2025年3月期 第2四半期決算説明資料

Ｓ＆Ｊ株式会社

証券コード：5599 / 東証グロース市場

2024年11月13日

1. 会社概要
2. 第2四半期業績
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（FY2024 / 2Q）

高いサービス継続率と高いストック収益の比率により安定的な年間利益確保を実現

売上高 / 前年同期比成長率 **908**百万円(FY2024/2Q) / **27.4**%(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 **1,616**百万円(FY2024/2Q)
営業利益 / 営業利益率 **188**百万円(FY2024/2Q) / **20.7**%(FY2024/2Q)	ストック売上比率(2) **88.6**%(FY2024/2Q)
サービス継続率(3) / 解約率(4) **99.4**%(FY2024/2Q) / **0.6**%(FY2024/2Q)	従業員数(5) / 増加数 **63**名(FY2024/2Q) / **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

2024年10月31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	64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P38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。

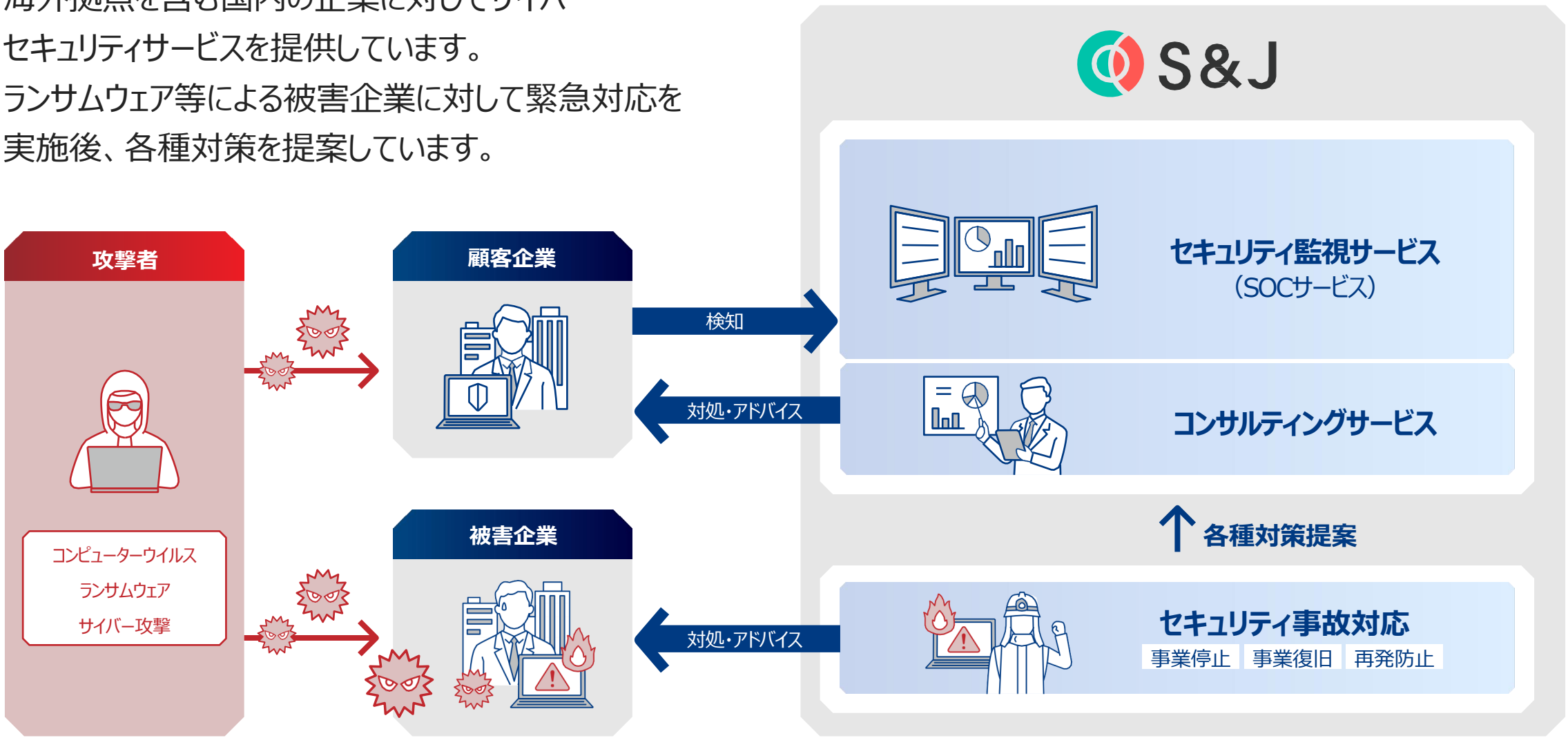
※媽祖は中国が発祥の海上守護神です。千里眼と順風耳を従え、航海の安全を守るとされています。

15年前から予見し提供していた"監視"と"対処"の重要性

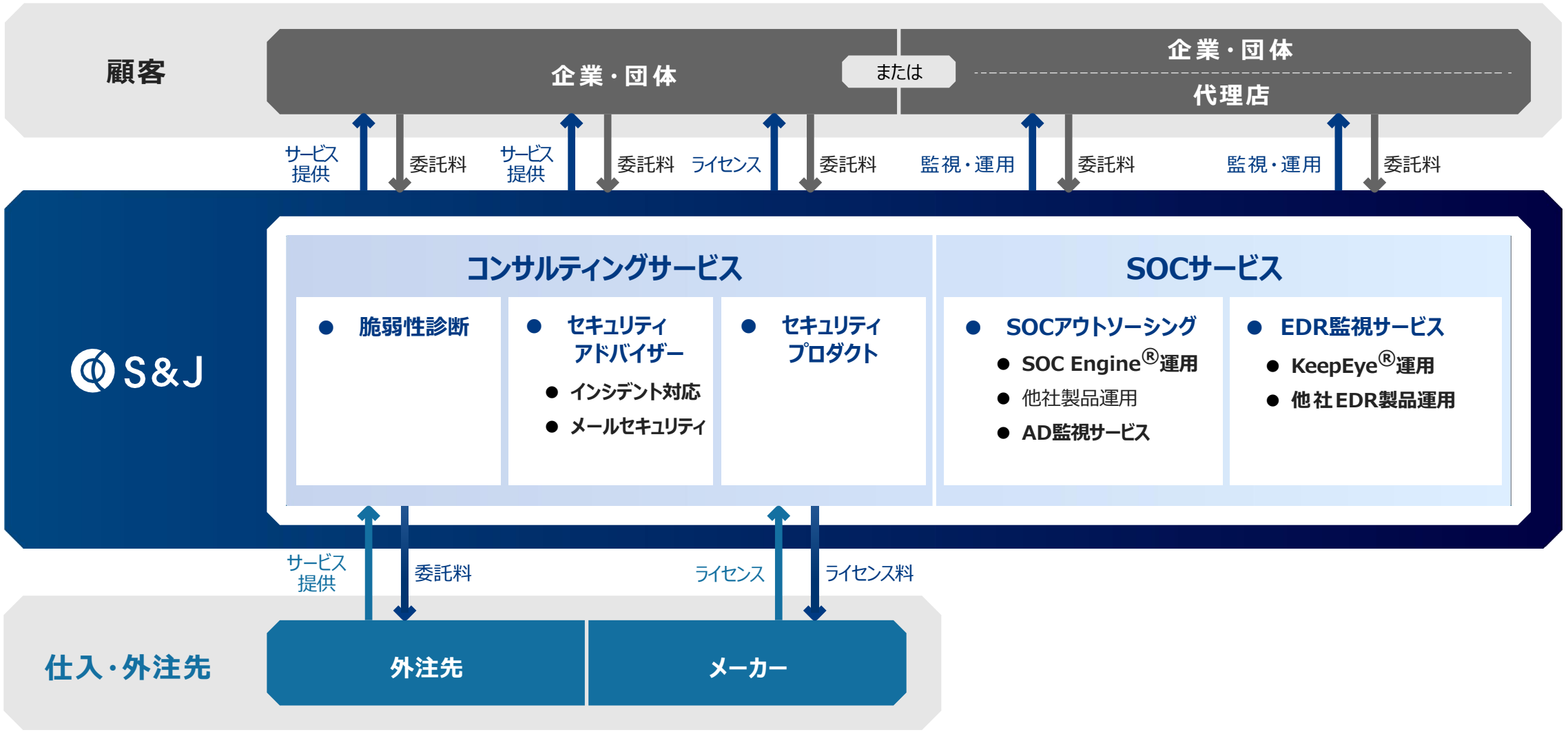
当社はセキュリティ“監視”だけではなく、サイバー攻撃に対する“対処”までを行い、今後の具体的な対応についてなどの“アドバイス”までを提供しています。
多くのセキュリティ事故対応に立ち会い、事故対応の経験に基づいたコンサルティングのアプローチがすべてのサービスに反映されているため、
お客様の期待を超えるアドバイスが実現できています。

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。



ビジネスモデル（収益構造）



インシデント対応まで包含したコミュニケーション型セキュリティ監視サービス

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。

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。

経済産業省のサイバーセキュリティ経営ガイドライン

経済産業省が策定公開したサイバーセキュリティ経営ガイドラインでは、“サイバーセキュリティは経営問題”と定義されており、2023年3月の改訂時には**善管注意義務違反**が追記された。
コロナ禍の影響もあり、テレワークが浸透する中、テレワークの隙を狙ったサイバー攻撃が増加しており、**インシデントの予兆の段階で即時の検知と対処**ができるような仕組みや体制を整備することが求められている。

I. 企業リスクマネジメントの一部としてのサイバーセキュリティ

経営者は、組織の意思決定機関が決定したサイバーセキュリティ体制が当該組織の規模業務内容に鑑みて適切でなかったため、組織が保有する情報の漏えいなどにより会社や第三者に損害が生じた場合、**善管注意義務違反や任務懈怠（けたい）に基づく損害賠償責任を問われ得るなどの会社法・民法等の規定する法的責任**やステークホルダーへの説明責任を負う。さらに、被害が深刻な場合の事業停止や新たな脅威に対処するための予算措置等の経営判断も要求され、**担当者への丸投げは許されるものではない。**

指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築

働き方の多様化への対応等、自組織のデジタル環境の見直しの結果、クラウドサービスへの移行や、ゼロトラストモデルの採用などの変更を行っても、インシデントの予兆を検知する仕組みが従来どおりのままでは見逃しや対応の遅れが生じてしまう。

対策例

- **ゼロトラストモデルに基づく対策を講じる際には、**境界防御の効果が期待できないことを踏まえた認証等の強化を図るとともに、**インシデントの予兆の段階で即時の検知と対処ができるような仕組みや体制を整備する。**
- **クラウドサービスを利用する際には、**クラウドサービスにおいて提供されるセキュリティ機能を考慮した選定を行い、それらの機能を活用するとともに、アクセス制限などの設定やアカウントの管理などが適切に維持・管理されるようにする

出典：経済産業省「サイバーセキュリティ経営ガイドラインVer3.0」

サイバーセキュリティ経営ガイドラインを満たしてい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

アラートを検知するだけではなく、対処方法まで含んでいる。

サイバーセキュリティ経営ガイドラインを満たしている当社のセキュリティ監視サービス

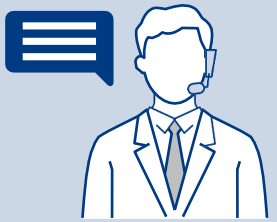
夜間などの顧客不在時の対応フロー

緊急対応が速やかに実施され、恒久対応方法まで含んでいる。

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

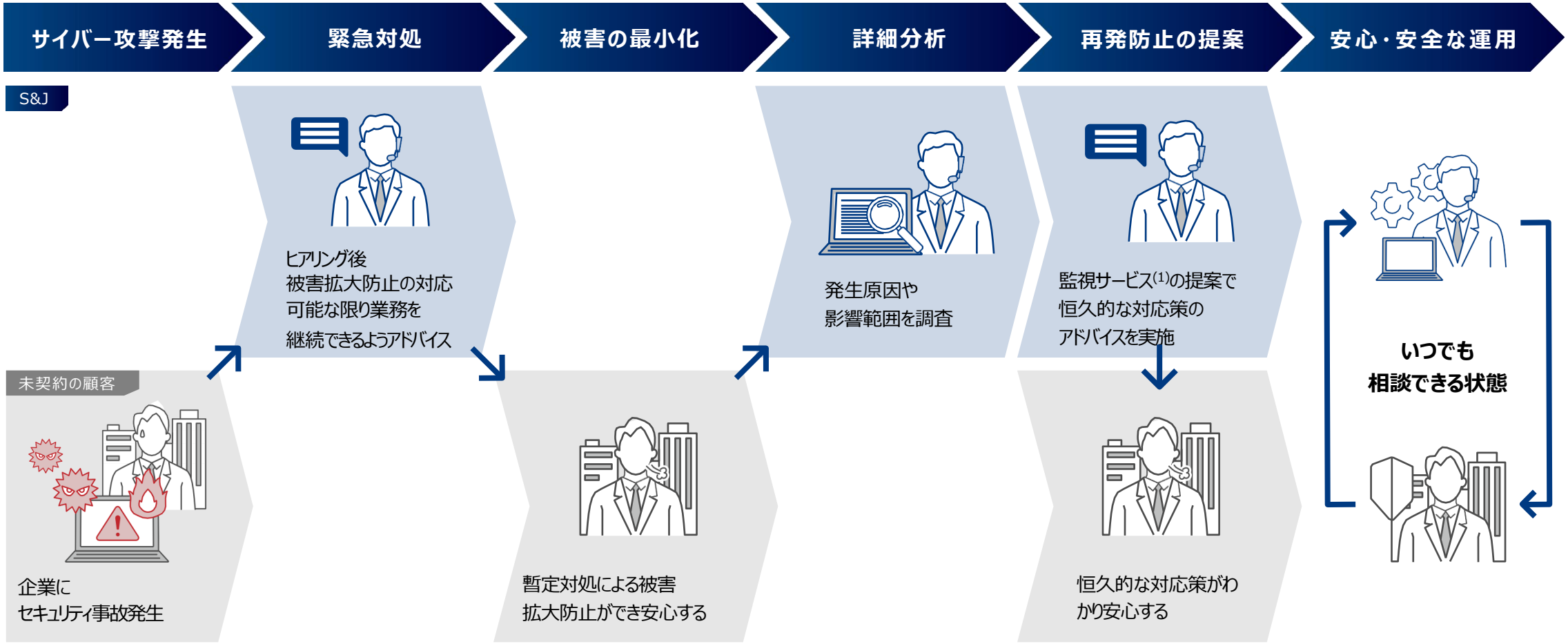
担当者不在時にサーバー攻撃が発生

対処済みで
恒久的な対応策もわかり安心する

サイバーセキュリティ経営ガイドラインを満たしてい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

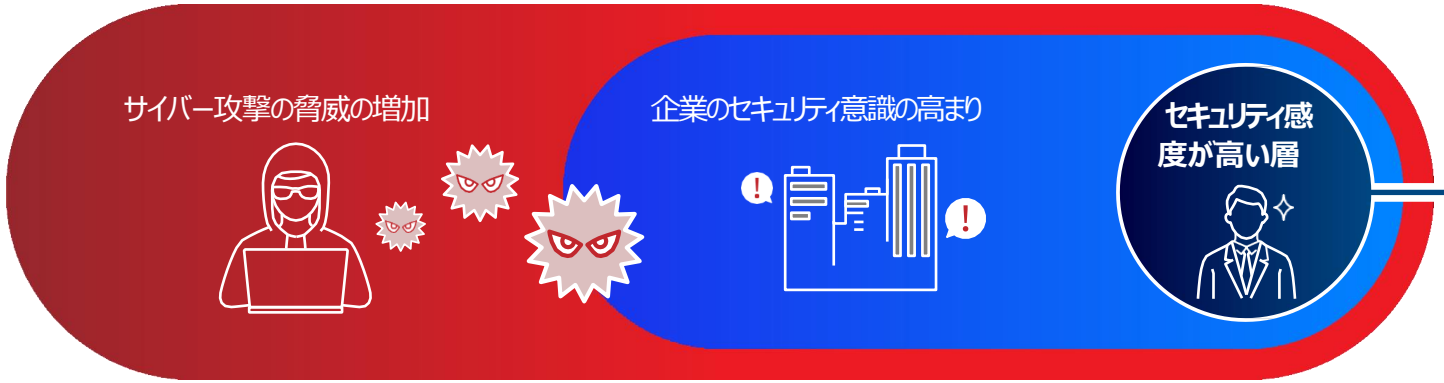
業務継続を優先的に考え、緊急対応の実施と恒久対応方法まで含んでいる。



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

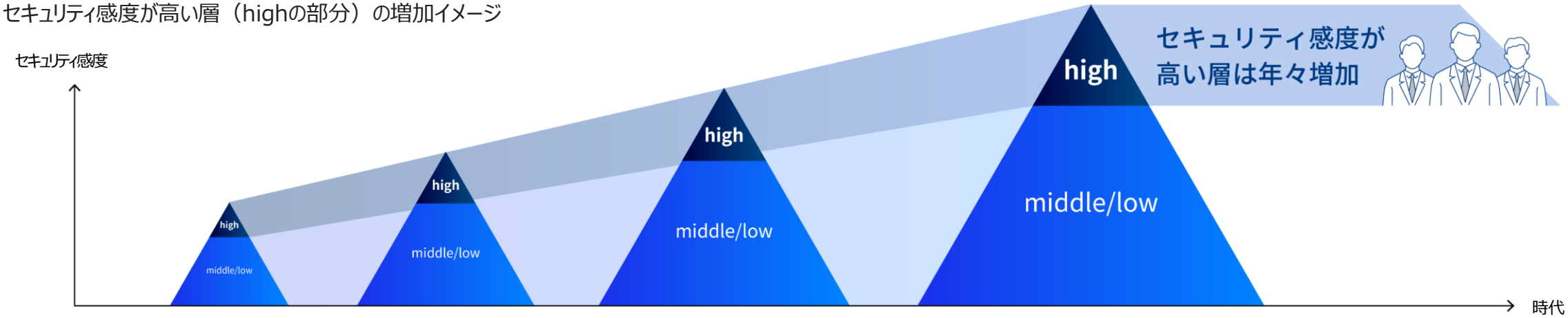


ここが当社のお客様

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



2. 第2四半期業績

業績サマリー(FY2024 / 2Q)

- 売上高は、908百万円と前年同期比27.4%増、進捗率45.1%（前年同期での進捗率は44.5%）。
- 営業利益は、188百万円と前年同期比53.3%増、進捗率46.7%（前年同期での進捗率は34.5%）。
- 当期純利益は、129百万円と前年同期比70.8%増、進捗率47.8%（前年同期での進捗率は36.1%）。

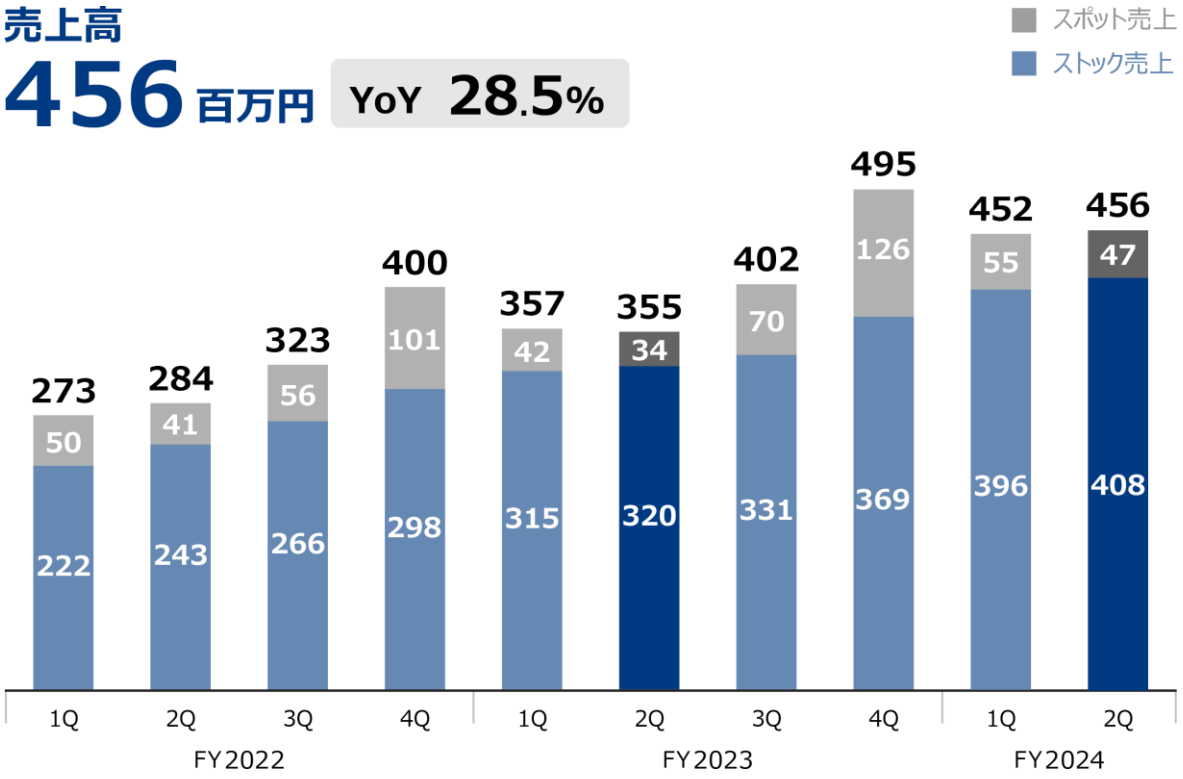
	FY2023 第2四半期		FY2024 第2四半期				FY2024通期（業績予想）	
	実績	対売上高	実績	対売上高	前年同期比増減額	前年同期比増減率	予想	進捗率
売上高	713	100.0%	**908**	100.0%	+195	+27.4%	2,013	45.1%
営業利益	122	17.2%	**188**	20.7%	+65	+53.3%	403	46.7%
経常利益	115	16.3%	**189**	20.8%	+73	+63.2%	403	46.9%
当期純利益	76	10.7%	**129**	14.3%	+53	+70.8%	271	47.8%

業績ハイライト　売上高、営業利益・営業利益率(FY2024 / 2Q)

- 売上高は、456百万円と前年同期比28.5%増。
  スポット売上は前四半期からやや減少となるも、ストック売上を順調に積上げている。
- 営業利益は、97百万円と前年同期比61.2%増、営業利益率は21.3%。
  移転費用等が第3四半期以降に発生することになったため、大幅な利益増。

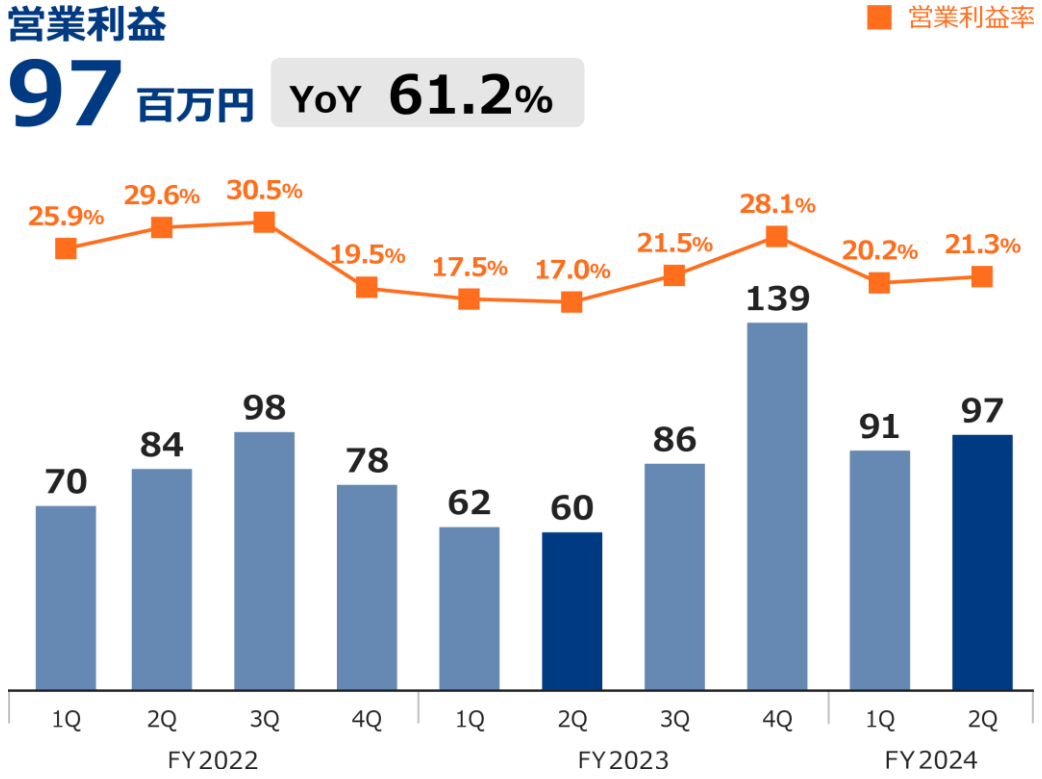
売上高

456 百万円　YoY 28.5%



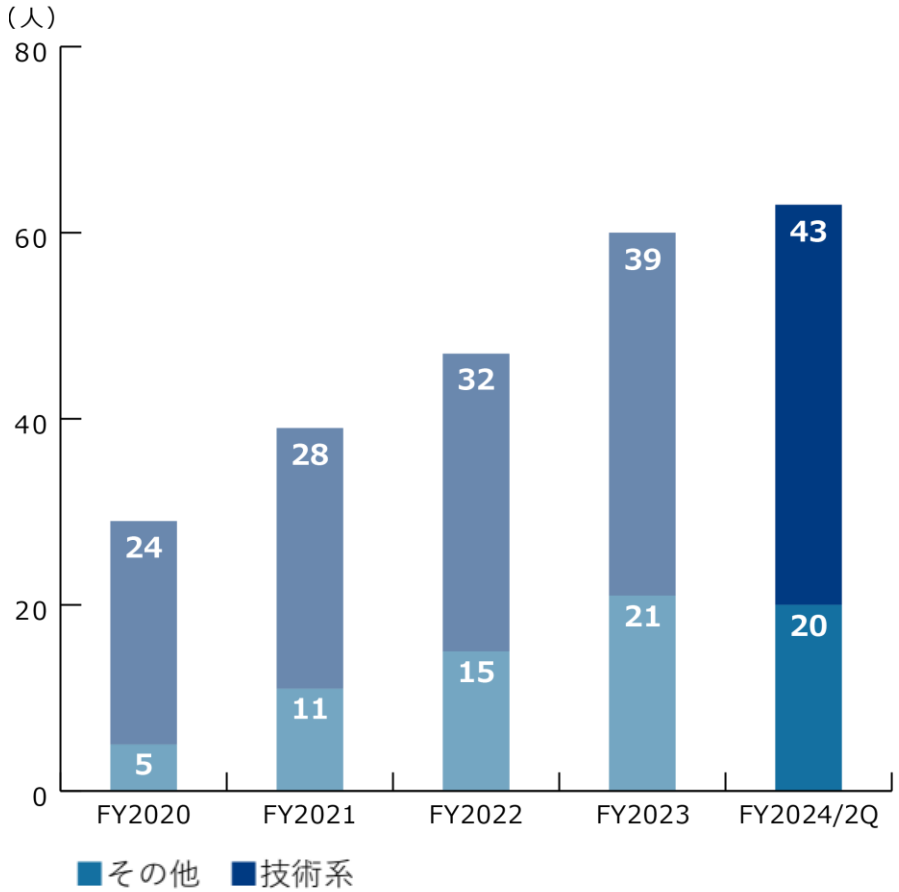
営業利益

97 百万円　YoY 61.2%



経営指標

人員推移 (1)



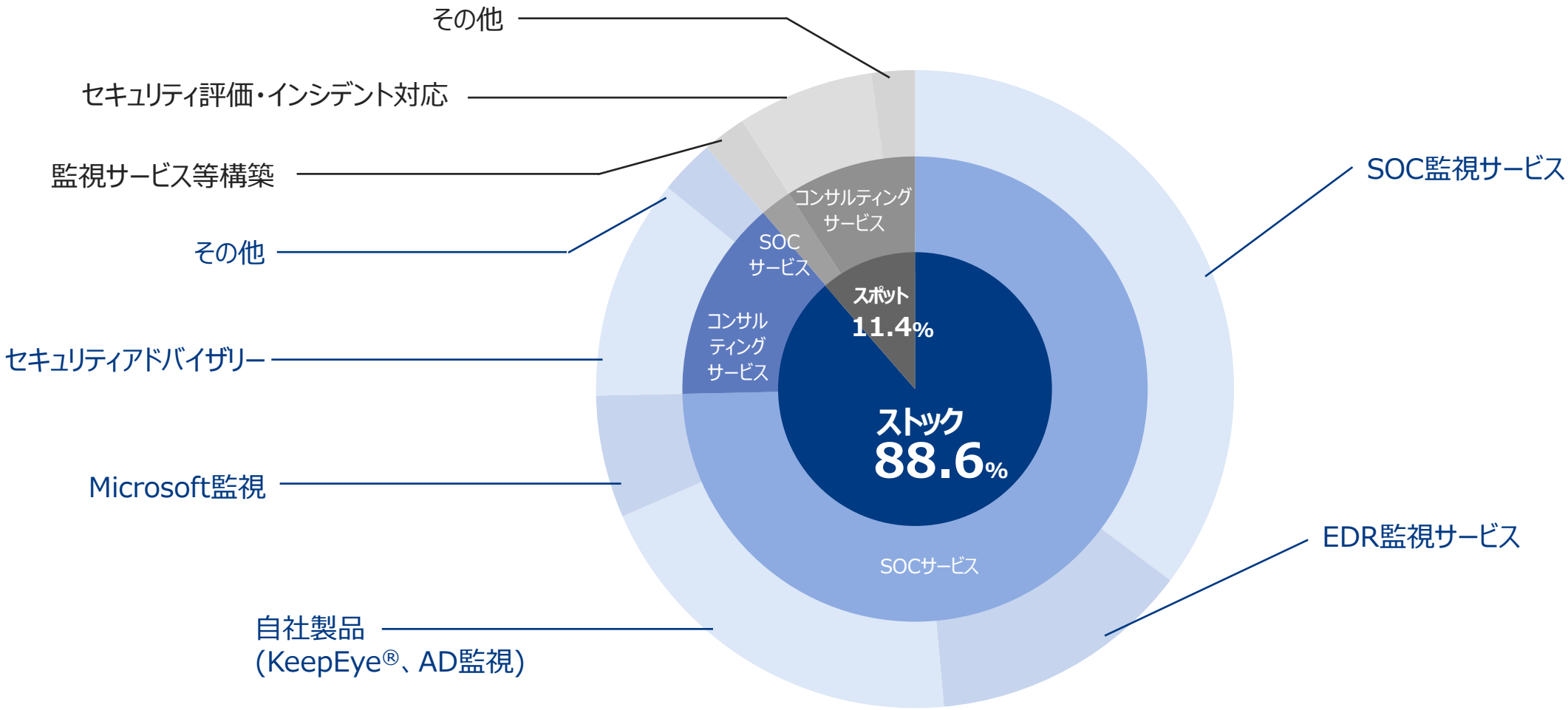
- **技術系人員の採用はほぼ計画どおりに進捗**
- **働きやすい職場環境の整備**
  - ①テレワークでの就業
  - ②有給休暇の充実（初年度15日/年、時間有休制度）
- **福利厚生制度の充実**
  - ①資格取得・維持支援制度
  - ②入社支度金制度
  - ③企業型確定拠出年金制度
  - ④GLTD保険 (2) 加入

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88.6%） FY2024 / 2Q

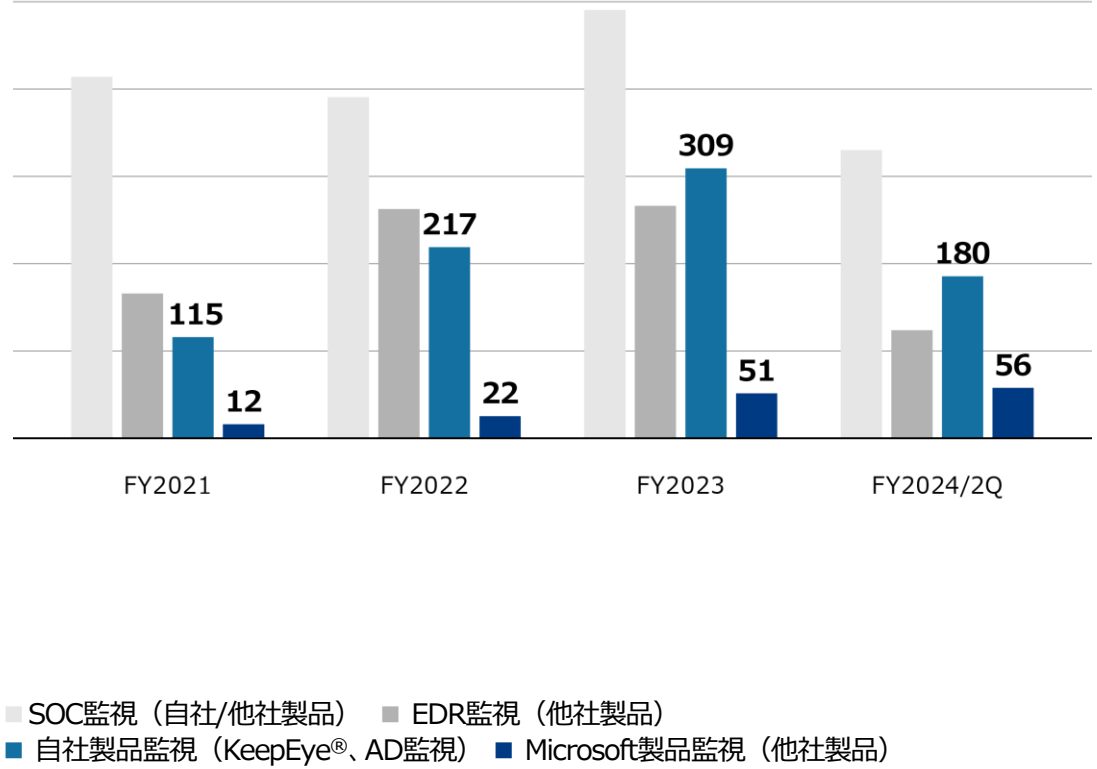


セキュリティ監視サービスの収益構造

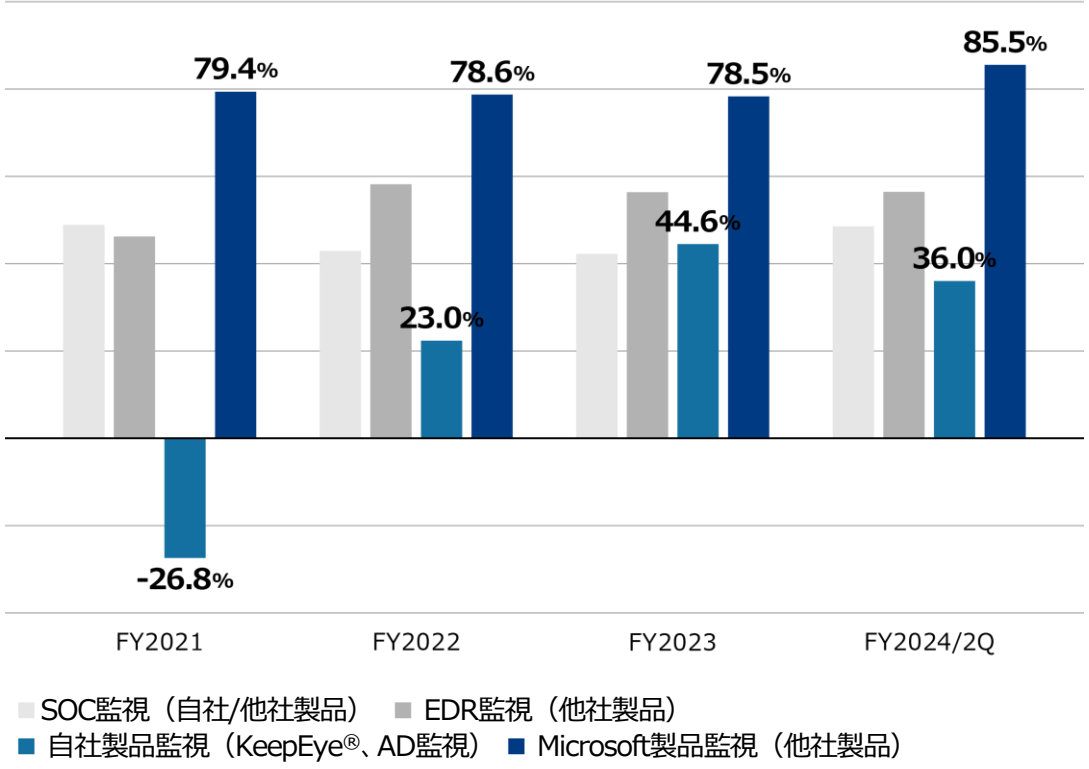
Microsoft 製品監視は売上は増加傾向が続いており、利益率も高水準を維持している。
自社製品監視（KeepEye®、AD監視）は、売上は堅調に推移している。利益率は若干低下したものの回復見込み。

売上

（百万円）



売上総利益率



成長戦略

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

- 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

FY2026 以降 テーマ：新規領域へのチャレンジ

- 社会インフラのIoT 化、企業のDX推進で求められるセキュリティ対策向け、コンサルティング / SOCサービスでのサービス開発

FY2025 テーマ：高度化サービス拡販/ ブランディング･マーケティング強化

- MXDR(1)、グローバル対応サービスの拡販
- 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

FY2023

- クラウド環境向けサービス開発
- SOCの高収益化
- コンサルティングサービスのストック化

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。詳細はP38用語解説に記載しています。

成長戦略

成長するクラウド関連に注力

- クラウド移行コンサルティングや監視サービス提供
- クラウド環境を含めたMXDRサービスを強化
- ライセンス販売をしているMicrosoftパートナーに、S&JサービスをOEM提供
- 直販では、Microsoftソリューションをコアにした統合サービス（SOC＋アドバイザリ）を提案

インシデント対応まで包含したコミュニケーション型SOCサービスをMXDRとして訴求

- 海外は自社内にセキュリティ専門人材を採用して自社で調査や対処が行えるため、アラートお知らせ型SOCサービスが主流
- 国内はセキュリティ専門人材がいる企業がほとんどなく、海外と同じアラートお知らせ型SOCサービスでは安心安全が確保できない
- 他社は収益性を重視して効率的な海外のビジネスモデルのまま、アラートをお知らせサービスを展開
- 当社は効率化を進めつつ、日本企業のニーズに合わせた影響分析 / コンサルのコミュニケーション / インシデント対応能力を融合したSOCサービスで安心安全を価値とした顧客満足度の高いサービスを提供
- 上記を当社のMXDRと定義して、サービス開発を推進

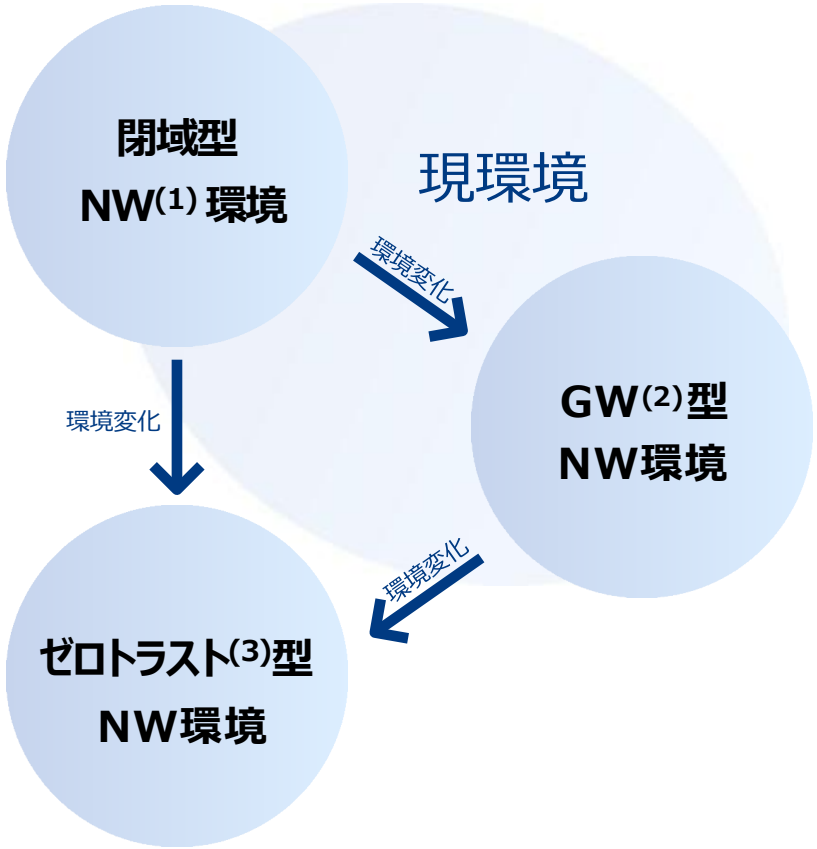
グローバル対応（多言語対応）を推進（SOC、コンサルティング）

- 現在は日本語のみの国内向けサービスを提供しているが、海外支店や現地法人などに対するサービス提供ニーズが強い
- 英語でのサービス提供に向けた検討を開始

新領域（社会インフラのIoT化、企業の DX推進）の事業化

- コンサルティング / 監視サービス提供

成長するクラウド関連に注力（ 企業IT環境変化に合わせた事業展開）



企業IT環境 分類	利便性 / リスク	対策対象	対策例	S&J提供サービス	今後必要な能力
閉域型 NW(1) 環境	● 利便性：低 ● リスク：低	● PC ● Server	● アーキテクチャ(4) ● 脆弱性パッチ適用 ● ウイルス対策 ● NW 監視		
現環境 → GW(2)型 NW環境	● 利便性：中 ● リスク：中	● PC ● Server ● NW ● GW	● アーキテクチャ ● 脆弱性パッチ適用(5) ● ウイルス対策 ● PC/Server監視 ● NW監視 ● GW監視	● セキュリティコンサル ● 自社製品も用いた SOC統合監視 (PC/Server/NW/GW) 監視 + 対処)	
ゼロトラスト(3)型 NW環境	● 利便性：高 ● リスク：高	● PC ● Cloud	● アーキテクチャ ● 脆弱性パッチ適用 ● ウイルス対策 ● PC/Cloud 監視	● セキュリティコンサル ● 自社製品も用いた SOC統合監視 (PC/Cloud) 監視 + 対処)	● Cloud製品の知識 ● Cloud監視ノウハウ

注：(1)NW：Network 社内ネットワーク環境。(2)GW：Gateway 社内ネットワークを外部のインターネットに接続する機能の総称を環境。(3)ゼロトラスト：ネットワークの境界に依存せず、「何も信頼しない」を前提に対策を講じるセキュリティの考え方。(4)アーキテクチャ：情報システムの設定方法や思想。(5)脆弱性パッチ適用：ソフトウェアの問題点や脆弱性を解消するためのプログラムを適用すること。

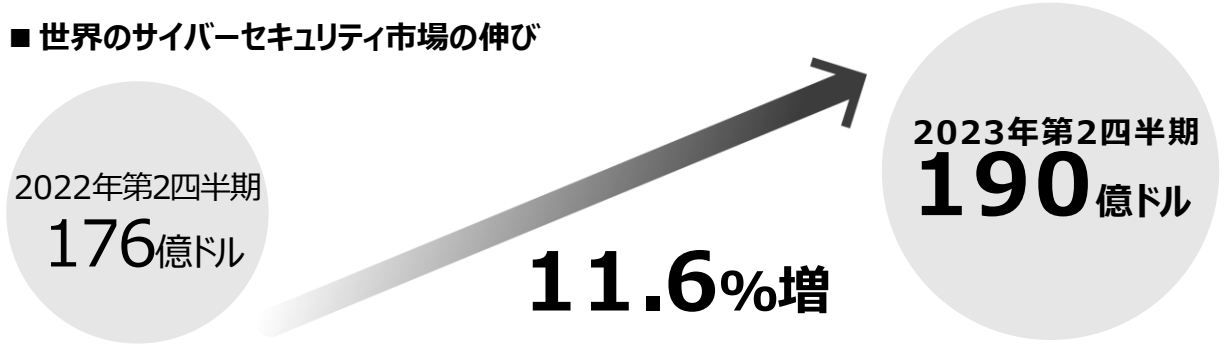
伸びるMicrosoftサイバーセキュリティ市場に注力

Microsoft製品を統合的に監視するSIEM製品と、他の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

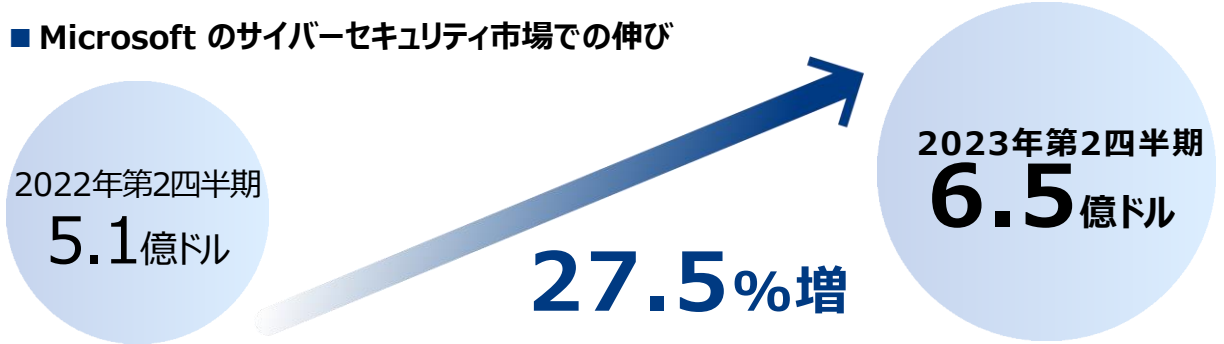
ベンダー	2022年第2四半期 市場シェア	2023年第2四半期 市場シェア	前年同期比 売上高成長率
Palo Alto Networks	8.50%	9.60%	25.40%
Fortinet	6.60%	7.00%	19.00%
Cisco	6.70%	6.10%	1.20%
CrowdStrike	3.10%	3.80%	34.30%
Check Point	3.90%	3.60%	2.80%
Okta	3.10%	3.40%	24.50%
Microsoft	**2.90%**	**3.40%**	**31.10%**
Symantec	3.10%	2.90%	5.60%
IBM	3.10%	2.70%	-2.00%
Trellix	2.90%	2.70%	3.00%
Zscaler	2.00%	2.50%	37.70%
Trend Micro	2.30%	2.20%	7.80%
その他	51.90%	50.20%	8.00%
合計	100%	100%	11.60%

2023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11.6%増の190億ドルとなった。

■ 世界のサイバーセキュリティ市場の伸び



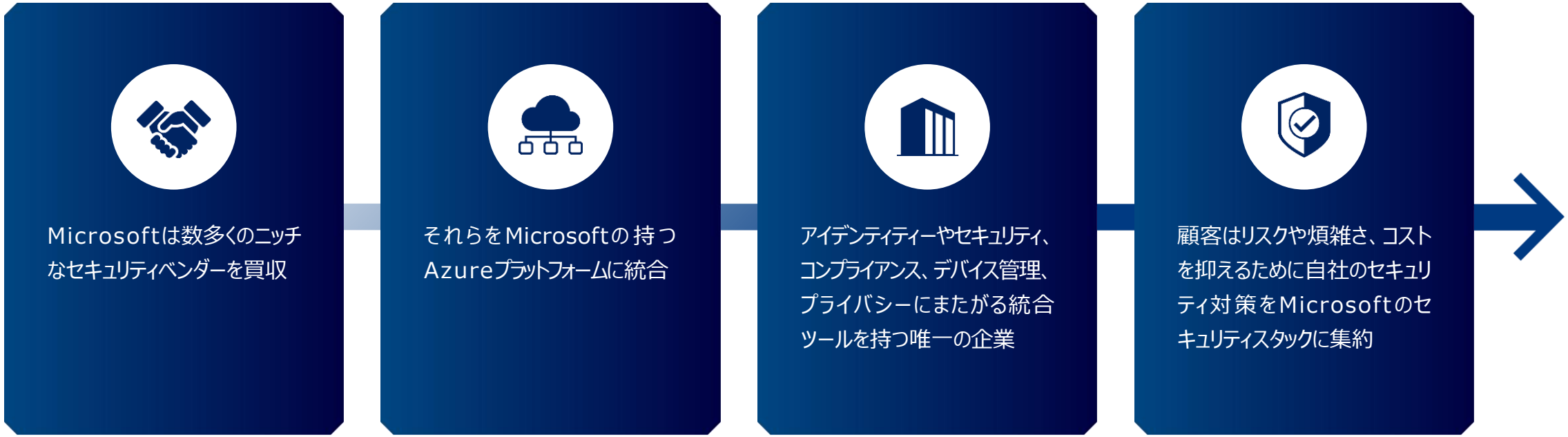
■ Microsoft のサイバーセキュリティ市場での伸び



出典：https://www.canalys.com/newsroom/cybersecurity-market-Q2-2023

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/

新領域（社会インフラのIoT化、企業のDX推進）の事業化

■ **新規参入ではなく、現在の事業の延長線で展開できる**

■ **代理店との協業により、社会インフラ監視へ領域を広げるブランディング戦略**

市場規模

- 急速な社会インフラの IoT化が進んでいる
- 但し、サイバー攻撃への対策が考慮されていないため、対策が急務
- 政府（主管：経済産業省）が CPS(1)の推進に取り組んでおり、市場は大きく拡大する

競合状況

- 現在は社会インフラ設備構築をしているベンダーが、セキュリティ案件も取っている

事業参入

- 社会インフラ監視をするためのノウハウ（UTM(2)/NDR(3)/ 生ログ）を有している

注：(1)物理的なプロセスとコンピューターシステムが密接に統合されているシステム。(2)ネットワークセキュリティのアプローチで、単一のデバイスまたはプラットフォームを使用し、さまざまなセキュリティ機能を統合的に管理し、監視すること。(3)ネットワークセキュリティのアプローチで、ネットワーク上での異常なアクティビティや悪意のある挙動を監視し、検出し、対応するためのテクノロジーやプロセスを指す。

中期経営計画（FY2024～FY2026）

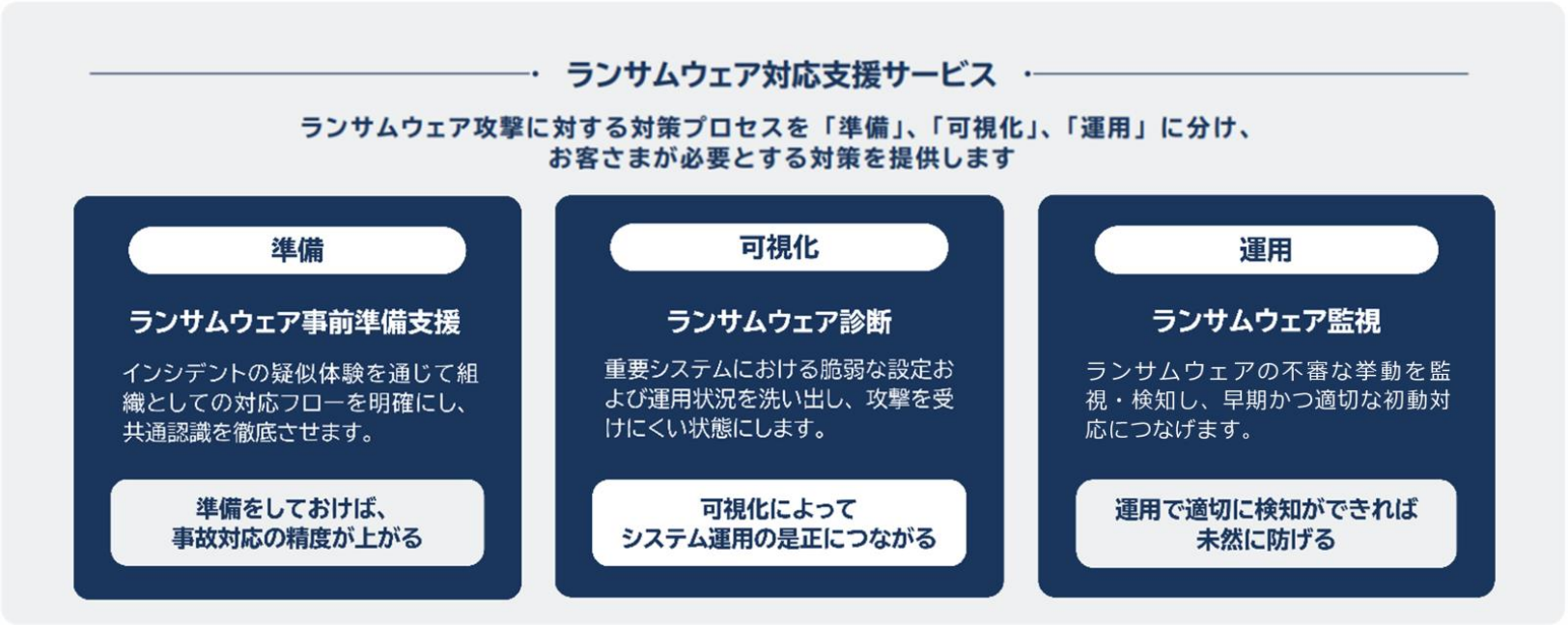
（単位：百万円）

		FY2023（実績）	FY2024	FY2025	FY2026
売上高 （年成長率）		1,610 （25.7%）	2,013 （25.0%）	2,519 （25.1%）	3,168 （25.8%）
	SOC （年成長率）	1,185 （27.6%）	1,533 （29.4%）	1,968 （28.4%）	2,487 （26.4%）
	コンサルティング （年成長率）	425 （20.7%）	480 （13.0%）	550 （14.6%）	680 （23.6%）
営業利益 （営業利益率）		348 （21.7%）	403 （20.0%）	562 （22.3%）	751 （23.7%）
経常利益 （経常利益率）		319 （19.8%）	403 （20.0%）	562 （22.3%）	751 （23.7%）
当期純利益 （当期純利益率）		218 （13.6%）	271 （13.5%）	382 （15.2%）	511 （16.1%）

4. トピックス

S&J×JBS、「ランサムウェア対応支援サービス」をリリース
～事前準備支援・診断・監視の3つの柱で提供～

- ランサムウェアの攻撃手法や最新の動向を正確に把握することが難しく、適切な対処が行えないという課題を抱えたお客様に対して、必要なポイントに絞って手軽かつ高度な対策を支援
- 攻撃への対応態勢を整備する「ランサムウェア事前準備支援」、攻撃の有無や運用上の不備を洗い出す「ランサムウェア診断」、攻撃を検出する「ランサムウェア監視」の3つのメニューで構成
- JBSが持つ、マイクロソフトを中心としたクラウド事業における「デジタル変革」や「クラウドセキュリティ」に関する知見と、S&Jの脅威に対する高度な分析力やセキュリティ事故対応力を組み合わせることで、高いレベルでの問題解決を実現

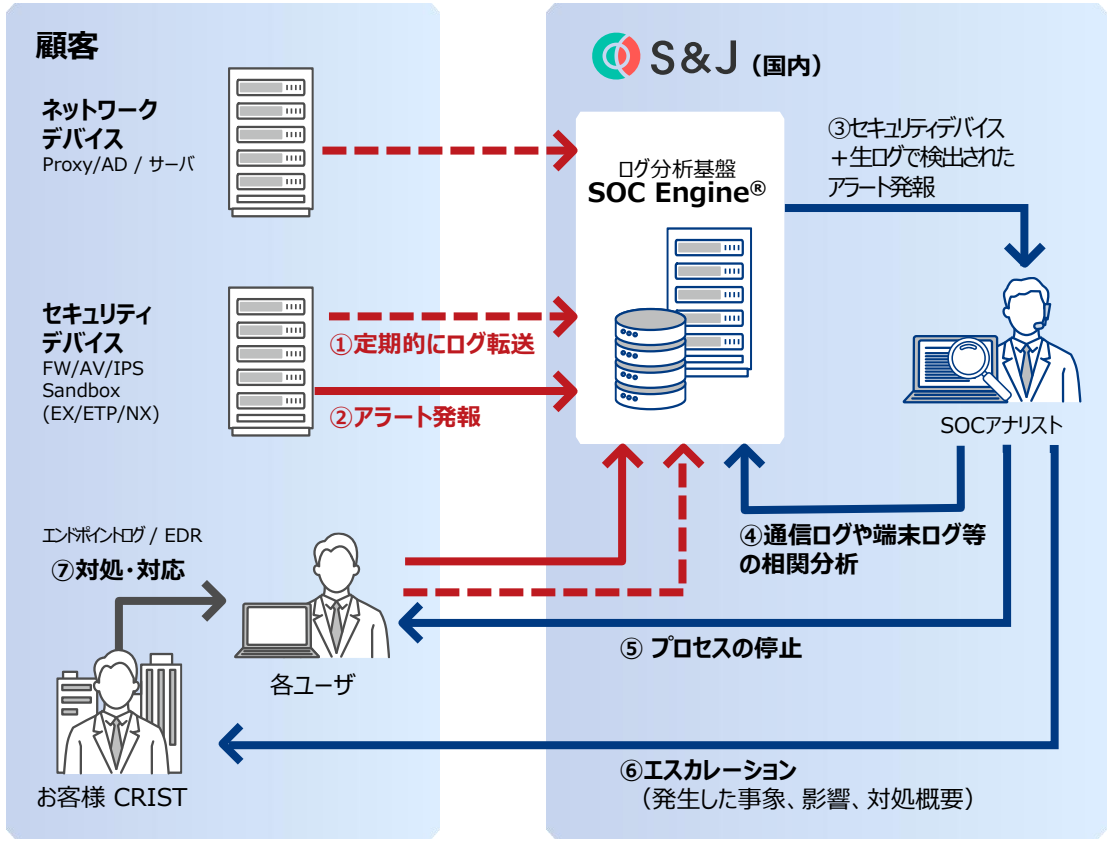


5. Appendix

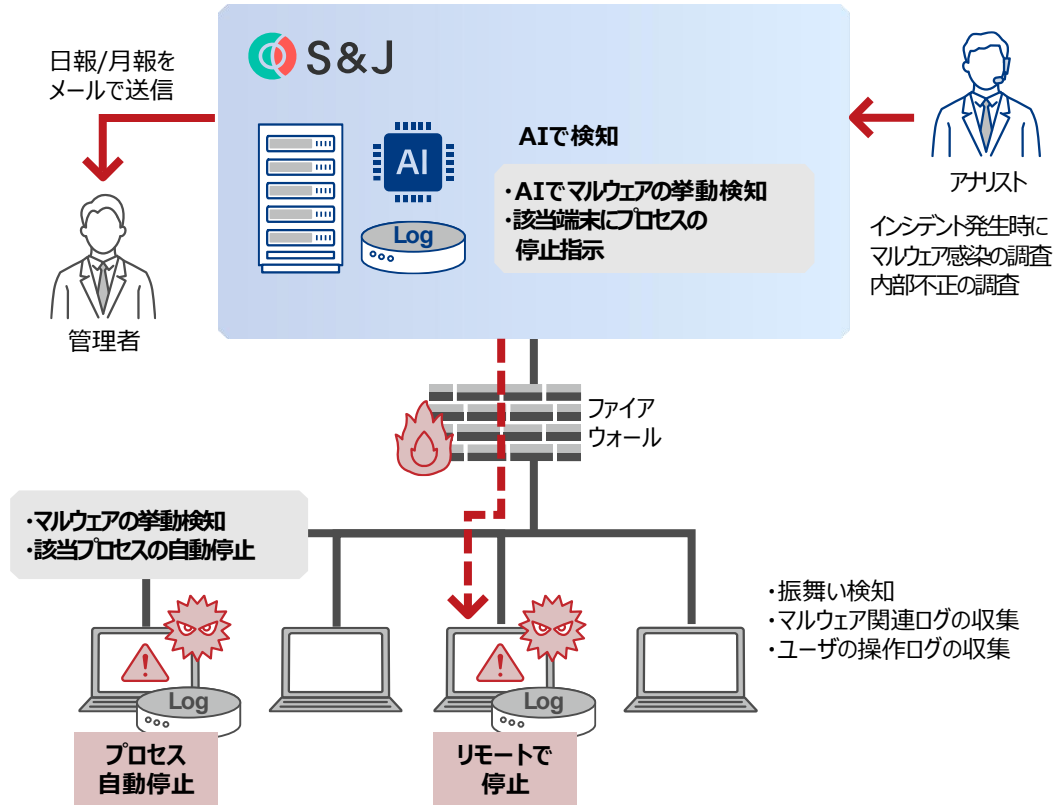
セキュリティ監視（SOC）サービス説明

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

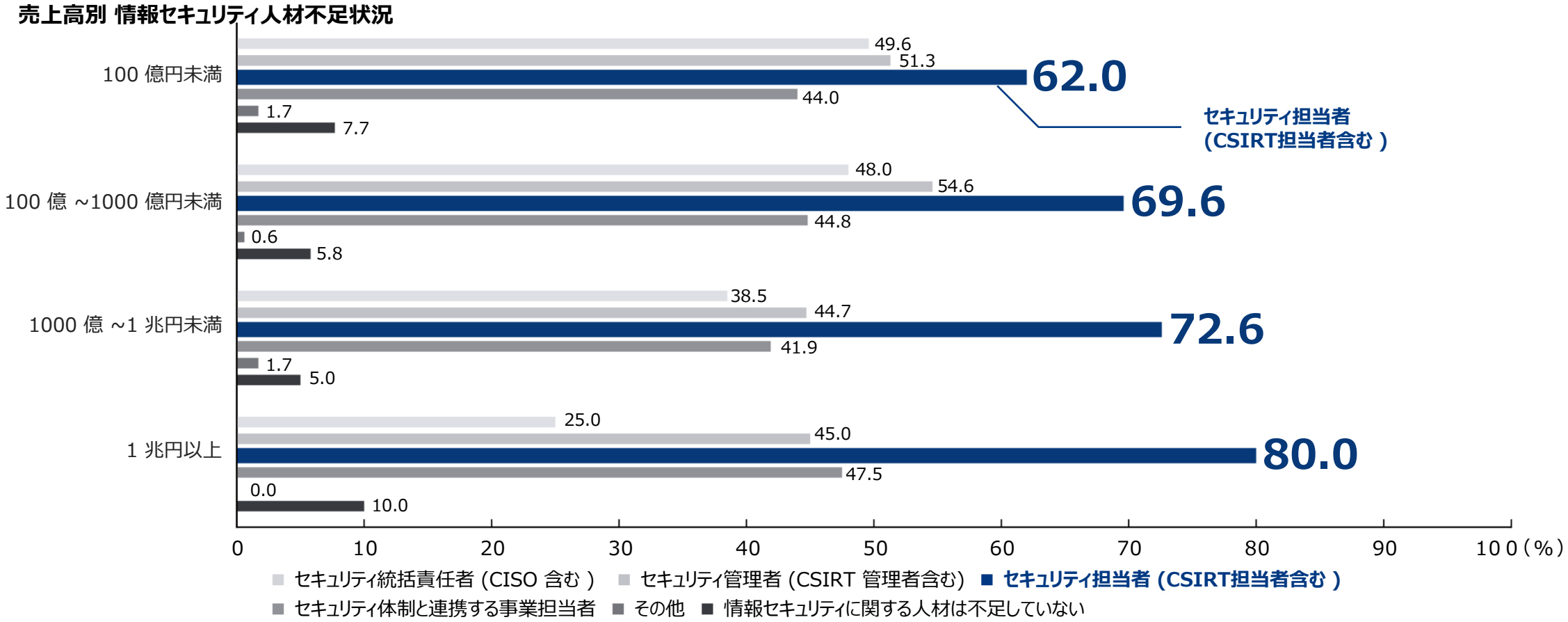
脆弱性診断

- 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

企業の抱える課題

売上高が大きい企業ほどセキュリティ人材のうちセキュリティ担当者の不足を感じている

サイバーセキュリティサービスの**アウトソーシングを行う当社へのニーズが高まっている**



出典：一般社団法人 日本情報システム・ユーザ協会（JUAS)「企業IT動向調査報告書2023 ユーザ企業のIT投資活用の最新動向（2022年度調査）」

市場環境

国内サイバーセキュリティ市場を取り巻く市場環境は、
サイバー攻撃の脅威の増加に伴い、企業のセキュリティ意識が益々高まっている

企業のセキュリティ意識の高まり

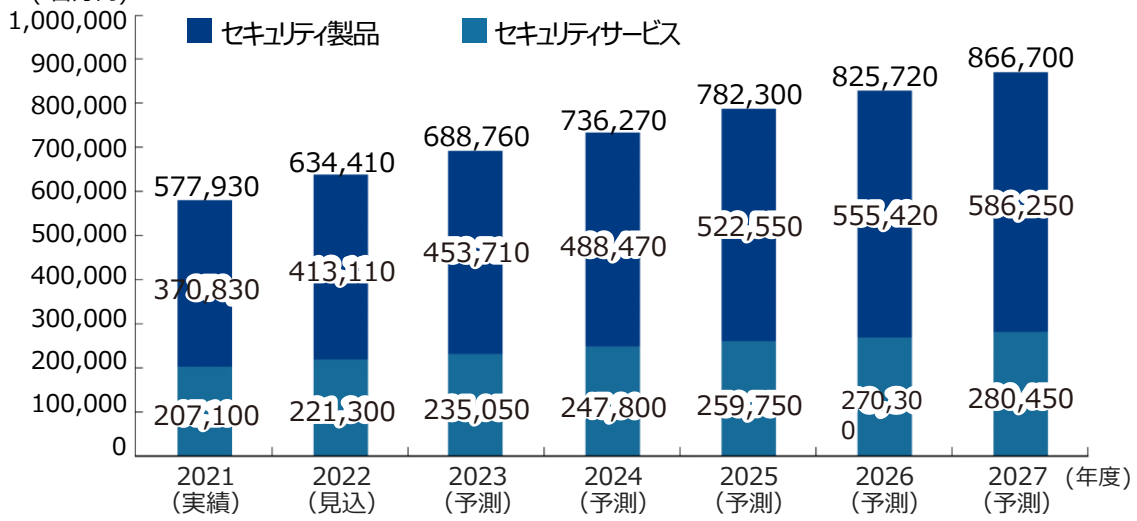
ネットワークセキュリティビジネスの現状と将来展望

ネットワークセキュリティビジネス市場

2021年度 5,779.3億円 > 2027年度 8,667億円

<ネットワークセキュリティビジネス市場全体推移>

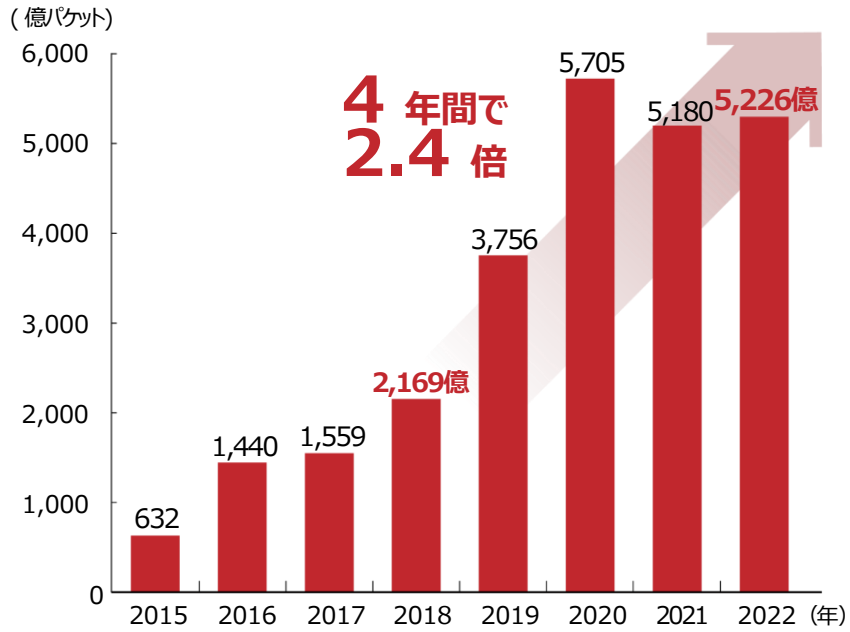
※CAGR（27/21）は 2021 年から 2027 年の年平均成長率を表しています。



市場全体 CAGR (27/21)	7.0%
製品市場 CAGR (27/21)	7.9%
サービス市場 CAGR (27/21)	5.2%

出典：富士キメラ総研「2022ネットワークセキュリティビジネス調査総覧＜市場編＞」

サイバー攻撃の脅威の増加



出典：国立研究開発法人情報通信研究機構（NICT）「NICTER観測レポート2022」、
表1：年間総観測パケット数の統計（過去10年間）から当社にて作表
2021、2022年減少の要因：2020年に観測された特定のスキャンパケットが観測されなかったため

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/