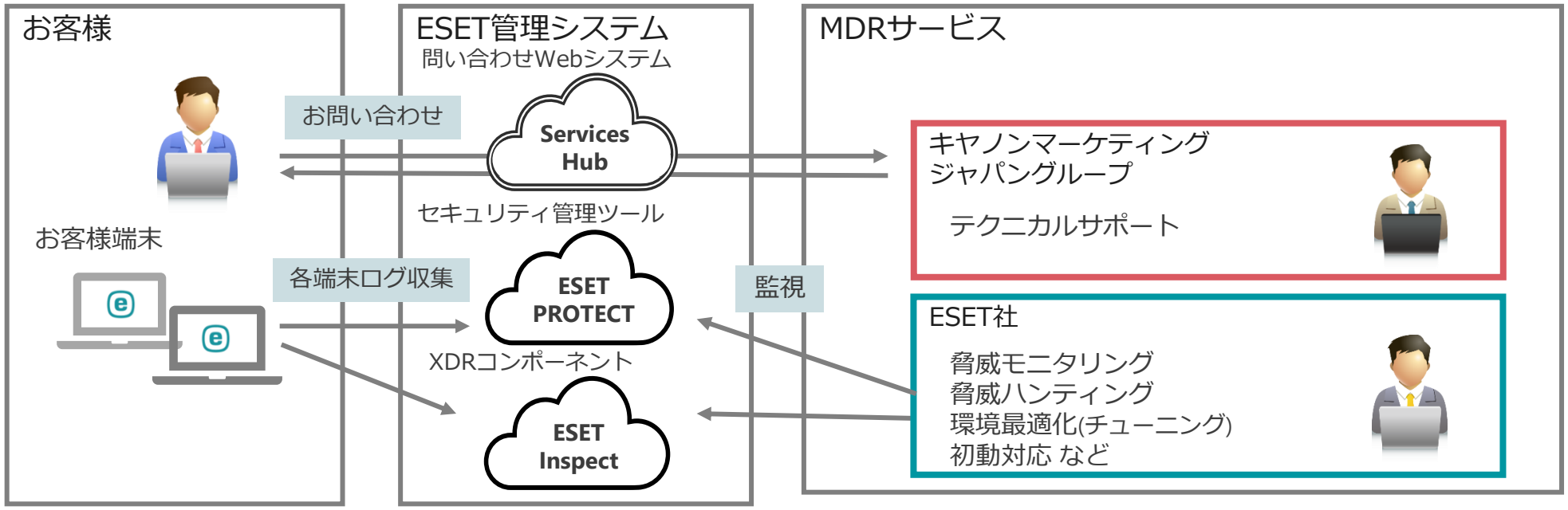
- 本資料は「ESET PROTECT MDR Lite」ご契約のお客様がインシデントが発生した場合のオペレーションについてまとめた資料になります。
- 本資料はEPPをすり抜けてしまった場合を前提としています。



I. 概要

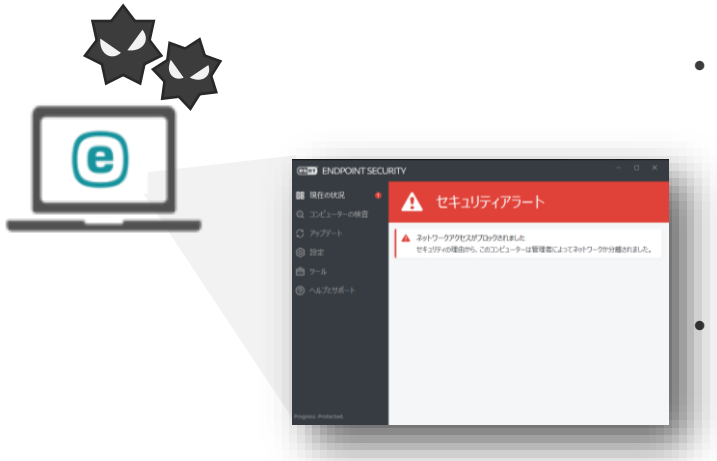
ESET PROTECT MDR Liteとは

「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。問い合わせはキヤ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

平均6分での脅威への対応

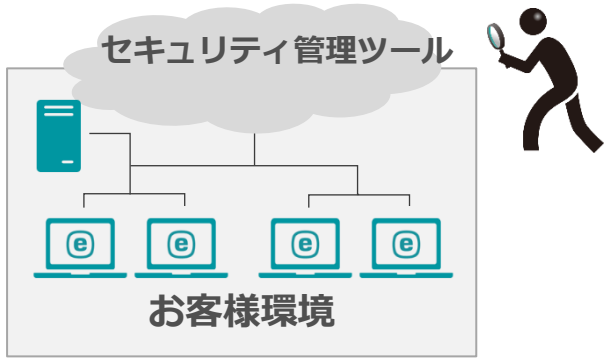


- 脅威が発生した場合、平均6分で初動対応

  例）NW隔離
  →クライアント上で
  アラートが表示されます

- 脅威の詳細(英語)の確認が可能

24時間365日体制の脅威監視

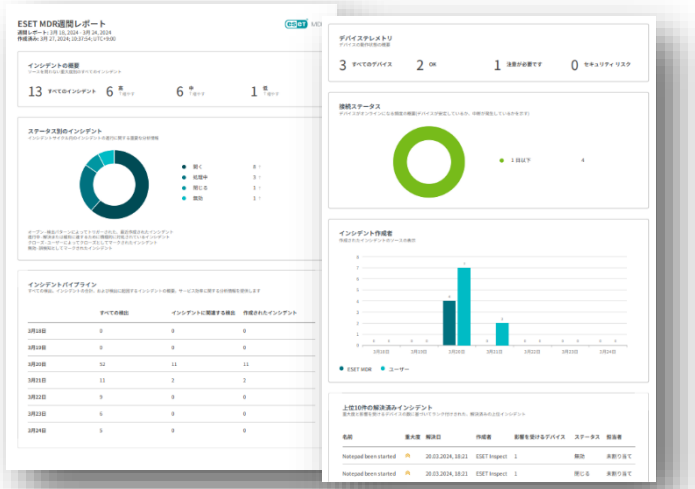


- 24時間365日お客様環境を監視、分析

日本語でのサポート

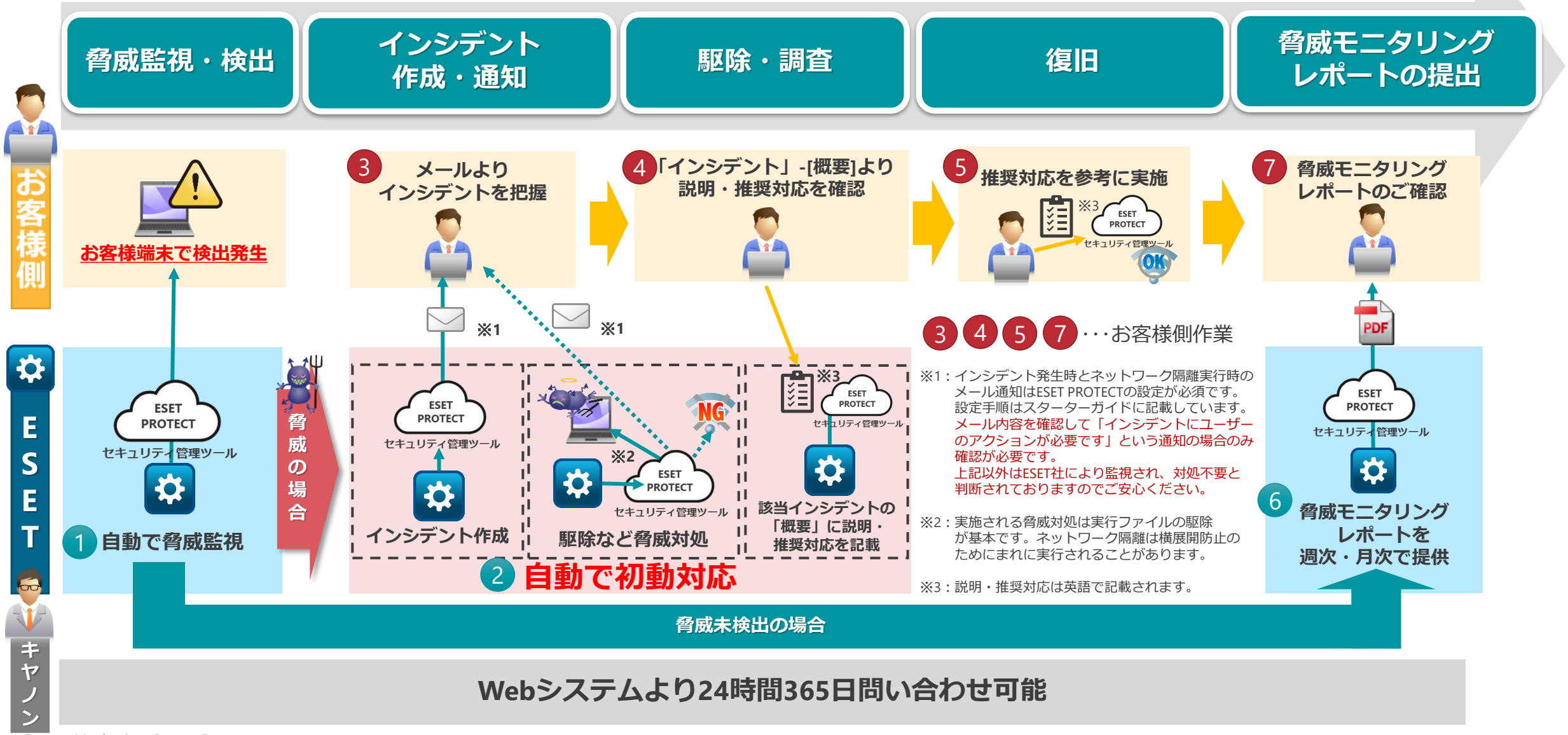
- Webシステムより24時間365日お問い合わせ可能

週次/月次でのレポート提供



- 環境内で発生したインシデントの状況やEPPの状態が把握可能

インシデント発生時の対応フロー



※1：インシデント発生時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。メール内容を確認して「インシデントにユーザーのアクションが必要です」という通知の場合のみ確認が必要です。上記以外はESET社により監視され、対処不要と判断されておりますのでご安心ください。

※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：説明・推奨対応は英語で記載されます。

Webシステムより24時間365日問い合わせ可能

ESET PROTECTご確認時の注意事項

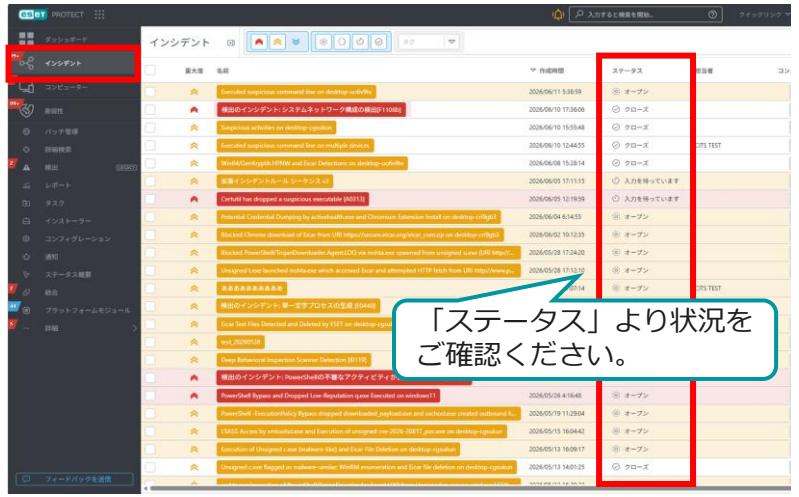
ESET PROTECTをご確認いただく際、ご注意いただきたい点をご案内いたします。
※お客様にご確認いただきたい情報はESET PROTECTに統合されております。 ESET Inspectをご確認いただく必要はありません。

・**「インシデント」について**
対応が必要なものは、「インシデントにユーザーのアクションが必要です」という通知が届いたインシデントのみです。

インシデント通知は2種類あります。

・**「インシデントにユーザーのアクションが必要です 」**
EP上でのステータス：「入力待ち」
ESET側の調査の結果、**お客様側で対応が必要**です。
必ずインシデントの内容確認と対処を実施ください。お客さま側で対応完了後、ステータスを「クローズ」に設定変更をお願いいたします。
手順についてはp18をご確認ください。

・**「ESET MDRがインシデントに対応しました」**
EP上でのステータス：「クローズ」
ESET側で対応完了済みですが、お客さま側で発生したインシデント内容についてご確認ください。

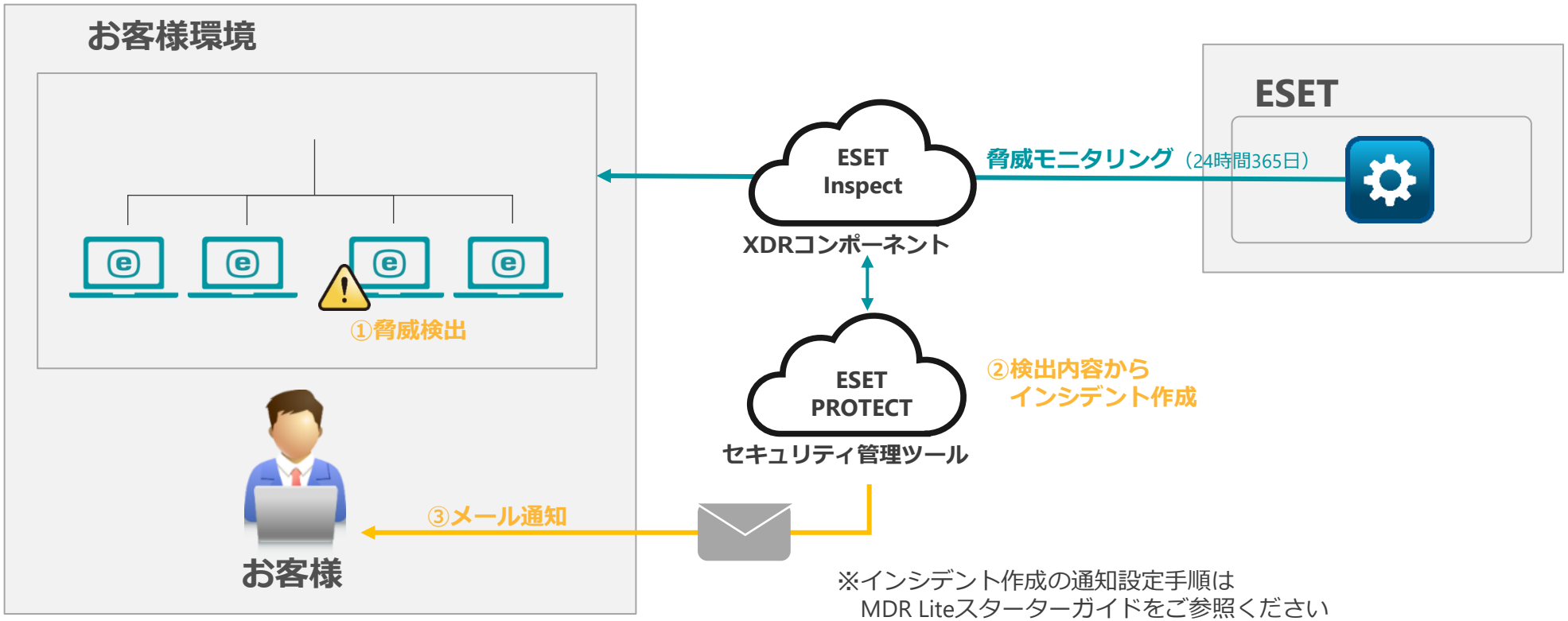


II. インシデント発生時のオペレーション

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。



※インシデント作成の通知設定手順は
MDR Liteスターターガイドをご参照ください

1．インシデント発生とメール通知

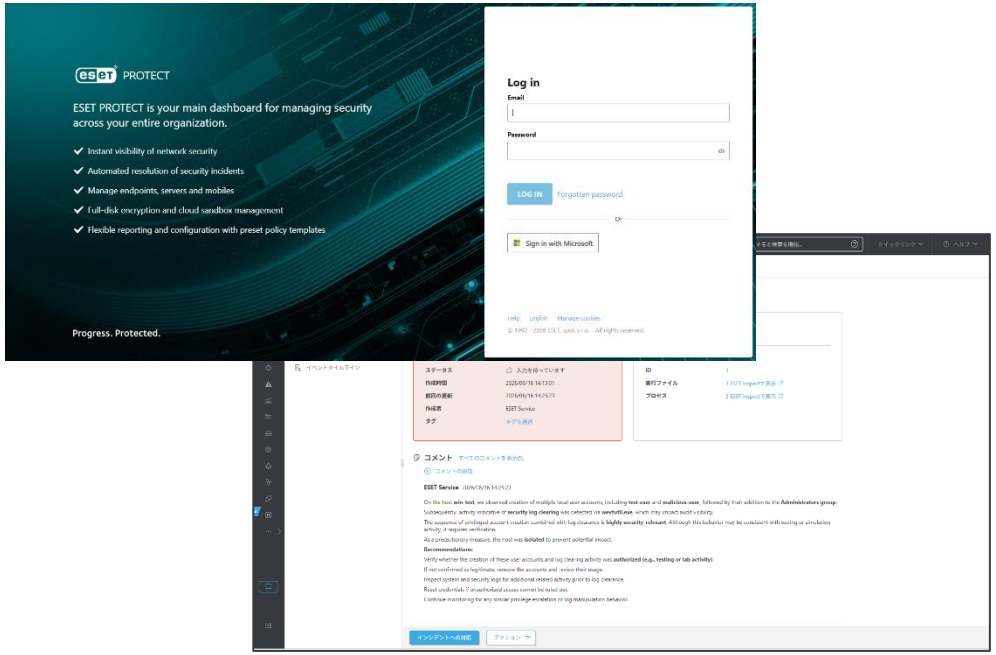
③ メールによるインシデント把握

インシデントのメール通知によりインシデントの疑いがあるものの検知を把握し「ESET PROTECT」にログインします。
※通知メールにあるURLをクリックいただければ「ESET PROTECT」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、そのまま該当のインシデント画面に移動できます。

■インシデント発生時の通知メールサンプル

お客様

■ESET PROTECTログイン画面



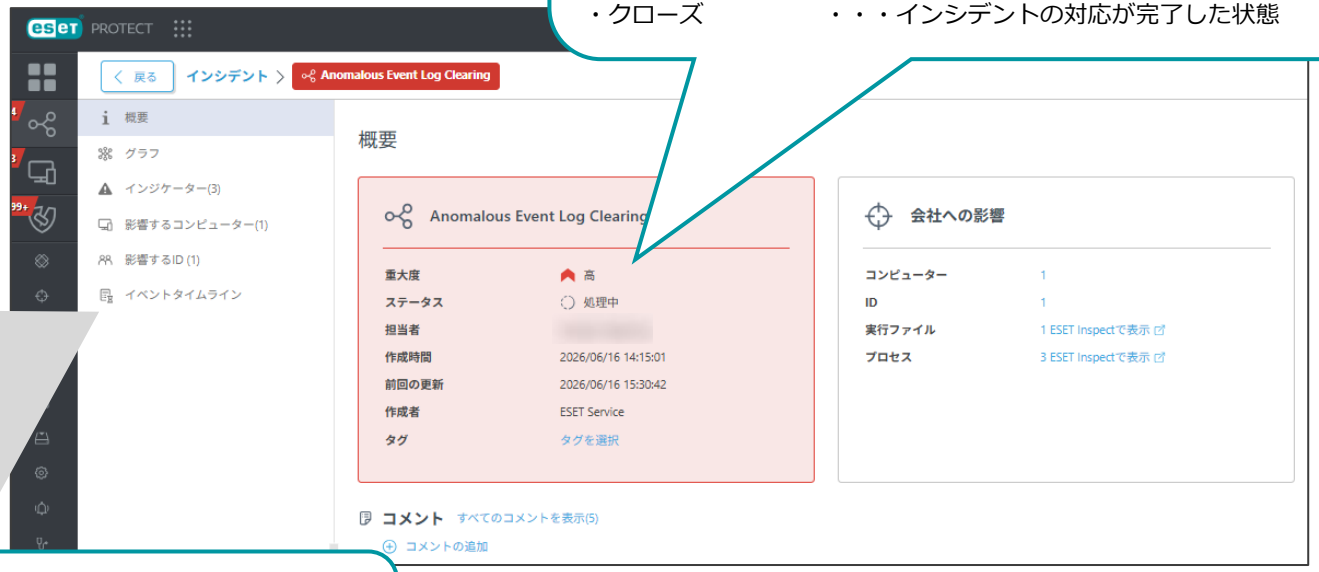
2．インシデント対応状況の確認

④-1 「インシデント」-[概要]より説明・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 PROTECTの「インシデント」の概要やイベントタイムラインより確認できます。

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。

■ESET PROTECTタイムライン画面



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

・オープン	・・・インシデントが作成されオープンな状態
・処理中	・・・インシデント調査、対応中の状態
・入力待ち	・・・ユーザーによる対処が必要な状態
・クローズ	・・・インシデントの対応が完了した状態

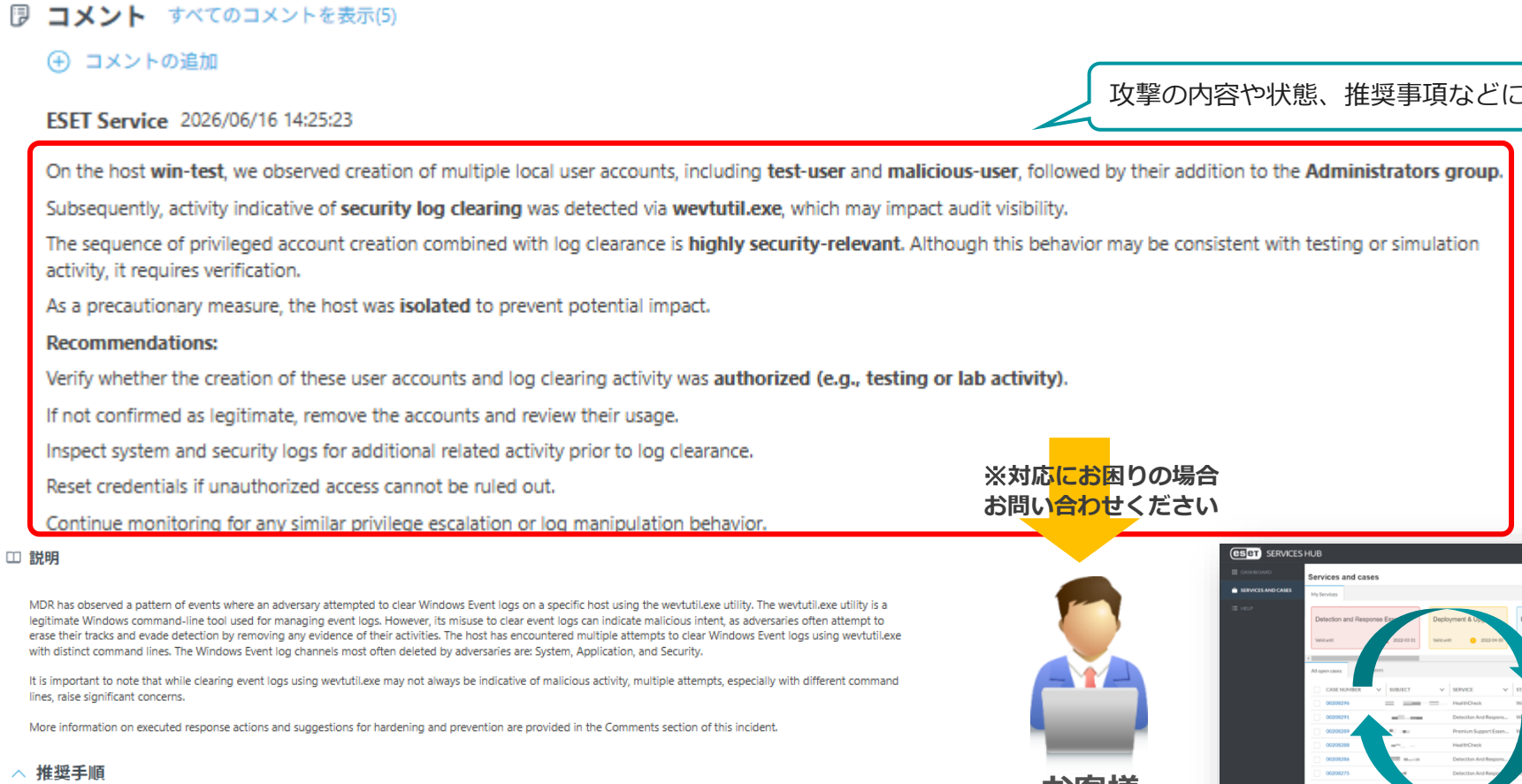
こちらのタイムラインよりプロセスキルなど
実施された初動対応やESET社の対応状況や
ESET社のコメントなど確認することができます。

2．インシデント対応状況の確認

④-2 「インシデント」-[概要]より説明・推奨対応を確認

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説明や推奨対応に関してコメントがされます。

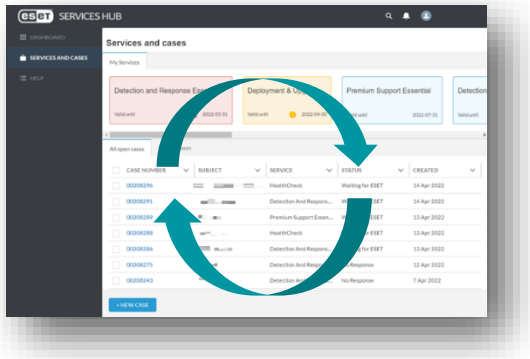
ESET社のコメントを確認して推奨対応を実施してください。※ESET社のコメントは英語で記載されます。



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。

※対応にお困りの場合
お問い合わせください

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

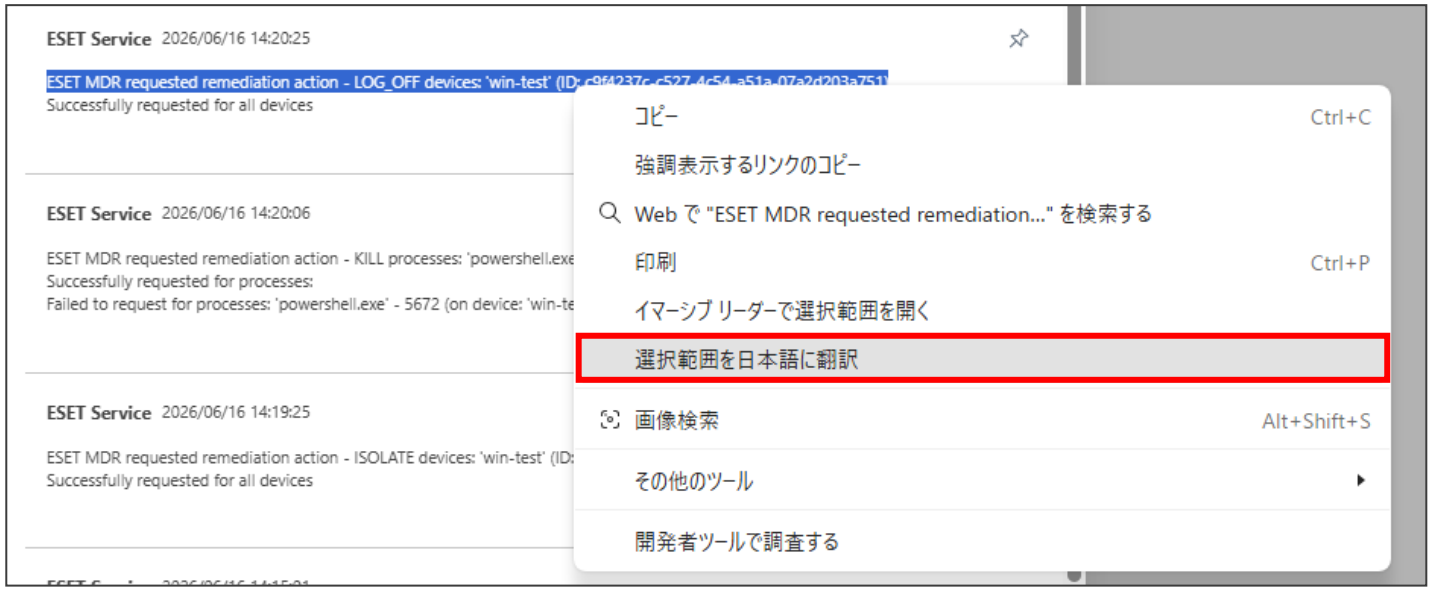
【参考】ESET社のコメント翻訳

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。



2．インシデント対応状況の確認

【参考】インシデント発生時のお問い合わせ

ご不明点等ございましたら問い合わせWebシステム「ESET Services Hub」よりお問い合わせください。
キヤ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。
お問い合わせの際は、ESET社のコメント全文とインスタンスIDの記載をお願いいたします。

【インスタンスID確認方法】

1. ESET Business AccountもしくはESET PROTECT Hubにログインします。
2. 画面右上 [ヘルプ]-[バージョン情報]を押下します。
3. 「ESET PROTECT」、「ESET Inspect」のID情報をご連絡ください。

※ここではESET PROTECT Hubを例にご案内しておりますが、
ESET Business Accountをご利用の場合でも確認手順は同じです。

3．NW隔離からの復旧【補足】

⑤-1 NW隔離実行の把握とその対応

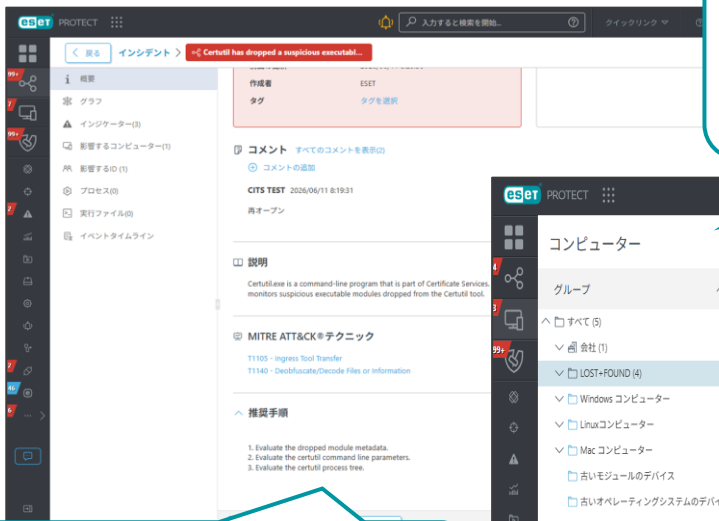
インシデントの初動対応は基本的に脅威駆除などが実行されますが、NW隔離が実施される場合もございます。NW隔離からの復旧作業はお客様作業になりますので、ESET社からの推奨対応を実施したのちにNW復旧作業を実施してください。

※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

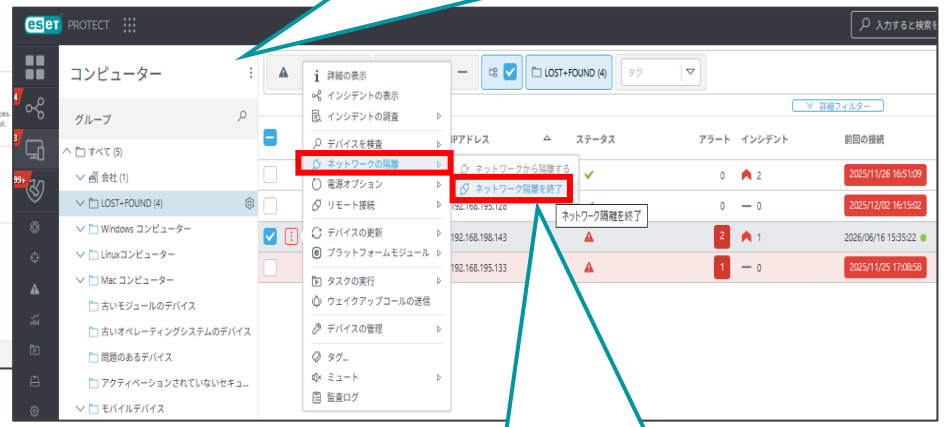
ESET社
初動対応完了後



①ESET PROTECTのメインメニューの「インシデント」-[概要]よりESET社の推奨対応を確認・実施

②ESET PROTECTのメインメニュー「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。

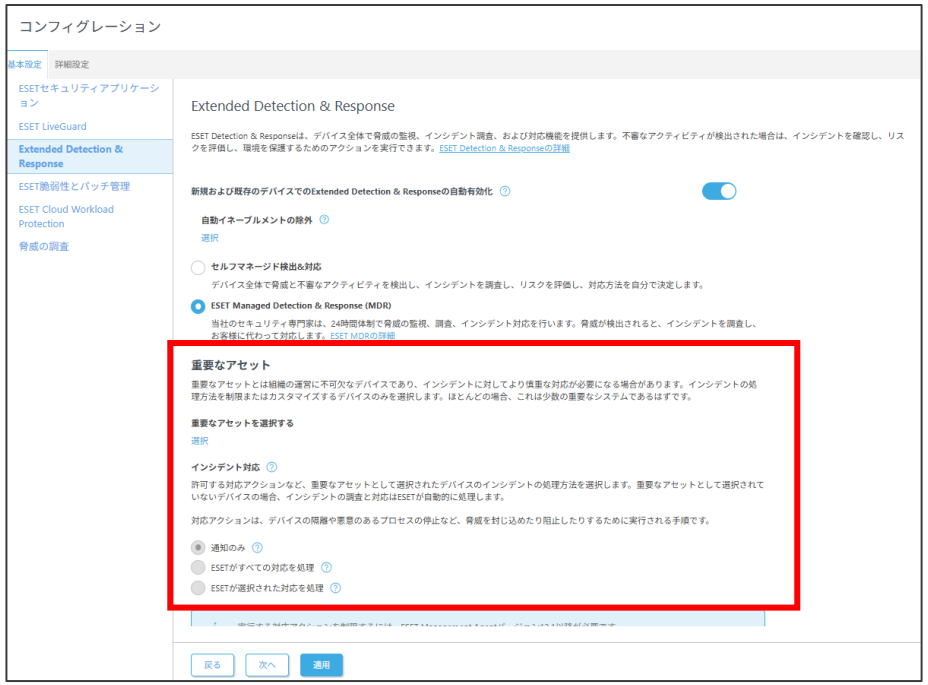


③対象端末を選択し[ネットワークの隔離]-[ネットワーク隔離を終了]よりNW復旧

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、「コンフィグレーション」- [Extended Detection & Response]より [重要なアセット]- [通知のみ]という設定を該当クライアントまたはグループに対して有効にしておくことで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。また初動対応として、特定のアクションのみ抑制することも可能です。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なため、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設定方法はスターターガイドをご参照ください。
　MDR Liteスターターガイド: https://eset-info.canon-its.jp/files/user/pdf/support/ep-mdr-lite_sg.pdf　※「3. 通知メールの設定」のセクションをご確認ください
※初動対応から除外したクライアントは、インシデント発生時の対応をお客様にて実施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。



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、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

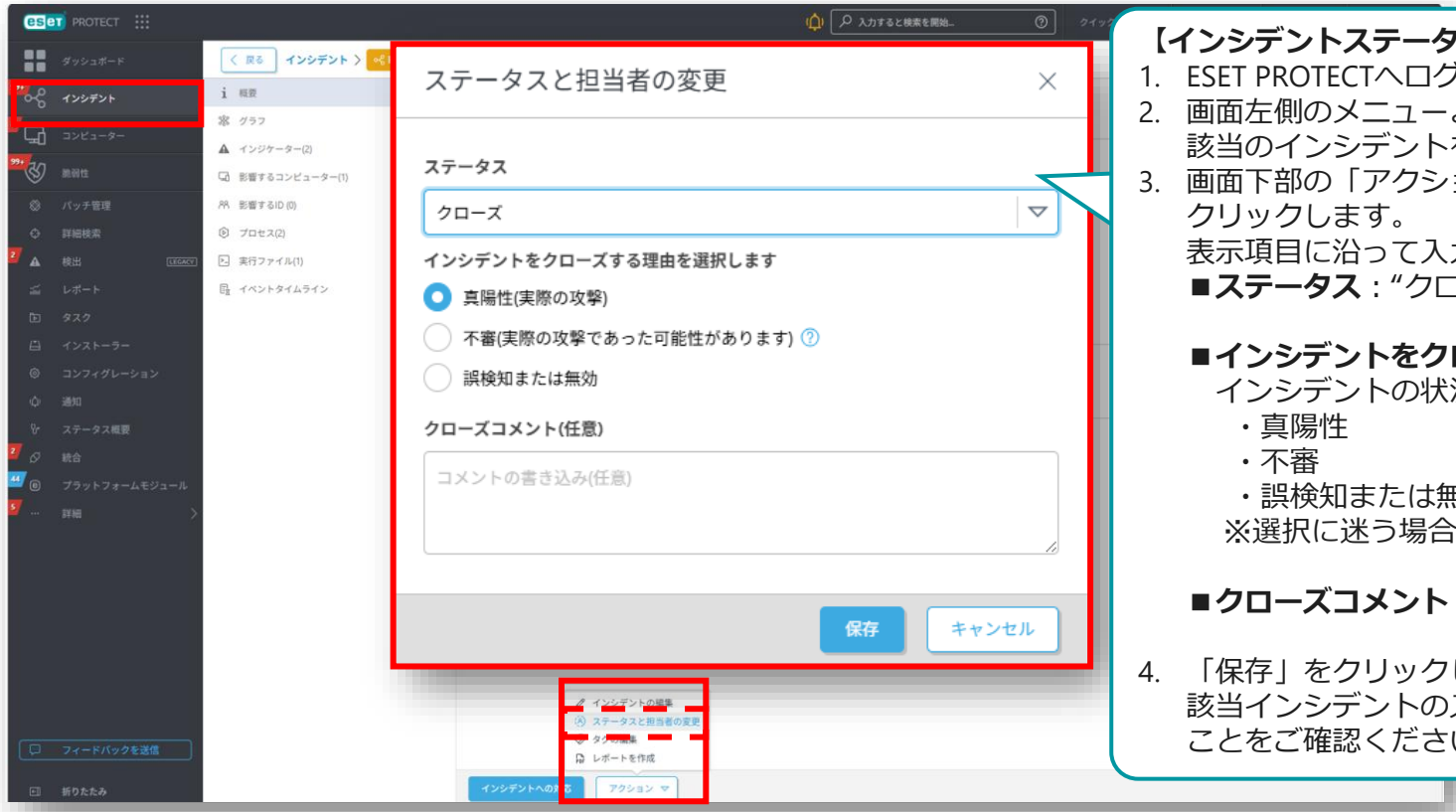
インシデント対応の一例として、インシデントレスポンスのデモ
動画がございますので対応の際の参考としてご参照ください。

▼【ESET Inspect】インシデントレスポンス デモ動画①
https://youtu.be/KMIcfBqjYZU
▼【ESET Inspect】インシデントレスポンス デモ動画②
https://youtu.be/SGWKGa65v3o

4．インシデントクローズ

⑤-2 インシデント対応完了後の作業

インシデントに対する推奨対応の実施や復旧等が完了しましたら、ESET PROTECT上でインシデントのステータス設定をご変更ください。
ステータス変更にあたり不明点や疑問点等ありましたらESET Services Hubよりお問い合わせください。



【インシデントステータス変更手順】

1. ESET PROTECTへログインします。
2. 画面左側のメニューより「インシデント」をクリックし、該当のインシデントを選択します。
3. 画面下部の「アクション」より[ステータスと担当者の変更]をクリックします。
   表示項目に沿って入力します。
   ■**ステータス**：“クローズ”を選択します。

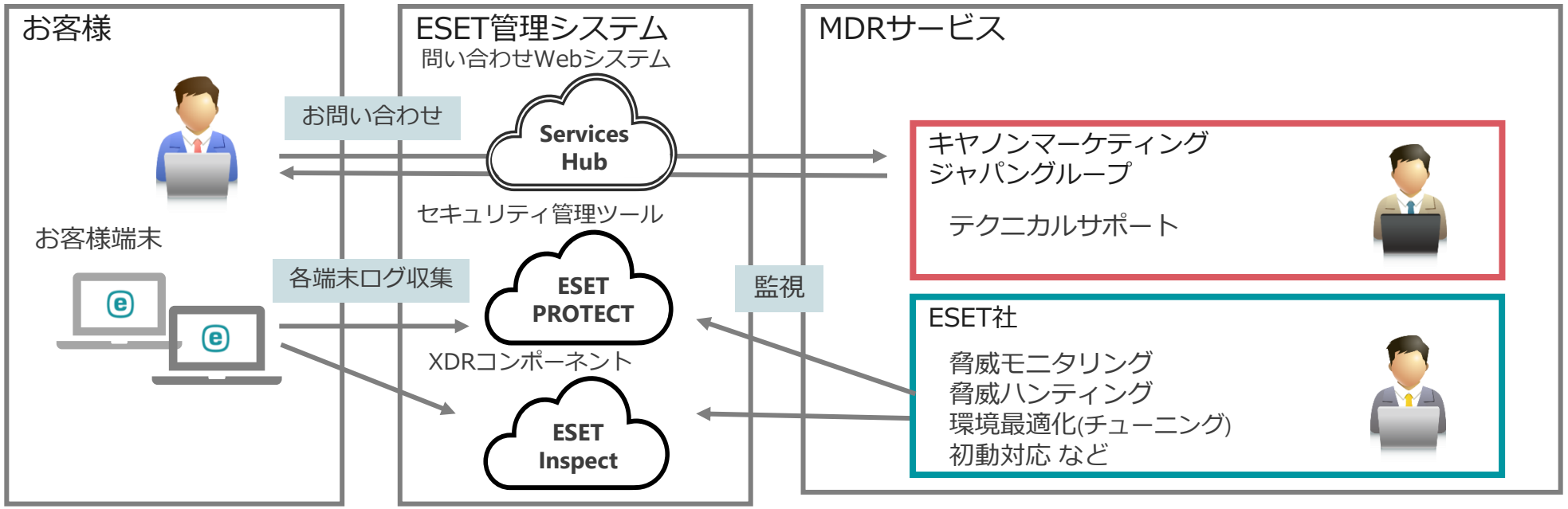
   ■**インシデントをクローズする理由を選択します**：
   インシデントの状況に合わせて以下3つの項目より設定します。
   ・真陽性　　：実際の攻撃であった場合
   ・不審　　：攻撃であった可能性がある場合
   ・誤検知または無効：誤検知または問題がなかった場合
   ※選択に迷う場合は、「不審」をご選択ください。

   ■**クローズコメント**：任意でご入力ください。

4. 「保存」をクリックして完了です。
   該当インシデントのステータスが「クローズ」に変更されていることをご確認ください。

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。