SB Technology

EDRの導入と運用課題を解決する方法

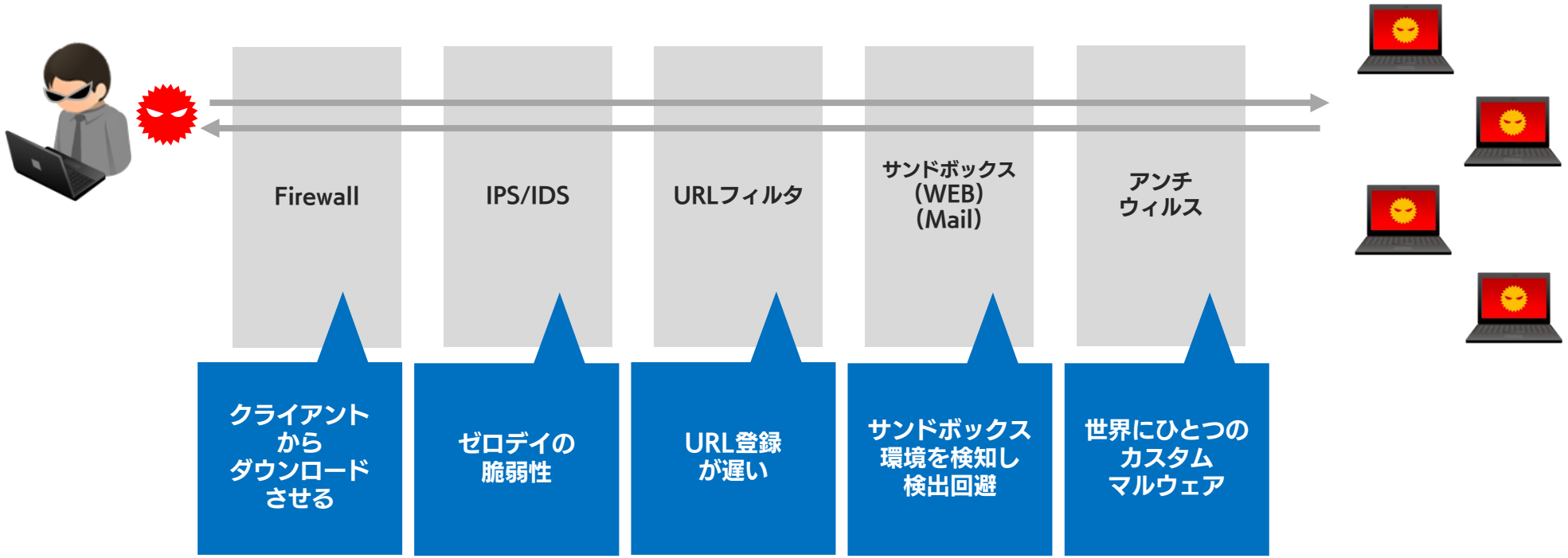
マネージドセキュリティサービスで
できること

SBテクノロジー株式会社

なぜマルウェア感染を防げないのか？

SB Technology

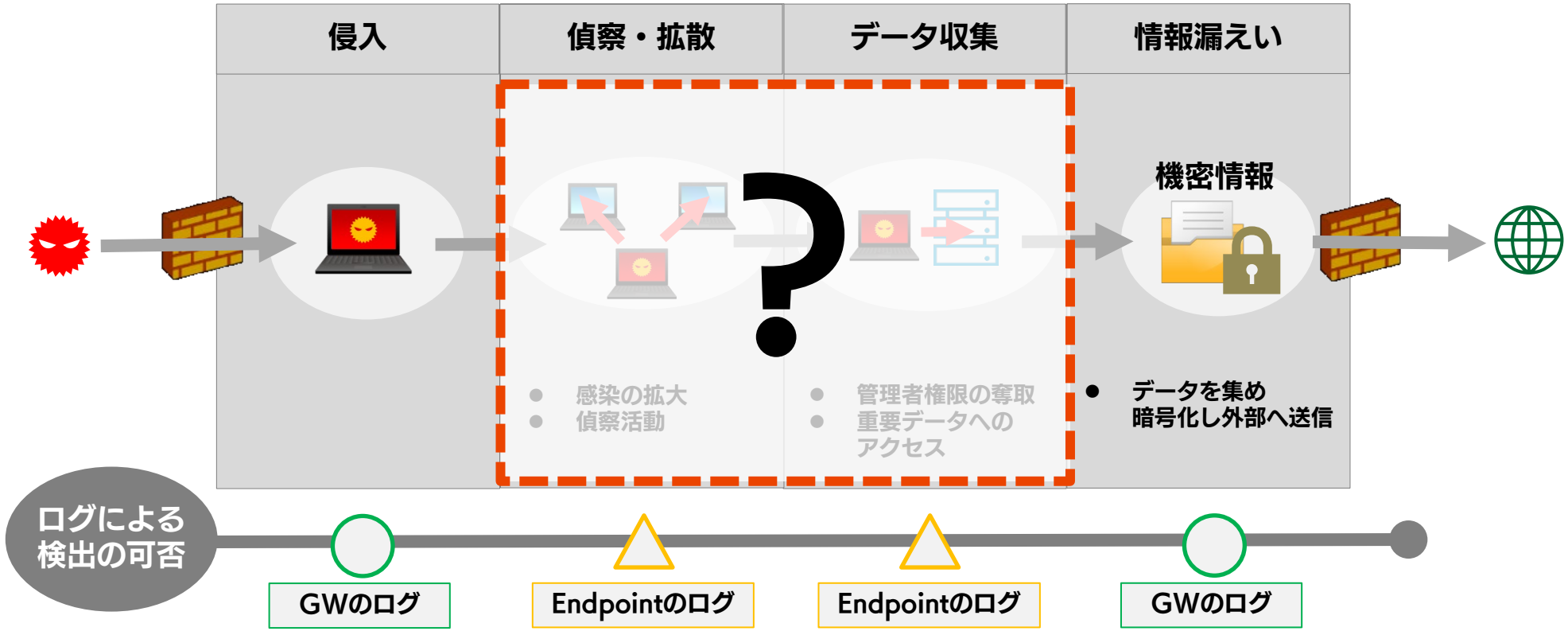
入口・出口の多層防御を回避するテクニック



攻撃者は既存の対策を知り尽くし
防御を回避しながら攻撃を仕掛けてくる

感染後のマルウェアの活動を検知できるのか？

マルウェア侵入後、何が行われていたのか？



断片的なログからの可視化・分析は
検知スピードや人的リソースの問題で限界がある

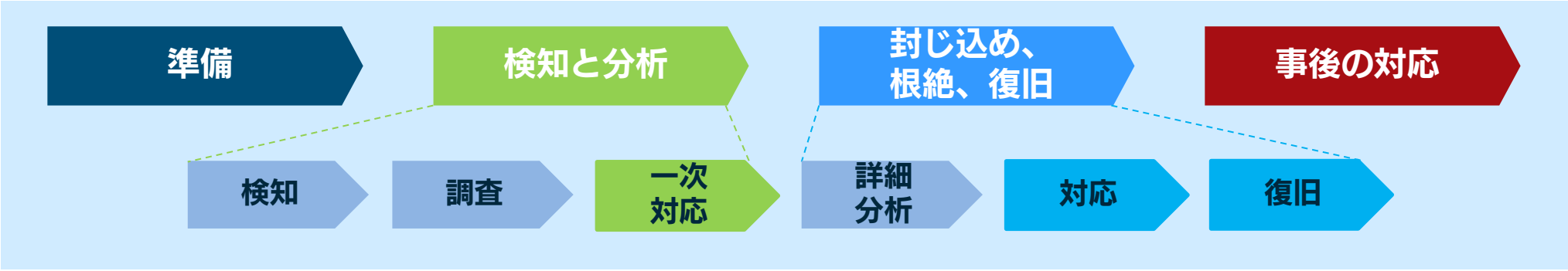
Endpoint Detection and Response(EDR)とは

SB Technology

EDRとは「高度な攻撃による侵入後の活動のリアルタイム検知（Detection）」と「影響範囲と原因を特定し迅速な対応（Response）」を実現し、SOCやCSIRTなどの活動を強力に支援する製品です。

- **[前提]サイバー攻撃に対するインシデント対応の考え方**
  - 不正プログラムの侵入を検知し、感染端末をネットワークから隔離する初動対応の一歩先へ
  - インシデントを収束させるために、侵入経路の特定および他の端末への影響調査が必要
  - 被害拡大/二次被害の回避、再発防止の施策を講じていくことが必要になる

- **EDR(Endpoint Detection and Response)**
  - インシデント対応の迅速化に向けて、エンドポイント端末を監視し、システムのアクティビティを記録するEDR
  - DetectionではIOC（脅威侵入の痕跡を定義したデータ規格）を用いた調査や製品で不審な振る舞いを検知することが可能
  - Responseでは影響範囲の調査、侵害経路等の確認をすることが可能



EDR導入後の課題

SB Technology

EDR製品は、大量のエンドポイントから様々な情報(ログ)を収集します。それらの情報から潜在的な脅威を探したり、過去に起きたインシデントを解析するためには高いスキルが必要となります。そのため、EDR製品は初心者向けのソリューションというよりは、プライベートSOCチームやインシデントレスポンスチームなど向けのソリューションであり、ある程度の知識・スキルが求められます。

EDR製品が収集する情報の一例

- **プロセス情報**
  プロセス種別, プロセス名, 階層, ネットワーク, URL, DNSリクエスト, 権限, security context, thread activity, インジェクション, memory forensics, section mismatch and more…
- **接続情報**
  IP/Port quintuple, 受信/送信バイト, DNS, URL, ARPテーブル, custom resolvers など
- **ファイル情報**
  Path, ファイル属性, ファイルサイズ, ハッシュ, 署名 (Authenticode), 作成・更新日時, バージョン, reputation information, loaded by… (Right now PE loading only, full file access coming)
- **ドライバ情報**
  名前, 全ファイル情報, デバイス/ドライバーオブジェクト (future)
- **オートラン**
  レジストリ, サービス, COMなど…
- **マシン**
  マシン名, OS バージョン, プラットフォームアーキテクチャ, タイムゾーン, ネットワーク構成/IP.
- **ユーザ情報**
  ユーザ名, ドメインログオンタイム, ドメイン, パスワード歴, 権限. セッション/WinStation/デスクトップ (used for PtT/PtH)

本当に攻撃だったのか、影響範囲はどれくらいなのか判断できますか？

これらの情報から潜在的な脅威を探せますか？

MSS for EDR とは

弊社セキュリティ監視センターから、 お客様環境のEDR製品を24時間365日体制でセキュリティアナリストが監視を行うサービスです。ログや検知したセキュリティアラートに対し、過検知の有無、影響度を判断し、考えられる被害、また、それに対する対策案まで含めてご担当者様へ通知します。

EDR製品

TREND MICRO Apex One XDR

Microsoft Defender for Endpoint

CROWDSTRIKE

Cybereason EDR

- 悪意あるふるまいを検知
- プロセスの抑制
- PCのログを集約

×

マネージドセキュリティサービス（MSS）

- 24時間365日　常時監視体制
- セキュリティの専門性

✓セキュリティ製品の知識
✓攻撃手法・脆弱性に関する知識・情報
✓ログ分析、解析のノウハウ

MSS for EDRの特徴

クイック レスポンス	EDR製品が検出し、アナリストが危険と判断した場合、製品の機能を用いて一次対処します。 ・ 不審なプロセスの停止 ・ 感染したエンドポイントのネットワーク隔離
オンデマンド リサーチ	お客様からのお問合せ（他セキュリティシステムで検出した気になる事象など）を起点にして、 EDR製品でエンドポイントの状況確認を行いご報告します。
プロアクティブ コントロール	一連の解析・隔離に加え、弊社MSS契約監視対象で関連インシデントの分析および不正な活動の抑制作業を実施します。 ※ 別途、他監視対象のMSS契約が必要です
グローバル 監視センター	海外拠点を持つお客様向けに当社の海外SOCから英語で分析・対処を行います。必要に応じて日本のSOCと連携して対応いたします。 ※ オプションとなります。

クイックレスポンス

SB Technology

セキュリティ監視センター

Managed Security Service

- お客様へのご連絡
- インシデント抑制

オペレーター

- アラート内容解析
- 影響度分析
- 影響範囲確認

アナリスト

これはお客様には影響がないアラートだ

影響が出ている端末は3台だ

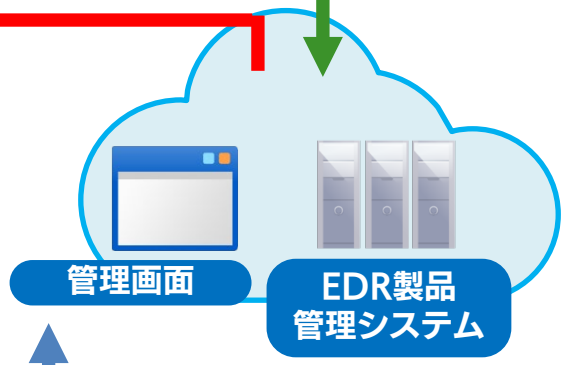
一次対処として、このプロセスを停止しよう

お客様にこの対策をお願いしよう

インシデント報告

インシデント抑制設定

アラート受信



専門家による運用支援

EDR製品を使う上で一番難しいアラート内容の解析、お客様にとっての影響度判断をセキュリティの専門家が実施し、インシデントに対する適切な対処を24時間365日支援します。

お客様
ご担当者様

影響範囲も、対策も分かった。一次対処も実施してもらっているので、恒久対策を実施しよう！

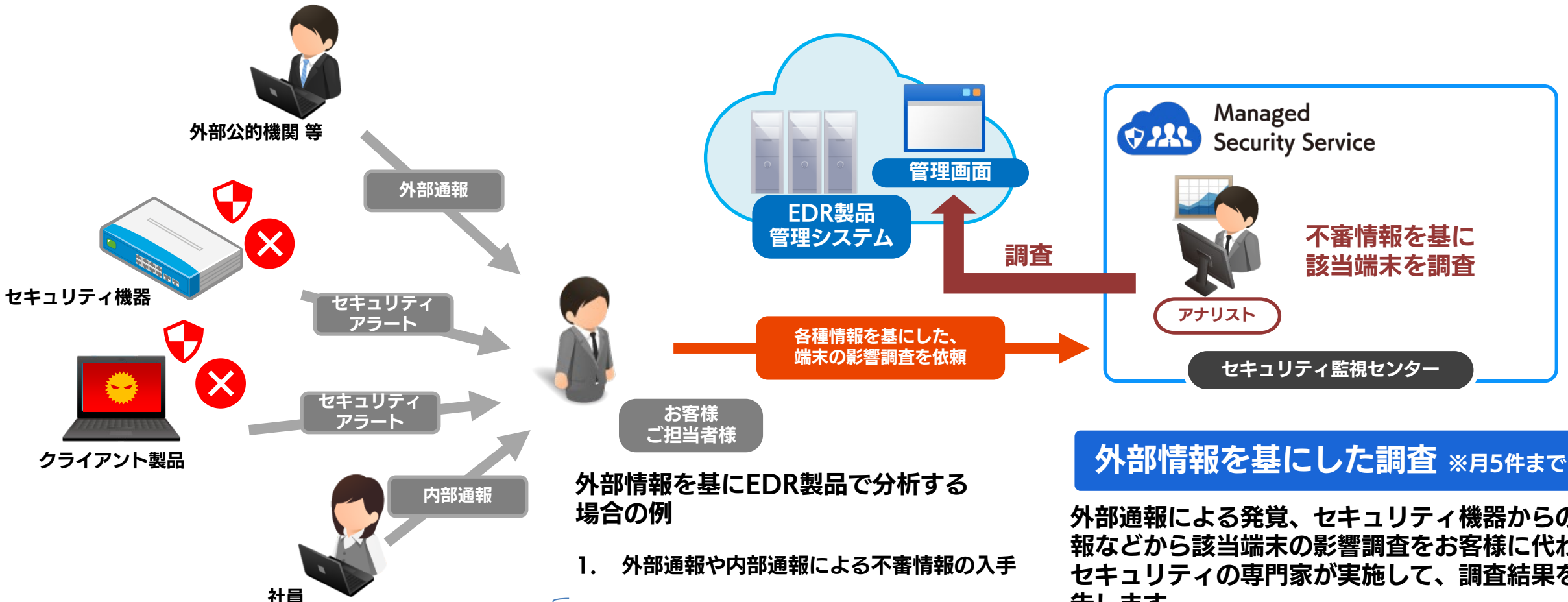
EDR製品からのアラート受領時の対応例

1. 製品からアラート発報
2. 製品の管理画面でアラート内容の確認
3. 製品の管理画面で詳細調査
4. 製品の機能で一次対処(ネットワーク隔離など)
5. 他端末への影響調査および一次対処

Managed Security Service

※フォレンジックなどの本格調査・復旧作業は別サービスとなります。

オンデマンドリサーチ



外部情報を基にEDR製品で分析する場合の例

1. 外部通報や内部通報による不審情報の入手
2. 製品の管理画面でアラート有無の確認
3. 製品の管理画面で詳細調査
4. 調査結果に基づく対処

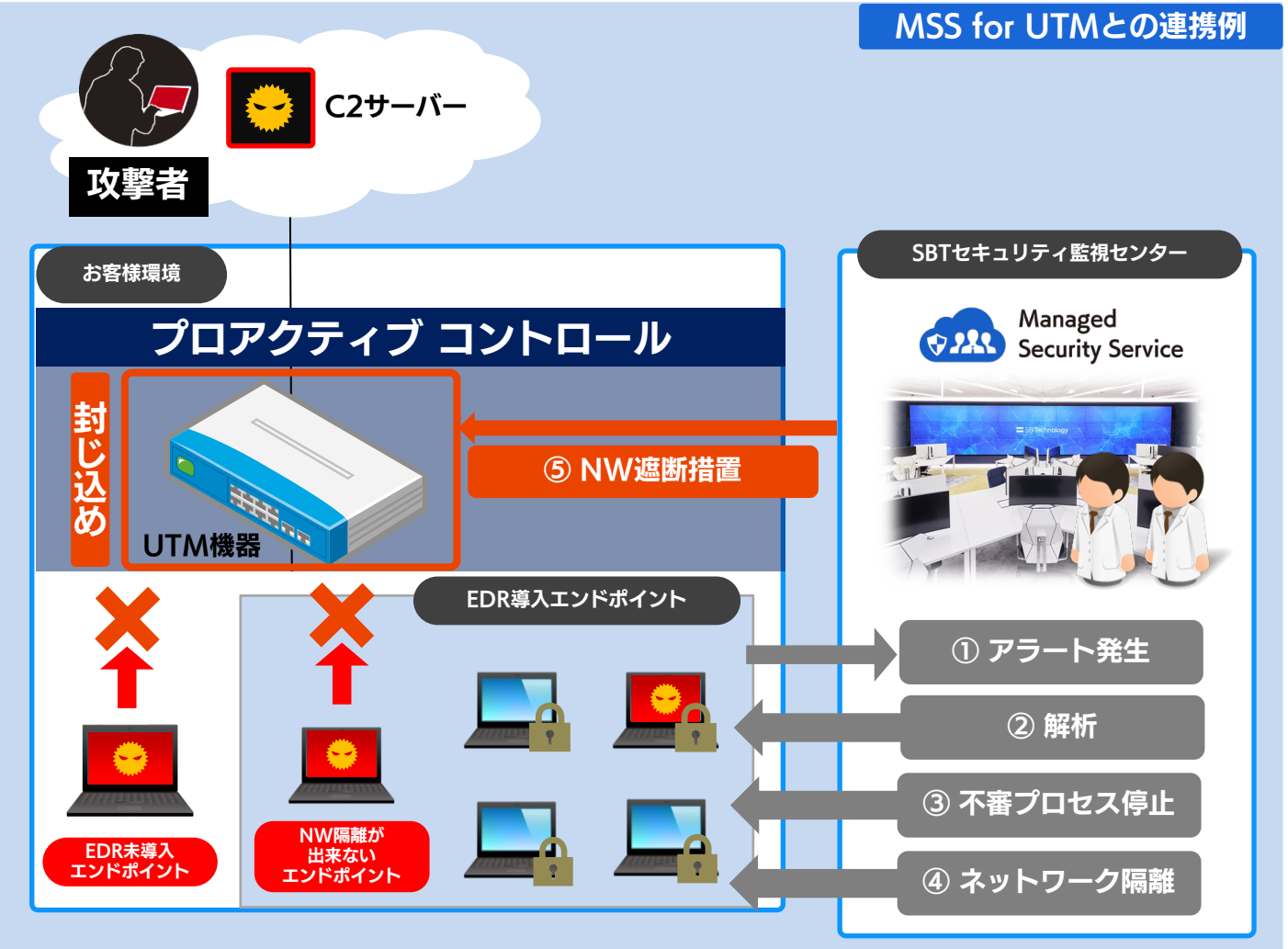
外部情報を基にした調査 ※月5件まで

外部通報による発覚、セキュリティ機器からの通報などから該当端末の影響調査をお客様に代わりセキュリティの専門家が実施して、調査結果を報告します。

調査範囲：監視対象に記録されているアラート・ログ

プロアクティブ コントロール

インシデント発生時、弊社MSS契約監視対象で関連インシデントの分析および不正な活動の抑制作業を実施します。
※別途、他監視対象のMSS契約が必要です。



拡散・拡大を阻止

攻撃者に乗っ取られた端末から外部への情報漏えいに対しネットワークの出入り口を封じることにより、EDR製品がインストールされていない端末の不正な活動を抑制することが可能です。
また、EDR導入端末の他端末に対する侵害試行のログ・アラートからEDR未導入端末の侵害を検知することが可能です。

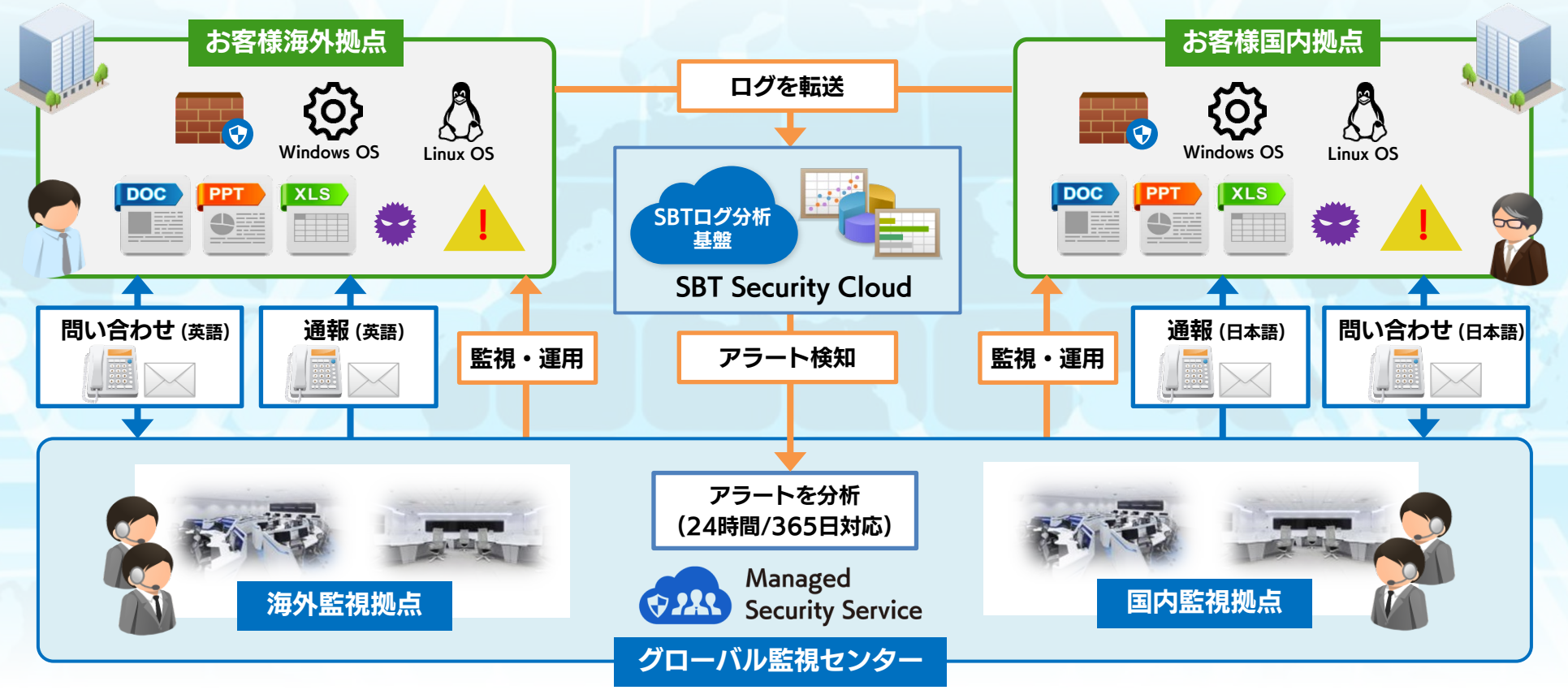
お客様負担の軽減

従来、インシデント報告を受領したお客さまにて速やかに実施することが求められていた初動対応である「封じ込め」を、弊社が迅速に実施することで、お客さま作業負担を大幅に軽減し、休日や夜間などの業務時間外における対応の遅れも回避できます。

英語対応も可能なグローバル監視センター(オプション)

対応サービス　セキュリティオペレーションセンター（SOC）
ネットワークオペレーションセンター（NOC）
Microsoft 365ヘルプデスク

対応言語　日本語・英語（その他言語については順次対応予定）



インシデントレベルに応じた通知

アラートは全件通知ではなく、影響度の高いもののみご連絡するため、お客様はシステムへの対処など必要な対応に専念することができます。

インシデントレベル 判断基準例※

※個々のサービスによって
下記とレベルが異なるものがございます

危険

安全

レベル4 複数の保護対象にまたがる不正な活動を確認した場合

レベル3 単一の保護対象で不正な活動を確認した場合

電話・メールで通知

レベル2 不正な活動の可能性があるが、判断にお客様への確認が必要な挙動を確認した場合

メールで通知

通知対象

レベル1 不正な活動かの判断に経過観察が必要な場合

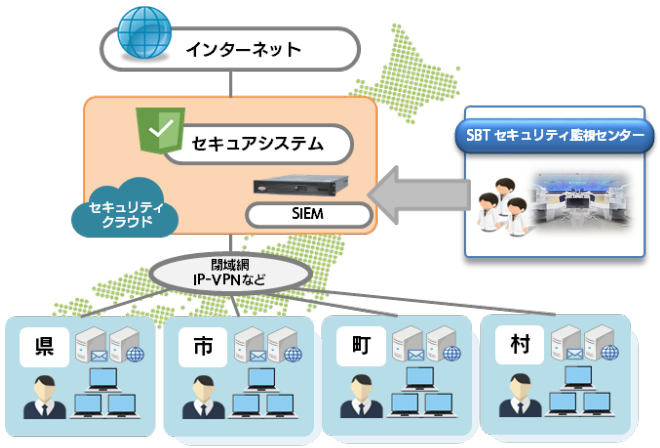
レベル0 通常の挙動

2022年自治体情報セキュリティクラウドにおける実績

SB Technology

自治体情報セキュリティクラウドとは

現在各市区町村が個別に設置しているWebサーバー等の監視対象を都道府県と市区町村が協力して集約し、監視およびログ分析・解析をはじめ高度なセキュリティ対策を実施するものです。



SBTの実績

12県
プライムベンダーとして機器調達、構築、運用の全てを獲得した件数

405団体
4県の情報セキュリティクラウドを利用する県庁含む自治体の数

約30万人
4県の情報セキュリティクラウドを利用する推定利用者の数

12県全てで、開発からSOC運用までを「弊社のみ」で完結

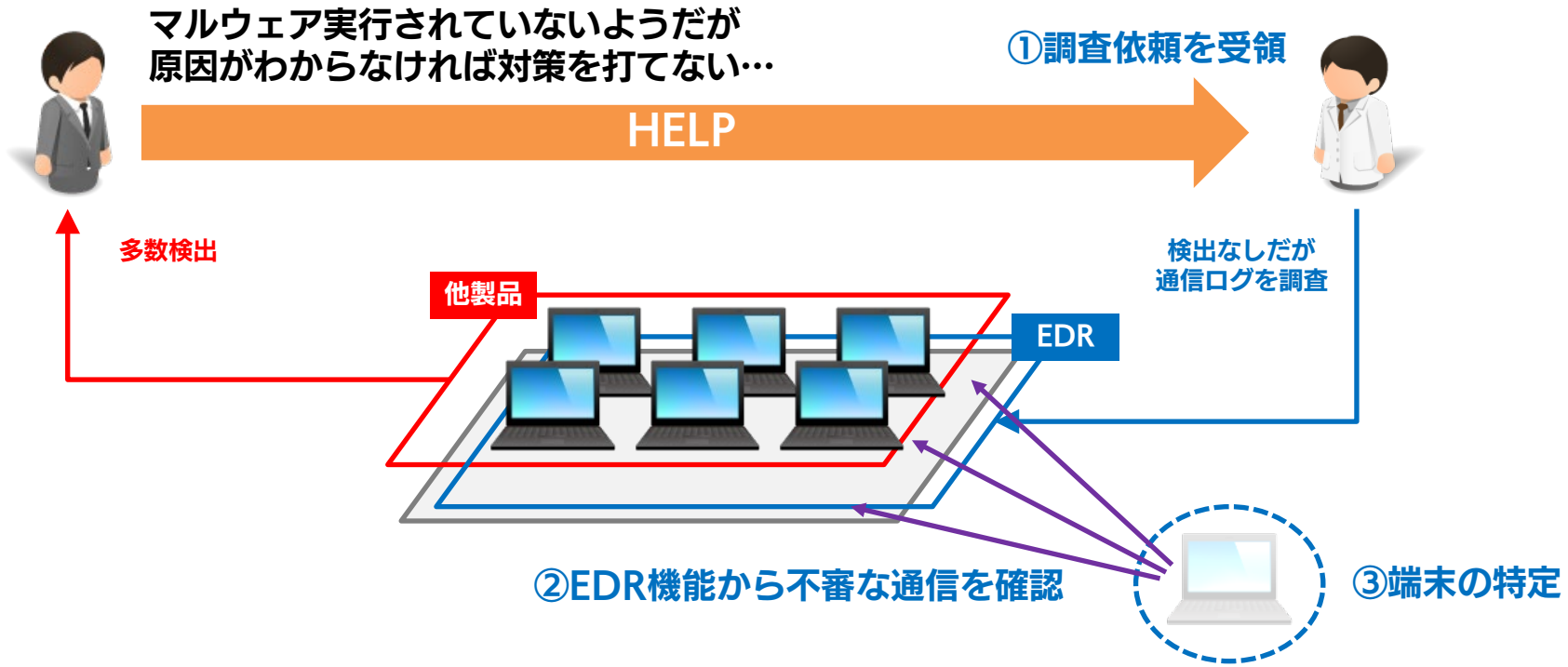
各セキュリティクラウドに導入したFirewall、IPS/IDS、WAF、Sandbox、ウイルス対策、EDRなどのセキュリティ対策機器や、Web、Proxy、DNS、MailRelayなど各種サーバー群も含め、弊社でSIEMを用いた統合的な相関分析を行っています。

この大規模セキュリティ運用で得られる国内攻撃傾向や、最新脅威情報などを他のお客様のセキュリティ監視にも活用

MSS 事例紹介

マルウェア感染発覚後の追加調査で感染元を特定し対処したケース

SBT MSS for EDRをご契約いただいたお客様において、多数のマルウェア検出が他製品で確認されご相談いただきました。マルウェアの実行は他製品によって防止されていたためにEDR製品による検出は確認できませんでしたが、マルウェア感染の原因を調査するためにEDR機能を利用し、感染元端末を特定、早期に業務復旧できるよう貢献しております。



MSS 事例紹介

SB Technology

マルウェア感染発覚後の追加調査で感染元を特定し対処したケース

当時のお客様の課題

複数の端末を監視している他製品にて同時期に不審なファイルを駆除したことが確認されましたが、感染経路が不明。
内部ネットワークにてマルウェアの拡散（Lateral Movement）が発生している可能性を懸念され、業務復旧は困難でした。

もしMSS契約がない場合は、
詳細な調査を長期間
実施しなければならないケースも…

✕ **業務復旧までに時間がかかる**
詳細調査費用の発生

MSS for EDRをご契約済みだったため
調査依頼を行うことができた

○ **業務復旧までの時間短縮**
追加費用の発生なし

MSSでの対応

EDRを利用して感染原因の調査を実施。不審ファイルが確認された複数の端末に対して、別の1台の端末からPort 135(Remote Procedure Call)宛の通信が発生していることを確認できたためお客様へご報告した。
結果としてPort 135宛通信を発生させていた端末はマルウェアに感染していたことが確認でき、適切に処理いただいて業務復旧を早期に実現できた。

まとめ

SB Technology

EDRとは「高度な攻撃による侵入後の活動のリアルタイム検知（Detection）」と「影響範囲と原因を特定し迅速な対応（Response）」を実現し、**脅威の侵入後の活動を早期に補足・対処する製品**です。

EDRでの検知は攻撃者が侵入成功しているため、**影響範囲を特定する専門知識を持つ人材と24時間の監視・対処まで行う体制が必要**なため、信頼できるMSSを選ぶ必要があります。

既存のセキュリティ機器や今後導入を予定しているセキュリティ対策も見据えて、**MSSを段階的に追加していくことで相関分析を行い**正確な検出と早期対処が行えます。

マネージドセキュリティサービス ラインアップ

SB Technology

多数のセキュリティデバイスに対応したマネージドセキュリティサービスをご用意しています。
EDR の各製品別詳細資料や、他のラインアップにもご興味がありましたら、ぜひご連絡ください。

Managed Security Service

＜対応製品＞

Microsoft
Defender for Endpoint

Cybereason EDR

TREND MICRO
Apex One XDR

CROWDSTRIKE
CrowdStrike Falcon

Microsoft 365 E5 Security
MSS for Microsoft 365

エンドポイントセキュリティ
MSS for EDR

クラウドネットワークセキュリティ
MSS for iboss Cloud Security

クラウドセキュリティ
MSS for CASB (McAfee MVISION Cloud)

Webアクセスセキュリティ
MSS for Secure Gateway (Zscaler)

Webサイトセキュリティ
MSS for Imperva Incapsula

サーバーセキュリティ
MSS for Trend Micro Deep Security

ゲートウェイセキュリティ
MSS for UTM (FortiGate / Palo Alto)

内部ネットワークセキュリティ（サンドボックス）
MSS for Trend Micro DDI

統合ログ分析セキュリティ
MSS for Microsoft Sentinel

SBテクノロジー株式会社

■ お問い合わせ先　https://inquiry.softbanktech.co.jp/public/application/add/505