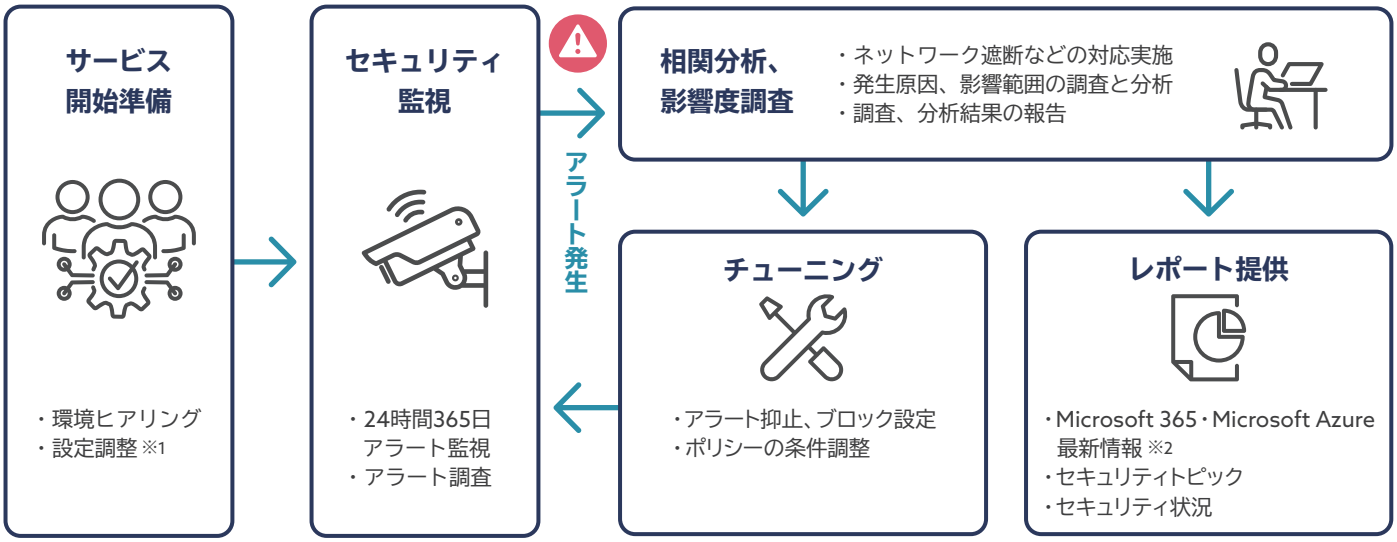
## Microsoft 365 と Microsoft Azure のセキュリティ統合監視を実現！

# JBS SOC

Microsoft 365 や Microsoft Azure のセキュリティ運用に不安を抱いているお客さま向けのサービスです。高度なログ分析により、本当に対応が必要なアラートを見極め、対処やチューニングを代行、支援することで、健全な環境の維持を実現できます。

## サービス概要

JBS とセキュリティ専門ベンダーである S＆J株式会社（以下、S＆J）との協業により提供する SOC（Security Operation Center）サービスです。Microsoft 365 E5 Security、Microsoft Defender for Cloud（以下、MDC）で検知されるアラートを 24 時間 365 日 セキュリティアナリストが監視し、お客さまの環境に応じて選定した複数ログを分析、適切な対応とセキュリティ監視の精度向上・既知の脅威をブロックするためのチューニングを実施します。




※1 JBS とお客さまによる作業　※2 アラート監視対象となる Microsoft 365 E5 Security、Microsoft Defender for Cloud の製品やソリューションに限る

## サービスメリット

Microsoft 365、Microsoft Azure だけでなく、お客さまの環境に適したログを相関分析することで、アラートのみの詳細分析だけでは分からない、お客さまの環境“だから”を考慮したセキュリティ監視を実現します。

### 本当に対処が必要なアラートだけに絞れる

あらかじめ、お客さまの環境を把握したうえで、Microsoft 365、Microsoft Azure のログと、ファイアウォールをはじめとする通信ログなどを Microsoft Sentinel を利用して相関分析します。これにより、発生原因と脅威の影響度を判断し、対処が必要なアラートのみをお客さまに通知します。

### 脅威への対処、チューニングは JBS におまかせ

対応が必要な脅威に対して、端末のネットワーク隔離などの対処を JBS が代行します。また、分析結果から過検知・誤検知と分かったアラートの抑止や、既知の脅威をブロックするチューニングも代行します。これにより、お客さまは実働せずとも脅威への対処や監視精度の向上が図れます。

### セキュリティ対策の改善に困らない

月次で監視状況を分析し、お客さまの環境のセキュリティ状態を評価します。評価した結果、問題がある場合はセキュリティ対策の改善案を JBS が提示します。お客さまはその改善案をベースに検討することができます。

## こんなお客さまにおすすめ

**セキュリティ専門家が社内に不足している**

**Microsoft 365、Microsoft Azure のセキュリティ運用経験、ナレッジが少ない**

**セキュリティ運用のために十分な体制を維持できない**

## サービス内容

### ■ 標準サービス

| メニュー概要 | | メニュー説明 |
|---|---|---|
| **セキュリティ監視** | ・アラート監視<br>・相関／影響度分析<br>・チューニング | セキュリティアナリストが24時間 365日 Microsoft 365 E5 Security と MDC で検知されるアラートを監視し、Microsoft Sentinel を利用して複数のログを相関分析した結果から、影響度を判断します。また、誤検知・過検知のアラート抑止や、既知の脅威をブロックするためのチューニングを行います。 |
| **アラート管理** | ・エスカレーション（通知）<br>・専用ポータルサイトの提供<br>・対処実施報告 | 対処が必要なアラートは影響度に応じた手段でお客さまにエスカレーションします。エスカレーションしたアラートはチケットとして管理し、ステータス管理やお客さまとのコミュニケーション、JBS で対処した実施内容の報告はポータルサイト上で行います。 |
| **報告・レポーティング** | ・レポート提供<br>・報告会 | 監視状況やセキュリティ状態を評価して記載したレポートと、Microsoft 365 E5 Security と MDC の更新情報やセキュリティトピックを記載した月次レポートを提供します。また、3か月ごとに報告会を開催し、提出しているレポートの報告など実施します。 |

### ■ オプションサービス

| メニュー概要 | メニュー説明 |
|---|---|
| ・有償版レポート<br>・セキュリティ運用代行<br>・インシデント対応 | 標準サービスで提供した月次レポートに付加情報を追加した有償版レポートの提供や、脆弱性対応や機能維持管理とはじめとするお客さま側で実施する必要があるセキュリティ運用業務を JBS が代行します。フォレンジック調査、インシデントハンドリング、対外対応など専門家が支援します。 |

## 価格（税抜）

お客さまの環境に応じて、見積もりします。詳しくはお問い合わせください。

| | |
|---|---|
| **前提条件** | ・Microsoft Defender for Endpoint が導入されている必要があります。<br>・お客さま環境の Microsoft Entra ID と紐づいた Microsoft Sentinel が必要です。<br>Microsoft Sentinel を導入していない場合はご相談ください。<br>・Microsoft Sentinel のログ取得、保管料はお客さま負担です。 |

JBS SOC は、JBS とＳ＆Ｊとの協業により提供されます。これまでに多数の Microsoft 365、Microsoft Azure のセキュリティ案件・運用を手掛けてきた JBS と、豊富なセキュリティ事故対応経験に裏打ちされた脅威分析力とアドバイス力に特徴のある、セキュリティ運用・監視を得意とするＳ＆Ｊが協業することで、Microsoft 365、Microsoft Azure を対象としたセキュリティ統合監視を実施します。
Ｓ＆Ｊは、2008年の創業以来、お客さまをセキュリティ事故から守ることを追求してきたセキュリティサービスの専門会社です。セキュリティ事故対応社数は200社以上、SOC導入社数は500社以上と豊富なセキュリティ運用の実績を持ちます。





お問い合わせ先
**日本ビジネスシステムズ株式会社**
〒105-6316
東京都港区虎ノ門1-23-1 虎ノ門ヒルズ森タワー16F
Tel：03-6772-4000 Fax：03-6772-4001
https://www.jbs.co.jp