Fujitsu Group Information Security Report 2015

FUJITSU

shaping tomorrow with you

CONTENTS

Fujitsu Group Information Security Report 2015

Report Summary

Target Period and Scope of the Report

This report covers the period up to March 2015 and focuses on efforts in information security by the Fujitsu Group.

Report Publication Date

This report was published in August 2015.

Fujitsu Information Security: Our Vision and Reality

"Creating a safe, pleasant, networked society" and Information Security

The Fujitsu Group established the "FUJITSU Way" as the Group's philosophy and principles. We are strongly aware of the change in the role and responsibility of the corporation in society, and established the following corporate philosophy to indicate the significance of the existence of the Fujitsu Group.

Corporate Vision

Through our constant pursuit of innovation, the Fujitsu Group aims to contribute to the creation of a networked society that is rewarding and secure, bringing about a prosperous future that fulfills the dreams of people throughout the world.

ICT (Information and Communication Technology) connects the world's people and creates a variety of ideas and opportunities. On the other hand, we are confronted by new issues due to the rapid proliferation of ICT. Preparation against the increasing number of cross-border cyber-attacks and assured protection of private and confidential information are items companies and organizations should respond to urgently. At the Fujitsu Group, we use technologies nurtured through our own systems operations as a base for responding to these types of problems while collaborating with a variety of related organizations.

The Fujitsu Group has a vision of a "Human Centric Intelligent Society" where anyone can use ICT to draw out their maximum potential in a world where society has sustainable growth. We think it is our social responsibility as a global ICT company to use the power of ICT to contribute to the realization of a sustainable earth and society and maintain and reinforce a safe and secure digital society.

Guided by this vision, the Fujitsu Group will continue to promote various information security initiatives to support tomorrow's intelligent society. In the FUJITSU Way, we require employees to maintain confidentiality as stipulated by the Code of Conduct, which sets forth rules and guidelines followed by everyone in the Fujitsu Group. At the same time, we have established the "Fujitsu Group Information Security Policy" that applies both in Japan and internationally. In addition, we have put in place regulations concerning information security based upon this policy. We have applied the rules to the entire Fujitsu Group, and strive to ensure compliance with each of these rules.

Furthermore, the Fujitsu Group also has a unified information security management system in place to thoroughly manage information and enhance information security. On the other hand, given that we are developing businesses across an expansive range of fields, we have also put in place an information security management system at the business division level. This is to ensure that we can swiftly address varying information management and information security issues, as required by the characteristics of individual businesses.

This "Information Security Report 2015" presents the Fujitsu Group's information security-related activities. We trust that this report will give you a stronger understanding of our commitment to information security.

Masami Yamamoto

Representative Director
Chairman
Fujitsu Limited

Fujitsu Group's Information Security

Under the corporate governance system, the Fujitsu Group promotes appropriate information management and information usage according to Group rules, as part of risk management.

» Corporate Governance and Risk Management

Corporate Governance

The main emphasis of Fujitsu's corporate governance is on having the non-executive directors provide oversight and advice to executive directors in their management execution role within the Board of Directors, while adopting the Audit & Supervisory Board system.

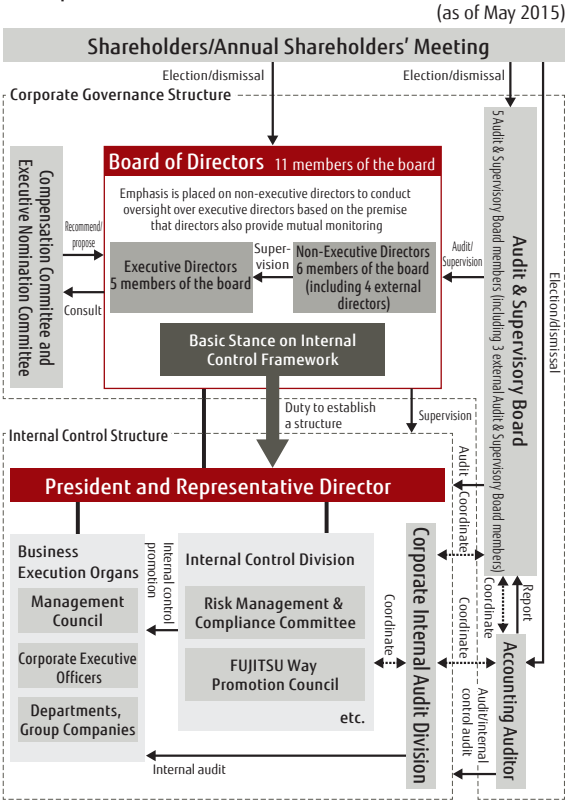
Specifically, while assuming mutual supervision between directors and oversight of directors by the Board of Directors, Fujitsu makes a clear distinction between the management execution role and the management oversight role on the Board of Directors and, moreover, makes sure that there are at least as many non-executive directors responsible for management oversight as there are executive directors responsible for management execution.

In addition, in selecting candidates for non-executive directors, consideration is given to the candidate's backgrounds and insight into Fujitsu's business so that effective advice that reflects a diversity of viewpoints can be obtained.

Furthermore, Audit & Supervisory Board members provide audits and oversight from the outside of the Board of Directors, and Fujitsu has established the Executive Nomination Committee and Compensation Committee of its own accord, thereby augmenting the Board of Directors. The overall approach is designed to raise shareholder value through effective corporate governance.

Corporate Governance Structure

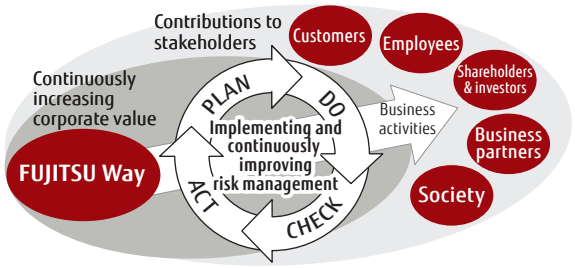
(as of May 2015)



Risk Management

Through its global activities in the ICT industry, the Fujitsu Group continuously seeks to increase its corporate value, and to contribute to its customers, local communities and all other stakeholders. Management places a high priority on properly assessing and dealing with risks that threaten the achievement of our objectives, taking steps to prevent the occurrence of these risk events, and establishing measures to minimize the impact of such events if they do occur, and prevent their reoccurrence. Moreover, we have built a risk management and compliance system for the entire Group and we are committed to continuously implementing and improving it.

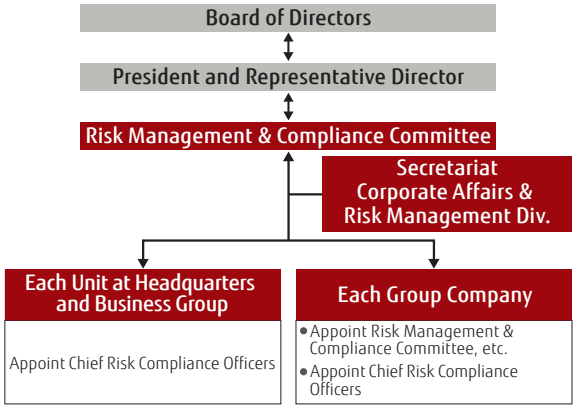
Implementing and Continuously Improving Risk Management



With the aim of integrating and strengthening its global risk management and compliance structures, the Fujitsu Group has established a Risk Management and Compliance Committee as an internal control committee that reports to top management.

The Risk Management & Compliance Committee appoints a Chief Risk Compliance Officer for each department and company throughout the Group, and encourages them to cooperate together both to guard against potential risks and to mitigate risks that materialize, thereby forming a risk management and compliance structure for the entire Group.

Risk Management & Compliance Structure



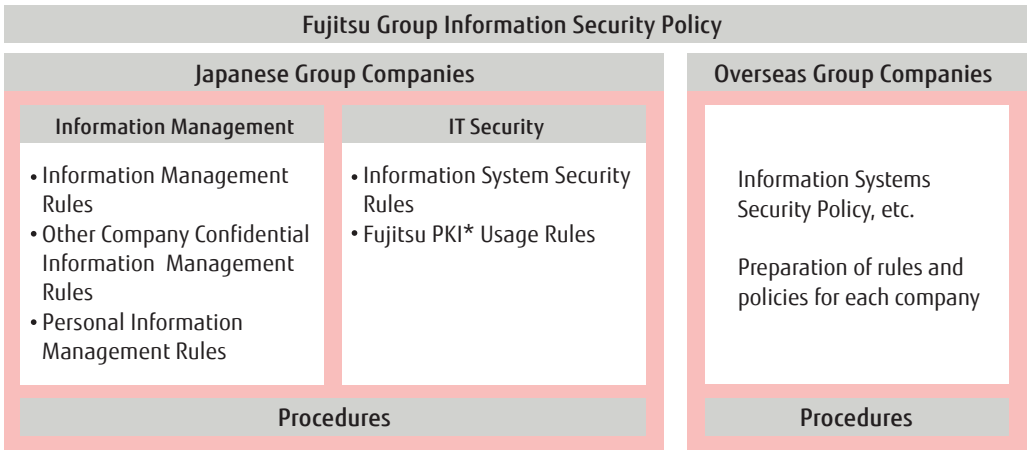
» Promotion of Information Security

Information Security Policy and Related Rules

The Fujitsu Group "seeks to be the customer's valued and trusted partner and build mutually beneficial relationships with business partners," and to enforce "confidentiality" as an essential part of social responsibility. The Group has established the "Fujitsu Group Information Security Policy" and promotes information security.

The Fujitsu Group uses the Information Security Policy Formulation Guidelines to abide by information security-related regulations, taking into account the laws and systems in various countries and ensuring compliance with the policies in each Group company. It also uses the Global Information Security Management Framework to select, decide on and implement information security measures, as well as to evaluate and improve them.

↓ Framework of Information Security Rules



* PKI: Public Key Infrastructure. Rules governing authentication of individuals, encryption, etc.

Fujitsu Group Information Security Policy

1. Objectives

Fully recognizing that information provides the basis for the Fujitsu Group's business activities and the risks that accompany the management of information, the Fujitsu Group conducts information security measures to achieve the objectives set forth below. In doing so, we seek to realize the Corporate Values of the FUJITSU Way, namely, "We seek to be the customer's valued and trusted partner" and "We build mutually beneficial relationships with business partners." At the same time, we will strive to maintain "confidentiality" as stipulated by the Code of Conduct as an essential part of our social responsibility.

(1) The Fujitsu Group properly handles information delivered by individuals, corporate clients or vendors in the course of its business to protect the rights and interests of these parties.
(2) The Fujitsu Group properly handles trade secrets, technical information and other valuable information in the course of its business to protect the rights and interests of the Group.
(3) The Fujitsu Group properly manages information in the course of its business to provide products and services in a timely and stable manner, with the view to maintaining its roles in society.

2. Activity Principles

The Fujitsu Group applies the following principles when conducting information security activities.

(1) Preservation of confidentiality, integrity and availability shall be the objective of information security, and information security measures shall be planned to meet this objective.
(2) The organizational structure and responsibilities shall be clearly defined to ensure the proper implementation of information security measures.
(3) The risks that accompany the handling of information and investments required for the measures shall be taken into consideration to properly implement the information security measures.
(4) Information security processes shall be organized into Plan, Do, Check and Act phases to maintain and enhance the level of information security.
(5) Executives and employees shall be provided with awareness and educational programs on information security and act with the knowledge of its sensitive nature to ensure the proper implementation of information security measures.

3. The Fujitsu Group's Measures

To ensure the implementation of information security measures based on the aforementioned objectives and activity principles, the Fujitsu Group shall prepare and implement related rules.

Promoting Information Security Education

We think it is important to not only inform employees of the rules but also to improve security awareness and the skills of each staff member in order to prevent information leaks. We therefore conduct face-to-face information security education during training of new recruits and training for promotions and advancement of employees of Fujitsu and our domestic Group companies, and conduct annual e-learning for all employees, including executives.

↓ e-Learning Screenshot

Raising Awareness Regarding Information Security

Guided by a common slogan that translates as "Declaration for complete information management! Information management is the lifeline of the Fujitsu Group," Fujitsu and domestic Group companies have been working to increase information security awareness at the individual employee level by displaying awareness posters at respective business locations, affixing information security awareness stickers to all business computers used by employees and implementing other measures.

Also, a tool was introduced to prevent e-mails from being accidentally sent outside the Company, and in parallel with promoting the use of ICT, we increased the awareness of information security among individual employees.

↓ Awareness-Raising Sticker: "Pledge to Enforce Rigorous Information Management" (in Japanese)

Information Security Seminars for Business Partners

The risk of information leakage is ever increasing in response to the drastically changing ICT environment in recent years. Accordingly, the Fujitsu Group has been holding information security seminars for business partners to whom it outsources software development and other services, as well as for Group employees.

Enhancing Personal Data Protection Systems

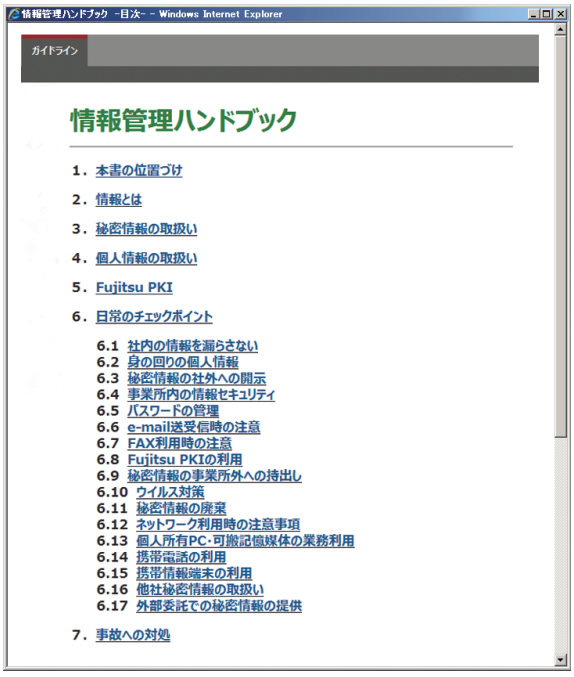
Fujitsu has established the "Personal Information Protection Policies" and "Personal Information Management Rules." We are also continually strengthening the system for protecting personal information based on these rules, such as by conducting annual training and audits on the handling of personal information.

In August 2007, Fujitsu acquired Company-wide PrivacyMark certification and renews this certification every two years. Domestic Group companies also acquire PrivacyMark certification individually as necessary and promote thorough management of personal data. Overseas Group companies also publish privacy policies that meet their various national legal and social requirements on their main public Internet websites.

Other Support

An "Information Management Handbook" has been issued to increase understanding of internal rules related to information management. This handbook can also be referenced over the intranet, allowing for immediate confirmation of any information management questions. In addition, the intranet is used to bring attention to information leaks by introducing some of the many incidents of information leakage from around the world. Furthermore, a security check day is held once a month to allow managers to verify the status of security measures in their own divisions.

↓ "Information Management Handbook" Screenshot (in Japanese)



Information Security Personnel Training: The Security Meister*1 Certification System

Cyber-attacks are becoming a social problem. Going forward, cyber-attacks are expected to become highly advanced and increasingly sophisticated with the introduction of the National Identification Number System (social security and tax number), and as society moves towards the age of the Internet of Things in which 50 billion devices will be connected to the Internet. Fujitsu, being in the front lines of system integration and service operations, is engaged in the training and development of information security personnel to improve the quality of its security and to realize solutions with robust security systems.

The Necessity of Training Professional Information Security Personnel

Threats related to cyber-attacks such as serious damage brought about by targeted attacks on companies and organizations are becoming diversified and sophisticated. With this in mind, one of Fujitsu's efforts to protect the information assets of its customers from those threats involved launching a system to search within the Fujitsu Group for engineers with a high level of security skills so that they can be trained and certified, and eventually dispatched in the field.

The Security Meister Certification System

Security specialists who can implement security measures to protect information systems from cyber-attacks will undergo systematic and continuous training, and be certified as Security Meisters. In this system, specialists are grouped into three categories, namely Field, Expert, and High Master, according to the functions and requirements of the job. There is a plan to train and certify 700 engineers by the end of fiscal 2016.

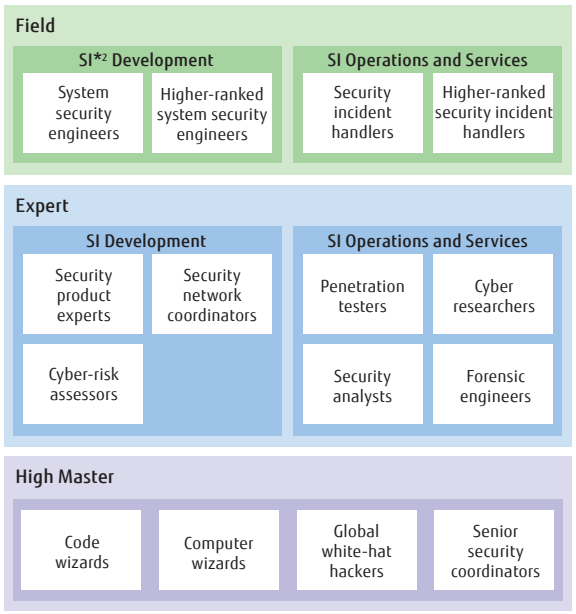
*1 The Security Meister Certification System is the official name of Fujitsu's personnel training system. The word "Meister" is of German origin which refers to a person who has extensive theoretical knowledge and practical skills in their profession.

Three Security Meister Categories

Defining the Types of Security Engineers

The Security Meister Certification System defines the types of security engineers who can adapt to the needs of ICT development and operations today. The 15 types of security engineers grouped into three categories defined by the various requirements of ICT development and operations are outlined in the model below.

Security Meister Model



In realizing this model, Fujitsu takes into consideration its consistency with Japan's IT skill standards and various security personnel models available overseas. Furthermore, High Master is defined as being equivalent to a white-hat hacker*3 or Top Gun*4.

*2 SI: System Integration
*3 White-hat hacker: Hacker who identifies security risks
*4 Top Gun: Security engineer with an advanced level of expertise

The following are examples of types of security engineers with their respective definitions. A System Security Engineer in the Field category is assigned to the Systems Development Division and is in charge of on-site security design and implementation of technical security countermeasures.

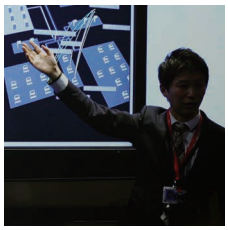
A Security Incident Handler is assigned to the Systems Operation Division and is in charge of the system security operation design and implementation of security countermeasures concerning information security incidents that occur on-site.

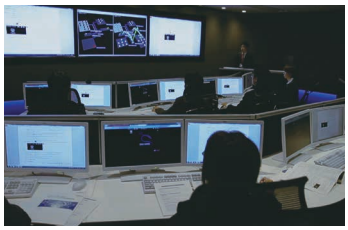
A Computer Wizard in the High Master category is assigned to the Development Division of embedded systems, can conduct original research and share and disseminate information by leveraging their technical capabilities. This kind of personnel utilizes cutting-edge security technology, is self-motivated and expected to participate in and give presentations at external organizations' events (including research and security seminars for local engineers).

Establishment of Training Programs

As part of establishing training programs for security engineers with emphasis on practical applications, Fujitsu has opened specialized training courses that correspond to each type of security engineer. A training program conducted in a cyber-range (virtual training area) has been newly set up. Fujitsu makes these training courses available to each of its customers.

A training scene





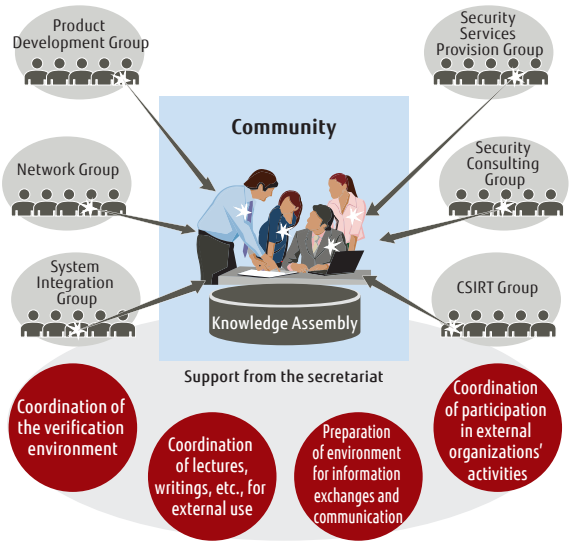
Searching for Capable Security Personnel and Increasing Their Number

Fujitsu is promoting the discovery of personnel with security skills and growth in the number of security engineers. Fujitsu also strives to consolidate knowledge and information from various divisions within the Company and has formed a Security Meister Community for the effective utilization of gathered resources. Experts sharing their knowledge within the community will result in the enhancement of their skills after they have been certified.

A security contest that includes hacking techniques is also being held internally. The security contest also utilizes the cyber–range, allowing 40 engineers to showcase their technical capabilities as they compete against each other at the same time.

In this manner, Fujitsu offers its customers safety and security as it proactively conducts security-related training.

Security Meister Community



Fujitsu's First Cyber Security Contest

Fujitsu held the "Fujitsu Cyber Security Workshop 2014" in December 2014 with 160 participants as part of its initiatives to enhance the technical capabilities of security engineers within the Fujitsu Group and to foster interaction among them.

The morning seminars with the theme of "Frontline of Security" were held in two locations with the executive management, managers and on-site engineers giving their respective insights.

In the afternoon, Fujitsu's first ever security contest was held with 20 pairs competing against each other, showcasing their skills in hacking and knowledge of security.

The security contest differs from the usual CTF (Capture the Flag) contests and involves various schemes and ingenuity.

The secretariat created about 70 unique problems with the cooperation of High Masters with advanced security skills. In addition to tasks requiring practical application of security technology such as finding an answer (a flag) somewhere on a web server or in packet data on a network, there were quiz-type questions covering extensive security areas.

There were also tasks related to social hacking, which require skills in wheedling or shoulder-hacking to acquire necessary information from the target.

By showing the progress of the contest through a dashboard specially designed for the event, contestants were not only able to showcase their skills, but the audience in another room were given real-time updates and explanations of the problems being solved at the same time, aiming to enhance the security capabilities of every attendee.

Among the impressions and comments given by participants included: "I haven't actually been using my skills as much as I would have liked, so being able to participate was great," "Now I know what I am capable of," "I want an archive of the questions," "I hope we can have an interdepartmental contest," and "Please set up a write-up site (to explain the questions)."

Going forward, Fujitsu will continue holding this contest as part of its initiatives to enhance the technical capabilities of cyber security personnel and to foster interaction among them.

Scene from the cyber security contest

IT Security Efforts

In situations where ICT is applied, the large volume of data related to business is collected and made easily accessible. This is accompanied by various risks such as the risk of information being leaked, damaged, or unavailable.

For this reason, the Fujitsu Group has positioned IT security, which seeks to ensure the secure management of information when using ICT, as a common Group-wide theme, and is working towards this end.

» Pursuing IT Security to Support Business Operations

At the Fujitsu Group, IT security aims to support business operations, without interfering with the convenience or efficiency of business.

If rules for information security measures are too excessive, employees will struggle to understand and observe them, making compliance impractical.

The Fujitsu Group strives to incorporate IT security measures into the business environment and business procedures as much as possible. Importantly, we believe that this allows employees to focus on their core duties.

In addition, security threats are constantly changing in step with advancement in ICT. To maintain effective measures against such threats, we believe that cutting-edge technology is needed to develop and implement technical measures, as well as analyze and address problems. To this end, we have put in place a dedicated team of IT security specialists.

In addition, technical countermeasures developed and implemented are put into practical application and tested for effectiveness and efficacy before being presented to customers and fed back in products*.

* Products include FENICS II Universal Connect

» IT Security Framework

The Fujitsu Group implements IT security measures based on IT security-related rules. For each measure designed according to the context of information use, there are information management functions for business systems, client security controls, integrated user management authentication systems, and network security controls. IT resource management is the foundation of all these elements. Furthermore, IT security audits are conducted to entrench and improve on these measures.

IT Security Framework

Information Security Rules			
• Definition of context	• Roles and responsibilities	• Establish PDCA cycles	
Information Management for application systems	**Client security control**	**Authentication system implementing integrated user management**	**Network security control**
Based on analysis of the business/information/user •Access control functions •Reliability features	•Automated measures •Measures preventing human error when sending e-mails •Corporate standard PCs	With a security card •Entrance management •Authentication •Document approval	•Network control •E-mail control •Network service use control
IT Resource Management as the Basis of IT Security			
• Management of goods as assets	• Security measures management	• License management	
Information Security Audits			
• Confirm implementation status			

IT Security-Related Rules

Fujitsu's IT security-related rules have the following three features, as set forth in Items 1–3 below.

1. Definition of context

The main contexts for ICT use are listed below. The IT security-related rules stipulate IT security measures that must be implemented in each context.

- Business systems that accumulate and process business information mainly on servers
- Offices and other worksites where PCs and other equipment are used
- Intra- and inter-office networks

2. Roles and responsibilities

The rules establish roles and responsibilities with respect to implementing IT security measures, and designate individuals responsible for implementing those measures in each business system and department. The rules also stipulate the authority of divisions supervising the implementation of measures.

3. Establish PDCA cycles

The rules govern the elements that compose each part of the PDCA cycle, including implementation of IT security measures, awareness-raising and education, promotion, incident response, evaluation and improvement in a bid to entrench and improve the measures.

Information Management in Business Systems

The Fujitsu Group uses ICT in a variety of operations, including finance and accounting, human resources and general affairs, sales, purchasing, systems engineering operations, production and logistics, and product development management. The information maintained and handled has security requirements that vary according to task and responsibility. By analyzing these requirements, we have implemented and applied an access control feature to control access to information based on the user's position and qualifications, and a reliability feature to meet the importance and continuity requirements of the business.

Client Security Control

An important information security issue is how human errors can be effectively dealt with. Relying only on human attentiveness in using ICT applications will not necessarily prevent information security incidents. Of course, education and awareness programs should be employed to draw attention to information security, but even then, information leakage and other incidents will occur beyond the reach of the ICT-based measures.

Based on this reality, we focused on the client business processes involving human action, and replaced the measures dependent upon human attentiveness with ICT enabled solutions after checking for feasibility.

■ Automated security measures for PCs

Application of security patches and updates for operating systems, applications, and virus definition files are automated.

■ Measures to prevent human error when sending e-mails

Information leakage can easily result from sending an e-mail or attachment to an incorrect e-mail address. To reduce the risk of information leakage, e-mail addresses are automatically checked, and the sender is required to reconfirm when e-mails are addressed to external persons.

■ Installation of Fujitsu standard PCs

Corporate standard PCs are those with identified models and specifications for internal corporate use. PCs with installed security measures, such as hard disk encryption, preset BIOS passwords, preset screen savers, installed resource management software, and installed anti-virus software, are used. In doing so, PC model selection, installation, and operation become standardized and there is a reduction in costs. This frees users from the responsibility of implementing security measures and aids the success of such measures.

■ Safe remote use of client devices

Client devices such as PCs and smartphones can be used remotely from outside the office, such as at home or while out on business. Such external access raises the risk of information leaks if the device is stolen or lost, therefore, it's an important objective to thoroughly inform employees of cautionary practices regarding remote devices through monthly "Security Check Days" and annual information security training.

ICT measures that could be introduced include a "Virtual Desktop Service" and "Smart Device Application" which protect against information withdrawal and keep important information secure when accessed through a remote client device.

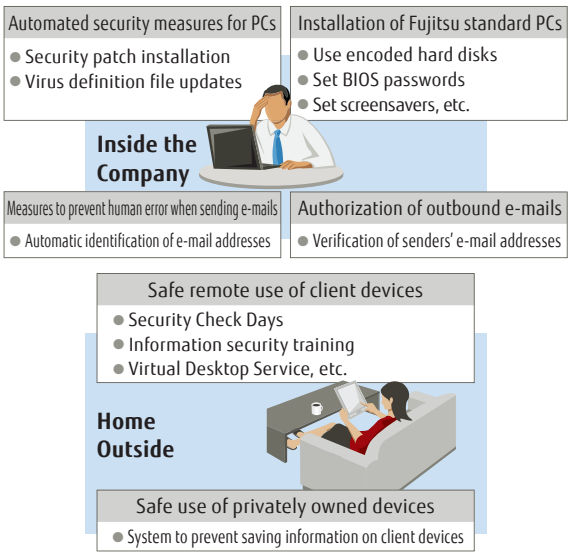
■ Safe use of privately owned devices (PCs, smartphones, etc.)

The Virtual Desktop Service and FENICS II Universal Connect are employed to enable safe use of privately owned devices like PCs and smartphones. These services ensure that internal information displayed on client devices cannot be saved on the devices to avoid the collection or leaking of confidential information due to user carelessness. Using this system with a personal device from home means that personal information and the internal network connection are separated within the device, ensuring the safe management of work information.

■ Management of e-mails sent outside of the Company

This system confirms whether a sender is authorized to send e-mail outside of the Company. It also prevents users who do not need external e-mail communication from sending e-mail to outsiders, thus preventing leakage of information.

↓ Client Security Control



IT Resource Management as the Basis of IT Security

IT resource management that manages resources related to servers and PCs does not only fulfill the role of asset management but is the basis of ICT application and IT security. The Fujitsu Group performs IT resource management with the "IT Resource Management System."

The IT Resource Management System maintains the following information.

■ Hardware resources: server and PC models, specifications

■ Software resources: software and software versions used on each server and PC

■ Application status of security patches

By managing software and software versions, the installation of software matching the license agreement is automated. In addition, the administrator can view the status of software resources and progress of security patch installation and instruct on remedial actions.

The IT Resource Management System is built on Systemwalker Desktop Patrol, a security management product of the Systemwalker family of integrated operation management software products, and integrates management of IT resources, security status, and software licensing.

Authentication System Implementing Integrated User Management

The Fujitsu Group provides each employee with an IC card, called a "Security Card," for authenticating employees and for other applications. The name and a photograph of the employee are printed on the face of the Security Card. In addition, the IC chip stores the name, employee number, and employee PKI (Public Key Infrastructure) certificate and key. This data is unique for each employee in the Fujitsu Group.

Because the Security Card is managed by the Human Resources Division and is issued at hire and returned at termination or retirement, the user is guaranteed to be a legitimate employee. In addition, the card is invalidated if lost to prevent abuse.

The primary applications of the Security Card are as follows:

Entrance management

Buildings and offices of the Fujitsu Group are equipped with security doors at the entrance. Employees coming into the office use their Security Card for entrance.

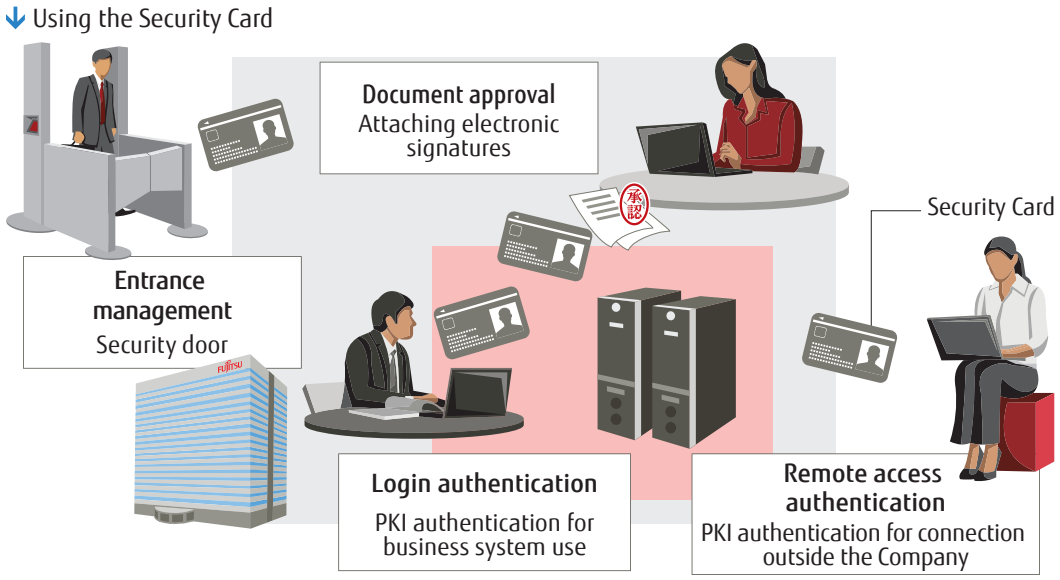
Authentication

Employees are required to use the Security Card when accessing business systems that require authentication. Authentication by PKI at login to business systems enables secure identification and authentication of employees along with simple operation.

Business systems can also be accessed from off premises, e.g., on business trips. In this case, the remote connection is authenticated by PKI, and the employee is securely identified.

Document approval

The Security Card is also used in approval of electronic documents. Approvers use the PKI feature to add their electronic signatures to the electronic documents. This action indicates that the approver has confirmed and approved that document and has the same effect as affixing an approval seal to a paper document.



Network Security Control

The Internet is indispensable to business as a means for business communication, for publicity and information provision, and for utilizing the large amount of external information. On the other hand, the serious threats originating in the openness and mechanisms of the Internet cannot be ignored. At the Fujitsu Group, a team of specialists armed with the latest technologies creates measures to combat these threats and conducts integrated management of Internet gateways across the globe with the aim of minimizing the burden on employees and ensuring security.

Network control

The following policies are in place for the network.

- Control of Internet connections and intranet construction and operation
  - Installation and operation of gateway systems, such as firewalls, by a team of experts
  - Screening and authorization of individual connections in business groups
- Maintaining security during operation
  - Measures against unauthorized access (server configuration, checking the status of device management, and monitoring and preventing unauthorized transmissions)
  - High availability measures including performance management and dependable system design
- Support for mobile devices
  - Implementing and operating a secure business environment for using remote PCs and smart devices* to access the intranet

    * Smart devices: Smartphones and tablets
- Adapting to shifting threats
  - Analyze trends, gather information and formulate countermeasures against new threats that are difficult to address with existing techniques, such as targeted e-mail attacks and Advanced Persistent Threat (APT)
  - Research on attacking techniques and responses
  - Awareness and training programs for users

Controlling e-mail servers

E-mail is currently indispensable for business execution. The following measures are in place for managing e-mail security.

- E-mail control
  - Installation and operation of e-mail servers by a specialist team
- Maintaining security during operation
  - Anti-virus measures
  - Anti-spam measures
  - High availability measures including performance management and dependable system design

Network service use control

The Internet environment outside the Group provides many network services such as file transfer and online meetings. Use of these services is selectively approved with necessary conditions based on the evaluation of business merits and requirements and improved client security controls. On the other hand, use of specific network services identified to have risks of information leakage is prohibited. In addition, to prevent accidental use, communication using these services is continually monitored.

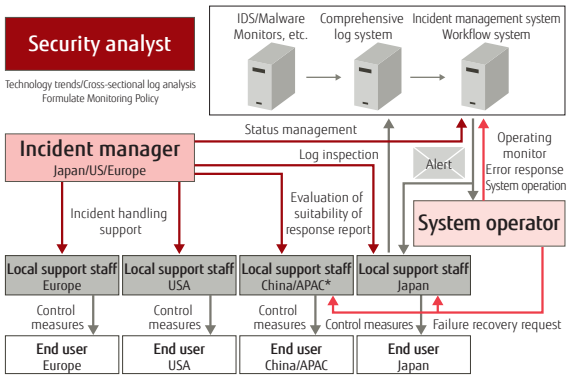
Intranet use control

The Fujitsu Group controls its intranet use because it recognizes that control of intranet use is an important factor of global controls under the "Fujitsu Group Information Security Policy." A priority information security measure is to attain and maintain common security standards regardless of country or territory. Consequently, intranet construction and use in Group companies worldwide are controlled based on security measures, common policies and management measures.

The Security Operation Center (SOC) conducts global control, supports the single global intranet and handles network incidents. Hundreds of millions of network alerts are detected daily among Group companies worldwide. We respond to these rapidly, determining their risk level and whether to handle them as an incident. Characteristics of the alerts are as follows:

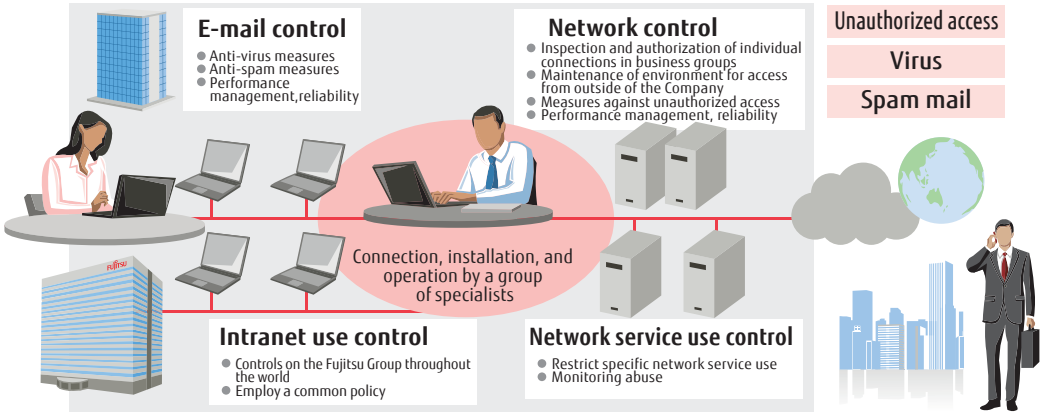
- Globally standardized risk guidelines and response processes
- Automatic evaluation of large volumes of data or logs
- SOC technicians stationed in all areas enable 24-hour response regardless of time zones
- Shorter response time due to a workflow system supporting connections between the incident manager and system operator
- Threat detection and new policy formulation conducted by specialist security analysts

SOC: Network Incident Handling



* APAC: Asia-Pacific

Network Security Control



IT Security Audits

An Audit Division, independent of the divisions implementing the foregoing IT security measures, performs audits of IT security measures based on an audit plan for a given fiscal year. The audits are conducted based on methods appropriate to the audit's target. Methods include having the auditor conduct an on-site visit to visually confirm the management status of devices and settings, inspecting reports on the results of inspections carried out by the divisions implementing IT security measures, and inspecting technical vulnerabilities via the network. The audited divisions use the audit findings to improve IT security measures.

Fujitsu Group Initiatives for Sound Protection of Customers' Information Assets

The organizations and Group companies in the Fujitsu Group that provide system integration service are called upon to maintain an even higher level of information management than the rest of the Fujitsu Group because they have many more opportunities to handle customer information assets and personal data.

That is why Fujitsu's Information Security Council Secretariat (Council Secretariat) provides its information security management system based on a security management framework to all related organizations and Group companies. Related organizations and Group companies apply the framework and promote policies.

Our Approach to Establishing an Organization to Promote Information Security

Cyber-attack threats have become sophisticated and diversified, resulting in global debate about various types of business regulations. Consequently, Fujitsu launched the Security Steering Committee in 2013 to share information on cyber security and discuss our business policies.

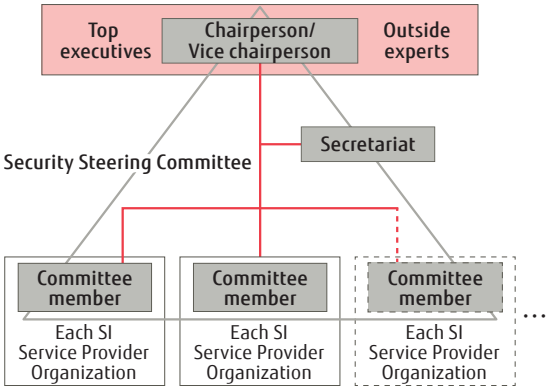
The Security Steering Committee is comprised of directors overseeing the various businesses undertaken by the System Integration Service Business; directors in charge of Japanese sales, marketing, and overseas sales divisions; and outside experts called upon to ensure impartiality.

Fujitsu abides by the principles of the "Fujitsu Technology and Service Vision." Reliability of information is important for a "Human Centric Intelligent Society," so it is vital to create a system where information utilization can continue on the assumption that accidents happen. The committee discusses and approves policies for projects requiring a global-level response, starting with countermeasures to the threat of cyber-attacks and observance of laws governing international cloud centers, as well as handling personal information.

The Security Steering Committee promotes activities to enhance the security quality of Fujitsu's system integration and services. The committee is a substructure of the Information Security Council (Council), which decides on the direction of the Fujitsu Group's security activities and is one of the Information Security Policy participating organizations (participating organizations).

In addition, the committee promotes security personnel training for system integration and services for the entire Fujitsu Group.

Security Steering Committee Structure

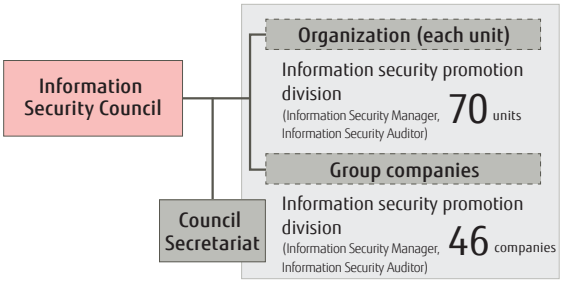


Development and Execution of Security Governance

Information security threats such as targeted attacks on specific corporations and groups, website attacks, and personal information leaks have been increasing unabated in recent years. This has created the need to implement risk management from a corporate management perspective. To this end, Fujitsu is pressing ahead with security initiatives under information security governance.

The System Integration Service Provider Organization and Group companies take part in the Council. Participating organizations formulate security plans, introduce security measures, promote information security activities and conduct internal audits based on the Security Management Framework (SMF; See the next page for details). They also strive to improve the management framework and security measures by confirming and evaluating the status of daily information security activities and security incidents and accidents.

Information Security Council Structure



» Information Security Management Promotion System

Participating organizations have established the "Information Security Council Activities Guidelines" with the goal of sound protection of customer and internal information to better handle information including customer information assets and confidential information. Based on these guidelines, participating organizations maintain and promote information security. Quarterly promotion meetings are held for information security managers and information security auditors from participating organizations to exchange information and opinions on security policies. The head of the participating organizations shall be the person responsible for promoting information security.

Furthermore, the Council Secretariat provides participating organizations with various assistance, as necessary, including support for effective measures and advice on enhancement initiatives needed to promote information security activities. This promotes the continuation of information security activities among participating organizations.

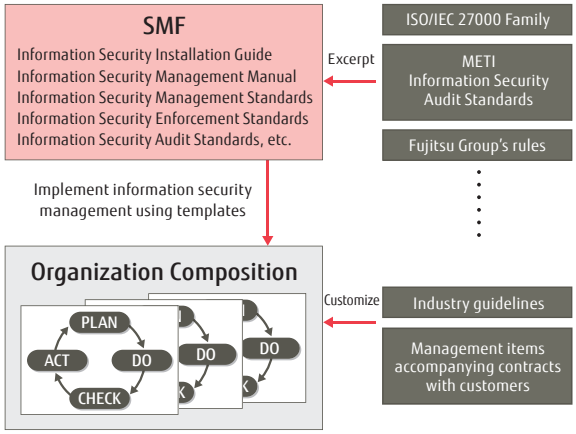
Conversely, each participating organization promotes the information security activities stipulated by the Council and maintains information security standards.

» SMF (Security Management Framework)

The Council Secretariat provides participating organizations with the SMF as a template to implement information security management. The SMF incorporates the ISO/IEC 27000 family, the Ministry of Economy, Trade and Industry (METI) Information Security Audit Standards, and other Japanese and international standards, in addition to the Fujitsu Group's regulations. The SMF consists of documents on the information security management system and the information security audit system. Participating organizations must comply with these documents while taking into account the industry guidelines of customers, administrative matters concerning contracts, and other factors. Each participating organization uses the SMF template to prepare its own information security-related documents and subsequent operations.

The relationships between the Fujitsu Group's rules, international standards, industry guidelines, and so forth are shown in the following diagram.

Relationship between the SMF and Fujitsu Group's Rules, International Standards, Industry Guidelines, etc.



» Security Improvement Efforts

Human Resources Development

Information Security Manager Training is implemented for information security managers and information security promoters who promote and manage information security at each participating organization. Since fiscal 2012, an e-learning program was also offered to encourage information security managers to continuously hone their own skills. There is also Information Security Auditor Training for internal information security auditors.

The Council actively encourages information security auditors to acquire auditor qualifications certified by the Japan Information Security Audit Association (JASA) to increase the quality of information security audits and move along their career path. As of fiscal 2014, 141 employees had acquired auditor qualifications and were actively engaged in internal audits and committee audits.

In addition, information security training materials are also provided and utilized by each participating organization.

Number of people in training

Training course name	Number of people
Information Security Manager Training (Group)	648
Information Security Manager Training (e-Learning)	652
Information Security Auditor Training	1,252

Periodic Security Checks

On "Security Check Days" implemented by the Fujitsu Group each month, personnel confirm the security settings of PCs and smart devices, as well as the administration of removable media devices. At the Council, the information security measure diagnostic tool (IT Policy N@vi) is installed in all PCs to diagnose the security measures and operational status of each PC. When a PC is started, diagnostic items* are automatically checked, with the results displayed on the PC monitor. Furthermore, by having the information security managers of each organization easily confirm the results of all PCs, Fujitsu has effectively increased the penetration of security measures.

The Council provides a security check sheet for smart devices that conforms to the Company-wide policy. The check sheet is used by various participating organizations to ensure smart device security.

* Diagnostic items: 19 items including OS, viruses, passwords, encryption, and prohibited configuration items

Information Security Measure Diagnostic Results Screen (in Japanese)

Information Security Audits

According to the Council, there are two types of information security audits: internal audits conducted by the participating organizations themselves and external audits of the participating organizations conducted by the Council Secretariat from an independent perspective.

Regular internal and external audits of the participating organizations lead to the penetration and entrenchment of information security management practices and the operational status and entrenchment of information security measures.

External audits are conducted yearly under themes stipulated by the Council Secretariat and audit plans are proposed. The Council Secretariat takes the lead in forming an audit team comprised of members who hold JASA auditor qualifications. The audit team confirms the promotion of information security management, identifies any deficiencies, and proposes improvements, among other activities. Outstanding measures in audited organizations will be introduced as examples at the Council and utilized to raise the level of security across all participating organizations.

In other activities, experts from the Council Secretariat implement special audits of specific projects, as well as participating organizations. This is to address individual requests from participating organizations and to meet operational requirements.

Social Media Training

SNS* has become quite popular as a communication tool in our daily life. With the increase in the number of users of SNS, for business or private purposes, the question of where corporate responsibility lies when problems occur has emerged.

In the face of these situations, Fujitsu has published the guidelines, Rules and Manners for Participating in Social Media. Based on these guidelines, the Council Secretariat has prepared an educational program titled Information Security Course for Social Media and delivers this to members.

The course explains the risks in using SNS and gives examples that guide learners on proper uses of the media.

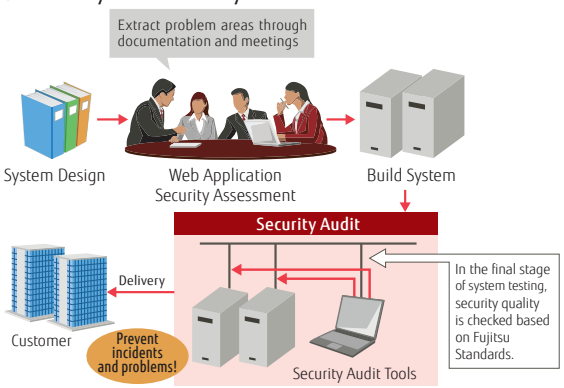
* SNS: Social Networking Service

Security Audits for Systems Delivered to Customers

The Fujitsu Group formulates security standards that should be satisfied in Internet-connected systems delivered to customers.

A pre-delivery security audit where specialized security departments objectively verify whether these systems meet guidelines is obligatory as part of quality inspections.

Security Audits for Systems Delivered to Customers



Security audits for systems delivered to customers comprise two parts: an "infrastructure pre-delivery security audit" for the infrastructure (OS/middleware) and a "web application security audit" for web applications.

Regarding web application security audits in particular, security assessments are performed at the systems design stage to rapidly extract and resolve any security problems related to web applications.

This ensures that the systems delivered to customers have been confirmed to meet a consistent security level established by the Fujitsu Group, while helping to prevent security incidents caused by unauthorized access from outside. Following the inception of security audits for systems delivered to customers, Fujitsu has confirmed a sharp decline in incidents caused by insufficient security measures in the systems integration process.

Initiatives toward the Improvement of Security Quality Including Cloud-based Services

It is important for service providers to respond to the ever-changing security threats to enable customers to be able to use services such as cloud-based services with a sense of safety and security. Fujitsu, as a service provider, clearly defines the security response that should be implemented, formulates guidelines and standards and conducts audits. In addition, Fujitsu has established a dedicated organization that will respond to incidents. It is also engaged in third-party evaluation and makes information available to the public.

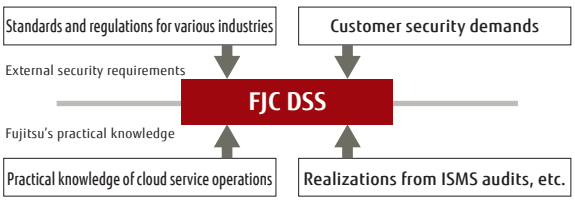
Initiatives through Countermeasure Standards for Cloud-Based Services

The reduction in security-related apprehensions and latency problems, expectations for the reduction and visualization of operating costs and business continuity coupled with the increase in cloud-based services operated in data centers within Japan herald the arrival of the cloud first era in which the public cloud becomes the preferred option.

Numerous organizations including METI, CSA and ENISA have published cloud security guidelines. ISO/IEC 27017, which is based on METI guidelines, is most likely to become the international standard for cloud security in fiscal 2015. However, the requirements of these guidelines are set in such a way that cloud service users can freely select the strength of security that they want to adopt, causing a disparity in the level of security measures for each cloud service provider.

Therefore, Fujitsu created its own security standards, the Fujitsu Cloud Data Security Standard (FJC DSS), by integrating these external security requirements, customers' security requirements and its own practical knowledge, to be put into practice together with the Next Generation Cloud Platform to be launched in fiscal 2015. This ensures that cloud services offered by Fujitsu meet a consistent security quality.

FJC DSS Development Policies



Initiatives through Guidelines and Audits

Fujitsu has established Service Security Response Guidelines, which include items that should be implemented in service development and operation processes to ensure the security quality of services offered to customers.

Divisions providing services put into practice the security measures based on these guidelines. Moreover, before launching a service, the audit department audits the status of security measures and ensures its quality.

During service operations, the security audit department continually conducts regular security audits. The security quality is maintained and continuously improved by taking corrective measures if necessary.

Fujitsu Cloud CERT Initiatives

Fujitsu Cloud CERT (Computer Emergency Response Team), a team that specializes in the security of services including cloud-based services, performs the following activities on a global scale in order to support customers' businesses and protect the cloud environment from various security threats.

1. Information security operations

For customers to securely use Fujitsu cloud-based services, Fujitsu Cloud CERT implements security measures, including point of contact detection of various external attacks and monitoring of the cloud service infrastructure, and operates under a 24-hour, 365-day system.

2. Emergency response

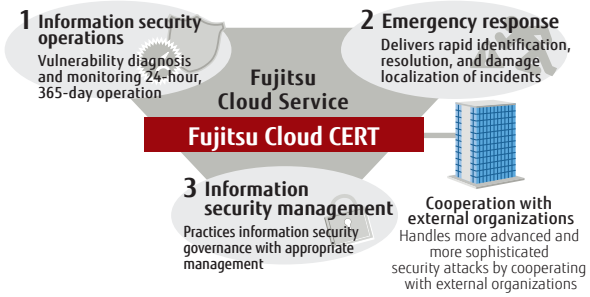
Fujitsu Cloud CERT has established response procedures that will be implemented when an incident occurs to achieve rapid and accurate identification, resolution, and damage localization of the incident.

3. Information security management

Fujitsu Cloud CERT properly manages the "people," "goods," and "information" in Fujitsu Cloud services to protect the important information of the customers. Moreover, Fujitsu Cloud CERT is a member of security-related organizations such as the Nippon CSIRT Association and FIRST* and plays an active role in improving global cloud security.

* FIRST: Forum of Incident Response and Security Teams

Activities of Fujitsu Cloud CERT



Product Security

Among the security enhancement initiatives that Fujitsu's software product development divisions engage in are responding to vulnerabilities in open source software and human resources development, which we describe here.

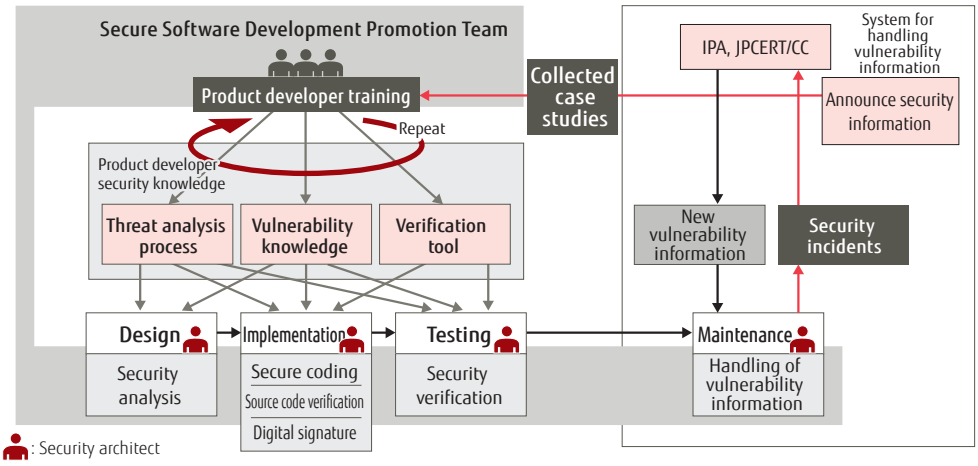
Software Security Quality Enhancement Initiatives

To improve the security quality of its software products including firmware, Fujitsu conducts the activities shown in the diagram below, led by the Secure Software Development Promotion Team. Specifically, Fujitsu incorporates the following four activities into its development process to ensure security quality:

1. In the design process, Fujitsu conducts security analysis (threat analysis) and uses the results to improve the design.
2. In the implementation process, Fujitsu conducts coding to avoid any built-in vulnerabilities (secure coding), verifies source code using verification tools, and adds digital signatures to programs as necessary.
3. In the testing process, Fujitsu conducts security verification using verification tools and runs tests from a security perspective.
4. In the maintenance process, Fujitsu monitors security vulnerabilities, rapidly provides security patches, and publicly discloses security information in coordination with the Information-technology Promotion Agency (IPA) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

For each process, Fujitsu deploys security architects with technical knowledge of security in each division, in order to entrench proper security responses in development activities. About 10% of all developers are certified as security architects.

Security Process for Software Products



Ensuring Security in Shipped Products Using Open Source Software

One part of the maintenance process referred to in 4 above involves ensuring the security of products using open source software, which is described here. Accompanying the increasing diversity of software product requirements is the growing variation of open source software that Fujitsu products use. That makes it crucial to provide rapid support for each open source software vulnerability. Fujitsu system engineering and product development divisions jointly created the Open Source Software Vulnerability Response System to comprehensively and effectively prevent response failures and provide rapid support.

Overview of the Open Source Software Vulnerability Response System

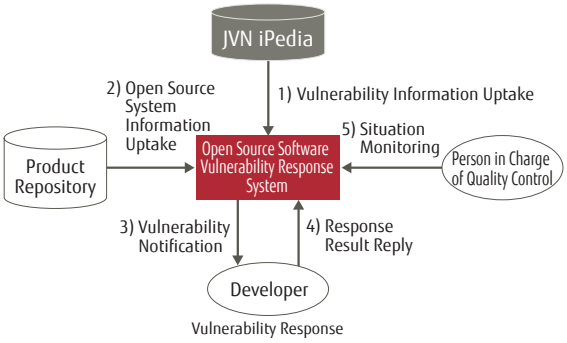
1. Fujitsu employs the Vulnerability Countermeasure Information Database JVN iPedia*1 as an information source about open source software vulnerabilities. This database covers vulnerabilities which have been given a number by the National Vulnerability Database (NVD)*2.
2. Based on information stored in the product repository, applicable open source software for each product is specified in the system for vulnerability information. This enables all open source software being used in products to be investigated for vulnerabilities.
3. Vulnerability information collected by the Open Source Software Vulnerability Response System is cross-checked against open source software divided by product in the product repository and immediately communicated to developers, starting the vulnerability response process.

4. Security is positioned as a high-priority issue and open source software vulnerabilities are given a high priority and investigated. Those responsible for product quality control in the product development divisions check the response status and issue appropriate instructions if they find the response to be lagging.

Various types of information publicly available on the Internet are used as source material.

*1 Vulnerability Countermeasure Information Database JVN iPedia is a vulnerability database jointly managed by JPCERT/CC and the IPA. It covers all vulnerability information registered in the NVD since 2007.
*2 The National Vulnerability Database is a vulnerability database managed by the U.S. National Institute of Standards and Technology.

Overview of the Open Source Software Vulnerability Response System



» Product Developer Training

Security training in software product development divisions follows two routes: Security Architect Training for professional human resources and General Training for general product developers and inspectors.

Security Architect Certification System

Security architects are those who have obtained professional qualifications within the Company to promote security response activities, enhance security quality in software products, and operate the Security Architect Certification System, which includes training programs given in software product development divisions.

The training program for security architects has a curriculum executed in four phases over several months for candidates recommended by each development division. The four phases are: (1) Prior learning and subjects, (2) Group training (exercise style), (3) Producing threat analysis reports, and (4) Certification review.

Following certification as a security architect, training programs are held regularly with details such as those listed below, at a rate of once or twice a year, to hone architects' skills.

- Describing Other Divisions' Security Activities
- Internal Incident Case Studies
- Research Reports by Expert Organizations
- Secure Development Process (Latest information)

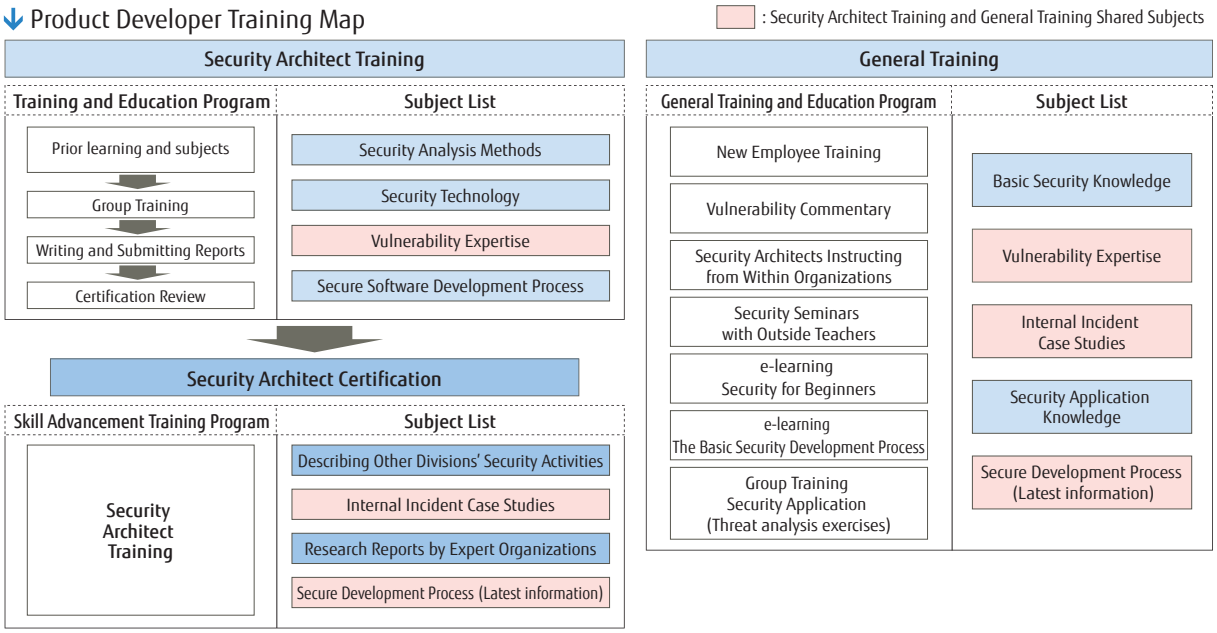
While striving to improve individual skills and update expertise through training programs, security architects exchanging information and opinions among themselves endeavor to raise their awareness.

General Training

General Training aims to enhance security response capabilities by utilizing a variety of methods, starting from e-learning for new employees and group training and progressing to training in each division and inviting outside teachers to host seminars.

Important topics such as vulnerabilities or secure development process are required knowledge for developers, too, so General Training shares aspects with Security Architect Training.

Product Developer Training Map



Research and Development into Security Technology for Supporting a Safe Lifestyle

Cyber-attacks are becoming fiercer and more cunning day by day, and threatening the security of corporate systems. On the other hand, with the onset of the Internet of Things (IoT) era, various information including personal data are collected from various types of devices, and safe use of the information is desired. To solve these problems, Fujitsu Laboratories Ltd. is developing cutting edge technologies.

This report introduces two technologies: One is the early detection technology against advanced persistent threats (APT), which are recently rampant cyber-attacks. Another is lightweight and highly secure mutual authentication technology between IoT devices.

» New Detection Technologies for APT (Advanced Persistent Threats)

Sophisticated Cyber-Attacks

In recent years, there has been a surge in increasingly sophisticated APT against specific organizations and individuals for the purpose of stealing information. In the APT, malicious programs called malware are often used.

The most common type of malware today is known as a Remote Access Trojan (RAT). With a RAT, the intruder outside a network remotely operates an infected PC within a network to collect internal data, disguising activities as routine business communications such as sending or receiving e-mails. Afterwards, when the attack begins, the content of the communications does not contain malware itself, and the traffic associated with the remote operations is almost always encrypted. This activity is difficult to discover using conventional anti-virus software or unauthorized intrusion-detection systems.

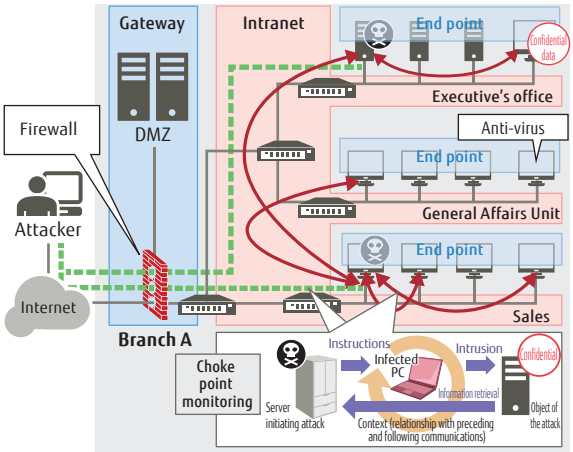
New Detection Technologies for Malware that Has Invaded Intranet

Fujitsu has developed technologies that are used in the intranet to detect latent RAT activities inside companies.

1. Choke Point Monitoring

Fujitsu Laboratories conducted research and development on ways to monitor choke points. Choke points are steps common for most malware, which the attacker cannot do without. By analyzing the types of communications flowing through an intranet and the related communications that precede or follow them, it is possible to detect latent activity within a network that is characteristic of a RAT. Looking at the type of communication along with the context creates a high rate of detection even when communications have been encrypted and there is no malware in communications.

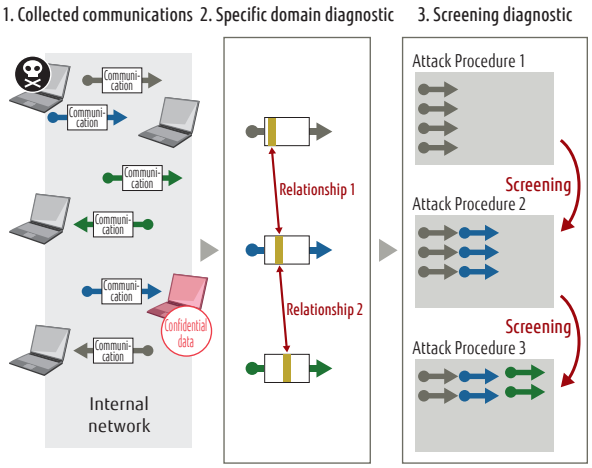
Choke Point Monitoring Method



2. Efficient RAT Communication Pattern Detection Technology

Choke point monitoring uses two technologies to effectively evaluate attacking communications. The first is specific domain diagnostic. Attack-related communications can be diagnosed using only the relationship between data on specific domains for multiple communications and the communication sequence, reducing the processing load required for analysis. The other method is screening diagnostic, which efficiently detects suspicious communications by screening individual communications at each attack stage, significantly reducing process times associated with locating multiple communications comprising an attack from an enormous volume of communications.

Overview of Technology for Detecting RAT Communication Patterns



In a gigabit network environment of approximately 2,000 devices with a large volume of routine business communications, these diagnostic systems were verified and evaluated while recreating the latent activity of a RAT. The result was complete detection of the RAT's attack communications, which represented 0.0001% of the overall volume. Moreover, no work-related communications were falsely detected as attack-related communications.

Effects of New Detection Technologies

By deploying networking equipment armed with these technologies, it is possible to monitor malicious traffic flowing through a network and detect APT malware before any data is leaked, which is difficult to do with firewalls or anti-virus software. Going forward, R&D will continue to focus on provision technologies against cyber attacks after detecting them.

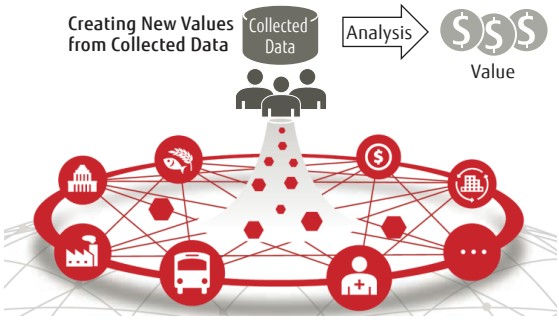
» Mutual Authentication Technology between Devices in the IoT Era

Ensuring IoT Security

In the approaching IoT era, when various devices such as air conditioners, lighting and cars in addition to mainframe computers will be connected to the Internet, new business that uses value created by analyzing data collected from devices has received a lot of attention. In this application, security is necessary to guarantee the validity of collected data and protect devices against illegal access. Moreover, high efficiency is required for the security technology in IoT because the number of devices is predicted to grow to about 50 billion. Fujitsu Laboratories is conducting R&D into technologies that will enable efficient mutual authentication among devices in the IoT world.

Currently, an authentication and encryption technology called Transport Layer Security (TLS) is used widely. TLS uses public key cryptography to correctly authenticate peers. Generally, public key cryptography requires a certificate that guarantees an association between the user or device and key being used. Authenticating communications peers requires exchanging certificates and then verifying these in cryptographic processes with a heavy load. With the massive expansion in the number of devices in the IoT world, preparing and managing certificates for all devices elicits an enormous amount of labor, and the explosive increase in cryptographic processing for certificate verification presents a challenge. Fujitsu Laboratories responded by developing a mutual authentication technology that does not use certificates.

Conceptual Drawing of IoT Use



Security for sensitive information in communications must be ensured

Newly Developed Technology

The newly developed technology uses a public key cryptography called ID-based encryption that uses an ID as a key. In public key cryptography used in TLS, RSA and elliptic curve cryptography use random numbers not associated with users as keys. Consequently, communications peers' certificates must be obtained and the validity of their keys (random numbers) verified before encryption. In contrast to this, ID-based encryption uses the partner's ID as a key, so it's possible to encrypt without having to obtain certificates or confirm their keys in advance.

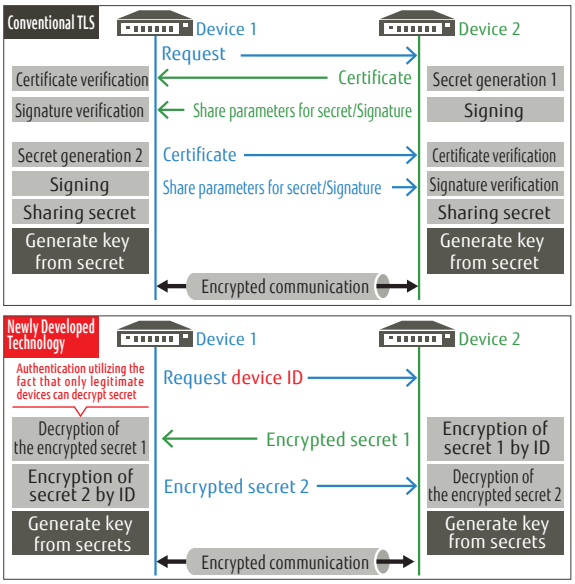
The newly developed mutual authentication technology uses this advantage to enable the exchange of a secret* using the other party's device ID for encryption. Next, it decrypts the encrypted secret obtained and from that secret generates a temporary key for encrypted communications. Only valid devices corresponding to ID used in ID-based encryption are capable of decrypting the confidential information and further communicating with the temporary key realizes mutual authentication and encrypted communications at the same time.

In addition, application of the mutual authentication technology to TLS was developed by extending its protocols. This technology shaped and optimized exchanges of secret with ID-based encryption to make it comply with existing TLS protocols. Until now, TLS had restrictions on the types of IP addresses or domain names that could be used as device IDs without exchanging certificates. But by effectively expanding the message at the onset of communication it is possible to use any information as a device ID.

This mutual authentication technology enables authentication using device IDs with the same ease of use as conventional TLS.

* A random number shared between the two peers in the connection.

Comparison between Conventional TLS and Development Technology



Effect of Newly Developed Technology

Employing the newly developed technology on a single-board microprocessor succeeded in using only 1/4th of the traffic data of TLS and the speed was 2.5 times faster. The newly developed technology enabled low volume mutual authentication between devices, efficiently realizing the security needed in the IoT world where enormous numbers of devices will be connected.

Initiatives for Ensuring Mutual Connectivity

Authentication developed at Fujitsu Laboratories is a technology that will be used as an IoT infrastructure. Going forward, for ensuring mutual connectivity in the IoT world with a network connecting tens of billions of devices, it is not originality but cooperation with other companies that will be important. For that reason, Fujitsu is currently moving forward with the Green University of Tokyo Project in developing application technologies for the IEEE1888 standard for Building Energy Management Systems (BEMS). Going forward, this project aims to make IEEE the standard.

Information Security Enhancement Measures in Cooperation with Business Partners

The business activities of the Fujitsu Group are supported by business partners, whose software, services, goods and materials provide the basis for the value added by Group companies.

The Fujitsu Group and its business partners build long-term bonds of trust, each enhancing its own abilities as a valued partner and together creating continuous and mutually prosperous relationships, all under the Fujitsu Way corporate policy.

The Fujitsu Group aims to eliminate information security incidents together with its business partners. To this end, the Group continuously implements measures such as education, awareness raising, audits and information sharing in connection with initiatives to deter security incidents.

» Information Security Enhancement Initiatives in 2014

Education and Raising Awareness

■ Information security seminars

Training was held on measures to eradicate or deter information security threats, including new ones such as IoT and cyber-attacks.

Actual incidents such as data theft and loss, erroneous e-mails, virus transmission and internal crime were used as examples and categorized under "carelessness," "unsuspecting" and "willful."

- Fiscal 2014: 1,200 participants from 950 business partners (in places including Tokyo, Kawasaki, Nagoya, Osaka, Fukuoka, etc.)

■ Out-of-office training

Instructors were dispatched to conduct training seminars for employees at the request of business partners.

- Fiscal 2014: Training received by 1,600 employees of 45 business partners

■ Workshops for employees in leadership roles

Fujitsu conducted workshops for employees in leadership roles at major business partners. The workshops focused on skills to prevent information security incidents and preparation of reports when information security incidents arise, analysis of the causes of such incidents, and formulation of corrective measures.

- Fiscal 2014: Workshops attended by 70 employees of 20 business partners (Tokyo and Osaka)

Business Partner Selection and Evaluation of Information Security Status

Selection of new business partners involves advanced evaluation of information security readiness, and is limited to those business partners who consent to contractual requirements concerning information security management and the handling of personal data.

Furthermore, a CD-ROM containing all relevant information is provided to promote a rapid rise in information security to achieve the level expected of Fujitsu's business partners.

Existing business partners are periodically examined based on factors including the Order for enforcement of the Act on the Protection of Personal Information and the taxpayer and social security number program.

Information Security Document Inspections

Regular visits are paid directly to business partners to confirm the state of information security.

Business partners are also encouraged to implement autonomous measures for information security by submitting required documents for information security document inspections.

Information Sharing and Presenting On-Site Support Tools

Fujitsu provides project information security plans at the start of projects to establish a security requirement consensus for supporting information security requirements, enabling rapid discovery of and response to issues.

Project Information Security Plans

It also continues to provide bimonthly publications and posters with the aim of sharing information and raising awareness.

Support for Overseas Business Partners

Opportunities have increased for business through cooperation with overseas business partners aimed at such objectives as supporting customers' overseas expansion, securing development resources, and responding to global products.

Fujitsu concludes "Information Management Procedure for Business Partners" agreements with overseas business partners as it does with Japanese partners, regulating the handling of information provided by Fujitsu in accordance with the conditions of each country. It also supports information security audits and training to strengthen and maintain wholesome partnerships.

Information security training in China

Third Party Evaluation/Certification

The Fujitsu Group is working to acquire third-party evaluations and certifications in its information security initiatives.

PrivacyMark Registration

The PrivacyMark registration status within Fujitsu and Fujitsu Group companies from the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) is as follows:

FUJITSU LIMITED
FUJITSU ADVANCED ENGINEERING LIMITED
FUJITSU ADVANCED QUALITY LIMITED
FUJITSU ADVANCED SYSTEMS LIMITED
FUJITSU APPLICATIONS, LTD.
FUJITSU ADVANCED PRINTING & PUBLISHING CO., LTD.
FUJITSU HUMAN RESOURCE PROFESSIONALS LIMITED
AB SYSTEM SOLUTIONS LIMITED
FUJITSU FIP CORPORATION
FUJITSU FOM LIMITED
FUJITSU FSAS INC.
OKINAWA FUJITSU SYSTEMS ENGINEERING LTD.
FUJITSU KAGOSHIMA INFORNET LIMITED
FUJITSU KYUSHU SYSTEMS LIMITED
FUJITSU COMMUNICATION SERVICES LIMITED
FUJITSU COWORCO LIMITED
FUJITSU CIT LIMITED
G-SEARCH LIMITED
FUJITSU SHIKOKU INFORTEC LIMITED
FUJITSU SYSTEMS EAST LIMITED
FUJITSU SYSTEMS WEST LIMITED
FUJITSU RESEARCH INSTITUTE
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
FUJITSU SOFTWARE TECHNOLOGIES LIMITED
TOTALIZATOR ENGINEERING LIMITED
TOYAMA FUJITSU LIMITED
FUJITSU TRAVELANCE LTD.
FUJITSU NIIGATA SYSTEMS LIMITED
FUJITSU PERSONAL SYSTEM LIMITED
FUJITSU PUBLIC SOLUTIONS LIMITED
FUJITSU BANKING INFORMATION TECHNOLOGY LIMITED
FUJITSU BROAD SOLUTION & CONSULTING INC.
PFU LIMITED
FUJITSU FRONTECH LIMITED
FUJITSU FRONTECH SYSTEMS LIMITED
BEST LIFE PROMOTION LTD.
FUJITSU HOKURIKU SYSTEMS LIMITED
FUJITSU MARKETING LIMITED
FUJITSU MISSION CRITICAL SYSTEMS LIMITED
FUJITSU YAMAGUCHI INFORMATION CO., LTD.
UCOT INFOTECHNO CO., LTD.
FUJITSU LEARNING MEDIA LIMITED
LIFEMEDIA, INC.
FUJITSU YFC LIMITED

ISMS Certification

Fujitsu and Fujitsu Group companies with divisions that have acquired ISMS certification based on International Standards ISMS (ISO/IEC 27001) for Information Security Management Systems are as follows:

FUJITSU LIMITED
FUJITSU ADVANCED ENGINEERING LIMITED
FUJITSU FIP CORPORATION
FUJITSU FSAS INC.
FUJITSU KAGOSHIMA INFORNET LIMITED
FUJITSU KANSAI-CHUBU NET-TECH LIMITED
FUJITSU KYUSHU SYSTEMS LIMITED
FUJITSU SHIKOKU INFORTEC LIMITED
ZIS INFORMATION TECHNOLOGY CORPORATION
FUJITSU SYSTEMS EAST LIMITED
FUJITSU SYSTEMS WEST LIMITED
FUJITSU GENERAL LIMITED
FUJITSU RESEARCH INSTITUTE
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
FUJITSU DEFENSE SYSTEMS ENGINEERING LIMITED
TOYAMA FUJITSU LIMITED
NIFTY CORPORATION
FUJITSU NETWORK SOLUTIONS LIMITED
FUJITSU PUBLIC SOLUTIONS LIMITED
FUJITSU BROAD SOLUTION & CONSULTING INC.
PFU LIMITED
FUJITSU FRONTECH LIMITED
FUJITSU MARKETING LIMITED
FUJITSU MISSION CRITICAL SYSTEMS LIMITED
FUJITSU MIDDLEWARE LIMITED
FUJITSU LEASING CO., LTD.
FUJITSU YFC LIMITED

Information Security Rating Certification

Information security ratings indicate the level of security, mainly in terms of whether or not information leaks and other security incidents could occur. Information here refers to technical data, trade secrets, and personal information handled by companies and other organizations.

The ratings are given by I.S.Rating Co., Ltd. The Fujitsu Group information security ratings are shown to the right.

Company Name	Rating Scope	Rating Mark
FUJITSU LIMITED	Tatebayashi System Center	AAA$_{is}$
	Akashi System Center	AAA$_{is}$
FUJITSU FIP CORPORATION	Yokohama Data Center	AAA$_{is}$
	Chubu Data Center	AAA$_{is}$
	Kyushu Data Center	AA$^{+}_{is}$
FUJITSU FSAS INC.	Tokyo LCM Service Center	AA$^{+}_{is}$

ISMS Auditor Certification

In 2002, the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) began full operation of an information security management system (ISMS) compliance evaluation system in Japan. The personnel certification institutions that register evaluations of auditors in Japan are the Japanese Registration of Certificated Auditors (JRCA) and International Register of Certified Auditors (IRCA) Japan.

The certification classifications for auditors include "ISMS Lead Auditor," "ISMS Auditor," and "ISMS Provisional Auditor." The number of people who hold ISMS auditor certifications at Fujitsu and Fujitsu Group companies is shown as follows.
<153 people>

JASA Auditor Certification

The NPO Japan Information Security Audit Association (JASA) is a certification organization for auditors who implement information security audits based on the "Information Security Audit System" issued by the Ministry of Economy, Trade and Industry in April 2003. The categories of qualifications are "CAIS*-Lead Auditor," "CAIS-Auditor," "CAIS-Assistant," and "CAIS-Associate."

Fujitsu and Fujitsu Group companies have the largest number of individuals who are qualified as JASA auditors. The number of such auditors is shown as follows.
<141 people>

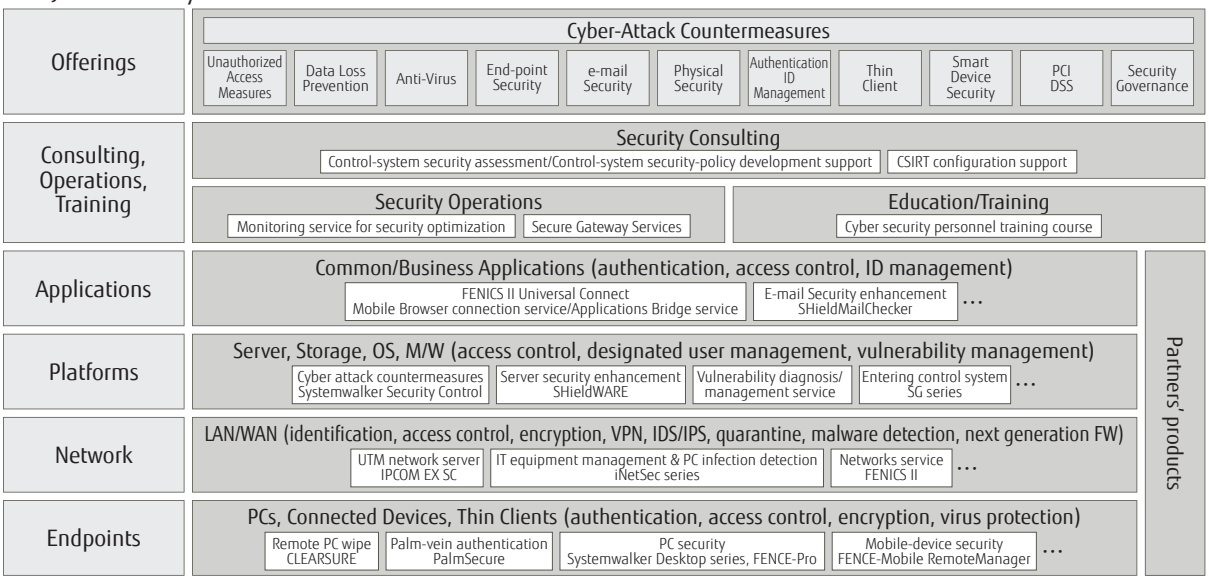
* CAIS: Certified Auditor of Information Security

FUJITSU Security Initiative

Fujitsu continuously works on achieving safe and secure ICT to continue supporting customers and sustainable business.

The growing popularity of cloud computing and smart devices has seen the regions utilizing ICT expand and cyber-attacks grow more sophisticated and cunning by the day, so taking measures against the attacks to ensure safe and secure utilization of ICT has become a significant issue. Through appropriate countermeasures and operations, Fujitsu, which is comprised of approximately 300 companies worldwide, currently deals with several hundred million individual cyber-attacks each day on its own Intranet. To apply this expertise to the security measures of its customers and deliver integrated support, including enhanced systems and operations as well as education and training of a company's personnel, Fujitsu has organized a line of products and services that follow its new "FUJITSU Security Initiative."

FUJITSU Security Initiative



Security Solutions

Currently, the environment encompassing information security is exposed to a variety of security risks, starting with external threats such as viruses and illegal access, and including cyber-attacks and data loss incidents which are increasing in conjunction with the widespread use of smart devices. Fujitsu's track record of practical experience provides security solutions based on consistent beliefs and thorough in-house implementation under "the Fujitsu Enterprise Security Architecture (ESA)" and "our Security Management Framework (SMF)." Providing solutions requires integrating the necessary security solutions and conforming to the ESA in order to effectively support companies' investments from a functional aspect. Presenting reference models based on internal practices enables customers to implement highly reliable solutions drawn from our track record.

Main Models Offered	For further details on security, please visit the following website (Japanese only): http://jp.fujitsu.com/solutions/safety/secure/
Security Governance	Supports the realization of "information security governance" in the organization based on continuous security measures from the perspective of overall company activities including ICT.
Cyber-Attack Countermeasures	Provides optimal measures to guard against new cyber-attack methods, while taking full advantage of conventional measures.
Smart Device Security	Provides solutions for customers' security concerns when using smart devices for business purposes.
Unauthorized Access Measures	Realizes a security cycle including surveillance 24 hours a day, 365 days a year, as well as planning, establishing measures, implementing measures, auditing, and monitoring.
Data Loss Prevention	Provides functions for drafting and establishing information management policies and encryption functions for protecting personal information and preventing information leaks.
Anti-Virus	Provides services including protection, virus removal, monitoring, and recovery support as anti-virus measures.
End-point Security	Creates an environment that protects customer systems from threats such as leaks of confidential information and virus damage at end-points (terminals of client-connected systems).
e-mail Security	Provides total security assistance needed to use e-mail securely, such as anti-virus measures and preservation of audit trails.
Authentication ID Management	Provides assistance for authentication and user information management, which are the foundations of information security, through various products and services, including biometric authentication, electronic certificates, and directories.
PCI DSS	Provides security measure solutions for helping to ensure compliance with the PCI DSS (Payment Card Industry Data Security Standard).
Thin Client	Provides total client virtualization using cutting-edge devices and secure networks. Also supports work style reforms by enabling mobile use of an extensive range of user devices.
Physical Security	Provides comprehensive solutions for physical security issues in the office.

FUJITSU LIMITED
Cyber Defense Center

1-17-25 Shin-kamata, Ohta-ku, Tokyo 144-8588 Fujitsu Solutions Square
E-mail: contact-isrep@cs.jp.fujitsu.com
URL: http://www.fujitsu.com/