

# サイバー攻撃からクラウド環境を守り セキュアなリモートワークを実現

Microsoft 365 E5 セキュリティ監視

## MSS for Microsoft 365



Managed  
Security Service

こんなことにお困りではありませんか？

1

製品知識に詳しい人材が  
いないため運用に不安

多数のコンポーネントで  
構成される Microsoft 365 を  
包括的に利用する事が困難

2

アラート分析の工数や  
負荷を軽減したい

日々大量のアラートが  
発生する中で専門的に  
解析できる人材がない

3

リモート環境を狙った  
攻撃に備えるには…

実際の攻撃に合う前にリモート  
ワーク環境に最適なセキュリ  
ティ対策をすぐに行いたい

『MSS for Microsoft 365』で解決！

1

豊富な製品導入実績のあ  
る当社にお任せ

Microsoft プロダクトの  
導入実績から得られた  
様々なノウハウをご提供

2

セキュリティ専門アナリ  
ストによる常時監視

セキュリティやクラウドの知見  
を持った専門アナリストが  
さまざまなログを的確に分析

3

最適な監視でゼロトラ  
ストセキュリティを実現

お客様のリモート環境を守るた  
め、ゼロトラストセキュリティ  
に特化した監視をご提供

## 概要

### Microsoft 365 E5 セキュリティ機能を最大限に活用し安全なリモートワーク環境を支援

生体認証を始め複数の認証方式を用いた SBテクノロジーのセキュリティ監視センター（SOC）では、経験豊富なセキュリティ専門アナリストが24時間365日お客様環境にある Microsoft 365 E5 のもつセキュリティ機能を常時監視します。

## 特長

### 特長 1

#### Microsoft 365 E5 によって巧妙かつ高度化したサイバー攻撃への対策

Microsoft 365 に含まれる各ソリューションのアラートを24時間365日監視および抑制対応し、重大な脅威が発見された場合は、各ソリューションを跨いだ相関分析をセキュリティ専門アナリストが実施します。

### 特長 2

#### 日々の膨大なアラートの対処も当社にお任せ

各 Microsoft 365 ソリューションが検出したインシデントをトリガーとして、当社のセキュリティ専門アナリストが関連するイベントログやセキュリティアラートを相関的に分析し、脅威の分析を行い影響度を判定します。

### 特長 3

#### エンドポイント上で検出されたアラート分析や調査、報告

Microsoft Defender for Endpoint と連携し、社内の端末内への影響範囲の分析、他の端末への被害拡大の調査、必要な処理まで当社が行います。  
(別途 MSS for EDR の契約が必要です)

## 展開イメージ

### Microsoft 365 E5 Security

- 標的型メール
- 情報搾取
- 不正アクセス
- マルウェア



※別途 MSS for EDR の契約が必要です。



分析

制御対応

### セキュリティ監視センター



お客様企業  
ご担当者

レポート

## 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

電話 03-6892-3154 受付時間：平日10:00～17:00

メール sbt-ipsol@tech.softbank.co.jp

URL <https://www.softbanktech.co.jp/>

詳しい情報はこちら

SBT

で

検索



● 本カタログに記載された社名・商品名等は各社の商標または登録商標です。  
● 本カタログに記載された内容およびその他の情報は予告なしに変更される場合があります。

SBT Technology  
10020357  
本社/芝大門/天王洲  
大阪/名古屋/福岡