Fiscal Year Ended March 2015 Results Briefing

FFRI, Inc. (TSE Mothers: 3692)

http://www.ffri.jp/

COMPANY OUTLINE

Company Outline

Company name:	FFRI, Inc.	
Address:	4F TOKYU LAND CORPORATION EBISU Bld., 1-18-18 Ebisu, Shibuya-ku, Tokyo	
Directors:	Chief Executive Officer	Yuji Ukai
	Chief Technology Officer	Ryoji Kanai
	Chief Financial Officer	Shigeki Tanaka
	Board Director (outside)	Ikuo Takahashi
	Auditor (outside)	Shoji Kondo
	Auditor (outside)	Kazutaka Shimohigoshi
	Auditor (outside)	Yoshitaka Sugiyama
Established:	July 3, 2007	
Capital:	¥252,463,300 (as of March 31, 2015)	

Business:

1. Computer security research, consulting
2. Network system research, consulting, provision of information, education
3. Planning, development, sales, leasing, maintenance, management, and administration of computer software and computer programs, and acquisition, transfer, lending, and management of related property rights such as copyrights, publishing rights, patent rights, utility model rights, trademark rights, and design rights
4. All work related to the above business

Significance of Company Name and Corporate Logo

- "FFRI" is an abbreviation for "**F**ourteen**f**orty **R**esearch **I**nstitute".
- "1440" refers to a jump in snowboard half-pipe competitions that includes four full 360 degree rotations.
- When this company was established, no one had successfully completed a four-rotation jump. Therefore, we named the company "1440 (360° × 4)" to symbolize our will to face challenges in unexplored areas.

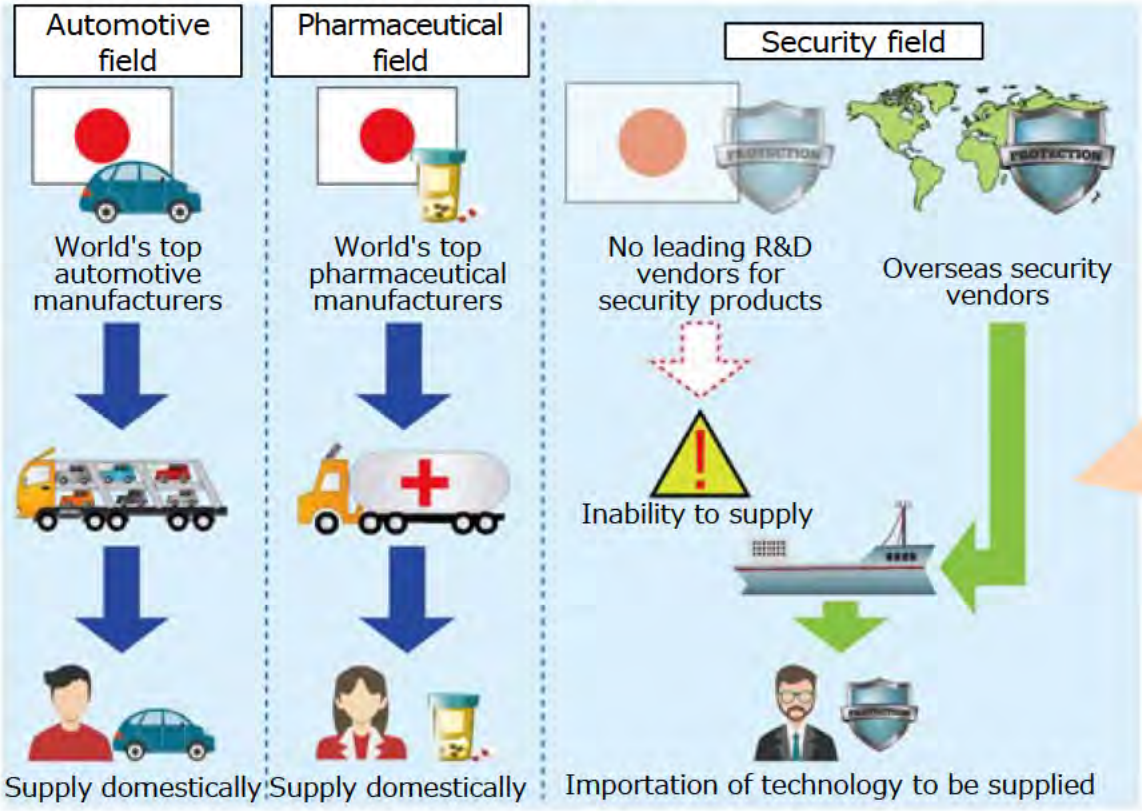
Fourteenforty Research Institute

FFRI

Our corporate logo features the number "1440" enclosed within an arrow that symbolizes the rotation of a snowboard, indicating our unwaning will to "face challenges in unexplored areas".

Corporate logo

Provision of Security Products in Japan, and Establishment of FFRI



In the field of cybersecurity, there are no R&D companies in Japan, resulting in reliance on overseas companies.

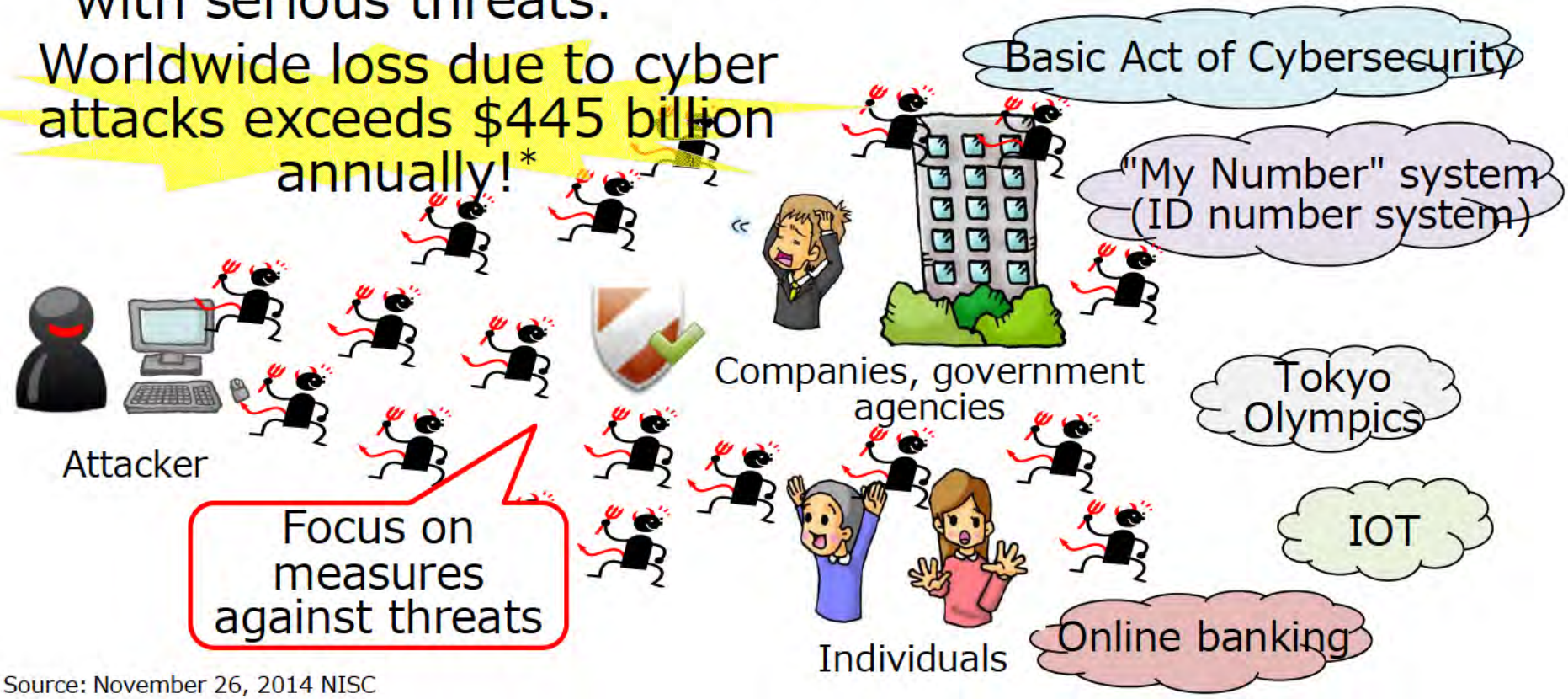
- Risk of problems that cannot be resolved in Japan
- Risk to national defense

WORK ENVIRONMENT

Environment Surrounding Cybersecurity

While society is made more convenient through technological innovation, users are forced to deal with serious threats.

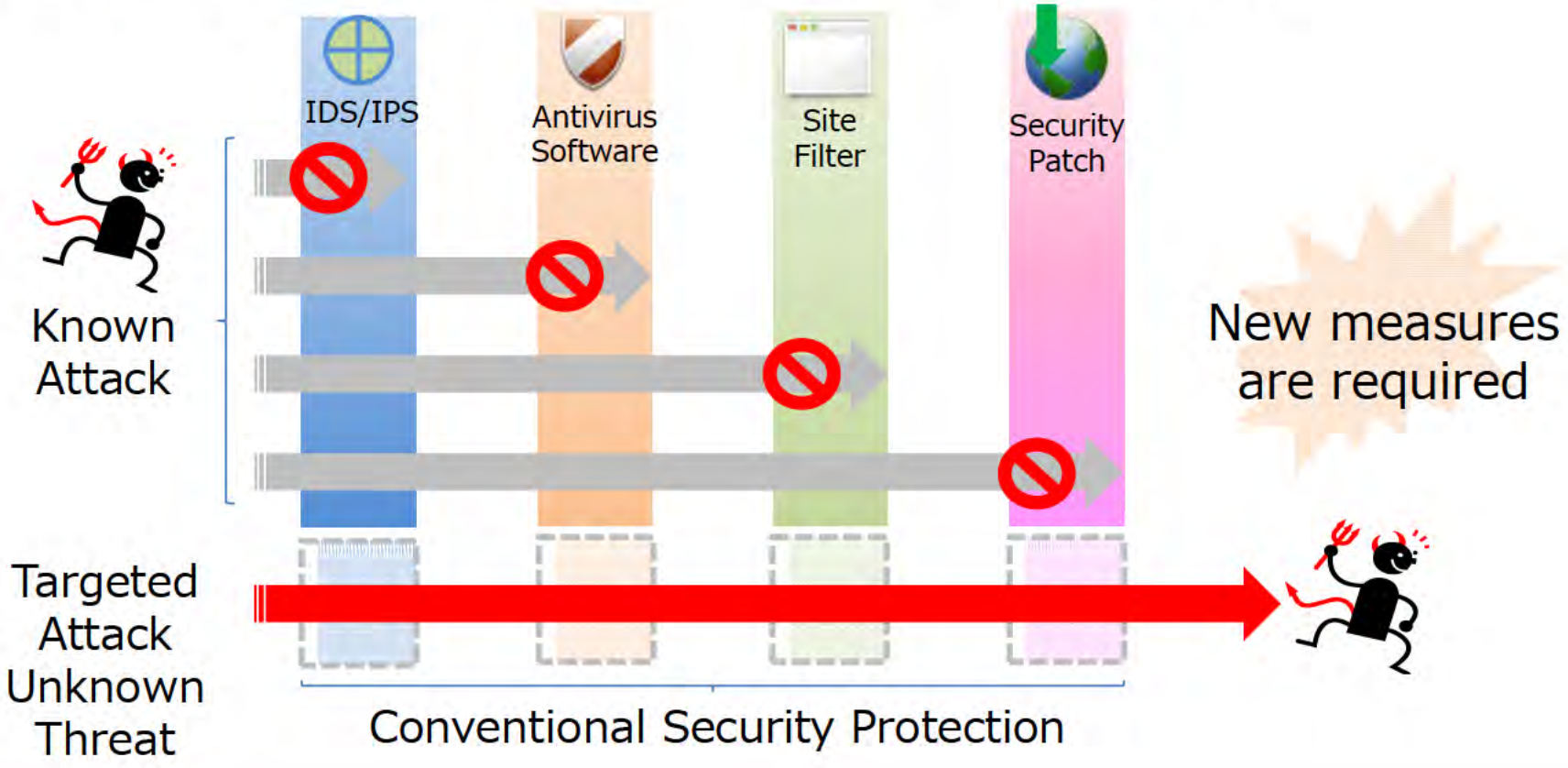
Worldwide loss due to cyber attacks exceeds $445 billion annually!*



* Source: November 26, 2014 NISC
"Current and Future State of Cybersecurity Policies in Japan"
The dollar value is an estimate. In reality, most loss is difficult to quantify, and often is not readily apparent.

FFRI

All conventional security protection together cannot provide full protection against targeted attacks and unknown threats.



Market Size Summary

Market Size

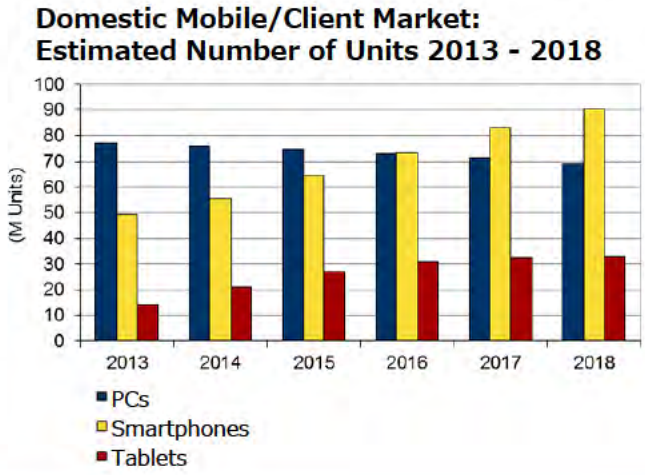
Domestic antivirus software market (2014 estimate) *1

Corporate use	Personal use
¥60.556 billion	¥60.727 billion

Potential Market Size

Estimated total number of domestic smartphones, tablets, and PCs *2

Approx. 153 million units (2014)

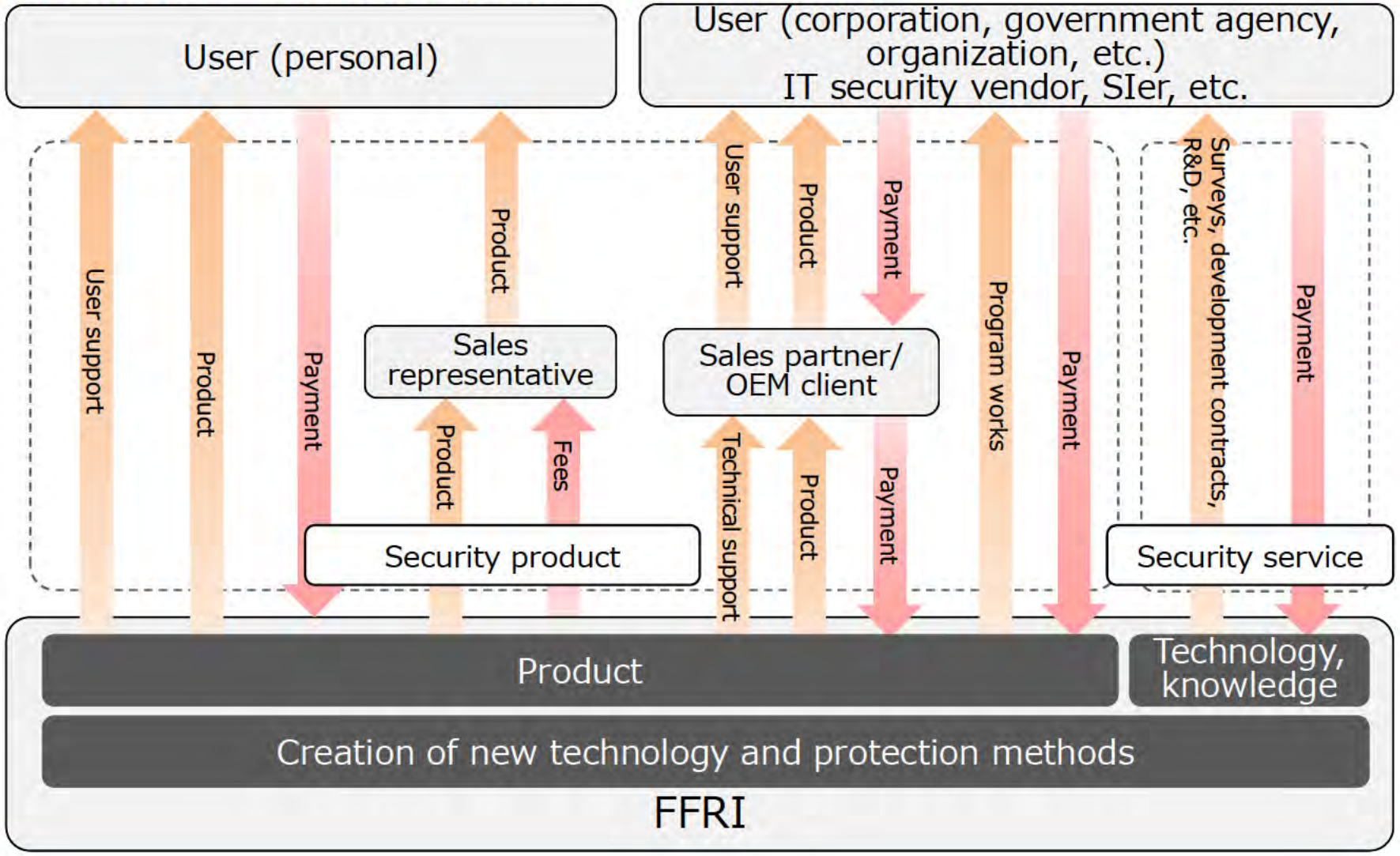


Source: *1 Information Security Market Survey FY2013 V1.0
NPO Japan Network Security Association

*2 IDC Japan Press Release
"Announcement of the analysis results for mobile and client computing market in Japan" (October 8, 2014)

BUSINESS DETAILS AND STRENGTHS

Business Model (as of March 31, 2015)



Main Product: FFR yarai

FFR yarai does not depend on pattern files but rather protects against malware and vulnerability attacks to protect valuable information assets from known and unknown threats.

Developed in Japan, it provides next-generation security to counter unknown threats by using progressive heuristic technology specialized for targeted attacks.

Main Security Products

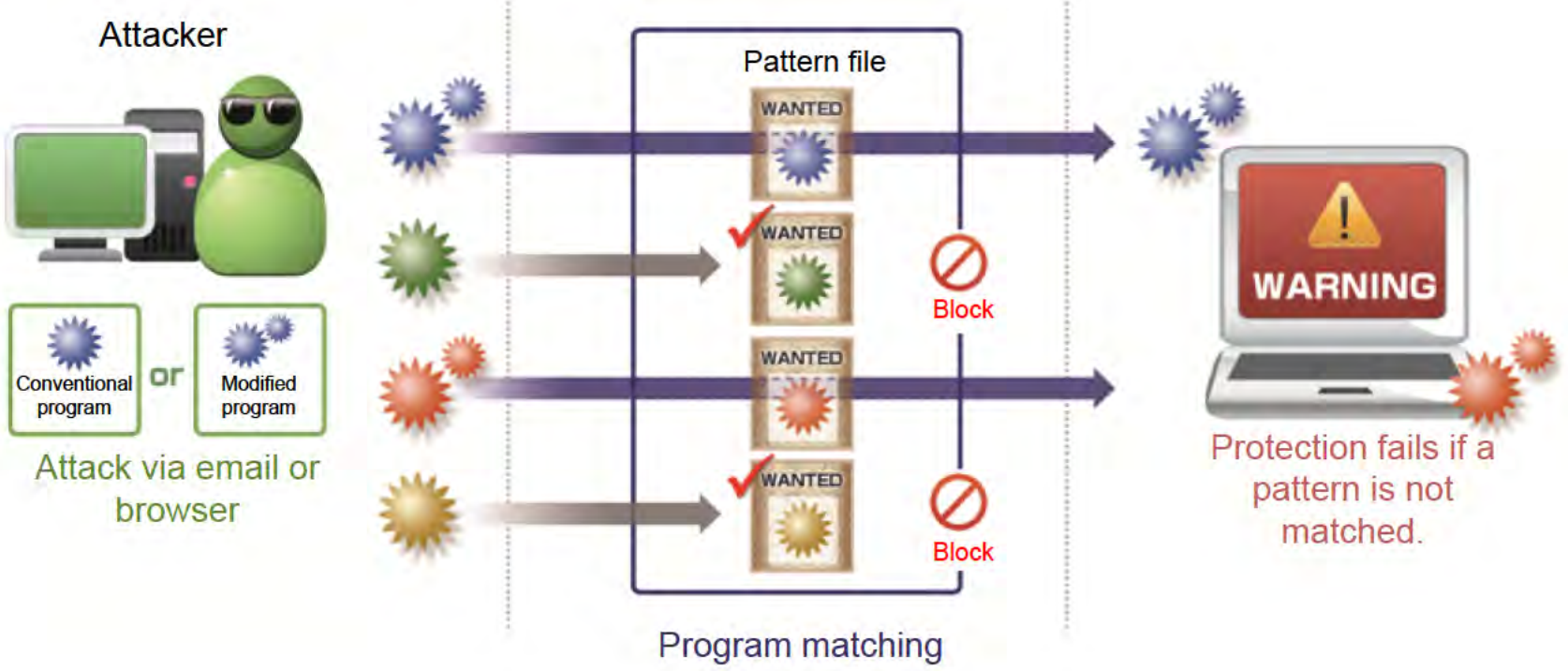
Corporate/ Personal	Name	Details
Corporate use	FFR yarai	Uses completely heuristic detection technology that does not depend on pattern files, to guard against both known and unknown malware and attacks that target vulnerabilities in security.
Corporate use	FFR yarai analyzer	Automatically analyzes programs, document files, and data files, and outputs reports that allow you to determine the risk of malware contamination and perform initial malware analysis in-house.
Personal use	FFRI proactive security	Security software based on FFR yarai, but tuned for personal use. Effective against unknown threats that can be difficult to handle with general antivirus software that depends on pattern matching technology.
Personal use	FFRI安心アプリチェッカー	Security application used to easily diagnose the risk from applications running on Android smartphones and tablets.

Security Services

Name	Details
Security investigation, analysis, research, etc.	Service that responds to users' needs, such as investigations of security robustness in computer systems and the effects caused by an actual cyber attack
Development contracts	Incorporation of unique cybersecurity measures to develop hardware and software that enhances the security of network systems operated by our clients
Inspection against targeted attack malware	Visualization of the risk of the leakage of confidential information, to provide support (and possible measures) for appropriate risk management against targeted attacks
Android device security analysis	Analysis of security threats on Android devices by analyzing various security risks and providing recommendations regarding possible measures
Prime Analysis	Comprehensive research service that provides support for resolving organizations' issues such as 0-day vulnerabilities and targeted attacks
FFRI ExpertSeminar	Technological training course for security engineers

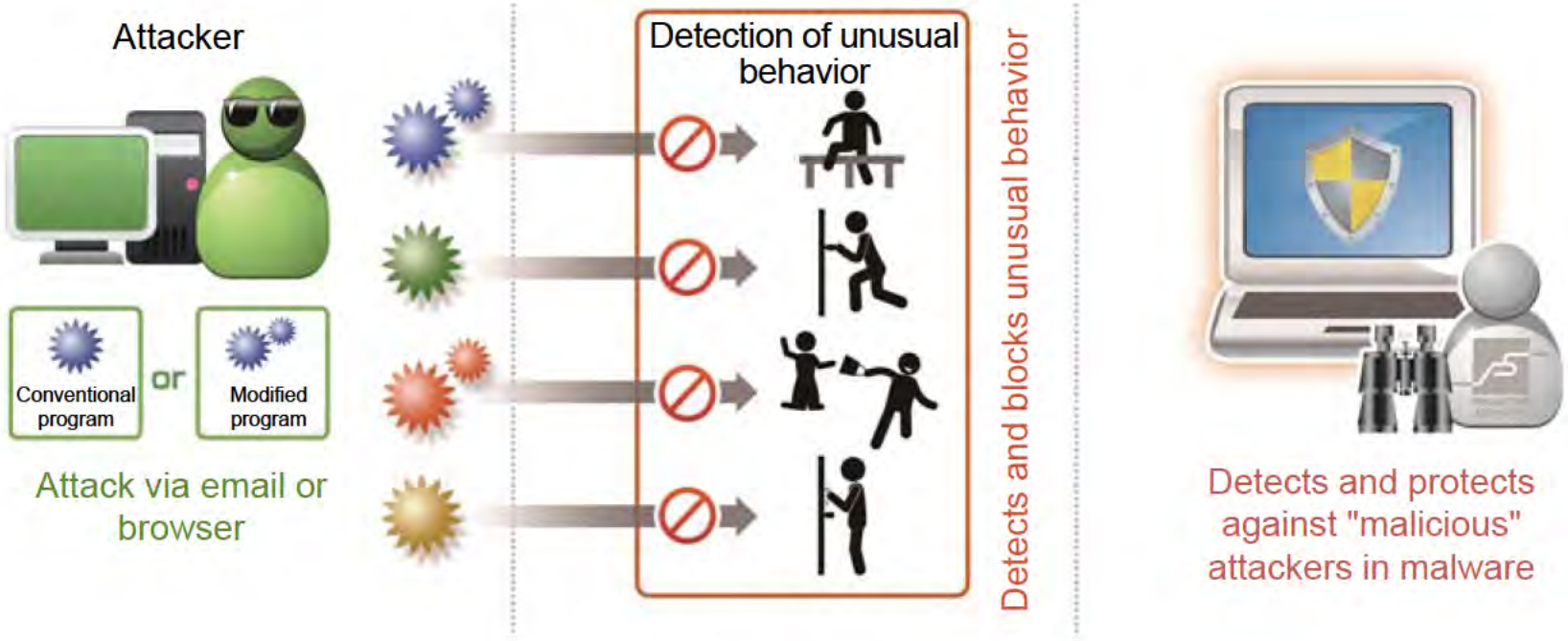
Technological Advantages of FFRI

- Pattern matching (conventional technology) protection method



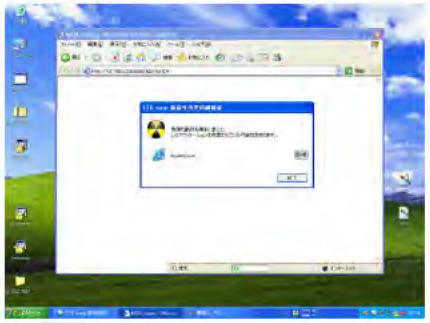
Technological Advantages of FFRI

- Heuristic (technology used by FFRI) protection method



Examples of Protection against Targeted Attack

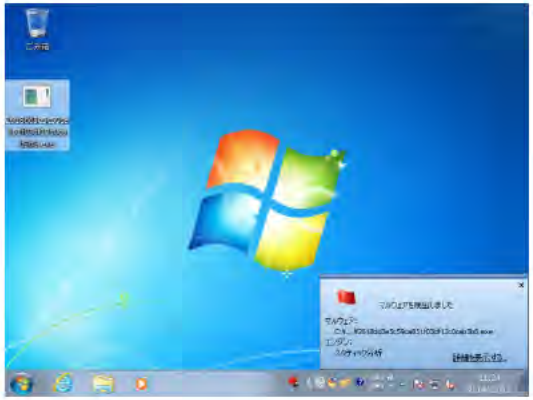
Yarai vs Targeted attack against national defense industry



A malware infection believed to be a targeted attack against a Japanese defense industry manufacturer occurred in September 2011.
As a result of the test on the malware sample suspected to be used for this incident, we confirmed that "FFR yarai" can detect the malware and successfully protect the system.

Yarai vs FBI warns of "destructive malware"

The US Federal Bureau of Investigation (FBI) warned companies in the United States of a malware attack that would destroy company computers. All data on infected systems would be completely wiped out.
As a result of the test on the malware sample suspected to be used for this incident, we confirmed that "FFR yarai" can detect the malware and successfully protect the system.



Points Regarding FFR yarai/FFRI proactive security

- Protection against unknown threats, including targeted attacks
- High-precision protection against threats through the use of measures against vulnerability attacks, as well as the implementation of progressive heuristic technology that utilizes five detection engines for both static and dynamic analysis
- Fully heuristic technology: lightweight operation with no need to update pattern files
- Complete software package that operates normally in a variety of environments
- Installed and operating successfully in many systems at major corporations and central government agencies

PERFORMANCE

Performance Highlights

Sales of FFR yarai are strong.

- Security measures actively implemented in corporations and government agencies ahead of the enforcement of the Basic Act of Cybersecurity and the start of the "My Number" system (ID number system)

Security services increased 10.5% compared to the same period last year.

- Year-on-year increase in security services due to the completion of several medium-sized projects through security investigation, research, and development contracts

Listed on Tokyo Stock Exchange Mothers.

- Improvement of name recognition outside the security industry

Expanding business to the consumer market.

- Release of “FFRI安心アプリチェッカー" for Android mobile devices in December 2014
- Gradually selling this application at T-Gaia locations throughout Japan
- Release of FFRI proactive security in April 2015

Research and Development

- Research results applied to products, and announced at international conferences such as Black Hat and CODE BLUE

Performance Summary

(Units: million yen)

Classification	March 2014	March 2015	Year-on-year (%)	Remarks
Sales	660	876	32.8	- Strong sales of FFR yarai - 10.5% year-on-year increase in security services
Operating income (Profit rate: %)	171 (26.0)	256 (29.2)	49.0	- Increased profit rate due to increase in security products
Ordinary income (Profit rate: %)	172 (26.1)	241 (27.6)	40.5	
Net income for the year (Profit rate: %)	115 (17.6)	171 (19.6)	47.9	

Performance Summary (Sales Breakdown)

(Units: million yen)

Classification		March 2014	March 2015	Year-on-year (%)
Security products	Continued sales	136	263	92.7
	New sales	227	341	50.2
	Subtotal	363	604	66.1
Security services		246	272	10.5
Other		50	-	-
Total		660	876	32.8

Note: Continued sales
Our main products are based on a 1-year subscription contract. Sales from existing contracts and the renewal of existing contracts are managed as continued sales.

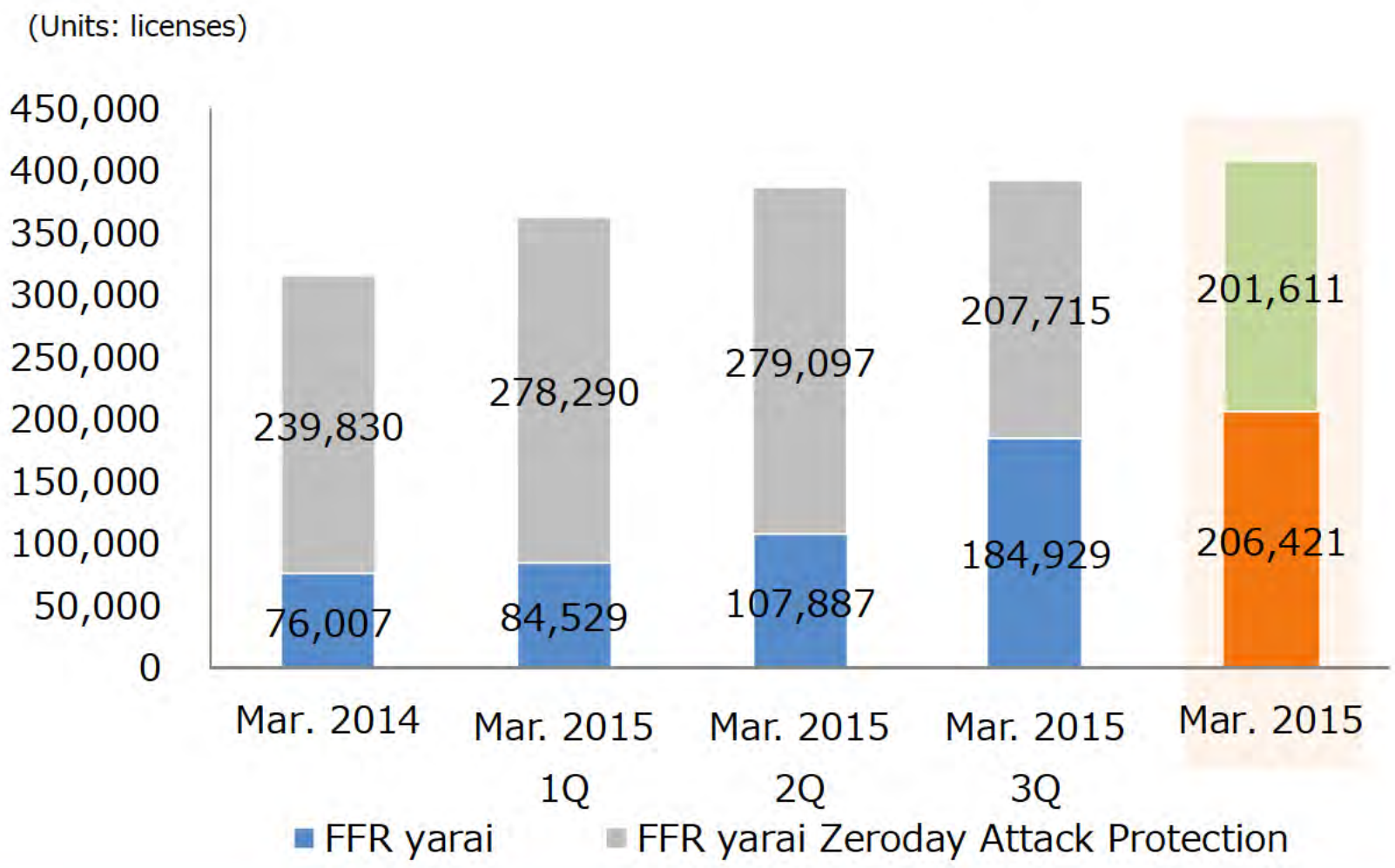
Trend in Contract Licenses

Sales of FFR yarai with a high unit price increased in the fiscal year ended March 2015

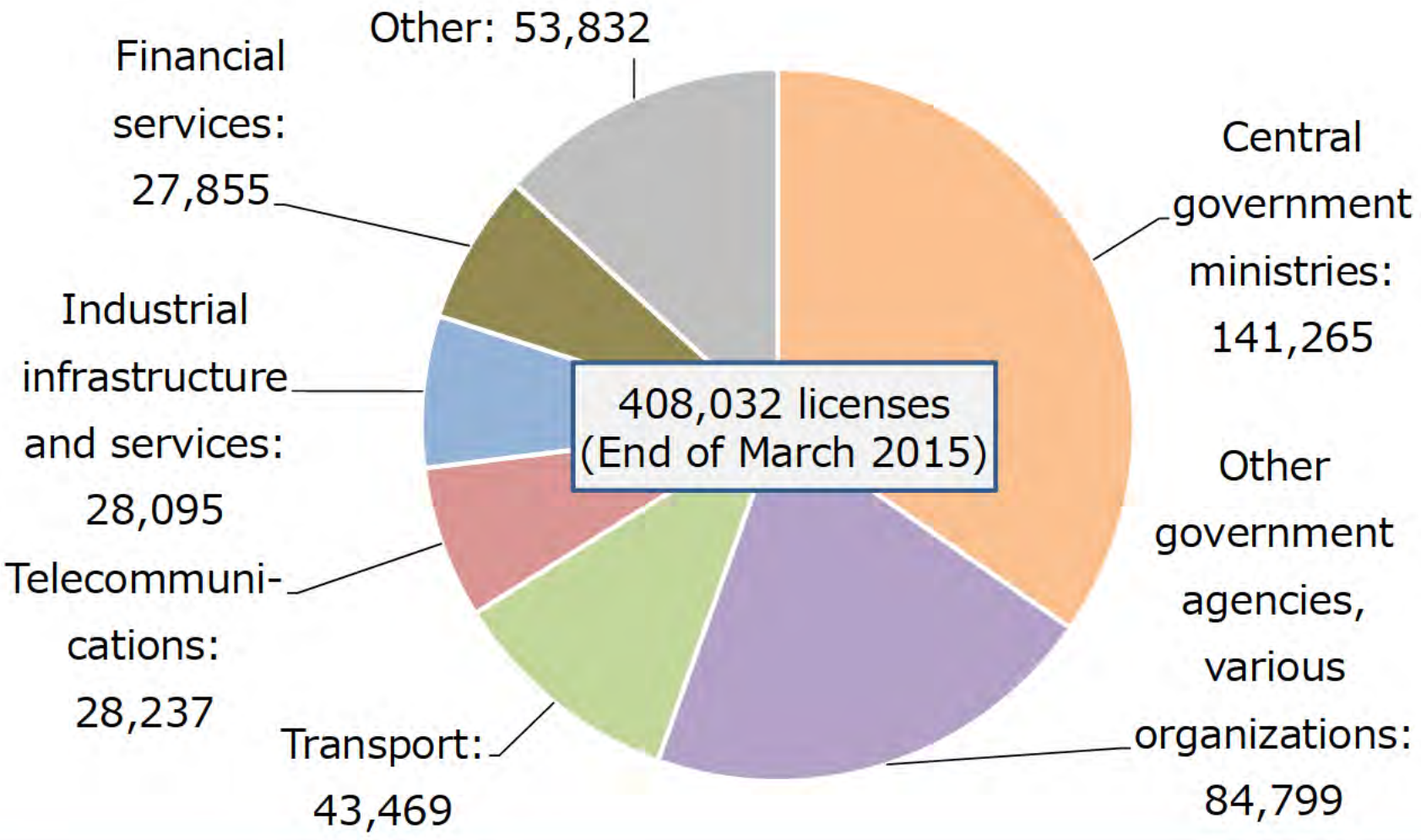
Period	Contracts (Licenses)			Product Unit Price (yen)	
	FFR yarai	FFR yarai Zeroday Attack Protection	Total	FFR yarai	FFR yarai Zeroday Attack Protection
March 2011	983	1,000	1,983	3,700	310
March 2012	14,843	21,237	36,080	4,160	440
March 2013	31,420	117,728	149,148	2,200	480
March 2014	76,007	239,830	315,837	2,240	350
March 2015	206,421	201,611	408,032	1,790	500

Notes 1. "Product Price" indicates the sales price for 1 license to a sales partner.
2. Adoption of volume discount pricing affects the product price on large-volume orders.
3. “FFR yarai Zeroday Attack Protection" is based on an entry-level vulnerability attack engine that is one of the five detection engines including in "FFR yarai". Due to an increase in recent years of threats that are not easily protected against using this function alone, new sales of this product will end on September 30, 2015.

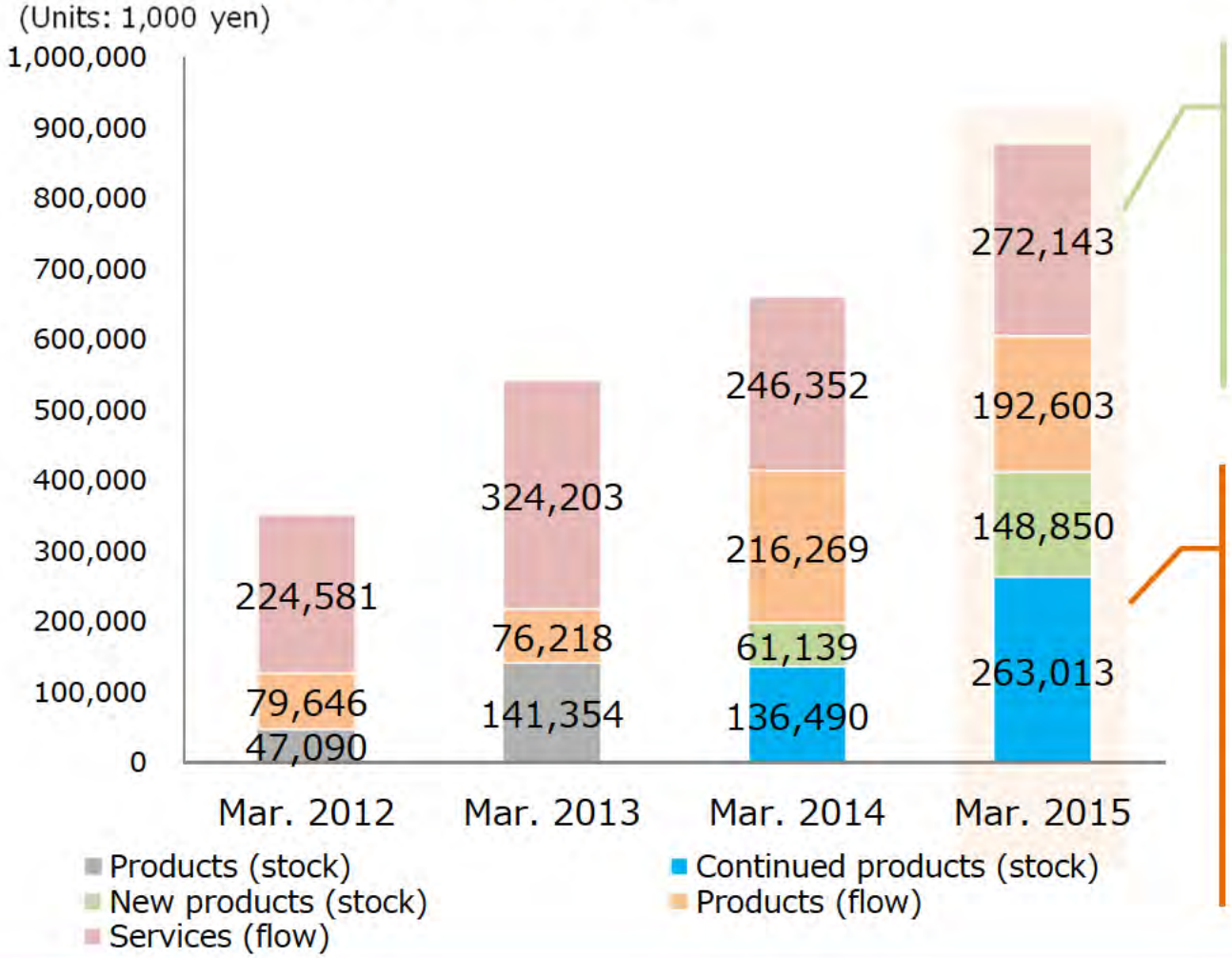
Trend in Contract Licenses by Quarter



Number of Contract Licenses by Business



Breakdown of Stock-type Revenue and Flow-type Revenue



Flow-type revenue

Sales calculated by delivery and acceptance timing
-Security services
-yarai analyzer
-Software transfer sales, etc.

Stock-type revenue

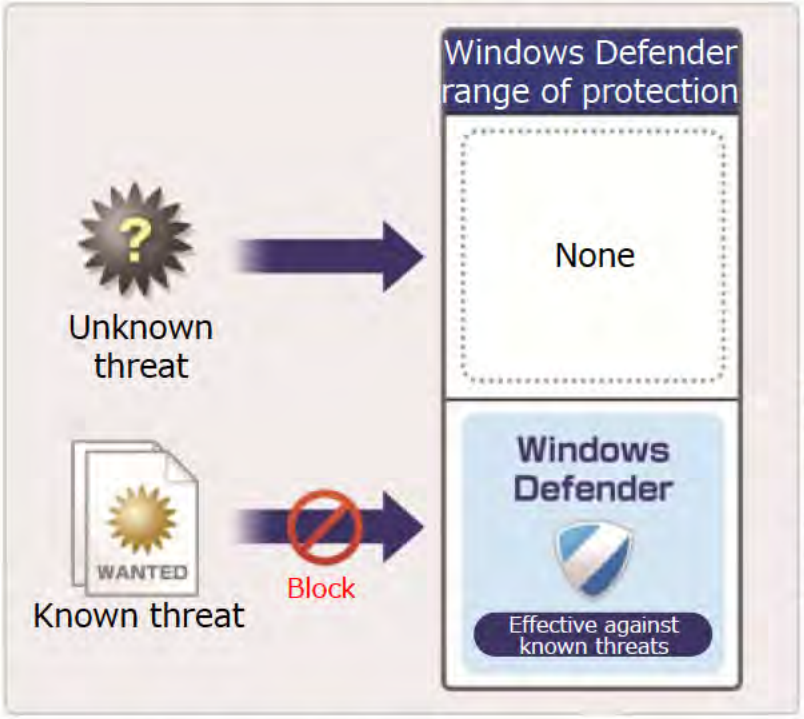
Estimated sales continuing each period, based on use
-FFR yarai
-FFRI app checker
-yarai analyzer maintenance contract, etc.

FUTURE EFFORTS

- By expanding our business to consumers, we are now able to offer a product lineup that meets the needs of all users.
- In the fiscal year ending March 2016, we will implement marketing activities to expand sales.

- March 2015	April 2015 - March 2016	April 2016 -
-Research and development -Expansion of systems and sales for corporations and government agencies -Release of consumer products	**Efforts** -Implementation of marketing activities for the consumer market Widely publicize products that are effective against new threats such as fraudulent money transfers in online banking. Prompt action is required in response to loss due to increasing fraud. -Expansion of sales to corporations and government agencies Respond to need for security measures ahead of the enforcement of the Basic Act of Cybersecurity, the start of the "My Number" system (ID number system), and the 2020 Tokyo Olympics. -Research and development Enhance product functionality, and lead research in new areas such as IOT. -Build and enhance overseas sales systems Enhance systems for the expansion of overseas sales.	-Research and development -Expansion of sales for consumer products -Expansion of sales to corporations and government agencies -Full overseas expansion -Expansion in new fields such as IOT

Replacement of the antivirus software market is being achieved with FFR yarai and FFRI proactive security.



Expansion of range of protection through introduction of FFR yarai and FFRI proactive security

yarai

PROACTIVE SECURITY

Since the range of protection is basically the same, there is little significance in the introduction of commercially available antivirus software.

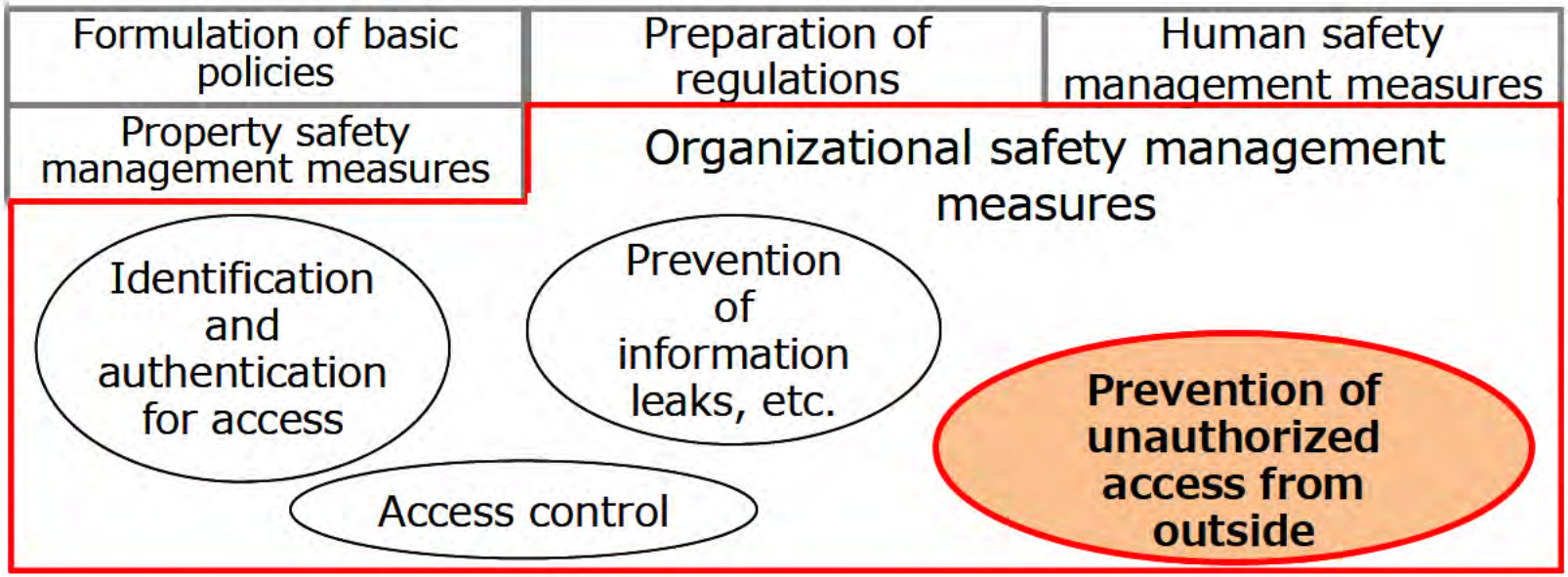
Antivirus software

Effective against known threats

* Windows Defender is a pattern-type antivirus software provided in Windows 8.1. For Windows 7, you can download and use Microsoft Security Essentials free of charge (for personal use only).

Responding to Needs with the Start of the "My Number" System (ID Number System)

According to Cabinet Office guidelines, mechanisms for protecting information systems from **external threats** must be introduced and operated as appropriate.



Performance Estimate

(Units: million yen)

Classification	March 2015 actual	March 2016 plan	Year-on-year (%)
Sales	876	1,815	107.1
Operating income (Profit rate: %)	256 (29.2)	263 (14.5)	2.7
Ordinary income (Profit rate: %)	241 (27.6)	263 (14.5)	8.9
Net income for the year (Profit rate: %)	171 (19.6)	176 (9.7)	2.7

Performance Estimate (Sales Breakdown)

(Units: million yen)

Classification			March 2015 actual	March 2016 plan	Year-on-year (%)
Security products	Corpo-rations	Continued sales	263	399	51.9
		New sales	341	373	9.4
	Individuals		0	760	-
	Subtotal		604	1,532	153.6
Security services			272	282	3.8
Total			876	1,815	107.1

Note: Continued sales
Our main products are based on a 1-year subscription contract. Sales from existing contracts and the renewal of existing contracts are managed as continued sales.

Seasonal Fluctuation in Sales

- Sales tend to be concentrated in the period from December through March, which is the end of the fiscal year for the corporations and government agencies who are our main clients.
  With our expansion into the consumer market, we expect this polarization in sales period to be gradually reduced in the future. However, the current trend will continue while corporations and government agencies account for the majority of our sales ratio.

(Units: million yen)

March 2016	1Q	2Q	3Q	Full year (plan)
Sales	-	-	-	1,815
Progress rate (%)	-	-	-	100.0

March 2015	1Q (actual)	2Q (actual)	3Q (actual)	Full year (actual)
Sales	164	282	430	876
Progress rate (%)	18.8	32.2	49.2	100.0

Handling of this Document

Future estimates and other information contained in this document are determined based on information available at this time, and are subject to change due to macro economic trends, market environments, industry trends related to our company, and other internal and external factors.

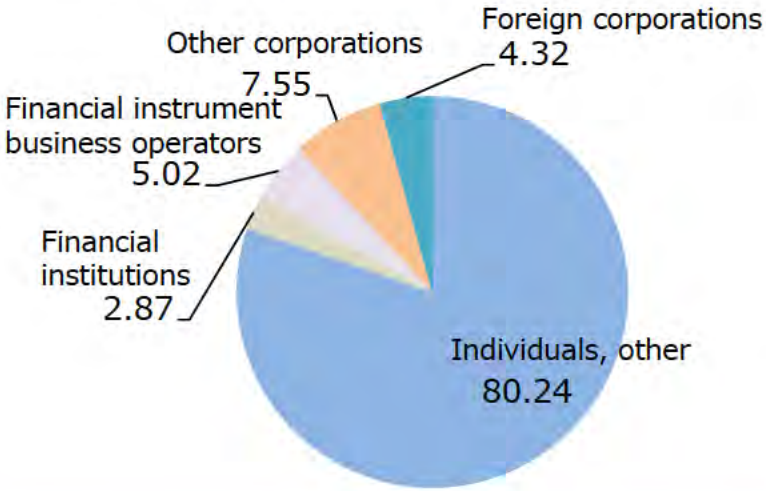
Therefore, please note that actual performance shall be subject to risk and uncertainty different from the estimates provided herein.

REFERENCE MATERIAL

Stock Conditions (March 31, 2015)

Number of shares outstanding	7,575,600
Number of shareholders	5,915

Shareholder composition



Major shareholders

Name	Shares (shares)	Ratio (%)
Yuji Ukai	1,992,000	26.29
Ryoji Kanai	1,626,000	21.46
NRI Secure Technologies, Ltd.	480,000	6.33
Shigeki Tanaka	126,000	1.66
Matsui Securities Co., Ltd.	122,400	1.61
Kazutaka Shimohigoshi	120,000	1.58
Japan Securities Finance Co., Ltd.	90,500	1.19
JP MORGAN CHASE BANK 385181	68,000	0.89
The Nomura Trust and Banking Co., Ltd. (Investment Trust Account)	67,700	0.89
Tetsuya Nagata	66,000	0.87
Total	4,758,600	62.77

Usage Patterns and Sales Price of Main Security Products

Personal/ Corporate	Name	Usage	License	Price	Dealer wholesale rate
Corporate use	FFR yarai	End point (installed and used on individual computers)	Subscription	Individual licenses ¥9,000/year (5-99 licenses) - ¥3,000/year (10,000 licenses -)	40% - 60%
Corporate use	FFR yarai analyzer	1 license per organization or site	Perpetual	¥3,000,000 per license (including first year maintenance fees) (Maintenance fees for the following year are 20% of the license fee (¥600,000))	60% - 80%
Personal use	FFRI proactive security	End point (installed and used on individual computers)	Subscription	¥8,500/year per license	-
Personal use	FFRI安心アプリチェッカー	End point (installed and used on individual devices)	Subscription	¥300/month per license	-

FFR yarai Progressive Heuristic Engine

* The 3DES encryption algorithm is used. (Settings cannot be changed by the user.)

Protects Applications from Vulnerability Attacks

ZDP Engine

Protects against Malware

Static Analysis Engine

Sandbox Engine

HIPS Engine

Machine Learning Engine

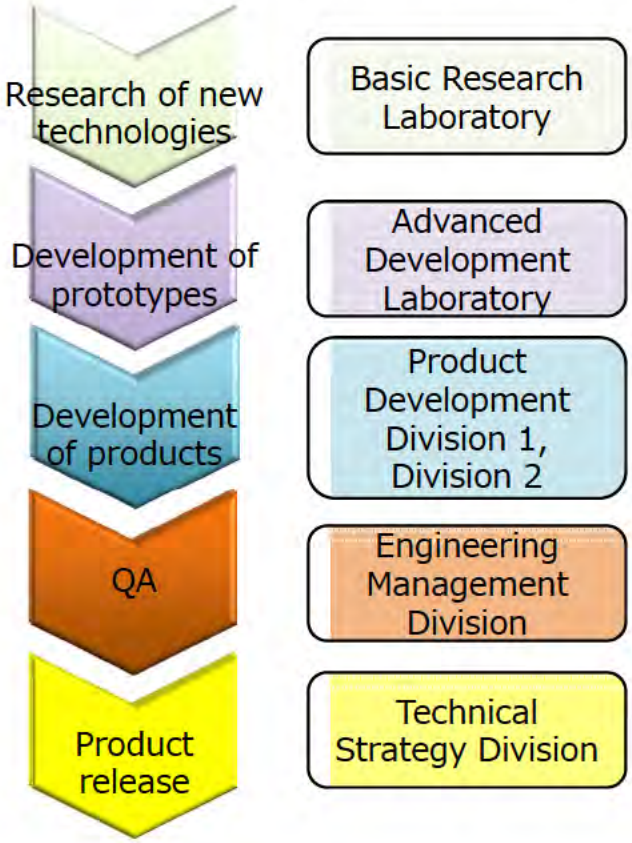
ZDP Engine	Protects against virus attacks that target known and unknown vulnerabilities such as attacks when viewing emails or Web pages. Protects against arbitrary code execution vulnerability attacks by use of our original API-NX technology (Patent No. 4572259).
Static Analysis Engine	Analysis performed without program operation. Detection is performed by using N-Static Analysis that incorporates numerous analysis methods including PE Structure Analysis, Linker Analysis, Packer Analysis, and Speculated Operation Analysis.
Sandbox Engine	Runs programs on a virtual environment that includes a virtual CPU, virtual memory and virtual Windows subsystems. Detection is based on a combination of commands based on our unique U-Sandbox Detection Logic.
HIPS Engine	Monitors the behavior of currently running programs. Our unique D-HIPS Logic detects behavior such as program intrusion, unusual network access, key logger and backdoor access behavior.
Machine Learning Engine	Monitors running programs based on big data related to malware that has been captured by FFRI. Behavioral characteristics in big data are extracted to detect malicious behavior in computer terminals by using machine learning to analyze such characteristics.

Organizational R&D System

Technical department system

Basic Research Laboratory [Role] Investigation and research of new security technologies
Advanced Development Laboratory [Role] Research, investigation, monitoring, and analysis of security technologies Development of product prototypes
Product Development Division 1 [Role] Design and implementation of software products (mainly for Windows)
Product Development Division 2 [Role] Design and implementation of software products (other)
Engineering Management Division [Role] Quality assurance related to products and services Support, installation, operation, construction
Technical Strategy Division [Role] Evangelist consulting activities Technical sales support

Flow of product development



Terminology

What is a targeted attack?

A targeted attack is a cyber attack that targets a specific corporation, organization, or individual.
This is a high-risk threat, because the attacker investigates the target thoroughly in advance and selects a method of attack according to the security measures in place on the target system.

What is malware?

Malware is software or a program designed with malicious intent, such as a computer virus or spyware.

Terminology

What is an unknown threat?

An unknown threat refers to an attack or malware that targets vulnerabilities that have yet to be discovered by the security vendor. Such threats cannot be successfully protected against with only operating system updates or the use of pattern-matching antivirus software.
Unknown threats have been seen more often with recent cyber attacks, resulting in a need for new measures.

What is heuristic detection?

Heuristic detection is a method for detecting the structure and behavior of characteristic programs such as malware, rather than attempting to match such programs to pattern files when malicious code is detected. This method can be used to respond to previously unknown viruses.