
 Yoshihiko Inami, CEO	Vario Secure Inc. (4494)
	

Company Information

Exchange	TSE Standard
Industry	Information and Communications
CEO	Yoshihiko Inami
Address	Sumitomo Corporation Nishiki-cho Bldg., 5F, 1-6, Kanda-Nishiki-cho, Chiyoda-ku, Tokyo
Year-end	February
Homepage	https://www.variosecure.net/en/

Stock Information

Share Price	Number of shares issued	Total market cap	ROE (Act.)	Trading Unit	
¥875	4,515,613 shares	¥3,951 million	7.9%	100 shares	
DPS (Est.)	Dividend yield (Est.)	EPS (Est.)	PER (Est.)	BPS (Act.)	PBR (Act.)
¥0.00	-	¥68.30	12.8x	¥1,191.32	0.7x

*The share price is the closing price on May 15. Each number are taken from the brief financial report for the FY Ended February 2023.

Earnings Trends

Fiscal Year	Revenue	Operating Profit	Profit before tax	Profit	EPS	DPS
February 2020 Act.	2,513	789	723	498	133.70	0.00
February 2021 Act.	2,545	764	707	491	131.78	39.44
February 2022 Act.	2,566	751	701	500	132.29	40.44
February 2023 Act.	2,634	581	542	383	93.41	40.50
February 2024 Est.	2,685	456	444	308	68.30	0.00

* Unit: million-yen, yen. Estimates calculated by the company. IFRS applied. Non-consolidated accounting. EPS figures are calculated based on the most recent number of shares due to the third-party allotment performed on September 27, 2022.

This Bridge Report presents Vario Secure Inc.'s earnings results for Fiscal Year Ended February 2023 and Growth Strategy etc.

Table of Contents

[Key Points](#)

[1. Company Overview](#)

[2. Fiscal Year Ended February 2023 Earnings Results](#)

[3. Fiscal Year Ending February 2024 Earnings Forecasts](#)

[4. Medium/long-term growth strategy](#)

[5. Conclusions](#)

[<Reference: Regarding Corporate Governance>](#)

Key Points

- The company offers comprehensive network security services through which their customers can safely use the Internet, under the mission: “To ensure that all enterprises using the Internet can easily and securely carry out their business, we will offer the very best services to Japan and to the world.”
- In the term ended February 2023, revenue increased 2.6% year on year to 2,634 million yen. While the Managed Security Services, which is the mainstay, performed well, the sales of the Integration Services business were sluggish. Operating profit decreased 22.7% year on year to 581 million yen. Despite an increase in sales, gross profit decreased 12.9% year on year due to a rise in the cost of sales because of the provision of allowance for the minimum purchase guarantees in procurement contracts and a loss on the valuation of inventories in Integration Services. SG&A expenses decreased 4.1% year on year, but profit fell.
- For the term ending February 2024, revenue is expected to increase 1.9% year on year to 2,685 million yen, while operating profit is projected to decrease 21.4% year on year to 456 million yen. Managed Security Services are forecast to perform well. Integration Services are expected to remain at the same level as in the second half of the previous fiscal year. The company will actively implement business investments such as hiring staff to expand its network and the security operation center (SOC), newly recruiting employees for planning new services and strengthening the sales department, and marketing activities to develop new sales channels. The company will not pay dividends. The basic policy was to aim for stable dividends while securing necessary internal reserves. However, for the four years from the term ending February 2024 to the term ending February 2027, the company will prioritize the allocation of funds to human resource investment, service development, M&A, etc., in order to realize the medium-term business plan for further growth.
- Through its medium/long-term business investment, the company aims to achieve growth by expanding security-related areas and sales channels. In order to accomplish this aim, the company has set "expanding the areas of managed services and strengthening competitiveness," "entering the growing security market," and "strengthening the new sales system that differs from the existing sales network" as its management policies. For the term ending February 2027, the company aims for revenue of 3,763 million yen and an operating profit of 920 million yen.
- Also, the company plans to release new services every quarter this fiscal year. We would like to keep an eye on the progress of initiatives aimed at expanding the service areas along with sales and profit.

1. Company Overview

[1-1 Corporate History]

In June 2001, Ambisys Inc. — the predecessor of the company — was founded with the business objectives to develop and operate information, communication, and security systems and provide consulting services on them. In May 2002, the company launched the managed security services using the integrated Internet security appliance equipment. In June 2003, the company name was changed to

Vario Secure Networks Inc. As an independent Internet security service company, the company steadily expanded its businesses and was listed on the Nippon New Market “Hercules” at the Osaka Securities Exchange in June 2006.

In the ensuing period, the company’s growth slowed down with a higher churn rate from existing customers and the increase in service installation locations stagnating, as a result of the deterioration in corporate profits and the decline in private capital investments triggered by the bankruptcy of Lehman Brothers.

In order to make speedy management decisions and improve corporate value under a dynamic and flexible management system in the constantly changing network security market, the company realized that upfront investments were unavoidable, which might temporarily deteriorate profits. Under such a condition, the company took a decision to delist shares and concentrate on improving corporate value, and in December 2009 duly delisted the shares on Hercules.

After delisting, the company renewed its management structure amid several major shareholder reshuffles, and increased its internal cost awareness, while working to expand its businesses by strengthening the existing sales force and developing new sales agents, as well as continuously conducting R&D to improve the quality of security services. As a result, the company was able to increase corporate value, which was the purpose of delisting, by strengthening its sales structure, creating new businesses, and strengthening the service menu. The company name was changed to its current name, Vario Secure, Inc. in September 2016.

To realise a sustainable growth and corporate value enhancement, the company was convinced of the importance of securing the flexible and diverse financing methods and also that by relisting, the company could further improve social credibility, secure excellent human resources, improve employees’ motivation to work, and aim for appropriate stock price formation and liquidity, the company got listed on the Second Section of the Tokyo Stock Exchange in November 2020. The company got listed on the TSE Standard Market in April 2022.

[1-2 Corporate Philosophy, etc.]

The company’s mission is **“to ensure that all enterprises using the Internet can easily and securely carry out their business, the company will offer the very best services to Japan and to the world.”**

Under this mission, as a company that provides Internet-related security services, it provides comprehensive network security services to assist with the safer use of the Internet by protecting the customers’ networks from attacks from the Internet, intrusions into internal networks, and various threats such as virus infections and data thefts.

[1-3 Market Environment]

(1) Growing demand for cybersecurity

◎ New types of cyber attacks receive increased attention

In January 2023, IPA (Information-technology Promotion Agency, Japan) released the Ten Major Threats to Information Security 2023. The Ten Major Threats to Information Security 2023 were selected by IPA from information security incidents that occurred in 2022 and are considered to have had a significant impact on society. The Ten Major Threats Selection Committee, consisting of approximately 200 members, including researchers in the information security field and practitioners from companies, deliberated and voted on the threat candidates.

In terms of "organizations," "damage caused by ransomware" was the top ranking for the second consecutive year, followed by "attacks exploiting weaknesses in the supply chain," which ranked third last year. On the other hand, "attacks that target before an updated program is released (zero-day attacks)" rose from seventh place in the previous year to sixth place, indicating that cyber attacks are becoming more diverse.

◎ Ministry of Economy, Trade and Industry of Japan calls employers to strengthen cyber security efforts

In December 2020, the Ministry of Economy, Trade and Industry (METI) issued a report urging business owners to strengthen cybersecurity efforts in response to the ever-increasing cyberattack entry points as well as the severities of the attacks.

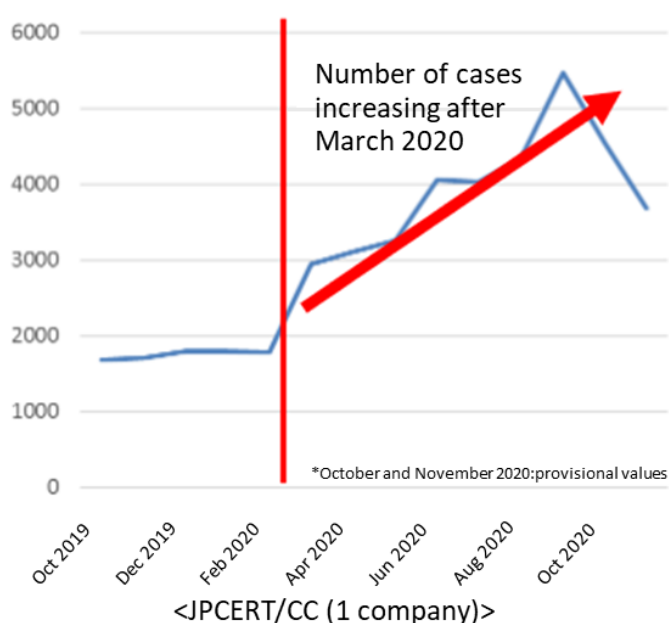
This report identified the following current issues:

- In recent years, the attack entry points in the supply chain used by attackers have been constantly increasing. These include overseas bases of business partners including SMEs and companies expanding overseas, as well as gaps created by the increase in telework due to the spread of the novel coronavirus.

- In addition to demanding ransoms to recover encrypted data, ransomware that uses the so-called “double threats” — threatens to release the data that was stolen in advance before encrypting unless ransom is paid — are rapidly increasing in Japan. This is due to the establishment of an ecosystem which enables attackers to systematically provide ransomware as well as collecting ransoms systematically, allowing them to operate easily without having to be highly skilled.
- With the globalization of businesses, more and more systems that are closely linked with overseas bases are being built; however, as a result of linking the Japanese domestic systems to those of overseas without sufficient measures, the risk of intrusion is increased as this enabled the attackers to construct intrusion routes at overseas bases where security measures are insufficient.

As shown in the graph below, since March 2020 when the novel coronavirus began spreading, the number of consultations concerning those unexpected events that would quickly spiral out of control without immediate counteractions has been increasing.

**Number of incident-related consultations to JPCERT/CC
(per month)**



(From the Ministry of Economy, Trade and Industry’s “Warning to Managers Concerning the Recent Cyberattacks (Summary Edition)”

Based on these, the report urges corporate managers to act on the following responses and initiatives:

- The severity of damage caused by cyberattacks is increasingly more serious and the damages are also more complex: management needs to be involved even more than previously.
- Responding to the damages caused by ransomware attacks is an important issue directly related to corporate trust, and sweeping management leadership is required from proactive prevention to postvention.

Under these conditions, the security service market is seeing an increase in demand.

The security service market requires advanced security measures, but companies that find it difficult to operate and manage in-house security measures tend to outsource operations and monitoring to security vendors, leading to an increase in the service usage.

The market size is expected to expand from 223.7 billion yen in the fiscal 2019 to about 322.2 billion yen in the fiscal 2025, with an average annual growth rate of 6.3% (from the company’s securities report. Source: Fuji Chimera Research Institute, Inc. “2020 Network Security Business Survey Overview (Market Edition)” published on November 17, 2020).

(2) IT personnel shortage

The METI ran a trial calculation of the output gap in IT human resources due primarily to the expansion of IT investment by companies using AI.

According to the report, if the productivity growth rate is 0.7%, the shortage in the number of IT workers in 2030 is estimated at 787,000 in the high-level scenario (3-9% growth in IT demand), 449,000 in the medium level scenario (2-5% of the same), and 164,000 in the low-level scenario (1%). Even if productivity were to rise to 2.4%, the high-level scenario still predicts a shortfall of 438,000 people.

Under these circumstances, it is difficult for companies to secure sufficient IT human resources within their companies, therefore a steady increase is expected for the demand for “managed service” that provide not only the functions but also combine the operation management as one when using IT systems.

* Gap in demand for IT personnel in 2030 (number of workers)

Productivity Growth Rate	Low-level scenario	Medium-level scenario	High-level scenario
In case of 0.7%	164,000	449,000	787,000
In case of 2.4%	-72,000	161,000	438,000

*Created by Investment Bridge based on the Ministry of Economy, Trade and Industry’s “Survey on Supply and Demand of IT Human Resource (Summary)” (April 2019).

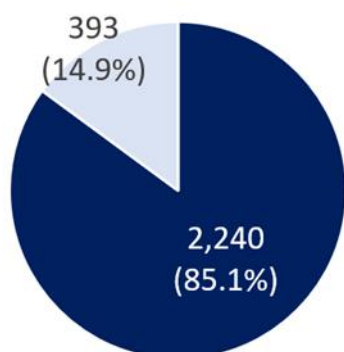
[1-4 Business Contents]

(1) Service category

The company provides two security services: Managed Security Services and Integration Services (segment: single segment of Internet security service business).

These services cover every step in the security framework: construction, identification, defense, detection, response, and recovery.

Service components (FY Feb. 2023 unit: million yen)



■ Managed Security Services ■ Integration Services

① Managed Security Services

In addition to the integrated Internet security service using VSR and the data backup service (VDaP), since the term ended February 2021, the company has been offering Vario EDR service that helps detect and respond to cyberattacks at lower operational costs, and Vario-NSS, which detects abnormal terminals and provides vulnerability management.

<Integrated Internet Security Service Using VSR>

Overview

This service provides comprehensive network security that protects corporate networks from the attacks from the Internet, intrusions into internal networks, and threats such as virus infections and data thefts, and enables customers to use the Internet safely.

The company’s integrated Internet security service uses VSR (Vario Secure Router) — a network security device developed by the company which integrates various security functions such as firewalls, IDS (intrusion detection system), and ADS (automatic defense system) into one unit — which is installed between the Internet and customers’ internal networks, and acts as a filter to remove threats such as attacks, intrusions, and viruses.

VSR is automatically managed and monitored by a proprietary operational monitoring system run by the company’s data center, and operational information statistics and various alerts are processed in real time without human interventions.

Statistics and alerts are provided in real time to user company administrators over the Internet via a reporting function called, the Control Panel. In addition, the company has established a 24/7 support center, and a maintenance network covering all 47 prefectures in Japan and an operation support system such as changing the equipment settings.

Since they are manufactured at several factories in Taiwan while the core software is developed in-house, it is more cost-effective than purchasing hardware and adding services, and this is one of the reasons contributing to VSR’s high operating income margin.



(Source: the company’s website)

Merits

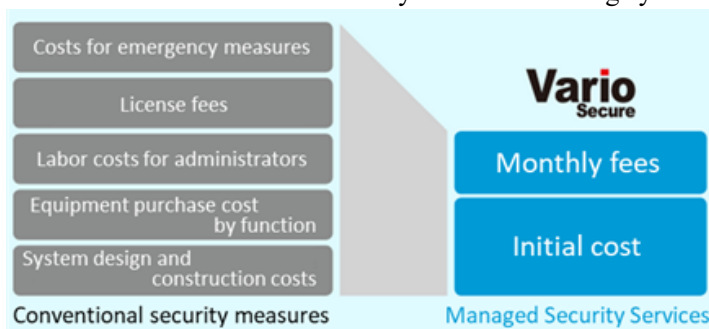
Previously, to introduce the security system such as above, it was necessary to install various security devices in-house and maintain them, making it more difficult for many companies to introduce sufficient network security measures because they required highly skilled engineers and high investments.

In addition, even after the introduction of the security system, monitoring, quick response to alerts, software updates, inquiries in the event of trouble, etc. required a great deal of effort and time, and the operational burden was extremely large.

In contrast, the company’s Managed Security Services, which provides the one-stop solution from initial introduction to operation and maintenance of VSR, a unique in-house product, provides significant benefits to customers in the following respects:

As VSR boasts 23 different security features per unit, it eliminates the need to purchase equipment and instead provides the security system via the rental equipment.
A monthly fee is set for each security feature, allowing customers to choose the options they need from a variety of security features.
By simply paying the initial cost incurred only at the start of the contract and monthly fees, it is possible to outsource most of the man-hours required for the operation of network security, such as using the control panel, changing settings, updating software, and local maintenance through monitoring and business trip support, reducing the burden of work.
In addition to inquiries from customers (end-users) to the company or distributors, the company actively detects and supports problems through remote monitoring. Operation and maintenance are remotely handled as much as possible by the company’s engineers, making it possible to respond more quickly compared to general on-site responses via call centers.
To deal with hardware failures, the company deploys inventory at warehouses of subcontractors throughout the country, and aims to replace the equipment within the target timeframe of four hours.

The ease of introduction and the clarity of the menu are highly evaluated by mid-tier enterprises and MSEs.



(Source: materials provided by the company)

(Number of VSR units installed)

Most of their customers are mid-sized and small businesses who would struggle to employ IT managers with expertise on their own. As of February 28, 2023, the number of VSR managed units was 7,450. They were installed in 47 prefectures throughout the country. It has a high market share amongst the mid-tier enterprises and SMEs.

<Data Backup Service (VDaP)>

The company provides a backup service that combines VDaP, where backup data are stored on a device, and the storage in a data center. After temporarily backing up corporate digital data to VDaP, data are automatically transferred to the data center to further increase the fault resistance.

In addition, since the latest and past data are kept as version-managed backup data, it is easy to select and recover the necessary digital data by providing an interface for the customers that are easy to use when recovering data.

Utilizing its experiences in monitoring and operating services for integrated Internet security service using VSR, the company also provides the service that efficiently covers the whole country by utilizing the system for installing equipment and responding to failures.

<Vario EDR Service>

Vario EDR Service visualizes cyberattacks that try to penetrate through antivirus measures and avoid security incidents before they happen. It adopts highly accurate detection methods using AI and machine learning, and against the high-risk incidents, it would conduct automatic isolation of terminals and initiate investigations by security specialists.

<Vario-NSS>

As the shortage of IT personnel in companies becomes more serious, the company will support the efficient operation of internal systems and promote the concept of "Information System as a Service." Vario-NSS automatically scans terminals connected to the corporate network by simply installing a dedicated terminal in the network for asset management, visualizes terminal information, and understands vulnerability response. This enables it to respond to terminals with security risks early and monitor unauthorized terminals, reducing the burden and risk on the IT asset management which tends to rely on personal operations. Through continuous updates, it can not only manage Windows terminals, but also centrally manage Red Hat Linux terminals which are widely used for internal servers, etc. reducing the burden on personnel in the information systems departments at customer companies.

② Integration Services

This consists of sales of Vario Communicate Router (VCR), an integrated security device (UTM) for small and medium-sized enterprises, and Network Integration Services (IS) for procurement and construction of network equipment.

<Sales of integrated security equipment VCR for small and medium-sized enterprises>

The company sells VCR, a security appliance device, in response to the growing security awareness among smaller businesses and clinics with fewer than 50 employees, due to regulatory changes such as revisions of the Basic Act on Cybersecurity among others.

Unlike Managed Security Services, UTM products are imported as their own brands from overseas manufacturers and sold to end-users through distributors specializing in small and medium-sized enterprises.

Throughout the warranty period, the manufacturers provide support on sold equipment and hardware failures, through the company's and/or distributors' support desk.

<Network Integration Services (IS)>

Their engineers cover the whole areas of designing, procuring, and building the network according to the needs of end-users, and are working to expand the business into the wider corporate network areas.

As with the VCR sales, the manufacturers provide support on sold equipment and hardware failures, through the company's and/or distributors' support desk.

(2) Revenue model

Managed Security Services provide one-stop service from the introduction of network security to management, operation, and maintenance, and is a stacked recurring business model that collects initial costs and fixed monthly costs from users.

There is a one-time charge for the Integration Services, associated with the sale of VCRs and the procurement and construction of network equipment.

(3) Sales channels

Sales are mainly indirect sales through distributors.

The company has signed contracts with distributors such as telecommunications carriers, Internet service providers, data center operators, etc., who are looking to provide added value to customers by attaching Vario Secure services, and has built a sales network covering the whole country. The company has established a system that can continuously create opportunities.

The company's distributors are divided into the original equipment manufacturers (OEM partners) and the reselling partners. An OEM partner is a partner that provides security services under the distributor's own brand and enters contracts directly with the customers (end users). As of the end of August 2022, the company has signed agreements with 31 companies for all managed services. A reselling partner is a partner that develops customers (end users) and engages in sales activities as an agent of Vario Secure, through which Vario Secure remains as the contracting entity with customers. As of the end of February 2023, the company has signed agreements with 71 companies for all managed services.

In addition to the above, to promote sales activities, Vario Secure as a security expert provides sales representatives who directly explain technical aspects to customers on behalf of distributors, and provides one-stop support from introduction to installation of services.

(4) Total number of end users of Managed Security Services

The total number of end-user companies of the overall Managed Security Services was 2,981 as of February 28, 2023.

[1-5 Characteristics and Strengths]

(1) Unique business model

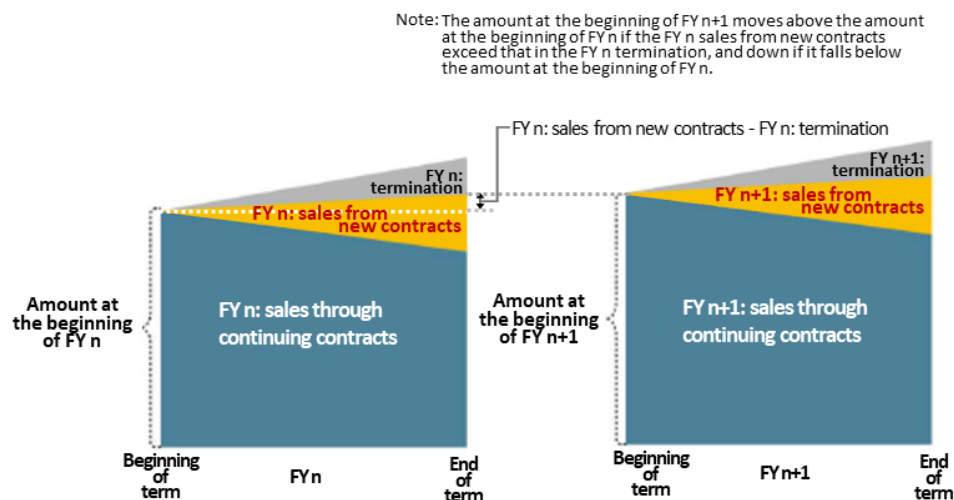
The company provides one-stop service for (1) procurement of equipment used in security services, (2) development of core software to be installed on equipment, (3) installation/setting of equipment, and (4) monitoring and operation after installation of equipment. There is no need for end-users to individually consider equipment selection and operation services, and they can quickly start using the service. In addition, since the service is provided as one-stop, the company can easily investigate the cause of a problem and respond. Support is available 24/7, allowing end-users to quickly receive support for inquiries and troubles. The company aims to reach customers within four hours if it deems that equipment needs replacing, and in the term ended February 2021, it almost achieved the target at 99%.

(2) Stable revenue model

As mentioned above, Managed Security Services are recurring business in which profits accumulate year by year due to the increase in the number of companies introduced by monthly billing, and as of the end of February 2022, Managed Security Services were provided at approximately 7,300 locations (number of VSR-installed locations) in all 47 prefectures nationwide.

In the term ended February 2023, Managed Security Services accounted for 85.0% of the company's total revenue. With a low churn rate of 0.49% (in 4th quarter of the term ended February 2023), a stable earnings model has been built, and it is possible to forecast revenues at a relatively early stage in the fiscal year.

[Recurring Revenue Model]



(Source: material provided by the company)

(3) Strong sales channels

As mentioned above, it has built strong sales channels with 31 OEM partners and 71 reselling partners, covering the whole country. It is an important asset for efficient sales for the company, which mainly targets small and medium-sized enterprises. In addition, since there are many OEM partners in the telecommunication industry and the company’s services are incorporated as an option in the menu of the operating company, it is easy for users to select and introduce when the Internet connections are newly installed or altered, leading to a high order rate.

(4) High market share

The company is the market leader in all following categories by employee number: 300 to 999, 100 to 299, and 0-99 in the Firewall/UTM* operational monitoring service market.

* Firewall/UTM operational monitoring service market: Sales Amount and Market Share by Employee Size (FY2021)

	0 – 99 employees	100 – 299 employees	300 – 999 employees
No. 1	Vario Secure 32.7%	Vario Secure 24.1%	Vario Secure 20.9%
No. 2	Company A 15.9%	Company A 14.6%	Company A 8.4%
No. 3	Company B 7.1%	Company B 8.8%	Company B 8.4%

* Created by Investment Bridge based on the company’s financial results briefing materials (source: ITR “ITR Market View: Gateway Security-Based SOC Service Market 2022”)

* UTM: Unified Threat Management. A network security measure operated by combining multiple security functions into one.

2. Fiscal Year Ended February 2023 Earnings Results

(1) Overview of business results

	FY 2/22	Ratio to sales	FY 2/23	Ratio to sales	YoY	Ratio to forecast
Revenue	2,566	100.0%	2,634	100.0%	+2.6%	-0.6%
Gross profit	1,597	62.2%	1,390	52.8%	-12.9%	-13.7%
SG&A and others	845	32.9%	810	30.8%	-4.1%	-
Operating profit	751	29.3%	581	22.1%	-22.7%	-25.9%
Profit before tax	701	27.3%	542	20.6%	-22.7%	-28.3%
Profit	500	19.5%	383	14.6%	-23.4%	-27.0%

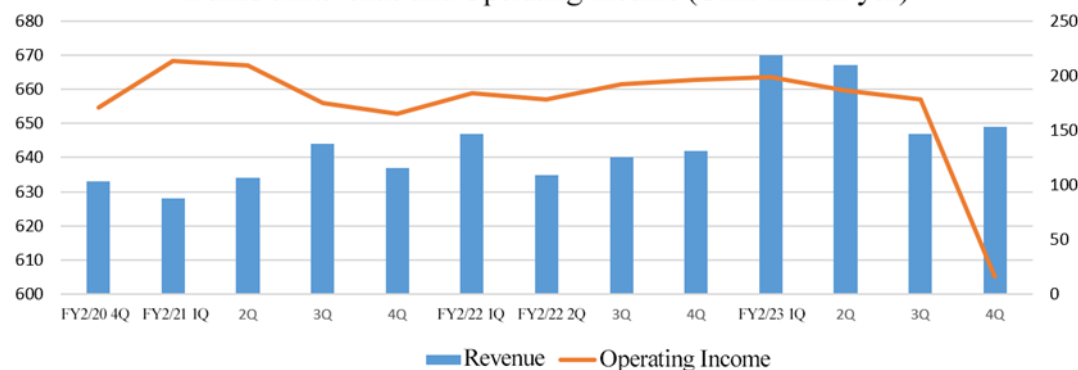
*Unit: million yen

Revenue increased and profit decreased

Revenue increased 2.6% YoY to 2,634 million yen. While the mainstay managed security services remained strong, the integration services business was sluggish.

Operating income declined 22.7% YoY to 581 million yen. Despite higher sales, gross profit declined 12.9% YoY due to an increase in cost of sales resulting from a provision for minimum purchase guarantees for procurement contracts and loss on valuation of inventories in the integration services business. SG&A expenses also declined 4.1% YoY, but profits declined.

Trends of Revenue and Operating Income (Unit: million yen)

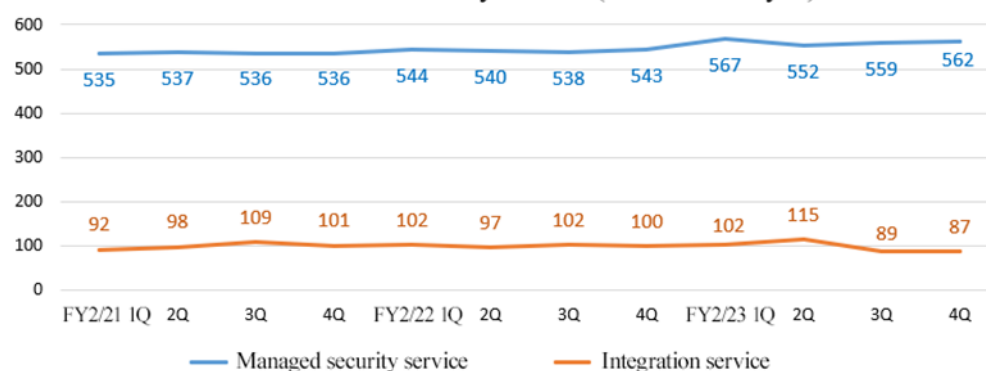


(2) Service trends

	FY 2/22	FY 2/23	YoY
Revenue			
Managed security service	2,165	2,240	+3.5%
Integration service	401	393	-1.9%

*Unit: million yen

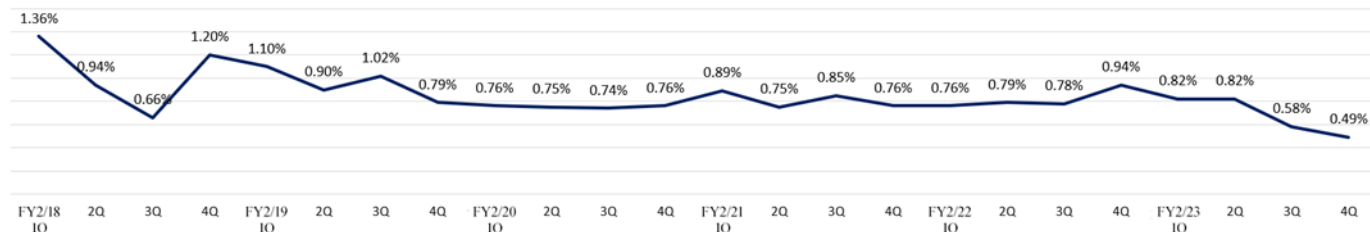
Transition of revenue by service (Unit: million yen)



①Managed security service

The sales of "Vario Endpoint Security" were strong. The churn rate remained low.

Churn Rate Trend



*Churn Rate (Monetary Base) = Quarterly cancellation amount / (initial monthly sales revenue in each fiscal year × 3 months)

②Integration service

The sales of integrated security equipment (UTM) were sluggish in the second half due to an unexpected escalation of the competitive environment, including changes in the distributors' initiatives. Although a new model with new services was additionally released, sales did not recover. Thus, a provision of 94 million yen for the minimum purchase guarantees in the procurement contracts and a loss on valuation of inventories of 64 million yen were recorded.

(3)Business Topics

- * In the VSR n series, the company has expanded the scope of the local breakout function to web conferencing applications, etc., in response to the spread of telework, and has enhanced functions such as HTTPS support for URL Filtering. As of March 1, 2023, 4 distributors and 37 companies have adopted it, and 53 units have been deployed. The company expects full-scale expansion from this term. In order to create more added value, the company will continue to actively utilize AI technology and strengthen functions in line with recent cyber-attack trends and customer security issues.
- * Against the backdrop of the spread of new cyber-attacks, orders for "Vario Endpoint Security," which is effective against malware, and "Vario Data Protect," which is a backup against ransomware, are increasing. The revenue from Vario Endpoint Security and Vario Data Protect is significantly growing. The revenue from Vario Endpoint Security increased 376.4% year on year, and the revenue from Vario Data Protect grew 10.3% year on year.
- * The company has finished 70% of the deliveries of the automation of VSR settings. In the past, when setting up VSR in response to customer needs, a sheet with input items was created, and input was made while looking at the sheet. However, as the number of orders increased, problems such as a shortage of staff and input errors occurred. Advances in automation have reduced these issues.
- * For HEROZ and Network Security Operations Center (SOC) operations, AI-based processing capabilities are being developed and PoC is currently underway. The company aims to apply it onsite during this fiscal year.
- * Approached specific industries (healthcare industry) to promote agency agreements, customer contracts, and pipeline discovery. Utilized webinars and inside sales to develop EDR and VDaP customers.

BRIDGE REPORT

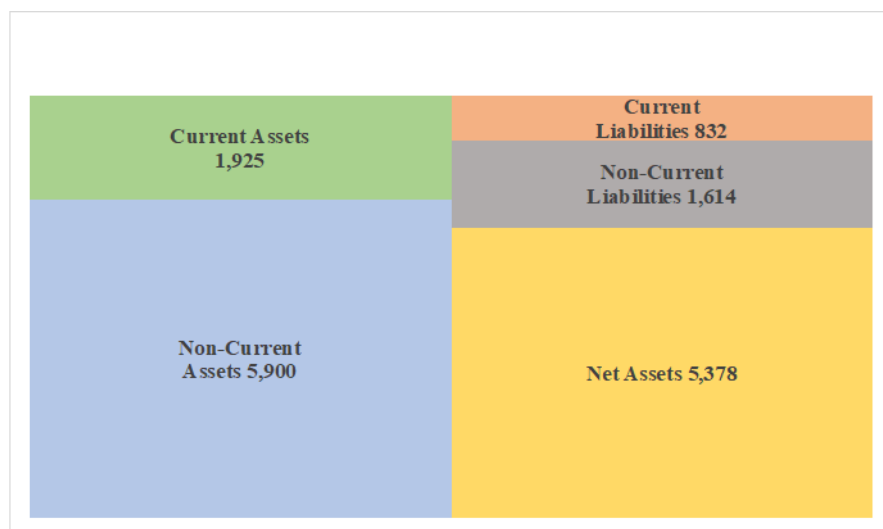


(4) Financial position and cash flows

© Main Balance Sheet

	End of February 2022	End of February 2023	Increase/ decrease		End of February 2022	End of February 2023	Increase/ decrease
Current Assets	1,249	1,925,	+676	Current Liabilities	2,403	832	-1,571
Cash and Cash Equivalents	389	1,039	+650	ST Interest Bearing Liabilities	1,786	200	-1,586
Trade and Other Receivables	464	443	-20	Trade and Other Payables	134	81	-52
Non-current Assets	5,872	5,900	+27	Non-current Liabilities	395	1,614	+1,219
Tangible Assets	206	158	-47	LT Interest Bearing Liabilities	-	1,300	+1,300
Goodwill	5,054	5,054	0	Total Liabilities	2,799	2,447	-351
Intangible Assets	242	296	+53	Net Assets	4,323	5,378	+1,055
Total Assets	7,122	7,826	+704	Retained Earnings	2,351	2,581	+229
				Total Liabilities and Net Assets	7,122	7,826	+704
				Total Borrowings	1,786	1,500	-286

*Unit: million yen.



* Prepared by Investment Bridge Co., Ltd. based on the disclosed material.

Balance of interest-bearing liabilities decreased by 286 million yen from the end of the previous term. Net D/E ratio decreased 23.7% from the end of the previous term to 8.6%. Equity ratio increased by 8.6 points to 68.7% due to decrease in liabilities and increase in retained earnings.

Repayment of interest-bearing liabilities and financial soundness improvement are progressing as planned.

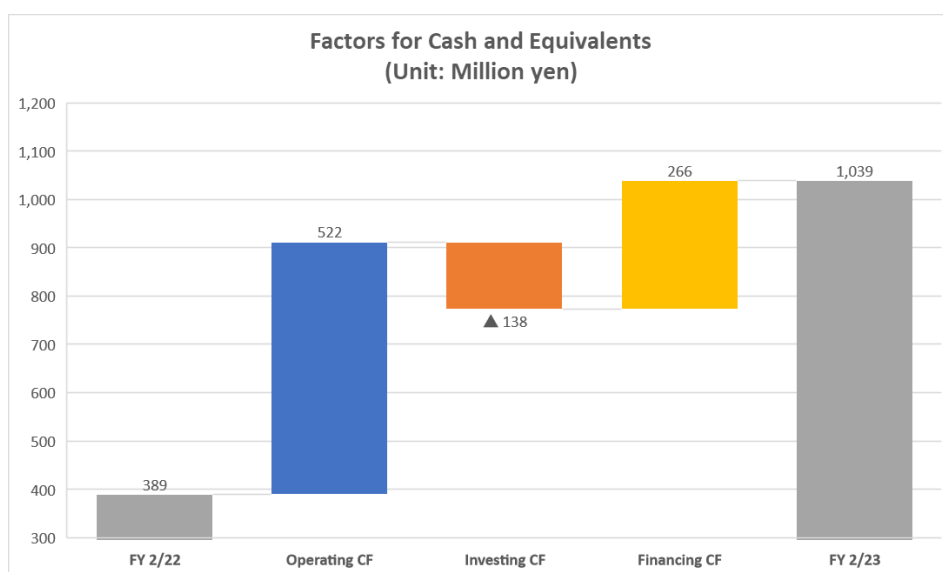
BRIDGE REPORT



◎ Cash Flows

	FY 2/22	FY 2/23	Increase/decrease
Operating Cash Flow	490	522	+32
Investing Cash Flow	-108	-138	-30
Free Cash Flow	381	383	+1
Financing Cash Flow	-586	266	+852
Balance of Cash and Equivalents	389	1,039	+650

*Unit: million yen



* Prepared by Investment Bridge Co., Ltd. based on the disclosed material.

The cash inflow from operating activities and free CF increased. Financing CF recorded a surplus due to income from issuing shares, etc.

The cash position improved.

3. Fiscal Year Ending February 2024 Earnings Forecasts

(1) Earnings forecasts

	FY 2/23	Ratio to sales	FY 2/24 Est.	Ratio to sales	YoY
Revenue	2,634	100.0%	2,685	100.0%	+1.9%
Gross profit	1,390	52.8%	1,458	54.3%	+4.8%
SG&A	810	30.8%	1,001	37.3%	+23.4%
Operating profit	581	22.1%	456	17.0%	-21.4%
Profit before tax	542	20.6%	444	16.5%	-18.0%
Profit	383	14.6%	308	11.5%	-19.5%

*Unit: million yen

Increase in revenue and decrease in profit estimated.

Revenue is expected to increase 1.9% YoY to 2,685 million yen, and operating profit is expected to decrease 21.4% YoY to 456 million yen.

Managed security services are expected to remain firm. Integration services are expected to remain at the same level as in the second

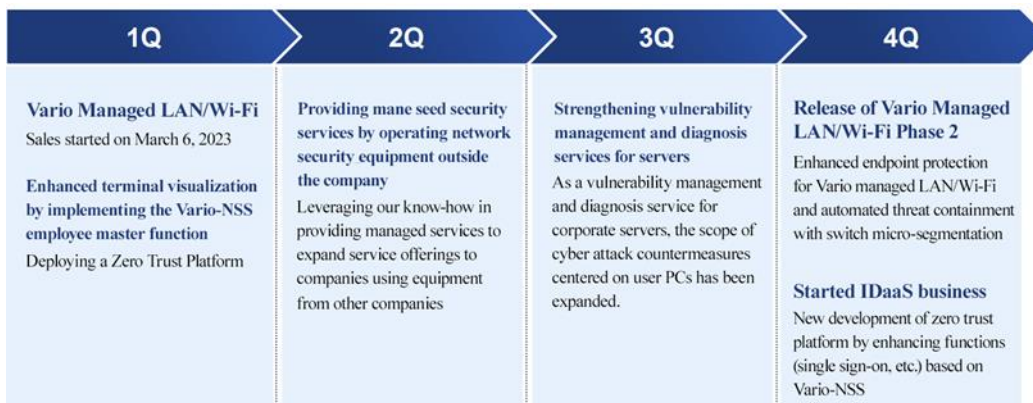
half of the previous fiscal year.

The company will aggressively invest in business, including hiring staff to expand the Network Security Operation Center (SOC), hiring new staff to strengthen the new service planning and sales divisions, and marketing to develop new sales channels.

No dividend will be paid. The company's basic policy has been to aim for stable dividends while securing necessary internal reserves, but for the four fiscal years from FY02/2024 to FY02/2027, priority will be given to allocating funds to human resource investment, service development, M&A, etc., in order to realize the medium-term business plan for further growth.

(2) New service release roadmap

This term, the company plans to release services centered on strengthening cyber-attack countermeasures and platform development for full-scale provision of zero trust security.



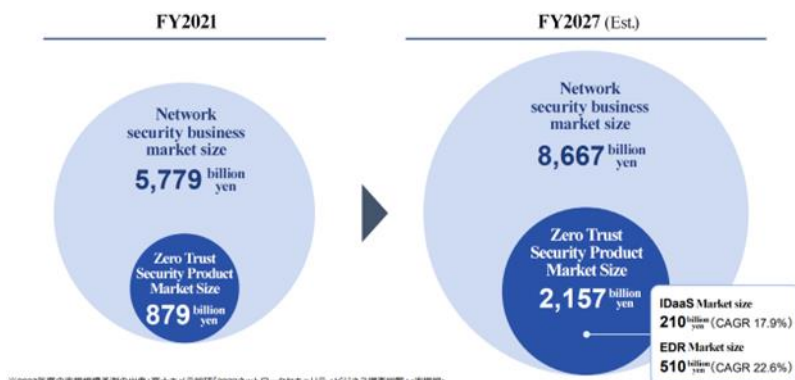
(Taken from the reference material of the company)

4. Medium/long-term growth strategy

(1) Network security business market trends

Security trends have irreversibly changed from perimeter defense (no intrusion) to zero trust (intrusion occurs) due to changes in the social environment, such as telecommuting, expanded use of cloud services, and the sophistication of cyberattacks.

In particular, the growth rate of the zero trust security* market is expected to exceed the growth rate of the entire network security business market, and the EDR and IDaaS markets, which are specific solutions for zero trust security, are expected to grow even higher.



(Taken from the reference material of the company)

***Zero-Trust Security**

Conventional security measures, it is assumed that the data and systems to be protected are in the internal network, however, with the spread of cloud computing, more and more data and systems that should be protected exist on the Internet, which is on the external network. As such, the boundaries have become vague, subjects to be protected exist both inside and outside the system, thus, it is becoming increasingly difficult to take sufficient countermeasures with the conventional approach. The “Zero-Trust Security” is a security measure based on the assumption that all communications should not be trusted (Zero-Trust) when considering the security.

(2) The company's management issues and solutions

The company acknowledges the external and internal environment and management issues in this market environment as follows.

External environment	Internal environment
<ul style="list-style-type: none"> ■ The conventional perimeter defense market is expected to grow at an annual rate of around 1.3% ■ There is a need for multi-layered zero-trust security measures that "do not allow intrusion" and "allow intrusion" ■ Demand for zero trust security is expected to grow further in the future 	<ul style="list-style-type: none"> ■ The appliance-type UTM product market for small and medium-sized enterprises has grown steadily, but the number of new installations of our VSR has remained flat recently. ■ Our main service is a perimeter defense type for the purpose of "not allowing newcomers" ■ Malware detection and prevention (Vario Endpoint Security) and ransomware-resistant backup (Vario Data Protect) show double digit growth

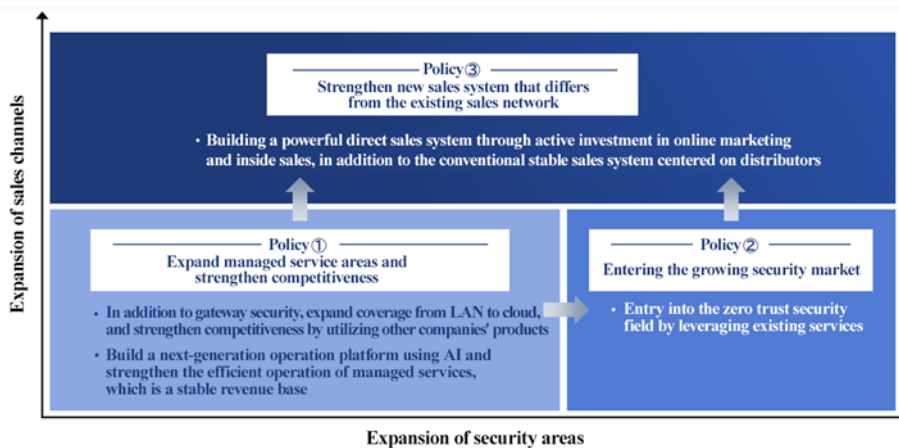
(Taken from the reference material of the company)

In order to solve these management issues, expand the zero-trust security market, and achieve sales and profit growth, the company believes it has to enhance its strengths, invest in growing markets, and strategically develop new customers.

(3) Medium-term management policy

In order to achieve growth by expanding security areas and sales channels through medium/long-term business investment, the company will promote the following three management policies.

- Policy 1 Expanding managed service areas and strengthening competitiveness
- Policy 2 Entering the growing security market
- Policy 3 Strengthening the new sales system that differs from the existing sales network

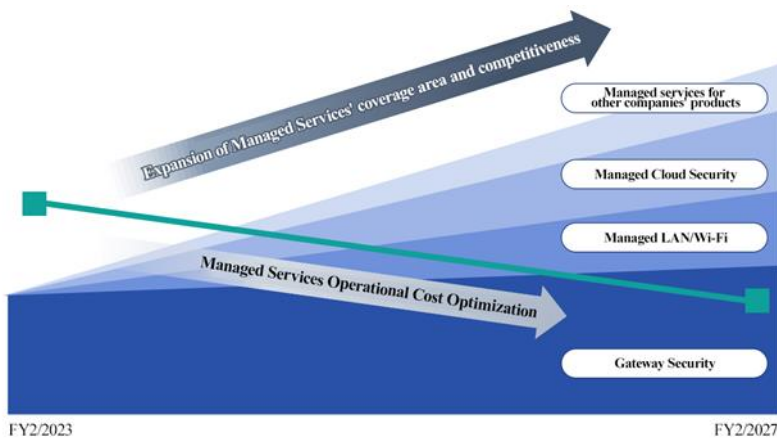


(Taken from the reference material of the company)

*** Policy 1: Expanding managed service areas and strengthening competitiveness**

In addition to gateway security, the company will expand the scope of managed services from LAN to cloud services and strengthen competitiveness by utilizing other companies' products.

Moreover, the company will build a next-generation operation platform using AI through an alliance with HEROZ and strengthen the efficient operation of managed services, which is a stable revenue base.



(Taken from the reference material of the company)

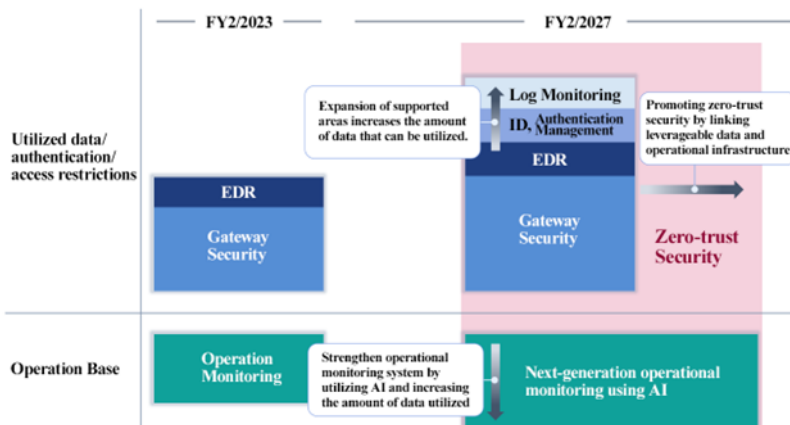
*** Policy 2: Entering the growing security market**

Utilizing existing services, the company will enter the zero-trust security field.

The company will increase the amount of data that can be used by expanding the areas of support, such as log monitoring and ID/authentication management.

In addition, the company will strengthen the operation monitoring system by utilizing AI and increasing the amount of data used.

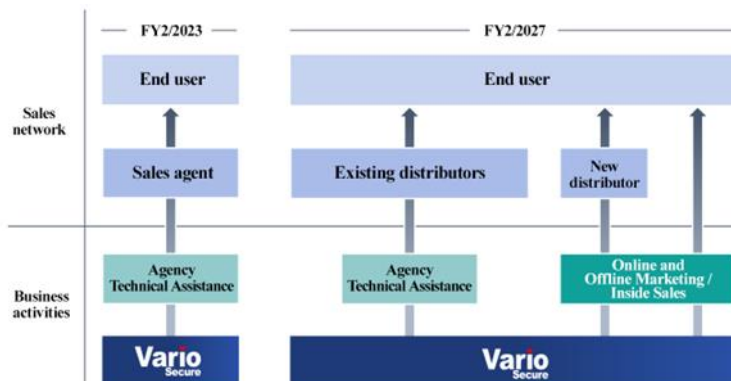
It will promote zero-trust security by increasing usable data and linking the operational infrastructure.



(Taken from the reference material of the company)

*** Policy 3: Strengthening the new sales system that differs from the existing sales network**

In addition to the conventional stable sales system centered on distributors, the company will build a solid direct sales system by actively investing in online marketing and inside sales. The inside sales team will work on developing new distributors.



(Taken from the reference material of the company)

BRIDGE REPORT

**(4) Medium-term investment plan**

Over the three years from the current term ending February 2024 to the term ending February 2026, the company will invest in marketing for acquiring new sales channels and in personnel and development for strengthening sales capabilities. The company also plans to invest 400 million yen in M&A for a total of 900 million yen in growth investment.

It assumes M&A with companies with expertise in vulnerability diagnosis and companies with strong sales capabilities targeting small and medium-sized enterprises.

FY2/2024 - FY2/2026

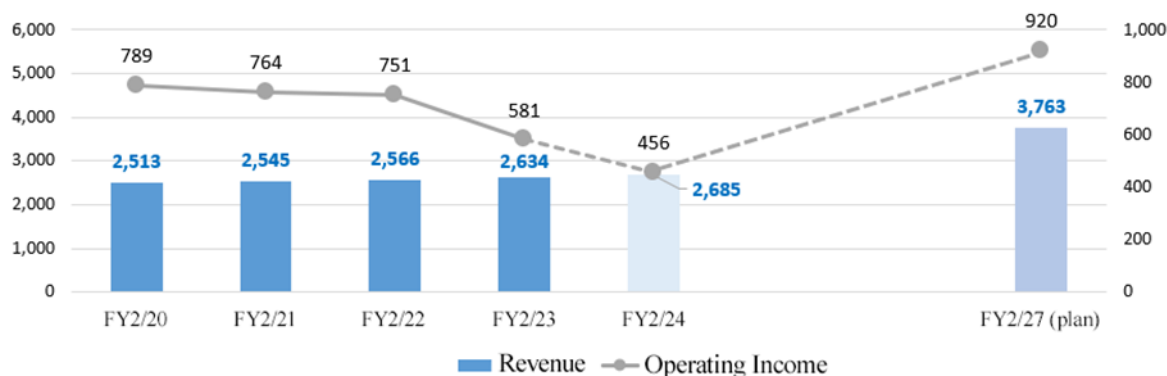
Personnel expenses New service planning and sales department reinforcement	258 million yen
Development costs / SOC operational enhancement costs Software development, etc.	155 million yen
Marketing costs Increased awareness, lead acquisition	100 million yen
M&A Maintenance, operation, vulnerability assessment, etc.	400 million yen
Total amount	913 million yen

(Taken from the reference material of the company)

(5) Medium-term management targets

For the term ending February 2027, the company aims for revenue of 3,763 million yen and an operating profit of 920 million yen. The CAGR target from the term ended March 2023 is 9.3% for revenue and 12.2% for operating profit.

Revenue and Operating Income Trends (Unit: million yen)



The sales composition ratio of Managed Security Services is expected to increase further from 85.0% in the term ended February 2023 to 94.3% in the term ending February 2027 due to growth from the expansion of security-related areas and the sales channels.

5. Conclusions

The company has decided not to pay dividends for the four terms from FY02/2024 to FY02/2027, prioritizing the allocation of funds to investment in human resources, service development, M&A, etc., in order to realize its medium-term business plan for further growth. There were various opinions about this decision within the company, and after deep discussions, the company reached the conclusion that "we should do everything we can to pursue growth. The entire company intends to push forward toward the goal of FY02/27, and they hope that you will look forward to their efforts.

The company intends to release a new service every quarter during the current fiscal year, and we will keep an eye on the progress of its

efforts to expand its service areas as well as its sales and profits.

<Reference: Regarding Corporate Governance>

◎ Organization type and the composition of directors and auditors

Organization type	Company with Audit Committee
Directors	11 directors, including 4 outside ones (4 independent executives)

◎ Corporate Governance Report

Last update date: May 25, 2023

<Basic Policy>

Our company's mission is "to ensure that all enterprises using the Internet can easily and securely carry out their business, we will offer the very best services to Japan and to the world," and have conducted our business to meet the expectations of our various stakeholders. Business management based on corporate governance, which forms the core of our business, is the most important administrative category and through a highly transparent, optimized management with a strengthened monitoring system, we are aggressively taking initiatives to improve our corporate value.

<Reasons for Non-compliance with the Principles of the Corporate Governance Code (Excerpts)>

Principle	Disclosed Content
<Supplementary Principle 2-4 ① Ensuring Diversity of Human Resources>	The company believes that it is important for each and every employee to embody the company's mission to enhance corporate value, and is working to ensure diversity by actively appointing excellent human resources without regard to gender, nationality, disability, or other factors. We will continue to consider the medium- to long-term human resource development policy and internal environment improvement policy.
<Supplementary Principle 3-1 ③ Sustainability Initiatives, etc.>	We provide comprehensive network security services so that all companies engaged in business can use the Internet safely and comfortably, and we believe that by promoting our business, we are responding to the resolution of issues concerning the sustainability of society. We are considering disclosing our investment in human capital and intellectual property in the future.
<Supplementary Principle 5-2 Formulate and Publish Management Strategies and Plans >	The Company has developed a management strategy and earnings plan, which is shared among the directors. We do not disclose our profitability and capital efficiency so that we can change our strategy flexibly as we are still a small company. In the future, when the company reaches a certain level of scale, we will present the information for disclosure.

<Reasons for Non-compliance with the Principles of the Corporate Governance Code (Excerpts)>

Principle	Disclosed Content
<Principle 1-4. Strategically Held Shares>	The company does not possess any strategically held shares. Further, the company will not hold any such shares, unless the alliance with invested companies would contribute to the improvement of the medium or long-term corporate value and is considered to contribute to the benefits of shareholders based on objective discussions, such as the comparison between the benefits and risk of ownership and the company's capital cost.
<Principle 3-1. Information Disclosure Enhancement>	In addition to the timely and appropriate legal disclosure of information, the company also publishes the following policies: (i) Management Philosophy, Strategy, and Plan

	<p>The company's corporate ethos is described on its website: https://www.variosecure.net/company/</p> <p>(ii) Basic Policies and Way of Thinking Regarding Corporate Governance Kindly refer to "I.1. Basic Way of Thinking" of this report for details on the company's basic policies and way of thinking regarding corporate governance.</p> <p>(iii) The Board of Directors' Policies and Procedures for Determining the Compensation for Management Staff and Directors The Board of Directors has established a policy for determining the details of remuneration for individual directors as described in the Section II.1. below. In addition, the Board consults with the arbitrary Remuneration Committee regarding the remuneration system and policies for directors, the calculation method used to determine specific remuneration amounts, and individual remuneration amounts, in order to reinforce the fairness, transparency, and objectivity of the procedures for determining the details of directors' remuneration. The Board of Directors consults a discretionary compensation committee regarding the compensation system and policies for Directors, the calculation method for determining the exact compensation amount, and individual compensation amounts. The Board of Directors has decided that the Representative Director will make the final decision on the individual compensation amounts reported by the discretionary compensation committee, within the compensation amount limit approved in the Stockholders' General Meeting through a resolution.</p> <p>(iv) Policies and Procedures for the Selection and Removal of a Management Staff Member by the Board of Directors and the Nomination of a Candidate for a Director Regarding the selection and removal of a Director, the Board of Directors will hold a final resolution based on the comprehensive decision on each employee's character as a manager as well as their experience, results, and expertise as a manager.</p> <p>(v) Explanation Regarding the Individual Nomination and Appointment During the Appointment or Removal of a Management Staff or the Nomination of a Candidate for the Board of Directors The reasoning behind each individual nomination is recorded in the regular General Meeting of Stockholders held every term, or in an extraordinary General Meeting of Stockholders.</p>
Supplementary Principle 4-1 (2) Disclosure of information on the medium-term management plan	Our company has announced our medium-term management plan and is striving to achieve it. Regarding the progress of the medium-term management plan, our company's policy entails working toward achieving the plan while making revisions to it as needed, taking into account environmental and strategy changes.
<Principle 5-1. Policies Regarding Constructive Dialogue with Stockholders>	The company uses its IR Department as a medium to promote dialogue with stockholders every day instead of only during Stockholders' General Meetings and offers information through its website and through phone calls. Further, the company has a system where the opinions of investors and stockholders obtained through these dialogues are reported to the Management Staff every time.

BRIDGE REPORT



This report is not intended for soliciting or promoting investment activities or offering any advice on investment or the like, but for providing information only. The information included in this report was taken from sources considered reliable by our company. Our company will not guarantee the accuracy, integrity, or appropriateness of information or opinions in this report. Our company will not assume any responsibility for expenses, damages or the like arising out of the use of this report or information obtained from this report. All kinds of rights related to this report belong to Investment Bridge Co., Ltd. The contents, etc. of this report may be revised without notice. Please make an investment decision on your own judgment.

Copyright(C) Investment Bridge Co., Ltd. All Rights Reserved.