LAC Co., Ltd.

Mid-term management plan

（FY2024-2026）

May 13, 2024

Looking back on the previous mid-term management plan

Differences from previous mid-term management plan target values

The results fell short of targets mainly due to delays in creating growth investments, including business opportunities and M&A, and improving productivity, despite growing from the time of making the plan

(Billion yen)

Subjects	FY2020	FY2023 Mid-term management plan goals	FY2023	Difference	
				In comparison with FY2020	In comparison with Targets
Net Sales	43.6 Security business 18.6 SI business 25.0	55.0 Security business 25.5 SI business 29.5	49.4 Security business 22.1 SI business 27.3	+5.7 **(+13.2%)**	-5.5 **Achievement rate 90.0%**
Operating income	2.1	3.0	2.1	+0.0 **(+2.7%)**	-0.8 **Achievement rate 72.5%**
ROE	2.6%	10% above	9.1%	+6.5pt	-0.9pt

Progress status of previous mid-term management plan

Main achievements

1 Endurance

- High-added-value services and recurring projects were expanded, centered on individual monitoring services based on the recognition level of security measures

2 Adaptability

- Automation × know-how-based diagnostic services were expanded
- AI-based financial crime preventive solutions were rolled out

3 Leveraging digital capabilities

- The internal IT environment × Zero Trust based on a telework system were advanced
- Generative AI was internally developed and utilized. Services were rolled out to offer support in adoption, diagnosis, etc. to other companies

Recognition of issues

The roll-out of services through digitalized business know-how by the Security Business has a long way to go

The advancement of management DX was delayed considerably partly due to the termination of in-house development of a backbone core system

New mid-term management plan

Awareness of the business environment surrounding LAC

IT Environment

Digital utilization is more diverse, extensive, and deeper

Connection between systems spreads widely and interdependency is more complex and deepened

Cybersecurity is essential everywhere

- Cybersecurity is a key industry for a digital society
- Significant lack of security personnel

Cyber threats become more serious

Business shutdown is a real threat, and financial crime too is growing rapidly

Malicious use of AI and other advanced technologies (including fake works, etc.) becomes noticeable

- It is essential to use technology better than attackers do

Demands from a national security perspective also mount

The perspective of national security that protests freedom and democracy in cyber space becomes essential in order to run business and live in an IT environment that has become social infrastructure

- Cybersecurity becomes the key to national security

Issues in society (customers)

Pursuit of cost-effectiveness that justifies digital utilization

- Higher efficiency of measures through AI and automation
- Easy-to-understand and affordable countermeasures

Response to complicating and sophisticating threats

- From points (case-by-case measures) to lines and planes (comprehensive measures)
- Requests for advanced financial crime preventive measures

Ensuring resilience throughout supply chains

- Security measures for middle-scale and small and midsize companies
- Security measures in overseas bases
- Consideration of and measures against business shutdown

Ensure the continuity of security measures

- Formulation and continuous operation of investment strategy for digital security

Ensure economic security

- Supply chain measures for critical infrastructure providers
- Security vendor that can compete on the international stage

Requests to LAC concerning Social Issues

Equipped with knowledge (intelligence) based on about 30 years of experience in the field

As a group with expertise in cybersecurity measures

Response leveraging automation and AI

Digitize people's know-how by utilizing AI and offer sophisticated and cost-effective services

Response with comprehensive service capabilities

Provide one-stop and optimal services against cyber threats that become more complex and sophisticated than ever before

Provide services that connect to measures for middle-scale and small and midsize companies

Further enhance the added value of Security business and SI business and advance new value creation from a medium- to long-term perspective

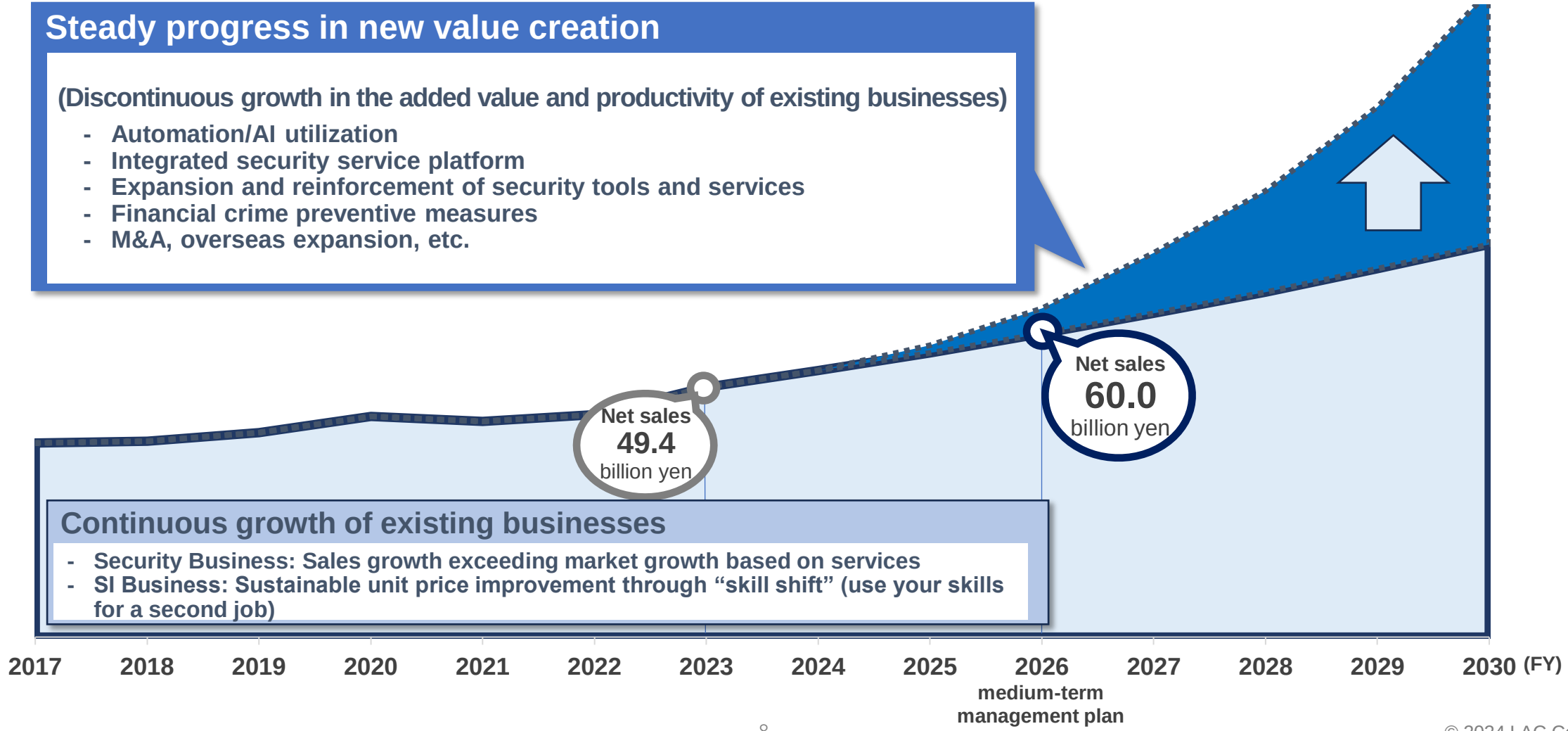
Towards mid- to long-term value creation

Set mid-term management plan targets with the continuous growth of existing businesses at the center and aim at higher growth through taking medium- to long-term measures

Steady progress in new value creation

(Discontinuous growth in the added value and productivity of existing businesses)

- Automation/AI utilization
- Integrated security service platform
- Expansion and reinforcement of security tools and services
- Financial crime preventive measures
- M&A, overseas expansion, etc.



Continuous growth of existing businesses

- Security Business: Sales growth exceeding market growth based on services
- SI Business: Sustainable unit price improvement through “skill shift” (use your skills for a second job)

New mid-term management plan goals

Target net sales of 60 billion yen, operating income and ordinary income each of 4 billion yen and ROE of 15%

Aim to surpass the targets through implementing medium- and long-term measures
Continue the policy of shareholder return with DOE of 5% as the basic indicator

（Billion yen）

Subjects	FY2023	FY2026 Mid-term management plan goals	Increase/decrease	
			Difference	Change
Net sales	49.4	60.0	+10.5	+21.3% （CAGR+6.6%）
Operating income	2.1	4.0	+1.8	+83.9% （CAGR+22.5%）
Operating income ratio	4.4%	6.7%	+2.3pt	-
Ordinary income	2.1	4.0	+1.8	+87.6% （CAGR+23.3%）
ROE	9.1%	15.0%	+5.9pt	-

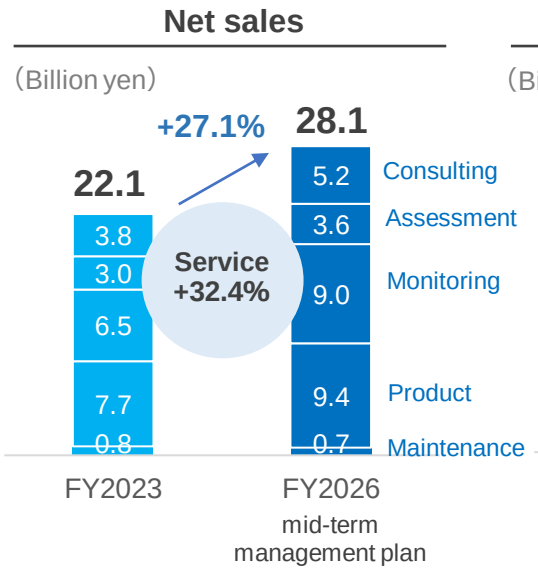
Shareholder Returns
Distribute profit by taking into account investment and the status of cash flows from a medium- to long-term perspective
DOE（Dividend-to-equity ratio） **Basic indicator 5%**

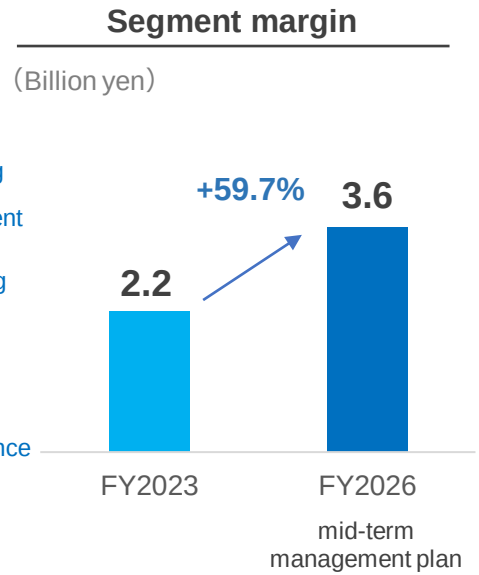
New mid-term management plan　Existing business - by segment

Security business (SSS business)

Expand service business centered on operation monitoring

- Expand consulting projects by increasing recurring ones
- Expand large-scale emergency response service projects by boosting response capabilities
- Expand diagnostic service projects by optimizing the balance between engineers and automation
- Expand comprehensive and all-encompassing operation monitoring service projects from individual monitoring
- Expand large-scale projects of product sales through continuous cooperation with product venders and consulting capabilities

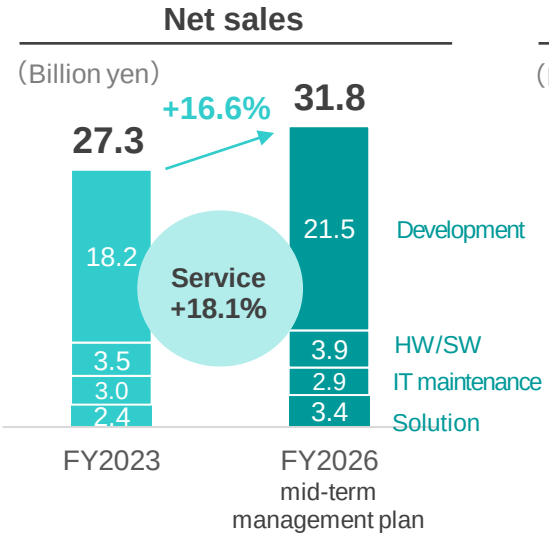


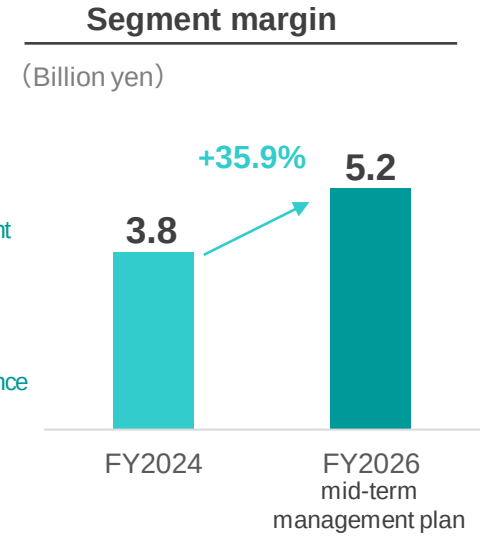


SI business (SIS business)

Drive the skill shift to high-unit-price projects

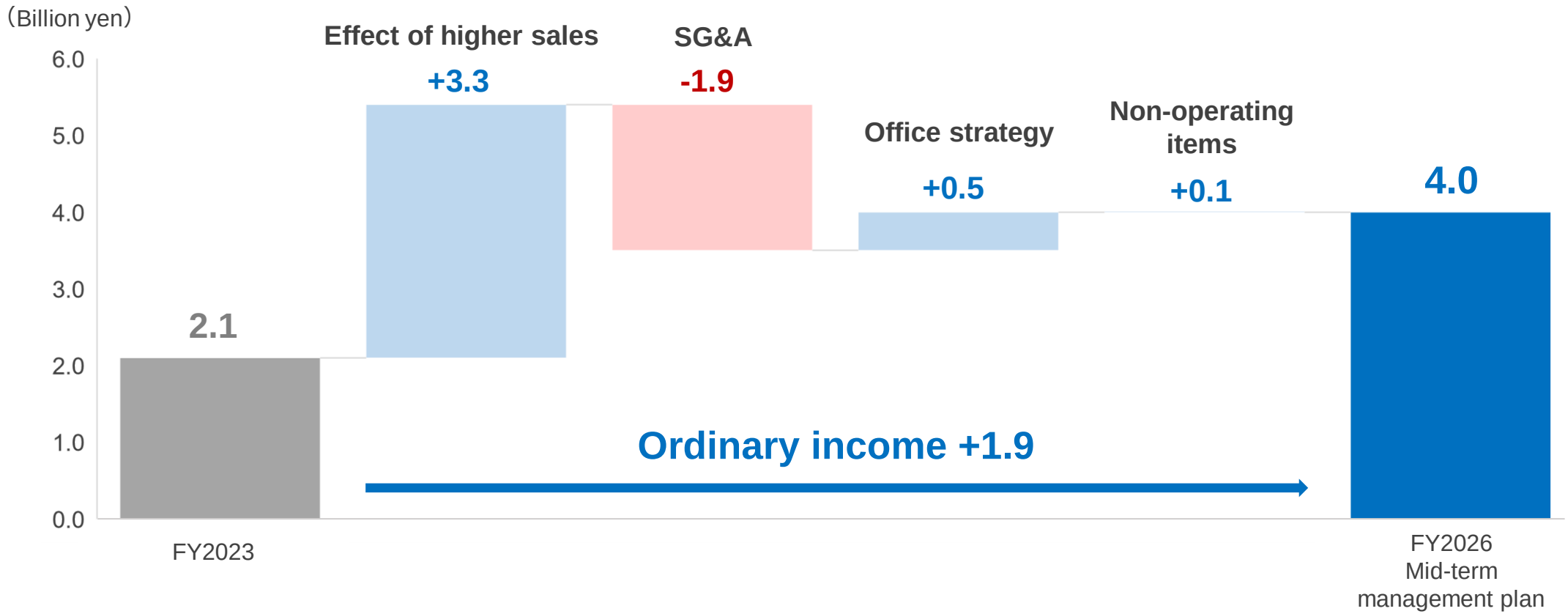
- Expand high-unit-price system development projects with the skill shift to specific technology fields based on solutions
- Secure a certain number of hardware/software (HW/SW) and maintenance projects in response to customer demand such as the return to on-premises
- Expand the continuation of subscription-type solutions that can be a base for specific technological fields





New mid-term management plan
Ordinary Income: Analysis of Factors for Change (YoY Comparison)

Ordinary income is expected to increase mainly due to the effects of higher sales and cost reduction based on an office strategy although expenses are forecast to be pushed up by higher SG&A expenses primarily resulting from strengthening a sales system



(Note) Although expenses for the office strategy are included in SG&A expenses, they are presented individually in the graph.

Steady progress toward new value creation

Combine AI and engineering to enhance the added value and productivity of security services

Strive to create a security tool that can compete on the international stage

AI × Security

Sophistication of threat detection, predictive analysis and response × productivity improvement by integrating AI into various services

Integrated security service platform

Enhancement of the added value of services × productivity improvement by building a foundation that analyzes and utilizes data collected from each service in a comprehensive manner

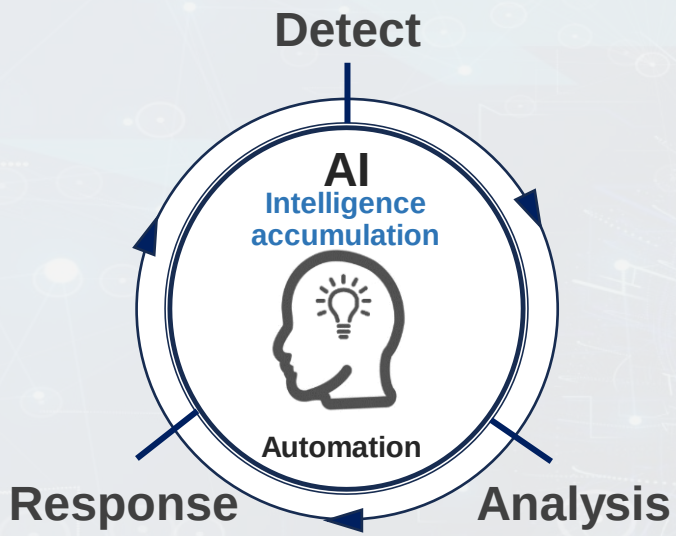
Security tools

Acquire tools that can compete on the international stage with an eye on strategic cooperation with security tool venders

AI ✕ Security

Sophisticate services and respond to rapidly expanding needs by replacing human handling with AI and automation

Respond to the needs of small and midsize companies through strengthening market competitiveness, and new services with high cost-effectiveness



Excellent track records that secure superiority, centered on large companies

- Number of JSOC clients
  Approx. 1,000 companies
- Number of cases diagnosed
  Cumulative total of approx. 27,500
- Number of emergency cases responded to
  Cumulative total of approx. 4,800

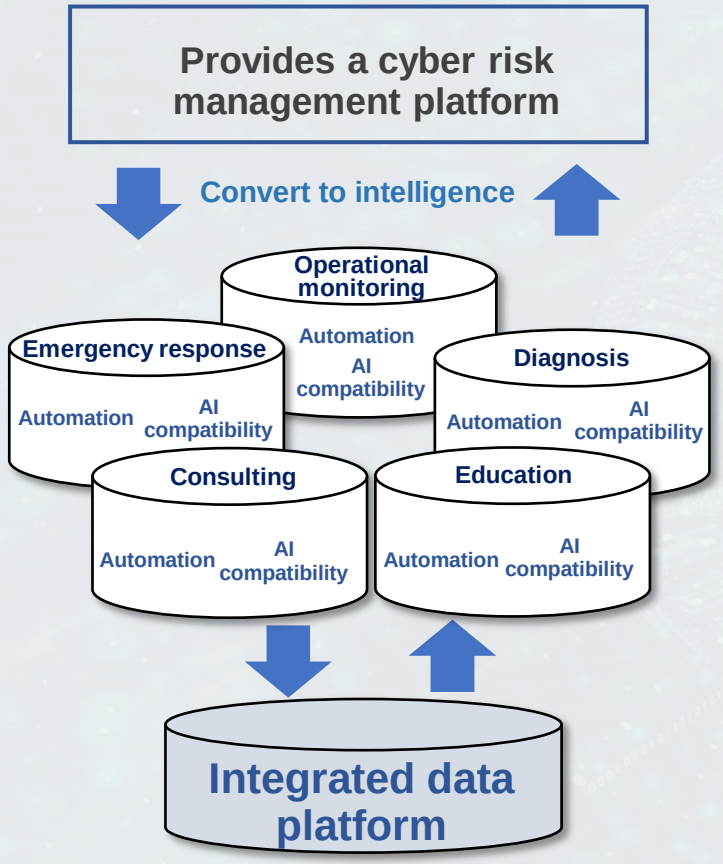
Service points (provided value)

- Advanced analysis of large volumes of accumulated threat data
- Enhancement of productivity by replacing human handling with AI and automation
- Development of new analytical tools against increasingly deceiving and evolving attacks
- Provision of services even covering small and midsize companies by leading automation to development of new services with high cost-effectiveness

Integrated security service platform

Elevate from operational monitoring to cyber risk management

Integrate the data analysis and utilization platforms of various security services



Service points (provided value)

- **Integrate and visualize cyber risks that are fragmented across networks, applications, terminals, etc.**
- **Improve convenience by providing customers that have already adopted diverse tools with an integrated platform**
  (Examples of tools: SASE, UEBA, CASB)
- **Provide optimal measures to customers by leveraging knowledge gained from integrated data platforms**
- **Plan to provide even to large-scale group companies**

SASE: Secure Access Service Edge. UEBA: User and Entity Behavior Analytics
CASB:Cloud Access Security Broker

Security tools

Pursue the acquisition of new security tools, including alliances with other companies, by leveraging the knowledge (intelligence) gained from approximately 30 years of experience in the field

Example of promotion of alliances

Operational monitoring

AI and automation × Threat Intelligence
(Joint venture with NRI)

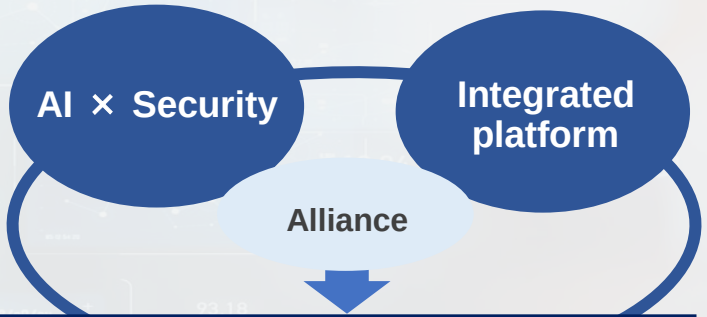
Diagnosis

AI and automation × Know-how
(In cooperation with Aeye Security Lab, Inc.)

Examples of tools developed in-house

Malware investigative tools "FalconNest"

PC self-diagnosis tool "Jishin-kun"



Grow into new security tools

Service points (provided value)

- Acquire security tools through coordination with threat intelligence of AI × security, integrated security services platforms, etc.

  Strategic alliance and acquisition are options in addition to in-house development

- Expand even into the security market for middle-scale and small and midsize companies

  Further sophisticate services by broadening the activity fields and accumulating intelligence

Purpose Vision upheld by LAC

Purpose

“Building a Trusted Society With Reliable Technology”

As the digital society becomes more sophisticated and complex, we will build safe and secure social infrastructure by utilizing a variety of highly sophisticated technologies and realize a society where people can support each other and be happy.

Vision

We aim to “become a role model for surviving in the digital society.”

We will continue to maintain the pioneering spirit that has led Japan's cybersecurity, protect people's activities in an increasingly deepening and sophisticated digital society, drive the culture of the security industry, and serve as a role model for surviving in the new era.

※ This document was prepared based on information available as of May 13, 2024 and is subject to change without notice.
※ The earnings targets, future forecasts, and other statements presented in this document are based on forecasts or assumptions based on information available at the time this document was prepared by the Group and are subject to direct or indirect impacts from various changes in the operating environment, including economic conditions and social trends. Accordingly, actual results, strategies, or other information may differ considerably from the forecasts or assumptions