Fujitsu Group Information Security Report 2014

FUJITSU

shaping tomorrow with you

Fujitsu Group Information Security Report 2014

CONTENTS

Fujitsu Information Security: Our Vision and Reality 3

1 Fujitsu Group's Information Security 4

2 IT Security Efforts 7

3 Fujitsu Group Initiatives for Sound Protection of Customers' Information Assets 11

4 Initiatives Enhancing Security Quality in Services 14

5 Product Security 16

6 Research and Development into Security Technology for Supporting a Safe Lifestyle 18

7 Information Security Enhancement Measures in Cooperation with Business Partners 20

8 Third Party Evaluation/Certification 22

9 FUJITSU Security Initiative 23

Report Summary

Target Period and Scope of the Report

This report covers the period up to March 2014 and focuses on efforts in information security by the Fujitsu Group.

Report Publication Date

This report was published in August 2014.

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 medium-term 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 business 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 2014" 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

President and Representative Director
Fujitsu Limited

Fujitsu Group's Information Security

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

Corporate Governance and Risk Management

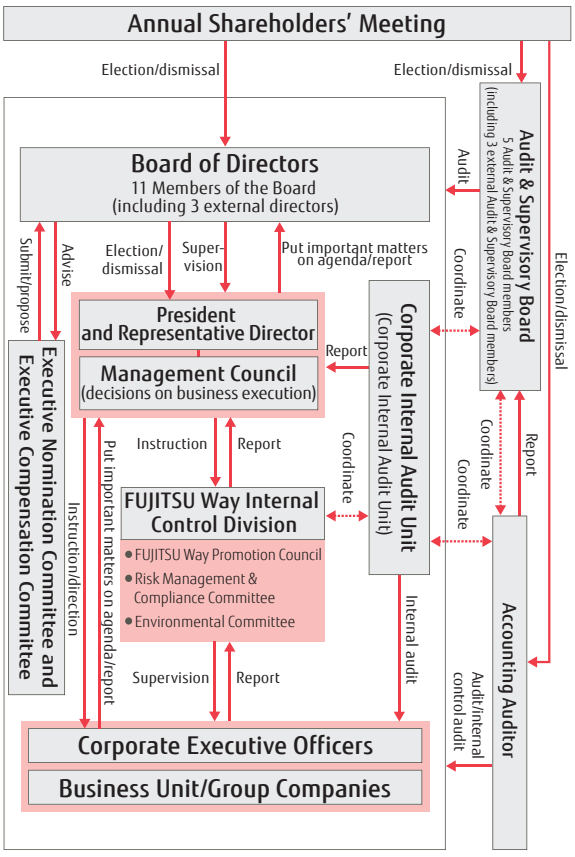
Corporate Governance

In order to continuously raise the Fujitsu Group's corporate value, along with pursuing management efficiency, it is also necessary to control the risks that arise from business activities. Recognizing that strengthening corporate governance is essential to achieving this, the Board of Directors has articulated the "Basic Stance on Internal Control Framework" and these measures are continuously implemented.

Furthermore, by separating management oversight and operational execution functions, we aim to accelerate the decision-making process and clarify management responsibilities. Along with creating constructive tension between oversight and execution functions, we are further enhancing the transparency and effectiveness of management by proactively appointing external directors.

With respect to Group companies, we are pursuing total optimization for the Fujitsu Group by clarifying each Group company's role and position in the process of generating value for the Group as a whole. Through this approach, we are managing the Group with the aim of continuously enhancing its corporate value.

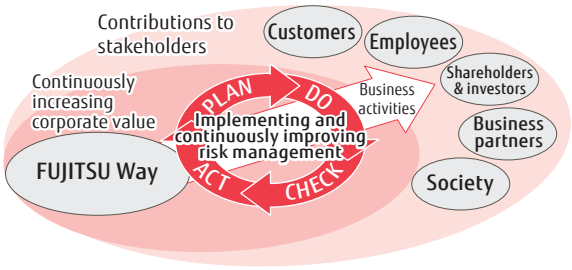
▼ Corporate Governance Organization Chart



Risk Management

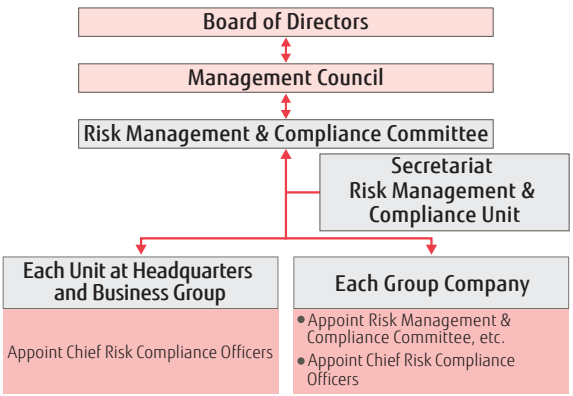
Through its global activities in the ICT industry, the Fujitsu Group continuously seeks to increase its corporate value, and to contribute to its customers, local communities and all other stakeholders. Properly assessing and dealing with the risks that threaten the achievement of these goals while preventing risk and minimizing the impact when risks materialize, and trying to prevent recurrence is assigned a high priority by management. Accordingly, we have put in place Group-wide risk management and compliance systems that we execute and continuously improve on.

▼ Implementing and continuously improving risk management



The Fujitsu Group established the Risk Management & Compliance Committee as an internal control committee reporting directly to management to promote the global risk management and compliance system. The Risk Management & Compliance Committee appoints Chief Risk Compliance Officers at each division of Fujitsu Limited and each Group company. With this Group-wide system Fujitsu Group, companies can mutually coordinate one another's activities, while promoting risk management and compliance from the standpoints of preventing potential problems and addressing any problems that have emerged.

▼ Risk Management 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.

Based on the "Fujitsu Group Information Security Policy," each company in the Fujitsu Group has put in place related regulations to guide the implementation of information security measures.

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

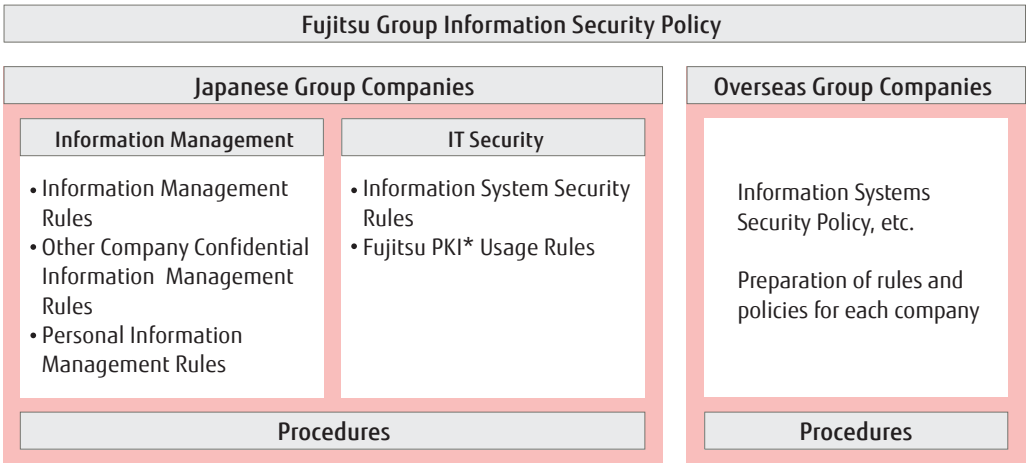
The Fujitsu Group applies the following principles when conducting information security activities.

(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.

▼ Framework of information security rules



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

Promoting Information Security Education

We think it is important to not only let employees know the types of rules but also to improve security awareness and 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 Japanese Group companies, and conduct annual e-learning for all employees, including executives.

▼ e-learning screenshot

Raising Awareness Regarding Information Security

Starting in fiscal 2008, 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 PCs used by employees, and implementing other measures.

Also, a tool was introduced to prevent e-mails from being sent outside the company in error, and in parallel with promoting the use of ICT we increased the awareness of information security among all 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

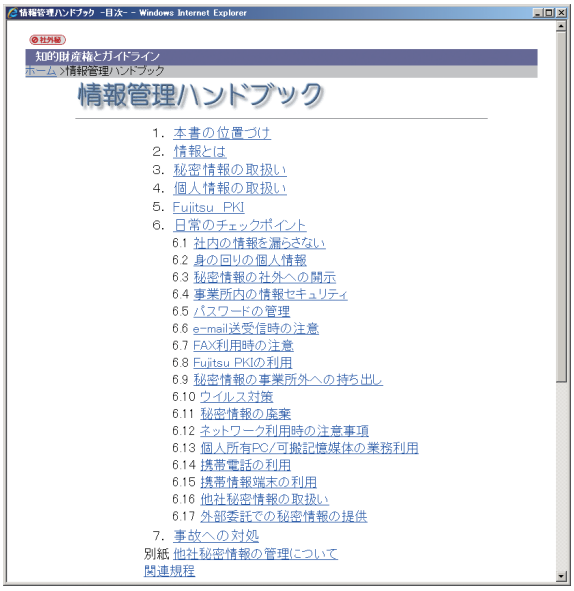
Fujitsu has established the "Personal Information Protection Policies" and "Personal Information Management Rules." We are also continually strengthening the system for protecting personal information based on these rules, such as by conducting annual training and audits on the handling of personal information.

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)



2 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.

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 authentication systems, information management functions for business systems, client security controls, and network security controls. Asset 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

• Establish scenarios • Define roles and responsibilities • Set up PDCA cycle

Authentication system implementing integrated user management	Information Management for application systems	Client security control	Network security control
With a security card • Entrance management • Authentication • Document approval	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	• 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 which vary according to the 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 virus definition files are automated.

Measures to prevent human error when sending e-mails
Information leakage will easily result from sending an e-mail to a wrong address. To reduce the risk of this 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 corporate standard PCs
The Fujitsu Group promotes the installation of "corporate 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 a reduction in costs and a reliable implementation of security measures are achieved.

Safe remote use of client devices
Client devices such as PCs 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 about remote device cautionary practice through monthly "Security Check Days" and annual information security training. In these cases, additional ICT measures that could be introduced include a "Virtual Desktop Service" which protects against information withdrawal and keeps important information secure when accessed through a remote client device.

When using a remote client device through the Virtual Desktop Service, the connection to the Internet is made through an internal server that enables exactly the same operations to be performed as if using an independent client device, such as using the information on the server or e-mail. Internal information displayed on client devices cannot be saved onto those devices. 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.

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 an application system called "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 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 photograph of the employee are printed on the face of the Security Card. Also, 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

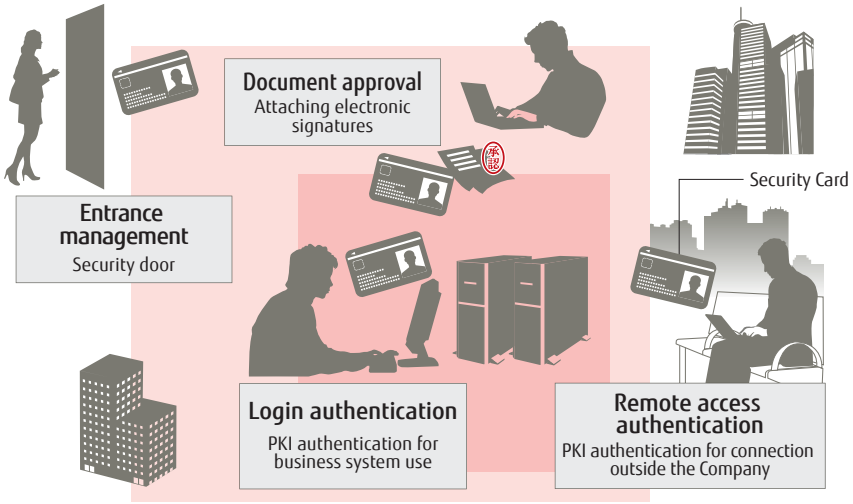
Employees are required to use the Security Card when accessing business systems that require authentication. Authentication by PKI at login to business systems enables secure identification and authentication of employees along with simple operation.

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.

▼ Using the Security Card



Network Security Control

The Internet is indispensable to business as a means for business communication, for publicity and information provision, or 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, 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
  - Inspection and authorization of individual connections in business groups
- Maintaining security during operation
  - Measures against unauthorized access (server configuration, checking the status of device management, 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

Employees are allowed to use e-mail to communicate with external addresses when it is needed for their roles. 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. Also, to prevent accidental use, communication using these services is continually monitored.

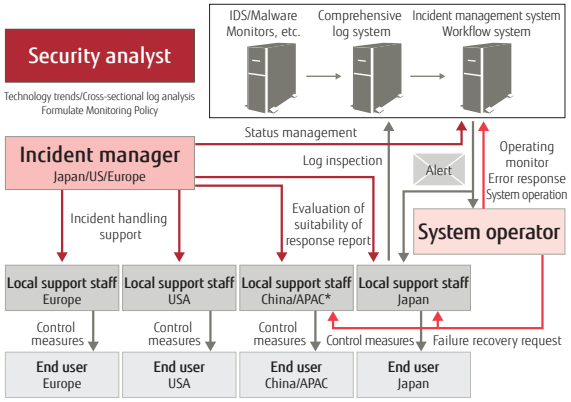
Intranet use control

The Fujitsu Group controls its intranet use because it recognizes that control of intranet use is an important factor as part of global control under the "Fujitsu Group Information Security Policy." The Fujitsu Group has a single intranet that connects all Group companies. 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:

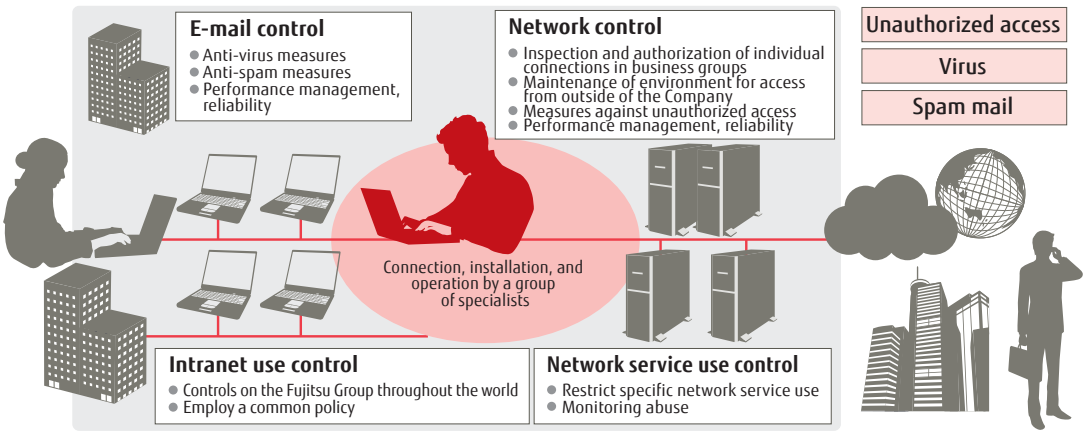
- Globally standardized risk guidelines and response processes
- Automatic evaluation of large volumes of items or logs
- SOC technicians stationed in all areas enable 24-hour response regardless of time zones
- Shorter response time due to a workflow system supporting connections between the incident 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.

3 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 provides a security management framework based on its information security management system to all related organizations and Group companies, as it presses ahead with security measures.

Our Approach to Establishing an Organization to Promote Information Security

The entire Fujitsu Group must devise measures and response policies to deal with the sophistication and diversification of cyber-attack threats and various types of business regulations enacted globally.

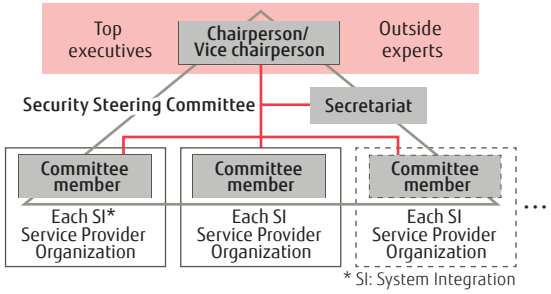
Consequently, Fujitsu launched the Security Steering Committee in 2013 to share information on cyber security and discuss our business policies.

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.

The committee discusses and approves policies for projects requiring a global-level response, including countermeasures to the threat of cyber-attacks and laws that cloud centers in each country must comply with, as well as how to handle personal information.

The Security Steering Committee is a substructure of the Information Security Council, which decides on the direction of the Fujitsu Group's security activities.

▼ Security Steering Committee Structure



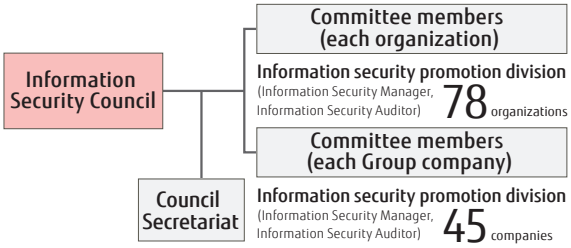
Information Security Council

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 Information Security Council (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 customer information assets and confidential information. Based on these guidelines, a council was established to maintain and promote information security. Every quarter, regular promotion meetings and liaison meetings are held for information security managers and information security auditors from participating organizations.

The head of the participating organizations shall be the person responsible for promoting information security. Furthermore, the Information Security Policy Council Secretariat (Council Secretariat) provides various assistance, as necessary, including support for effective measures and advice on enhancement initiatives needed to promote information security activities. This is to ensure proper information security activities in an efficient manner.

Through these council activities, participating organizations receive information and services related to information security. Conversely, each organization and Group company maintains the information security standards defined by management rules and promotes the information security activities stipulated by the participating organizations.

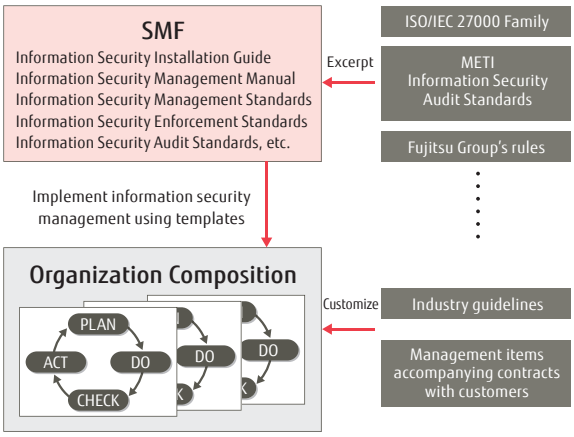
SMF (Security Management Framework)

At the Council, the SMF is provided as a template to implement information security management. The SMF includes 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 rules. 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 industry guidelines of customers with whom they have business relationships, administrative matters concerning contracts, and other factors. Each participating organization prepares information security-related documents covering its own information security management and audit standards, which have been optimized by incorporating the foregoing factors. Information security operations are conducted in line with these documents.

In fiscal 2013, ISO/IEC 27001 and 27002 were revised. Based on this, the SMF is scheduled to be updated in accordance with international standards.

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 provided to information security managers and information security promoters who promote and manage information security at each participating organization. Through this training program, which has been attended by 614 individuals to date, Fujitsu is working to promote information security management at each organization and Group company. In fiscal 2012, an e-learning program was also offered to encourage information security managers to continuously hone their own skills and participate in the training program. There have already been 588 participants in the e-learning program.

Furthermore, Information Security Auditor Training is provided to information security audit managers involved with internal audits, and internal auditors who conduct audits. To date, Information Security Auditor Training has been attended by 1,200 individuals.

In considering training options for auditors, Fujitsu actively encourages auditors to acquire auditor qualifications certified by the Japan Information Security Audit Association (JASA) in order to increase the quality of information security audits and move along their career path. By the end of last year, 137 employees had acquired auditor qualifications and are actively engaged in internal audits and committee audits. Aside from training for managers and auditors, we also provide common information security training materials to participating organizations, and each of these organizations utilizes them.

Maintaining Security Through IT Infrastructure Standard Operation Service

The Council has introduced Council standard PCs as a means of ensuring the continuous implementation of information security measures.

The Council Infrastructure Operation Service Division provides comprehensive services to each organization with an emphasis on maintaining information security across the entire PC lifecycle. This ranges from distributing PCs to employees, to PC installation support, daily operation and disposal.

With this service, when a problem is discovered through status monitoring, such as a PC with insufficient security measures, a PC that has not been used for a long period, or the installation of prohibited file sharing software, it is brought to the attention of the organization manager and user.

Furthermore, by undertaking PC repurposing and disposal tasks on behalf of employees, the organization performs batch data removal when disposing of PCs. Through these services, the organization reduces the workload of employees with respect to security measures, while mitigating security risks.

Periodic Security Checks

On Company-wide "Security Check Days" implemented 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 is installed in all PCs to diagnose the security measures and operational status of each PC.

When a PC is started, 19 diagnostic items (items including OS, viruses, passwords, encryption, and prohibited configuration items) are automatically checked, with the results displayed on the PC monitor. Furthermore, by having the information security managers of each organization confirm the results of all PCs, Fujitsu has effectively increased the penetration of security measures. This measure also reduces the workload of managers in confirming the status of PC security measures. The Council provides a security check sheet

for smart devices that conforms to Group-wide policy. The check sheet is used by various participating organizations to ensure smart-device security.

▼ Information Security Measure Diagnostic Results Screen (in Japanese)

Information Security Audits

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 Security Committee.

Through internal audits and committee audits conducted every year, Fujitsu confirms the penetration and entrenchment of information security management practices and the operational status and entrenchment of information security measures within the participating organizations.

Internal audits are led by auditors who have completed the aforementioned Information Security Auditor Training, and are conducted within each participating organization. External audits are positioned as external audits within the Council. These audits are carried out from an independent perspective, with audited organizations selected from a sample every year.

External audits are conducted by auditors who hold JASA auditor qualifications. When audits are performed, an audit team is formed by the Council Security Committee Secretariat and auditors who do not belong to the audited division. The audit team confirms the promotion of information security measures, identifies any deficiencies, and proposes improvements, among other activities.

Furthermore, strong points revealed by the audits are presented as notable examples of information security know-how within the Council at the Council Security Committee General Meeting. These best practices are then applied across the Council. Furthermore, from the previous fiscal year, committee audits have also implemented document audits of all participating organizations in addition to the on-site audits conducted previously. The goal is to enhance the quality of internal audits by regularly ascertaining the implementation status of these audits, and providing feedback to participating organizations.

In this manner, efforts are made to maintain and enhance information security throughout the Council by continuously implementing a combination of audits from different perspectives.

In other activities, the Council implements special audits of specific projects, as well as participating organizations. This is to address individual requests from participating organizations and to meet operational requirements. In special audits, experts from the Council Security Committee General Meeting Secretariat conduct an individual information security audit based on specific audit themes established according to the individual requests and operating requirements of the participating organization.

In-House Practices for Tablet Operation Management

The Fujitsu Group is promoting the use of tablets to transform work styles, aiming to discover new business scenes and find new sales expansion models.

As tablets are a greater security risk than conventional notebook PCs, users are required to have a raised level of security consciousness. We have instituted individual operational rules that maintain security without detracting from convenience and started executing a certification system for specified organizations.

Users need to do more than simply follow information security rules; they must acquire knowledge and skills related to tablet operation such as the reasons and objectives for using a tablet, ICT skills, intellectual property and SNS* utilization methods. They undergo training and tests and those who attain a certain skill level are recognized as eligible tablet users. Users maintain the aforementioned skills and confirm these annually for sustainable security maintenance and improvement. Conversely, users who cause security accidents are required to undertake appropriate training and testing to reaffirm their security awareness.

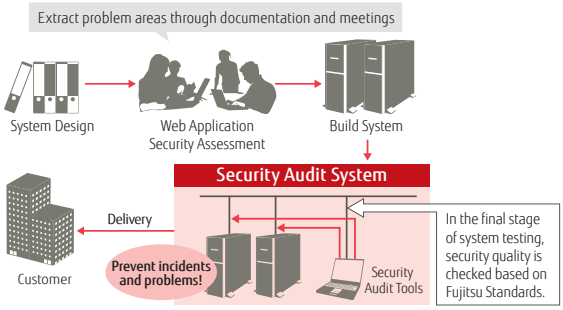
In addition, mobile device management rules are also applied and the Tablet Operation Secretariat confirms all tablet security measures are up-to-date.

* SNS: Social Networking Service

Security Audits for Systems Delivered to Customers

Fujitsu has established "Security Requirements for Customer Internet Connection Systems" (the "Security Requirements") and "Secure Web Guide" as a security measure for Internet connected systems delivered to customers. Systems integrators are obligated to ensure that the Security Requirements and Secure Web Guide are fulfilled before delivering systems to customers. In the process, specialized security departments objectively verify whether these systems meet these two guidelines.

▼ Security Audits for Systems Delivered to Customers



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

More specifically, to resolve any security problems related to web applications in the upstream process, security assessments are performed at the systems design stage. This ensures that the systems delivered to customers 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.

4 Initiatives Enhancing Security Quality in Services

To provide an Internet-based service, service providers must always respond to ever-changing security threats to ensure customers can use the service while feeling safe and secure. Fujitsu clarifies the security response items it should implement as a service provider and has instituted and audits guidelines and standards. In addition, it has established a dedicated organization to execute measures against incidents, and actively seeks impartial evaluation and information disclosures.

Establishment and Auditing of Guidelines and Measure Standards

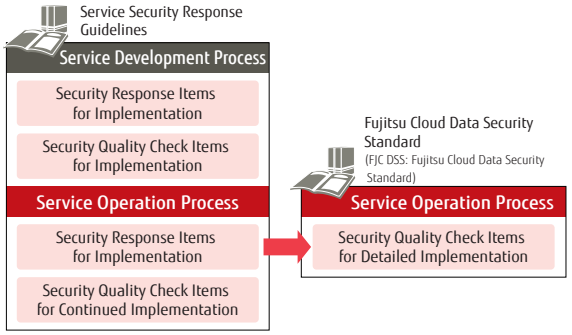
Fujitsu has established Service Security Response Guidelines, which are items that should be executed during the service development and operation processes to ensure the security quality of services provided to customers. Divisions providing services ensure security quality through practical application of the security measures displayed on the right, based on the contents of the guidelines.

Moreover, before starting services, auditing divisions audit the status of security measures to confirm that security quality is ensured.

Regarding service operations, we have established and abide by the "Fujitsu Cloud Data Security Standard" (FJC DSS), which provides a more detailed description of our security measurement standards for services, starting with cloud-based services. The FJC DSS is a set of standards we originally formulated based on global security standards, customer security requirements and technology cultivated through experience operating Fujitsu's cloud-based platforms. These are security measure standards that are applied in-house.

In addition, security audit divisions continually conduct regular security audits to check whether security quality is being ensured, and, if necessary, take corrective actions to ensure and continuously enhance security quality.

▼ Guidelines and Measure Standards



Fujitsu Cloud CERT Initiatives

In order to continue providing a "trusted" service as demanded by today's businesses, Fujitsu established "Fujitsu Cloud CERT" in 2010 as a team specializing in service security, starting with cloud-based services.

CERT is an abbreviation of Computer Emergency Response Team, and refers to a team of specialists who rapidly and accurately handle security emergencies that occur in a computer environment. Fujitsu Cloud CERT is the first cloud CERT organization in the world to be granted permission to use the CERT name publicly by Carnegie Mellon University in the USA.

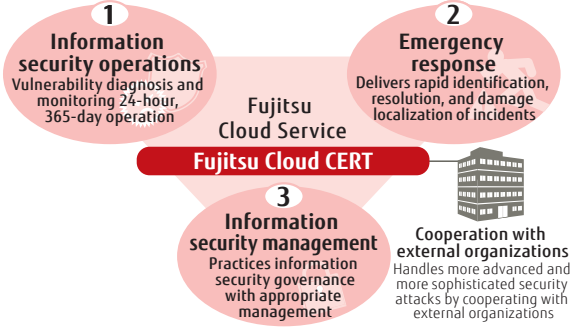
Fujitsu Cloud CERT performs the following activities on a global scale in order to support our customers' businesses and protect the cloud environment from various security threats.

1. Information security operation

In order for customers to securely use the Fujitsu cloud service, 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.

Moreover, even in environments where there are currently no known vulnerabilities, new vulnerabilities are discovered daily. Conducting regular security vulnerability diagnostics discovers these vulnerabilities in an objective manner and deals with them. Furthermore, a major feature of this activity is the implementation of risk control by continuously monitoring for vulnerable information and focusing on incident prevention through such means as timely patch applications. Constantly implementing these total security measures enhances security quality.

▼ Activities of Fujitsu Cloud CERT



2. Emergency response

In order to respond appropriately to unforeseeable security incidents, Fujitsu Cloud CERT has established response procedures for when an incident occurs. In the event of an incident, these procedures will be implemented to achieve rapid and accurate identification, resolution, and damage localization of the incident.

3. Information security management

In order to protect information important to our customers, Fujitsu Cloud CERT provides appropriate management of "people," "things," and "information" in the Fujitsu cloud service.

Fujitsu Cloud CERT is a member of security related organizations such as the Nippon CSIRT Association and the Forum of Incident Response and Security Teams (FIRST), and acts to improve global cloud security in conjunction with these organizations.

Third Party Evaluation and Disclosure of Information

Fujitsu discloses information on cloud security. One such activity is obtaining third party evaluations. For example, in the course of providing the FUJITSU Cloud IaaS Trusted Public S5* service globally, Fujitsu obtained Information Security Management System (ISMS) certification in divisions fulfilling key roles such as primary customer responses and datacenter operation. Furthermore, Fujitsu has published the white paper, "Fujitsu's Initiatives for Fujitsu Cloud Security Measure Standards."

*Fujitsu's public (IaaS) cloud service.

●●Column●●

"Symptomatic Treatment," "Definitive Treatment" and "Preventive Treatment" of Cyber-Attacks

Recently, we have received a growing number of inquiries about the best methods to protect against the increasingly sophisticated cyber-attacks on public internet servers. Neglecting management of public servers can result in information being stolen or websites being tampered with unknowingly, while the server could also be used as a stepping stone that makes it complicit in other cyber-attacks. This adversely affects a company's reputation and links to a loss of trust. Public servers can be attacked by anybody, anywhere around the world and consideration must be made of the fact that it's impossible to know when an attack will come. So, what kind of security is needed for a public server?

The first thing that most would suggest is setting up a firewall or installing an IPS*1 and WAF*2. Recently, next-generation firewalls that identify and control applications inside transmitted data have become an option. Point of contact defense against attacks is administered immediately, which makes it a highly effective measure on a limited scope. Note, however, that this is nothing more than "symptomatic treatment*3" and cannot be an effective measure when considered from a medium- to long-term perspective.

The next measure to consider is "definitive treatment*4." Definitive treatment is ascertaining where vulnerabilities lie in an application layer through a web vulnerability diagnostic (black box test) and source code review (white box test) that directly checks source code in a web application and repairs vulnerabilities. In the short-term, this method is laborious and treatment cost intensive, but, from the medium- and long-term perspective, it is an effective treatment.

Finally, preventative measures are important steps against cyber-attacks. Using the example of web application development, say the developer creates a secure design and is thorough with coding. We'll call this "built-in defense against vulnerabilities." Secure design in the upstream development process can reduce total costs. The importance of prevention has recently been attracting particular attention and initiatives in this regard are gaining greater priority.

Measure Features

	Immediate effect	Effect	Total cost performance
Symptomatic treatment	High	Medium	Low
Definitive treatment	Medium	High	Medium
Preventative treatment	Low	High	High

On the front lines of tackling cyber-attacks, continuous countermeasures are crucial as new threats and vulnerabilities are generated daily. Attack methods gain sophistication every day and designs that initially had no vulnerability can later become vulnerable. The first security measure of defense against cyber-attacks on a public server is "built-in defense against vulnerabilities," starting in the upstream development process (preventative treatment). Once the server has gone public and entered the operation process, in combination with such acts as continuous monitoring for vulnerabilities (preventative treatment), real-time vulnerability control through IPS and WAF (symptomatic treatment) and periodic vulnerability diagnosis and treatment (definitive treatment) should be conducted constantly. It is important to take the viewpoint of having a good balance between the short-, and medium- and long-term, so implement preventative measures, defend against any attack that may occur and move forward while eliminating anything that could be a cause.

*1 IPS: Intrusion Prevention System
*2 WAF: Web Application Firewall
*3 Symptomatic treatment is a medical term and refers to a type of medical treatment that relieves symptoms or avoids outbreaks.
*4 Definitive treatment is a medical treatment that describes measures to discover fundamental causes and eliminate disease rather than responding to symptoms.

5 Product Security

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

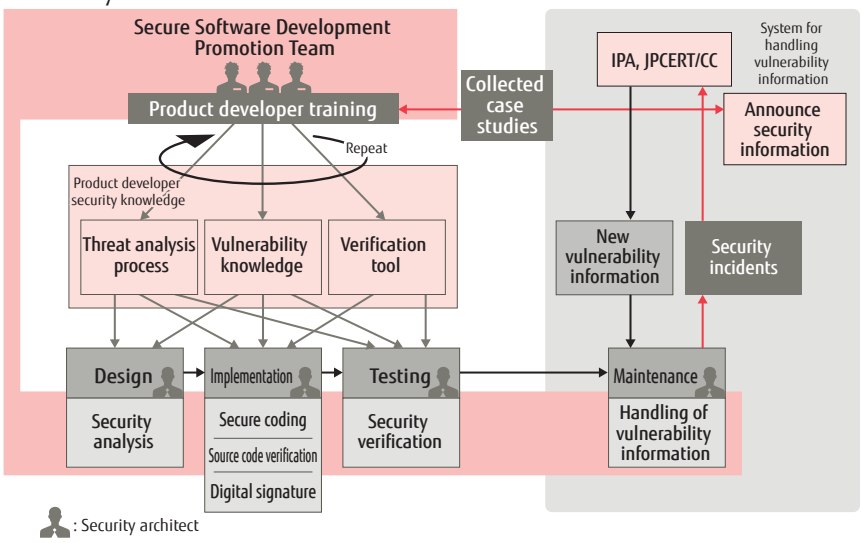
Software Security Quality Enhancement Initiatives

To improve the security quality of its software products, 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 publicizes 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



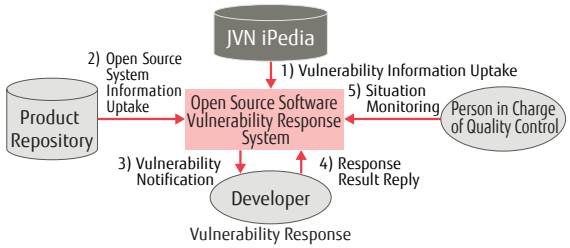
Ensuring Security in Shipped Products using Open Source Software

One part of the maintenance process referred to in 4. 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.

▼ Overview of the Open Source Software Vulnerability Response System



*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.

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
- Examples of Internal Breakdown Case Studies
- Research Reports by Expert Bodies
- Security Software Development Process (Latest information)

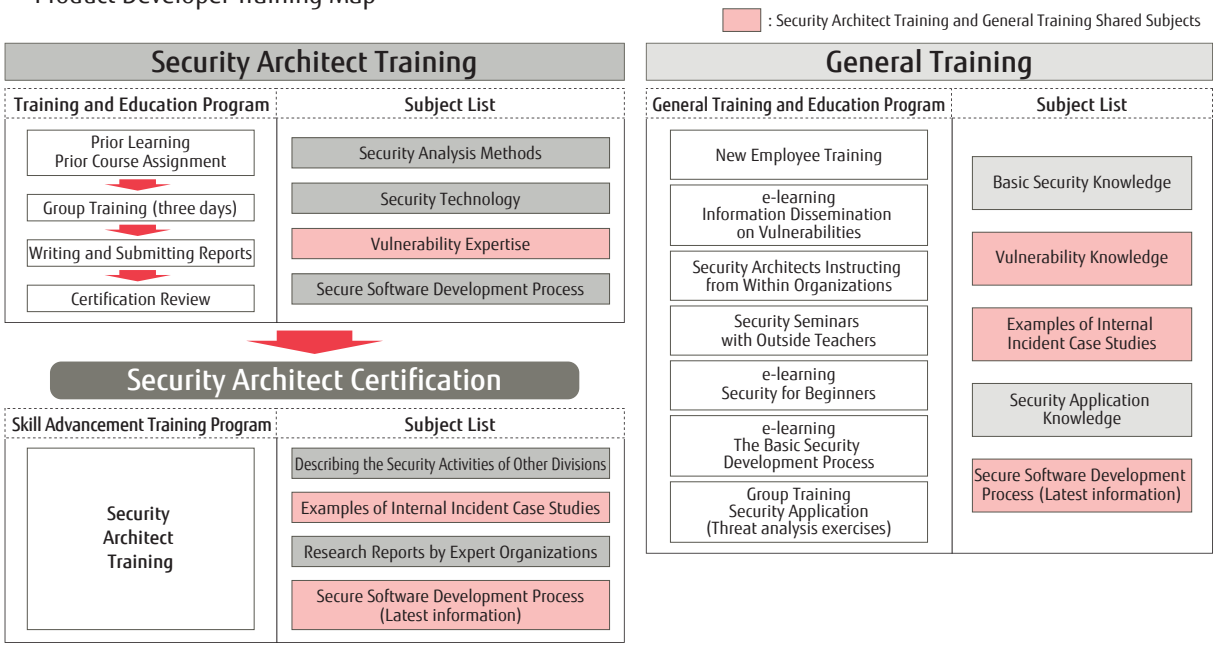
While striving to improve individual skills and update expertise through training programs, security architects exchanging information and opinions among themselves endeavor to raise their awareness.

General Training

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

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

▼ Product Developer Training Map



6 Research and Development into Security Technology for Supporting a Safe Lifestyle

New security technologies are being sought to protect and simultaneously utilize information, such as personal information, in the face of increasingly complicated and sophisticated cyber-attacks. Fujitsu Laboratories Ltd. responds to requirements for new technologies and develops sophisticated technologies.

Fujitsu Laboratories' Security Technology Initiatives

Fujitsu Laboratories is moving forward with security research. Its scope, for example, is expansive, extending from required technologies such as homomorphic cryptography, which enables processing and searching of encrypted data, and elemental technologies such as vein authentication in system security fields like privacy protection to countermeasures against cyber-attacks. Research results contribute significantly to the enhancement of security in the products and services that Fujitsu provides.

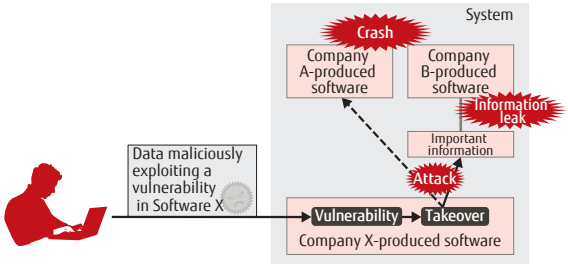
This report provides an introduction on a new inspection method using fuzzing to eliminate vulnerabilities and a new biocode technology capable of canceling biometric security if need be.

Technologies to Evaluate and Detect Unknown Vulnerabilities Submerged in Systems

Creating Secure ICT Systems

Cyber-attacks are a major issue for management in contemporary companies. Many cyber-attacks maliciously exploit software vulnerabilities to unleash their attacks. That has prompted Fujitsu Laboratories to undertake research and development into technologies for effective detection and elimination of unknown software vulnerabilities.

▼ Example of Malicious Use of Software Vulnerabilities in a Cyber-Attack



Evaluating Unknown Vulnerabilities Using Fuzzing

Systems are comprised of multilayered software from firmware to Web applications, so software with insufficient countermeasures against vulnerabilities may be incorporated carelessly, or unknown vulnerabilities may be discovered by a new technology that couldn't be envisaged at the time of development with the long-term operation of a system.

Recently, the fuzzing method has attracted attention as a technology to detect these system vulnerabilities during the product development stage through "evaluation" which simulates "attacks."

Fuzzing is a kind of black box test that involves providing "fuzz data," which is data that developers don't expect to be tested, to a system undergoing testing and monitoring any changes to detect vulnerabilities.

With fuzzing, failure to sufficiently account for test cases means there will be unlimited assessment data, and this cannot be evaluated in a realistic amount of time.

Fujitsu Laboratories developed the following technologies to counter this.

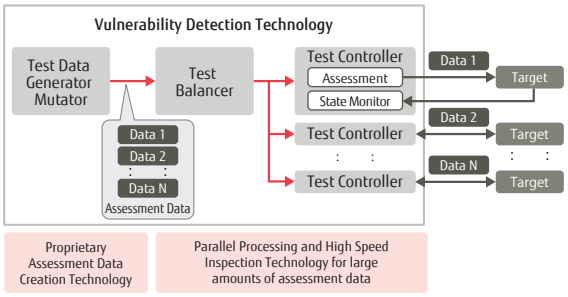
1. Assessment Data Creation Technology

The structure of data input for normal operations is automatically analyzed and separated into several parts to create assessment data with high likelihoods of discovering vulnerabilities like buffer overflow and integer overflow. Fujitsu Laboratories has conventionally used our proprietary expertise to detect many vulnerabilities and has reduced the amount of required assessment data necessary for a realistic timed evaluation.

2. Parallel Processing/High Speed Inspection Technology

Distributing large amounts of assessment data among multiple targets, inspecting them simultaneously, and then implementing high throughput inspection processing enables vulnerability detection within limited development times.

▼ Overview of Using Fuzzing to Detect Unknown Vulnerabilities Technology



The fuzzing test tool, including our research results, has already been put into operation, detecting vulnerabilities in multiple Fujitsu products under development, and it has been utilized on products as a pre-shipment countermeasure. Furthermore, since recent ICT systems include multi-vendor products, such as network switches, we have also evaluated other vendors' products and reported to them on the various vulnerabilities discovered so they can improve them.

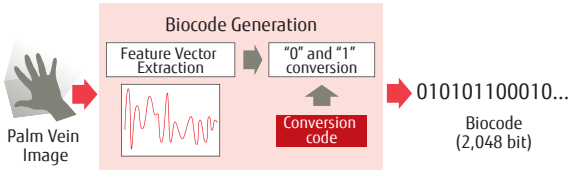
Biometric Authentication Technology using Biocode

Biocode Technology and Background

Biometric authentication technology has gained popularity in recent years as a technology to confirm identities. Biometric authentication technology uses one part of the body to confirm identities, but the biometric data used in identification cannot be changed, so it requires strict care when handling. To further expand use of biometric authentication there must be a technology to provide simpler handling of biometric information in authentication systems.

Fujitsu Laboratories developed a technology that extracts and matches 2048-bit biometric code (biocode) containing the features of the veins in the palm of the hand with high accuracy. In contrast to existing methods where processing involved comparing and matching palm vein feature patterns, it generates biocode where vein images are displayed in binary format, drastically accelerating the comparison and matching processes.

▼ Extracting Feature Code from Biometric Information



This technology uses a conversion code that generates a single piece of biometric information into multiple biocodes. For example, even in the case of leaked registered data, a new feature code can be generated and registered. The identification performance of this biocode has a false acceptance rate at the 1/100,000 level. Matching times among biocodes on a PC can be shortened from the existing several milliseconds to approx. 1 microsecond and data sized at 2048-bits enables use on IC cards and QR codes. The data size can be changed in accordance with the identification performance.

Technology that can generate multiple feature codes from a single piece of biometric data is known as "cancelable biometrics" or "renewable biometrics," and is being researched mainly in the EU, a leader in privacy protection. However, as biometric information collected by sensors is slightly different every time and variations occur depending on imaging or input conditions, identification performance can have a false acceptance rate at the 1/1,000 level. While using conventional pattern matching or image features, the rate of false acceptance diverged significantly from 1/100,000 to 1/1,000,000.

Newly Developed Technology

The two technologies developed, palm vein image normalization technology and feature code extraction technology, have been applied in the registration and matching processes in palm vein authentication.

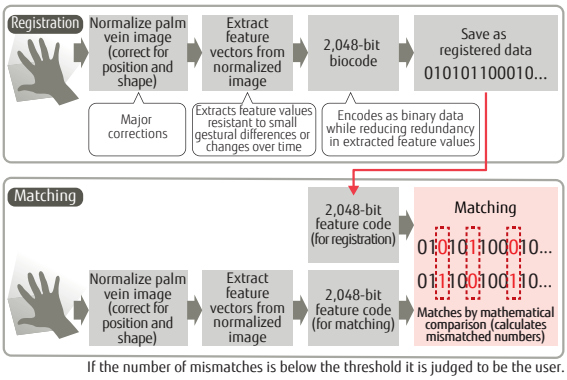
1. Palm Vein Image Normalization Technology

Palm vein image normalization uses hand contour information to correct for position and shape and converts palm vein images captured by the sensor into images where the hand is in a fixed position and shape.

2. Feature Code Extraction Technology

Feature code extraction segments the palm vein images and then extracts a vector of the vein pattern features from each region. Extracted feature vectors employ a data compression technology to extract a final feature code with 2,048 bits of data. It is difficult to reconstruct the original image from the extracted feature code.

▼ Overview of Palm Vein Authentication Using Biocode



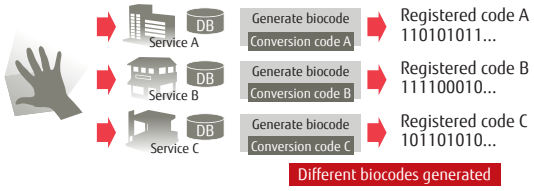
If the number of mismatches is below the threshold it is judged to be the user.

Results and Envisaged Applications

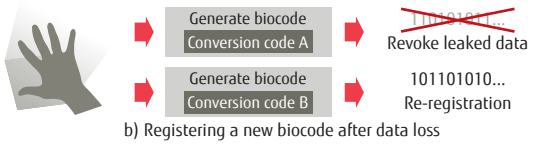
Using a conversion code to change from a biocode makes it possible to generate multiple feature codes from a single palm vein image and allows for use while changing passwords. As a different biocode can be used for each service, individuals can use the palm vein authentication with greater ease of mind.

As biometric systems using biocode technologies come further into widespread use, they are likely to be used in a wide range of services and scenarios, such as Internet access control and as a payment method in stores.

▼ Image of Applications of this Biometric Authentication Technology



a) Separate biocode registered for each service



b) Registering a new biocode after data loss

Going forward with the aim of commercializing this technology, Fujitsu Laboratories plans to further improve the image normalization technology and increase the accuracy of biocode extraction technology while going through technological improvement and studying a wide range of scenarios where biometric authentication can be applied.

7 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.

Through a never-ending accumulation of learning, 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 prevent information security incidents and any recurrence of past incidents. In doing so, the Fujitsu Group is pressing ahead with business activities that give due consideration to maintaining information security.

Fiscal 2013 Information Security Enhancement Initiatives

1. Business Partner Selection
2. Education and Raising Awareness
3. Confirmation of Information Security Status
4. Support for Responses to Information Security Incidents
5. Evaluation of Information Security Status
6. Sharing Information
7. Fujitsu Group Governance
8. Support for Overseas Business Partners

Information security incidents at business partners are declining as a result of the diffusion of information security rules and the promotion of measures based on continuous PDCA cycles.

Nevertheless, in recent years new threats of stealing information have arisen, targeting users with poor IT literacy and vulnerable devices and services.

The Fujitsu Group seeks to mitigate such new risks associated with information leaks relating to external services and servers, smart devices, and other factors, by maintaining an accurate grasp of the latest developments in the ICT environment. To prevent data loss, promotion of planning new information security measures is encouraged through training and other awareness raising activities.

1. Business Partner Selection

Selection of new business partners involves evaluation of candidate firms' information security readiness, and is limited to those business partners who consent to contractual requirements concerning information security management and handling of personal data in the course of outsourcing.

In regard to existing business partners, the Fujitsu Group also regularly selects outsourcers to which it entrusts personal information and conducts management and supervision of business partners' information security based on the Act on the Protection of Personal Information.

2. Education and Raising Awareness

■ Information security training seminars for business partners

In 2013, Fujitsu conducted training seminars based on the following theme: "Information Security Latest Trends and Measures," and centered around training sessions regarding threats to the latest ICT and countermeasures for these.

- Smart devices
- Social networking services (SNS)
- External services and servers
- Offshore development
- Targeted attacks
- BYOD (Bring Your Own Devices) and more

● Fiscal 2013: Approx. 1,200 participants from around 1,000 business partners (In places including Tokyo, Osaka, Nagoya and Fukuoka)

Furthermore, Fujitsu provided participants with training seminar materials featuring synthesized-speech narration. The goal is to have the participating suppliers make use of these materials as awareness-raising tools within their organizations.

■ Conducting out-of-office training for business partners

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

● Fiscal 2013: Training received by approx. 1,200 employees of around 40 business partners

■ Workshops for new graduate recruits of business partners

Fujitsu conducted workshops for new graduate recruits of major business partners. The workshops are designed to increase IT literacy through an information security basic training workshop using examples of information security accidents caused by using smartphones.

● Fiscal 2013: Approx. 200 employees of around 40 business partners (Tokyo and Osaka)

■Workshops for employees in leadership roles at major business partners

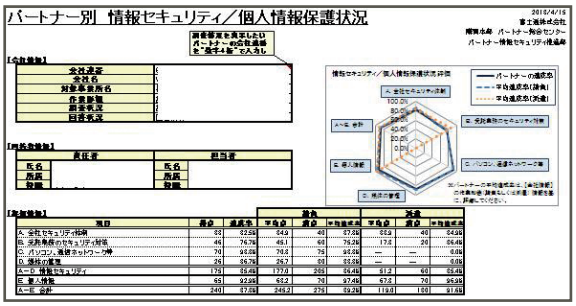
Fujitsu conducted workshops for employees in leadership roles at major business partners.

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, among other topics.

- Fiscal 2013: Approx. 60 employees of around 50 business partners (Tokyo and Osaka)

3. Confirmation of Information Security Status

Based on the basic contracts with its business partners, the Fujitsu Group undertakes regular confirmation of business partners' information security status. It also offers guidance on formulating and carrying out the resulting corrective measures; and follows up on the corrective measures.



Furthermore, the Group makes corrective recommendations and follows up on corrective actions when a business partner experiences an information security incident.

In addition, at the request of clients and others, Fujitsu conducts audits encompassing information security requirements of business partners, projects, and so forth. The Group also conducts annual information security status surveys (including personal data management) targeting all business partners.

- Fiscal 2013 audits: Approx. 130 business partners
- Fiscal 2013 status surveys: Approx. 1,500 business partners

4. Support for Responses to Information Security Incidents

In the event of an information security incident, the Fujitsu Group cooperates with the relevant frontline division, including the affected business partner, to perform an initial investigation (such as assessing the impact of leaks), and to otherwise assist with corrective responses.

5. Evaluation of Information Security Status

The Fujitsu Group evaluates business partners' information security based on status confirmations, and responses to information security incidents, etc. In the event of serious incidents or situations where no improvement is evident, the Group may review the business relationship or suspend new orders with the business partner, as necessary.

6. Sharing Information

The Fujitsu Group designates information security officers for business partners, and undertakes timely sharing of the latest information security-related information including throughout the Fujitsu Group.

- For the purpose of sharing the latest news on information security with business partners and raising awareness, Fujitsu has published the "Information Security Plaza" and distributed awareness-raising posters every two months since April 2009.

▼Issued in November 2013
"Information Security Plaza" and awareness poster

7. Fujitsu Group Governance

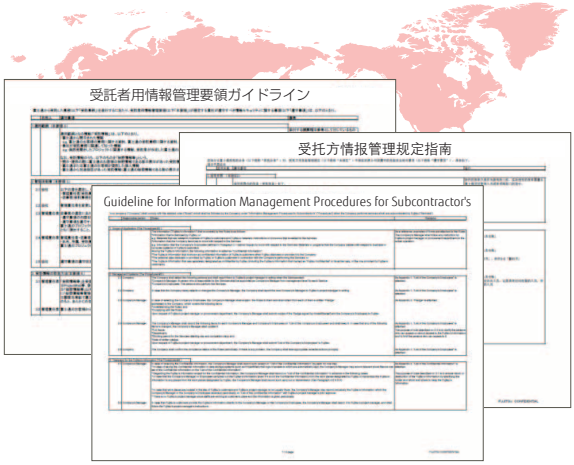
Measures to strengthen the information security at the Fujitsu Group's business partners are promoted throughout the entire Group.

Intra-Group information security liaison committee meetings are held quarterly, sharing information on case studies of information security incidents and other matters, and striving to formulate and share even more effective preventive measures and policies.

8. Support for Overseas Business Partners

In recent years, opportunities have increased for offshore development through cooperation with overseas business partners aimed at curtailing development costs and supporting global products.

Fujitsu is striving to maintain information security by exchanging the "Information Management Procedure for Business Partners" with global business partners (English-speaking areas and China). This procedure requires overseas business partners to follow the same promotion of information security policies, as well as initiatives for determining country risk and responding to this.



8 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 SOLUTIONS TOKAI 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 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
ZIS INFORMATION TECHNOLOGY CORPORATION
FUJITSU SYSTEMS EAST LIMITED
FUJITSU SYSTEMS WEST LIMITED
FUJITSU GENERAL LIMITED
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
FUJITSU RESEARCH INSTITUTE
FUJITSU DEFENSE SYSTEMS ENGINEERING LIMITED
TOYAMA FUJITSU LIMITED
NIFTY CORPORATION
FUJITSU NETWORK SOLUTIONS LIMITED
FUJITSU PUBLIC SOLUTIONS LIMITED
BANKING CHANNEL SOLUTIONS LIMITED
FUJITSU BROAD SOLUTION & CONSULTING INC.
PFU LIMITED
FUJITSU MARKETING LIMITED
FUJITSU MISSION CRITICAL SYSTEMS LIMITED
FUJITSU MIDDLEWARE LIMITED
FUJITSU MOBILE-PHONE PRODUCTS 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 Information Processing Development Corporation (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.

<148 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.

<137 people>

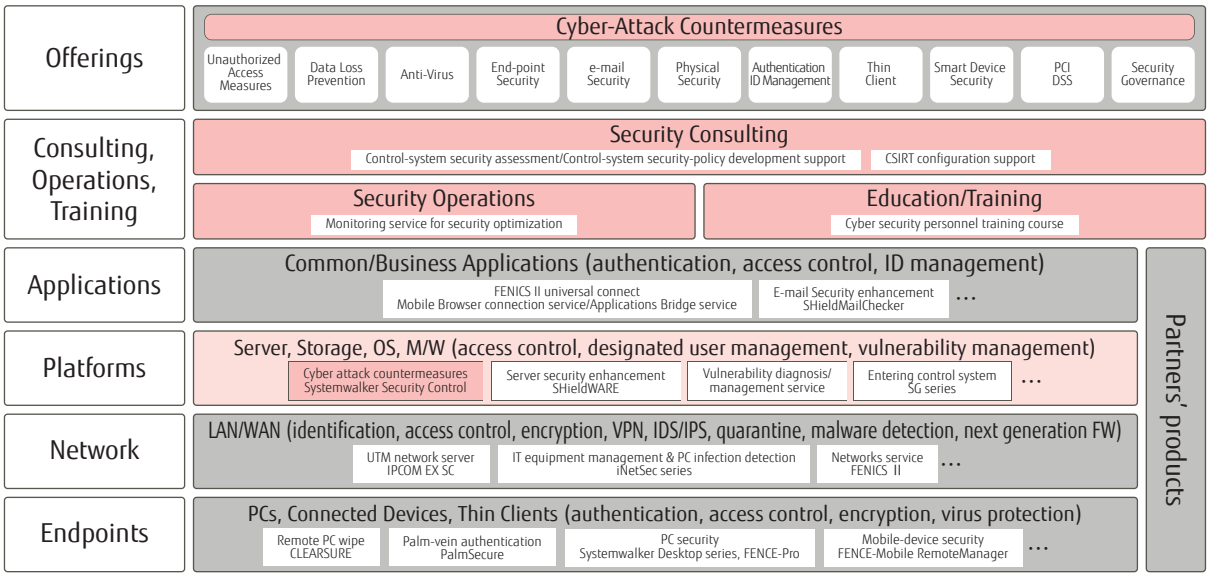
*CAIS: Certified Auditor of Information Security

9 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 which 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

Security Technology 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/