2027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

2026年8月12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（FY2026 / 1Q累計）

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

591百万円(FY2026/1Q) / **10.0**%(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

2,138百万円(FY2026/1Q)

営業利益 / 営業利益率

88百万円(FY2026/1Q) / **15.0**%(FY2026/1Q)

ストック売上比率(2)

90.2%(FY2026/1Q)

サービス継続率(3) / 解約率(4)

99.1%(FY2026/1Q) / **0.9**%(FY2026/1Q)

従業員数(5) / 増加数

82名(FY2026/1Q) / **3**名増(前期末比)

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

2026年6月30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	82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 事業管掌
石川 剛

取締役 セキュリティ人材開発部長
上原 孝之

取締役 管理部長
經田 洋平

取締役 技術管掌
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

取締役(監査等委員)
河合 透

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。詳細は本資料の「用語解説」に記載しています。

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。

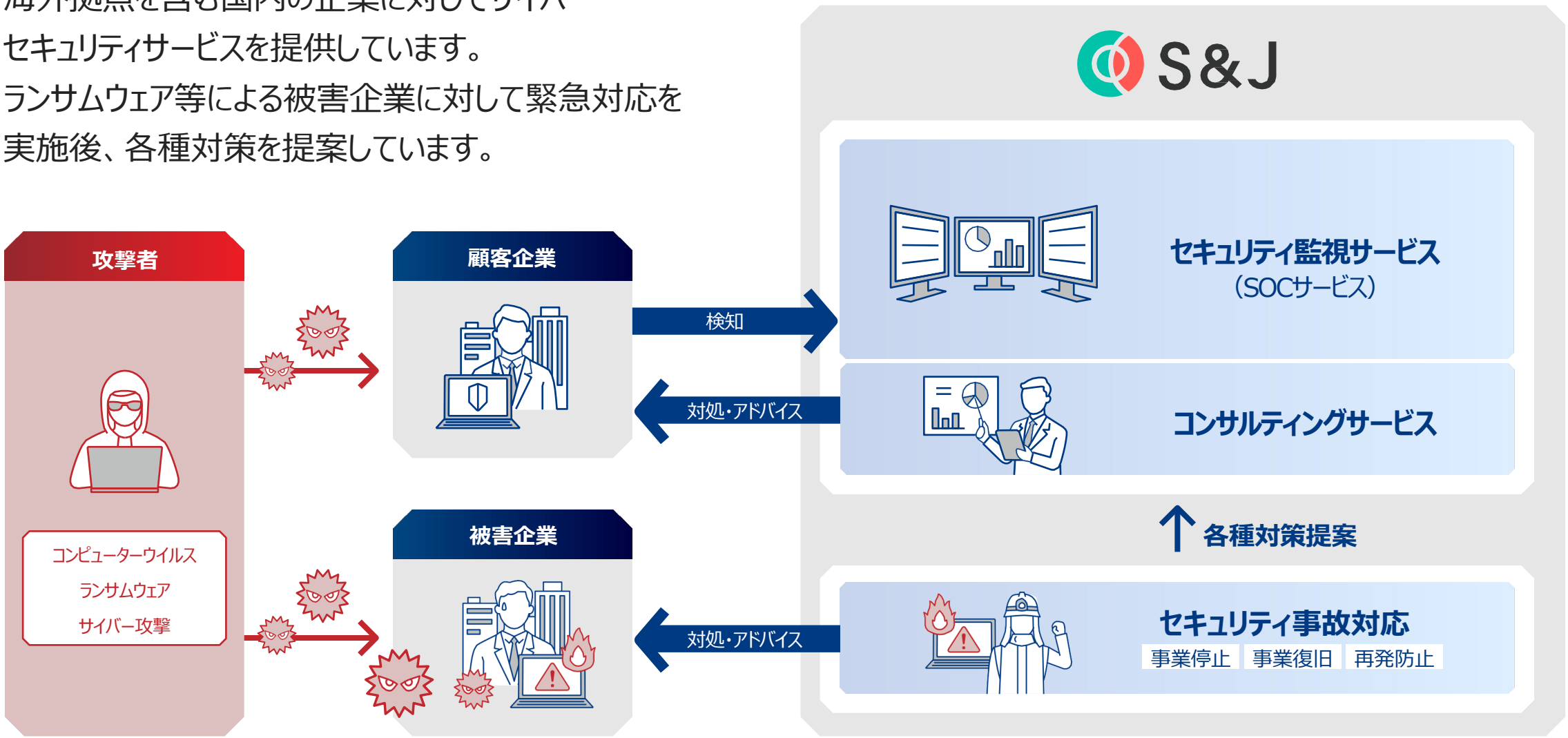
※媽祖は中国が発祥の海上守護神です。千里眼と順風耳を従え、航海の安全を守るとされています。

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

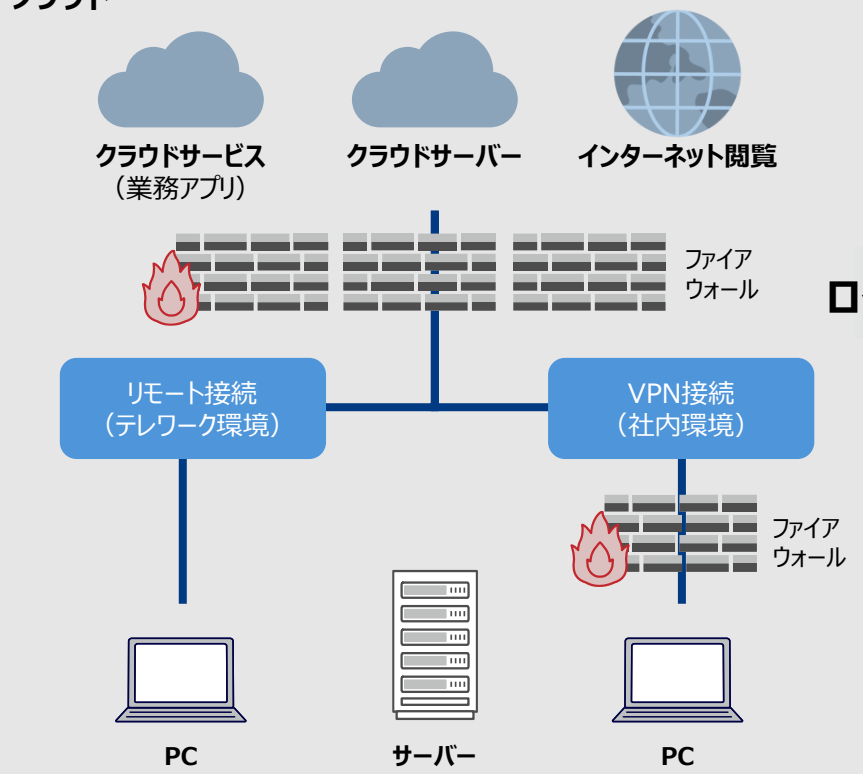
海外拠点を含む国内の企業に対してサイバーセキュリティサービスを提供しています。
ランサムウェア等による被害企業に対して緊急対応を実施後、各種対策を提案しています。



SOCサービス

お客様（企業・団体等）のネットワークを監視し、マルウェアなどのウイルス感染等への対処を支援

監視対象（例）



ログ収集

S&J

アナリスト

分析・一次対処・報告

- さまざまな機器のログを収集
- 不審な通信や振る舞いを検知
- 検知した内容を分析
- 一次対処の実施
- 対処方法の連絡
- 分析結果の報告

報告

お客様

お客様

対処

- 事象の確認
- 恒久対策の実施

コンサルティングサービス

お客様のセキュリティ運用を支援

・年間契約をベースとしたアドバイザーサービス

・お客様のセキュリティ課題に対して、
中長期的な視点での支援を提供

・お客様と継続的なコミュニケーションをとりつつ、
伴走しながら、セキュリティ施策をリード

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

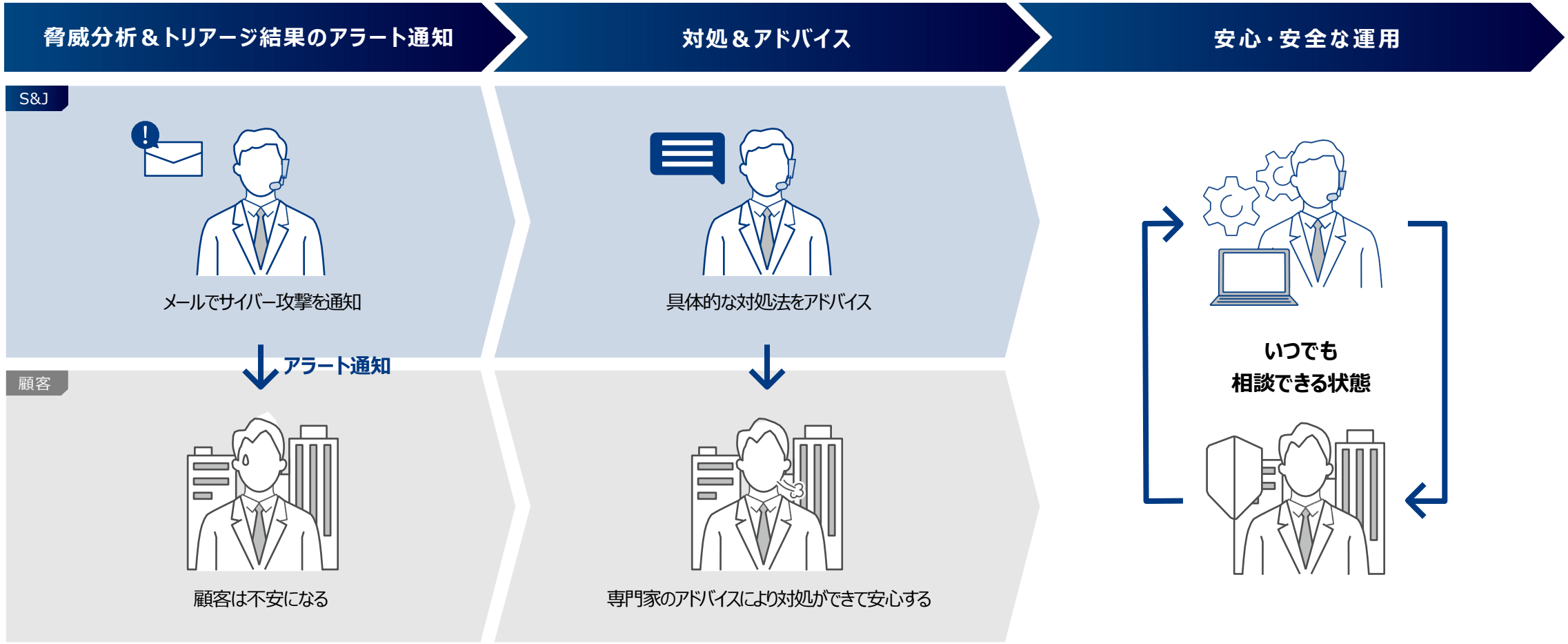
- **お客様とのコミュニケーションをとりつつ、対処方法等を推奨できるセキュリティ監視サービスを目指す。**
- **危険性が高く、緊急性が高い場合には遠隔での対処を実施する。**

- 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

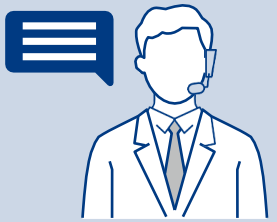
＜夜間などの顧客不在時の対応フロー＞

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

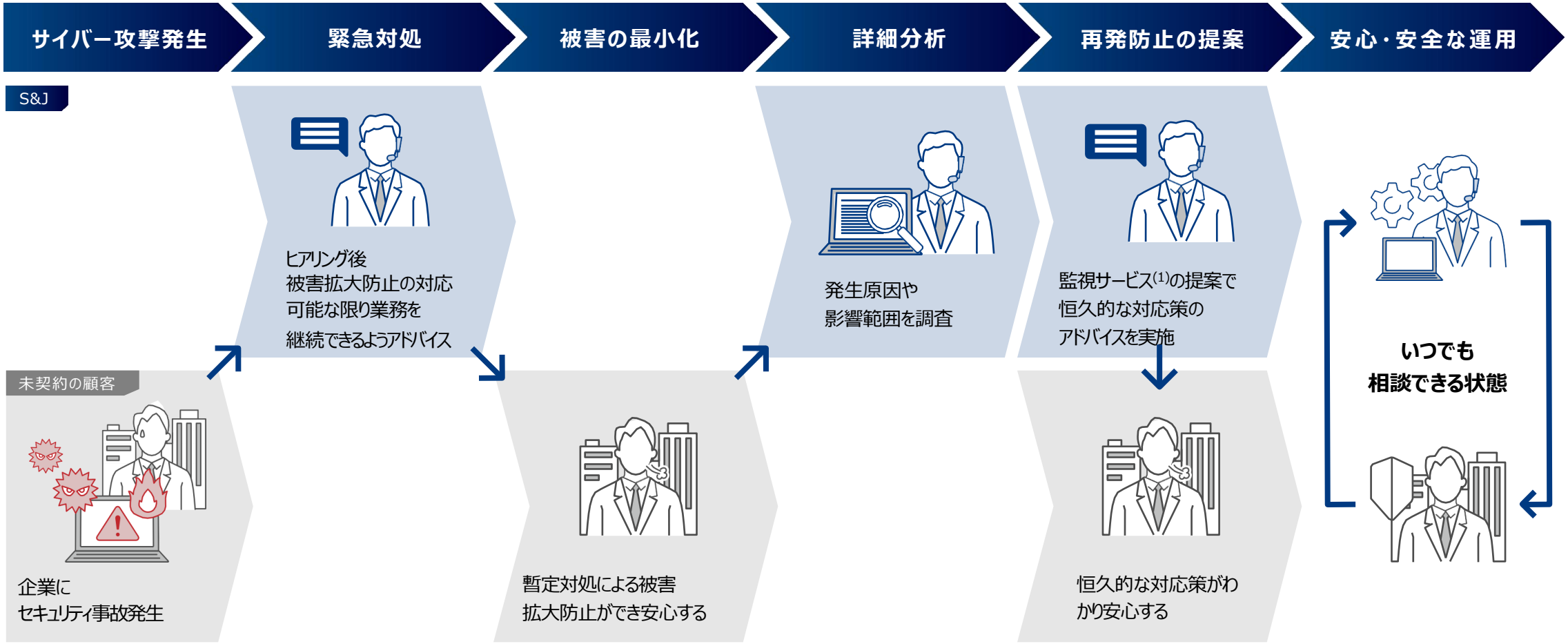
担当者不在時にサーバー攻撃が発生

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＞

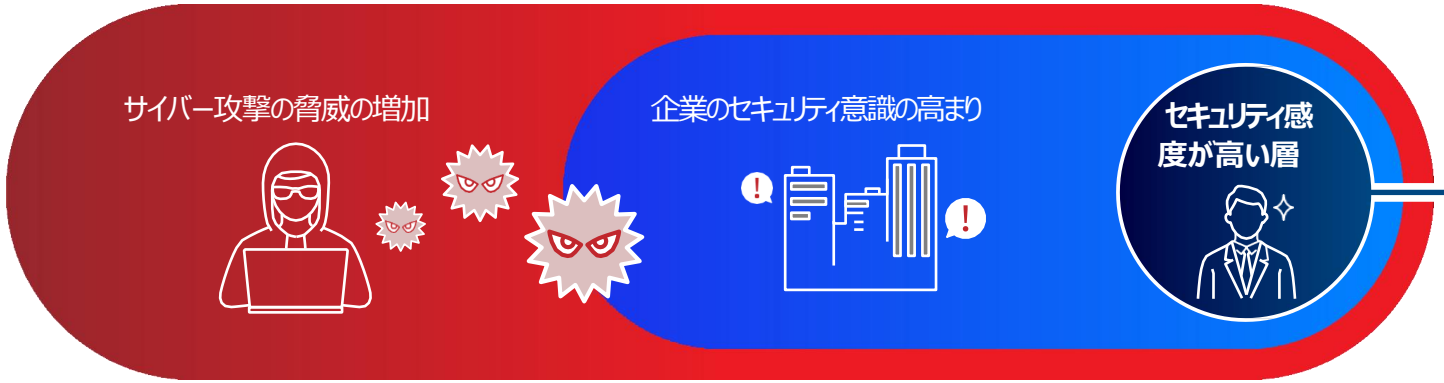
業務継続を優先的に考え、緊急対応の実施と恒久対応方法まで含んだ支援が可能。



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

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

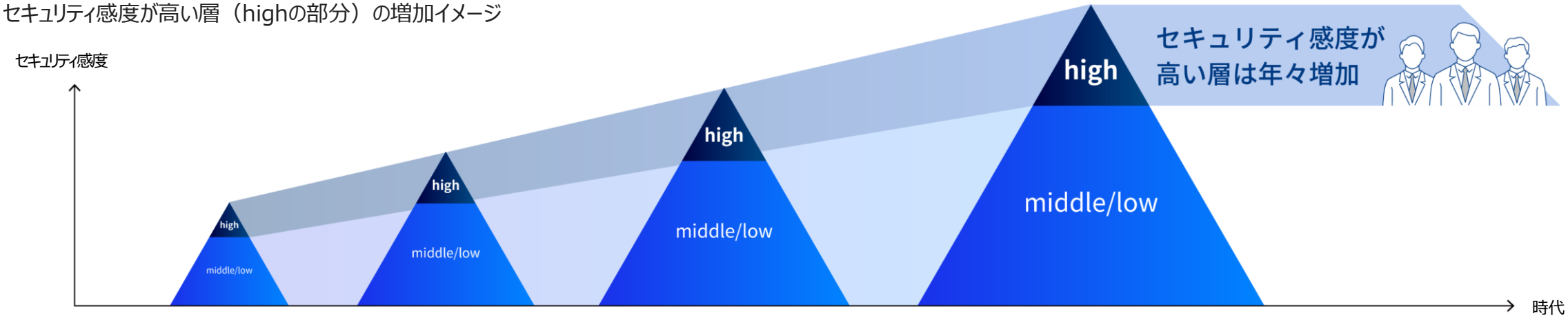


ここが当社のお客様

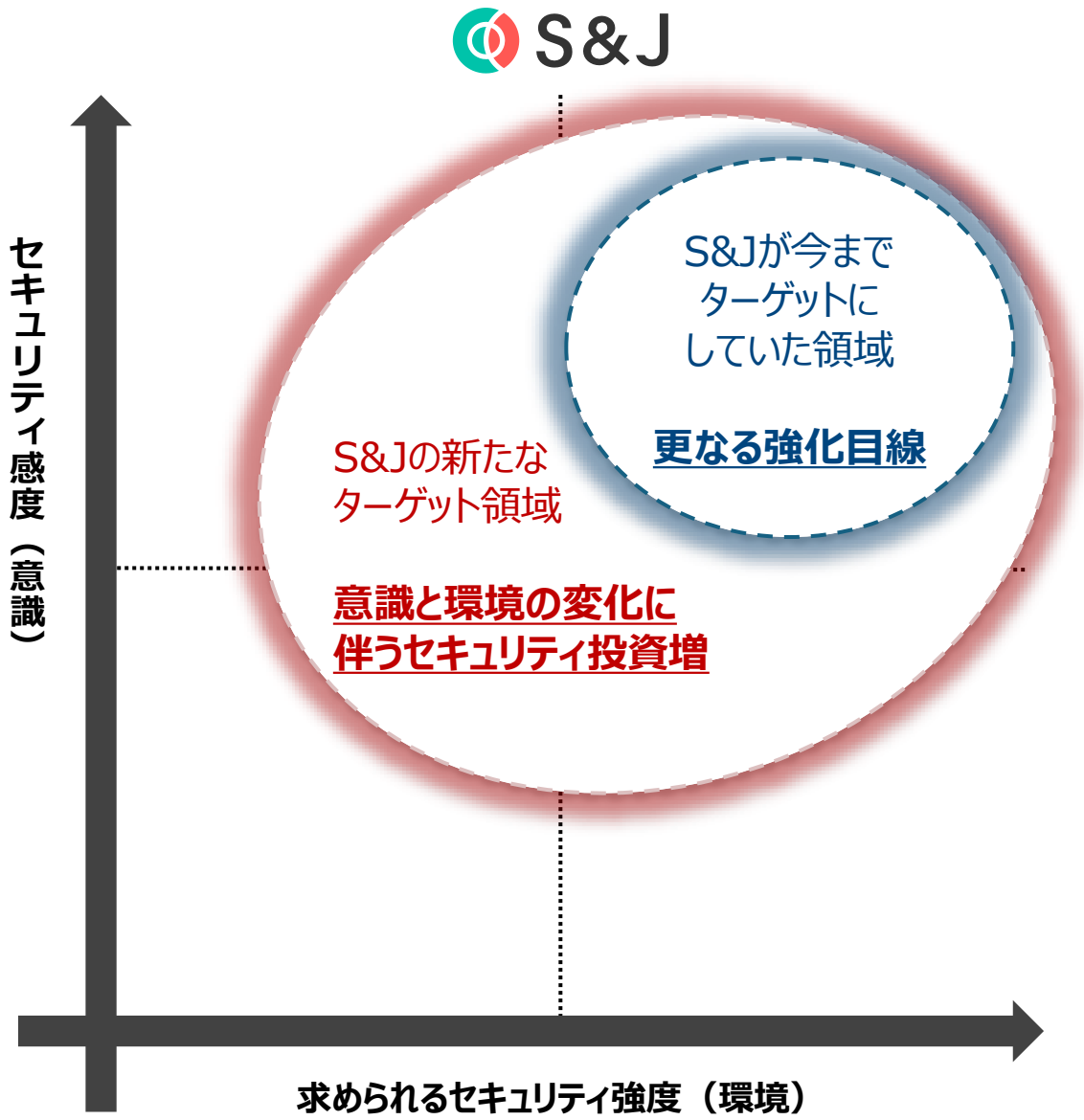
当社の**「セキュリティ感度が高い層」**の定義

- 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

Security Operation Centerでのブランディング/価値訴求をするSOCツアー

- サイバー攻撃の手口や対処方法を伝えるSOCツアーは、参加者から高い満足度を得ている。
- 新規顧客の獲得に加え、既存顧客におけるアップセルや解約率低下につながっている。

延べ**100社以上**でSOCツアーを実施
※2026年4月末時点

お客様の声

「セキュリティのプロとして豊富な知識を有しており、セキュリティに関する相談事などをしたいと思った。」 、「非常に満足でした！！」

「AD監視サービスにおける監視の強みをより実感できました。また、セキュリティに強い企業であることを感じ、AD（監視サービス）以外の話も伺いたいと思いました。」

「ADが攻撃の起点になることは漠然と理解していましたが、対策がとれていない状況なので、AD監視について知ることができて良かった。」

「今まで以上に安心感や信頼性が高まりました。ある種、社会貢献されていると感じました。」

2. 第1四半期業績

業績サマリー(FY2026 / 1Q累計)

- 売上高は、591百万円と前年同期比10.0%増、進捗率21.6%。
- 営業利益は、88百万円と前年同期比30.3%減、進捗率14.3%と人件費と通信費の増加の影響により減益。
- 当期純利益は、59百万円と前年同期比31.9%減、進捗率14.7%。

	FY2025 第1四半期		FY2026 第1四半期				FY2026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	537	100.0%	**591**	100.0%	+53	+10.0%	2,740	21.6%
営業利益	127	23.6%	**88**	15.0%	△38	△30.3%	620	14.3%
経常利益	127	23.6%	**87**	14.9%	△39	△30.9%	600	14.6%
当期純利益	87	16.3%	**59**	10.1%	△27	△31.9%	405	14.7%

第2四半期累計（業績予想）に対する進捗

- 第１四半期の業績は、おおむね計画どおりの着地となり、進捗率も順調に推移している。
- 前期の採用増による人員増・昇給等と、新サービス開発に伴うインフラ基盤の通信費増加により、第１四半期の営業利益率は15.0%となるものの、第２四半期の営業利益率は18.6%に逓増となる。
- 第２四半期累計の業績予想が、前年同期比で減益となるのは、前年同期における採用計画の遅れに伴う経費の後ろズレが要因としてあげられる。

	FY2026 第1四半期		FY2026 第2四半期		FY2026 第2四半期累計（業績予想）				（参考）FY2025 第2四半期累計	
	実績	対売上高	計画(1)	対売上高	予想	対売上高	進捗率(2)	前年同期比増減率	実績	対売上高
売上高	591	100.0%	658	100.0%	**1,249**	100.0%	47.3%	13.2%	1,104	100.0%
営業利益	88	15.0%	122	18.6%	**210**	16.9%	42.0%	△24.3%	278	25.2%
経常利益	87	14.9%	116	17.7%	**204**	16.4%	43.0%	△27.2%	280	25.4%
当期純利益	59	10.1%	78	11.9%	**137**	11.0%	43.3%	△28.7%	193	17.5%

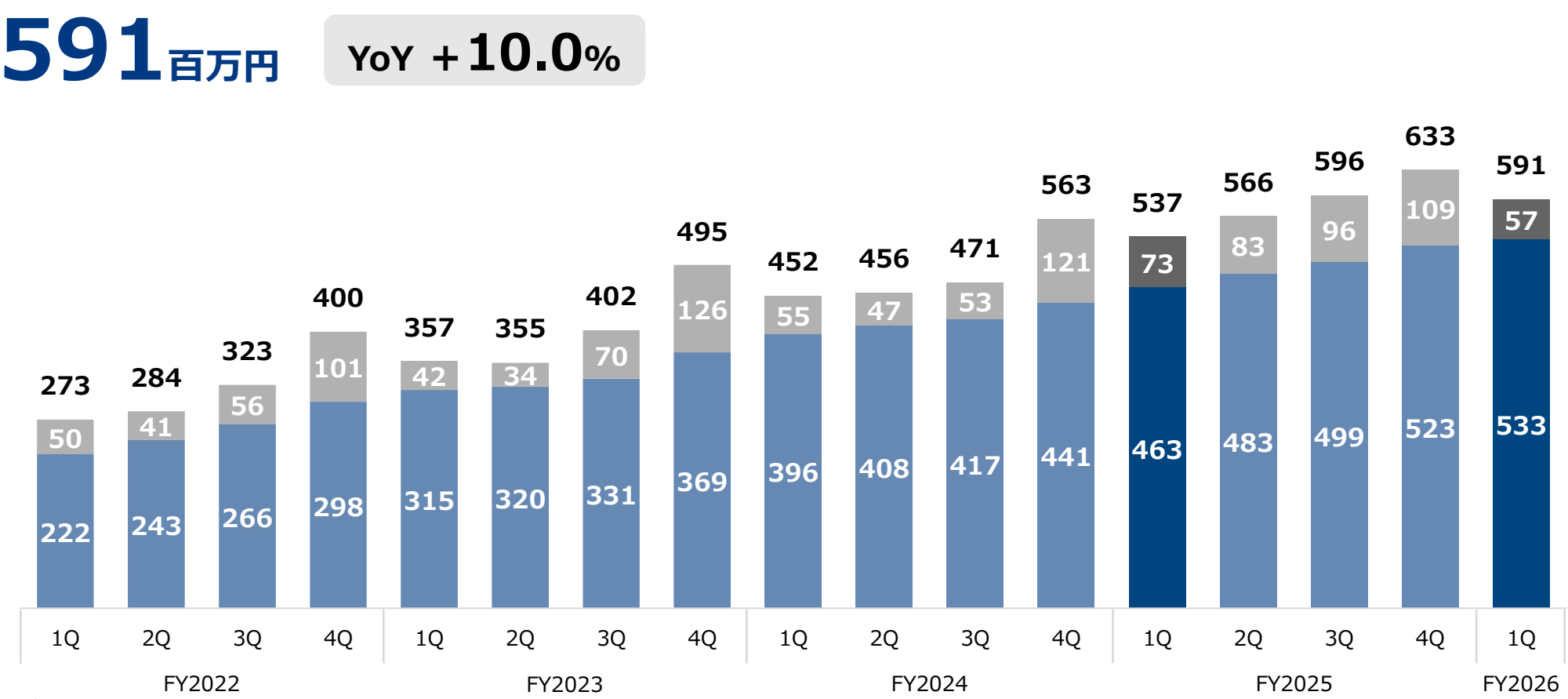
（注）：(1)計画は、第2四半期累計（業績予想）－第1四半期実績で算出
(2)第2四半期累計（業績予想）を100%とした場合の第1四半期実績が占める割合

業績ハイライト　売上高（FY2026/1Q）

- 売上高は、591百万円と前年同期比10.0%増。
- スポット売上については、前年同期におけるインシデント対応支援の反動減や脆弱性診断の大幅減により低調となるが、ストック売上である監視サービス等の増加により、増収。

売上高

591百万円　YoY ＋10.0%



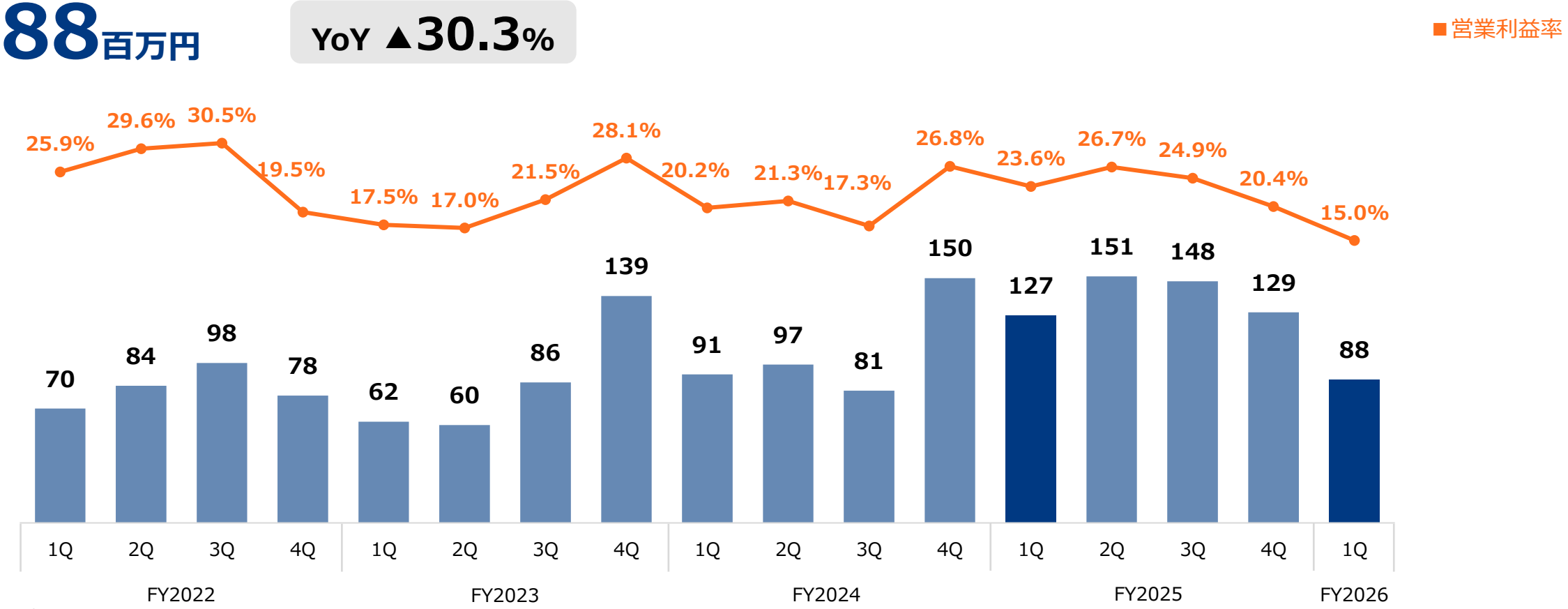
業績ハイライト　営業利益・営業利益率（FY2026/1Q）

- 営業利益は、88百万円と前年同期比30.3%減。
- 前期の採用増・昇給等による人件費の増加に加え、インフラ基盤における通信費等の増加により、減益。

営業利益

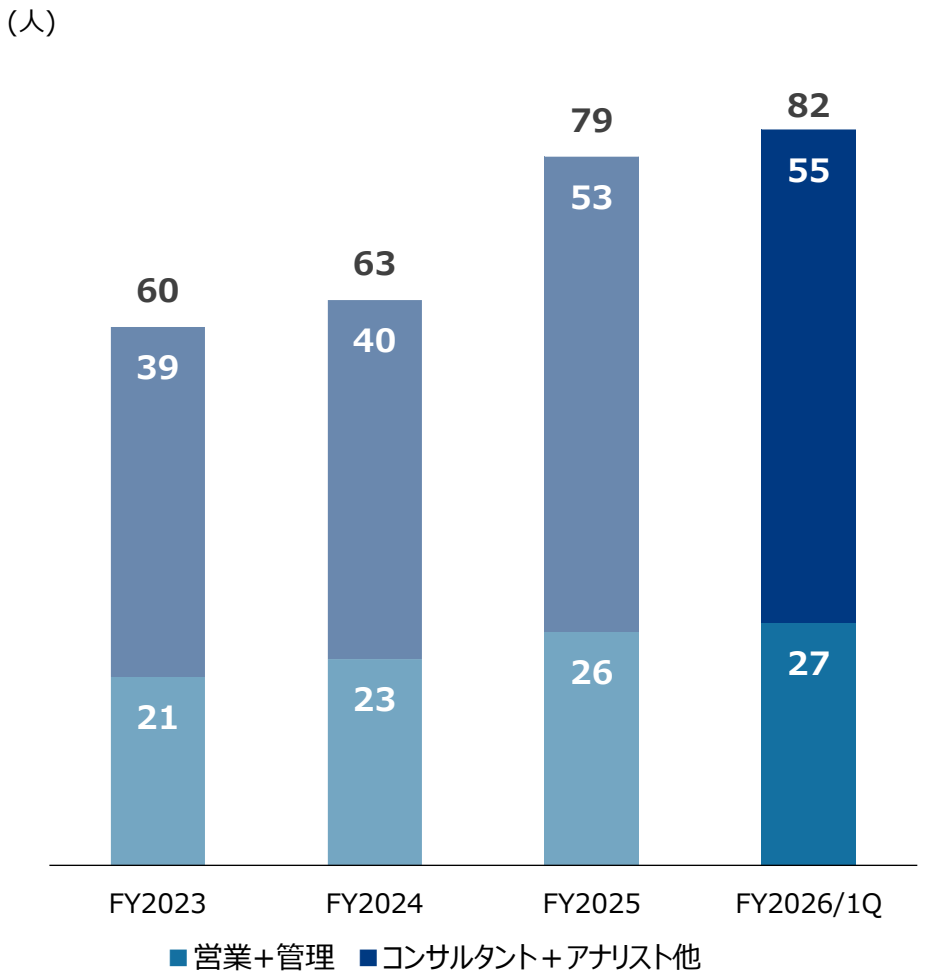
88百万円

YoY ▲30.3%



経営指標

人員推移 (1)



- **人員の採用はおおむね予定通りに推移しており、通期計画87名に対して、実績82名。**

- **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。

ストック売上強化に向けた取り組み

1．Microsoft製品監視を拡販するためのパートナー体制強化

＜2026年3月末＞

・Microsoftライセンス販売/SIパートナー
【2社】

＜2026年6月末＞

・Microsoftライセンス販売/SIパートナー
【 7社 】
・Microsoftライセンスディストリビューター
【 1社 】

・案件の増加
・当社サービス提供に向けた協業を推進中

2．ランサムウェア攻撃の増加によるセキュリティ対策の見直し需要増加

＜FY2026　1Q＞

・セキュリティ対策を強化するコンサルティングサービスの問い合わせが増加
（実践的なサイバーBCP/セキュリティ評価/ロードマップ策定支援）

＜FY2026　1Q＞

・コンサルティングサービスの受注増加
（顧客課題の可視化）

・SOCサービスのアップセル推進

ストック売上拡大に向けた活動を強化

成長にあわせた株主還元施策

配当

株主の皆様への配当を安定的かつ継続的な配当を実施するため、配当性向20%以上を目安とし、利益成長に応じた増配を目指す、とした配当方針に変更しております。(1)

- 2026年3月期より、配当を開始する（初配）
- 配当方針の変更：配当性向20%以上を目安とし、利益成長に応じた増配を目指す
- 2026年3月期の1株当たり配当金の実績は、15円00銭

2027年3月期1株当たり配当予想

通期 **17.00円**

中間予想　0.00円
期末予想　17.00円

（注）：(1)2025年11月12日付け「配当方針の変更及び配当予想の修正（初配）に関するお知らせ」
※上記の予想は、発表日現在において入手可能な情報に基づくものであり、不確定な要素を含んでおります。
従いまして、実際の配当はさまざまな要因により予想数値と異なる場合があります。

自社株買い

経営環境の変化に対応した機動的な資本政策を遂行するため、2025年2月および2025年12月に自己株式の取得を決定し、取得を実施している。

- 2025年2月～5月までの自己株式取得(1)において、110,200株（119百万円）の取得を実施
- 2025年12月～2026年3月までの自己株式取得(2)において、160,000株（299百万円）の取得を実施

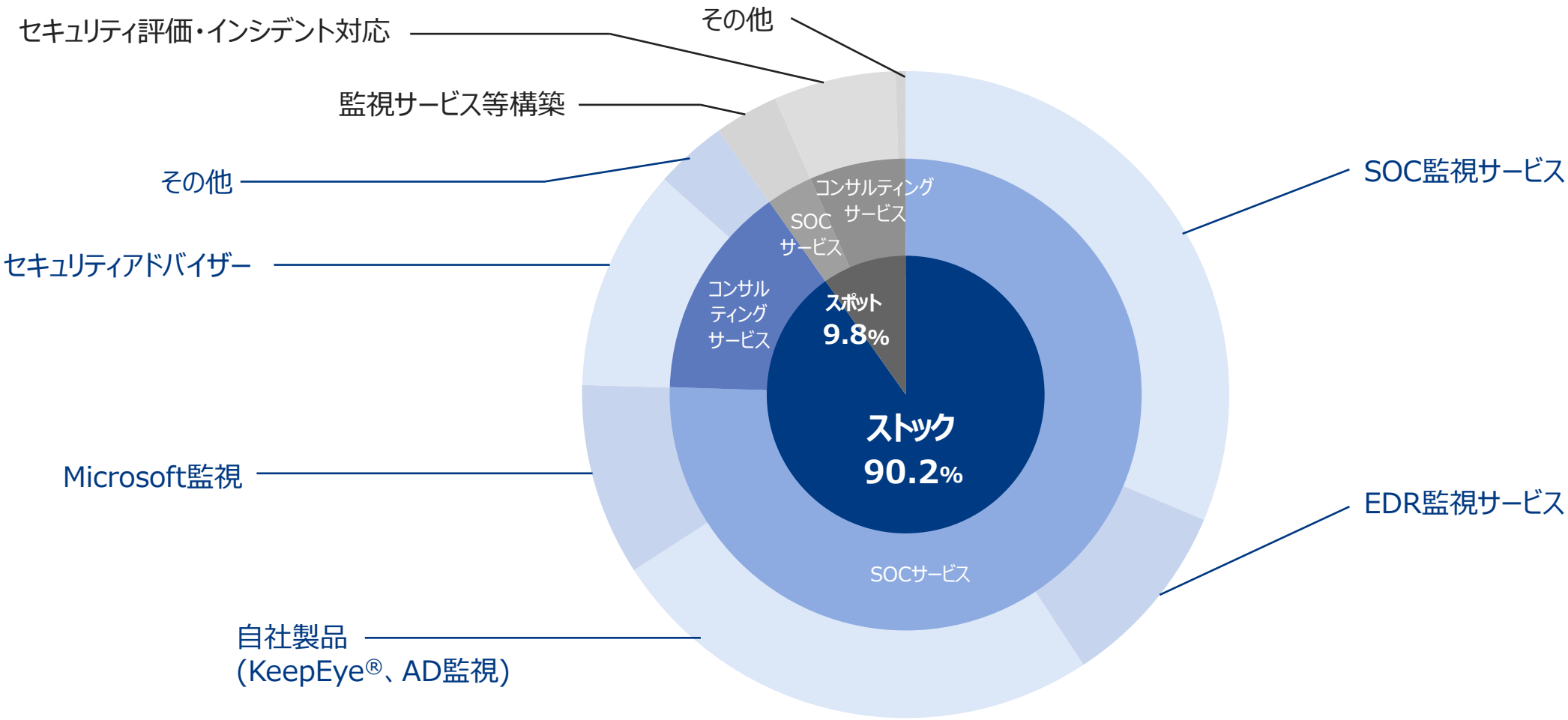
取得期間	株式数(上限)	価額の総額(上限)
2025年2月～５月	120,000株	120百万円
2025年12月～2026年3月	160,000株	300百万円

（注）：(1) 2025年2月14日付け「自己株式取得にかかる事項の決定について」にもとづく取得。
(2) 2025年12月17日付け「自己株式取得にかかる事項の決定について」にもとづく取得。

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90.2%） FY2026 / 1Q実績



成長戦略①：サイバーセキュリティ市場で圧倒的な成長が見込まれる Microsoftに独自サービスも含めて注力

政府/民間ともに導入が伸びているMicrosoft 365 （Business Premium、E3、E5）向けに特化した独自サービスを提供。
ライセンス提供、環境構築から、統合的な運用監視までも一気通貫で提供。
これまで非注力であったSMB市場に対して、当社独自サービス「My SOC 365」をMicrosoftライセンス販売パートナーと協業での拡販。

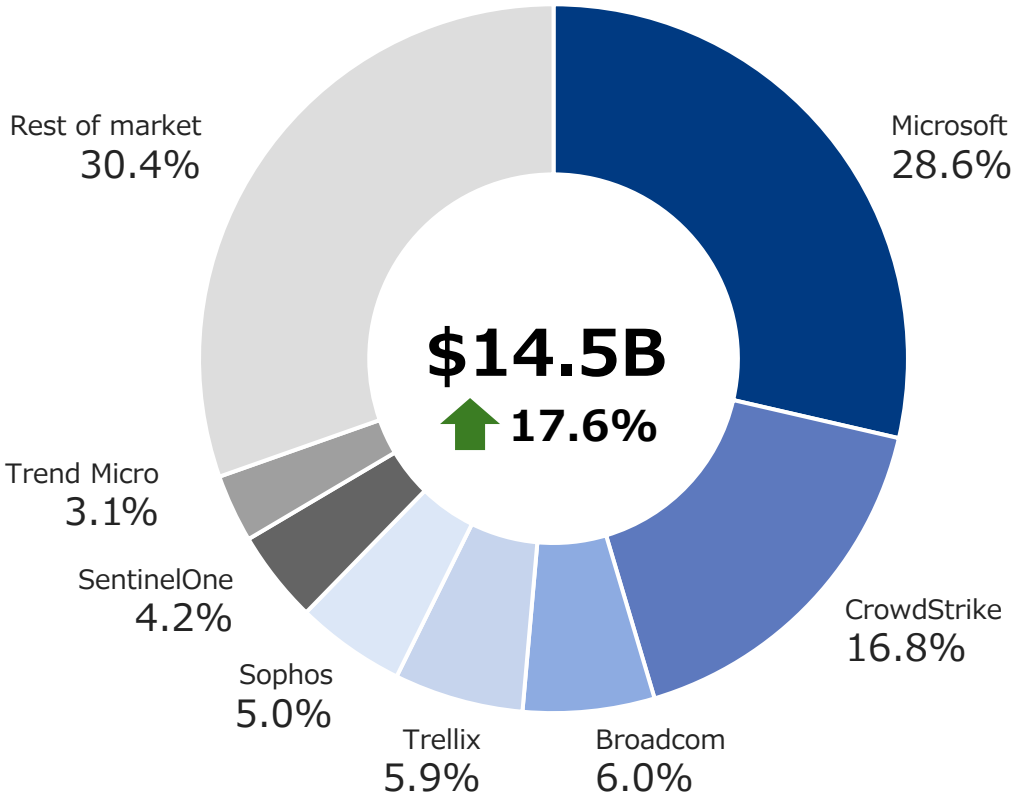
2023年、2024年全世界での
ベンダー毎エンドポイントセキュリティ売上

（単位：$M）

ベンダー	2023年	2024年	2024年 市場シェア	2023年～2024年 売上高成長率
Microsoft	**3,237.5**	**4,151.0**	**28.6%**	**+28.2%**
CrowdStrike	2,121.8	2,437.2	16.8%	+14.9%
Broadcom	713.9	873.7	6.0%	+22.4%
Trellix	724.3	849.0	5.9%	+17.2%
Sophos	606.1	722.4	5.0%	+19.2%
SentinelOne	489.3	616.1	4.2%	+25.9%
Trend Micro	446.4	450.7	3.1%	+0.9%
ESET	408.8	446.4	3.1%	+9.2%
Palo Alto Networks	400.0	430.6	3.0%	+7.6%
Kaspersky	281.8	331.7	2.3%	+17.7%
Rest of market	2,908.5	3,201.6	22.1%	+10.1%
Total	12,338.5	14,510.4	100.0%	+17.6%

出典：Source: IDC's Semiannual Software Tracker, 2025 https://idcdocserv.com/US53349725e_Microsoft

2024年全世界での
エンドポイントセキュリティマーケットシェア



成長戦略②：AIが変える開発速度・SOC品質・収益構造

生成AIを製品の機能開発およびSOC業務に活用し、機能開発速度とSOC品質を同時に引き上げる。
人員増加を抑えながらスケールできるビジネスモデルを実現し、収益性の向上を加速させる。

課題	生成AI活用	得られる効果
【機能開発】多くの工数がかかる 新機能の追加や既存機能を改善において、実装・テスト・ドキュメント作成に膨大な工数がかかり、リリースに時間がかかる	**実装・テスト・ドキュメント作成をAIが支援** 生成やレビューといったAIを利用することで、作業者の支援を行う	**実装工数 約40～50%削減** リリース頻度2倍・新機能投入スピードの加速を実現済み。 今後、更なるスピード加速と高速化を目指す
【SOC品質】手作業の部分がある セキュリティレポートの作成が手作業中心 アナリストの脅威分析において自動化・AI化の余地が大きい	**AIがレポート作成・脅威分析を支援** レポート内の脅威傾向・リスク評価・改善提言をAIにより自動作成（一部サービス） アナリストの脅威分析をAIが支援。1人あたりの対応顧客数を拡大	**分析品質の均質化・工数削減** アナリストが高度分析・顧客対応に集中できる体制へ
【収益構造】人員依存 売上拡大に応じて採用コスト・人件費が増大し、スケールのネックとなっている	**AI活用で全領域の人的工数を圧縮** 開発・SOC・コンサル・IRなど全領域でAI活用を横展開し、人員増加を抑制	**売上増・利益率改善を同時に実現** 売上成長×採用コスト削減の両立でスケーラブルな収益構造を実現

AIを競争優位の核に据え、人員増加を抑えながら売上増・利益率改善を両立させるスケーラブルな収益構造を実現する

成長戦略③：パートナー戦略強化

売上規模拡大に向け販売パートナーとのアライアンスを強化し、販売パートナー数を5倍以上に増やす戦略。

Microsoftライセンス販売を得意とするリセラーをパートナーとしてMicrosoft製品監視の拡販を行い、その顧客基盤に他サービスをアップセル。

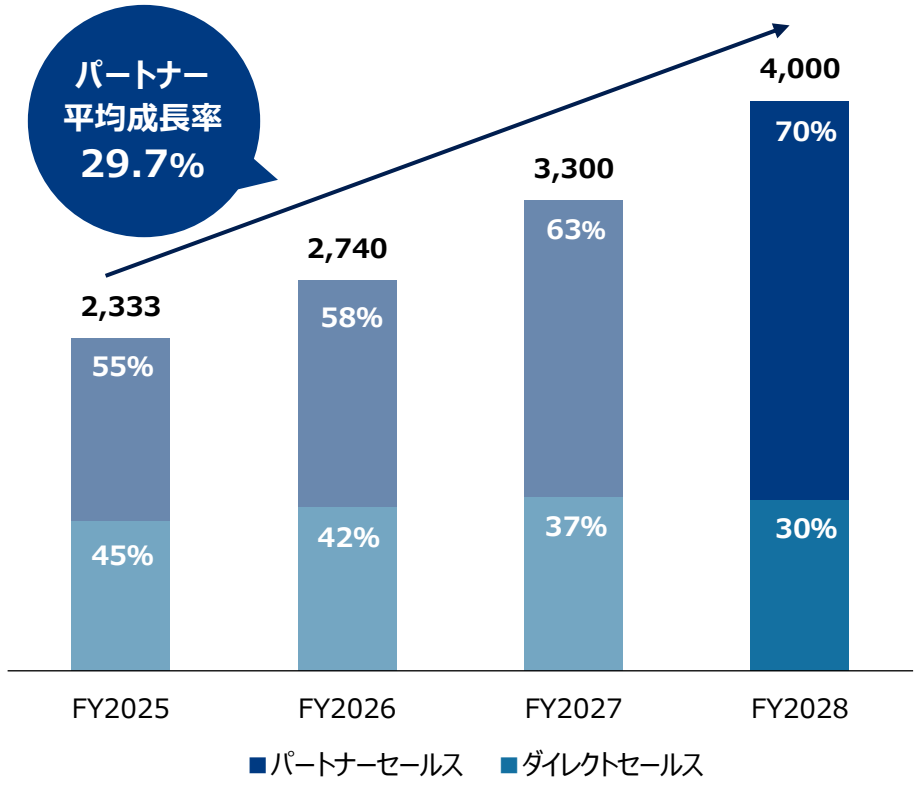
注力サービスのパートナー強化

- Microsoftライセンス販売を得意とするパートナーを開拓し、新規顧客獲得だけでなく、既存顧客へのS&J独自サービスのアップセル
- 自社製品を中心にサービスごとに各地方の有力SIer（ローカルキング）との協業

トータルサービスのパートナー強化

- 統合SOC、コンサルティング等のトータルサービスを提供するパートナーを2社獲得する
- 候補先としては、企業のITインフラを担っているMSP（Managed Service Provider）事業者など、S&Jのセキュリティ事業が補完関係となる先を対象とする

FY2028には売上比率70%をパートナー経由に



成長戦略の中期計画

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

S&Jの目指す姿

- より多くのお客様で大規模インシデントゼロを実現
- より高収益化を図るためのAIを用いたサービス / インフラ化

FY2028 テーマ：お客様の大規模インシデントゼロをお約束できる企業へ

- グローバルでユニークなソリューション × インシデントゼロに本気な従業員の実現
- 大規模インシデント発生時は無償支援（フォレンジック/ハンドリング）をお約束

FY2027 テーマ：パートナーアライアンスによる事業拡大

- 高度化/省力化を実現するためにAIを最大限活用した競争力のあるSOCインフラへの更改
- 強みのあるサービスをお客様やパートナーに対して、手離れの良いサービスとして提供
- 強みのあるソリューションを拡販できるパートナーを増強

FY2026 テーマ：ビジネスモデルの変革

- Microsoft365向けSOCサービス拡張と、ライセンス販売を含めたSI支援の拡販
- SOCサービスのAIアナリスト化による高収益化と、提供キャパシティー強化
- 経済産業省のサプライチェーン対策評価制度向けに既存サービスを拡張して提供

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

対応結果

- ライセンス販売は一定の拡大、SI支援ビジネスは受注増
- グローバルSOCサービスの準備はできたが、DX/IoT向けSOCサービスは時期尚早
- 既存顧客へのブランディングによりアップセルが実現。新規顧客への開拓も開始

中期経営計画（FY2025～FY2028）

- 中期経営計画の見直しのとおり、直近の状況を鑑みて売上高を修正。
- 利益面では、AI技術の利活用による収益性の向上により、利益率の大幅な改善を計画。

（単位：百万円）

		FY2025（実績）	FY2026	FY2027	FY2028
売上高 （年成長率）		2,333 （20.1%）	2,740 （17.9%）	3,300 （20.4%）	4,000 （21.2%）
	SOC （年成長率）	1,767 （22.6%）	2,037 （15.3%）	2,447 （20.1%）	2,975 （21.6%）
	コンサルティング （年成長率）	566 （13.0%）	702 （24.1%）	853 （21.4%）	1,025 （20.2%）
営業利益 （営業利益率）		556 （23.8%）	620 （22.6%）	800 （24.2%）	1,120 （28.0%）
経常利益 （経常利益率）		555 （23.8%）	600 （21.9%）	800 （24.2%）	1,120 （28.0%）
当期純利益 （当期純利益率）		405 （17.4%）	405 （14.8%）	530 （16.1%）	740 （18.5%）

4. トピックス

2026年6月16日

S&J、ランサムウェアの暗号化を阻止する新ソリューション「KeepEye RansomSafe」の提供開始

～EDR回避時も暗号化前に検知・除去し、顧客の事業停止リスクを抑制～

- ランサムウェアによる業務システム等へのデータ暗号化攻撃に特化した監視サービスとなる
- S&Jが自社開発したエージェントを各端末にインストールすることで、各端末を監視する
- ランサムウェアが端末に到達した時点から解析を開始し、特有の挙動に着目して高精度な検知を実現した
- ランサムウェアが検知された場合には、専門のインシデント対応支援チームが24時間365日、初動対応を支援し、事業停止リスクを低減する
- 企業活動に大きな影響を及ぼす業務システム等の暗号化による事業停止を防ぐことに特化している
- 既存のセキュリティ製品（EDR製品等）に追加して導入できるため、製品の入れ替え（リプレイス）等の手間やコストが発生しない

サイバー攻撃のニュースに関連して、代表取締役社長三輪のコメントが掲載

掲載日（放映日）	メディア名	タイトル
2026年7月16日	NHK ニュース7	『ニチレイ』障害の影響広がる
2026年7月17日	東洋経済オンライン	冷食・低温物流大手のニチレイで「不正アクセス」、KFCやくら寿司、イオンへ影響広がる… 被害拡大や長期化のおそれは？
2026年7月22日	TBSテレビ　Nスタ	『隠すことを選んだようですね』ニチレイのシステム障害めぐりロシア系ハッカー集団が犯行声明
2026年7月22日	読売新聞 夕刊	『ニチレイ』システム障害、ロシア系ハッカー集団が犯行声明… データ流出防ぎたいなら連絡するよう要求
2026年7月22日	共同通信	ニチレイ攻撃と犯行集団　身代金要求型ウイルス
2026年7月23日	時事通信	ニチレイ障害、ハッカー集団が犯行声明　内部データ窃取か、出荷は全面再開へ
2026年7月24日	時事通信	サイバー攻撃、ＡＩで高速化　日本企業『狙われ続ける』―Ｓ＆Ｊ社長
2026年8月10日	テレビ東京　WBS	ニチレイ ハッカー集団がデータ公開

2026年8月4日

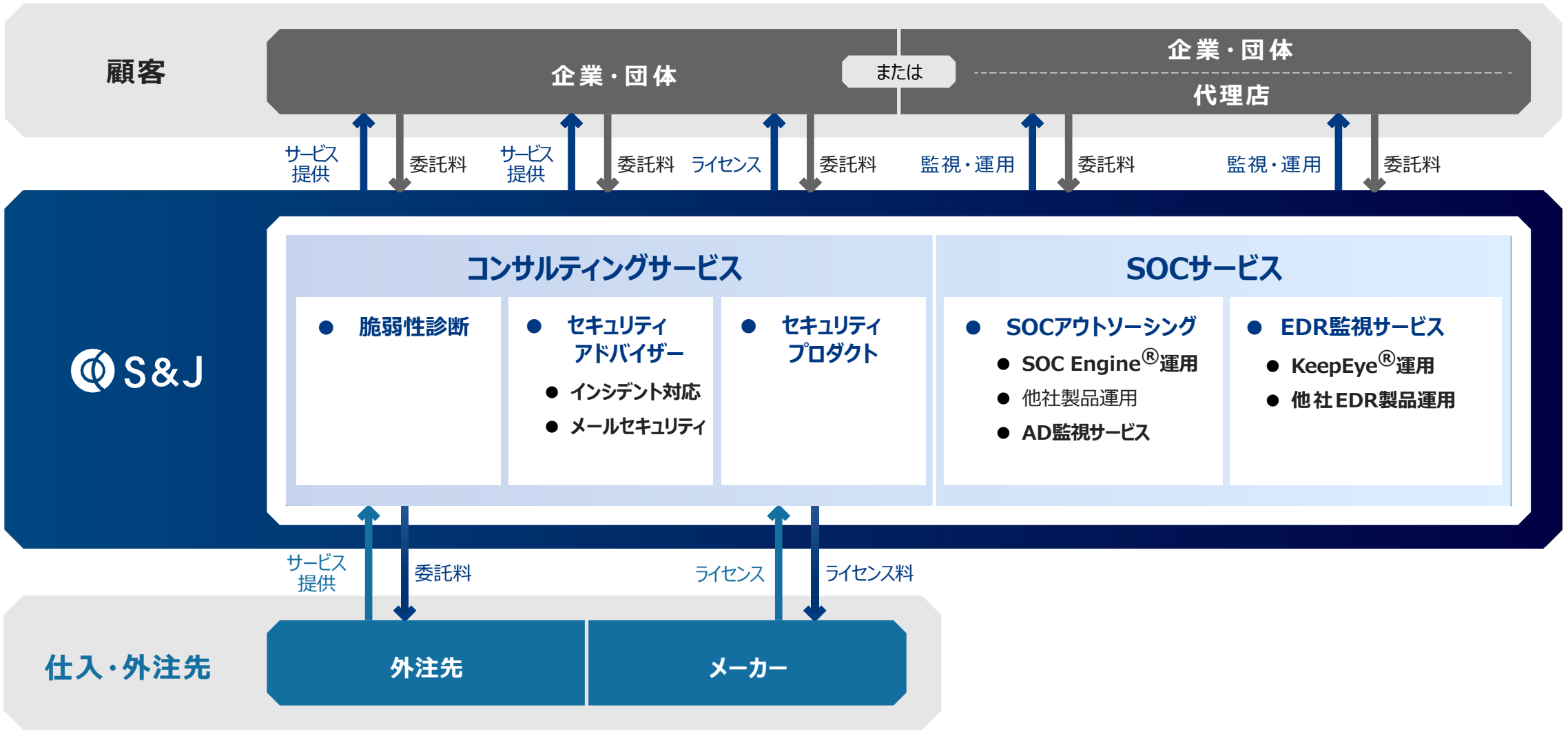
S&J、SOC自律化の潮流に応え「My SOC 365」にAI自動対処機能を搭載、脅威検知から対処完了までを数十秒で実行

～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～

- Microsoft365向けセキュリティ監視サービス「My SOC 365サービス」に新機能としてAI自動対処機能の提供を開始
- 「My SOC 365サービス」は、Microsoft365 E7/E5 /E3/Business Premiumをセキュリティプラットフォームとして利用する監視サービス
- 新機能は、AIが脅威を検知するとログを分析し、アカウント停止や端末の利用制限などの初動対処を自動で実行する
- 従来は脅威検知から対処までに数時間かかるものを、新機能では数十秒に短縮し、特に夜間・休日における被害拡大を防ぐことに貢献する
- 自動対処により停止したアカウントや隔離端末は簡単に復旧可能なため、自動対処への不安を解消し、業務への影響も低減できる
- 新機能の利用にあたっては追加のソフトウェア導入は不要であり、追加費用も不要

5. Appendix

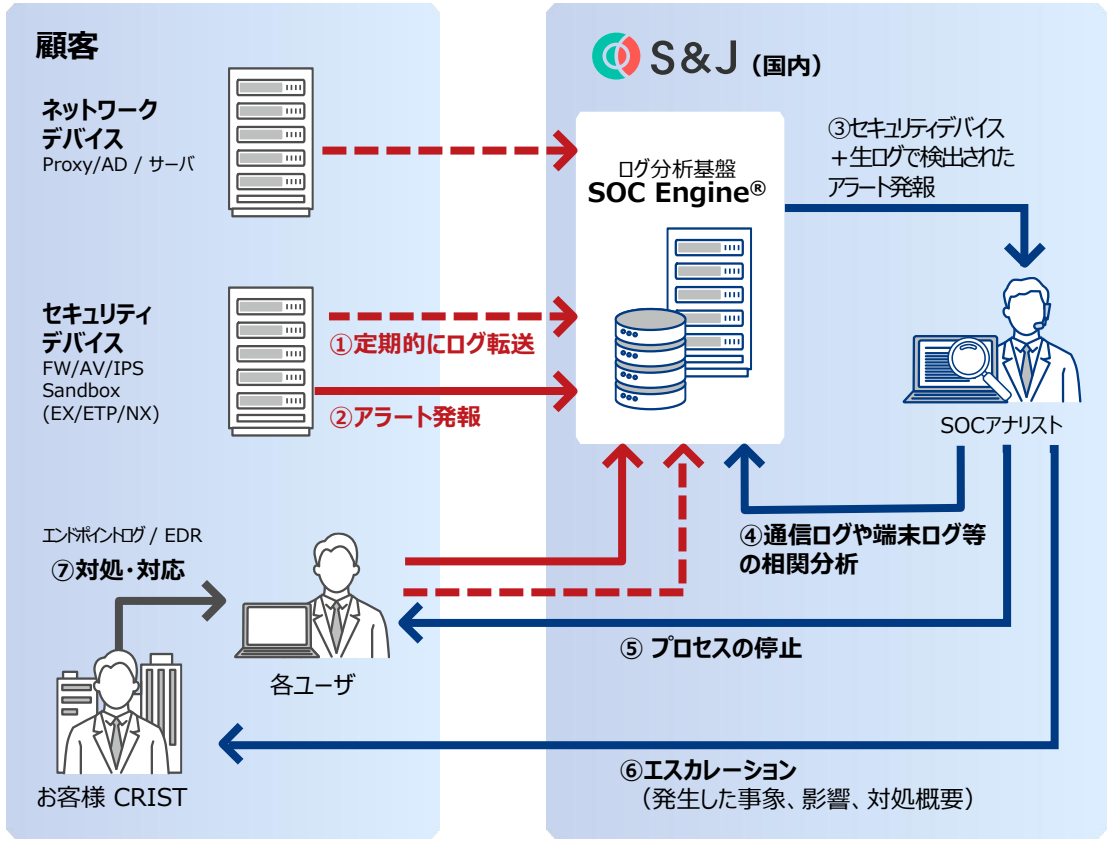
ビジネスモデル（収益構造）



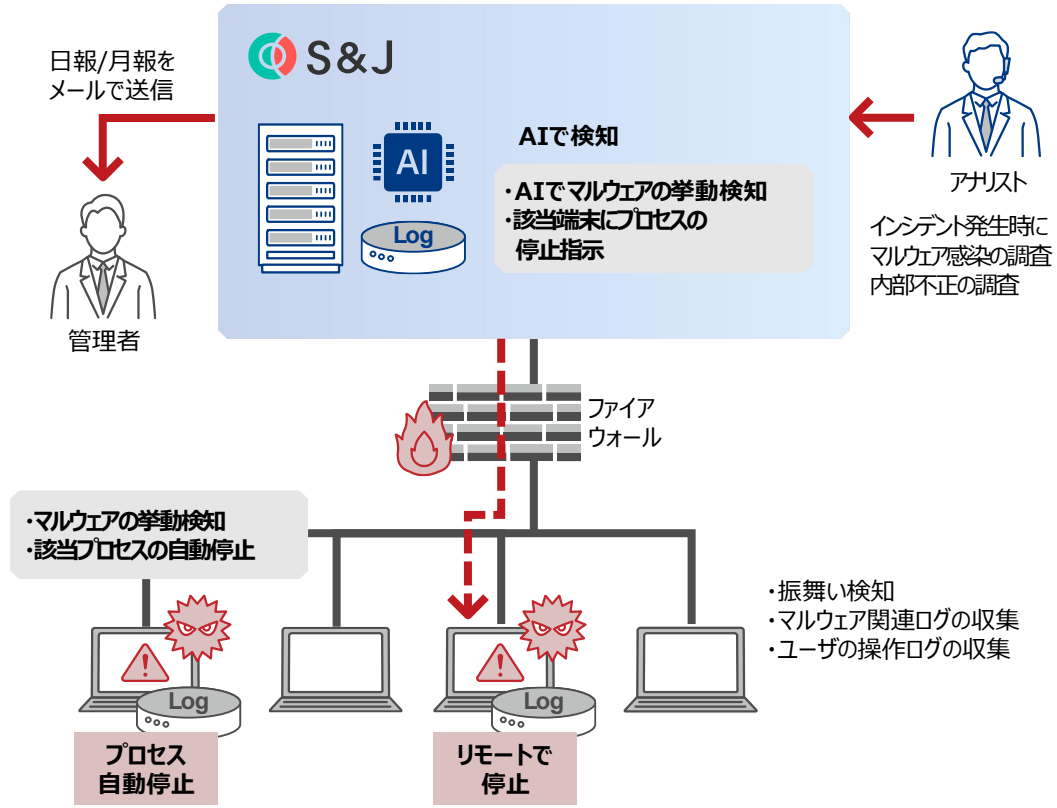
セキュリティ監視（SOC）サービス説明

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。

サービス別売上高（FY2026/1Q）

（単位：百万円）

	FY2025	FY2026/1Q	FY2026/2Q	FY2026/3Q	FY2026/4Q	FY2026/1Q累計
SOCサービス	1,767	465				465
SOC監視サービス	762	185				185
EDR監視サービス	239	55				55
自社製品監視	520	148				148
Microsoft監視	155	56				56
その他	90	18				18
コンサルティングサービス	566	125				125
合　計	2,333	591				591

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/