Fujitsu Group Information Security Report 2018

FUJITSU

shaping tomorrow with you

Contents
Editorial Policy

Editorial Policy

As a global Information and Communication Technology (ICT) company, the Fujitsu Group regards the maintenance and further strengthening of information security as its vital social responsibility to achieve a secure, safe digital society.

We started publishing the Information Security Report in 2009, and this year marks our 10th issue. In addition to the measures we have been implementing for some time, we are also carrying out various efforts in line with social trends.

I hope you will gain an understanding of the Fujitsu Group's security initiatives, and also that this report proves helpful in improving your security.

Thank you for reading.

■ Reporting Period

The basic reporting period includes activities from FY 2017 (April 1, 2017 to March 31, 2018). However, some activities outside of this period are included.

■ Reporting Organizations

The reporting organizations are Fujitsu Limited and 502 consolidated subsidiaries (including overseas companies).

■ Reference Material

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

■ Publication Date

- Japanese version: June 2018
- English version: August 2018

Continually Strengthening Information Security for a Prosperous Future With ICT

Mitsuya Yasui
Chief Information Security Officer (CISO)
Fujitsu Limited

The Fujitsu Group has set forth a vision of achieving a "Human Centric Intelligent Society," a prosperous, sustainable society through the usage of technology and data by people.

To accomplish this, we are striving to leverage AI, IoT, and other cutting-edge technologies and connect the knowledge of different industries for social innovation and creating business value based on the theme of "Human Centric Innovation: Co-creation for Success." This brings about success in business and society through co-creation with customers and partners.

It goes without saying that information security is gaining greater importance for achieving this vision and theme.

Cyberattacks, exemplified by advanced persistent threats (APTs), have been gaining sophistication and complexity in recent years. Maintaining security is extremely important for reliably safeguarding personal, confidential, and other information from unauthorized access. In addition, the European Union's General Data Protection Regulation (GDPR) was enacted in May 2018. This stipulates stricter regulations for the handling of personal information, as well as sanctions for violations, from the viewpoint of basic human rights. Accordingly, companies must handle personal information with even greater care.

The Fujitsu Group has long made information security initiatives before other companies according to our FUJITSU Way Code of Conduct and our slogan, "Information management is the lifeline of the Fujitsu Group."

Today, the chief information security officer (CISO) is appointed based on the Fujitsu Group Information Security Policy, and this company culture is inherited by our global information security management frameworks.

The Information Security Report 2018 introduces the Fujitsu Group's information security initiatives. It also includes information about our "defense in depth" approach against increasingly sophisticated cyberattacks, GDPR initiatives, and work-style reform through strengthened information security.

I hope you will come to understand the information security implemented by the Fujitsu Group, which will keep striving to earn your trust.

Thank you very much for reading.

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

Basic Policy

Fujitsu Group Information Security Policy

With ICT as our core business, the Fujitsu Group's Corporate Vision states that we will "contribute to the creation of a safe, pleasant, networked society." We work to ensure information security throughout the Group while maintaining and improving the level of customer information security by providing ICT products and services.

In April 2016, we determined the Fujitsu Group Information Security Policy with the aim of sharing this thinking throughout the Group and having each employee take action. It was formulated with guidance from the Risk Management and Compliance Committee, which reports directly to the Board of Directors. This Basic Policy conforms to the Cybersecurity Management Guidelines established by the Ministry of Economy, Trade and Industry and the Information-technology Promotion Agency, Japan (IPA) in December 2015.

KEIDANREN (Japan Business Federation) also announced its Declaration of Cyber Security Management* in March 2018. The Fujitsu Group supports KEIDANREN's declaration as the same principle set forth in the Fujitsu Cyber Security Declaration, which was released in November 2016.

As a leading ICT company, the Fujitsu Group will contribute to the cybersecurity of customers and society at large by cultivating new technologies through proactive research and development, and also offering various ICT solutions incorporating these technologies.

* KEIDANREN's Declaration of Cyber Security Management (link to the KEIDANREN website)
http://www.keidanren.or.jp/policy/2018/018.pdf

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/imagesgig5/InformationSecurityPolicy_en.pdf

Management Frameworks

Information Security Management Frameworks

Given the recent increase in cyberattacks, the Fujitsu Group appointed our chief information security officer (CISO) under 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 have built a framework to rapidly and accurately deal with the risk of increasingly numerous and sophisticated cyberattacks.

Moreover, 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 Americas, EMEIA, Oceania, Asia, and Japan.

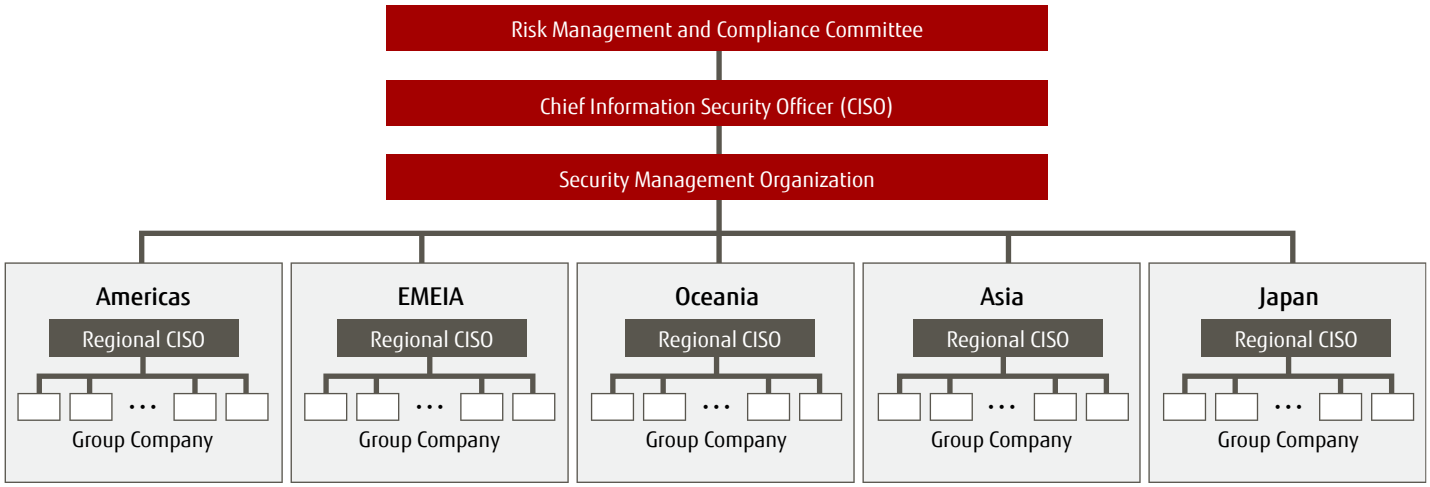
Risk Management and Compliance Committee

The Risk Management and Compliance Committee is an organization that reports directly to the Board of Directors, which controls risk management and compliance for the entire Fujitsu Group that does business globally. The committee consists of Fujitsu Limited's president and representative director, executive directors, and chief risk management & compliance officer. The committee is also in charge of managing information security risk, 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 authority for global information security measures in the Fujitsu Group. The CISO reports regularly and as necessary to the Risk Management and Compliance Committee about the status of security measures.

Information Security Management Framework



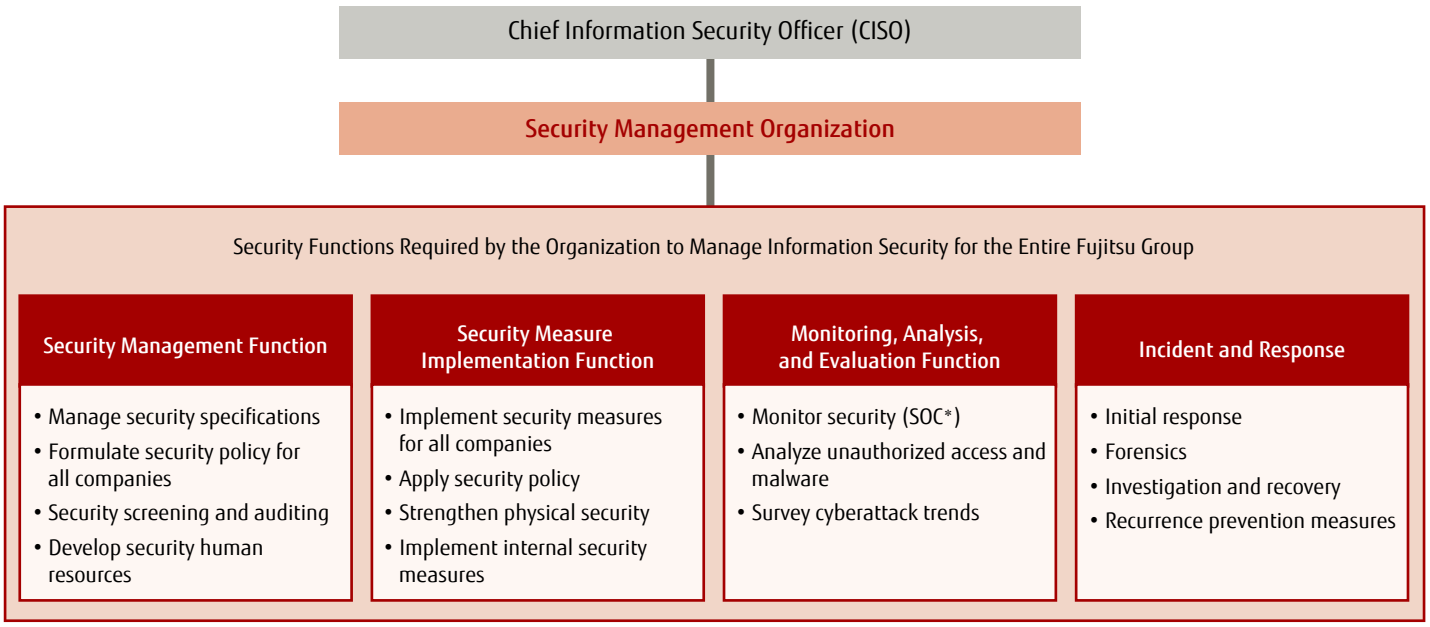
Security Management Organization

The Security Management Organization is an organization under the direct control of the CISO for strengthening the Fujitsu Group's information security measures. It drafts common Group rules, measures, and plans on information security, and is also in charge of integrated management. Specifically, it is in charge of the Fujitsu Group's security management; security measure implementation; security monitoring, analysis, and evaluation; and incident and response functions.

Regional CISO

Regional CISOs are the chief information security officers located in each of the five regions, and are granted the highest authority and responsibilities for information security within their regions. These officers formulate information security measures for the regions under their authority, and promote the reliable execution and reporting of information security measures implemented by Group company security teams.

Security Management Organization Functions



*SOC: Security Operations Center

Security Management

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 and implements information security measures. Under the shared global Fujitsu Group Information Security Policy, we have set forth information management and information security regulations for Group companies.

Each overseas Group company creates and establishes rules and policies in accordance with the regulations of its country.

Security Screening

The Fujitsu Group conducts security screenings when connecting to our intranet, including at new company launches. Specifically, we perform onsite surveys and verify security risks according to the security conditions prescribed by ISO 27001.

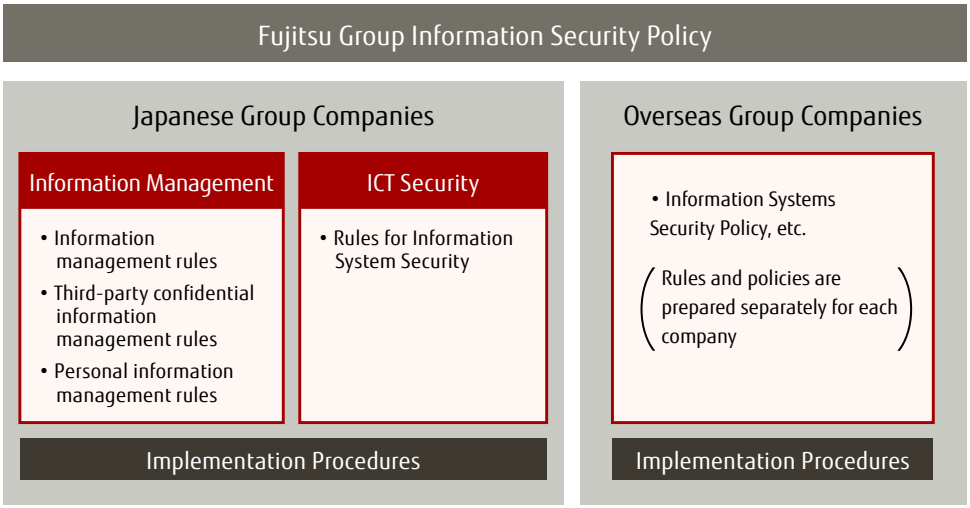
In addition, we maintain safety by screening for security vulnerabilities when servers are connected to the Internet, and also periodically confirm vulnerability afterwards.

Security Auditing

The Fujitsu Group conducts information security audits of our worldwide business departments. These audits are performed by an audit department that is independent from the business department. They specifically investigate information management operation status and ISMS conformance.

The audit results are provided as feedback to each business department and are used to increase information security.

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

Developing Security Human Resources

Information Management Training

To prevent information leakage, it is essential that we not only make employees aware of regulations, but also that each employee improve their information security awareness and skills. To that end, Fujitsu and domestic Group companies provide information management training to employees. Specifically, all employees (including officers) participate in annual e-Learning. New employees and those receiving promotions also receive information security training.

Overseas Group companies conduct yearly information security training for their employees, and information security managers are also given security training for managers.

Raising Information Management Awareness

In 2007, we formulated our shared slogan for the domestic Fujitsu Group: "Declaration for complete information management! Information management is the lifeline of the Fujitsu Group." We are working to raise awareness of information management, specifically by hanging informational posters in the business offices of Fujitsu and domestic Group companies, and also implementing measures such as putting stickers on the work computers of all employees.

We also use our intranet portal to share information about the frequent security leaks across the world and encourage employees to pay attention to information management. Furthermore, the monthly security check day is for managers to confirm the status of security measures in their departments.

Information Management Handbook

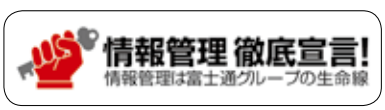
The proper handling of information is the foundation of the Fujitsu Group's corporate activities, as well as our lifeline.

The Fujitsu Group establishes information security regulations and implements security measures to prevent issues caused by information leakage.

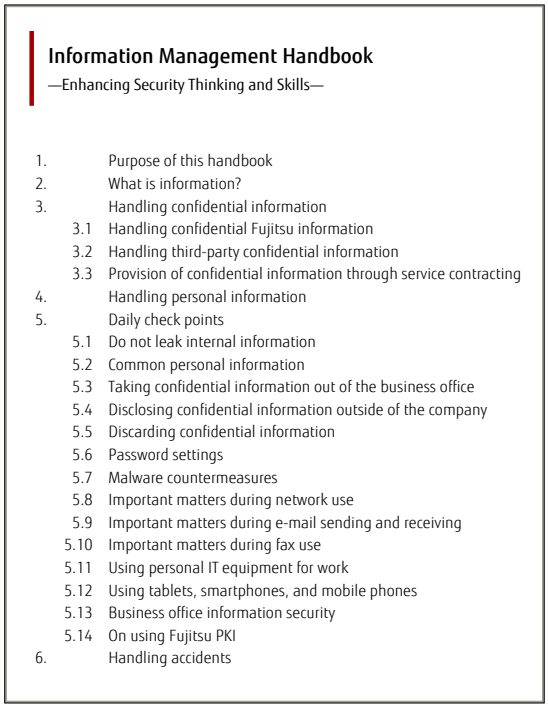
The Information Management Handbook is published to enhance understanding of information management according to these regulations. It also provides immediate answers to information management-related questions.

e-Learning screen

Declaration for complete information management sticker



Information Management Handbook



Information Management Handbook
—Enhancing Security Thinking and Skills—

Security Measures

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

Cyberattacks, exemplified by advanced persistent threats (APTs), are becoming increasingly sophisticated, diverse, and complex in recent years. Conventional, single-layer security measures are no longer able to completely defend against these attacks.

The Fujitsu Group has adopted the "defense in depth"—a multilayer defense mechanism that utilizes several different measures instead of one—as its basic concept for information security. Defense in depth has three goals: preventing attacks by raising multiple defensive barriers, rapidly detecting attacks by establishing multiple detection functions, and minimizing damage after infiltration. With a combined defense of this type, we can prevent attacks and minimize damage.

The Fujitsu Group has adopted three priority security measures to protect internal information: information management, aimed at protecting information; cybersecurity, centered on measures to guard systems against cyberattacks; and physical security, which prevents unauthorized access to offices, factories, and other facilities.

Security Measure 1: Information Management

Information Classification

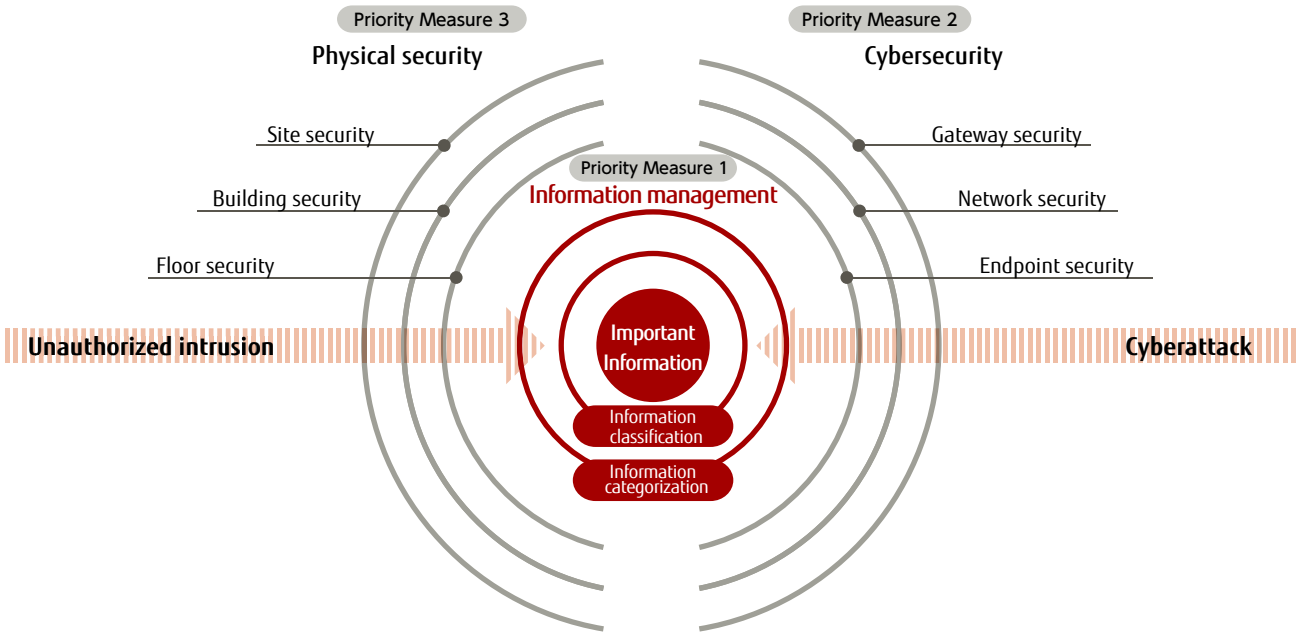
The domestic Fujitsu Group has formulated information management rules on the handling of information circulated internally. In this way, we classify, properly manage, and operate internal information circulation.

Similarly, overseas Group companies also classify and manage information according to the circumstances in their countries. Internal-use-only and restricted information are managed according to the information management rules, and third-party confidential information is managed according to the third-party confidential information management rules.

Information Categorization (Classifying Public and Confidential Information)

The Fujitsu Group categorizes classified information based on the level of care its handling necessitates according to legal requirements, value, importance, and other qualities. Information is protected by taking security measures in line with each category.

Defense in Depth Conceptual Image



Information Protection Management Systems

Domestic Group companies carry out autonomous activities at work sites to properly safeguard third-party confidential information and our confidential information. Specifically, these include establishing suitable management and implementing information-protection efforts based on different customers and clients (such as rules for different industries and business categories) and audits by in-house, third-party organizations.

In this way, they work to build information protection management systems to confirm initiative status and improve their protection of information.。

Personal Information Protection

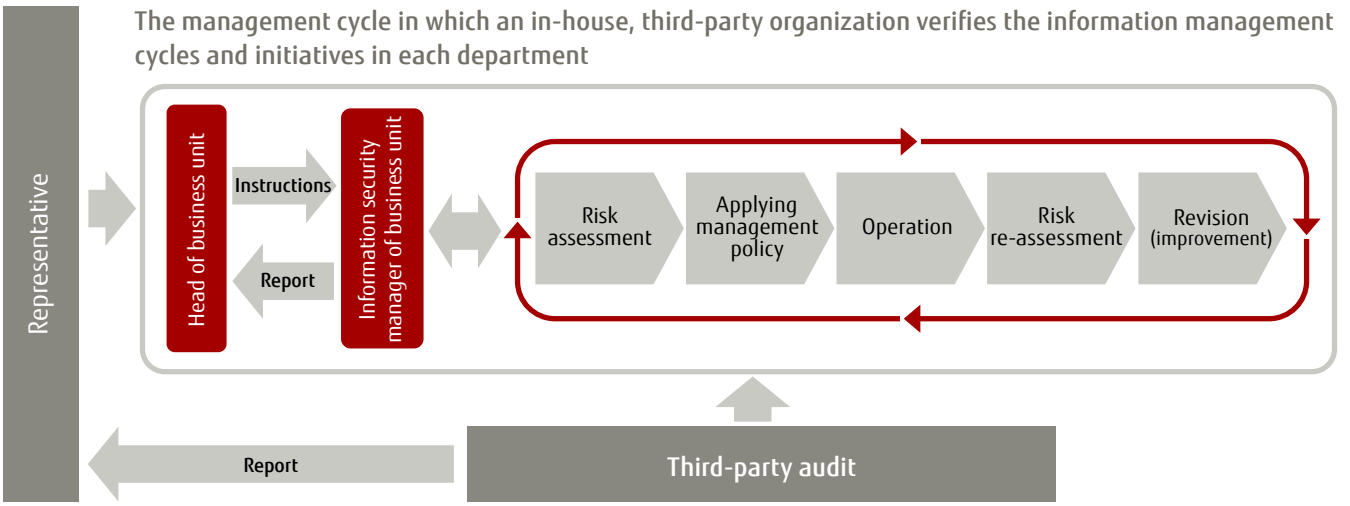
As more data is circulated around the world, Fujitsu Group companies are working to strengthen their safeguarding of

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 Protection Management Systems



personal information for safer, smoother information protection.

Fujitsu earned the PrivacyMark in August 2007. We are also working to continually enhance our personal information protection, including annual training and audits on personal information handling.

Domestic Group companies also acquire the PrivacyMark as needed and implement thorough personal information management. Privacy policies, based on the laws of each country and social demands, are posted on the websites of overseas Group companies.

PrivacyMark

Fujitsu received PrivacyMark certification from the JIPDEC. The PrivacyMark is granted to business operators that appropriately handle personal information under personal information protection management systems that conform to JIS Q 15001:2006.

PrivacyMark

GDPR Response

In order to respond to GDPR, the Fujitsu Group is working to strengthen protection of personal data throughout our entire Group, mainly via the following initiatives.

Building A Global Structure

We have built a GDPR-based global personal information protection structure with approval from the Risk Management and Compliance Committee, the supreme decision-making body for risk management and compliance under the direct control of the Board of Directors.

Development and Awareness-Raising for Internal Rules, Etc.

Under the guidance of the CISO organization and legal departments, we have cooperated with the EMEIA region, etc., in order to develop internal rules such as guidelines related to the protection of individual rights in response to GDPR and check sheets for the formulation, design, and initial setting of systems and/or services. We also updated the operation process with the rules and held employee training.

Response to Regulations on Transfer Outside of EU

In response to regulations on the transfer of personal data outside of the EU, we applied to the Dutch Data Protection Authority (DPA) in December 2017 for our Binding Corporate Rules for Processors (BCR-P), which are common rules established across the Fujitsu Group related to the handling of personal data that customers have entrusted to the Fujitsu Group for processing.

* General Data Protection Regulation (GDPR): The GDPR (EU regulations requiring companies, organizations, and groups to protect personal information) was enacted on May 25, 2018. It includes regulations on transferring personal data out of the European Economic Area and the obligation to report data leaks within 72 hours. Companies, organizations, and groups in violation of the GDPR may face a fine of up to 4% of their overall group's annual revenue or 20 million euros, whichever is greater.

Security Measure 2: Cybersecurity

The Fujitsu Group implements separate measures at multiple layers based on network characteristics to prepare for cyberattacks. We are working to protect against increasingly sophisticated, diverse, and complex cyberattacks via our "defense in depth" security. This combines gateway security measures, including firewalls and advanced persistent threat (APT) measures; network security measures, such as unauthorized access detection; and endpoint security measures, including malware measures and security patch management.

Gateway Security Measures

To defend against cyberattacks, it is essential to prevent intrusion from the outside. The Fujitsu Group has installed gateways at the border between the external Internet environment and the Fujitsu Group internal information networks to block unessential communications from outside and ensure security. Specifically, we have adopted firewalls to guard against unauthorized access to the border with the Internet layer and an unidentified malware detection system as an advanced persistent threat (APT) countermeasure. We also monitor e-mail and web communications as entrance/exit measures.

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 re-verify all e-mails sent outside the company using automated recipient identification and automatically confirm external transmission eligibility. This prevents users whose work does not require external e-mail communication from sending e-mails or leaking information outside of the company.

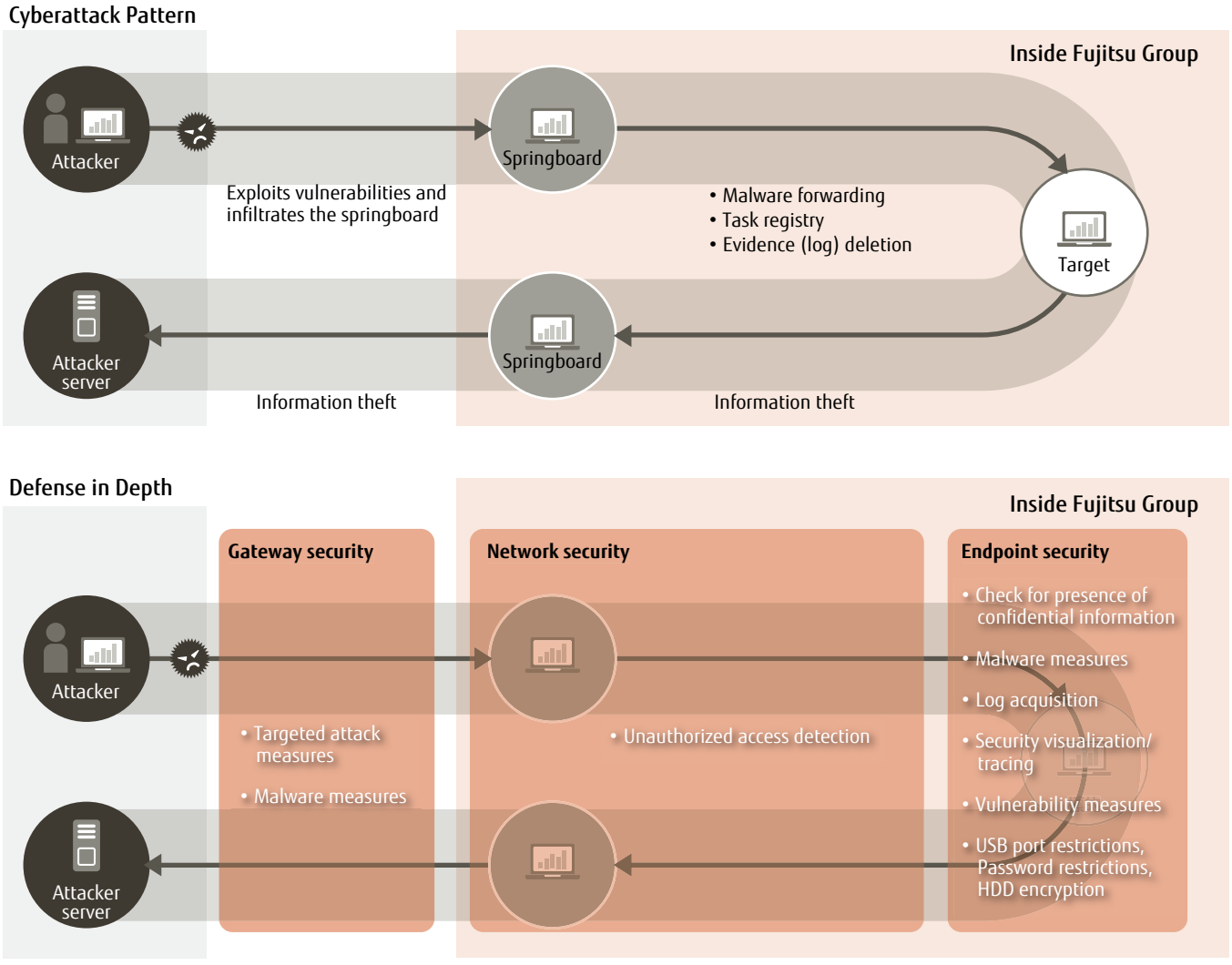
Web Access Security

To ensure safety, all access to the Internet 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 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 computer or smart device. We encrypt communications over the access routes and utilize two-factor authentication to prevent unauthorized access and ensure security. As a work-style reform initiative, we introduced virtual desktops and provide an environment for remote working that maintains security by preventing data from remaining on the computer being used.

Cyberattack and Defense in Depth Cybersecurity Measures



Network Security Measures

Conventional cyberattack countermeasures are focused on gateway (entrance) measures that block intrusion from outside. But with advanced persistent threats (APTs) and other increasingly sophisticated cyberattacks in recent years, it is becoming difficult to fully protect against intrusions from cyberspace with this approach, and internal measures to rapidly detect threats in internal networks are essential.

The Fujitsu Group has installed devices that detect unauthorized internal communications as a way to discover suspicious communications on our internal networks. We are also verifying new technologies under development through in-house implementation as a step towards commercialization and practical application.

Endpoint Security Measures

Advanced persistent threat (APT) e-mails and other cyberattacks targeting endpoints (such as computers and mobile devices) are increasing in recent years, requiring further measures compared to the past.

The Fujitsu Group has also incorporated our "defense in depth" concept into security measures for endpoints used by employees. We implement the necessary security measures in each endpoint layer, including malware measures, log acquisition, and HDD encryption.

To prevent information leakage, we use virtual desktops and thin-client devices that cannot save data. The data that was previously saved on individual employee computers is unified and centrally managed in department and individual storage for heightened security.

For computers other than thin clients, we take measures so data cannot be saved on the computer. We have also introduced IT Policy N@vi and prevent employees from taking information out of the company by limiting USB devices, such as USB memory and portable disks used for work.

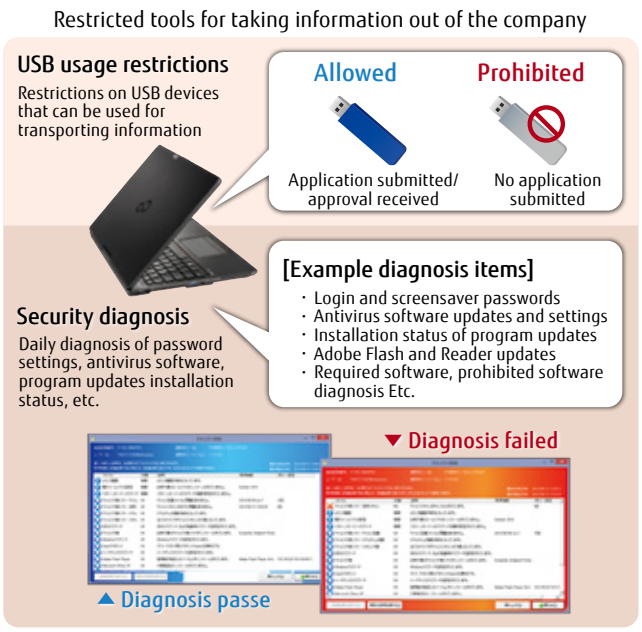
In addition, computers with OS and software that are no longer supported are forcibly isolated from the network to reduce security risks.

Individual employees previously implemented various security measures on their computers, but we have reduced this burden by using standard computers and thin-client devices with these endpoint security measures. We are also working to improve security through the centralized management of endpoint security, which is standardized in the organization.

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

Overview of Restricted Tools for Taking Information Out of the Company



Authentication Security Measures

We have introduced IC cards, called "security cards," for employee authentication and other purposes. The security cards are printed with their name and facial photograph. The IC chips include their name, employee number, and employee Public Key Infrastructure (PKI) certificate and key. These are managed by the human resources department, which guarantees that the card user is a legitimate employee. These cards are used for reliable identity verification, system login verification, and electronic document approval that has the same effect as stamping a sanctioned seal on paper documents.

We have also introduced palm vein authentication and one-time passwords (OTP) to some usage scenes.

Security Measure 3: Physical Security

We also implement measures according to the "defense in depth" concept for physical security—the third priority measure after information management and cyber security. Specifically, we have built a physical security environment combining human guards and mechanical security in three layers: sites, buildings, and floors.

We safeguard important information from unauthorized physical invasions in this way. Overseas companies also implement similar physical security measures in line with the circumstances of their country.

Physical Security Policy

We are enhancing physical security with a combination of human guards, security gate card readers, and surveillance cameras.

1	Prevent the intrusion of unidentified, suspicious persons
2	Prevent straightforward incursions by malicious persons (including terrorism)
3	Manage entry/exit by employees and visitors
4	Leave evidence of information improperly carried out by employees
5	Create a high-security environment with ICT

Introducing Cutting-Edge Technologies

To build more advanced physical security environments, proof-of-concept tests are currently underway at some in-house offices. These tests use security gates with vein authentication devices that can prevent identity impersonation.

Security gate using palm authentication

Security Monitoring, Analysis, and Evaluation

Security Monitoring

We record roughly one billion logs per day using security monitors located around the world. Efficiently and effectively controlling these logs is essential for information security management.

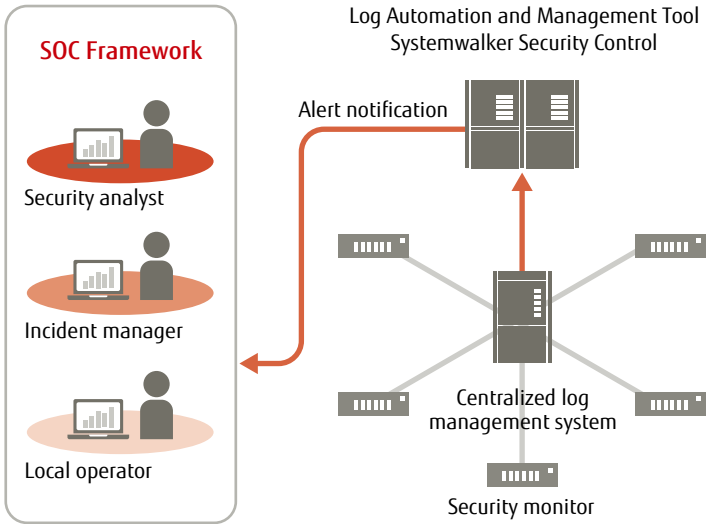
The Fujitsu Group has established a Security Operations Center (SOC) that functions 24 hours a day, 365 days a year to create a structure for fast, accurate incident and security alert responses. The logs generated from the security monitors installed in multiple locations within the company's network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

The SOC is comprised of local operators, incident managers, and security analysts, who analyze the details of the alert notification e-mail; determine the quality, scope, and seriousness of the threat; rank the response priority; and handle the threat quickly and accurately.

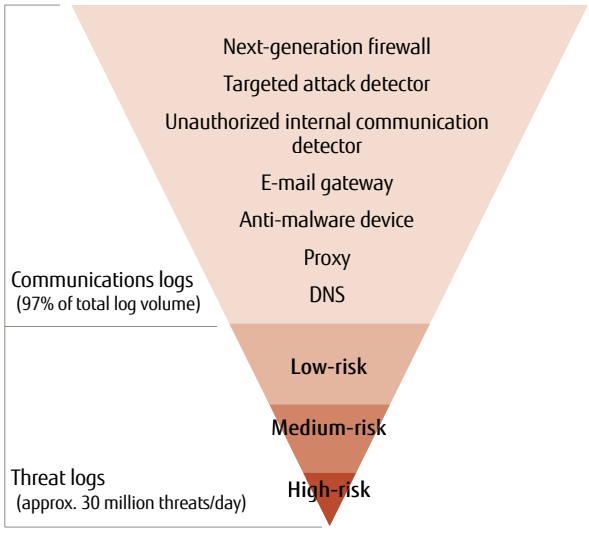
Surveying Cyberattack Trends in Cooperation with External Institutions

To cope with the threat of changing cyberattacks, we share information with external institutions to predict cyberattacks, respond to threats based on actual attack information, minimize risks, and prevent incidents.

Security Monitoring (SOC) Framework



Security alert classifications



Incident and Response

Initial Response

The Fujitsu Group has established a force specialized in incident response for cyber security under the command of the CISO. When an incident occurs, this force collaborates with the SOC to identify the affected equipment and promptly isolate and remove it from the network to minimize damage. It also communicates with related departments to build a response structure. This force verifies various possibilities and takes measures against secondary damage to keep the damage from spreading.

Forensics

Evidence is preserved* using specialized devices on the equipment that was isolated from the network during the initial response. Copies of the preserved evidence, as well as alerts and logs obtained by the SOC, are analyzed to identify the damage, causes, and extent of impacts.

* Preservation of evidence: Cyberattack traces must be swiftly collected and analyzed to identify the incident's causes and damage. Electromagnetic evidence (hard disks, logs, etc.) is preserved (including copying) from equipment involved in the incident to ensure these traces are not lost.

Research and Recovery

Forensics, unauthorized program analysis, and other methods are used to ascertain information for identifying impacts and taking measures based on the risks. At the same time, the causes are elucidated and threats are removed. Recovery is performed starting with areas for which safety has been confirmed.

Expansion of Measures to Prevent Re-occurrence

The circumstances are reported to the Risk Management and Compliance Committee. Moreover, investigations and audits on similar incidents are carried out under the CISO. Company-wide measures to prevent re-occurrence are implemented in cooperation with related departments.

Special Feature

Work-Style Reform Leveraging ICT and Information Security

The Fujitsu Group is promoting work-style reform through ICT, such as strengthened information security. The results of this implementation are offered as services to help customers reform their work styles as well.

Fujitsu's Work-Style Reform Leveraging ICT

Due to globalization and changing labor structures (including employee ages), flexible work styles are needed nowadays so diverse individuals can be active and make use of their skills. To support digital innovation by customers through Connected Services (our Management Direction), the Fujitsu Group is shifting to work styles that support co-creation with customers, innovation creation, business speed improvement, and digitalization. We are also making proactive efforts for employee growth and improved productivity, including the further improvement of expertise. One facet of this is Fujitsu's work-style reform aimed at each individual being able to produce value in limited amounts of time by leveraging ICT, such as strengthened information security.

In FY 2010, the Fujitsu Group began full-scale efforts to promote work-style reform to support balance between child rearing, caregiving, and work. Since FY 2011, we have introduced our Global Communication Platform* encompassing overseas Group companies and are implementing work-style reform in terms of both system innovation and ICT utilization.

In April 2017, we officially introduced our telework system utilizing ICT—such as thin-client computers, virtual desktops, and the Global Communication Platform—for all employees. It is expected that this program will enable flexible work styles in tune with work characteristics and circumstances in any location (including homes, satellite offices, business trips, and during travel), and also help improve productivity.

The Fujitsu Group will continue verifying and revising our teleworking and other systems with the thorough utilization of ICT. We are working to transform the awareness of management and employees. We have also summarized the results, new realizations, and know-how from implementing work-style reform as our Seven Approaches. We will offer services for implementing work-style reform—from planning to solution adoption and operation—and contribute to customers' work-style reform.

* Global Communication Platform: A global communication infrastructure system including e-mail, portal sites, document management, teleconferencing, telephone calls, social media, video, etc.

Seven Approaches for Work-style Reform

Determine a vision

Depict future work styles to turn ideals into reality

Communication reform

Smoother information sharing over distances

Utilization of teleworking

For consistent work at any time or place

Establish new work styles

Change each individual's time-related awareness and actions

Digitalize office spaces

Digitalize office spaces to optimize work environments

Mobile work support

Change work styles to improve productivity

Select devices based on the worker

Optimal devices for each place and task

Security
Technology

Large-Scale, In-house Implementation of Palm Vein Authentication for Stronger Security and Greater Convenience

Used for Virtual Desktop Login and Security Gates

The Fujitsu Group is switching from passwords to palm vein authentication for login authentication on virtual desktops, one facet of our work-style reform. We are expanding the palm vein authentication system to roughly 80,000 domestic Group employees starting from 2018.

With palm vein authentication, the user merely scans their palm with a vein authentication device installed inside or attached to the outside of a computer terminal. The device is instantly unlocked with no need to enter a password. This system is made for stronger security and better convenience; palm veins are difficult to reproduce, so there is no risk of password leakage. It is also accelerating teleworking and other diverse work styles.

We have also switched from employee cards to palm vein authentication on the security gates inside two large offices, and are conducting a proof-of-concept test for 5,200 employees at these two offices. Based on these results, the Fujitsu Group is striving to expand this authentication to gates and doors at other business offices and build advanced physical security that prevents identity impersonation.

Vein authentication device　Near infrared image　Vein pattern image

The World's First Palm Vein Authentication System

Fujitsu developed the world's first palm vein authentication method. This contactless vein authentication can read vein patterns on the palm to authenticate the individual. This secure, safe biometric authentication technology safeguards personal information while improving convenience and security.

Fujitsu's Personal Authentication Platform server is used as the palm vein authentication and management infrastructure to build a cloud-based system for both virtual desktop login and security gate authentication. A sophisticated image enhancement technology instantly compares the data read from the palm vein authentication device and the vein data of 80,000 employees registered in the Personal Authentication Platform. This enables accurate, prompt authentication.

Virtual desktop login authentication

Security gate authentication

Published by

FUJITSU LIMITED

Corporate Affairs & Risk Management Unit

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