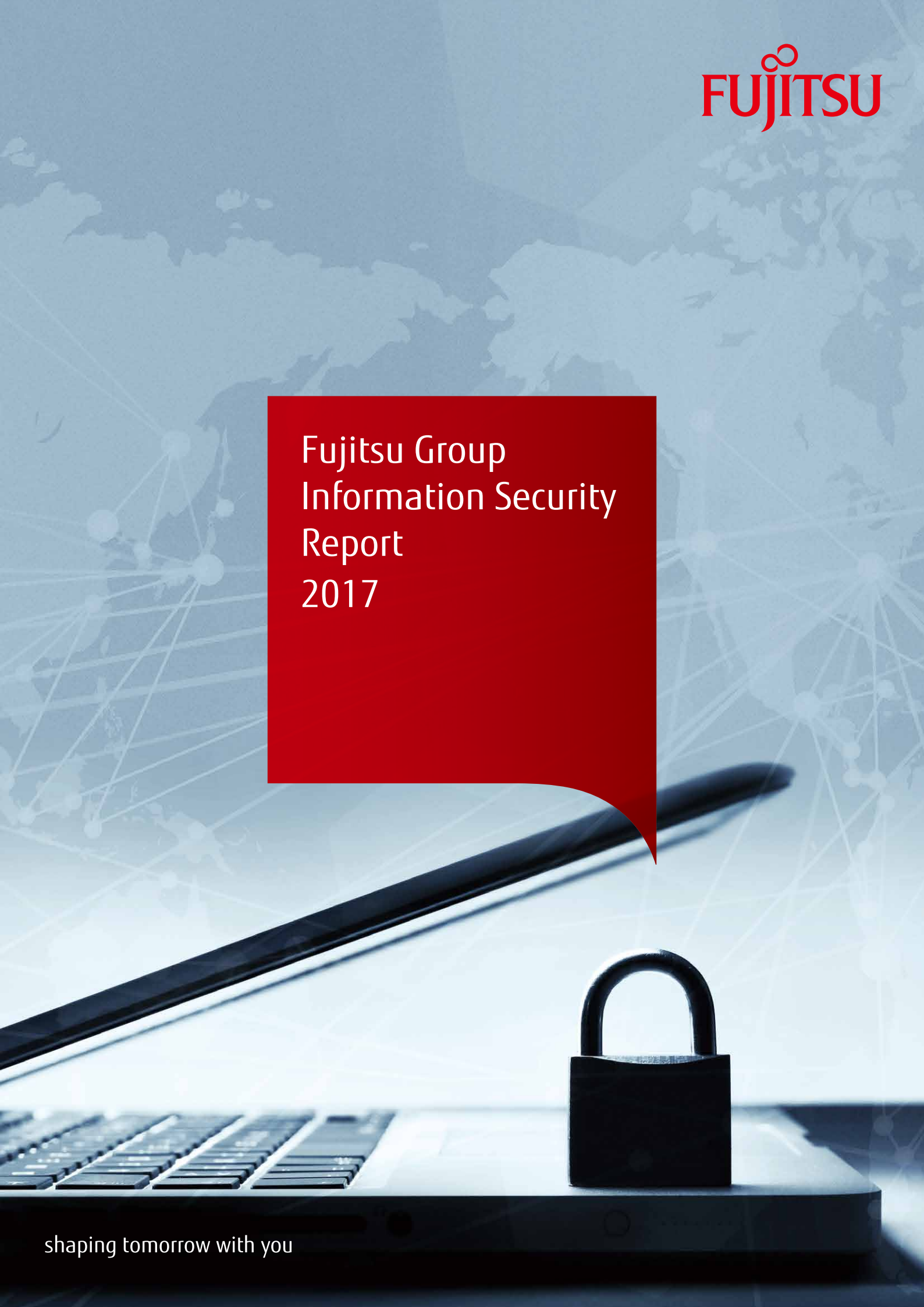
FUJITSU

Fujitsu Group Information Security Report 2017



shaping tomorrow with you

Editorial Policy

As a global information and communication technology (ICT) company, the Fujitsu Group understands the importance of strengthening information security and is thus taking various measures to realize a safe, secure digital society.

In this information Security Report, we describe the various information security measures being advanced by the Fujitsu Group. Having first been compiled in 2009, this report is the ninth such installment.

This report focuses on Fujitsu Group internal information security and its measures.

Through this report, we hope to foster an understanding of the Fujitsu Group and its support for realizing a safe, secure digital society.

Reporting Period

The basic reporting period includes activities from FY 2016 (April 1, 2016–March 31, 2017). However, some activities from outside this period are also included.

Reporting Organizations

The reporting organizations are Fujitsu Limited and its 514 consolidated subsidiaries (including overseas subsidiaries).

Referenced Materials

Ministry of Economy, Trade and Industry "Information Security Report Model"

Date of Publication

- Japanese version: June 2017
- English version: September 2017

Contents

Further strengthening information security for a more comfortable and secure networked society

ICT has connected people all over the world, and has given birth to various ideas and opportunities. On the other hand, the rapid growth of ICT has also presented us with new issues. In preparation for the continued increase in cross-border cyberattacks, ensuring robust protection of personal and confidential information has become a matter that must be dealt with immediately by all types of companies and organizations. The Fujitsu Group works with various related institutions to respond to cybersecurity related problems, and also utilizes the technologies we have acquired through the operation of our own systems.

The Fujitsu Group envisions a rich, sustainable "human-centric intelligent society" in which anyone can utilize ICT to draw out their maximum potential and in which information generates new value in a safe, secure manner. Through the power of ICT, we feel it is our social responsibility as a global ICT corporation to contribute to the realization of a sustainable world and society, and to maintain and strengthen the safety and security of the digital society.

Under this vision, at the Fujitsu Group we adhere to our internal policies based on the FUJITSU Way* code of conduct as a way of optimally managing and utilizing information. At the same time, to implement our corporate vision as stated in the FUJITSU Way, we have reestablished our globally shared Fujitsu Group Information Security Policy in accordance with the Cybersecurity Management Guidelines published by the Ministry of Economy, Trade and Industry in Japan and the Information-technology Promotion Agency, Japan (IPA), by which we actively work to ensure and improve information security.

Moreover, at the Fujitsu Group, we have built a unified information security management framework to ensure thorough information management and strengthened information security. As we operate across a wide range of business fields, we have designed an information security management framework for all business-unit levels which allows us to rapidly respond to the different problems related to information management and information security as required by the different natures of these individual businesses.

This Information Security Report 2017 introduces the activities related to Fujitsu Group information security. We humbly request that you take the time to read the contents of this report.

Naoyoshi Takatsuna

Chief Information Security Officer (CISO)
Fujitsu Limited

※ Fujitsu Group "FUJITSU Way" Vision and Values: http://www.fujitsu.com/jp/about/philosophy/

Internal Fujitsu Group Information Security

Taking measures to deal with ever-increasingly advanced, sophisticated cyberattacks has become a major issue for corporations. Likewise, it has become critical to strengthen the measures, organizations, and processes based on visualization of the current situation, and to continuously advance information security and apply these security measures in order to respond rapidly and unwaveringly to the growing societal problem of cyberattacks.

With ICT as the core of its business, the Fujitsu Group is driving and ensuring better information security within the Fujitsu Group through a variety of initiatives, including its basic policy and rules on information security, shared group ICT infrastructure, and security measures.

Basic Policy

To realize the "creation of a safe, pleasant, networked society" as proposed in the FUJITSU Way group vision and values, the Fujitsu Group is working to ensure and improve information security based on the Fujitsu Group Information Security Policy, our global security policy.

Fujitsu Group Information Security Policy

As a company that places ICT as our core business, the Fujitsu Group's corporate vision is to contribute to the "creation of a safe, pleasant, networked society," under which we work to ensure information security throughout the group, while ensuring and improving the level of customer information security by providing ICT products and services.

With the publication of the Cybersecurity Management Guidelines by the Ministry of Economy, Trade and Information and the Information-technology Promotion Agency, Japan (IPA) in December 2015, our Risk Management and Compliance Committee, which reports directly to the Board of Directors, reviewed our group-wide global security policy, and in April 2016 formulated the Fujitsu Group Information Security Policy.

Fujitsu Group Information Security Policy (excerpt*)

(Global Security Policy)

I. Purpose

In accordance with the Cybersecurity Management Guidelines formulated by the Ministry of Economy, Trade and Industry, the purpose of the Information Security Policy (hereafter, the "Basic Policy") is to set forth the measures, frameworks, and other basic matters required to ensure information security within the Fujitsu Group, as well as execute our corporate vision set forth in the FUJITSU Way, by which we have declared, both internally and externally, that the Fujitsu Group aims to ensure information security throughout the group and actively work to ensure and improve the information security of our customers through our products and services as a company that has placed ICT as the core of its business.

II. Basic Principles

(1) The Fujitsu Group, in all its business dealings, shall appropriately handle information provided by customers and partners as individuals and organizations, thereby protecting the rights and interests of said individuals and organizations.

(2) The Fujitsu Group, in all its business dealings, shall appropriately handle trade secrets, technical information, and any other information of value, thereby protecting the rights and interests of the Fujitsu Group.

(3) The Fujitsu Group shall endeavor to conduct research and development and train personnel, as well as provide products and services that contribute to ensuring and improving our customer's information security in a timely and reliable fashion in order to contribute to the continued growth of our customers and society as a whole.

* Fujitsu Group Information Security Policy (full text)
http://www.fujitsu.com/global/about/csr/management/security/

Management Frameworks

Independent of the chief information officer (CIO), the Fujitsu Group has appointed a chief information security officer (CISO) under the authority of the Risk Management and Compliance Committee to strengthen its information security governance as a global ICT company.

Information Security Management Frameworks

Given the recent increase in cyberattacks, the Fujitsu Group appointed a chief information security officer (CISO) under the authority of the Risk Management and Compliance Committee in August 2015. By separating out the responsibility for information security management, traditionally handled by the chief information officer (CIO), and appointing an independent officer dedicated to and specialized in information security management, we organized a framework that more rapidly and accurately manages risk measures in light of the growth of increasingly sophisticated cyberattacks.

Moreover, in aiming to strengthen our global information security management framework, we have appointed regional chief information security officers (regional CISOs) around the world under the authority of the CISO. Specifically, we are working to strengthen the global information security governance that supports our global ICT business in the five regions of the US, EMEIA, Oceania, Asia, and Japan.

Risk Management and Compliance Committee

The Risk Management and Compliance Committee reports directly to the Board of Directors, which handles risk management and compliance for the entire Fujitsu Group. The committee consists of Fujitsu's representative director president, executive, and chief risk management & compliance officer. The committee is also in charge of handling information security risk, which is a major risk.

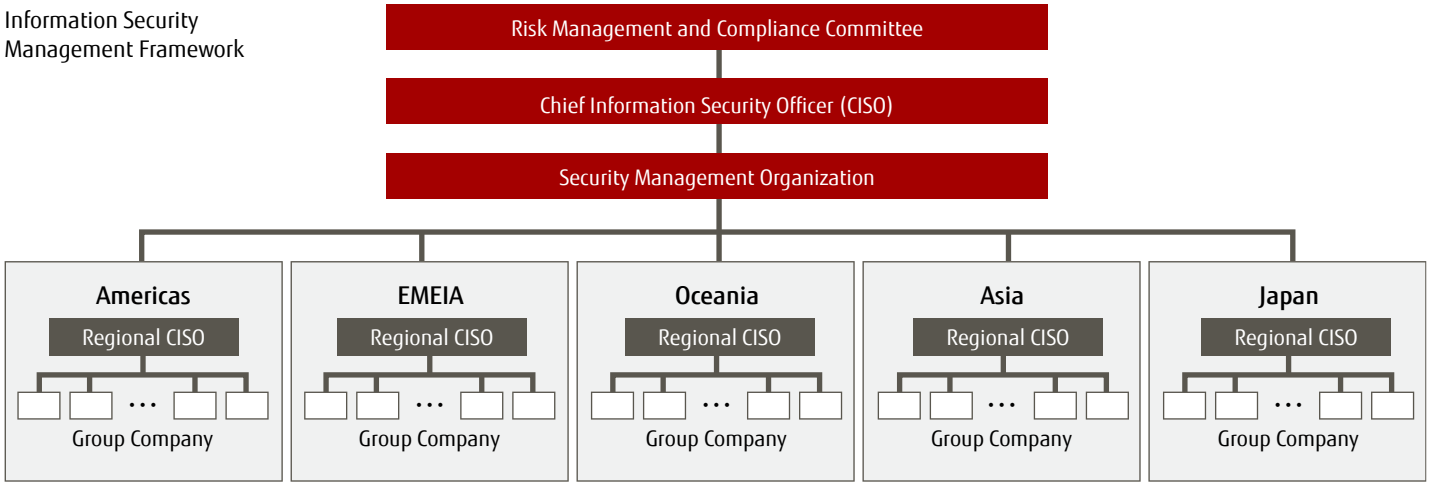
Chief Information Security Officer (CISO)

The chief information security officer (CISO) is appointed from the Risk Management and Compliance Committee, and is granted the responsibility and powers to manage global information security within the Fujitsu Group. The CISO reports regularly and as necessary to the Risk Management and Compliance Committee regarding the execution status of security measures.

Regional CISO

The regional CISOs are the chief security officers located in each of the five regions, and are granted the highest powers and responsibilities to manage information security within their region of authority. These officers formulate information security measures for the regions under their authority, and promote the thorough execution and reporting of information security as implemented by each group company's security team.

Information Security Management Framework



Security Management Organization

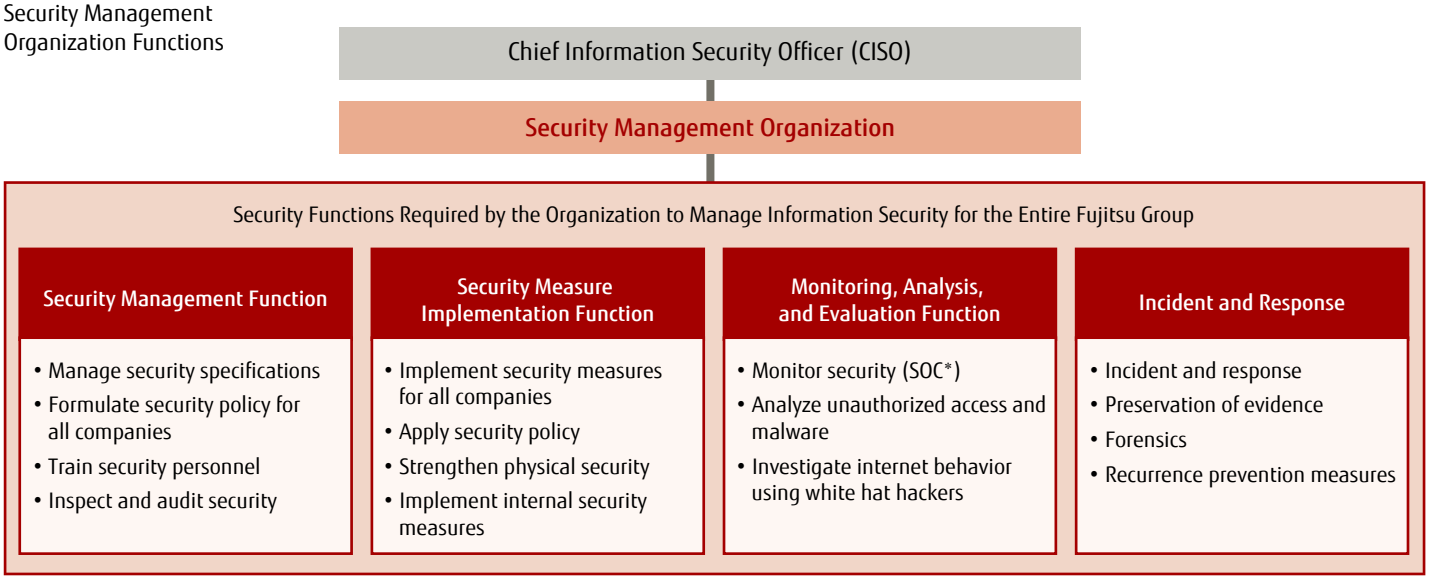
The Security Management Organization reports directly to the CISO for the purposes of strengthening Fujitsu Group information security, and plans common group rules and measures to promote unified management. This organization has four major functions designed to manage the Fujitsu Group security management function; security measure implementation function; monitoring, analysis, and evaluation function; and incident and response function.

Security Management Function

Company Security Policy Formulation

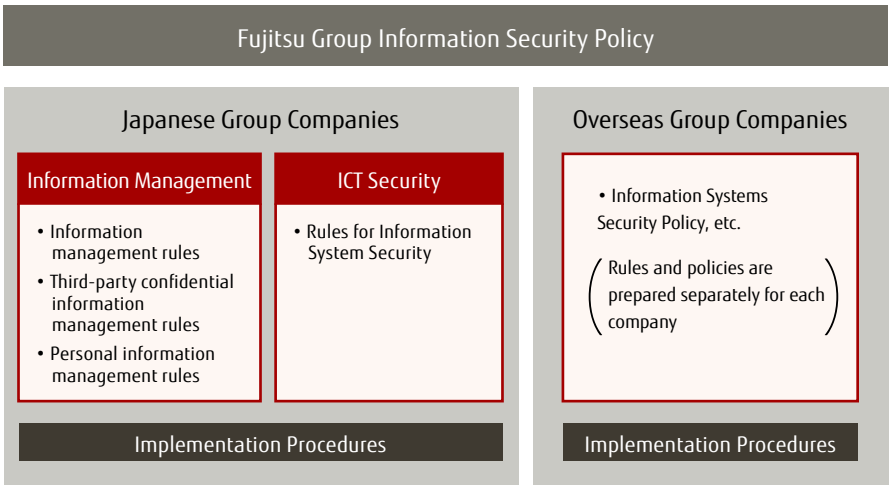
Based on the Fujitsu Group Information Security Policy, each Fujitsu Group company around the world prepares internal policies for information management and ICT security, by which they implement information security measures. Under the shared global Fujitsu Group Information Security Policy, we have prepared policies related to information management and information security for the group companies in Japan. For overseas group

Security Management Organization Functions



*SOC: Security Operations Center

Information Security Policy Framework



Information Management Rules
Rules for appropriately handling information for work

Third-party Confidential Information Management Rules
Rules for appropriately handling third-party confidential information

Personal Information Management Rules
Rules for appropriately handling personal information based on personal information protection policy principles

Rules for Information System Security
Management rules for maintaining the confidentiality, integrity, and availability when using information devices, information systems, and networks

companies, they create and prepares rules and policy in accordance with the regulations of the respective country.

Security Screening and Auditing

The Fujitsu Group conducts information security audits for each business department globally. These audits are conducted by an audit department that is independent of the business departments. The audits are conducted in a manner that considers the characteristics, business strategies, and ongoing information security measures, etc., of the different business departments. For example, in addition to conducting on-site investigations to determine whether setup is in accordance with the rules at the time the intranet was installed, we also perform audits at the time public servers on the internet go on-line, as well as regular vulnerability audits in Japan.

In accordance with ISO 27001-compliant security requirements, we utilize assessment tools to evaluate the management of overseas group companies. Business departments that have been audited then work to improve their information security measures based on the audit results.

Information Security Training

To prevent information leaks, we feel it is important to raise the security awareness and skill level of each individual employee, not only inform our employees of the various policies. Therefore, all 100,000 employees of Fujitsu and group companies in Japan are provided with information security training during new employee training and promotion/advancement training, and all employees, including officers, are provided with security e-Learning in both Japanese and English every year.

Similarly, we provide employees of our overseas group companies with security training once per year in approximately 10 languages. Moreover, we provide overseas information security managers with the required security training for managers.

e-Learning Screen

Information Security Awareness Development

Fujitsu Group companies in Japan formulated and raised a domestic shared group slogan, "Declaration for complete information management! Information management is the lifeline of the Fujitsu Group," in 2007. Along with posting educational posters in the business offices of Fujitsu and its group companies in Japan we place sticker on every employee's work computer, for example, to raise the awareness of each individual employee regarding information security.

In addition to these measures, we encourage the alertness of our employees by using our intranet to inform them of the frequent and global occurrences of information leaks, and hold security check days once per month as a way of ensuring that our managerial employees verify the security status of their own departments.

Complete Information Management Seal

Declaration for complete information management! Information management is the lifeline of the Fujitsu Group

Information Management Handbook Publication

In Japan we publish the Information Management Handbook to deepen the understanding of internal policies regarding information management. This handbook can also be viewed on the intranet so that policies can be checked immediately whenever there is a question regarding information management.

Information Management Handbook

—Enhancing Security Thinking and Skills—

■ Collaboration with Partners

Partner Information Security Management (selection, status evaluation, verification)

When selecting new partners, we verify the partner's information security condition and limit partners to those who have consented to agreements regarding important matters for information security management and handling of personal information during work contracting.

In regard to existing partners, we also conduct an annual written survey of the partner's information security status and select contractors based on required matters, such as the Act on the Protection of Personal Information. We also provide the results of the written survey, including the overall status and evaluation tools, as feedback to our partners so that they can implement initiatives to improve security.

Once a partner has been selected, we conduct annual information security audits. We visit our partners and inspect their information security compliance status based on any agreements. When the results of the inspection reveal a need for correction, we draw up a rectification plan and provide implementation guidance.

Information Security Audits (FY 2016):
Approximately 190 companies

Information Security Training Sessions

Recently, rapid changes in the ICT environment has led to a greater risk of information leaks than in the past, which in turn has led us at the Fujitsu Group to hold information security training sessions for both group employees and our partners to which software development and services are contracted.

Given that preparing for advanced persistent threats(APTs) and ensuring other cybersecurity measures is an urgent matter for our partners, as well, in FY 2016 we held training sessions under the main theme of "Security Risk Response."

At the request of our partners, we also conducted on-site training sessions to which we dispatched lecturers. In addition, for partners that requested leader class skill training, we conducted on-site workshops in which group exercises and discussions were used to improve risk response skills. So that the workshop style training sessions could be attended by many of our partners, we planned and conducted collective workshops to which even single individuals could apply.

Information Security Training Session Details (FY 2016)

Approx. 900 companies/approx. 1,200 attendees
(Sendai, Tokyo, Kawasaki, Chiba, Nagoya, Osaka, Takamatsu, Fukuoka, Okinawa)

- On-site Training Sessions: Approx. 80 companies/approx. 1,300 attendees
- On-site Workshops: Approx. 10 companies/approx. 180 attendees
- Collective Workshops: Approx. 20 companies/Approx. 30 attendees

Information Sharing and On-site Support Tool Provision

Awareness Poster

Since 2009, we have provided "Information Security Plazas" and "Awareness Posters" to our partners as a way of sharing and providing the latest information regarding information security.

Moreover, we provide project specific "Project Information Security Plans" to which all employees consent as a means of sharing information security requirements at the start of each project, and which serves as a means of aiding early discovery and response to problems. In addition, we also provide a "Compliance Status Check Sheet" as a self-inspection tool.

Overseas Partner Response

For the purposes of responding to the globalization of our customers, reducing development costs, and securing personnel, we have been increasing business cooperation with overseas partners.

Fujitsu, as do in Japan we conclude Information Manage-

On-site Workshop

Information Security Training in India

ment Guidelines for Contractors agreements with our overseas partners, which provide for handling of entrusted information in accordance with the conditions of the specific country. We also conduct regular information security audits and provide information security training.

Personal Information Protection

Fujitsu acquired the PrivacyMark in August 2007, and has continuously worked to strengthen our personal information protection framework, which includes annual personal information handling training and audits. Our group companies in Japan also acquire the PrivacyMark when necessary, and work to ensure personal information management. On the public websites of our overseas group companies, we post privacy policies designed to meet the laws and social requirements of each country. The Fujitsu Group companies are working on reinforcement of personal information protection system for a more secure and smooth protection of personal information in an ever-evolving state of global data circulation.

Security Measure Implementation Function

In accordance with the security policies, we implement the following security measures to the entire group companies.

Network Security

We have installed firewalls between the external internet environment and the Fujitsu Group internal information network to protect against unauthorized access, and have adopted an unauthorized intrusion detection system to maintain the safety of our intranet. Our Security Operations Center (see page 12) monitors detection information 24 hours a day, 365 days a year.

E-mail Security

Our e-mail gateways for handling external threats include spam mail and malware (virus) countermeasures, such as IP reputation and sender domain authentication. In addition, we automatically reverify all transmissions sent outside the company using automated e-mail recipient identification and automatically verify external transmission eligibility, thereby preventing any user who does not need external e-mail communication from transmitting e-mails or leaking information outside of the company.

Web Security

As a means of providing safe internet access procedures, all access to the internet necessarily passes through proxy servers, which check for malware and filter URLs to prevent access to malicious websites. In addition, proxy utilization is limited by user authentication, which both prevents unintended access and records user access logs.

Remote Access

We provide a remote access environment that allows work to be conducted safely when connecting to the intranet from outside the company via personal computer or smart device. We encrypt communications over the access routes and utilize two-factor authentication to prevent unauthorized access. In addition, as an initiative to innovate working-styles, we have introduced virtual desktops and provide an environment that allows for work to be carried out remotely while ensuring security by preventing data from remaining on the personal computer being used.

Endpoint Security

We automatically apply OS and application security updates, as well as renew malware definition files on employee computers. In addition, we utilize thin clients for terminals on which data cannot be saved to strengthen our information leak prevention measures. Similarly, we are continuing to install standard personal computers and thin clients equipped with these endpoint security measures. As a result, we have been able to reduce the burden required of each individual employee for implementing different security measures on personal computers, and at the same time have improved the level of security by implementing standardized endpoint security in a systematic, unified manner.

Authentication Security

We have introduced IC security cards for employee authentication and other purposes. The face of the security card is printed with the name and photograph of the employee, and the IC chip is loaded with the name, employee number, employee public key infrastructure (PKI) certificate, and key. These cards which are managed by the human resources department, guarantee the card user is the proper employee. These cards can be used for both system login authentication via secure identity verification and electronic document settlement, which is as effective as stamping a sanctioned seal on paper documents.

Monitoring, Analysis, and Evaluation Function

Security Monitoring

We record 1 billion logs per day using security monitors located around the world. When implementing information security management, it is essential to efficiently and effectively manage these logs.

The Fujitsu Group has established a Security Operations Center (SOC) that functions 24 hour a day, 365 day a year, and has created a mechanism that allows for fast, accurate incident and security alert response. The logs generated from the security monitors installed in multiple locations within the company's network are compiled and centralized in the Log Integration Management System. These logs are then transmitted to Systemwalker Security Control, a log automation and control tool, which then sends an alert notification e-mail to the SOC if it confirms a threat.

The SOC comprises local operators, incident managers, and security assistants, who analyze the details of the received alert notification e-mail, determine the quality, scope, and weight of the threat, rank the response priority, and handle the threat in a fast, accurate manner.

White Hat Hacker Internet Behavior Surveys

To respond to the evolving threat of cyberattacks, we use white hat hackers to investigate global incidents and vulnerabilities, and use cyber intelligence to investigate logs based on the risk information generated from unauthorized access and malware analysis, thereby minimizing the risk of new threats and preventing the occurrence of incidents.

Incident and Response Function

Incident and Response

The Fujitsu Group has established a dedicated incident and response team. When an incident occurs, the team cooperates with the SOC to identify the location of occurrence and affected terminals, after which the team uses specialized devices to appropriately preserve evidence*. In addition, the team employs measures to prevent secondary damage and to reduce the spread of damage.

*Preservation of evidence: Rapidly collecting traces of the cyberattack and analyzing these is essential to identifying the cause of the incident as well as any damage. To ensure these traces are not lost, electromagnetic evidence (hard disks, logs, etc.) from the equipment related to the incident is preserved (copied, etc.).

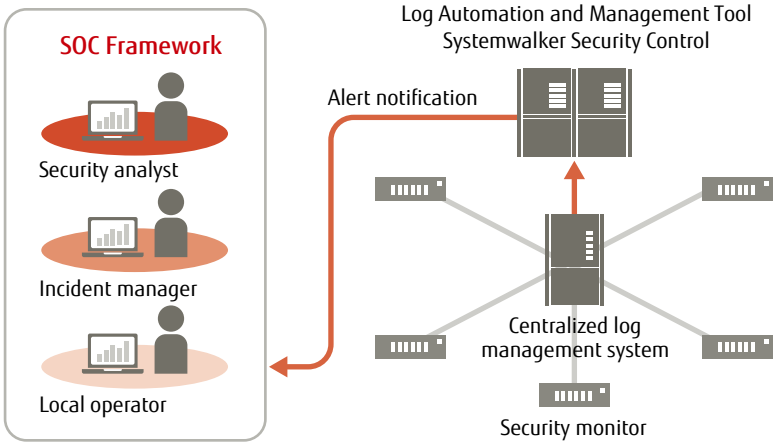
Forensics

We analyze the preserved evidence, as well as the alerts and logs acquired by the SOC. We then identify the damage, cause, and affected scope to rapidly bring the situation to a close.

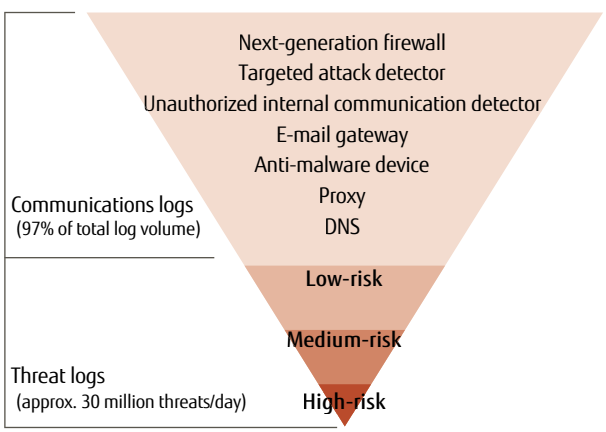
Recurrence Prevention Measures

We then report the risk discovered by the investigation to the Risk Management and Compliance Committee. Under the CISO, we further investigate whether similar incidents have occurred, and deploy recurrence prevention measures to all companies in cooperation with the related departments.

Security Monitoring (SOC) Framework



Security alert classifications



Priority Measures

From the perspective of defense in depth, the Fujitsu Group has streamlined its information security priority areas and is aggressively promoting the three priority measure areas of information management, cybersecurity, and physical security.

Three Priority Measures Based on the Concept of "Defense in Depth"

Recent cyberattacks, often experienced as "advanced persistent threats(APTs)" have become more sophisticated, diverse, and complex than in the past, so conventional single-layer security measures are no longer able to completely defend against these.

The Fujitsu Group has adopted the concept of "defense in depth," a multilayer defense mechanism that utilizes several different defense measures instead of one, as its basic concept for information security. Defense in depth has three goals: "Prevent attacks by raising multiple defensive barriers," "Rapidly detect attacks by establishing multiple detection functions," and "Minimize damage after infiltration." By appropriately deploying these, we can prevent attacks and minimize damage.

The Fujitsu Group has adopted three priority security measures to protect internal information, namely "information management," which aims to protect information, "cybersecurity," which is centered on measures that protect systems against cyberattacks, and "physical security," which prevents unauthorized access to offices, factories, and other facilities.

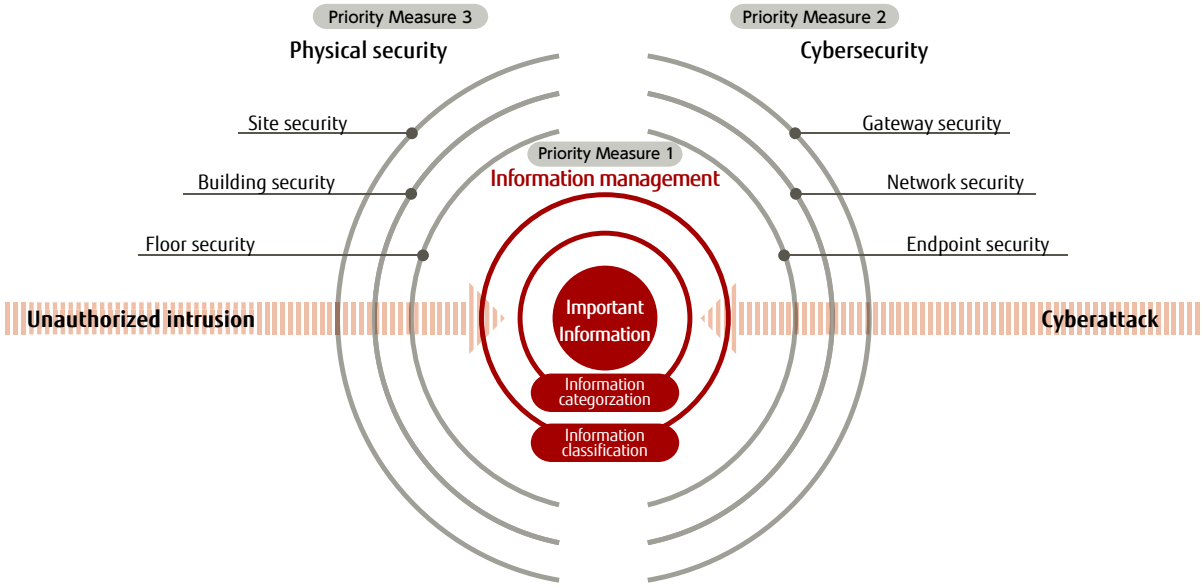
Priority Measure 1: Information Management Security

Information Classification

The Fujitsu Group in Japan has established a set of rules for handling information circulated internally called the Information Management Policy, by which we categorize, appropriately manage, and utilize internally circulated information. In other countries as well, we categorize and manage information according to the situation of each country in a similar manner.

Internal-use-only information and restricted information are managed in accordance with the Information Management Policy, whereas third-party confidential information is managed in accordance with the Third-party Confidential Information Management Policy.

Defense in Depth Conceptual Image



Information Categories

Information Categories			Examples	Personal Information Examples
Public Information			Catalogs, manuals, press releases, public website, etc.	Executive officer information posted on the public website, etc.
Confidential Information	Fujitsu Confidential Information	Internal-use-Only Information	Information other than restricted information • Internal rules, etc.	Organizational chart
		Restricted Information	Information that should not be disclosed to unrelated parties • Information on under development technologies	Human resources information, customer lists, etc.
	Third-party Confidential Information			Personal information received as a result of contracted work

Public Information	Public information refers to disclosed items, including public websites, catalogs, and manuals.
Confidential Information	Confidential information is categorized into Fujitsu Confidential Information and Non-Fujitsu Confidential information, where Fujitsu Confidential Information is further categorized as Internal-use Only Information and Restricted Information.
Internal-use-Only Information	Internal-use only information refers to information that must not be disclosed outside the company, including internal rules and internal reports, etc.
Restricted Information	Restricted information refers to information that should not be known to unessential personnel, such as human resource information, information on under development technologies, and customer lists.
Third-party Confidential Information	Third-party confidential information refers to information subject to confidentiality by agreement, such as confidential information acquired from customers and other companies through contract agreements, non-disclosure agreements, licensing agreements, and such.
Personal Information	Personal information refers to personal information independently acquired by Fujitsu and personal information held by customers that is received by and for which access has been granted to Fujitsu coinciding with services entrusted by the customer for contracted development. Personal Information includes Japan's social security and taxation number.

Information Categorization (Public Information, Confidential Information Categories)

Information handled inside the company is categorized as shown in the figure above. We also rank the seriousness with which information should be handled in terms of legal requirements, value, and importance, etc., and, in Japan, we categorize information on four levels, namely public information, internal-use only information, restricted information, and third-party confidential information.

We have defined rules for how information of each category should be handled and protected. Our domestic group companies in Japan conduct on-site audits once per year to determine if the PDCA cycle for managing important information in accordance with these rules is being implemented. Our overseas group companies also categorize information similarly to how we do domestically.

Priority Measure 2: Cybersecurity

The Fujitsu Group implements separate measures at different layers in accordance with the network characteristics in preparation for cyberattacks. Through defense in depth security that combines gateway security measures, which include firewalls and advanced persistent threats(APTs) measures, network security measures, which include unauthorized access detection, and endpoint security measures, which include malware countermeasures and security patch management, we are working to protect against increasingly sophisticated, diverse, and complex cyberattacks.

Gateway Security Measures

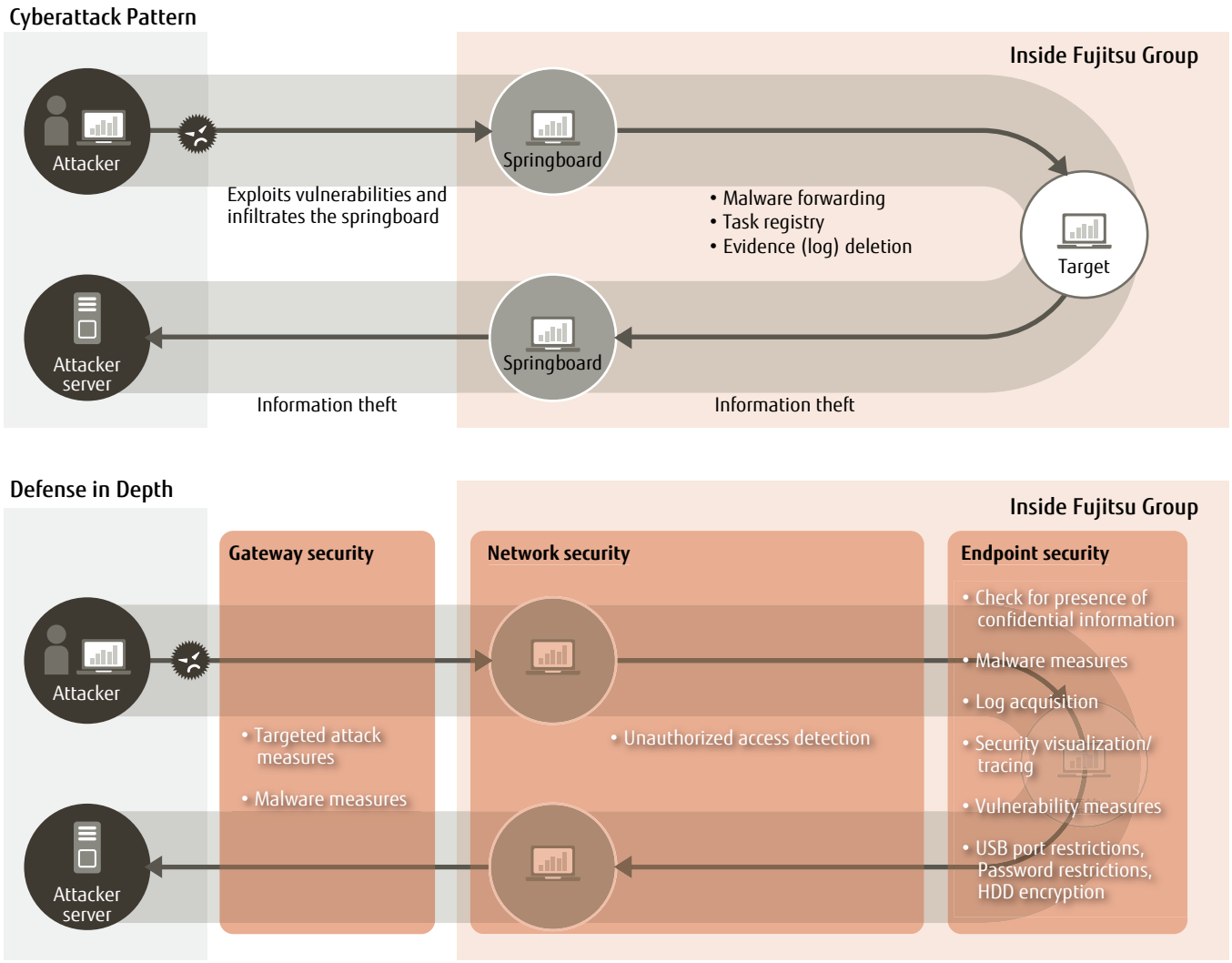
When preventing cyberattacks, it is essential to prevent intrusion from outside. The Fujitsu Group has installed a gateway at the border between the external internet environment and the Fujitsu Group internal information networks, thereby blocking unessential communications from outside to ensure security. Specifically, we have adopted a firewall to protect against unauthorized access to the border with the internet layer, an unidentified malware detection system as a advanced persistent threats(APTs) countermeasure, and monitor e-mail and web communications as entrance/exit measures.

Network Security Measures

Whereas conventional cyberattack countermeasures are focused on gateway measures that block intrusion from outside, the recent advancement of cyberattacks, including advanced persistent threats(APTs) has made it increasingly difficult for this approach to fully protect against intrusion from cyberspace. This has made internal measures that rapidly detect threats in the internal network essential.

The Fujitsu Group has installed devices that detect unauthorized internal communications as a measure to detect suspicious communications on its internal networks, and is also demonstrating new technologies under development by implementing these internally as a step towards commercialization and actual operations.

Cyberattack and Defense in Depth Cybersecurity Measures



Endpoint Security Measures

The recent increase in targeted e-mail attacks and other cyberattacks targeting endpoints such as personal information terminals has led to a stronger demand for countermeasures than in the past.

The Fujitsu Group is also adopting and implementing the concept of "defense in depth" for endpoint security, including for employee personal computers and mobile terminals. We have taken the necessary security measures by separating endpoints into individual layers, including malware countermeasures, log acquisition, and HDD encryption. In accordance with the shared global Fujitsu Group Information Security Policy, we manage security by limiting network

Main Endpoint Security Measures

Layer	Security Measures
Data	Confidential information check
Security tools	Malware countermeasures
Logs	Log acquisition
Security patch	Security visualization and tracking
OS	Vulnerability measures
Device	USB port restrictions, password restrictions, HDD encryption

Priority Measures

access from personal computers with operating systems for which support is no longer provided.

As an information leak countermeasure, we also apply restrictions so that confidential information, including customer data, cannot be saved to personal computers or written to external media.

Priority Measure 3: Physical Security

We take measures to provide security at sites including factories and on office floors, not just at the entrances of offices. In accordance with the concept of defense in depth, we also apply security measures here that clearly separate the line of flow for employees and visitors in order to strictly control entry and exit. In addition, using security cards and surveillance cameras allows us to capture detailed information for entry and exit, while at the same time enhancing our tracking capability during emergencies. We also take similar physical security measures in other countries in accordance with the situation of each country.

Policy

- Only authorized personnel are allowed on sites, inside buildings, and on floors.
- Regardless of whether the individual is an employee or not, we always capture and record the entry and exit of all personnel.

Site Security

In addition to entry and exit security gates at which passage is checked by guards, we detect intrusion via external fence sensors and surveillance cameras to strictly control access, thereby ensuring that only authorized personnel may enter.

Building Security

We have implemented entry and exit control at building entrances using security gates and security cards to prevent unauthorized entry.

Floor Security

We have separated work areas in which internal networks have been installed from other work areas, and further restricted entry and exit to these areas in order to prevent those without authority from accessing important information. Even when there is an attending employee, for example, anyone other than a Fujitsu Group employee is prohibited from entry to ensure security. Specifically, during entry and exit, security cards are used to authenticate the individual, where palm vein authentication is used when we feel it is necessary to further increase the level of security.

Palm Vein Authentication Security Gate (European Office)

Published by

FUJITSU LIMITED

Corporate Affairs & Risk Management Unit

Shiodome City Center, 1-5-2 Higashi-Shimbashi, Minato-ku, Tokyo 105-7123, Japan