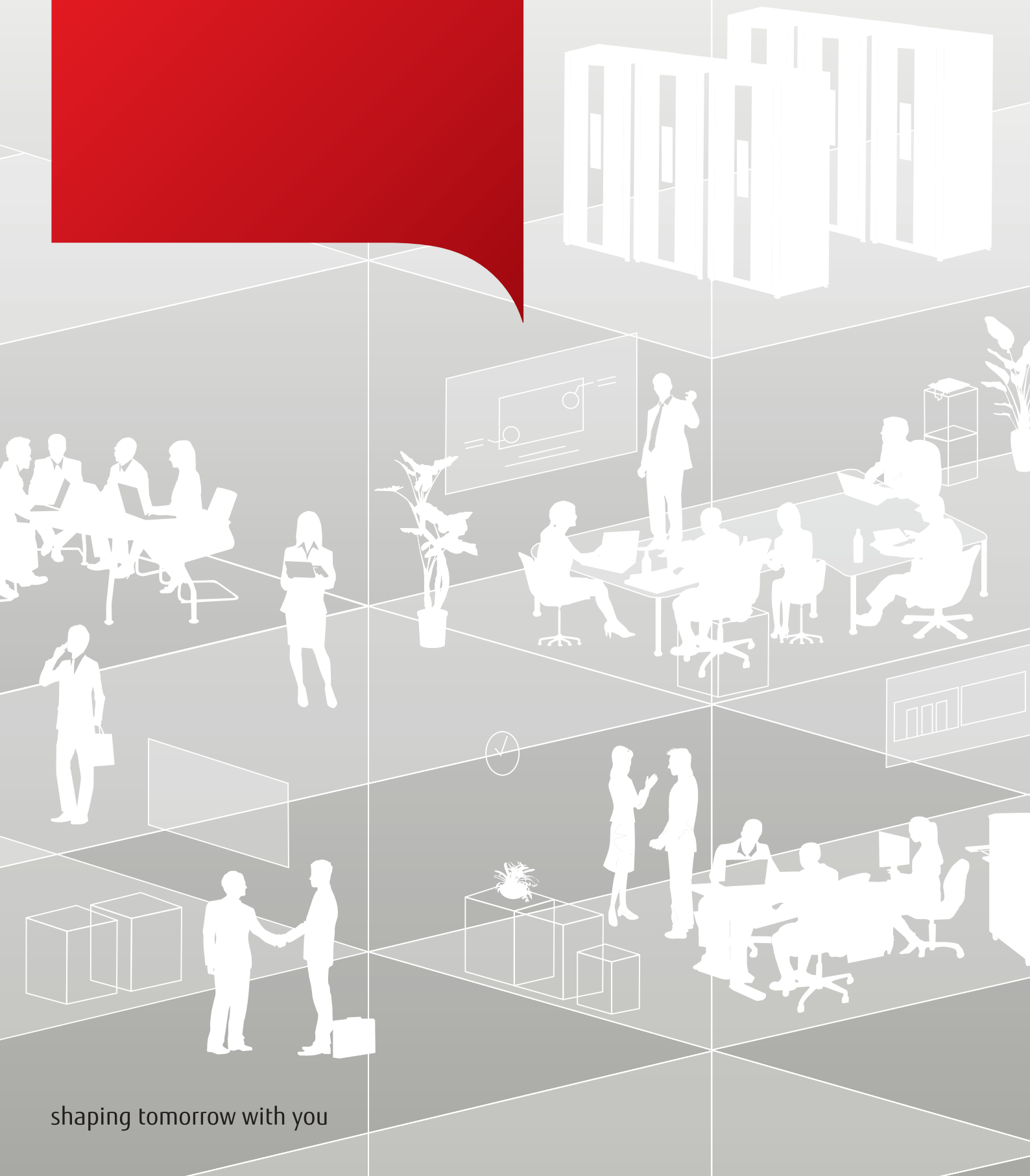
Fujitsu Group Information Security Report 2013

FUJITSU



shaping tomorrow with you

Fujitsu Group Information Security Report 2013

CONTENTS

Report Summary

Target Period and Scope of the Report

This report covers the period up to March 2013 and focuses on efforts in information security by the Fujitsu Group.

Report Publication Date

This report was published in August 2013.

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.

Advancements in Information and Communication Technology (ICT) have turned people's dreams into reality. This progress has created a global-scale network community that knows no bounds and has changed business, changed lifestyles, and greatly changed society. And today, ICT applications are entering a new era brought about by the popularization of smart devices and cloud computing technology.

As an enterprise supporting ICT infrastructure, the Fujitsu Group aims to realize a "Human Centric Intelligent Society," a prosperous society where people can live with peace of mind, by constantly pursuing the possibilities of human-centric ICT and continuously creating new value.

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 five related set of rules 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 2013" 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

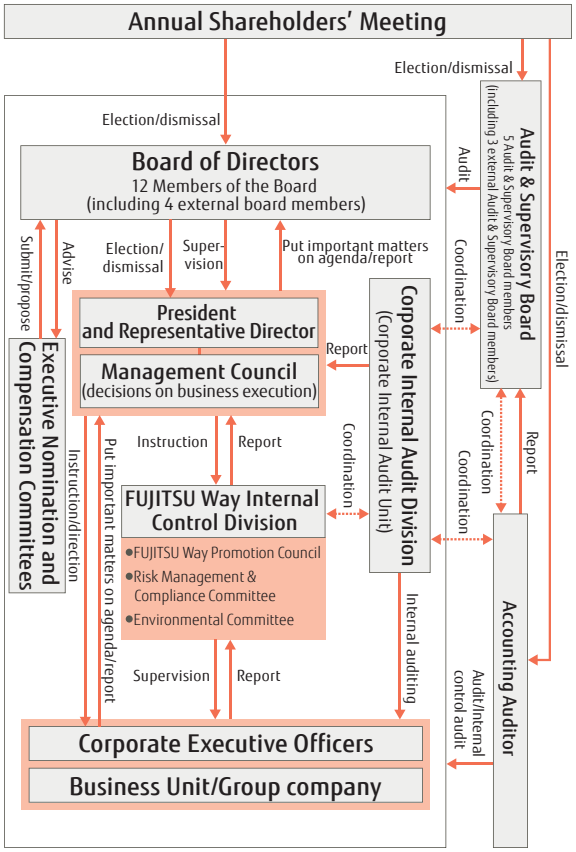
Corporate Governance

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.

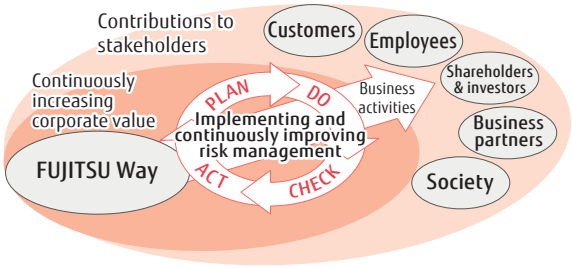
▼ Corporate Governance Framework



Risk Management

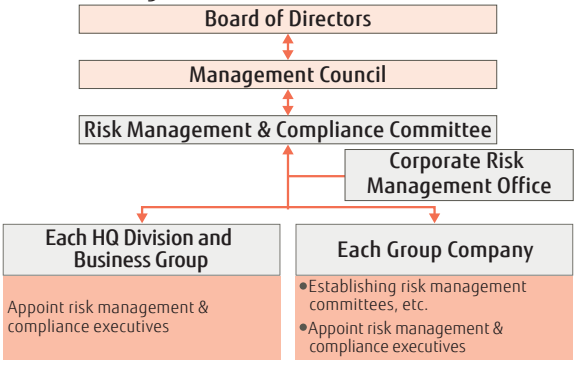
Through its global activities in the ICT industry, the Fujitsu Group continuously seeks to increase its corporate value, and to contribute to its customers, local communities and all other stakeholders. Properly assessing and dealing with the risks that threaten the achievement of these goals is assigned a high priority by management. Accordingly, we have put in place a Group-wide risk management system in accordance with the FUJITSU Way, along with promoting activities designed to prevent risk and minimize the impact when risks materialize. In this manner, we are executing and continuously improving on our Group-wide risk management.

▼ Implementing and continuously improving risk management



Furthermore, in July 2012, the Fujitsu Group integrated the existing Risk Management Committee and the Compliance Committee to form the new Risk Management & Compliance Committee. The goal is to unify and strengthen the global risk management and compliance system. The Risk Management & Compliance Committee appoints Risk Management & 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



Information Security

Information Security Policy and Related Rules

The Fujitsu Group has established the "Fujitsu Group Information Security Policy," as a consistent policy throughout the world, and is promoting information security in accordance with the policy.

Based on the "Fujitsu Group Information Security Policy," we have put in place five related sets of rules to guide the implementation of information security measures.

Fujitsu Group Information Security Policy

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.

- 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.
- 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.
- 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.

Activity Principles

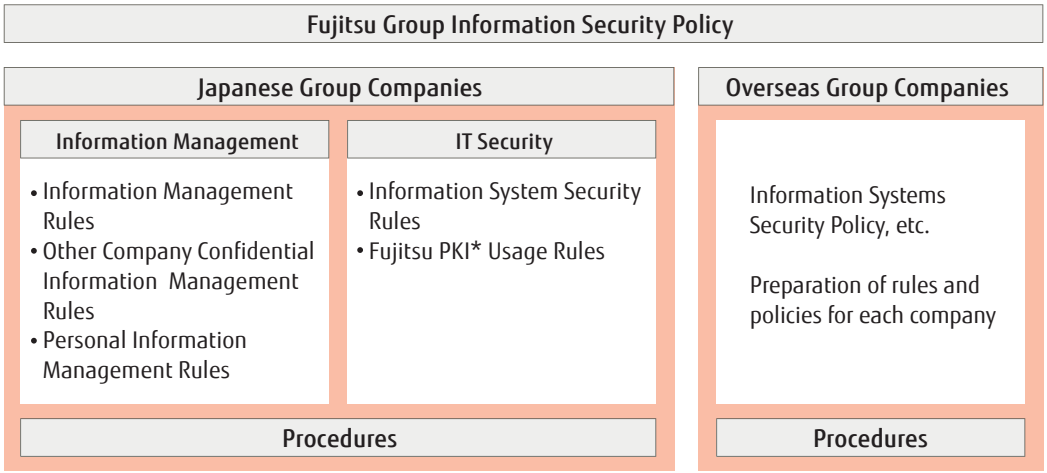
The Fujitsu Group applies the following principles when conducting information security activities.

- Preservation of confidentiality, integrity and availability shall be the objective of information security, and information security measures shall be planned to meet this objective.
- The organizational structure and responsibilities shall be clearly defined to ensure the proper implementation of information security measures.
- 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.
- Information security processes shall be organized into Plan, Do, Check and Act phases to maintain and enhance the level of information security.
- 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.

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 advancements 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

Guided by the common Group-wide slogan, "Pledge to Enforce Rigorous Information Management: Information Management Is the Lifeline of the Fujitsu Group," Fujitsu and its domestic Group companies have been working to increase information security awareness at the individual employee level by displaying posters at each business location, affixing information security awareness stickers to all business PCs used by employees, and other measures.

Within the Company, the activity status of divisions implementing measures for effective information security is disclosed on the intranet as reference examples, as a means of encouraging each division to promote voluntary security promotion activities.

Also, a mail checker 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 general public has seen a large number of incidents of information leakage and loss take place recently. 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

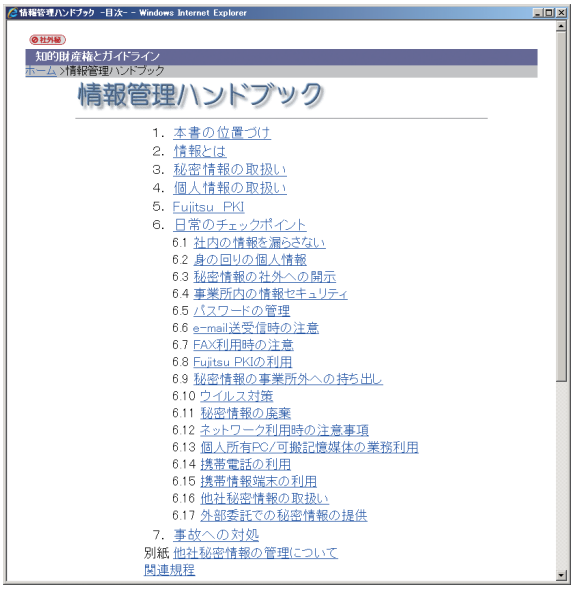
Fujitsu has established the "Personal Data Protection Policy" and "Personal Information Management Rules" in compliance with the Act on the Protection of Personal Information. We are also continually strengthening the system for protecting personal information based on these rules, such as by conducting 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)



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.

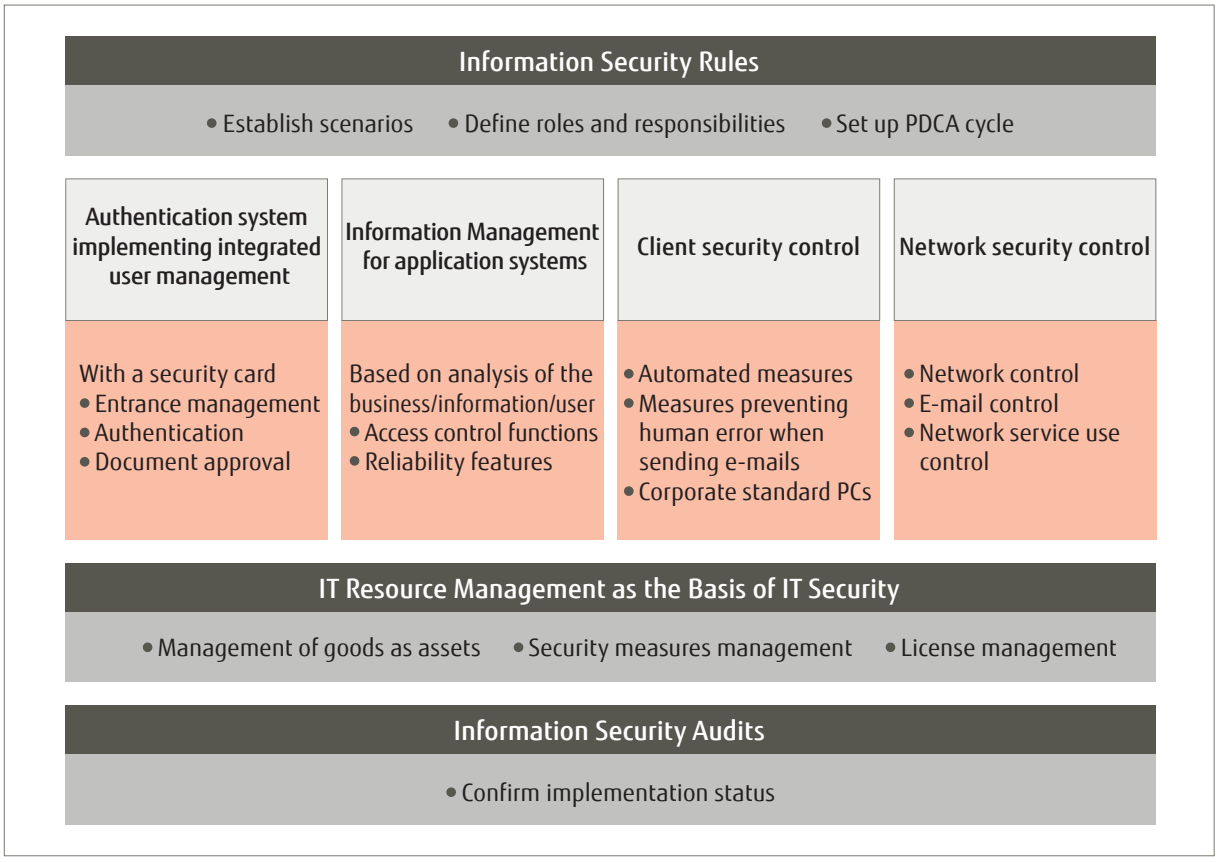
The Fujitsu Group strives to incorporate IT security measures into the business environment and business procedures as much as possible. Importantly, we believe that this allows employees to focus on their core duties.

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



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.

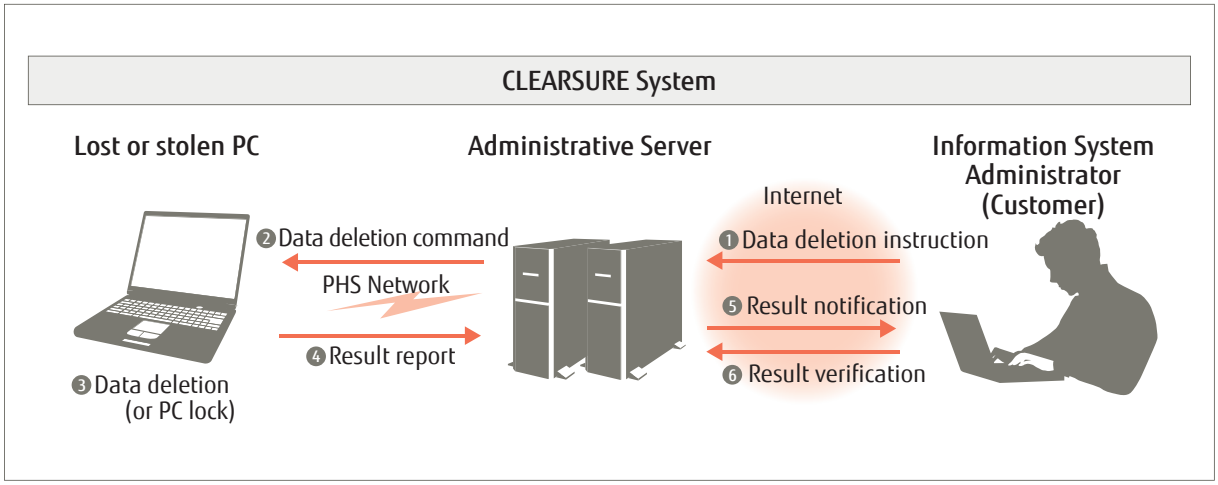
Installation of corporate standard PCs

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. Furthermore, as a measure for the loss or theft of laptop PCs, corporate standard PCs are equipped with a function to remotely invalidate data on laptop PCs.

This significantly reduces the possibility of information leakage in case of loss or theft of a PC. This feature is provided to customers as the remote data erasure solution "CLEARSURE."

▼ Measures Against Laptop PC Loss or Theft



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

Authentication

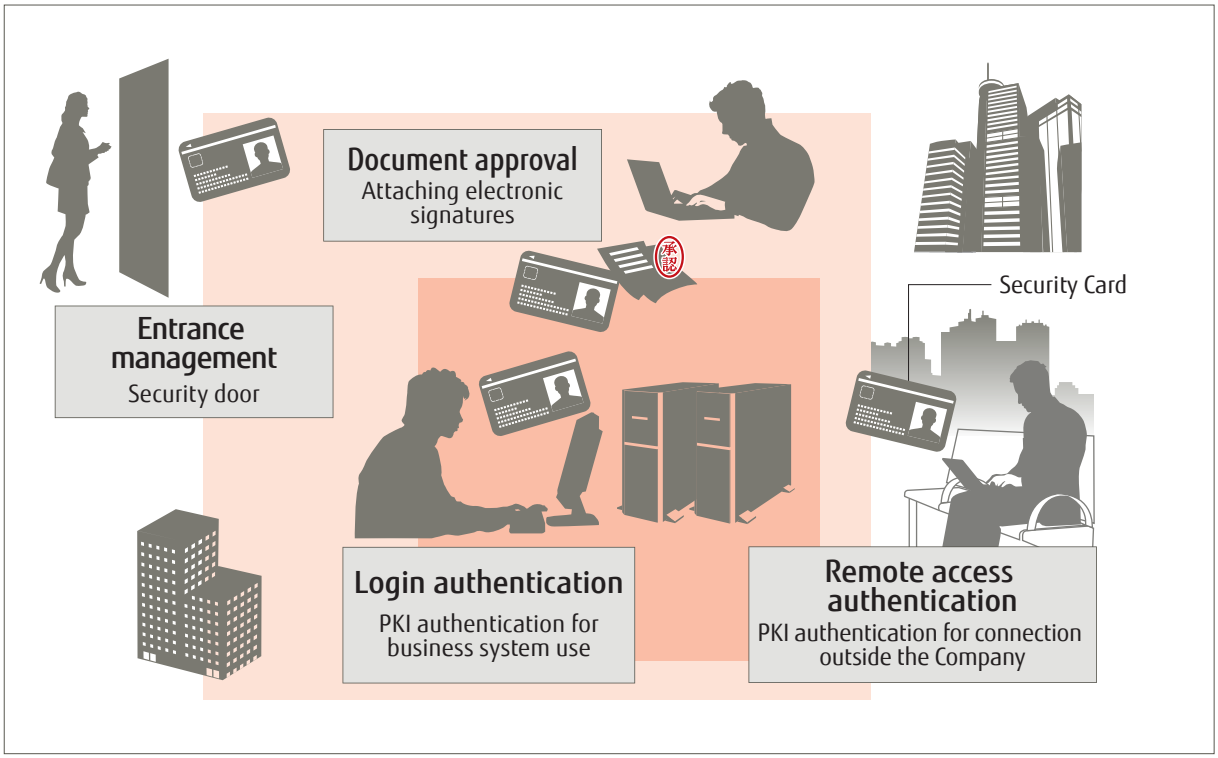
Employees are required to use the Security Card when accessing business systems that require authentication. Authentication by PKI at login to business systems enables secure identification and authentication of employees along with simple operation.

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

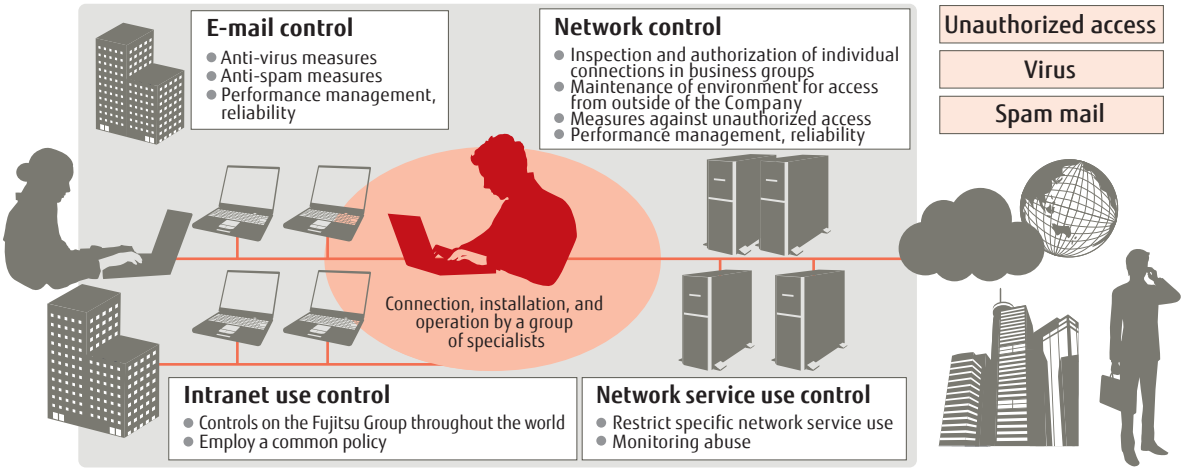
Network service use control

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

Intranet use is controlled throughout the Fujitsu Group. The construction and use of intranets by Group companies around the world are controlled based on a common policy and management measures. This is an example of a global control measure based on the "Fujitsu Group Information Security Policy."

▼ 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.

Security Measures for Cloud Services

Cloud computing is a new processing scheme to realize a flexibility and agility of computing that is not possible in traditional systems. However, the shift to cloud computing presents new problems, such as issues with security and reliability, to the user. This section introduces the security initiatives implemented by Fujitsu in cloud computing services.

Challenges of Cloud Computing

Cloud computing has a beneficial impact on business in speeding up management, facilitating the deployment of ICT in new businesses, and in other ways. On the other hand, companies must address security threats unique to this new service format. For example, cloud services host numerous user accounts and multiple users' data on the same IT resources. Therefore, security incidents could have a potentially larger impact. Other concerns include attacks that take advantage of the vulnerabilities of virtualization technologies used in cloud systems, attacks on third parties through the malicious use of cloud resources, as well as misconduct within cloud service providers that support cloud infrastructure.

To counter these threats, it is important to consider conventional security by implementing border defenses and multilayered defenses in the network, servers, and web applications. However, it is also necessary to consider security in light of factors specific to cloud services, such as addressing risks related to virtualization technology and operational and management responses to changes in the scope of responsibility for IT resources. When providing cloud services, Fujitsu strives to ensure security from both organizational and technical perspectives.

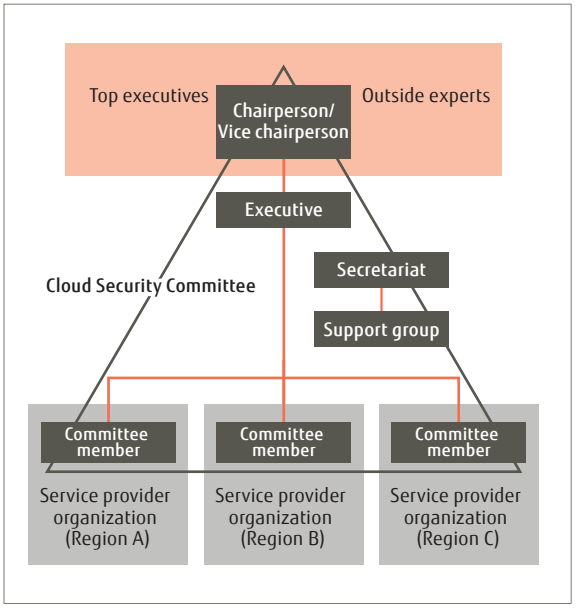
Fujitsu Global Cloud Platform (FGCP) Initiatives

Fujitsu provides two types of public cloud services: FGCP/S5, which is an infrastructure as a service; and FGCP/A5, which is a platform as a service. When providing these two services, Fujitsu adopts the eight perspectives shown in the diagram below as security measures supporting its service infrastructure. Of these, we present the following two perspectives: the organization for security and information security incident management.

▼ Overview of Security Measures for FGCP Service Platform Covering Eight Perspectives

Information security policy	Organization for security	Human resources security
Physical and environmental security	Acquisition, development, and maintenance of information systems	Information security incident management
Business continuity management	Compliance	Resource management
Access control	Communications and operations management	

▼ Cloud Security Committee



In the course of providing cloud services, Fujitsu established a Cloud Security Committee as an internal committee in 2011. As shown in the diagram to the right, the committee is chaired by Fujitsu management, and comprises external experts to ensure objectivity, and the heads of each organization providing services. The committee discusses and approves policies on matters that require a response on a global level, such as applicable laws and handling of personal information at cloud centers in each country, in addition to cyber-terrorism, unauthorized use and other threats.

Furthermore, when security incidents occur within a cloud, it is crucial to make decisions and take action to minimize the extent of the impact. Fujitsu has set up an incident response structure encompassing overseas operations, and conducts training drills. Fujitsu Cloud CERT (Computer Emergency Response Team), a team of cloud security specialists, plays a crucial role in undertaking security measures that are common to these services. Fujitsu Cloud CERT will be covered on the following page.

Security Initiatives for Each Service

FGCP/S5 and FGCP/A5 incorporate security measures according to the characteristics of each service. The security functions provided by these two services are based on the three perspectives shown in the diagram below. These functions enable users to achieve secure systems development and operation using cloud services.

▼ Three Perspectives of Security Functions Provided by FGCP

Information security policy	Organization for security	Human resources security
Physical and environmental security	Acquisition, development, and maintenance of information systems	Information security incident management
Business continuity management	Compliance	Resource management
Access control	Communications and operations management	

In Fujitsu's cloud services, users configure virtual systems and operate execution environments at a service portal site. At the portal site, customers can use functions that support resource management, such as displaying lists of systems and resources in operation.

Furthermore, privilege management is crucial to controlling access. Here, users can flexibly establish privileges according to the organization. For example, FGCP/S5 provides a function that enables users to customize how privileges are granted to resource administrators.

Users can set privileges for each user ID by adding or deleting accessible resources. Because users conduct systems development and operation via the Internet, communications must be protected by encryption and other functions. Furthermore, FGCP/S5 enables secure systems comprising a three-tier structure of Web, applications, and database. Through these features, Fujitsu provides highly secure systems that offer the same level of security as an on-premise environment.

Fujitsu Cloud CERT Initiatives

In order to implement a "trusted" cloud as demanded by today's businesses, Fujitsu established "Fujitsu Cloud CERT" in 2010 as a team specializing in cloud security. 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 information security measures, including vulnerability diagnosis and monitoring of the cloud service infrastructure, and operates under a 24-hour, 365-day system.

2. Emergency response

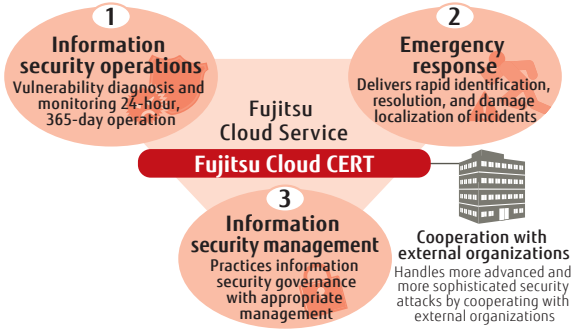
In order to respond appropriately to unforeseeable security incidents, Fujitsu Cloud CERT has established response procedures for when an incident occurs. In the event of an incident, these procedures will be implemented to achieve rapid and accurate identification, resolution, and damage localization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

▼ Activities of Fujitsu Cloud CERT



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 FGCP/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 "Approach to Information Security for the Cloud" white paper.

Approach of Fujitsu Solution Business Group

Fujitsu's Solution Business Group (SBG) is called upon to maintain an even higher level of information management than the rest of the Fujitsu Group because it has many more opportunities to handle customers' information assets and personal data. That is why the SBG provides a security management framework based on its information security management system to all SBG divisions and Group companies, as it presses ahead with security measures.

SBG Characteristics

The SBG provides solutions and system integration services focused on information system consulting and integration, and infrastructure services centered on outsourcing services.

Fujitsu's services business holds the leading market share in Japan and the third-largest share worldwide. We provide services across a wide range of countries and regions, including Europe, the Americas, Asia and Oceania.

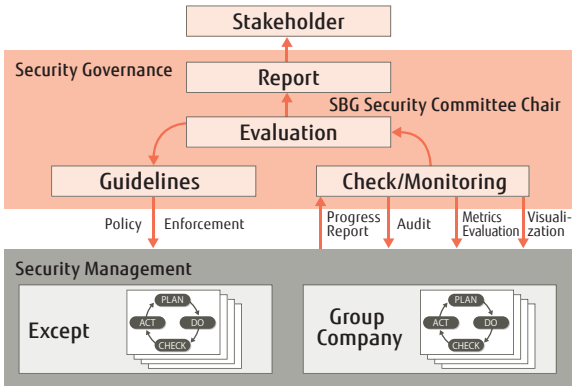
In the outsourcing field in particular, datacenters are set up in approximately 100 bases in 16 countries around the world, focusing on Japan and Europe. These datacenters provide services that answer a variety of needs such as reducing the operational workload of customer ICT and supporting their environmental priorities.

Development and Execution of SBG 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 developing an information security governance framework in tandem with promoting security initiatives.

The SBG Security Committee is attended by various sales and system engineering (SE) operations divisions and Group companies comprising the SBG. The SBG Security Committee Chair establishes the overall direction for information security activities. Based on this direction, divisions and Group companies conduct a range of activities based on the Security Management Framework (SMF: See next page for details). These activities include formulating security plans, introducing security measures, promoting information security activities within the divisions and Group companies, and conducting internal audits. The SBG Security Committee also strives to improve the management framework and security measures by confirming and evaluating the status of daily information security activities and security incidents and accidents.

▼ SBG Information Security Governance



SBG Information Security Management Promotion System

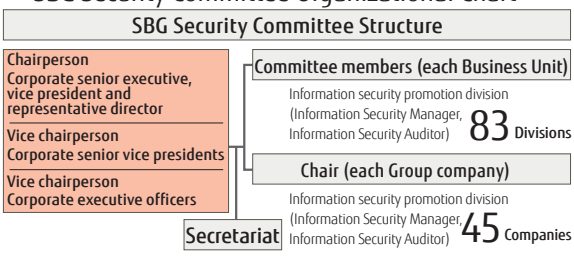
The SBG has established the "Solution Business Group Information Security Policy" with the goal of sound protection of customers' information and internal information in order to handle customers' information assets and confidential information. Based on this policy, the SBG Security Committee was established to maintain and promote information security. Every quarter, a meeting is held of the SBG Security Committee Chair, information security managers from each division and Group company, and information security audit managers.

Heads of each division and Group company presidents promote information security management as SMF managers.

Furthermore, the SBG Security Committee 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 that each division and Group company is able to conduct proper information security activities smoothly.

Through these SBG Security Committee activities, each division and Group company receives information and services related to information security. Conversely, each division and Group company maintains the information security standards defined by the SBG by promoting the information security activities that the committee requests.

▼ SBG Security Committee Organizational Chart

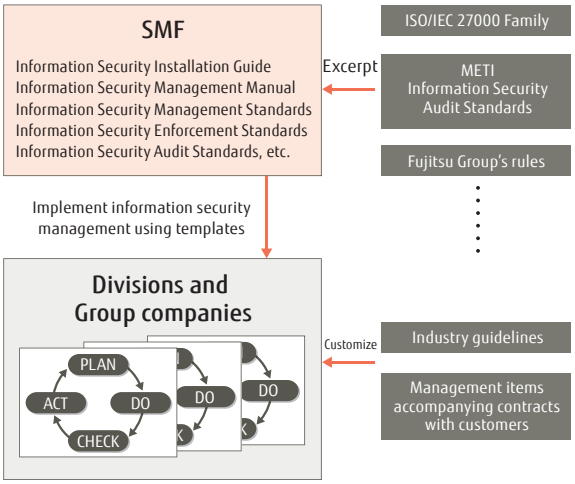


SMF (Security Management Framework)

At the SBG, 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. Each division and Group company 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 division and Group company prepares information security-related documents covering their own division's 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 2012, the Fujitsu Group's rules were updated, accompanied by revisions to the SMF documents and revisions to the SMF documents and audit checklists. 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 division and Group company. Through this training program, which has been attended by 596 individuals to date, Fujitsu is working to promote information security management at each division 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 for the first time. There were 397 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 1,100 individuals, who are now actively engaged in internal audits of divisions and Group companies.

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 advance their careers. To date, 127 employees have acquired auditor qualifications and are actively engaged in internal audits and committee audits. Besides training for managers and auditors, the SBG provides standard training materials common to all of the SBG, which are used in each division.

Maintaining Security Through IT Infrastructure Standard Operation Service

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

The SBG Infrastructure Operation Service Division provides comprehensive services to each division 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 division manager and user.

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

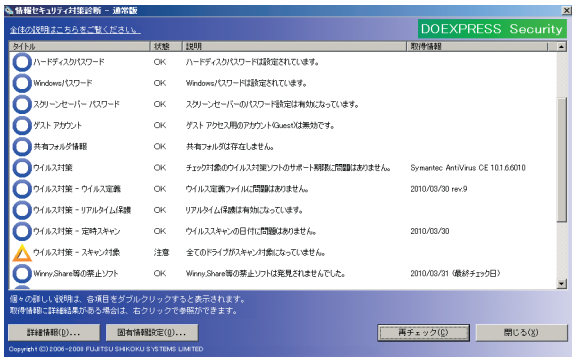
Periodic Security Checks

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 SBG, the information security measure diagnostic tool (DOEXPRESS Security) is installed in all PCs to diagnose the security measures and operational status of each PC. When a PC is started, the diagnostic items

(21 items including OS, viruses, passwords, encryption, and prohibited configuration items) are automatically checked and diagnosed with the results displayed on the PC monitor. Furthermore, by having the information security managers of each division confirm the diagnostic results of all PCs, Fujitsu has effectively increased the penetration of security measures. This measure has also reduced the workload of managers in confirming the status of PC security measures.

The SBG provides a security check sheet for smart devices that conforms to Company-wide policy. The check sheet is used by various divisions 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 divisions and Group companies themselves, and committee audits of the divisions and Group companies conducted by the SBG 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 SBG.

Internal audits are led by auditors who have completed the aforementioned Information Security Auditor Training, and are conducted within each business division and Group company. Committee audits are positioned as external audits within the Fujitsu Group. These audits are carried out from an independent perspective, with audited divisions selected from a sample every year.

Committee audits are conducted by auditors who hold JASA auditor qualifications. When audits are performed, an audit team is formed by the SBG 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 SBG at the SBG Security Committee General Meeting. These best practices are then applied across the SBG.

Furthermore, from the previous fiscal year, committee audits have also implemented document audits of all SBG divisions and Group companies 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 divisions and Group companies.

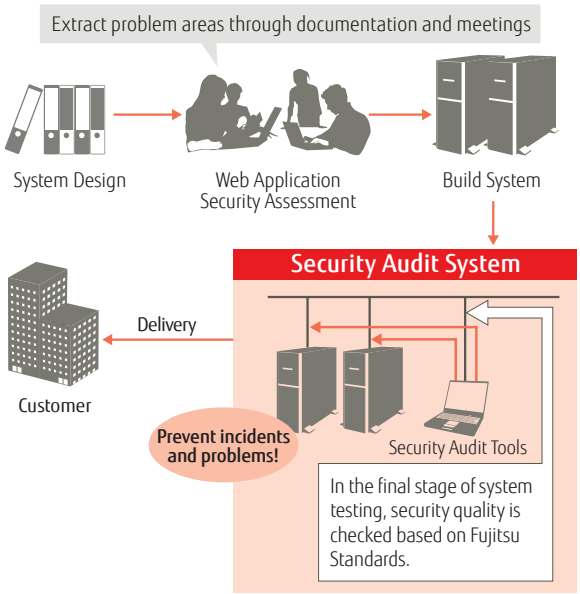
In this manner, efforts are made to maintain and enhance information security throughout the SBG by continuously implementing a combination of audits from different perspectives.

In other activities, the SBG implements special audits of specific projects, as well as divisions and Group companies. This is to address individual requests from divisions and Group companies and to meet operational requirements. In special audits, experts from the SBG 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 Group company.

Security Audits for Systems Delivered to Customers

Fujitsu has established "Security Requirements for Customer Internet Connection Systems" (the "Security Requirements") as a security measure for Internet-connected systems delivered to customers. Systems integrators are obligated to ensure that the Security Requirements are fulfilled before delivering systems to customers. In the process, specialized security departments objectively verify whether or not these systems meet the Security Requirements.

▼ 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 Fujitsu, 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.

Product Security

Fujitsu's software product development divisions are working to enhance the quality of security through standardization. The goal is to ensure that the quality of security for Fujitsu's software products meets or exceeds a certain base level of security quality.

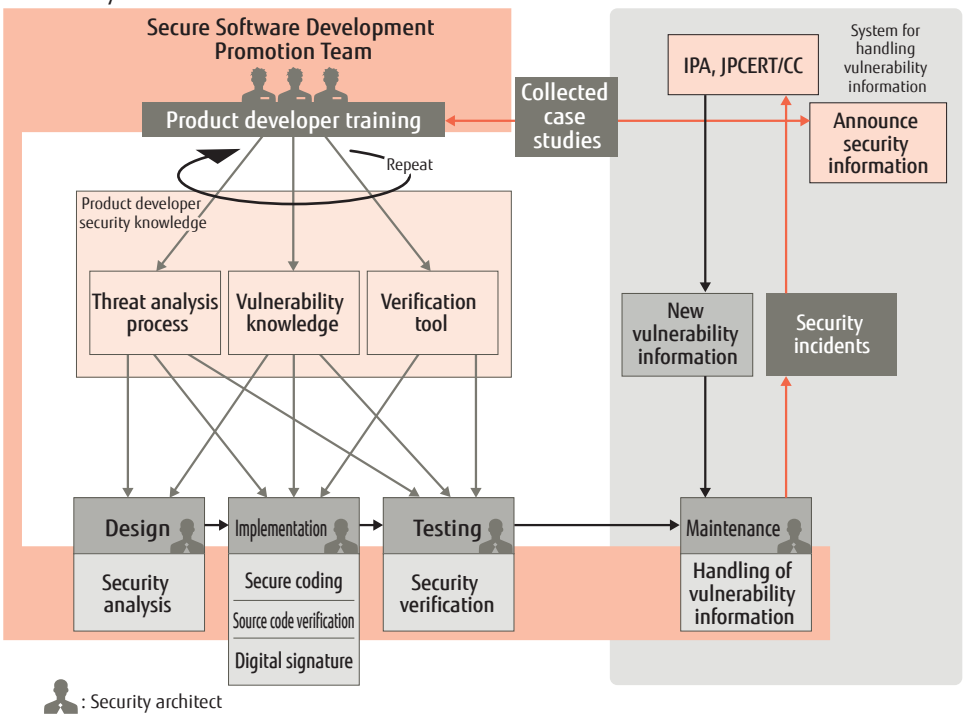
Security Quality Activities for Software Products

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 so as 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).

On the human resources front, Fujitsu nurtures security architects with technical knowledge of security in each division, in order to entrench proper security responses in development activities. As of December 2012, 313 individuals had been certified as security architects.

▼ Security Process for Software Products



Initiatives to Standardize Work Tasks

Addressing Inconsistent Quality Caused by Reliance on the Individual in Security Response Activities

In traditional development activities, Fujitsu promoted flexible security response activities according to product characteristics by giving product development divisions control over activity content and quality. However, this approach can result in inconsistent levels of security quality between various products.

For example, when developing web applications, developers must write robust programs that can withstand attacks by attackers, malware, and other sources. However, if the detailed decisions and responses are left up to individual development sites, there is a tendency for countermeasures and other measures to become reliant on individuals. Furthermore, if this situation is left unremedied, omission of security safeguards and integration errors become more likely. This can make it difficult to maintain a consistent level of quality in terms of product security.

Standardization to Prevent Inconsistent Quality

In response, Fujitsu has standardized the points to be considered in various development processes as well as the tasks to be executed, in order to prevent security measures from becoming reliant on individuals. In the standardization process, Fujitsu clarified its interpretation of vulnerability countermeasures, and its methods for evaluating the standardization of security measures.

Standardizing tasks enables Fujitsu to measure the conformance of security measures undertaken by developers. Furthermore, to make it easier for developers to select the tasks they need to carry out, Fujitsu has defined a standardized task menu that classifies the tasks into different groups.

Fujitsu has established mandatory and voluntary tasks within the standardized task menu. The mandatory tasks must always be implemented, except where software product's function does not apply. By establishing mandatory tasks, Fujitsu is able to ensure that it meets or exceeds a certain base level of security quality. For this reason, the mandatory tasks have been positioned as baseline tasks. The voluntary tasks are undertaken as deemed necessary based on the strategic positioning of products and other factors. For example, the voluntary tasks are selected when developing security and other such products that require a more secure response. The following table provides an image of the standardized task menu plus the baseline and voluntary tasks.

▼ Standardized Task Menu and Baseline/Voluntary Tasks

Menu	Baseline Tasks	Voluntary Tasks
Identification and authentication	ID/Password based authentication	Digital certificate/PIN-based authentication
Access control	Role-based access control (RBAC)	Mandatory access control (MAC)
Encryption	Apply ciphers in the e-Government Recommended Ciphers List/Key generation by PKCS#5	HSM key management and random key generation

* Tasks have been abstracted

On-site Security Quality Initiatives Based on Standardized Tasks

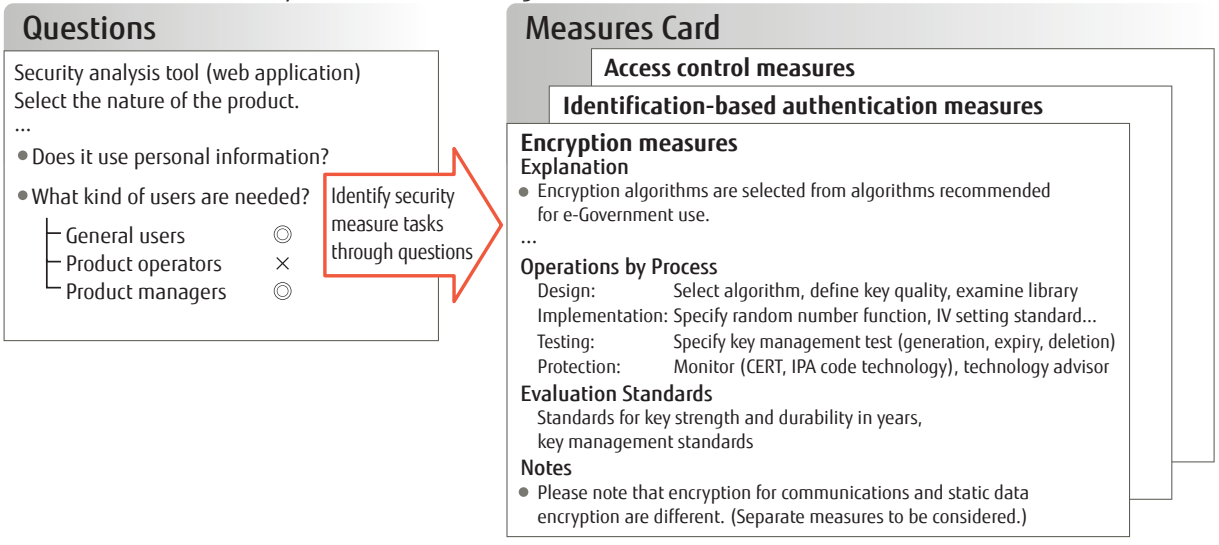
Specific on-site security quality initiatives based on standardized tasks are presented below. The Secure Software Development Promotion Team has developed a tool to identify security measures to ensure security quality even if the developer does not have the specialized knowledge needed to perform a security analysis. The diagram below shows an image of how this tool is applied. By having the developer answer a series of questions, the tool is able to automatically identify security measure tasks according to the characteristics of the product. In this example, the tool identifies the need for encryption measures based on a question about whether or not personal information is handled. The tool also identifies user authentication requirements based on questions regarding the software product's users, and access control requirements in cases where there are multiple roles.

The Secure Software Development Promotion Team also carries out continuous improvements of the standardized tasks. Working closely with the security architects who are active at development sites, the team strives to incorporate new tasks that arise on the development floor into the standardized tasks.

Fujitsu will first implement standardization initiatives with emphasis on web applications, considering the clear requirements for these applications and the strong level of demand for them. Thereafter, Fujitsu plans to expand standardization to software products in general.

In this way, Fujitsu will standardize security response processes for software products. This will eliminate reliance on individuals and define baseline tasks to ensure that security quality meets or exceeds a certain base level.

▼ Identification of Security Measure Tasks through Questions



Research and Development into Security Technology for Supporting a Safe Lifestyle

Amid growing smartphone use in business and increasingly sophisticated cyber-attacks, companies face a burgeoning range of threats that could cause personal and confidential information leaks. New security technology is needed to fend off these sorts of new threats. Fujitsu Laboratories Ltd. is working to develop cutting-edge technologies to meet demands for new security technology.

Approach to Security Technology at Fujitsu Laboratories

Fujitsu Laboratories conducts research designed to safeguard information utilized by companies from a variety of threats. Its research covers an expansive scope, ranging from systems security to support secure and safe societies to various elemental technologies. Examples include secure development processes to eliminate system and product vulnerabilities, countermeasures against cyber-attacks, privacy protection technology utilizing the latest encryption and masking technologies, and biometric authentication technology. These and other technologies have made a substantial contribution to enhancing the security of the systems and products provided by Fujitsu.

Notably, in biometric authentication technology, Fujitsu Laboratories was first in the world to develop a non-contact palm vein authentication technology. It has also developed ultra-small, high-precision fingerprint authentication technology for tablet PCs and smartphones.

In this report, we present two examples of our cutting-edge technology initiatives: technologies for protecting sensor data to enable transmission and use, and technologies for "exit defenses" against targeted attacks, which are designed to prevent information leaks caused by cyber-attacks.

Protecting Sensor Data Privacy from Collection to Utilization

The handling of personal and confidential information has become a key priority in terms of the use of big data. Recently, there has been a steady increase in data collected from sensors all around us, including digital home appliances, smart meters and smartphones. This data contains information that can identify an individual, such as user IDs, as well as personal information such as location history and information about absences from home. Linked together, this data can reveal the patterns of an individual's daily life. This could, for example, put the individual at risk for a targeted home burglary. Furthermore, regulations aimed at ensuring the safe use of personal information are being revised globally. Examples include stricter personal information protection regulations in Europe, and the program to accelerate the revitalization of Japan (anonymization guidelines). Going forward, technologies that balance the dual priorities of protecting and using this data will play a vital role.

Fujitsu Laboratories has developed two technologies for protecting privacy, from the point of collection of sensor data through to the application of analysis results.

1. Partial Decryption Technology

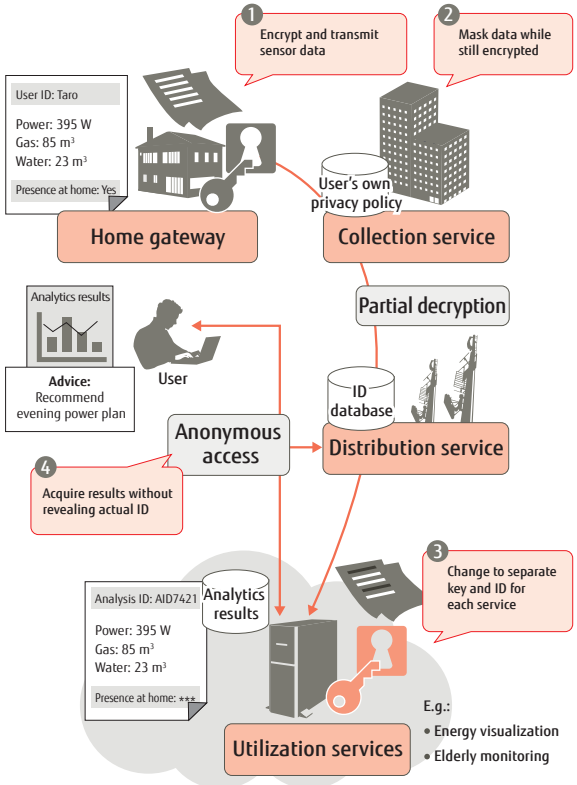
This technology enables sensor data to be modified while it remains encoded. Modifications include changing the user ID to an anonymized ID, masking the data, or changing it to a different code number for each data utilization service.

2. Anonymous Access Technology

This technology enables data analysis to be performed using an anonymized ID, and enables users to obtain analysis results without having to reveal their own user ID to service providers.

For example, through these technologies, users will be able to entrust data collection service providers with all of their home gateway and other sensor data (❶). This will allow users to securely provide these service providers with the data needed for each type of service like energy visualization and elderly monitoring services. In coordination with data collection and distribution services, sensor data can be processed while remaining encoded and forwarded to each data utilization service. (❷, ❸) The data utilization services will analyze the masked data with just an anonymized ID, allowing the user to obtain the results anonymously. (❹)

▼ Example of Secure Usage of Sensor Data through Partial Decryption Technology and Anonymous Access Technology



Technology for "Extrusion Prevention" against Targeted Attacks

1. Why "Extrusion Prevention" Is Needed

Cyber-attacks known as targeted attacks are now posing a threat. These attacks are carried out by sending e-mails containing content that is likely to attract the interest of the target, with specially created viruses attached to the e-mail messages. The attacks employ adroit techniques that are difficult for anti-virus software and other security products to detect. For this reason, some cases have been reported where the damage has expanded for a long term without noticing the intrusion.

Until now, countermeasures against cyber-attacks have focused mainly on public servers. Going forward, security measures will also be needed for the internal intranet environment, which had previously been considered a safe area. Although it is always important to stop any attacker from hacking into a network in the first place, it is also imperative to take steps to detect any threats as quickly as possible and minimize the damage, based on the assumption that intrusions will happen. This approach is premised on the concept of "extrusion prevention" which entails controlling suspicious requests for communication to the outside from an exploited computer.

Until now, detection technology was based on identification using characteristic key words registered as signatures, as well as web filtering technology (URL filtering technology) designed to block harmful websites. However, as a result of diversifying usage formats and the increasing sophistication of attack strategies, these approaches can no longer adequately distinguish threats from ordinary communications.

In particular, there is a new type of virus that establishes a command and control (C&C) communication path to external servers after intruding an organization's network, and these kinds of viruses are emerging in large numbers on a daily basis. Security measures based on URLs and characteristic key words cannot keep up with these viruses. Furthermore, considering that there is only a limited amount of information that can be used to specify these viruses, communications via business applications can be falsely detected as a virus.

In response, Fujitsu Laboratories has focused on the characteristics of communication sessions, targeting the HTTP/HTTPS protocol that permits communications with external servers. This resulted in the development of a Detection System for Malicious HTTP Communications based on three technologies that solve the problems inherent in conventional detection technologies.

2. Detection System for Malicious HTTP Communications

The Unauthorized HTTP Communications Surveillance System consists of the following three technologies:

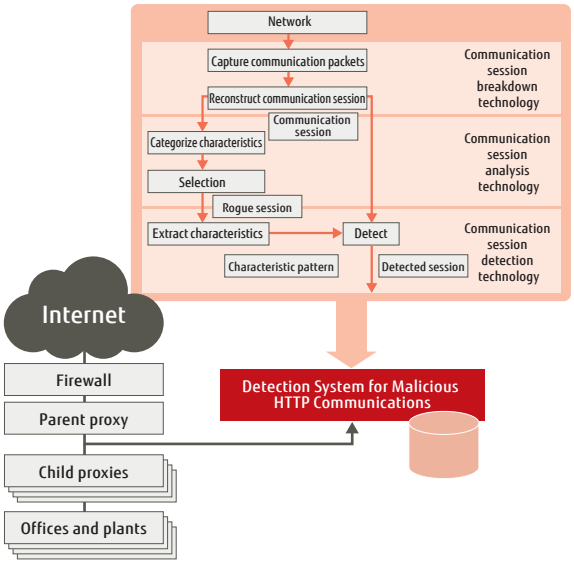
- Communication session breakdown technology
- Communication session analysis technology
- Communication session detection technology

The first technology is a communication session breakdown technology that collects communication packets bound for the external environment at the stage prior to the parent proxy, and reconstructs all processing between the server and client as a communication session.

The second technology is a communication session analysis technology that quantifies data flow characteristics in the collected communication sessions based on a variety of indexes. These technologies were used to observe the status of communications from within an organization to external sites for a period of more than several months, and the features were analyzed.

As a result, Fujitsu Laboratories confirmed that several different features characterize the behavior of communication sessions involving ordinary website accesses and specific communication applications. By statistically processing the quantified communication statuses, Fujitsu Laboratories was able to establish correlations among composite indexes and classify them into several groups. Meanwhile, Fujitsu Laboratories also confirmed the existence of rogue communication session clusters that do not fit into any of these correlations or groups. Based on these findings, Fujitsu Laboratories found it could identify features that differ from ordinary business communications by focusing on the entire flow of communication session behavior, even when improper communications are disguised as ordinary business communications that cannot be distinguished at first glance.

▼ Overview of Detection System for Malicious HTTP Communications



Based on the achievements of these proprietary surveys and studies, Fujitsu Laboratories developed the third technology-communication session detection technology, and built a prototype Detection System for Malicious HTTP Communications. Having conducted detection tests in a virtual environment modeled on an organization's internal network, Fujitsu Laboratories is currently testing the operation of the system in an actual environment.

This research has enabled the identification of improper C&C communications with external servers by viruses, which were previously difficult to identify. The detection system can improve the false detection rate to around 1/300 compared with conventional methods. The false detection rate is the rate at which ordinary communications are falsely detected as improper communications.

Furthermore, in addition to communications by viruses, this detection system can be used to detect communications by a variety of applications as well. For example, the system can detect the use of prohibited applications within an organization. As such, the system also provides an effective technology for monitoring compliance within an organization's internal network.

Looking ahead, security administrators who manage the internal networks of organizations will be called upon to confirm any traces of intrusion by external threats within their networks. Fujitsu Laboratories believes that this detection system will provide an effective means of performing this sort of confirmation work.

Information Security Enhancement Measures in Cooperation with Business Partners

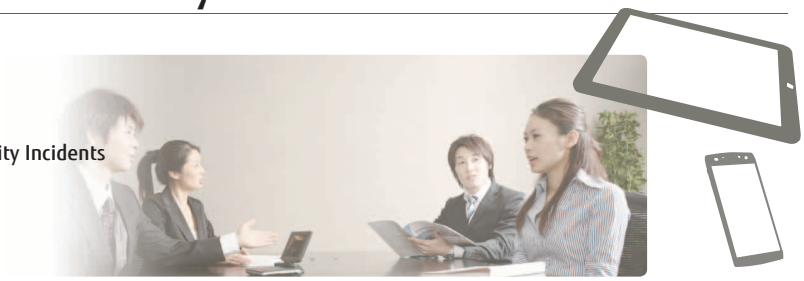
The business activities of the Fujitsu Group are supported by business partners, whose software, services, goods, and materials provide the basis for the value added by Group companies.

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 throughout the supply chain 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 2012 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, there has been a higher risk of information leaks in recent years. This reflects increased business use of external services (cloud services, etc.) triggered by the need for corporations to implement business continuity management (BCM). Business use of social networking services (SNS) has also been on the rise as companies seek to share information. Another factor has been rapid shifts in technology and the ICT environment, including a sharp increase in smart devices serving as infrastructure for the aforementioned services and the increasing diversification and sophistication of networks.

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 this end, in October 2012 the Fujitsu Group revised and applied its "Information Management Procedure Guidelines for Business Partners," which is an agreement on information security between the Fujitsu Group and its business partners. In this manner, the Fujitsu Group is working to continuously bolster information security enhancement initiatives.

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 2012, Fujitsu conducted training seminars based on the following theme: "Strengthening Information Security in Line with the Worksites of Outsourced Operations." The seminars were centered around a presentation featuring case studies of information security incidents and information security measures for projects where staff are stationed permanently on-site and offshore operations.

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

- October 2012: Approx. 1,250 participants from around 1,000 business partners

In the questionnaire, approximately 99% indicated that the training seminars were effective.

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. The training seminars are based on the theme, "Information Security: Latest Trends and Measures."

- Fiscal 2012: Training received by approx. 1,000 employees of around 50 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 foster the IT literacy needed by working professionals and businesspeople, and to confer basic knowledge concerning information security in business.

- Fiscal 2012: Approx. 150 employees of around 40 business partners

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 preparation of reports when information security incidents arise, analysis of the causes of such incidents, and formulation of corrective measures, among other topics.

- Fiscal 2012: Approx. 50 employees of around 30 business partners

3. Confirmation of Information Security Status

Based on the contracts with its business partners, the Fujitsu Group undertakes regular confirmation of business partners, information security status; 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 2012 audits: Approx. 140 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 status 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 security-related information including throughout the Fujitsu Group.

- For the purpose of sharing the latest news on information security, Fujitsu has published the "Information Security Plaza" (information data) and awareness-raising posters every two months since April 2009. In the December 2012 issue, Fujitsu provided an awareness-raising poster designed to prevent theft or loss of information in connection with drinking and other festivities during the New Year's holiday season.

▼ Educational poster

- In conjunction with the revision of the "Information Management Procedure Guidelines for Business Partners", Fujitsu has created updated versions of the Information Security Handbook, Information Security Compliance Status Check Sheet, and the Information Security Educational Material, and has provided these publications to business partners.

7. Fujitsu Group Governance

Measures to strengthen the information security at the Fujitsu Group's business partners are promoted throughout the entire Group. By fostering intra-Group cooperation on each information security measure, and sharing information on case studies of information security incidents and other matters, the Group strives to formulate and share even more effective preventive measures and to promote these measures at business partners.

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. This procedure requires overseas business partners to follow the same procedures for handling entrusted information as domestic business partners.

In conjunction with the revision of the "Information Management Procedure Guidelines for Business Partners" in Japan, Fujitsu provided its overseas business partners with an English translation of the guidelines in October 2012. Fujitsu also revised a Chinese version of the guidelines for its business partners 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 SOLUTIONS 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 LIMITED
FUJITSU KAGOSHIMA INFORNET LTD.
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 LTD.
BEST LIFE PROMOTION
FUJITSU HOKURIKU SYSTEMS LIMITED
FUJITSU MARKETING LIMITED
FUJITSU YAMAGUCHI INFORMATION CO.,LTD
UCOT CORPORATION
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 IT PRODUCTS LIMITED
FUJITSU ADVANCED ENGINEERING LIMITED
FUJITSU ADVANCED SOLUTIONS LIMITED
FUJITSU FIP CORPORATION
FUJITSU FSAS INC.
FUJITSU KAGOSHIMA INFORNET LTD.
FUJITSU KANSAI-CHUBU NET-TECH LIMITED
FUJITSU KYUSHU SYSTEMS LIMITED
FUJITSU COMMUNICATION SERVICES 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
FUJITSU BROAD SOLUTION & CONSULTING INC.
PFU LIMITED
FUJITSU MARKETING LIMITED
FUJITSU MISSION CRITICAL SYSTEMS LTD.
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$^{+}_{is}$

IT Security Evaluation Certification

Fujitsu's main ICT products that have received evaluation certification based on the ISO/IEC 15408 international standards for security evaluation criteria are as follows:

- Systemwalker Centric Manager Enterprise Edition
- Systemwalker Operation Manager Enterprise Edition
- Symfoware Server Enterprise Extended Edition
- Interstage Application Server Enterprise Edition
- Interstage Security Director
- OS IV/MSP Secure AF2
- IPCOM EX-Series Firmware Security Component
- Si-R Security Software (routers, switches)
- SR-S Security Software (routers, switches)
- SafetyDomain (authentication control software)
- PalmSecure (palm vein authentication device)

Note: For details, please inquire separately.

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 to the right.

145

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 "Certified information security senior auditor," "Certified information security auditor," "Information security auditor provisional," and "Information security auditor 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 to the right.

127

Safe and Secure Solutions from Fujitsu

Fujitsu's Safe and Secure "SafetyValue" Solutions

In recent years, companies have been facing the need to develop a new risk management model. To do so, companies must enhance business continuity by changing their management priorities from pursuing selection and concentration to implementing decentralization and sharing, while ensuring efficiency. Fujitsu provides safe and secure "SafetyValue" solutions to continuously support the businesses of its customers through ICT based on the concept of shifting to sustainable businesses.

How Fujitsu Defines "Safe and Secure"

Features of "SafetyValue"

- **Customer-oriented**
  Proposes the best solutions for resolving customer problems in terms of the three perspectives of business continuity, security, and energy.
- **Improved usefulness**
  Creates an environment where information resources can be used efficiently while carefully protecting customer resources.
- **Environmental contribution**
  Assists with building an office environment that enables diverse work styles and efficient management aiming for the most efficient use of energy.

"SafetyValue" Solution Framework

"SafetyValue" is built on the three pillars of business continuity, security, and energy, all of which originate from the business challenges of our customers. Through "SafetyValue," Fujitsu seeks to enhance user-friendliness in order to enable the secure and efficient use of information resources, and to build an office environment that enables both optimal use of energy and diverse work styles. Fujitsu's security solutions are presented below.

Three pillars for delivering sustainable business

Business Continuity	We provide a complete range of services ranging from establishment and implementation of business continuity planning and operational management, to support of continual improvement activities and delivery of robust business continuity measures. We make full use of our in-house, hands-on expertise and the latest cloud computing technology to provide powerful assistance for the business continuity efforts of our customers.
Security	We propose the most appropriate solutions, not only for handling new security risks that arise from virtualization and the shift to cloud computing, but also for supporting innovation for better work styles and improved productivity by ICT.
Energy	We propose total solutions for establishing plans, increasing transparency, and improving ICT–not only for business continuity and secure company activities, but also for efficient energy usage.

Solutions Lineup

Solutions for 14 Areas of Information Security (April 2013)

Security	For further details on security, please visit the following website (Japanese only): http://jp.fujitsu.com/solutions/safety/secure/
Security Controls	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 Prevention Measures	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.
Security Consulting	Offers integrated assistance for establishing information security management in an organization from establishing basic information security policies to entrenching management practices.
Measures Against Unauthorized Access	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.
Measures Against Information Leaks	Provides functions for drafting and establishing information management policies and encryption functions for protecting personal information and preventing information leaks.
Anti-virus measures	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 assistance for security measures needed to use e-mail securely, such as anti-virus measures and preservation of audit trails.
Authentication and 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 PCI DSS (Payment Card Industry Data Security Standard)
Thin Clients	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.
Pinpoint Security	Security products for easily introducing security measures for specific purposes.

FUJITSU LIMITED

Information Security Center

1-17-25 Shin-kamata, Ohta-ku, Tokyo 144-8588 Fujitsu Solutions Square
E-mail: isc-secreport@ml.css.fujitsu.com
URL: http://www.fujitsu.com/