SB Technology

大企業向けマネージドセキュリティサービス

MSS for UTM ご説明資料

SBテクノロジー株式会社

FortiGateとは

SB Technology

FortiGateとは、フォーティネット社が開発する、ファイアウォールをはじめ複数のネットワークセキュリティ機能を一台に統合した「オールインワン」アプライアンスです。企業の規模や状況に応じた柔軟なセキュリティ対策を低コストでかつ簡単に導入することが可能です。近年、国内では大規模企業でのご利用が増えています。

Fortinet社 FortiGateシリーズ

複数のセキュリティ機能を1台で提供するUTM（統合脅威管理）アプライアンスです。
独自開発の「FortiASIC」を搭載しており、ハードウェア処理による高速なファイアウォール/UTM処理を実現します。

選択可能な主なセキュリティ機能

- IPS/IDS
- アンチウイルス
- アンチスパム
- クラウドサンドボックス
- Webフィルタリング

※本サービスでは、アンチスパムのログ・アラートは監視・分析対象外です。
※パロアルトネットワークス製品も監視可能です。

導入後の課題

SB Technology

UTMを導入しただけでは脅威への対策は完全とは言えません。通過してしまった通信のログ情報から、防御機能で阻止できなかった攻撃の兆候や異常に気付き、インシデント発生時はいち早く処置ができる体制が必要です。

セキュリティ運用監視に求められる項目

UTMログ監視・分析（例）

ファイアウォールログ

- ドロップ(遮断)が増加している
- 夜間、業務時間外の通信が増加
- 不審なIPへの通信がある
- 他機能ログの追跡調査（相関分析）

IPS/IDS

- 検知した攻撃の種類・影響・結果
- 新たな脆弱性と検知遮断状況の確認
- 他機能ログの追跡調査（相関分析）

アンチウイルス・サンドボックス

- 検知したマルウェアの種類、送信元
- 同一検体の他PCでのDL・実行履歴
- 他機能ログの追跡調査（相関分析）

URLフィルタリング・アプリコントロール

- 不審なURLへの通信がある
- 不審なアプリの通信がある
- 他機能ログの追跡調査（相関分析）

稼働監視・機器運用

シグネチャーチューニング

脆弱性情報の把握と対策

即時対応できる体制

MSS for UTM の概要

SB Technology

そこでMSS for UTMによって、弊社セキュリティ監視センターからお客様環境の UTM(Unified Threat Management)製品を24時間365日体制でセキュリティ監視を行います。UTM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、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通知をご担当者様が受け取れます。

UTM製品

FORTINET

paloalto NETWORKS

- ファイアウォール
- アンチウイルス
- IPS/IDS
- クラウドサンドボックス
- アプリケーションコントロール
- Webフィルタリング

✓オールインワン、1台で実現する多層防御
✓出入口対策

×

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

サービス内容

SB Technology

専門アナリストによるセキュリティに特化した「監視」と「運用」を統合し提供、セキュリティイベントの早期発見と安定したシステム稼働を実現します。

インシデント監視

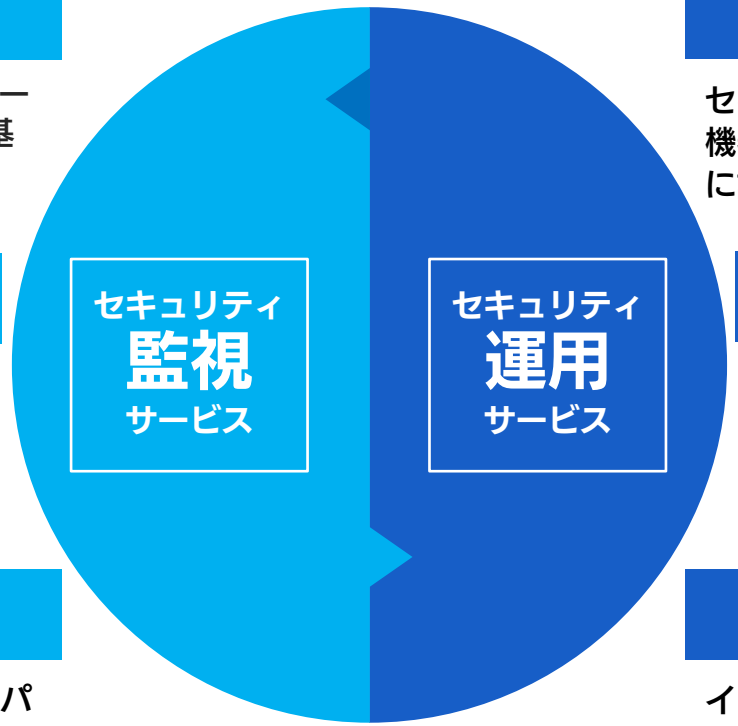
UTM機器が検知したセキュリティアラートをトリガーに、セキュリティアナリストが影響度を判断し弊社基準に基づきお客様への通報を行います。

セキュリティログ監視

外部C＆Cサーバとの通信や通信量増加によるセッション数の急上昇を検知、ネットワーク状態の傾向変化から不審な通信状況を監視します。

システム監視

ノード(疎通、ログ受信、管理ポート、冗長構成）、パフォーマンス(メモリ、CPU、ディスク)、シグネチャ更新など稼働状況を常に監視します。



通信遮断

セキュリティアナリストがインシデントと判断しUTM機器において不正通信が遮断可能な場合には、お客様に許可をいただいたうえで当該通信を遮断します。

セキュリティオペレーション

IPSのシグネチャチューニング作業やFirewallアクセスリストの設定変更をセキュリティエンジニアがお客様に代わって実施します。

レポート

インシデント検出状況を月次で集計しご提供します。

※ 本サービスにTAC(製品保守)は含まれません

特徴１　マルチファンクションによる相関分析

SB Technology

一つのインシデントに対し、単一機能ログ分析で留めずに各機能のログを横断的に分析し精度を高めます。

検知　分析　報告

異常検知

- ファイアウォール
- IPS/IDS

Managed Security Service

- ✓ 感染の有無
- ✓ 影響度
- ✓ 影響範囲
- ✓ 対策

複数機能のログを横断的に調査

基本メニュー
- URLフィルタリング
- アンチウイルス

基本メニュー
- アプリケーションコントロール

原因・影響が明確！

ご担当者様

他社 MSS

ファイアウォール、IPS/IDS のログのみで判断

インシデントが発生した「可能性」がある・・・

可能性だけじゃ…

ご担当者様

特徴2　プロアクティブ（事前予防型）コントロール

SB Technology

UTM機器による一連の解析・遮断に加え、他のMSS監視製品を活用し追加の調査・対策を行います。

※別途、他監視対象のMSS契約が必要です。

具体的な原因、影響範囲を特定

UTM製品で検知したアラートに対し、エンドポイント等のログや情報を組み合わせて解析することで、より具体的な原因・被害範囲の調査が可能になります。

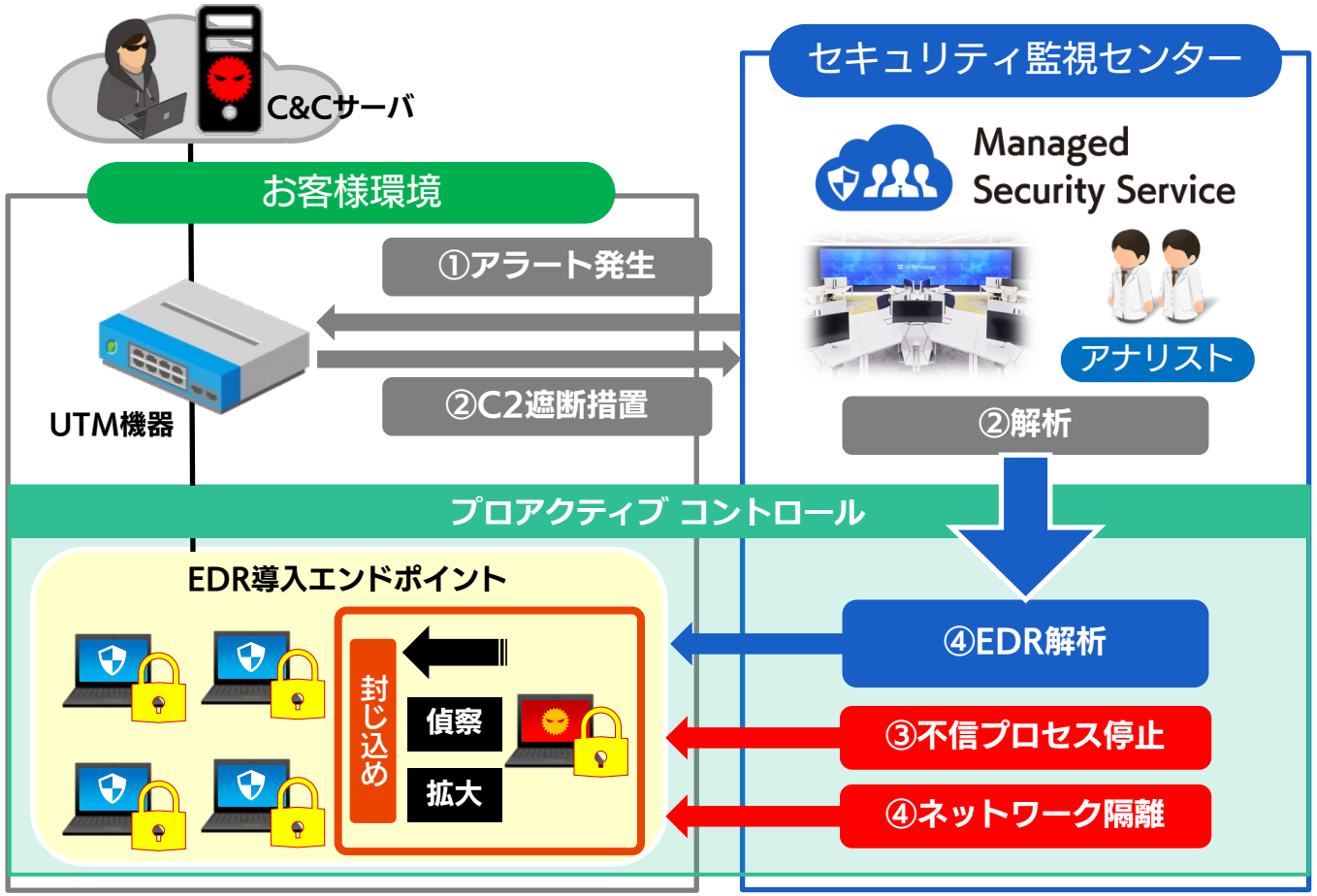
拡散・拡大を阻止

攻撃者に乗っ取られたPCから内部への偵察活動や感染拡大に対し、端末単位でセキュリティ脅威を封じ込めることにより、業務全体への影響を最小限にした上で、復旧対策が可能です。

お客様負担の軽減

従来、感染源情報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。

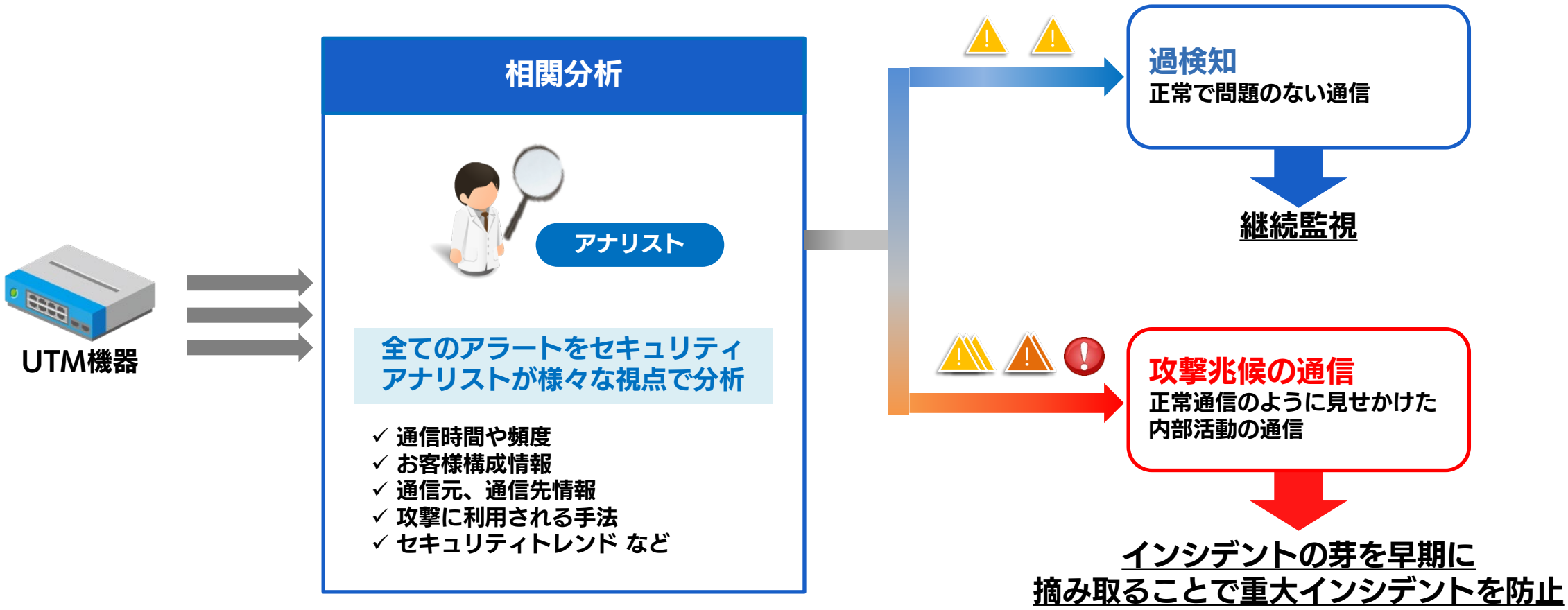
【MSS for UTM とMSS for EDR との連携例】



特徴３　全てのアラートが監視・分析対象

SB Technology

アラートのリスクレベルが「低」場合でも、攻撃の兆候が含まれている場合があります。本サービスはリスクレベルに関係なく、全てのアラートを監視・分析対象としています。



インシデントレベルに応じた通知

SB Technology

アラートは全件通知ではなく、**影響度の高いインシデントのみご連絡**します。そのため、お客様はシステムへの対処など必要な対応のみ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

危険

安全

		インシデント状況例	対応例	
レベル4	攻撃成功を確認し、内部への侵入成功の事実をログから確認した場合	・マルウェアによるC&C通信 ・攻撃者による感染端末を利用した外部への攻撃	・端末の切り離し、調査 ・端末のクリーンインストール ・外部接続の遮断	電話・メールで通知
レベル3	攻撃成功を確認したが、内部への侵入成功の事実をログから確認できない場合	・不正なサイトへアクセスし、マルウェアをダウンロード	・不正サイトへのアクセス遮断 ・利用者への状況確認	電話・メールで通知
レベル2	実際に影響を与えようとする攻撃を検知しているが、攻撃の成功・失敗に確認を要する場合	・不審なファイルが添付されたメールの大量検知 ・不正なサイトへのHTTPリクエスト	・不正サイトへのアクセス遮断 ・利用者への注意喚起	メールで通知
レベル1	スキャン行為など実害の無い調査活動や過検知と判断したものや、攻撃の失敗が確認できており実害がない場合	・ポートスキャン ・脆弱性調査	・継続監視	
レベル0	通常の通信または誤検知と判断した場合	・誤検知	-	

通知対象

特徴5　24時間365日 セキュリティアナリストが対処

24時間365日　有人監視体制

当社のセキュリティアナリストが24時間365日体制で発生したアラートを監視。影響度を分析して一次対処まで行います。

項目	内容
監視拠点	都内某所（非公開）
稼働時間	24時間365日（※アナリストも24時間体制）
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	CISSP GIAC (GIAC Reverse Engineering Malware) 情報処理安全確保支援士 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、JPCERT/CCなど） ● 検証環境常設 ● 弊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	40億イベント/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 ● 非常用電源を72時間以上確保

※ 2022年4月時点

特徴6　英語対応も可能なグローバル監視センター

SB Technology

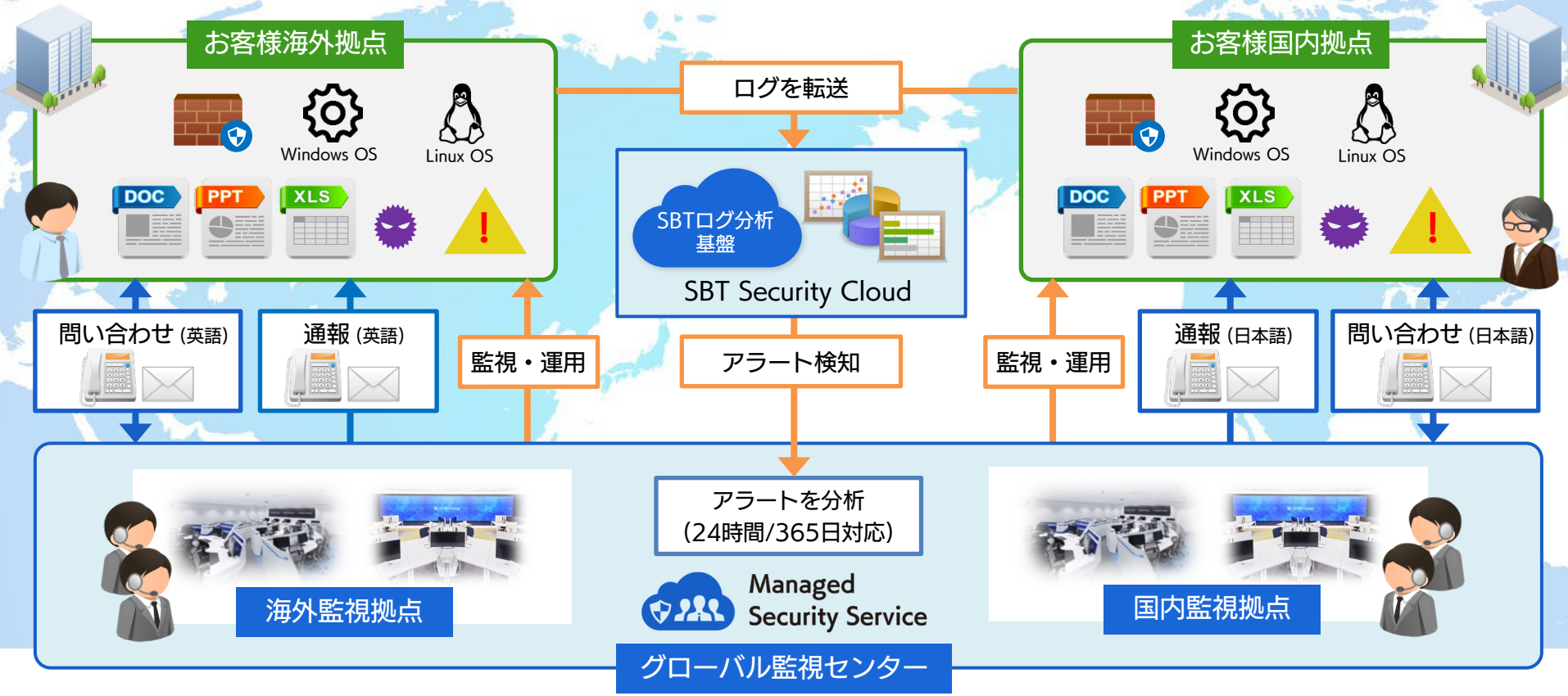
お客様の海外拠点に対しては、当社海外監視拠点から英語で監視・対処する体制をご用意しています。
※グローバル監視センターの利用は別途お見積が必要です。

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）

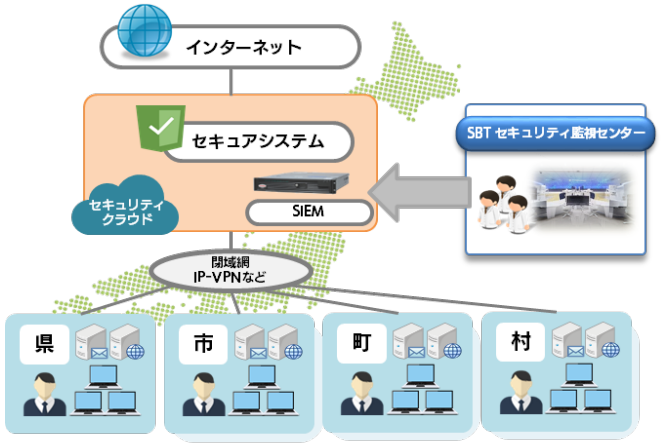


特徴7　自治体情報セキュリティクラウドにおける実績

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。



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

417団体
12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
12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、弊社でSIEMを用いた統合的な相関分析を行っています。

自治体情報セキュリティクラウドでは12県の実績があり、安心してお客様のシステムをお預けいただけます。

特徴８ セキュリティ強化にあわせた段階的導入

SB Technology

既存環境強化

入口／出口対策強化
フェーズ1

- Webサイトセキュリティ MSS for Imperva Incapsula
- Webアクセスセキュリティ MSS for Secure Gateway (Zscaler)
- クラウドネットワークセキュリティ MSS for iboss Cloud Security
- ゲートウェイセキュリティ MSS for UTM (FortiGate / Palo Alto)

脆弱性を狙った
攻撃や不正通信検知

内部対策強化
フェーズ2

- クラウドセキュリティ MSS for CASB (McAfee MVISION Cloud)
- 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
- サーバーセキュリティ MSS for Trend Micro Deep Security

- 標的型攻撃
- ゼロデイ攻撃
- サンクションIT

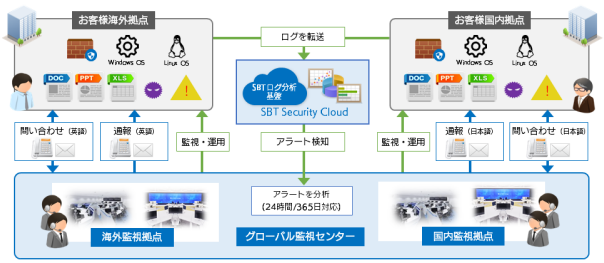
拡張強化

インシデントレスポンス強化
フェーズ3

- IDセキュリティ MSS for Microsoft 365
- 統合ログ分析セキュリティ MSS for Microsoft Sentinel
- エンドポイントセキュリティ MSS for EDR (Trend Micro Apex One / Cybereason EDR / Microsoft Defender for Endpoint)

- 端末解析
- 不正行動分析

将来



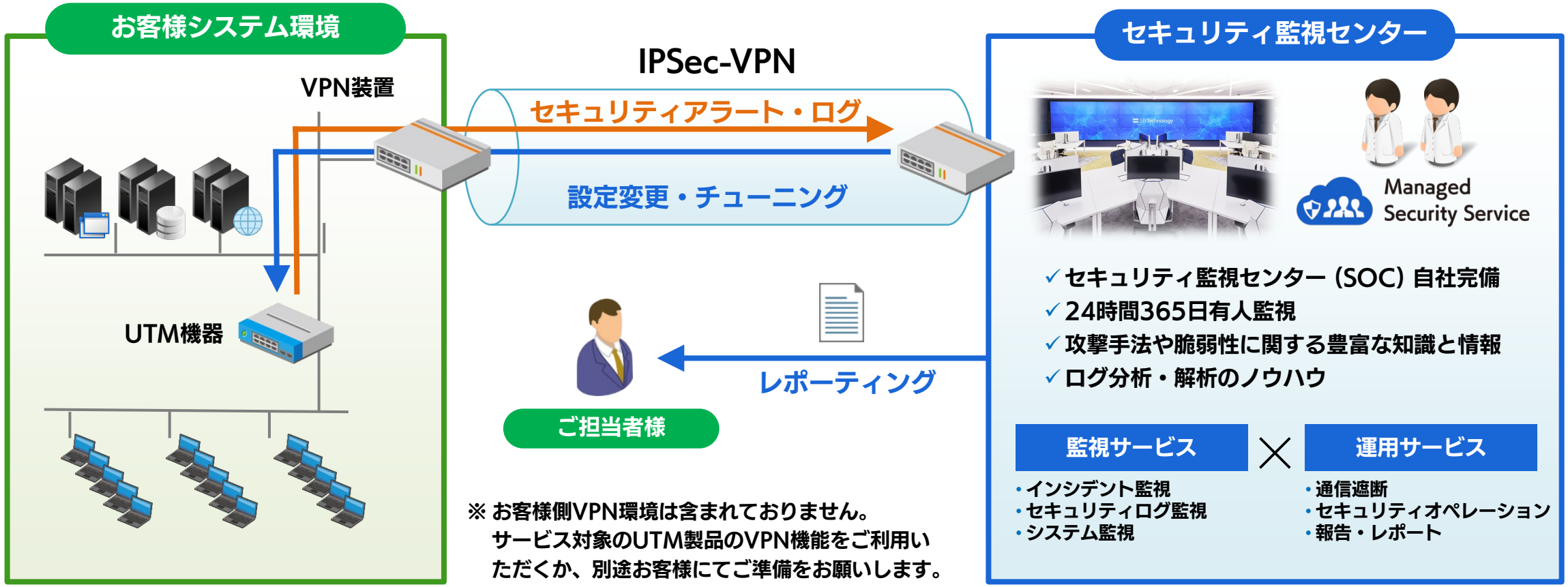
グローバル拠点も含めた
セキュリティ監視

複数のセキュリティ機器の相関分析でインシデントの早期発見・早期対処ができるため、
将来の投資ロードマップを見据えたセキュリティ投資が可能になります。

サービス構成

SB Technology

対象の UTM 製品で検知したセキュリティアラートを元に、弊社セキュリティ専門アナリストが分析の上で影響度によって必要な対処を実施し、弊社基準に基づきお客様への通知を行います。



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

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

IDセキュリティ
MSS for Microsoft 365

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

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

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)

SB Technology

SBテクノロジー株式会社

〒160-0022
東京都新宿区新宿6丁目27番30号
新宿イーストサイドスクエア17階

https://www.softbanktech.co.jp/

お問い合わせフォームへ ▶