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
¥1,151	3,802,613 shares		¥4,376 million	12.1%	100 shares
DPS (Est.)	Dividend yield (Est.)	EPS (Est.)	PER (Est.)	BPS (Act.)	PBR (Act.)
¥40.50	3.5%	¥128.01	9.0x	¥1,137.83	1.0x

*The share price is the closing price on October 26. Number of shares outstanding, DPS, EPS are taken from the brief financial report for the second quarter of FY Ending February 2023. ROE and BPS are the results of the previous year.

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 Est.	2,650	785	756	525	128.01	40.50

* Unit: million-yen, yen. Estimates calculated by the company. IFRS applied. 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 the second quarter of Fiscal Year Ending February 2023 and Growth Strategy etc.

Table of Contents

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."**

- **Their specialties and strengths include (1) an original business model, which offers a one-step solution with the procurement of devices used for security services, the development of key software installed into those devices, installation and setting up of those devices, and monitoring and operation of the devices after installation, (2) a stable earnings model, which is based on a recurring revenue business, whose revenues increase year by year through an increase in the number of companies installing their products with a monthly charging system, and on a low cancellation rate, (3) a strong marketing channel covering the entire country with partnered companies in OEM and partnered companies in resale, and (4) a high share among small and medium sized enterprises, which appraises the ease of installation of their products.**

- **The sales revenue for the second quarter of the term ending February 2023 stood at 1.337 billion yen, up 4.2% year on year. The managed services, mainly EDR, performed well as planned, and integration services, which had large projects, also increased. Operating income increased 6.3% year on year to 385 million yen. Gross profit increased only 0.7% year on year, however, SG&A expenses declined 3.7% year on year, even though they have strengthened the organizational structure for the security operation center and the adjacent areas including EDR, and advertising expenses augmented.**

- **There is no change in the earnings forecast. For the term ending February 2023, the company forecasts a 3.2% year on year increase in revenue to 2,650 million yen and a 4.4% year on year rise in operating profit to 785 million yen. A new series of Managed Security Service was launched in March, with the aim to further grow the mainstay business. In addition, with the increase of remote work due to the novel coronavirus pandemic, the company will strengthen security measures on the terminal side and expand its adjacent business of Data Backup Service in case of an emergency. The company aims to increase sales and profit by absorbing investments for strengthening the structure of the security operation center (SOC) and adjacent areas (EDR, etc.), increasing the number of remote marketing staff, and advertising and promotional expenses. The company targets a dividend payout ratio of 30% on an IFRS basis. The dividend forecast for the term ending February 2023 is ¥40.50/share, up ¥0.06/share from the previous term. The expected dividend payout ratio is 29.3% on an IFRS basis.**

- **As the data that should be protected now exist both inside and outside systems, "Zero-Trust Security," which is based on the presumption that all communications should not be trusted (zero-trust), is expected to grow rapidly in the future. The company has been researching and dealing with this matter since around 2020, and EDR, which is strongly growing this fiscal year, is the first product to cultivate the Zero-Trust Security market.**

- **While the company continues to strengthen their relationship with HEROZ, the company intends to continue leveraging the strengths of both companies to capture this market, and we would like to pay attention to what specific initiatives and measures they will have and their progress.**

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

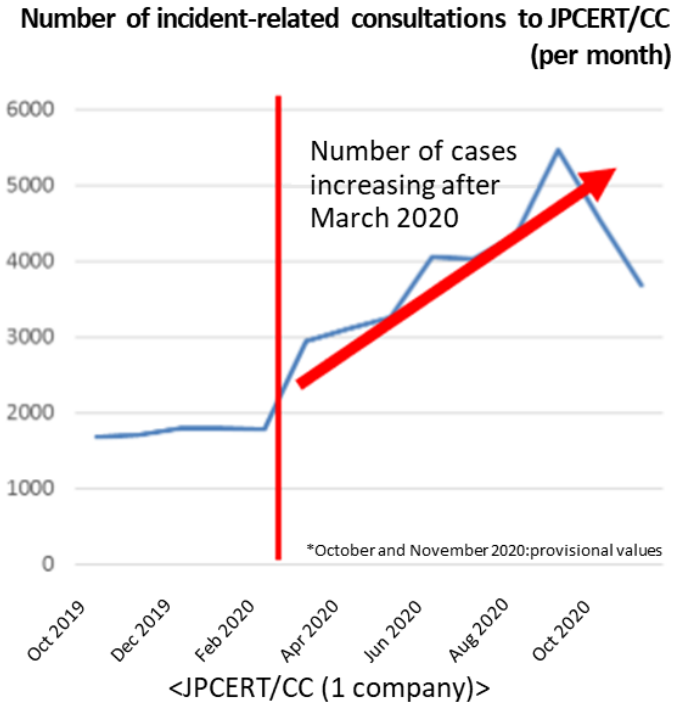
◎ New types of cyber attacks receive increased attention

In August 2021, IPA (Information-technology Promotion Agency, Japan) released the Ten Major Threats to Information Security 2021. The Ten Major Threats to Information Security 2021 were selected by IPA from information security incidents that occurred in 2020 and are considered to have had a significant impact on society. The Ten Major Threats Selection Committee, consisting of approximately 160 members, including researchers in the information security field and practitioners from companies, deliberated and voted on the threat candidates.
The top threat was "damage by ransomware" as in the previous year, followed by "theft of confidential information by targeted attacks," the same as the previous year. On the other hand, "Zero-day attacks," which target users before the release of a modified program, ranked seventh, 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.



(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

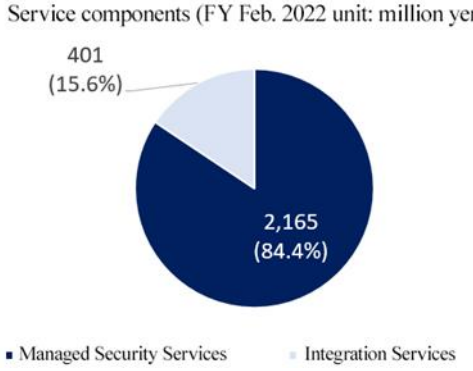
*Created by Investment Bridge based on the Ministry of Economy, Trade and Industry's "Survey on Supply and Demand of IT Human Resource (Summary)" (April 2019).

[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.



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

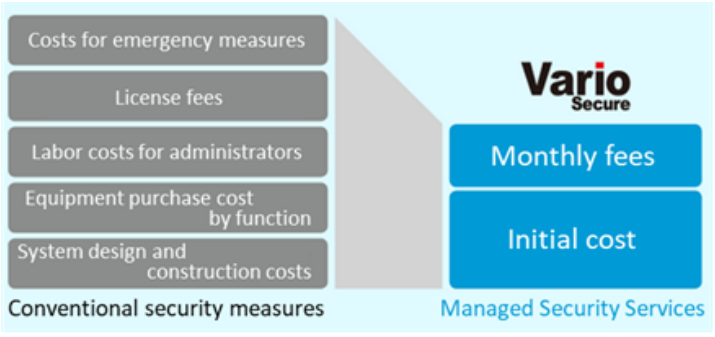
Previously, to introduce the security system such as above, it was necessary to install various security devices in-house and maintain them, making it more difficult for many companies to introduce sufficient network security measures because they required highly skilled engineers and high investments.

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 August 31, 2022, the number of VSR managed units was 7,379. 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 August 2022, the company has signed agreements with 69 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 2,926 as of August 31, 2022.

[1-5 Characteristics and Strengths]

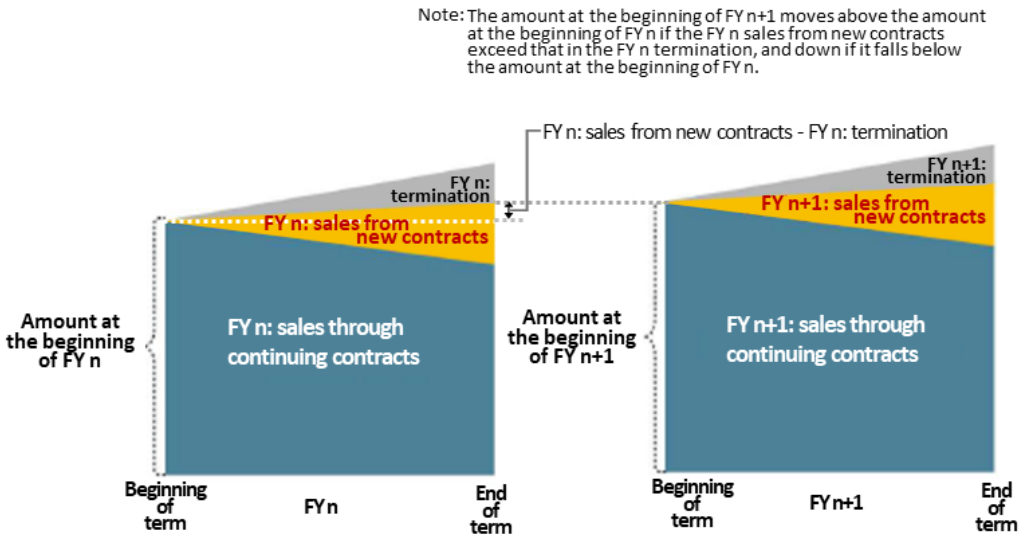
(1) Unique business model

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 2022, Managed Security Services accounted for 84.4% of the company's total sales revenue. With a low churn rate of 0.82% (in the term ended February 2022), 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 69 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

With its easy implementation of high-level security services as well as the operation and management, 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 (FY2020)

	0 – 99 employees	100 – 299 employees	300 – 999 employees
No. 1	Vario Secure 30.3%	Vario Secure 25.3%	Vario Secure 22.1%
No. 2	Company A 14.8%	Company A 14.9%	Company A 9.0%
No. 3	Company B 13.3%	Company B 9.3%	Company B 8.7%

* Created by Investment Bridge based on the company's financial results briefing materials (source: ITR "ITR Market View: Gateway Security-Based SOC Service Market 2021")

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

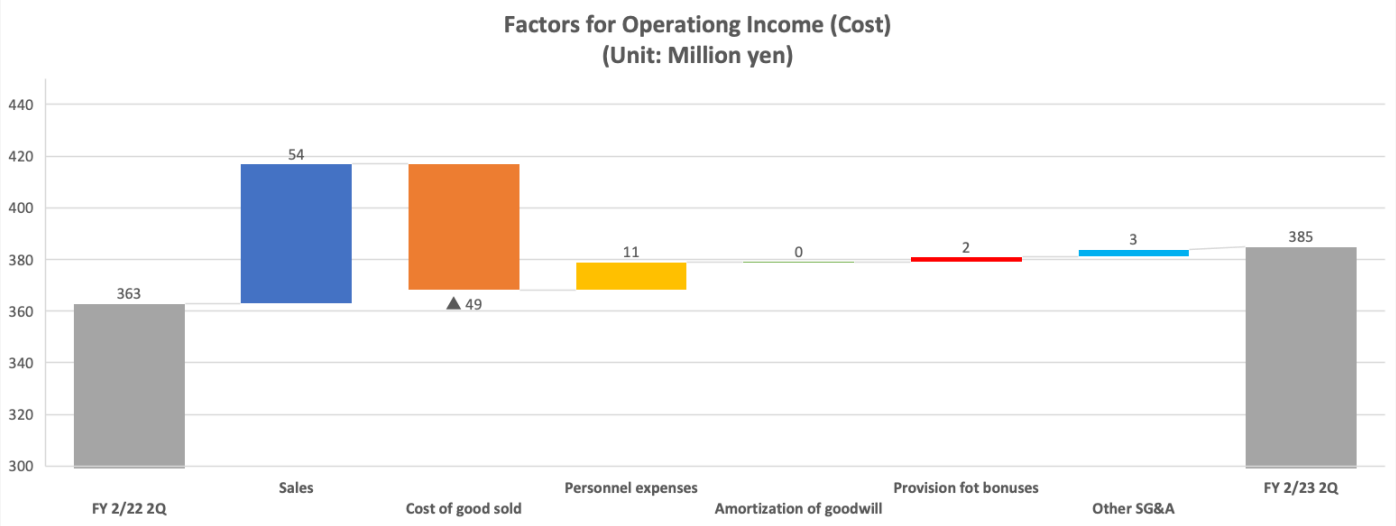
2. The second quarter of Fiscal Year Ending February 2023 Earnings Results

(1) Overview of business results

	FY 2/22 2Q	Ratio to sales	FY 2/23 2Q	Ratio to sales	YoY
Revenue	1,283	100.0%	1,337	100.0%	+4.2%
Gross profit	792	61.8%	797	59.7%	+0.7%
SG&A and others	429	33.5%	413	30.9%	-3.7%
Operating profit	363	28.3%	385	28.9%	+6.3%
Profit before tax	337	26.3%	355	26.6%	+5.3%

Profit	233	18.2%	245	18.3%	+5.1%

*Unit: million yen

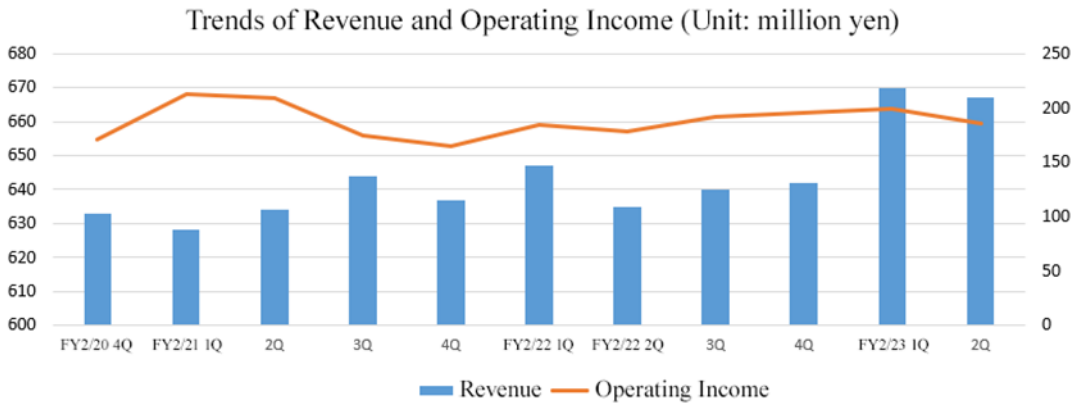


*Prepared by Investment Bridge Co., Ltd. based on the disclosed material.

▲ in the expense item represents an increase in expenses.

Sales and profit increased.

The sales revenue for the second quarter of the term ending February 2023 stood at 1.337 billion yen, up 4.2% year on year. The managed services, mainly EDR, performed well as planned, and integration services, which had large projects, also increased. Operating income increased 6.3% year on year to 385 million yen. Gross profit increased only 0.7% year on year, however, SG&A expenses declined 3.7% year on year, even though they have strengthened the organizational structure for the security operation center and the adjacent areas including EDR, and advertising expenses augmented.



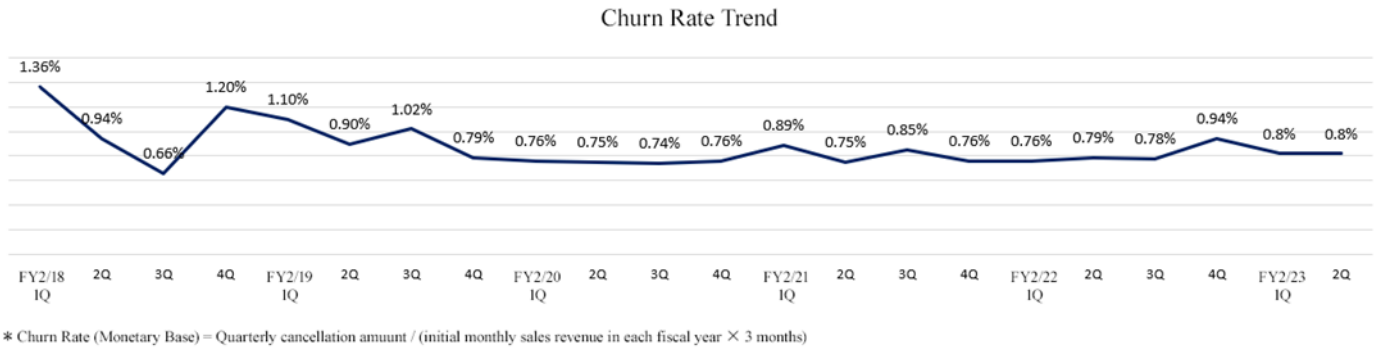
(2) Service trends

	FY 2/22 2Q	FY 2/23 2Q	YoY
Managed security service	1,084	1,119	+3.3%
Integration service	199	217	+9.1%

*Unit: million yen

◎ Churn rate

The churn rate remained low.



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

(3) Business Topics

* The company began providing the cyber-attack-resistant backup service "VDaP-Vario Data Protect" on an OEM basis to their main distributer, USEN ICT Solutions.
  "VDaP-Vario Data Protect" is a backup service that mitigates the risk of ransomware infection and protects critical corporate data using dedicated backup devices and proprietary systems.
* To address cyber-attacks that have become more sophisticated and organized, the company released a webpage for downloading white papers to introduce the background of the attacks and examples of countermeasures. They also provide information for corporate security enhancement measures to small and medium-sized enterprises that lack technical personnel and countermeasures.
* In the first half of the current fiscal year, the company participated in online events and seminars, in addition to continuing to hold webinars about their services. They focused on countermeasures for ransomware and Emotet, which have increased in the number of infection damages, and disseminated timely information.
  In the exhibit at the Japan Association for Medical Informatics Spring Conference, they proposed the backup service "VDaP-Vario Data Protect" as a countermeasure against ransomware attacks on electronic medical record data, which have been on the rise in recent years, and it generated a lot of interest.

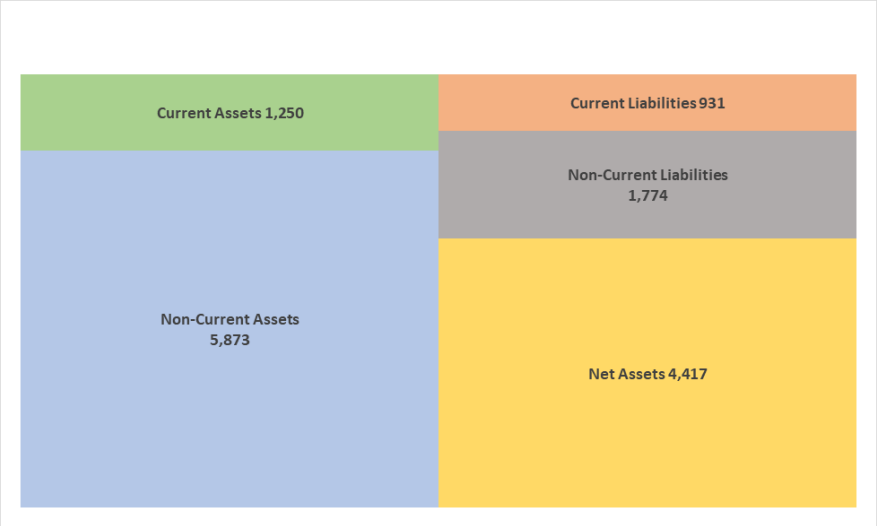
(4) Financial position and cash flows

◎ Main Balance Sheet

	End of February 2022	End of August 2022	Increase/ decrease		End of February 2022	End of August 2022	Increase/ decrease
Current Assets	1,249	1,250	+1	**Current Liabilities**	2,403	931	-1,472
Cash and Cash Equivalents	389	239	-150	**ST Interest Bearing Liabilities**	1,786	300	-1,486
Trade and Other Receivables	464	490	+25	**Trade and Other Payables**	134	124	-9
Non-current Assets	5,872	5,873	+0	**Non-current Liabilities**	395	1,774	+1,379
Tangible Assets	206	165	-41	**LT Interest Bearing Liabilities**	28	1,400	+1,371
Goodwill	5,054	5,054	0	**Total Liabilities**	2,799	2,706	-92
Intangible Assets	242	271	+29	**Net Assets**	4,323	4,417	+93
Total Assets	7,122	7,123	+1	**Retained Earnings**	2,351	2,443	+91
				Total Liabilities	7,122	7,123	+1

and Net Assets			
Balance of Interest-bearing Liabilities	1,815	1,700	-115

*Unit: million yen. Borrowings include lease liabilities.



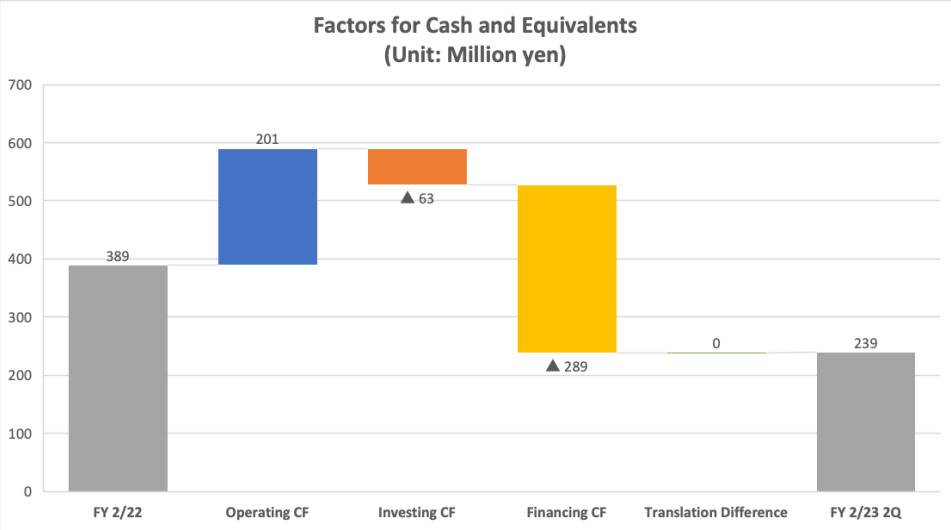
* Prepared by Investment Bridge Co., Ltd. based on the disclosed material.

Balance of interest-bearing liabilities decreased by 115 million yen from the end of the previous term. Net D/E ratio increased 0.8% from the end of the previous term to 33.1%. Equity ratio increased by 1.3 points to 62.0% due to decrease in liabilities and increase in retained earnings.
Repayment of interest-bearing liabilities and financial soundness improvement are progressing as planned.

◎ Cash Flows

	FY 2/22 2Q	FY 2/23 2Q	Increase/decrease
Operating Cash Flow	243	201	-41
Investing Cash Flow	-53	-63	-9
Free Cash Flow	189	138	-51
Financing Cash Flow	-369	-289	+80
Balance of Cash and Equivalents	414	239	-175

*Unit: million yen



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

The surpluses of operating CF and free CF decreased.
The cash position fell below from the end of the previous term.

3. Fiscal Year Ending February 2023 Earnings Forecasts

(1) Earnings forecasts

	FY 2/22	Ratio to sales	FY 2/23 Est.	Ratio to sales	YoY
Revenue	2,566	100.0%	2,650	100.0%	+3.2%
Gross profit	1,597	62.2%	1,612	60.8%	+0.9%
Operating profit	751	29.3%	785	29.6%	+4.4%
Profit before tax	701	27.3%	756	28.5%	+7.9%
Profit	500	19.5%	525	19.8%	+4.9%

*Unit: million yen

There is no change in the earnings forecast. Increase in revenue and profit estimated.

There is no change in the earnings forecast. Revenue is estimated to be 2,650 million yen, up 3.2% from the previous term and operating profit is projected to be 785 million yen, up 4.4% from the previous term.

A new series of Managed Security Service was launched in March, with the aim to further grow the mainstay business. In addition, with an increase of the remote work triggered by the novel coronavirus pandemic, the number of inquiries for reinforcement of security measures on the terminal side as well as the adjacent business of the Data Backup Services in case of emergencies has been increasing in a healthy manner. The company aims to increase sales and profit by absorbing investments for strengthening the structure of the security operation center (SOC) and adjacent areas (EDR, etc.), increasing the number of remote marketing staff, and advertising and promotional expenses.

The company targets a dividend payout ratio of 30% on an IFRS basis. The dividend forecast for the term ending February 2023 is ¥40.50/share, up ¥0.06/share from the previous term. The expected dividend payout ratio is 29.3% on an IFRS basis.

(2) Main initiatives

To strengthen core businesses and expand operations in adjacent businesses.

① To grow the mainstay business

The company will grow its Managed Security Service by strengthening its support (quality, efficiency, and speed) and service capabilities. Specifically, the newly released “n-series” provides additional functions that are in high demand by customers, and the UI has been substantially revamped, and effects and outcomes of these efforts are beginning to emerge.

In addition, the company will promote automation through VSR-Config and is considering offering bundled services jointly with HEROZ, with which it has formed an alliance.
Through these efforts, the company aims to add value and differentiate itself from its competitors.

② Business expansion into adjacent businesses
The company will expand business not only in VSR (Internet Gateway), but also in adjacent areas where needs are growing, such as VDaP, EDR (EPP), and V-NSS. EDR, which was launched in October 2021, has been attracting business inquiries.
It will accelerate the speed of its business expansion by further focusing on initiatives that have proven successful in the previous term, such as the use of webinars, strengthening approaches to specific industries, including the medical industry, and remote marketing.
The company will strive to find distributors through EDR, sell office equipment, and penetrate the medical industry through VDaP.

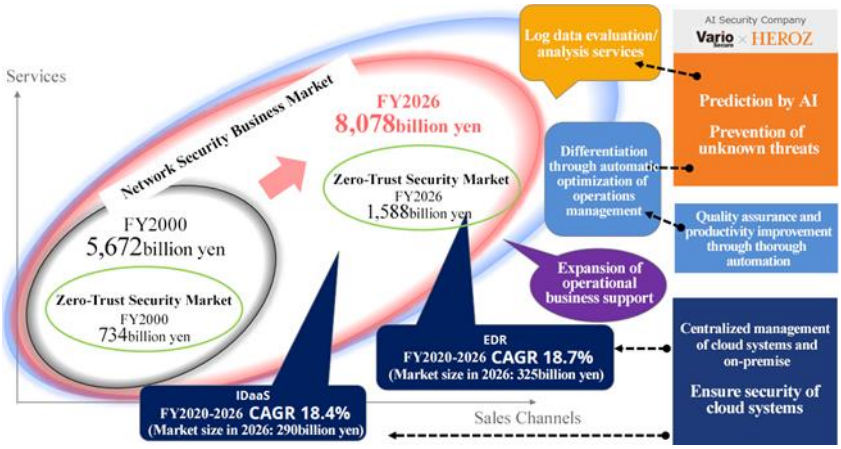
4. Medium-and-long term Growth Strategy

(1) Growth Strategies and Market Trends

The company has been working on three themes since the term ended February 2020: "User Interface Integration," "Strengthening/Linkage of the Key Software," and "Optimization/Automation of the SOC (Security Operation Center)." These measures have been making steady progress, with concrete results beginning to emerge, such as "progress in the alliance with HEROZ" and "release of n-series."

In particular, the collaboration with HEROZ is expected to lead to the higher value-added services including the installation of the AI traffic forecasting function, as well as productivity improvements through SOC optimization/automation. In addition, they believe it is possible to establish a competitive and unique positioning to centrally manage both on-premise systems and cloud-based systems.

As such, the company has begun to see a specific picture of the above three themes, and has set forth the following growth strategies. They will launch EDR, EDR operational support, and IDaaS, to gain a share in the Zero-Trust Security* market, and at the same time, aims to optimize service development and operation management with HEROZ, and monetization.



(Taken from the reference material of the company)

***Zero-Trust Security**
Conventional security measures have been to divide the networks into the reliable "internal" network and the unreliable "external" network, and take measures at the boundaries of these networks. The internal networks include the company's internal LAN and data center connected via a VPN, and the external networks include the Internet. Firewalls and various security devices are installed at the boundaries to monitor and control communications, thereby blocking cyber-attacks from the outside.

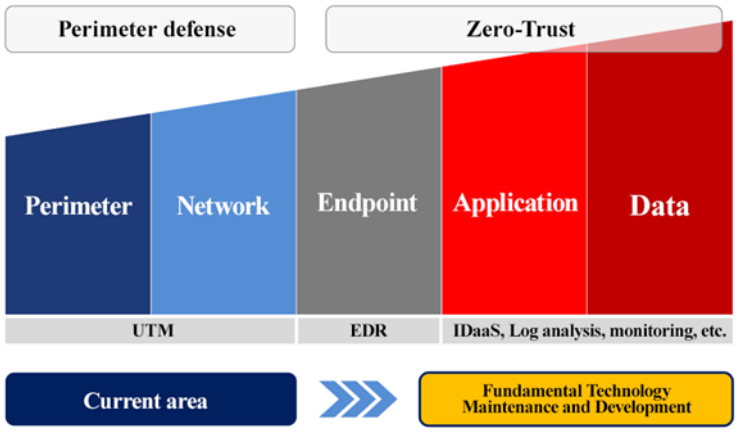
For these conventional security measures, it is assumed that the data and systems to be protected are in the internal network, however, with the spread of cloud computing, more and more data and systems that should be protected exist on the Internet, which is on the external network. As such, the boundaries 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.

◎ Strengthening Basic Technology (to the Zero-Trust Zone)

The company will expand the domain of the managed security services business and establish fundamental technologies to expand their services to the Zero-Trust zone.

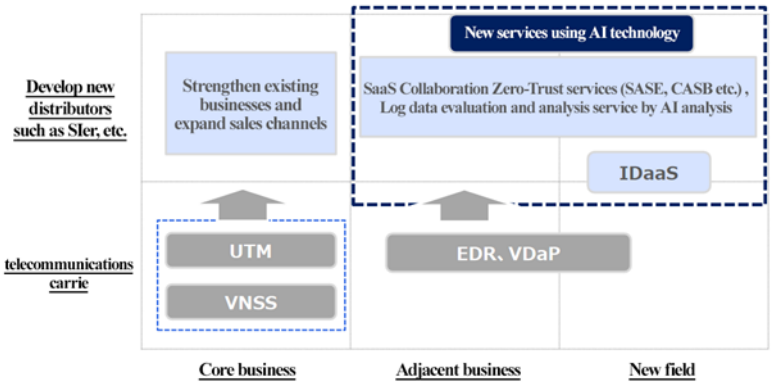
They have long been working to incorporate the Zero-Trust Security with EDR that controls the endpoint. In the future, they will further expand their business domain to include IDaaS, log analysis, and monitoring.



(Taken from the reference material of the company)

◎ Pursuing Existing Business and Creating New Services using AI Technology

From on-premise PC servers to cloud based systems, the company aims to be a unique company that can provide the managed security services that can perceive and manage corporate networks in a cross-functional and centralized manner.



(Taken from the reference material of the company)

◎ Strengthening the Relationship with HEROZ

The company believes that further strengthening the relationship with HEROZ is essential for establishing their position and brand as an "AI Security Company" that utilizes AI technologies in order to carry out business development as described above, and conducted a third-party allotment to HEROZ in September 2022, following the allotment in September 2021.

HEROZ's shareholding ratio is now 42.88%.

(2) What The Company Aims to Be

The company aims to realize a concept of "Information System as a Service," in which the company expands the area of services beyond the Internet, to provide service covering the overall corporate network infrastructure.

In about five years, the company intends to pursue evolution into an "AI Security Company" that provides services ranging from the safety and security of corporate Internet connections to overall corporate network infrastructure to make "Information System as a Service" attainable.

5. Conclusions

As the data that should be protected now exist both inside and outside systems, "Zero-Trust Security," which is based on the presumption that all communications should not be trusted (zero-trust), is expected to grow rapidly in the future. The company has been researching and dealing with this matter since around 2020, and EDR, which is strongly growing this fiscal year, is the first product to cultivate the Zero-Trust Security market.
While the company continues to strengthen their relationship with HEROZ, the company intends to continue leveraging the strengths of both companies to capture this market, and we would like to pay attention to what specific initiatives and measures they will have and their progress.

<Reference: Regarding Corporate Governance>

◎ Organization type and the composition of directors and auditors

Organization type	Company with company auditor(s)
Directors	6 directors, including 2 outside ones (one independent executive)
Auditors	3 auditors, including 3 outside ones (three independent executives)

◎ Corporate Governance Report
Last update date: May 25, 2022

<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 4-1② Information Disclosure Related to the Medium-Term Management Plan>	The company formulates its target amounts based on a medium to long term point of view, but does not publicly announce those amounts. As the scale of the company is still small, it refrains from disclosing for any quick changes in strategy can be possible. The company will

	disclose the information once it reaches a certain scale.
Principle 5-2. Formulation and Public Announcement of Management Strategy and Plan	The company formulates management strategies and earning plans, which it shares with its board members. Regarding earning capacity and capital efficiency, as the scale of the company is still small, it refrains from disclosing for any quick changes in strategy can be possible. The company will disclose the information once it reaches a certain scale.

<Disclosure Based on 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 The company's corporate ethos is described on its website: https://www.variosecure.net/company/mission/ (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. (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. (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. (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.
<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.