SecuAvail

The market environment graph on page 6 of the disclosure materials released on June 20, 2025 has been updated.

Business Plan and Matters Concerning Growth Potential

SecuAvail Inc.（3042）

August 18, 2025

Table of Contents

I .Company Overview

Business Objectives and Overview

Since our founding in 2001, during the early days of the Internet, our Group has remained committed to a singular mission as a dedicated provider of network security solutions: enabling our customers to operate their systems safely and with confidence. Recognizing network security operations as a vital component of the critical infrastructure underpinning modern socioeconomic activity, we have upheld a service philosophy of delivering responsible, round-the-clock (24/7/365) network security support since our inception.

The Group consists of the parent company and two consolidated subsidiaries—CareAvale Inc. and LogStare Inc.—forming a total of three entities.

Company Name	SecuAvail Inc.
Date of Establishment	August 20, 2001
Representative	Representative Director and President　Masaomi Yoneima
Stock code	3042
Number of consolidated employees	106 (as of March 31, 2025)
Business activities	Network security operation, monitoring, and log analysis services
Head office location	530-00441-1-19 Higashi Tenma, Kita-ku, Osaka-shi, Osaka Urban Ace Higashi Tenma Building
Wholly owned subsidiary	CareAvail Inc. LogStare Inc.

Corporate Philosophy and Mission

Corporate Philosophy

「Contribution」

To deliver services of the highest quality, contribute to our customers' business growth, bring fulfillment to our employees and their families, and advance the Company while contributing to society and our local communities.

Mission

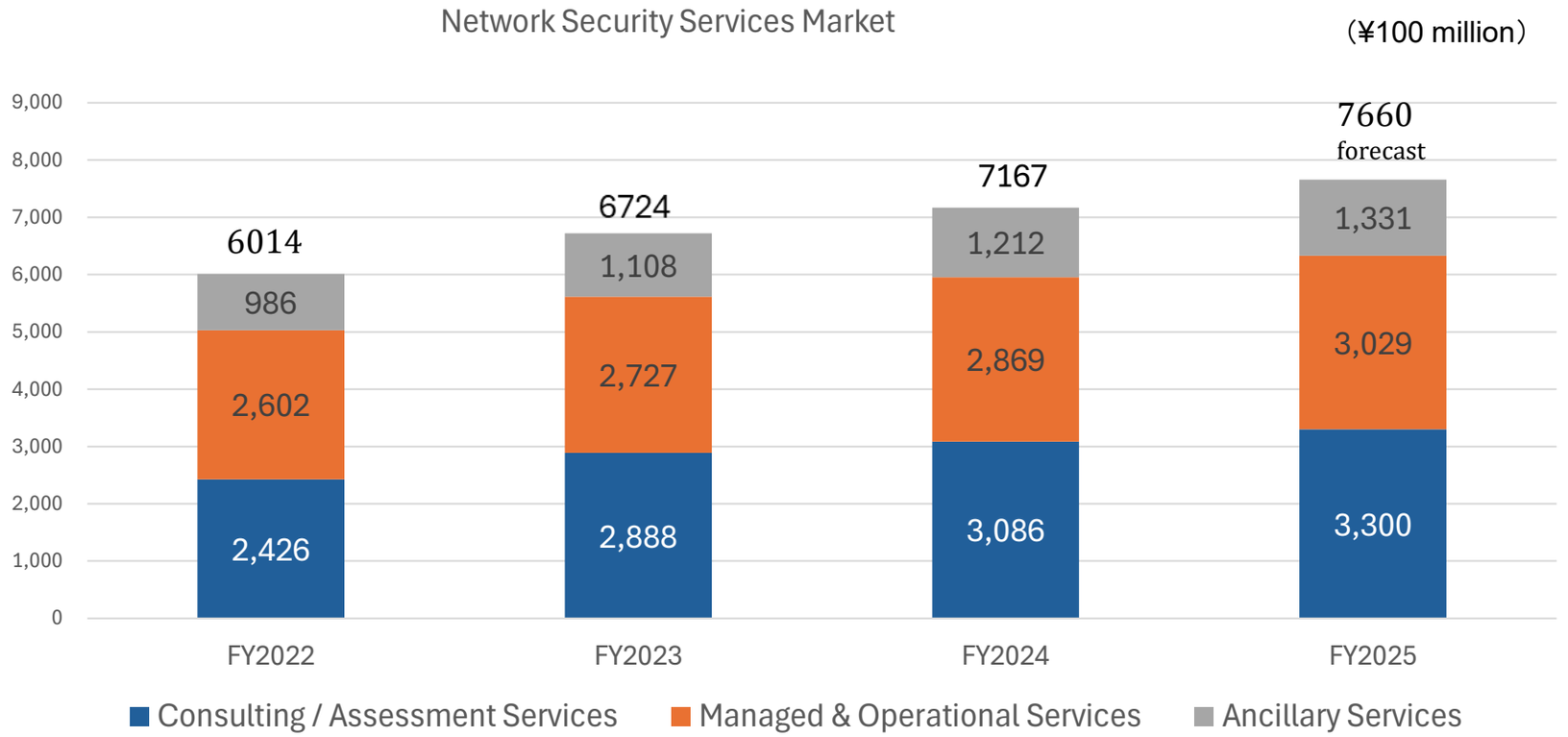
We aim to be a long-term, trusted partner, ensuring our customers' system security and enabling them to operate their businesses with confidence through the delivery of network security, reliable, and value-adding services.

Secure (安全) security × Avail (役立つ) Available

Ⅱ. Market Environment

Market Enviroment of Core Businesses

Cyberattacks exploiting system vulnerabilities remain a persistent threat, affecting companies of all sizes in Japan and abroad, and posing increasingly serious risks to the global socioeconomic environment.
With security incidents and data breaches continuing to rise each year, the need for robust information security measures and comprehensive log management has never been greater.



Source: JNSA Research Committee, “FY2024 Domestic Information Security Market Survey Report”

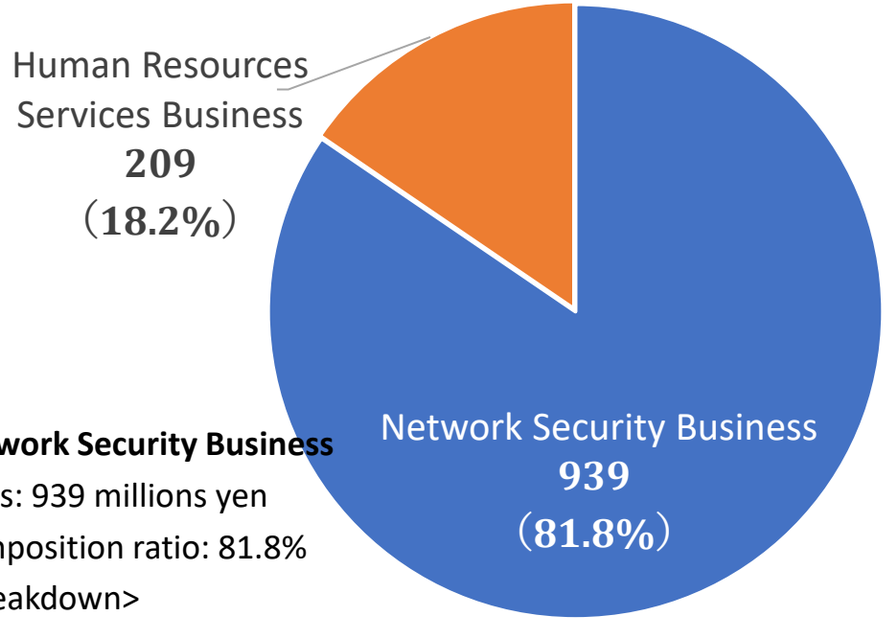
Ⅲ. Business Activities

Consolidated Sales and Cost Composition for the Fiscal Year Ending March 2025

Our group operates primarily in two business segments: the “ Network Security Business," which focuses on network security operation and monitoring services as well as the development and sales of various security operation platforms; and the "Human Resources Services Business," which involves training and dispatching information security engineers.

Unit: million yen

【Consolidated sales composition】



Network Security Business

Sales: 939 millions yen

Composition ratio: 81.8%

<Breakdown>

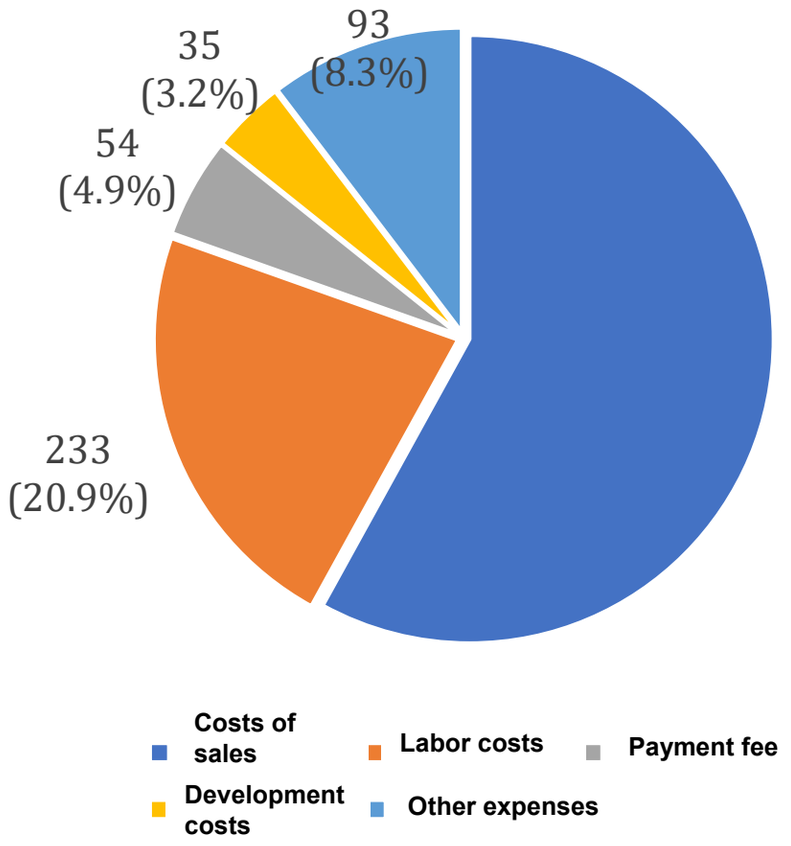
Product Sales: Sales of products and product maintenance

Net sales: 215 million yen (22.9% of total sales)

Service Sales:Net sales: 724 million yen (77.1% of total sales)

SOC services and the development and sales of various security operation platforms

【Consolidated cost composition】



Network Security Business

The core business of our group is the network security business, conducted through two main companies. The first is SecuAvail Inc., which provides the security monitoring service “NetStare.” The second is LogStare Inc., whose primary business is the development and sale of various security operation platforms under the service concept of “Contributing to customers’ operations,” aimed at delivering higher value-added services. The distinctive features of each company’s proprietary services enhance the group’s overall competitive advantage.

Provided by SecuAvail Inc.

NetStare®

NetStare® is a fully integrated security operations service that monitors customers’ network infrastructure 24/7/365, enabling early detection of equipment failures, network outages, and cyberattacks. Combining a Security Operation Center (SOC) and a Network Operation Center (NOC), it provides real-time monitoring, network setup support, log and risk analysis, vulnerability assessments, and security policy improvement. Developed entirely in Japan, NetStare® is one of the few fully domestic SOC services in the industry, delivering comprehensive IT security solutions tailored to modern business needs. Its unique domestic development approach and integrated capabilities set it apart in the market, positioning the service for sustained growth in the expanding global cybersecurity sector.

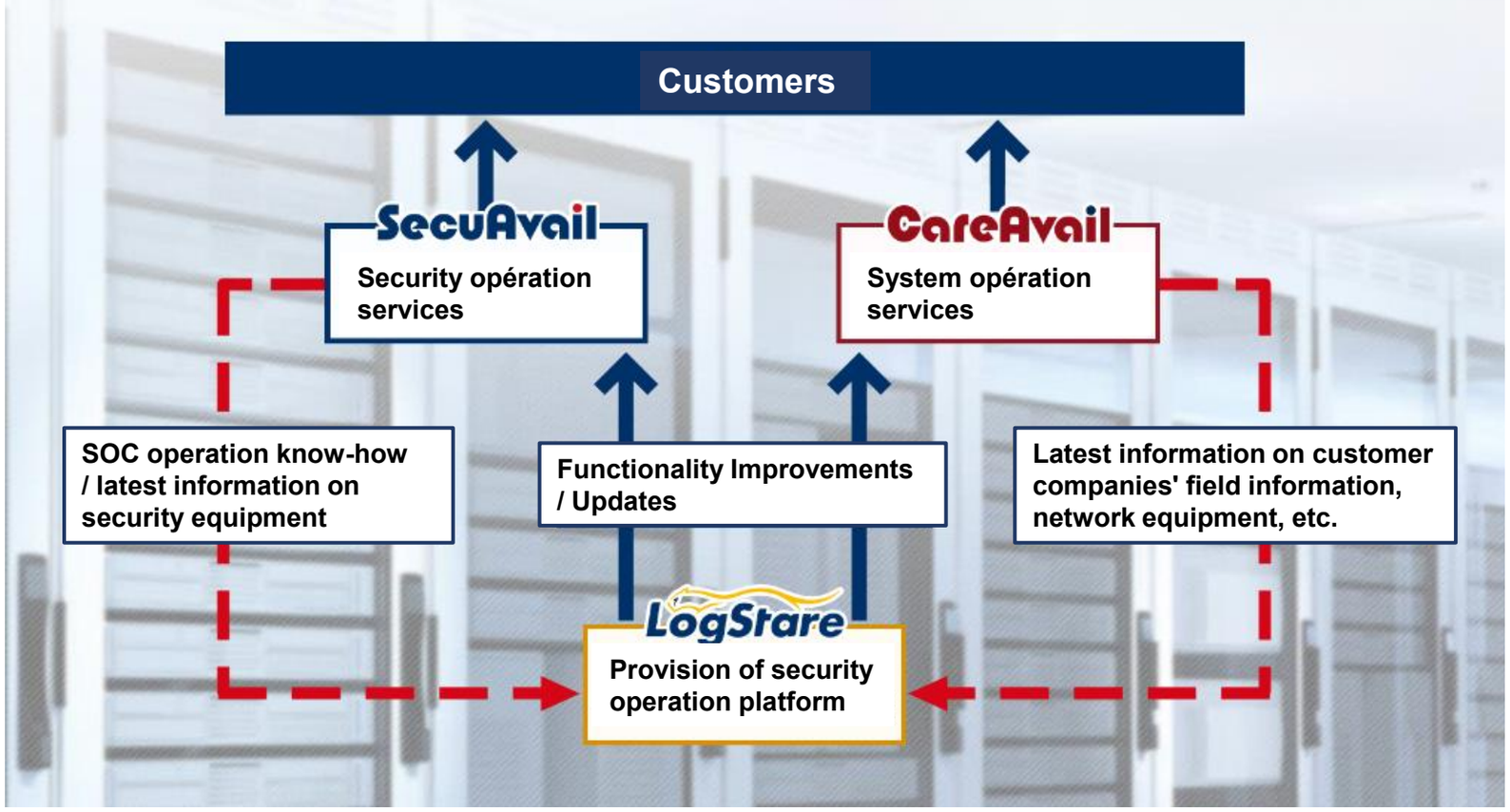
Provided by LogStare Inc.

LogStare

LogStare is a next-generation managed security platform that integrates system monitoring, log management, and AI-based forecasting into a single software solution. Traditionally, security operations software has been divided into separate tools for system monitoring and log management, with additional analytics tools required for report creation and forecasting—making full implementation and proper operation a significant burden for customers. LogStare comes preloaded with report templates actually used in SecuAvail’s Security Operation Center (SOC), enabling immediate use upon deployment. By minimizing implementation barriers and costs, consolidating multiple functions into one software product, and offering it via the cloud, LogStare delivers a unique competitive advantage unmatched by other companies.

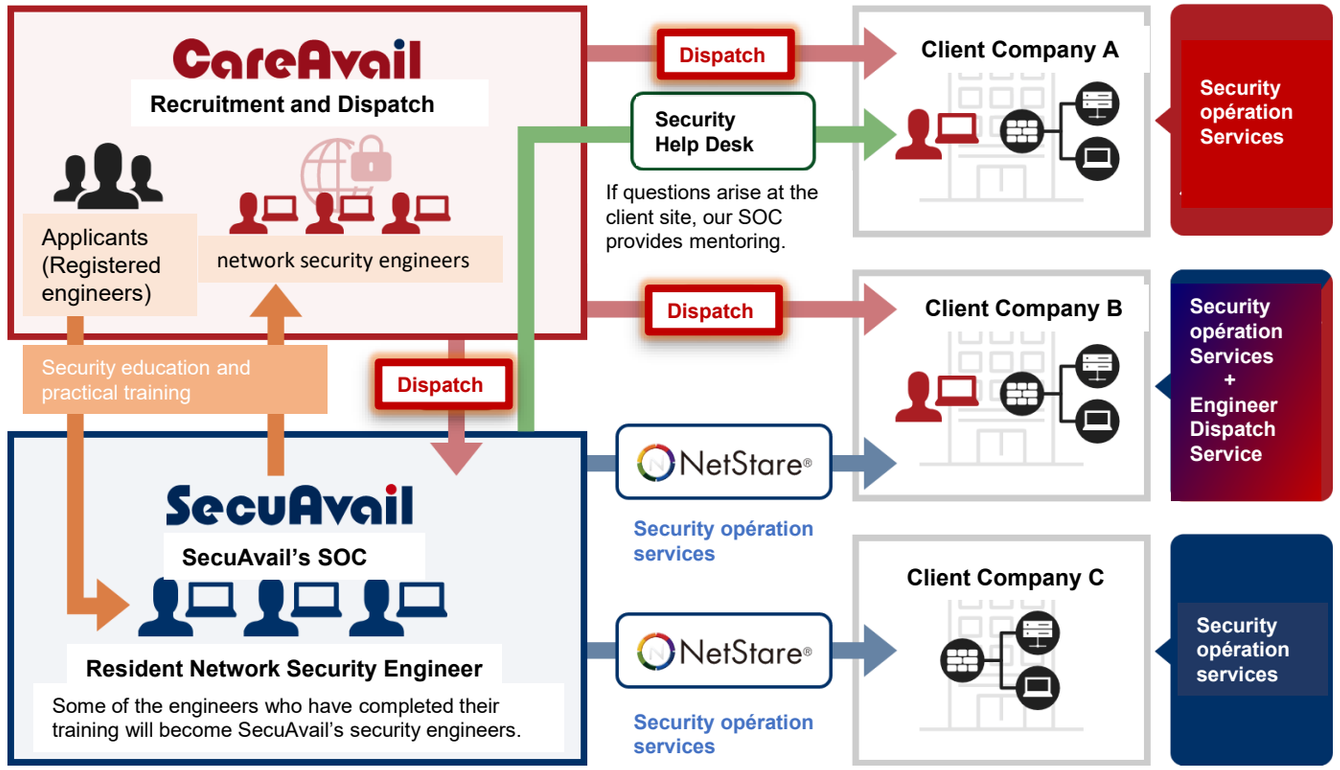
Establishing a Vertically Integrated Business in the Network Security Business

Our Group has established a vertically integrated business model centered on its flagship comprehensive security operations service, enabling the seamless integration of real-time field intelligence and developments essential for effective security monitoring and management.



Human Resources Services Business

The Human Resources Services business, conducted through our consolidated subsidiary CareAvail Inc., focuses primarily on dispatching network security engineers to clients.Recognizing that effective network security measures require the expertise of trained professionals, we develop and dispatch skilled security engineers to address the growing societal demand driven by increasing network connectivity. This approach enables us to meet the needs of clients facing a shortage of qualified information security engineers.

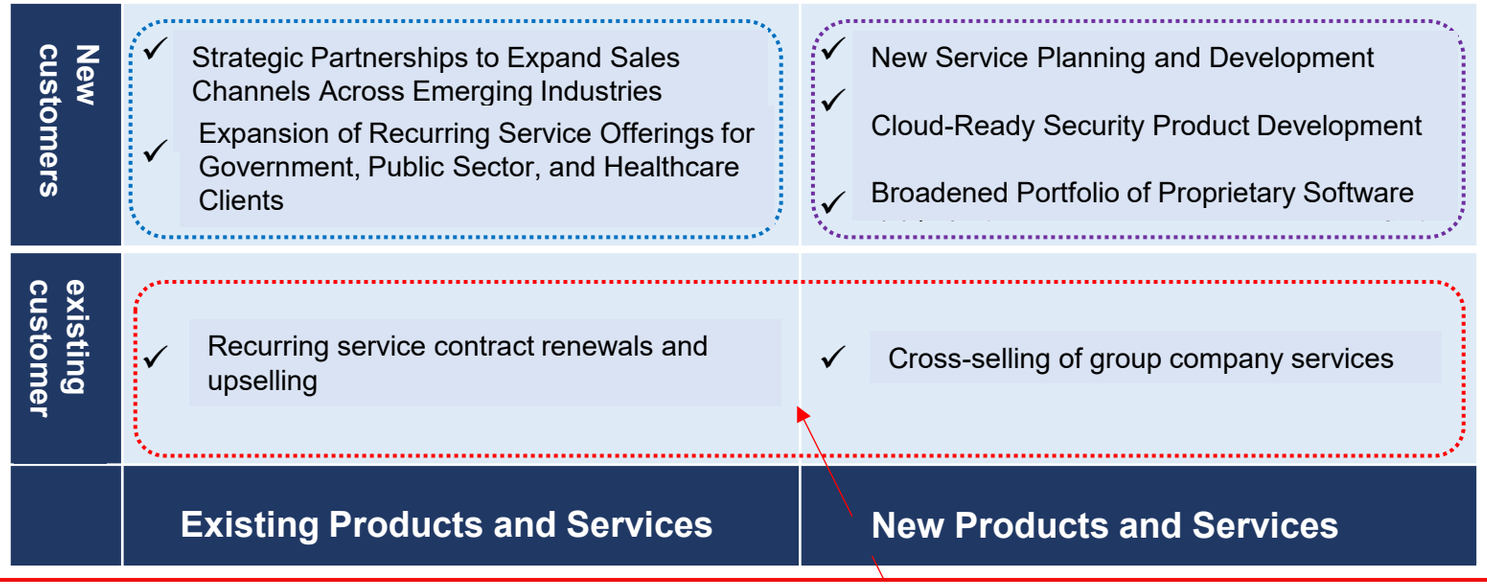


Our unique strength lies not only in dispatching network security engineers, but also in offering a hybrid model—combining our security operations service with engineer dispatch to existing cyber security clients.

Progress of Strategic Business Initiatives

We have actively pursued strategic partnerships, including alliances with Broadband Security Inc., a company with strong expertise in IT security services, and Medical Ocean Inc., which specializes in providing services centered on medical DX (digital transformation). As a result, we successfully acquired nine new partner companies over the past year. These collaborations have enabled us to expand our sales channels in the medical sector as well as among local governments and public institutions.

In our core security operations monitoring service (SOC service), we focused on raising awareness and expanding sales of “NetStare for Medical,” a cybersecurity service for healthcare institutions, and “NetStare for OT/IoT,” a service for automotive industry supply chains. Our subsidiary LogStare Inc. strengthened its development of security products for cloud environments—such as log analysis for Box and Google Workspace—as well as the enhancement of its operational platforms



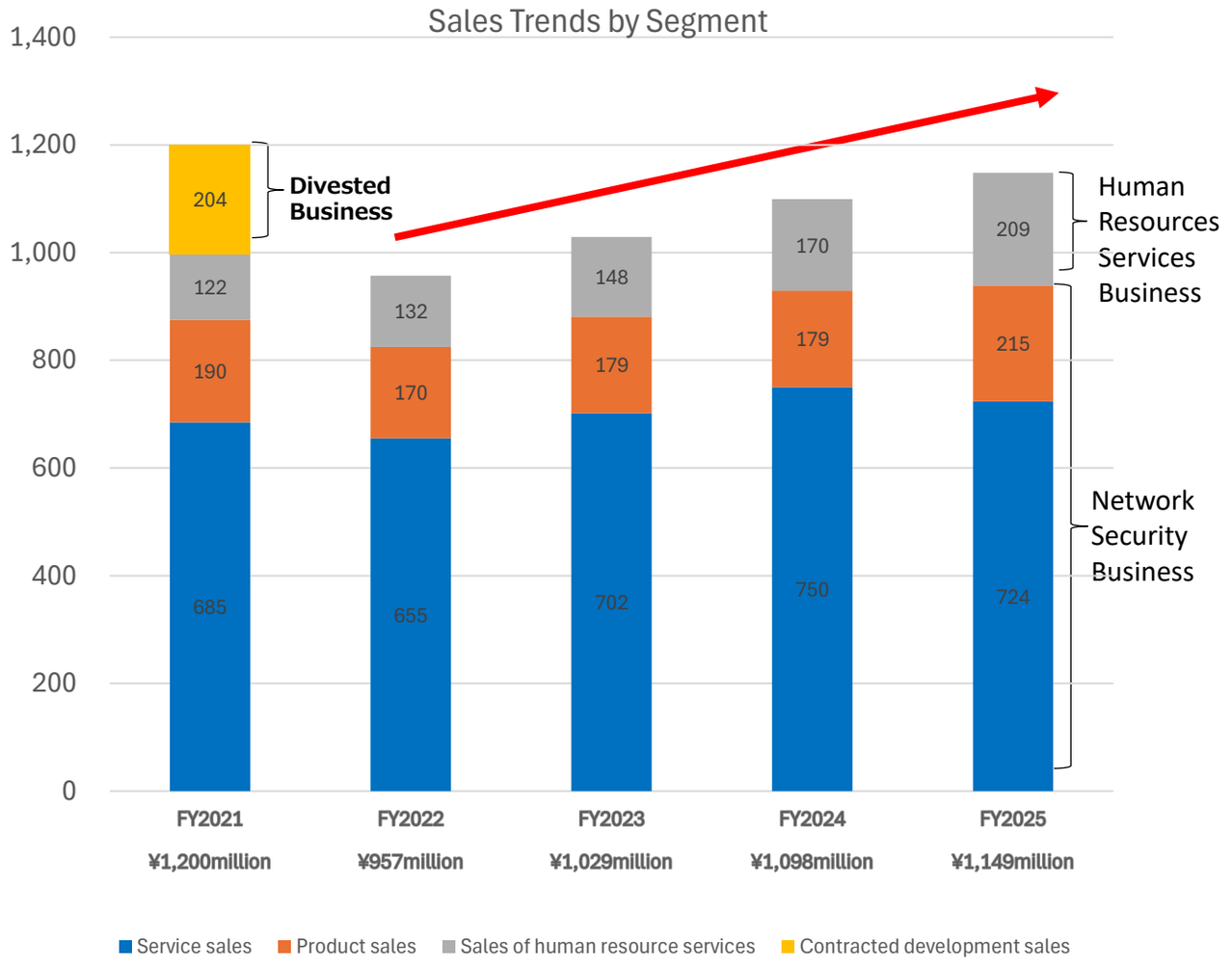
We continue to work on establishing a stable revenue base by securing new contracts and renewals for our security operations monitoring service (SOC service), a recurring service that is one of our core strengths.
To strengthen client relationships and expand upselling and cross-selling opportunities, we enhanced our support structure by assigning staff with technical expertise to customer follow-up.

Ⅳ.Financial Highlights

Sales Performance by Business Segment

The revenue composition of our Network Security Business is centered on highly sustainable services, particularly security monitoring and operations services. We continue to focus on acquiring new contracts and renewing existing ones for stable, subscription-based services. For the fiscal year ending March 2025, Network Security Business recorded revenue of ¥939 million, representing a year-on-year increase of 1.2%. The segment accounted for 81.8% of total revenue, compared to 84.5% in the previous fiscal year. But, the proportion of high-margin product sales increased, resulting in a profit improvement of ¥59 million year-on-year. Going forward, we will continue to strengthen our efforts to acquire and renew contracts for subscription-based services, which serve as a stable source of recurring revenue, while further enhancing profitability.

Our Human Resources Services Business operates a distinctive model: we recruit aspiring network security engineers, train them with practical training through a proprietary development program leveraging SecuAvail Inc.'s extensive expertise, and subsequently dispatch them to client organizations. In the fiscal year ended March 2025, this segment generated revenue of ¥209 million, a 22.9% year-on-year increase, accounting for 18.2% of total revenue (up from 15.5% in the previous fiscal year).



Consolidated Performance Summary

We began providing security services to hospitals and other medical institutions in compliance with the Ministry of Health, Labour and Welfare's Guidelines for Medical Information Systems. In addition to establishing partnerships with major distributors, we expanded our services from public institutions such as government offices and universities into the medical sector—serving facilities ranging from Japan's leading hospitals to community healthcare clinics. However, progress fell short of expectations due to delays in negotiations for new service projects, postponements in implementation schedules, and contract terminations by certain existing clients.

(Unit: ￥million)

	March 31, 2024 (Actual)	March 31, 2025 (Forecast) ※	March 31, 2025 (Actual)	Year-on-year comparison		Forecast Achievement Rate
				Amount Change	Rate of Change	
Net sales	1,098	1,240	1,149	+50	+4.6%	92.7%
Network Security Business	928	–	939	+11	+1.2%	
Human Resources Services Business	170	–	209	+39	+23.0%	
Cost of sales	655	–	698	+42	+6.5%	
Gross profit	443	–	450	+7	+1.7%	
Selling, general and administrative expenses	475	–	415	△60	△12.7%	
Operating profit (loss)	△32	50	35	+67	–	70.2%
Operating profit margin	△3.0%	–	3.1%	–	+6.0pt	
Ordinary profit (loss)	△38	48	37	+75	–	77.8%
Net profit (loss) before income taxes	343	–	36	△307	△89.4%	
Net profit (loss) attributable to owners of the parent	228	33	42	△186	△81.3%	129.7%

※Earnings forecast released on May 15, 2024

Consolidated Earnings Forecast for the Fiscal Year Ending March 2026

We project consolidated net sales of ￥1,320 million, representing a 14.9% increase year-on-year. To achieve this growth, we plan to invest in talent acquisition and training, targeting operating profit of ￥109 million and ordinary profit of ￥109 million. Our key initiatives include strengthening partnerships to drive upselling and acquire new customers. In addition, we will focus on expanding sales and improving profitability through the enhanced rollout of services related to generative AI, which were planned and developed in the previous fiscal year.

（Unit: ￥million ）

	March 31, 2024 (Actual)	March 31, 2025 (Actual)	March 31, 2026 (Forecast)		
			Plan	Year-on-Year Change (Amount)	Year-on-Year Growth Rate
Net sales	1,098	1,149	**1,320**	＋170	＋14.9%
Operating profit (loss)	△32	35	**109**	＋73	＋210.8%
Operating profit margin	△3.0%	3.1%	**8.3%**	－	＋5.2pt
Ordinary profit (loss)	△38	37	**109**	＋71	＋192.4%
Net profit(loss) attributable to owners of the parent	228	42	**75**	+32	+76.9%

V . Growth Strategy

Medium-Term Business Plan

Earnings Forecast Update

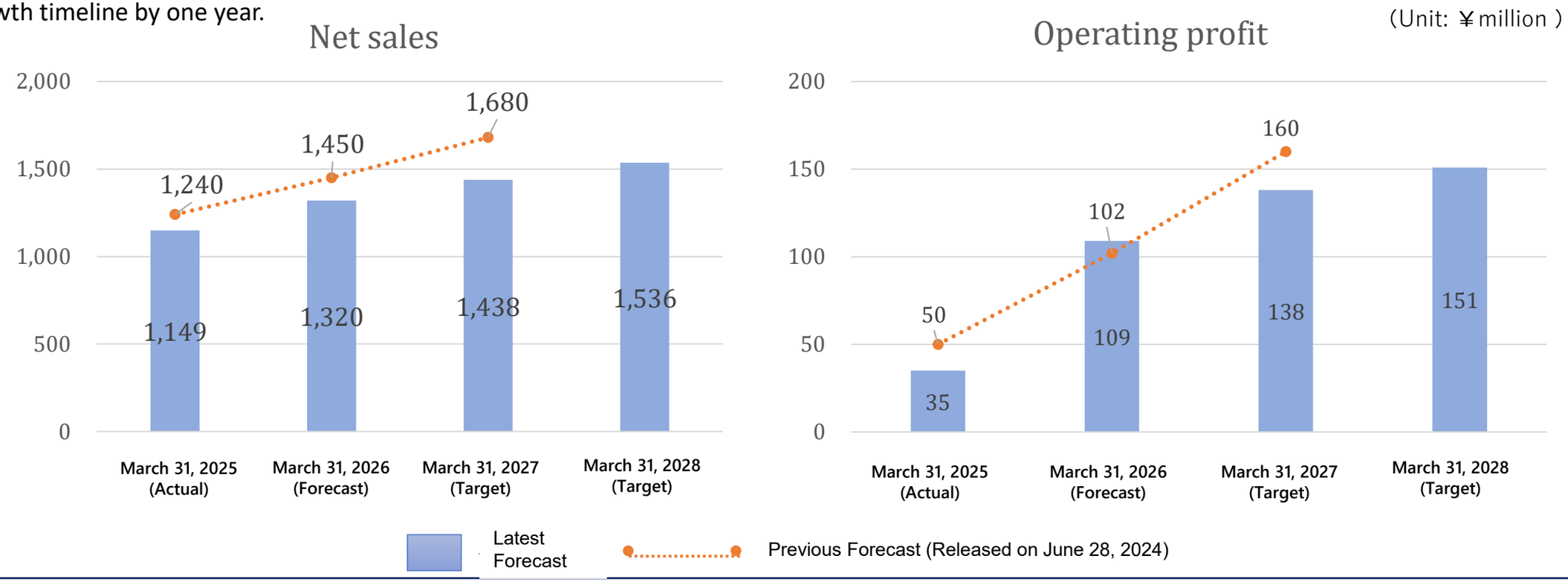
From the fiscal year ending March 2026 through March 2028, we aim to increase overall revenue scale by 16% while improving profitability. Our targets are as follows:

FY2027: Revenue of ¥1,438 million, operating profit of ¥138 million, and ordinary profit of ¥138 million

FY2028: Revenue of ¥1,536 million, operating profit of ¥151 million, and ordinary profit of ¥151 million

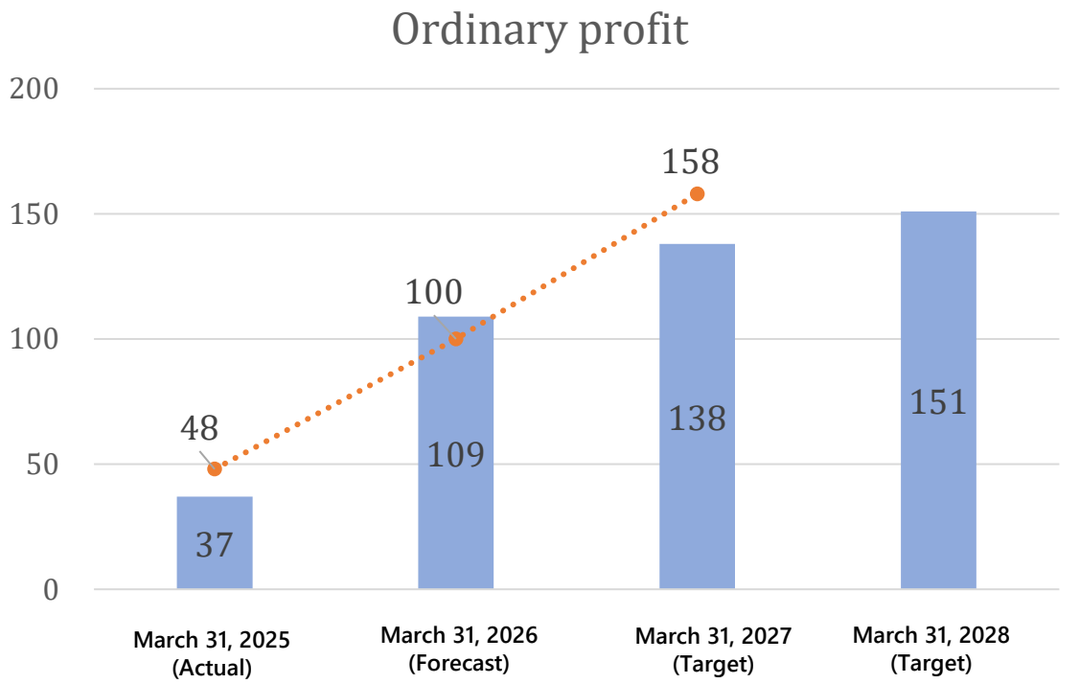
Update from Previous Disclosure (June 28, 2024) Due to delays in client negotiations and service implementation, actual revenue for FY2025 came in at ¥1,149 million, falling short of the previously forecasted ¥1,240 million. In response, we have revised the revenue plan downward by shifting the growth timeline by one year.

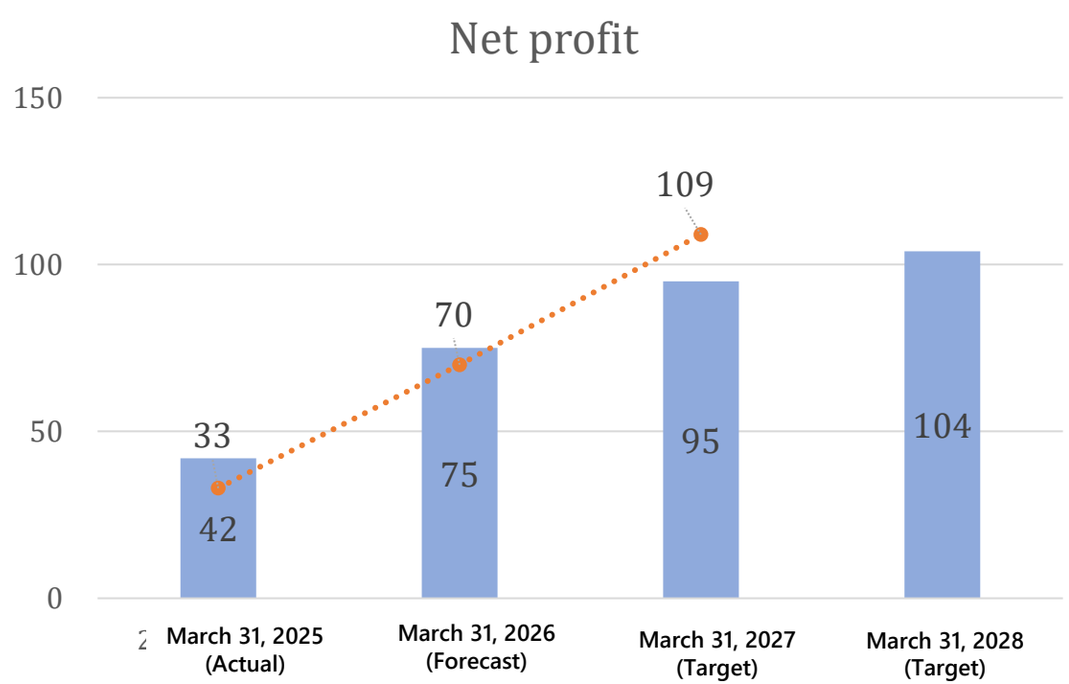
(Unit: ¥million)



Medium-Term Business Plan

(Unit: ￥million)





Latest Forecast

Previous Forecast (Released on June 28, 2024)

Note : The above figures do not include non-operating income/losses or extraordinary gains/losses.

Key Growth Strategies

1. Strategic Partnerships

●Deepening Relationships with Existing Partners
- Partner enablement and content expansion
- Planning and development of customized services for partners

●Acquisition of New Partners
- Planning and hosting webinars and seminars for partners
- Participation in trade shows and industry events
- Planning and joint development of new services targeting specific industries (Key focus areas: Healthcare, Manufacturing (OT/IoT))

2. Sales Strategy

- Strengthening organizational capabilities to drive new customer acquisition and deepen existing relationships
- Expansion of partner-focused sales team (additional 2–3 personnel)
- Enhancement of inside sales activities through the expansion of the Okinawa Customer Service Center

Key Growth Strategies

3． Product & Service Strategy

- Enhancing the value-added features of our services
- Expanding product and service lineups tailored to specific market segments (e.g., “NetStare Series,” “LogStare Series”)

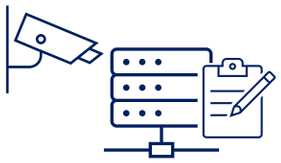
（1）「NetStare for Medical」

This is a security operations center (SOC) service specializing in cybersecurity measures for medical institutions such as hospitals. It addresses critical challenges faced by hospitals—including supply chain attacks and ransomware threats, which have become increasingly severe in recent years. Hospitals can choose from five service options based on their size, budget, and specific security needs.

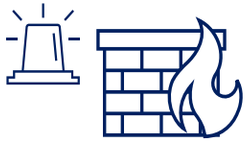
(2)「NetStare for OT/IoT」

In recent years, cyberattacks targeting the automotive industry have become increasingly severe. NetStare for OT/IoT is a specialized Security Operations Center (SOC) service designed to protect the automotive supply chain from such threats.

7 Cybersecurity Solutions Lineup

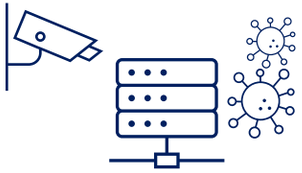


Network Monitoring and Log Management



Network Perimeter Defense

UTM MSS

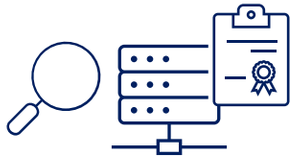


Insider Threat Monitoring

Ransomware Detection

VPN Connectivity and Vulnerability Management

Microsoft 365 Log Management



Security Assessment

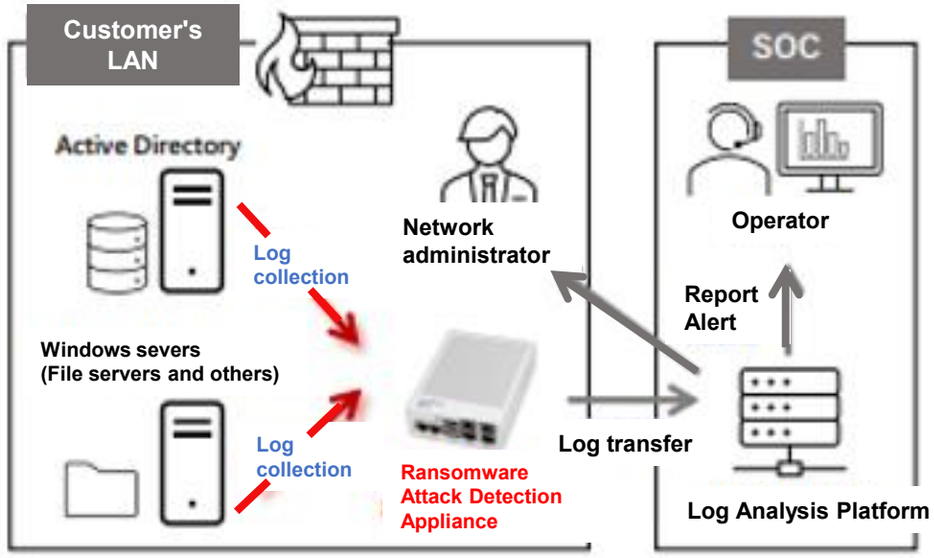
(3)「Ransomware Attack Detection Appliance」

This compact, agentless appliance monitors audit logs from Windows servers such as Active Directory and file servers. Using proprietary detection logic, it identifies ransomware infiltration and dormancy at an early stage, helping prevent damage escalation.

As an agentless solution that requires no dedicated servers or OS procurement, it can be deployed quickly with minimal impact on existing environments. Simply install it, and ransomware protection is in place.

Installation examples

By simply installing aExamples of equipment installation compact appliance in the customer's environment, log collection can begin without deploying agents—ensuring zero impact on existing systems.All collected logs are securely transmitted to SecurAvail's 24/7 Security Operation Center (SOC), where they are continuously monitored and analyzed by security engineers. In the event of a ransomware detection, clients can consult directly with SecuAvail's SOC for expert response and support.



Key Growth Strategies

LogStare

(1) Cloud Compatibility

LogStare × M365 Box Google

As cloud-first and cloud-native strategies become mainstream, more companies are adopting public cloud services such as Box and Microsoft 365. However, the move to multi-cloud environments often results in fragmented management tools and more complex operations, creating challenges for IT teams.LogStare solves these issues with advanced log analysis that strengthens the security of diverse cloud services, helping IT administrators manage and protect their cloud environments more efficiently.

LogStare Recognized as an Ecosystem Solution for Box
LogStare has been officially recognized as an ecosystem solution for Box, the leading content cloud platform. Through seamless integration with Box, LogStare enables organizations to detect unauthorized access, prevent data leaks caused by misconfigured file sharing settings, and strengthen overall IT security and governance. As an ecosystem solution, LogStare benefits from unlimited API calls when connected to Box. This allows enterprises to fully leverage Box—even in environments where large volumes of event logs are generated—without incurring additional costs, ensuring scalable and cost-effective log analysis.

(2) Generative AI

LogStare × Generative AI

LogStare Integrates Generative AI for Enhanced Log Analysis
Building on its core strengths in automated log collection, normalization, and report generation, LogStare now incorporates generative AI to deliver deeper insights from log reports. This innovation significantly boosts the efficiency and effectiveness of Security Operation Center (SOC) activities, empowering organizations to make faster, more informed decisions.

Key Growth Strategies

4. M&A and Investment Strategy	Accelerating growth through potential M&A and investments in companies with expected business synergies, particularly in the field of network security. *(Note: There are currently no specific M&A or investment deals under consideration.)*
5. Investor Relations Strategy	・Enhancing the content and functionality of our corporate website. ・Strengthening information dissemination related to our group's business activities, including the release of new products and services.

Ⅳ.Risk Factors

Recognized Risks

Risks That May Affect Our Future Growth and Execution of Business Plans

Overview of Key Risks	Likelihood	Timing	Impact	Change in Significance from Previous Year	Our Response Policy
Information Management	Low	Unknown	High	No Change	Our internal systems are protected by multiple layers of security, including firewalls, antivirus software, and email filtering systems, ensuring a high level of reliability in our cybersecurity framework.Key servers operate in a multi-unit configuration and are housed in fault-tolerant data centers that are strictly managed, equipped with uninterrupted power supply, and designed to enable rapid recovery in the event of an incident or system failure. Furthermore, our group has implemented robust measures to prevent information leakage. This includes the execution of individual non-disclosure agreements (NDAs) with all officers and employees upon both joining and leaving the company.
System Failure	Medium	Unknown	High	No Change	To prepare for potential system failures, we provide services and implement technical measures within intelligent buildings that feature advanced earthquake resistance, fire protection, and water leakage prevention systems, as well as on-site emergency power generation capabilities.
Competition	Medium	Medium to Long Term	Unknown	No Change	We are committed to medium- to long-term investment in the development of new products and services by integrating our core business resources with emerging technological innovations.

Note: The above is an excerpt from the “Business Risks” section of the Securities Report. For further details, please refer to the full “Business Risks” disclosure in the Securities Report.

Important Notice Regarding This Document

This document contains forward-looking statements, including projections, future plans, and performance targets related to our corporate group. These statements are based on assumptions made at the time of preparation and are subject to change due to various factors. Actual results may differ materially from the forecasts presented herein.

The next disclosure of “Business Plans and Growth Potential” is scheduled for June 2026.

Visualization of network security - SECurity for the futURE -

SecuAvail