Managed Security Service

SB Technology

MSS for EDR 紹介資料

SBテクノロジー株式会社

マネージドセキュリティサービス（MSS）ラインナップ

SB Technology

当社セキュリティ専門アナリストによる24時間365日のセキュリティ監視サービス

Managed Security Service

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

IDセキュリティ
MSS for Microsoft 365

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

エンドポイントセキュリティ
MSS for EDR
(Trend Micro Apex One / Cybereason / Microsoft Defender ATP)

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

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

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

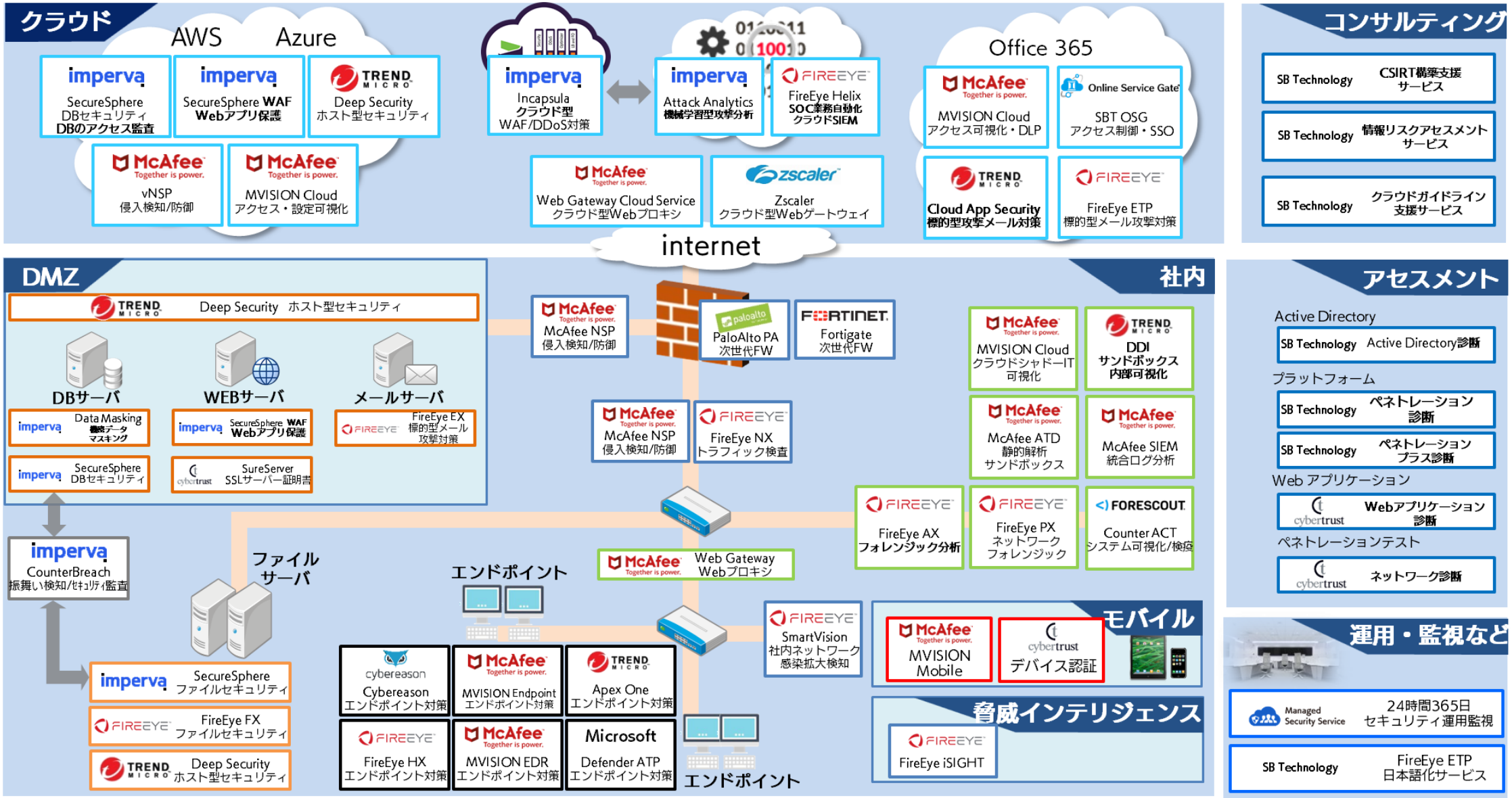
クラウドセキュリティ
MSS for CASB (McAfee MVISION Cloud)

Eメールセキュリティ
MSS for FireEye ETP

統合ログ分析セキュリティ
MSS for SIEM (McAfee SIEM)

SBT セキュリティソリューションマップ

SB Technology



当社MSS 4つの強み

SB Technology

- 自治体情報セキュリティクラウドにおける実績
- セキュリティ対応の専門チームとの連携
- セキュリティ監視(SOC)とシステム監視(NOC)のワンストップ提供
- 英語対応も可能なグローバル監視センター

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。

4県

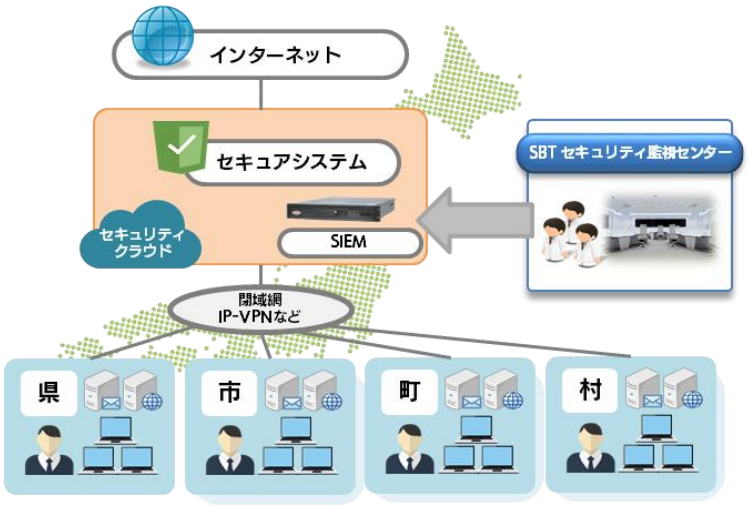
プライムベンダーとして
機器調達、構築、運用の
全てを獲得した件数

121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

11万人

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



4県全てにおいて開発からSOC運用まで弊社のみで完結

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など各種サーバ群も含めて、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活かします。

セキュリティ対応の専門チームとの連携

SB Technology

「セキュリティポリシー策定」「監視・分析」「調査・研究」「オンサイト対応」の各専門チームが連携してお客様のセキュリティ運用を支援します。

セキュリティ監視センター

お客様先の監視対象デバイスからの情報だけではなく、脅威情報調査室から共有される最新情報も活かして分析業務にあたる。
悪性なIPアドレス、Webサイトなどが判明した場合には、事前にブロック処理をするなど、プロアクティブに対応する。

連携

導入

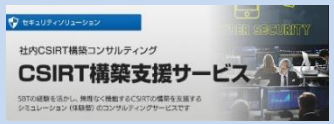
緊急対応

脅威情報調査室

独自ハニーポッドの運営や外部活動などから最新の脆弱性情報・脅威情報の収集や、攻撃手法の研究などを行うリサーチセンター。
弊社Webサイトへの脆弱性情報の公開なども行う。

コンサルティングチーム

お客様のセキュリティ対策状況を可視化し、課題を見極めたうえでCSIRTなどセキュリティ体制の構築支援やインシデント発生時の対応フローの整備を行う。



インシデントレスポンスチーム

重大なセキュリティ事故が発生した際に、被害を最小限に留めつつ事業を継続させるための復旧対応支援や、各種原因調査を行う緊急対応チーム。

セキュリティ監視とシステム監視のワンストップ提供

SB Technology

SOC（セキュリティ監視）だけでなく、NOC（システム監視）も自社完備！
MSSで検知した脅威に対する対応もワンストップで提供します。

ソフトバンク・テクノロジー　マネージド・サービス

お客様
ご担当者様

カスタマポータル

お客様専用
Webポータル

- ✓ 対応状況
- ✓ 履歴管理
- ✓ 情報提供

ネットワークオペレーションセンター

インフラ・ネットワークに関する
作業を行なうエンジニア集団

- ✓ システム基盤の運用監視
- ✓ インシデント発生時の一次対応
- ✓ 恒久対策の実施

セキュリティ監視センター

高度な情報セキュリティ対策に関
する知識を有するアナリスト集団

- ✓ セキュリティ運用監視
- ✓ インシデント対応時の指示
- ✓ 恒久対策の検討

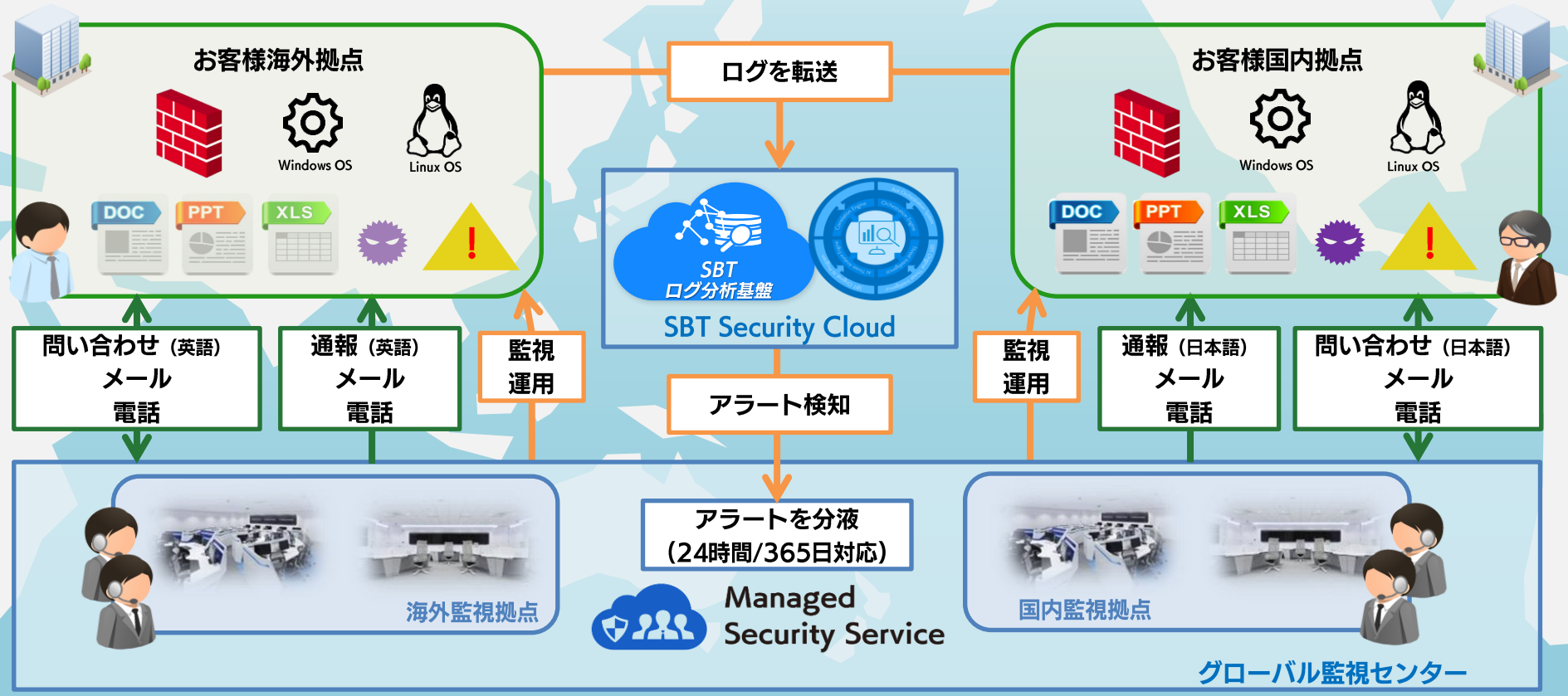
※ご契約内容によってご利用いただける範囲が異なります。
※SOCとNOCは各々ご契約が必要となります。

英語対応も可能なグローバル監視センター

SB Technology

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）

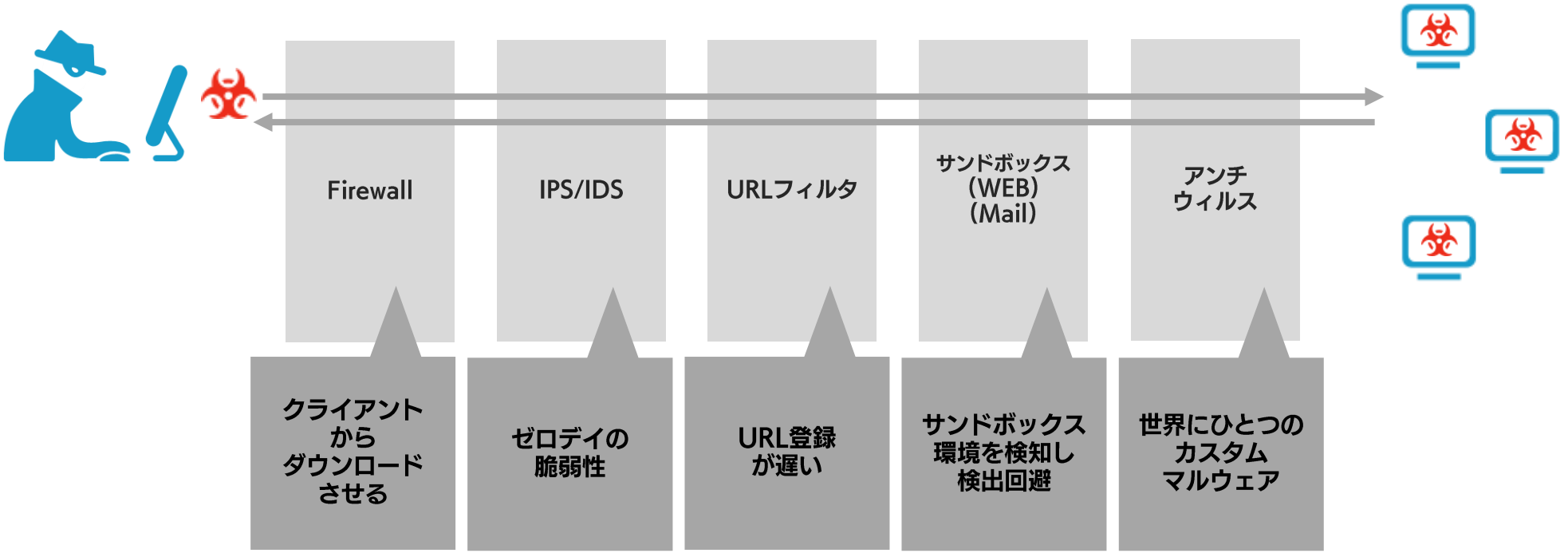


MSS for EDR サービス内容

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

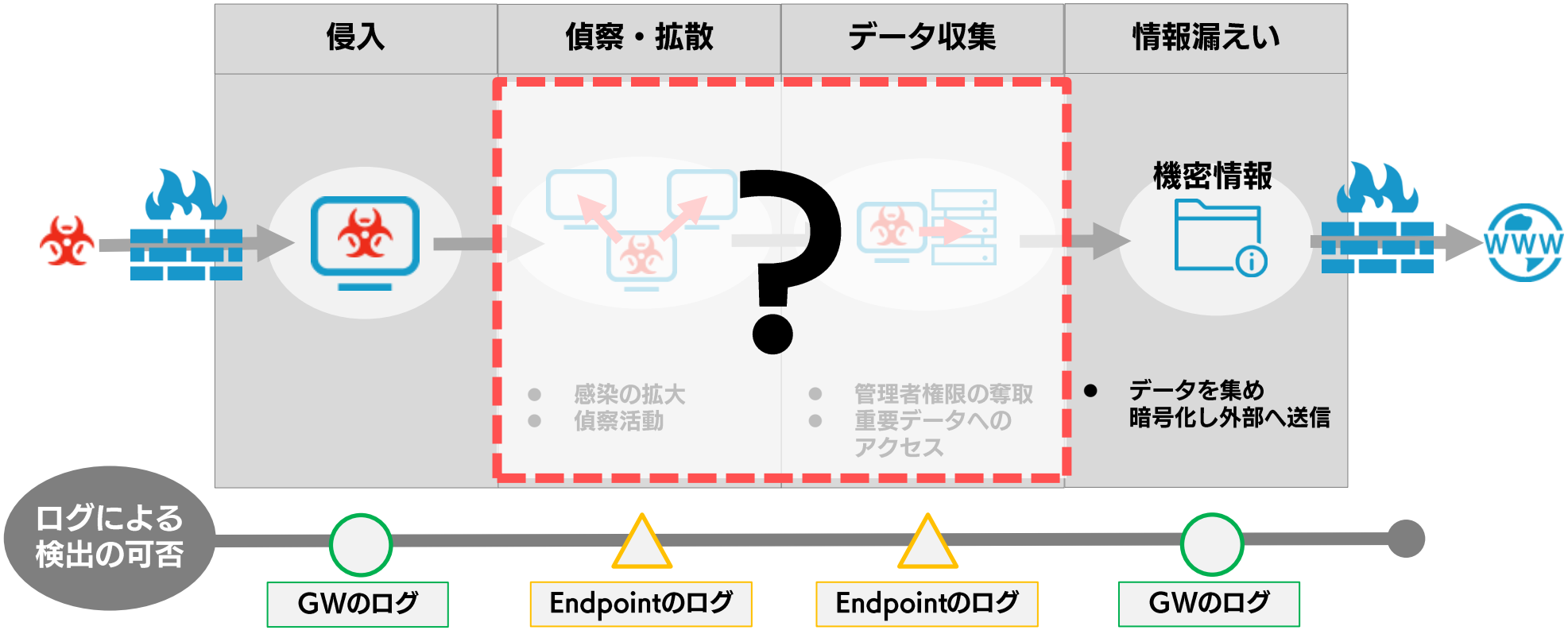


攻撃者は既存の対策を知り尽くし
防御を回避しながら攻撃を仕掛けてくる

感染後のマルウェアの活動を検知できるのか？

SB Technology

マルウェア侵入後、何が行われていたのか？

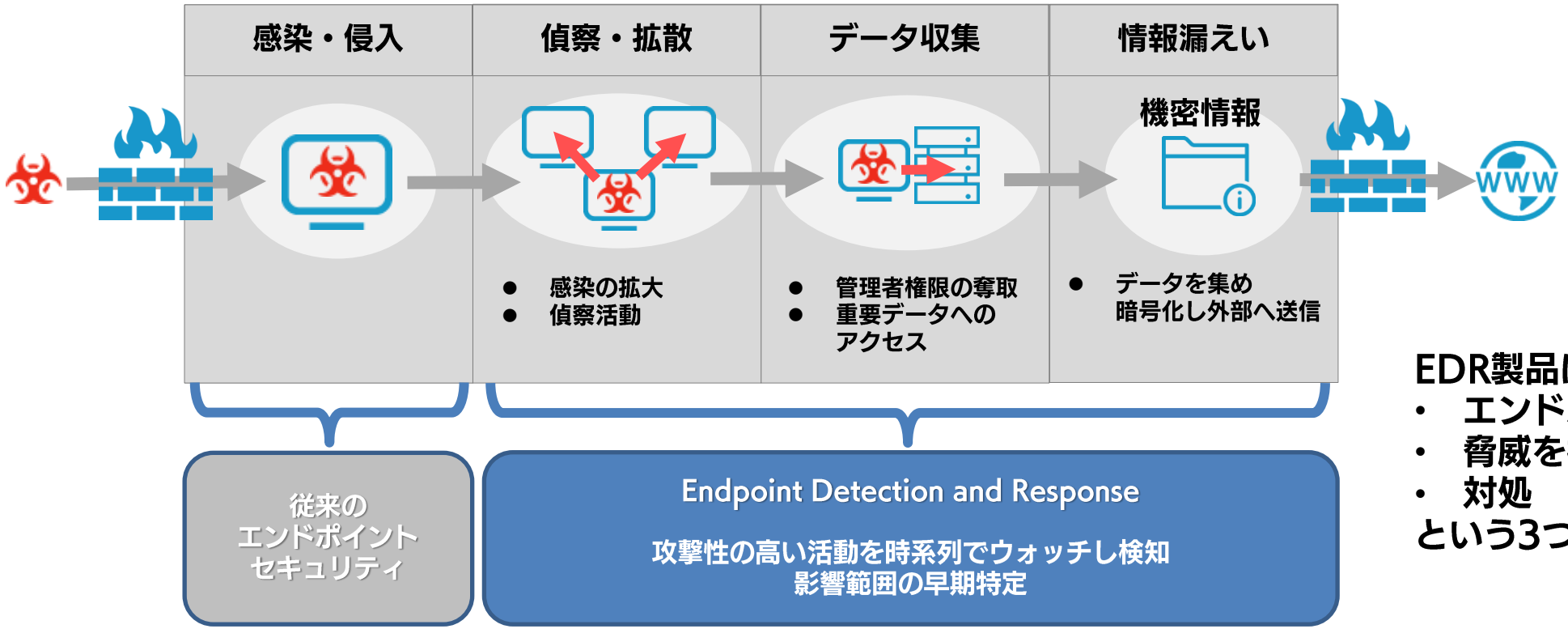


断片的なログからの可視化・分析は
検知スピードや人的リソースの問題で限界がある

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。



侵入防止型
（既知・未知のマルウェア対策）

侵入後の検知＆対処
（攻撃を成立させない仕組み）

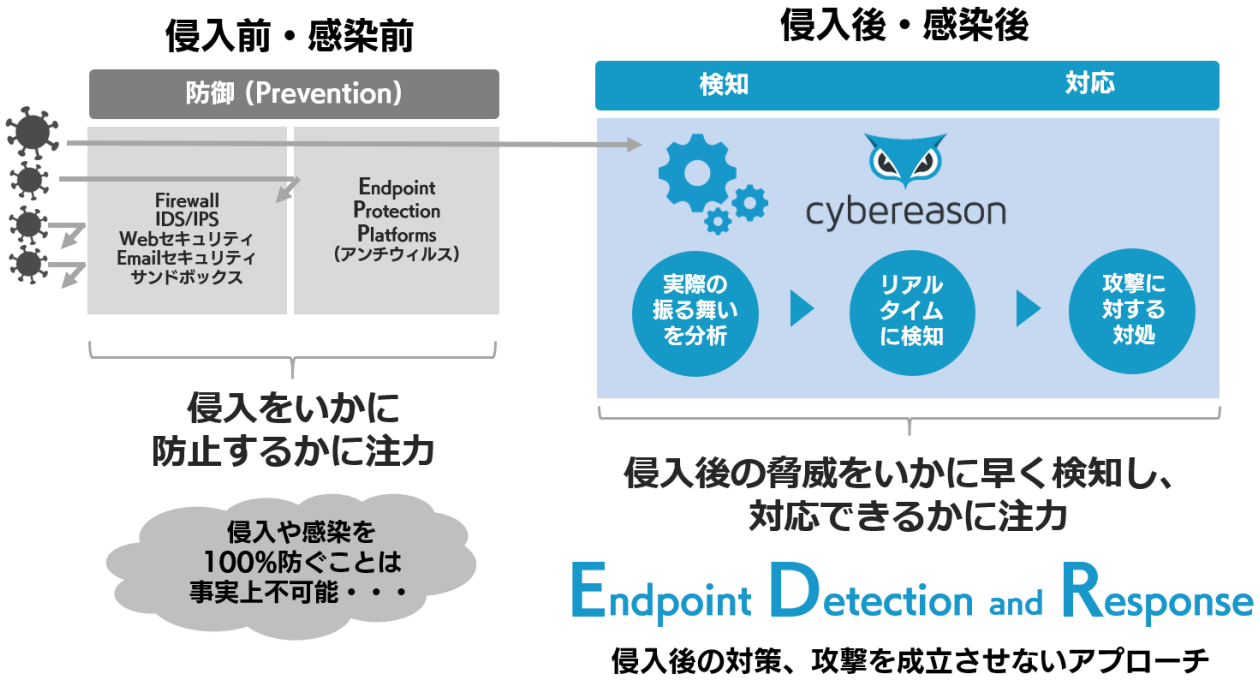
EDR製品は、
- エンドポイントからのログを収集
- 脅威を検知
- 対処

という3つのステップで成立

AIを活用したサイバー攻撃対策
エンドポイントセキュリティソリューション

特徴

- PCのログを集約し、**悪意のある振る舞い**をリアルタイム検知
- **AI**、パターン認識、行動解析など様々な分析ノウハウを実装したエンジン
- 800万回/秒のリクエストを処理する、**大規模解析**クラウドプラットフォーム
- 振る舞い検知とDeception技術(おとり)を活用した、**ランサムウェア対策**



Microsoft Defender ATP

SB Technology

Microsoftが収集する膨大なセキュリティインテリジェンスと機械学習を利用した検知手法をベースに既知および未知の脅威を検知するエンドポイントセキュリティソリューション

Windowsにビルトイン

追加インフラ＆デプロイメント不要
低コストで継続的なアップデート

行動特性による侵入検知をCloudで実現

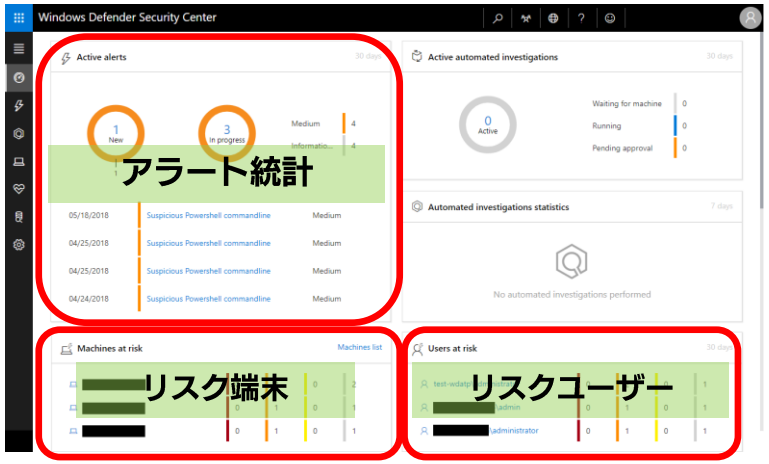
既知および未知の攻撃を検知しアラート出力
リアルタイムデータと履歴データの蓄積

調査に必要な豊富なデータ

侵入範囲を容易に把握可能
エンドポイント横断したデータ解析
ファイル・URL解析

強力な脅威情報ナレッジ データベース

パートナーが持つ脅威情報データと連携
様々な侵入者のプロファイルを検知



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

SB Technology

弊社セキュリティ監視センターから、 お客様環境のEDR(Endpoint Detection and Response)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、
誤検知の有無、危険度を判断し、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

- Cybereason
- Microsoft Defender ATP

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）

Managed Security Service

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

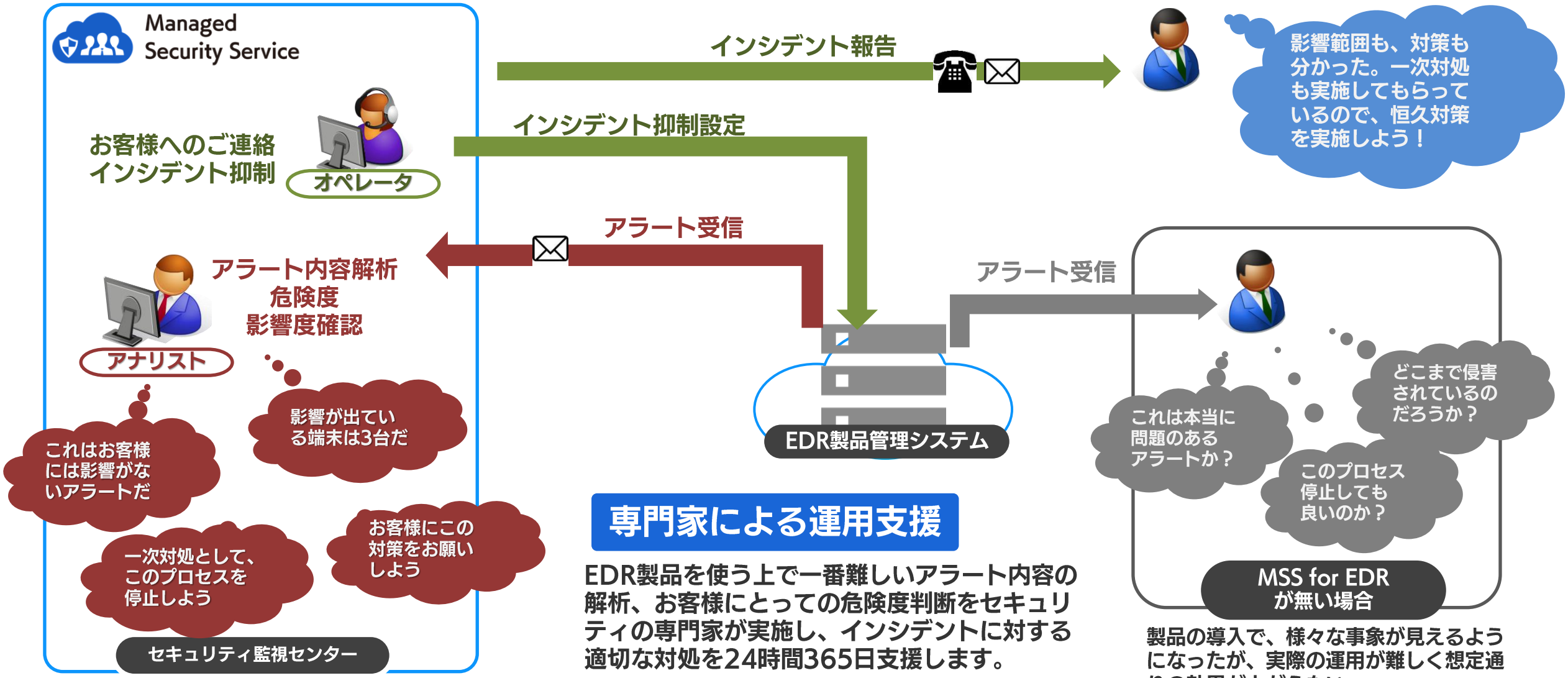
MSS for EDRの特徴

SB Technology

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、EDR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

クイックレスポンス

SB Technology



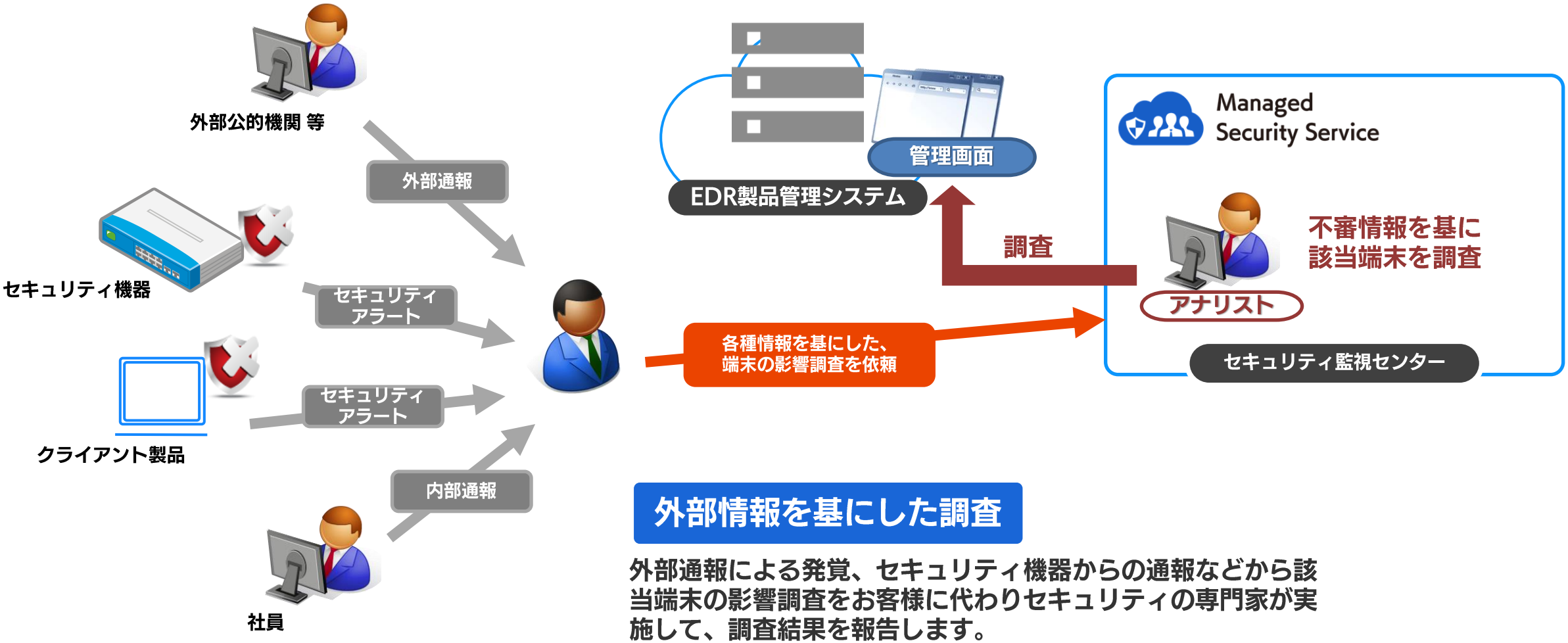
専門家による運用支援

EDR製品を使う上で一番難しいアラート内容の解析、お客様にとっての危険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。

製品の導入で、様々な事象が見えるようになったが、実際の運用が難しく想定通りの効果が上がらない

オンデマンドリサーチ

SB Technology



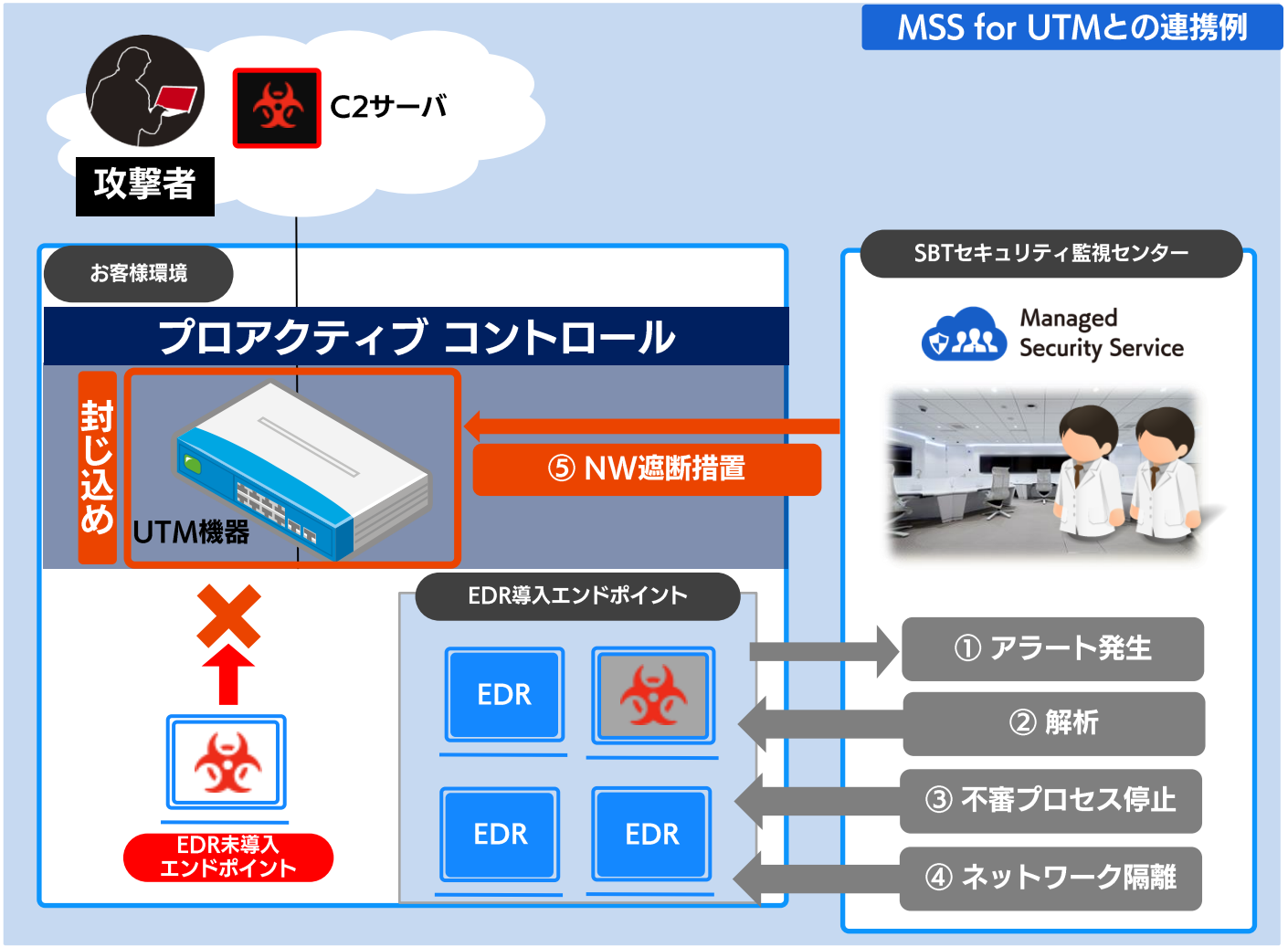
外部情報を基にした調査

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。

プロアクティブ コントロール

SB Technology

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。

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。

サービス内容

SB Technology

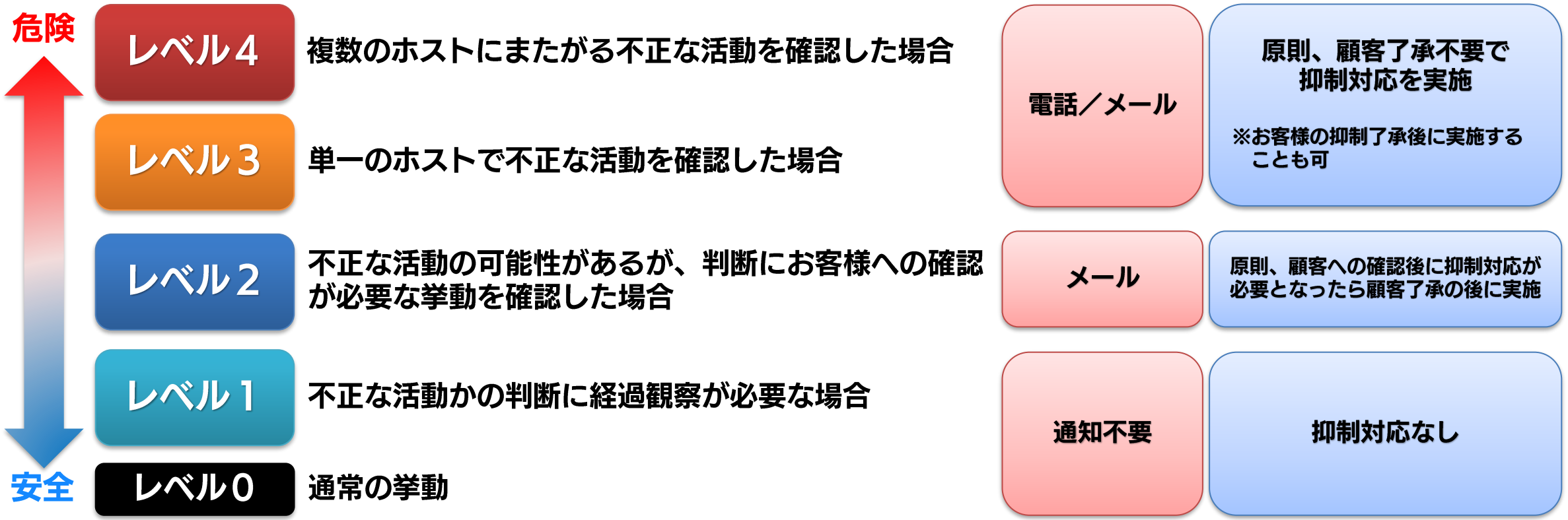
提供するサービス仕様は以下のとおりです。

大分類	中分類	項目	提供形態	内容
システム (サービス)監視	Webコンソール 監視	死活監視	標準	Webコンソールへの疎通確認が取れない場合にメール・電話にて連絡します。
セキュリティ監視	セキュリティ インシデント監視	インシデント検出	標準	製品が検知したセキュリティアラートを用いてセキュリティアナリストがインシデントの検出とその危険度を判定します。
	セキュリティ インシデント対応	インシデント報告	標準	インシデントを検出した場合に、弊社基準に基づきお客様へご報告します。
		インシデント抑制	標準	製品の機能を用いてインシデントを抑制します。抑制とはインシデントに一次対処する機能を指します。
		プロアクティブ コントロール	他監視対象の MSS契約	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。
問合せ対応		製品検知内容	標準	弊社からお客様への通報有無に関わらず製品で検知したアラートについての弊社見解をご回答します。
		オンデマンド リサーチ	標準 (月5件まで)	EDR製品以外の不審情報※を起点にして、EDR製品の手動調査機能を用いた調査をアナリストが行います。状況確認の結果インシデントが確認できた場合、抑制作業を実施します。 ※「不審情報」とは情報セキュリティの文脈においてコンピュータに関わる情報を指します。例としては何かしらのセキュリティ製品で検知のあったIPアドレスやホスト名等です。
レポーティング	月次レポート	簡易レポート	標準	発生したインシデントのサマリ(概要一覧とそのステータス)を記載します。
		詳細レポート	オプション	お客様のアラート、インシデントの発生状況や、弊社監視センター全体での検知傾向、世間の動向からお客様環境の状況について総合所見を記載します。
その他		リモート報告会	オプション	弊社アナリストが月次レポートの内容を基に報告を行います。

危険度に応じた通知

SB Technology

セキュリティアラートに対して、以下の判断基準を基に危険度を判定し、そのレベルに応じて対処が必要なインシデントについてお客様に通知します。
また、影響度に応じた一次対処を実施します。



挙動・・・システムの動作
活動・・・攻撃者の動作

サービス対象製品

2020年01月現在

SB Technology

MSS for EDR
サービス提供対象製品

- Cybereason 『Cybereason EDR』
- Microsoft 『Microsoft Defender ATP』
- Trend Micro 『 Apex One™ 』

※上記以外の製品については、別途ご相談ください。

セキュリティ監視センター

SB Technology

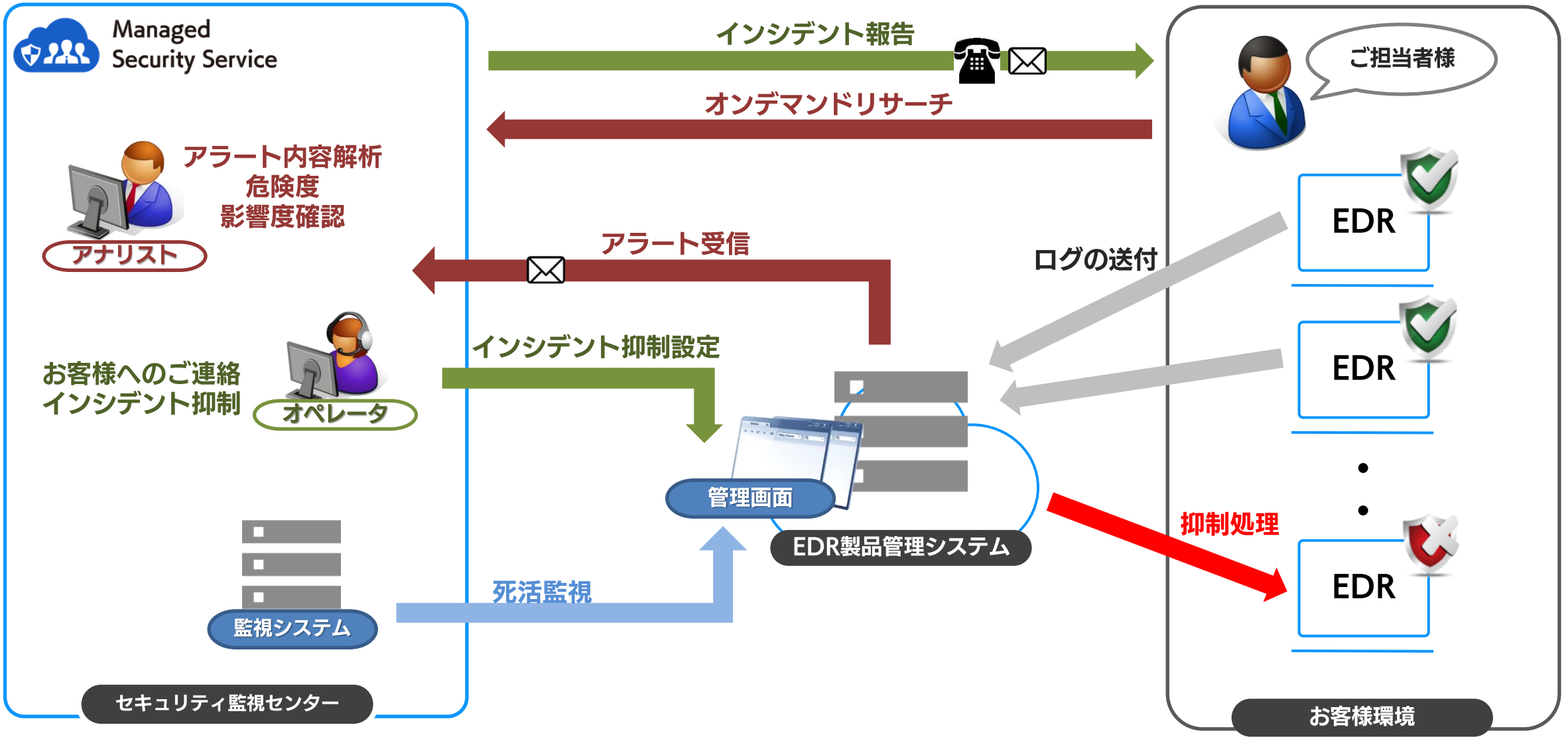
24時間365日　有人監視体制

生体認証を始め複数の認証方式を用いた高セキュリティルームでセキュリティの専門家が24時間365日休むことなく安定したサービスを提供します。

項目	内容
監視拠点	都内某所（非公開）
稼働時間	24時間365日
体制	センター長・チーフアナリスト・インシデントアナリスト セキュリティアナリスト・オペレーター
資格者	McAfee SIEM認定技術者 CISSP 情報セキュリティスペシャリスト ネットワークスペシャリスト 他、ベンダー資格者等多数在籍
情報収集	外部からの情報収集（IPA等） 独自ハニーポット、検証環境常設 当社リサーチャーによる情報提供 海外コミュニティからの情報収集
監視イベント数	10億イベント/日
セキュリティ	生体認証とICカードによる入室認証 24時間の監視カメラによる録画 記録可能デバイスの持ち込み禁止 運用監視通信の限定

※2018年1月時点

運用監視構成



月次レポート / 報告会

SB Technology

月次レポートは、簡易な標準レポートとオプションの詳細なレポートの2種類を用意しております。

- **簡易レポート**
  発生したインシデントのサマリ(概要一覧とそのステータス)を記載します。

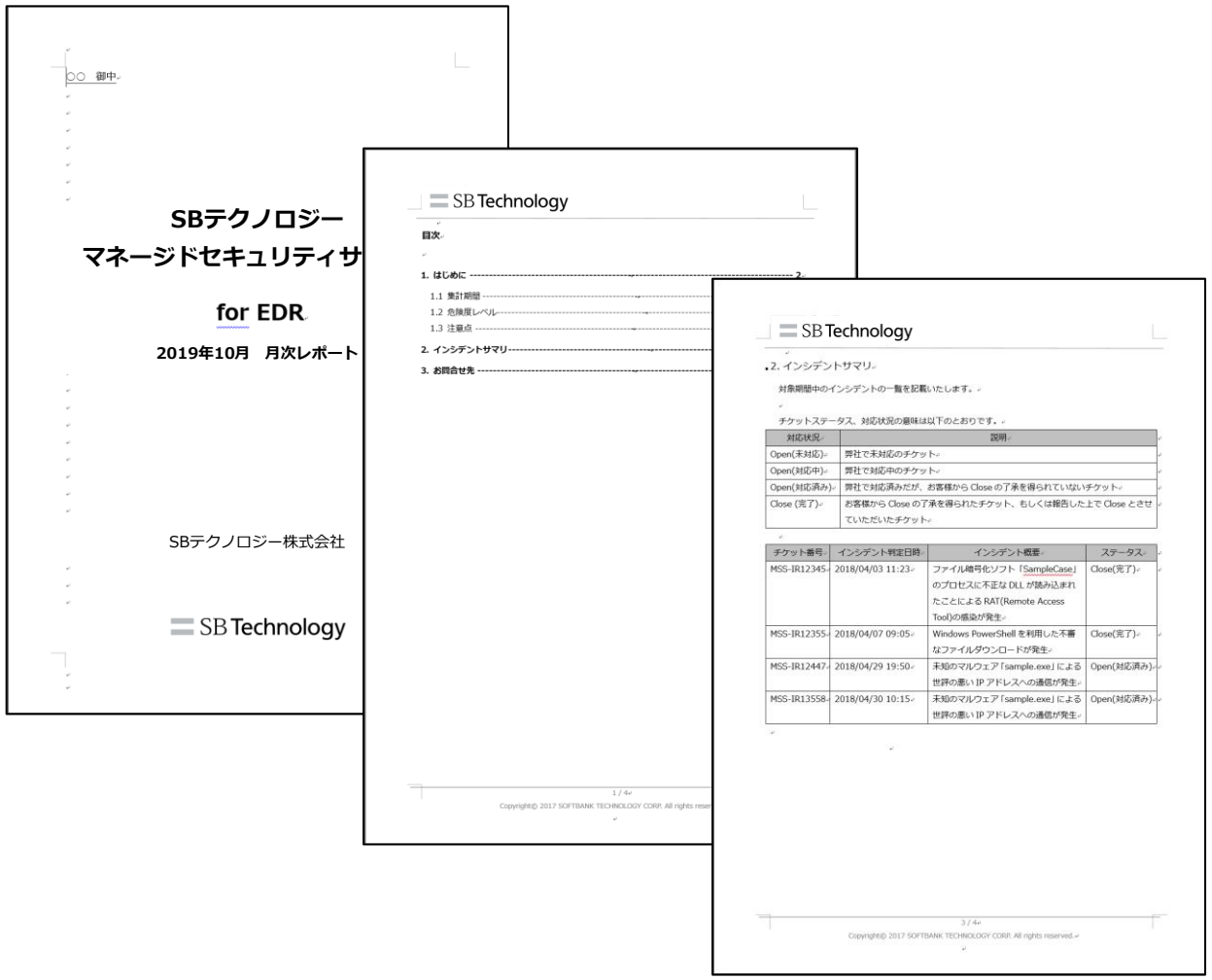
- **詳細レポート(オプション)**
  お客様のアラート、インシデントの発生状況や、弊社監視センター全体での検知傾向、世間の動向からお客様環境の状況について総合所見を記載します。

	簡易レポート	詳細レポート
インシデントサマリ	○	※インシデント一覧に含まれる
総合所見	–	○
インシデント一覧	–	○
オンデマンドリサーチ対応状況	–	○
セキュリティトピックス	–	○

報告会

オプションとして提供する報告会では、弊社セキュリティアナリストが、詳細レポートに基づき、且つセキュリティトレンドを加味した解説を行います。

月次レポート － 簡易レポート －



簡易レポート

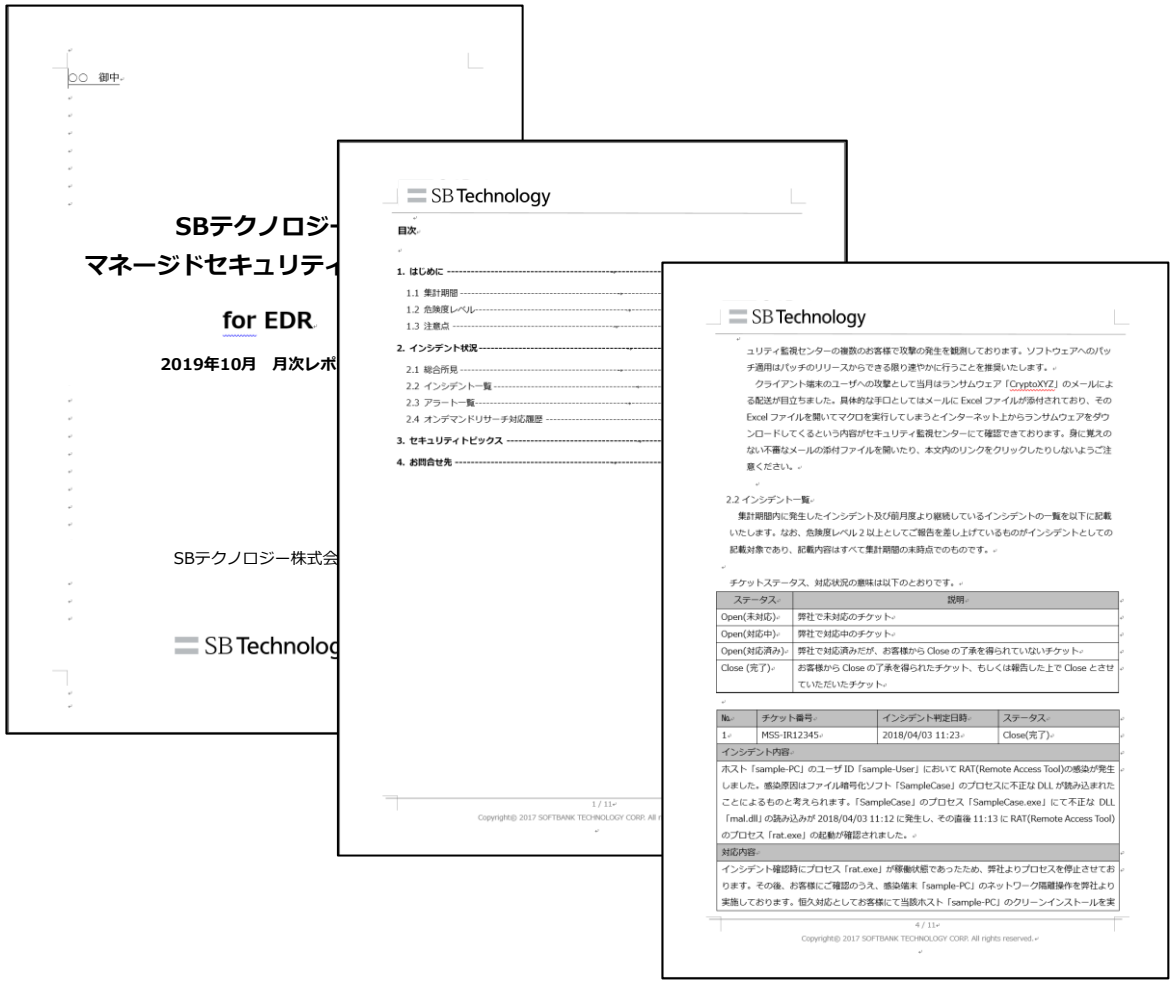
簡易月次レポートとして、インシデント発生状況をまとめた内容をPDF形式にてご提供いたします。

＜簡易月次レポート内容＞
・インシデントサマリ

月次レポート － 詳細レポート －

※オプション(有償)

SB Technology



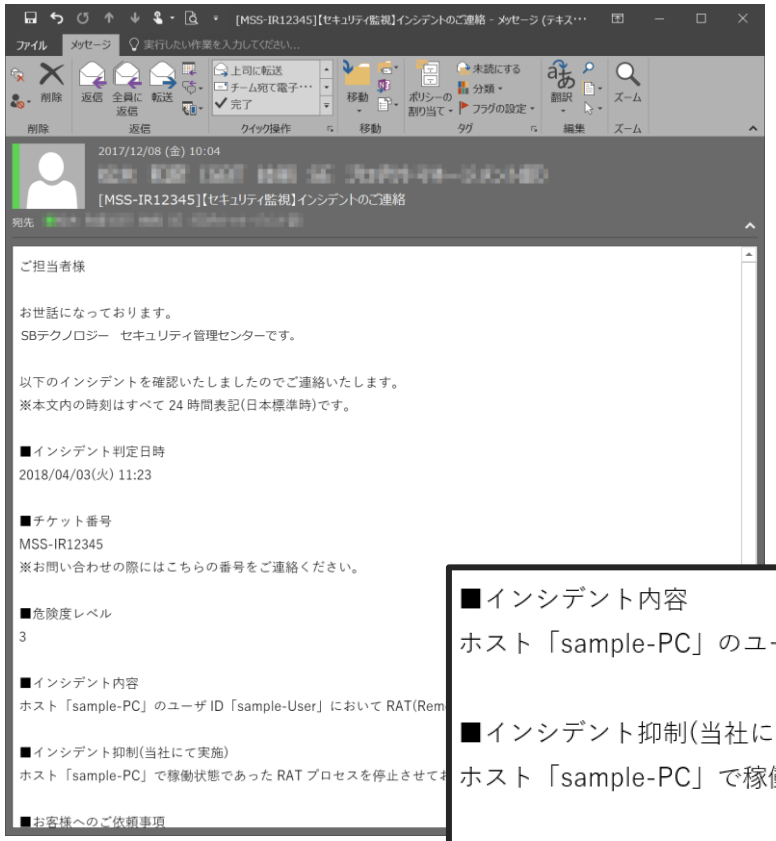
詳細レポート

詳細月次レポートとして、稼働状況、およびインシデント発生状況をまとめた内容をPDF形式にてご提供いたします。

＜詳細月次レポート内容＞

- **インシデント状況**
  - **総合所見**
  - **インシデント一覧**
  - **オンデマンドリサーチ対応状況**
- **セキュリティトピックス**

メール通知



インシデントを検出した際に、お客様に危険度や解析内容をメールにて報告します。

＜メール通知内容＞
- **インシデント判定日時**
- **チケット番号**
- **危険度レベル**
- **インシデント内容**
- **インシデント抑制(弊社にて実施)**
- **お客様への依頼事項**
- **関連検知情報**

■インシデント内容
ホスト「sample-PC」のユーザ ID「sample-User」において RAT(Remote Access Tool)の感染が確認されました。

■インシデント抑制(当社にて実施)
ホスト「sample-PC」で稼働状態であった RAT プロセスを停止させております。

■お客様へのご依頼事項
以下のご検討をお願いいたします。
・当該ホスト「sample-PC」のネットワークからの隔離。※許可をいただければ弊社からの隔離操作も可能です。
・アンチウィルスソフトの最新のパターンファイルを使用したフルスキャンによる感染状況の確認。
・当該ホスト「sample-PC」のクリーンインストール。

MSSカスタマーポータル

SB Technology

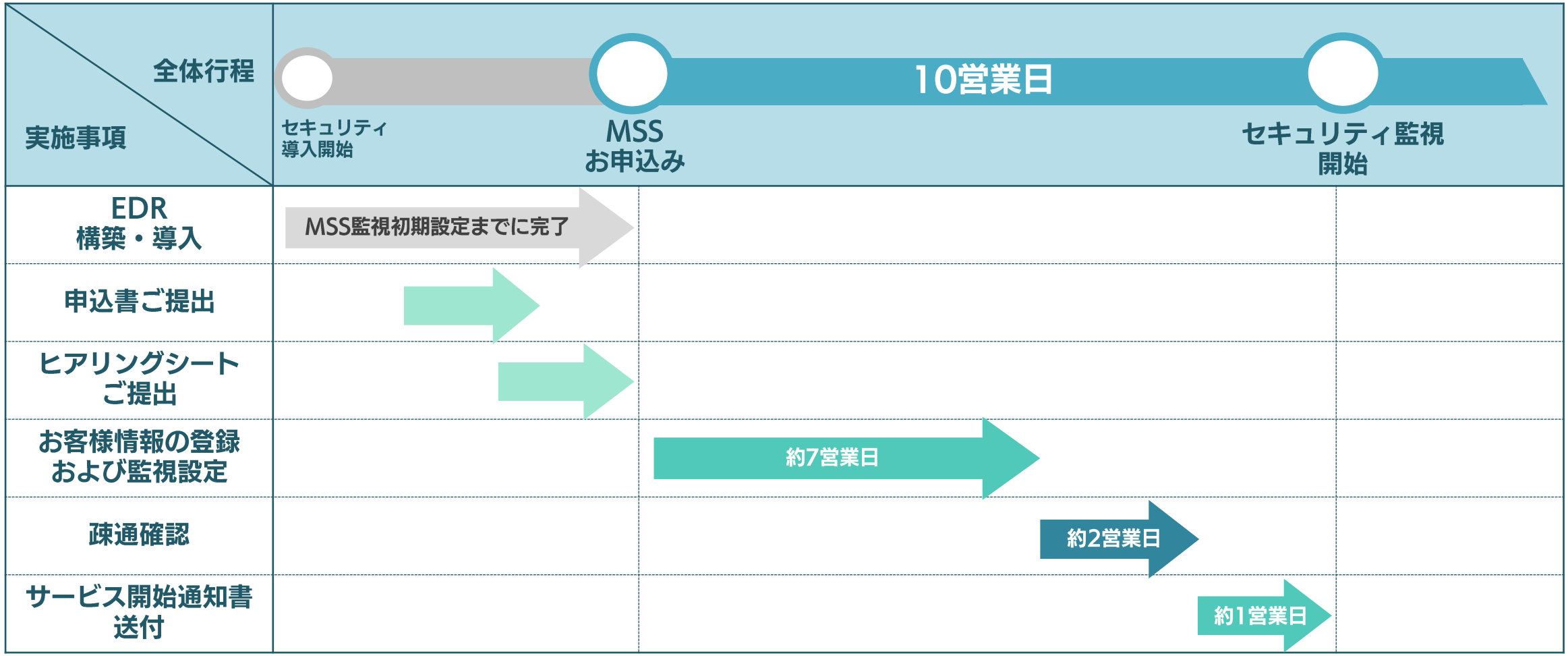
MSSをご契約いただいたお客様へカスターマーポータルをご提供いたします。

メニュー	機能
トップ	ポータルサイトのホームページ
お知らせ	ご案内(お知らせ)やメンテナンス情報など
チケット対応状況	進捗済みのインシデント お問い合わせ一覧および詳細
ダウンロード	月次レポートなどの資料提供
お問い合わせ	お客様からのお問い合わせフォーム
契約情報	ご契約情報の確認
各種申請書	各種申請書の提供
よくあるご質問	よくあるご質問を提示

導入スケジュール

SB Technology

お申込みからサービス開始までの流れは以下となります。



：お客様作業　：弊社作業　：お客様/弊社作業

情報革命で人々を幸せに

～ 技術の力で、未来をつくる ～

SB Technology