



GLOBAL
SECURITY
EXPERTS

**Financial Results Presentation for the
Fiscal Year Ended March 31, 2026**

**Global Security Experts, Inc., Securities Code: 4417
April 2026**

1	FYE3/2026 Full Year Summary	Page 3
2	Growth Strategy in an Age of Rising AI	Page 4
3	FYE3/2026 Financial Results Overview	Page 11
4	FYE3/2027 Consolidated Performance Forecast	Page 20
5	Shareholder Return	Page 23
6	Medium-Term Business Plan and Growth Strategy	Page 26
7	ESG Initiatives	Page 39
8	Appendix	Page 41

Business performance also grew steadily for FYE3/2026

Consolidated net sales

YoY

+25.2%

11,022.08

million yen

Consolidated operating income

YoY

+38.6%

2,238.05

million yen

Operating income margin

YoY

+2.0 percentage points

20.3%

- ✓ **Record high values** for both net sales and profit
Achieved the sales growth rate +25% target as planned in the medium-term management plan
- ✓ While recognizing increased costs due to expanding operations, **operating income is +38.6% YoY**
- ✓ Improvement in the gross profit margin due to AI utilization in each business also contributed to this increase, with the operating income margin increased by 2.0 points YoY, **and growth continues for the 8th consecutive year**

GSX

GLOBAL
SECURITY
EXPERTS

Growth Strategy in an Age of Rising AI

Structural Reasons Why the Rise of AI Is Increasing Security Needs and How This Impacts GSX's Business

As the evolution of AI further tilts the balance in favor of cyberattackers, simply introducing AI tools is not enough to defend against cyberattacks

In addition to existing security risks, companies now face new risks associated with the adoption of AI, making them even more dependent on external specialists

The rise of AI is therefore a structural driver of growth for GSX

Cyberattackers are already using AI tools, leaving them constantly ahead



Security needs expand as AI adoption advances



- Cyberattackers also use AI
AI facilitates the automation, intensification, and increased sophistication of attacks
- Security measures **cannot be replaced** by AI tools alone

**Security
needs surge
with the rise
of AI**

Misuse of AI
etc...



Risk of information
leakage

Gaps in
governance

Semi-large and medium-sized companies, SMEs

- **New security risks emerge** in association with the adoption of AI (AI misuse, information leakage, gaps in governance, etc.)
- Difficulty involved in safely selecting, operating, interpreting, and controlling AI **increases reliance on external specialists**

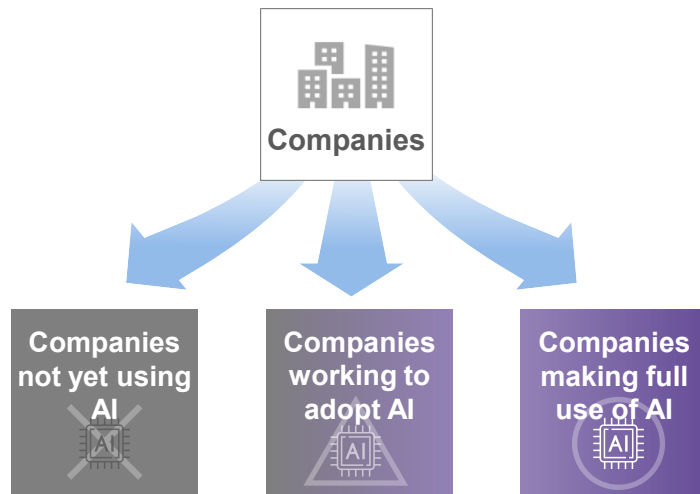
The rise of AI is not a threat;
it is a powerful tailwind for GSX's business

GSX's Vision for Strategy in the AI Era

In GSX's customer market, disparities are expected to emerge between companies in how they respond to the rapid evolution of AI

GSX is evolving by adapting the strengths of its existing businesses to the AI era
GSX provides AI-era security services tailored to the specific needs of all companies

GSX Group's response to changes in its customer market



Disparities between those companies that are advancing AI adoption without major difficulty and those that are not

GSX

Lineup of services to support companies in every condition

GSX Group's strengths

Cybersecurity Business

Customer base centered on semi-large and medium-sized companies and SMEs

Security Training Business

Expertise and track record in educational course development and certification in specialized fields

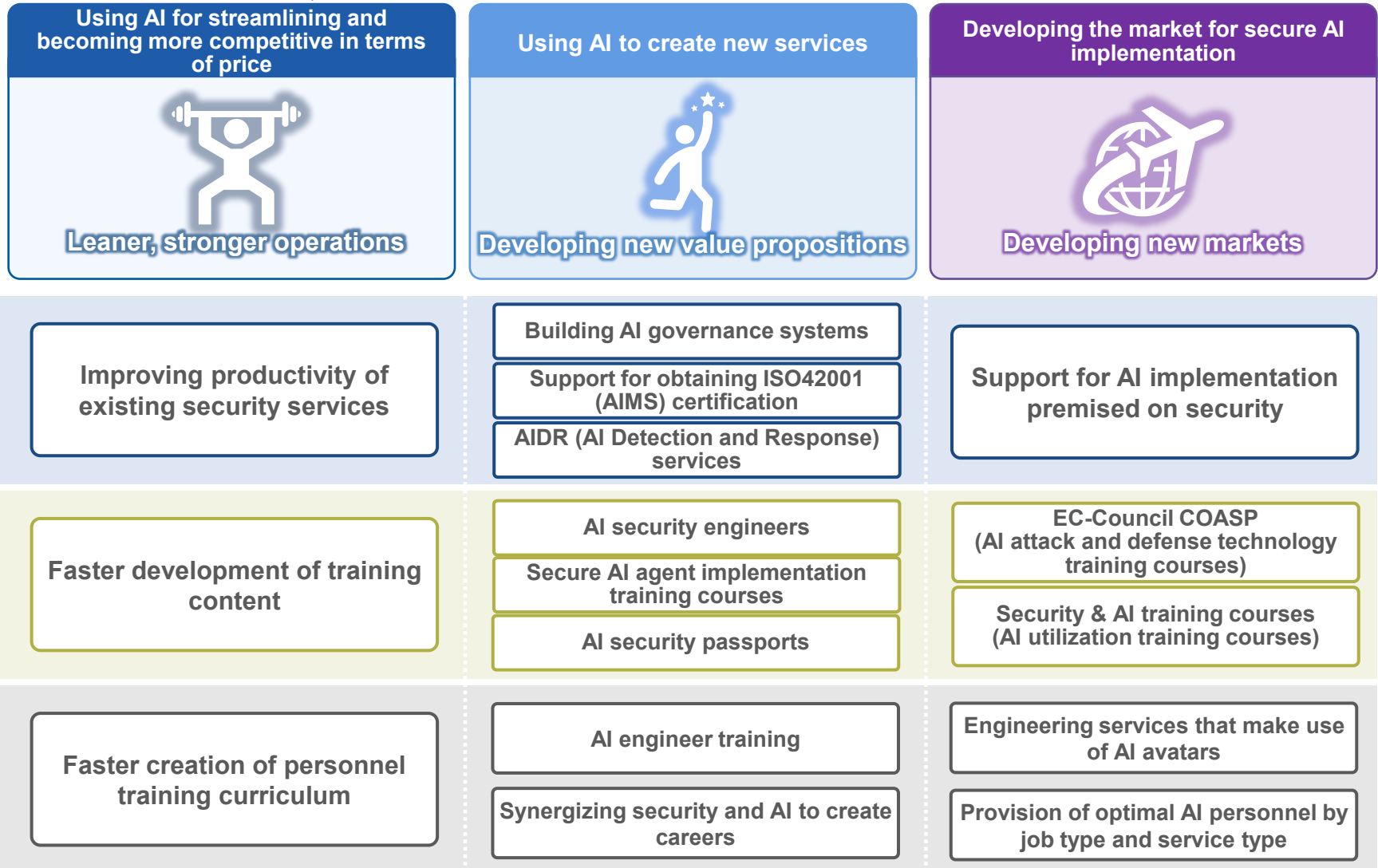
Security Personnel Business (CyberSTAR)

Unique business model to train, increase the pool of, and provide specialized personnel

Evolving by adapting GSX Group's strengths to the AI era
Expand the market GSX can serve

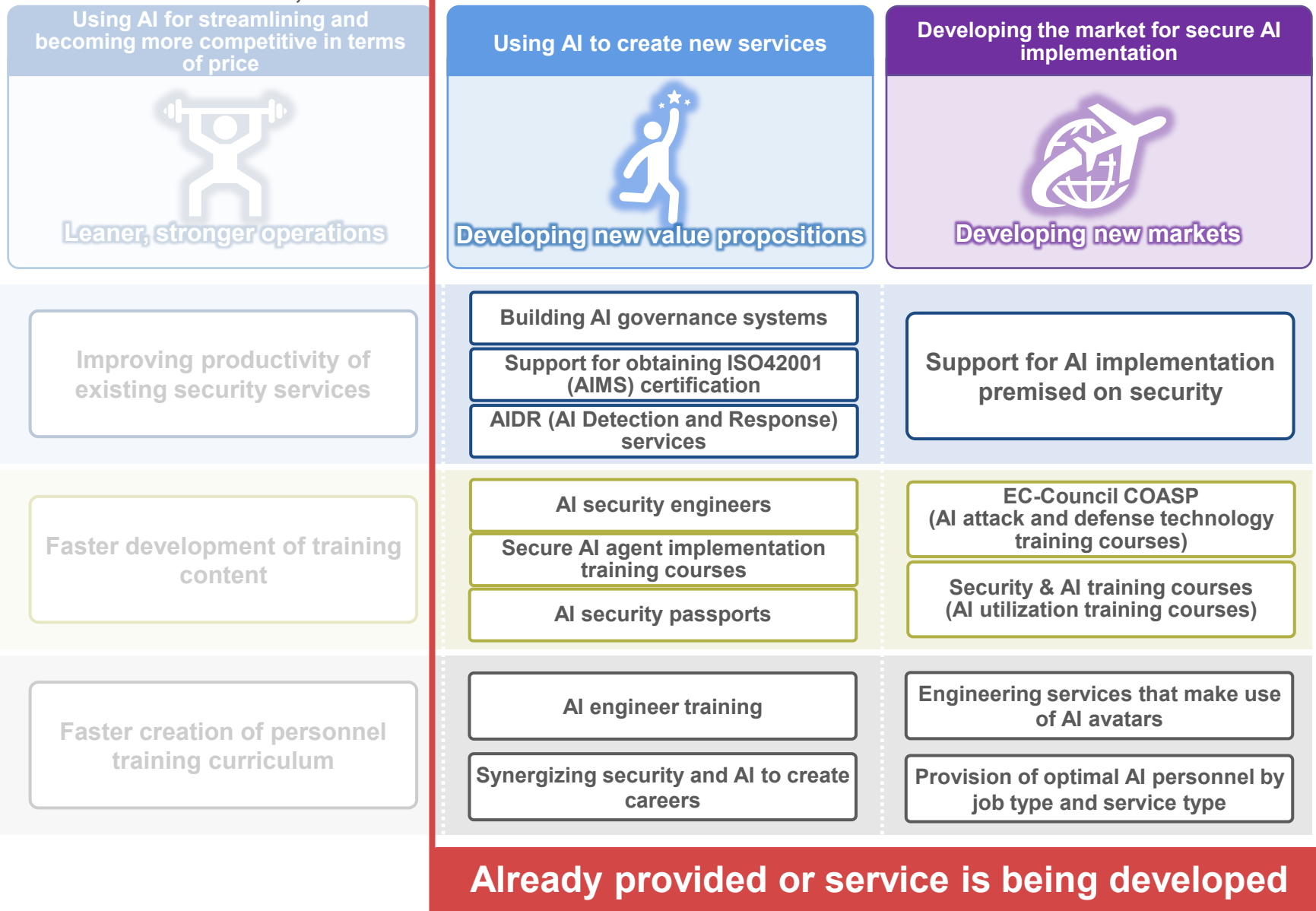
Providing Services Adapted to the AI Era

Advancing initiatives in each business that start with internal streamlining and extend to the creation of AI-powered services, entry into new AI businesses, and more



Providing Services Adapted to the AI Era

Advancing initiatives in each business that start with internal streamlining and extend to the creation of AI-powered services, entry into new AI businesses, and more



Cybersecurity Business



Launching new service "Security Document Assessment" that combines AI and consulting

Overview

Collaborating with Segue Security Co., Ltd., to integrate the Company's consulting expertise with RiskLoom, an AI-powered services for assessing security policy documents provided by Segue Security

Provided value

- Synergizing AI and consulting expertise to streamline document **gap analysis** of security policies
- Visualizing compliance with 11 types of guidelines, such as supply chain evaluation systems

Benefits of AI adoption

Shortening the diagnostics period to **approximately one-third** of its previous duration / Preventing omissions through **comprehensive checks of all items** using AI / Supporting **11 types of standards** (such as ISMS) to allow for broad-based assessment / Consultants then **focus their expertise on scrutinizing analysis results and determining response priority**



Developing SecOps.AI, an integrated AI tool for security operations — Development of key functions is completed, and the tool is now in the fine-tuning phase

Overview

Developed as a tool for using AI to provide integrated support for overall security operations. Integrated automation of the entire process, from detection and analysis using monitoring products through report creation

Main functions

- Automatic generation of AI analysis reports: Completing the process from incident detection → report creation in just a few minutes
- MCP integration: Collecting and reasoning in real time through process tree analysis, threat intelligence acquisition, and behavioral correlation analysis

Benefits of AI adoption

Reducing security operation work-hours by **approximately 50% (actual result)** / Eliminating reliance on specific individual personnel and **standardizing analysis quality** / Achieving RAG that **continuously improves accuracy** by accumulating, vectorizing, and reusing analysis results



Transformation of log analytics operations

Overview

Increasing the sophistication of and automating the process from log analysis to report creation, transforming operations that conventionally relied on human labor

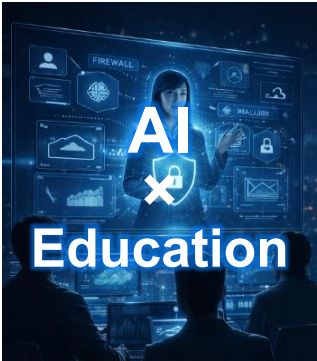
Main functions

- Training AI on the expertise of experienced analysts and systematizing analysis logic
- AI performs the process from log analysis to report drafting, **rapidly generating highly accurate and multifaceted digital reports**
- A separate AI checks deliverables, **ensuring that quality is consistent and building a feedback loop**

Benefits of AI adoption

Substantially reducing work-hours for and accelerating analysis and reporting operations / **Standardizing quality** by eliminating reliance on specific individual personnel / **Two-stage quality assurance:** both human checks and AI review

Security Training Business



Release of multiple new AI-related training courses	
Training course example	AI security engineers: Training course for learning technologies that enable participants not only to use AI, but also to safely design systems that incorporate AI
	Secure AI agent implementation training course: Training course for learning technologies that enable participants to securely develop AI agents
	AI security passports: Training course for acquiring the knowledge needed to safely leverage AI
	EC-Council COASP: Security (Red Team) training course for hands-on learning of how AI is attacked and the technologies used to defend against such attacks

Security Personnel Business



Building a model for developing training materials that is systematized with AI	
Issues before AI adoption	• Creating training materials was time-consuming • Fixed content that resisted updating • Case-by-case optimization was difficult
Measures taken	AI used across all stages (defining requirements → generating training materials → refining expressions → review) to generate high-quality on-demand training materials
Effects	Increased speed and quality / Process uniquely optimized for each case / Expanded the pool of personnel who can be proposed / Improved the order placement rate

GSX

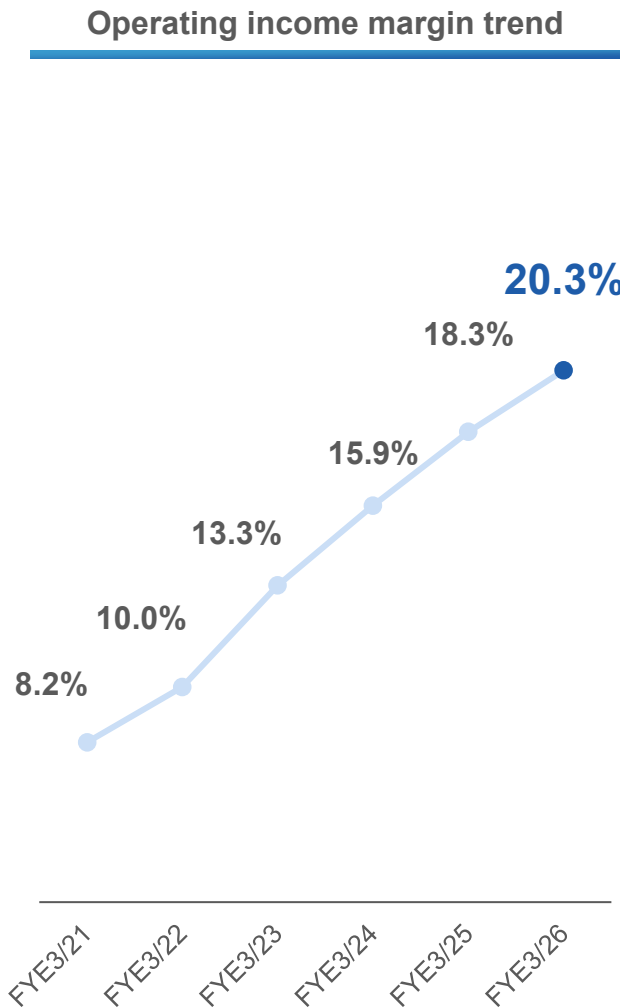
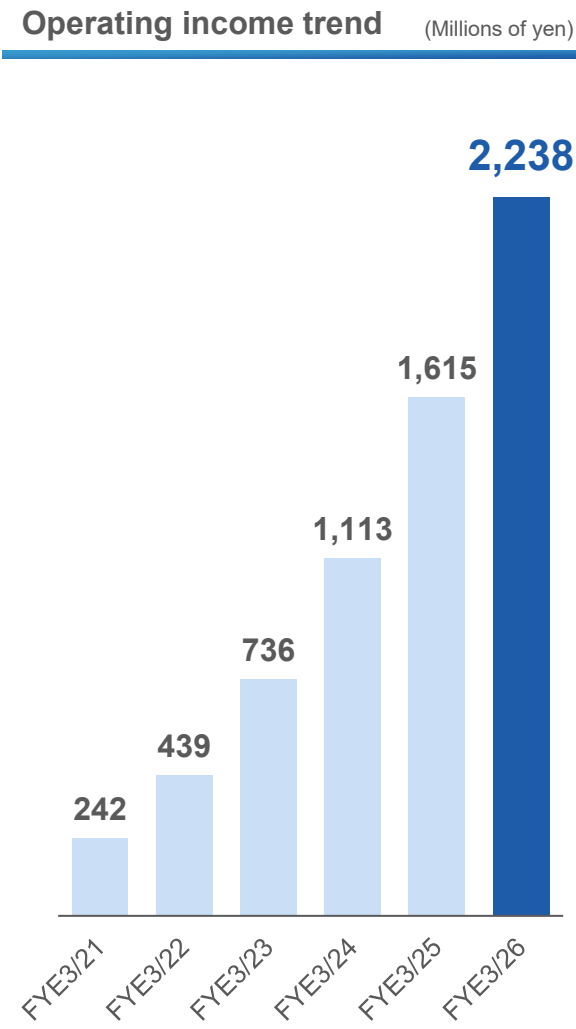
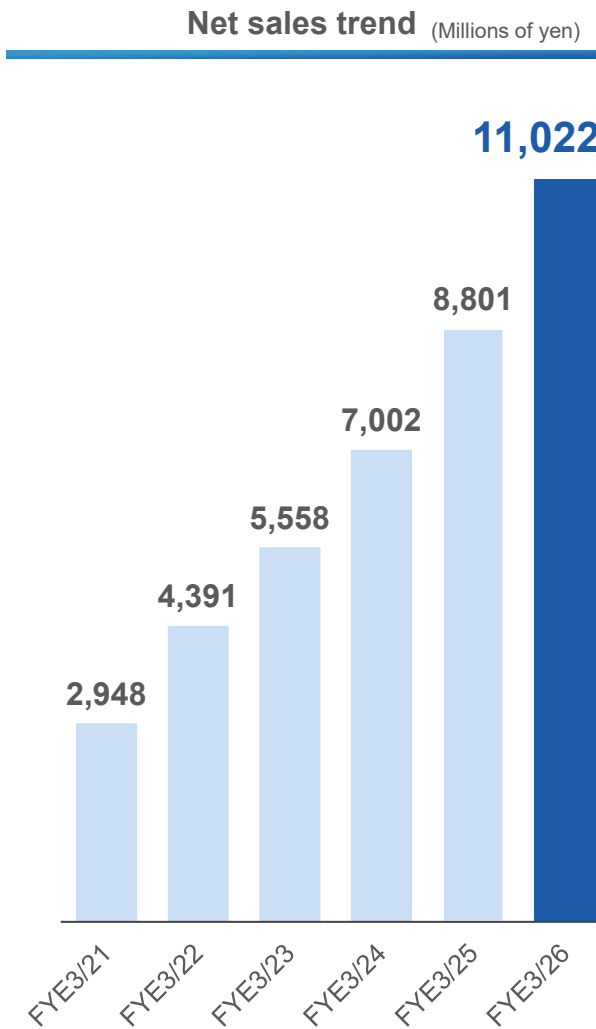
GLOBAL
SECURITY
EXPERTS

FYE3/2026 Financial Results Overview

Full-Year Performance Trends

The top line expanded in a stable manner and there was rapid growth of profit that exceeded this

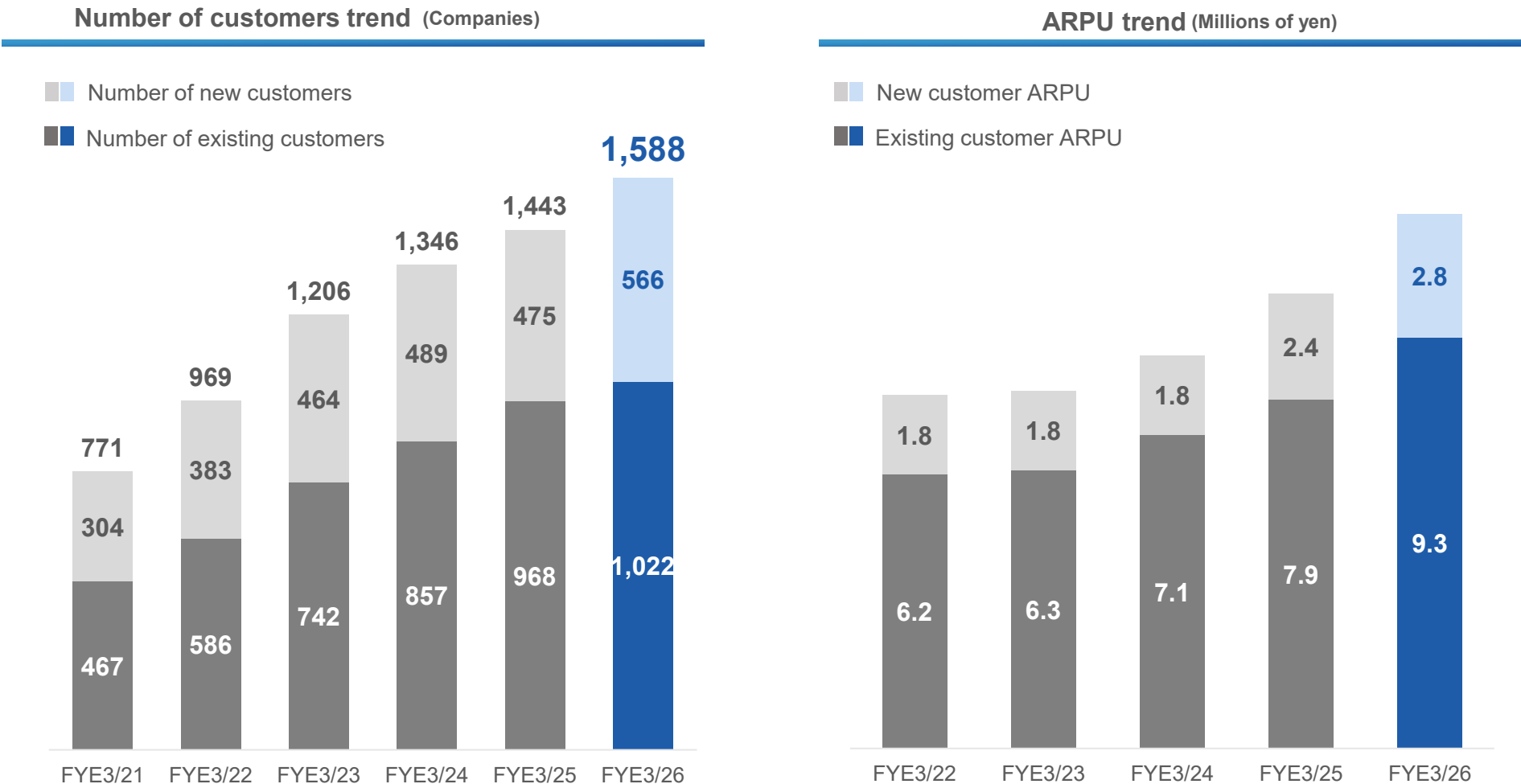
Achieved management with a highly profitable structure



Number of Customers & ARPU Trends

Both the number of new customers and the number of existing customers increased steadily

In the fiscal year ended March 31, 2026, ARPU increased significantly due to the effects of up-selling and cross-selling, as well as the acquisition of projects involving a greater proportion of semi-large companies among the customer mix of semi-large and medium-sized companies and SMEs



*Figures prior to FYE3/21 are for reference only

Consolidated Net Sales & Gross Profit Composition

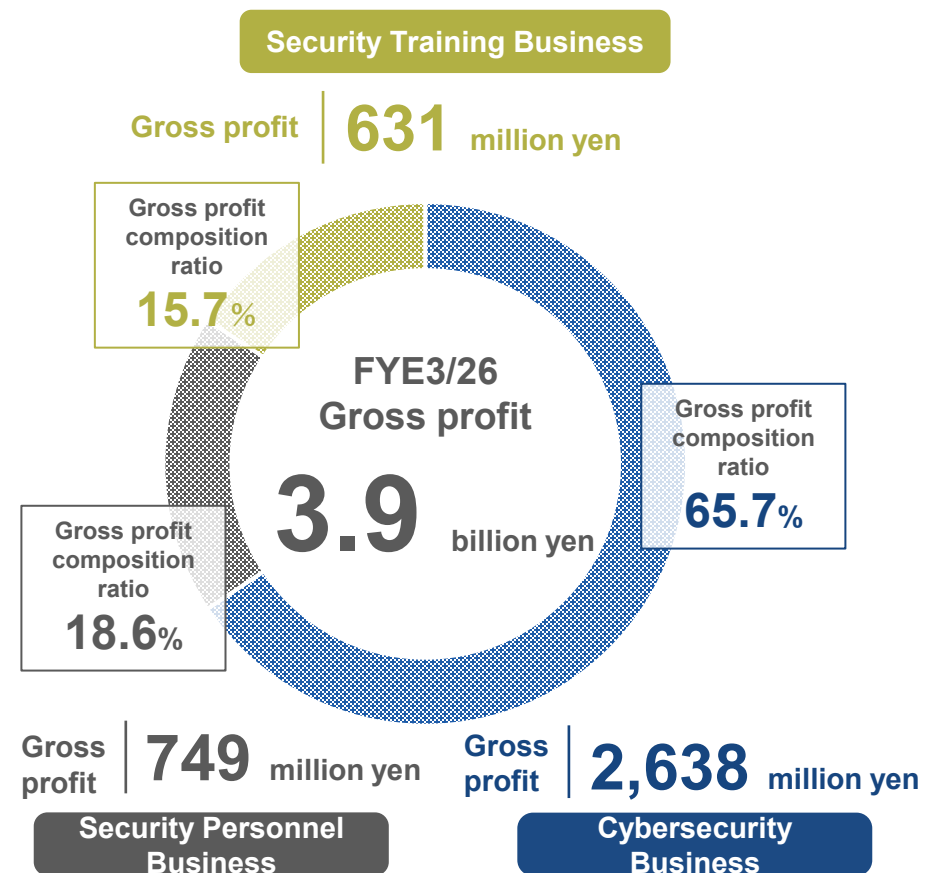
The composition ratio for FYE3/2026 is as planned

These figures consist of the security training business and security personnel business that are growing rapidly, based on stable profit from the cybersecurity business

Net sales composition ratio



Gross profit composition ratio



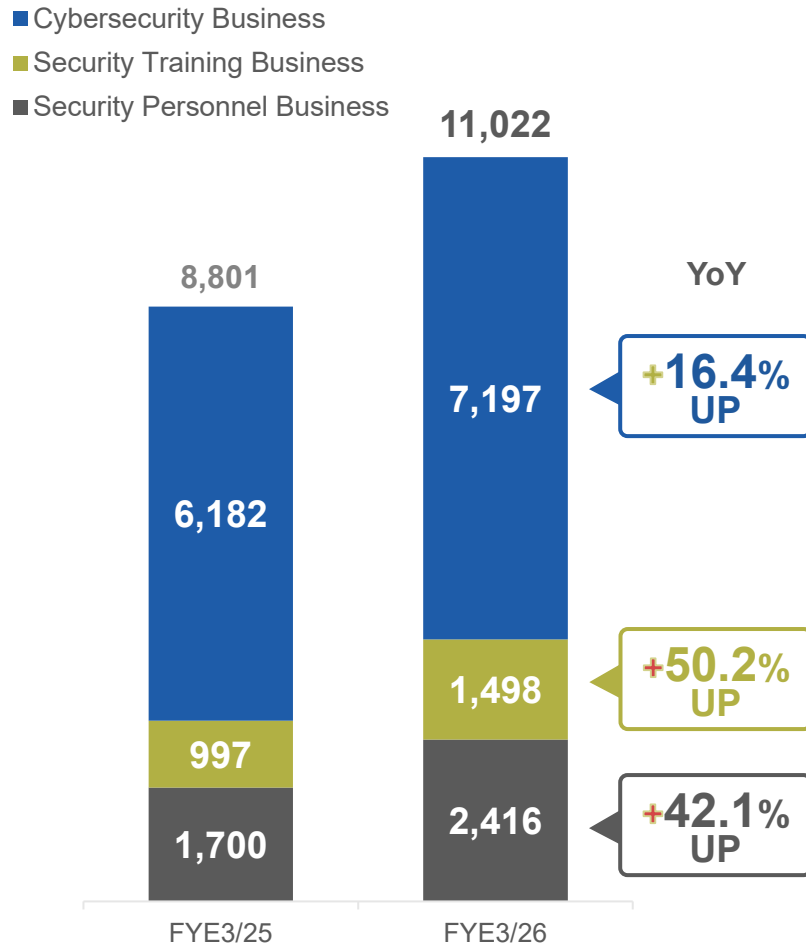
*Amounts for net sales by business segment are prior to elimination of internal transactions

Net Sales & Gross Profit by Business YoY (Full-Year Cumulative)

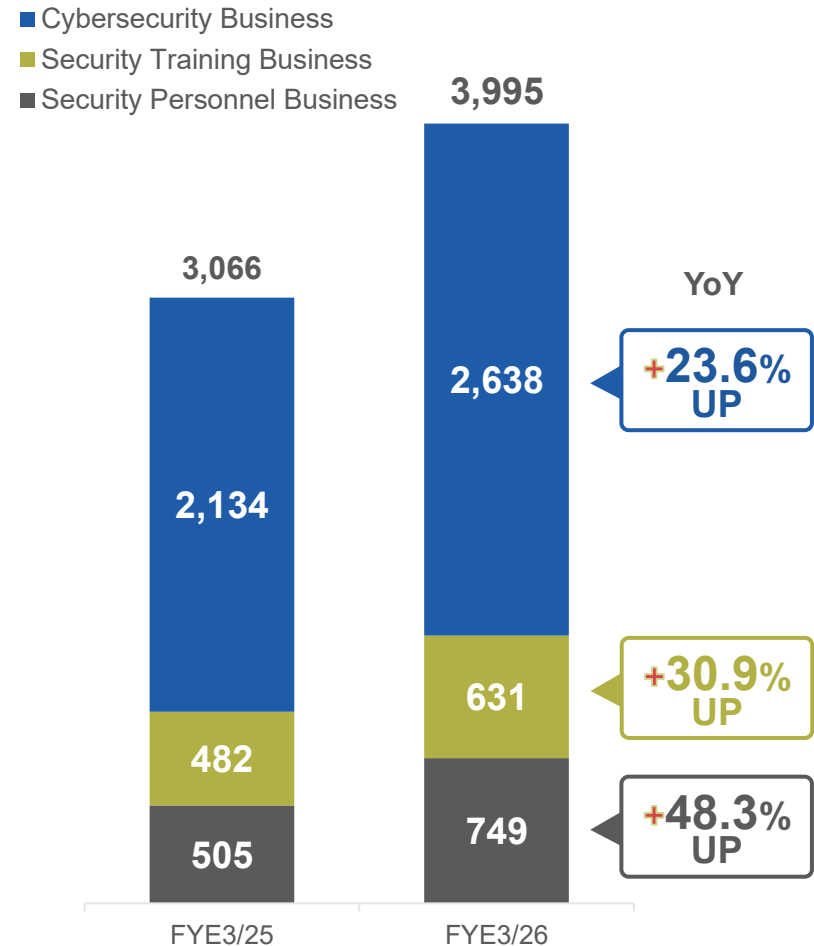
Both net sales and gross profit increased

The security training business and security personnel business are making great progress

Net sales (Millions of yen)



Gross profit (Millions of yen)



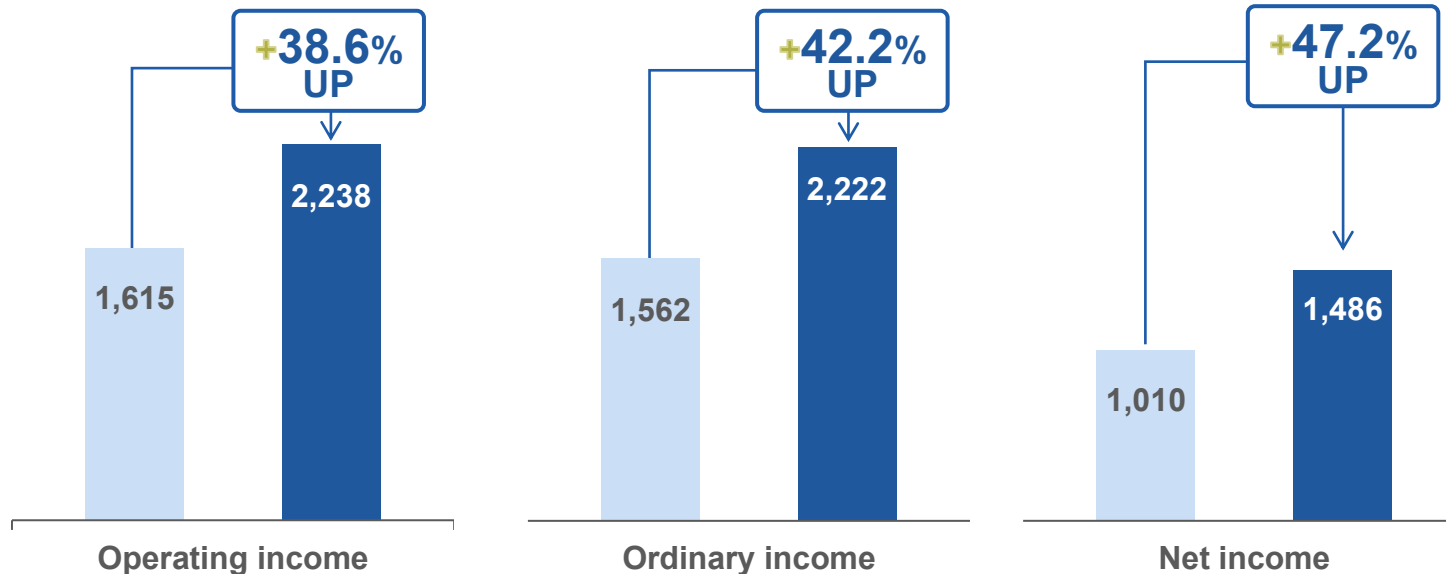
*Amounts for net sales by business segment are prior to elimination of internal transactions

Impact on Ordinary Income and Net Income

Shift to consolidated accounting from FYE3/2025: Reflects profit and loss for the equity-method affiliates BroadBand Security, Inc. and Secure Innovation Inc.

Growth rate of profit against previous year (Millions of yen)

■ FYE3/2025
■ FYE3/2026



| Impact on ordinary income

- Share of loss of entities accounted for using equity method: 1.7 million yen *Mainly due to the impact of Broadband Security (June settlement)
- Interest expenses: 19 million yen
- Non-operating income: 15 million yen (interest income: 2 million yen, subsidies: 7 million yen)

| Impact on net income

- Loss on change in equity: 10 million yen (mainly due to changes in equity resulting from the exercise of stock options by Broadband Security)
- Loss on valuation of investment securities: 2 million yen (due to review of value of unlisted stocks)

Consolidated Profit and Loss (Cumulative)

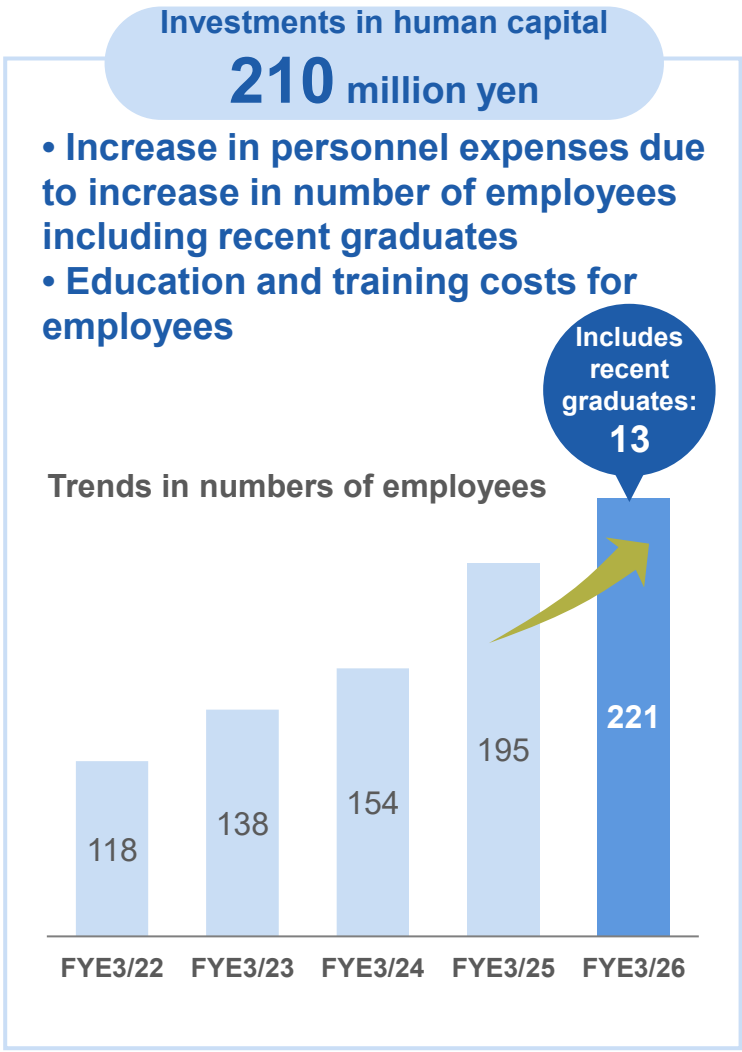
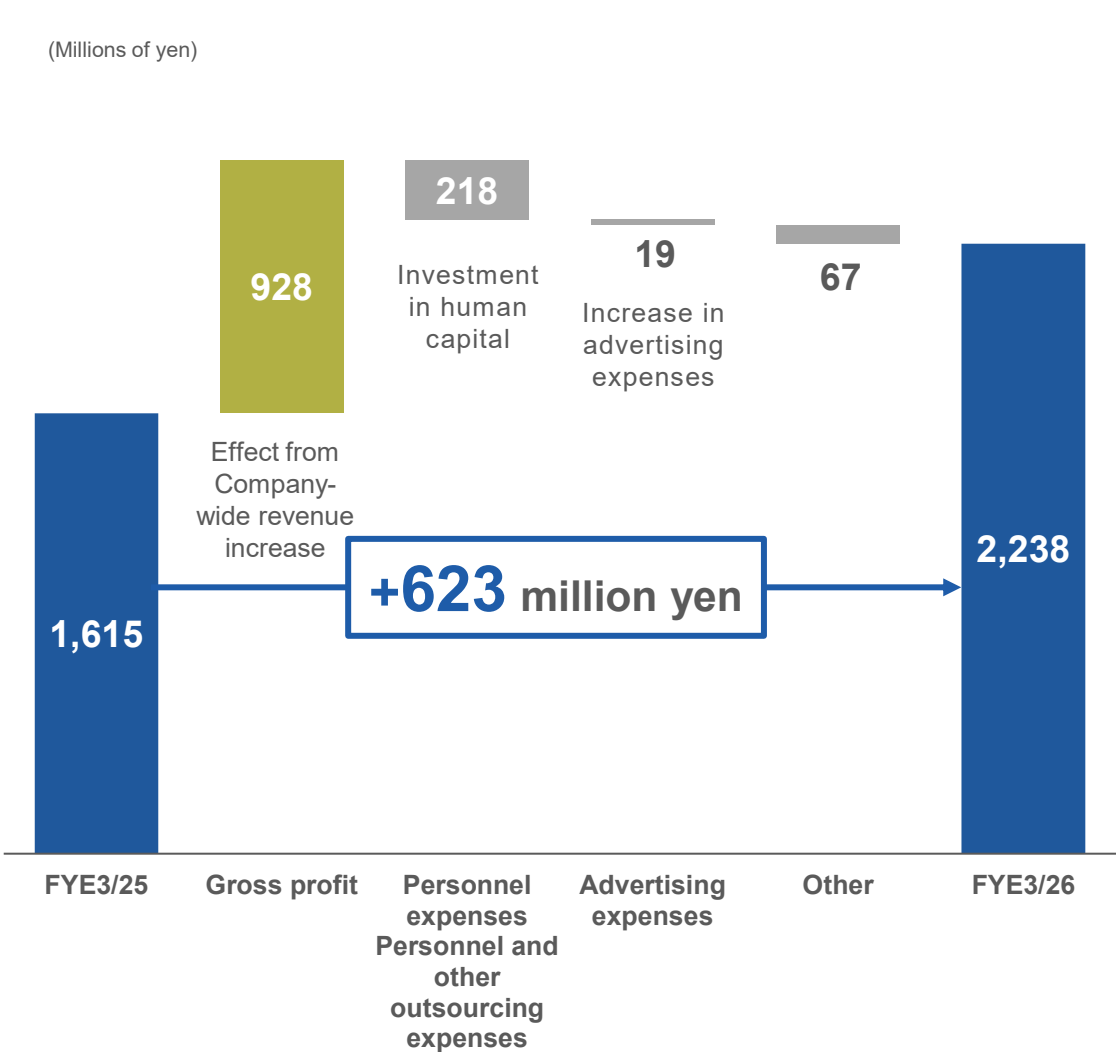
(Millions of yen)	FYE3/2025 Results	FYE3/2026 Results	YoY Change	YoY Change (%)
Net sales	8,801	11,022	+2,220	+25.2%
Gross profit	3,066	3,995	+928	+30.3%
Gross profit margin	34.8%	36.2%	+1.4 percentage points	-
Selling, general, and administrative expenses	1,451	1,757	305	+21.1%
Selling, general, and administrative expense ratio	16.5%	15.9%	-0.5 percentage points	-
Operating income	1,615	2,238	+623	+38.6%
Operating income margin	18.3%	20.3%	+2.0 percentage points	-
Ordinary income	1,562	2,222	+659	+42.2%
Ordinary income margin	17.8%	20.2%	+2.4 percentage points	-
Net income	1,010	1,486	+476	+47.2%
Earnings per share (EPS, yen)	67.24	98.85	+31.61	-

*The Company conducted a 2-for-1 split of shares of common stock on June 1, 2025.

Earnings per share information is calculated based on the assumption that the stock split was conducted at the beginning of the previous consolidated fiscal year.

Operating Income Change Analysis (Cumulative)

Operating profit increased +623 million yen year on year due to growth that exceeded proactive investment in human capital



Consolidated Balance Sheet

(Millions of yen)	FYE3/2025	FYE3/2026	YoY Change	YoY Change (%)
Current assets	4,799	6,344	+1,545	+32.2%
Cash and deposits	1,385	1,644	+258	+18.7%
Accounts receivable - trade, and contract assets	2,149	2,749	+599	+27.9%
Other	1,264	1,950	+686	+54.3%
Non-current assets	3,341	3,614	+273	+8.2%
Property, plant and equipment	276	250	-26	-9.5%
Intangible assets	98	114	+16	+16.8%
Investments and other assets	2,966	3,249	+282	+9.5%
Total assets	8,141	9,959	+1,818	+22.3%
Current liabilities	3,630	4,280	+649	+17.9%
Accounts payable - trade	430	512	+81	+19.0%
Short-term borrowings	400	300	-100	-25.0%
Current portion of long-term borrowings	219	217	-2	-1.1%
Other current liabilities	2,580	3,250	+670	+26.0%
Non-current liabilities	1,431	1,277	-153	-10.7%
Long-term borrowings	1,308	1,091	-217	-16.6%
Other non-current liabilities	123	186	+63	+51.6%
Net assets	3,078	4,401	+1,322	+42.9%
Equity-to-asset ratio	37.8%	44.2%	+6.4 percentage points	—

GSX

GLOBAL
SECURITY
EXPERTS

FYE3/2027 Consolidated Performance Forecast

Basic Policy

Continue to expand net sales and strengthen the management base to support medium- to long-term growth by placing importance on improving profit margins

Aim for consolidated net sales of +25% YoY and an operating income margin of 21.3%

(Millions of yen)	FYE3/2026 Results	FYE3/2027 Forecast	Change	Change (%)
Net sales	11,022	13,778	2,756	+25.0%
Operating income	2,238	2,939	703	+31.3%
Operating income margin	20.3%	21.3%	+1.0 percentage point	-
Ordinary income	2,222	2,973	756	+33.8%
Ordinary income margin	20.2%	21.6%	+1.5 percentage points	-
Net income	1,486	1,998	512	+34.4%
Earnings per share (EPS, yen) *	98.85	132.74	33.89	-

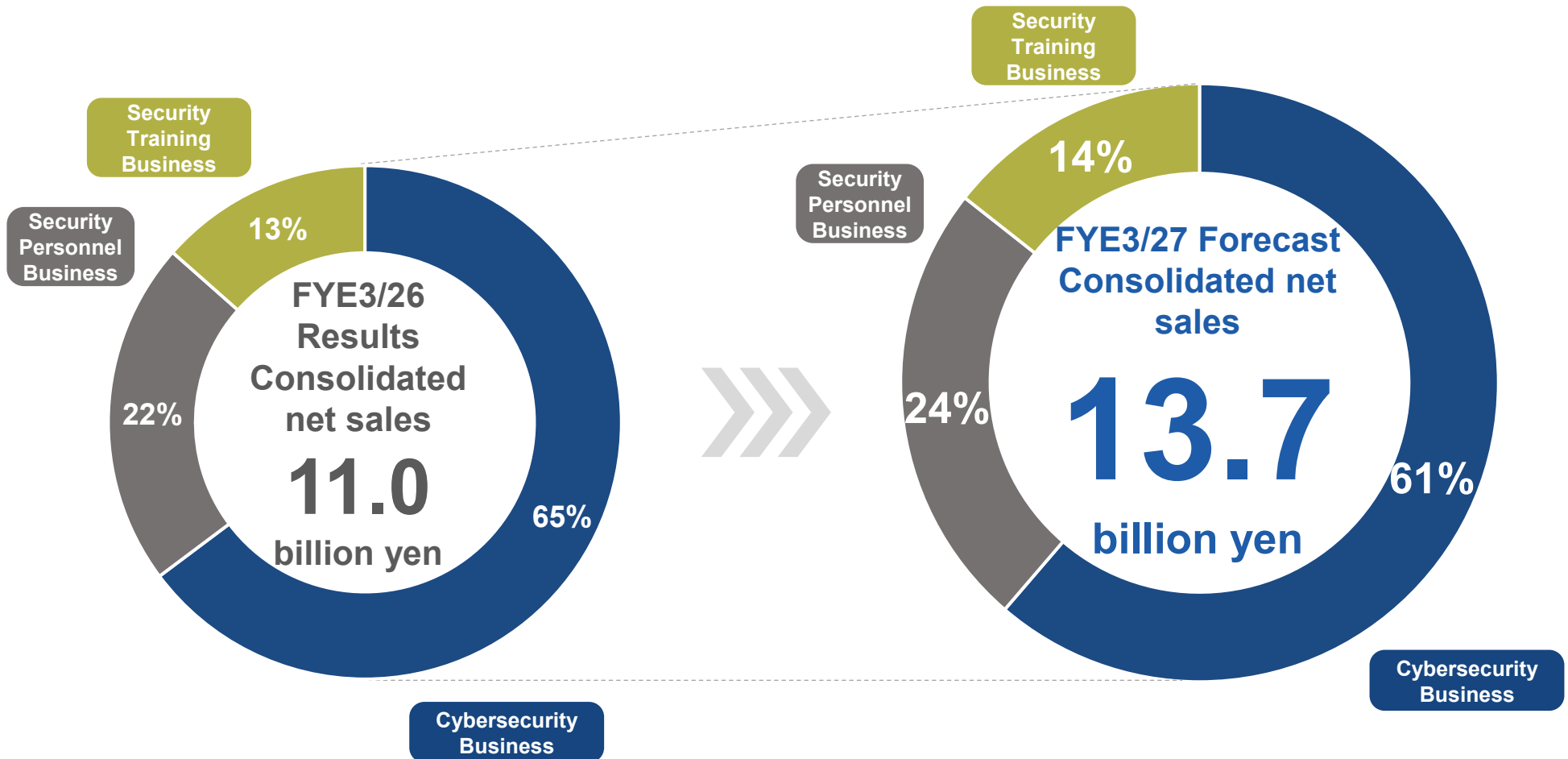
*The Company conducted a 2-for-1 split of shares of common stock on June 1, 2025.

Earnings per share information is calculated based on the assumption that the stock split was conducted at the beginning of the previous consolidated fiscal year.

FYE3/2027 Forecast of Consolidated Net Sales Composition

The cybersecurity business is experiencing stable growth while the security training business and security personnel business are making progress

All businesses are expected to increase their revenue compared to the previous year



GSX

GLOBAL
SECURITY
EXPERTS

Shareholder Return

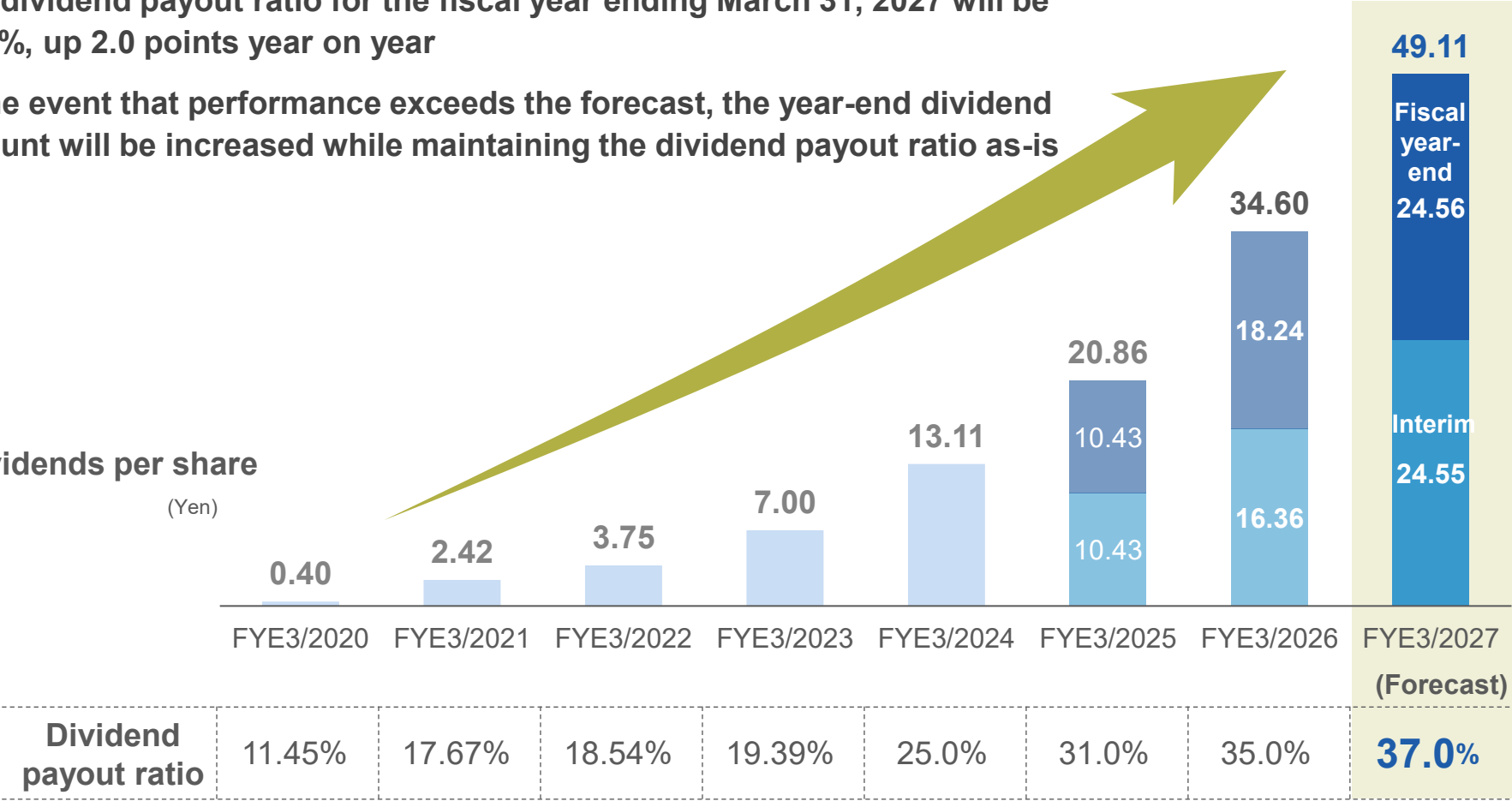
Information About Dividends

In the fiscal year ended March 31, 2026, the year-end dividend amount was increased to 1.87 yen more than previously forecast

The dividend payout ratio for the fiscal year ending March 31, 2027 will be 37.0%, up 2.0 points year on year

In the event that performance exceeds the forecast, the year-end dividend amount will be increased while maintaining the dividend payout ratio as-is

Dividends per share
(Yen)



Note: Dividends prior to the fiscal year ended March 31, 2025 take into account stock splits implemented to date

Shareholder Benefit Program

GSX has implemented shareholder benefits twice a year to thank shareholders for their ongoing support and to increase the attractiveness of holding the Company's shares.

Date of record	Twice per year <u>March 31</u> and <u>September 30</u> of each year
Benefits	Any one of these items ■ QUO Card, 2,000 yen value ■ (Security education service) SecuriST CISO course ■ (Security education service) SecuriST zero trust coordinator introductory/basic course ■ (Security education service) SecuriST certified web application vulnerability assessors ■ (Security education service) SecuriST security passport
Eligible shareholders	Shareholders who hold two units (200 shares) or more of the Company's stock listed or recorded in the shareholders' register as of the record dates of each year and who have continuously held the Company's shares for six months or more

GSX

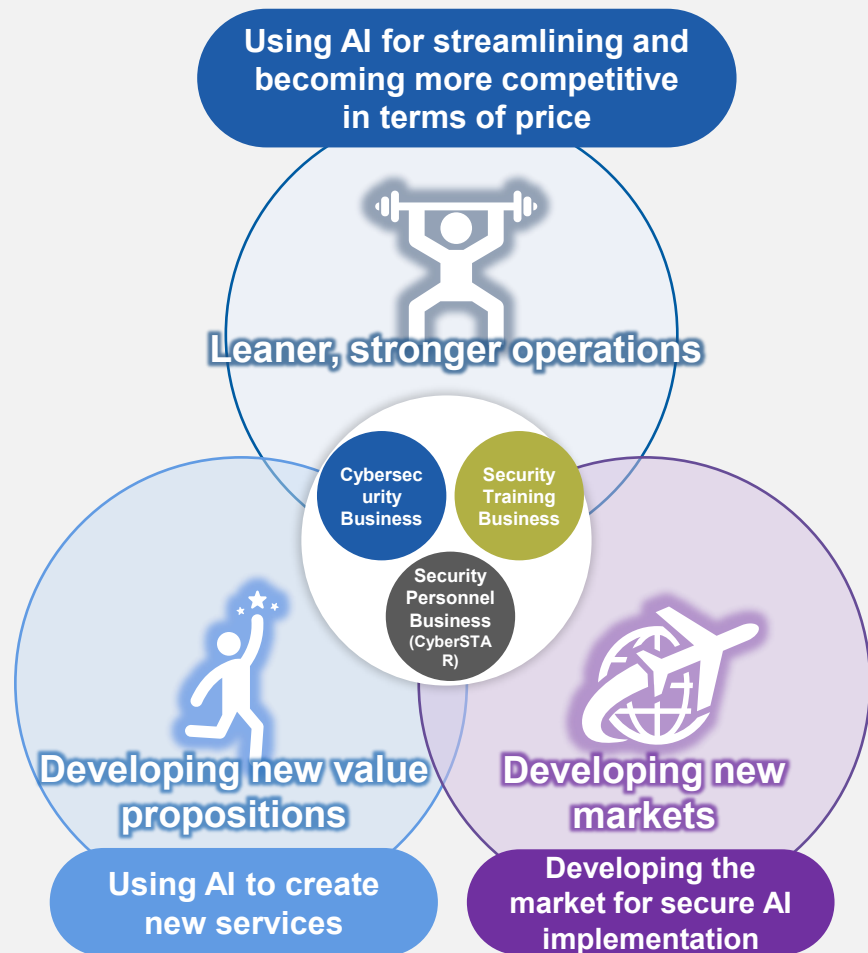
GLOBAL
SECURITY
EXPERTS

Medium-Term Business Plan and Growth Strategy

GSX Group's Growth Strategy

Aggressively promote our growth strategy for an age of rising AI and, at the same time, our strategy for growth through nationwide expansion

AI Group's growth strategy



Strategy for growth through nationwide expansion



Medium-Term Quantitative Targets

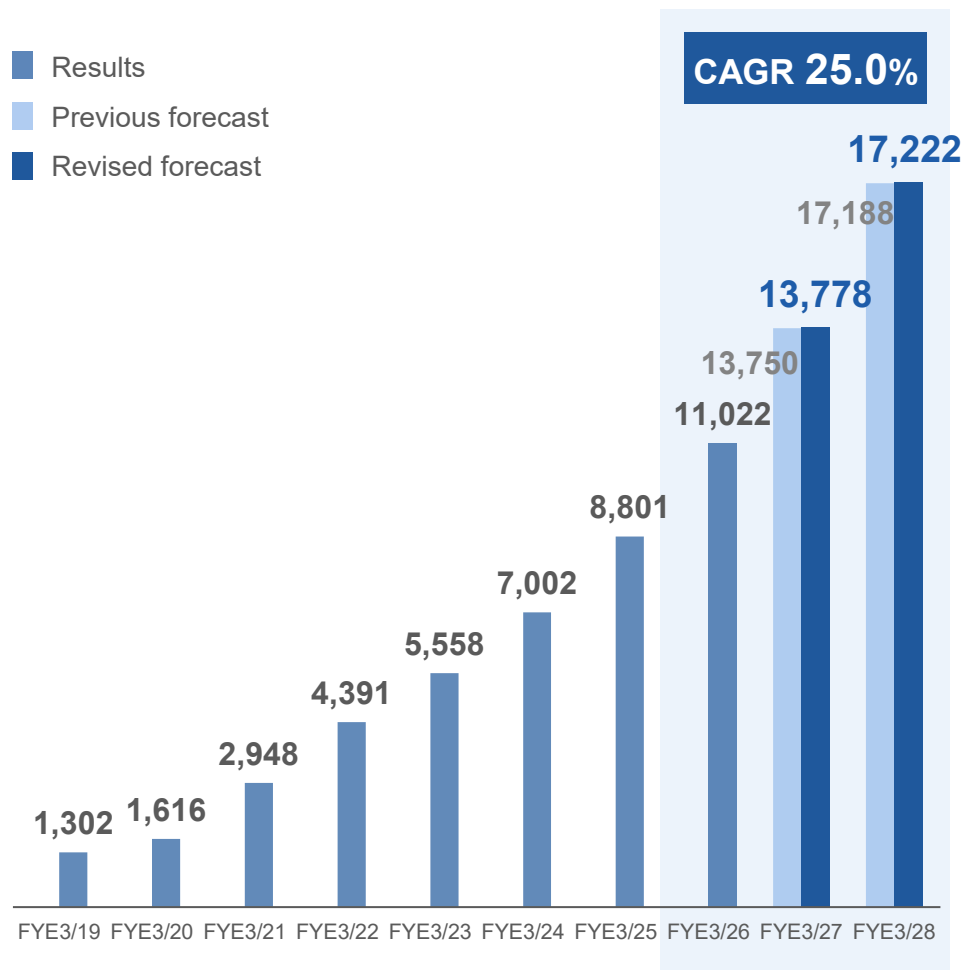
Update based on FYE3/2026 results

25% annual net sales growth in existing businesses; aim to increase operating income margin by 1.0 percentage point annually

Net sales

(Millions of yen)

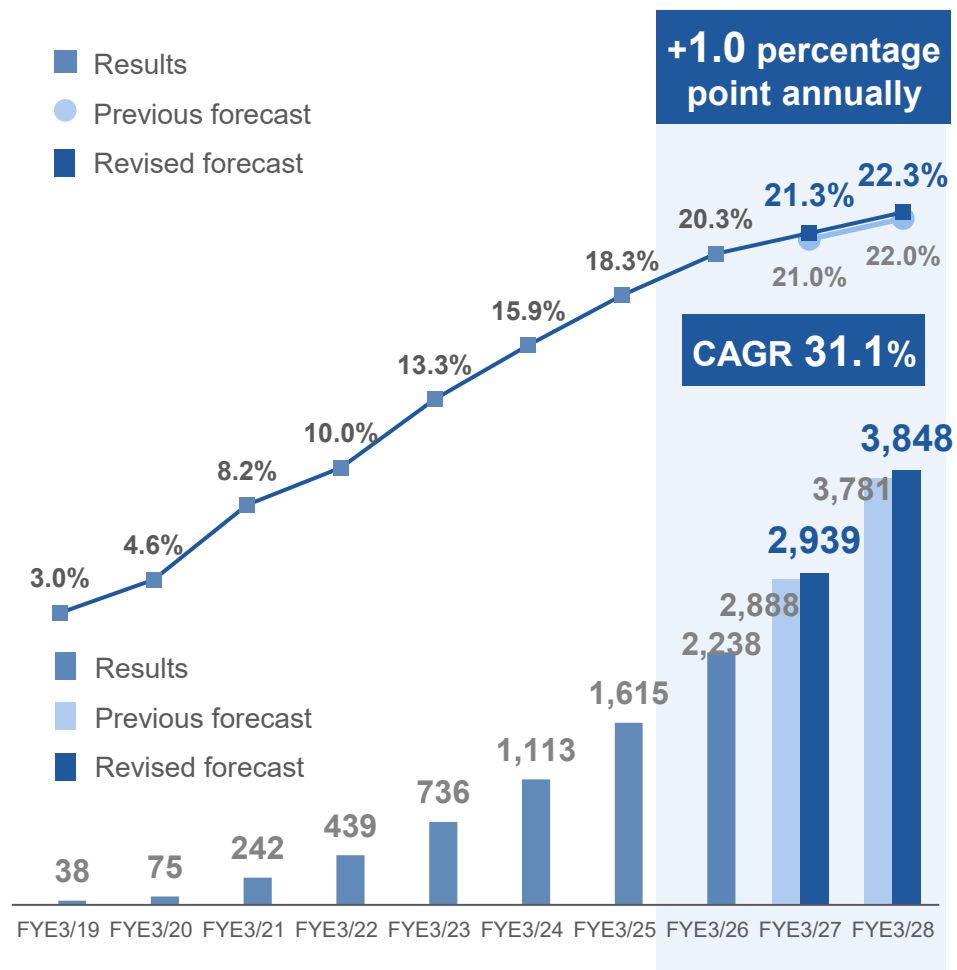
- Results
- Previous forecast
- Revised forecast



Operating income and operating income margin

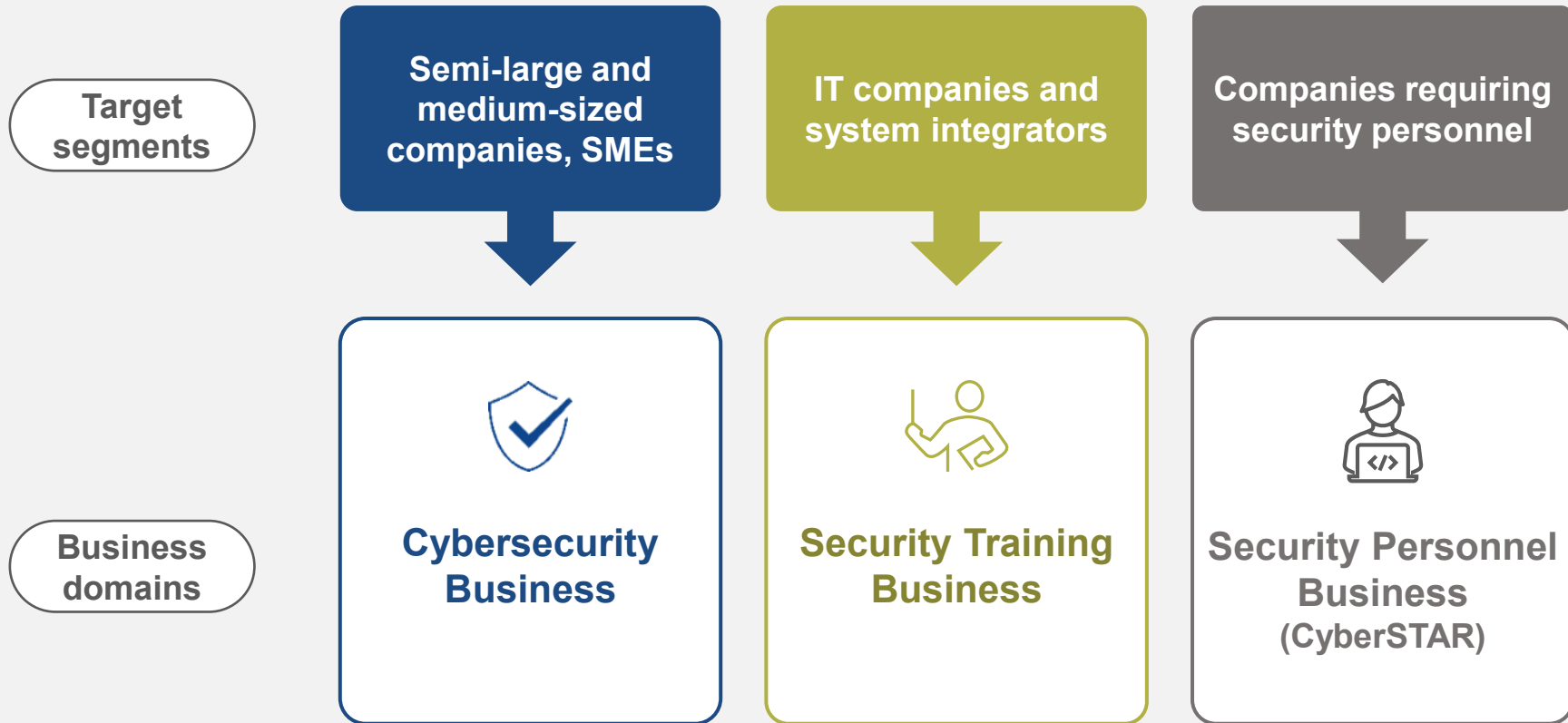
(Millions of yen)

- Results
- Previous forecast
- Revised forecast



*Consolidated results from FYE3/2025

From FYE3/2025, we have clearly established three target segments—semi-large and medium-sized companies and SMEs, IT companies and system integrators, and companies requiring security personnel—organizing these as business domains



One-stop cybersecurity support for semi-large and medium-sized companies and SMEs

Targeted Email Training Services



No. 1
share

when
including OEM
provision

Over
11,000
cumulative
clients

Improving employee security awareness
Building/strengthening organizational
structures

Implementing and operating security
products
Building security infrastructure and
developing systems

Security solutions services



Product
introduction



Operation
services



Emergency
response



Infrastructure
building



System
development

Consulting Services (Management Consulting)

Visualizing
issues

Planning

Building
systems

Main services

Information security
improvement planning

Management system
improvement support

System and security audits

Incident response training
services

Consulting

Providing one-stop services
including survey, analysis,
assessment, and system
improvement

Diagnosing
vulnerabilities

Providing a wide range of
vulnerability diagnostics from
in-house white hat hackers

Vulnerability Diagnostic Services (TIGER TEAM SERVICE)



Design
document
review



Platform
diagnostics



IoT security
diagnostics



Smartphone
app security
diagnostics



Web
application
diagnostics

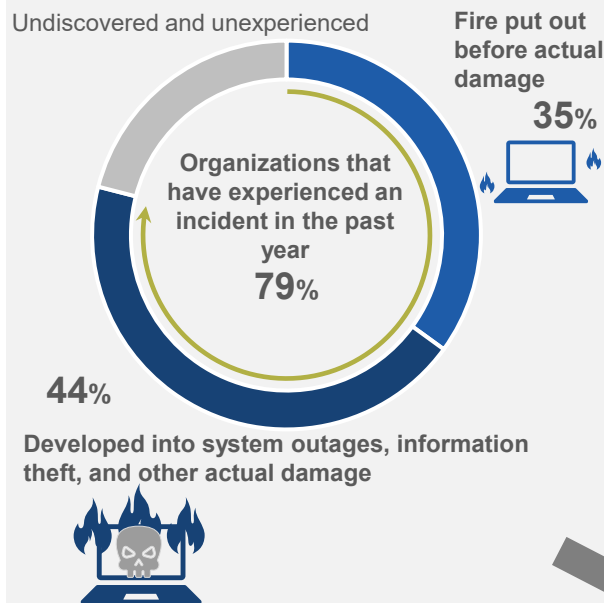
Emergency
response

Security training
services

Security solution
implementation and
operation

Frequent Security Incidents

Organizations that have experienced an incident in the past year comprise **about 80% of all organizations**



Social Pressure

Pressure for security measures from various stakeholders

Numerous security guidelines from government/ministries

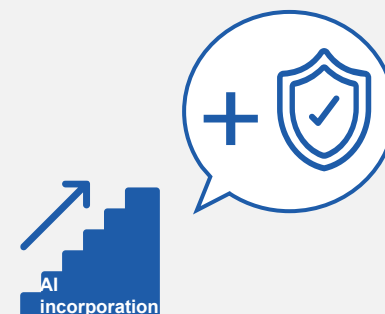
Increased pressure for security measures from ordering customers and Group companies

Semi-large and medium-sized companies, SMEs

Acceleration of AI

Combining AI with security measures:

- ✓ AI is urgently needed to improve corporate competitiveness
- ✓ AI must be combined with security measures



Semi-large and medium-sized companies and SMEs have no choice but to adopt security measures

They also have no choice but to be mindful of security measures necessitated by the promotion of AI

Providing training in the security and AI domains for IT companies and system integrators to help them add value to their IT personnel



GSX
Original

Training Options
for IT/Non-Security Personnel



Cumulative number of participants: 23,599
(As of March 31, 2026)

Certified web application vulnerability assessors
Course fee: 220,000 yen

Secure web application designers
Course fee: 132,000 yen

Certified network vulnerability assessors
Course fee: 220,000 yen

Zero trust coordinators
Course fee: 88,000 yen

Training Options for Security Personnel

EC-Council

International security certificationsCumulative number of participants: 10,442
(As of March 31, 2026)

Major courses

CND
Certified Network Defender

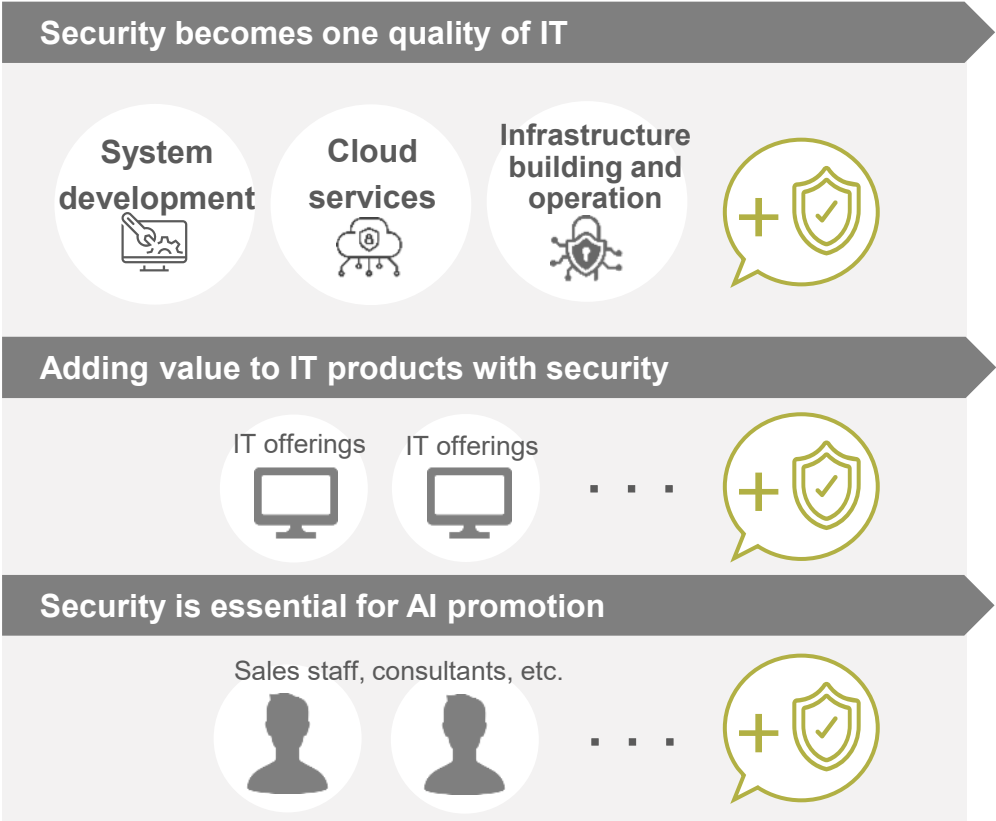
CEH
Certified Ethical Hacker

Course fees

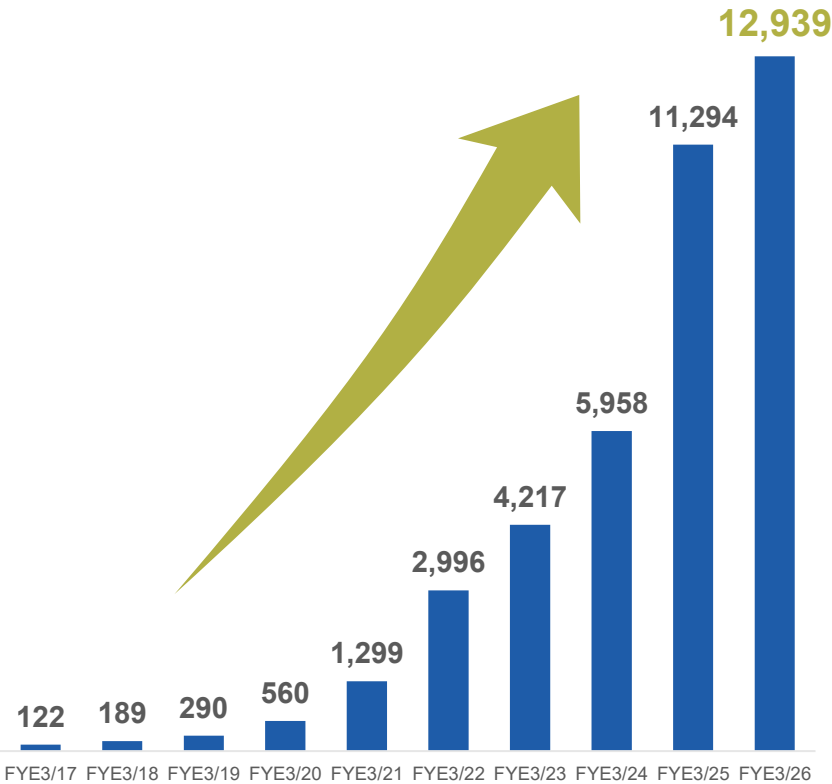
Approx. 320,000 yen

Approx. 540,000 yen

© GLOBAL SECURITY EXPERTS 32



GSX Training Course Enrollment (Single Year)



Even Japan’s Ministry of Economy, Trade and Industry, in its Cybersecurity Management Guidelines, calls for securing “**Plus-Security**” human resources

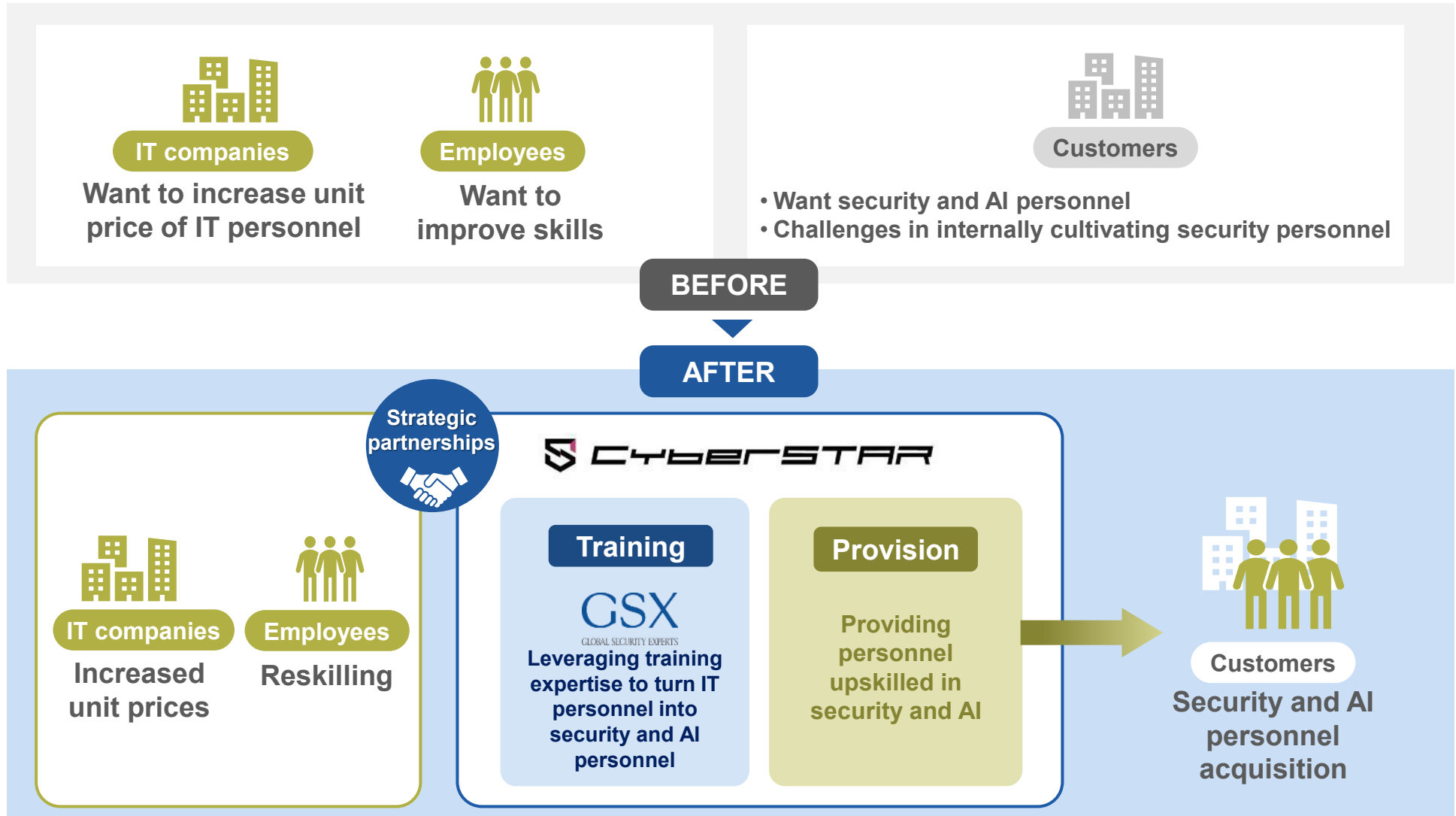
Security and AI training needs are growing rapidly for IT personnel at IT companies and system integrators

* Definition of “Plus-Security”:
The ability to have security awareness in carrying out one’s own work and to acquire the ability to implement necessary and sufficient security measures, or the state of having acquired it.

© GLOBAL SECURITY EXPERTS 33

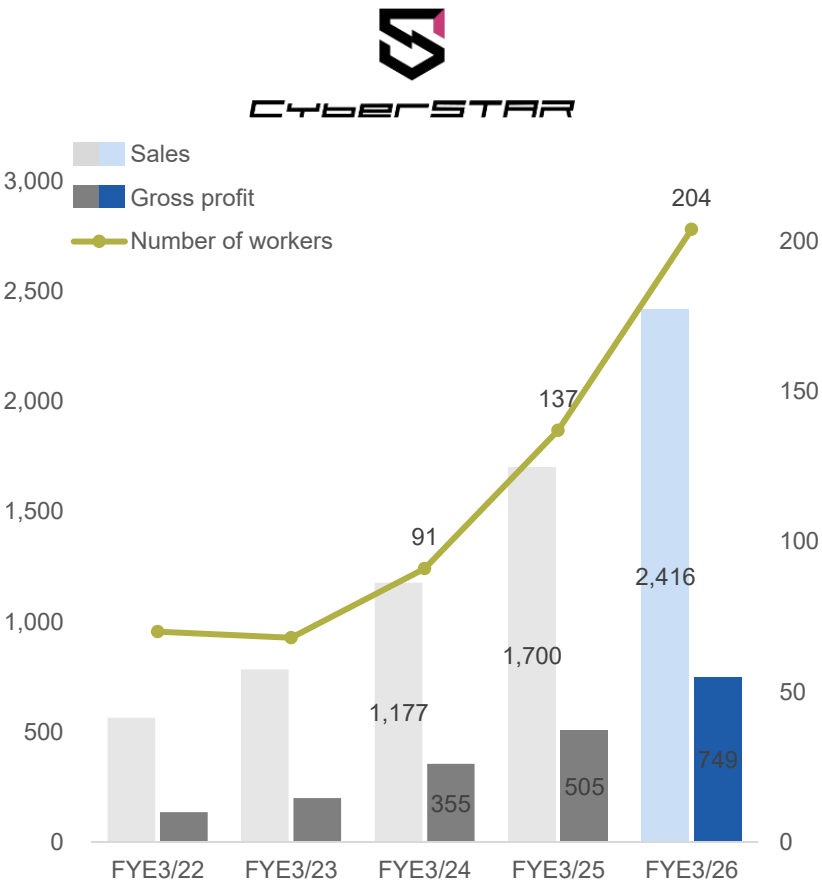
Meet the security and AI personnel needs of all companies, regardless of size

As a security training company GSX, establish an original business model that provides benefits to both IT companies that have IT personnel and customers that need security and AI personnel



Shortage of Cybersecurity Personnel in Japan

Although the number of security personnel required is increasing, growth in the number of security personnel is slowing. The shortfall in such personnel has increased to more than triple its level two years ago.

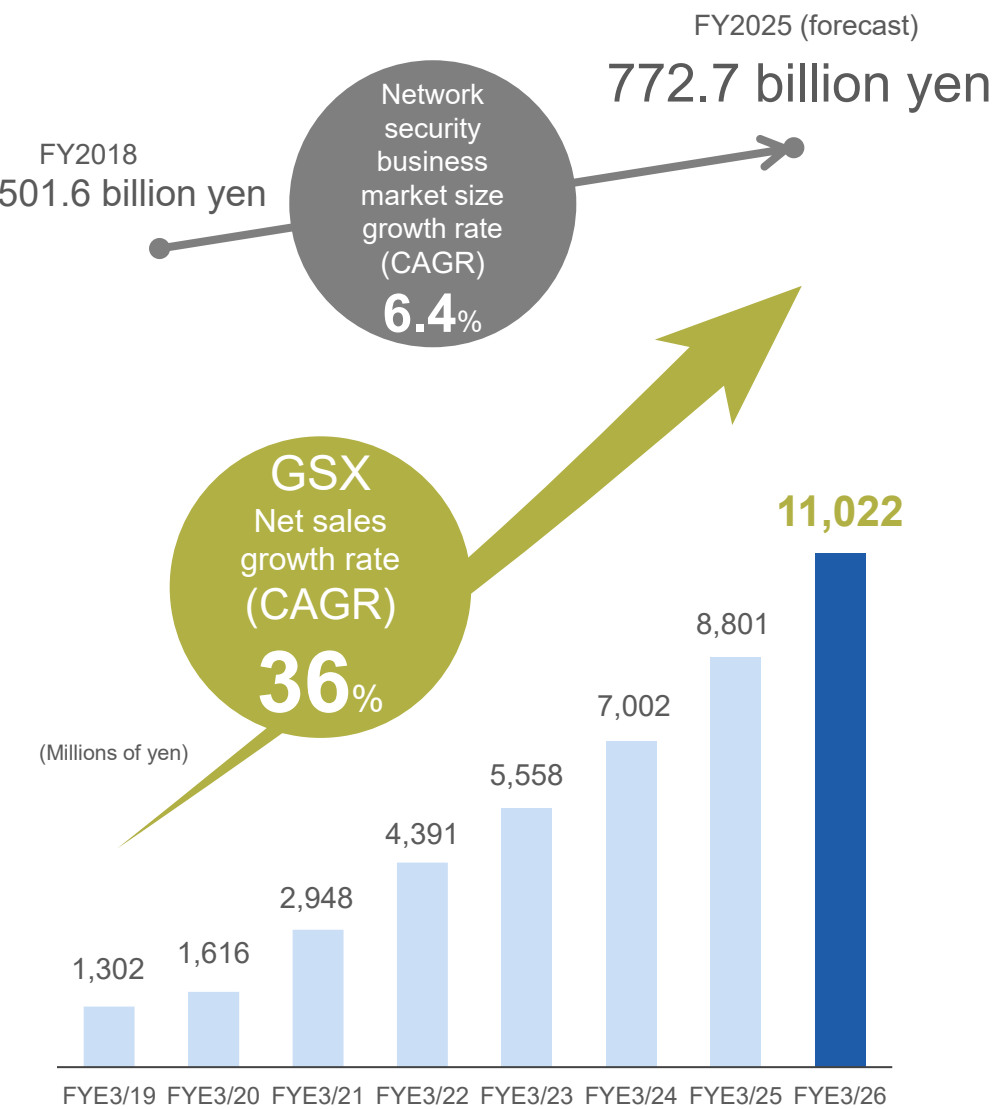


While 90% of Japanese companies are suffering from a security personnel shortage, information security has become a popular job for workers who want to develop their careers.

Business schemes that solve both security personnel needs and reskilling at the same time are attracting attention.

GSX Growth Far Outpaces Security Market Growth

Net sales growth rate (CAGR) of 36%, well above the market growth rate of 6.4%



Reasons for GSX's High Growth and Future Prospects

Reason 1

Dramatic increase in security needs among semi-large and medium-sized companies, and SMEs

Outlook

Currently wide open potential
Further expansion to happen going forward

Reason 2

Dramatic increase in security and AI training needs among IT companies and system integrators

Outlook

Acquisition of security and AI skills by IT engineers to become de facto standard

Reason 3

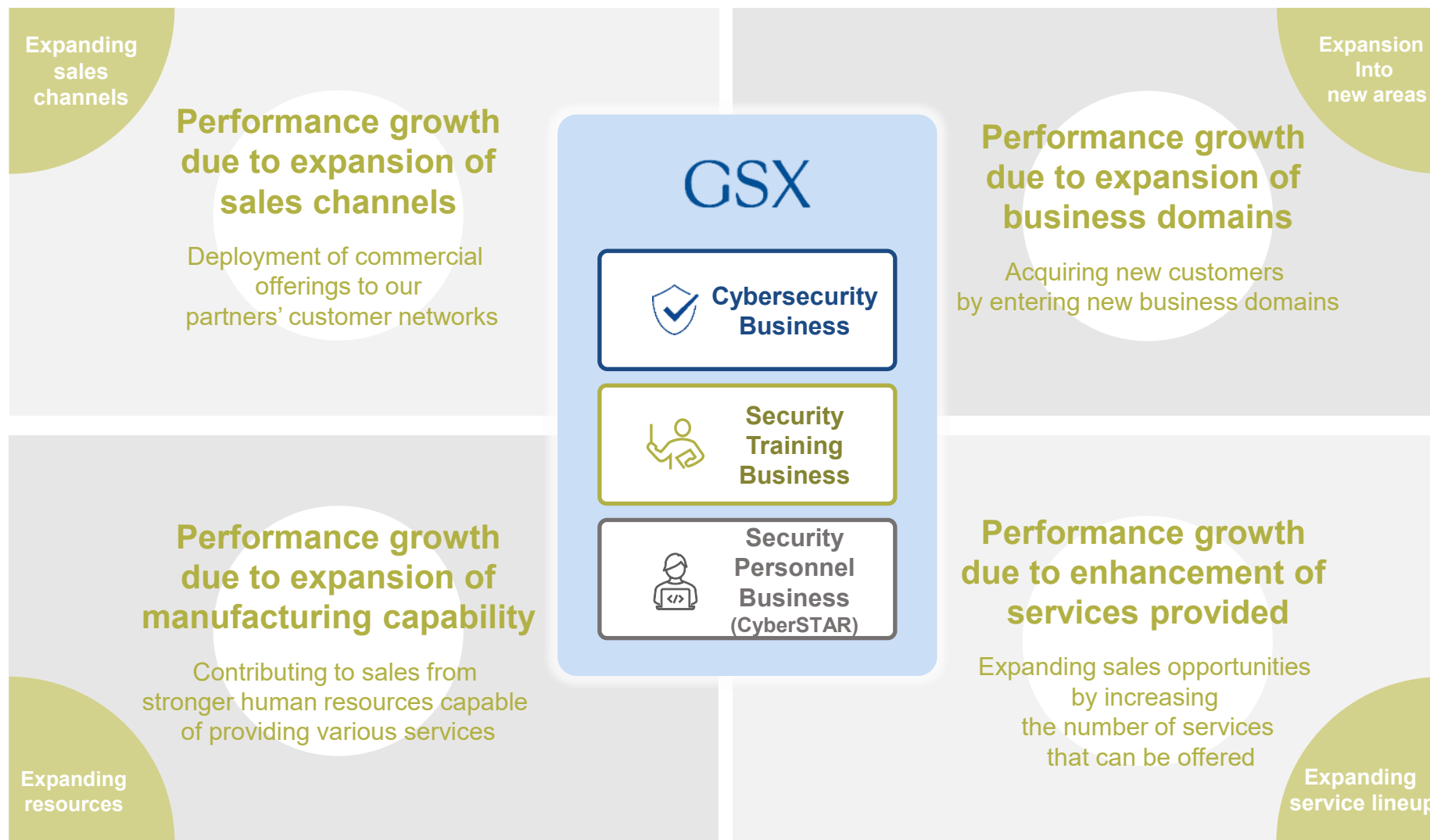
Unique personnel business model to train and provide security and AI personnel

Outlook

The shortfall in personnel continues.
The need for security and AI personnel has grown further.

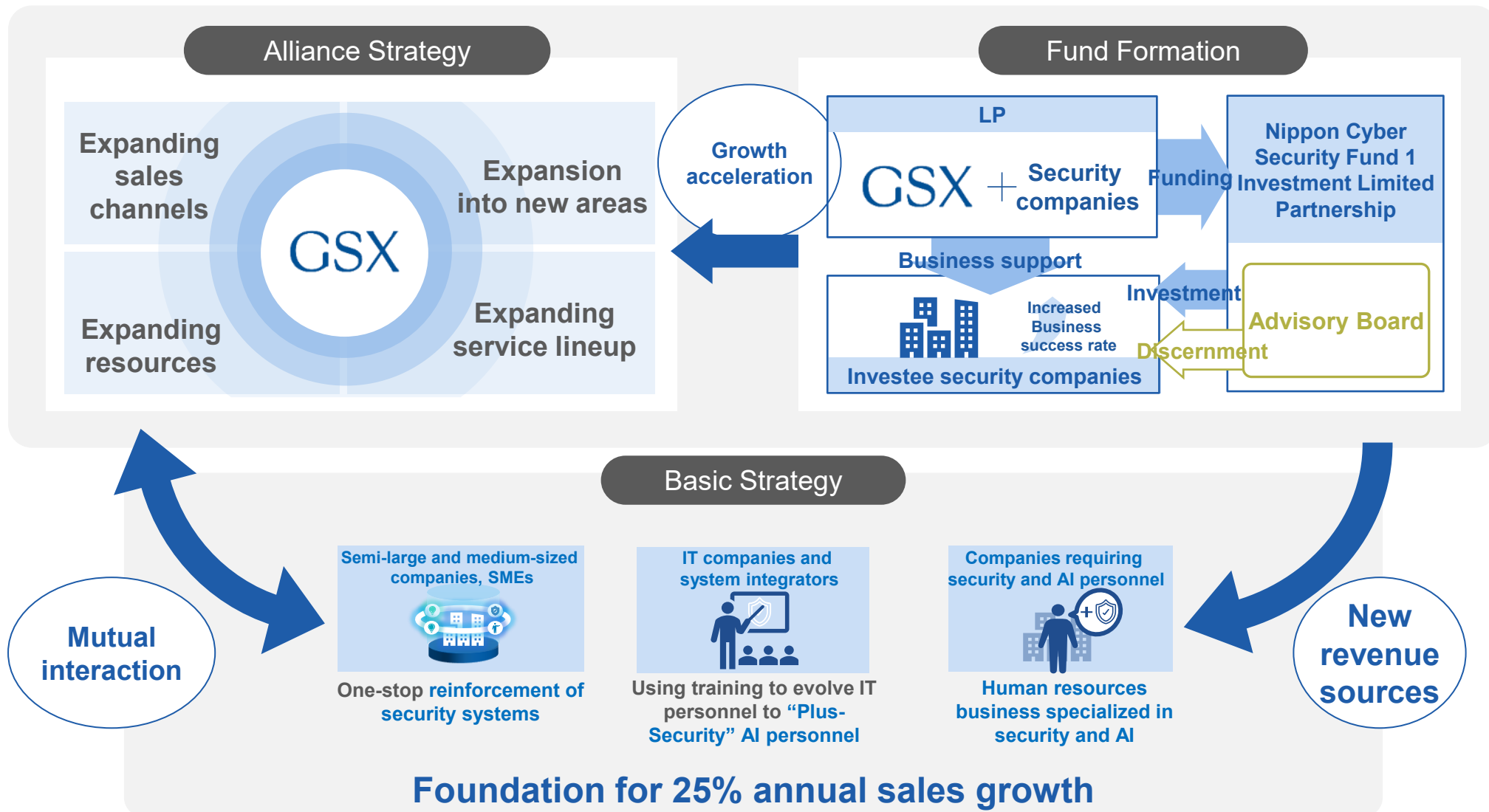
Capital and Business Alliances With 25% Annual Sales Growth and Confidence in Further Growth

Alliance strategy to achieve 25% annual sales growth and ensure further growth as stated in the medium-term business plan
Capital and business alliances with strategic partner companies that can strongly drive business forward in four areas for GSX's growth



Business Strategies

Basic strategy as the foundation for 25% annual sales growth and alliance strategy and fund formation to ensure further growth



GSX

GLOBAL
SECURITY
EXPERTS

ESG Initiatives

We will proactively address ESG and the SDGs with the aim of both realizing a sustainable society and increasing corporate value.

In our Internet society, cybersecurity threats are one of the most important social issues that threaten people's lives and livelihoods. There is also an overwhelming shortage of cybersecurity personnel who can solve these problems. As a cybersecurity training company, we aim to bring about a prosperous society where everyone can live in peace through our business.



E Environment

- Participation in the Japan Climate Initiative (JCI)
- BBS Group greenhouse gas reduction targets: Scope 1+2: 42% reduction, Scope 3: 25% reduction in greenhouse gas emissions in FY2030 (vs. FY2023), aiming to achieve net zero greenhouse gas emissions for the Group in FY2050
- Going paperless



S Social

- Promoting efforts for respect of human rights
- Cultivating human resources and creating a facilitative work environment
- Promoting diversity & inclusion
- Initiatives for health and safety
- Local revitalization and job creation



G Governance

- Strengthening corporate governance
- Ensuring compliance
- Initiatives for risk management
- Establishing various reporting contact points
- Strengthening stakeholder engagement



GSX

GLOBAL
SECURITY
EXPERTS

Appendix

A cybersecurity training company

that operates throughout the security industry,
aiming to improve the self-defense capabilities of companies throughout Japan

—Purpose—

To protect all companies from security threats
To unwaveringly tell companies what needs to be done for this protection

—Mission—

To improve the self-defense capabilities of companies throughout Japan

Corporate Profile

A cybersecurity specialist company, established at the dawn of cybersecurity

Engaged in three businesses: Cybersecurity Business, Security Training Business, and Security Personnel Business

*CyberSTAR Inc., a wholly owned subsidiary, was established on April 1, 2024 by spinning off the cybersecurity human resources SES

Corporate Profile

Company Name	Global Security Experts, Inc.
Established	April 2000*1
Representative	Shiro Aoyagi, President and CEO
Share capital	546 million yen *As of March 31, 2026
Business Lines	The Company operates a Cybersecurity Business that provides one-stop support for cybersecurity measures for semi-large and medium-sized companies and SMEs, a Security Training Business that provides security education for IT companies and Sler human resources, and a Security Personnel Business that provides security human resources SES.
Business Segment	Cybersecurity Business (single segment)
Number of Employees	Consolidated: 221 Non-consolidated: 187 *As of March 31, 2026
Main shareholders	Business Brain Showa-Ota Inc. KANEMATSU ELECTRONICS LTD. Marubeni I-DIGIO Holdings Co., Ltd.

List of Officers

President and CEO	Shiro Aoyagi
Vice President and COO	Shinichi Hara
Managing Director	Tsuyoshi Miki
Managing Director	Takayuki Nakamura
Director	Chikara Yoshimi
Director	Takashi Suzuki
Director	Kei Goto
Outside Director	Soichi Kondo
Outside Director	Yukinori Okada
Outside Director	Sen Ueno
Outside Director (Audit & Supervisory Board Member)	Junji Inoue
Outside Director (Audit & Supervisory Board Member)	Shintaro Furuya
Outside Director (Audit & Supervisory Board Member)	Shigeyuki Mizutani

Note *1: The date of establishment is the date of change of the trade name to Global Security Experts



President and CEO

Shiro Aoyagi

- Apr. 1998:** Joined Beacon Information Technology Inc. (currently UNIRITA Inc.)
- Jan. 2009:** Director and General Manager of Security Business Division, Cloud Technologies, Inc.
- Mar. 2012:** Joined the Company
- Oct. 2012:** General Manager of Business Development Department
- June 2014:** Executive Officer and General Manager of Sales Division
- Apr. 2017:** Director and General Manager of Corporate Planning Division
- Apr. 2018:** President and CEO (to present)



Vice President and COO

Shinichi Hara

- Apr. 1991:** Joined AMADA METRECS CO., LTD. (currently AMADA CO., LTD.)
- Apr. 2000:** Representative Director, Advanced Link Co., Ltd.
- Apr. 2012:** Director, StartCom Co., Ltd.
- Apr. 2018:** Joined the Company, Executive Officer, Vice President, and General Manager of Corporate Planning Division
- June 2018:** Vice President and COO (to present)



Managing Director
Area Management

Tsuyoshi Miki



Managing Director
General Manager of Training
Business Division

Takayuki Nakamura



Director
Branch Manager of West
Japan Branch

Chikara Yoshimi



Director
Assistant General Manager of
Cybersecurity Business Division
Director of Cybersecurity
Research Institute

Takashi Suzuki



Director
Assistant General
Manager of Cybersecurity
Business Division

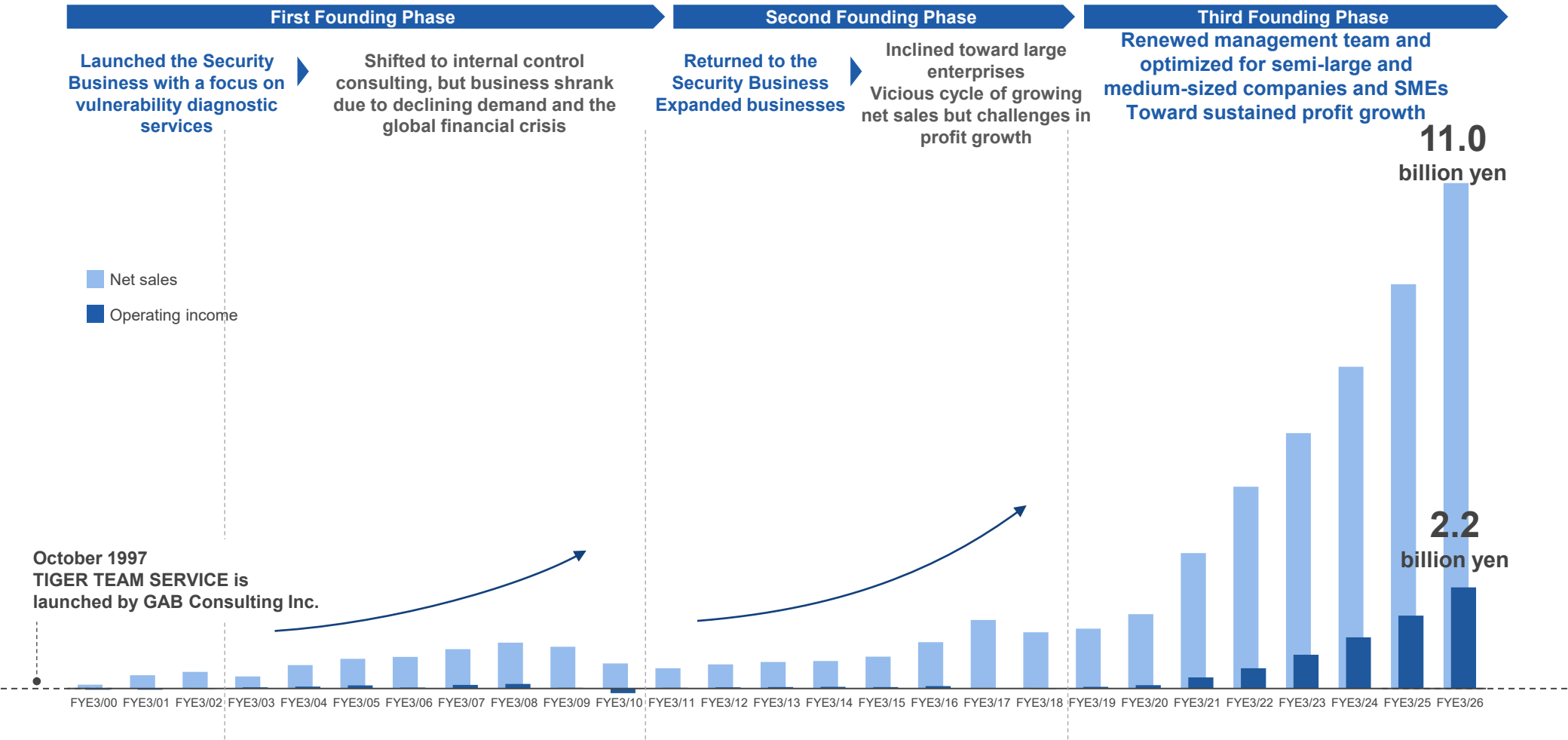
Kei Goto

History: A Cybersecurity Specialist Company that Has Existed Since the Dawn of Cybersecurity Market



Our founding business is a vulnerability diagnostic service within the Consulting Business. We began providing services at the dawn of Japan’s domestic cybersecurity market with a focus on vulnerability diagnostic services, and while accumulating security expertise, expanded business by incorporating peripheral areas.

Today, we are entering a phase of sustained profitable growth by optimizing services for semi-large and medium-sized companies and SMEs by leveraging experience from our first and second founding phases.

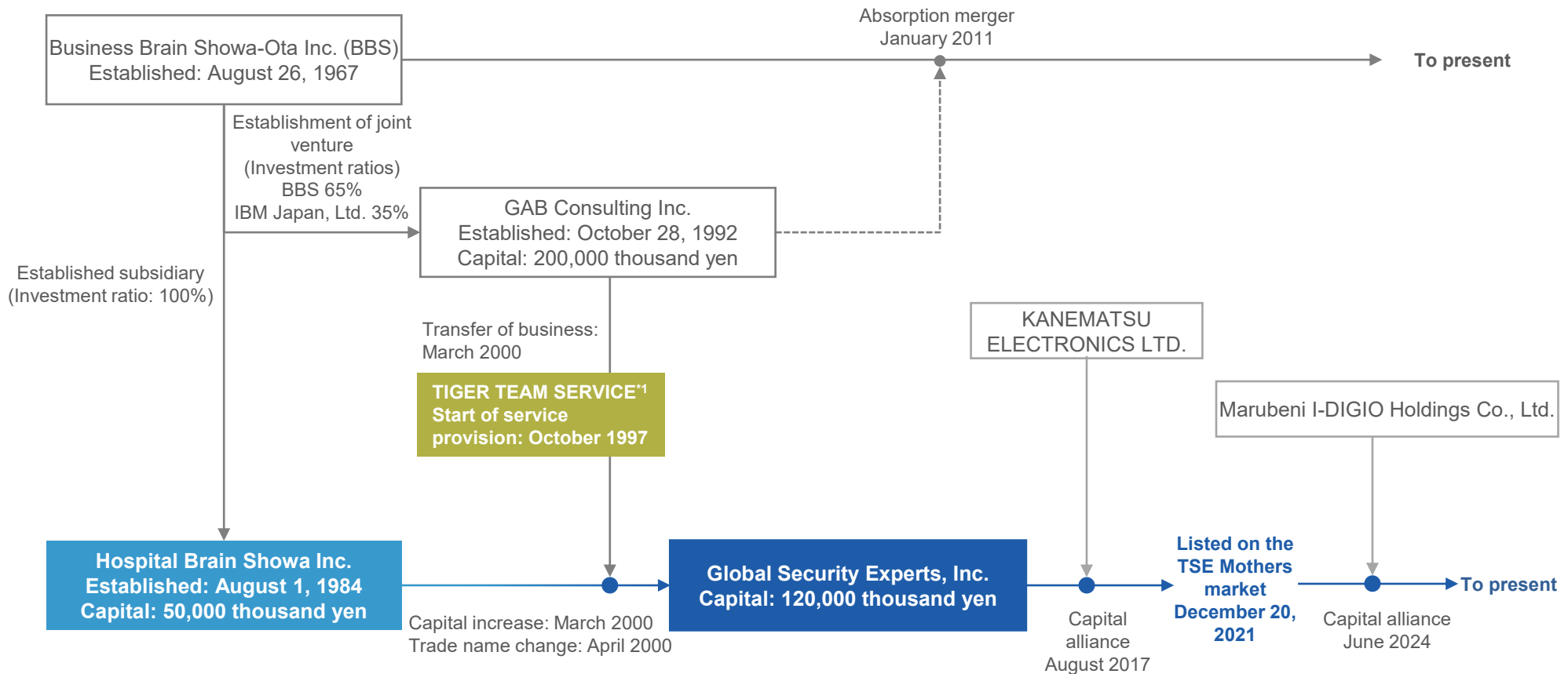


Note *1: Founded in 1984 as Hospital Brain Showa Inc. See the Appendix for information on the Company’s origins.
Note *2: From FYE3/2021, the IT Solutions Business, which was accepted via transfer on April 1, 2020, is included (IT Solutions Business net sales in FYE3/2021 were 730 million yen).

Our Origins

Predecessor company Hospital Brain Showa Inc. established as a consolidated subsidiary of Business Brain Showa-Ota Inc.

In 2000, TIGER TEAM SERVICE was transferred to Hospital Brain Showa Inc. from a Group company, and the Company was reborn as one specializing in cybersecurity, changing its name to today's Global Security Experts.

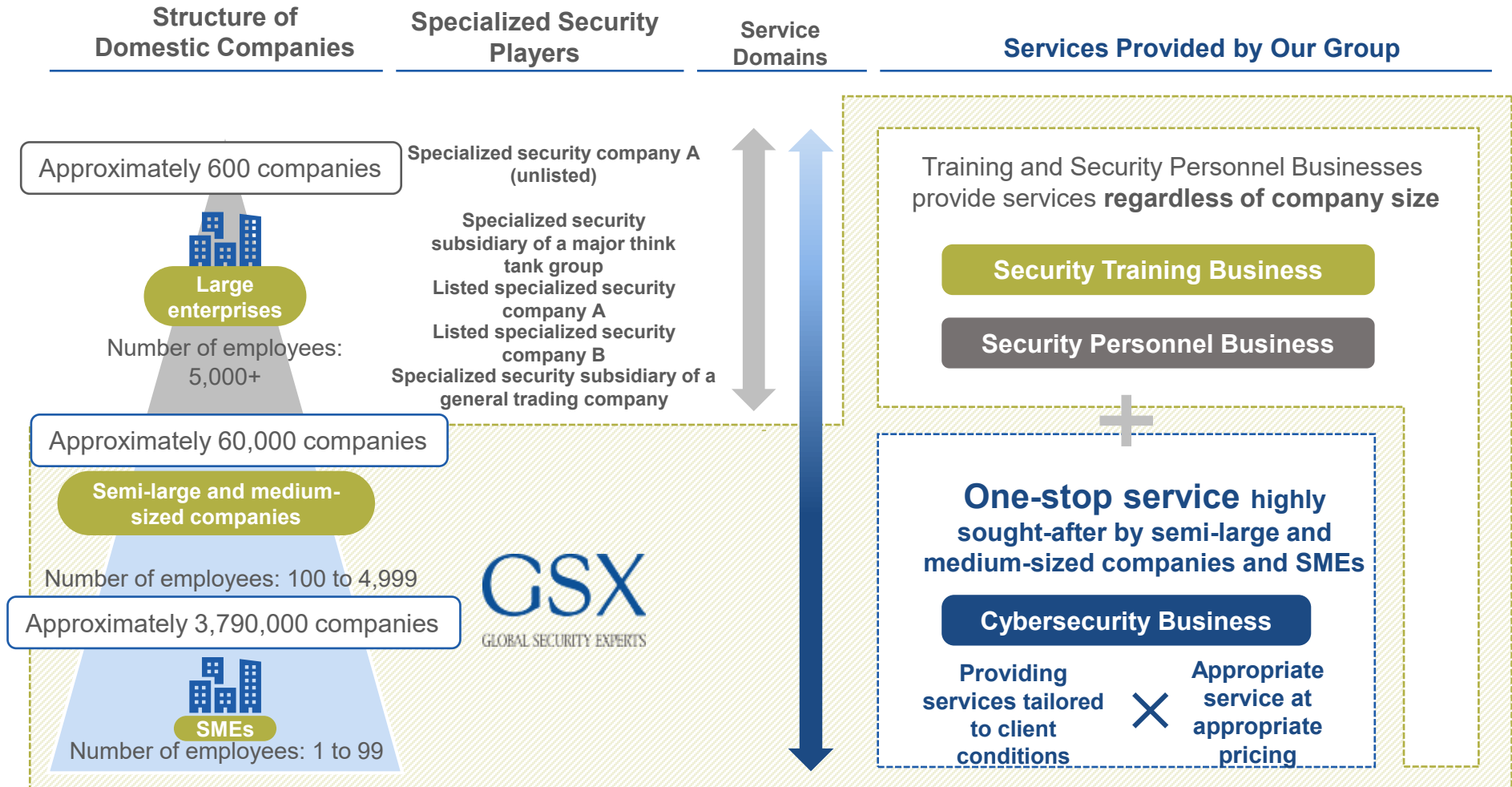


Note 1: TIGER TEAM SERVICE refers to penetration testing/simulated attack inspection services

Uniquely Positioned, Primarily Targeting Semi-Large and Medium-Sized Companies and SMEs

A large disparity exists between the security needs of large enterprises and other types of companies. For this reason, other security specialists have continued to focus their strategies on large enterprises.

GSX is in a unique position in the category of specialized cybersecurity firms, which is difficult for other companies to compete in.



Differences in Security Needs and Service Optimization

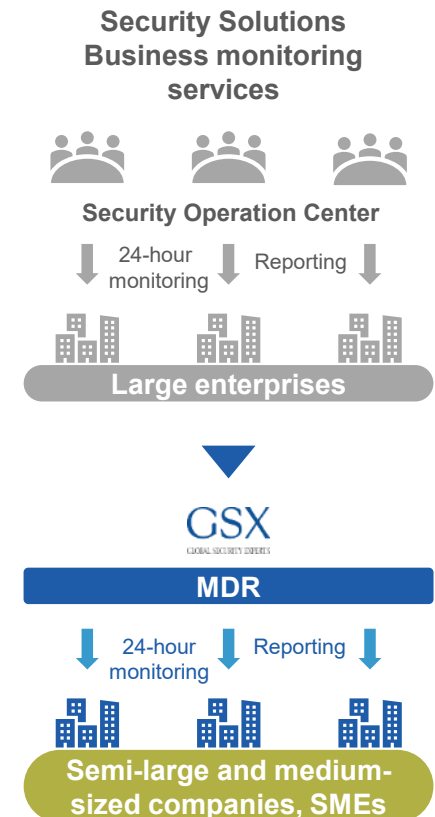
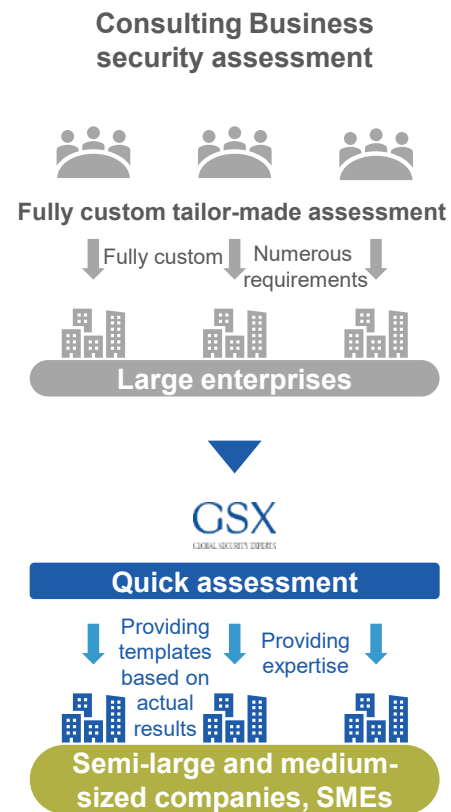
Large enterprises seek security measures to completely eliminate threats, while semi-large and medium-sized companies and SMEs seek the minimum necessary security measures to eliminate reputational risk to their business partners and to adapt to their own business type.

Our extensive security expertise enables us to optimize our services to the level required by semi-large and medium-sized companies and SMEs while maintaining effectiveness.

Needs by Company and Players Providing Services

	Large enterprises	Semi-large and medium-sized companies, SMEs
Major corporate needs	Complete elimination of security threats	Security audit certification Elimination of dangerous threats to the company
Services required	Fully custom consulting services	Light consulting services (Package of only services required)
Players providing services	Specialized security subsidiary of a major think tank group Specialized security company A (unlisted) Specialized security subsidiary of a general trading company Listed specialized security company A Listed specialized security company B	

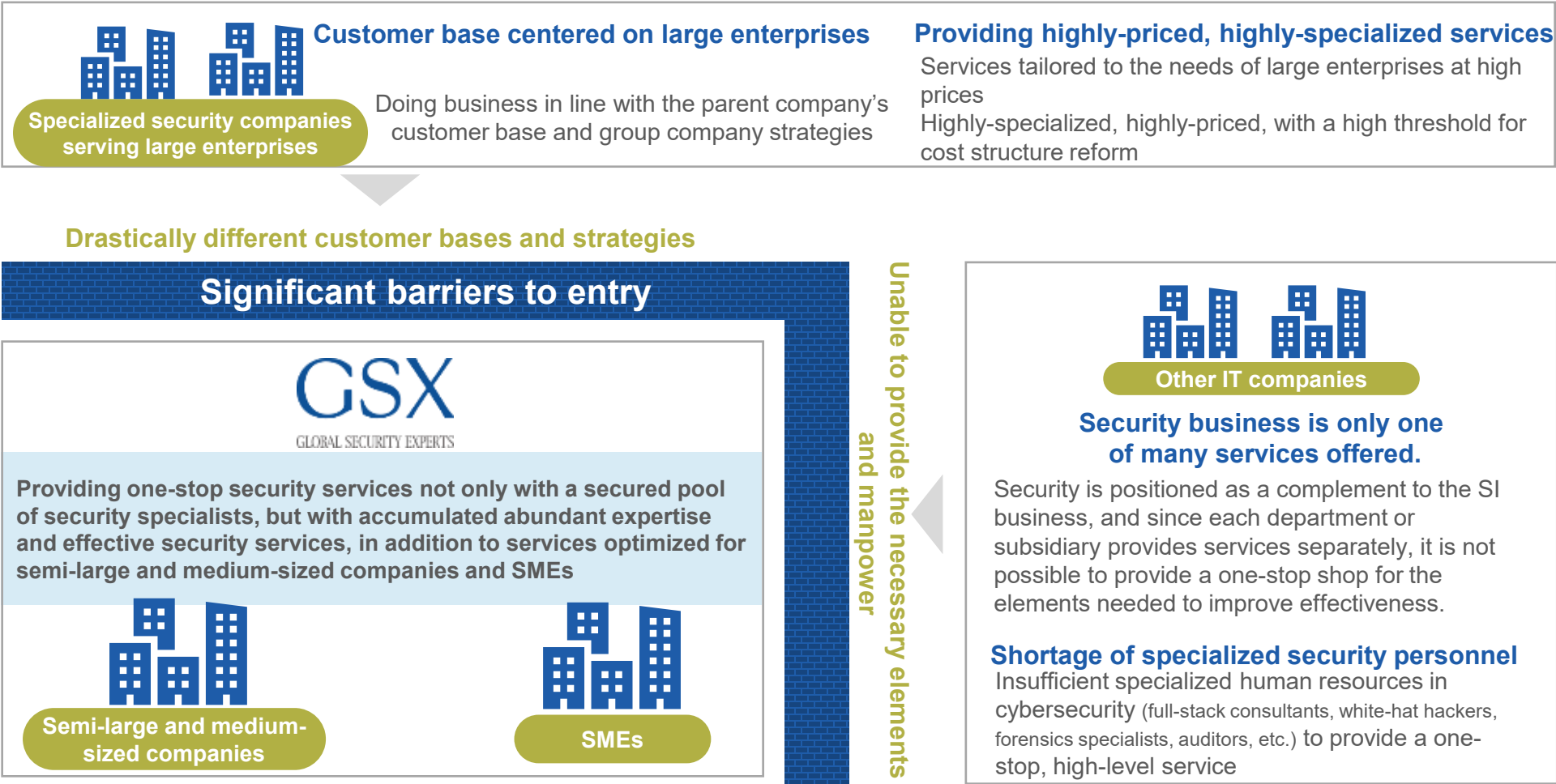
Optimization of Security Services for Semi-Large and Medium-Sized Companies and SMEs



Structural challenges exist for competitors attempting to enter the market for semi-large and medium-sized companies and SMEs.

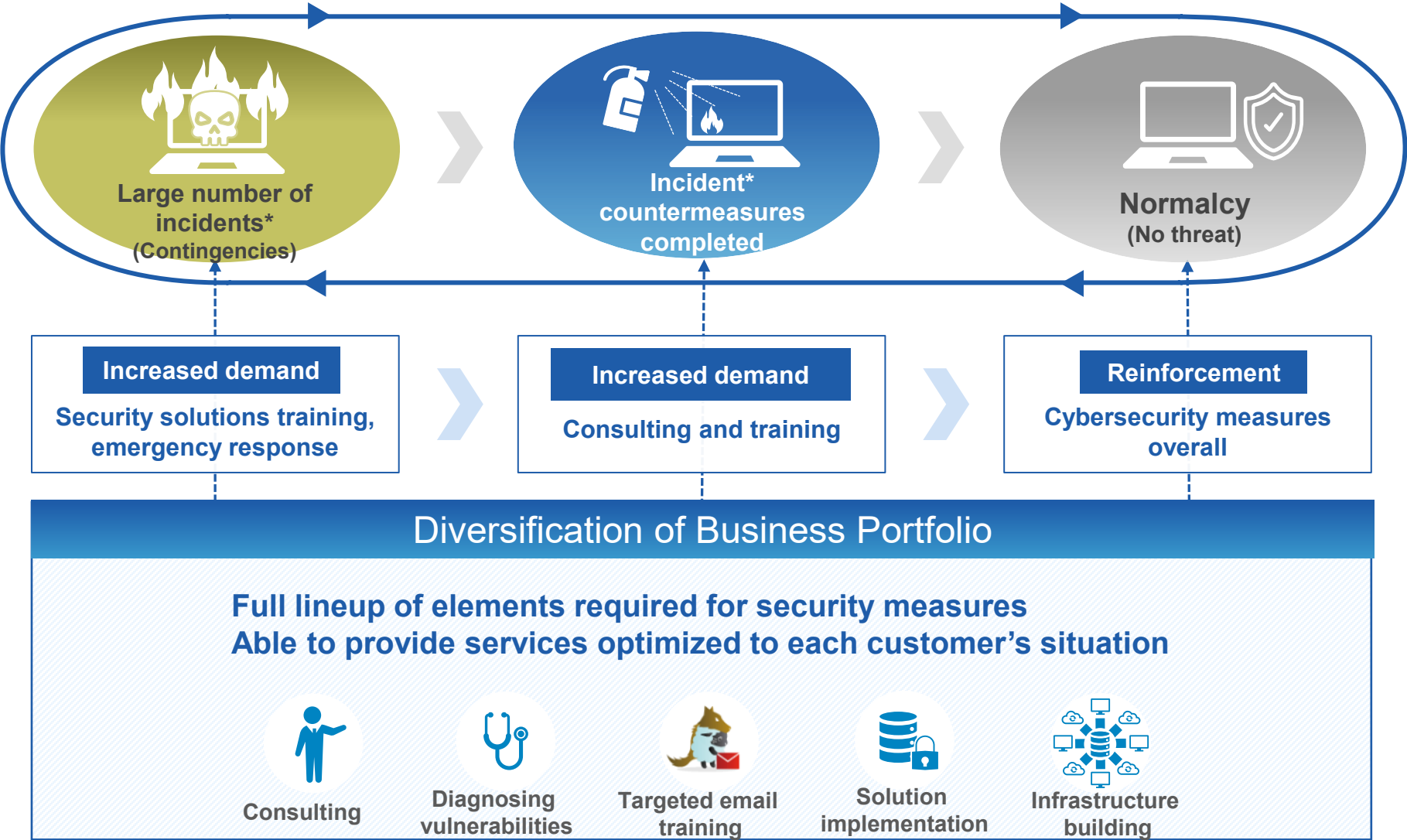
The market environment is not conducive to earning short-term revenue, and in order to continue to be customers’ preferred vendor, it is necessary to have the knowledge and infrastructure to continue to provide a one-stop shop for all security-related services.

Structural Challenges for Competitors



Lineup that Can Provide Appropriate Services Tailored to the Customer's Situation

A structure that facilitates long-term transactions by providing optimal services tailored to the situation



* Incident: Information leakage due to malware or virus infection, potential information leakage due to system lockup or website tampering, etc.

GSX's Sales and Capacity Strategies (Business Expansion Model)

Increasing the number of customers and ARPU by implementing different approaches to new and existing customers

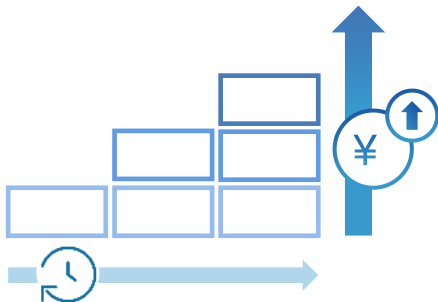
Carrying out capacity strategy by cultivating security personnel in IT companies and partnering with and fostering industry peers to support increased orders

Sales Strategy

Capacity Strategy

Existing customers

Up-sell



New customers

Partner strategy
Marketing strategy



Expanding net sales

Number of customers

ARPU

Capacity strategy

Delivery partner strategy



IT companies

Industry peers



Security companies

GSX's strength is its balance of existing and new customers.

Sales Strategy — Existing Customers: Up-Sell/Cross-Sell

Cross-selling and up-selling through multi-faceted service offerings.

ARPU* of existing customers is higher than that of new customers, and we have achieved efficient business expansion through ongoing transactions.

Efficient Business Expansion Through Business Synergies

Providing ongoing multifaceted support and building a medium- to long-term transaction cycle

System operation and incident response
Ex: Forensic investigation

Support for implementation and operation of security systems and services
Ex: EDR introduction

Building common understanding through education and training
Ex: Email training



Organizational structure reform and constitutional improvement through consulting
Ex: CSIRT establishment

Visualizing security measure status
Ex: Assessments

Cross-Selling/Up-Selling Enabled Through Comprehensive Process Coverage

Since we provide all the processes necessary for security measures, we are capable of a variety of sales approach angles and acquiring the following processes.

Training

Assessment

Organizational development and reform

System implementation and operation

| Ransomware protection

First order

Incident response

Cross-sell/up-sell

EDR introduction

| Strengthening organizational capabilities

First order

Assessment

Cross-sell/up-sell

CSIRT establishment and training

| In-housing diagnostics

First order

Diagnosing vulnerabilities

Cross-sell/up-sell

Training course: SecuriST

Sales Strategy: Become a Sales Partner for IT Companies Throughout Japan

Leveraging the customer base and presence of IT firms to open up markets that had previously been untapped opportunities

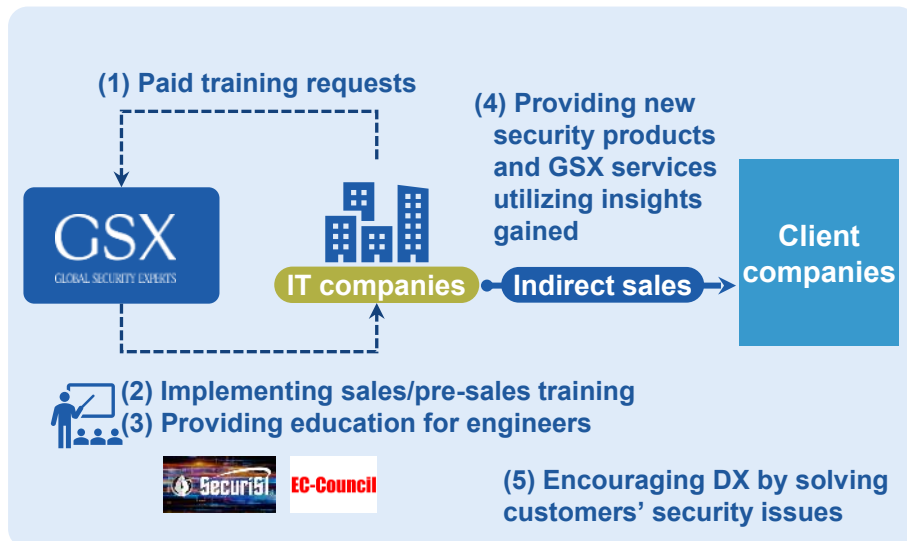
By partnering with GSX, IT companies can expand their security and DX-related businesses through synergies with their own products and services.

Benefits of Becoming a GSX Sales Partner

IT company needs

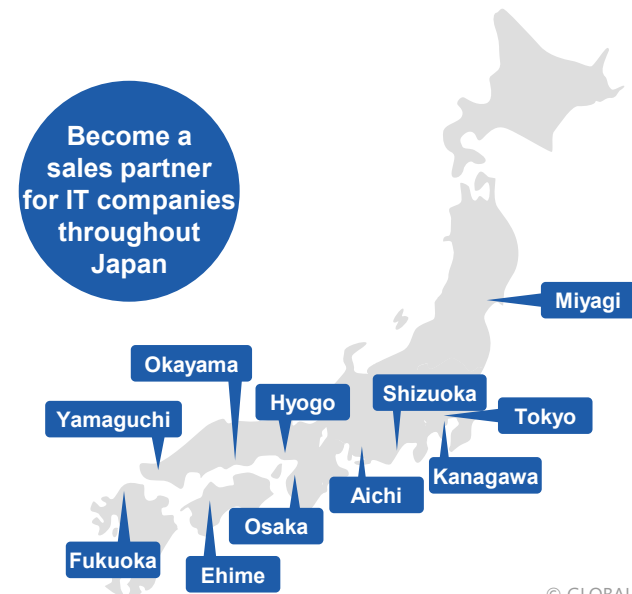
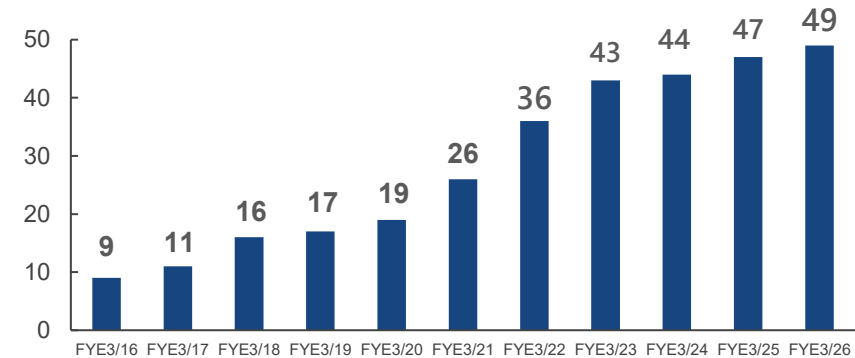
- Hard to just sell new security offerings* needed for DX
- Want to train employees to expand sales of these products and expand their security business, and further expand DX-related business (the mainstay business of system integration) by using security as a hook.

*Fields such as zero trust and multi-cloud



Number of Sales Partners and Nationwide Expansion

(Companies)



Capacity Strategy: Developing Delivery Partner Companies

Expanding order capacity by leveraging highly specialized training content to cultivate security personnel in IT companies, partnering with and fostering industry peers, and developing a large number of players in the security market

Expanding Order Capacity by Fostering Security Companies

Capacity Strategy Results



Sales Strategy — New Customers: Strengthening Digital Marketing Strategy

For new customer acquisition, implementing digital marketing measures that lead to orders and shifting to an efficient and effective digital marketing focus to acquire high quality leads

Selecting media that specialize in security in each area of digital marketing and implementing digital marketing initiatives that utilize video and other media



Producing videos of all training offerings (SecuriST, EC-Council, CISSP) and distributing on NewsTV to strengthen sales promotion

In just one year, we tripled enrollment!



What makes GSX cybersecurity training so appealing?



Strengthening digital marketing

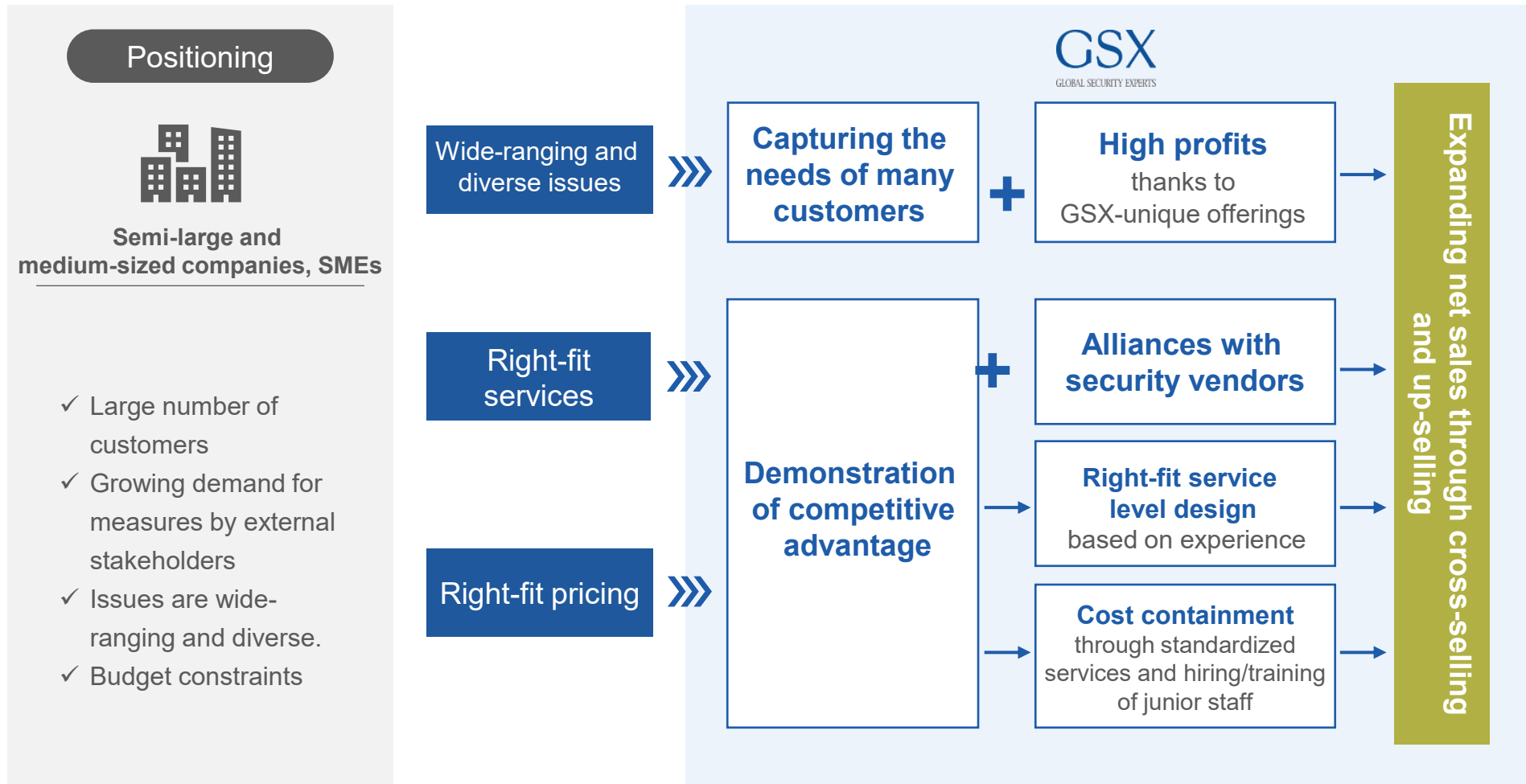

NewsTV


YouTube


Facebook


X (Formerly Twitter)





With the promotion of DX, including the use of IoT and cloud computing, and the increase in telecommuting, the number of connections with other entities has increased, internal and external threats in organizations have changed, and a variety of incidents have occurred.

Internal Threats

(Intentional) Threats by employees or other stakeholders

- **Unauthorized property removal**
(Leakage of personal/confidential information)

Industrial company S: Leakage of confidential information due to contact from a foreign company

Company I: Unauthorized removal of customer information by an outsourced employee

Company S: Unauthorized removal of confidential information by an employee upon joining a competitor

(Negligence) Threats by employees or other stakeholders

- **System misconfiguration/mistaken email communications**

(Information leakage, loss, or alteration)

Company M: Incorrectly sent email to a job-seeking student

Company A: Sent a newsletter in CC rather than BCC

Company R, P, AB, others:
Salesforce misconfiguration

Threats from cyberattacks

Threats to overseas group affiliates

- **Attacks on overseas group companies**
(Production stoppage, information leakage)

Company D: Subsidiaries in Mexico and Germany

Company B: Subsidiary in the U.S.

Company P: Subsidiary in Canada

Securities company D: Subsidiary in the U.K.

Supply chain threats

- **Attacks on the supply chain, vulnerabilities, mismanagement**
(production stoppages, information leaks)

Company T: Cyberattack on supplier temporarily halts production at all plants.

Company K: Victim of ransomware due to use of the company's services

Company T: Leakage of personal information by a distributor

External Threats

- **Unauthorized access**
(Account theft, website vulnerabilities)

Company MD: Office365 account theft
→ Information leakage

E-commerce sites (multiple): Leakage of personal and credit card information

- **Targeted attacks (ransomware)**
(Leakage of confidential information, stoppage of production/services)

Company P (U.S.): Shutdown of operations

Company K: Service suspension

Company N: Delay in reporting financial results

Company H: Closed domestic and overseas offices and suspended factory operations

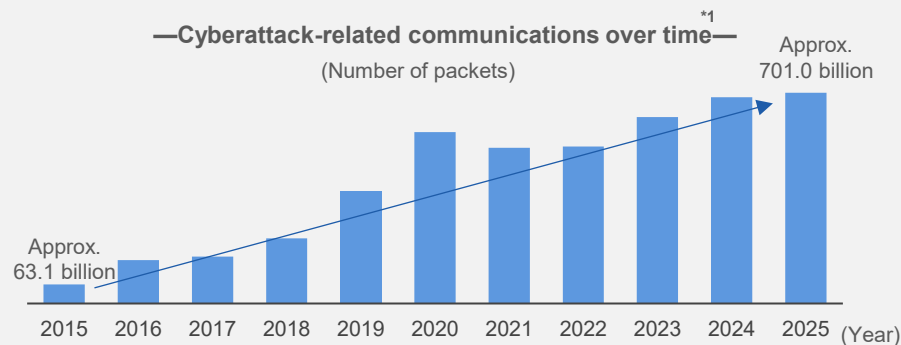
Market Environment for the Domestic Cybersecurity Market

In the cybersecurity market, demand for countermeasures is on the rise. In addition, the rapid shift of companies to digital technologies is a tailwind for growth in this market.

On the other hand, an unprecedented shortage of security personnel presents challenges.

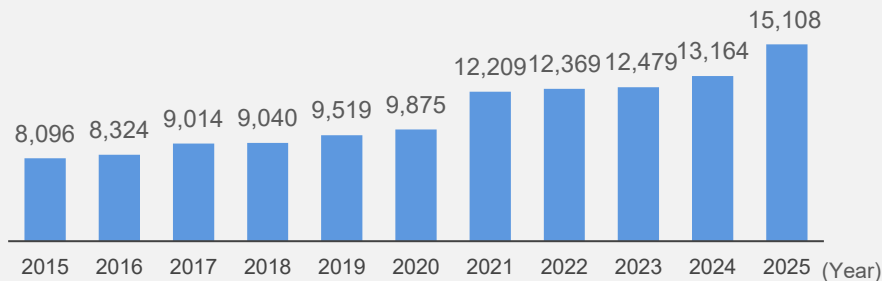
In this market environment, there is a growing need for GSX to provide one-stop services from upstream to downstream of security training and implementation.

Increase in Cyberattacks (Threats)



—Number of cybercrime arrests over time— (Arrests)

*2



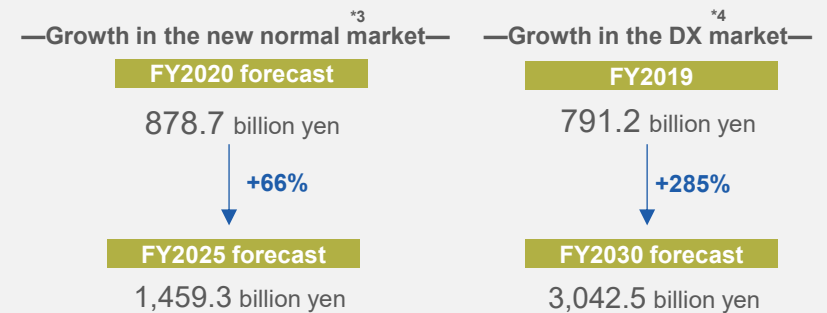
Source 1: NICTER Observation Report 2025, National Institute of Information and Communications Technology (NICTER)

Source 2: Threats in Cyberspace 2025 (National Police Agency)

<https://www.nict.go.jp/press/2026/02/05-1.html>

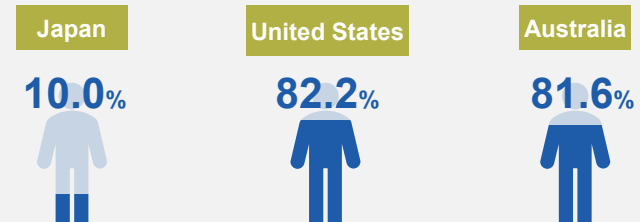
https://www.npa.go.jp/bureau/cyber/pdf/R07_cyber_jousei.pdf

Rapid Shift of Companies to Digital Technologies



Shortage of security personnel

—Degree of sufficiency for personnel engaged in security measures (by country)—^{*5}



Source 3: The ICT Transformation Solution Market in the New Normal Era Accelerated by the After/With-COVID Era, Fuji Chimera Research Institute, Inc.

Source 4: 2020 Future Outlook of the Digital Transformation Market, Fuji Chimera Research Institute, Inc.

Source 5: Survey on Information Security in Enterprises 2020, NRI Secure Technologies, Inc.

Financial Highlights

Fiscal Period		FYE3/2022	FYE3/2023	FYE3/2024	FYE3/2025	FYE3/2026
Net sales	(Thousands of yen)	4,391,317	5,558,022	7,002,941	8,801,647	11,022,080
Ordinary income	(Thousands of yen)	414,331	737,512	1,104,319	1,562,981	2,222,786
Net income	(Thousands of yen)	261,099	488,120	783,428	1,010,077	1,486,742
Share capital	(Thousands of yen)	485,000	529,833	544,999	545,921	546,553
Number of shares outstanding	(Shares)	3,327,000	7,383,000	7,629,600	7,644,600	15,309,600
Net assets	(Thousands of yen)	1,565,478	1,720,169	2,433,625	3,078,911	4,401,238
Total assets	(Thousands of yen)	3,482,070	4,124,589	6,536,708	8,141,157	9,959,520
Net assets per share	(Yen)	117.63	118.13	161.54	205.08	292.4
Dividends per share (of which interim dividends per share)	(Yen)	3.75 (-)	7 (-)	13.11 (-)	20.86 (10.43)	34.60 (16.36)
Basic earnings per share	(Yen)	20.23	36.10	52.42	67.24	98.85
Equity-to-asset ratio	(%)	44.96	41.71	37.23	37.8	44.2
Return on equity	(%)	20.82	29.71	37.72	32.8	39.8
Dividend payout ratio	(%)	18.5	19.4	25.0	31.0	35.0
Operating cash flow	(Thousands of yen)	328,219	594,948	713,549	1,018,887	1,134,568
Investment cash flow	(Thousands of yen)	(294,649)	(212,159)	(2,005,260)	(411,367)	(151,230)
Financial cash flow	(Thousands of yen)	460,634	(455,995)	1,447,820	(457,415)	(725,700)
Cash and cash equivalents at end of period	(Thousands of yen)	1,146,528	1,073,322	1,229,432	1,379,536	1,637,175
Number of employees	(Persons)	118	138	154	195	221

Note 1: As consolidated financial statements have been prepared since the fiscal year ended March 31, 2025, non-consolidated financial statements are presented for prior fiscal years.

Note 2: A 300-for-1 stock split of common stock was conducted on October 22, 2021, a 2-for-1 stock split of common stock was conducted on November 1, 2022, and a 2-for-1 stock split of common stock was conducted on June 1, 2025. Net assets per share and basic earnings per share were calculated based on the assumption that the stock split was conducted at the beginning of the fiscal year ended March 31, 2021. Also, dividends per share (of which interim dividends per share) represent the amount after taking into account the stock split.

This document contains forward-looking statements about Global Security Experts, Inc.'s financial results, business operations, and industry trends that are based on Global Security Experts, Inc.'s current plans, estimates, forecasts or projections.

Various risks and uncertainties are inherent in these forward-looking statements.

Known or unknown risks, uncertainties, and other factors may cause the Company's actual results to differ materially from those contained in any forward-looking statement.

The actual future business activities and performance of Global Security Experts, Inc. may differ from the forward-looking statements described in this document.

Forward-looking statements in this document are made by Global Security Experts, Inc. based on information available at the time of preparation, and will not be updated or modified in any way to reflect future events or circumstances.

Some figures that have not been audited by an auditing firm are included for reference purposes only.

GSX

GLOBAL
SECURITY
EXPERTS