Securities Code:4258

AMIYA Corporation

Financial Results Presentation Materials

AMIYA

Q3 FY 12/2026

01

Company Overview

AMIYA is a comprehensive provider of made-in-Japan cybersecurity solutions

Identity

AMIYA

Building sovereign cyber defense capability is a first-order priority for Japan—critical to the nation's economic security, and equally so to how companies invest in managing their own risk.

AMIYA is a comprehensive provider of made-in-Japan cybersecurity solutions, with core competitive advantages in proprietary security software and service development.

Harnessing our proprietary AI attack detection and cloud network virtualization technologies, we deliver security through a next-generation cyber network.



SECURE THE SUCCESS.

Deliver certain success for businesses built on safety and security



ProductxService

AMIYA is a comprehensive cybersecurity provider, offering both proprietary products and managed services



One-stop Vendor

A one-stop shop security platform, handling the entire lifecycle from R&D to go-to-market



SecurityxNetwork

Team of professionals with core competencies in both cybersecurity and networking (ICT)

Copyright @ AMIYA Corporation

AMIYA's core products and services are developed and operated in-house

domestic

Data Security Business

Accessible SIEM **ALog** Over 6,500 contracts *cumulative



Comprehensive Cybersecurity services

NATURE SERIES



Cloud-based CSIRT services

セキュサポ



Network Security Business

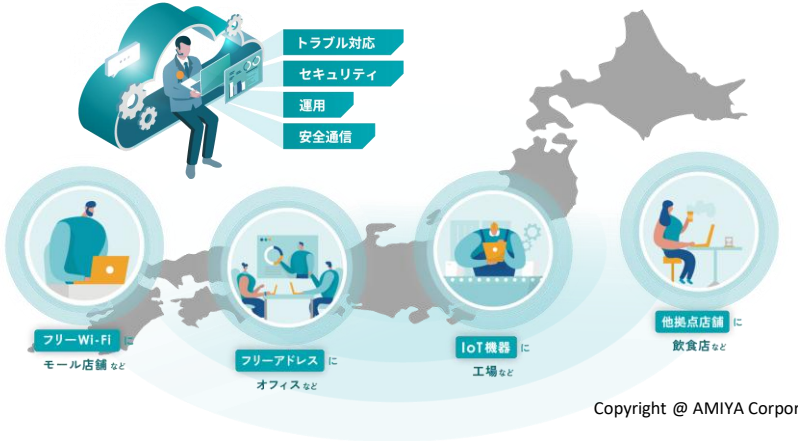
Fully managed SASE **Verona** Over 6,200 contracts *cumulative

*Network All Cloud—Track Record



Cloud-based Wi-Fi

Hypersonix



Copyright @ AMIYA Corporation

AMIYA's performance over the last three years

Looking back at the previous MTP (FY2023 - 2025) we successfully **doubled revenue and ARR**, while driving a **four-fold increase in operating profit**. Subscription-driven contract liabilities (advances received) **doubled**, alongside a **three-fold increase in EPS**.

Revenue/FY2025

¥5.94 B

2.0x vs. prior 3 yrs.

Operating Profit/FY2025

¥1.05 B

4.0x vs. prior 3 yrs.
OP Margin 17.7%

ARR/EoFY2025

¥3.80 B

At least 60% of total revenue comes from recurring subscriptions

Contract liabilities/EoFY2025

¥2.06 B

2.4x vs. prior 3 yrs.

EPS/FY2025

¥90.8

3.2x vs. prior 3 yrs.

Annual Client Churn (ALog) / FY2025

3-yr avg. 0.8%

Industry avg:
5% - 15%

Achievement

Copyright @ AMIYA Corporation

AMIYA by the Numbers

Track Record 10K+

Extensive sales track record as a vendor of made-in-Japan security solutions geared primarily toward large enterprises

Number of enterprise contracts (cumulative):
DS Business: **6,500** NS Business: **6,200**

Made-in-Japan SIEM Market Share No.1

After dominating the domestic market, we are expanding into the global SIEM market

Global SIEM market is expected to reach **¥1.8** trillion by 2030

Major channel partners 40+

Many of our channel partners are prominent IT vendors and wholesale distributors

Fujitsu, NEC, Hitachi Group, OTSUKA CORP, HP Japan, and many others

Recurring Revenue 60%+

Recurring revenue from subscriptions now accounts for over half of all revenues

Shifted to subscription model in earnest in 2024

ARR* 4-fold growth

Predictable profitability is non-negotiable for a growth company

On track for a 4-fold increase from **¥1.8** B (2022) to **¥7.2** B (2028)

*ARR: Annual Recurring Revenue

Market CAGR 20%+

Global market for cybersecurity solutions is a growth sector

SASE CAGR is expected to grow **24%** between 2025 and 2030

Retention Rate 99%

Client trust is vital in the cybersecurity industry. Low subscription churn numbers are the key to unlocking a high LTV

DS Business:
ALog churn rate: **0.7%**

NS Business:
Network All Cloud churn rate: **1.2%**

*As of Q3 2026



R&D Investment 4 x the industry avg.

R&D to revenue ratio of 4.7% is above the industry average

Median
All industries: 1.2%
ICT: 3.1%

20+ annual releases

Copyright @ AMIYA Corporation

02

Financial Highlights

AMIYA

Raised our full-year forecast on Oct. 27 following strong sales performance

Revenue Rev

FY2025 Q3
¥4,212 M

FY2026 Q3
YoY+26.3%
¥5,320 M

Full Year Forecast
¥7,002 M

Progress
76.0%

Revised Full Year Forecast
¥7,850 M

Progress
67.8%

Operating Profit OP

FY2025 Q3
¥795 M

FY2026 Q3
YoY+29.6%
¥1,030 M

Full Year Forecast
¥1,200 M

Progress
85.9%

Revised Full Year Forecast
¥1,470 M

Progress
70.1%

Profit attributable to owners of parent NI

FY2025 Q3
¥538 M

FY2026 Q3
YoY+30.6%
¥702 M

Full Year Forecast
¥850 M

Progress
82.7%

Revised Full Year Forecast
¥1,003 M

Progress
70.1%

Copyright @ AMIYA Corporation

AMIYA

Revenue across all product lines exceeded prior-year levels, growing by up to 34% YoY

National policy driving demand Growing interest in made-in-Japan solutions

The SCS Assessment System helped drive YTD Q3 revenue growth across all product lines, with SI leading the pack at +34% YoY.

The surge in cyberattacks that began in September will likely drive further interest in made-in-Japan products.

Consistent margin expansion fueled by strong orders and ARR growth

While we planned for heavy upfront investments this year, stronger-than-expected order volume absorbed the costs.

YTD Q3 operating margin reached 19.4%, and our steady ARR growth ensures sustained high profitability.

Solid momentum in flagship log products; Promising SASE surges

ALog—which boasts a gross margin over 70%—saw revenue grow 27.6% YoY and cumulative orders jump 44.6% YoY.

Network All Cloud (including SASE) posted 26.3% YoY revenue growth and a 49.0% YoY increase in licenses.

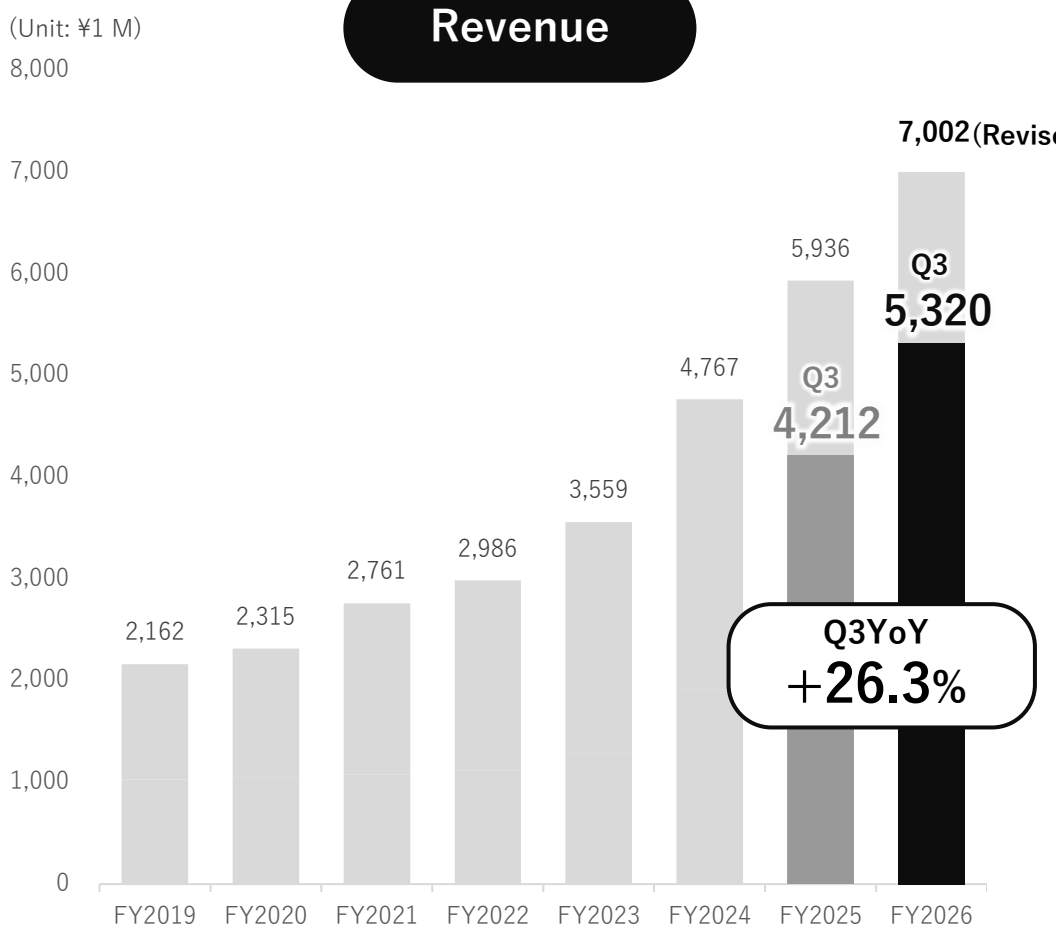
Copyright @ AMIYA Corporation

AMIYA

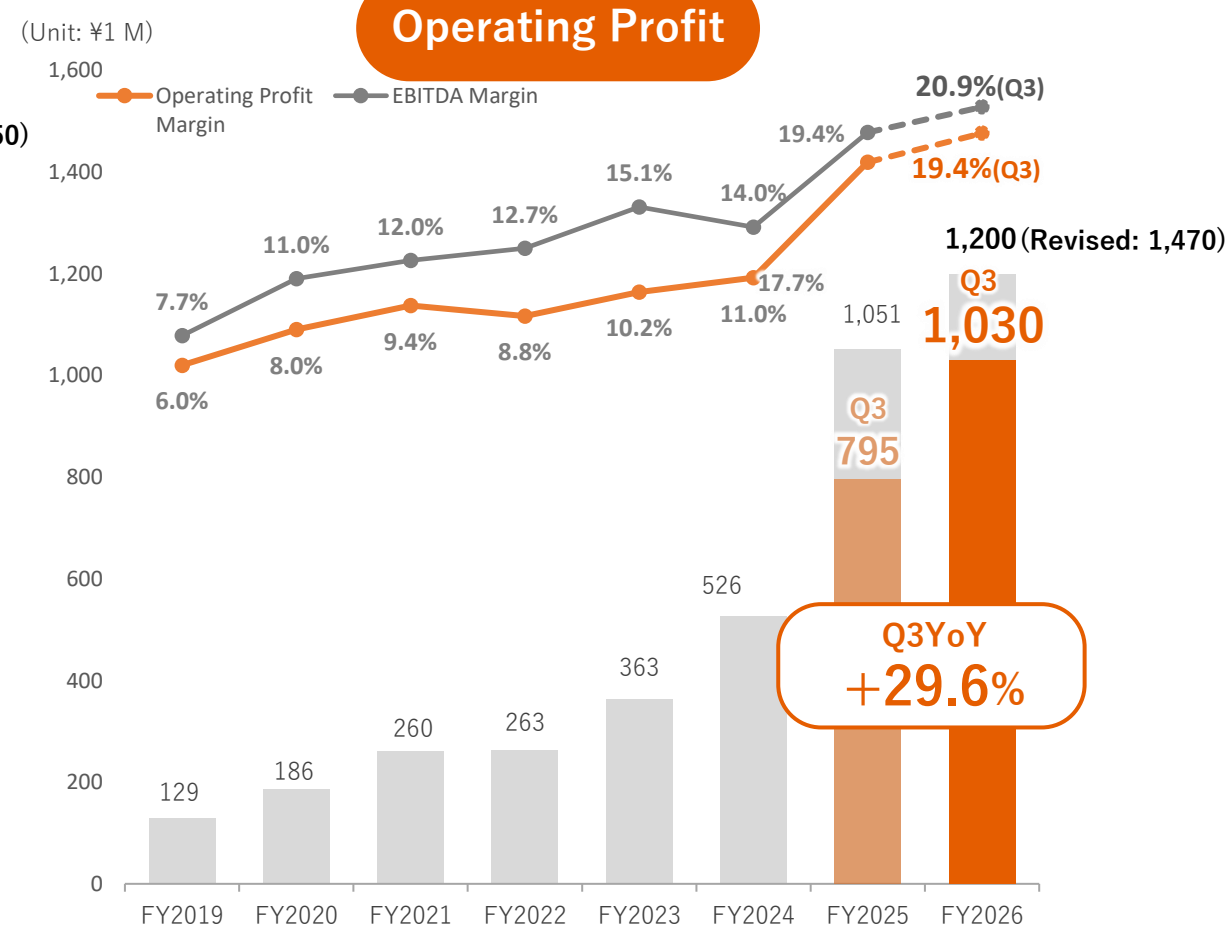
Operating margin continues to expand despite heavy upfront investments

Top-line revenue grew 26.3% YoY and operating profit surged 29.6%, expanding our operating margin to 19.4%

Revenue



Operating Profit

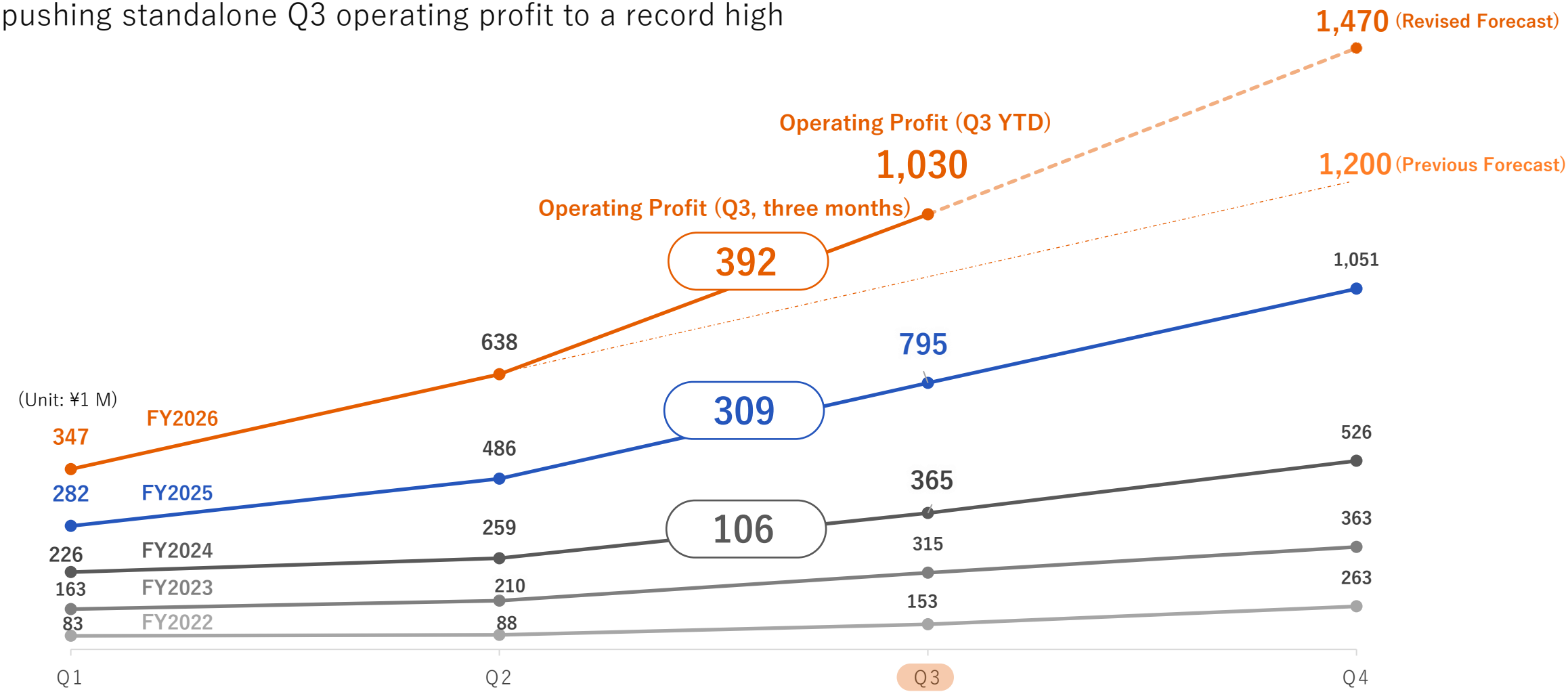


Copyright @ AMIYA Corporation

OP Quarterly Trend

Compounding subscription ARR is driving a sharp acceleration in profitability

Compounding subscriptions are accelerating profit growth, pushing standalone Q3 operating profit to a record high



Copyright @ AMIYA Corporation

AMIYA

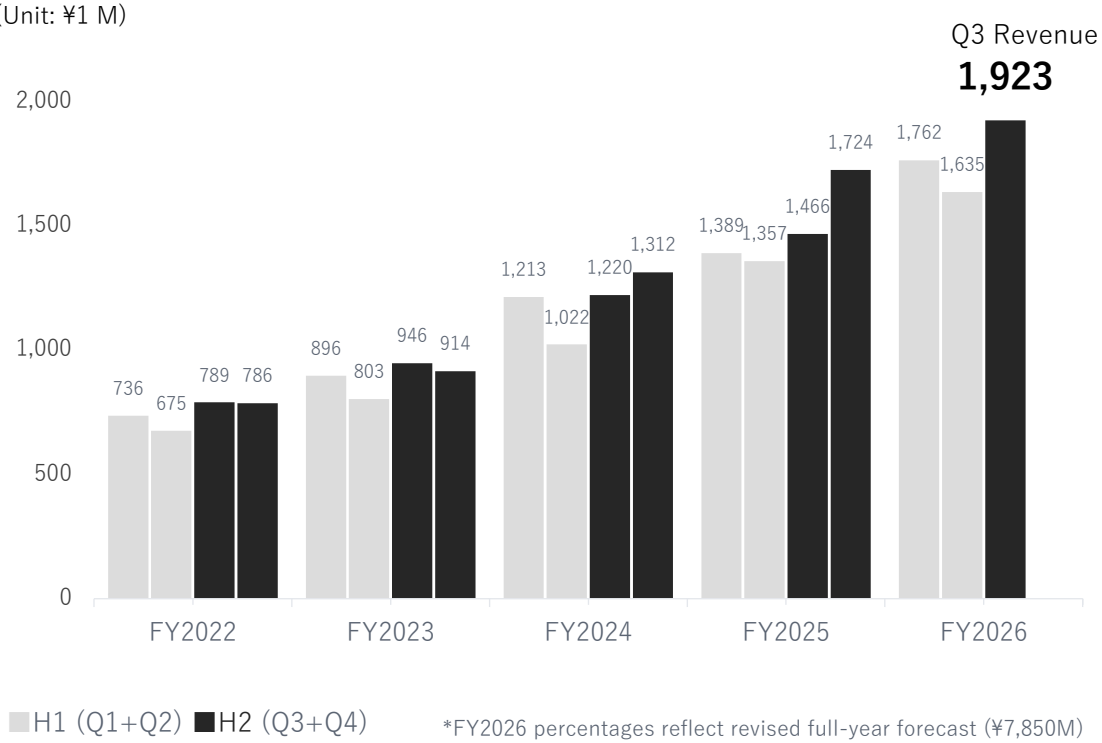
Historically, our business tends to be heavily weighted toward H2

Fueled by compounding ARR, both revenue and operating profit continue to skew toward H2 (Jul–Dec).
Q3 standalone operating profit is up 6x over the past four years.

Revenue (Standalone)

FY2022	FY2023	FY2024	FY2025	FY2026
H1 47.3%	H1 47.7%	H1 46.9%	H1 46.3%	H1 43.3%
H2 52.7%	H2 52.3%	H2 53.1%	H2 53.7%	H2 (forecast) 56.7%

(Unit: ¥1 M)

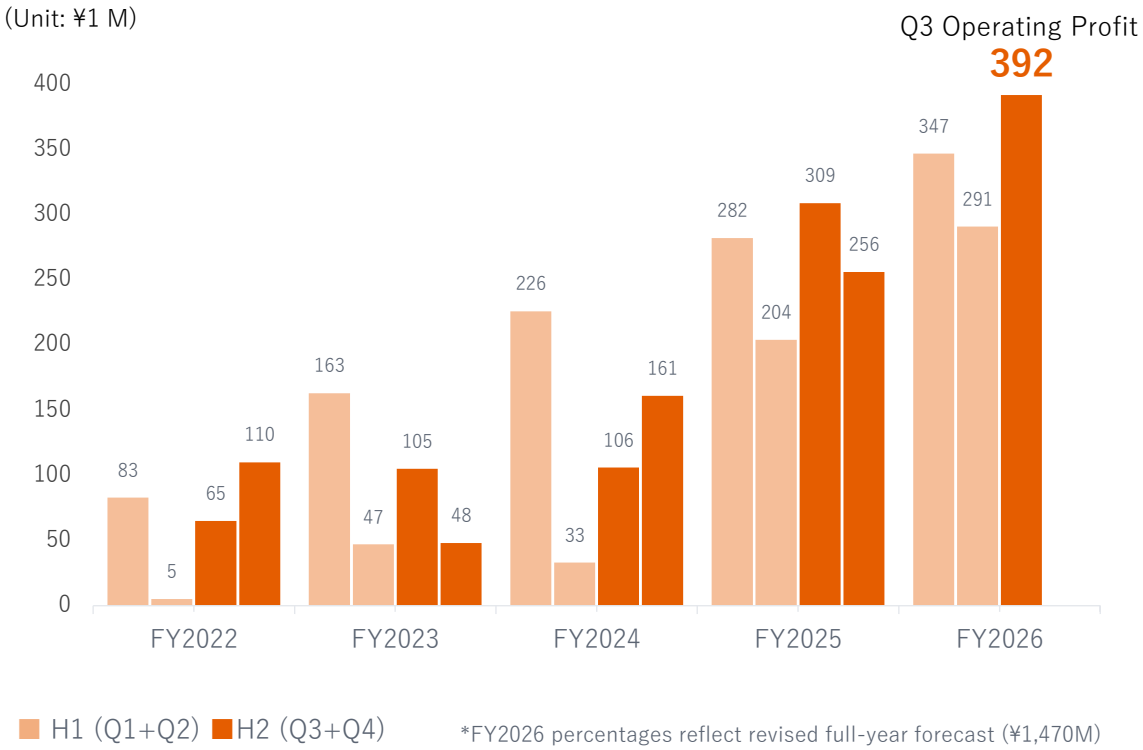


*FY2026 percentages reflect revised full-year forecast (¥7,850M)

Operating Profit (Standalone)

FY2022	FY2023	FY2024	FY2025	FY2026
H1 33.4%	H1 58.0%	H1 49.4%	H1 46.3%	H1 43.5%
H2 66.6%	H2 42.0%	H2 50.6%	H2 53.7%	H2 (forecast) 56.5%

(Unit: ¥1 M)



*FY2026 percentages reflect revised full-year forecast (¥1,470M)

Copyright @ AMIYA Corporation

AMIYA

ARR growth (+34% YoY) continues to outpace total revenue (+26% YoY) as our recurring revenue base scales

Company-wide ARR

QoQ	YoY
+6.3%	+34.0%

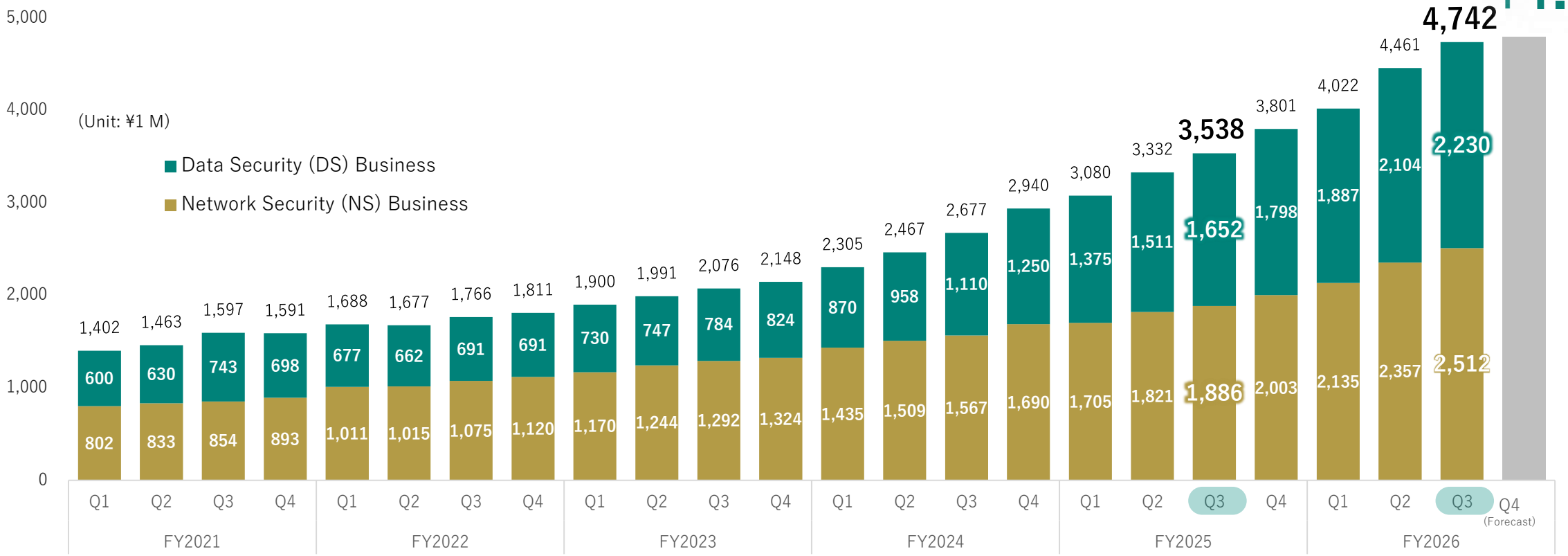
DS Business ARR

QoQ	YoY
+6.0%	+35.0%

NS Business ARR

QoQ	YoY
+6.6%	+33.2%

Initial Target ¥4.8 B

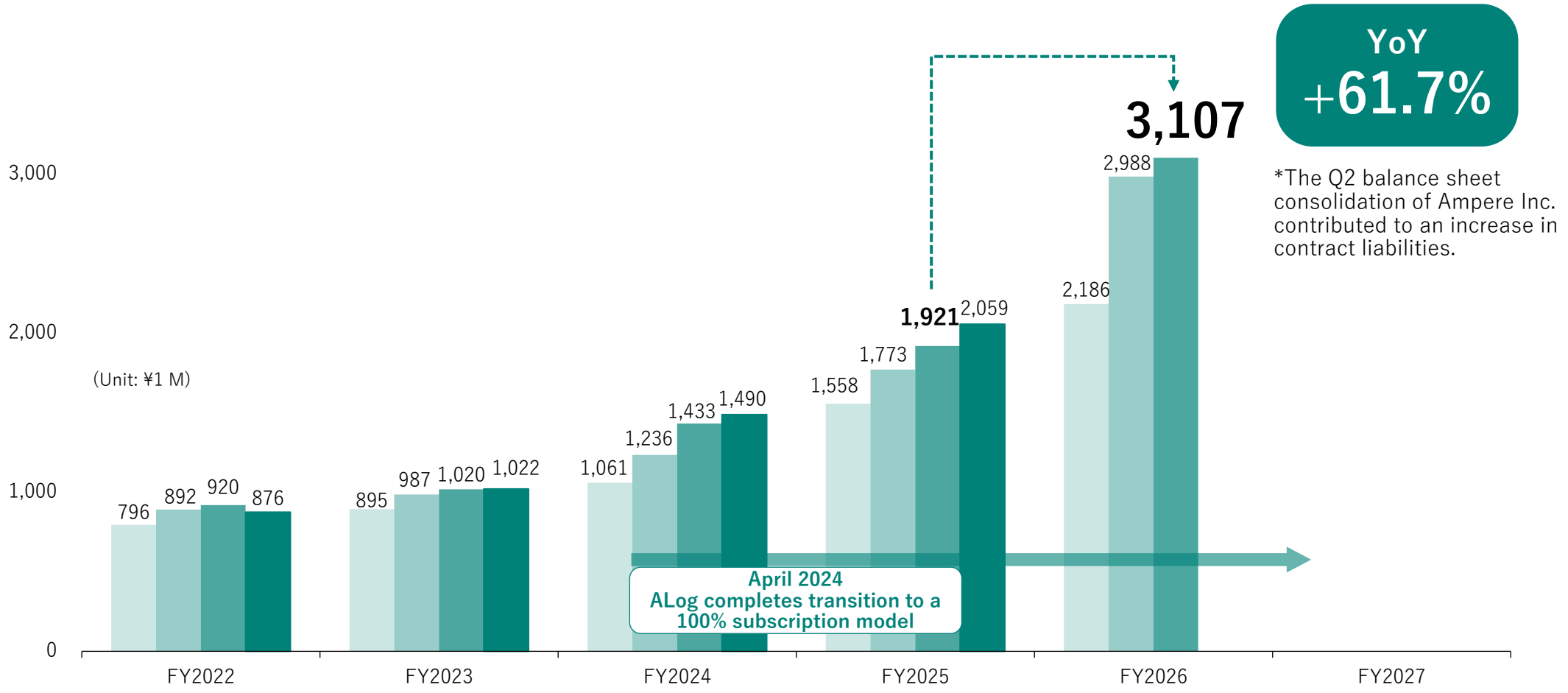


Copyright @ AMIYA Corporation

AMIYA

Contract liabilities increased 61.7% YoY

The growth in contract liabilities underscores a healthy pipeline of future revenue not yet recognized on the P&L

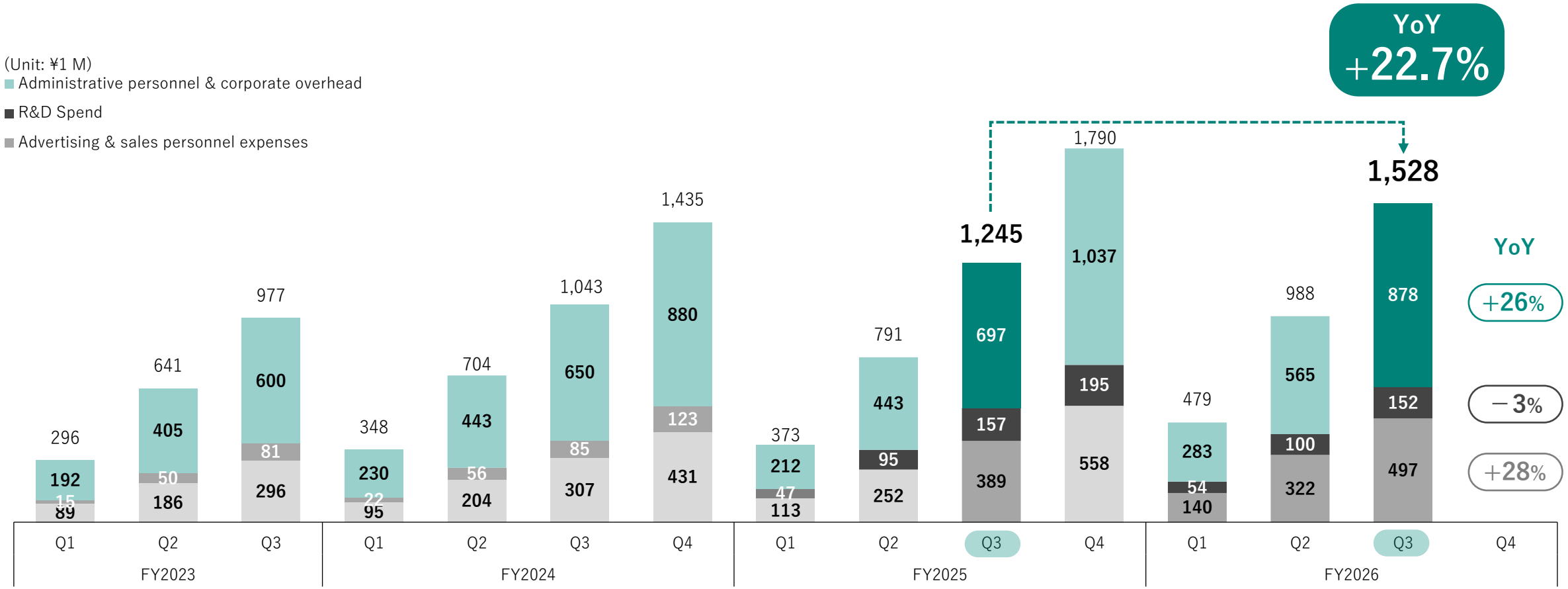


Copyright @ AMIYA Corporation

Quarterly Trends in SG&A

Accelerating marketing and advertising investments to drive made-in-Japan brand awareness

The increase in corporate overhead was driven by financing and M&A advisory fees.
Advertising spend primarily directed at trade shows to capture surging SASE demand.



Copyright @ AMIYA Corporation

Summary by Segment

Japan's focus on economic security is accelerating the adoption of our made-in-Japan solutions

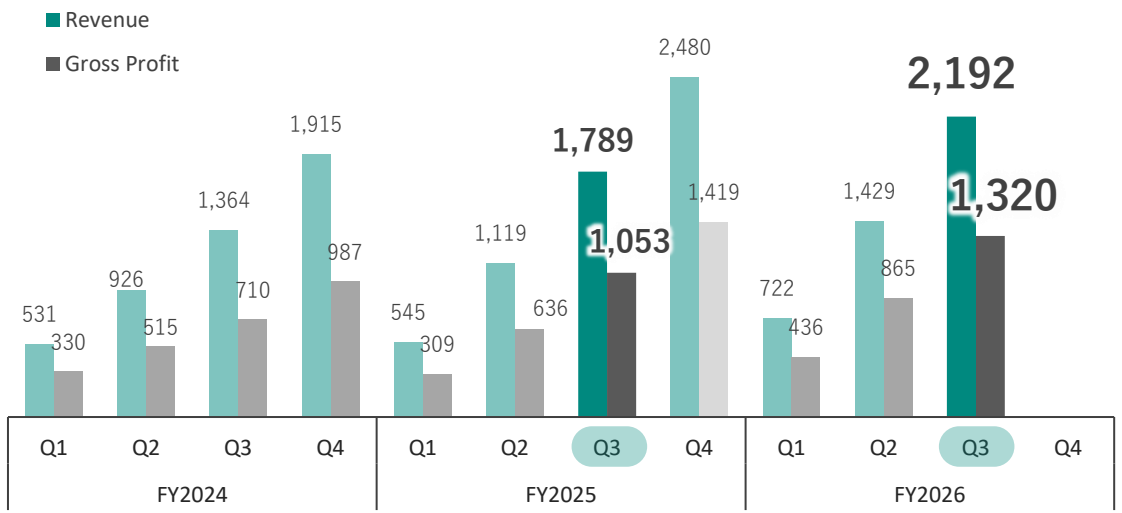
Data Security Business

Spurred by a recent surge in cyberattacks, demand for incident response and SCS Assessment System* compliance is rising.
Order intake from major manufacturing and IT enterprises remains robust.
Our core ALog products continue to drive segment profitability, lifting gross margins to 60%.

FY2026 Q3 YoY

Revenue	Gross Profit	Segment Profit
+22.5%	+25.3%	+38.2%

(Unit: ¥1 M)

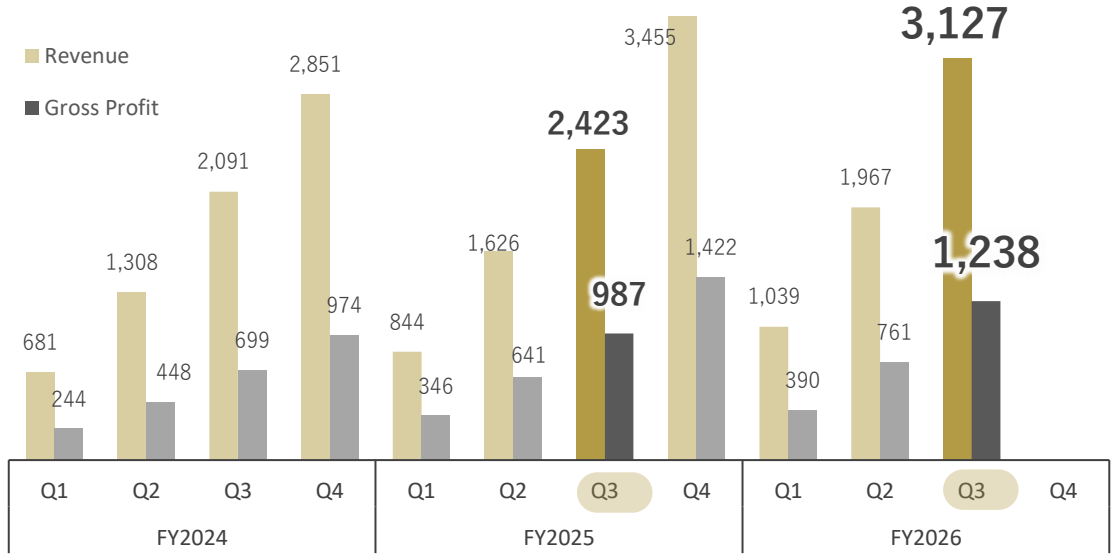


Network Security Business

Robust enterprise SASE demand is fueling growth for our Network All Cloud services.
We anticipate sustained momentum, backed by the platform's proven ability to neutralize ransomware and phishing threats.
Segment margins improved sequentially from H1, absorbing our ongoing investments in marketing and R&D.

FY2026 Q3 YoY

Revenue	Gross Profit	Segment Profit
+29.1%	+25.5%	+18.4%



*SCS Assessment System: A government initiative to strengthen supply chain cybersecurity

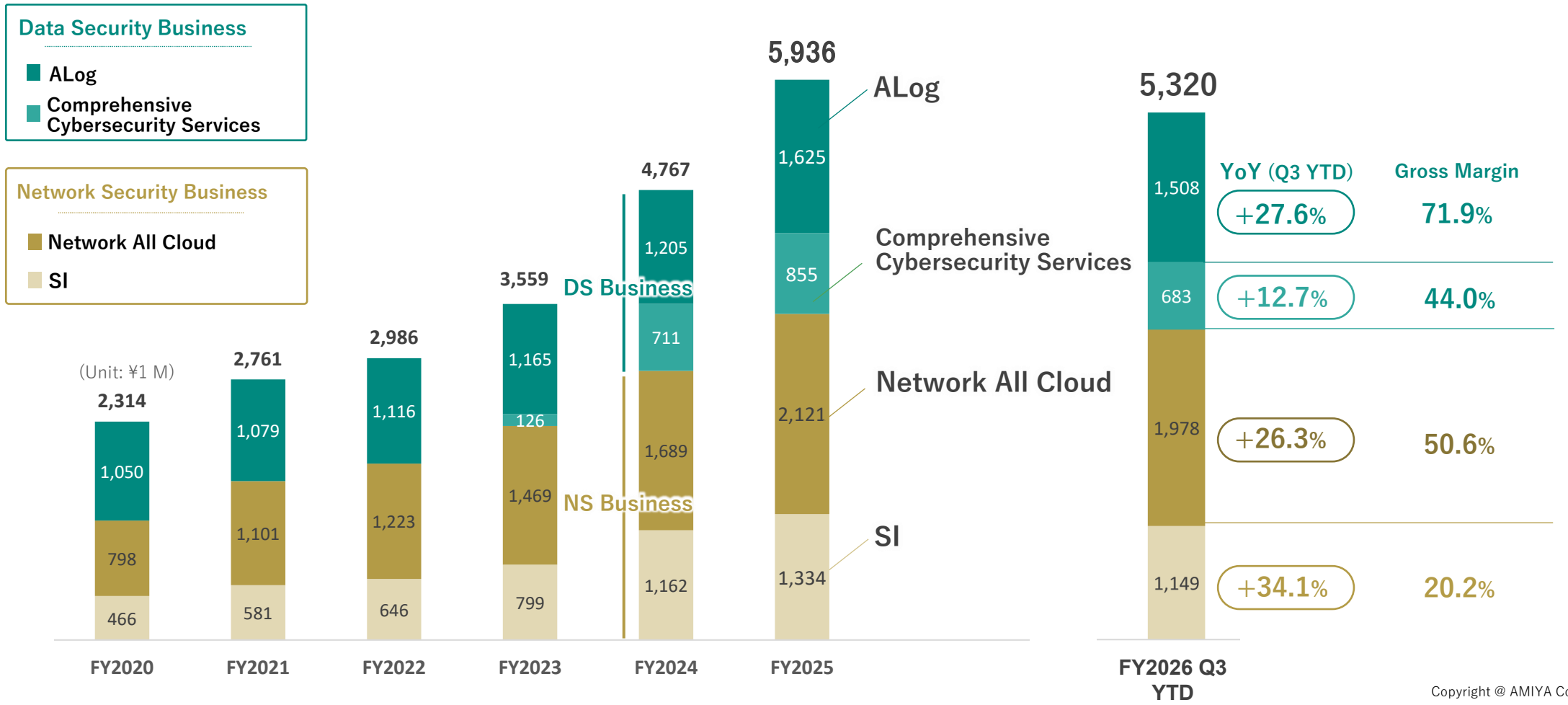
Copyright @ AMIYA Corporation

AMIYA

Revenue by Core Product

High-margin recurring revenue streams—specifically our 100% subscription-based **ALog** and SaaS-driven Network **All Cloud**—**are now scaling rapidly**.

Comprehensive cybersecurity services are also gaining momentum, while our legacy system integration (SI) business continues to deliver steady, lower-margin growth.

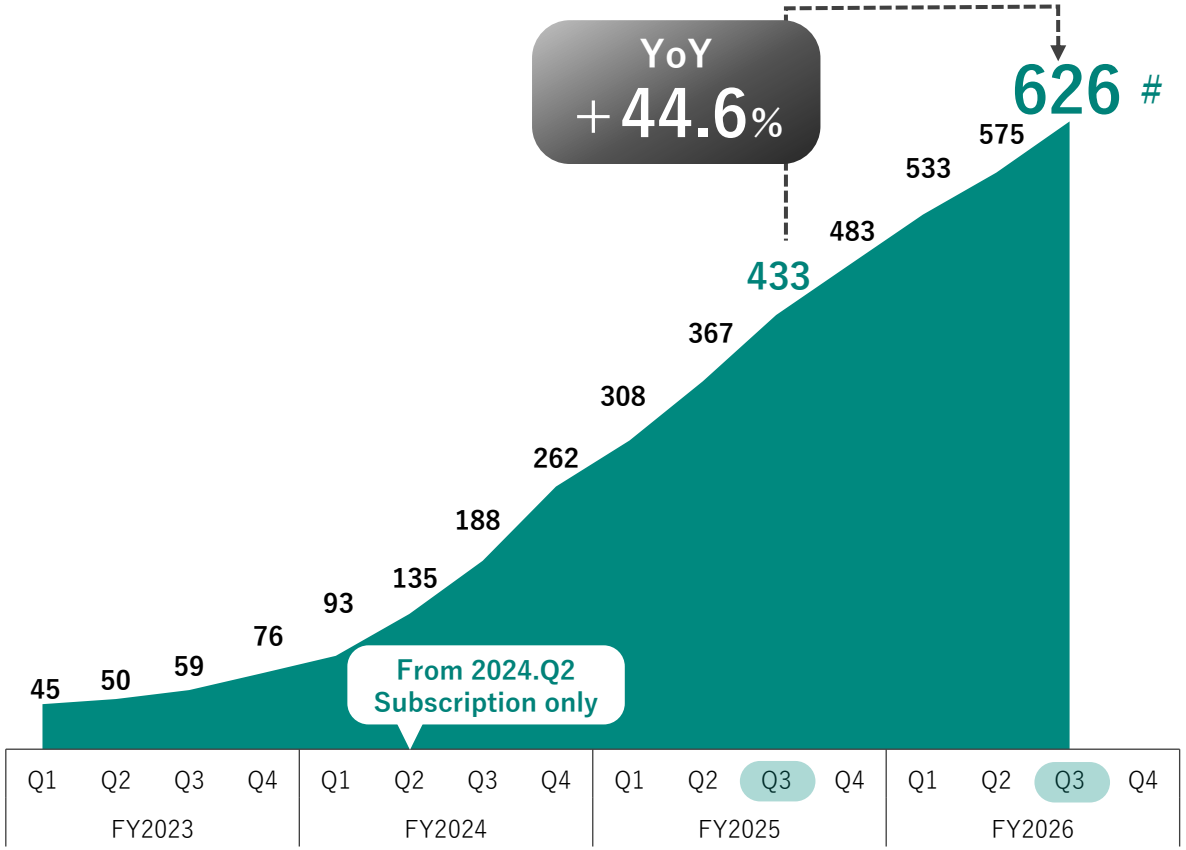


Copyright @ AMIYA Corporation

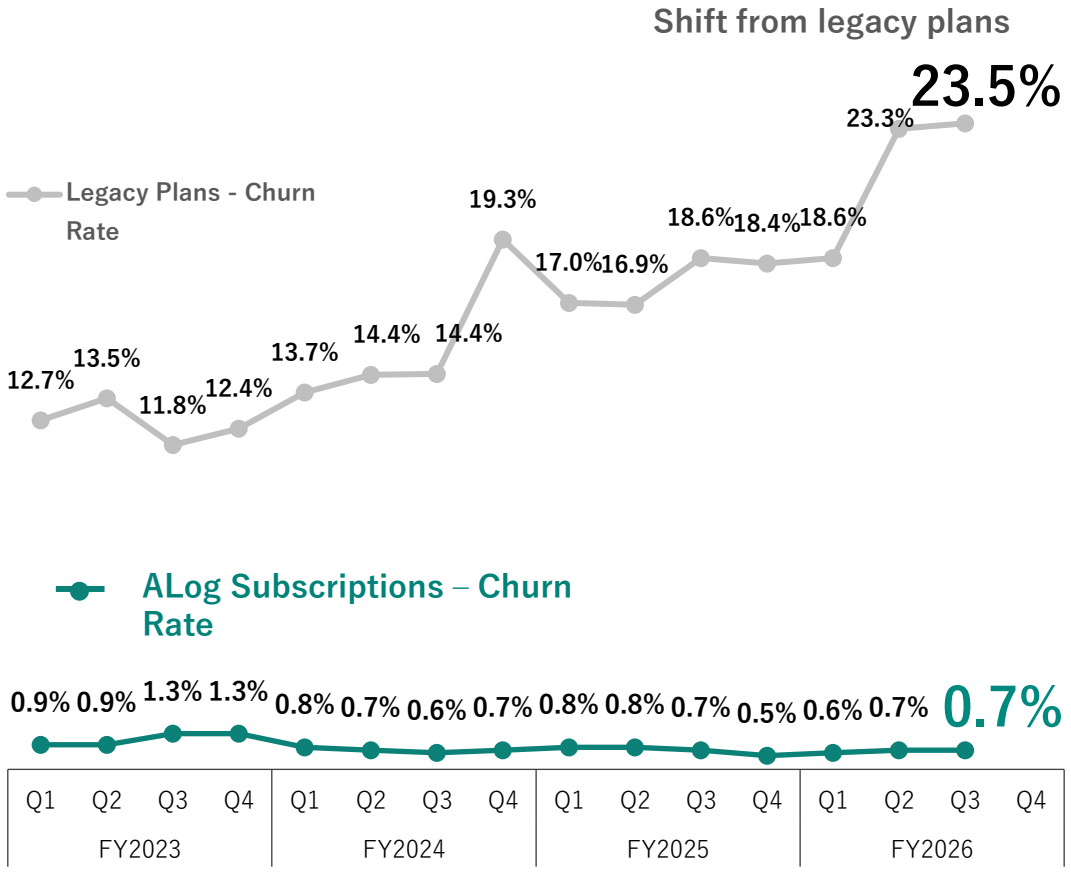
AMIYA

ALog Subscriptions and Churn Rate

Subscriptions (Cumulative)



Annual Subscription Churn

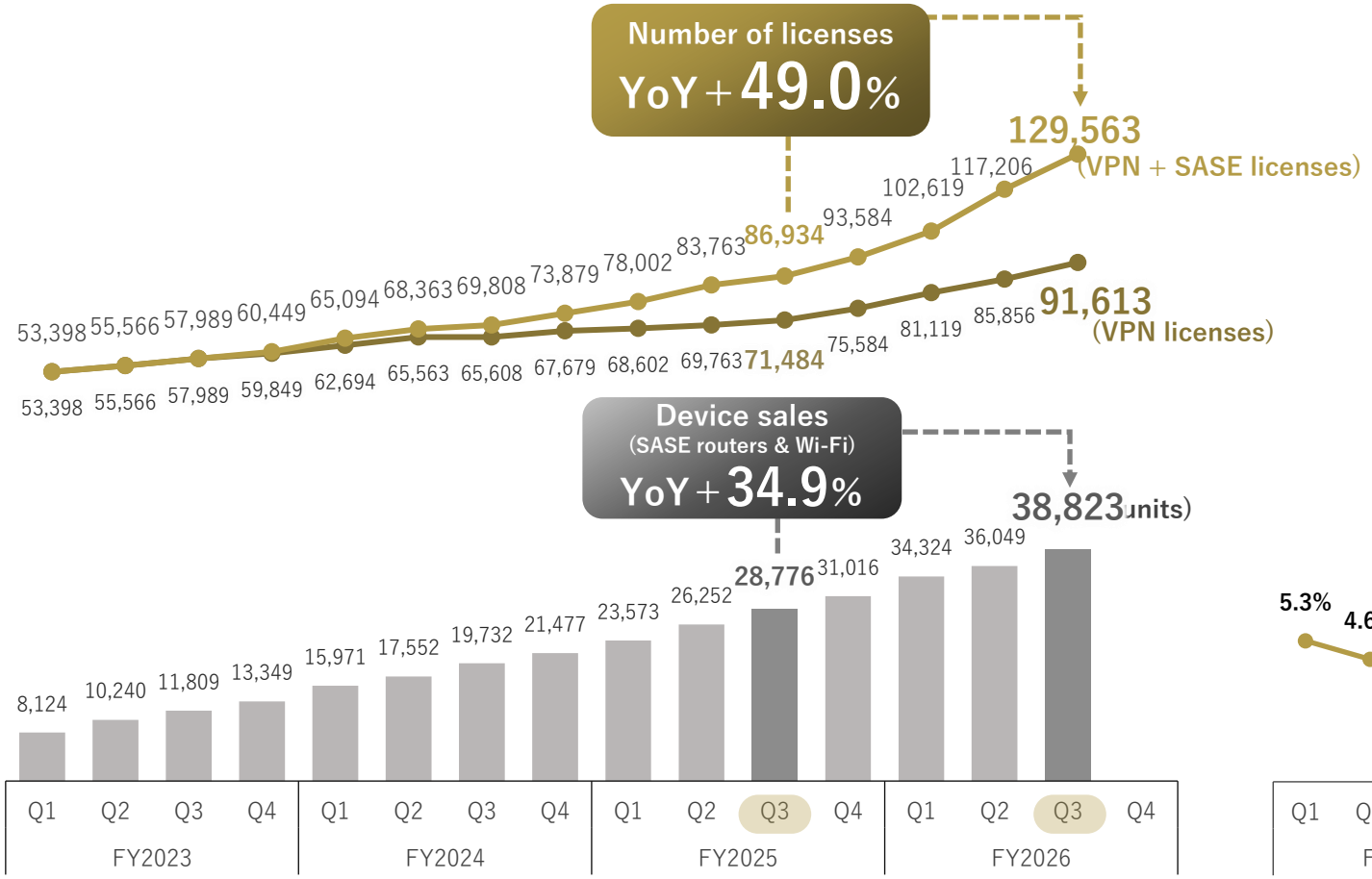


Copyright @ AMIYA Corporation

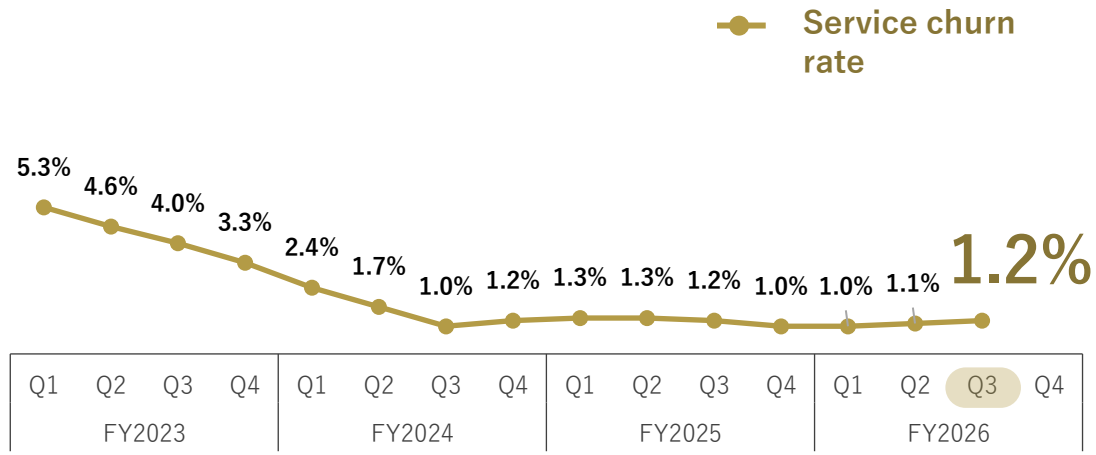
AMIYA

Network All Cloud® Subscriptions and Churn Rate

Devices / Licenses (Cumulative)



Annual Service Churn



Copyright @ AMIYA Corporation

03

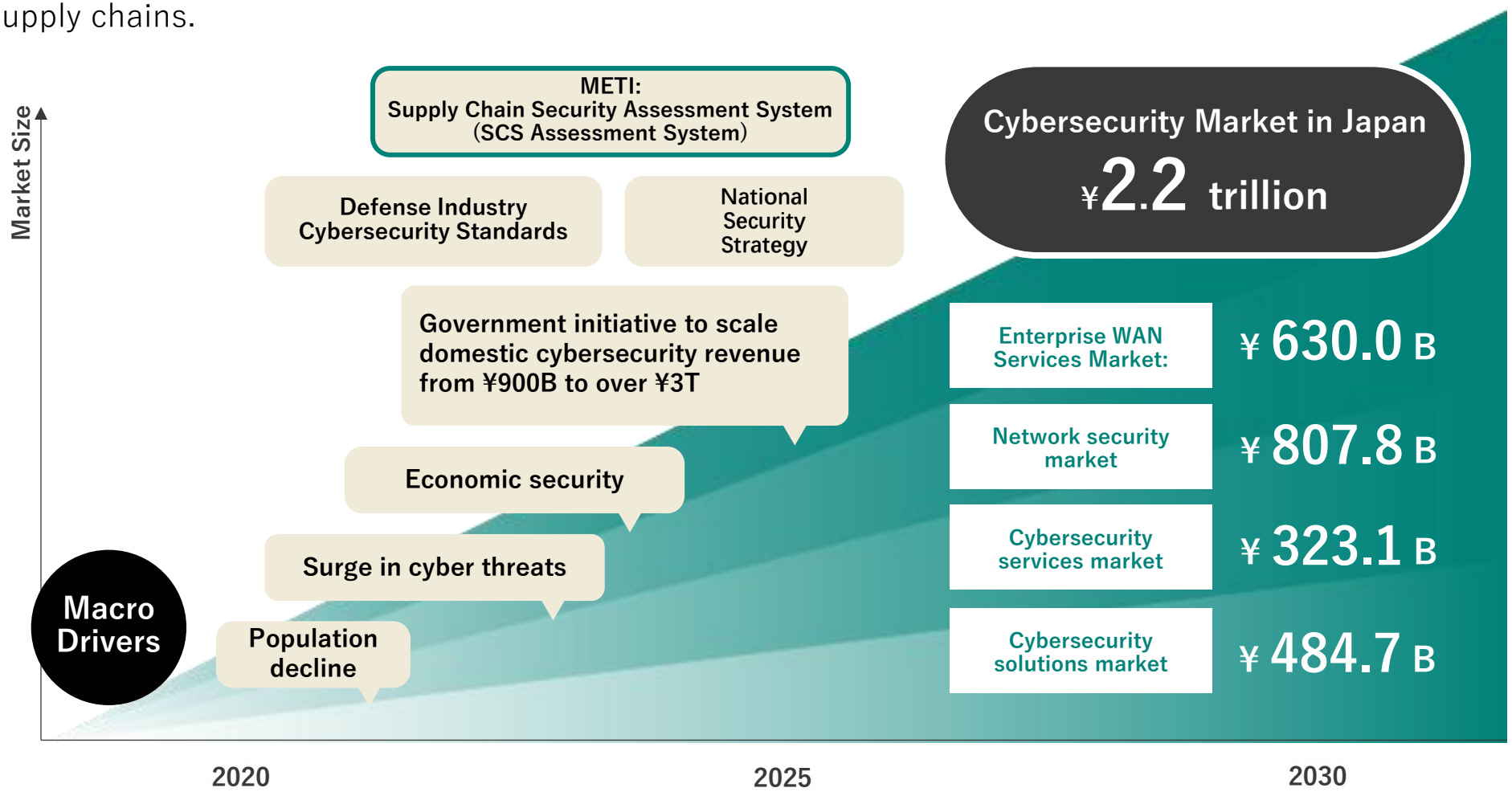
Sustainable Growth and Growth Strategy

AMIYA

Escalating cyber threats and the new SCS Assessment System are acting as major demand tailwinds

In response to a surge in cyberattacks, both the government and major enterprises are mandating strict cyber hygiene across their supply chains.

Growth Market



*: IDC WAN service market forecast for Japan
*: Fuji Chimera network security overview

Copyright @ AMIYA Corporation

Key Global Cybersecurity Solutions

Security Categories	Market Scale Projections (2030)	Global players	Japanese players
EDR Monitor and block unauthorized device activity	¥2.3 T	CrowdStrike (¥43 T) SentinelOne (¥1.3 T)	
IDaaS Unified access to multiple services through a single secure login	¥1.5 T	Microsoft (¥600 T) Okta (¥5.7 T)	
SIEM Collect logs for incident response	¥1.8 T	Splunk *Acquired by Cisco for ¥4 T IBM (¥33 T)	Streamlined SIEM ALog
SASE Cloud-delivered model providing a secure internet gateway	¥ 6.7 T	Cisco Systems (¥67 T) Palo Alto Networks (¥51 T) Fortinet (¥21 T) Zscaler (¥5.1 T)	Fully managed SASE Verona

() Market cap as of September 30, 2026
(Implied USD/JPY rate: $1 = ¥157)

Copyright @ AMIYA Corporation

AMIYA

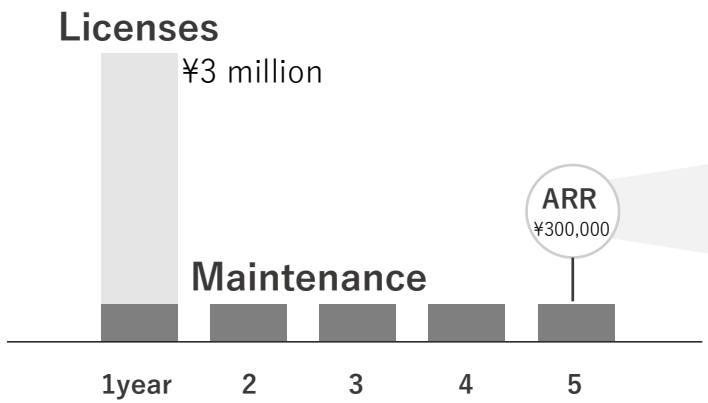
Sales Strategy　Transitioned to a Subscription Pricing Model

April 2024: ALog transitioned to a subscription-only model. **Revenue grew approx. 7x compared to legacy maintenance fees**, while **churn dropped from 14% to under 1%**.

Revolution

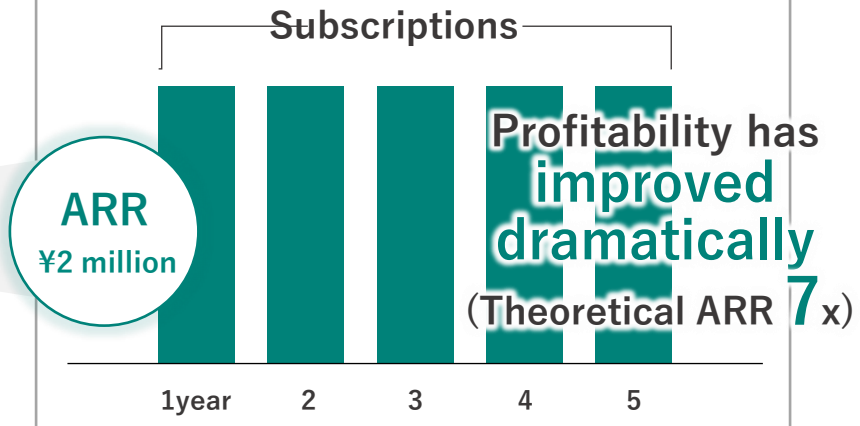
Perpetual License

- One-time purchase → inexpensive maintenance fees
- Revenue recorded as a lump sum
- Client touchpoints limited to initial deployment
- Growth dependent on new client acquisition
- Transactional, one-off sales model



Subscription Model

- Monthly/annual subscriptions → Recurring use
- Recurring revenue
- Client touchpoints continue post-deployment
- Stable ARR growth
- Ongoing value proposition



* Figures are approximate estimates based on actual results

Copyright @ AMIYA Corporation

AMIYA

Sales Strategy　A Hybrid Model for Multi-Dimensional Growth

Drive top-line growth with SI and consulting (non-recurring) while stacking stable subscription revenue (recurring).
We will leverage both engines to scale earnings and drive our recurring revenue mix to 60%.

DS Business

Data Security Business

Data-centric security

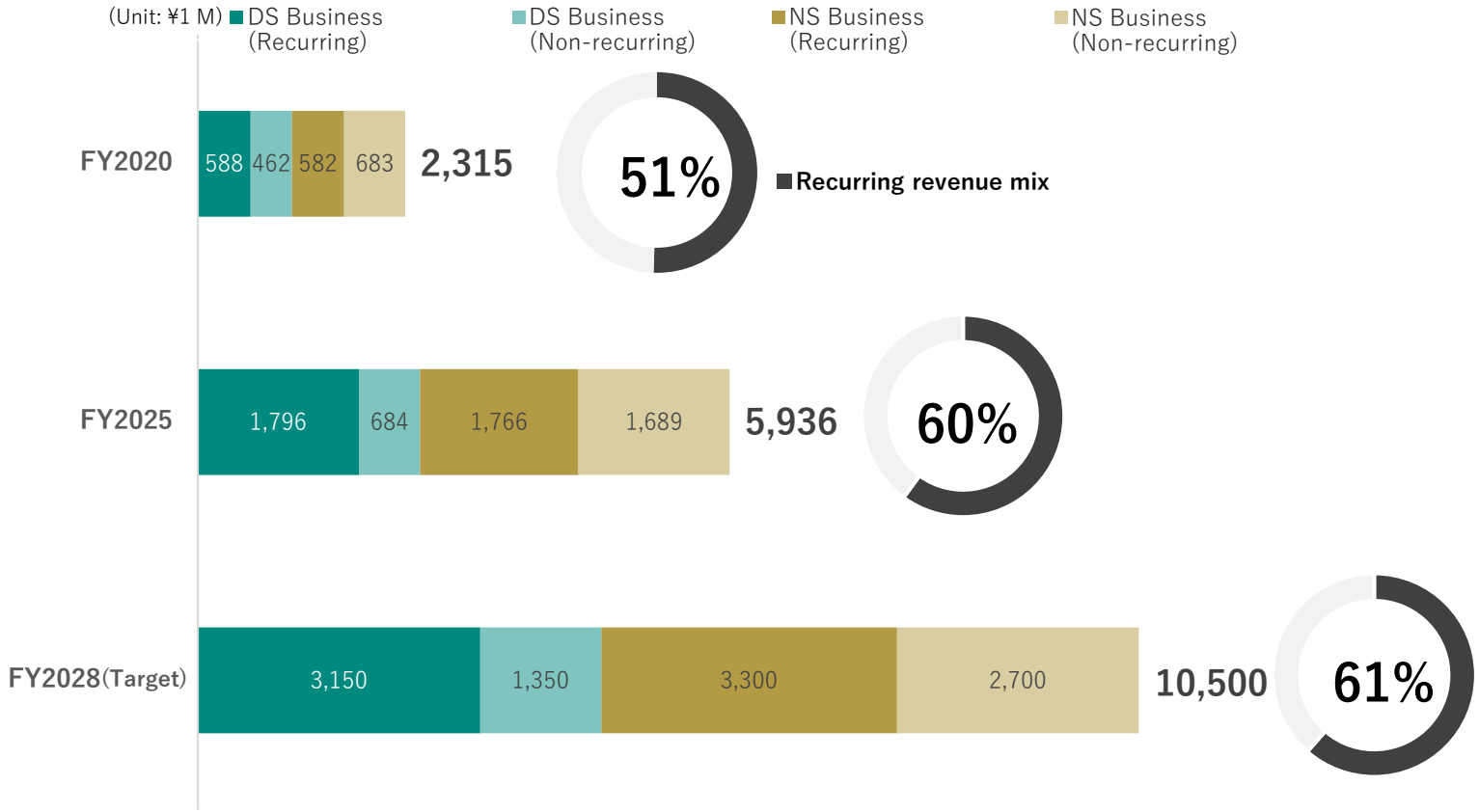
×

NS Business

Network Security Business

Infrastructure-centric security

Model Change

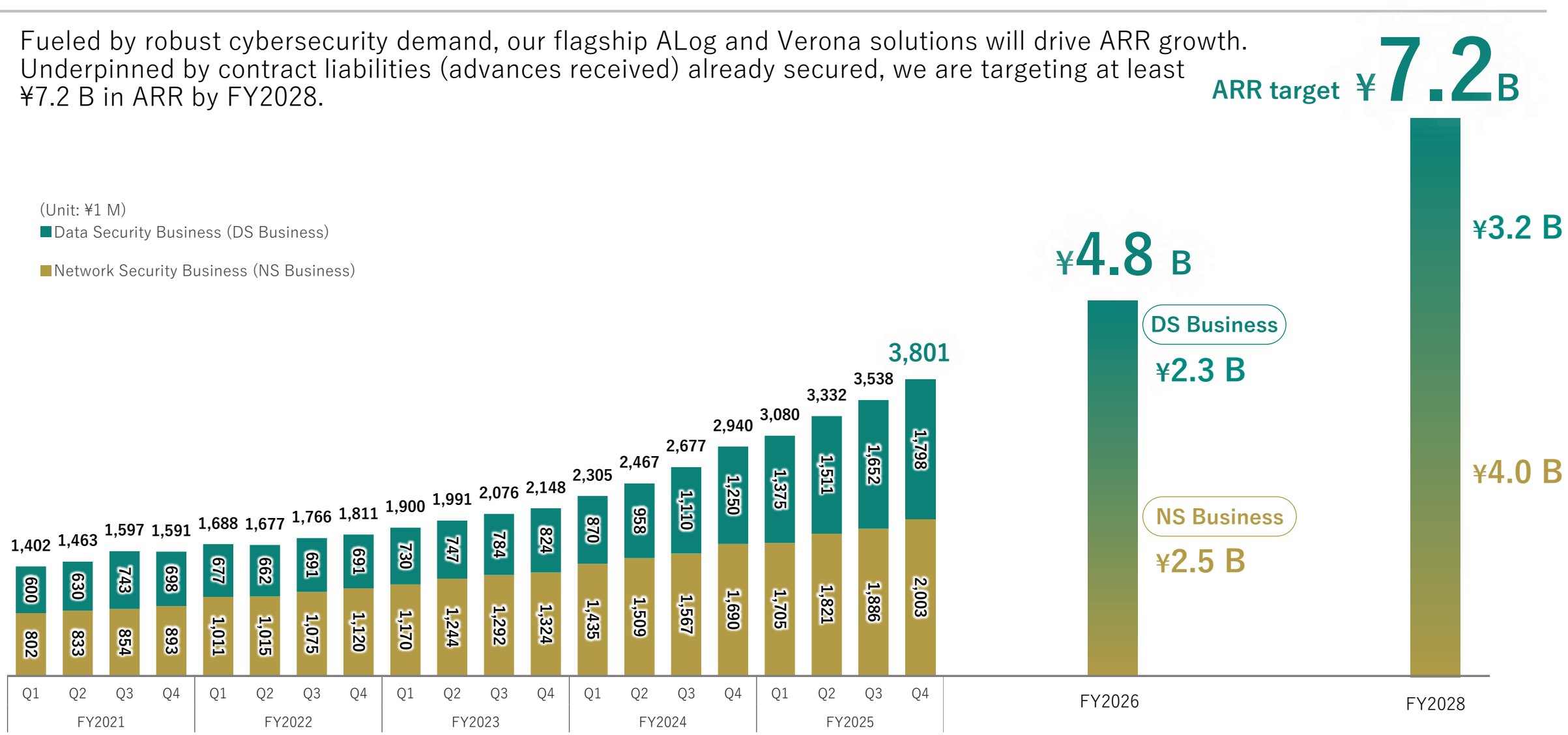


Copyright @ AMIYA Corporation

AMIYA

Sales Strategy　Annual Recurring Revenue (ARR) as Our Core KPI

Fueled by robust cybersecurity demand, our flagship ALog and Verona solutions will drive ARR growth. Underpinned by contract liabilities (advances received) already secured, we are targeting at least ¥7.2 B in ARR by FY2028.



Copyright @ AMIYA Corporation

AMIYA

Sales Strategy Product capabilities rival industry majors; branding is the key to growth

Ramping up advertising and sales promotion in FY 2026 to cement our status as the premier made-in-Japan cybersecurity vendor

Interop Tokyo 2026





Various online events





Partner summits



Information Security EXPO



Copyright @ AMIYA Corporation

AMIYA

Capital Strategy　Unlocking Growth Upside Through Capital Alliances

Industry leaders are actively taking equity stakes in AMIYA, recognizing the value of our made-in-Japan cybersecurity solutions. These investments reflect strong confidence in our R&D capabilities and growth potential.

NTT DOCOMO BUSINESS
NTT Group

- Japan's largest telecom group
- Hundreds of thousands of corporate clients
- Leading provider of enterprise ICT infrastructure

Strategic Synergies:

ALog-driven threat monitoring service

Canon Marketing Japan
Canon Group

- Top-tier domestic IT provider
- Vast network of tens of thousands of corporate clients
- Unrivaled domestic sales and support network

Strategic Synergies:

Joint development of domestic SASE solutions

Ryoyu Systems
Mitsubishi Heavy Industries Group

- Mitsubishi-affiliated systems integrator
- Expertise in the defense, space, and infrastructure sectors
- Manages MHI Group's core IT infrastructure

Strategic Synergies:

Joint development of industrial OT security solutions

Sales: Partners handle direct sales while we focus on product training and sales support, expanding our sales channels without a significant increase in headcount.
Technology: Leveraging partners' advanced technical requirements to drive feature expansion and performance upgrades across our product line.

Cyber Solutions

Made-in-Japan email and authentication security vendor

Strategic Synergies: **Cross-diversification of security services**

H.C. Networks

Leading ORIX-affiliated network systems integrator

Strategic Synergies: **Large-scale collaboration on network security**

Copyright @ AMIYA Corporation

AMIYA

Capital Strategy Aggressively Investing in Long-Term Gains Over Short-Term Profits

To prove the strength of our made-in-Japan security solutions, we are prioritizing future growth over immediate profits.
For our FY2026 investment year, we are allocating an additional ¥150 M YoY to SASE marketing and headcount.

	2023	2024	2025	2026	2027	2028
DS Business	Launched cybersecurity service business		Released ALog subscription edition	Develop new SIEM capabilities (V2/V3)		Develop AI-SOC capabilities
NS Business	Developed Verona SASE		Developed Verona for iOS/Mac	Expand SASE capabilities	ISMAP certification	In-house hardware manufacturing
New Business & HR Investment	¥200 M	¥180 M	¥120 M	¥160 M		
R&D	¥130 M	¥120 M	¥200 M	¥220 M		
Advertising	¥100 M	¥120 M	¥130 M	¥220 M		
Total Investment	¥430 M	¥420 M	¥450 M	¥600 M		

Hire engineers and consultants to scale our cybersecurity services

Verona SASE R&D
(Transitioning from Intel to ARM)

ALog R&D
(Expand SIEM and AI capabilities)

Ramp up advertising
(Exhibit at and hosting industry events)

Copyright @ AMIYA Corporation

AMIYA

AI Strategy　Leveraging AI to Revitalize Japanese Engineering

Far from being a threat to our SaaS model, we see AI as an inflection point to dramatically accelerate Japanese engineering, designating it as our highest R&D priority. By building a proprietary local LLM, we will accelerate development cycles and rapidly bring new capabilities to market.

① Exponentially Accelerating Development via AI

Elevating Made-in-Japan Security Platforms

For years, only well-capitalized North American giants could build high-performance, feature-rich platforms.

AI levels the playing field, giving us the leverage to outpace them and spearhead a domestic cybersecurity revival.

Headcount disparity:
North American vendors (Thousands of employees) VS AMIYA (~300)

Development speed
3x* faster

Code volume
6x* more

② Scaling AI Features

Boosting R&D and Operational Productivity

Advances in generative AI are accelerating the integration of AI features into our existing product lineup.

Predictive threat detection, **automated analysis**, and **automated remediation** are now within reach for domestic development.

Our preventive services, such as **managed SOC** and **vulnerability assessments,** will also benefit from AI-driven development.

ALog	+	=	▶
ALog SIEM: Log analysis	EDR: Device monitoring	XDR: Full-system correlation analysis	AI-Driven Automated Remediation: Establishing a world-class analytics platform
~FY2026	FY2027	FY2028	FY2029

AI has driven a 3x increase in development speed and a 6x increase in code volume.
We are exploring the development of Autonomous Security Operations by 2029.

* YoY comparison as of September 2026. Internal measurement based on the ALog product.

Copyright @ AMIYA Corporation

AMIYA

M&A Strategy　Aggressively Pursuing Cybersecurity M&A

We are prioritizing cybersecurity M&A to build out our comprehensive security portfolio.
We target companies that are highly P&L accretive and possess advanced technologies that directly enhance our core business.

M&A Target Policy: Investment Focus Areas

Priority	Data Security Business	Network Security Business
High	● Expand AI-driven development for SIEM, EDR, and XDR ● Scale SOC and MDR threat monitoring operations ● Secure top talent for consulting, vulnerability assessments, and advanced R&D	● Accelerate advanced R&D for SDN, SASE, and Zero Trust ● Scale operational teams to meet surging SASE demand ● Strengthen domestic manufacturing and sales channels for network hardware
Medium	Shared Business Capabilities	Acquire security and AI engineering talent / Cybersecurity staffing firms / Strategic partnerships in AI-SOC and AI security

M&A Investment Discipline & PMI: Execution and Integration

M&A Investment Discipline

- ✓ Directly expands our core cybersecurity footprint
- ✓ Cutting-edge AI/cloud/security tech with strong standalone profitability

PMI Framework

Standardization (Process Integration)	Talent Development (Enhancing Human Capital)	Value Creation Generating Group Synergies
Align with publicly-listed company governance and security standards	Apply AMIYA's security training protocols and promote cross-group personnel exchange	Drive product/service cross-selling and insource procurement and manufacturing

Copyright @ AMIYA Corporation

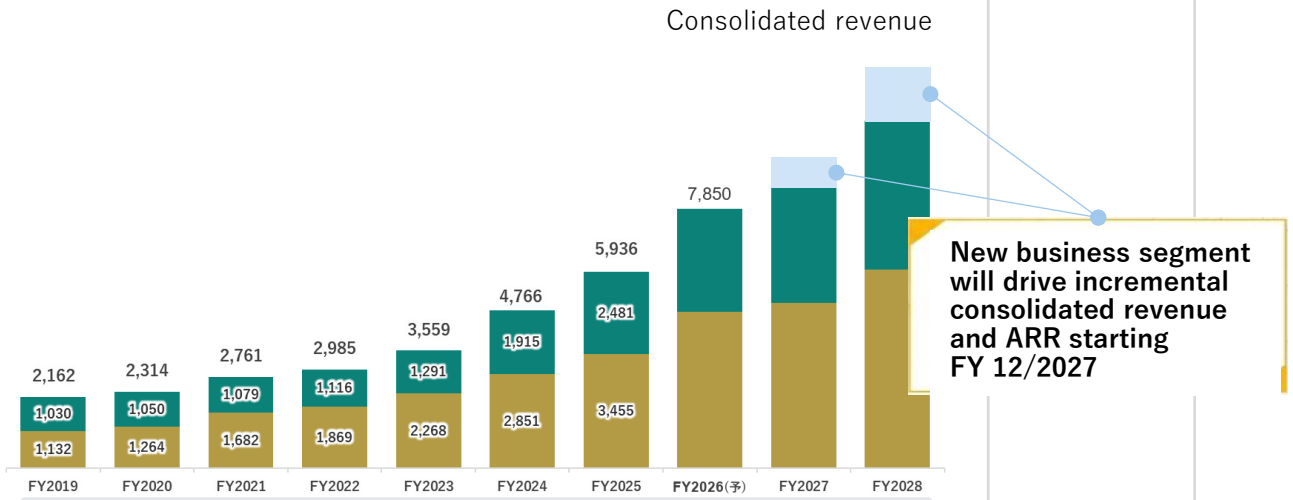
M&A Strategy

Acquired an industrial equipment maker with an eye to in-house, made-in-Japan hardware production

Disclosed May 13, 2026

Acquired industrial and IT equipment manufacturer Ampere Inc. to lay the groundwork for in-house SASE device production.
P&L consolidation begins in Q4.

Objective 1:
Expand the Group's footprint through a new security business

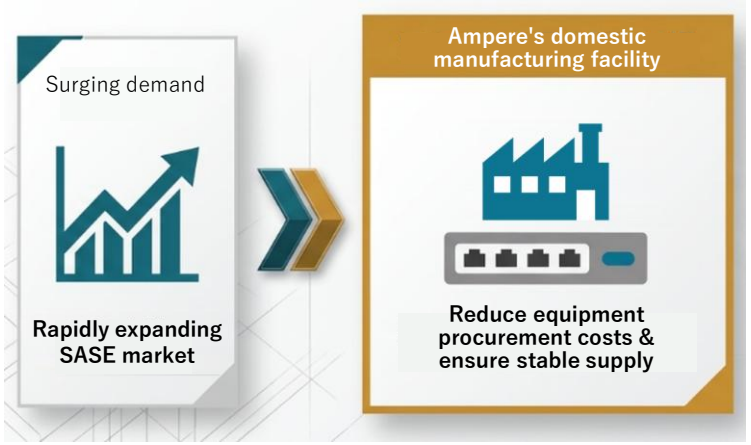


New business segment will drive incremental consolidated revenue and ARR starting FY 12/2027

Projected contribution: ¥1.5B–¥1.7B in revenue and approx. ¥200M–¥300M in ARR

Our newly launched Industrial Security Business—anchored by UPS distribution and hardware manufacturing—is projected to generate an incremental ¥1.5B–¥1.7B in revenue and approx. ¥200M–¥300M in ARR

Objective 2:
Unlock synergies by setting up a domestic manufacturing base to meet surging SASE router demand



Expanding operating margins in the NS Business

Establishing a domestic manufacturing base allows us to insulate our business from FX-driven import inflation and supply chain delays for SASE hardware—ultimately reducing procurement costs and ensuring a stable supply.

Copyright @ AMIYA Corporation

R&D Strategy ALog Enhanced automated monitoring for advanced cyber defense

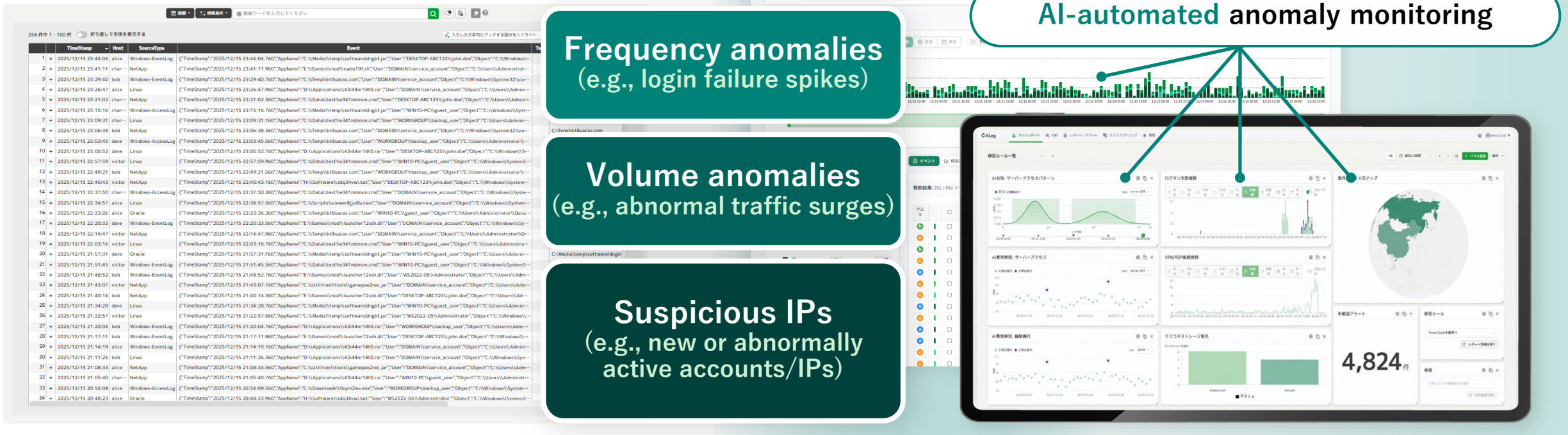
AMIYA

Legacy ALog

SIEM Requirements		
	Collect logs	Integrate data
	Store logs	Forensic searches during critical incidents
	Cyberattacks & malfeasance - Root cause analysis	
	AI-based early-warning detection	

✓ Next-Gen ALog (July 2026 release date)

	Collect logs	Integrate data
	Store logs	Forensic searches during critical incidents
	Cyberattacks & malfeasance - Root cause analysis	
	AI-based early-warning detection	



Copyright @ AMIYA Corporation

R&D Strategy Verona

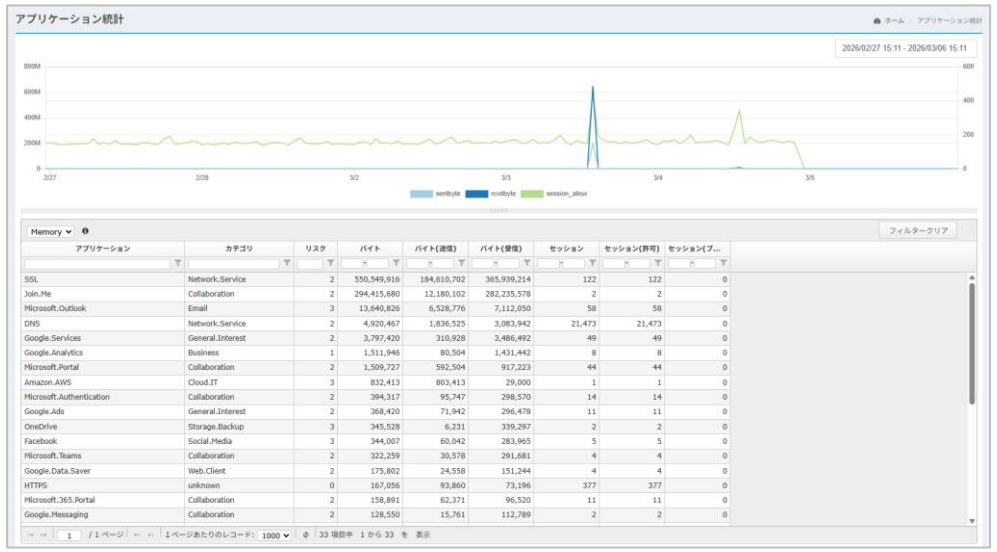
Expanding capabilities ahead of SASE market growth

Verona SASE (Current)

SASE Requirements	SWG	URL filtering
	FWaaS	Antivirus
		Anti-spam
		IDS / IPS
	CASB	Application control
		Tenant control
	DLP (Data Loss Prevention)	

✓ Next-Gen Verona

SWG	URL filtering
FWaaS	Antivirus
	Anti-spam
	IDS / IPS
CASB	Application control
	Tenant control
DLP (Data Loss Prevention)	





Our goal: Rival global brands worth tens of trillions of yen

Copyright @ AMIYA Corporation

AMIYA

Core Product KPIs

Data Security Business

Track Record **6,500** contracts (Cumulative)

Streamlined SIEM

ALog

Usage-based pricing by log volume; monthly subscriptions range from ¥150K to ¥3M depending on client size

◆ Sales Model

New contracts (annual)		ARPU (Annual)		Churn rate (Annual)
250	×	¥2.4 M	×	0.7%
(15–25 / month)		(¥200,000 x 12 months)		

◆ Major Channel Partners

- Fujitsu Group
- NEC Group
- Hitachi Group
- Kanematsu Electronics
- HP Japan
- OTSUKA CORPORATION
- DAIWABO INFORMATION SYSTEM
- SB C&S
- Networld Corporation

Network Security Business

Track Record **6,200** contracts (Cumulative)

Virtual Networking Suite

Network All Cloud

Fully managed SASE

Verona

Cloud-based Wi-Fi

Hypersonix

First-year revenue is a mix of non-recurring device sales (approx. 60%) and recurring SaaS subscriptions (approx. 40%)
ARR

◆ Sales Model

New contracts (annual)		ARPU (Annual)		Churn rate (Annual)
300	×	¥4.2 M 40% contributes to ARR	×	1.2%
(20–30 / month)		(¥350,000 x 12 months)		

◆ Major Channel Partners

- NTTPC Communications
- NTT DOCOMO BUSINESS
- Canon Marketing Japan
- NEC Group
- Toshiba Tec Solution Service
- BIGLOBE
- Sony Biz Networks
- OPTAGE

Copyright @ AMIYA Corporation

AMIYA

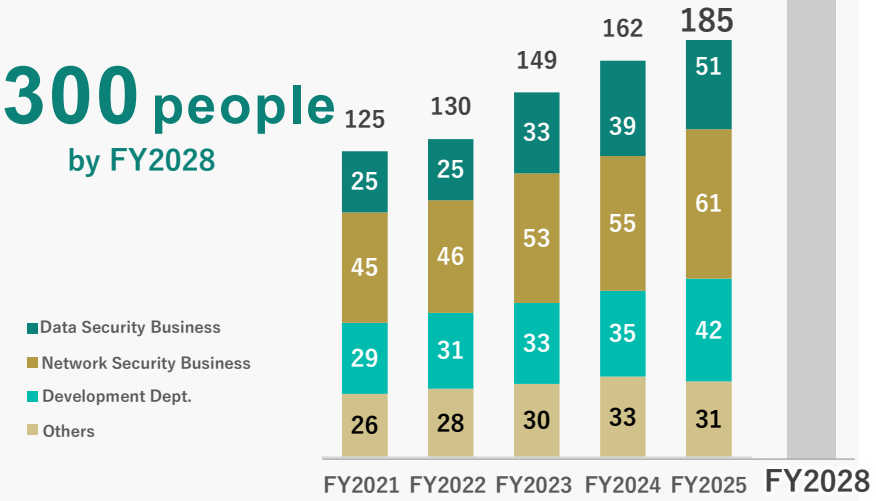
Talent Strategy Building an elite security organization through a better work environment

*All figures on a non-consolidated basis (As of Sept 30, 2026)

Workforce

Hire and train elite security talent, with a focus on new graduates

300 people by FY2028



Key Certifications

Train and retain highly specialized cybersecurity professionals

Threat Analysis & Incident Response:	GIAC GCFE / CRTP / OSCP
Network & Cloud Defense:	CCNP Security / LPIC-3 Security / CCSK AWS Certified Security – Specialty
Security Management:	CISSP / Registered Information Security Specialist (RISS)
Risk Assessment & Remediation:	CISA / ISMS Provisional Auditor

Foundational Technologies

Network Specialist | CCNP | Applied Information Technology Engineer

*Notable certifications held by our staff

Talent Strategy

Management that truly cares about employee motivation, wellbeing and fulfillment

Diverse workstyles:

Flextime
Remote work / work from satellite office
Workcations

Results-oriented:

Performance incentive / President's Award
Year-end bonuses
Stock-based compensation (RS/PSU)
Employee Stock Ownership Plans (20% match)

Support employee development:

Technical/Upper-management training
Encourage/reward employees for obtaining certifications
Specialist Track Remuneration System
Proactive Promotion of Young Talent

Employee turnover

Uncommonly low turnover for our industry

4.9%

*Industry average: 9% - 13%

Average overtime hours worked

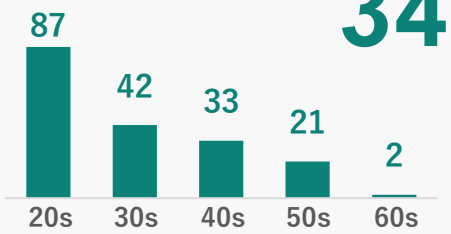
Uncommonly low overtime for our industry

9.3h/month

*Industry average: 20h -25h / month

Average Age

34



Copyright @ AMIYA Corporation

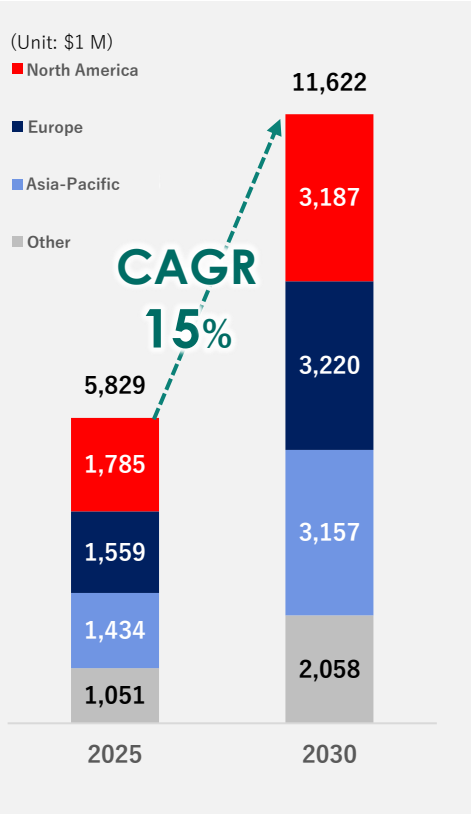
Appendix

Global SIEM players vs. ALog

Global SIEM Market

Globally, the log management market is known as the “SIEM market.”
Estimated ¥1.8 trillion market by 2030.

*Calculated at USD 1 = JPY 157 (As of Sept 30, 2026)



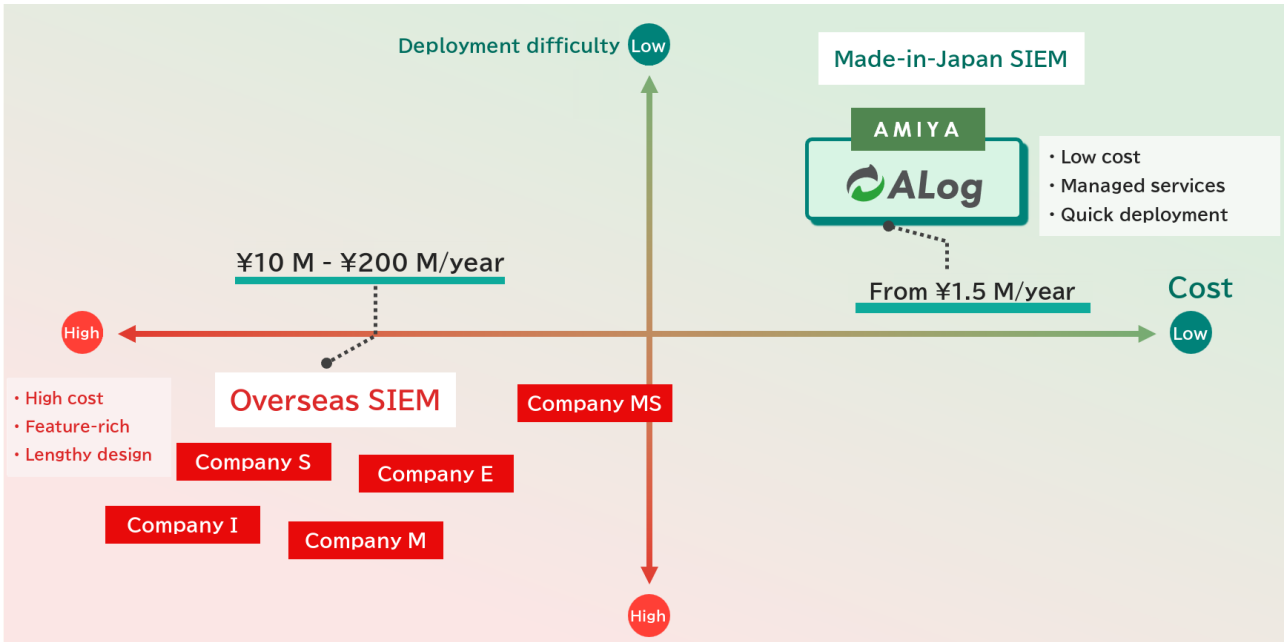
Top global leaders include Splunk, McAfee, and IBM

Splunk Inc.

Industry leader Splunk was acquired by the world's largest networking equipment provider, **Cisco Systems, for approx. $28B (approx. ¥4T)** in March 2024

Key Players

North American vendors dominate the SIEM market with expensive, feature-heavy products.
ALog is designed for rapid deployment, accessible pricing, and ease of use.

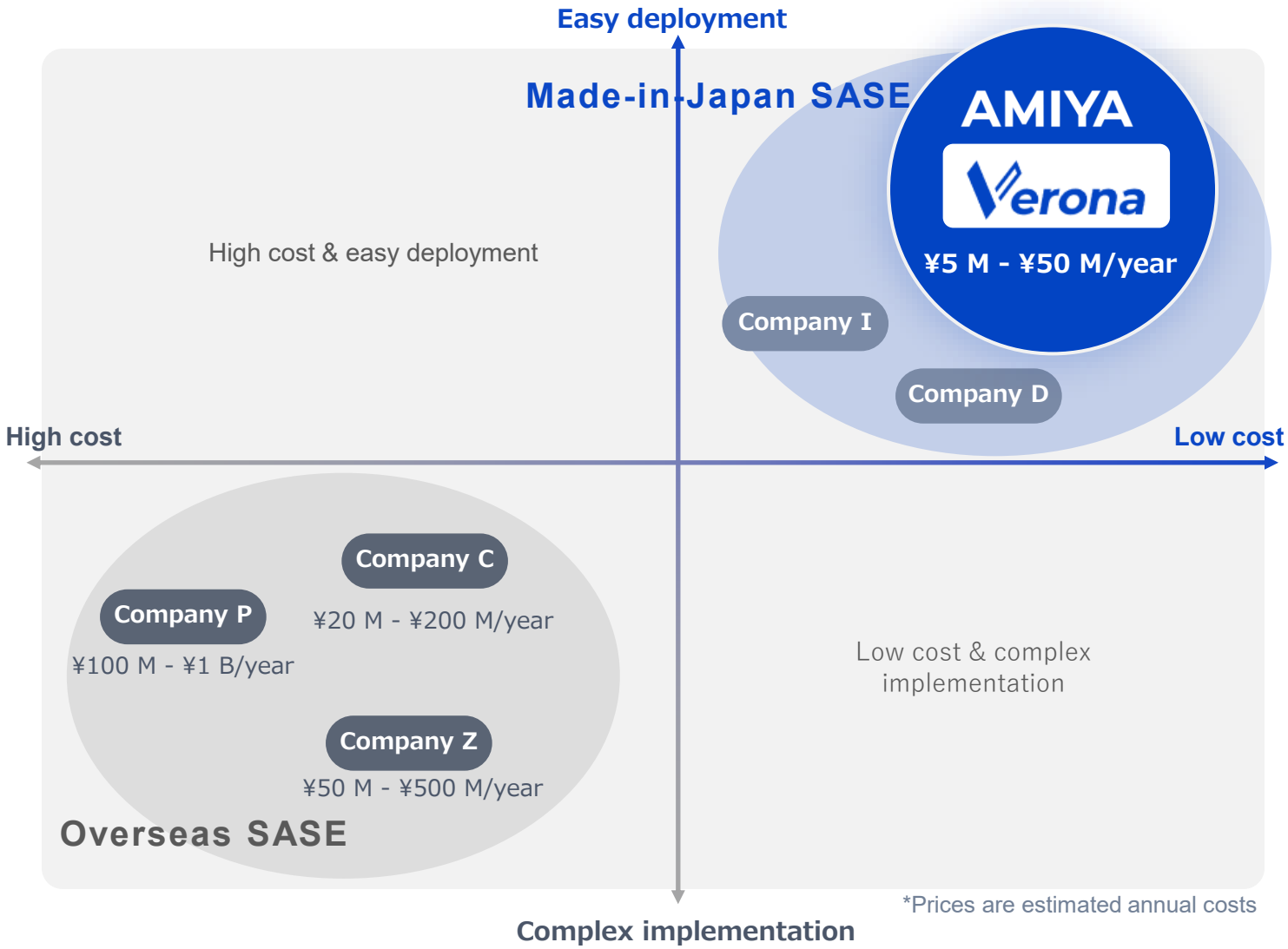


Source: Grand View Research, Inc.
Security Information and Event Management (SIEM) Market Analysis and Segment Forecast to 2030

Copyright @ AMIYA Corporation

Appendix

Global SASE players vs. Verona



Comparison with overseas solutions

North American vendors dominate the SASE space with costly, feature-heavy platforms.
Verona is designed to deliver **managed services**, **competitive pricing**, and **advanced capabilities**.

	Verona	Overseas SASE
Managed services	◎ Hands-on ops support	× Self-managed
Pricing	◎ Competitive pricing	× High cost
Deployment	◎ Short lead time / quick deployment	× Lengthy design phase required
Features (DLP/Sandboxing)	△ Under development	◎ Built-in

Copyright @ AMIYA Corporation

04

Business Overview

Data Security Business

AMIYA

Source: Deloitte Tohmatsu MIC Research Institute, "Current Status and Future Outlook of the Internal Threat Prevention Solutions Market," published March 2026

Accessible SIEM

ALog

Automated log collection across all systems



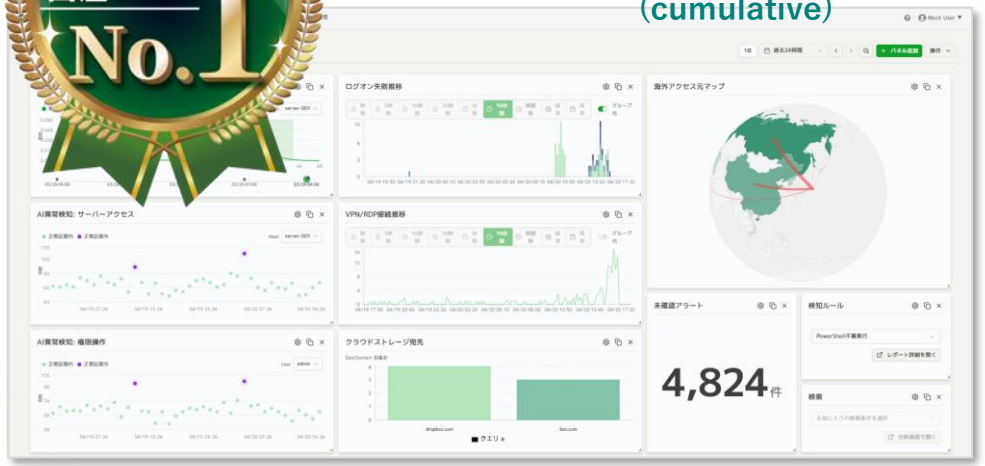
Automated analysis of Indicators of Compromise

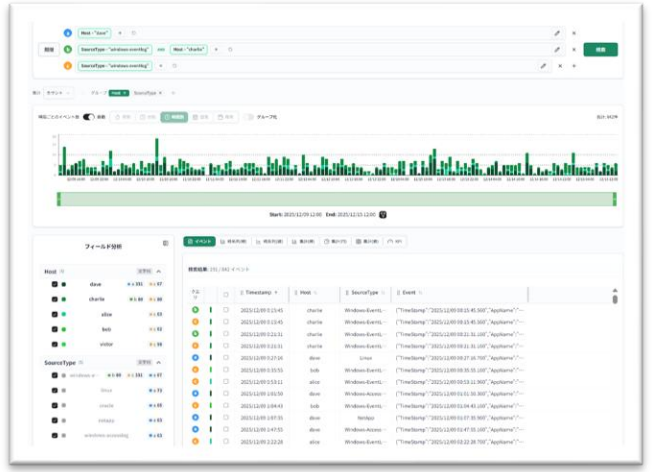
Compliant with the SCS Assessment System

AI-driven behavioral detection of insider threats

セキュリティ情報イベント管理ツール市場 国産SIEM No.1

6,500 contracts (cumulative)



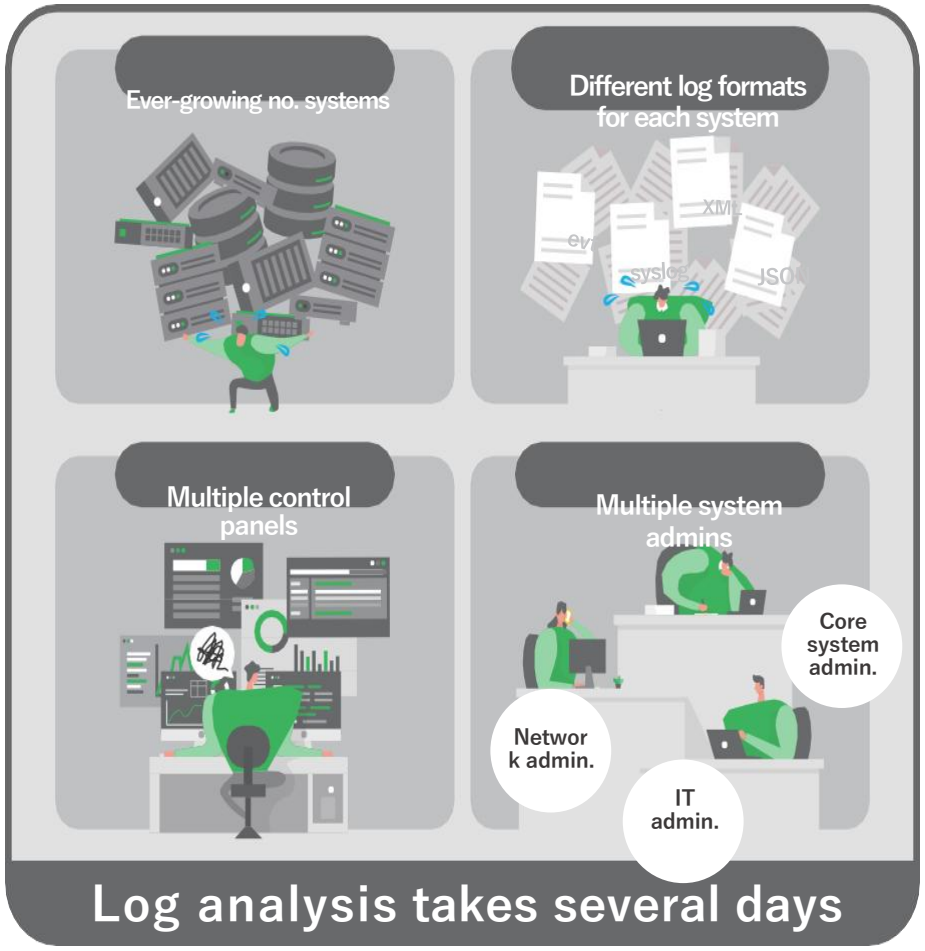


Copyright @ AMIYA Corporation

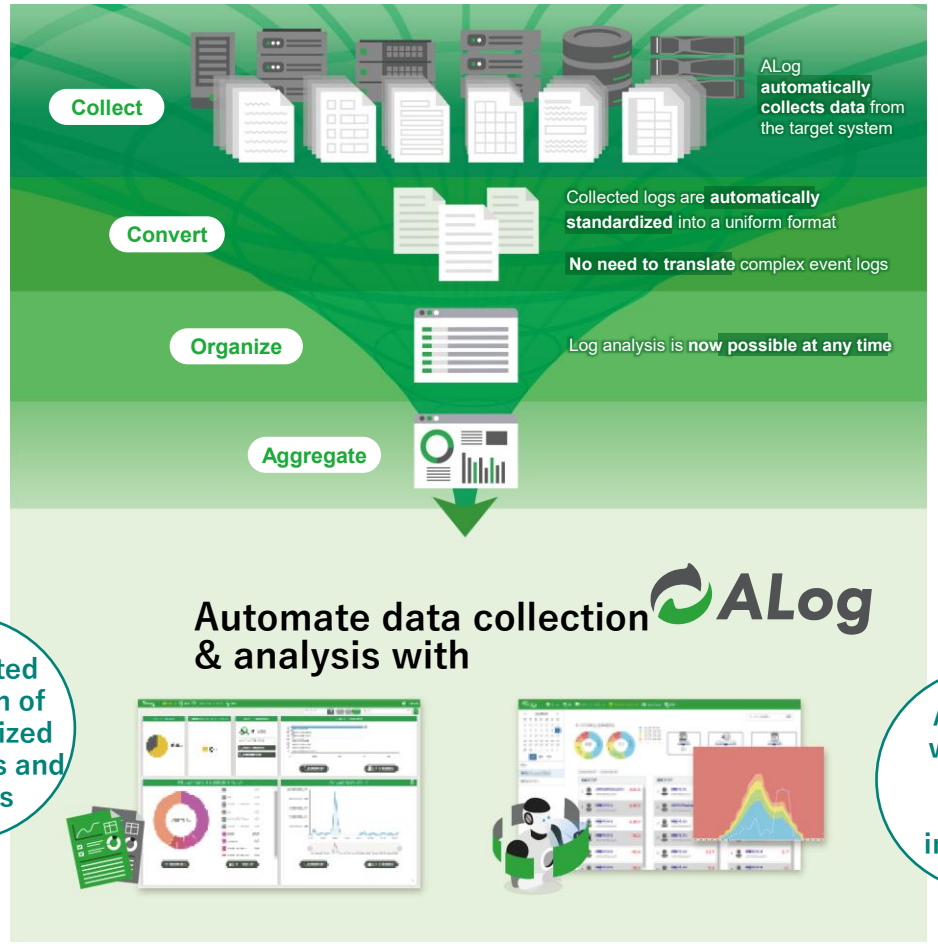
AMIYA

ALog | Automated Risk Assessment Powered by AI as a Competitive Edge

Before



After



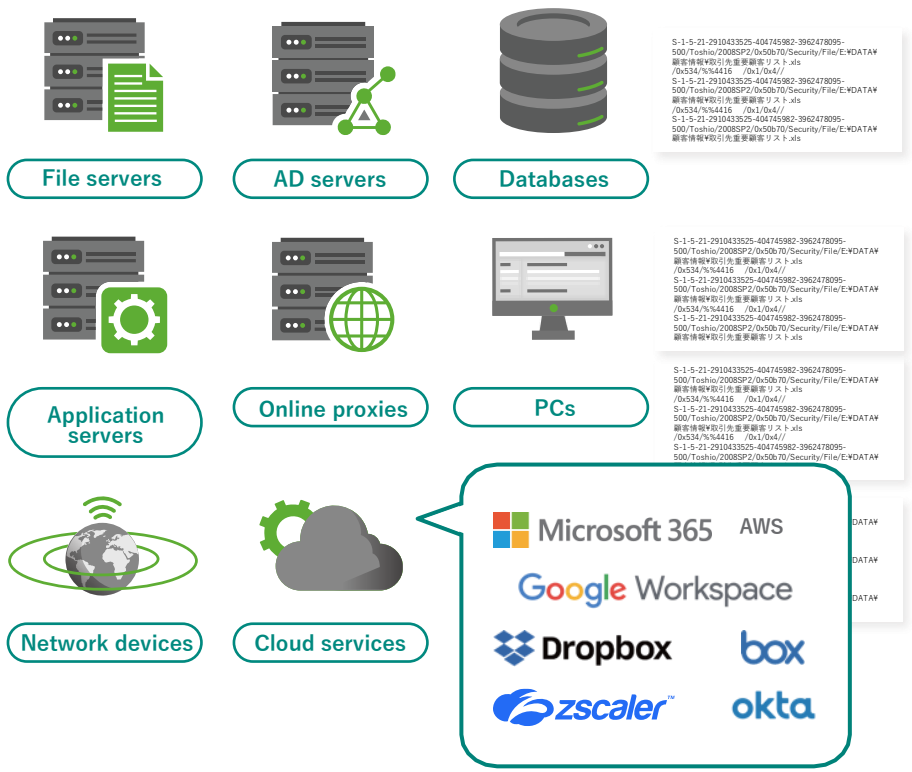
Traditionally, logs had to be normalized on a per-system basis.
With ALog, normalization of log types and elements is performed automatically.

Copyright @ AMIYA Corporation

ALog | The Only Solution to Convert Massive Data Logs into Human-readable Format

AMIYA

Complex logs in different formats



Automatically converts data into human-readable format

When?	Who?		Where?	What?
Date & Time	User	Server	File Path	Operation
2021/02/03 12:15:04	amiya¥Sasaki	amyfs001	D:¥¥Sales¥Key_client_list.xls	READ
2021/02/03 20:11:04	amiya¥Yamada	amyfs001	D:¥¥Planning¥FY13_Biz_Plan.doc	WRITE
2021/02/03 22:05:03	amiya¥Akiyama	amyfs001	D:¥¥Accounting¥Payroll_Tanaka.xls	DELETE

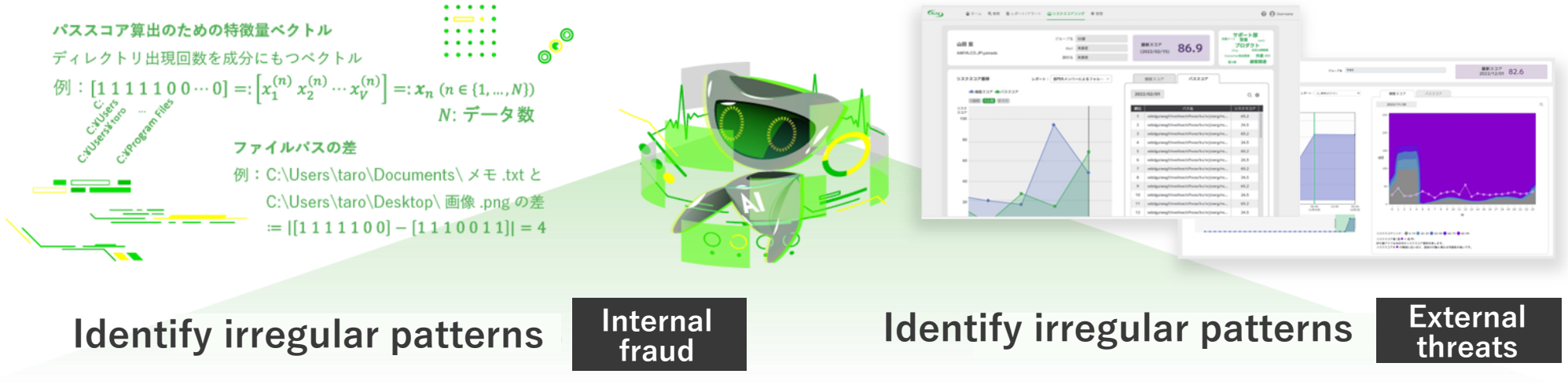
Patented technology
Log Conversion (Patent no. 6501159)
AI risk scoring (Patent no. 7576646)

As logs generate massive volumes of data, technologies that can process large amounts of data in real time are essential.
Our track record of 6,500 cumulative contract deployments, combined with our patents and know-how, gives us a unique advantage that even major players cannot replicate.

Copyright @ AMIYA Corporation

AMIYA

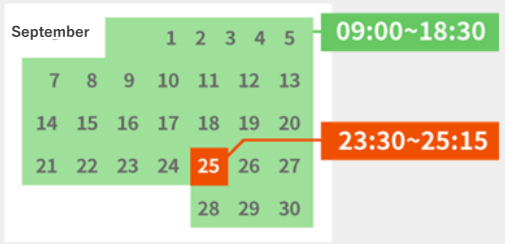
ALog | Integration of AI to automate risk assessment functions is a competitive differentiator unique to Amiya



Identify irregular patterns — Internal fraud

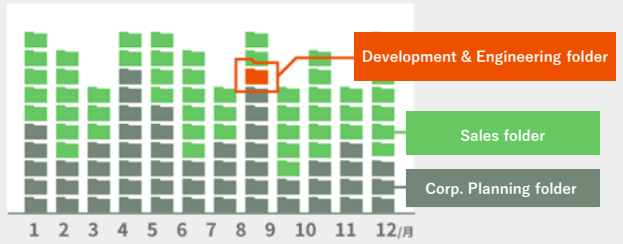
Identify irregular folder access times

Data Access Logs by User: Sato



Identify irregular folder access patterns

Folder Access Logs by User: Suzuki



Identify irregular patterns — External threats

Ransomware forcibly encrypts files



Analyzing logs requires a high level of specialized expertise, making it unrealistic for customers to handle on their own. ALog leverages AI to automatically detect and flag behavior that deviates from normal patterns — with no prior registration required

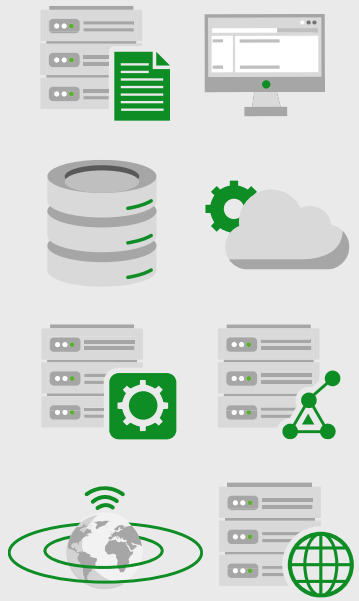
Copyright @ AMIYA Corporation

AMIYA

ALog MDRサービス／セキュサポ | Managed Threat Monitoring for SMEs

SOC/CSIRT
Managed threat monitoring

Leverage a wide range of collected log data



ALog

ALog takes care of the operational side.
Fully managed cybersecurity by our remote experts

Monitoring


Monitor & defend against cyberattacks & internal malfeasance

Analysis


Root Cause Analysis

Report


Create reports for clients

Optimization


Suggest protocols and improvements

Proprietary solutions.
Competitive pricing.

SOC services
- Defend against cyberattacks
- Defend against internal fraud
- Improvement reports
- Incident response support
- Cyber liability insurance

Cyberdefense
- Defend against vulnerabilities
- Cybersecurity help desk

SOC (Security Operations Center) services, traditionally costly and difficult to adopt, are becoming more affordable through made-in-Japan solutions and managed operations, making them accessible to small and medium-sized enterprises. For AMIYA, this drives growth in ARR and ARPU.

Copyright @ AMIYA Corporation

AMIYA

Comprehensive Cybersecurity Services

Beyond product sales, our competitive edge lies in delivering a full spectrum of end-to-end cybersecurity services

Consulting | Security assessments | Training & education | Incident response

Annual planning	IT Environment Assessment	Defense / Monitoring	Detection	Response /Remediation	Recovery
Risk assessment	Asset management	**Verona** (SASE)	**ALog** (SIEM)		Fast forensics
Create / update written security policies	Attack surface assessments	EDR (Endpoint Detection & Response)	ALogMDR / SecuSapo(Managed SIEM services)		Full forensics
Security audits	Vulnerability assessment (Web/Platform)	IDaaS/SSO (Identity management)	SOC(Cyberattack monitoring)		Log analysis
Obtain security certifications (ISO27001/P-Mark)	Assess security configurations	Cybersecurity talent SES	Screen for internal fraud	Emergency Incident response	
Creation of CSIRT teams	Penetration testing	Spear phishing simulated drills	Threat intelligence	CSIRT response drills / Backup-based recovery	

➡ Comprehensive coverage spanning vulnerability assessments, incident response, audits, and training.

Copyright @ AMIYA Corporation

Network Security Business

AMIYA

Network virtualization enables fully remote, cloud-based management of communications infrastructure

Network All Cloud®

Fully managed SASE

Verona



Cloud-based Wi-Fi

Hypersonix



Cloud-based IT management services

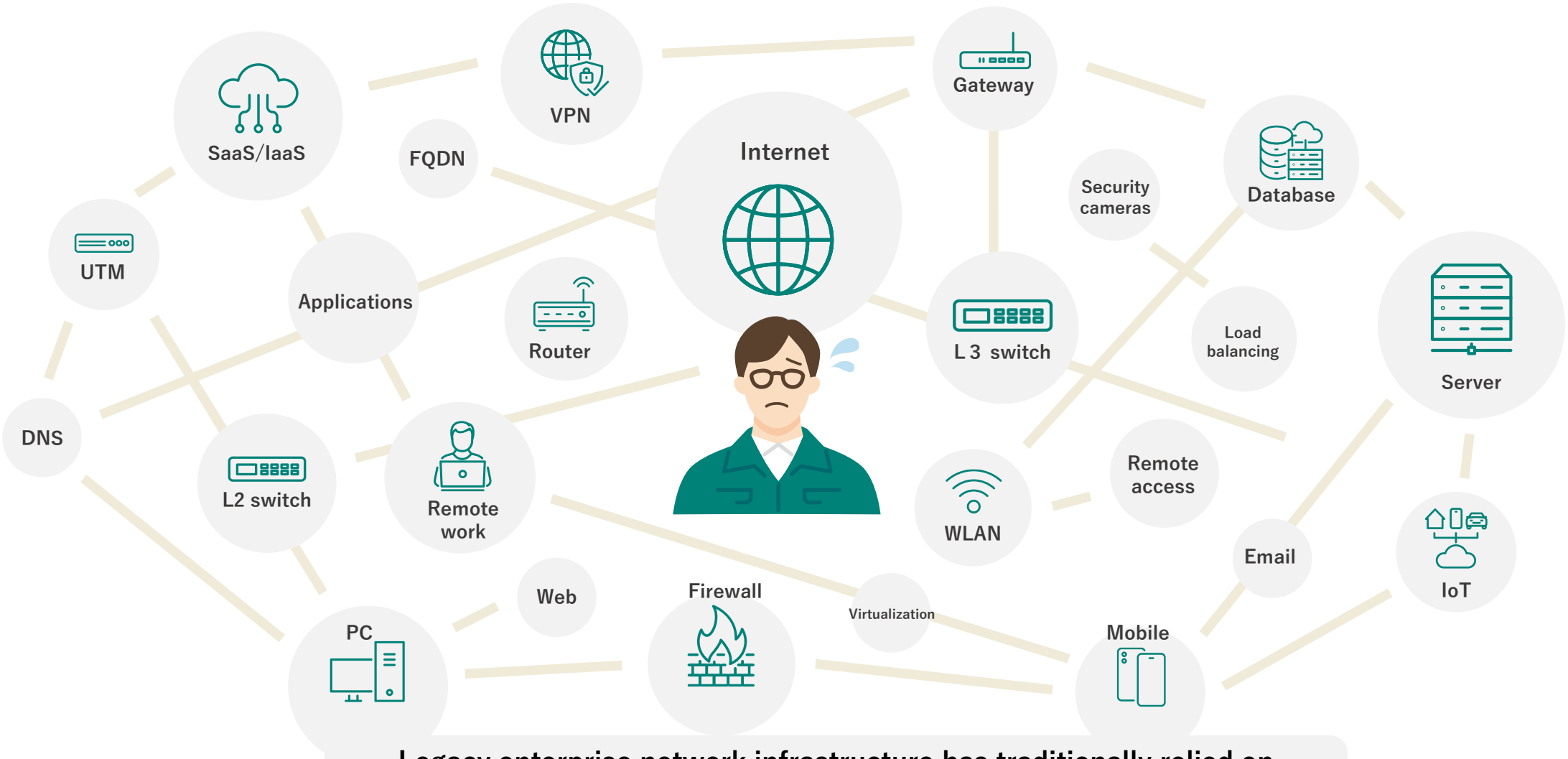
ランサポ



Copyright @ AMIYA Corporation

AMIYA

Legacy Networks | Used to Rely on Manual, On-premise Setup & Configuration



Legacy enterprise network infrastructure has traditionally relied on manual, on-premise maintenance setups—an anomaly in today's cloud era.

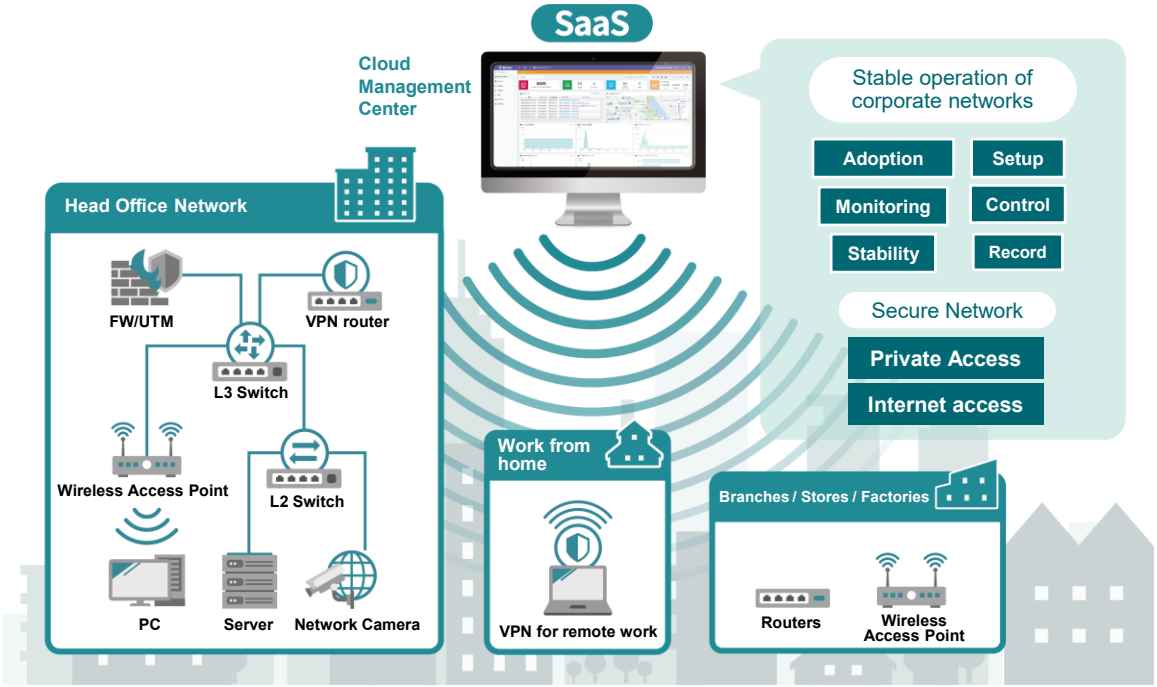
Copyright @ AMIYA Corporation

AMIYA

Network All Cloud® | One of Japan's Leading Network Virtualization Services

Network Virtualization

Network All Cloud®



Point 1

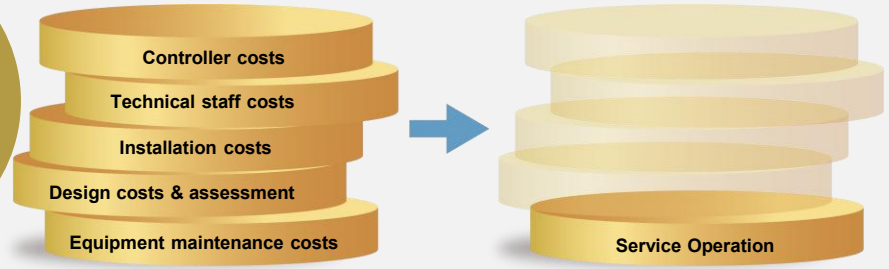
High Retention Driven by Infrastructural Stickiness

Contracts ▶ (cumulative) 6,200

Retention ▶ As of Sep. 2026 99%

Point 2

Enables Significant Cost Savings vs. Legacy Solutions



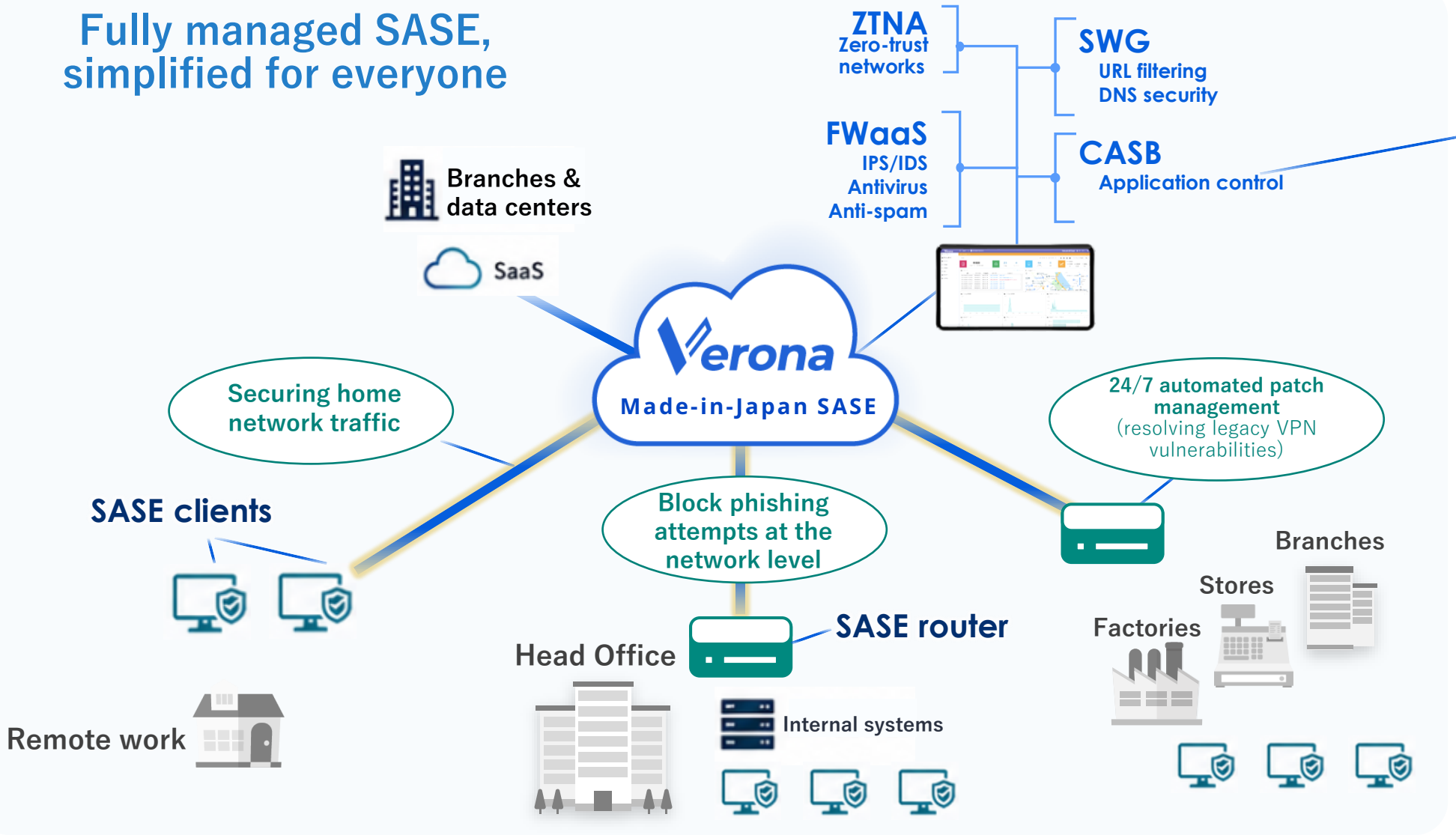
Traditional corporate LAN/WAN costs have tended to be high due to on-site work performed by system integrators. With the proliferation of virtualized networks, all SI work can now be performed remotely, reducing the associated costs.

Copyright @ AMIYA Corporation

AMIYA

Verona | SASE: An essential defense against ransomware and phishing

Fully managed SASE, simplified for everyone



Verona

- Web access control
- Internal access control
- SaaS Control
- Traffic visibility & threat detection
- Securing branches & remote work (SD-WAN / SASE)
- AI-driven traffic analysis & decision support
  - Traffic visibility & correlation analysis
  - Anomaly detection & risk assessment
  - Automated traffic control & isolation

Delivering reliable security through made-in-Japan technology and support

Copyright @ AMIYA Corporation

AMIYA

Verona offers feature parity with high-priced global brands

Core SASE Capabilities

SASE: An integrated network and security service



		Global competitor P	Global competitor Z	Domestic competitor A	Verona
SD-WAN		○	△	×	○
ZTNA	Always-On & Forced Tunneling	○	○	×	○
	Device Posture (Endpoint Health Checks)	○	○	×	○
	Micro-segmentation	○	○	×	○
SWG	URL filtering	○	○	○	○
	DNS security	○	○	○	○
CASB		○	○	○	○
FWaaS	IPS/IDS	○	○	○	○
	Antivirus & Anti-Spam	○	○	○	○
	Sandboxing / DLP	△	△	×	Next release
PoP (Global High-Speed International Routing)		○	○	×	×
Managed operations (Deployment, operation, monitoring & updates from our center)		×	×	△	○

Due to its complexity, outsourced management is strongly recommended. Patches are applied centrally to prevent vulnerabilities.

Feature parity at less than 1/3 the cost (Managed Services included)

Copyright @ AMIYA Corporation

AMIYA

Deliver certain success for businesses built on safety and security