Note: This document has been translated from the Japanese original for reference purposes only. In the event of any discrepancy between this translated document and the Japanese original, the original shall prevail.

FY2023 Q2 Financial Results

Second Quarter of the Fiscal Year Ending March 31, 2024

Cybertrust Japan Co., Ltd.
TSE Growth: 4498
October 25, 2023

Executive Summary

FY2023 Q2 Financial Results

Increase in both sales and profit compared to the same period of the previous year
Achieved record high net sales and operating income for the second quarter

Authentication and Security

Made good progress due to factors such as iTrust-based identity verification needs rising for local government benefits
iTrust sales **up 75% year on year**

Linux/OSS

Inquiries for extended support for CentOS7 increased, with progress being made for undertaking this
Full-year forecasts are expected to be reached

IoT

Although EMLinux support grew, professional services remained flat
There is a high level of needs for Cybertrust services using international security standards, etc. and measures such as providing new versions of EMLinux supporting SBOM are **consistently progressing**

FY2023 Full-Year Forecast

Net sales and operating income are forecast to increase in Q4
Progress is being made as planned toward the achievement of the full-year forecast

Net sales: 7,500 million yen (+20% YoY) **Operating income: 1,400 million yen (+30% YoY)**

Expect to post increases in sales and profits as stable, high-revenue services coupled with the three high-growth-driver services (iTrust, Linux support, and EMLinux) drive forward performance

Agenda

- FY2023 Q2 Financial Summary
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
  - Overview of Others
- FY2023 Full-Year Forecast
- APPENDIX

FY2023 Q2 Consolidated Results (6 months)

Year-on-year increase in both sales and profits, record high Q2 net sales and operating income

Net sales rose 3.6% YoY to 2,981 million yen

Operating income increased 3.7% YoY to 425 million yen

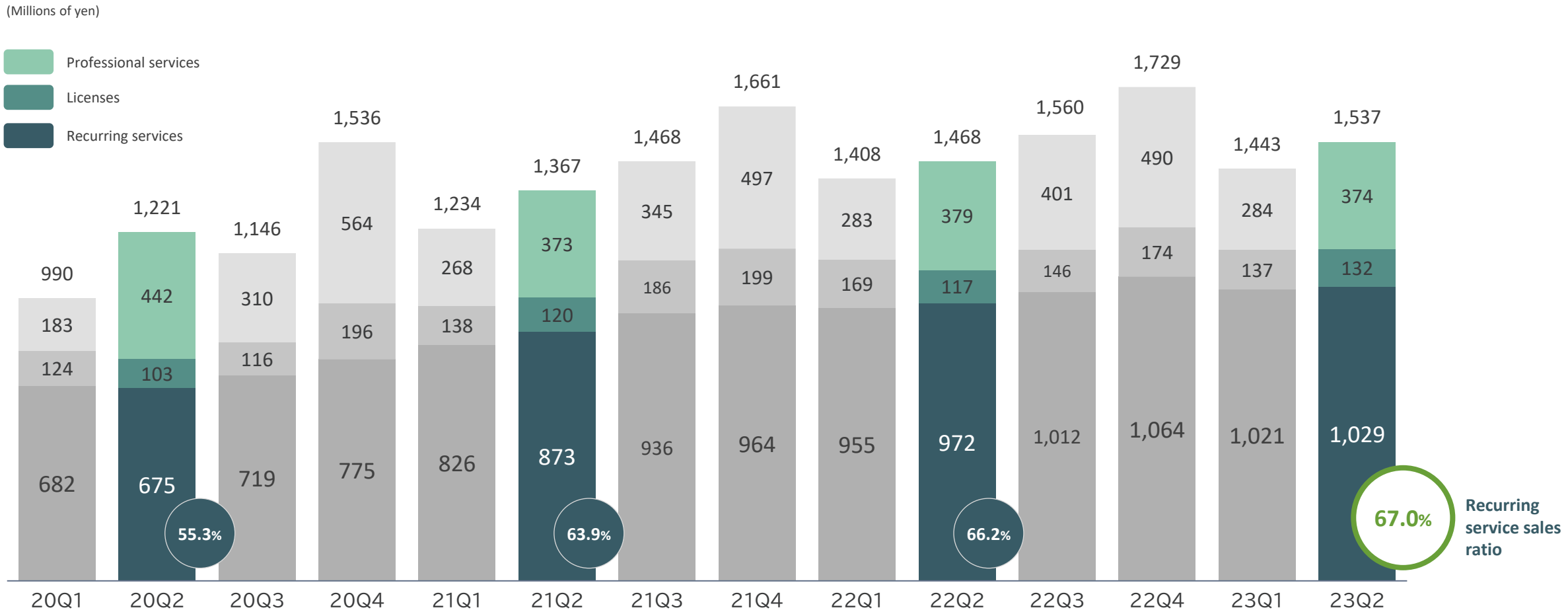
- Strong build-up of recurring service sales under Authentication and Security Services on the back of expansion of digital transformation market
- Made progress for the anticipated expansion in demand for recurring services in Linux/OSS Services from Q4
- Recurring services were strong in IoT Services

(Unit: Millions of yen)	FY22 H1	FY23 H1	YoY Change
Net sales	2,877	2,981	+3.6%
Operating income	410	425	+3.7%
Ordinary income	417	426	+2.3%
Profit attributable to owners of parent	280	282	+1.8%
EBITDA	687	722	+5.1%

Trend in Quarterly Sales by Transaction Type

Record high Q2 recurring service sales ratio of 67.0%

Growth driven by high growth-driver services



Seasonal variations: Transactions such as server certificates, whose contract amounts are recorded in lump sum, are concentrated in Q4

Sales by Service Segment

- **Authentication and Security** — Strong performance by recurring services such as significant growth in iTrust, a high-growth-driver service, due to expansion of digital transformation market
  Net sales including recurring sales posted steady growth year on year, rising 9%
- **Linux / OSS** — New CentOS contracts increased under high-growth-driver service Linux support
- **IoT** — High-growth-driver service EMLinux support sales increased
  Contract development orders for professional services were delayed

(Unit: Millions of yen)	FY22 H1		FY23 H1		YoY Change	
	Net sales	Sales ratio	Net sales	Sales ratio	Increase	Increase rate
Authentication and Security Services	1,692	58.8%	1,844	61.9%	151	**+9.0%**
Linux/OSS Services	704	24.5%	661	22.2%	(42)	**(6.1%)**
IoT Services	480	16.7%	474	15.9%	(5)	**(1.2%)**
Total net sales	2,877	100%	2,981	100%	103	**+3.6%**

- FY2023 Q2 Financial Summary
- **Overview by Service Segment**
  - **Authentication and Security Services**
  - Linux/OSS Services
  - IoT Services
  - Overview of Others
- FY2023 Full-Year Forecast
- APPENDIX

Recurring services grew led by high-growth-driver service iTrust

(Unit: Millions of yen)

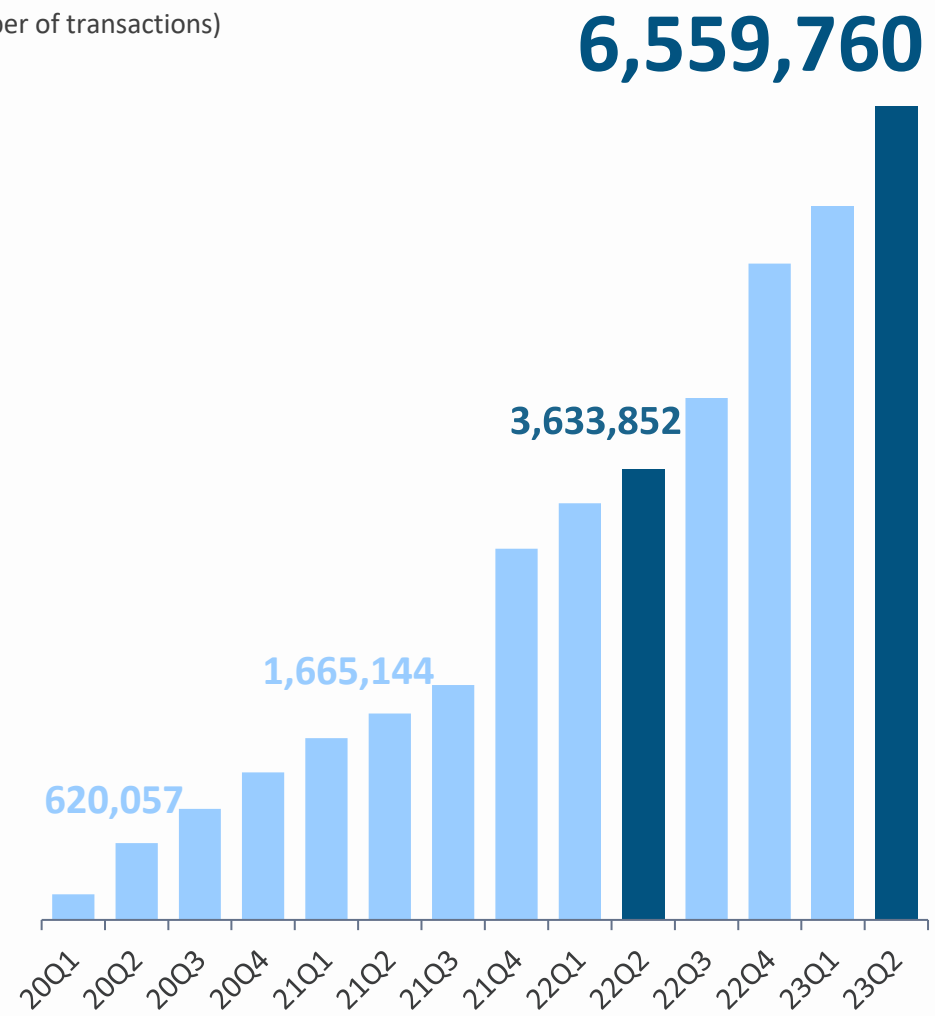
Authentication and security service net sales (Sales by transaction type)	FY22 H1	FY23 H1	YoY Change
Recurring services (Recurring service sales ratio)	1,402 (82.9%)	1,538 (83.4%)	+9.7% (+0.5 pp)
Licenses	85	97	+14.1%
Professional services	204	208	+1.9%
Total net sales	1,692	1,844	+9.0%

Recurring service sales ratio of 83.4% (+0.5pt YoY)

- Mainstay iTrust grew significantly by 75% year on year as eKYC service for financial institutions and local governments, and electronic contract services expanded
- In Device ID, cloud-based authentication services and remote access services for corporates grew
- Renewal rate improved for SureServer. Steady progress being made in acquisition of new customers
  - Achieved the highest number of EV server certificates in the domestic market with a share of 48.14% certificates **No.1 share** for seven successive years since August 2017
- Sales ratio by transaction type progressed as expected as a result of focusing on recurring services led by high-growth-driver services to strengthen revenue base

Quarterly Trend in KPI of High-Growth-Driver Service iTrust

Number of iTrust transactions (number of paid API use)



Number of transactions 6.55 million per quarter

*In Q2, identity verification using Individual Number Cards grew more than expected due to benefits started by specific local governments in September

YoY change 1.8 times

* 10x over 3 years

Trust service boasting outstanding performance

*Cybertrust Japan study as of the end of September 2023

Initiatives to Expand Scope of Use of iTrust

Examples of use in local governments

iTrust (Identity Verification)

Using the app of partner company TRUSTDOCK to perform identity verification in a local government benefits project

Cybertrust Japan x TRUSTDOCK

Transactions increased as iTrust (identity verification) is required for each and every applicant

PR: Strengthening partnership between Cybertrust Japan and TRUSTDOCK

First use of electronic consent forms in the healthcare industry!

iTrust (Digital Signature)

Adoption of electronic consent forms for the first time in the healthcare industry due to promotion of healthcare DX by the government

Signatures and consent for surgery and hospitalization can be made digitally using iTrust (digital signature)

Cybertrust Japan x Contrea

Transactions increased with expanded usage at partner companies as digitalization of the healthcare industry gathered pace

PR: Cybertrust Japan' iTrust digital signature certificates and remote signature services used in Contrea's MediOS electronic consent forms

Collaboration aimed at the spread of electronic seals

iTrust (Electronic Seal)

Using electronic seals to realize reliable data circulation

The integrity of the issuer of the electronic document can be proven using iTrust (electronic seal)

Cybertrust Japan x Infomart

Cybertrust Japan x SKYCOM

Registered with JIPDEC Trusted Service as first certification authority in Japan able to issue electronic seal certification
Leading the spread of electronic seals

PR: Cybertrust Japan and SKYCOM working together to provide reliable data circulation using electronic seals

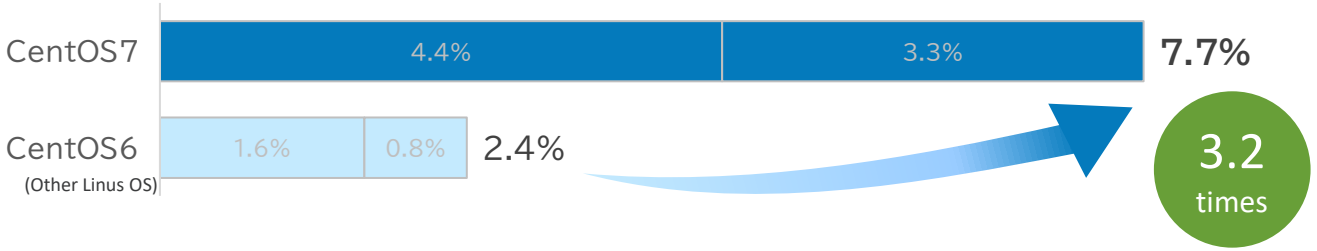
- FY2023 Q2 Financial Summary
- **Overview by Service Segment**
  - Authentication and Security Services
  - **Linux/OSS Services**
  - IoT Services
  - Overview of Others
- FY2023 Full-Year Forecast
- APPENDIX

Linux Support Progress and Initiatives

Increase in number of contracts for CentOS extended support, aiming for preparations for Q4

Extended support demand for CentOS7 expected to be up to **more than triple**

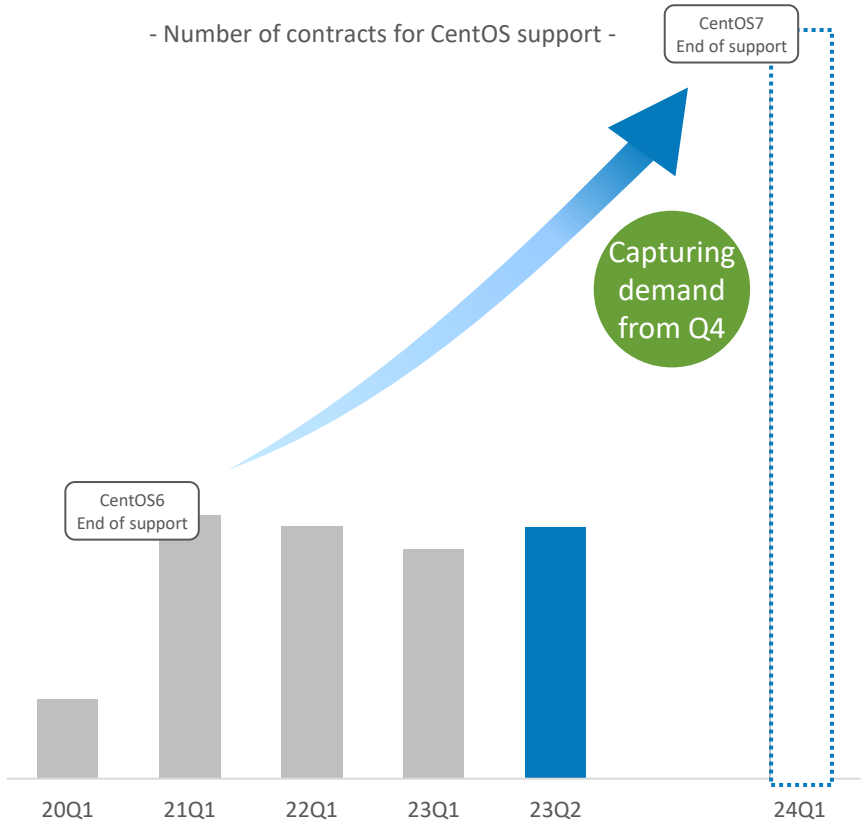
- (Linux systems) Comparison of “installed Server OS” and “Server OS with Plans to Install/Upgrade” -



Source: Nork Research 2022 Report on Status and Outlook of Server & Endpoint IT Infrastructure Implementation/Operation

Increase in number of contracts with major companies

- Number of contracts for CentOS support -



Progress being made for undertaking extended support for CentOS7

- Expansion of service lineup (Release of CentOS Extended Support LITE)
- Preparation of sales promotion activities with partners (learning center development organizing partner development, sales tools, etc.)

* End of support for CentOS6 in November 2020

Initiatives Aimed at Expansion of Sales of Linux Support

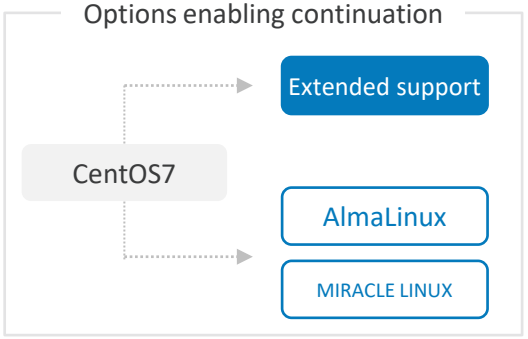
Start of provision of CentOS Extended Support LITE

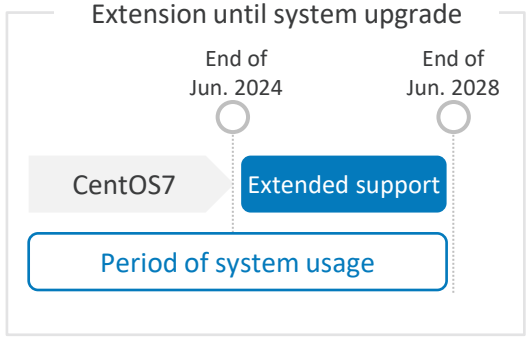
CentOS Extended Support LITE

Can be implemented from a single server for customers in small and medium environments

In addition to the existing “CentOS Extended Support” for large environments, providing “LITE” will enable all customers to use CentOS in the long term with a sense of security

Expansion of customer base





PR: Start of provision of update packages and Japanese technical support after end of maintenance renewal of CentOS for small-scale systems.

Start of provision of Linux Live Patch Service

Linux Live Patch Service

Providing live patches enabling security updates without stopping system operation

Cyber attacks on vulnerabilities are increasing
Daily OS updates are essential as a countermeasure
Providing a safe and secure environment able to automatically deal with changing threats through a Linux live patch service not provided by CentOS

Increased value

A mixture of multiple LinuxOS can coexist

CentOS　RHEL　Alma Linux
Rocky Linux　Oracle Linux

PR: Start of provision of “Linux Live Patch Service” offering security updates without interrupting the OS

AlmaLinux Progress and Initiatives

Amicable problem resolution with RedHat

23/5 Partnership announcement concerning AlmaLinux

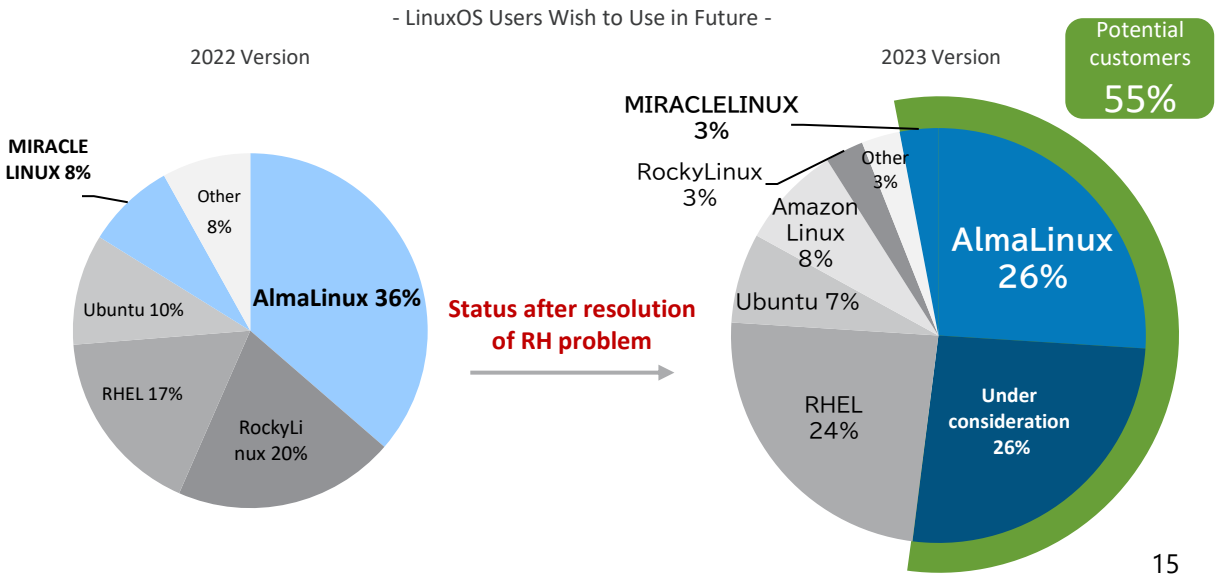
23/6 Occurrence of problems with restrictions on provision of source code by RedHat

23/7 **The AlmaLinux OS Foundation resolved the problems by continuing to provide an OS compatible with Red Hat Enterprise Linux**

Promotion of joint development with AlmaLinux

Build strong partnerships in the domestic market with AlmaLinux, which is the strongest candidate for a successor to CentOS

Expand revenue by deploying both (1) “AlmaLinux” to migrate as a successor OS and (2) “CentOS Extended Support” for customers considering where to migrate



PR: 23/5, 23/5, 23/6, 23/7

Source: DesigNET Questionnaire on Which LinuxOS You Wish to Use in Future (Aug. 24, 2023)

- FY2023 Q2 Financial Summary
- **Overview by Service Segment**
  - Authentication and Security Services
  - Linux/OSS Services
  - **IoT Services**
  - Overview of Others
- FY2023 Full-Year Forecast
- APPENDIX

Although EMLinux support grew, professional services remained flat

(Unit: Millions of yen)

IoT service net sales (Sales by transaction type)	FY22 H1	FY23 H1	YoY Change
Recurring services	32	41	+25.9%
Professional services	390	384	(1.5%)
Licenses	57	48	(15.1%)
Total net sales	480	474	(1.2%)

■ EMLinux support contracts increased, and recurring service sales grew

- In addition to onboard devices, factory equipment, and control devices, it is also being newly used in medical equipment and OA equipment

■ In professional services, there has been an increase in security consulting

- Acquired major projects leading to future opportunities such as security consulting for onboard devices and next-generation communication platforms
- Inquiries based on regulatory trends in each country have been solid

■ Contract development such as custom development has not progressed

- Existing customers' projects such as onboard devices, factory equipment, and control devices have been solid
- More projects taking longer to close and order being delayed due to changes in trends in orders received from customers
- Launch of a new version of EMLinux supporting security legislation

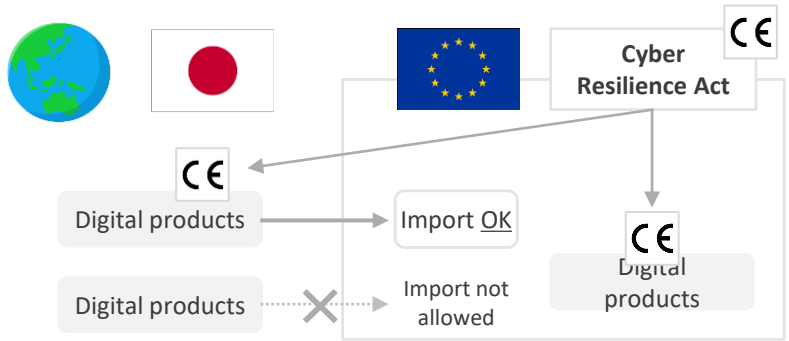
EMLinux Initiatives to Address Security Risks in Supply Chains

Obligations on manufacturers are being clarified and expanding in scope

Environment surrounding supply chain security

SBOM vulnerability management on a device basis will be mandatory for almost all digital devices from 2025

Discussion of the Cyber Resilience Act mandating security measures for digital products has progressed in Europe, and use of SBOM in vulnerability management is clearly outlined
Noncompliant products cannot be shipped from 2025, and there is a risk of Japanese companies losing competitiveness in the global market



[Main obligations = Issues]

- **SBOM creation**
- **Program update functions including vulnerability countermeasures etc.**

Start of provision of EMLinux supporting security legislation

EMLinux

EMLinux resolves the main issues by supporting SBOM standard formats

EMLinux

In addition to providing existing “vulnerability test function” standards, SBOM preparation enables tracking of the versions and license information for each package
Support for ensuring customers’ supply chain security

Source: METI EU Cyber Resilience Act, METI Cyber Security Measures

PR: The latest version of EMLinux Linux OS including ultra long-term support provides support for the enhancement of supply chain security and the improvement of development/operation efficiency supporting SBOM.

- FY2023 Q2 Financial Summary
- **Overview by Service Segment**
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
  - **Overview of Others**
- FY2023 Full-Year Forecast
- APPENDIX

Cybertrust Japan's Initiatives Driving OSS Security

First support for global standardization as a thought leader

Expansion of impact of security in the software supply chain

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The OSS global community, led by the U.S.,* formulated the OSS Security Mobilization Plan

Cybertrust Japan is focusing on three of the ten streams of the OSS Security Mobilization Plan

- SBOMs Everywhere
- Improved Software Supply Chains
- Digital Signatures

EMLinux AlmaLinux

Start of provision of products and services supporting SBOM as a result of activities

* OpenSSF (Open Source Security Foundation): Global community engaged in activities aimed at strengthening the security of open source software promoted by the Linux Foundation

- FY2023 Q2 Financial Summary
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
  - Overview of Others
- **FY2023 Full-Year Forecast**
- APPENDIX

FY2023 Full-Year Forecast

High growths in excess of 20% in net sales and in excess of 30% in operating income

Recurring growth is expected to continue with high-growth-driver services

Unit: Millions of yen	FY22	FY23	YoY change	
			Change	Rate of change
Net sales	6,167	**7,500**	+1,332	+21.6%
Operating income	1,053	**1,400**	+346	+32.9%
Operating margin (%)	17.1	**18.7**	—	—
Ordinary income	1,065	**1,400**	+334	+31.4%
Profit attributable to owners of parent	725	**950**	+224	+31.0%
EBITDA	1,623	**2,100**	+476	+29.3%

FY2023 Dividend Forecast

As of the beginning of FY2023, Cybertrust forecasts to pay **17.50 yen per share** as dividend, which is the same amount as that it paid in FY2022.

Dividend Policy	Cybertrust's basic dividend policy is to pay dividends from the surplus, once a year, as year-end dividend in a stable and continuous manner with the aim of deepening shareholders' understanding of Cybertrust's policy of business expansion from a medium- to long-term perspective, while actively investing in growth aimed at enhancing corporate value over the medium to long term.

	Interim dividend	Year-end dividend
FY2022 results (First dividend)		17.50 yen*
FY2023 forecast	0.00 yen	17.50 yen

* Cybertrust carried out a 2-for-1 stock split of shares of common stock on April 1, 2023. The year-end dividend of 35 yen per share for FY2022 is with respect to the number of shares before the split, and the amount in the table shows the dividend per share calculated after the stock split.

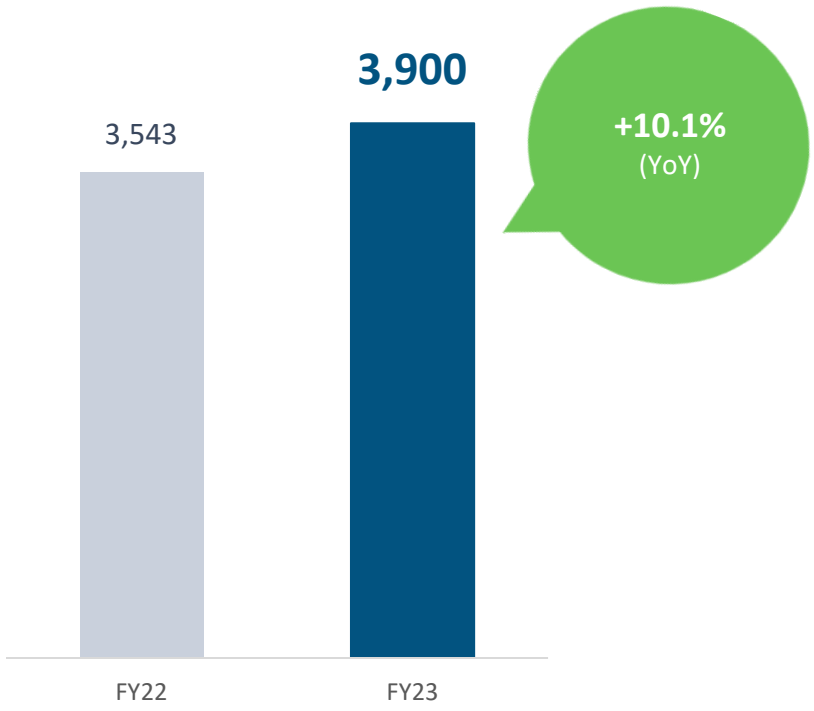
- FY2023 Q2 Financial Summary
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
  - Overview of Others
- FY2023 Full-Year Forecast
- **APPENDIX**

Numeric data

Forecast for the Year Ending March 31, 2024 (Sales by Service)

Authentication and security

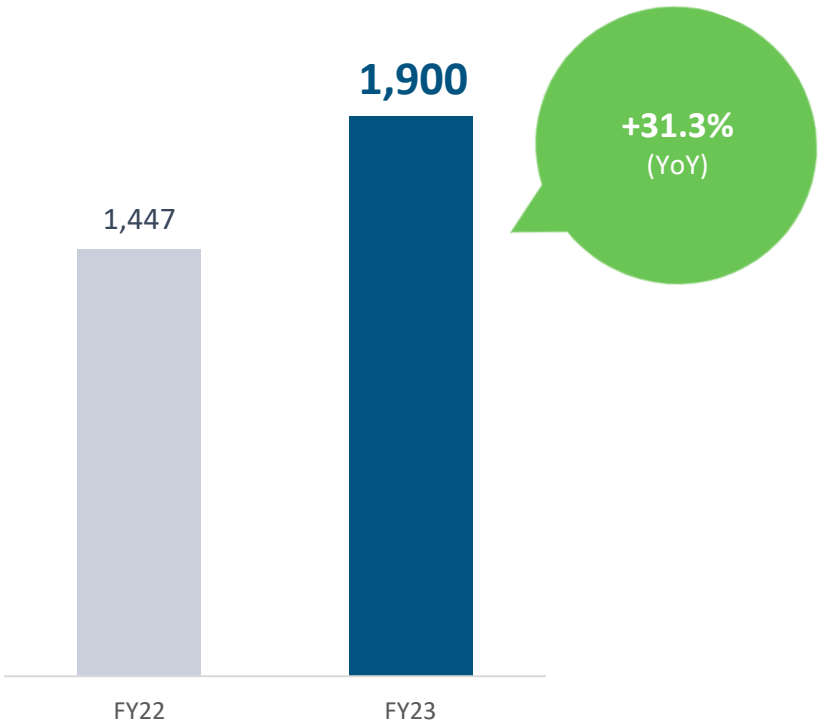
(Millions of yen)



Continued growth in the device-related ID, iTrust
Expansion of recurring revenue

Linux / OSS

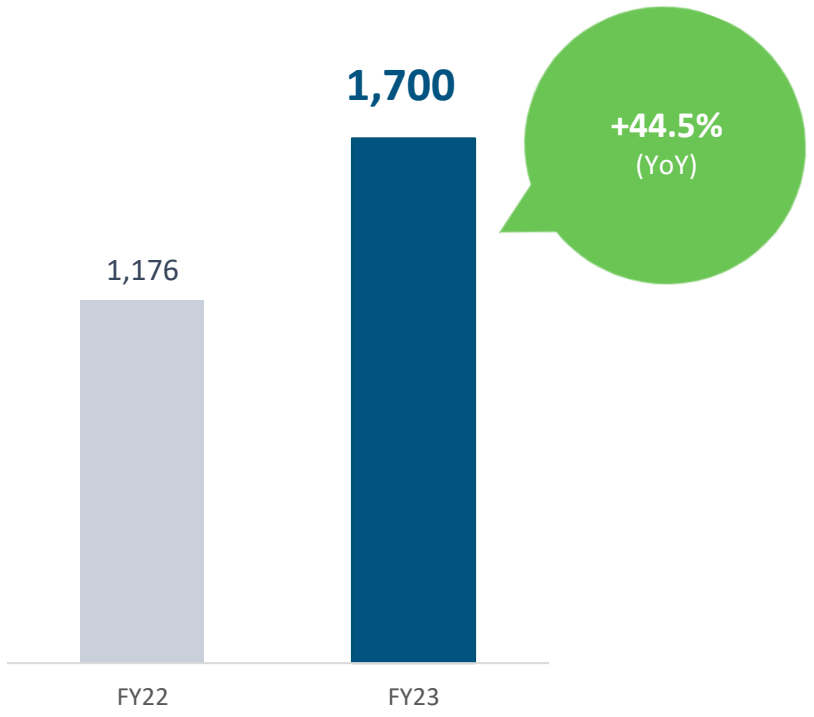
(Millions of yen)



MIRACLE LINUX to continue growing
Increase in support subscribers

IoT

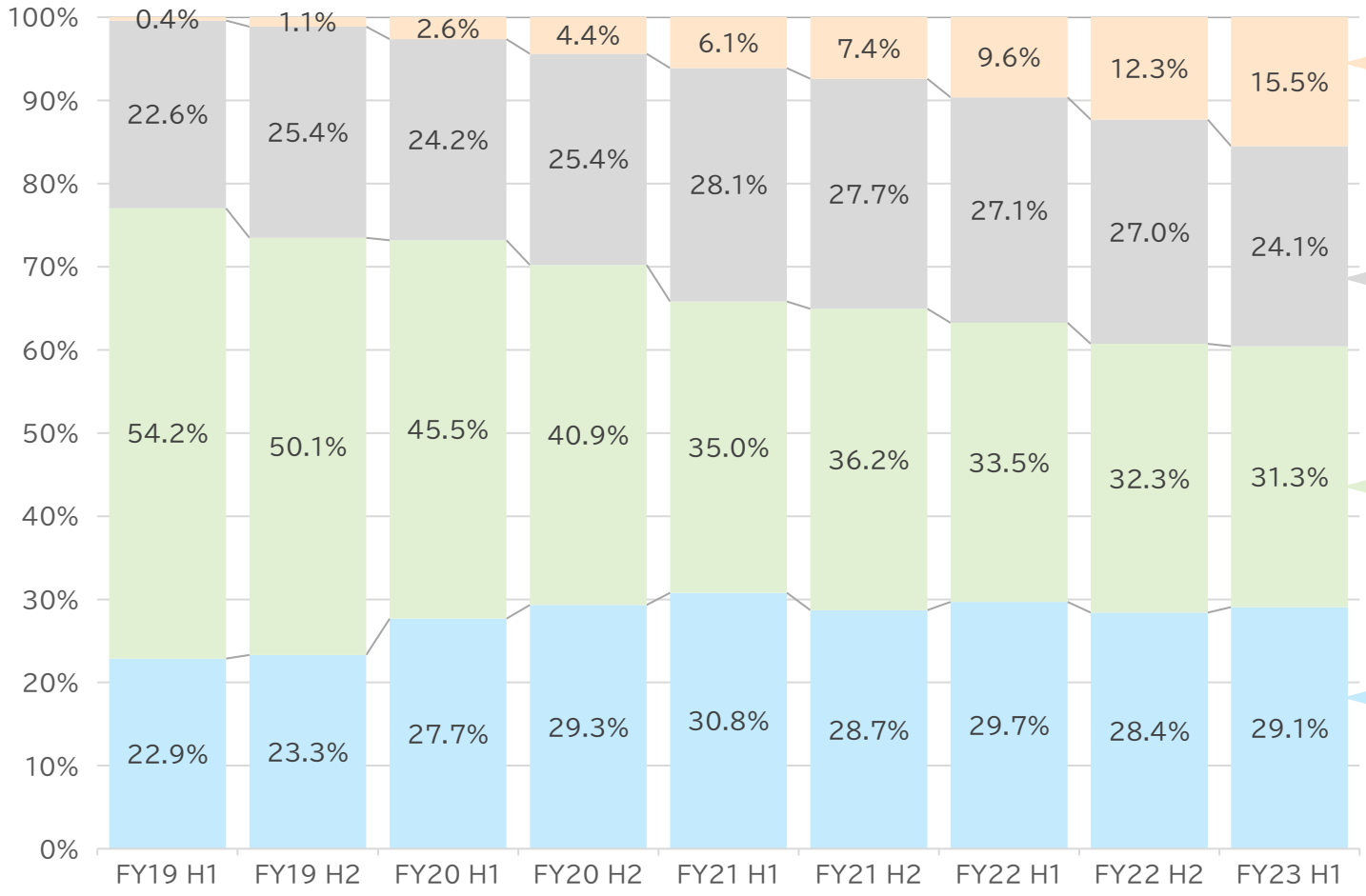
(Millions of yen)



Contract development recovered, security consulting and EMLinux contracts increased due to the progress of international safety standards.

Composition ratio of major products to recurring service sales of Authentication and Security service

Device-based ID, iTrust has grown steadily, following server certificates.



iTrust
Continued high growth and expansion of the revenue scale in authentication and security services

Others
FY23H1 scale down due to revision of some contracts for specific large Managed PKI projects, etc.

SureServer
The impact of shortening the valid period of certificates has run its course in FY21 H1, and earnings have stabilized since FY21H2

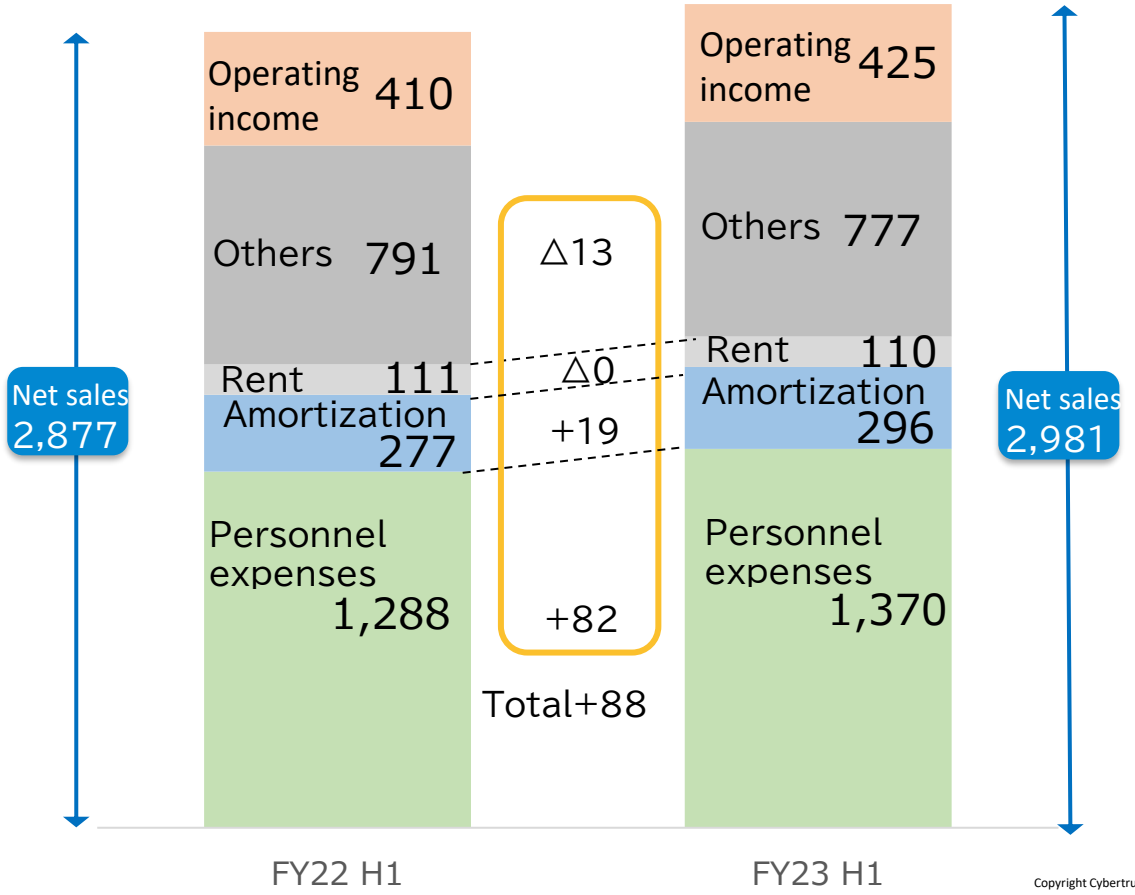
Device ID
Continued increase in YoY sales from FY19H1

cost-structure

Amortization expenses increased due to capital investment required for continuous growth of recurring services.

Changes in Costs and expenses (Consolidated)

(Millions of yen)



Capital investment policy

Aggressive investment in facilities and self-developed software for future growth of IoT services, as well as expansion of the capacity to provide digital authentication services, which are performing well.

FY23 H1 COST STRUCTURE

Major changes in the cost structure compared to the previous fiscal year are as follows

Overall cost	**Up 88 million yen**
Personnel expenses	**Up 82 million yen** New graduates and mid-career recruitment
Amortization	**Up 19 million yen** Increase related to capital expenditures and software development for device ID, iTrust and IoT, etc.

Consolidated PL (Detailed Sales by Service)

Consolidated Financial Results (Millions of yen)	FY20	FY21	FY22
Net sales	4,895	5,731	6,167
Authentication and security services	2,925	3,359	3,543
License	126	203	155
Professional services	592	567	448
Recurring service	2,205	2,588	2,939
Linux/OSS services	1,095	1,472	1,447
License	296	334	336
Professional services	182	164	124
Recurring service	617	973	985
IoT services	874	899	1,176
License	118	108	115
Professional services	725	752	981
Recurring service	30	38	80
Cost of sales	2,734	3,167	3,281
Gross profit	2,160	2,563	2,886
Selling, general and administrative expenses	1,586	1,694	1,832
Operating income	574	868	1,053

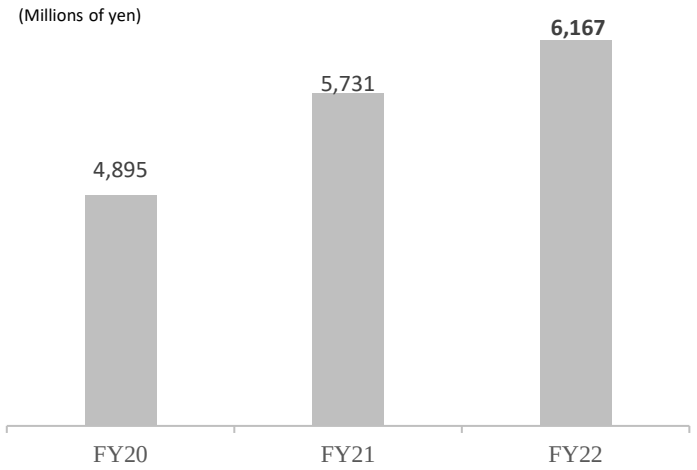
consolidated BS

(Millions of yen)

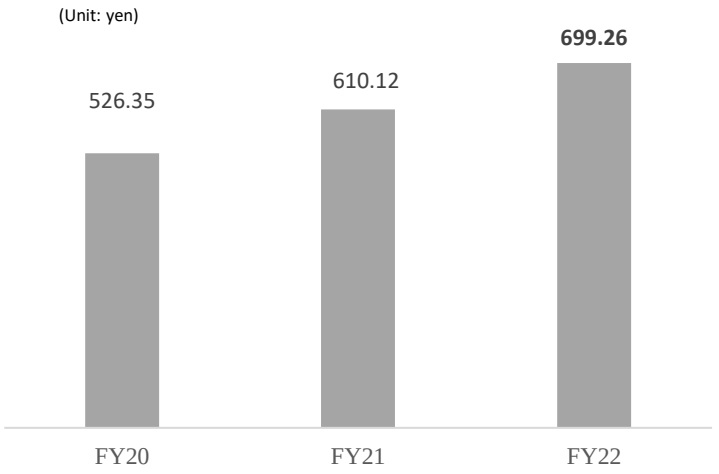
	End of Mar. 2021	End of Mar. 2022	End of Mar. 2023	YoY comparison
Current assets	3,124	4,613	**5,401**	+788
Cash and deposits	1,962	3,577	**4,366**	+788
Trade notes and accounts receivable And Contract Assets	893	861	**878**	+16
Fixed assets	2,725	2,606	**2,465**	△141
Property, plant and equipment	544	531	**513**	△17
Intangible assets	1,735	1,629	**1,512**	△117
Investments and other assets	444	445	**439**	+5
Total assets	5,851	7,222	**7,868**	+645
Current liabilities	1,585	1,786	**1,705**	△80
Long-term liabilities	413	562	**538**	△24
Net assets	3,853	4,874	**5,625**	+750

Major Consolidated Management Indicators

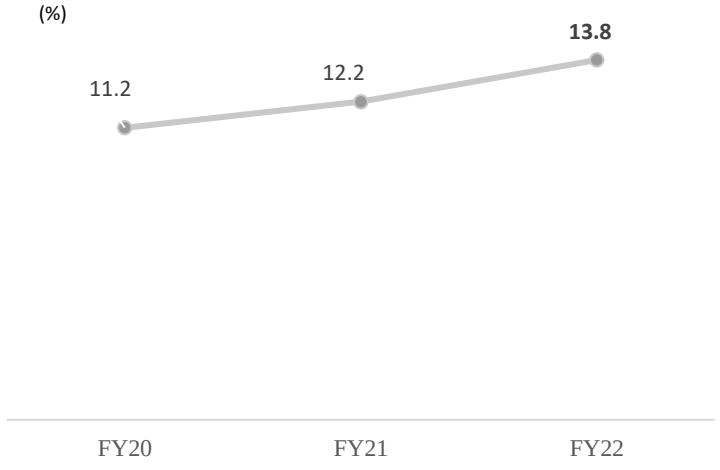
Net sales



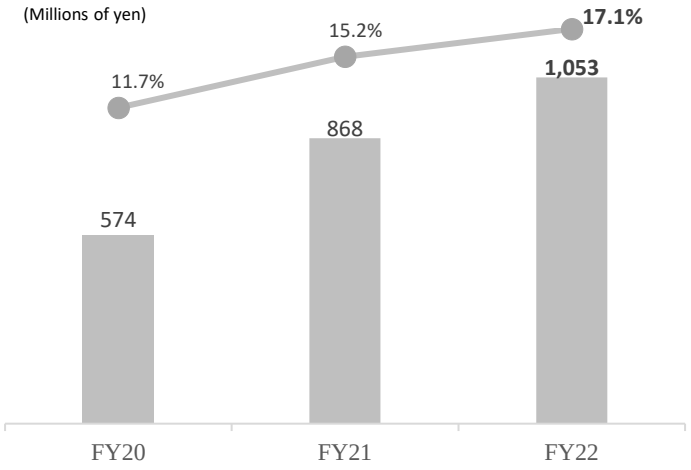
Book value per share (BPS)



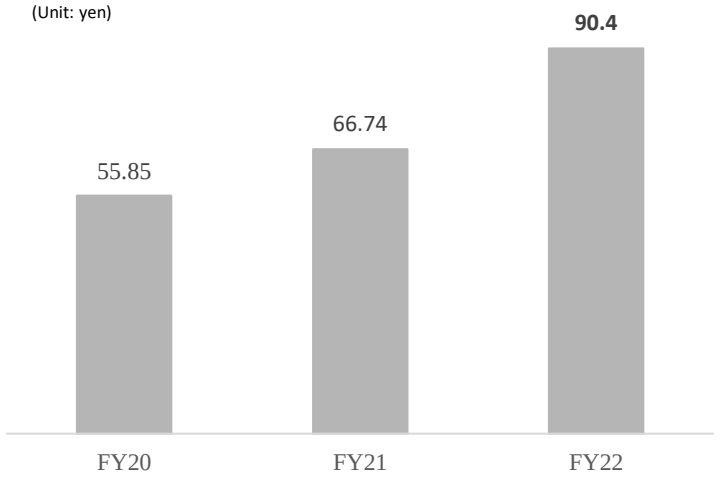
Return on equity (ROE)



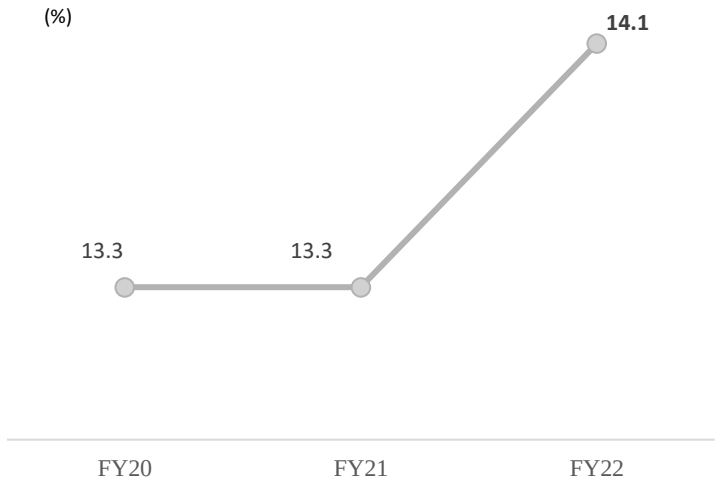
Operating income and operating income margin



Earnings per share (EPS)



Return on assets (ROA)



Corporate Information

Security and Trust

We will realize a Safe and Secure Digital Society

As a socially responsible company,
We recognize that “responding to the Sustainable Development Goals (SDGs)” is a key management issue.

Through our business and corporate activities, we work to resolve a variety of social issues in order to realize a sustainable society.

Contributing to the Realization of a Sustainable Society Along with Business Growth

Social Issues Addressed through Business Activities

By promoting trust services to support DX Realization of a safe and secure digital society

- Provision of our certification services and IoT services

Development of technology through open innovation

- Formulating specifications at OSS communities and trade associations,
  Implementation of PoC (Proof of Concept),
  Participated in activities that included making recommendations to the government and disseminating information
- Partnerships and Joint Efforts to Solve Social Issues with Companies Promoting DX

Social Issues Addressed through Corporate Activities

Achieving corporate growth by creating resilient organizations

- To enable diverse ways of working,
  Establishment of various systems such as telework systems
- Implementing measures such as active recruitment of women to realize gender equality

KPI

- **Percentage of female employees in managerial positions: Achieved at least 8.2%**
- **Various career courses: Achieved at least two items from A to D in the last three fiscal years**

A: Conversion of women from non-permanent employees to permanent employees: Temporary employees may also be hired
B: Shifting employment management categories to support women's career advancement
C: Reemployment of previously employed women as permanent employees
D: Recruitment of women aged 30 or older as permanent employees

Contributing to a Sustainable Society by Saving Resources and Energy

- Our data center is a facility that introduced carbon-free electricity
  In addition, power consumption is reduced by introducing power-saving hardware products and integrating equipment, and lighting, air conditioning, and other equipment are saved.
- Promoting paperless operations through the full introduction of electronic contracting services

KPI

- **Renewable energy use ratio: Achieve 100% by 2030**
- **Achieve a procurement rate of 90% or more of equipment that complies with environmental standards in the procurement of new equipment and materials**
- **Electronic contract ratio: Achieved 100% by 2030**
- **Deletion of printed materials: 50% reduction by 2030 compared to 2022**

By addressing four materiality issues (important social issues), we will contribute to the realization of a sustainable society as well as the growth of our business. The four materiality and major initiatives are described above.
Please refer to our website (https://www.cybertrust.co.jp/corporate/sdgs/(Link)) for further information on our SDGs initiatives.

About Us

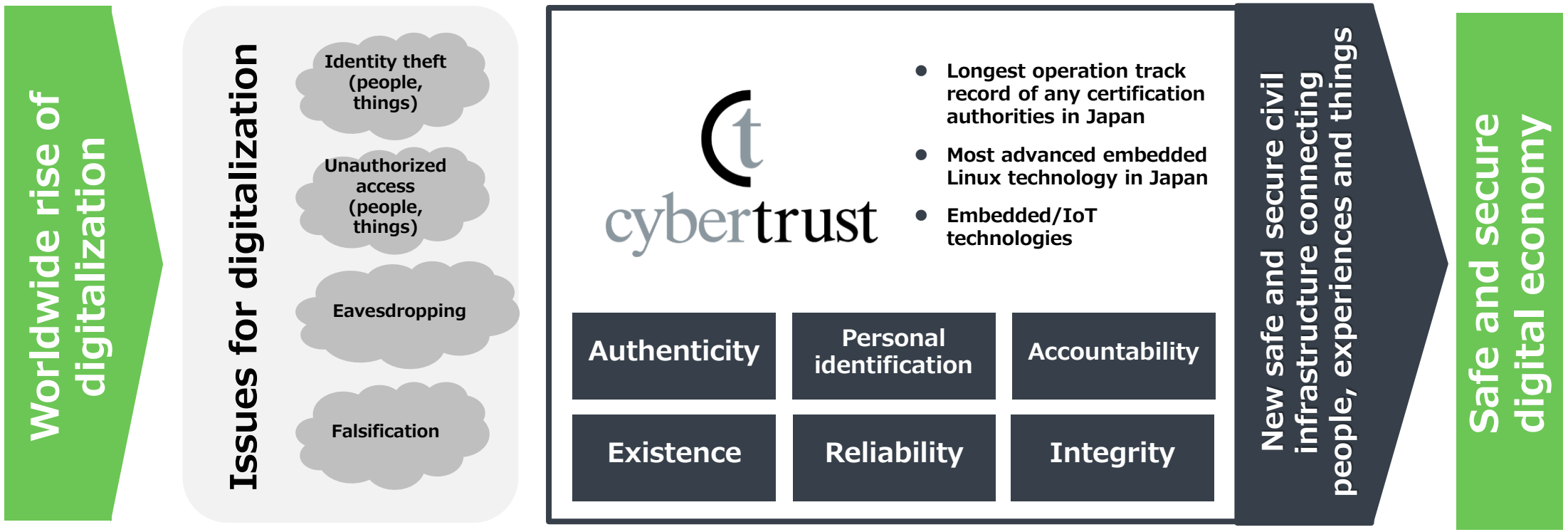
Company Name	Cybertrust Japan Co., Ltd.
Date of Establishment	June 1, 2000
Address	Ark Hills Sengishiyama Mori Tower 35F, 1-9-10 Roppongi, Minato-ku, Tokyo 106-0032, Japan
Board of Directors	Yasutoshi Magara, Chairman and Representative Director Yuji Kitamura, President and Representative Director Tetsuya Shimizu, Director Haruaki Kayama, Director Minoru Yanada, Outside Director Yoko Hirose, Outside Director Yumiko Tajima, Outside Director
Capital	812,505 Thousand yen (as of September 30, 2023)
Major shareholders (as of September 30, 2023)	SB Technology Corp. OBIC BUSINESS CONSULTANTS CO.,LTD SBI Securities Co., Ltd. SECOM CO., LTD Dai Nippon Printing Co., Ltd. Hitachi, Ltd. NTT DATA Japan Corporation THE BANK OF NEWYORK 133595 Custody Bank of Japan, Ltd.(Trust Account) Rakuten Securities, Inc.

Business Activities	■ Certification services and security solutions businesses ■ Develop Linux OS, use OSS for enterprise Software development, support and consulting services ■ IoT related business and embedded Linux related business
Affiliated companies	< Consolidated subsidiaries > Lineo Solutions Corporation Cybersecure Tech Inc. < Affiliates > Nippon Registry Authentication Inc. Other 1 company
Business Sites	Head Office (Roppongi 1-chome), Matsue Lab.

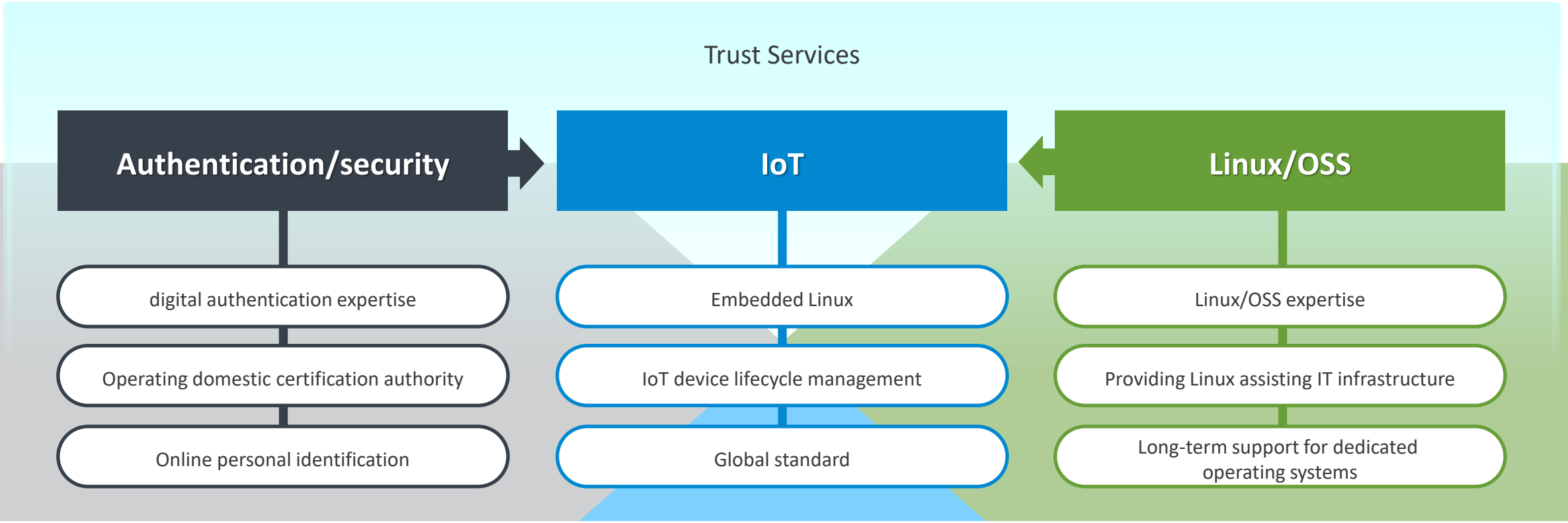
Business Overview

Issues Solved by Cybertrust and Value Provided

Providing essential trust services in the era of digital transformation (DX)



Cybertrust provides original Trust services for solving DX issues by combining Authentication and security and Linux/OSS technologies.



Overview of Authentication and Security Services

Providing trust services for areas such as digital certificate, digital Identity verification and digital signature - the 'ID cards' of the digital economy
An operation track record as Japan's first commercial certification authority and one conforming to international audit standards

Cybertrust's lineup of authentication and security services

Real-world certificates

- Driver's License
- Passports
- Certificates of registered hanko ID stamps

Guaranteed by government agencies

Procedures in writing, by post or other real-world means

Digital-economy certificates

- **digital certificate**
- **digital Identity verification and digital signature**

Guaranteed by certificate authorities*

*Organizations that identify applicants, issue certificates and manage the issued certificates.
Cybertrust has operated Japan's first commercial certification authority for over 20 years.

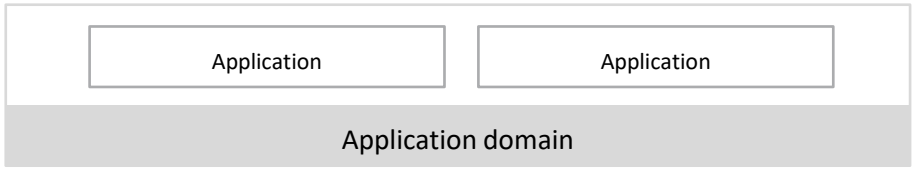
Server certificate (SureServer)	Website existence SureServer Prime
Device certificate (Device ID)	Authenticating devices permitted for operations use
User certificate	Authentication of employees, members or others
iTrust services	Ensuring the reliability of electronic transactions

- A business operator approved by the competent Minister pursuant to the provision of Article 17, paragraph (1), item (vi) of the Act on the Certification Business of the Local Government Information System Organization for digital signature, etc.

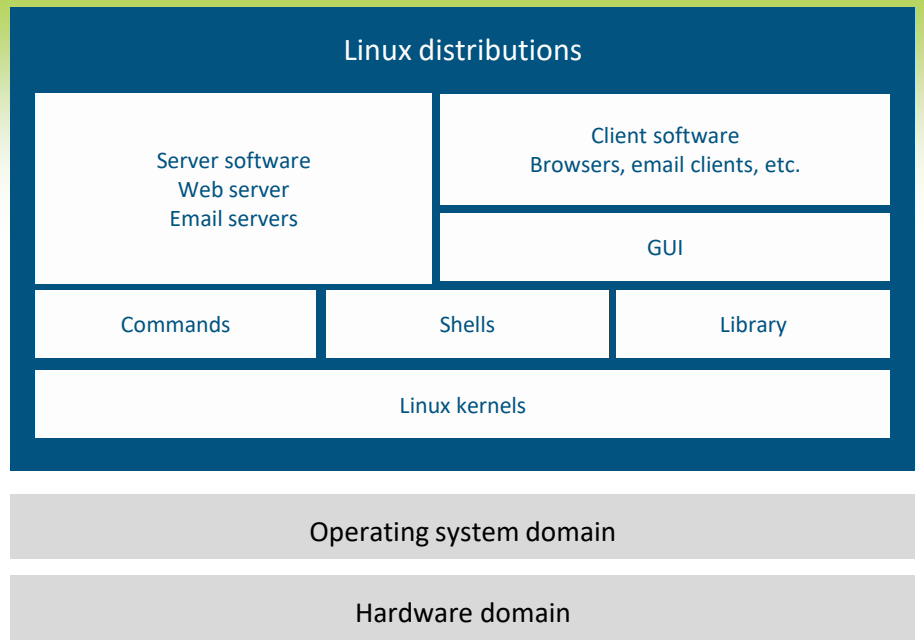
Overview of Linux / OSS Services

Japan's only Linux/OSS distributor run by a group of engineers active in the global OSS community

General Siers



Building application systems on operating systems



Functions needed for the Linux kernel are brought together and then provided and supported as Linux distributions

Extensive track record of use with critical systems

Air traffic control systems, industrial equipment, communication infrastructure, vehicles, rolling stock, others

Long-term support (10 years or more) can be provided

- OSS community support ends in 5 to 6 years.
- Performance parts for product repairs can be held 5 to 9 years after the end of production or sales

Cybertrust product areas with established track records
Server monitoring, vulnerability management, security, Linux for t

MIRACLE LINUX Powered by Cybertrust Japan
MIRACLE ZBX
MIRACLE VulHammer
EMLinux

Overview of IoT Services

Providing technology expertise ranging from Linux operating systems for IoT devices to authentication and lifecycle management

providing secure operation of IoT devices **Linux/OSS technology**	used to verify IoT device authenticity **Authentication and security technology**	enabling lifecycle management of IoT devices **IoT device/cloud connection technology**
Cybertrust product: EMLinux	Cybertrust service: Secure IoT Platform	Secure IoT Platform (SIOTP)

- Provides IoT devices with vulnerability updates for 10 years (extendable).

- Ensures safety, verifies authenticity and provides long-term lifecycle management for IoT devices.
- Covers cybersecurity measures needed in cloud environments such as OTA updates and secure boot.

One of very few providers worldwide that can provide a comprehensive lineup of all the technologies needed

Conformance with international IoT device manufacture and operation standards (IEC62443/NIST SP800/FIPS140-3/WP29-ISO21434, etc.)

Medium-Term Management Plan

BizX 20/40 (Medium-Term Management Plan)

cybertrust

Medium-Term Management Plan

Achieve dramatic growth in performance over three years from FY2022 through initiatives to address the five key themes for business transformation

1 Organization growth and human resource development

- Securing engineers and other human resources with high-level and specialized knowledge and skills
- Implementing training and skills improvement support for employees
- Engagement policy aimed at building a better organization and workplace environment

2 New market creation and focus

- Focus on high-growth-driver services of iTrust, Linux support, and EMLinux
- Initiatives for OSS Security Mobilization Plan
- Strengthening of partner ecosystem

3 R&D for the future

- Prior art research by R&D department
- Initiative for commercial post quantum cryptography certification service

4 Global expansion

- Collaboration with Quantinuum (U.K.)
  The world's largest integrated computing company
  Completed integration of quantum-computing-hardened private keys into new IoT authentication platform

5 Stable system operation and quality assassurance

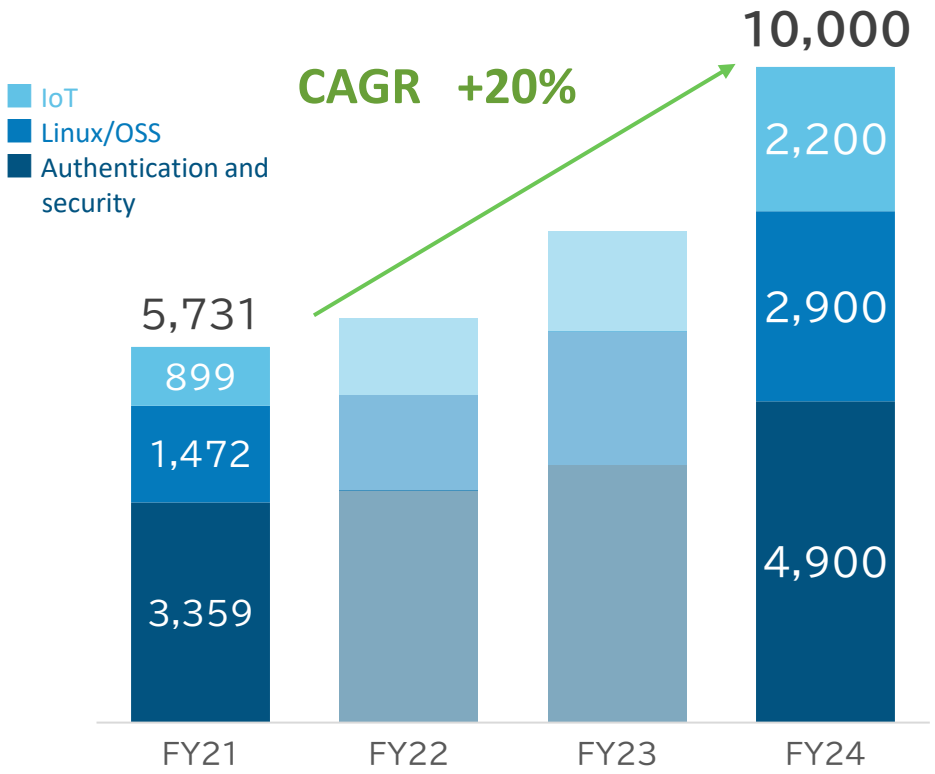
- Improving the availability of trust service provision platform, whose impact on socioeconomic activities are expanding along with the spread of digital transformation

BizX 20/40 (Medium-Term Management Plan)

cybertrust

Net sales target to be achieved by FY2024: 10.0 billion yen

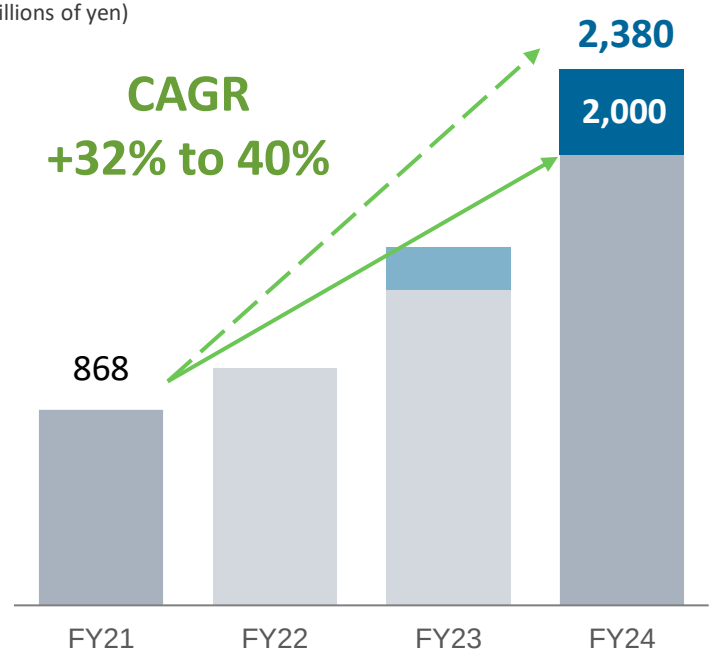
Aim for **20% growth in CAGR** centered on recurring sales of various services



Operating income of 2.0 billion yen or more by FY2024

- **Operating margin** goal **of 20 to 24%**
- The target compound annual growth rate (CAGR) was set by taking into account the impact of external environment uncertainties such as (1) trends in international safety standards and (2) continuation of unstable semiconductor supply

(Unit: Millions of yen)



Steady growth in FY2022, the first year of the Medium-Term Management Plan Progressing as planned in FY2023 by focusing on high-growth-driver services for achieving the goals for FY2024, the final year of the plan

BizX 20/40 (Medium-Term Management Plan)

Aim for net sales of 10 billion yen and operating income of 2 billion yen in 2024 through stable, high-revenue services and high-growth-driver services

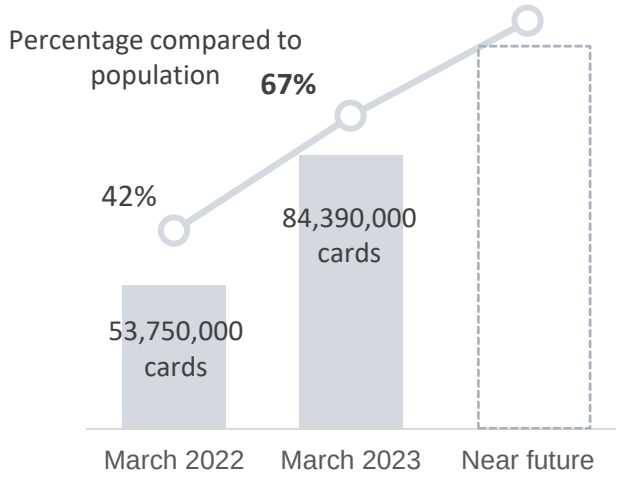
1. iTrust (Identity Verification) Business Model

Authentication and Security

cybertrust

Adoption of Individual Number Cards to continue

- Number of Individual Number Cards issued -



Source: Ministry of Internal Affairs and Communications "Number of Individual Number Cards issued by municipalities"

Increase in online identity verification usage

Expectations on increased usage in daily life as situations where Individual Number Cards are used expand further

Till now	From now
Account opening	Various online transactions
Smart payment	Online applications to administrative agencies

Various identity verification

- Bank account opening
- Securities company account opening
- Insurance policies
- QR code-based payment Linking with account
- Real estate transactions
- Purchase of second-hand goods
- Mobile phone contracts
- Ticket purchases
- Sharing services
- Administrative procedures
- Income tax returns
- Child-rearing
- Relocation

etc.

Increase in iTrust transactions

Use of iTrust increases as identity verification needs at partner companies

Use of identity verification documents such as Individual Number Cards, etc.

Just hold it over the card

Linked with the software embedded in the partner's application

Transaction billings

Online identity verification through iTrust identity verification

Increased profitability of iTrust = increased profitability of recurring services

2. iTrust (Digital Signature) Business Model

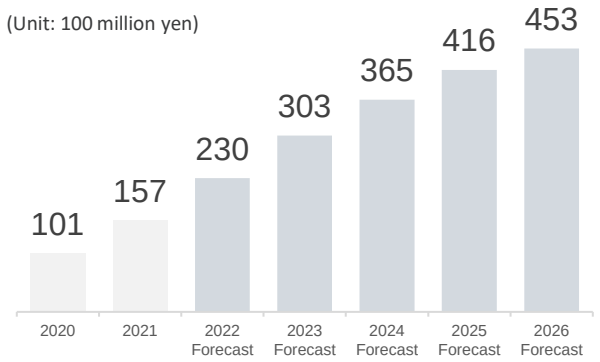
Authentication and Security

cybertrust

Further progress in digitalization

Digitalization advancing as society breaks away from seal usage, converts to paperless operations, and related laws are enacted

- Changes in electronic contract service market size -



Source: ITR “ITR Market View: Legal Tech Market 2022”

Expansion of scope of use of digital signatures

Expansion in scope of use of digital signatures that prove the authenticity of electronic documents such as electronic books and electronic contracts

Till now	From now
Electronic contracts (Usage expanded to real estate-related contracts etc. with revisions to the law)	Electronic books Certificates, etc. issued by companies, organizations

Legislation

October 2023	Start of digital invoicing system
December 2023	End of deferral period for electronic storage obligation under the Act Concerning Preservation of Electronic Books

Various digital signatures

Electronic contracts between companies

Electronic contracts (real estate, financial, etc.)

Electronic books

Electronic invoices

Verification documents,

etc.

Increase in iTrust transactions

Use of iTrust increases as the scope of use of digital signatures expands at partner companies

Contracts, etc. in electronic format

PDF

PDF

through the API embedded in electronic contract services of partner companies

(seal)

Transaction billings

Digital signature with iTrust remote signature

Increased profitability of iTrust = increased profitability of recurring services

3. Realize Growth of Recurring Business through Paid Support Business

Linux/OSS

cybertrust

Two pillars

[1] International collaborations

Initiative for development of international standard OS and provision of paid support service that can lead to secure long-term operation

Contribution to AlmaLinux OS Foundation
Long-term provision of international standard OS AlmaLinux

Collaboration with CloudLinux
Provision of value-added paid support service
that can ensure security and realize optimum operating cost

Contribution to Open Source Security Foundation
Provision of secure software through SigStore, software supply chains, and SBOM standardization

[2] Collaboration with Japanese partners

Provision of OS that can be safely operated by medium-sized enterprises and SMEs as well as large companies over a long period of 16 years, and paid support for international standard OS by Japanese companies in collaboration with partners around the nation

Indicators for business expansion

December 2021
Number of paid support service contracts tripled through digital marketing after end of support for CentOS8

MIRACLE LINUX
More than 70,000 downloads

Cybertrust Japan Partner Network
Increased to 151 companies nationwide

June 2024
Support ends
for CentOS7

Paid Linux/OS Support
Growth from increase in number of new contracts and renewal rate

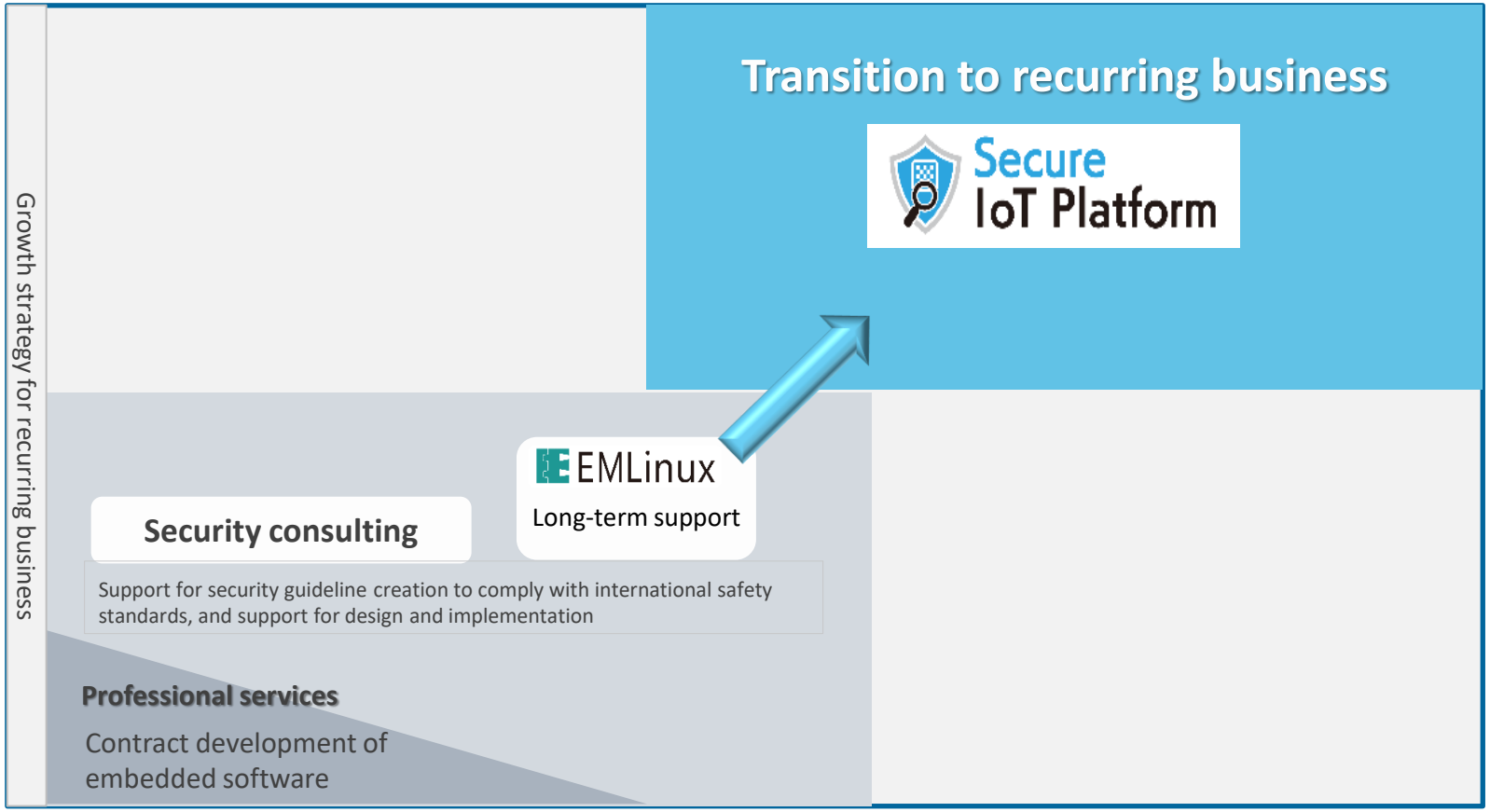
Expects net sales of 1 billion yen

- June 2023 BizX20/40 Medium-Term Management Plan 2nd phase
- March 2025 BizX20/40 Medium-Term Management Plan final phase

4. Realize Growth of Recurring Business through Expansion of EMLinux Business

IoT

cybertrust



Increase in number of EMLinux contracts

Adopted by IoT device developers to comply with IoT security requirements both within and outside Japan

Work with OSS community and continuously offer security upgrades for vulnerabilities, etc. for a 10-year period

EMLinux development
Increase in number of contracts

Increase in number of SIOTP contracts

Recurring service that verifies the authenticity and prevents falsification and forgery of data in combination with the digital certificate issued by the Certification Authority operated according to international standards by Cybertrust Japan over the lifecycle of IoT devices from manufacturing to scrapping

Collaboration with OSS Global Community Leading to Business Expansion

Cybertrust Japan's concept regarding OSS community activities

Some 90% of software worldwide are developed using OSS

Numerous new technologies are taken up and developed by OSS community

Cybertrust Japan aims to expand the market by earning the trust of customers through contributions that enable safety and security, high quality, and long-term support in the OSS community

Contributing to and driving forward OSS Security Mobilization Plan

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Against the background of growing security issues, OSS global community, led by the U.S.,*1 formulated the OSS Security Mobilization Plan

Cybertrust Japan expresses its commitment to participate and contribute to the security mobilization plan

Improved trust by developing and offering own products compliant with the security mobilization plan

- Digital Signatures Sigstore
- SBOM
- Supply chains

Actively participating and contributing so as to ensure safe and secure usage of software by eliminating security risk of falsification of software component lists and software

Contribute to high-growth-driver services by installing it in Cybertrust Japan products and by offering paid service

Achievement from collaboration with OSS community

Provision of OS that can be safely operated by medium-sized enterprises and SMEs as well as large companies over a long period of 12 to 16 years, and paid support for international standard OS by Japanese companies in collaboration with partners around the nation

AlmaLinux

MIRACLE LINUX

CentOS Extend Support

EMLinux

*1 OpenSSF (Open Source Security Foundation): Global community engaged in activities aimed at strengthening the security of open source software promoted by the Linux Foundation.
*2 CIP(Civil Infrastructure Platform) is an OSS community for providing long-term maintenance of embedded systems in social infrastructure applications. Cybertrust Japan is a CIP member. >CIP project site (English)

Glossary ①

Term	Description
digital certificate	Digitized identity certificates that properly certify and identify targets. These certificates verify the authenticity of people, goods, etc. by examining and issuing them by a certification authority as a reliable third-party organization.
digital authentication	Preventing spoofing or falsification of information by electronically verifying that each user on a network or system having multiple users is the authorized user.
certification authority	An organization with the authority to issue, revoke and manage digital certificates. Certification authority is made up of registration authority (for investigating certificates) and issuing authority (for issuing, revoking and managing certificates).
Server Certificate	A digital certificate used to verify the existence of the website's operator and encrypt data transmitted between the browser and web server.
EV server certificate	EV stands for 'Extended Validation'. The most reliable SSL/TLS certificate. Issued in accordance with rigorous and globally uniform investigation standards. Can be issued only by digital authentication providers that have passed audits set forth by auditing organizations.
Multi-domain certificate	A certificate that can be registered in a Subject Alternative Names (SAN) area and used for several domains, even for FQDN that contain different domains
Wildcard certificate	Certificates Available in One Certificate for Different Subdomains in the Same Domain
SSL conversion	Encrypting the interaction (communication) between a website and the user browsing the site

Glossary ②

Term	Description
Client certificate	A digital certificate that installs a certificate on the user's device (such as a PC or smartphone) to authenticate the user as the authorized user. There are two main types: User certificates and device certificates.
Device certificate	Issued to information devices such as smartphones and tablets. Prevents access from unauthorized information devices by controlling in-house network access authorization to 'only devices with certificates.
User certificate	Used to authenticate individuals, such as employee ID cards and system login cards
e-seal	A measure such as encryption to indicate the organization from which the electronic document, etc. was issued, and a mechanism to confirm that the document, etc. has not been tampered with since the measure was taken.
VAR	A vendor partner contract in which some of the services sold have Device ID embedded or selectable as an option.
Linux	An operating system having free and publicly released source code that lets anyone use, copy, alter or redistribute it. Linux can be rebuilt by selecting the functions needed, so is used to provide servers and embedded systems for electrical appliances and a wide range of other applications.
OS	Stands for 'operating system'. The underlying program that manages an entire computer system and provides the usage environment shared by the various types of application software running on the system.
OSS (Open Source Software)	Software having free and publicly released source code (the instructions that define the software). Anyone can use, improve or redistribute open-source software.
Linux distributions	A collection of Linux kernels and other software packages that can be easily installed and used by users

Glossary ③

Term	Description
RHEL	Abbreviation for Red Hat Enterprise Linux. A Linux distribution developed and sold by Red Hat for business use.
CentOS	Community-based free LinuxOS that is highly compatible with RHEL
OSS community	A nonprofit organization of users, developers and fans created mainly to develop, improve or exchange information about open-source software (OSS). Members located throughout the world share source code, collaborate on development projects, share relevant information, hold workshops and the like.
SBOM	Software Bill of Materials: A software bill of materials that lists the components, dependencies, and types of licenses included in the software.
Integrated monitoring tool	A tool used to identify and analyze operating statuses by acquiring operation information from a server to determine whether it is operating normally.
Embedded	A term used to describe devices or systems intended to perform limited functions specialized for certain applications. Examples of embedded devices include household appliances, vehicles, and electronic devices such as mobile phones or cameras.
Real time (RT)OS	A type of operating system used widely in embedded systems. Differs from the general-purpose operating systems in common use by prioritizing real-time operation.
ROT	Root of Trust: A fundamental part of hardware and software security that provides reliability.
Sigstore	Signature-service to verify the source and authenticity of OSS

Glossary ④: Security-Standard "FIPS 140-3"

Summary	
What is FIPS 140-3?	Standard for cryptographic modules established by the National Institute of Standards and Technology (NIST:National Institute of Standards and Technology) that was certified in March 2019.
Roles of FIPS 140-3	Functions as a standard for realizing secure information system construction by covering areas related to secure design, implementation, and operation of cryptographic modules.
Importance of FIPS 140-3	In response to the recent occurrence of cyber security incidents centering on critical infrastructures, not only hardware/software vendors but also service vendors and cloud service providers in the U.S. are required to introduce and implement FIPS140-3.
FIPS 140-3 advantages	Products/services conforming to FIPS 140-3 are guaranteed to implement cryptographic modules with the highest level of security and to have high reliability. The use of FIPS 140-3 is critical to protecting sensitive security-information and data.
Trends in U.S. Government Procurement Standards	Similar measures are required to safely build and operate products and services in systems and cloud services operated by civilian goods and private entities, regardless of the Department of National Security and the Department of Defense purchasing requirements.
International influence	Influence is spreading internationally as it is a U.S. government-led standard Many countries/organizations adopt FIPS 140-3 as a security standard and use it to develop products/protect information systems.
Influence in Japan	As many domestic companies incorporate and operate in the global supply chain, it is essential to meet FIPS140-3 and maintain their certification.
Transition from FIPS 140-2	FIPS140-2 will also expire on September 21, 2026, so transition to FIPS140-3 is required.

Essential for ensuring reliability and safety as the most important security standard

Product name comparison table

Function	Official product name	Abbreviations in this document
【Authentication and Security]		
SSL/TLS server certificate	SureServer	SureServer
device authentication	Cybertrust Device ID	Device ID
Certification bureau outsourcing services	Cybertrust Managed PKI	Managed PKI or MPKI
Identity verification, Certificate for document signing and digital signature	iTrust identity verification services, iTrust identity verification service , iTrust Remote Signing Service	iTrust ※Indicated as a service that encompasses the three services shown on the left
Identity Verification	iTrust identity verification service	iTrust (identity verification)
Certificate for document signing	iTrust digital signature certificate	iTrust (digital signature) ※Indicated as a service that encompasses the two services shown on the left
digital signature	iTrust Remote Signing Service	
e-seal	iTrust certificate for e-seal	iTrust （e-seal）
[Linux / OSS]		
Server OS/cloud infrastructure	MIRACLE LINUX	MIRACLE LINUX
Integrated monitoring	MIRACLE ZBX	MIRACLE ZBX
[IoT]		
Linux for IoT	EMLinux	EMLinux
IoT Trust Services	Secure IoT Platform	SIOTP

Product and Service Introduction Pages

Product and service introduction page	URL
CyberTrust Co., Ltd. Web website	https://www.cybertrust.co.jp/(Link)
【Authentication and Security]	
SureServer service	https://www.cybertrust.co.jp/sureserver/(Link)
Cybertrust Device ID Service	https://www.cybertrust.co.jp/deviceid/(Link)
iTrust service	https://www.cybertrust.co.jp/itrust/(Link)
[Linux / OSS]	
MIRACLE LINUX goods	https://www.cybertrust.co.jp/miracle-linux/(Link)
CentOS support service	https://www.cybertrust.co.jp/centos/(Link)
MIRACLE ZBX goods	https://www.cybertrust.co.jp/zabbix/(Link)
MIRACLE VulHammer goods	https://www.cybertrust.co.jp/zabbix/vul-hammer/(Link)
[IoT]	
EMLinux products	https://www.cybertrust.co.jp/iot/emlinux.html
Secure IoT Platform Services	https://www.cybertrust.co.jp/siotp/index.html

Press Release List（FY23 Q2～）

07.05

Cybertrust Japan to DX ongoing customer management operations for financial institutions and others with iTrust identity verification service

07.18

Cybertrust Japan Collaborates with Accessilens to Improve Website Accessibility

08.02

Cybertrust Japan Launches iTrust certificate for e-seal, enabling safe and secure data distribution of various electronic documents

08.08

Cybertrust Japan Adopts Persefoni's Carbon Accounting and Management Software

08.10

Cybertrust Japan offers medical DX solution to support security measures of medical institutions

08.22

Cybertrust Japan launches post-maintenance update CentOS fix package for small systems and technical support in Japanese

08.30

Cybertrust Japan launches "Linux Live Patch Service" for non-disruptive OS security updates

09.01

Identity verification by public certification service for individuals of Individual Number Card Increased 22 Times in 18 Months. Cybertrust Japan and TRUSTDOCK strengthen cooperation.

09.05

Cybertrust Japan and Skycom collaborate to ensure reliable data distribution using e-seals

09.11

Cybertrust Japan and Tokyo System House begin providing mainframe migration support services for legacy mission-critical systems.

09.14

Cybertrust Japan 's iTrust digital signature certificate and remote signing service adopted for Contrea's MediOS electronic agreement

09.21

Launched the latest version of vulnerability management tool that can be linked with JP1, Japan's No. 1 operation management software in terms of market share

Disclaimer

- The materials and information provided in this presentation contain ‘forward-looking statements’.
- They are based on current expectations, forecasts and risk-bearing assumptions, and involve uncertainties that could lead to results that differ materially from these statements.
- These risks and uncertainties include general industry and market conditions, and general domestic and international economic conditions (interest rate and foreign exchange rate fluctuations).
- Information in these materials that is not about the Company is taken from sources such as publicly released information. The Company makes no guarantees regarding the accuracy, suitability or any other properties of this information.
- The names of us and third-party products or services described in this document are trademarks or registered trademarks of each company. “SureServer,” “iTrust,” “MIRACLE LINUX” and “MIRACLE ZBX” are registered trademarks of Cybertrust Japan Co., Ltd.

cybertrust

Security and Trust