2026 年 8 月 4 日
S & J 株式会社
代表取締役社長　三輪　信雄
東証グロース：5599

# S&J、SOC 自律化の潮流に応え「My SOC 365」に AI 自動対処機能を搭載、脅威検知から対処完了までを数十秒で実行

**～セキュリティ人材不足の市況に対し、夜間休日も自律対処・ワンクリック復旧で運用負荷を軽減～**

セキュリティ監視サービスやセキュリティ事故対応などのサイバーセキュリティ事業を展開するＳ & Ｊ株式会社（本社：東京都港区、代表取締役社長：三輪　信雄、証券コード：5599、以下「S&J」）は、Microsoft 365 を統合セキュリティプラットフォームとして最大限活用する「My SOC 365 サービス（以下、My SOC 365）」において、AI が複数ログを自ら調査・分析し、人の判断を待たずに初動対処まで自律実行する「自動対処機能」の提供を 2026 年 8 月 3 日（月）に開始しました。


「自動対処機能」は、My SOC 365 が検知した脅威に対して、AI が攻撃の確からしさと対処の推奨度を判定し、S&J 独自の対処ルールに基づいてアカウントの無効化や端末の隔離などの初動対処を自動で実行する機能です。人手では数時間を要していた分析から初動対処までを脅威検知から数十秒に短縮し、攻撃の被害拡大を迅速 に防ぎます。また、対処で停止したアカウントや隔離した端末は、安全確認のうえ顧客がワンクリックで復旧できます。
本機能は、2026 年 4 月 23 日の My SOC 365 提供開始発表時に「今後の展望*」としてお知らせしていた、インシデント対応の自動化を支援する SOAR 機能を具体化したものです。

*2026 年 4 月 23 日発表「S&J、AI により Microsoft 365 を統合セキュリティプラットフォーム化する『My SOC 365 サービス』の提供を開始」：
https://prtimes.jp/main/html/rd/p/000000039.000062785.html

## 背景：SOC 運用の自律化という世界的潮流と、被害の拡大を左右する「初動　対処の速さ」

セキュリティオペレーションセンター（SOC）の現場では、AI が検知だけでなく判断・対処までを担う自律型 SOC への移行が世界的な潮流となっています。そして、S&J は My SOC 365 の提供によりセキュリティ人材不足に悩む企業のセキュリティ監視を最

短 5 日で実現しましたが、今回の「自動対処機能」は、この人材不足という社会的な構造課題に対する回答をさらに一歩進めるものです。

こうした潮流に加え、サイバー攻撃による被害の大きさは、脅威を検知してから封じ込めるまでの初動対処の速さに大きく左右されます。しかし、多くの企業では、不審サインインやマルウェアを検知しても脅威/影響分析までに数時間以上かかることに加え、対処後の戻し方がわからないといった理由からアカウント停止や端末隔離に踏み切る判断ができず、初動が遅れがちです。特に夜間・休日は対応できる顧客担当者 が不在となり、攻撃者に猶予を与えてしまうケースが少なくありません。

S&J は、セキュリティ事故対応の豊富な実績に基づく対処ルールと AI による判定を組み合わせた自動対処機能の提供により、顧客担当者の判断や作業を待つことなく初動対処を自律実行し、顧客の被害を最小化します。

## My SOC 365 の概要

My SOC 365 は、AI と S&J 独自の運用ノウハウを組み合わせ、Microsoft 365（Microsoft Entra ID、Office 365、Microsoft Defender）に集約されたセキュリティログを 24 時間 365 日収集・分析し、高度な脅威検知と監視体制を最短 5 日で実現するサービスです。専任のセキュリティ人材を確保できない中堅・中小企業をはじめ、Microsoft 365 E7／E5／E3／Business Premium を導入する企業を対象に、2026 年 4 月 23 日発表、同年 5 月 11 日より提供しています。

## 自動対処機能の概要

| | |
|---|---|
| サービス名 | My SOC 365 サービス（読み方：マイ ソック サンロクゴ サービス） |
| 追加機能名 | 自動対処機能 |
| 提供開始日 | 2026 年 8 月 3 日（月） |
| 対処内容 | アカウントの無効化、端末の隔離 など |
| 対象プラン | ・スタンダードプラン<br>・プレミアムプラン |
| 利用料金 | 各プランの標準機能 として追加費用なし |
| 新規導入相談の受付 | 専用 Web ページにて受付 |
| 専用 Web ページ | https://www.sandj.co.jp/services/mysoc365/ |
| 導入済みユーザーの申し込み方法 | 顧客に事前告知の上、自動実装 |

## 自動対処機能の特徴

**1. AI による判定 で、過剰対処と見逃しの削減**

アラートを検知するたびに、熟練したセキュリティアナリストの調査手順を AI が実行。必要なログを自ら再検索・分析し、攻撃の確からしさを高い精度で見極めます。導入時のノイズチューニングが不要なため、過剰対処と見逃しの双方を抑えた初動対処を実現します。

**2. 脅威検知から数十秒、夜間・休日も自動実行**

セキュリティ事故対応の実績に基づく S&J 独自の対処ルールにより、アカウントの無効化や端末の隔離を検知から数十秒で自動実行します。顧客担当者が不在となりがちな夜間・休日もシステムが自律的に対処するため、攻撃者に猶予を与えません。

**3. 自動対処からの復旧はワンクリック**

自動対処で停止したアカウントや隔離した端末は、安全確認のうえポータルからワンクリックで復旧できます。「対処後の戻し方がわからない」という運用上の不安を解消し、自動対処を可能 にします。

**4. 業務影響をコントロールする安全装置**

自動対処の緊急停止機能や、特定のアカウント・デバイスを対処対象から除外する設定を備えており、顧客の業務実態に合わせて自動対処の適用範囲を柔軟にコントロールできます。

**5. 追加のソフトウェア導入は不要**

My SOC 365 はエージェントレスで動作するため、自動対処機能の利用にあたって端末へ追加のソフトウェア導入は不要です。既存の Microsoft 365 環境をそのまま活かし、セキュリティ投資 の効果を最大化します。

## 今後の展望

S&J は今後も「Microsoft 365」と「My SOC 365」の連携をより強化しながら、AI 活用による“検知・判断・対応”の高度化を通じて顧客のセキュリティ運用をトータルで支援し、インシデントによる実害ゼロの実現に向けて取り組んでまいります。

**■ S & J 株式会社について**

S&J は、サイバー攻撃や内部関係者による情報漏えい等の内部犯行など、情報セキュリティは経営課題として認識されてきている状況下、「防御・検知・対処」や「技術・体制」のバランスを重視した製品やサービスを提供しています。

SOC（セキュリティオペレーションセンター）は、従来のアラート監視での脅威お知らせサービスに加え、顕在化した脅威による顧客環境での高度な影響分析やトリアージをアナリストが行い、影響に応じて事故の封じ込めのハンドリングやフォレンジックまで迅速な対応をすることにより、業務継続と再発防止策を支援しています。

| | |
|---|---|
| 商号 | S & J 株式会社 |
| 所在地 | 〒105-0004 東京都港区新橋一丁目 1 番 1 号 日比谷ビルディング 8F |
| 設立 | 2008 年 11 月 |
| 資本金 | 4 億 4162 万円 |
| 代表取締役社長 | 三輪 信雄 |
| 事業内容 | サイバーセキュリティ事業<br>■ セキュリティ監視／運用<br>■ コンサルティングサービス<br>■ セキュリティ事故対応 |
| Web サイト | https://www.sandj.co.jp |

**■プレスリリースに関するお問い合わせ**

S & J 株式会社 広報担当 E-mail：pr@sandj.co.jp / TEL：03-6205-8500（代表）

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

※本リリースのすべての内容は、作成日時点でのものであり、予告なく変更される場合があります。
また、様々な事由・背景により、一部または全部が変更、キャンセル、実現困難となる場合があります。
予めご了承ください。

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝