FUJITSU

Fujitsu Group

Information Security Report 2010

Information Security Report 2010

shaping tomorrow with you

CONTENTS

Report Summary

Target Period and Scope of the Report

・This report covers the period up to March 2010 and focuses on efforts in information security by the Fujitsu Group.

Report publication date

・This report was published in August 2010.

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 principle.
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. These unceasing advancements have given rise to a global networked society, bringing major changes to the business world, our personal lives and society as a whole. Without ICT, the modern world would cease to function. In providing ICT infrastructure solutions to underpin our modern world, the Fujitsu Group seeks to create an environment where everyone can equally enjoy the benefits of a networked society that is rewarding and secure. Through the constant pursuit of new possibilities enabled by ICT, the Fujitsu Group aims to continuously create new value, bringing about a prosperous future that fulfills the dreams of people throughout the world.

Based on this corporate philosophy and from the perspective of information security, we are involved in strengthening information security through policies to observe corporate regulations and promote appropriate information management and utilization.

Specifically, in our Code of Conduct, which indicates the items to which employees should strictly comply in the “FUJITSU Way,” there is written policy regarding maintaining confidentiality and the concepts, which are the foundation of security, are clearly worked out. In addition, seven related regulations concerning information management based upon these concepts have been applied to the entire Fujitsu Group.

To aim for thorough information management and increased information security, the Fujitsu Group is creating a corporate-wide information security management system. However, business is developing over various fields, and the response to the different issues in information management and information security born from the special characteristics of individual business is to construct information security management systems for each business group unit so that information security policies corresponding to those business characteristics can be promoted.

This "Information Security Report 2010" describes what the Fujitsu Group is doing for information security. Please take the time to read it.

Masami Yamamoto

President
Fujitsu Limited

Fujitsu Group's Information Security

Under the information security governance system, the Fujitsu Group promotes appropriate information management and information usage while observing labor regulations and corporate regulations.

Information Security Governance System

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 our 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 outside directors.

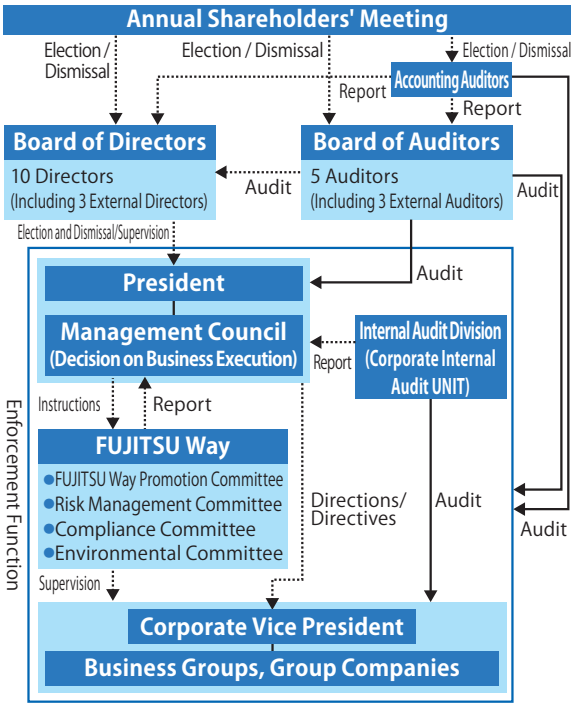
With respect to group companies, we are pursuing total optimization for the Fujitsu Group by clarifying each group company's role and position in the process of generating value for the group as a whole and managing the group to continuously enhance its corporate value.

We have established a Risk Management Committee as the body to promote risk management in accordance with the Fujitsu Way. By establishing rules and guidelines for risk management, we have set practical action standards focused on both preventing potential risks from arising and responding to any incidents that do materialize, so as to advance global risk management.

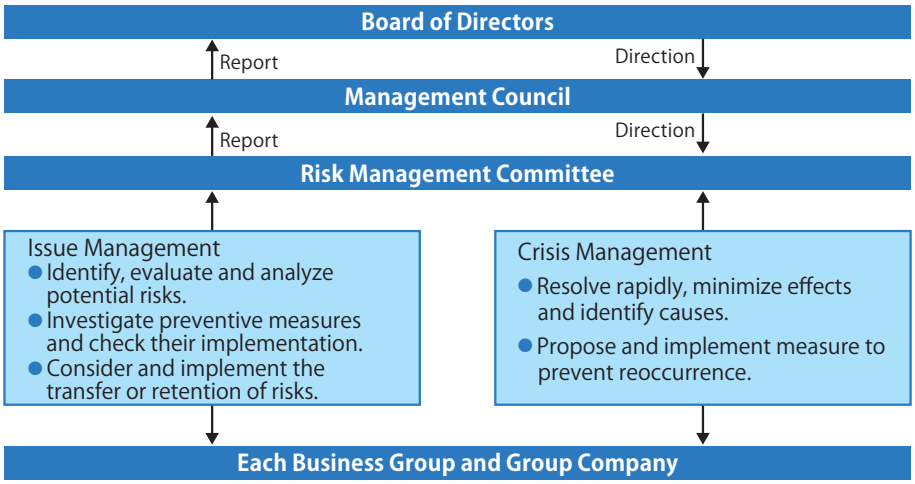
To manage potential risks, the Risk Management Committee maintains close coordination with risk management executives of each business group to extract, evaluate and analyze a variety of risk-related information. At the same time, it continuously monitors the progress of risk incident prevention measures.

To prepare for the case that an incident occurs or is seen to be threatening to occur despite these preventive measures, rules have been established for reporting risk-related information and these are enforced at all locations

■ Corporate Governance System



■ Risk Management System and Risk Management Cycles



throughout the group, including overseas.

When the incidents occurring or seen to be threatening concern deficiencies or flaws in products and services, or information security, etc., all related divisions must report them immediately to the Risk Management Committee and to the management in each related business group. With regard to major risks, these are immediately reported to senior management, including the Management Council and Board of Directors as necessary. Then, in collaboration with the risk management executives of the frontline management, the affected divisions and each related business group, an ad hoc response units is set up to resolve the problem quickly and minimize its effects, to determine the cause, and to make and implement proposals to prevent its recurrence.

Information Management

The Fujitsu Group is involved in strengthening information security based on policies to comply with work regulations and to promote appropriate information management and utilization.

Specifically, our "Code of Conduct," part of the "FUJITSU Way," stipulates the corporate philosophy, corporate policies and employee guidelines and code of conduct and contains written policy regarding maintaining confidentiality. It also clarifies the concept that is the foundation of information security. The seven information management related regulations, that is "Rules for Management of Confidential Information" "Rules for Management of Personal Data" "Rules for Management of Third Parties' and Customers' Confidential Information" "Information System Security Regulations," "Fujitsu PKI*1 Use Regulations*2," "PC/Network Use Regulations," and "Intellectual Property Rights Treatment Regulations," were established based on this concept. These are stipulated as Fujitsu Group regulations to be applied to Fujitsu and domestic group companies and the group as a whole strives to comply with them.

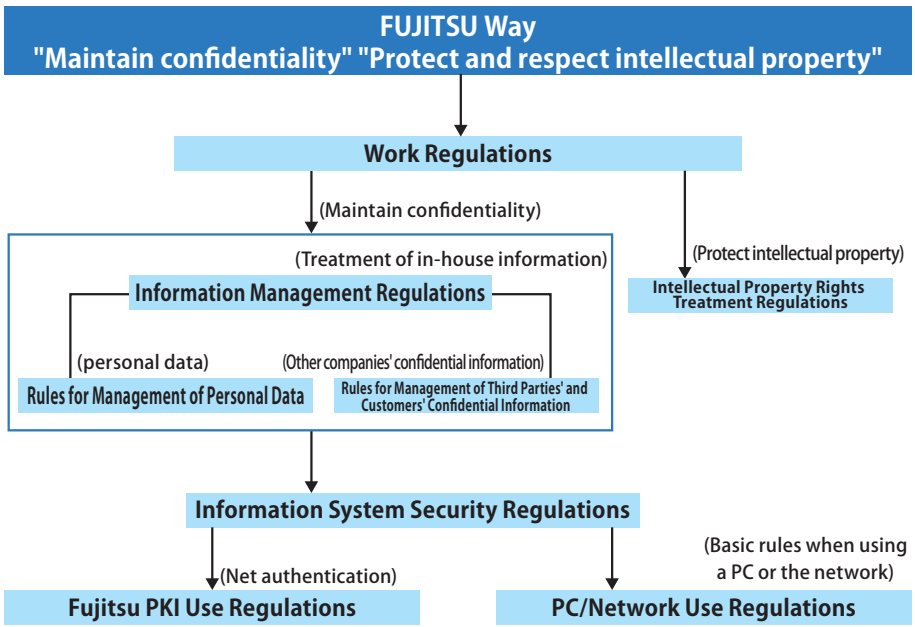
"Rules for Management of Confidential Information" have been established to appropriately manage corporate information handled during business. Furthermore, the treatment of information received from customers or Other companies is stipulated in "Rules for Management of Third Parties' and Customers' Confidential Information" and the treatment of personal data is stipulated in "Rules for Management of Personal Data".

The "Information System Security Regulations" stipulate security for information systems that process information on the network. These regulations contain three aspects of information systems: construction, application, and use. Particular emphasis has been placed on the use aspect. The "PC/Network Use Regulations" stipulate standards regarding information security measures when using PCs, removable media devices such as USB memory, or the internal network. Furthermore, the "Fujitsu PKI Use Regulations" stipulate basic actions when using a mechanism for identity authentication or encryption in order to more reliably manage information.

*1 PKI is an abbreviation for Public Key Infrastructure (information security infrastructure based on public key encryption technology)

*2 Fujitsu PKI Use Regulations: Regulations concerning use of mechanisms for identity authentication or encryption used on the network.

■ Information Management Related Regulation System

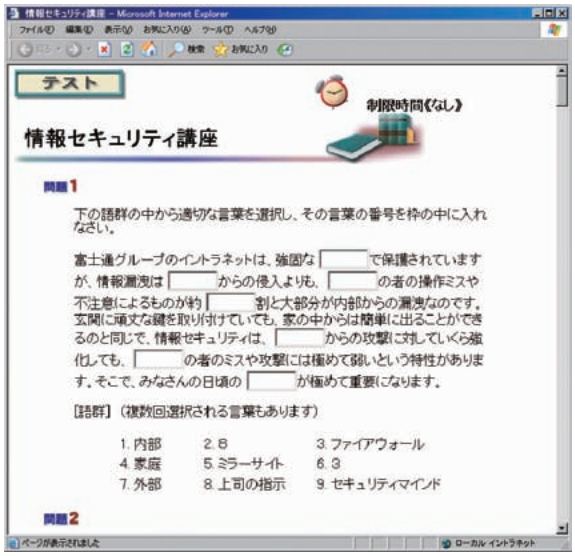


Information security education

We think it is important to not only let the employees know the types of regulations but also to improve security awareness and skills of each staff member in order to prevent information leaks. By providing information management education to all employees, including executive, temporary staff, and part-time staff, awareness concerning appropriate information management is made complete. New hires are also taught about the importance of information management when they are hired.

In addition, information security education is included in the training courses for core and senior employees and appropriate education is implemented through collective format or e-learning.

■ e-Learning Screen in Japan



Raising awareness regarding information security

Within the company, the activity status of divisions implementing measures for effective information security are released on the intranet as reference examples, and each division promotes independent security promotion activities.

For example, using 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 displayed posters at each of their business locations and affixed seals to all employees' PCs in an effort to increase the awareness of information security in every individual employee.

■ The seal: "Declaration for complete information management!" in Japan

Held information security presentation for clients

These days, there have been many occurrences of information being leaked or lost. In response, the Fujitsu Group has held information security presentations that were not only for group employees but also for clients who commission software development and services.

Enhancing personal data protection systems

At Fujitsu, in addition to maintaining "Personal Data Protection Policy" "Rules for Management of Personal Data" were established in compliance with Act on the Protection of Personal Information that came into full force in April 2005. Based on these regulations, education and audits regarding handling of personal data is implemented every year. In August 2007, we acquired company-wide PrivacyMark certification and are working to further strengthen our personal data protection.

Domestic Group companies are also acquiring PrivacyMark certification individually as necessary, and promoting thoroughgoing management of personal data.

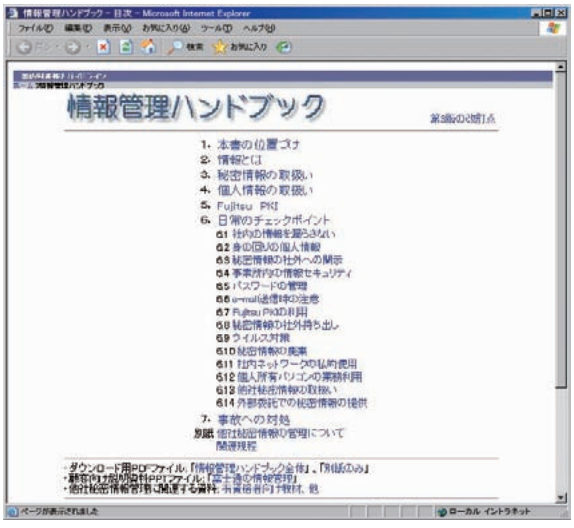
Overseas Group companies are also publishing privacy policies that meet their various national legal and social requirements on their main public Internet websites.

Other support

An "Information Management Handbook" is distributed to all Fujitsu employees to increase understanding of internal regulations related to information management. This handbook can also be referenced over the intranet allowing for immediate confirmation for 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, a security check day is held once a month, management verifies the status of security measures in their own divisions, and

■ "Information Management Handbook" Screen in Japan



activities are held to bring information leakage the attention of employees.

As described above, the "FUJITSU Way" clarifies the Fujitsu Group policy and, based on labor regulations, stipulates the seven regulations to deal with the various situations related to information management.

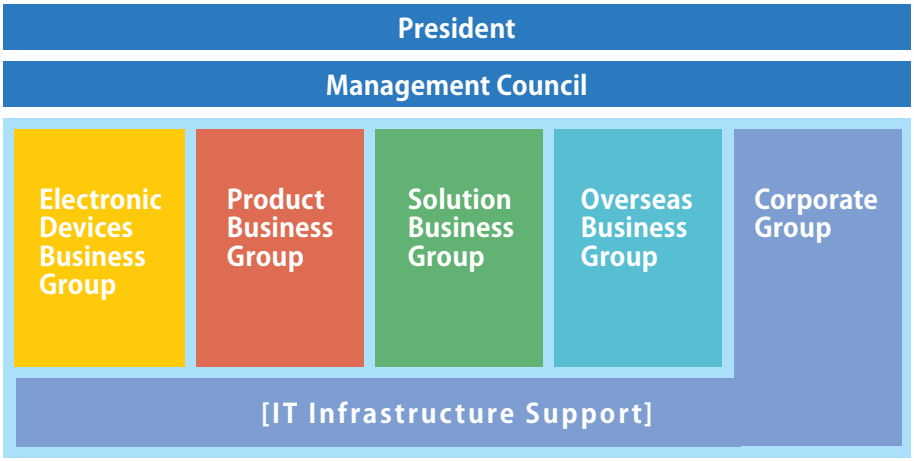
In addition, with the handbook for employee education, Fujitsu employees strive to comply with these regulations and act so as not carelessly leak internal information.

Information Security by Business Group

The Fujitsu Group develops a broad range of businesses for a wide variety of industries and corporations and has "Business Groups" as a structural system to promote each business. And due to the different issues in information management and information security required by the special characteristics of individual business, information security management systems are built for each business group unit so that information security policies corresponding to those business characteristics can be promoted. This system is supported by having a corporate-wide common IT infrastructure to strengthen information security to have thorough information management.

In addition, the Fujitsu Group has acquired PrivacyMark certification and Information Security Management System (ISMS) compliance assessment system certification, and provides thorough management of confidential information, such as personal data or client information.

■ Management System for Information Security



[Corporate Group]
This division consists of the administrative divisions, including finance/accounting, human resources, legal, and sales, and the division that support information systems for the entire Fujitsu Group and promotes the unification of administration and IT.

[Solution Business Group]
Applying IT as the foundation for advanced technologies and high quality products, this division provides business solutions (business optimization), including IT services, outsourcing services, and network services, to clients who are primarily corporations.

[Product Business Group]
This division provides IT infrastructure products that are central to high performance/high reliability servers to support important client systems, state-of-the-art network devices to support advanced network systems, and high performance, user friendly PCs and mobile telephones.

[Electronic Devices Business Group]
This division provides logic LSI, which is the nucleus of technology, and related electronic products as optimal solutions to contribute to improving the competitiveness of client's products.

[Overseas Business Group]
This division provides a wide variety of IT service solutions backed by state-of-the-art technology to customers all over the globe (US, EMEA, APAC, and China) as "One Fujitsu" based on the concept of "Think Global" and "Act Local".

IT Security Efforts

In situations where IT is applied, the large volume of data related to business is collected and placed so that it can be easily handled. This is accompanied by various threats such as information being leaked, damaged, or unavailable.

For this reason, the Fujitsu Group, as a common theme, is wholly involved in IT security to ensure safe management of information for IT applications.

Pursuit of IT Security to Support Business

In the Fujitsu Group, IT security does not aim to interfere with the convenience or efficiency of business, but rather, to support business.

If regulations for information security measures are too excessive, then a burden is placed on the employees to understand and observe the regulations, which makes compliance with them unrealistic.

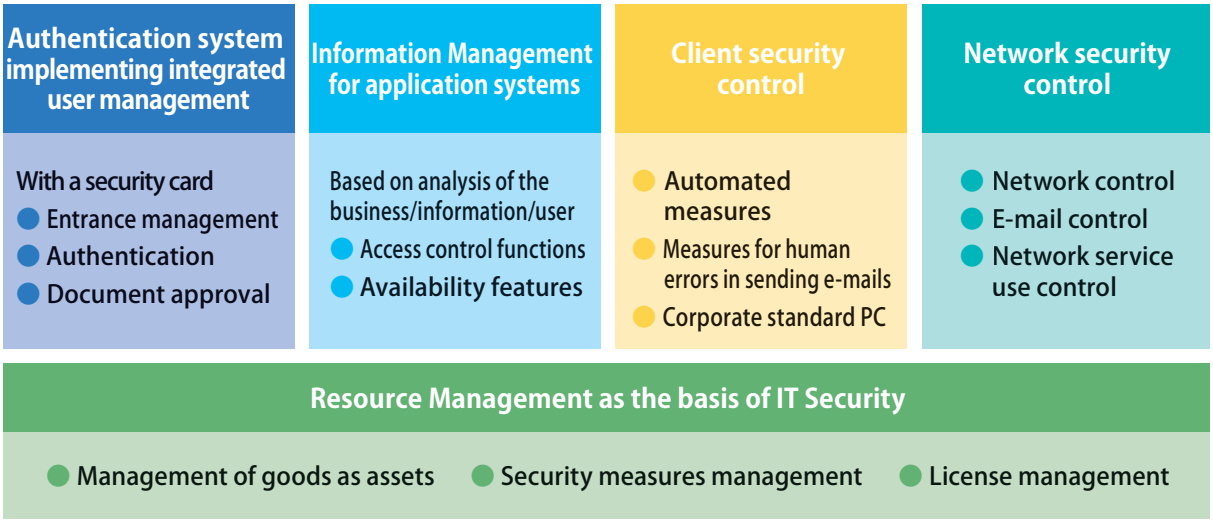
Fujitsu Group IT security implements measures that consider the business environment and business procedures as much as possible. We believe that making it possible for the employees to give their attention to their jobs is important.

In addition, to maintain measures effective against threats changing with IT progress, we have set a team of IT security specialists believing that state-of-the-art technology is necessary to solve problems and to develop and implement technical measures.

IT Security Framework

Fujitsu Group IT Security is supported by "information management for application systems" and "client security" as well as the common mechanisms of "resource management," "authentication systems," and "network security."

■IT Security Framework



Information management in business systems

The Fujitsu Group applies IT to various tasks such as finance/accounting, human resources, marketing, sales, SE tasks, production/distribution, and product development management. The information maintained and handled here has security requirements 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 availability feature to meet the importance and continuity requirements of the business.

Client security control

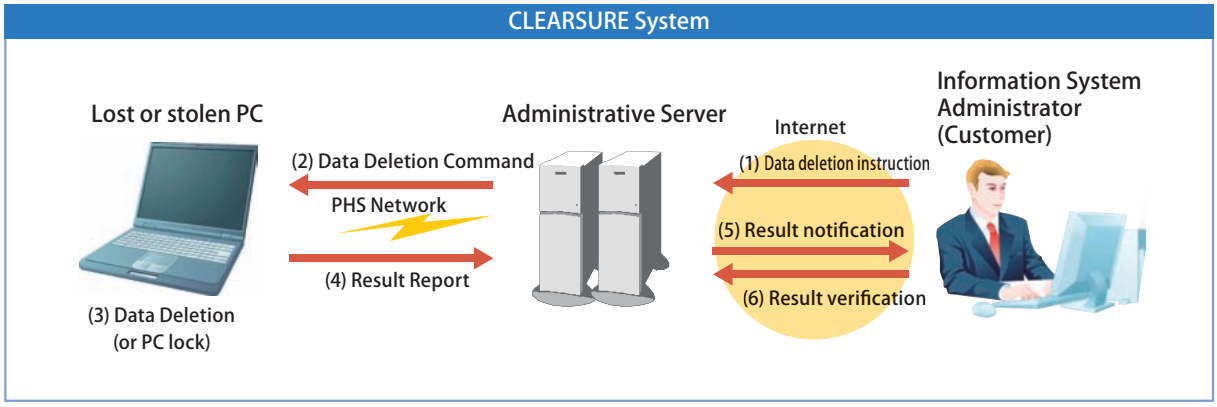
An important information security issue is coping with human error. Relying only on human attentiveness in IT applications will not necessarily prevent information security incidents. Of course education and awareness program should be employed to draw attention to information security, but even then information leakage and other incidents will occur beyond the scope of the IT measures.

Based on this reality, we focused on the business processes of the client that involved human action and considered whether it was possible to replace measures reliant on attentiveness with IT measures. These possibilities were then substantiated.

- Automated measures for PC
  Application of security patches and updates for virus definition files are automated.
- Measures for human errors in 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 it is addressed to external persons.
- Installation of corporate standard PC
  The Fujitsu Group promotes the installation of "corporate standard PCs." Corporate standard PCs are those with identified models and specifications for corporate internal 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 delivered. In doing so, PC models 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 note PCs, corporate standard note PCs have the function of remotely invalidating data. This significantly reduces the possibility of information leakage in case of loss or theft of PC. This feature is provided to customers as the mobile security solution "CLEARSURE."

■ Measures against Note PC Loss or Theft



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 IT application and IT security. The Fujitsu Group performs IT resource management with a 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
- Status of installing 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 is 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 to the office use their Security Card for entrance.

[Authentication]

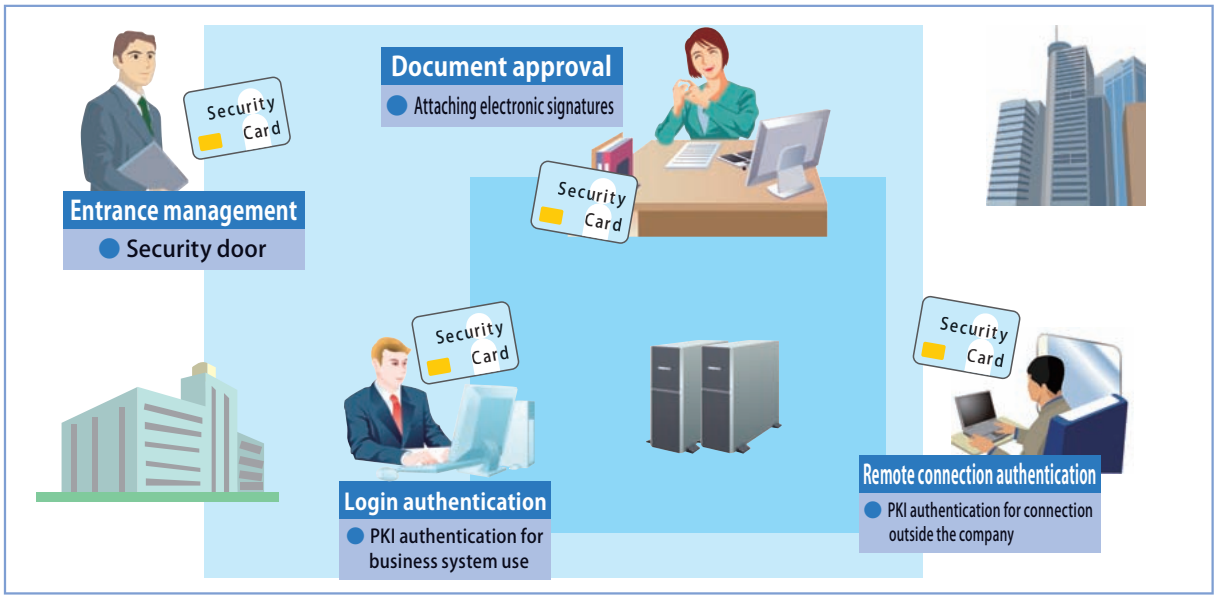
The Security Card is required to use the application system. Authentication by PKI at login to application systems enables secure identification and authentication of employees along with simple operation.

Application system can be also accessed from outside the company as when on a business trip. In this case, the remote connection is authenticated by PKI, and the employee is securely authenticated.

[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 group of specialists armed with the latest technologies create measures for these threats to minimize the burden on employees and guarantee 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 DMZs*1 and firewalls by specialist groups
  - Inspection and authorization of connections performed by divisions

*1 DMZ (DeMilitarized Zone): The DMZ is a region that is separated from both the external network and the internal network using a firewall for networks connected to the Internet

- Maintenance and operation of an environment to allow access from outside the company into the Fujitsu Group using a mobile device
- Maintaining security during operation
  - Measures against unauthorized access (server configuration, monitoring and preventing unauthorized transmissions)
  - Reliability design, performance management for stable operations

[E-mail control]

Use of e-mail addressed to persons outside of the Fujitsu Group is allowed where it is necessary for business. The following measures are in place for safety management.

- E-mail control
  - Installation and operation of e-mail servers by specialist group
- Maintaining security during operation
  - Anti-virus measures
  - Anti-spam measures
  - Reliability design, performance management for stable operations

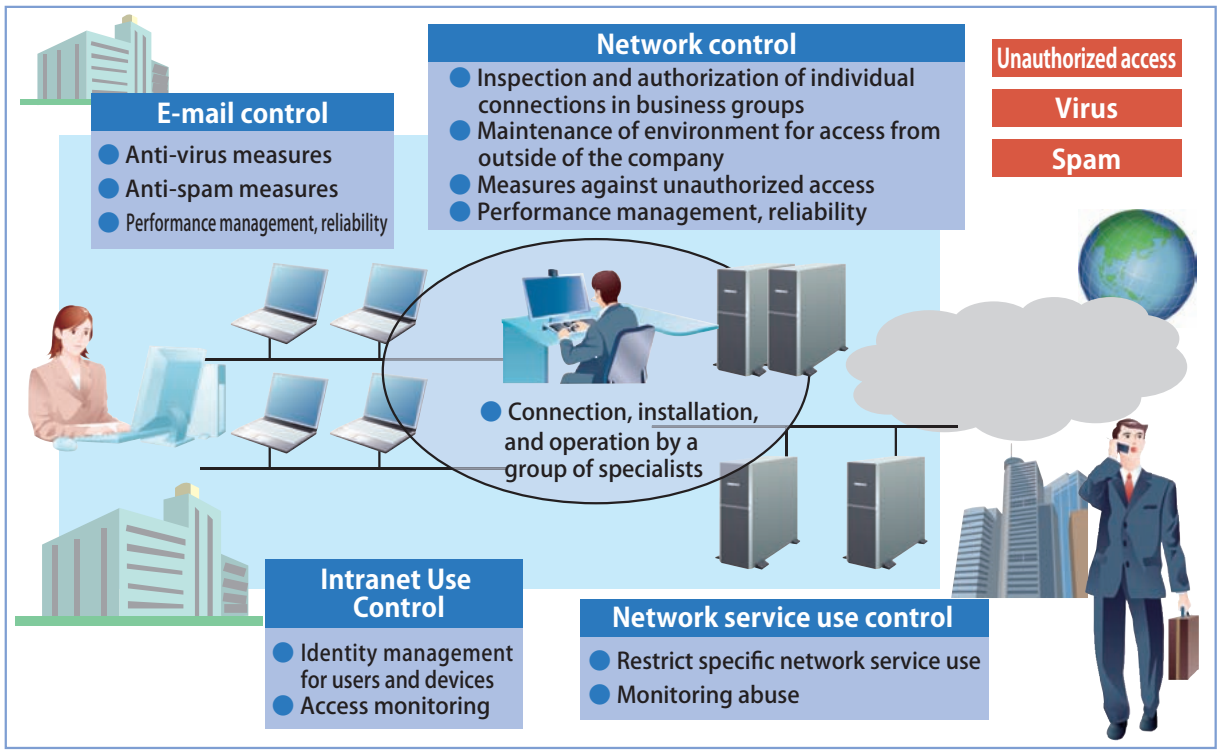
[Network service use control]

The Internet environment outside the company provides many network services such as file transfer and online meetings, but in many cases the use of these is prohibited. However, use is allowed with restrictions when the convenience and necessity for business and the current status of the improved client security control is taken into consideration. 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 extends scope of control on the use of intranet throughout the group. Users and devices are managed, and legitimacy is verified through authentication when connecting.

■ Network security control



Product Security

To have our customers feel secure in using Fujitsu products, we promote equipping products with security features and make efforts to maintain information security.

Efforts toward equipping products with security features

There has been focus on cloud computing and virtualization technology, and security awareness for information processing systems, such as measures against information leaks, has increased.

At Fujitsu, in order to comply with ISO/IEC 15408[*1], the international security evaluation standards for information systems, from the product development stage, we are involved in implementing advanced, high standard security features, and for our various flagship products, we continue to work to acquire ISO/IEC 15408 compliance evaluation system certification, starting with information system operation and management software.

In addition, for consumer products such as PCs or mobile telephones, we strive to implement security features not available in products from other companies to prevent information leaks to guarantee information security and allow our customers to feel secure during use.

*1 ISO/IEC 15408: International standard regulations for security specialists to evaluate and certify whether information security features for an IT product or system are sufficient. Product evaluation certification is called "IT Security Evaluation and Certification Scheme" and is managed by the Information-technology Promotion Agency (IPA)

Initiative for Software Products

Product development

Keeping the requirements of ISO/IEC 15408 in mind, product development with a high degree of security is promoted with design guidance and auditing by a security architect[*2] from the product development stage and implementation of security inspection using inspection tools for all products.

Releasing product vulnerability information

At Fujitsu, product security information can be accessed from the top page of our website. We release information regarding product vulnerability to our customers as soon as possible in order to inform about risks and measures.

Also, we built a system to notify customers as quickly as possible through linking with the JVN[*3] vulnerability measures information portal site.

*2 Security Architect: A specialist in secure software development who has passed the company's strict certification test (as of February 2009, a total of 258 had acquired certification)

*3 JVN (Japan Vulnerability Notes): JVN provides vulnerability information and their solutions for software products used in Japan and targets to contribute to information security measures. It is operated jointly by the JPCERT Coordination Center and the Information-technology Promotion Agency (IPA)

Mobile Telephones ~ microSD Password Feature ~

By setting a password in the microSD card, even if the microSD card is removed by theft or loss, because it cannot be read by another PC or mobile telephone, there is no worry that important personal data may be leaked. Robust security is realized through an access lock[*4] and a screen off lock[*5] as well as a Fujitsu unique fingerprint sensor[*6] and password setting for the microSD card.

*4 Access Lock: Keys are locked each time the telephone is closed.

*5 Screen off lock: Touch panel operations and keys are locked after a set time passes with no operations after the screen turns off.

*6 Fingerprint sensor: Instead of entering a terminal security code, authentication can be made with a fingerprint alone by sliding a registered finger.

■ microSD Card Password Configuration System

Example Approach for Solution Business Group

Because the Solution Business Group often handles customers' information assets and personal data, a high level of information management is required. Based on the information security management system, a security management framework is provided to all divisions, and the enforcement of security policies is promoted.

Solution Business Group Characteristics

As focus shifts to cloud computing and virtualization technology, the way IT is used is changing.

The Solution Business Group (SBG) provides the most up to date business solutions using IT for our corporate customers. For IT operations for customers, such as IT system development/construction, outsourcing, and network services, a high level of information management is required because there are many opportunities to handle the information assets of the customer. In addition, there are also cases when internal confidential information or personal data is used. Taking into account the importance of these kinds of information, SBG is working toward information security measures based on a secure IT infrastructure.

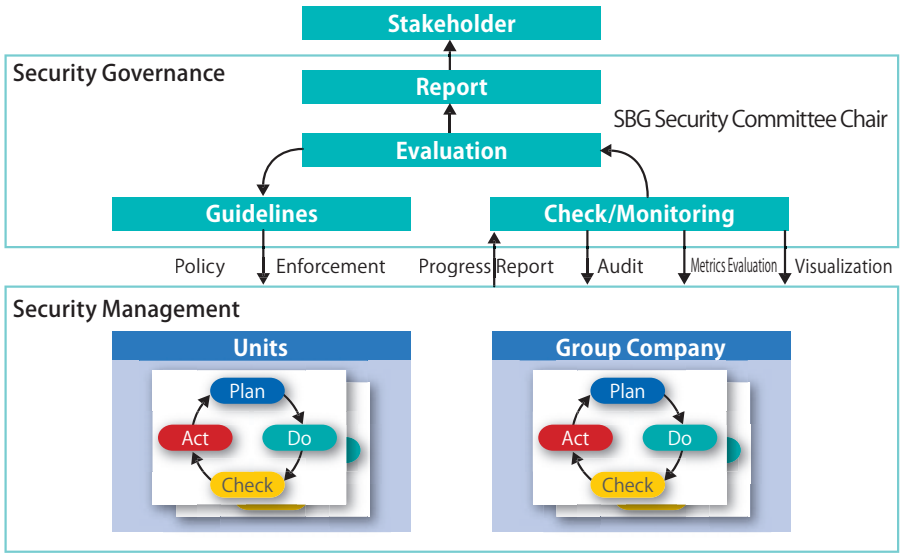
SBG Security Governance Construction/Practice

Security incidents, such as leaked personal data or attacks on corporate or organizational websites, prosper in mass media. The current situation is that information security risks are not decreasing. In this situation, the issue of security measures co-existing with business for corporation has become even more important. To resolve this issue, it is important for information security to largely capture the viewpoint of management and to work strategically.

SBG believes that the foundation is ensuring the safety and security of the customer and partners who apply IT and acts from the viewpoint of the customer. Recognizing that not only is enforcement of security measures expected but also appropriate information security activity, security management is pursued under security governance.

The SBG Security Committee Chair sets guidelines for information security, each department and the group company follows these guidelines, and drafts a security plan, introduces security measures, promotes daily activities, and promotes internal audits, etc., based on a security management frame work (SMF: see next page for details). And, these activities are checked and monitored and evaluated as to whether they are working effectively. Furthermore, activity contents are transmitted outside the company.

■ SBG Information Security Governance

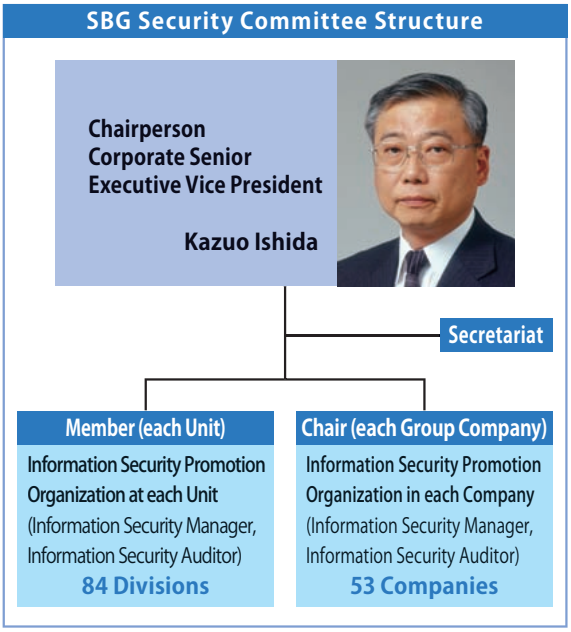


SBG Information Security Management Promotion System

The unit and group companies of SBG provide information systems that from the foundation of social and economic activities and are the frontline in dealing with customers. The "Solution Business Group Information Security Policy" was stipulated with the goal of sound protection of customer's information and internal information in order to handle customer's information assets or confidential information. The "SBG Security Committee" was established based on this policy and performs the maintenance and promotion of information security. Every quarter, a meeting is held for the SBG Security Committee Chair, information security managers from each unit and group company, and information security auditors.

Heads of each unit and group company presidents promote information security management as the SMF manager.

■ SBG Security Committee Organizational Chart

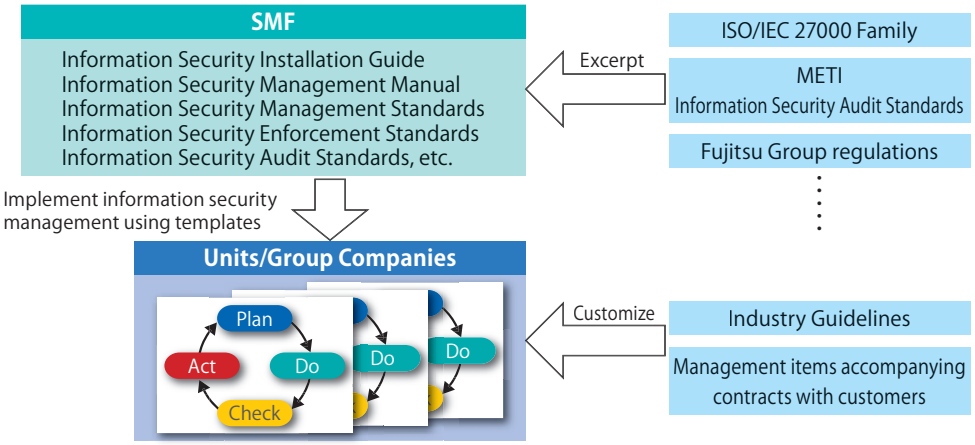


SMF (Security Management Framework)

At SBG, SMF is provided as a template to implement information security management. SMF includes the ISO/IEC 27000 family, which is the international standard for information security, the Ministry of Economy, Trade and Industry (METI) information security audit standards, and other domestic and international standards with the Fujitsu Group regulations. SMF consists of an information security management system and information security audit system. The management system includes information security management standards, information security enforcement standards, and information security enforcement guidelines. The audit system includes information security audit standards and information security audit enforcement guidelines. Furthermore, the Information Security Management Manual and the Information Security Installation Guide are included. At units and group companies, the industry guidelines of the customer for their divisions and the management items related to contracts with the customer are included and are customized to create departmental information security standards and information security audit standards.

The relationship between SMF and the Fujitsu Group regulations, international standards, and industry guidelines is shown below.

■ Relationship between SMF and the Fujitsu Group regulations, international standards, and industry guidelines



Security Improvement Efforts

Human Resources Development

"Information Security Manager Training" is provided to information security managers that perform guidance and management of information security at each unit and group company and for security promoters within departments. Presently, 450 employees have completed this training. Also, "Information Security Auditor Training" is provided to information security auditor managers and auditors who promote internal audits. Presently, 750 employees have completed this training. Specifically, auditors are encouraged to acquire qualifications from the Japan Information Security Audit Association (JASA) in order to increase the audit quality and improve their career path.

Through this, we have the highest number of qualified individuals in Japan (104).

Also, an "Auditor's Gathering" is held where audit practical reports and improvement announcements are given to promote improved audit techniques.

Security maintenance through it infrastructure standard operation service

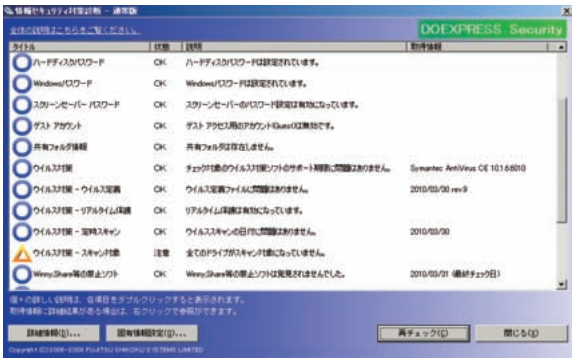
The SBG service division, in addition to installing "corporate standard PCs," develops a comprehensive service in each units and makes information security maintenance the main point throughout the life cycle of the PC: from distribution to the employee, installation support, daily operation, to disposal. 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, batch processing is used to delete data when the PC is discarded. By developing these services, the burden on employees related to enforcing security is lessened and reliability is improved.

Periodic security checks

A company-wide "Security Check Day" is implemented each month when a security inspection of PCs and an inspection of removable media devices are performed. Furthermore, anticipating occasional security threats, inspection items are added and security measure status is checked. If even a single PC has insufficient security measures, there is the possibility that information may be leaked, so an all-point check without exceptions is performed.

At SBG, the information security measure diagnostic tool (DOEXPRESS Security) is installed in all PCs to diagnose the security status of each PC. When a PC is started, the diagnostic items for in-house security regulations (20 items including OS, viruses, passwords, encryption, and prohibited configuration items) are automatically checked and diagnosed with the results displayed on the PC monitor. Also, the information security manager can collectively monitor the status of all PCs and easily grasp the overall security enforcement in the division. Furthermore, the diagnostic result log of the information security measures diagnostic tool is analyzed and when the existence of prohibited software is verified, a warning e-mail is sent to the manager of the division where the PC belongs. In doing so, security enforcement is realized effectively and reliably.

■ Information Security Measure Diagnostic Results Screen in Japan



Improving security awareness

Along with a daily awareness of security issues, a portable information security point collection (Information Security Pocketbook) was created and distributed to employees so that appropriate response could be taken when an incident or problem occurred. It is provided as a template so that independent measures could be added by the group companies. In addition to the portable version, there is a web version available. We strive so that security checks can be made a various work locations.

■ Security Education Site Screen in Japan

Security audits for systems delivered to customers

At Fujitsu, "Security Requirements for Customer Internet Connection Systems" (Security Requirements) is provided as a security measure for Internet connected system delivered to customers. It is mandatory that a security specialist department objectively verify that the contents of the "Security Requirements" are fulfilled before delivery to the customer.

In regards to web applications, because problems are resolved with an upper process, security checks are performed at the design stage.

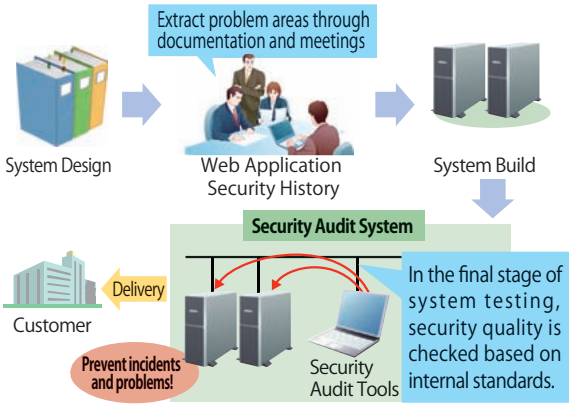
By doing so, the Internet connection system delivered to customers is ensured to have a homogeneous security level.

The customer system security audit is divided into an "infrastructure pre-delivery security audit system" for the infrastructure (OS/middleware) portion and a "web application security audit system" for the web application portion.

Information security audits

Internal division audits and audits by the SBG Security Committee on the division are performed periodically to perform information security management and security measures auditing. Internal audits are performed by auditors in information security management who have completed the "Information Security Auditor Training." The SBG Security Committee audit is performed by an audit team composed by auditors from the committee bureau and from outside the audited organization.

■ Security Audits for Systems delivered to Customers

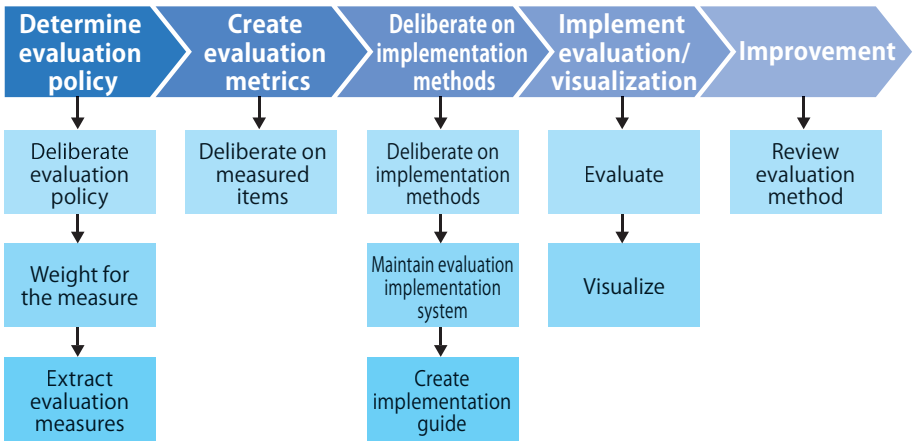


Monitor and Evaluate Activity

Information security activity includes activity on the management side and activity on the measures for PC security side. The SBG Security Committee evaluates to what level these activities are being performed using quantitative metrics. Evaluations by these metrics proceed through the following phases: Determine evaluation policy → create evaluation metrics → deliberate on implementation procedures → implement evaluation/visualization → Improvement. This is applied in each units and Group Company in SBG. Evaluation results are summarized as activity status throughout SBG and evaluation results for each units and Group Company. These results are then reported to the SBG Security Committee Chair and managers in each division (Heads of Units and Group Company Presidents).

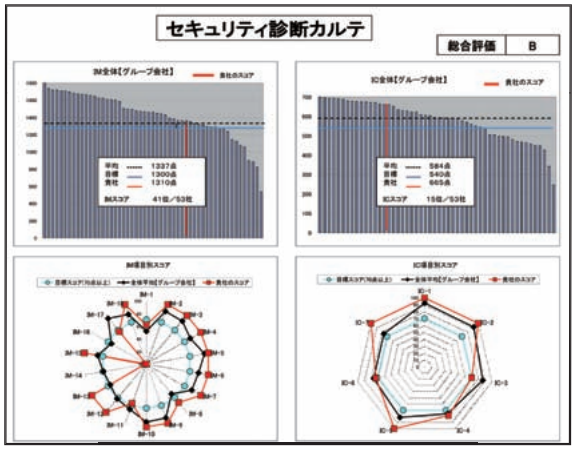
The evaluation concept and evaluation targets are determined in the "determine evaluation policy" phase. In the "create evaluation metrics" phase, elements that reflect the actual state of security activity and that can be quantitatively measured are considered. In this consideration, the international standards ISO/IEC 27000 family for effective measurements and the US National Institute of Standards and Technology (NIST) SP800 series are also referenced. In the "deliberate on implementation procedures" phase, determination is made by taking into consideration the method for collecting the elements to be measured, the amount of data to be collected, and the operational costs. Furthermore, the mechanism for the actual measurements

■ Phases from Determining Policy for Metrics Evaluation to Evaluation/Visualization



and an implementation guide will be maintained. In the "implement evaluation/visualization" phase, the measured elements are tabulated and analyzed and summarized in a security diagnostic chart.

■ Image of Security Diagnostic Chart in Japan



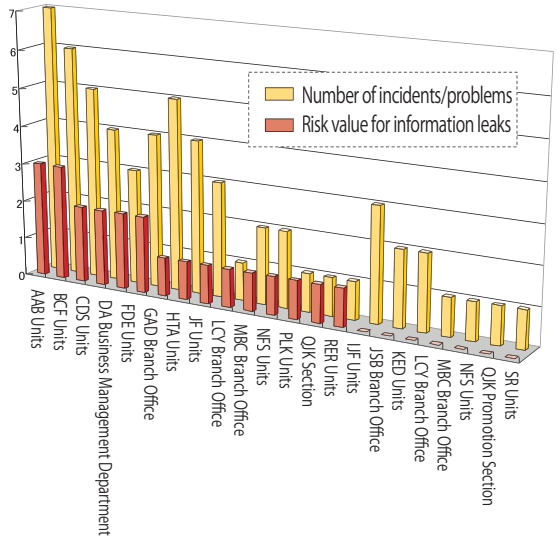
Risk evaluation for incident/problem information leaks

Information security incidents and problems include lost or stolen PCs or removable media devices and information leaked to the Internet via file sharing software. However, the chance that information will be leaked can be reduced by implementing passwords on PCs, hard disk encryption, and measures to prohibit installing file sharing software. Information security incidents and problems are evaluated by the number of occurrences as well as the risk value for information leaks. According to the type and existence of confidential or personal data, this evaluation examines the security measures status on the PC or removable media device where the information is stored and assigns a level as the risk value of an information leak.

Through this evaluation, the problem is not simply viewed as a simple occurrence of a PC being lost or stolen, but allows visualization of the risk that occurs with information leaks.

At SBG, along with risk evaluation by collecting incident and problem data periodically, publicizes the name of the worst division to bring awareness to prevent re-occurrence.

■ Risk evaluation for incident/problem information leaks

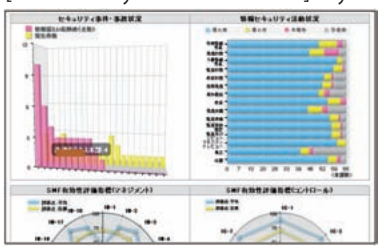


Visualization of Information Security Activities

The status of information security activities are measured and evaluated with several evaluation metrics. Furthermore, the evaluation results are presented visually to be understood uniformly. The visualization is presented in layers for the SBG Security Committee Chair, Divisional Managers, and Information Security Managers. The SBG Security Committee Chair layer displays the security status for all SBG and the evaluation results for each division. The Divisional Manager layer displays the results of the security evaluation for each division and the security management status. The Information Security Manager layer displays progress of security activities and specific security evaluations. The following shows the visualization for information security activities.

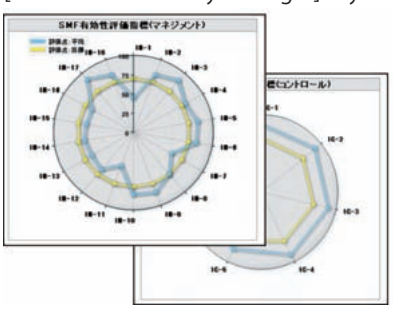
■ Visualization of Information Security Activities in Japan

[SBG Security Committee Chair] Layer



[Divisional Manager] Layer

[Information Security Manager] Layer



Case Study in Electronic Devices Business Group

The Electronic Devices Business Group (abbreviate to EDBG) develops LSIs with customers, and these customers require high-level control of confidential information such as design specification and design data. To ensure the required high-level control of confidential information, EDBG runs a secured document management system.

For a next step, EDBG plans to add protected document function, developed by Fujitsu Laboratories, to the entire life cycle management of confidential documents.

Secure Document Management System

This system provides a secure environment for the management of confidential documents, reducing the risk of information leaks without complicated procedures for users.

Putting this system to use, EDBG has established the following information management guidelines aimed at strengthening the management of confidential information:

Confidential documents are to be managed under the secure document management system.

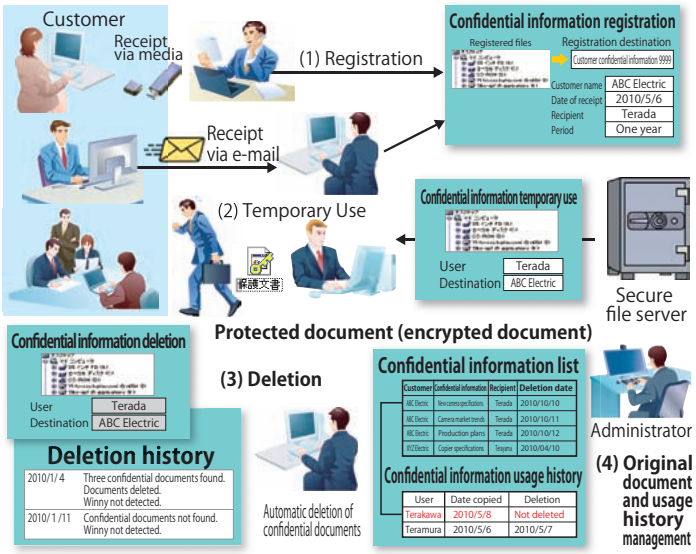
●Registration of confidential documents

Upon receipt of confidential documents, the document name, client name, date of receipt, name of recipient, storage period, etc. will be attached to property of the original document, which will then be recorded in the secure file server.

●Use of confidential documents

When temporarily using confidential documents, the certified person, destination, and planned period of use for files from the secure file server will be set, and the files copied to the user's PC. When the planned period of use has expired, the system will delete the confidential documents from the PC to which they were copied.

■ Secure Document Management System in action



Merits of the secure document management system

- Management of original confidential documents: Original Document Management Function
  Performs central management of confidential document name, client name, date of receipt, recipient name, storage period, and other original document management information, on the managed secure server.
- Management of temporary use of confidential documents: Temporary-Use Document Deletion Function
  Confidential documents copied from the secure file server to a user's PC for temporary use are deleted automatically at a specified time.
- History management for confidential documents: Usage History Management Function
  Performs central management of confidential document user, date of use, purpose of use, date of deletion, and other usage history information, on the managed secure server.
- Security management for users' PCs: Prohibited Software Deletion Function
  The system automatically checks for and deletes installations of prohibited software such as file sharing software.

Strengthened security function through protected documents

Encrypted and protected by the system, protected documents are usable only by persons authenticated by the system.

- Document protection for the life cycle of confidential documents
  Confidential documents temporarily copied from the secure file server are reliably protected with a protected document status over their life cycle. Documents protected include:
  - Confidential documents retrieved from secure file server
  - Edited protected documents
    - Edited and saved protected documents
    - Documents edited via copy & paste from protected documents
- Protected document status for confidential documents from a variety of applications
  Through the development of application-independent protection architecture technology, document protection is available for a wide range of documents.
  - Not only text but also components (images, charts) in protected documents are protected.

Case Study in Fujitsu Services Ltd. UK&I

Fujitsu Services Ltd. UK&I (hereafter FS UK&I) is a leading provider of IT systems, services, and products to private enterprise and public institutions, with clients in sectors ranging from retail, financial services, telecommunications, government, defense, and consumer.

FS UK&I is also a major IT supplier to the British government, providing services to many of its divisions.

Its Information Security Team provides services to manage the security and business continuity aspects of customer information at all stages of the client solution life cycle.

Information Security Management

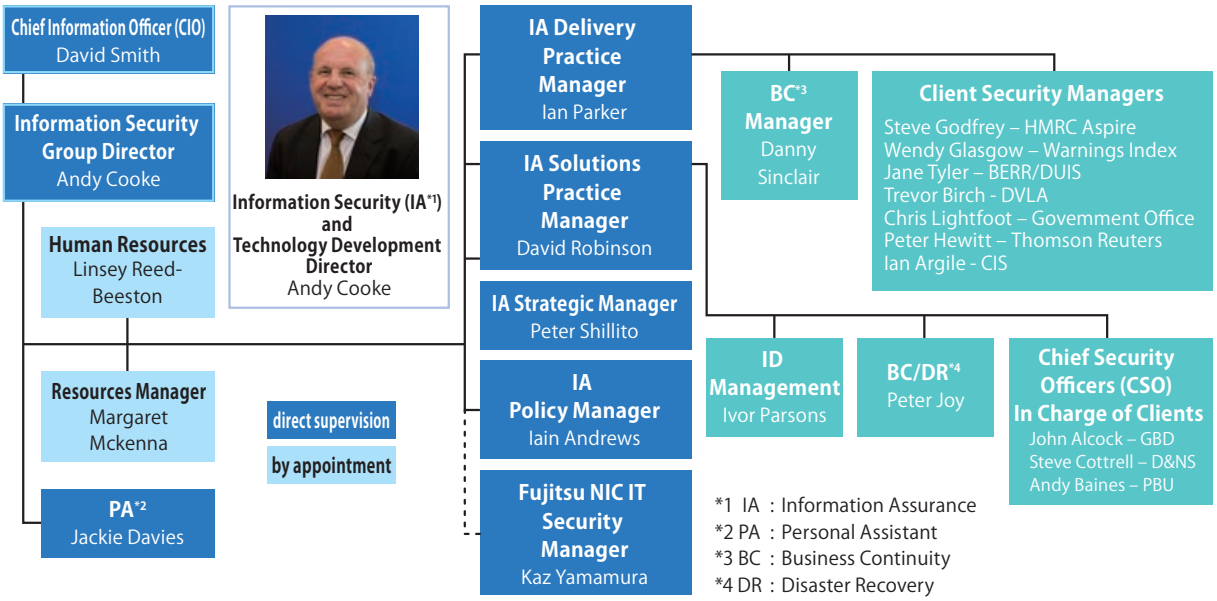
FS UK&I has achieved ISO/IEC 27001 certification for its networks and data centers, and is working to achieve certification for the user-facing services it offers clients such as the Royal Mail Group and Thomson Reuters.

The company plans to further expand the scope of its certifications, centered on its core business areas.

FS UK&I's information security-related documents consist of its Master Security Policy and Security Manual, which are based on Fujitsu's Global Information Security Policy and Global Information Security Controls Framework.

In conjunction with Fujitsu, FS UK&I also carries out internal audits to ensure that it conforms to the demands of global security.

■ Organizational chart for the Information Security Team



Information Security Measures

The same security services that FS UK&I offers to clients are used in-house by the company for its own security activities. These internal security measures are outlined below.

Security policies

FS UK&I's core security policies are established as a part of the company's business management system, and form the basis for the Security Manual. In addition, FS UK&I and Fujitsu's association with external organizations and business partners follows policies set out in the Code of Connection, a code which was announced at the Global Security Forum held recently in Japan.

Other security-related policies are drawn up in conjunction with Fujitsu's Global Information Security Controls Framework.

Information protection for devices

FS UK&I is moving ahead with volume-level encryption for all notebook PCs, desktop devices, and removable digital media connected via USB, in response to the expanding security demands of British government agencies and suppliers.

The company is rolling out the encryption software to meet these demands in steps, with implementation near completion.

Enhancement of education and awareness

FS UK&I requires security awareness training, including log management and reporting during secure operations, for all employees.

The company has also developed an online package for this training; it has fully implemented the package in divisions responsible for government business, and is rolling out implementation to all employees.

In addition, FS UK&I is looking into more effective mechanisms for security awareness training, such as methods for making security-related information known to all employees.

Toward the improvement of employees' awareness with respect to customer relations, the company is undertaking security education and awareness training focused on the customer environment.

Auditing

FS UK&I undertakes information security auditing. In November and December of 2009, as stipulated under contracts, the company conducted an audit of IA services provided to external clients, with the results and follow-up plans from the audit reported to the FS UK&I corporate governance committee in December 2009.

In the fourth quarter of fiscal 2009, FS UK&I conducted an information security audit in cooperation with Fujitsu.

Within divisions in charge of government business, FS UK&I has launched efforts to evaluate the British government's information maturity model.

Web filtering

Together with Symantec Corporation, FS UK&I is investing in anti-spam services and working to strengthen the functionality of its Internet scanning solution. The result has been a marked improvement in security functionality, with a projected 20% annual reduction in costs as well.

Services Provided

FS UK&I meets a wide range of client needs through the provision of security services that include the following components:

- Security solution design
- Security consulting
- Design and consultation for business continuity and disaster recovery
- Design and consulting for ID and access management

Outsourced services

- Security operation and operations management
- Auditing and compliance monitoring
- Chief security officer
- Security management

Case Study in Fujitsu (China) Holdings Co.

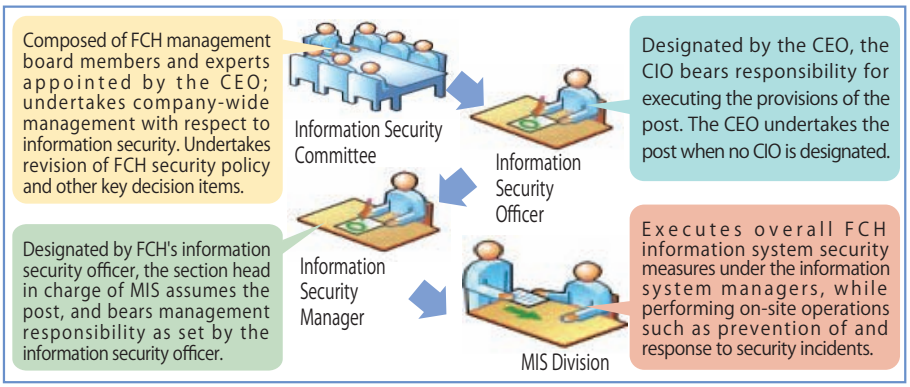
Fujitsu (China) Holdings Co. (hereafter FCH) was established in China as a 100% subsidiary of the Fujitsu Group, forming the core of Fujitsu's operations in the nation. From its headquarter in Shanghai, its branches in Beijing, Tianjin, Chengdu, and Shenzhen, and its service centers in 27 locations nationwide, the company offers total business solutions including solutions, services, and platforms. (Certification: ISO9001, CMMI V1.2 L4 Level 3 SI vender authorized by Chinese Government)

Information Security Management

Implementation structure

The Information Security Committee, composed of management board members, appoints security officers and information security managers. Under the information security managers, the Management Information System (MIS) division carries out FCH's overall information system security measures, while implementing operations such as prevention of and response to security incidents.

■ FCH's information security implementation structure

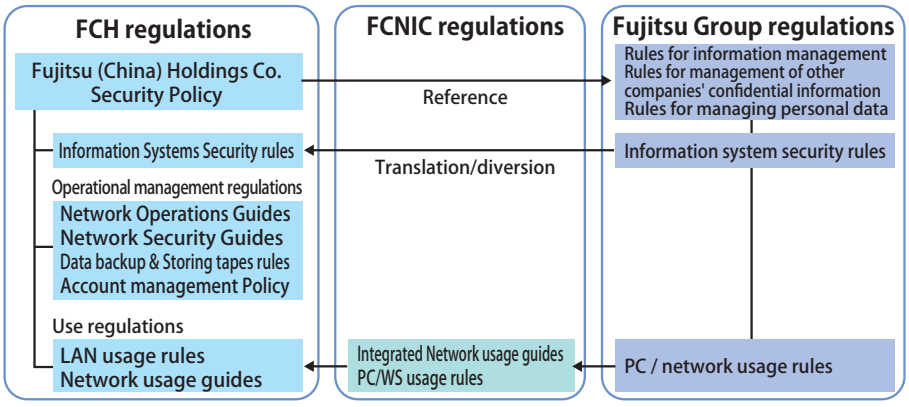


Creation and observance of information security policy

FCH's information security policy conforms to Fujitsu Group security regulations (Rules for Management of Confidential Information, Rules for Management of Third Parties' and Customers' Confidential Information, Rules for Management of Personal Data), covering all information systems and information assets used in the company's business, as well as all users.

If the information security officer determines a violation during the execution of business by an FCH employee, with regard to compliance with laws, regulations, and related Fujitsu Group regulations, or with regard to FCH information security policies, then action (including disciplinary action based on human resource regulations) may be taken against the employee in question, as appropriate for the severity of and the conditions surrounding the incident.

■ Relationship between FCH information security policy and Fujitsu Group regulations



Information Security Measures

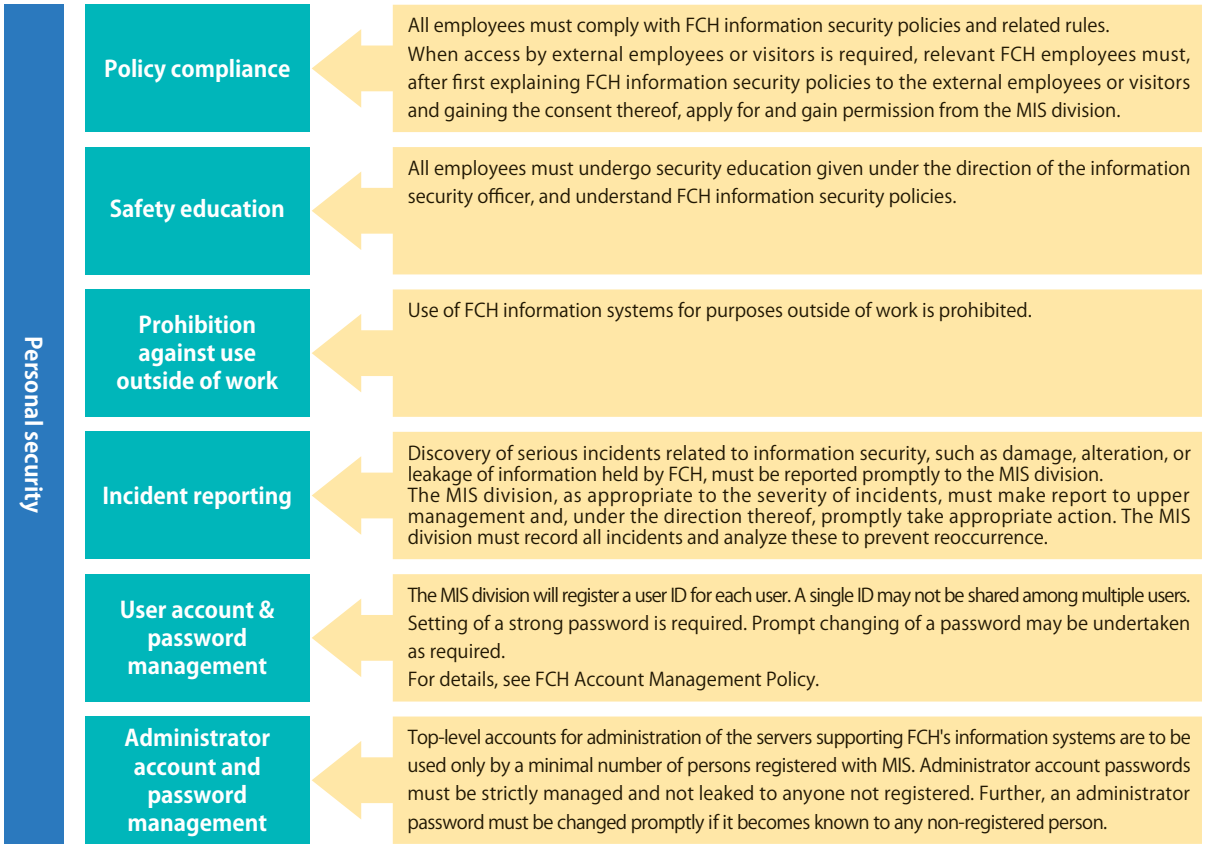
IT asset management

At FCH, the Management Information System (MIS) division provides services to all employees, with the goal of maintaining information security with respect to the distribution, daily operation, and disposal of standardized PCs to employees. The division monitors the condition of all PCs through the installation of Systemwalker DTP, and keeps users appraised regarding application of security patches using WSUS, automation of virus definition file updating, virus infections, installation of prohibited software, BIOS/Windows password setting, software licensing volume, and so on.

Personal security management

Personal security is a major element of information security. FCH's information management committee has set the following detailed regulations within IT security policy for management of employees' security:

■ Personal security policy, detailed regulations



Information security checks

Within FCH the MIS division periodically checks the status of security measure implementation. Information security audits and network security audits are also performed periodically by FCNIC (Fujitsu China Network Information Center) or by Fujitsu.

Enhancement of security awareness

Throughout the execution of business with the global accounts, Japanese firms, and large Chinese firms that are FCH's clients, in order to enhance each employee's concern for security and to enable appropriate response to incidents or accidents, a series of regulations and documents are available via the company's internal portal. Further, all personnel education directed at new employees includes security-related regulations.

Case Study in Offshore Development

Recently, it has seen an increase in opportunities for offshore development in conjunction with companies overseas, particularly in China. With respect to such offshore development, the Fujitsu Group implements information security measures and works to maintain the same level of information security that it achieves domestically.

Contractual Measures

In China and the main five companies *1 (a general customer and Fujitsu group of the offshore development), "Information Management Items for Outsourcers" that provides for the handling of trust information that Fujitsu provided is exchanged, and observed. What should be especially noted by the offshore development is extracted, and in addition, "Information Management Rule" is provided, and observed by itself.

*1 Beijing Fujitsu, Fujitsu Xian, Fujian Fujitsu, Nanjing Fujitsu, and Jiangsu Fujitsu.

Examples of Development Environment Measures

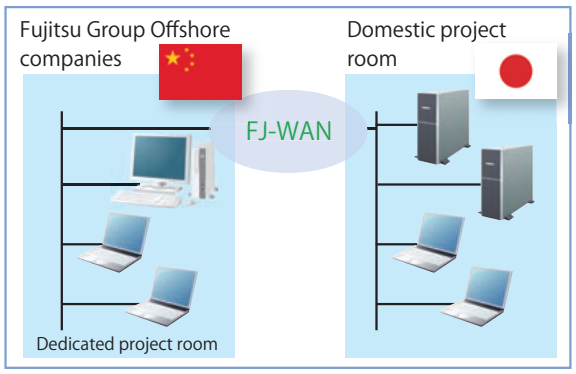
Use of dedicated networks

Fujitsu and its group companies use a closed network, FJ-WAN, to ensure the same level of information security achieved within Japan. Moreover, for projects with greater security requirements, the company deploys servers within FJ-WAN for remote access by the offshore development partner, creating a development environment in which no project assets remain with the overseas company.

Establishment of dedicated project rooms

The Fujitsu Group establishes dedicated project rooms allowing managed locking and unlocking of entrances at specified times and by specified persons, via Identification cards and PIN numbers. The project rooms also prevent against removal of the information assets through prohibition of carried-in items and through server-based restrictions against use of media such as USB flash drives and CD-ROMs.

■ Visualization of development environment



Other Measures

Awareness activities and the Risk Management Committee

The Information Security Handbook, a Chinese-language summary of the Information Management Items for Outsourcers, is distributed to outsourcers to support information security awareness activities.

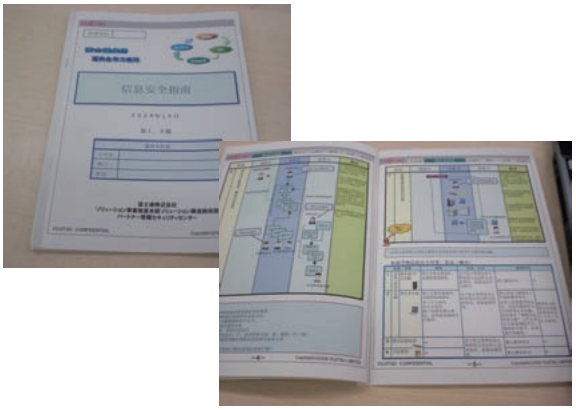
In addition, each project's information security management officer conducts information security education for the system engineers performing onsite work.

The Fujitsu Group also establishes a Risk Management Committee within each offshore company to promote risk management aimed at preventing and responding to risks.

Acquisition of international standards for information security

The Fujitsu Group's five main Chinese companies have achieved certification based on the international standards ISO 9001 and ISO/IEC 27001. A number of other companies not yet certified are undertaking steps toward that goal.

■ Chinese-language Information Security Handbook



Information Security Enhancement Measures in Cooperation with Suppliers

The business activities of the Fujitsu Group are supported by suppliers whose software, services, goods, and materials from the base of the value added by Group companies.

Through a never-ending accumulation of learning, the Fujitsu Group and its suppliers 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.

The Fujitsu group hangs out "Information security accident extermination" with the customer in the entire supply chain, executes measures of the education, enlightenment, the audit, and the intelligence sharing, etc. continuously for prevention and the relapse prevention plan of the information security accident, and is promoting the active conduct of business that considers the maintenance of the information security.

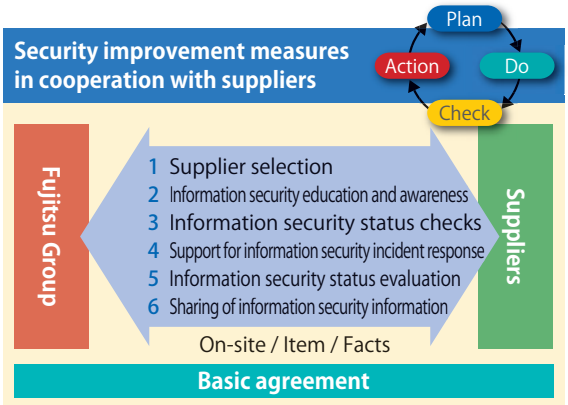
Tendency and measures of recent information security accident

The information security accident in the customer depends on thoroughness and the infiltration of measures, and the decreasing tendency includes the information leakage to the Internet with the file-sharing software, the loss, the theft of the bag due to carelessness, the wrong transmission by E-mail and the fax, and the losses of the identification card and the cellular phone, and so on.

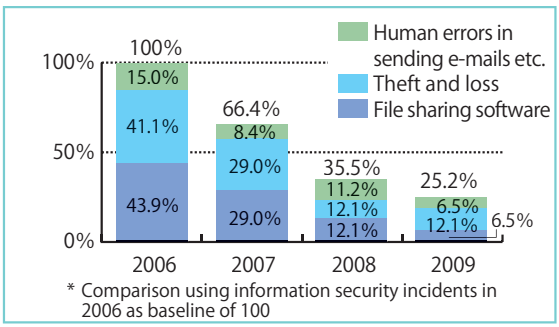
In fiscal year 2009, existing measures were enhanced by new measures directed more closely to on-site activities:

(1) On-site workshops for suppliers
(2) Publication of latest information in the Information Security Plaza awareness newsletter
(3) Enactment of project-level information security inspections

■ Security improvement measures in cooperation with suppliers



■ Trends in information security accidents



Supplier selection

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

In addition, the Fujitsu Group supervises subcontractors and other suppliers with respect to the Act on the Protection of Personal Information.

Information security education and awareness

In addition to education and awareness training aimed at subcontracted suppliers, the Fujitsu Group provides e-learning and other educational measures, educational materials, recent security information, and information security enhancement tools both to suppliers and within the Group.

- Information security training seminars for suppliers
  - About 1300 companies / 1800 people in January, 2009
  - About 1100 companies / 1200 people in December, 2009
- On-site training seminars
  Dispatch of lecturers to provide training seminars for supplier employees, at request of suppliers: 54 companies, about 1600 people
- e-learning inside Fujitsu
  - About 1100 people in January, 2009
- e-learning aimed at Fujitsu Group companies
  - 2H 2009 49 companies / about 13000 people

■ Information security training seminar

Information security status confirmation

Based on the contracts with its suppliers, the Fujitsu Group undertakes regular checks of suppliers' information security status; offers guidance on planning and carrying out the resulting corrective measures; and conducts follow-up on the corrective measures. Further, the Group makes corrective recommendations and conducts follow-up on corrective actions when a supplier experiences an information security incident.

- Fiscal 2009 audit about 240 companies (about 1000 total companies)
- Information security status surveys (including personal data management) targeting major suppliers
- Inspection of suppliers and of project-level information security demands, upon request

Support for information security incident response

In the event of an information security incident, the Fujitsu Group cooperates with the affected supplier or other section to perform initial investigation (such as assessing the impact of leaks), and to otherwise assist with response.

Information security status evaluation

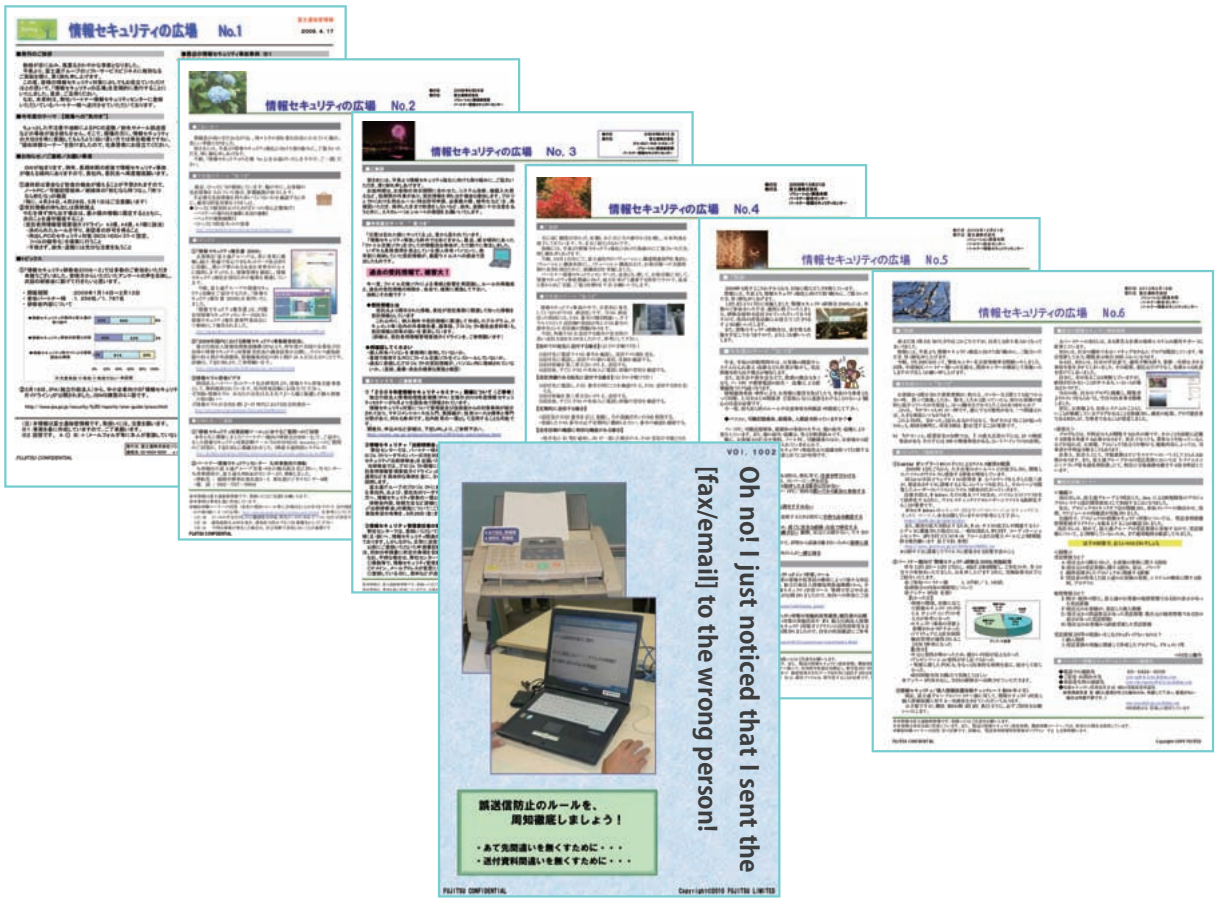
The Fujitsu Group evaluates suppliers' information security status based on status checks, response to information security incidents, etc. In the event of serious incidents without sufficient improvement effected, the Group may halt the relationship or suspend new orders, as necessary.

Sharing of information security information

The Fujitsu Group designates information security officers for suppliers, and undertakes timely sharing of the latest security-related information.

- From April 2009, Information Security Plaza has been published every other month to share the latest information on information security. The Fujitsu Group also provides awareness-building posters to prevent information security incidents.

■ Information Security Plaza and awareness poster in Japan



Social Contribution Activities Related to Information Security

In the information security industry, IT device vendors, communications carriers, consulting firms, and other corporations, governmental agencies and independent administrative institutions, and educational research organizations work together daily to create standards and guidelines and perform joint research. The Fujitsu Group has been actively involved in social information security activities over many years.

ISO/IEC* JTC 1/SC 27

ISO/IEC JTC 1 is a Joint Technical Committee established by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) for international standardization. SC27 is a sub-organization under this committee (the 27th sub-committee) and handles security techniques. Deliberation on international standards related to information security, such as ISO/IEC 27000 family and ISO/IEC 15408 series, takes place here.

Fujitsu participates as a regular member corporation in the SC27 Committee of the Information Technology Standards Commission of Japan of the Information Processing Society of Japan, which is the National Body for SC 27. We have continued to assign members to actively participate in the deliberation over standards.

In the information security industry, IT device vendors, communications carriers, consulting firms, and other corporations, governmental agencies and independent administrative institutions, and educational research organizations work together daily to create standards and guidelines and perform joint research. The Fujitsu Group has been actively involved in social information security activities over many years.

- ISO/IEC 15408-1: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- ISO/IEC 15408-2: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components
- ISO/IEC 15408-3: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
- ISO/IEC 27001: Information technology -- Security techniques -- Information security management systems -- Requirements

*: International Organization for Standardization/International Electrotechnical Commission

NPO Japan Network Security Association (JNSA)

Fujitsu is a corporate member of NPO Japan Network Security Association and has participated in various working group activities since 2004. The working groups in which Fujitsu group members have been active up until February 2010 are as follows.

- Vulnerability Quantification Working Group (formerly the Technical Committee)
- Web Application Security Working Group (formerly the Technical Committee)
- Information Security Ranking Working Group (formerly the Policy Committee)
- Security Incident Investigation Working Group (Survey and Research Committee)
- Security Awareness Working Group (Social Activities Committee)
- Secure Programming Working Group (Standards Investigation Committee)
- Information Security Control Map Working Group (Standards Investigation Committee, leader and sub-leader role)
- Information Security Check sheet Working Group (Western Japan Branch, leader role)

Other Social Contribution Activities

In addition to the above, we sent participating members to the following working groups and organizational activities.

- $(ISC)^2$ International Information Systems Security Certification Consortium
- Information Technology Research and Standardization Center, Japanese Standards Association, Information Security Management and Evaluation Standardization Survey and Research Committee (WG2)
- Cryptography Research and Evaluation Committees (CRYPTREC)
- Standards Certification Unit, Industrial Science and Technology Policy and Environment Bureau, Ministry of Economy, Trade and Industry
- Trusted Computing Group Specialists Committee, Japan Electronics and Information Technology Industries Association (JEITA)
- Research Group for Security Requirements in Procurement, Information-technology Promotion Agency (IPA)
- Security Committee, Linux Consortium
- Secure Private Consortium
- Database Security Consortium
- Japan Information Security Management Systems User Group
- Japan Information Security Audit Association (JASA)
- Tokyo University CCR Information Security Community
- ISMS Technical Committee, Japan Quality Assurance Organization (JQA)
- Research Society for Cloud Computing and Japan's Competitiveness, Ministry of Economy, Trade and Industry
- Smart Cloud Research Group, Ministry of Internal Affairs and Communications

Security Measures for Cloud Computing

Cloud computing is a new processing scheme to realize the flexibility and agility of computing that is not possible in traditional systems. However, cloud computing presents new security problems, such as security and reliability, to the user.

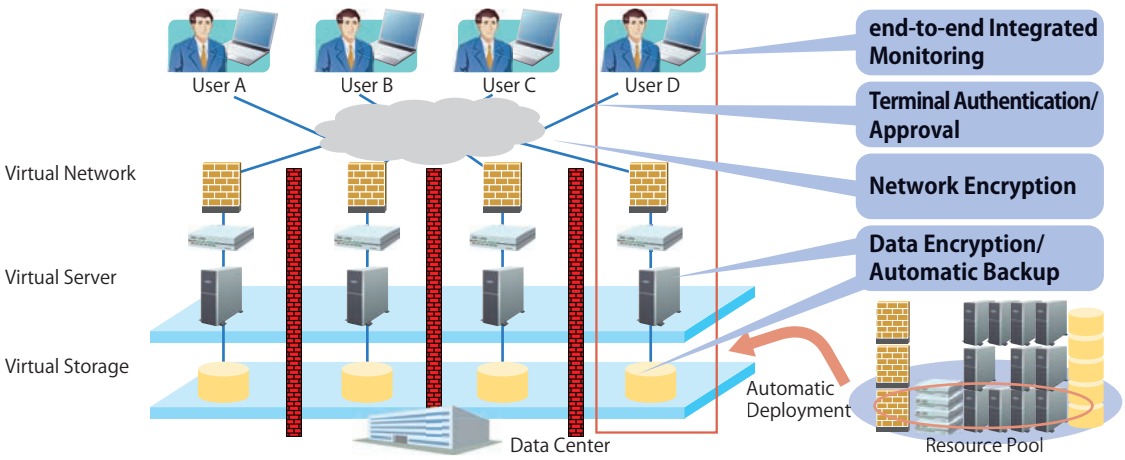
Here, the concepts of cloud security architecture to realize "Access Control," "Authentication and ID Management," and "Security Visualization," which are very important cloud computing characteristics, are introduced.

Access Control

The most distinctive feature of the platform (foundation) to realize cloud computing is that it is completely virtual. By having each system layer be virtual, flexibility in the structure and operation required for cloud PC is realized.

The Trusted Service Platform (TSP), the foundation of Fujitsu cloud computing, realizes the same level of security for each network, operating system, and data layer as in the example of using established, advanced virtualization technology to reliably segment the logical environment and physically separate the computing environment as in the "Secure Platform" project by the Ministry of Economy, Trade and Industry. Specifically, the software source code for the virtual server layer that is central to virtualization was reviewed by our company in order to ensure sufficient trust.

■ Cloud Computing Environment Segments



Authentication and ID Management

Several options are planned to be provided for Fujitsu's cloud computing in order to strengthen common authentication with ID and password. For example, one-time password authentication is a mechanism whereby a temporary password is displayed on a dedicated card or mobile telephone and the temporary password user would enter that password into a Web screen as authentication data. By doing so, even if that password were stolen, since it cannot be used again, authentication security would be significantly increased. Also, by using device authentication technology that uses electronic certification, a more secure authentication than password authentication that is more easily broken by guessing or information leaks can be realized.

When several systems are operating on cloud computing, managing user information becomes a major issue.

With Fujitsu cloud computing, we plan to offer our customers an ID management foundation for cloud computing that is based on open ID management frameworks such as SAML and WS-Federation.

Visualization of Security Measures

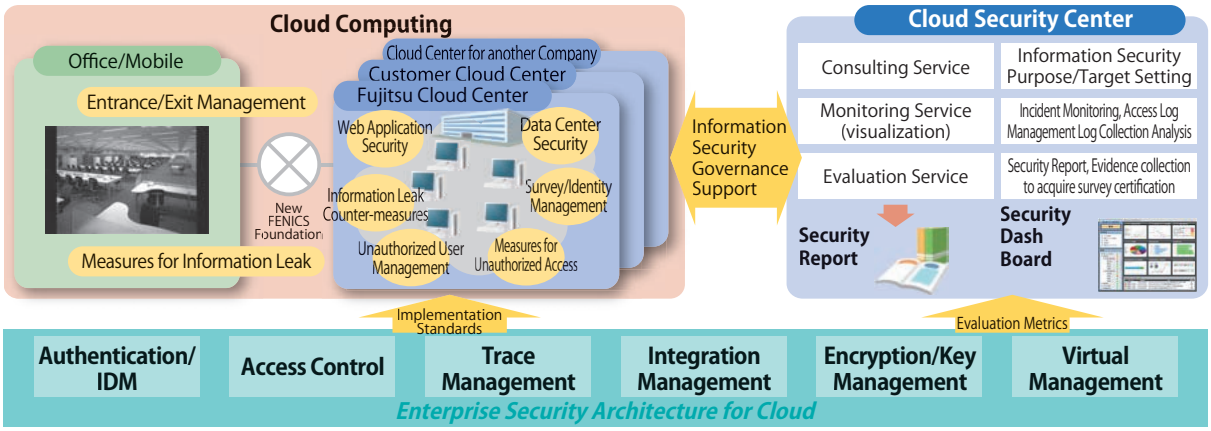
A characteristic of cloud computing is that "unnecessary items are not seen." Because this is so, the fact that "necessary items can be seen correctly" is a requirement for security and reliability for cloud computing.

Fujitsu began offering "Information Security Visualization Services" from 2009 to visualize customer's information security measure efficiency and cost-effectiveness.

Furthermore, we began providing security monitoring services using ArcSight, monitoring foundation software used all over the world including the US, from 2010. This service provides a report with value added from the viewpoint of collecting information, uniform management, information security governance, internal control, and security measure efficiency regarding security from the various customer systems including the administrative system in cloud computing. By maintaining a versatile information collection infrastructure such as this, security management in the cloud era, and by extension internal control and corporate risk management, can be performed more efficiently.

The work of monitoring and recording this kind of security in Fujitsu cloud computing is implemented by a specialist organization independent from the division providing the cloud service. By doing so, cloud computing security can be evaluated from a view independent of the service operation.

Cloud Monitoring Concept



Fujitsu Security Measures for Cloud Services

Requirement	Measure	Result
Authentication	• Client Certification + PIN Authentication	• Security is reliably improved compared to password methods
ID Management	• ID Management System (LDAP*1) Installation	• Ghost ID exterminated through prompt updates of ID information
Access Control	• Segmentation with VLAN • Role-based access control	• Leak problem prevention by reliably separating data in the cloud (Ensure security under multi-tenant environments) • Set detailed rights for system administrators and control unnecessary operation
Trace Management	• Periodic inspection of operation logs	• Prevent unauthorized internal use through operation monitoring by the company system administrator
Integration Management	• Integration management via an integrated console	• Prompt discovery and response to security incidents
Encryption/ Key Management	• Issuing secure certification with "SHA-256*2" Thorough management and operation of an expired certificate list	• Reliable prevention of information leaks due to occurrences of key management problems • Prompt access prevention when a certificate expires
Availability Design	• BC measures through redundant mirroring between structures/multi-centers that depends on component mirroring	• Improved service operation availability • Decreased RTO*3
Physical security	• Install new physical security - Entrance/exit management using biometrics - Location management with RFID	• Providing safe, secure cloud infrastructure → Security rating of AAA

*1 LDAP: Lightweight Directory Access Protocol. Protocol to access the directory database on a TCP/IP network, such as the Internet or an intranet.
*2 SHA-256: Hash function that appears in the e-Government recommended ciphers list
*3 RTO: Recovery Time Object. Targeted recovery time.

Third Party Evaluation/Authentication

Fujitsu and Fujitsu Group companies are working toward acquiring third party evaluations and certification regarding information security efforts, personnel skills, and products.

Privacy Mark Acquisition Status

Fujitsu or Fujitsu Group companies allowed to use the PrivacyMark from Japan Information Processing Development Corporation (JIPDEC) are listed below.

Fujitsu Limited
Fujitsu Advanced Solutions Limited
Fujitsu Advanced Printing & Publishing Co., Ltd.
Fujitsu Human Resource Professionals Limited
AB System Solutions Limited
Fujitsu FIP Corporation
Fujitsu FOM Limited
Fujitsu FSAS Inc.
Fujitsu Okayama Systems Engineering Limited
Fujitsu Kagoshima Infornet Limited
Fujitsu Kansai Systems Ltd.
Fujitsu Kyushu Systems Limited
Fujitsu Credit Solutions Limited
Fujitsu Communication Services Limited
Fujitsu CoWorCo Limited
Fujitsu CIT Limited
G-Search Limited
Fujitsu Shikoku Infortec Limited
Fujitsu Shikoku Systems Limited
Fujitsu System Solutions Limited
Fujitsu Research Institute
Fujitsu Social Science Laboratory Ltd.
Fujitsu Software Technologies Limited
Fujitsu Chugoku Systems Limited
Fujitsu Chubu Systems Limited
Totalizator Engineering Limited
Fujitsu Tohoku Systems Ltd.
Fujitsu Nagano Systems Engineering Limited
Fujitsu Niigata Systems Limited
NIFTY Corporation
Fujitsu Personal System Limited
Fujitsu Public Solutions Limited
Fujitsu Broad Solution & Consulting Inc.
PFU Limited
Fujitsu Business Systems Ltd.
Fujitsu Frontech Limited
Fujitsu Frontech Systems Ltd.
Best Life Promotion
Fujitsu Hokuriku Systems Limited
Fujitsu Hokkaido Systems Limited
Fujitsu Yamaguchi Information Co., Limited
UCOT Corporation
Fujitsu Learning Media Limited
Lifemedia, Inc.
Fujitsu YFC Ltd.

ISMS Certification Acquisition Status

Fujitsu and Fujitsu Group companies that organizations that acquired the ISMS certification based on Information Security Management System International Standards ISMS (ISO/IEC 27001) are listed below.

Fujitsu Limited
Fujitsu IT Products Limited
Fujitsu Advanced Engineering Limited
Fujitsu Advanced Solutions Limited
Fujitsu FIP Corporation
Fujitsu FSAS Inc.
Fujitsu Kagoshima Infornet Limited
Fujitsu Kyushu Systems Limited
Fujitsu Credit Solutions Limited
Fujitsu Communication Services Limited
Fujitsu Shikoku Infortec Limited
Fujitsu Shikoku Systems Limited
ZIFTEC
Fujitsu System Solutions Limited
Fujitsu Social Science Laboratory Ltd.
Fujitsu Research Institute
Fujitsu Defense Systems Engineering Limited
Fujitsu Tohoku Systems Ltd.
Fujitsu Tokki Systems Limited
Toyama Fujitsu Limited
Fujitsu Nagano Systems Engineering Limited
NIFTY Corporation
Fujitsu Network Solutions Limited

Fujitsu Broad Solution & Consulting Inc.
PFU Limited
Fujitsu Business Systems
Fujitsu Mission Critical Systems Ltd.
Fujitsu Middleware Limited
Fujitsu Mobile-phone Products Limited
Fujitsu Leasing Co., Ltd.
Fujitsu YFC Ltd.

Information Security Rating Acquisition Status

Information security ratings are an index that indicates the security level such as whether there are problems with alteration, leakage, or service stoppage of information such as technical information, confidential corporate information, or personal data handled by the company or organization.

The ratings are given by I.S.Rating Co., Ltd. The Fujitsu Group information security ratings are given below. The Tatebayashi System Center acquired an "AAAis" rating, the highest rating, as a data center business.

Company Name	Rating Scope	Rating Mark
Fujitsu Limited	Tatebayashi System Center	AAAis
Fujitsu Social Science Laboratory Ltd.	Software Service Department	Ais
PFU Limited	Solutions and Services Department	Ais

IT Security Evaluation Certification Acquisition

Following representative IT products that have received evaluation certification based on ISO/IEC 15408 international standards for security evaluation criteria.

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

ISMS Qualification Acquisition Status

The following number of employees at Fujitsu and group companies qualified as ISMS auditors.
<qualified ISMS auditor number: 137>

JASA Auditor Qualification Acquisition

Japan Information Security Audit Association (JASA) is a certification organization for auditors who implement information security audits based on the 2003 Ministry of Economy, Trade and Industry's "Information Security Audit System." The categories of qualifications are "Certified information security senior auditor," "Certified information security auditor," "Information security auditor provisional," and "Information security auditor associate."

In Fujitsu and group companies, qualified personnel participate in internal audits and information security audits requested by customers. The following number of employees at Fujitsu and group companies qualified as JASA auditors.
<qualified JASA auditor number: 104>

Contact Department
Fujitsu Limited
Information Security Center
1-17-25 Shin-kamata, Ohta-ku, Tokyo 144-8588
Fujitsu Solutions Square
E-mail：isc-smf@ml.css.fujitsu.com
URL：http://www.fujitsu.com/

FUJITSU

FUJITSU LIMITED

www.fujitsu.com

VOC FREE

Waterless Printing. Naturally.

FSC Mixed Sources
Product group from well-managed forests and other controlled sources
www.fsc.org Cert no. SA-COC-1577
© 1996 Forest Stewardship Council

This report uses forest-registered paper,VOC-free ink,and a waterless printing process that generates no harmful liquids.