



2025年2月期  
第2四半期

# 決算説明資料


2024年10月11日

バリオセキュア株式会社 | 証券コード：4494

# INDEX

目次

1. 会社概要
2. 2025年2月期第2四半期 決算概要
3. 2025年2月期業績予想
4. トピックス
5. 中期成長戦略
6. Appendix

The background features a light blue and white color scheme with faint, stylized circuit board traces and geometric shapes. A prominent horizontal blue gradient bar spans the middle of the page. The text '1. 会社概要' is centered within this bar.

# 1. 会社概要

▶ 会社名	バリオセキュア株式会社 (Vario Secure Inc.)		
▶ 創業	2001年6月21日		
▶ 代表者	代表取締役社長 山森 郷司		
▶ 資本金	7億5,179万円		
▶ 従業員数	93名※		
▶ 所在地	本社 〒101-0054 東京都千代田区神田錦町1-6 住友商事錦町ビル5F 大阪オフィス 〒550-0014 大阪府大阪市西区北堀江1-2-19 福岡営業所 〒812-0013 福岡県福岡市博多区博多駅東1-12-17		
▶ 事業内容	マネージドセキュリティサービス インテグレーションサービス		
▶ 役員構成	代表取締役社長	山森 郷司	取締役営業本部長 伊藤 裕介
	取締役	林 隆弘	取締役 井口 圭一
	取締役	森 博也	取締役監査等委員 畑 敬子
	取締役監査等委員	高橋 可奈	取締役監査等委員 森脇 基
▶ 親会社	HEROZ株式会社(持ち株比率約42%)		
▶ Web	<a href="https://www.variosecure.net/">https://www.variosecure.net/</a>		
▶ 認証	ITSMS(ISO20000)、ISMS(ISO27001)、プライバシーマーク		

2024年8月末時点。ただし、代表者及び役員構成は同年10月1日時点

※正社員、契約社員、嘱託社員の合計

## ミッション





インターネットを利用する全ての企業が  
安心して快適にビジネスを遂行できるよう、  
日本そして世界へ全力でサービスを提供する



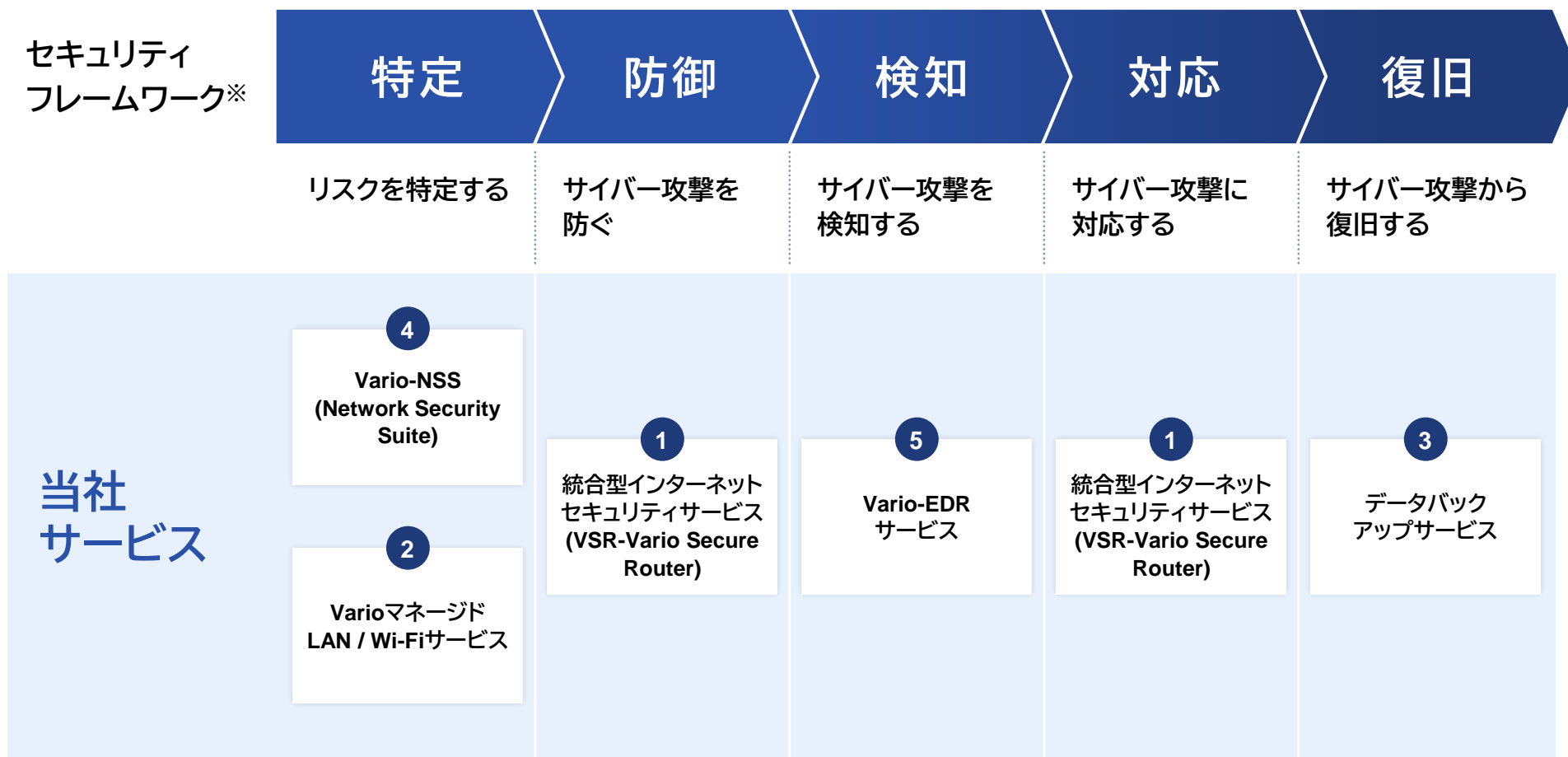
当社は、インターネットセキュリティサービスを提供する企業として、インターネットからの攻撃や内部ネットワークへの侵入行為、ウィルスの感染やデータの盗用といった各種脅威から企業のネットワークを守り、安全にインターネットを利用することができる総合的なネットワークセキュリティサービスを提供しています。



企業のインターネット利用を安全・快適にできるサービスを提供しております。

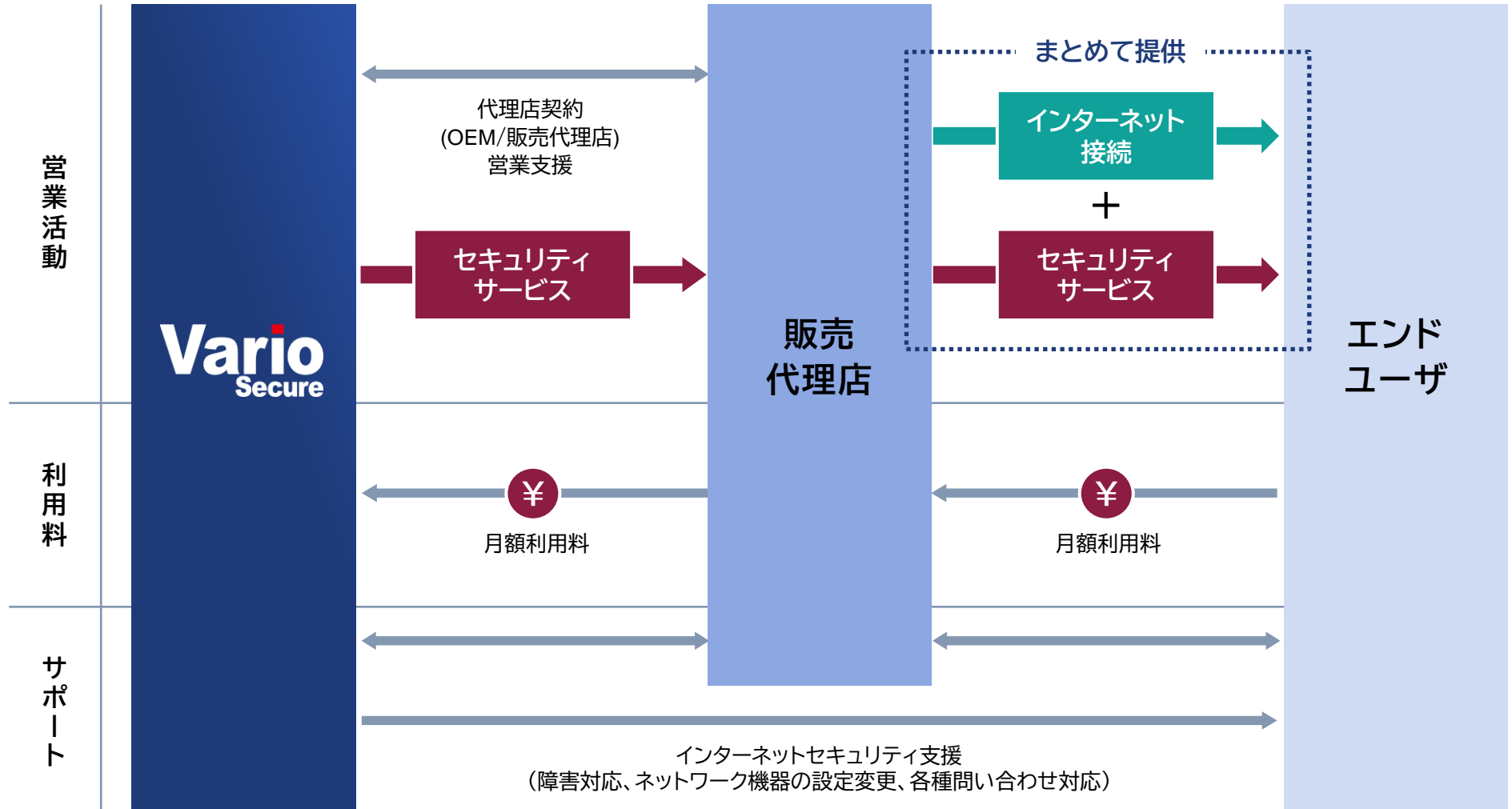
	マネージドセキュリティサービス	インテグレーションサービス
サービス形態	導入支援・導入・運用・保守 24時間/365日、日本全国	機器販売・構築
収益モデル	リカーリング型(月額課金)	一時課金型
サービス内容	<b>①統合型インターネットセキュリティサービス(マネージド型)</b> インターネットの出入口を守る  マネージドセキュリティサービス専用機器 VSR-Vario Secure Router	<b>⑥中小企業向け統合セキュリティ機器販売(販売型)</b> 50名以下ならこれ1台で安心  中小企業向け統合セキュリティ機器 VCR-VarioCommunicate Router
	<b>②VarioマネージドLAN / Wi-Fiサービス</b> 社内LANスイッチ/Wi-Fiアクセスポイントを守る	<b>⑦ネットワークインテグレーションサービス(以下、IS)・ネットワーク機器の調達や構築</b> 社内のネットワークの構築(無線LANネットワーク)
	<b>③データバックアップサービス</b> もしもの時のデータ保持  データバックアップサービス専用機器 VDP-Vario Data Protect	
	<b>④Vario-NSS(Network Security Suite)</b> 不正端末発見, 脆弱性管理	
	<b>⑤Vario-EDRサービス</b> 少ない運用負担で、サイバー攻撃の発見と対応を支援 	

構築から復旧まで、セキュリティ対策の全プロセスをカバーしております。



※政府機関「米国国立標準研究所(National Institute of Standards and Technology, NIST)」が2014年に発行したNIST サイバーセキュリティフレームワーク(Cyber Security Framework, CSF)。

主力の統合型インターネットセキュリティサービスは、主にインターネット回線に付帯して提供しております



通信キャリア、Sler、電力系通信会社様等との間でOEM契約を締結し、長期にわたるパートナーシップを構築しております。

## マネージドセキュリティサービスのOEMパートナー 全31社(2024年8月末時点)



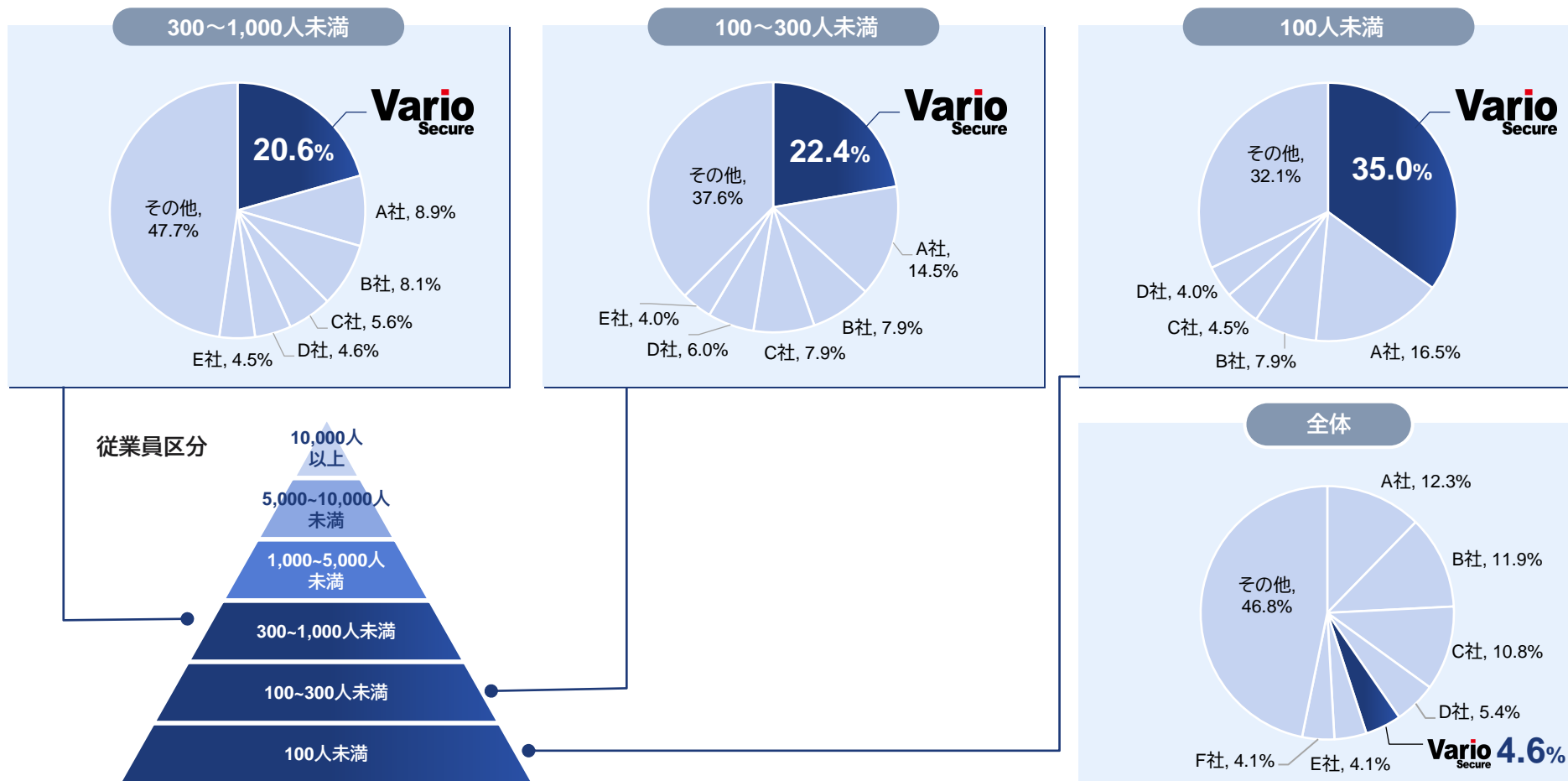
他多数

※左上から右下への50音順



ファイアウォール/UTM運用監視サービス市場において従業員1,000人未満の企業ではトップシェアです。

## ■ ファイアウォール/UTM運用監視サービス市場ベンダー別売上金額シェア(2022年度)



出所:ITR「ITR MARKET VIEW ゲートウェイ・セキュリティ対策型SOCサービス市場2023」ファイアウォール/UTM運用監視サービス市場(2022年度)

## 2. 2025年2月期第2四半期 決算概要

安定したストック型売上比率及び低解約率を背景に、前年同期比増収を達成。各重要な業績指標は安定的に推移しております。

## 決算ハイライト



## 重要な業績指標



※解約率(金額ベース) = 四半期解約金額 ÷ (各年度の期初ベース月次売上収益 × 3ヶ月)

当第2四半期の業績は対前年比で増収でしたが、原価増の影響により減益での着地でした。

(百万円)	2024年2月期 第2四半期実績	2025年2月期 第2四半期実績	前年同期比増減
売上収益	662	<b>680</b>	2.8% (+18)
営業利益	145	<b>122</b>	△16.0% (-23)
四半期利益	92	<b>81</b>	△11.3% (-10)
一株当たり当期利益(円)※	42.21	<b>40.45</b>	△1.76

※一株当たり当期利益(EPS)=通期利益÷発行済み株式数

財政状態に大きな変化はなく、継続的な収益の積み上げと借入返済により、自己資本比率は漸増の傾向です。

(百万円)	2024年 2月期末	2025年2月期 第2四半期末	増減
資産合計	7,649	<b>7,676</b>	26
流動資産	1,608	<b>1,607</b>	△1
非流動資産	6,041	<b>6,069</b>	28
のれん	5,054	<b>5,054</b>	0
負債合計	2,101	<b>1,945</b>	△156
流動負債	776	<b>726</b>	△49
非流動負債	1,325	<b>1,218</b>	△106
資本合計	5,548	<b>5,731</b>	183
負債及び資本合計	7,649	<b>7,676</b>	26

## 財務指標

	2024年 2月期末	2025年2月期 第2四半期末
のれん純資産倍率※1	0.91x	<b>0.88x</b>
有利子負債	1,300百万円	<b>1,200百万円</b>
負債比率※2	23.4%	<b>20.9%</b>
Net D / E レシオ※3	8.6%	<b>7.1%</b>
Net D / EBITDA倍率※4	0.68x	<b>0.55x</b>
自己資本比率※5	72.5%	<b>74.7%</b>

※1: のれん純資産倍率= のれん / 資本

※2: 負債比率= ((短期借入金+長期借入金) ÷ 自己資本) × 100

※3: Net D/E レシオ= 純有利子負債 / 資本 (純有利子負債= 有利子負債残高(短期借入金+長期借入金) - 現金及び現金同等物(預金))

※4: Net D/EBITDA倍率= 純有利子負債 / EBITDA (EBITDA(償却前営業利益)は、金利や税、減価償却費を計上する前の利益)

※5: 自己資本比率= (自己資本 ÷ 総資本) × 100

IFRS (国際会計基準)

マネージドセキュリティサービスは、前年比大幅増のエンドポイントセキュリティ(Vario-EDR)が寄与し、安定的に売上が拡大。インテグレーションサービスは、ネットワーク構築が堅調に推移しました。

(百万円)	2024年 2月期 第2四半期実 績	2025年 2月期 第2四半期実 績	増減	構成比	主な増減要因
売上収益	1,306	<b>1,354</b>	+3.7% (+48)	<b>100%</b>	Vario-EDRやVarioマネージドLAN / Wi-Fiのサービスラインナップ拡充を踏まえたクロスセルの強化を通じて売り上げ拡大
マネージドセキュリティサービス	1,139	<b>1,168</b>	+2.6% (+29)	<b>86.3%</b>	需要が堅調なネットワーク構築を中心に計画し、ISは計画を上回って好調に推移
インテグレーションサービス	166	<b>185</b>	+11.4% (+18)	<b>13.7%</b>	

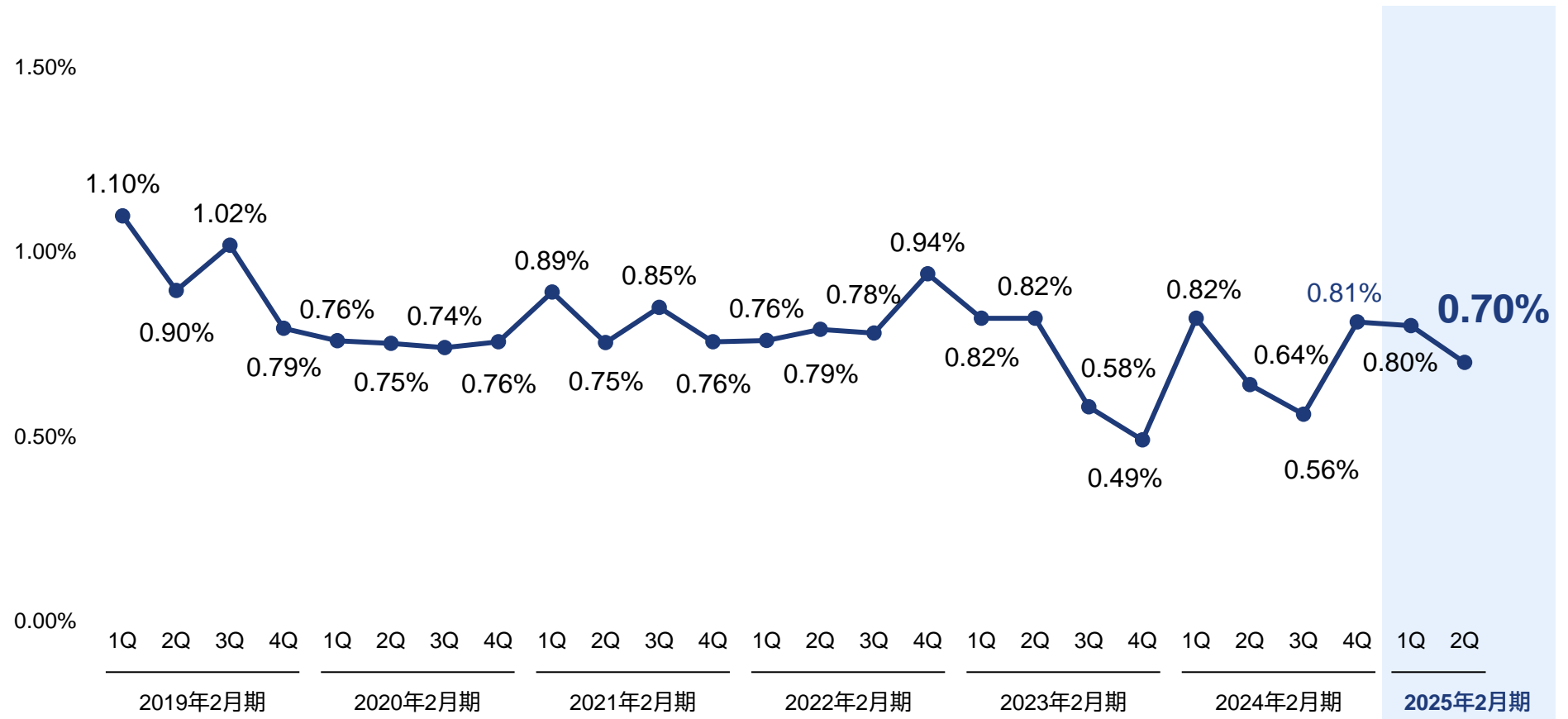
主な増減要因

Vario-EDRやVarioマネージドLAN / Wi-Fiのサービスラインナップ拡充を踏まえたクロスセルの強化を通じて売り上げ拡大

需要が堅調なネットワーク構築を中心に計画し、ISは計画を上回って好調に推移

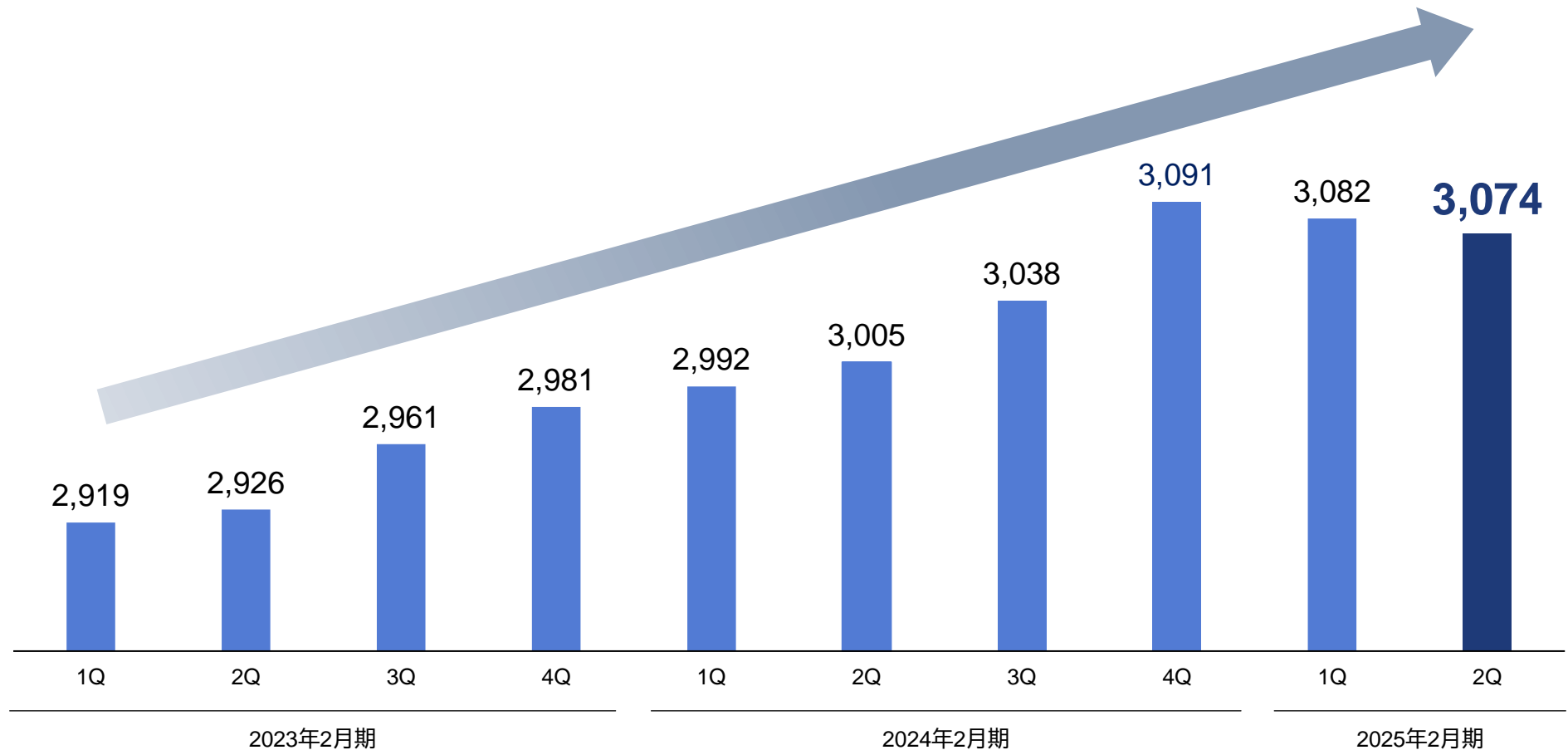
統合型インターネットセキュリティ(マネージドセキュリティサービス)の解約率※は、1%以下の低い水準で継続して推移しています。

## ■ 四半期解約率の推移



※: 解約率(金額ベース) = 四半期解約金額 ÷ (各年度の期初ベース月次売上収益 × 3ヶ月)

マネージドセキュリティサービスのエンドユーザー企業数は、今期に入って微減傾向にありますが、長期傾向としては堅調に増加しており、安定的な収益基盤に寄与しています。





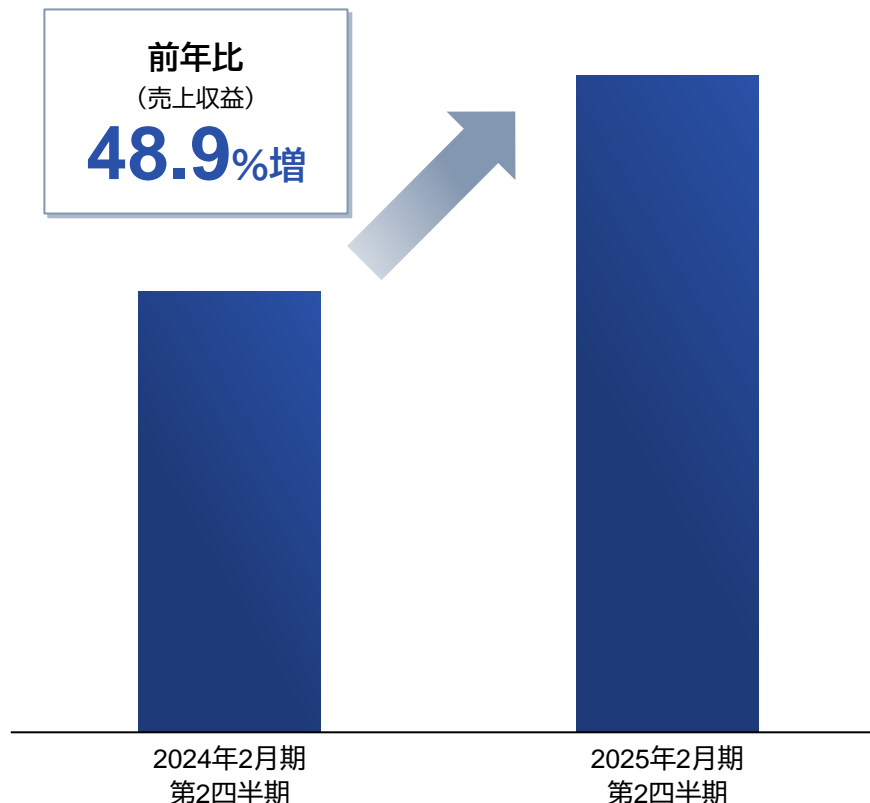
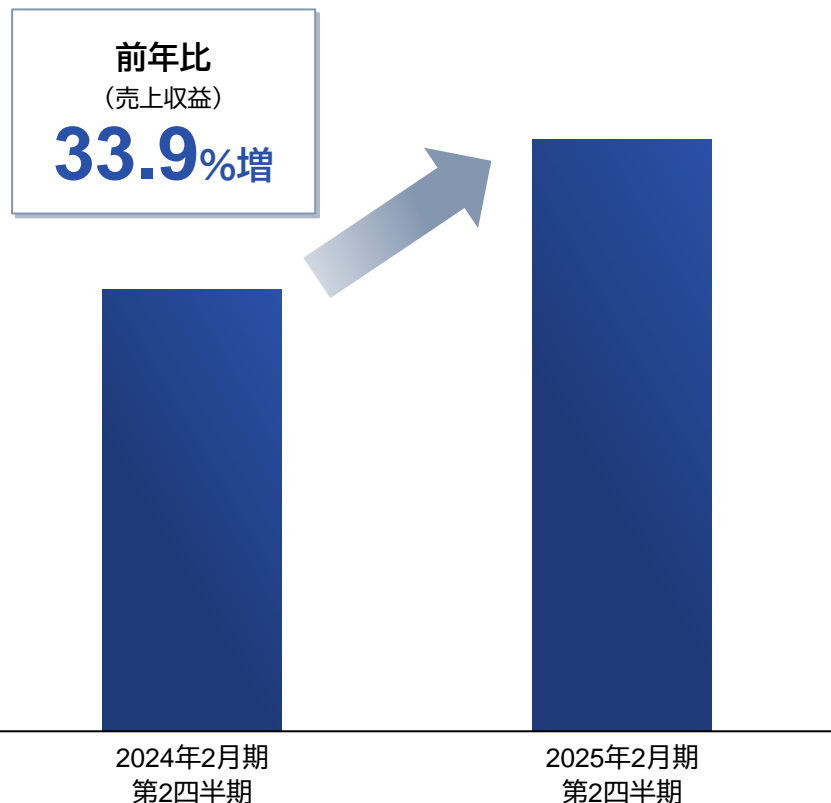
パソコンやサーバー等の情報機器への侵入を検知、拡大を阻止するマルウェア対策を担う、エンドポイントセキュリティ(Vario-EDR)が前年比33.9%増と大幅に伸長。その他ISも大きく伸長しました。

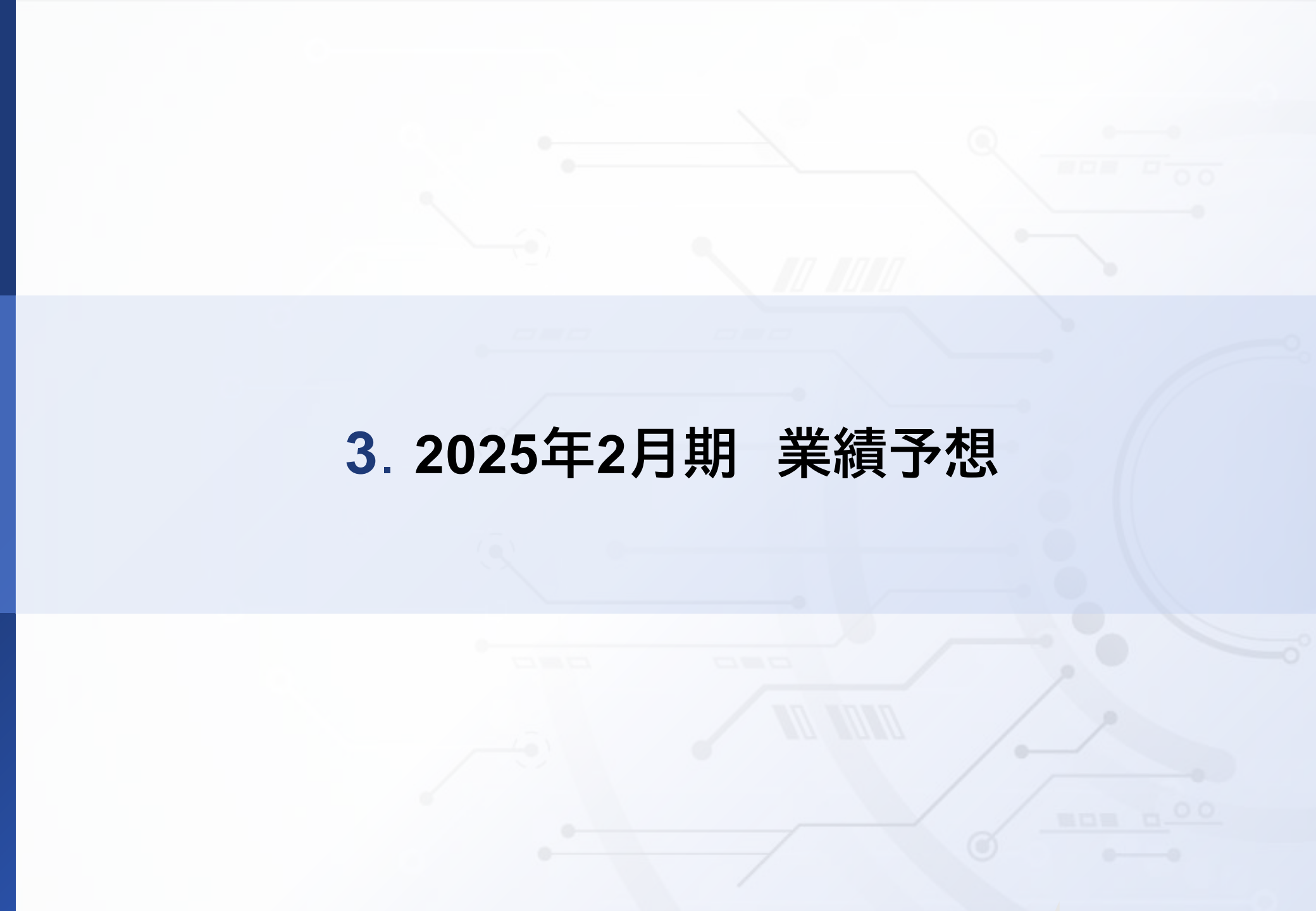
マルウェア検知・防御

## Vario Endpoint Security 売上収益

機器の調達や構築

## ネットワークインテグレーションサービス 売上収益





### **3. 2025年2月期 業績予想**

中期的成長に向けた戦略投資(営業、技術要員の増加や、ゼロトラストへの投資)を踏まえ、営業利益・当期利益は減益を見込むものの、売上高は4.3%の成長を計画。当第2四半期時点では堅調に進捗しています。

(百万円)	2024年2月期 通期実績	2025年2月期 通期計画	2025年2月期 第2四半期実績	進捗率
売上収益	2,640	2,753	<b>1,354</b>	49.2%
営業利益	520	485	<b>273</b>	56.4%
当期利益/四半期利益	347	336	<b>182</b>	54.4%
一株当たり当期/ 四半期利益(円)	76.96	74.47	<b>40.45</b>	—

成長投資の  
ための  
減益計画

The background features a light blue and white color scheme with faint, stylized circuit board traces and geometric shapes. A prominent horizontal blue gradient bar spans the middle of the page. The text '4. トピックス' is centered within this bar.

## 4. トピックス

クラウドからオフィス環境まで中堅・中小企業の規模に合ったセキュリティサービスを提供。セキュリティの担保と運用保守の省力化を図る「Vario Ultimate ZERO」を8月にリリースしました。

## 最低限の構成でゼロトラストセキュリティを実現するマネージドサービス = *Vario Ultimate ZERO*

クラウド型ネットワーク・セキュリティ **新サービス**

### Vario SASE

Vario FWaaS   Vario SWG   Vario IPS

- クラウドからオンプレまで対応可能
- 接続の経路上でセキュリティ確保

+

業務アプリケーションPortal **新サービス**

### Vario IDaaS

Vario IDaaS

- 認証・シングルサインオン
- アクセス(端末)管理
- アカウント管理・サービス登録
- ディレクトリ統合

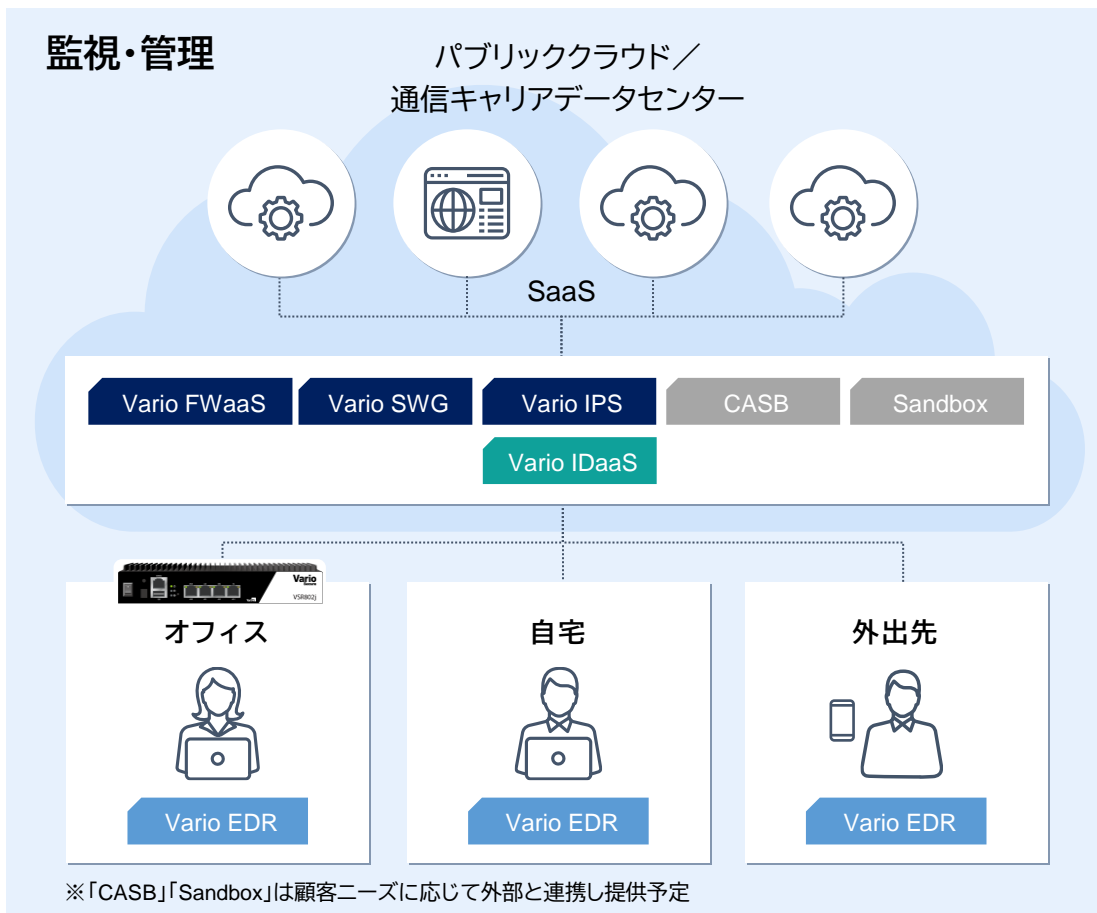
+

最新のサイバー攻撃の検知・防衛 **既存サービス**

### Vario EDR

Vario EDR

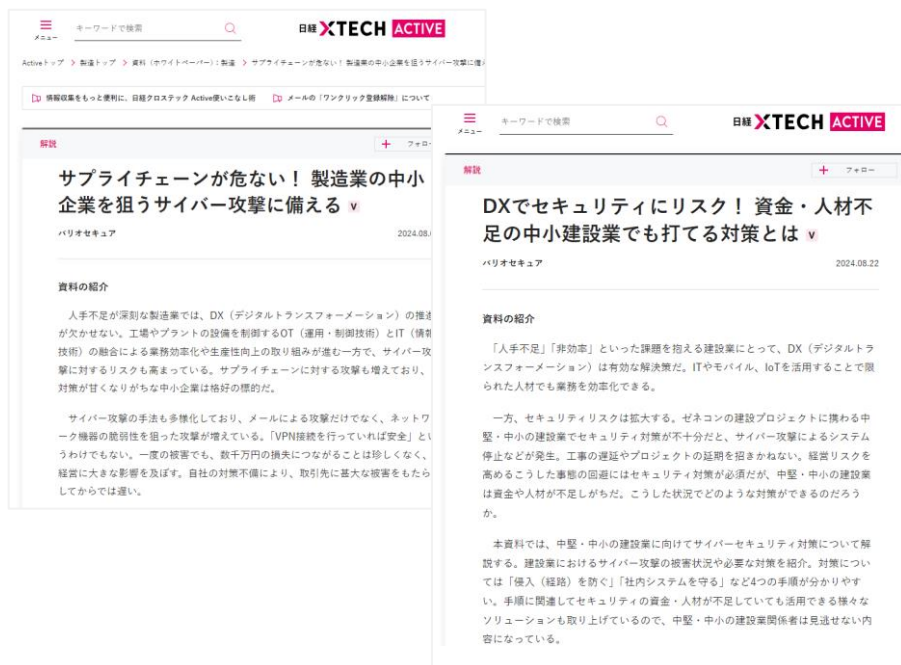
- ランサムウェア対策
- 未知の攻撃への対策
- マルウェア感染された端末の自動隔離



「製造業」「建設業」など、デジタル化(DX)によりサイバーセキュリティ対策の必要性が高まる業種をターゲットとした訴求を開始しました。

## 製造業・建設業向けのリード獲得施策を実施

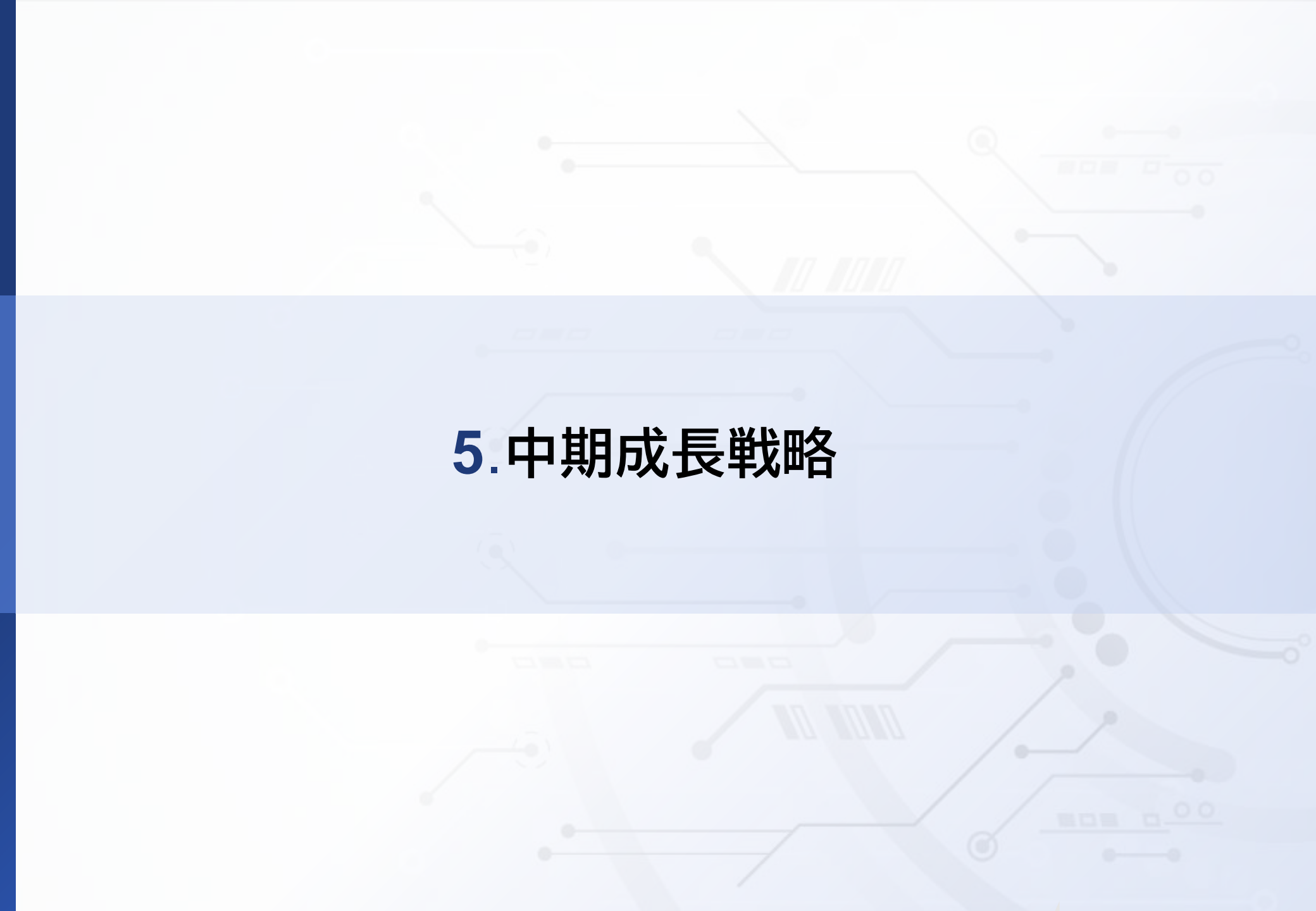
日経クロステックの「製造業」「建設業」のカテゴリにてホワイトペーパーを活用したリード獲得施策を実施



## EDR/EPPの無料トライアルWEB申し込みを開始

「Vario EDR/EPP」を30日間無料でお試しできるトライアルサービスのWEB申し込みを開始



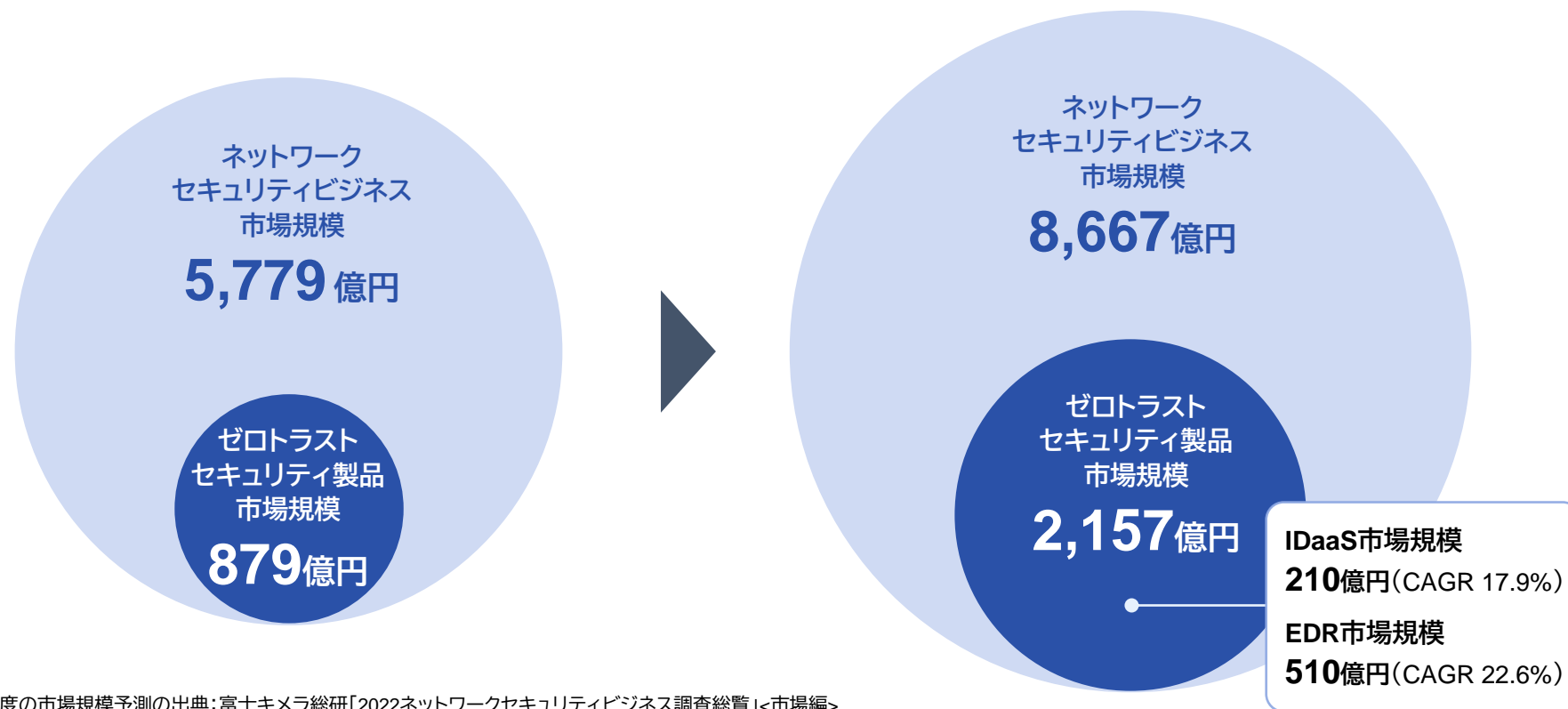
The background features a light gray, stylized circuit board pattern with various lines, nodes, and geometric shapes. A prominent horizontal band of light blue color spans across the middle of the image. The text '5. 中期成長戦略' is centered within this blue band.

## 5. 中期成長戦略

在宅勤務等の社会環境の変化、クラウドサービスの利用拡大、サイバー攻撃の高度化の影響を受け、セキュリティのトレンドが境界防御型(侵入させない)からゼロトラスト(侵入ありき)へと不可逆的に変化しています。

2021年度

2027年度(予測)



※2027年度の市場規模予測の出典: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>  
I.総括編 1.ネットワークセキュリティビジネス市場の展望  
I.総括編 9.市場規模推移 2-9 IDaaS、2-23 EDR



## 外部環境

- 従来の境界防御型の市場成長は年率1.3%※程度の予測
- 「侵入させない」と同時に、「侵入ありき」の多層防御のゼロトラストセキュリティ対策が求められている
- ゼロトラストセキュリティへのニーズは、今後一層高まる見込み

## 内部環境

- 中小企業向けのアプライアンス型UTM製品市場で安定成長してきたが、当社VSRの直近の新規設置台数は横ばい
- 当社の主力サービスは「侵入させない」を目的とした境界防御型
- マルウェア検知・防御(Vario Endpoint Security)、ランサムウェア対応型バックアップ(Vario Data Protect)は、2桁以上の成長実績



## 経営課題解決の方向性

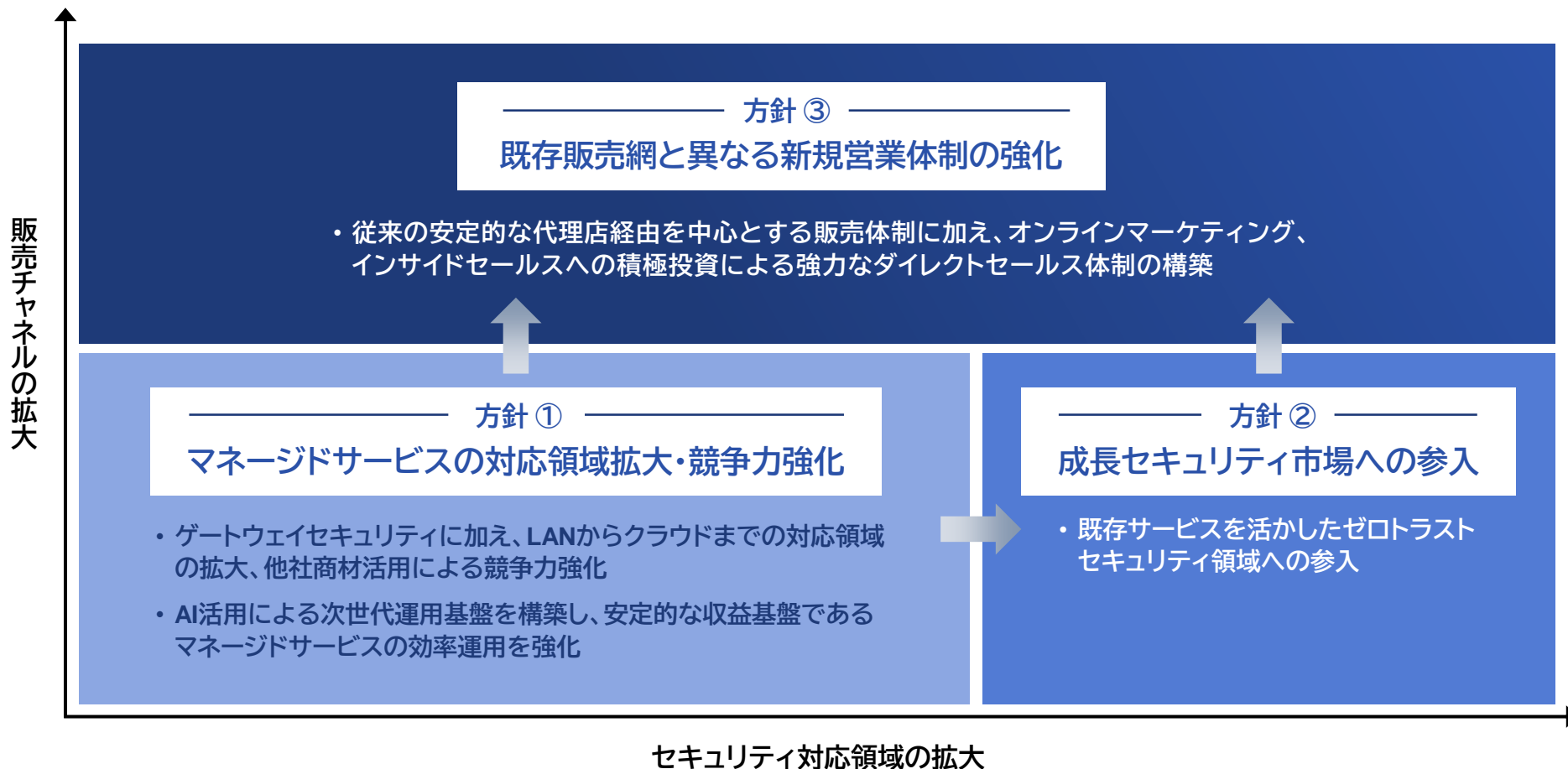
### 強みの深化と成長市場への投資と戦略的な顧客開拓の実行

✓ 強みの深化

✓ 成長市場への投資

✓ 戦略的な顧客開拓

中長期的な事業投資により、「マネージドサービスの対応領域拡大・競争力強化」「成長セキュリティ市場への参入」「既存販売網と異なる新規営業体制の強化」を推進します。



事業投資の一環としてM&Aに注力、そのターゲットを設定。ターゲットの絞り込みと優先順位付けを行い、当社とのシナジーが見込める会社との連携を目指します。

## メインターゲット「セキュリティ関連のIT会社」

### 中期経営方針に沿って当社の不足を埋めるターゲット

#### 中期経営方針

#### ターゲット

方針①  
「マネージドサービスの対応領域拡大・競争力強化」  
に基づき



1 | セキュリティ関連サービスを提供している会社

方針②  
「成長セキュリティ市場への参入」  
に基づき



2 | セキュリティ関連の商品・システムの開発力、特別な技術を持っている会社  
〔セキュリティ機器メーカー、システム開発会社、  
セキュリティ商品の運用サービスもしくは  
エンジニアが多い会社〕

方針③  
「既存販売網と異なる新規営業体制の強化」  
に基づき



3 | 多くの顧客基盤を保持している会社

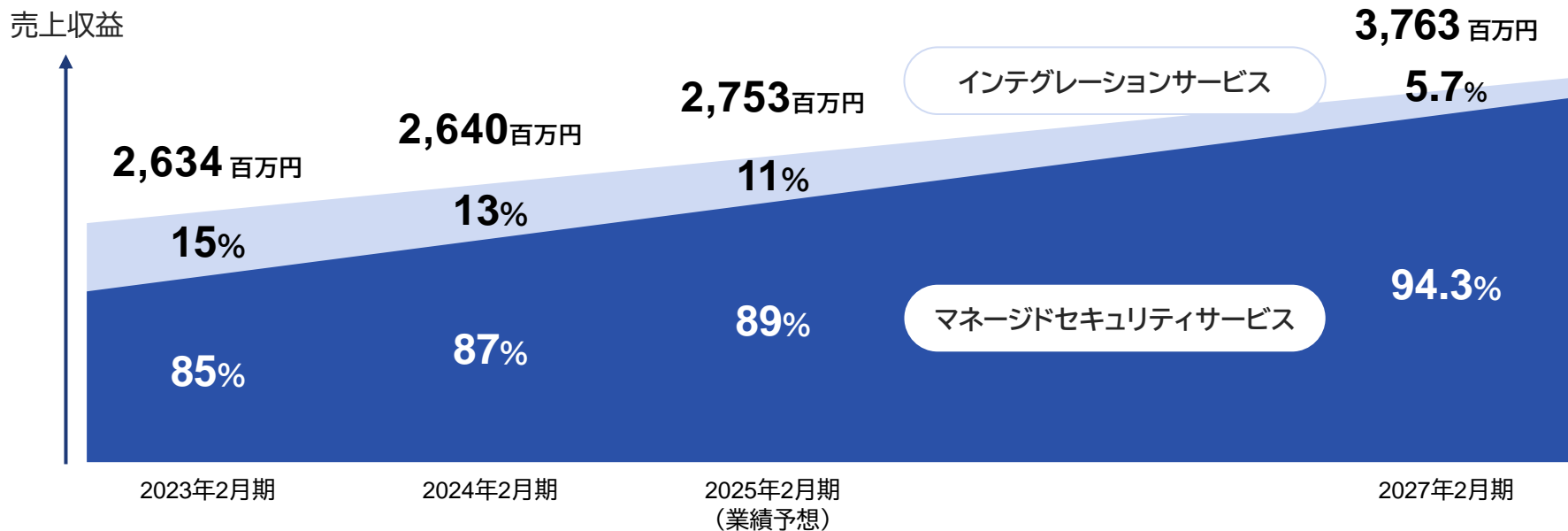
2027年2月期に売上高3,763百万円、営業利益920百万円の実現を中期目標計画として設定しており、今後のゼロトラストセキュリティ商材の投入等により実現を目指します。

2024年2月期実績

売上収益	<b>2,640</b> 百万円
営業利益	<b>520</b> 百万円

2027年2月期目標

売上収益	<b>3,763</b> 百万円
営業利益	<b>920</b> 百万円



IFRS(国際会計基準)

The background features a light blue and white color scheme with faint, stylized circuit board traces and geometric shapes. A prominent horizontal blue gradient bar spans the middle of the page. The text '6. Appendix' is centered within this bar.

## 6. Appendix

## Q1 バリオセキュアの強みを教えてください

当社は、ネットワークセキュリティの導入から管理、運用・保守までをワンストップで提供し、ユーザーから初期費用及び定額の月額費用を徴収するストック型の「リカーリングビジネスモデル」により、安定的な収益基盤を構築しており、独自のビジネスモデルが強みです。

## Q2 マネージドサービスの拡大は、人材も必要となり、売り上げは伸びても利益が伸びないのではないのでしょうか

当社では運用保守サービスにシステムの自動化及びAIを活用することで変動費を固定費化し、コストがリニアに上昇しないようコントロールに努めております。

## Q3 中計をどのように達成していくのでしょうか

既存の統合型インターネットセキュリティの価値提供とお客様の課題を解決するクロスセルによる販売増に加え、新規サービスによる新しい需要の取り込みにより達成していく予定です。

## Q4 PBR1倍割れの対策は行わないのですか

中計を通して目標利益を達成していくとともに、動画配信や個人投資家向けセミナーへの参加等により、IRを積極的に行うことでPERを高めていく予定です。

企業のインターネット接続からテレワークのセキュリティまで様々なニーズに対応しています。

お客様ニーズ		サービス	メリット
①	インターネット接続のセキュリティ/運用をまかせたい	統合型インターネットセキュリティサービス(VSR)	<ul style="list-style-type: none"> <li>専用機器を設置するだけの簡単導入</li> <li>社内担当者の運用負担を大幅軽減</li> <li>手間なく機器を最新状態に維持できる</li> <li>24時間365日の運用監視、サポートに対応可能</li> <li>万が一の障害時の手厚いサポート</li> </ul>
②	社内の端末情報を負担なく把握したい	Vario-NSS	<ul style="list-style-type: none"> <li>専用機器を設置するだけの簡単導入</li> <li>端末へのソフトウェアインストールは不要</li> <li>端末のIPアドレス情報などを自動取得</li> <li>脆弱性管理を大がかりなシステム不要で実現</li> <li>運用負担の少ないシンプル構成</li> </ul>
③	テレワーク端末の脆弱性対策と、社員の業務状況を可視化したい	Vario Telework Manager	<ul style="list-style-type: none"> <li>テレワークの端末情報を把握・管理が可能</li> <li>テレワークのセキュリティレベルを向上</li> <li>脆弱性を可視化し、更新の未適用を把握</li> <li>テレワーク社員の業務状況を、通信量、アプリの稼働状況から確認可能</li> </ul>
④	管理や運用負担なく、社内の重要データをバックアップしたい	Vario Data Protect	<ul style="list-style-type: none"> <li>必要な機器、ソフトウェア、クラウド環境を月額定額でご利用可能</li> <li>ランサムウェア感染リスクを軽減した仕組みによる安全なバックアップ</li> <li>ローカルのバックアップ用機器+クラウド2拠点への冗長対策済み</li> <li>管理・運用負担を軽減したマネージド型サービス</li> </ul>
⑤	標的型攻撃やランサムウェアなどのサイバー攻撃被害を未然に防ぎたい	Vario EDRサービス	<ul style="list-style-type: none"> <li>高度化したウィルス、マルウェア対策として効果的</li> <li>マネージド型サービスにより、リスクの高い攻撃検知後の対応をサポート</li> <li>少ない運用負担で、社内だけでなくテレワーク環境の端末保護にも有効</li> </ul>
⑥	メールの誤送信防止を強化したい	メールセキュリティサービス	<ul style="list-style-type: none"> <li>メールを一定期間保留し、メール送信のキャンセルに対応</li> <li>上長の承認機能など、重要メールの送信ミスを防止</li> <li>様々なルール設定に対応した送信ブロック機能により送信ミスを排除</li> </ul>
⑦	社内のファイル共有を安全かつ便利に実施したい	FileFlex	<ul style="list-style-type: none"> <li>社内のファイルサーバのファイルを、クラウドやVPNを利用することなく簡単、安全にファイル共有可能</li> <li>アクセス権限の設定やアクセス履歴確認など、自由度を損なうことなく安全性を確保</li> </ul>
⑧	自社のネットワーク課題を解決するための環境を構築したい	ネットワークインテグレーションサービス	<ul style="list-style-type: none"> <li>様々な環境構築実績を持つ、ネットワーク、セキュリティを熟知した技術者による対応</li> <li>お客様ニーズに沿った幅広い機器・サービスの選定が可能</li> <li>オンプレミスからクラウドまで幅広い領域をカバー</li> </ul>
⑨	社内のネットワークスイッチ、Wi-Fiアクセスポイントの運用をまかせたい	VarioマネージドLAN / Wi-Fi	<ul style="list-style-type: none"> <li>オフィス内LAN / Wi-Fiの運用・管理を強力サポート</li> <li>ネットワークスイッチやWi-Fiアクセスポイントのお客様管理負担を大幅に軽減</li> <li>24時間365日の機器監視による安心運用</li> </ul>

IPAが「情報セキュリティ10大脅威2024(組織編)」を公表。「ランサムウェアによる被害」が昨年に引き続き首位です。

順位	組織	前年順位
1位	ランサムウェアによる被害	1位
2位	サプライチェーンの弱点を悪用した攻撃	2位
3位	内部不正による情報漏えい	4位
4位	標的型攻撃による機密情報の窃取	3位
5位	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)	6位
6位	不注意による情報漏えい等の被害	9位
7位	脆弱性対策情報の公開に伴う悪用増加	8位
8位	ビジネスメール詐欺による金銭被害	7位
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	5位
10位	犯罪のビジネス化(アンダーグラウンドサービス)	10位

出典:情報セキュリティ10大脅威 2024:IPA 独立行政法人 情報処理推進機構



略語(表記)	内容
VSR	Vario Secure Router 当社マネージドセキュリティサービスで利用している専用機器
Vario-NSS	Vario Network Security Suite 当社マネージドセキュリティサービスで提供している社内ネットワーク向けサービス。デバイス探査/デバイス監視/脆弱性管理を提供している
VDaP	Vario Data Protection 当社マネージドセキュリティサービスで提供しているハイブリッド型バックアップサービス
VSR-Config	VSR-Config 当社マネージドセキュリティサービスで利用している専用機器の自動設定ツール
EDR	Endpoint Detection and Response エンドユーザが利用するパソコンやサーバー(エンドポイント)における不審な挙動を検知し、迅速な対応を支援するサービス
EPP	Endpoint Protection Platform 従来型のアンチウイルスソフトウェアなど、エンドポイントにインストールするセキュリティプラットフォームの総称
UTM	Unified Threat Management ファイアウォール・アンチウイルス・IPS/IDS・Webフィルタリングなど、複数のセキュリティ機能を統合したアプライアンス製品のこと
OEM	Original Equipment Manufacturing(Manufacturer) 他社ブランドの製品を製造すること(あるいはその企業)を指す
SOC	Security Operation Center 24時間365日体制でネットワークやデバイスを監視し、サイバー攻撃の検出や分析、対応策のアドバイスを行う

インターネットを利用する全ての企業が  
安心して快適にビジネスを遂行できるよう、  
日本そして世界へ全力でサービスを提供する

**Vario**  
**Secure**

- 本資料には、当社に関連する予想、見通し、目標、計画等の将来に関する記載が含まれています。これらは、当社が作成時点において入手した情報に基づく、当該時点における予測等を基礎として作成されています。これらの記載は、一定の前提および仮定に基づいており、また、当社の経営陣の判断または主観的な予想を含むものであり、国内外の経済状況の変化、市場環境の変化、社会情勢の変化、他社の動向等の様々なリスクおよび不確実性により、将来において不正確であることが判明しまたは将来において実現しないことがあります。したがって、当社の実際の業績、経営成績、財政状態等については、当社の予想と異なる結果となる可能性があります。
- 本資料における将来情報に関する記載は、作成時点のものであり、当社は、それらの情報を最新のものに随時更新を行う義務を負うものではありません。
- 本資料に記載されている当社以外の企業等に関する情報および第三者作成にかかる情報は、公開情報または第三者が提供する情報等から引用したものであり、そのデータ、指標、分析等の正確性、適切性等について、当社は独自の検証を行っておらず、何らその責任を負いません。