2026年3月期 第1四半期決算説明資料

Ｓ＆Ｊ株式会社

証券コード：5599 / 東証グロース市場

2025年8月13日

1. 会社概要
2. 第1四半期業績
3. 成長戦略
4. トピックス
5. Appendix
6. 用語解説

1. 会社概要

サイバーセキュリティカンパニー

経営理念

お客様の期待を常に考え「ありがとう」と言われる
セキュリティサービスを提供する。

経営方針

セキュリティ監視、対処、アドバイスを通じて、お客様に安全と安心を提供する。
自動化・AI活用を推進して効率化を図り、お客様とのコミュニケーションの機会を最大化する。

業績ハイライト（FY2025 / 1Q）

高いサービス継続率と高いストック売上比率により安定的な年間利益確保を実現

売上高 / 前期比成長率

537百万円(FY2025/1Q) / **18.8**%(前年同期比)

ARR(1)/翌事業年度の売上基盤として見込まれる金額

1,929百万円(FY2025/1Q)

営業利益 / 営業利益率

127百万円(FY2025/1Q) / **39.2**%(FY2025/1Q)

ストック売上比率(2)

86.4%(FY2025/1Q)

サービス継続率(3) / 解約率(4)

99.4%(FY2025/1Q) / **0.6**%(FY2025/1Q)

従業員数(5) / 増加数

66名(FY2025/1Q) / **3**名増(前期比)

注：(1)Annual Recurring Revenue（年間経常収益）の略。各サービスにおける月額固定の継続的契約（主に年間契約）をストック売上と定義し、事業年度末のストック売上を 12 倍することにより算出。(2) 各サービスにおける月額固定の継続的契約（主に年間契約）をストック売上と定義し、事業年度における全体の売上に占めるストック売上の割合 (3)100%－解約率 (4) 前月のストック売上高に対して、当月の解約・減額等の売上高の比率を算出し、事業年度を通じた平均値（各月の解約率の12 か月分÷12）(5) 期末の従業員数。役員、派遣社員、SES 等は含まない。

当社紹介

2025年8月1日現在

会社概要

会社名	Ｓ＆Ｊ株式会社
設立	2008年11月7日
資本金	4億4,162万円
決算月	3月
従業員数	72名（派遣社員、SES除く）
事業内容	SOC(1)サービス コンサルティングサービス

役員一覧

代表取締役社長
三輪 信雄

取締役 営業部長
石川 剛

取締役 セキュリティプロフェッショナルサービス部長
上原 孝之

取締役 管理部長
經田 洋平

取締役 コアテクノロジー部長
半澤 幸一

取締役
星野 喬

取締役(監査等委員)
大桃 健一

取締役(監査等委員)
谷井 亮平

取締役(監査等委員)
林 孝重

注：(1)SOC：Security Operation Center。ネットワークの監視を行い、サイバー攻撃の検知や分析、対策を講じる専門組織。詳細は用語解説の頁にて記載しています。

社名とシンボルについて

社名

"S&J" は「千里眼」（Senrigan）と「順風耳」（Junpuji）のアルファベット表記の頭文字に由来しています。

S&J

当社のロゴと社名には、常にインシデントの兆候を探り（検知）、事前に対策を講じ（防御）、事故が発生した場合にも迅速に対処し（対処）、被害を最小限に抑えるサービス提供への熱意が込められています。

シンボル

「千里眼」（緑鬼）
"媽祖※の進む先やその回りを監視し、
あらゆる災害から媽祖を守る役目を担います。

「順風耳」（赤鬼）
あらゆる悪の兆候や悪巧みを聞き分けて、
いち早く媽祖に知らせる役目を担います。

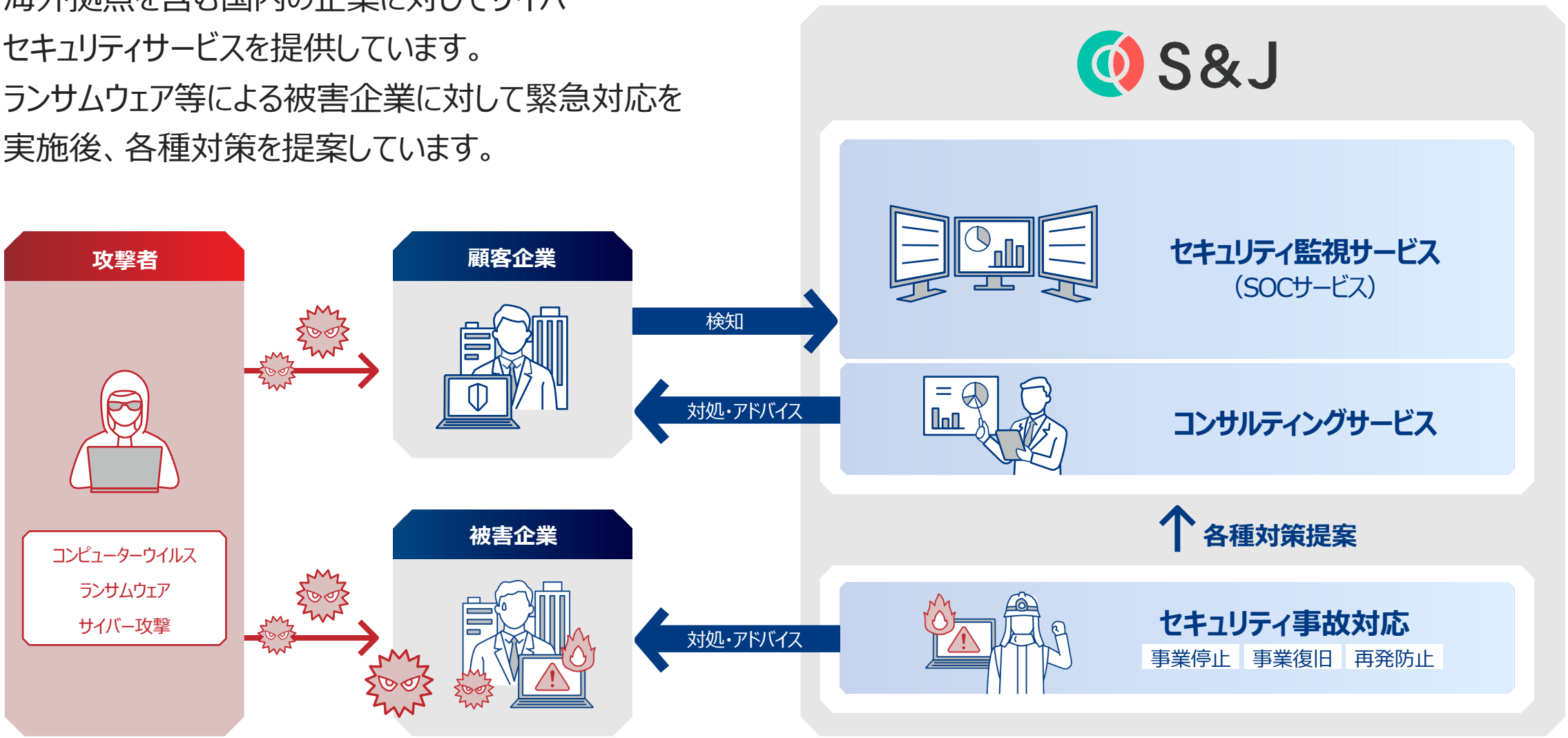
※媽祖は中国が発祥の海上守護神です。千里眼と順風耳を従え、航海の安全を守るとされています。

創業当初から予見し提供していた"監視"と"対処"の重要性

当社はセキュリティ“監視”だけではなく、サイバー攻撃に対する“対処”までを行い、今後の具体的な対応についてなどの“アドバイス”までを提供しています。
多くのセキュリティ事故対応に立ち会い、事故対応の経験に基づいたコンサルティングのアプローチがすべてのサービスに反映されているため、
お客様の期待を超えるアドバイスが実現できています。

事業概要

海外拠点を含む国内の企業に対してサイバーセキュリティサービスを提供しています。
ランサムウェア等による被害企業に対して緊急対応を実施後、各種対策を提案しています。



S&Jの強みと特徴

【柔軟性】

●カスタムメイド可能なセキュリティ監視サービス(SOC)

【技術力】

●高度な技術力による自社開発製品(国産)を用いた競争力のあるSOC

【知見・実績】

●ランサムウェアなどのインシデント対応経験が豊富

従来のセキュリティ監視サービスと、当社のセキュリティ監視サービスの違い

従来のセキュリティ監視サービス（アラートお知らせサービス）

- 監視機器からのアラートのうち、重要度、影響度をフィルタリングしてお知らせする。
- 環境に応じた対処方法までの説明がなされていない。
  ▶ **対処方法はお客様にて検討必要**
- 主にメールなどで一方的かつ画一的な対応が主流となっている。

- 危険性は理解したが、具体的な対処方法がわからない。
- 夜間や休日などにアラートを知らされても対処できない。

顧客ニーズの変化

- 自社環境に応じた具体的な対処、推奨される対処方法を教えて欲しい。
- 危険性が高い場合には、対処して欲しい。

当社のコミュニケーション型セキュリティ監視サービス

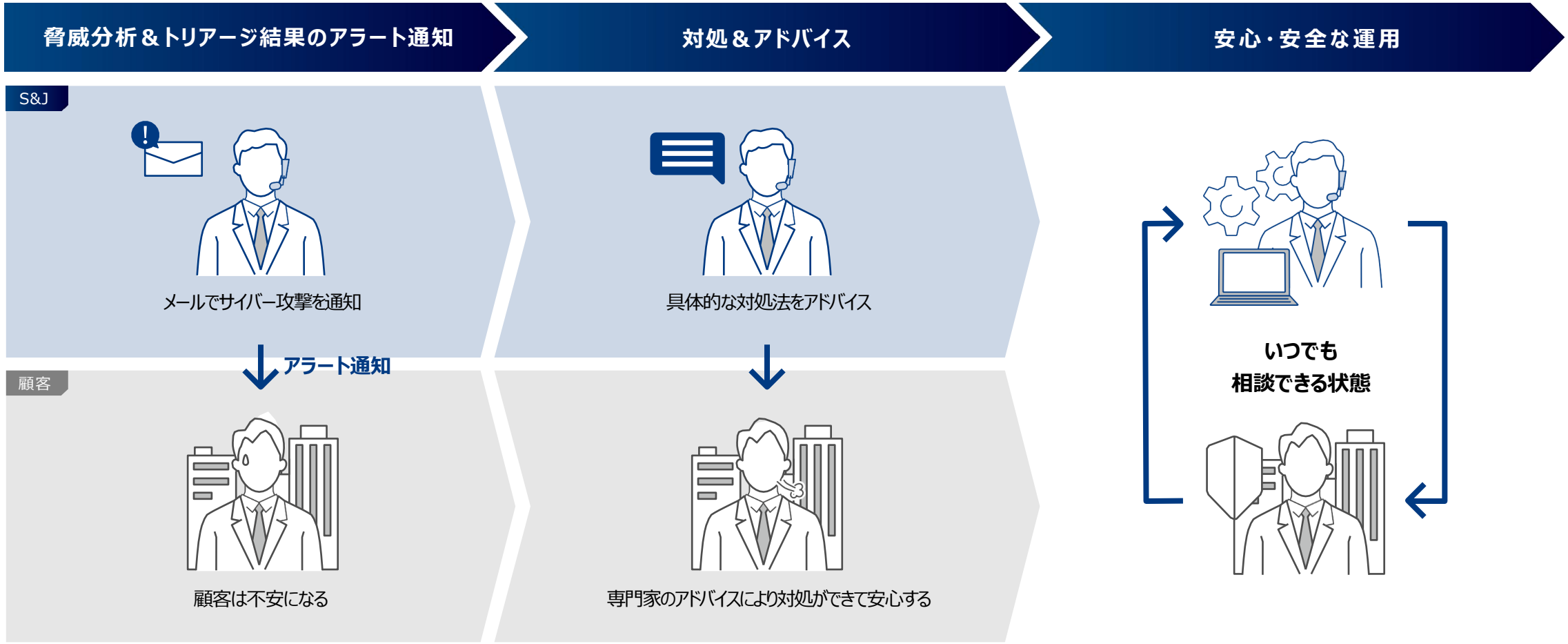
- **お客様とのコミュニケーションをとりつつ、対処方法等を推奨できるセキュリティ監視サービスを目指す。**
- **危険性が高く、緊急性が高い場合には遠隔での対処を実施する。**

- 環境に応じた対処方法がわかる。
- 夜間や休日に危険性が高い場合には対処してくれている。

セキュリティ運用のワークフローをアウトソーシングできる当社のセキュリティ監視サービス

＜深刻ではないアラートの場合＞

お客様環境を考慮した脅威分析＆トリアージを行うことにより、適切な対処方法まで助言が可能。



セキュリティ運用のワークフローをアウトソーシングできる当社のセキュリティ監視サービス

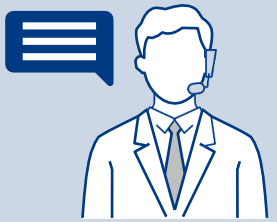
＜夜間などの顧客不在時の対応フロー＞

当社によって緊急対応が速やかに実施され、恒久対応方法まで含んだ支援が可能。

サイバー攻撃発生	緊急対処	出社時には解決済み 事後アドバイス	安心・安全な運用

S&J

遠隔でネットワーク隔離
緊急対応を実施し被害を最小化



翌日には一次対処が完了済み
加えて恒久的な対応策のアドバイスの実施

いつでも
相談できる状態

顧客

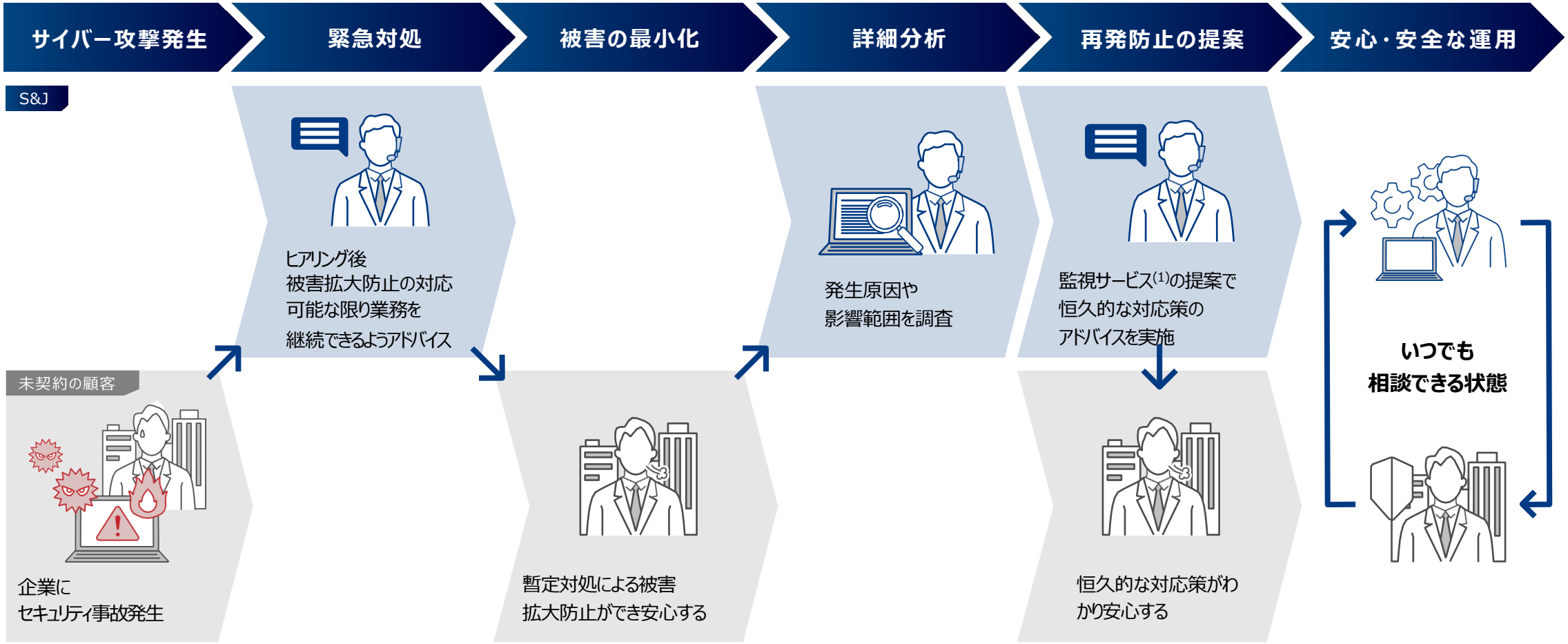
担当者不在時にサーバー攻撃が発生

対処済みで
恒久的な対応策もわかり安心する

セキュリティ運用のワークフローをアウトソーシングできる当社のセキュリティ監視サービス

＜セキュリティ事故対応フロー＞

業務継続を優先的に考え、緊急対応の実施と恒久対応方法まで含んだ支援が可能。



注：(1)SOC監視、EDR監視、自社製品監視、Microsoft 製品監視など。

SOCツアーの開催

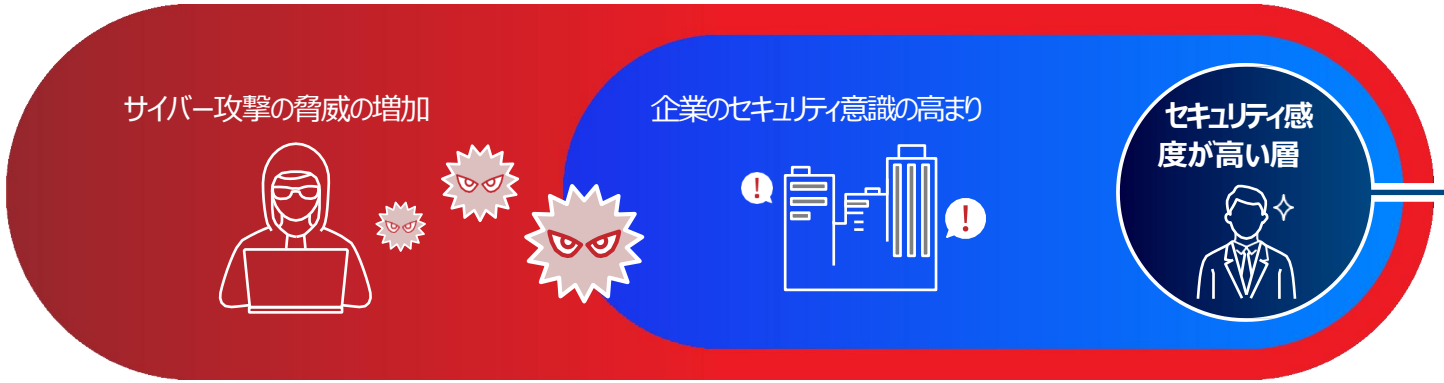
【SOC概要】
①さまざまな製品に対応したセキュリティ監視
②自社開発能力を最大限活かした監視サービス
③インシデント対応に最適化した分析/対応環境

【SOCツアー実施の目的】
①既存顧客のアップセル・解約率の低減
②競合排除・受注期間の短縮
③協業企業とのアライアンス向上・案件相談の増加

【SOCツアーの特徴】
①先進的な設備
②SOCコンセプトの共有
③サイバー攻撃被害対応の模擬体験
④模擬体験を通じた高い技術力の訴求

当社の顧客層

セキュリティ感度が高い層が当社のメイン顧客層

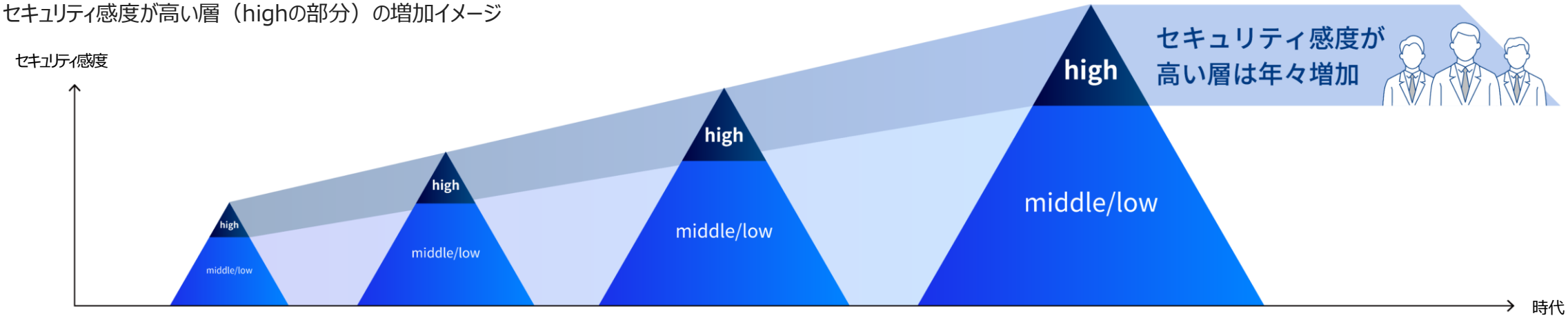


ここが当社のお客様

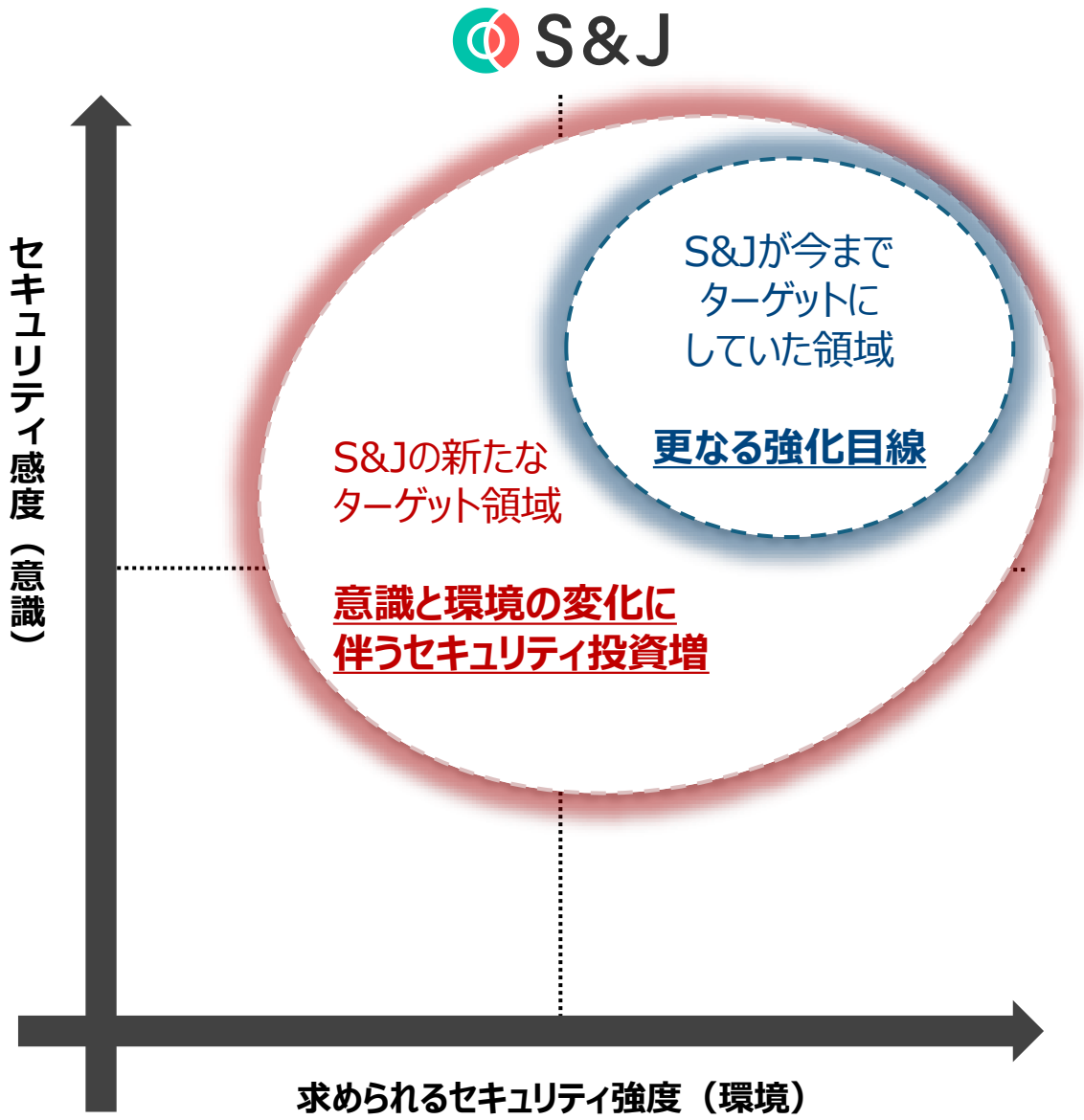
当社の**「セキュリティ感度が高い層」**の定義

- セキュリティ運用の苦労を実感として分かっている
- セキュリティに対しての知見をしっかりと持っている
- 既存のSOCベンダーのサービスに不満を持っている
- 未来のセキュリティ環境について想像力を働かせている

セキュリティ感度が高い層（highの部分）の増加イメージ



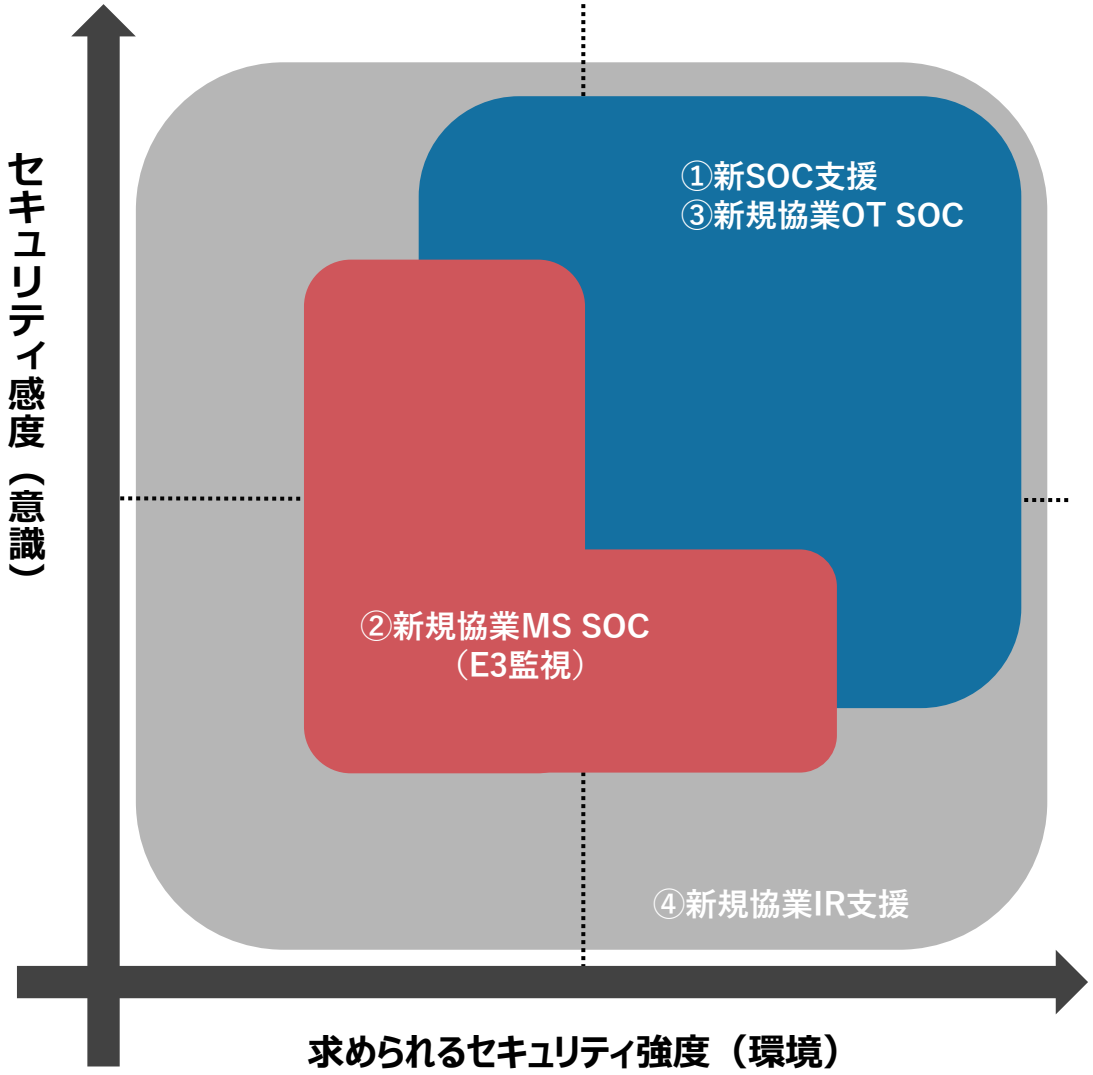
S&Jが狙う市場



【当社のターゲット】

- セキュリティ意識が高く、更なるセキュリティの強化が必要なお客様
- お客様の意識と環境が変化し、高度なサービス品質が必要になってきた
- 競合他社が存在する領域だが、高品質なサービスで差別化が可能

S&Jの新たなサービスと販売戦略



①新たな「監視センターの在り方」の訴求によるお客様のファン化

- 無人監視や、監視センター自体の「場」の有効活用による最先端な監視モデル
- 監視範囲の拡大による新たなターゲット領域へのアプローチ
- AI機能強化による監視サービスの高度化と顧客数の拡大

②Microsoft市場への参入アプローチ

- Microsoft社との協業によるMicrosoft市場へ提供可能なSOCサービス開発中
- Microsoft市場への新たな収益モデルの確立
- AI監視によるサービスと人員の効率化

③新たに攻撃対象となった製造業環境へのアプローチ

- サイリーグ社との協業による「OT環境」への監視サービススキーム検討中
- 製造業向けに提案手段が増えたことによる新たな収益モデルの確立

④新規協業IR支援でのアプローチ

- サイリーグ社との協業によるインシデントレスポンス支援のスキーム検討中
- 両社が支援するお客様すべてが対象となる、監視提案の「トリガー」となりえるサービス

2.第1四半期業績

業績サマリー(FY2025 / 1Q)

- 売上高は、537百万円と前年同期比18.8%増、進捗率21.3%
- 営業利益は、127百万円と前年同期比39.2%増、進捗率24.5%
- 当期純利益は、87百万円と前年同期比39.2%増、進捗率24.9%

	FY2024 第1四半期		FY2025 第1四半期				FY2025通期（業績予想）	
	実績	対売上高	実績	対売上高	前年同期比増減額	前年同期比増減率	予想	進捗率
売上高	452	100.0%	**537**	100.0%	+85	+18.8%	2,519	21.3%
営業利益	91	20.2%	**127**	23.6%	+35	+39.2%	519	24.5%
経常利益	91	20.3%	**127**	23.6%	+35	+38.6%	521	24.4%
当期純利益	62	13.9%	**87**	16.3%	+24	+39.2%	352	24.9%

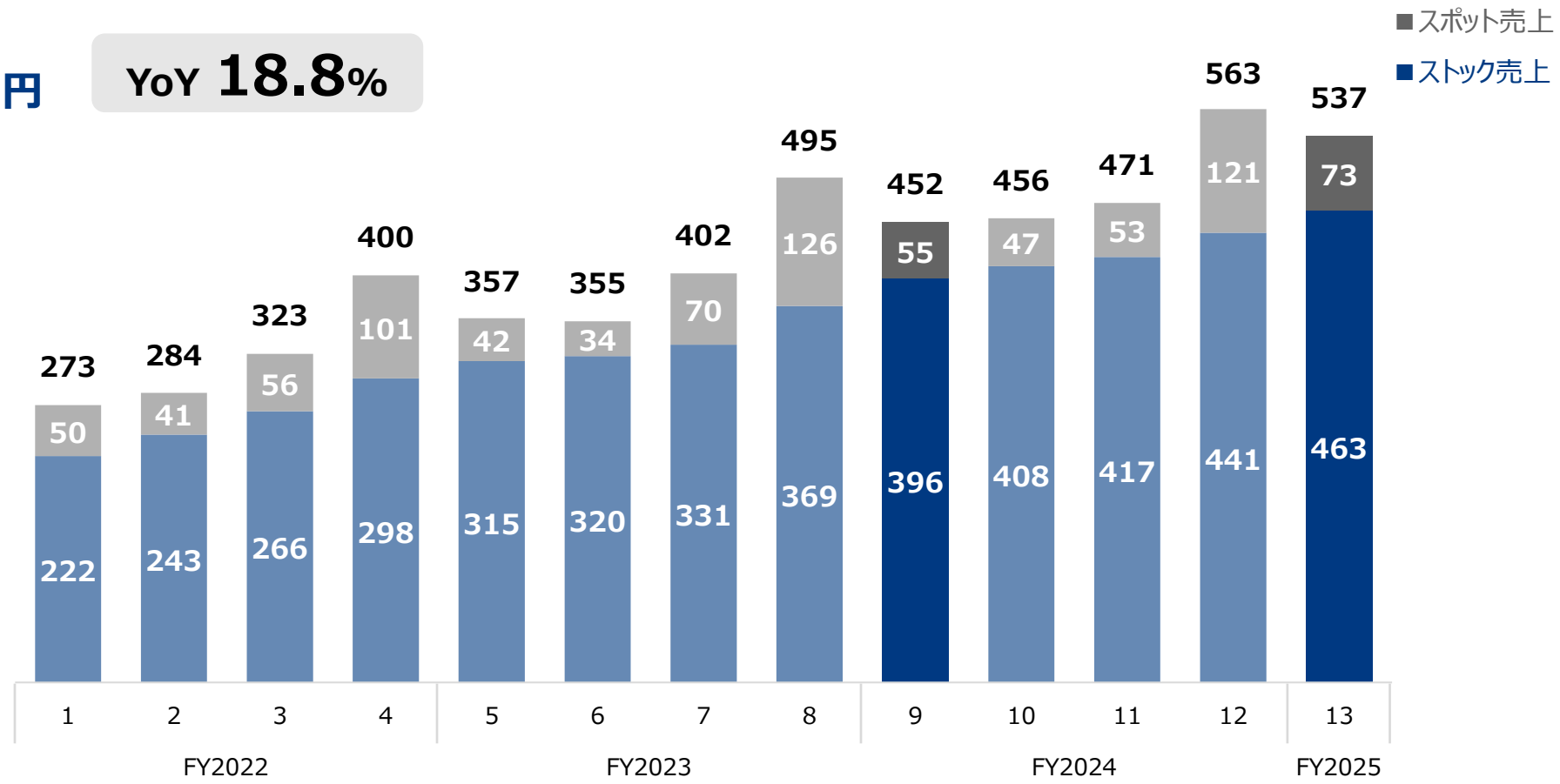
業績ハイライト　売上高（FY2025/1Q）

- 売上高は、537百万円と前年同期比18.8%増。
  ストック売上である監視サービスの積上げに加え、スポット売上であるインシデント対応支援等を実施。

売上高

537百万円

YoY **18.8%**

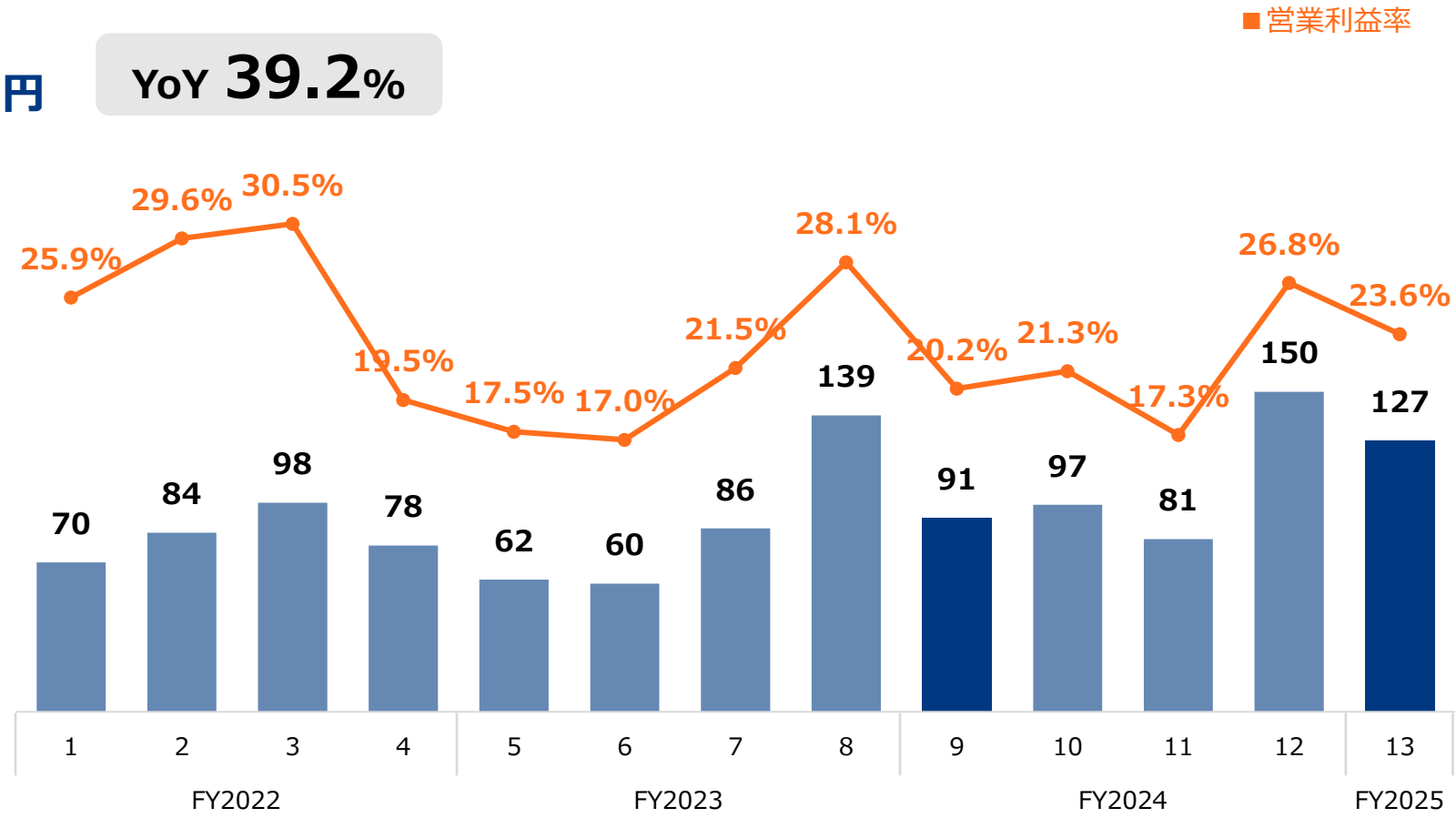


業績ハイライト　営業利益･営業利益率（FY2025/1Q）

- 営業利益は、127百万円と前年同期比39.2%増。
  オフィス移転によるコスト増があるものの、売上の積上げにより大幅増益。

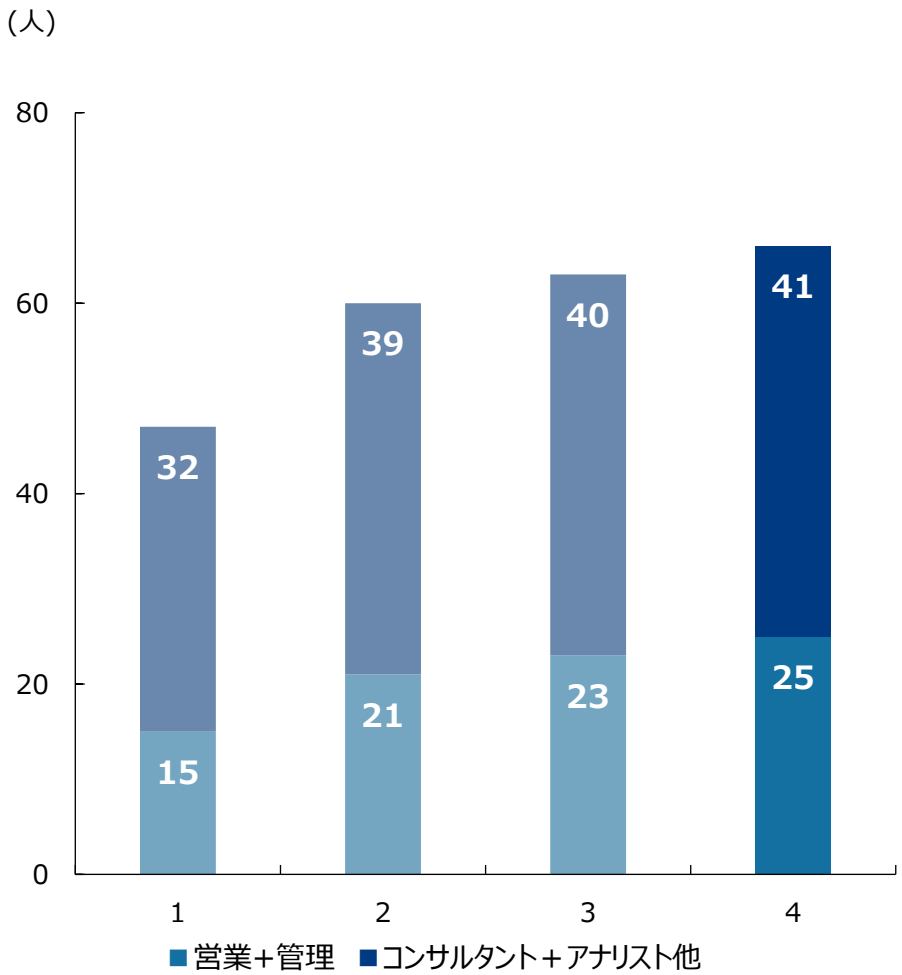
売上高

127百万円　YoY 39.2%



経営指標

人員推移 (1)



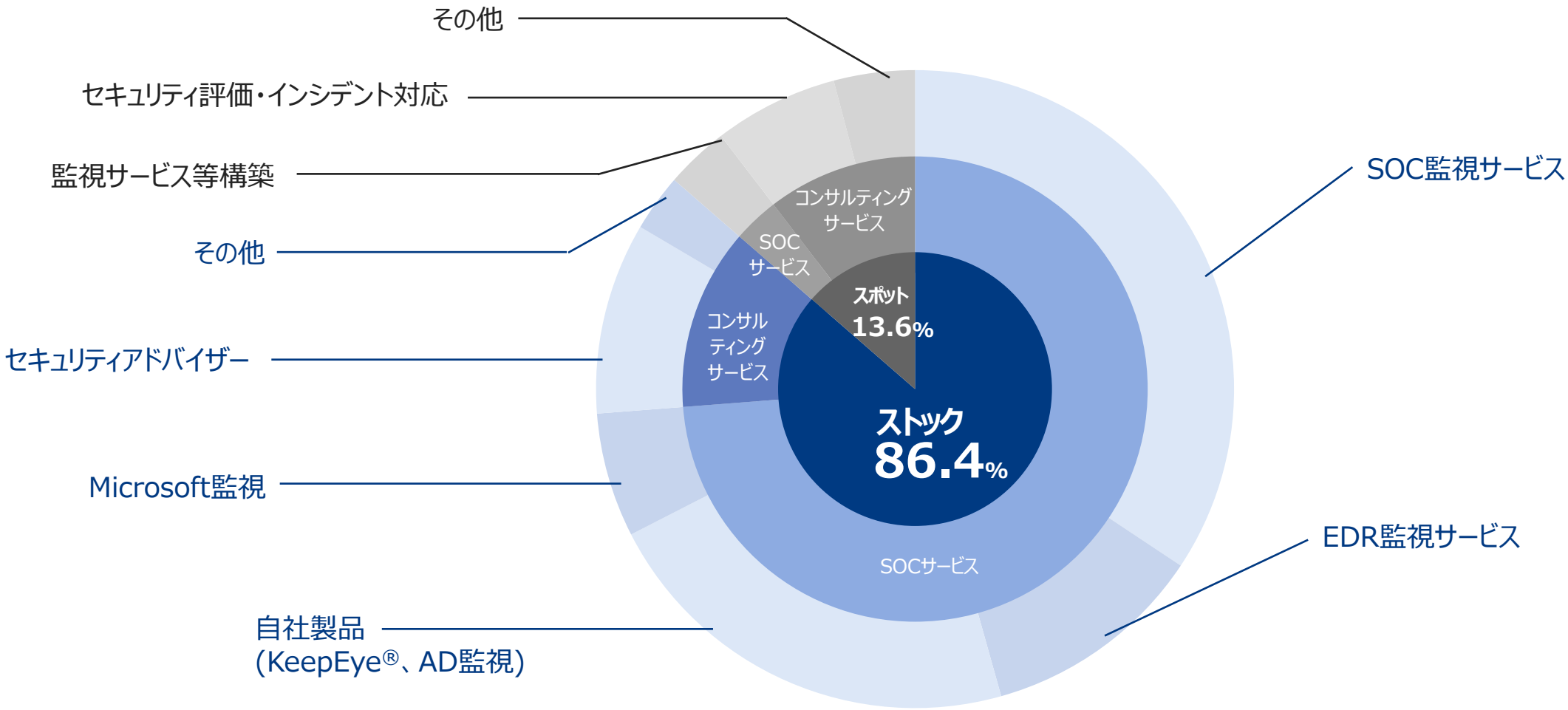
- **人員の採用は順調に推移**
- **働きやすい職場環境の整備**
  - ①テレワークでの就業
  - ②有給休暇の充実（初年度15日/年、時間有休制度）
- **福利厚生制度の充実**
  - ①資格取得・維持支援制度
  - ②入社支度金制度
  - ③企業型確定拠出年金制度
  - ④GLTD保険 (2) 加入

注：(1)役員や派遣社員は含まれない。(2)GLTD保険：Group Long Term Disabilityの略、ケガや病気で長期間就業不能になった場合の所得を補償する保険。

3. 成長戦略

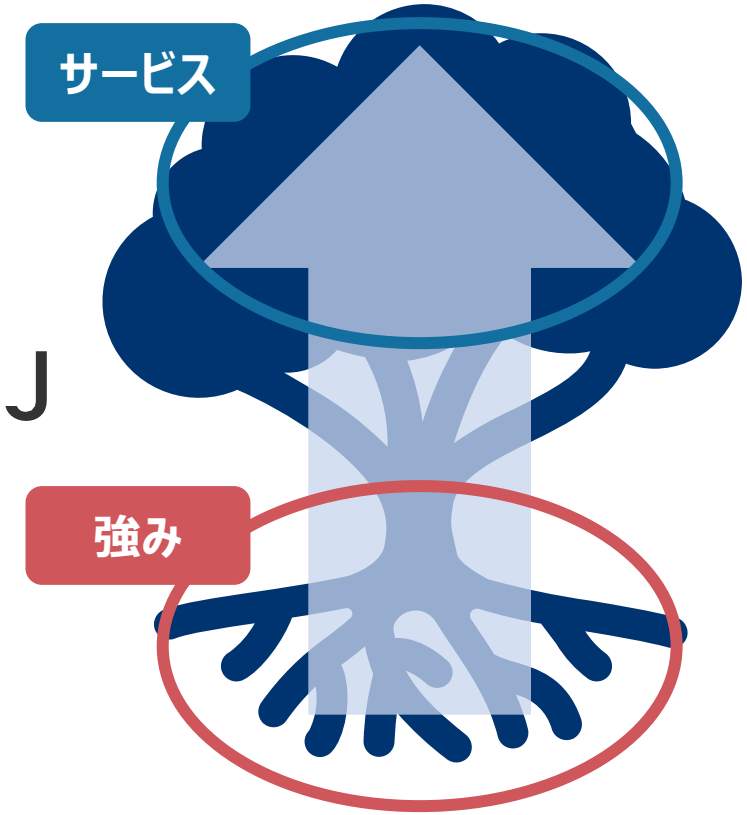
収益内訳

ストック売上で構成された強固な収益基盤（ストック売上比率86.4%） FY2025 / 1Q



成長戦略の根幹となるS&Jの強み

- S&Jの強みは、圧倒的なサイバー攻撃被害対応能力と実績
- 被害現場で経験してきたことを、各サービスに活かせる
- MSSではなく、10年以上前から提供してきた統合SOCの圧倒的実績



S&J

サイバー攻撃被害対応実績が増えれば増えるほど、
実践的な対策・監視・対処のあるべき姿を把握
その経験を活かしてお客様に適切な対処や再発防止を助言する
コミュニケーション型統合SOCサービス（＝MXDR(1)）
で支援

×

S&Jの強みの根源は、
サイバー攻撃被害対応能力と
統合SOCの実績

注：(1)MXDR：Managed Extended Detection and Response。システム全体における脅威検知とインシデントへの処置までを代行するサービス。

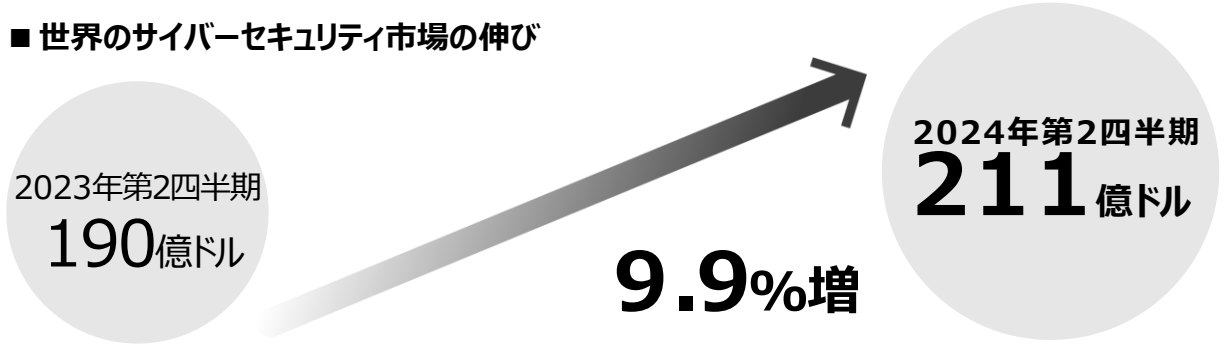
成長戦略①：サイバーセキュリティ市場で圧倒的に伸びているMicrosoftに注力

Microsoft 365 E3/E5を用いた統合的な運用監視と、お客様で利用している既存機器やサービスを柔軟に組み合わせて監視サービスを提供できる当社の強みを活かして注力する

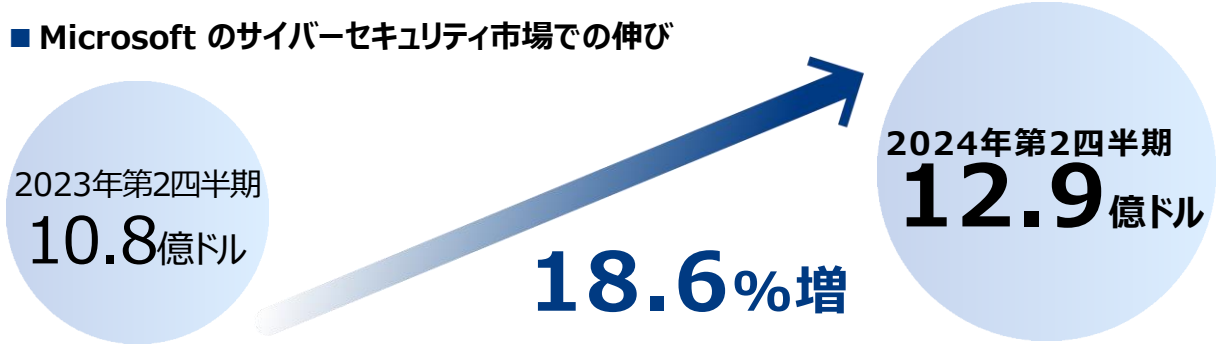
ベンダー	2023年第2四半期 市場シェア	2024年第2四半期 市場シェア	前年同期比 売上高成長率
Palo Alto Networks	9.50%	9.70%	11.20%
Fortinet	6.90%	7.00%	11.10%
Microsoft	**5.70%**	**6.10%**	**18.60%**
Cisco	6.00%	5.80%	5.30%
CrowdStrike	3.70%	4.50%	33.20%
Okta	3.40%	3.60%	16.60%
Check Point	3.60%	3.50%	6.70%
Zscaler	2.50%	3.00%	31.30%
Symantec	2.90%	2.70%	3.20%
IBM	2.70%	2.50%	2.50%
Trellix	2.60%	2.40%	2.10%
Splunk	2.40%	2.40%	13.50%
その他	48.10%	46.80%	6.90%
合計	100%	100%	9.90%

2024年第2四半期のサイバーセキュリティ市場は前年同期比9.9%増の211億ドルとなった。

■ 世界のサイバーセキュリティ市場の伸び



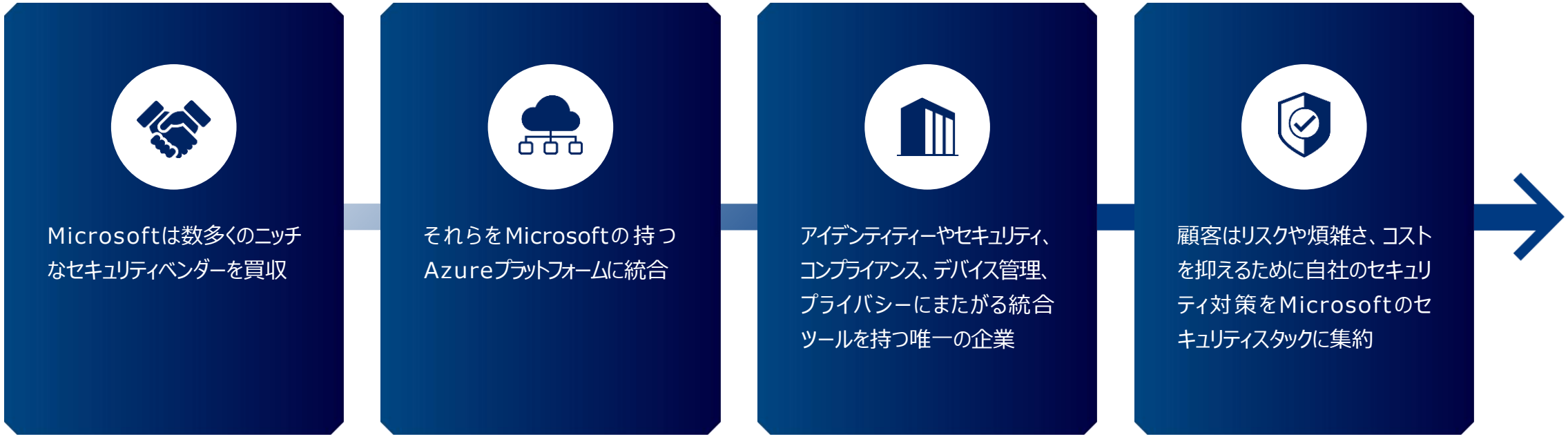
■ Microsoft のサイバーセキュリティ市場での伸び



出典：https://www.canalys.com/newsroom/worldwide-cybersecurity-technology-market-Q2-2024

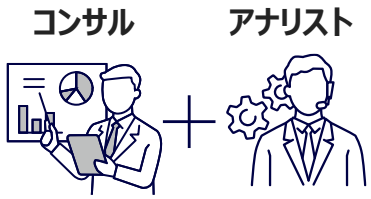
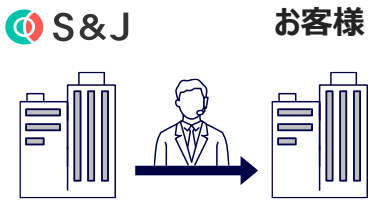
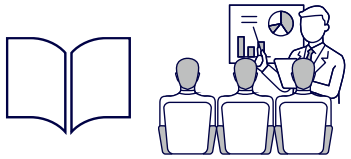
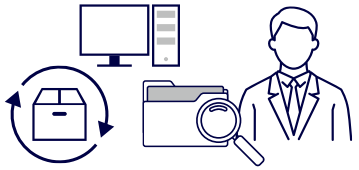
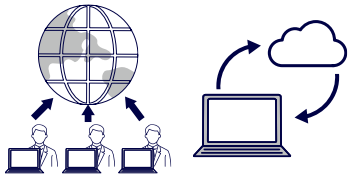
Microsoftのセキュリティビジネスが伸長する理由

当社の幅広い製品を監視してきた知見・経験を活かし、Microsoft製品を含む統合的な監視サービスをいち早く提供し、収益の拡大をはかる



出典：CYBERSECURITY DIVE Published Jan.30 2023 https://www.cybersecuritydive.com/news/microsoft-20b-security-revenue/641498/

成長戦略②：当社への期待・ニーズに合わせた新サービスをアップセル

	既存サービスの拡張	新領域へのチャレンジ ⇒ より総合的なアドバイスができるコミュニケーション型SOCへ			
新サービス	 リードアドバイザリー支援	 セキュリティ専門家による常駐支援	 人材育成可能な教育支援	 プロダクト販売からのSI支援	 グローバル・DXIoT対応支援
期待ニーズ	総合的なアドバイス 	専門家不在への対処 	セキュリティ知見不足への対処 	上流工程からの関与 	監視のグローバル対応DX/IoT推進 
既存サービス	• セキュリティ戦略の立案と実運用へのアドバイス • インシデント対応を含めた、相関分析やトリアージまで行う統合SOC • 企業の弱点を可視化する脆弱性診断				

成長戦略の中期計画

S&Jの目指す姿

- 信頼されるセキュリティアドバイザー
- IT / IoT環境のセキュリティ課題に応える価値創造を通じ、企業価値を向上

目指す姿に向けて

- 高収益化
- 成長性の追求
- スピードの追求
- プレゼンス向上

FY2027 以降 テーマ：AIを活用した分析とコミュニケーションの強化

- AIアナリスト化による分析の高度化と省力化
- AIアドバイザによる即時助言対応と省力化

FY2026 テーマ：新規領域の拡販

- 常駐支援ビジネスの立ち上げ
- Microsoftを中心にしたライセンス販売を含めたSI支援の拡販
- 教育支援及びグローバル・DX・IoTに対応したSOCサービスの拡販

FY2025 テーマ：MXDRサービスの進化/ ブランディング・マーケティング強化

- 教育支援ビジネス・ライセンス販売を含めたSI支援ビジネスの立ち上げ
- グローバル・DX・IoTに対応したSOCサービス化
- 新SOCをコアにした企業認知度のブランディング及び、サービス認知度向上のマーケティング

FY2024 テーマ：サービスの高度化 / クラウド環境向けサービス拡販

- SOCとコンサルティングを包含し、MXDRサービスとして遡及
- グローバル対応（多言語対応）の推進（SOC、コンサルティング）
- クラウド環境向けサービス拡販

対応結果

- 組織体制の変更を行いサービス提供開始
- 英語対応の準備が完了し、今後は各国法や多言語対応を検討
- Microsoftクラウドサービスは実現済み　AWS/Googleクラウドは協業での提案推進中

4. トピックス

2025年5月20日

S&JとサイリーグHD、共同開発による事前契約型インシデント対応サービスを2025年7月より提供開始

～企業・組織のレジリエンスを高める新サービス――緊急時も迅速・確実な対応を実現～

- 限られた一部企業にしか提供できなかった高水準のサイバーセキュリティサービスを、より多くの企業・団体に向けて展開可能に
- 年間契約により、突発的なインシデント対応費用の不確実性を排除し、安定した予算管理が可能
- 脅威インテリジェンスや定期ミーティングによって、潜在的リスクを可視化し、平時からの継続的な改善を支援
- 経験豊富なセキュリティ専門家が事前にアサインされるため、被害発生時の初動対応を迅速かつ的確に実施

S&J

セキュリティ監視、脅威検知、インシデント対応といった実務に精通した多くの専門人材を擁し、先進的な技術力と運用ノウハウ

×

CyLeague

サイリーグHDとそのグループ会社は、全国の企業・自治体とのネットワークを活かした幅広い課題把握と展開力に強みを有する

お客様は、あらかじめ「CyLeague サイバーレジリエンス・パッケージ ～サイバー攻撃対応サービス～」の契約を結んでおくことで、万一のサイバー攻撃の被害発生（インシデント発生）時にはS&Jのセキュリティの専門チームが対応に着手し、対応開始までの時間的ロスを最小化し、復旧までの期間短縮や業務への影響抑制が可能となります。また、四半期ごとの脅威インテリジェンス提供や定例会を通じて、最新のリスク情報を共有し、組織の対応力を継続的に高めていく仕組みも備えています。これにより本サービスは、単なる緊急時の対応窓口にとどまらず、お客様の事業継続と成長を支える「戦略的パートナー」としての支援を提供いたします。

2025年8月6日

S&JとサイリーグHD 、SMBCサイバーフロントの新プランに事前契約型インシデント対応支援機能を提供開始

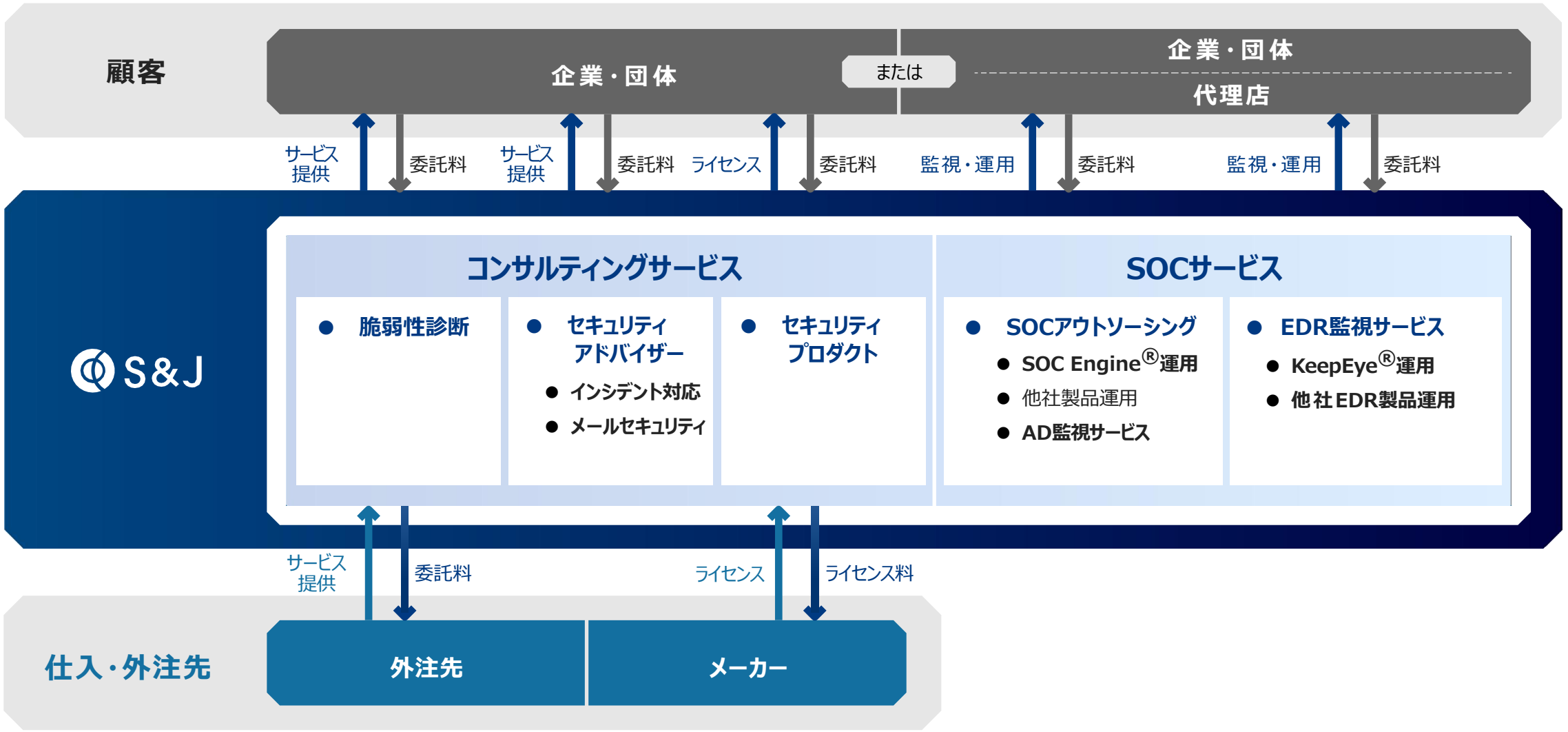
～中堅・中小企業のサイバーレジリエンスを強化する新たな協業モデル～

- 株式会社三井住友フィナンシャルグループを中心として設立されたサイバーセキュリティ対策事業会社となるサイバーフロント株式会社と協業
- SMBCグループの営業力を活かして、中堅・中小企業の経営層に対するアプローチを広く展開
- 万が一のセキュリティインシデント発生時に円滑に対応を開始できる体制をあらかじめ確保でき、迅速な初動と早期の業務復旧支援をするサービスを提供

S&J は、今後もサイリーグHDとSMBCサイバーフロントとの連携を強化し、全国の中堅・中小企業に対し実効性のあるサイバーインシデント対策をお届けするとともに、今回の協業モデルを通じて、パートナーやアライアンス企業との連携を広げることで、日本全体のサイバーレジリエンスの底上げに貢献してまいります。

5. Appendix

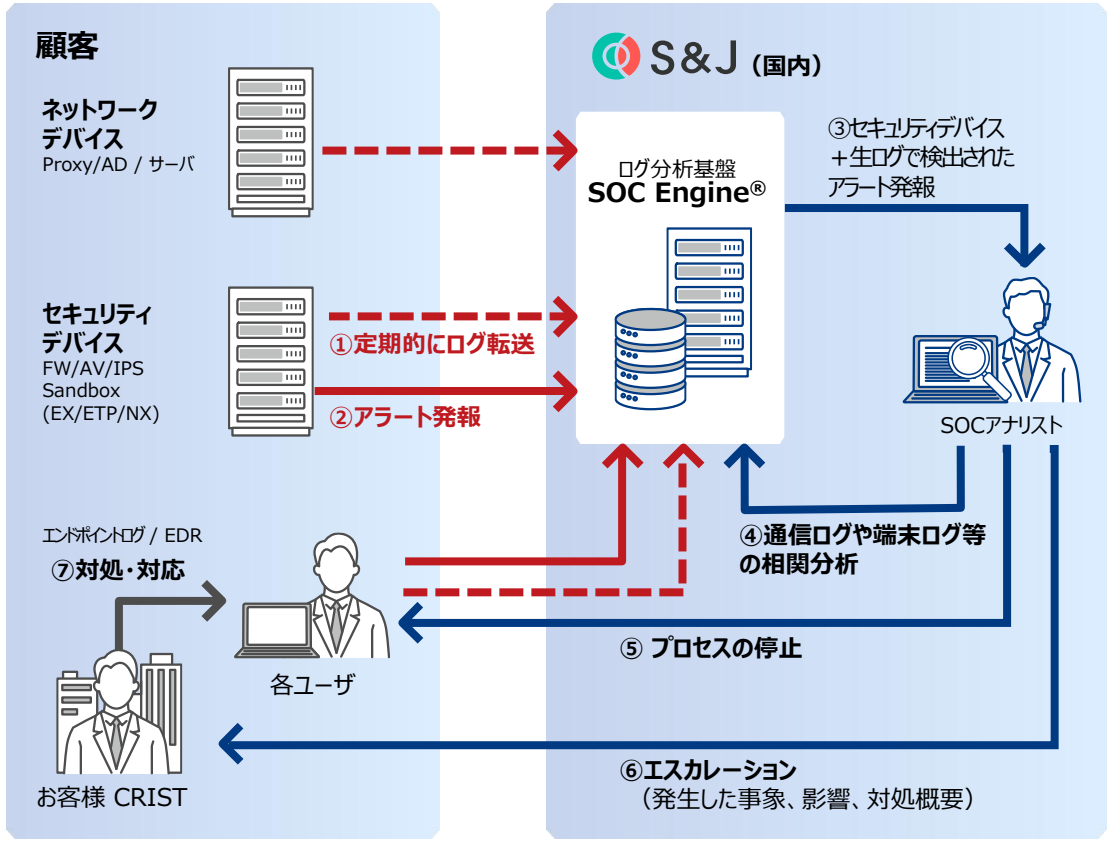
ビジネスモデル（収益構造）



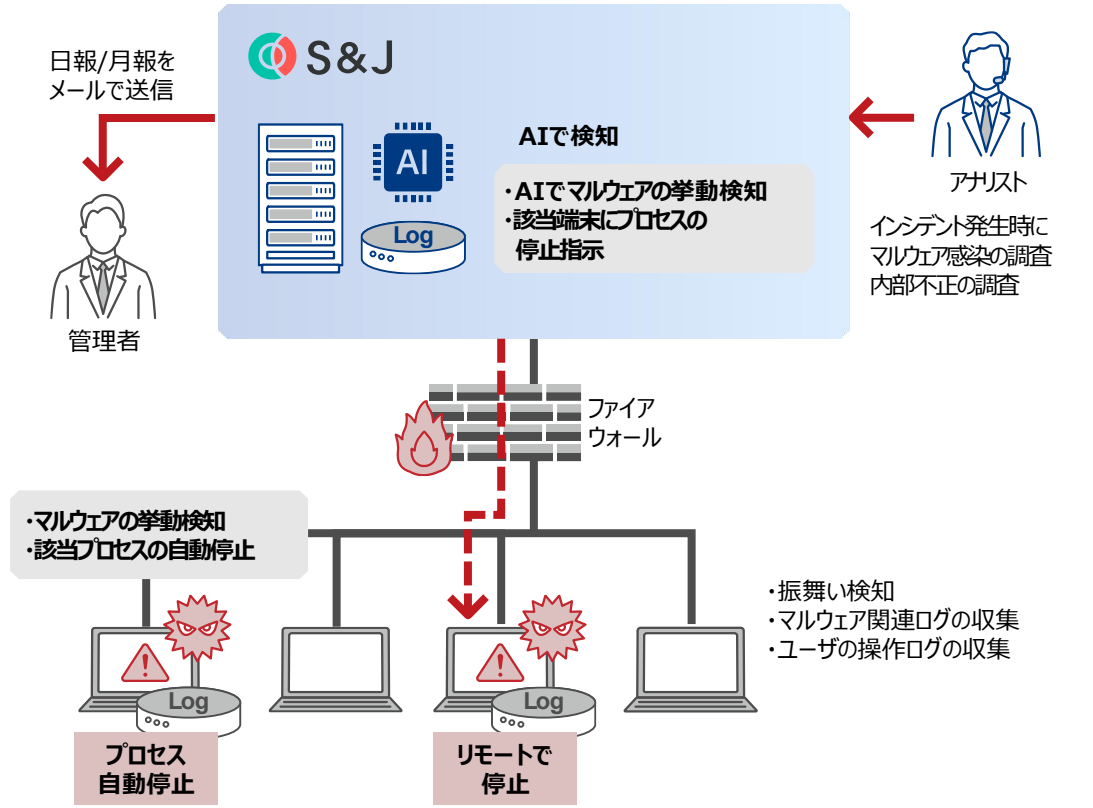
セキュリティ監視（SOC）サービス説明

セキュリティ監視サービスを提供

SOC監視サービス（SOC Engine®(1)の場合）



EDR監視サービス（KeepEye®(2)の場合）



注:(1) 当社独自開発のSIEM(Security Information and Event Management)製品　(2) 当社独自開発のEDR(Endpoint Detection and Response)製品

コンサルティングサービス説明

セキュリティ・コンサルティングサービスを提供

セキュリティアドバイザー

- 「やり過ぎず」、「不足しない」、最適な対策を実現
- 数多くのセキュリティ事故対応の経験と知見をもとに、お客様の環境にあわせた適切なアドバイス
- 定例会でのアドバイス/メールでのご相談

インシデント対応支援

- 事業が継続できない部分を判断
- 事業活動が完全に停止するのを防ぐ
- 重要業務からどうすれば復旧できるかを助言
- 随時メールや定例会で調査状況の報告を行い、完了時に報告書を提出
- 被害拡大を防ぐために必要な対処の支援
- アドバイザが被害が出ない状況になったか判断しアドバイス
- インシデントが起きにくい環境整備

セキュリティ評価

- 既存のセキュリティ対策の有効性を評価
- 今後のセキュリティ対策についての中期計画策定の支援
- セキュリティ対策への投資を最適化

脆弱性診断

- 最新の脅威動向を押さえ、セキュリティ事故に精通した専門家が診断を実施
- セキュリティ事故発生前に脆弱性や脅威を発見し、対策することで事業継続のリスクを低減する。
- お客様の環境にあわせた診断を実施

リスクと対応方針

リスク項目	顕在化可能性 / 時期	影響度	認識しているリスク	対応策
サービス内容	中 / 中期	大	当社が環境変化等に対応できず、サービスの陳腐化又は競合他社の企業努力等の要因により、技術的・価格的に優位性を維持できない場合、業績に影響を与える可能性があります。	新技術の開発、また研究の結果あるいは知見・経験などを情報発信するなどの取り組みにより、当社サービスの競争力の維持・向上に努めております。
代理店との関係	低 / 中期	中	当社は販売代理店契約を締結し、当社サービスにおける顧客拡大・収益基盤強化を図っておりますが、代理店が十分に機能しない場合には、当社業績に影響を与える可能性があります。	代理店との良好で安定的な取引関係の構築に努めるとともに、販売支援やマーケティングの強化や新たな代理店の拡充などに注力しております。
競合との関係	中 / 中期	中	当社サービスがお客様のニーズに合わず、あるいは他社同種サービスとの競合になる等した場合には、当社業績に影響を与える可能性があります。	新規サービスを拡充し、お客様からの様々なニーズに対応できるようにすることにより、当社事業基盤の強化を図ってまいります。
想定を上回る解約	低 / 中期	中	当社の事業はストック型収益により構成されていますが、お客様のセキュリティ環境の変更等の理由により、毎年一定の解約が発生しており、当社の想定を超える解約が発生した場合には、当社の事業及び業績に影響を与える可能性があります。	お客様に継続して利用いただくために顧客満足度を高め、解約率を低く維持するためにサービス等の改善や施策を行っております。
小規模組織及び人材確保・育成	中 / 中期	中	当社が事業を拡大及び継続するために、開発力の強化・技術ノウハウの蓄積・営業力の増大・そのための高度なサイバーセキュリティ技術や知識を有する優秀な人材の確保が課題となりますが十分な人員が確保できない等の場合に、当社の成長が鈍化する可能性があります。	当該人材の確保の施策としてテレワークでの就業や福利厚生制度の充実及びと社内教育の強化に努めております。

※その他のリスクについては、有価証券報告書の「事業等のリスク」をご参照ください。

6. 用語解説

用語解説

SOC（ソック）

Security Operation Center：ネットワークの監視を行い、サイバー攻撃の検出と分析、対応を図る組織あるいは役割です。同じくセキュリティ関連の組織であるCSIRTとの違いとしては、CSIRTではインシデントが発生したときの対応に重点が置かれているのに対し、SOCは脅威となるインシデントの検知に重点が置かれているという特徴があります。

CSIRT（シーサート）

Computer Security Incident Response Team：コンピュータセキュリティにかかるインシデント（事象）に対処するための組織の総称です。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定等を行ないます。

SIEM（シーム）

Security Information and Event Management：様々なログを一元的に管理し、当該ログを自動的に相関分析して、セキュリティリスクの把握を行い、システム管理者の負担を軽減する「セキュリティ情報及びイベント管理製品」を指します。CSIRTやSOCの運営基盤としてセキュリティ情報を一元管理することを可能とする製品です。

マルウェア

不正かつ有害な動作を行う意図で作成された悪意のあるソフトウエアや悪質なコードの総称で、ウイルス、ワーム、トロイの木馬等を含みます。

EDR（イーディーアール）

Endpoint Detection and Response：各ユーザが利用するパソコンやサーバ等のエンドポイントにおけるマルウェアなどによる不審な挙動が検知された場合にお客様にエスカレーションを実施し、防御をすることで被害の拡大を防ぐことを目的としたサービスです。

アラート

SIEMなどのセキュリティ製品にて収集したログデータ等に基づき、不審なイベントや異常な挙動などを検知して、アラートとして通知することを指します。

インシデント対応 / IR（Incident Response）

マルウェア感染や不正アクセスなどのセキュリティ上の脅威となる事象をセキュリティインシデントといい、そのインシデントへの対応を指します。当社は、インシデントが発生したお客様への対応を支援しており、インシデント対応支援としてサービス提供しています。

ゼロトラスト（Zero Trust）

ネットワークの境界に依存せず、「何も信頼しない」ことをコンセプトにセキュリティ対策を行うことを指します。クラウドサービスの利用やテレワークの増加など、社内ネットワークが外部と通信するケースが増加し、ネットワークの境界が曖昧になっていることなどが背景にあります。

オンプレ

オンプレミス（on-premises）：サーバーやネットワーク機器などを自社内で保有し運用するシステムの利用形態となります。クラウドとの対比で利用されます。

本開示の取り扱いについて

- 本資料には、将来の見通しに関する記述が含まれています。これらの将来の見通しに関する記述は、本資料の日付時点の情報に基づいて作成されています。これらの記述は、将来の結果が業績を保証するものではありません。このような将来予想に関する記述には、既知及び未知のリスクや不確実性が含まれており、その結果将来の実際の結果や業績は、将来予想に関する記述によって明示的又は黙示的に示された将来の結果や業績の予想とは大きく異なる可能性があります。
- これらの記述に記載された結果と大きく異なる可能性のある要因には、国内及び国際的な経済状況の変化や、当社が事業を展開する業界の動向などが含まれますが、これらに限定されるものではありません。また、当社以外の事項・組織に関する情報は、一般に公開されている情報に基づいております。
- 本資料は、情報提供のみを目的としており、日本その他の地域における有価証券の販売の勧誘や購入の勧誘を目的としたものではありません。

S&J

私たちは、最適なセキュリティサービスをより多くのお客様へ提供し、
事業の成長を支える環境づくりに貢献いたします。

S＆J株式会社
〒105-0004 東京都港区新橋1-1-1 日比谷ビルディング8F
TEL：03-6205-8500　FAX：03-6205-8510
https://www.sandj.co.jp/