Fujitsu Group Information Security Report 2011

FUJITSU

shaping tomorrow with you

CONTENTS

Report Summary

Target Period and Scope of the Report
This report covers the period up to March 2011 and focuses on efforts in information security by the Fujitsu Group.

Report publication date
This report was published in August 2011.

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 human-centric ICT solutions, 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, five 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 2011" 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 corporate governance system, the Fujitsu Group promotes appropriate information management and information usage while observing internal company rules regarding information security for a complete system of risk management.

Corporate Governance and Risk Management

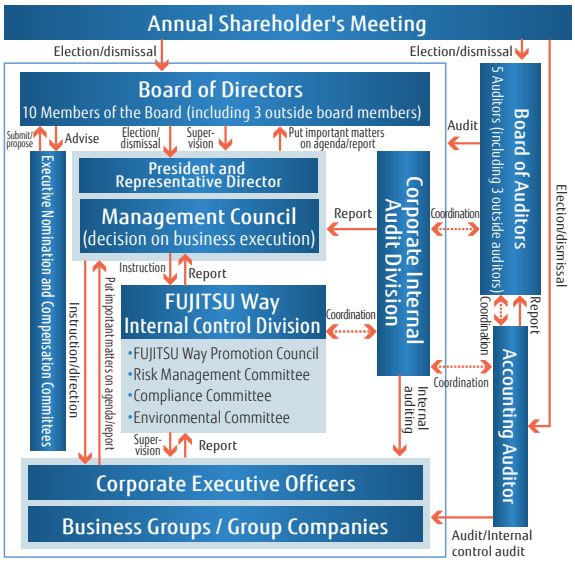
Corporate Governance

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 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.

Corporate Governance Framework

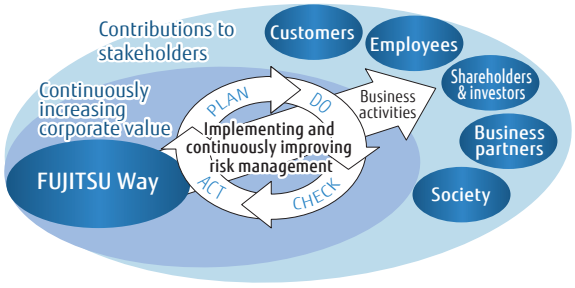


Risk Management

We are working to strengthen our Group-wide risk management structure, promoting activities aimed at preventing risks from materializing and minimizing the impact should an incident occur.

Through its global activities in the ICT industry, the Group continuously seeks to increase its corporate value, and to contribute to its customers, local society and indeed all stakeholders. Properly assessing and dealing with the risks that threaten the achievement of our objectives is assigned a high priority by management. The entire Group has built a risk management system in accordance with the Fujitsu Way, and is committed to its continuous implementation and improvement.

Implementing and continuously improving risk management



We have also established the Risk Management Committee as a body to perform risk management. This committee reports directly to the Management Council.

The Risk Management Committee appoints risk management executives in all business units and companies throughout the Group, and encourages cooperation among them both to guard against potential risks and to mitigate risks that are threatening, forming a risk management structure for the entire Group.

Risk Management Structure

Information Security

Information Security Policy and Related Rules

We have established the "Fujitsu Group Information Security Policy" that applies both in Japan and internationally, and are working to promote information security.

We have also implemented five related rules based on the "Fujitsu Group Information Security Policy" and are implementing measures for information security.

Fujitsu Group Information Security Policy

1. Objectives

Being fully aware of the fact that information provides basis for the Fujitsu group's business activities and the risks that accompany the management of information, Fujitsu group meets the information security requirements to achieve the following objectives. This is to conform to the Corporate Values of FUJITSU Way, "we seek to be the customer's valued and trusted partner and we build mutually beneficial relationships with business partners.", and to enforce the "confidentiality" defined in Code of Conduct as essential part of social responsibility.

(1) Fujitsu group properly maintains information delivered by individuals, corporate clients or vendors in the business processes to protect the rights and interests of these subjects.

(2) Fujitsu group properly maintains trade secret, technical information and other valuable information in the business processes to protect the rights and interests of the group.

(3) Fujitsu group properly maintains information in the business processes to provide products and services in a timely and stable manner and to ensure social functionality of the group.

2. Principles

Fujitsu group applies the following principles in meeting the information security.

(1) Preservation of confidentiality, integrity and availability shall be the objective of information security, and the information security measures shall be planned to meet the objective.

(2) Organizational structure and responsibility shall be clearly defined to ensure the proper implementation of the information security measures.

(3) The risks that accompany the handling of information and investments required for the measures shall be taken into consideration to properly implement the information security measures.

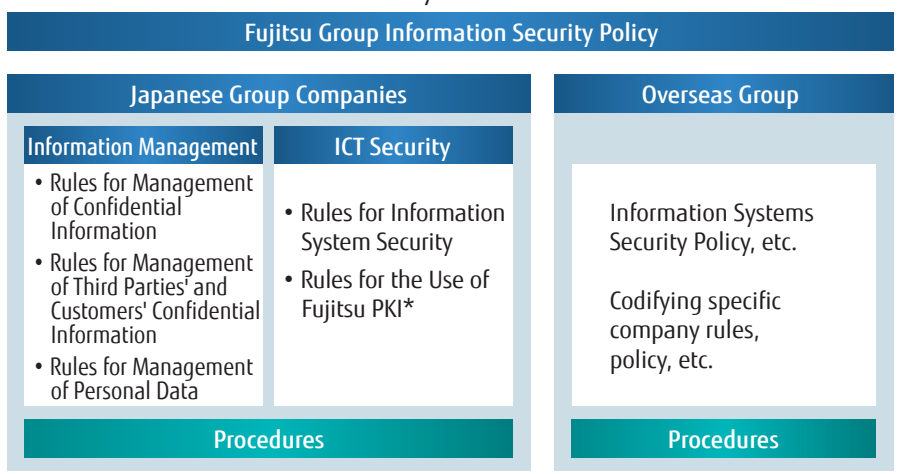
(4) Information security processes shall be organized into Plan, Do, Check and Act phases to keep and enhance the level of information security.

(5) Executives and employees shall be provided with awareness and education program on the information security and act with the knowledge of its sensitive nature to ensure the proper implementation of the information security measures.

3. Fujitsu group's activities

To ensure the implementation of the aforementioned objectives and principles, each Fujitsu group company shall prepare its policy and related procedures in compliance with this policy, and implement them.

Framework of information security rules



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

Promoting 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. 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 Screen in Japan

Raising awareness regarding information security

Fujitsu and Japanese group companies displayed posters at each of their business locations use a common slogan that translates as "Declaration for complete information management! Information management is the lifeline of the Fujitsu Group". They also affixed seals to all employees' PCs in an effort to increase the awareness of information security in every individual employee.

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.

Also, a mail checker tool was introduced to prevent E-mail 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.

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

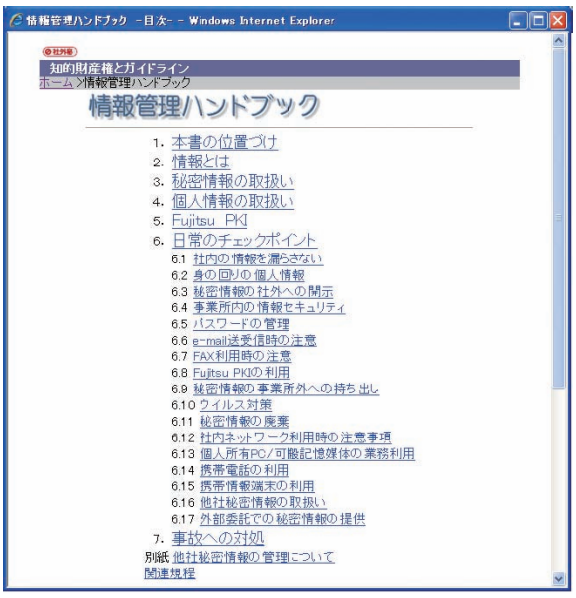
Fujitsu has established the "Personal Data Protection Policy" and "Rules for Management of Personal Data" in compliance with Act on the Protection of Personal Information. We are also continually strengthening the system for protecting personal information based on these rules such as holding annual education and audits on the handling of personal information.

We acquired company-wide PrivacyMark certification in August 2007 and updated the certification in September 2009. Japanese 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" has been issued 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

"Information Management Handbook" Screen in Japan



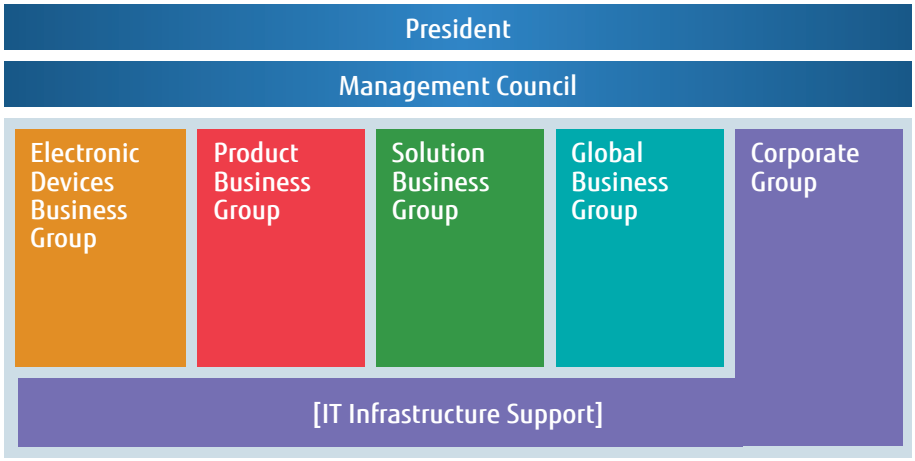
the many incidents of information leakage from around the world, a security check day is held once a month, and management holds activities to verify the status of security measures in their own divisions.

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 electronic components such as batteries, relays, connectors, and compound components in addition to LSIs and semiconductor packages, which are built into digital home electronics, automobiles, mobile phones, servers, etc.

[Global 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 as "One Fujitsu" based on the concept of "Think Global, Act Local."

IT Security Efforts

In situations where IT (Information Technology) 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 business application systems" and "client security" as well as the common mechanisms of "IT resource management," "authentication systems," and "network security."

IT Security Framework

Authentication system implementing integrated user management	Information Management for application systems	Client security control	Network security control
With a security card ● Entrance management ● Authentication ● Document approval	Based on analysis of the business/information/user ● Access control functions ● Reliability features	● Automated measures ● Measures for human errors in sending e-mails ● Corporate standard PC	● Network control ● E-mail control ● Network service use control

IT Resource Management as the basis of IT Security

● Management of goods as assets ● Security measures management ● License management

Information management in business application systems

The Fujitsu Group applies IT to various tasks such as finance/accounting, human resources, marketing, sales, systems engineer 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 reliability 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

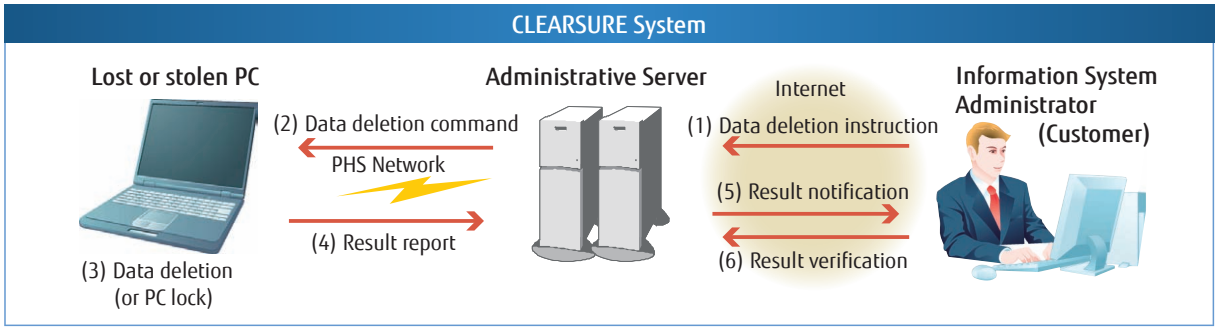
e-mail to a wrong address. To reduce the risk of this information leakage, e-mail addresses are automatically checked, and the sender is required to reconfirm when it is addressed to external persons.

- 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 laptop PCs, corporate standard laptop 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 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 IT 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, specification
- 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 office of the Fujitsu Group are equipped with security doors at the entrance. Employees coming to the office use their Security Card for entrance.

[Authentication]

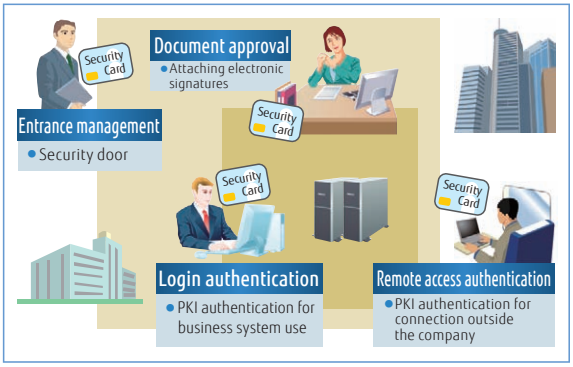
The Security Card is required to use the application system. Authentication by PKI at login to application systems enables secure identification and authentication of employees along with simple operation.

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* and firewalls by specialist groups
  - Inspection and authorization of connections performed by divisions

* 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 (Supports the latest devices such as smartphones)
- 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

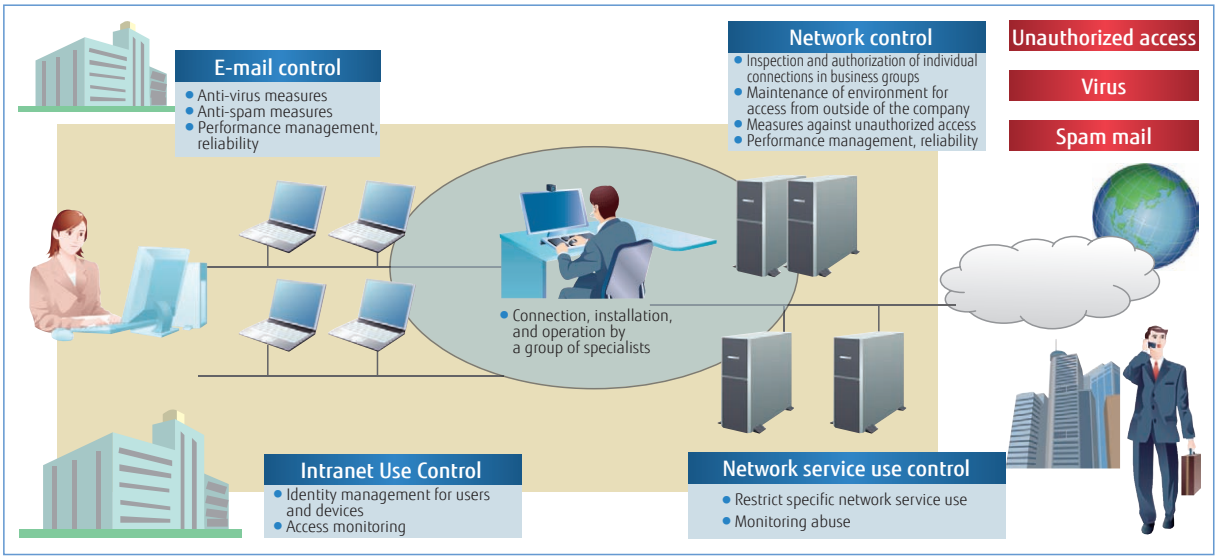
[Network service use control]

The Internet environment outside the company provides many network services such as file transfer and online meetings. Use of these services are selectively approved with necessary conditions based on the evaluation of business merrits 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]

Use of intranet is controlled throughout the Fujitsu Group. Users and devices are managed, and legitimacy is verified through authentication when connecting. The control extends to all of the companies in the group as one of the globally governing practices based on the "Fujitsu Group Information Security Policy."

Network security control



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. This section introduces the security initiatives implemented in the Fujitsu Cloud Computing Service.

Security in the Fujitsu Cloud Computing Service

In a cloud system, a lot of user accounts and data are concentrated in the same ICT resource. Because the users and cloud service provider need to cope with various possible threats in this form of system, it is important to be aware of the individual areas of responsibility and to mutually cooperate. This section describes the approach to security governance initiatives, approach to compliance (adhering to laws, etc.), various security measures, and emergency system for handling security that are implemented in the Fujitsu Cloud Computing Service.

Security Governance

One of the features of cloud services is that many geographically separated bases work together and cooperate to provide an optimal service. Because of this, it is necessary to implement uniformly controlled security standards at each of the bases throughout the world. In the Fujitsu Cloud Services, a "Cloud Services Information Security Policy" has been established that is applied to all cloud data centers including at Fujitsu overseas group companies as a framework for all cloud services provided by Fujitsu data centers. A Cloud Security Committee has also been established in Fujitsu Cloud Services made up of executives concerned with the senior exective president as the committee chairperson as a place for establishing a global information security framework that encompasses the service execution organizations in each of the countries around the world and as a forum for regular risk evaluation and decision-making. Furthermore, the development division, operation division, and security related divisions that form the basis of the cloud services within the Fujitsu Group Cloud Services work together to form a framework that is able to holistically and comprehensively handle within the group the variety of information security risks that exist within the cloud service.

Compliance

In the cloud, the positioning and boundaries between stakeholders (system users, system owners, and cloud service providers) differ greatly from conventional models. Because of this, it is becoming important to clearly define the division of duties and partitioning of responsibilities that were often vague in the past. In the Fujitsu Cloud Services, the conditions under which Fujitsu has access to the virtual system deployed by the customer is clearly defined such as by contract. This is to clarify the handling of the important information that the customer has entrusted to Fujitsu in accordance with the law and to protect the rights and interests of the customer. Furthermore, the ways in which Fujitsu handles confidential information such as customer proprietary information that the customer registers and inputs into the virtual system is clearly stated in a contract. The contract also clearly defines the kinds of measures that Fujitsu can take in which kinds of circumstances, such as if it becomes clear that the customer is using the cloud service for illegal purposes.

The task of maintaining compliance by following the demands of the various laws and regulations while using the cloud service is an important issue for customers, and requires simultaneously auditing the status of adhering to compliance. Because of this, logs need to be recorded appropriately so that the accesses and operations of cloud users can be investigated at a later time. The Fujitsu Cloud Service provides functions to assist our customers with compliance. For example, in the Fujitsu On-demand Virtual System Service, a log of the operations performed by users who have administrator privileges and by Fujitsu operators is recorded and stored for 7 years as an evidentiary trail for the purpose of maintaining customer compliance and auditing.

Policies and procedures are defined in relation to maintaining and storing cloud service data, and data preservation measures are implemented such as reliable information leak and information tampering prevention in accordance with these. For example, in order to prevent leaking of information when disposing of information in the on-demand virtual system service, all

of the storage areas that had been used are securely erased by overwriting with zeros when returning a customer virtual system that had been entrusted by the customer and when disposing of physical storage. Furthermore, the data that is saved in the storage is protected by powerful storage encryption schemes that comply with various international guidelines.

Security Measures

The Fujitsu Cloud incorporates a variety of security technology measures to ensure that customers can feel secure using the service.

In the Fujitsu Cloud Service, all of the customers who manage the cloud are allocated a unique user ID, and unauthorized usage of user IDs is prevented by strict authentication. An example is when a user uses the portal website that provides functionality such as configuration settings for the on-demand virtual system service, the deployment of the virtual system, and the confirmation of the operational status. In this case, the user downloads a digital certificate for personal authentication after the user is registered, and logs in using that digital certificate. Moreover, when using the digital certificate, two-factor authentication using a PIN (Personal Identification Number) codes of 16 digits or more is implemented, alleviating the risk of unauthorized usage of the digital certificate by a third party. In order to reduce the risk of unauthorized usage of user IDs, the service also implements a function that locks out user IDs after a fixed number of attempts if a user login fails several times in a row for repeated login attempts, and a function that requests re-login by digital certificate if a login session has been idle for more than a certain period of time.

In terms of network security, for example in the on-demand virtual system service, the network environment is logically partitioned between customers by a firewall function that is provided as standard. Furthermore, the internal segment of the customer system can be logically partitioned in up to 3 layers as a virtual network. This makes it possible to create a network configuration in the cloud of having a segment that is directly accessible from the Internet, a DMZ segment, and an internal segment, and allows customers to prevent direct access from the Internet to virtual servers that are responsible for important tasks such as the business application server and database server.

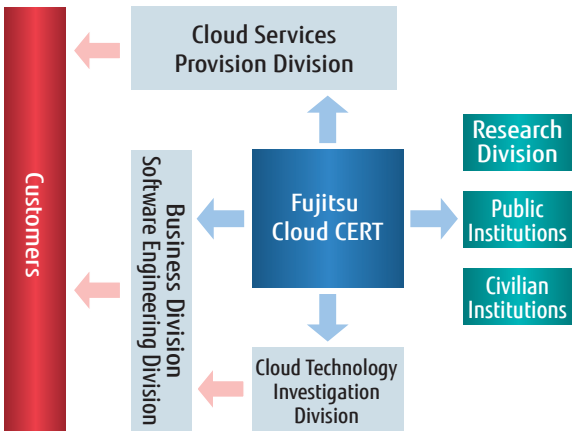
To archive the optimization of service and the continuous quality maintenance and improvement, the data center that supports Fujitsu's cloud service has been executing the activities of systematization and operation quality evaluation/improvement of the operation services using the PDCA cycle. Moreover, the "Tatebayashi system center", which is a state-of-the-art data center, acquired the highest information security rating of "AAA_{is}" by I.S.Rating Co.,Ltd for the first time in Japan in February 2010 for these activities.

Security Emergency Response System (Fujitsu Cloud CERT)

Common policies, processes, and procedures are established throughout the entire Fujitsu organization globally so that a flawless response can be made in the event that an information security incident occurs in the cloud computing environment, such as unauthorized intruders or virus infection. Even if a security incident occurs, a complete system is established in preparation that can quickly and reliably identify and report on information security related incidents by following these. Furthermore, in 2010 Fujitsu established an independent security emergency response division (Fujitsu Cloud CERT) for handling business related to cloud service security. The Fujitsu Cloud CERT handles establishing the above-mentioned "Cloud Service Information Security Policy", security monitoring and security diagnosis in each service environment, and the response during an emergency in cooperation with groups inside Fujitsu as well as external bodies.

Cloud computing is still a new field and the security requirements that are needed are therefore expected to change in the future. In order to comply with these new requirements, Fujitsu schedules continual enhancement and revision of the security of the cloud service in the future. The latest directions in the Fujitsu cloud service are introduced periodically such as on the public site.

Positioning of Cloud CERT



Approach of Solution Business Group

Because the Solution Business Group (SBG) 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.

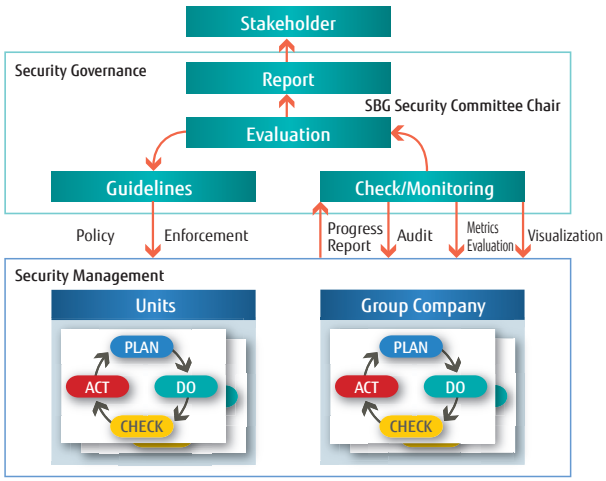
Solution Business Group Characteristics

The Solution Business Group (SBG) provides the most up to date business solutions using ICT for our corporate customers. The business solutions consist of (1) IT system consulting, (2) system architecture, (3) data center and IT operational administration outsourcing service, (4) network services, (5) system support services, and (6) security solutions. The Fujitsu service business has the No. 1 share in Japan and the No. 3 share globally, and is expanding services throughout a wide range of countries and regions from Europe and America to Asia and Oceania. In the outsourcing field in particular, data centers are setup in 91 bases in 16 countries around the world focusing on Japan and Europe, and these provide services that handle a variety of needs such as reducing the operational workload of customer ICT and supporting the environment.

SBG Security Governance Construction/Practice

Security threats to companies and organizations such as website attacks and leaking of personal information are growing, and demand risk management from a management perspective. Security activities are therefore 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 activities within each organization, and promotes internal audits, etc., based on a security management frame work (SMF: see next page for details). The chair also checks, monitors, evaluates the status of everyday activities and the status of security incidents and accidents, and works on improving the mechanisms and measures.

SBG Information Security Governance

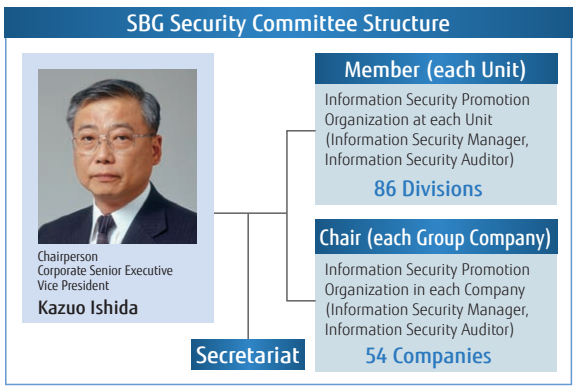


SBG Information Security Management Promotion System

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.

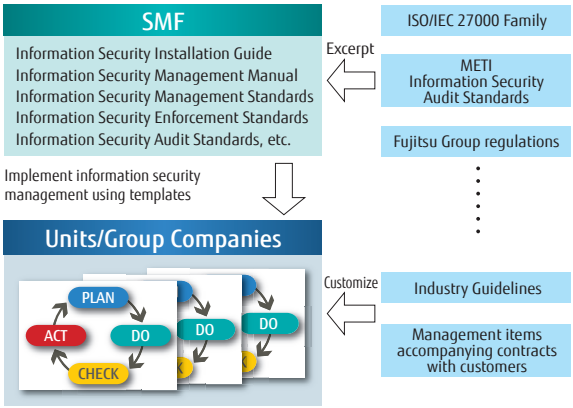
SBG Security Committee Organizational Chart



SMF (Security Management Framework)

At SBG, SMF is provided as a template to implement information security management. SMF includes the ISO/IEC 27000 family, the Ministry of Economy, Trade and Industry (METI) information security audit standards, and other Japanese and international standards with the Fujitsu Group regulations. SMF consists of an information security management system and information security audit system. The relationship between the SMF and Fujitsu Group rules, international standards, industry guidelines, etc. is shown in the diagram on the right. 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.

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, 487 employees have completed this training. Also, "Information Security Auditor Training" is provided to information security auditor managers and auditors who promote internal audits. Presently, 788 employees have completed this training. Specifically, auditors are strongly encouraged to acquire qualifications from the Japan Information Security Audit Association (JASA) in order to increase the audit quality and improve their career path, and 126 employees have acquired auditor qualifications.

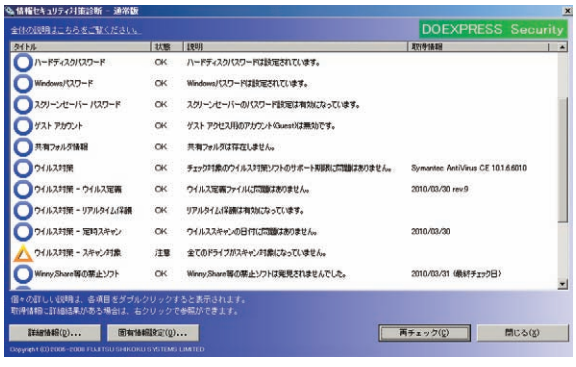
Security maintenance through it infrastructure standard operation service

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. 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 (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, the information security managers of each division can monitor the diagnostic results of all PCs to improve the effectiveness of security measures. This also reduces the on-site workload of implementing security measures.

Information Security Measure Diagnostic Results 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.

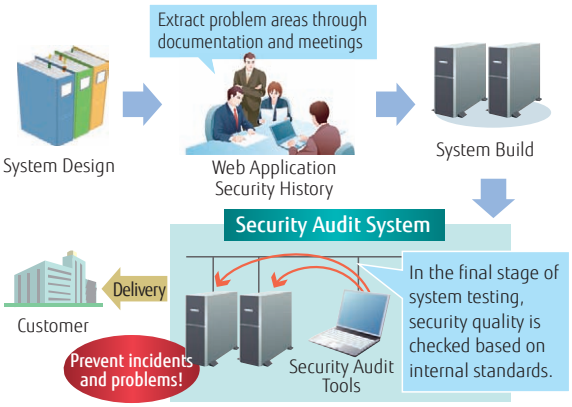
In regards to web applications, because problems are resolved with an upper process, security checks are performed at the design stage.

This ensures that the Internet connection system delivered to customers has a homogeneous security level and prevents security incidents by unauthorized access.

Security incidents due to Fujitsu errors were actually drastically reduced after beginning operation of security audits of customer systems.

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.

Security Audits for Systems delivered to Customers



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 with JASA certifications from the committee bureau and from outside the audited organization.

Monitor and Evaluate Activity

Evaluate information security 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. The SBG security committee carried out the evaluations on each of the units and Group Companies in SBG in 2009 and 2010. 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 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.

Phases from Determining Policy for Metrics Evaluation to Evaluation/Visualization

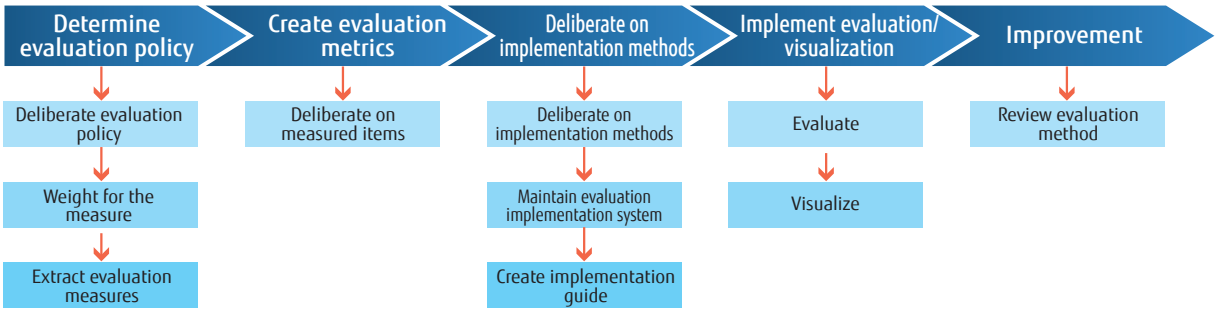
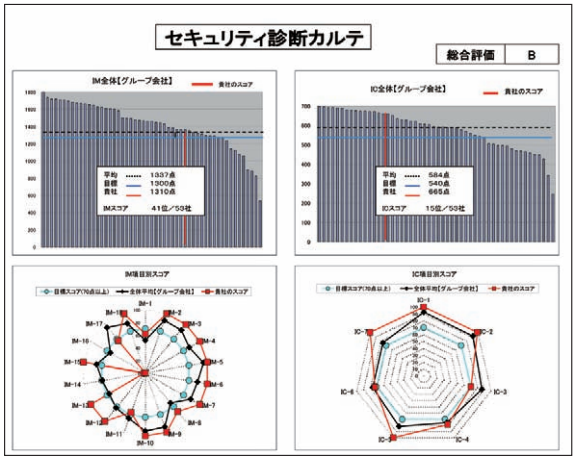


Image of the Security Evaluation Report (Security Diagnostic Chart) in Japan



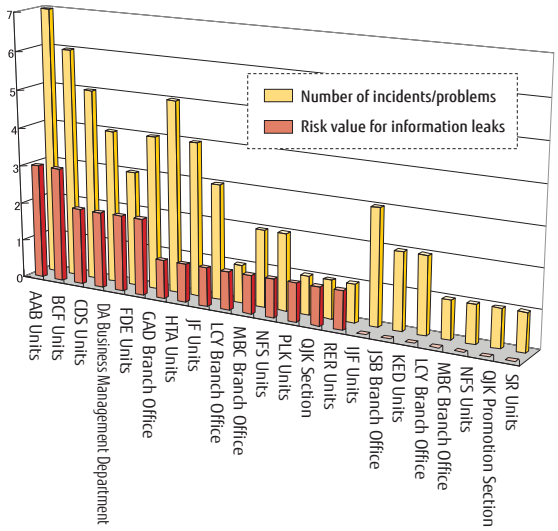
Risk evaluation for incident/problem information leaks

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

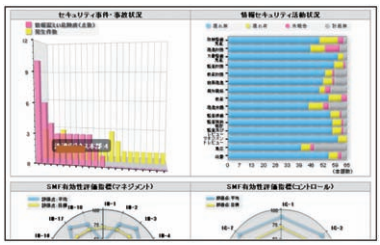


Visualization of Information Security Activities

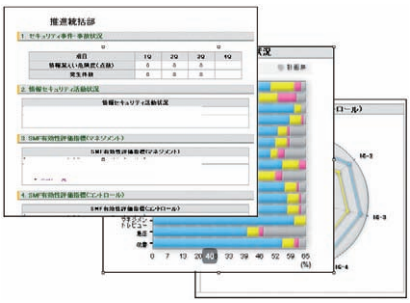
The status of information security activities are measured and evaluated with several evaluation metrics. Furthermore, the evaluation results are presented visually to be understood uniformly. The visualization is presented in layers for the SBG Security Committee Chair, Divisional Managers, and Information 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

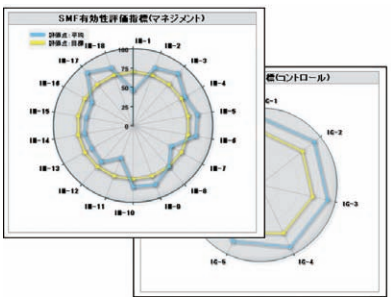
[SBG Security Committee Chair] Layer



[Divisional Manager] Layer



[Information Security Manager] Layer



Product Security

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

Approach to Ensuring Security of Software Products (Improved Development Process)

The problem of security is an issue that requires handling with great care during all stages of designing, implementing, and testing developed products. We have therefore incorporated activities for ensuring security quality into the development process.

(1) At the design stage, a security analysis (vulnerability analysis) is performed.
(2) At the implementation stage, verification is performed at the source code level using a tool and digital signature is employed as necessary.
(3) At the test stage, the handling of vulnerabilities that were found during the design is checked, and security verification is performed using a tool.
(4) Furthermore, by acquiring ISO/IEC 15408 international standard certification, the qualities are evaluated independently.

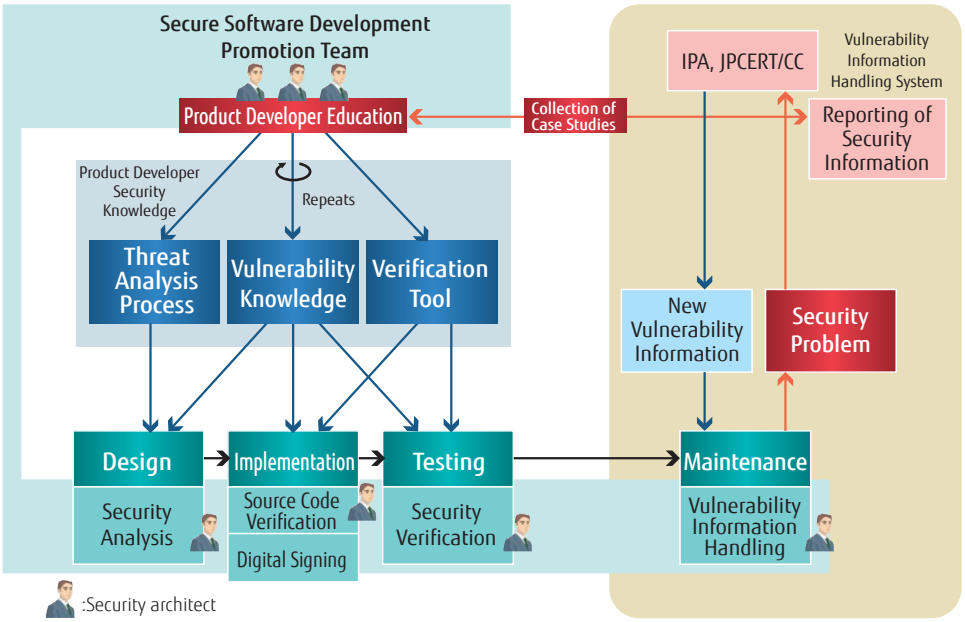
However, since high-quality security cannot be ensured by procedures alone, we also continuously engage in activities to improve the skills of our developers. Developer skill training is conducted through cooperation between the secure software development promotion team and the security architect.

Furthermore, the handling of security incidents after the product has shipped is also important, and a system for handling vulnerability information has been built to handle new vulnerability information discovered even after a product has shipped (providing security patches and publishing product security information) that also works in cooperation with external bodies such as IPA* and JPCERT/CC.

Security problems that are discovered in the maintenance stage are reflected in the product development stage as knowledge and experience, and are collected into case studies for preventing the problems from occurring again that are used for educating product developers.

* Information-technology Promotion Agency, Japan

Software Product Development Process



Approach to Improving Product Security Quality (Skill Training for Developers)

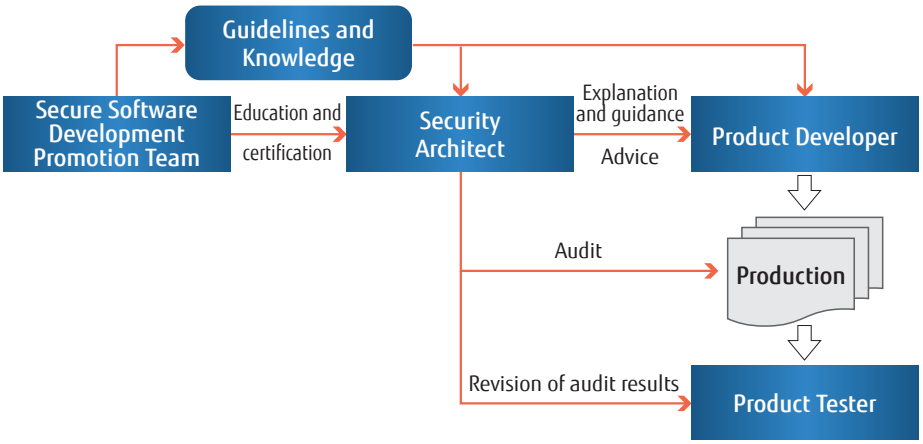
Simply incorporating security response activities into the development process does not improve security quality. Product developers need to improve their skill regarding security. Although Fujitsu engages in activities to improve the skills of our product developers, we have also created a "Security Architect System" for improving product quality to another level. The Security Architect System creates a person who has detailed knowledge of

security in the product development teams with the aim of that person leading secure product development.

A security architect is a developer who has been nominated by the product development division and trained and certified by the secure software development promotion team, with 281 security architects currently certified. Even after certification, training seminars are held periodically to engage in activities to improve skills.

The security architect acts as an advisor for developers during product development, and audits and checks the results of development. When handling vulnerability information during the maintenance stage, the security architect compiles the information for the development division. The security architect also trains developers as necessary in cooperation with the secure software development promotion team. In this way, activities for improving software security quality are carried out focusing on the security architect.

Security Architect System



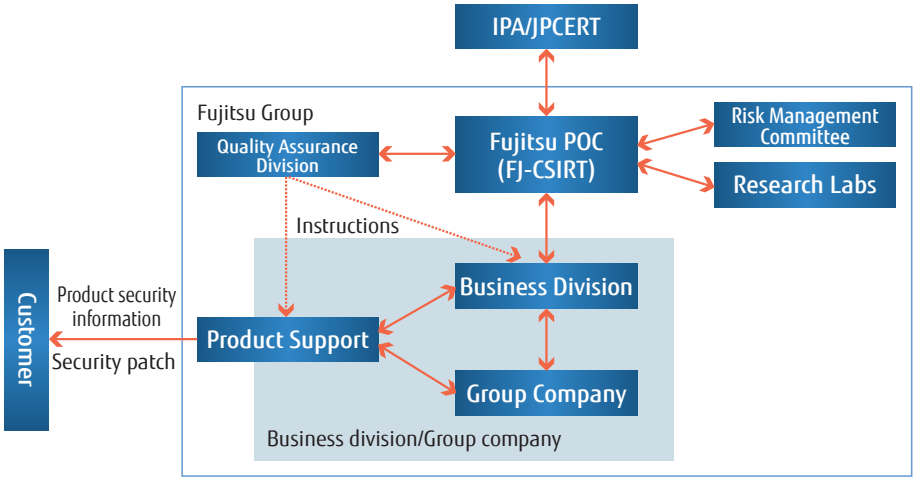
System for Ensuring the Security of Shipped Products (Security Response System Structure)

In order to handle security incidents after a product ships, a system is established that rapidly responds to newly discovered vulnerability information by disclosing product security information and providing security patches to customers.

This system is structured centering on a Fujitsu POC (Point Of Contact). Although the Fujitsu POC is within the secure software development promotion team and works together with the development division, they are a mobile organization that also works together with quality assurance division, risk management committee, and research labs.

Under this organization, vulnerability information handling (investigating the impact of vulnerability information) starts triggered by new vulnerability information, discovery of vulnerabilities in Fujitsu products, or product security problems, and instructions are given to the product support division for publishing product security information and providing security patches as necessary.

Security Incident Handling



Approach of Fujitsu Social Science Laboratory

Fujitsu Social Science Laboratory Limited (Fujitsu SSL) is expanding business in both "SI (outsourced development)" and "solutions." In "solutions," we are providing a variety of customers with a wide range of solutions using the "Powered Solution", our suite of system solutions. In the field of security, Fujitsu SSL is providing a variety of solutions that employ cutting edge security technology for delivering a safe and secure business environment. Fujitsu SSL has also integrated its ISMS, QMS, and PMS into the Integrated Management System (IMS*1) in order to improve corporate value and performance both within our company and for our customers.

Fujitsu SSL was also the first software service company in Japan to be accredited with the information security rating "A_{is}" in 2008, which has been upgraded to "A^{+}_{is}" in 2011.

*1: IMS: Integrated Management System

Goals and Measures of Management System Integration

Integration of management systems was pursued with the goal of increasing management efficiency by establishing, maintaining, and optimizing quality management, information security management, and personal information protection management. To achieve this goal, the following measures were taken:

(1) Unifying policies and targets
Unifying management system policies and targets in order to build and operate an efficient integrated management system without any inconsistencies between management systems.

(2) Unifying promotion division
Merging the promotion divisions into one in order to maintain smooth operation.

(3) Standardizing certification bodies
Standardizing the two certification bodies (of ISMS and QMS) into a single IMS certification body in order to reduce certification and scheduling adjustment costs.
Combining the certification audit that had been conducted independently into a single audit to reduce the audit workload.

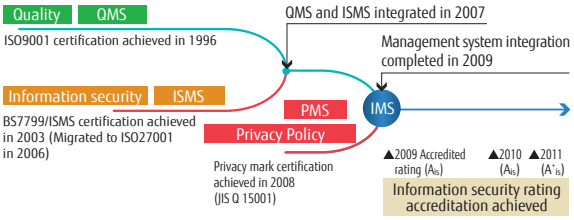
(4) Integrating internal auditing
Building and operating a system that can educate integrated auditors and carrying out a one-stop internal audit that had previously been carried out separately by the 166 QMS internal auditors, 12 ISMS internal auditors, and 44 PMS internal auditors.

Customers are thus provided with safe and secure services that incorporate the knowledge gained through these internal company operations and practices.

Flow of Management System Integration

To improve management efficiency, the scope of management activities were expanded from divisional activities to company-wide activities in 2007. Management system integration was finally completed in 2009, when PMS and the privacy policy were integrated into the IMS.

Flow of Management System Integration

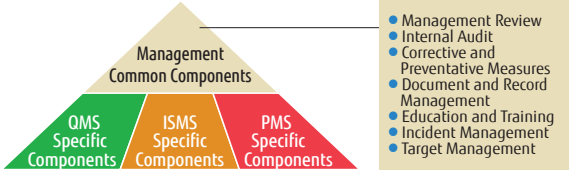


Integrated Management System Structure

The integrated management system was constructed with the common and specific components of the management system as specified in the PAS99 (Publicly Available Specification) requirement specifications for integrated management systems developed by BSI*2 in the UK.

*2: BSI: British Standards Institution

Integrated Management System Structure



Information Security Measures

Information security measures currently implemented company-wide are as follows:

Measure to prevent mis-sending email	Fujitsu SSL's "SHieldMailChecker" enables setting of e-mail security policy levels that take into account our organization and business security requirements.
Inventorying IT equipment	Fujitsu SSL's "KiKiManage" can inventory company-issued devices such as USB and mobile phones on a regular basis. It also allows remote locking of mobile phones, so that they cannot be used in the event they are lost or stolen.
Checking the implementation status of security measures	Fujitsu SSL's "SafeManager" prevents software-related security incidents by checking security measures implemented on PCs as well as vulnerabilities, evaluating the status of such measures, and providing feedback to administrators.
Checking IMS security operations	Fujitsu SSL's "IMS daily operation check tool" has been deployed throughout the company to promote IMS operation by facilitating a self-check of the implementation status of information security measures.
Managing PCs taken out of the office	Fujitsu SSL's "Mobile PC check-out tool" has been deployed throughout the company to manage PCs taken out of the office, ensuring the security level of mobile PCs and reducing the workload in each division in managing mobile PCs.
Security education management	We have made it possible to check the status of individuals and divisions receiving training by providing a function for browsing the history of IMS-related education to prevent people from missing their training requirements.

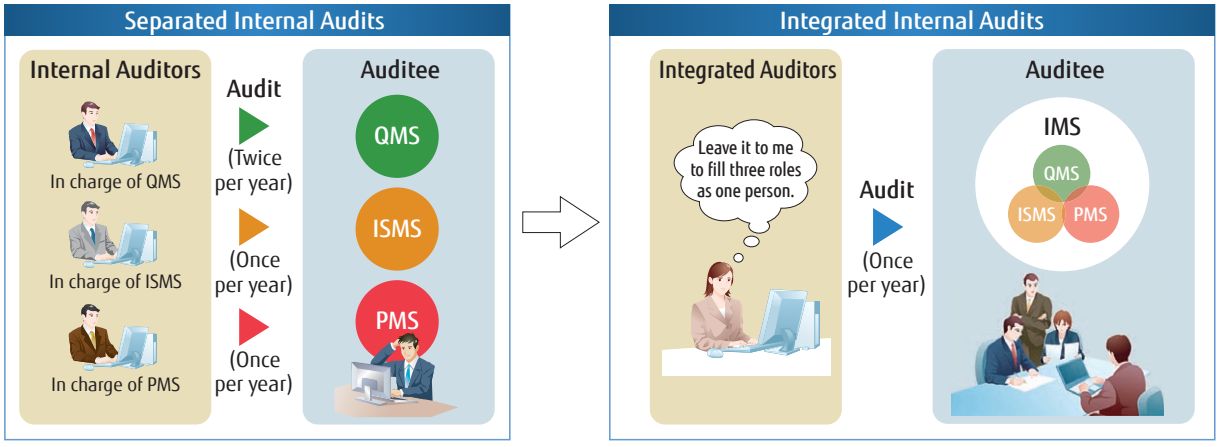
Internal Auditing and Integrated Auditors

In order to achieve integrated internal auditing, 102 integrated auditors (among whom 21 hold JASA*3 auditor qualifications) were trained over a 4 year period to perform IMS (QMS, ISMS, and PMS) internal auditing simultaneously. This reduces the workload of people being audited and reduce audit costs within the company.

The auditing team consists of auditors from different divisions who are not allowed to audit a division that they belong to. Forming this kind of audit team allows the activities of the auditees to be seen from a fresh and unbiased perspective, as well as leading to improvements that are applicable to the division of the auditors themselves. The internal company audits also diagnose vulnerabilities in the internal company network and servers, and to ensure and maintain security from a technical and operational perspective.

*3: JASA: Japan Information Security Audit Association

Revision of the Audit System



Contributions to Society (Activities for Disseminating and Promoting Information Security Auditing)

Following the inauguration of JASA in 2003, we worked to establish, disseminate, and promote information security auditing systems. From 2006, we began holding auditor training as a JASA certified education and training institution, training over 300 auditors. We are continually working to improve, disseminate, and promote information security into the future in order to realize a safe and secure advanced information society.

Approach of Fujitsu America Inc.

The FAI security program provides guidance and policy for IT Security requirements to all Fujitsu America business functions, departments, projects and personnel. This program is led by the FAI IT Security team based in Dallas Texas. It also provides security services to Fujitsu North American Companies (FNAC); FAI, FBR, FCAI, FCPA, FFNA and FFCA, FLA, FMSA, FSA and FSWP, and PSI .

The services include but are not limited to: firewall and proxy management, vulnerability management, security assessments, security configuration reviews, and incident response and forensic investigations.

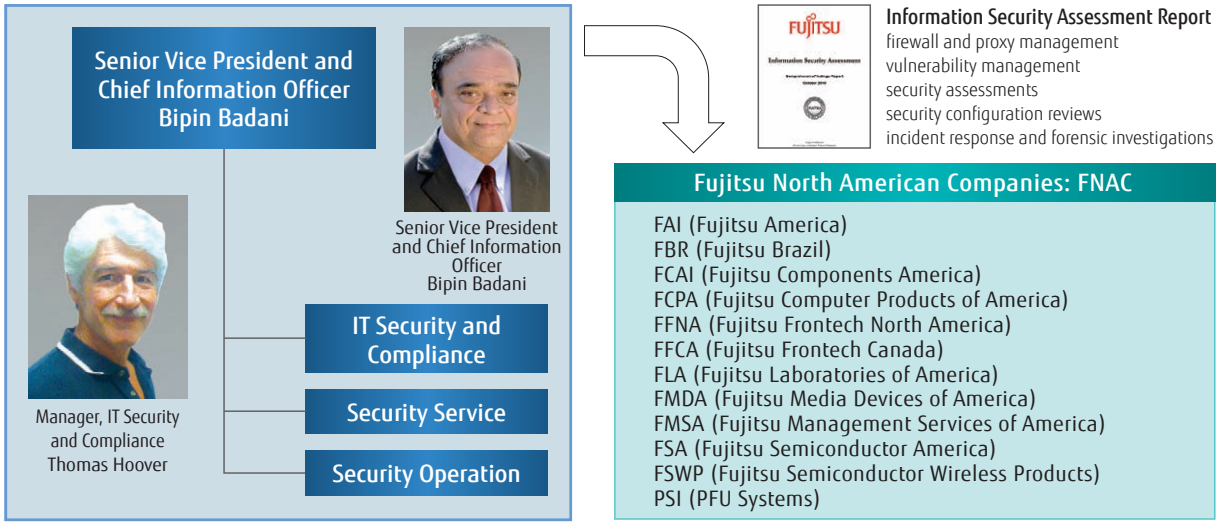
IT Security Organization

The FAI IT Security team has implemented a program to assess its internal compliance to the requirements of the Global Information Security Policy. The Lumension Risk Manager (LRM) application is utilized to collect and record information relating to each business units security compliance posture. This tool is utilized to survey internal business interests to identify key Business Interests then link them to security controls. The security controls are then assessed and scored on compliance to the requirements of the IT Security Policy. This provides a composite risk score for each Business Unit's security posture. Recommendations are made on how controls can be enhanced to provide even stronger security protection.

The Fujitsu Global Information Security Controls Framework that was published on April 28, 2010 and subsequently mapped into LRM's Unified Control Framework.

Having our security standard mapped into the tool provides the foundation for assessing the security posture FAI. It also provides the ability to map our security program against other security standards such as COSO and COBIT, to name a few.

IT Security Organization



In 2010, the FAI IT Security Team conducted annual IT assessments for FNC, FCAI, FLA, FSA, and FCPA. All of which received a satisfactorily grade meet the requirements of the security program.

FAI also conducts third party assessments of its Information Security program to meet client regulatory and industry obligations. The two primary assessments are listed below.

SAS70

Fujitsu America Inc. participates in annual SAS70 Type II*1 audit performs by the auditing company (KPMG) to independently verify that FAI have the requisite levels of control and security to meet the user organizations' audit requirements. These assessments are conducted for the three primary data centers in Dallas, Sunnyvale and Columbus.

During the SAS70 audit the auditor performs independent and complete reviews of the design and operating effectiveness of IT controls in respect of the required standards. Also the auditor provides assurance that the requirements of these standards have been met.

The final SAS70 assessments resulted in unqualified opinions*2 of the security programs in these locations. This information is provided to the client to demonstrate the effectiveness of the security program.

PCI DSS

All FAI locations that host client applications that store, process or transmit Card Holder Data are required to maintain their PCI Report of Compliance (RoC).

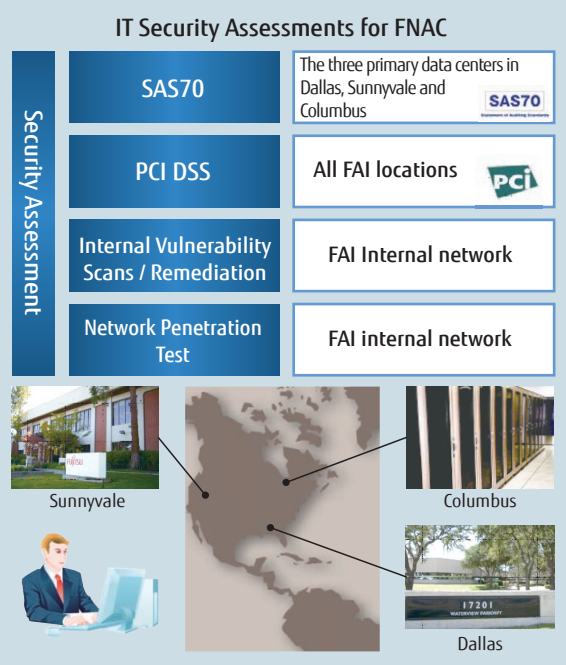
The annual certification process is designated by the Payment Card Industry (PCI) Security Standards Council. FAI undergoes rigorous annual assessment certification performs by PCI Qualified Security Assessor (QSA) in accordance to PCI DSS*3 standards and requirements. FAI systems are also required to be scanned by PCI Approved Scanning Vendor (ASV) on on-going basis - to validate adherence to certain DSS requirements by performing vulnerability scans of Internet facing environments of our PCI clients.

*1: SAS70 Type II: This is an auditing standard for evaluating the effectiveness of internal controls regarding outsourced business as established by the American Institute of Certified Practicing Accountants (AICPA). Type II is used with the aim of evaluating the effectiveness of internal controls in outsourced business over a fixed period.

*2: Unqualified opinions: An opinion stating that the result of an audit by an auditor is that the financial statement was created appropriately.

*3: PCI DSS: A global security standard in the credit industry established by the 5 major international card brands for evaluating the safe management of credit card information and transaction information.

IT Security Assessments



Vulnerability Management

FAI has implemented a vulnerability management program that requires a vulnerability assessment of all new servers that will be migrated to the production network. The scan results are validate for acceptable levels of risk and no server is introduced into the production network until his risk vulnerabilities have completed remediation. Ongoing scans of existing servers are conducted throughout the year to identify new vulnerabilities that are present on the network.

Information Security Operations

Security Operations at FAI consists of three distinct functions:

(1) Information Security – performs technical duties such as vulnerability management, investigations, reporting, id provisioning, Change Control support and incident response.

(2) Security Infrastructure – responsible for firewall, proxy & IDS management

(3) MSSP – supports security solutions for customers. Current services include IDS support.

The Security Operations Team also conducts quarterly Wireless Scans of the data center campuses to analyze and detect wireless network threats.

This identifies any rogue wireless access point that could provide an entry point to our secure network.

Research and Development of Security Technology for Supporting Safe Lifestyles

As we welcome in the era of cloud computing, there is demand to be able to use cloud services safely anywhere and anytime using PCs and mobile devices such as mobile phones. At Fujitsu Laboratories, leading edge technical research and development has been progressing for realizing this security.

Approach to Security Technology at Fujitsu Laboratories

Fujitsu Laboratories is conducting research and development into leading edge technology across a wide range of topics including system security for realizing information security governance in corporations and for realizing a safe Internet society, encryption and masking of digital information which is foundational technology for supporting security, biometric authentication for appropriately authenticating people, and paper encryption for protecting printed information.

In the field of biometric authentication that authenticates the identity of a person based on physical characteristics, in particular, Fujitsu Laboratories was the first in the world to develop technology for securely authenticating without contact the vein patterns in the palms of people's hands. We are also developing compact, high precision fingerprint authentication technology for personal computers.

In term of system security, Fujitsu Laboratories is progressing with technological development for constructing and diagnosing secure systems with few vulnerabilities and with research and development into new security solutions in the cloud environment.

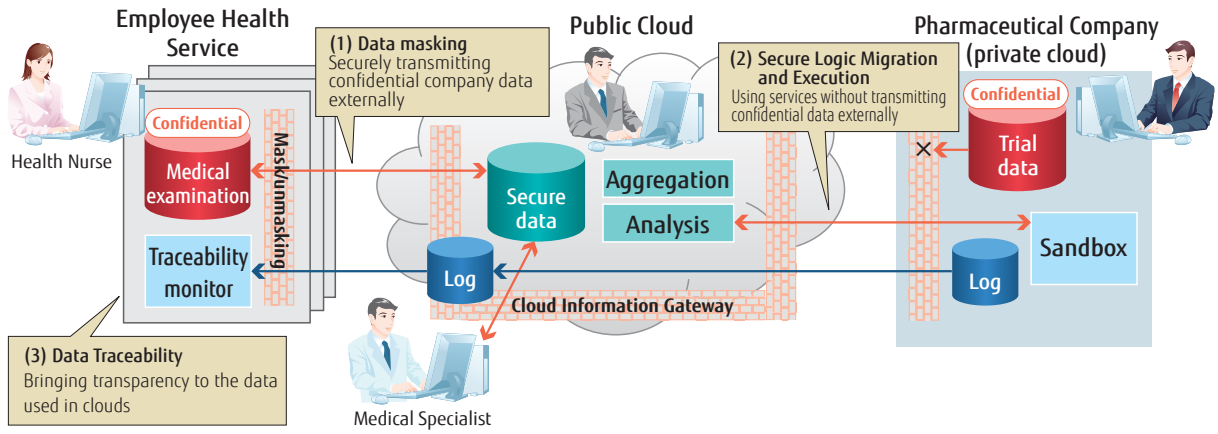
Development of Inter-Cloud Data Security Technology

As usage of the cloud becomes more diversified, new requirements are expected to grow such as safely utilizing personal information in cross-industry collaboration for new product developments. Conventional encryption technology alone is not sufficient for securely entrusting confidential data to be processed and analyzed in a cloud operated by a third party. We have therefore developed a new data loss prevention technology in the cloud era that focuses on the data that is transferred between clouds to secure personal and confidential information and make it possible to visualize the usage of that data. (Press release from 19th Oct. 2010: http://www.fujitsu.com/global/news/pr/archives/month/2010/20101019-01.html)

(1) Data masking: Although there is resistance to provide confidential information such as medical examination results in a company to the cloud, it may lead to new uses of information by sharing and processing information within the industry by specialists. Data masking is a technology that conceals confidential parts contained within data to make the data itself safe when communicating with an external cloud, and then unmasks the result of this processing. This not only applies to personal information that can identify individuals, but also to confidential information such as the number of infections in tabular form by region and month. The tabular data sent to the cloud is scrambled by random values so that even cloud administrators cannot know the original values, but cloud services can aggregate the values without using the unscrambling key. Furthermore, each user can obtain different detail levels of the aggregated result, such as prefecture level, city level, town level, etc., using different decryption keys.

(2) Secure Logic Migration and Execution: For confidential information that cannot be taken outside of the company, the applications and data in the cloud can be moved into a closed private cloud and executed

Inter-Cloud Data Security



securely in special execution environment (sandbox).

(3) Data Traceability: This makes it possible to track data entering and leaving the cloud, check that there are no unauthorized leaks of confidential information by investigating the characteristics of text, and bring transparency to data flows and usage spanning multiple clouds. This reduces user concerns such as about what has happened to data entrusted to the cloud.

These functions are deployed in information gateway at both company and cloud, and make it possible to securely transfer confidential information between clouds without any special awareness by users or application developers. In the cloud era, this is expected to become essential technology for utilizing confidential and personal information in clouds such as open government and cooperative works such as new product development by multiple organizations.

Technology for Integrity Assurance of Digital Video Clip

With widespread adoption of technologies such as surveillance cameras in recent years, the use of recorded video as evidence has been growing.

While digital storage of video data is convenient, the data is easy to manipulate. This has led to a growing demand for proof that video images have not been tampered with when they are used as evidence (also referred to as digital authenticity of video evidence). Furthermore, when a long duration of video is used as reference material, it is necessary in terms of both convenience and protecting privacy to disclose only part of the video by cutting out video that includes ordinary people and create an excerpt of only the commission of the crime. In this kind of situation, there is demand for determining the integrity of the disclosed part of the video.

In order to address these needs, we have developed the world's first technology for integrity assurance of video that offers evidentiary value and probative force that can stand up in court even for partial clips of recorded video.

(1) Integrity Assurance of Recorded Video

We have developed a technology that adds digital signatures (similar to a manual signature on paper) for verifying authenticity to video data.

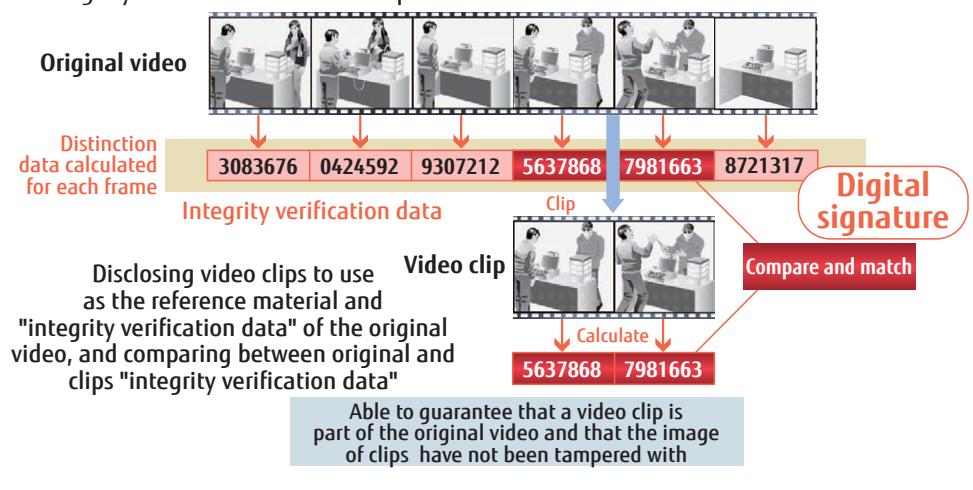
The method, which was developed independently by Fujitsu Laboratories, strictly verifies the integrity of video data by calculating distinction data (information confirming that if there have been any tampering) for the minimum unit of video (such as single frames of video) using a cryptographically secure hash function and managing the video together with a digital signature of the distinction data (integrity verification data).

(2) Integrity assurance even of video clips

Because the distinction data for each frame of video is managed as "integrity verification data", the integrity can be verified not only for whole video but also for clips of it. More specifically, integrity assurance of video clips is achieved by following procedures: i) disclosing clips and "integrity verification data" of original video, ii) calculating the integrity verification data of each frame from clips, iii) and, complete matching between verification data of original and clips. The video clips can be used for strict evidence because it can be confirmed that the clips are parts of the original video with this technology, for example, only a scene of a crime in surveillance video is clipped.

This technology can be applied to following situations that require strict integrity verification of video data such as surveillance cameras for preventing crime, drive recorders for preventing accidents, and video evidence of surgeries for malpractice suit. And this technology can be utilized in forensic fields that require preservation of evidence and audit trail by video data.

Integrity Assurance of Video Clips



Approach 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 in Japan.

Contractual Measures

In China and the main five companies* (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.

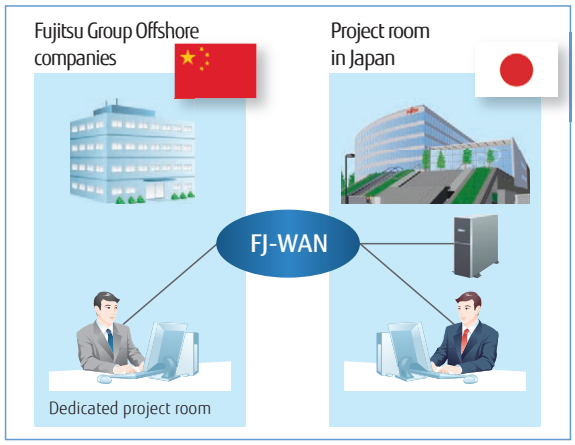
* Beijing Fujitsu, Fujitsu Xian, Fujian Fujitsu, Nanjing Fujitsu, and Jiangsu Fujitsu.

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.

Visualization of development environment



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.

On-site Security Surveillance

Depending on the project, security monitoring, periodic checks, and data deletion confirmation are carried out as necessary at the start, during implementation, and at the end. There are also cases where the customers themselves ask for on-site inspections and audits of offshore companies if desired.

Awareness activities and the Risk Management Committee

The Information Security Handbook, a Chinese-language summary of the Information Management Items for Outsourcers, and the 2010 Information Security Education self-training 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 on-site 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

Our offshore companies have acquired ISMS certification based on the Information Security Management System international standard (ISO/EIC 27001). Companies that have not yet been accredited are progressing with the procedures for acquiring certification.

Understanding the information security status at offshore outsourcers

In 2010, Fujitsu carried out a survey into the status of information security measures at offshore outsourcers. Based on the information in the responses that were received, vulnerabilities where divided into outsourcing vendor-specific and vendor-common vulnerabilities, and measures were implemented to enhance information security in the offshore businesses.

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 corporate policy.

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

Although there are many types of information security accidents at customers, including information leaks to the Internet by file sharing software, loss and theft due to carelessness, and mis-sending of emails and faxes, in all of these cases there is a trend of reduced incidence with the introduction and thorough implementation of countermeasures.

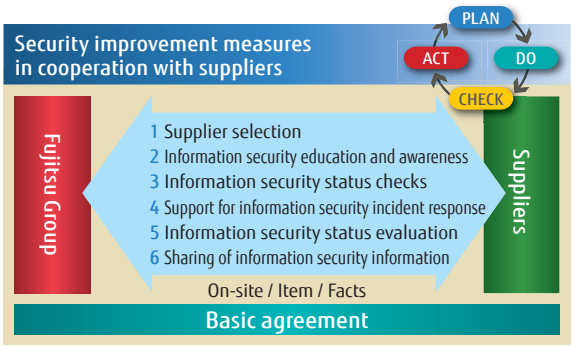
In fiscal year 2010, existing measures were enhanced by new measures directed more closely to on-site activities:

(1) Internal information security enhancements at supplier companies (Information security education material and on-site training seminars for supplier companies)

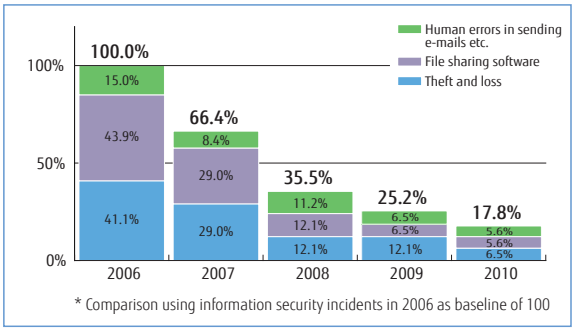
(2) Enhanced selection, management, and oversight of suppliers who are entrusted with personal information under the act on the protection of personal information

(3) Enhanced information security governance within the Fujitsu Group

Security improvement measures in cooperation with suppliers



Trends in information security accidents



* Comparison using information security incidents in 2006 as baseline of 100

Supplier selection

Selection of new suppliers involves evaluation of candidate firm's' 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
  - Professional Awareness of Information Security -
  - About 1400 people / 1300 companies in December, 2010
    Questionnaire results - 98% understood and responded
- Continue holding on-site training seminars for suppliers
  Lecturers continued to be dispatched in 2010 to hold training seminars for supplier employees on request.
  Approx. 70 companies/1,500 employees trained
  Cumulative total: Approx. 130 companies/1,900 employees
- "Management and Oversight of Outsourcing Vendors E-Learning" for Fujitsu employees
  - Approx. 16,000 employees in December 2010
- Provision of information security educational material to supplier companies

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 2010 audit about 140 companies (about 1100 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

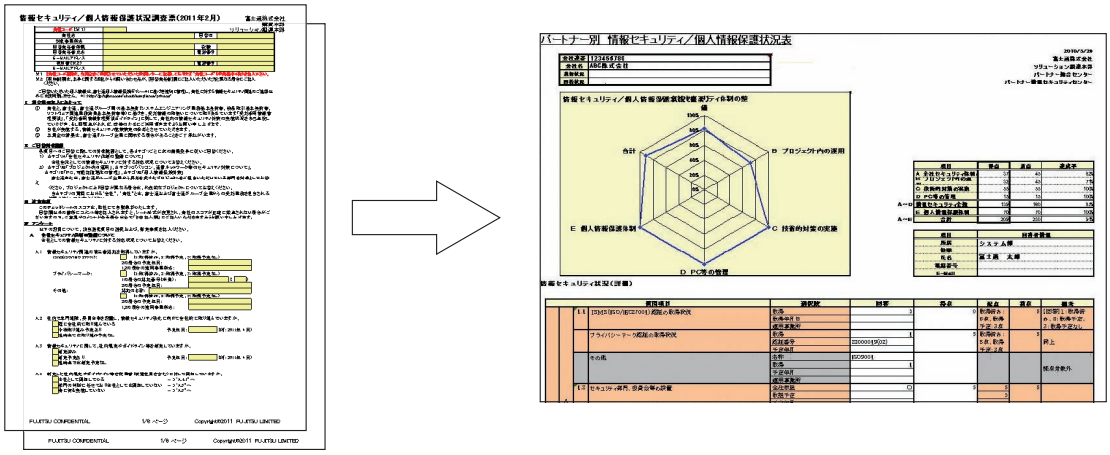
The Fujitsu Group evaluates suppliers' information security status based on status checks, response to information security incidents, etc. In the event of serious incidents without sufficient improvement effected, the Group may halt relationship or suspend new orders, as necessary.

Sharing of information security information

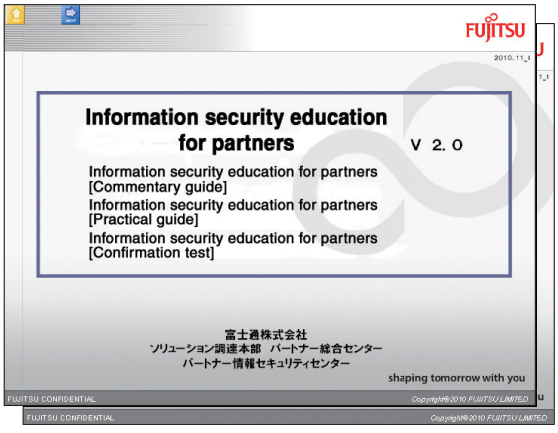
The Fujitsu Group designates information security officers for suppliers, and undertakes timely sharing of the latest security-related information including the Fujitsu Group.

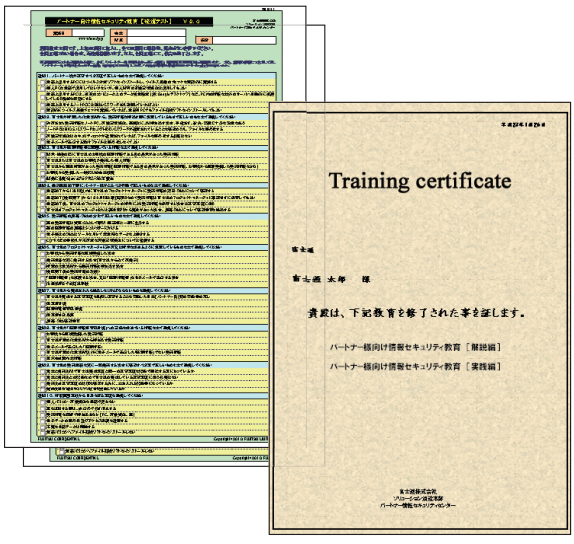
- From April 2009, Information Security Plaza has been published every other month to share the latest information on information security. The Fujitsu Group also provides awareness-building posters to prevent information security incidents.

Supplier information security and personal information protection status survey and evaluation charts in Japan



Information security educational material for suppliers





Fujitsu Information Security Solutions

SafetyValue - Fujitsu Safety and Security Solutions Focusing on the Cloud Era

In recent times, along with growing the business, ensuring the reliability and continuity of business even when faced with security incidents, natural disasters, and new type influenza has become the most important management challenge. Even from the perspectives of internal controls and CSR, it has become essential to establish information security governance as an imperative of corporate governance. Fujitsu is providing the "SafetyValue" safety and security solution that implements integrated risk management in response to these management needs of our customers.

Features of SafetyValue

"Customer Centric" Solution Framework

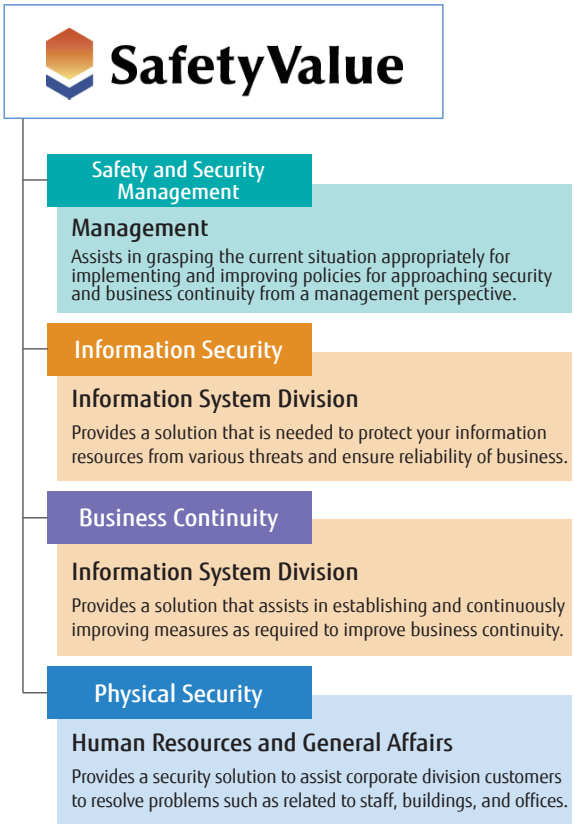
The "SafetyValue" solution framework has been reorganized as a customer-centric solution that matches the roles and responsibilities that customers use in their organizations.

SafetyValue aims for complete transparency to help customers themselves make management decisions by understanding current conditions, support for an advanced IT environment that aims for complete utilization of information resources, and improved user friendliness.

More specifically, SafetyValue consists of the four areas of "safety and security management", "information security", "business continuity", and "physical security" which are associated with the "management", "information system division", and "human resources and general affairs divisions" in the customer's organization. (See the figure on the right for details.)

This document focuses on the area of "information security" that is associated with customer's "information system division", and introduces solutions for reliably resolving the issues facing the customer.

SafetyValue Framework and Description



Information Security

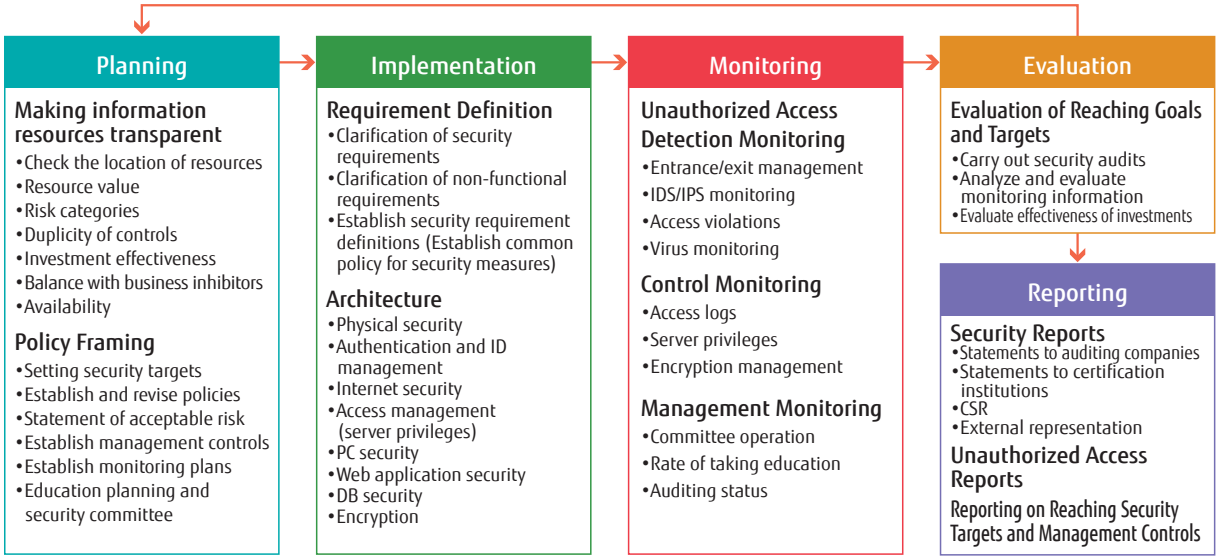
Assistance for Establishing Information Security Governance

Fujitsu has developed and provides services for implementing information security governance in our customers' organizations.

This involves "visualizing" the security risks that face a customer system, creating proposals for the best countermeasures, defining requirements, and architecting designs based on a process established independently by Fujitsu. The operation of customer businesses is also assisted while ensuring security by conducting monitoring using a 24 hour-a-day, 365 days-a-year system. In order to systematically confirm the status of implementation of security measures and the status of adhesion to appropriate security measures in the customers' business, and to evaluate in terms of effectiveness the effects of investment on security measures that are difficult for management to decide, we appropriately propose and assist with analyzing and implementing measures for management problems.

Fujitsu offers powerful assistance for our customers to establish the appropriate corporate governance for the cloud era through consultation based on Fujitsu's abundance of experience and the utilization of high quality services based on our secure infrastructure.

Fujitsu Information Security Governance Establishment Process



Fujitsu SafetyValue Solution Offerings

Information security measures implemented based on information security governance need to be investigated after considering the effectiveness and efficiency of the security measures. Fujitsu assists in the establishment of information security governance that can be implemented based on the optimal solutions based on the cost effectiveness as required when the customer is investing in corporate strategies.

Fujitsu provides 11 solutions for realizing the establishment of information security governance.

For example, security visibility consulting advances visibility from the four perspectives of security management, security controls, security risks, and security traceability, and provides the sequence of operations from checking problems to defining operational areas, defining requirements, designing indicators, and verification using Fujitsu custom procedures. This makes it possible to construct a dashboard revealing the status of the customers' information resources and risks in real time, and makes it possible to "visualize" the current state of customer security measures.

In this way, Fujitsu both strongly protects customer information resources and improves convenience of IT to assist with information security measures by providing customers with solutions that handle a variety of security risks, including information leak accidents, internal crime, and attacks from the Internet.

Solutions for 11 Areas of Information Security

Information Security	Details are here ▶ http://jp.fujitsu.com/solutions/safety/secure/
Security control	Supports the realization of "information security governance" in the organization based on continuous security measures from the perspective of overall company activities including IT
Information Security Visibility	Supports the establishment of information security governance and offers information security visibility and monitoring
Security Consulting	Offers integrated assistance for establishing information security management in an organization from establishing information security basic policies to settling on management
Unauthorized Access Countermeasures	Realizes the security cycle including auditing 24 hours per day 365 days per year as well as planning, establishing measures, implementing measures, auditing, and monitoring.
Information Leak Countermeasures	Provides functions for creating and implementing information management policies and encryption functions for protecting personal information and prevent information leaks
Virus Countermeasures	Provides services such as for assisting with defense, disinfection, monitoring, and recovery as measures for preventing viruses
Carry-in PC Countermeasures	Delivers an environment that protects the customer system from threats such as confidential information leaks and virus damage caused by PCs that have been brought into the office
E-mail Security	Total assistance for security countermeasures for safely using electronic mail, including measures against mis-sending, antivirus measures, and preservation of audit trails
Authentication and ID Management	Assists with authentication, which is the foundation of information security, and operational management of user information through a directory product that offers integrated management of biometric authentication, digital certificates, and user account information.
Printing Security	Provides a group of products for managing and protecting printed documents and functions for personal authentication when printing, and delivers measures for preventing information leaks from printed matter
PCI DSS	Provides security measuring for helping to comply with PCI DSS (Payment Card Industry Data Security Standard)

Third Party Evaluation/Certification

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

PrivacyMark Certification

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.

*: The organization name was changed from 1st April 2011

FUJITSU LIMITED
FUJITSU ADVANCED ENGINEERING 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 LTD.
OKINAWA FUJITSU SYSTEMS ENGINEERING LIMITED
FUJITSU KAGOSHIMA INFORNET LTD.
FUJITSU KANSAI SYSTEMS LIMITED
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 LIMITED
FUJITSU SOFTWARE TECHNOLOGIES LIMITED
FUJITSU CHUGOKU SYSTEMS LIMITED
FUJITSU CHUBU SYSTEMS LIMITED
TOTALIZATOR ENGINEERING LIMITED
FUJITSU TRAVELANCE LTD.
FUJITSU TOHOKU SYSTEMS LTD.
TOYAMA FUJITSU LIMITED
FUJITSU NAGANO SYSTEMS ENGINEERING LIMITED
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 HOKKAIDO 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 that have 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 KANSAI-CHUBU NET-TECH 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 LIMITED
FUJITSU RESEARCH INSTITUTE
FUJITSU CHUBU SYSTEMS LIMITED
FUJITSU DEFENSE SYSTEMS ENGINEERING LIMITED
FUJITSU TOHOKU SYSTEMS LTD.
TOYAMA FUJITSU LIMITED
FUJITSU NAGANO SYSTEMS ENGINEERING LIMITED
NIFTY CORPORATION
FUJITSU NETWORK 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 LTD.

Information Security Rating Certification

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.

Company Name	Rating Scope	Rating Mark
FUJITSU LIMITED	Tatebayashi System Center	AAA_{is}
	Akashi System Center	AA^{+}_{is}
FUJITSU FIP CORPORATION	Yokohama Data Center	AAA_{is}
	Chubu Data Center	AA^{+}_{is}
	Kyushu Data Center	AA^{+}_{is}
FUJITSU FSAS INC.	Tokyo LCM Service Center	AA^{-}_{is}
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED	Software Service Department	A^{+}_{is}
PFU LIMITED	Information security rating for product business	A^{+}_{is}
	Information security rating for solution and service business	A^{+}_{is}

IT Security Evaluation Certification

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
- 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)

ISMS Auditors

Following number of employees at Fujitsu and group companies are qualified as ISMS auditors.
<qualified ISMS auditor number: 156>

JASA Auditors

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."

In Fujitsu and group companies, qualified personnel participate in internal audits and information security audits requested by customers. Following number of employees at Fujitsu and group companies are qualified as JASA auditors.
<qualified JASA auditor number: 126>

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/