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

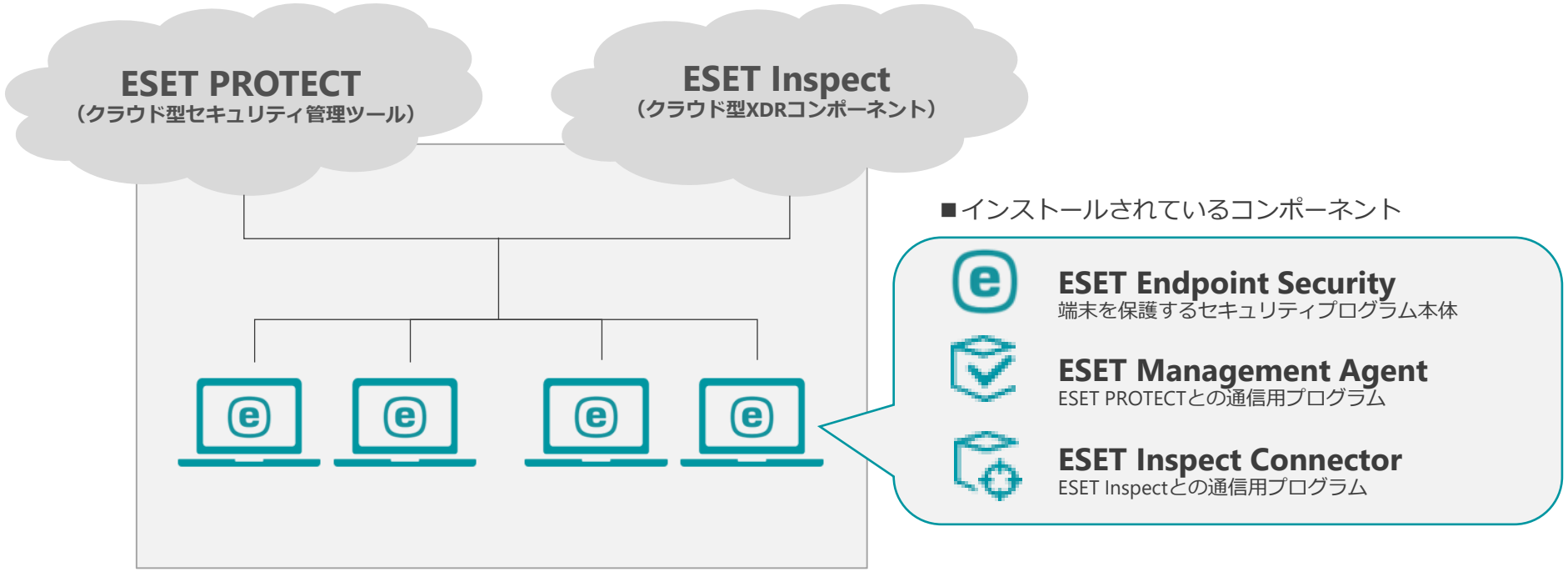
キヤノンマーケティングジャパン株式会社

第1版 2024年8月27日

目次

本資料について

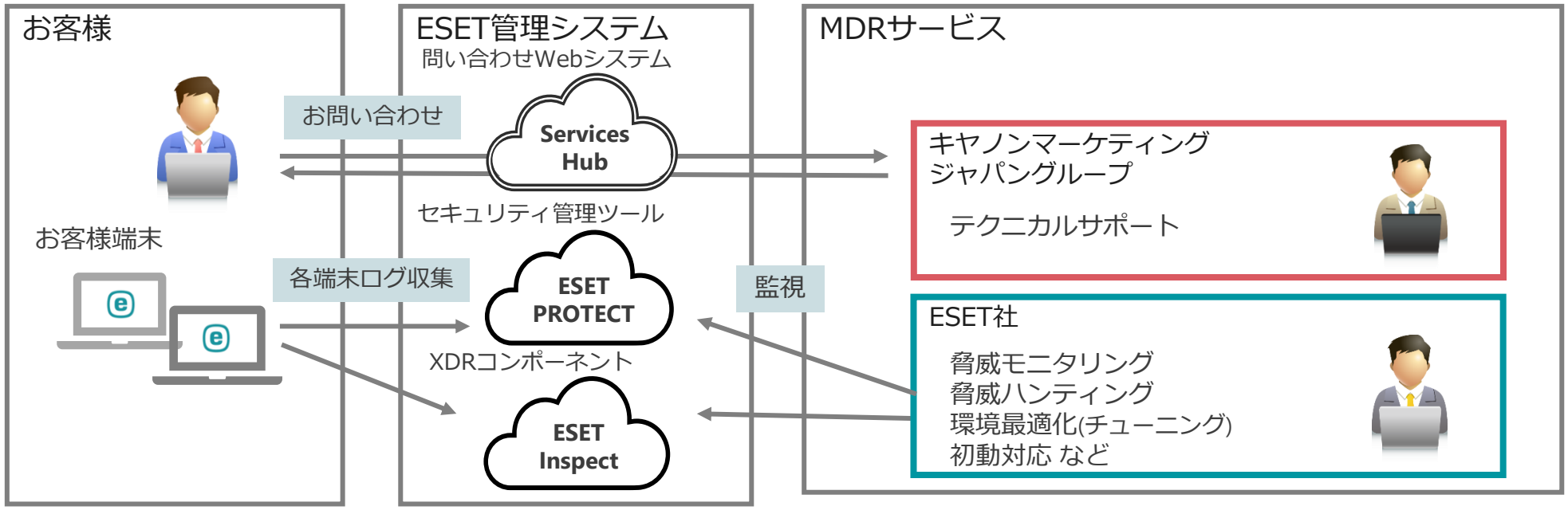
- 本資料は「ESET POTECT MDR Lite」ご契約のお客様がインシデント発生した場合のオペレーションについてまとめた資料になります。
- 本資料はEPPをすり抜けてしまった場合を前提としています。



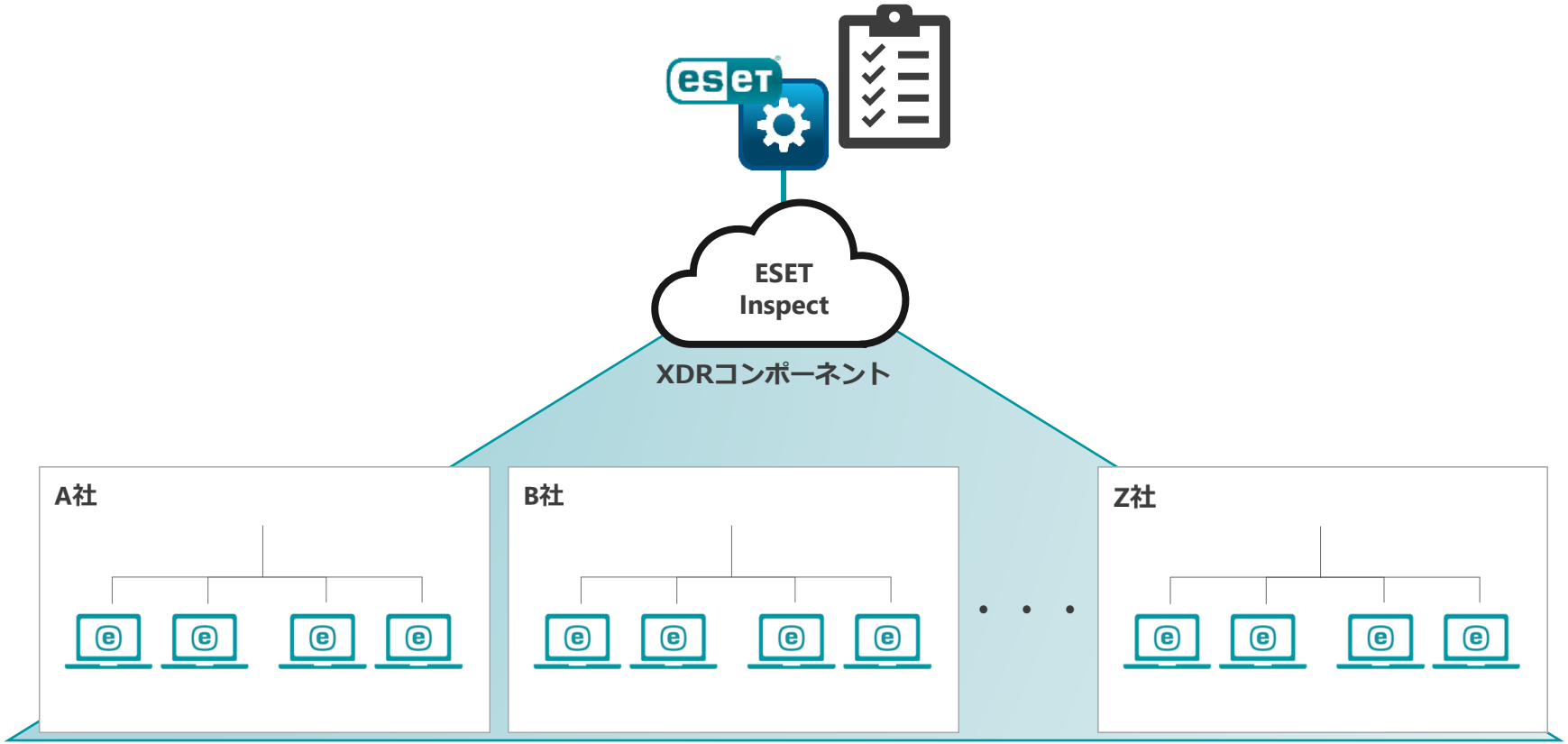
I. 概要

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。



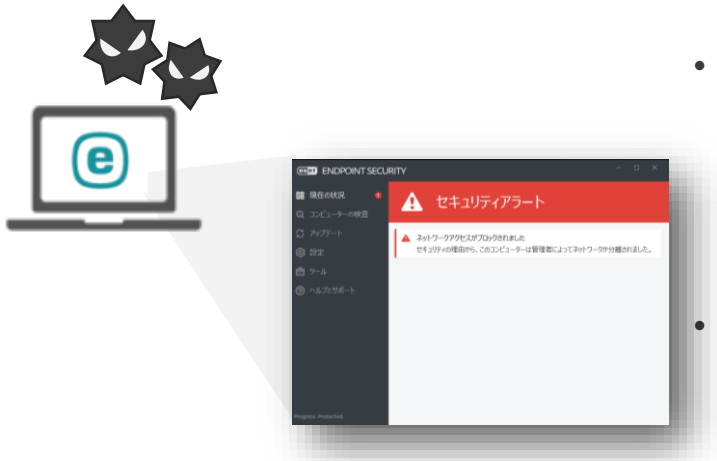
ESET PROTECT MDR Liteとは



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。

ESET PROTECT MDR Liteとは

最短20分での脅威への対応

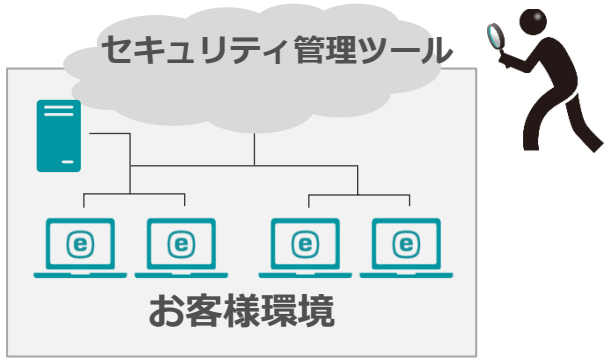


- 脅威が発生した場合、最短20分で初動対応

  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

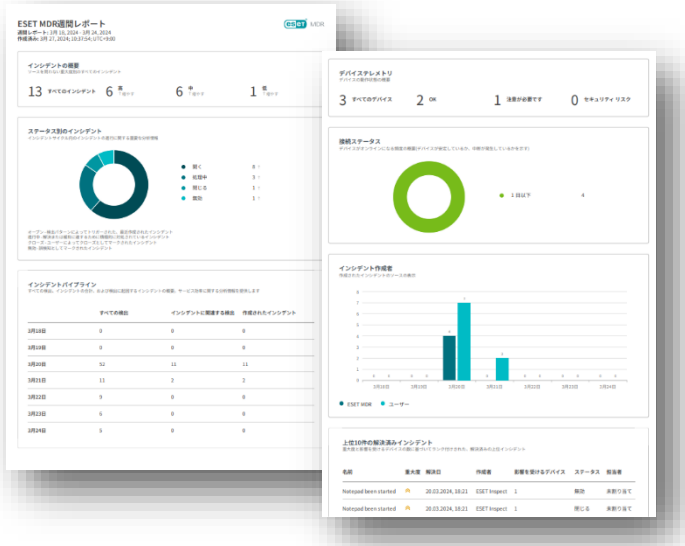


- 24時間365日お客様環境を監視、分析

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

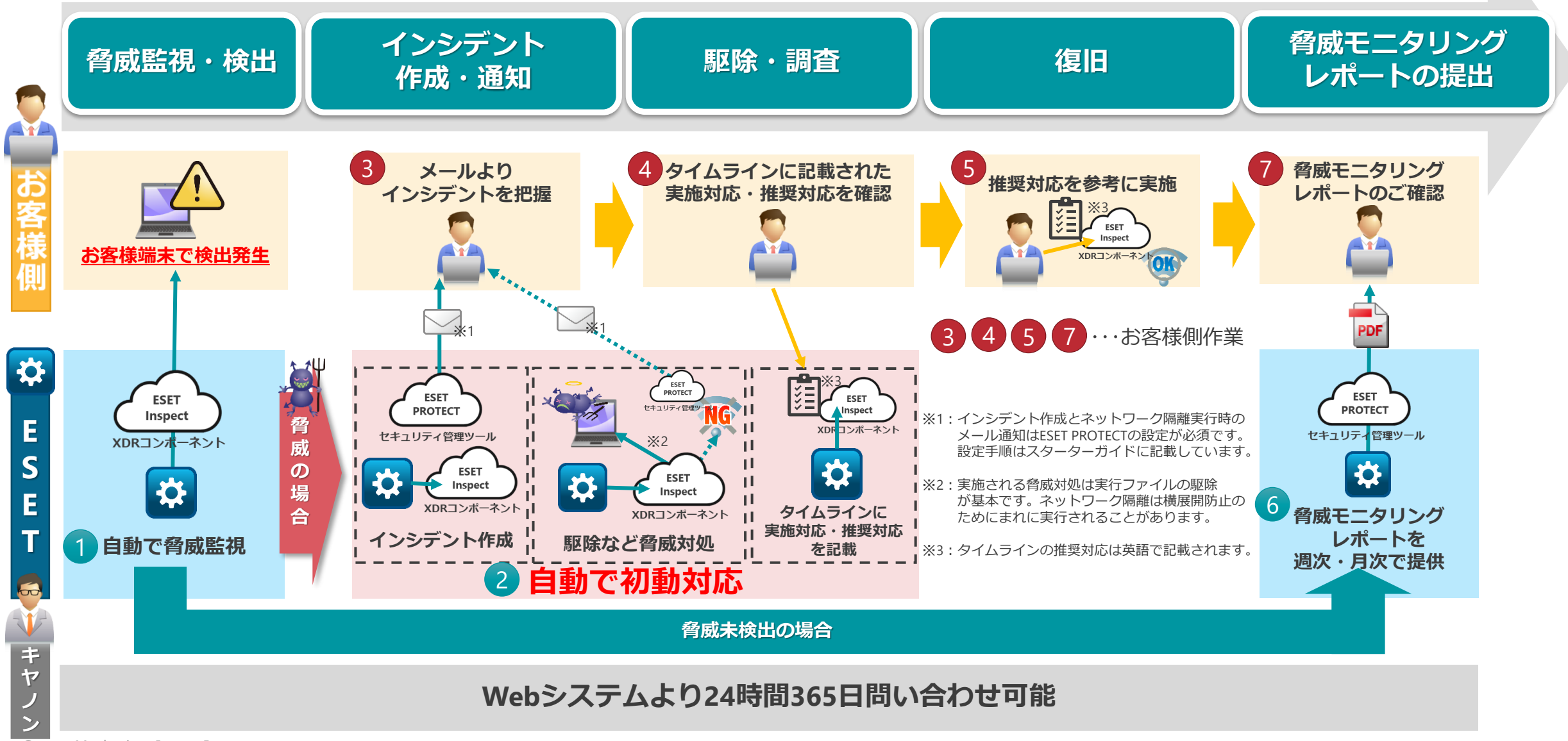
週次/月次でのレポート提供



- 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

- セキュリティ管理
  ツールよりレポート
  ダウンロード可能

インシデント発生時の対応フロー

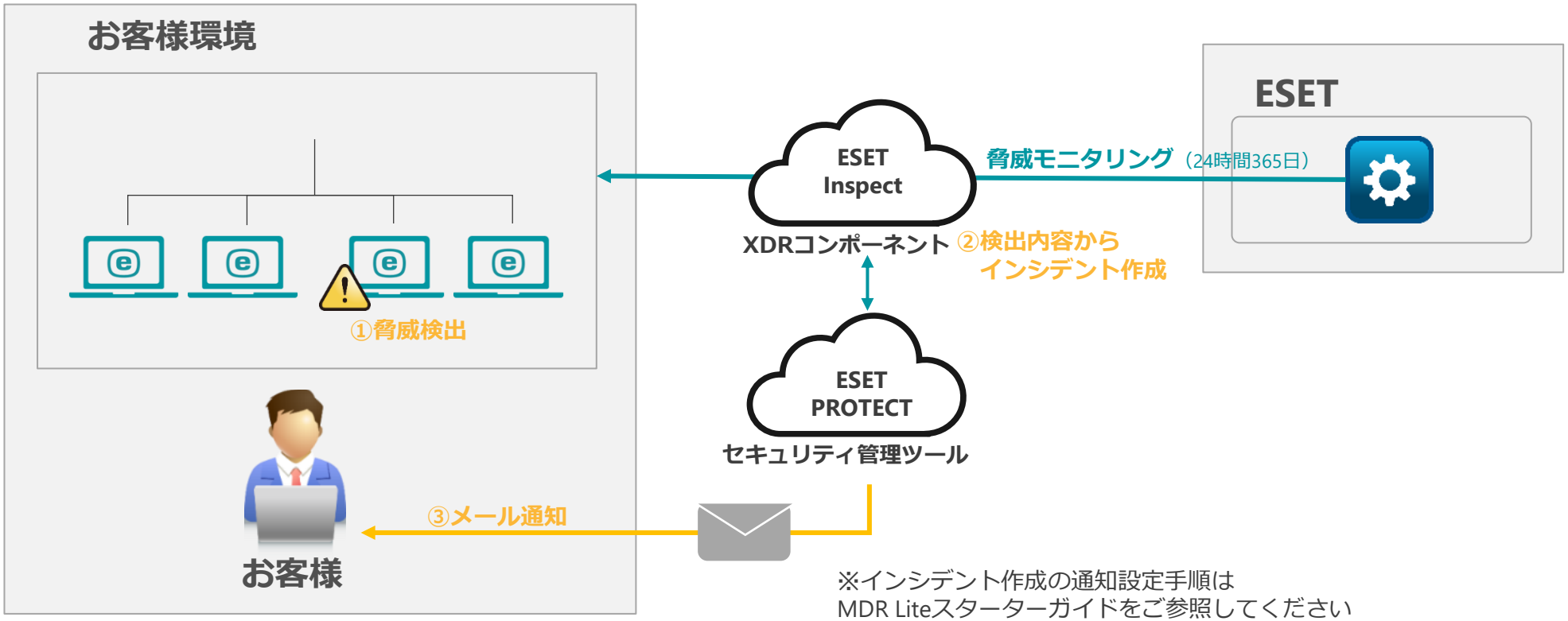


II. インシデント発生時のオペレーション

1．インシデント発生とメール通知

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してください

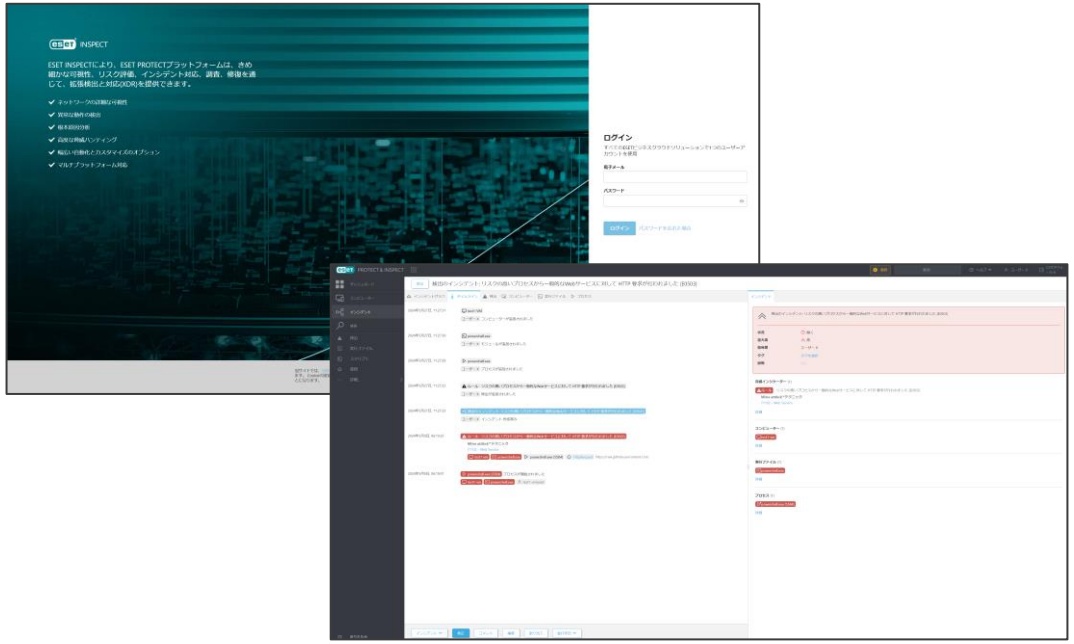
1．インシデント発生とメール通知

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

■ESET Inspectログイン画面



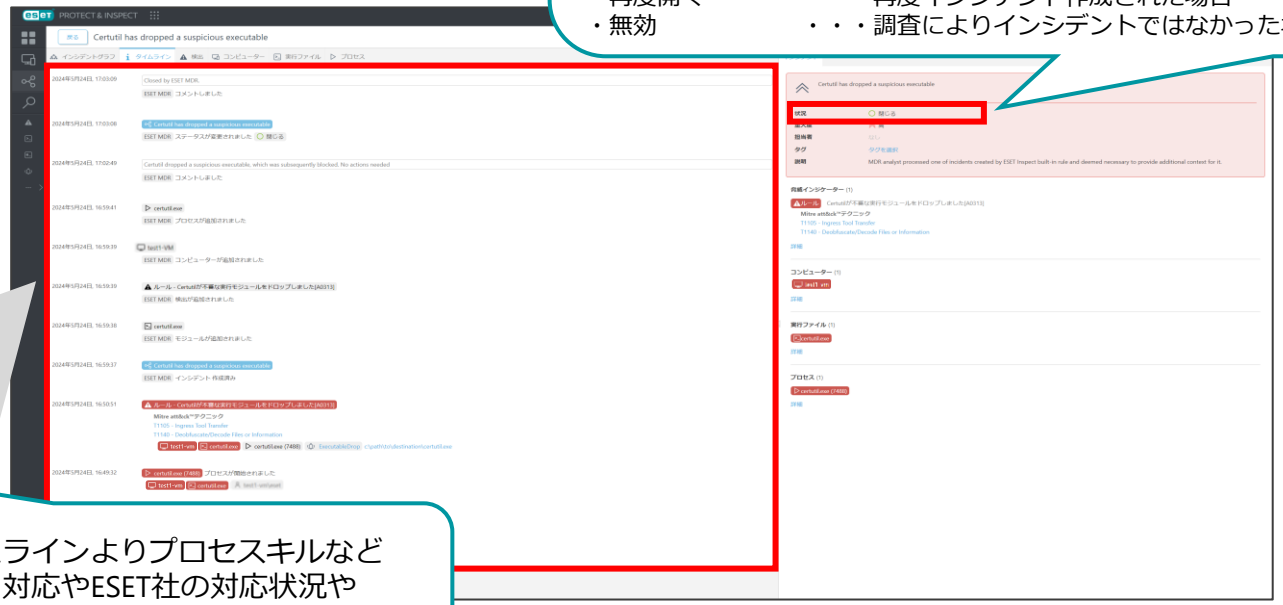
2．インシデント対応状況の確認

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。

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 Inspect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

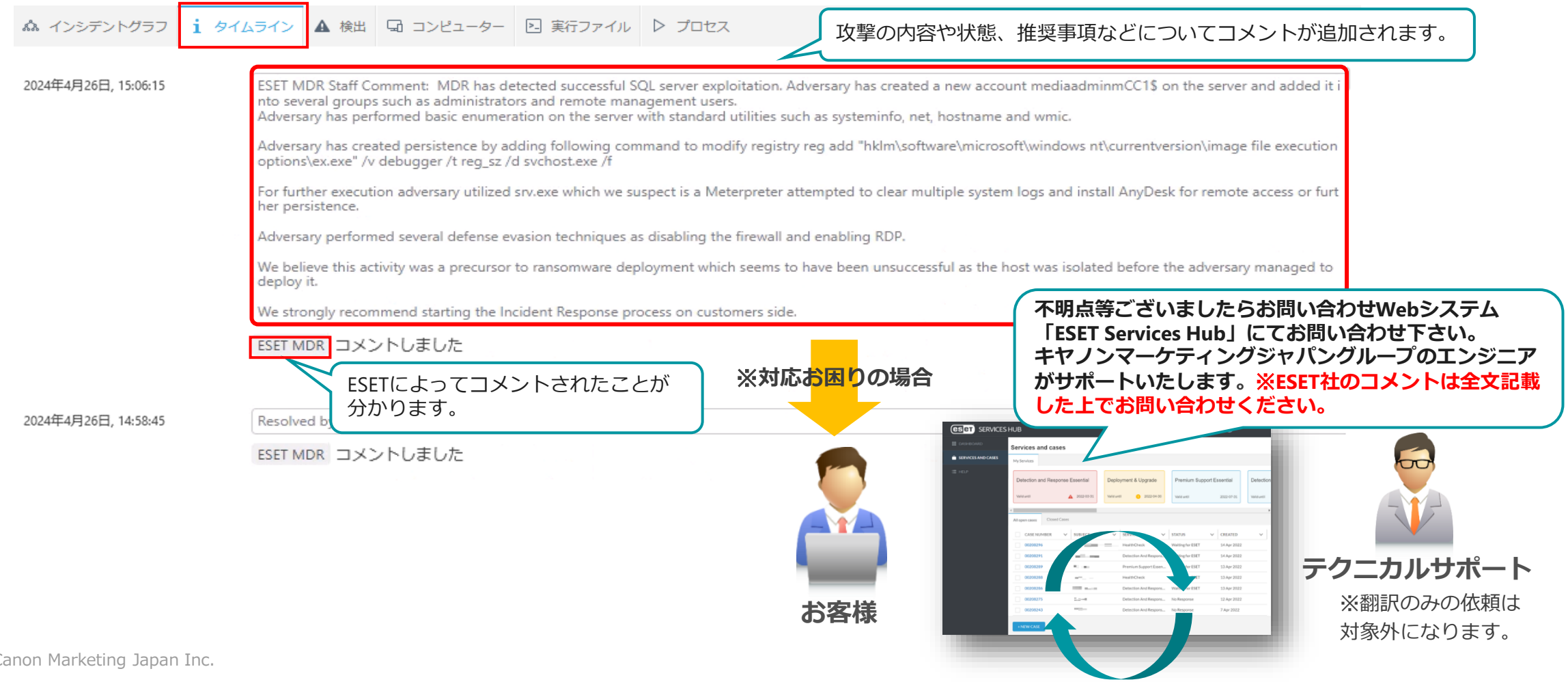
・進行中	・・・インシデント対応中
・保留	・・・インシデント対応保留
・解決	・・・インシデント対応完了
・閉じる	・・・ユーザー影響がないと判断された場合
・再度開く	・・・再度インシデント作成された場合
・無効	・・・調査によりインシデントではなかった場合

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。**



2．インシデント対応状況の確認

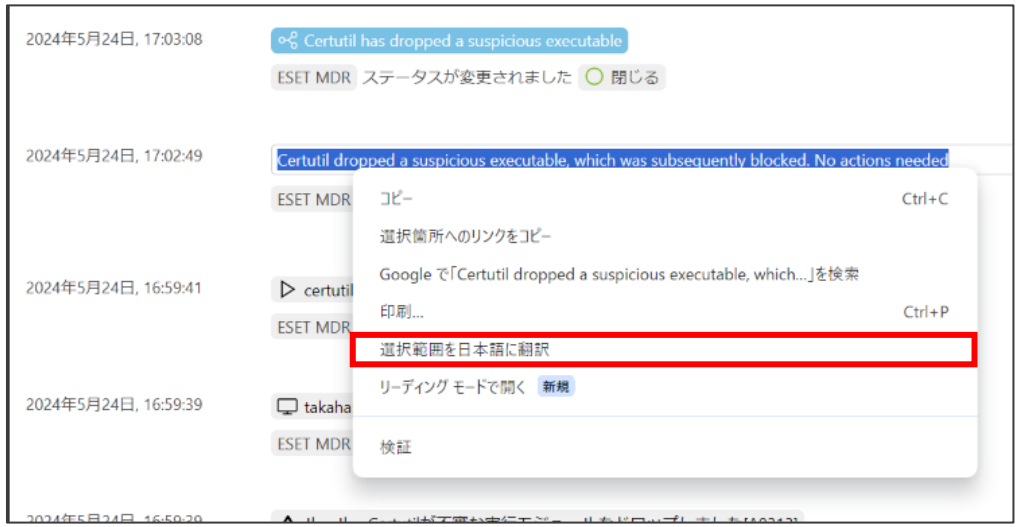
【参考】ESET社のコメント翻訳

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。

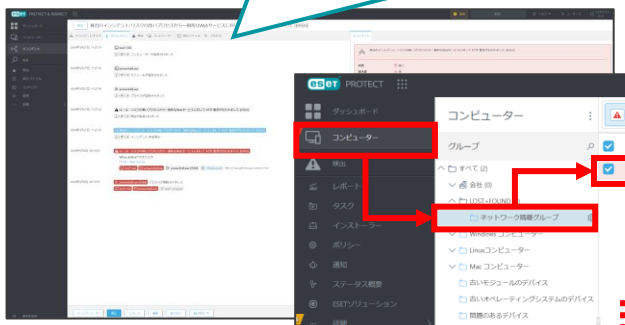
※NW隔離の通知設定を実施いただければ、迅速に隔離された端末を把握することが可能です。設定手順はMDR Liteスターターガイドをご参照ください。

■ネットワーク隔離通知メールサンプル

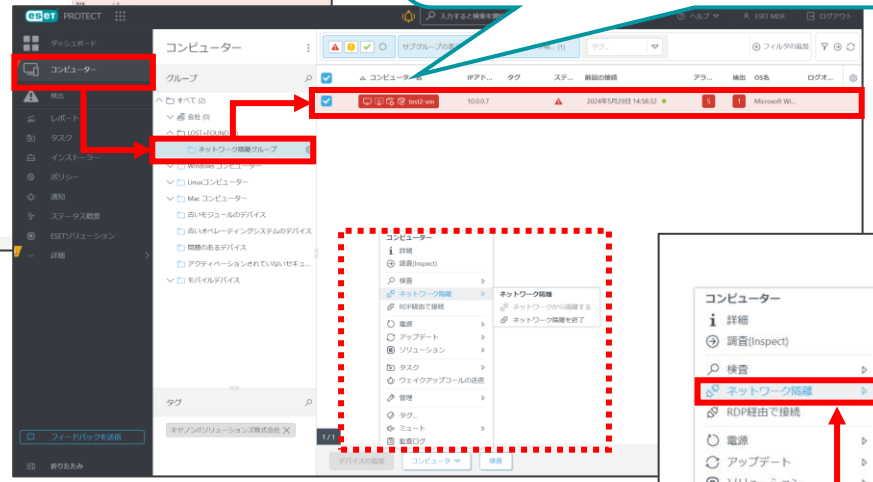
お客様

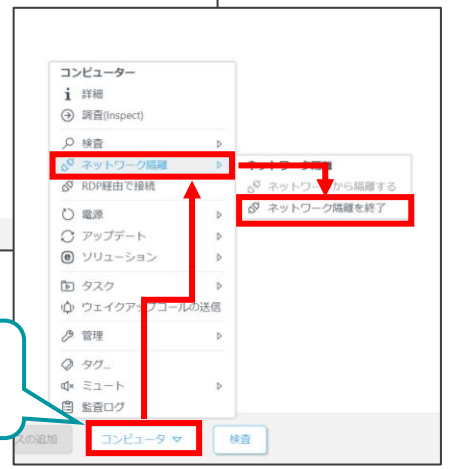
ESET社
初動対応完了後

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。





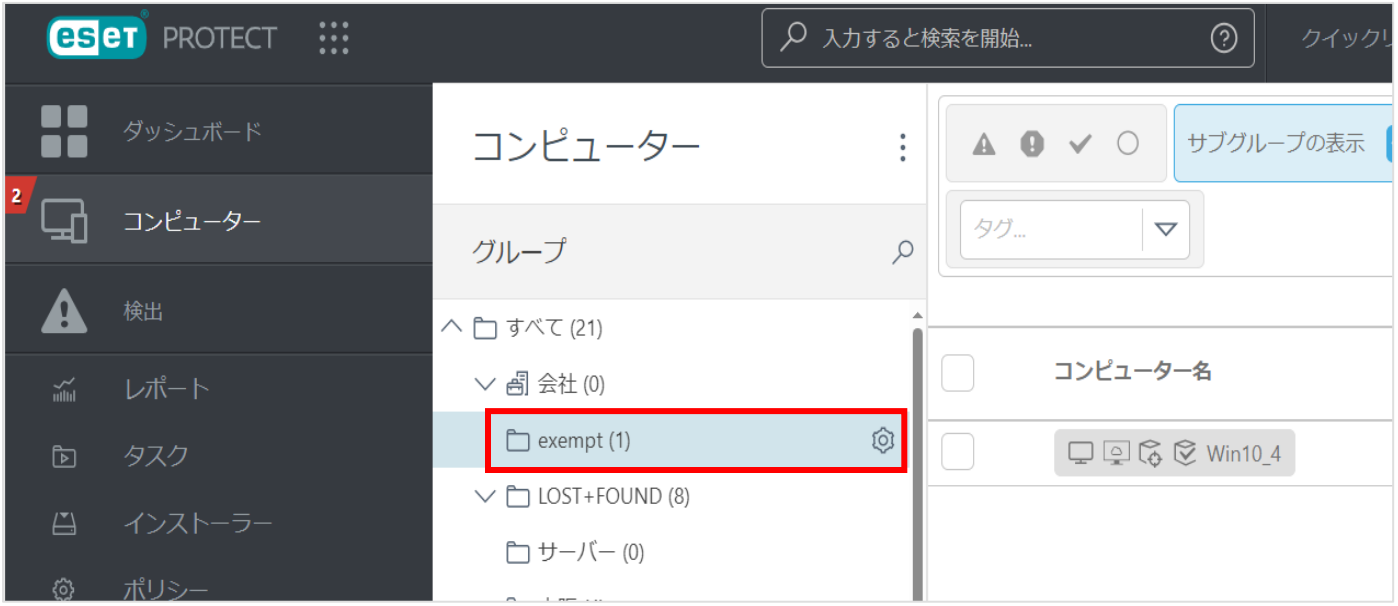
③「コンピュータ」-「ネットワーク隔離」
-「NW隔離を終了」よりNW復旧

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。

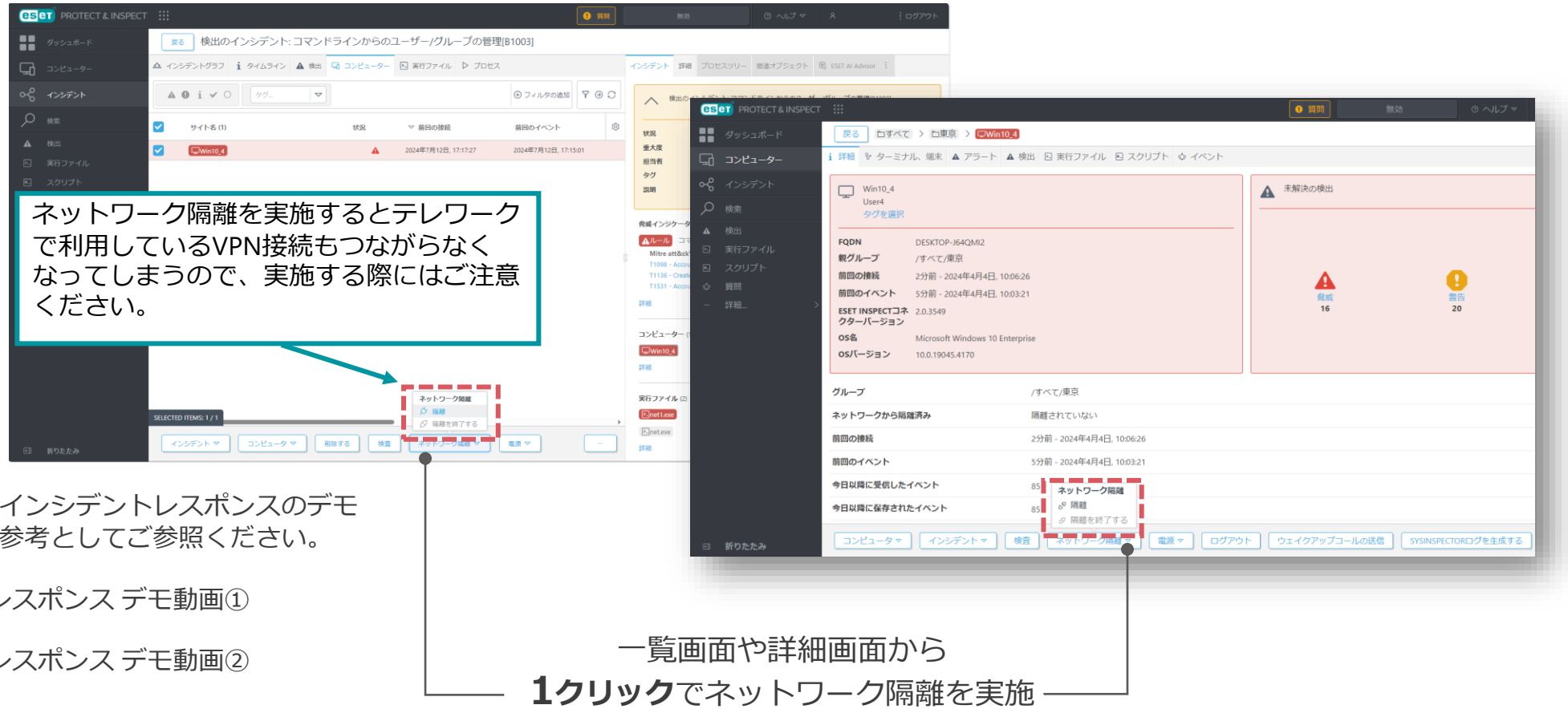
※初動対応から除外するグループの作成方法については、スターターガイドをご参照ください。
※初動対応から除外したクライアントについては、インシデント発生時の対応をお客様にて対処いただく必要がありますので、初動対応から除外するかどうかは慎重にご判断ください。



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

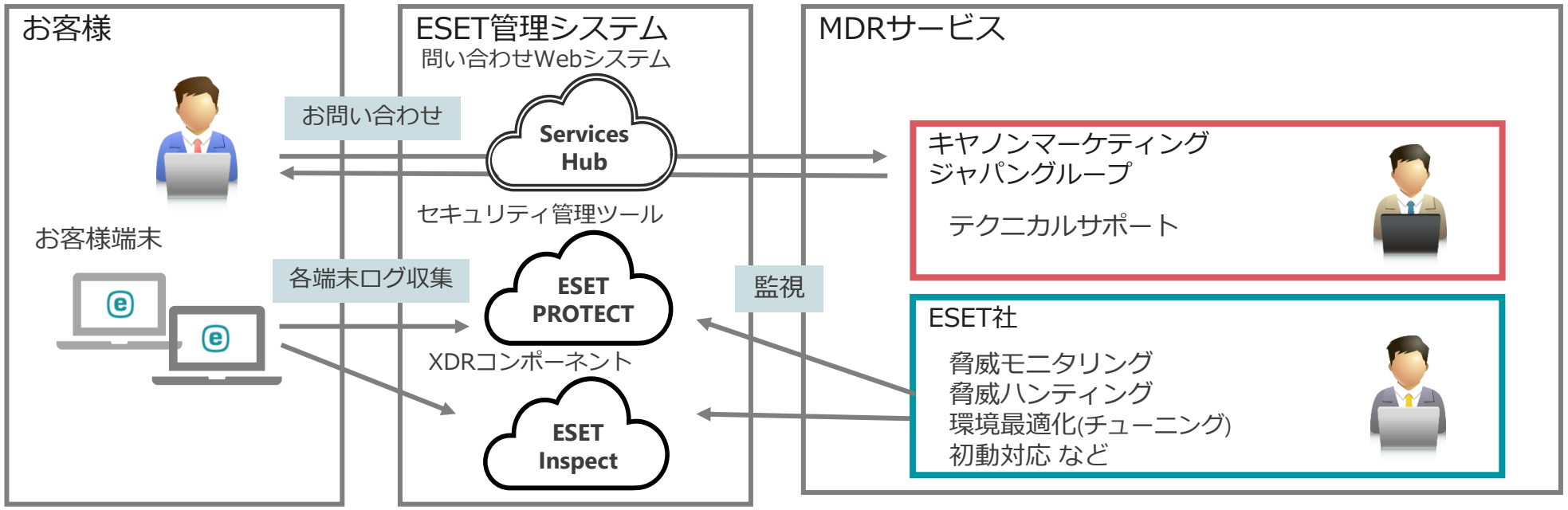


インシデント対応の一例として、インシデントレスポンスのデモ動画がございますので対応の際の参考としてご参照ください。

▼【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

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。