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.

cybertrust

FY2024 Q1 Financial Results

First Quarter of the Fiscal Year Ending March 31, 2025

Cybertrust Japan Co., Ltd.

TSE Growth: 4498

July 30, 2024

Executive Summary

FY2024 Q1 Financial Results

Increase in sales compared to the same period of the previous year

Record-high net sales

Profit declined due to systematic investment activities

- Investments including temporary expenses for full-fledged operation of Cybertrust's root certification authority

FY2024 Full-Year Forecast

Net sales and operating income are forecast to increase from Q2

- CentOS extended support accumulated order backlog beyond expectations

Progressing as planned toward the achievement of the full-year forecast

Agenda

- FY2024 Q1 Financial Summary
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
- Management Topics
- FY2024 Full-Year Forecast
- Appendix

- **FY2024 Q1 Financial Summary**
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
- Management Topics
- FY2024 Full-Year Forecast
- Appendix

FY2024 Q1 Consolidated Results

Record high Q1 net sales; decline in profit due to systematic investment activities

Net sales rose 3.4% YoY to 1,493 million yen

Operating income decreased 19.4% YoY to 144 million yen

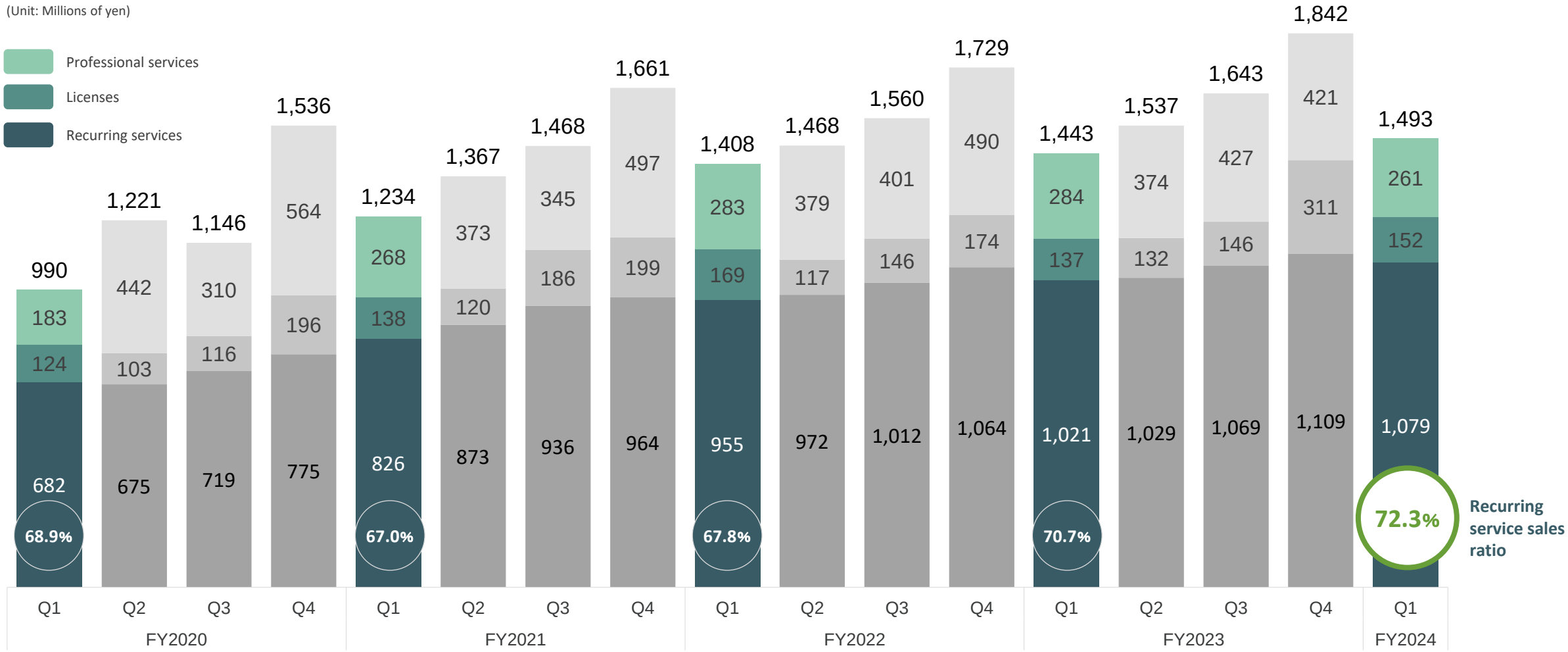
(Unit: Millions of yen)	FY23 Q1	FY24 Q1	YoY Change
Net sales	1,443	1,493	+3.4%
Operating income	179	144	(19.4%)
Ordinary income	179	148	(17.6%)
Profit attributable to owners of parent	116	103	(10.9%)
EBITDA	330	263	(20.2%)

* Decline in profit, caused by planned expenses including temporary expenses for the external audit prior to full-fledged start of the Company's root certification authority and increase in personnel costs, is within the scope of the plan

Trend in Quarterly Sales by Transaction Type

Record high Q1 recurring service sales ratio of 72.3%

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: Grew with accumulation of recurring services centered on high-growth-driver service iTrust
- Linux/OSS: CentOS7 extended support accumulated order backlog beyond expectations
- IoT: Sales of contract development was stagnant despite growth in EMLinux support and strong performance by security consulting

(Unit: Millions of yen)	FY23 Q1		FY24 Q1		YoY Change	
	Net sales	Sales ratio	Net sales	Sales ratio	Change	Rate of change
Authentication and Security Services	885	61.3%	921	61.7%	36	**+4.1%**
Linux/OSS Services	312	21.6%	322	21.6%	10	**+3.3%**
IoT Services	246	17.1%	249	16.7%	2	**+1.1%**
Total net sales	1,443	100%	1,493	100%	49	**+3.4%**

- FY2024 Q1 Financial Summary
- **Overview by Service Segment**
  - **Authentication and Security Services**
  - Linux/OSS Services
  - IoT Services
- Management Topics
- FY2024 Full-Year Forecast
- Appendix

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

(Unit: Millions of yen)

Authentication and Security Service net sales (by transaction type)	FY23 Q1	FY24 Q1	YoY Change
Recurring services (Recurring service sales ratio)	763 (86.3%)	807 (87.6%)	+5.8% (1.3 pp)
Licenses	53	47	(9.5%)
Professional services	68	66	(3.5%)
Total net sales	885	921	+4.1%

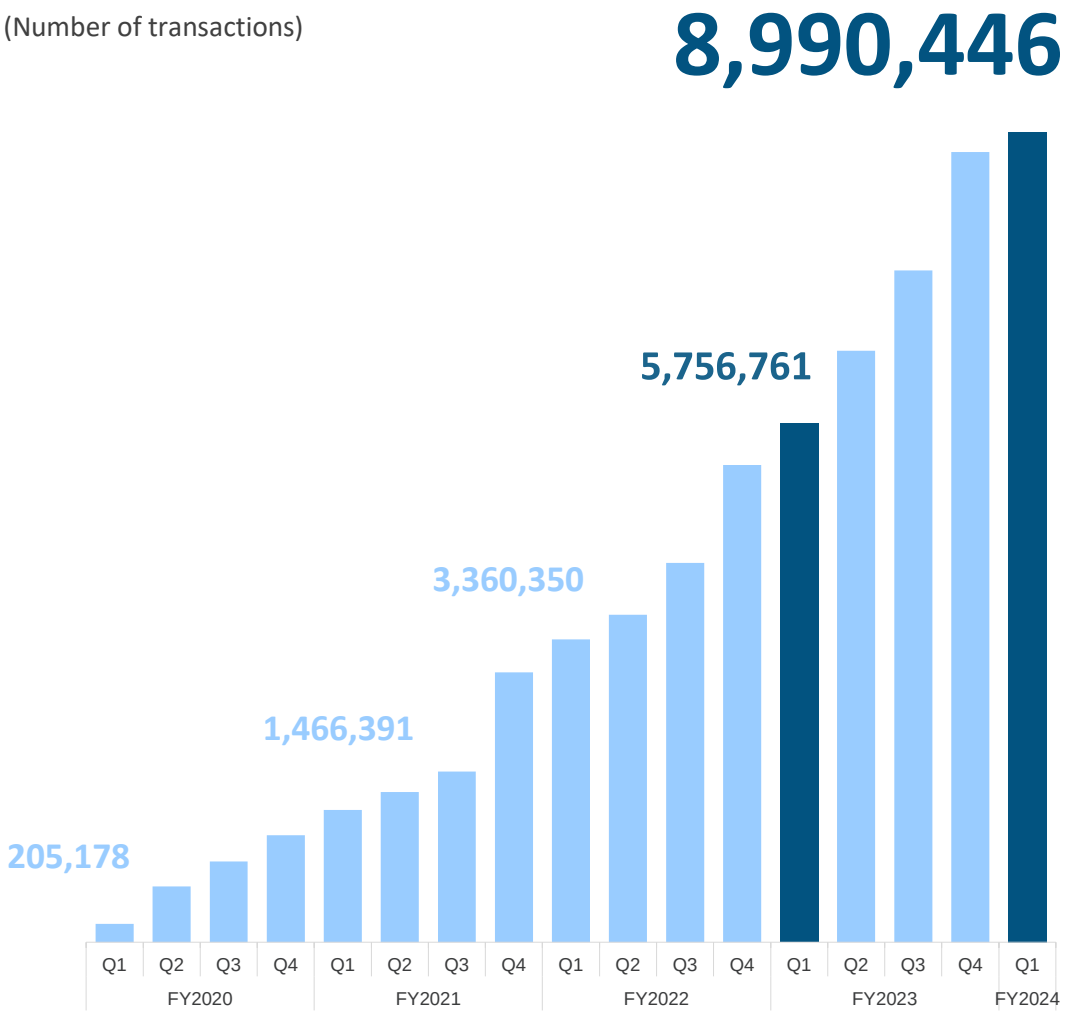
Recurring service sales ratio of 87.6% (+1.3pt YoY)

- High-growth-driver service iTrust grew 34.9% year on year as eKYC service for financial institutions and electronic contracts expanded
- In Device ID, cloud-based authentication services and remote access services for corporates grew
- 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
- Cybertrust's public root certification authority for server certificates obtained approval from Mozilla

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

Number of iTrust transactions (number of paid API use) grew

(Number of transactions)



Number of uses: 8.99 million per quarter

YoY change: 1.6 times

Trust service boasting outstanding performance

*Cybertrust Japan study as of the end of June 2024

Initiatives to Expand Scope of Use of iTrust (Identity Verification)

Trend towards stricter identity verification

The government will make identity verification, through reading of IC chip data, mandatory for in-person/over-the-counter mobile phone contracts under the Act on Prevention of Transfer of Criminal Proceeds and Act for Prevention of Improper Use of Mobile Phones*

Online/in-person identity verification

Online	Partner iTrust	In person
Centralize, in principle, to public certification service for individuals using Individual Number Card		**Reading IC chip in Individual Number Card, etc. made mandatory**

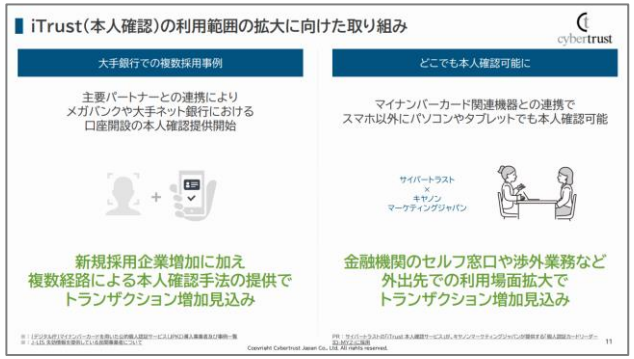
* Online has already been, in principle, centralized under Priority Policy Program for Realizing Digital Society

Transactions expected to rise due to head start in offering of online/in-person identity verification methods

* "Comprehensive Measures to Protect People from Frauds" by Ministerial Meeting Concerning Measures against Crime
* Digital Agency's "Summary of 'Comprehensive Measures to Protect People from Frauds' by Ministerial Meeting Concerning Measures against Crime"
* June 18, 2024, "Press conference of Digital Agency Minister Taro Kono"

Examples of identity verification carried out in person and at stores

In-person/over-the-counter identity verification carried out by reading IC chip data utilizing iTrust identity verification together with identity verification document reader



* (Reference) Excerpt from "FY2023 Q3 Financial Results" (p11) published on January 30, 2024

Transactions expected to rise from increased instances of in-person usage at telecom carrier counters

* Cybertrust's iTrust identity verification service is adopted for ID-MY2 Personal Authentication Card Reader provided by Canon Marketing Japan
* Cybertrust's blog "Reading of IC chip in identity certificates to be made mandatory for mobile phone contracts concluded in person"

- FY2024 Q1 Financial Summary
- **Overview by Service Segment**
  - Authentication and Security Services
  - **Linux/OSS Services**
  - IoT Services
- Management Topics
- FY2024 Full-Year Forecast
- Appendix

Linux/OSS Services | Performance and Initiatives by Service Segment

CentOS7 extended support accumulated order backlog beyond expectations

(Unit: Millions of yen)

Linux/OSS Services net sales (by transaction type)	FY23 Q1	FY24 Q1	YoY Change
Recurring services	236	224	(5.2%)
Licenses	59	82	+40.4%
Professional services	16	15	(7.4%)
Total net sales	312	322	+3.3%

Recurring services

- Order backlog for CentOS7 extended support steadily accumulated thanks to the success of strengthened sales promotion activities such as campaigns for the end of CentOS7 community support in June 2024
- Offered new AlmaLinux service menu, promoted ties with collaborative partners, and acquired support service contracts

CentOS7 Extended Support　Acquisition Status of New Projects

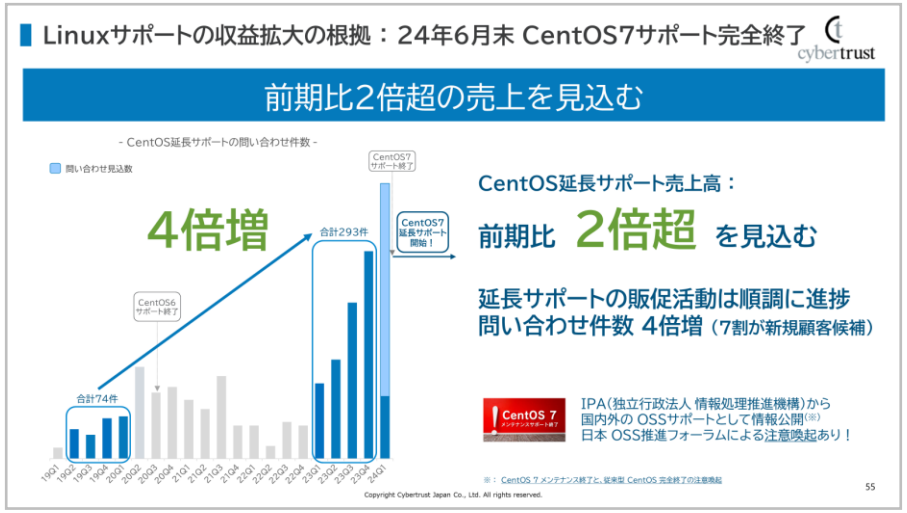
Order backlog for new CentOS7 extended support projects

In excess of 550 million yen

*As of June-end 2024

Order backlog steadily accumulated beyond expectations

Steady progress beyond initial expectations compared to the FY2024 net sales forecast



* (Reference) Excerpt from “FY2023 Financial Results” (p20) published on April 24, 2024

- FY2024 Q1 Financial Summary
- **Overview by Service Segment**
  - Authentication and Security Services
  - Linux/OSS Services
  - **IoT Services**
- Management Topics
- FY2024 Full-Year Forecast
- Appendix

IoT Services | Performance and Initiatives by Service Segment

Sales in contract development was stagnant despite growth in recurring services and security consulting

(Unit: Millions of yen)

IoT Services net sales (by transaction type)	FY23 Q1	FY24 Q1	YoY Change
Recurring services	21	47	+121.7%
Professional services	199	179	(9.9%)
Licenses	25	22	(13.3%)
Total net sales	246	249	+1.1%

Increase in sales of recurring services

- Recurring services expanded due to active development of products by existing customers and horizontal expansion into other products
  - (1) Full-scale development of industrial control devices, onboard devices, medical equipment, and other products
  - (2) Horizontal expansion into other products such as onboard devices and OA equipment

Professional services

- Security consulting projects for compliance with standards, laws, and regulations related to international safety standards continued to increase
- Acquisition of contract development projects was stagnant

Initiatives Aimed at Further Revenue Expansion of IoT Services (Progress in Q1)

Initiatives related to market environment

- Strengthening security solutions for social infrastructure companies from the perspective of economic security
  - Guidelines for government procurement/social infrastructure (NIST SP800-171)
  - Guidelines for factories (IEC62443)
  - Guidelines for medical devices (ISO 81001)
  - European CRA, etc.

Cybertrust's NIST SP800-171 compliance support solution
https://www.cybertrust.co.jp/solutions/sp800-171.html

- Provision of consulting service related to IoT Product Security Conformity Assessment Scheme of Ministry of Economy, Trade and Industry
  - Started offering vulnerability assessment service for embedded equipment that supports post-shipment vulnerability handling

Development of collaborative partners

- Overseas partner
  - Started discussions on joint development of social infrastructure security solutions, etc. with CHANGING Information Technology of Taiwan
  - Bringing together IoT Services of the two companies, with an eye on consumer products as well, and promoting domestic and overseas business expansion

- Enhancing capability to develop projects by promoting collaboration with partners having strengths in integration
  - Progress in joint proposals, from consultation to implementation, with information security divisions of major corporations
  - Joint proposal with IT solution providers for application layer and development of response structure
  - Strengthening of integration partner for sales expansion of EMLinux

- FY2024 Q1 Financial Summary
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
- **Management Topics**
- FY2024 Full-Year Forecast
- Appendix

Participation in Security Funds

Cybertrust has joined Nippon Cyber Security Fund 1 Investment Limited Partnership, Japan's first fund that is financed by as well as invests in security companies, as a limited partner (investing company)

NCSF
日本サイバーセキュリティファンド

cybertrust

Strengthening cooperation with security companies, which are the investors, to bring together services, develop sales channels, and carry out joint marketing to contribute to improvement of security at semi-large and second tier companies as well as SMEs

*Cybertrust is promoting strengthening the security of businesses by investing in the Nippon Cyber Security Fund 1 Investment Limited Partnership

- FY2024 Q1 Financial Summary
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
- Management Topics
- **FY2024 Full-Year Forecast**
- Appendix

FY2024 Full-Year Forecast

Double-digit growth in net sales and operating income

Side-by-side with growth investments, high-growth-driver service iTrust and Linux service will lead growth

Unit: Millions of yen	FY23	FY24	YoY change	
			Change	Rate of change
Net sales	6,466	**7,200**	+733	+11.3%
Operating income	1,112	**1,300**	+187	+16.9%
Operating margin (%)	17.2	**18.1**	-	-
Ordinary income	1,121	**1,300**	+178	+15.9%
Profit attributable to owners of parent	518	**860**	+341	+65.8%
EBITDA	1,716	**2,039**	+323	+18.8%

FY2024 Dividend Forecast

As of the beginning of FY2024, Cybertrust forecasts to continue paying a stable dividend
Forecast of **17.50 yen per share**

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
FY2023 results		17.50 yen
FY2024 forecast	0.00 yen	17.50 yen

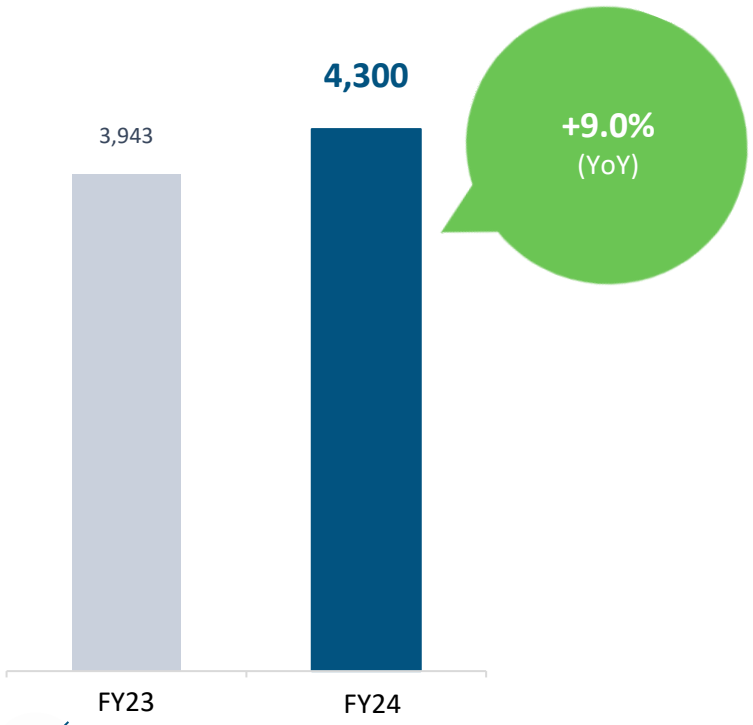
- FY2024 Q1 Financial Summary
- Overview by Service Segment
  - Authentication and Security Services
  - Linux/OSS Services
  - IoT Services
- Management Topics
- FY2024 Full-Year Forecast
- **Appendix**

Numeric data

2025 Full-Term Results Expected (sales by service)

Authentication and security

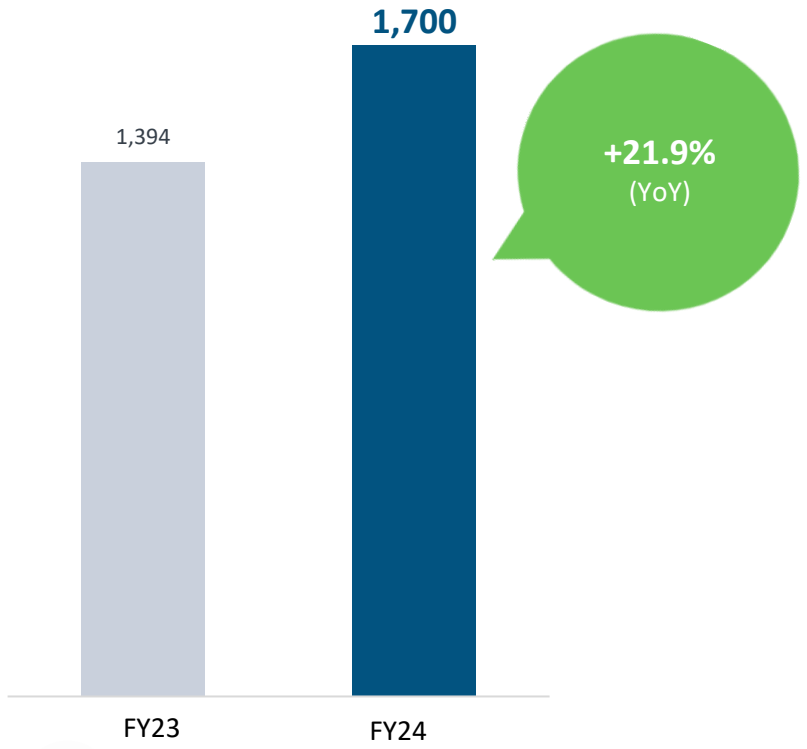
(Millions of yen)



By continuing to grow iTrust
Increase recurring revenue

Linux / OSS

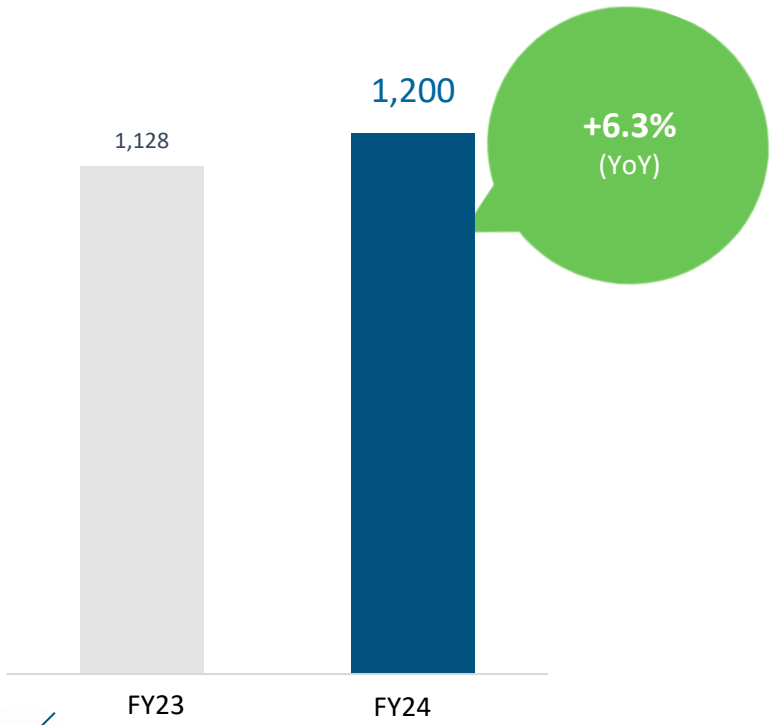
(Millions of yen)



CentOS extension support increased
Increase recurring revenue

IoT

(Millions of yen)



Due to an increase in demand for response to standards and laws and regulations related to economic security
As a high-growth driver service
Double-digit growth in recurring

Consolidated PL (Detailed Sales by Service)

(Millions of yen)

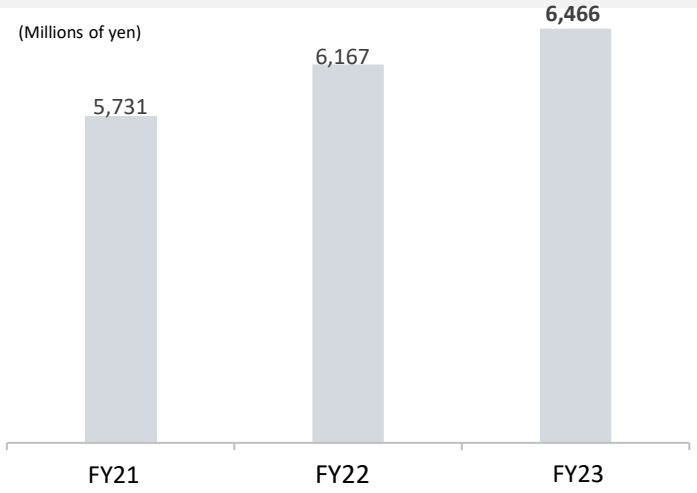
Consolidated Results	FY22	FY23	Change
The sales	6,167	6,466	+298
Authentication and security services	3,543	3,943	+399
LICENSE	155	158	+3
Professional services	448	598	+149
Recurring service	2,939	3,186	+247
Linux/OSS servicing	1,447	1,394	(52)
LICENSE	336	294	(42)
Professional services	124	157	+33
Recurring service	985	942	(43)
IoT servicing	1,176	1,128	(48)
LICENSE	115	111	(4)
Professional services	981	917	(64)
Recurring service	80	100	+19
Cost of sales	3,281	3,414	+132
Gross profit	2,886	3,052	+166
Selling, general and administrative expenses	1,832	1,940	+107
Operating income	1,053	1,112	+58

consolidated BS

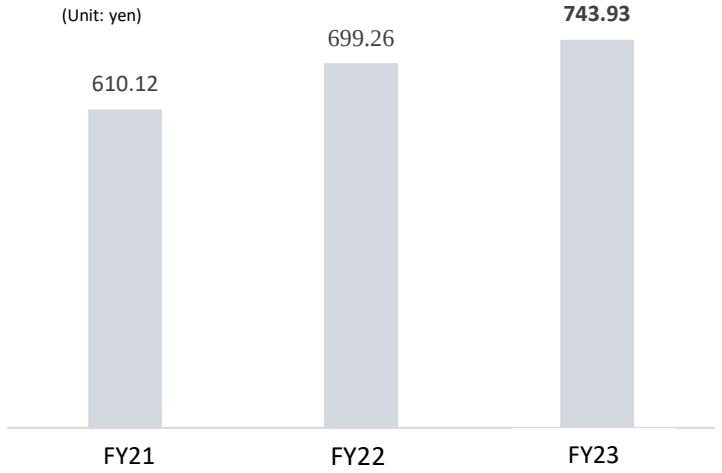
(Millions of yen)	End of March 2023	End of March 2024	Change	Rate of change
Current assets	5,401	6,181	+779	+14.4%
(Cash and deposits)	4,366	4,891	+525	+12.0%
(Notes, accounts receivable and contract assets)	878	1,068	+190	+21.7%
Fixed assets	2,465	2,235	△229	(9.3)%
(Software)	980	592	△387	(39.6)%
(Software in progress)	368	425	+56	+15.5%
Total assets	7,868	8,417	+548	+7.0%
Liabilities	2,243	2,384	+141	+6.3%
(Current liabilities)	1,705	1,841	+135	+7.9%
(Contract liabilities)	766	810	+44	+5.8%
Net assets	5,625	6,032	+407	+7.2%
(Shareholders' equity)	5,619	6,025	+405	+7.2%
(Stated capital)	806	820	+13	+1.7%
(Retained earnings)	2,773	3,151	+378	+13.6%
Total liabilities and net assets	7,868	8,417	+548	+7.0%

Major Consolidated Management Indicators

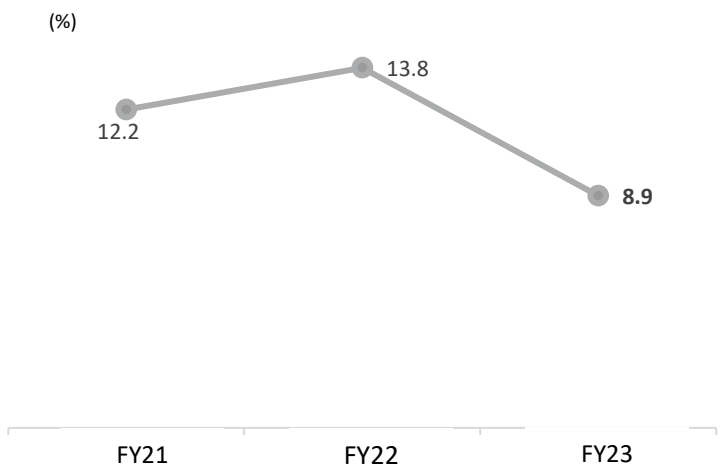
The sales



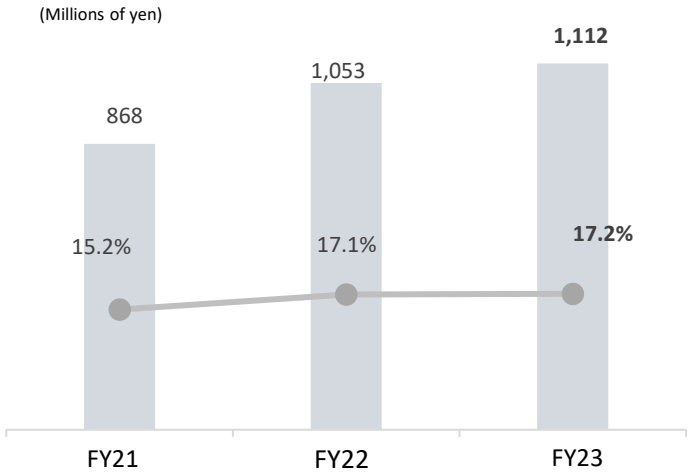
1Net assets per share (yen)BPS)



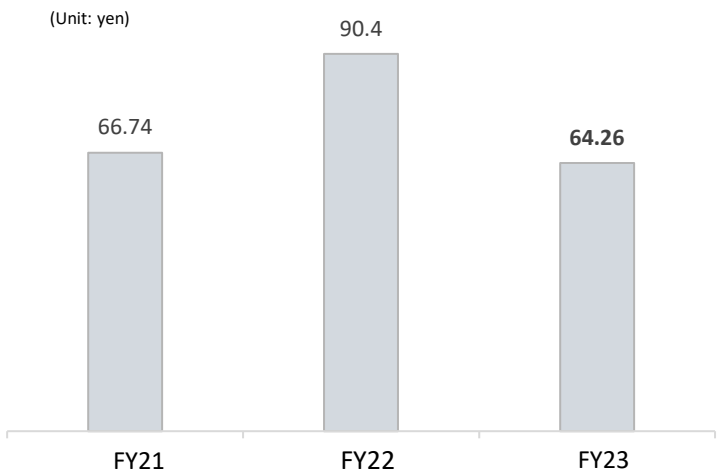
Return on equity (ROE)



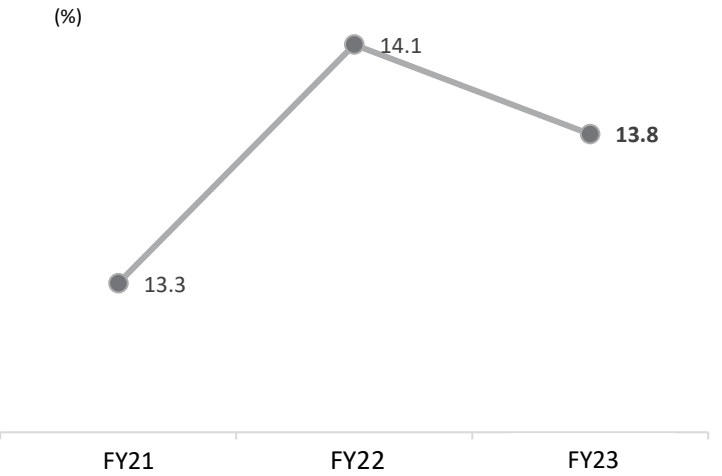
Operating income and operating income margin



1Net income per share (yen)EPS)



Return on assets (ROA)



※The Company conducted a 2-for-1 stock split on April 1, 2023. Per share amounts have been calculated assuming that the stock split was implemented at the beginning of FY21 period.

Corporate Profile

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.

About Us

Company Name	Cybertrust Japan Co., Ltd
Date of Establishment	June 1, 2000
Address	〒106-0032 Ark Hills Sengishiyama Mori Tower 35F, 1-9-10 Roppongi, Minato-ku, Tokyo
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	820,236,000 yen (as of March 31, 2024)
Major shareholders (as of March 31, 2024)	SB Technology Corp. OBIC BUSINESS CONSULTANTS CO.,LTD Daisuke gomi SECOM CO., LTD Dai Nippon Printing Co., Ltd. Hitachi, Ltd. NTT DATA Japan Corporation Custody Bank of Japan, Ltd.(Trust Account) THE BANK OF NEWYORK 133595 Norihiro Kuroda

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> Japan RA Co., Ltd. Other 1 company
Business Sites	Head Office (Roppongi 1-chome), Matsue Lab.

History

On October 1, 2017, we (former MIRACLE LINUX Corporation) as the surviving company completed an absorption-type merger with former Cybertrust Japan co., Ltd. and name change of and commenced operations as Cybertrust Japan co., Ltd.

Year and month	Summary
Jun. 2000	MIRACLE LINUX CORPORATION is established in Minato-ku, Tokyo, with capital of 220 million. Began providing services centered on the server OS business as a developer of domestically produced Linux for companies, with Oracle Corporation Japan and NEC Corporation as major shareholders
Oct. 2000	Released MIRACLE LINUX v1.0 products
Dec. 2007	With the purpose of developing Linux distributions for enterprises that meet the needs of the Asian region and strengthening Asianux branding, Established Asianux Conrporation jointly with Red Flag of China and Hancom of South Korean
Aug. 2008	Entered Zabbix business and began providing server monitoring services
Feb. 2009	Released Embedded MIRACLE and entered the embedded OS business
Jun. 2010	Start of shipments of digital signage products
Jul. 2014	SOFTBANK TECHNOLOGY CORPORATION (currently SB TECHNOLOGY CORPORATION) acquires our shares and becomes a consolidated subsidiary of SOFTBANK TECHNOLOGY CORPORATION
May, 2015	Relocated headquarters to Shinjuku, Tokyo
Oct. 2015	Opened Matsue Lab as a development and support base in Matsue City, Shimane Prefecture
Mar. 2017	SOFTBANK TECHNOLOGY CORP. (currently SB TECHNOLOGY CORP.) and the former Cybertrust Japan co., Ltd. jointly launched solutions that comprehensively support the ecosystem for developing IoT equipment.
Oct. 2017	Acquisition of former Cybertrust Japan co., Ltd. and change its name to Cybertrust Japan co., Ltd.
Aug. 2018	Head office moved to Minato-ku, Tokyo
Jul. 2019	With the purpose of forming a business alliance with Lineo Solutions Inc., which develops embedded LinuxOS, we acquired a portion of the shares of Lineo Holdings, Inc., Converted Lineo Holdings Inc. into a holding-method related company
Sep. 2019	Commenced business alliance with SECOM Trust Systems Co., Ltd. for server certificate business
Oct. 2019	Realizing a IoT development environment that enables continuous development and launching EM+PLS, a service that supports the long-term use of IoT products
May, 2020	With the purpose of strengthening its business alliance with Lineo Solutions Inc., which develops embedded LinuxOS, the Company acquired all of the shares of Lineo Holdings, Inc., Made Lineo Holdings Inc. and Lineo Solutions Inc. wholly owned subsidiaries
Apr. 2021	Shares are listed on the Tokyo Stock Exchange Mothers Market.
Feb. 2022	Completed liquidation of consolidated subsidiary Lineo Holdings Inc.
Apr. 2022	Transitioned to the Tokyo Stock Exchange Growth Market following a review of the Tokyo Stock Exchange's stock market classification

History

The history of the former Cybertrust Japan co., Ltd. since its establishment until its mergered is as follows

Year and month	Summary
Sep. 1995	NSJ Corporation established to develop software
May, 1999	Contracted as the sole Japanese distributor of Baltimore Technologies Plc ("Baltimore")
May, 2000	Company name changed to Baltimrore Technologies Japan Co.,Ltd.
Jun. 2000	Merged with Cybertrust Co., Ltd. (Kita-ku, Sapporo) (The company launched Japan's first commercial electronic certification office in May 1997.)
Dec. 2003	Betrusted Holdings,Inc. entered into a business alliance with ("Betrusted") (Due to the acquisition of Betrusted, a major U.S. security services company, from Baltimore. Subsequently, this business was acquired by Verizon Australia Pty Limited ("Verizon").
Jul. 2004	Company name changed to Betrusted Japan Co., Ltd.
Jul. 2005	SOFTBANK BB CORP. (currently SOFTBANK CORP.) acquired the shares of Betrusted Japan Co., Ltd. and became a consolidated subsidiary of SOFTBANK BB CORP.
Jan. 2007	Company name changed to Cybertrust Japan co., Ltd.
Apr. 2014	SOFTBANK TECHNOLOGY CORP. (currently SB TECHNOLOGY CORP.) acquired the shares of SOFTBANK BB CORP. (currently SOFTBANK CORP.)'s ownership Cybertrust Japan co., Ltd. and became a consolidated subsidiary of SOFTBANK TECHNOLOGY CORP.
Apr. 2015	Contracted as the company's sales agent following Verizon's transfer of SSL and other businesses to DigiCert, Inc.
Oct. 2017	Eliminated due to merger with MIRACLE LINUX CORPORATION

Sources: (Link) for the 23rd Quarter (2022/4/1-2023/3/31)

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**
- **Reduction 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.

Policies and indicatorsators and Targets

We have established KPI (evaluation indicators) for the following two of the four materiality items in the strategic plan.

Materiality	KPI (Valuation Indicators)
Achieving Corporate Growth by Creating Resilient Organizations	**Percentage of female employees in managerial positions: Achieved at least 8.2% (at least average for the information and communications industry)** Various career courses: Achieved at least two items from A to D in the comingt 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
Contribute to a sustainable society through resource and energy conservation	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 Reduction of printed materials: 50% reduction by 2030 compared to 2022

Policies and indicators concerning the development of human resources, including ensuring diversity of human resources, and the improvement of the internal environment, and trends in the performance of these indicators.

Policy guidelines		Year ended March 31, 2022	Year ended March 31, 2023	Year ended March 31, 2024
Recruiting Activities to Secure Human Resources and Create Continued Jobs	Number of Employees: Total (People)	222	230	233
	Number of employees: Male (persons)	172	177	181
	Number of employees: Female (people)	50	53	52
	Percentage of Female Employees (%)	22.5	23.0	22.3
Percentage of female employees in managerial positions 8.2% or more	**Ratio (%)**	**9.1**	**10.5**	**10.3**
At least 10% of male workers take childcare leave	Ratio (%)	15.0	28.6	50.0
Percentage of Female Employees in Full-time Employment	Ratio (%)	-	11.8	0
Average length of continuous employment of woman full-time employees	Years (years)	-	9.4	10.4
Engagement Assessment and ES Survey Core Year-on-Year or higher (Note)	Number of points	3.83	3.83(64)	68

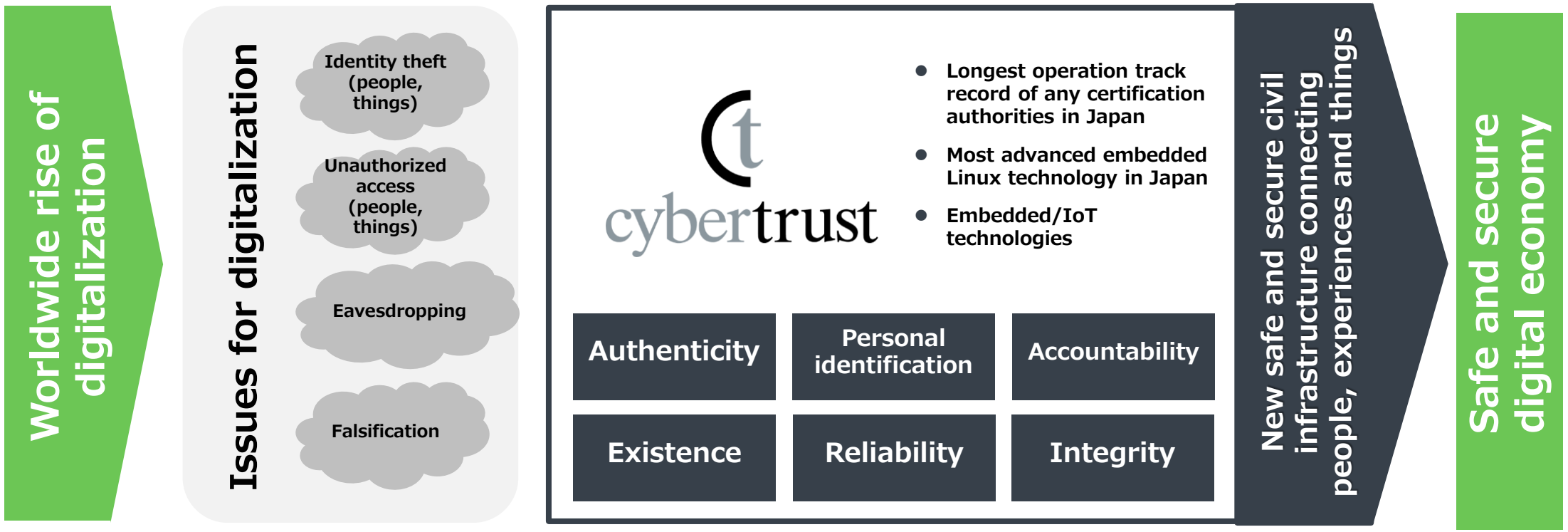
(NOTE)The aggregation format of scores has changed since the year ended March 31, 2024. Scores for the year ended March 31, 2023 using the same calculation method are shown in parentheses, and have improved for the year ended March 31, 2024.

Sources: Annual Securities Report (Link) for the 24th period (2023/4/1-2024/3/31)

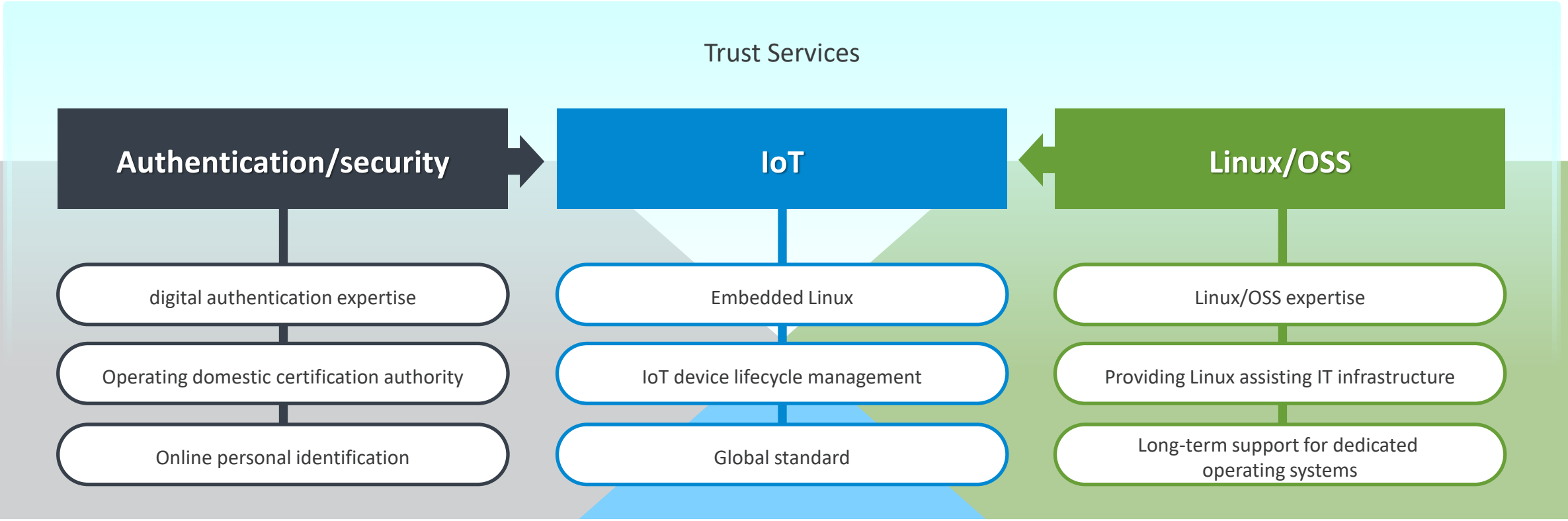
Business Overview

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**
  - 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
- **digital Identity verification and digital signature**
  - **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.

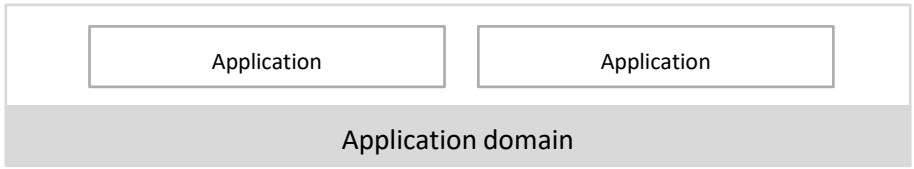
Guaranteed by certificate authorities*

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

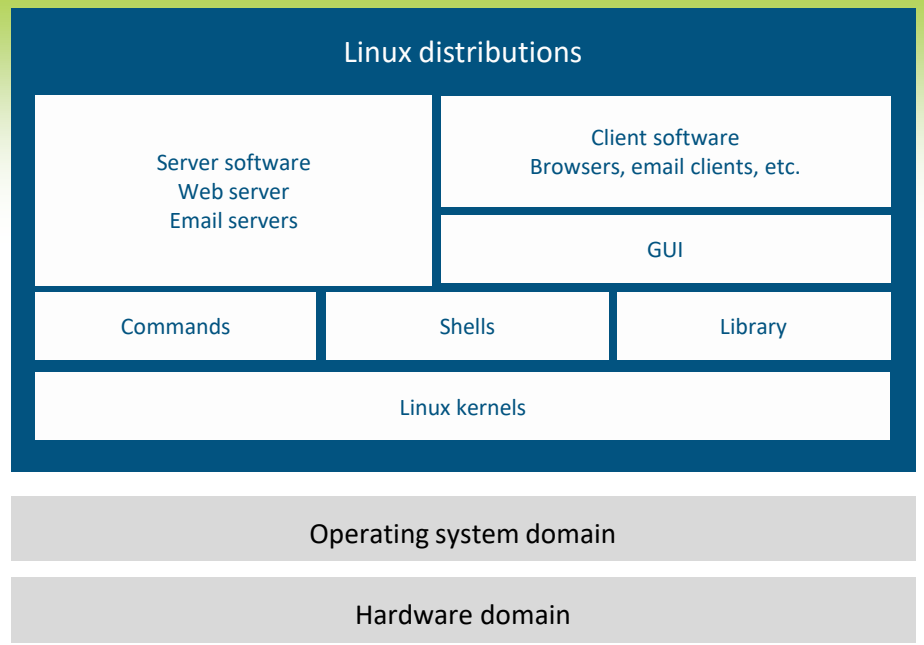
Overview of Linux / OSS Services

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.)

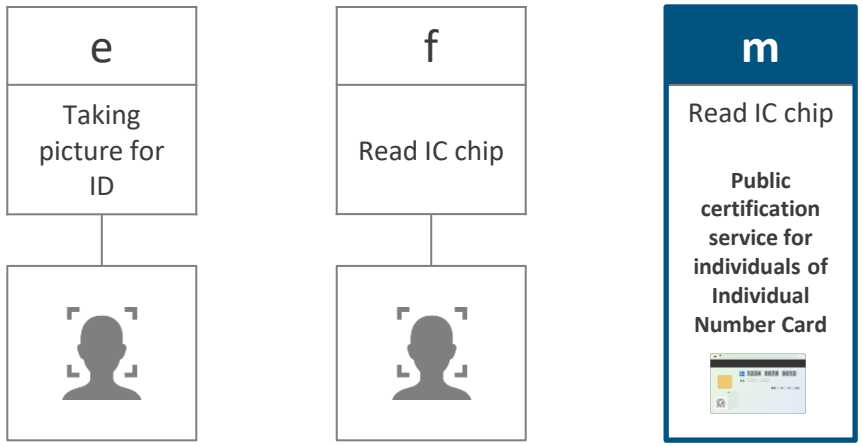
Basis for Revenue Expansion of iTrust: Linked to/Promotion of National Policy

2024/4/24
FY2023 Financial Results
Reprinted

Identity verification

In the Priority Policy Program for Realizing Digital Society*, **identity verification will, in principle, be centralized through public certification service for individuals of Individual Number Card**

Main identity verification methods (Identity verification becoming stricter-->)



Partners

iTrust

Identity verification
Digital signature

April 2024

Number of Individual Number Cards issued
99,870,000 cards

78.8% of the population

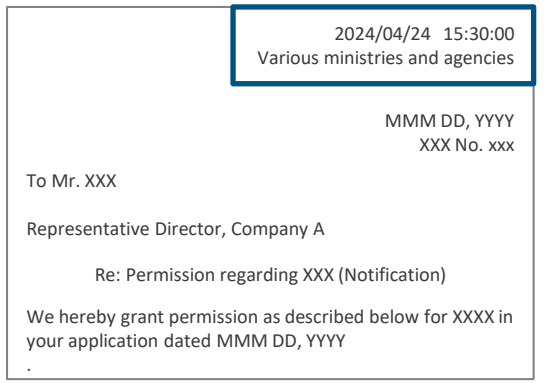
Transactions will rise with increased use of Individual Number Card (public certification service for individuals) for identity verification

*: Digital Agency's "Priority Policy Program for Realizing Digital Society (P54) Cabinet decision on June 9, 2023
*: Regulation for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (Article 6, wa)
*: Ministry of Internal Affairs and Communications "Status of Individual Number Cards issuance" as of April 2024

Digital signature

In line with the basic concepts regarding digitalization of disposition notices, etc.*, **respective ministries and agencies are aiming to digitalize all applications by 2025**

Digital signature of various ministries and agencies


2024/04/24 15:30:00
Various ministries and agencies

MMM DD, YYYY
XXX No. xxx

To Mr. XXX

Representative Director, Company A

Re: Permission regarding XXX (Notification)

We hereby grant permission as described below for XXXX in your application dated MMM DD, YYYY
.

Transactions will rise with increased use of digital signatures for notifications of permits and approvals by administrative agencies

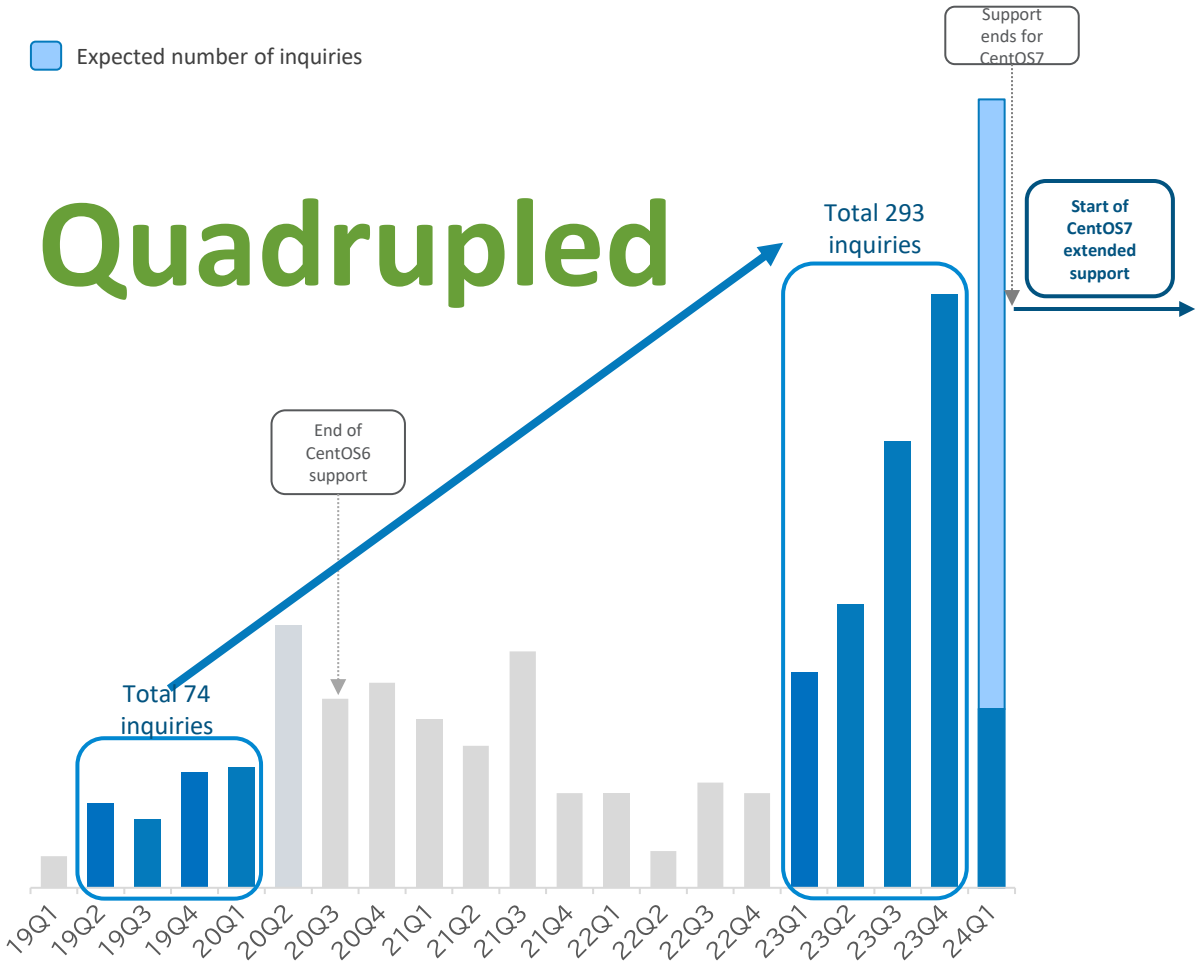
*: Digital Agency "Basic concepts regarding digitalization of disposition notices, etc."

Basis for Revenue Expansion of Linux Support: CentOS 7 Support to End at the End of June 2024

2024/4/24
FY2023 Financial Results
Reprinted

Sales expected to more than double YoY

- Number of inquiries regarding CentOS extended support -



Sales of CentOS extended support:

Expected to more than double YoY

Sales promotion activities for extended support making steady progress

Number of inquiries quadrupled (70% new customer candidates)

Information disclosed by Information-technology Promotion Agency, Japan (IPA) as OSS support both in Japan and overseas*
Japan OSS Promotion Forum has issued a warning!

*: Warning regarding end of CentOS7 maintenance and complete termination of conventional CentOS

Initiatives Aimed at Further Revenue Expansion of Linux Support

2024/4/24
FY2023 Financial Results
Reprinted

Promotion of AlmaLinux development and supply system

AlmaLinux

International standard OS AlmaLinux, widely viewed as leading successor OS for CentOS

Contribution to stable, long-term supply

- Contribution to community activities such as development
- Persons in charge of OSS technology become board members and get involved in development policy, etc.

Activities aimed at spreading

- Holding domestic events, etc. in collaboration with the community and CloudLinux

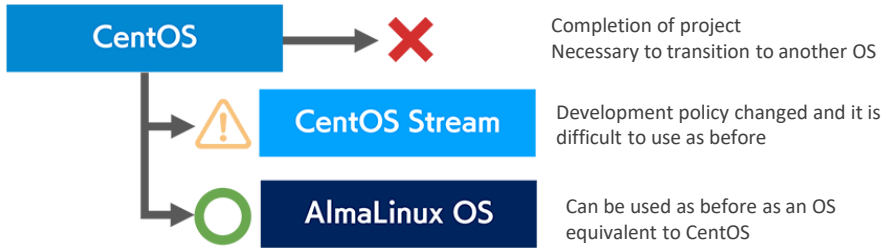
Sales activities in collaboration with major companies

Offer high value-added paid service primarily to financial and manufacturing companies in collaboration with major server companies

High quality, long-term support	Reduction of system maintenance cost	Compliant with international safety standards
Provision of upgrade programs for a maximum 16-year period	LivePatch service with zero downtime	Provision of FIPS 140-3-compliant patches

Provision of one-stop service in Japan

Promotion of transition to AlmaLinux from CentOS aimed at companies offering hosting and online services



*: LivePatch: Non-disruptive update service for system failure, etc.
*: FIPS 140-3: Security encryption-related U.S. government certification standards

Expects revenue expansion from requirements for compliance with standards and laws and regulations related to economic security

International trends in promotion of economic security

Establishment of standards and laws and regulations related to economic security

- SP800-171, FIPS 140-3, Security alliance system (US)
- IEC62443 (International standard)
- Cyber Resilience Act (Europe)

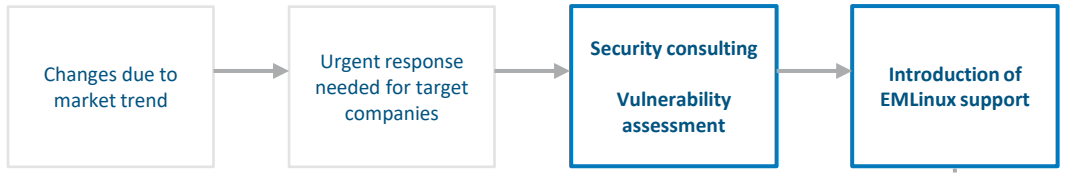
More specific response schedule with consensus among heads of states of various countries

Promulgation of the Economic Security Promotion Act

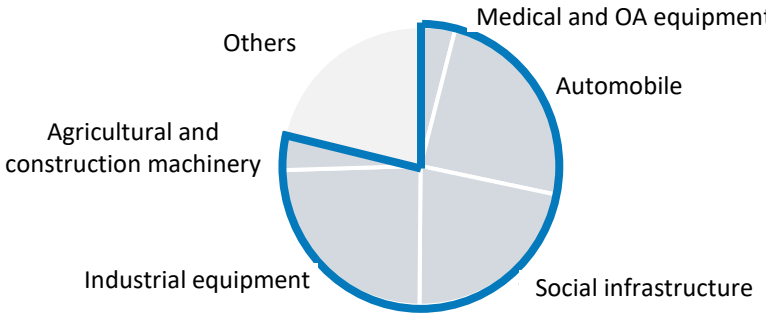
- Legalized compliance across the entire supply chain for government and defense procurement
- Strengthened standards and laws and regulations for companies in 14 critical infrastructure business fields
- IoT Product Security Conformity Assessment Scheme
- Urgent need to comply with standards, laws and regulations, and SBOM on export products of various countries

Initiatives aimed at revenue expansion of the Cybertrust's services

- Expected number of potential customers exceeding the initial figure for the previous year, of which 80% are companies requiring compliance with standards and laws and regulations
- The seminar on compliance with standards and laws and regulations held in Q4 of FY2023 attracted more than 10 times the participants, and inquiries tripled
- Double-digit growth in recurring services from active promotion jointly with partners of consultation and EMLinux support introduction



Increase in inquiries from companies requiring compliance with standards and laws and regulations



<Industry attributes of Cybertrust's IoT-related customers>

Initiatives Aimed at Further Revenue Expansion of IoT Services

2024/4/24
FY2023 Financial Results
Reprinted

Development of collaborative partners

Enhancing capability to handle projects by promoting collaboration with partners having strengths in large-scale development projects

- Building a structure to handle large-scale development projects with major system integrators
- Building a structure to provide security solutions to social infrastructure, industrial equipment, and automobile fields with major security service companies

Overseas partner (Taiwanese ODM-related security company)

- Promotion of overseas expansion through SIOTP and partner product collaboration

Expansion of distribution channels

- Strengthening collaboration with trading companies dealing with semiconductors with high customer demand and boost sales promotion measures such as industry-specific joint seminars

Initiatives related to market environment

Strengthening security solutions for social infrastructure companies from the perspective of economic security

- Guidelines for government procurement/social infrastructure (NIST SP800-171)
- Guidelines for factories (IEC62443)
- Guidelines for medical devices (ISO 81001), etc.

Cybertrust's NIST SP800-171 compliance support solution
https://www.cybertrust.co.jp/solutions/sp800-171.html

Provision of consulting service related to IoT Product Security Conformity Assessment Scheme of Ministry of Economy, Trade and Industry

- Developing potential customers for security consulting, EMLinux, and SIOTP by improving Cybertrust's visibility and highlighting its technical capability

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 Japan 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 (FY24 Q1~)

04.03

Cybertrust Device ID, a terminal authentication service, is linked to Canon IT Solutions's cloud-based integrated ID management service

04.09

Cybertrust's iTrust Remote Signing Service enhances functions and supports XAdES

04.23

Cybertrust iTrust Identity Confirmation Service adopted by Individual Number management one-stop service “Mynaone”

04.24

A high-performance Contec FA computer is equipped with Cybertrust Japan's clustering software, and is adopted as a log server for social infrastructure systems.

05.21

Through technological collaboration between Simplex and Cybertrust Japan, we have realized strict identity verification for on-line completion using the Individual Number Card in DMM FX.

05.30

Collaboration between Cybertrust iTrust identity verification service and Pokepay realization by Pocket Change to achieve strict identity verification

07.03

Launched Zabbix based system monitoring software update "MIRACLE ZBX 7.0" and 10-year long-term support

07.10

Cybertrust Japan began offering a vulnerability research service for embedded devices to support post-shipment vulnerability responses

07.23

Cybertrust Japan leverages AlmaLinux's SBOM to strengthen measures against cyber-attacks

07.26

SureServer

Public Root Certification Authority for Cybertrust Japan's server certificate obtains Mozilla approval

07.29

Cybertrust Japan invested in Japan Cybersecurity Fund No. 1 Investment Limited Partnership to strengthen security of the business
~Contribute to accelerating growth of the security industry as a whole by promoting mutual cooperation with security companies

※：Cyberthrust Press Release (Link)

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