FUJITSU

Fujitsu Group Information Security Report 2012

rity Report 2012
Information Security Report
Informa
Information Security Report 2012
Information Security Report 2012
Information Security Report 2012
Information
Information Security Report 2012
Information Security Report 2012
Information Security Report 2012
mation Security Report 2

shaping tomorrow with you

CONTENTS

Report Summary

Target Period and Scope of the Report

This report covers the period up to March 2012, and focuses on efforts in information security by the Fujitsu Group.

Report publication date

This report was published in August 2012.

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. Although this progress has created a global-scale network community that knows no bounds and has changed business, changed lifestyles, and greatly changed society, the use of ICT is currently limited to new generations. With the spread of smart devices and the cloud, we are attempting to realize an age where the amenity of computers and networks can be enjoyed without an awareness of them, in other words, a human-centric ICT society where humans are the main actor. As a company that supports this kind of ICT infrastructure, the Fujitsu Group is contributing to building a network society where anyone can live with equal comfort and security, and is aiming to realize a rich intelligent society that is human-friendly by continually pursuing the possibility of human-centric ICT and continuously creating new value.

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.

More specifically, we are striving to promote information security as defined by the "Fujitsu Group Information Security Policy" and are pursuing compliance with maintaining confidentiality from among the range of behavior indicated in the "FUJITSU Way" that should be adhered to by staff. 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 2012" describes what the Fujitsu Group is doing for information security.

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

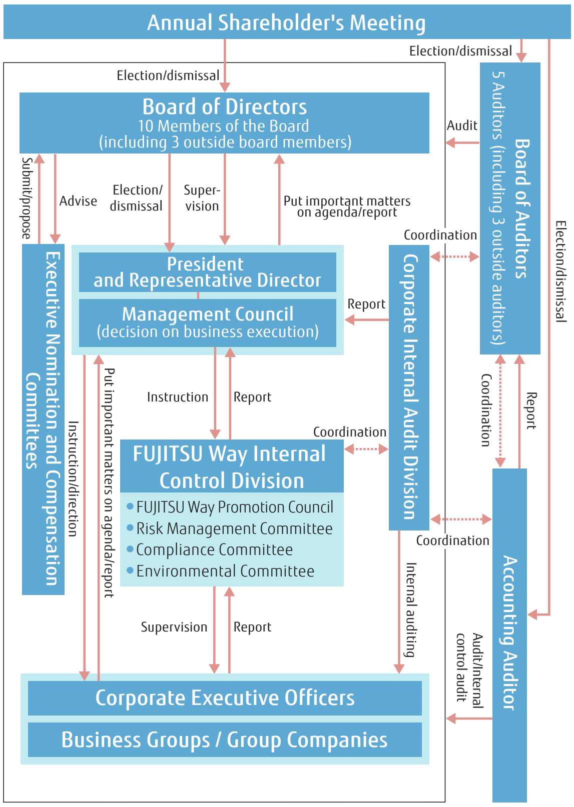
Corporate Governance

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.

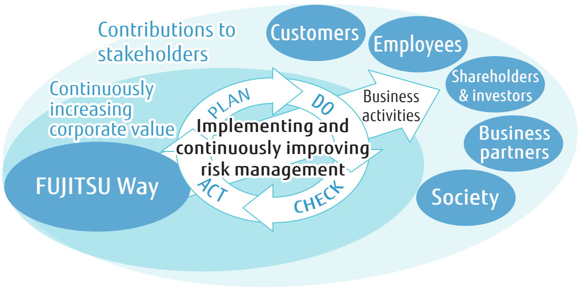
Corporate Governance Framework


Annual Shareholder's Meeting
Election/dismissal
Election/dismissal
Board of Directors
10 Members of the Board
(including 3 outside board members)
Audit
Board of Auditors
5 Auditors (including 3 outside auditors)
Submit/propose
Advise
Election/dismissal
Super-vision
Put important matters on agenda/report
Coordination
Election/dismissal
President and Representative Director
Management Council
(decision on business execution)
Report
Executive Nomination and Compensation Committees
Instruction/direction
Put important matters on agenda/report
Instruction
Report
Coordination
Corporate Internal Audit Division
Coordination
Report
FUJITSU Way Internal Control Division
FUJITSU Way Promotion Council
Risk Management Committee
Compliance Committee
Environmental Committee
Coordination
Accounting Auditor
Supervision
Report
Internal auditing
Audit/Internal control audit
Corporate Executive Officers
Business Groups / Group Companies

Risk Management

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, is promoting activities to prevent and variety of risks and to minimize the impact in the event they occur, and is committed to the continuous implementation and improvement of risk management throughout the group.

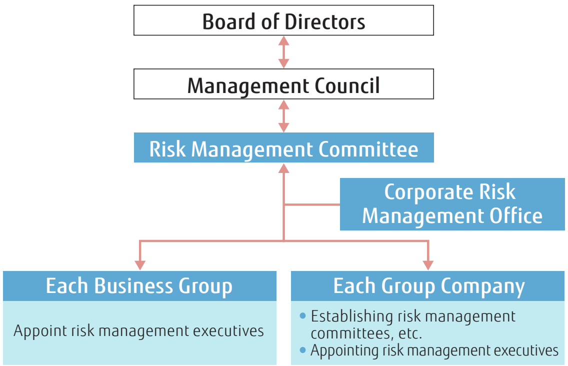
Implementing and continuously improving risk management


Contributions to stakeholders
Customers
Employees
Shareholders & investors
Business partners
Society
Continuously increasing corporate value
Business activities
PLAN
DO
CHECK
ACT
Implementing and continuously improving risk management
FUJITSU Way

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


Board of Directors
Management Council
Risk Management Committee
Corporate Risk Management Office
Each Business Group
Appoint risk management executives
Each Group Company
Establishing risk management committees, etc.
Appointing risk management executives

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

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.

- 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.
- 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.
- 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.

Principles

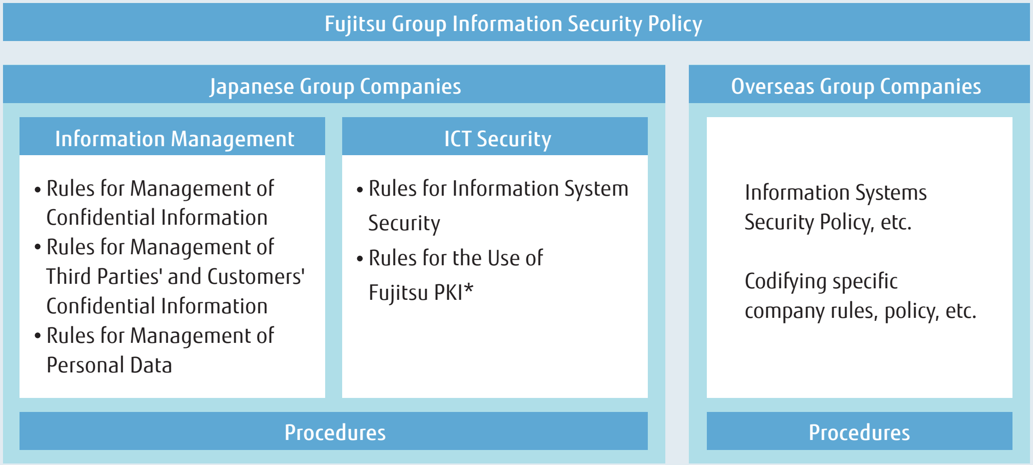
Fujitsu group applies the following principles in meeting the information security.

- 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.
- Organizational structure and responsibility shall be clearly defined to ensure the proper implementation of the information security measures.
- The risks that accompany the handling of information and investments required for the measures shall be taken into consideration to properly implement the information security measures.
- Information security processes shall be organized into Plan, Do, Check and Act phases to keep and enhance the level of information security.
- 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.

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



Fujitsu Group Information Security Policy

Japanese Group Companies

Information Management
- Rules for Management of Confidential Information
- Rules for Management of Third Parties' and Customers' Confidential Information
- Rules for Management of Personal Data

ICT Security
- Rules for Information System Security
- Rules for the Use of Fujitsu PKI*

Procedures

Overseas Group Companies

Information Systems Security Policy, etc.

Codifying specific company rules, policy, etc.

Procedures

* 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 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 presentations 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

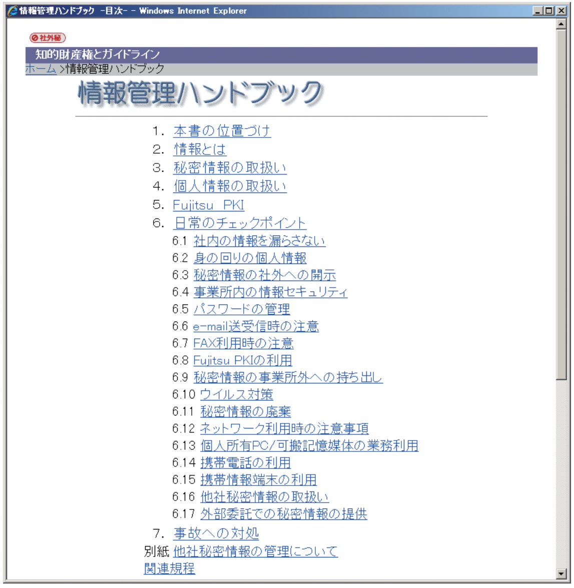
Fujitsu has established the "Personal Data Protection Policy" and "Rules for Management of Personal Data" in compliance with Act on the "Protection of Personal Information". We are also continually strengthening the system for protecting personal information based on these rules such as holding annual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

We acquired company-wide PrivacyMark certification in August 2007 and updated the certification every two years. Japanese group companies are also acquiring PrivacyMark certification individually as necessary, and promoting thorough 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 of any information management questions. In addition, the intranet is used to bring attention to information leaks by introducing some of the many incidents of information leakage from around the world, 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 Management Handbook" Screen in Japan


情報管理ハンドブック -目次- - Windows Internet Explorer
社外秘
知的財産権とガイドライン
ホーム >情報管理ハンドブック

情報管理ハンドブック

1. 本書の位置づけ
2. 情報とは
3. 秘密情報の取扱い
4. 個人情報の取扱い
5. Fujitsu PKI
6. 日常のチェックポイント
   - 6.1 社内の情報を漏らさない
   - 6.2 身の回りの個人情報
   - 6.3 秘密情報の社外への開示
   - 6.4 事業所内の情報セキュリティ
   - 6.5 パスワードの管理
   - 6.6 e-mail送受信時の注意
   - 6.7 FAX利用時の注意
   - 6.8 Fujitsu PKIの利用
   - 6.9 秘密情報の事業所外への持ち出し
   - 6.10 ウイルス対策
   - 6.11 秘密情報の廃棄
   - 6.12 ネットワーク利用時の注意事項
   - 6.13 個人所有PC/可搬記憶媒体の業務利用
   - 6.14 携帯電話の利用
   - 6.15 携帯情報端末の利用
   - 6.16 他社秘密情報の取扱い
   - 6.17 外部委託での秘密情報の提供
7. 事故への対処

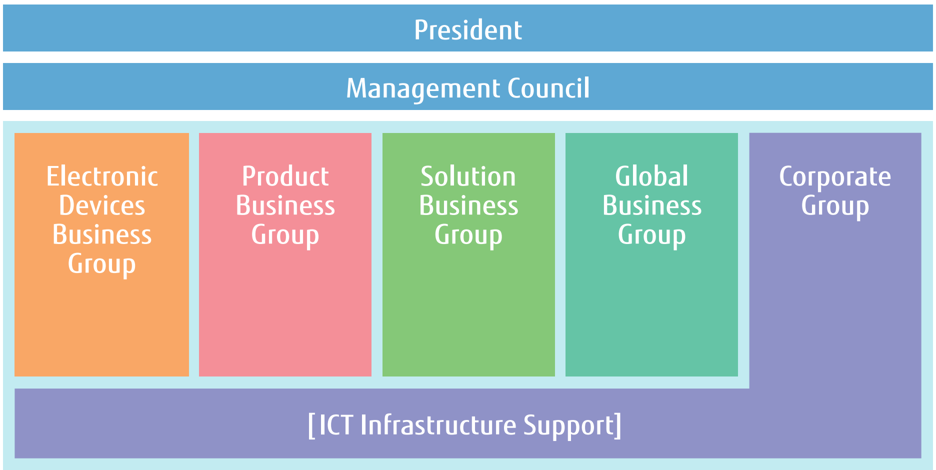
別紙 他社秘密情報の管理について
関連規程

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. 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 ICT 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, including 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 ICT.

Solution Business Group

Applying ICT as the foundation for advanced technologies and high quality products, this division provides business solutions (business optimization), including ICT services, outsourcing services, and network services, to primarily corporate clients.

Product Business Group

This division provides ICT infrastructure products that are paramount 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 ICT 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 ICT (Information and Communication 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 ICT 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 allowing employees to focus on their jobs is important.

In addition, to maintain measures effective against threats changing with ICT 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 "ICT 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 preventing human error when sending e-mails ● Corporate standard PC	● Network control ● E-mail control ● Network service use control

ICT 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 ICT 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 how human errors can be effectively met. Relying only on human attentiveness in using ICT applications will not necessarily prevent information security incidents.

Of course education and awareness programs should be employed to draw attention to information security, but even then information leakage and other incidents will occur beyond the reach of the ICT based measures.

Based on this reality, we focused on the business processes involving client devices and human action, and replaced the measures dependent upon human attentiveness with those embedded in ICT.

■Automated measures for Personal Computers (PCs)

Application of security patches and updates for virus definition files are automated.

■Measures preventing human error when sending e-mails

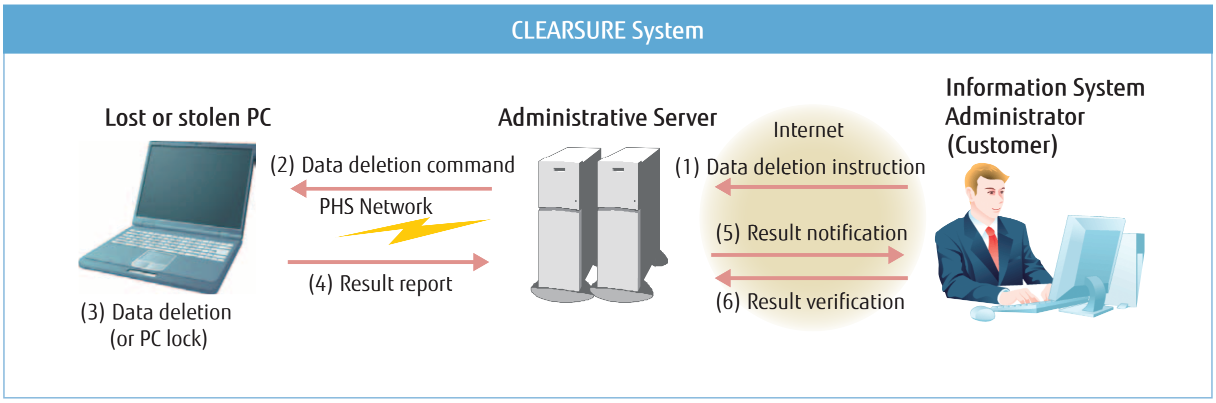
Information leakage will easily result from sending an e-mail to a wrong address. To reduce the risk of this information leakage, e-mail addresses are automatically checked, and the sender is required to reconfirm when it is addressed to external persons.

■Installation of corporate standard PCs

The Fujitsu Group promotes the installation of "corporate standard PCs." Corporate standard PCs are those with identified models and specifications for 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 model selection, installation, and operation become standardized and a reduction in costs and a reliable implementation of security measures are achieved.

Furthermore, as a measure for the loss or theft of laptop PCs, corporate standard laptop PCs have the function of remotely invalidating data. This significantly reduces the possibility of information leakage in case of loss or theft of a PC. This feature is provided to customers as the remote data erasure solution "CLEARSURE."

Measures against laptop PC Loss or Theft



ICT resource management as the basis of IT security

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

The IT Resource Management System maintains the following information.

- Hardware resources: server and PC models, specifications
- Software resources: Software and software versions used on each server and PC
- 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 ICT 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

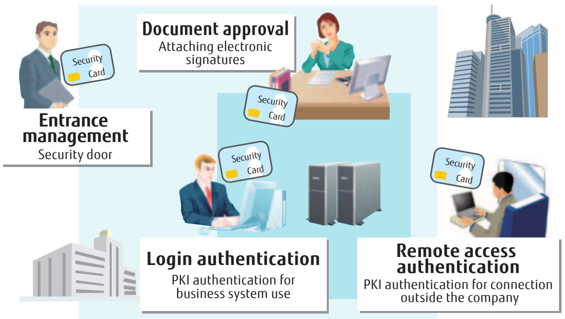
Employees are required to use the Security Card when accessing application systems. Authentication by PKI at login to application systems enables secure identification and authentication of employees along with simple operation.

Application systems can also be accessed from off premises, e.g., on 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


Document approval
Attaching electronic signatures
Security Card
Entrance management
Security door
Login authentication
PKI authentication for business system use
Remote access authentication
PKI authentication for connection outside the company

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 gateway systems such as firewalls by a team of experts
- Inspection and authorization of connections performed by divisions

■Maintaining security during operation

- Measures against unauthorized access (server configuration, checking the status of device management, monitoring and preventing unauthorized transmissions)
- Reliability design, performance management for stable operations

■Support for mobile devices

- Implementing and operating a secure business environment for remote PCs and smart devices* in connecting into the intranet

*: Smart devices: Smart phones and tablets.

■Response to new threats

- Survey and analysis on new threats such as targeted e-mail attacks and APT (Advanced Persistent Threat)
- Research on attacking techniques and responses
- Awareness and training programs for users

E-mail control

Employees are allowed to use e-mail to communicate with external dresses when it is needed for their roles. Following measures are in place for managing e-mail security.

■Controlling e-mail servers

- Installation and operation of e-mail servers by specialist group

■Maintaining security during operation

- Anti-virus measures
- Anti-spam measures
- High availability measures including performance management and endable system design

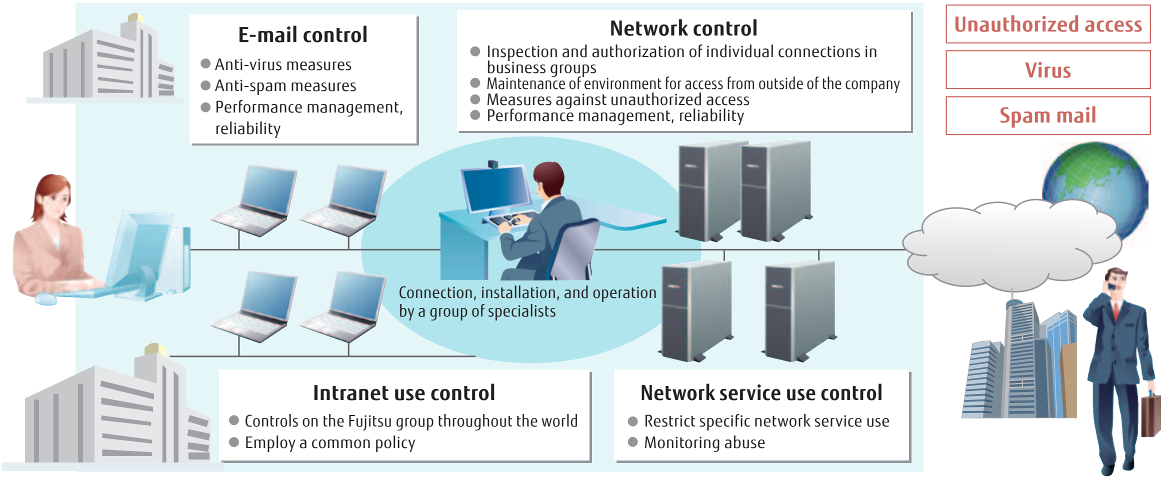
Network service use control

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 merits and requirements and improved client security controls. On the other hand, use of specific network services identified to have risks of information leakage is prohibited. Also, to prevent accidental use, communication using these services is continually monitored.

Intranet use control

Use of intranet is controlled throughout the Fujitsu Group. The construction and use of intranets in each company in the group throughout the world is controlled based on a common policy as one measure in the global system based on the "Fujitsu Group Information Security Policy".

Network security control


E-mail control
● Anti-virus measures
● Anti-spam measures
● Performance management, reliability
Network control
● Inspection and authorization of individual connections in business groups
● Maintenance of environment for access from outside of the company
● Measures against unauthorized access
● Performance management, reliability
Unauthorized access
Virus
Spam mail
Connection, installation, and operation by a group of specialists
Intranet use control
● Controls on the Fujitsu group throughout the world
● Employ a common policy
Network service use control
● Restrict specific network service use
● Monitoring abuse

Security Measures for Cloud Services

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 deficiencies in security and reliability, to the user. This section introduces the security initiatives implemented in the Fujitsu Cloud Computing Service.

Challenges of Cloud Computing

By using ICT in the cloud, there are many benefits including the simplification of design and architecture, but there also lays many security threats. For example, since many user accounts and user information exists in the same ICT resource within the cloud, it is possible that the impact from an attack would be much greater than in a standard system. Concerns also exist over attacks penetrating vulnerabilities in the virtualization technology that is used in the cloud, the possibility that an attack is mounted against a third party by attacking and misusing a cloud environment as a tool, and unauthorized activity by the internal workers who support the cloud infrastructure.

To counter these kinds of threats, it is important to consider conventional security by implementing border defenses and multilayered defenses in the network, servers, and web applications. However, it is also necessary to consider factors specific to the cloud, such as risks related to virtualization technology and management risks due to changes in the responsibilities over ICT resources. It is also important for cloud service providers and users to recognize their respective scopes of responsibility when using the cloud and to mutually cooperate.

The Fujitsu Approach

The Ministry of Economy, Trade and Industry has published "Information Security Management Guidelines for the Use of Cloud Computing Services" for cooperation between users and providers of cloud services. Fujitsu has referred to these guidelines when a customer is considering implementing a cloud service and has organized them into 11 key aspects.

11 key aspects

1 Information security policy
2 Organization for security
3 Resource management
4 Human resource management
5 Physical and environmental security
6 Communication and operational management
7 Access restrictions
8 Acquisition, development, and maintenance of information systems
9 Information security incident management
10 Business continuity management
11 Compliance

The Fujitsu information security policy is based on the "FUJITSU Way", which represents the ideals and direction of the Fujitsu Group. Furthermore, the "Fujitsu Group Information Security Policy" is set uniformly across the entire company, including foreign subsidiaries, and the related standards are set and information security measures are implemented by following this policy.

In order to implement information security measures appropriately in the cloud service, Fujitsu has organized a "Cloud Security Committee" where the committee chairman is an employee on the management level. This committee also includes external experts for ensuring impartiality, and performs regular risk analyses and audits of the cloud service and decides the policies for handling risk.

In order to protect systems from cyber attacks and unauthorized internal activity, Fujitsu cloud services implements various security measures including authentication and ID management using digital certificates, encryption of communication and storage, and centralized surveillance through an integrated management console.

Furthermore, the "FGCP/S5" Fujitsu IaaS is able to build secure systems consisting of three layers of web, application, and database, and delivers systems with high reliability on par with on-premise systems.

Fujitsu cloud service equipment is installed in the server room of a durable data center, and there is complete redundancy of equipment, parts, and networks. This equipment is protected by technology including palm vein authentication devices that manages the coming and going of visitors, and surveillance cameras and RFID tags for managing the locations of workers within the data center.

The Fujitsu cloud service systems, including these information security measures, are managed by following operational procedures based on ITIL®.

Fujitsu continually implements and improves these information security measures, and proactively responds to cloud-related threats. The approaches made by Fujitsu that could not fit into this section are published in the "Approach to Information Security for the Cloud" white paper on the website.

Global Approach

Fujitsu is now expanding a cloud platform into 5 countries that is of the same high-quality platform they have implemented in Japan.

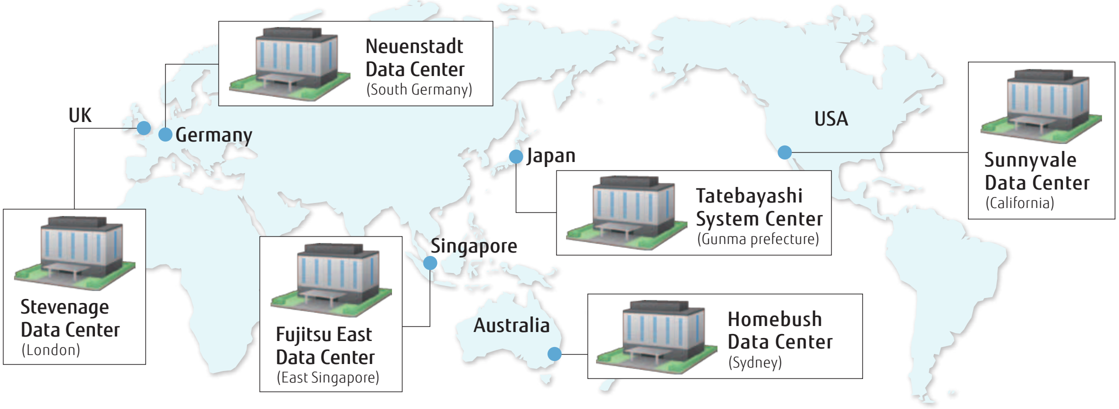
The Fujitsu Group has established an information security policy that is uniform across the entire company including global subsidiaries, and appropriately undertakes management of personal information for each country. Based on this policy, the Fujitsu cloud service has unified the global operational management and built on the operational management system they began in Japan.

Furthermore, the Fujitsu cloud service has also set up a shared support center for handling inquiries from customers around the world and a back line support center for resolving technical problems. This system provides standardized global support from anywhere in the world.

In order to allow customers to securely use the Fujitsu cloud service, our global subsidiaries implement measures against information leaks from unauthorized internal activities using thorough lifecycle management (from hiring to retirement) of the employees who work in the cloud service.

At many of our major global subsidiaries various certifications have been acquired for increasing the added value of services and improving the quality of data centers, such as the acquisition of an ISMS certification.

▼ Fujitsu cloud data center locations


Neuenstadt Data Center (South Germany)
UK
Germany
Japan
USA
Sunnyvale Data Center (California)
Tatebayashi System Center (Gunma prefecture)
Stevenage Data Center (London)
Singapore
Fujitsu East Data Center (East Singapore)
Australia
Homebush Data Center (Sydney)

Efforts by Fujitsu Cloud CERT

In order to implement a "trusted" cloud as demanded by today's businesses, Fujitsu established "Fujitsu Cloud CERT" in 2010 for exclusively handling cloud security. CERT is an abbreviation of Computer Emergency Response Team, and refers to a team of specialists who rapidly and accurately handle security emergencies that occur in a computer environment. Fujitsu Cloud CERT was granted permission to use the CERT name publicly by the Carnegie Mellon University in the USA, and is the first cloud CERT organization in the world.

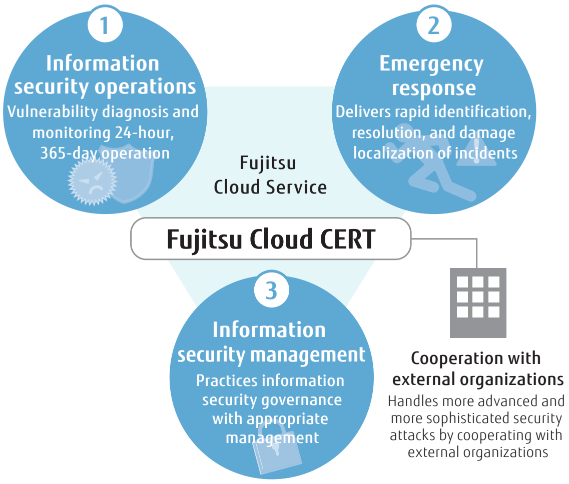
Fujitsu Cloud CERT performs the following activities on a global scale in order to support our customers' businesses and protect the cloud environment from various security threats.

(1) Information security operation
In order for customers to securely use the Fujitsu cloud service, Fujitsu Cloud CERT implements information security measures including vulnerability diagnosis and monitoring of the cloud service infrastructure, and operates using a 24-hour, 365-day system.

(2) Emergency response
In order to respond appropriately to unforeseeable security incidents, Fujitsu Cloud CERT has established responsive measures for when an incident occurs. In the rare event an incident does occur, these measures implement rapid and accurate identification, resolution, and damage localization of the incident.

(3) Information security management
In order to protect information important to our customers, Fujitsu Cloud CERT provides appropriate management of "people", "things", and "information" in the Fujitsu cloud service, and practices information security governance.

We are also affiliates of security related organizations such as Nippon CSIRT Association and FIRST, and act to improve global cloud security.


1
Information security operations
Vulnerability diagnosis and monitoring 24-hour, 365-day operation
2
Emergency response
Delivers rapid identification, resolution, and damage localization of incidents
Fujitsu Cloud Service
Fujitsu Cloud CERT
3
Information security management
Practices information security governance with appropriate management
Cooperation with external organizations
Handles more advanced and more sophisticated security attacks by cooperating with external organizations

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.

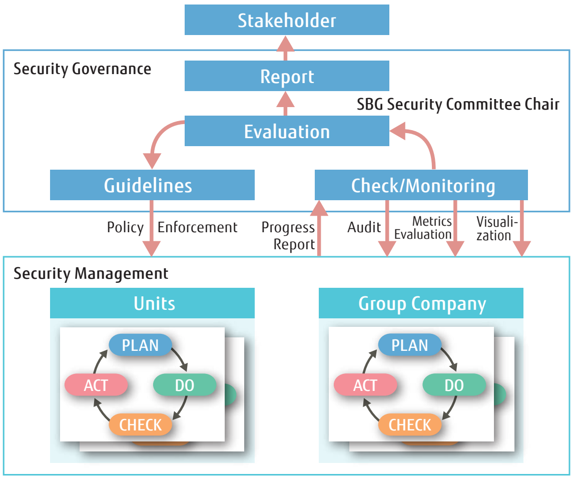
Solution Business Group Characteristics

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) ICT system consulting, (2) system architecture, (3) data center and ICT 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 including Europe, the Americas, China, and the Asian Pacific region. In the outsourcing field in particular, data centers are setup in approximately 100 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

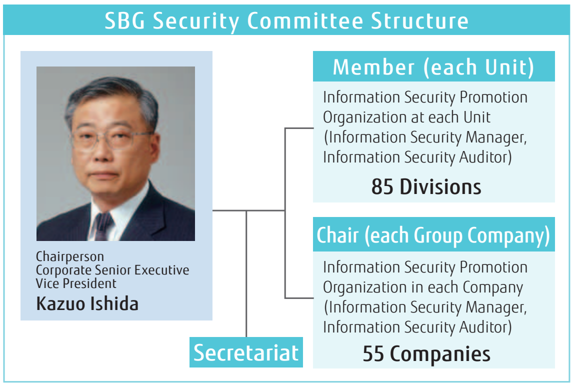


SBG Information Security Management Promotion System

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.

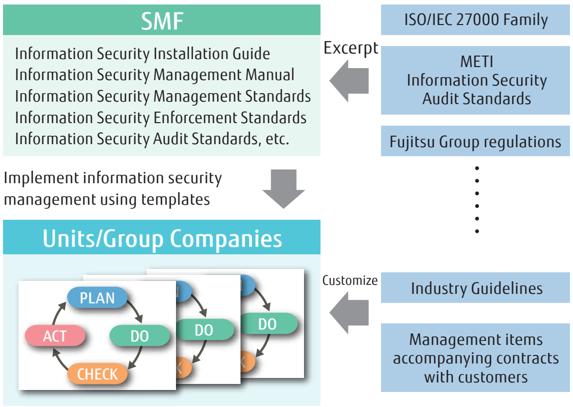
SBG Security Committee Organizational Chart


SBG Security Committee Structure
Chairperson
Corporate Senior Executive Vice President
Kazuo Ishida
Secretariat
Member (each Unit)
Information Security Promotion Organization at each Unit
(Information Security Manager, Information Security Auditor)
85 Divisions
Chair (each Group Company)
Information Security Promotion Organization in each Company
(Information Security Manager, Information Security Auditor)
55 Companies

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


SMF
Information Security Installation Guide
Information Security Management Manual
Information Security Management Standards
Information Security Enforcement Standards
Information Security Audit Standards, etc.
Excerpt
ISO/IEC 27000 Family
METI Information Security Audit Standards
Fujitsu Group regulations
Implement information security management using templates
Units/Group Companies
PLAN
ACT
DO
CHECK
DO
DO
Customize
Industry Guidelines
Management items accompanying contracts with customers

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, 563 employees have completed this training. Also, "Information Security Auditor Training" is provided to information security auditor managers and auditors who promote internal audits. Presently, 840 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 141 employees have acquired auditor qualifications.

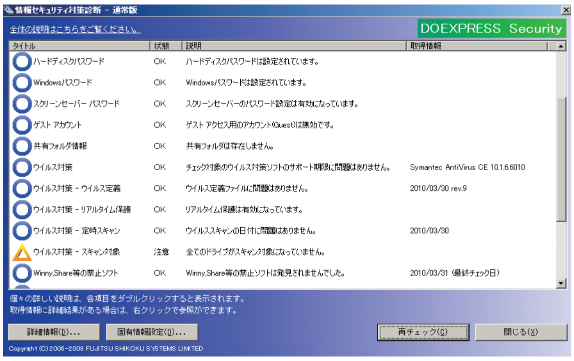
Security maintenance through IT infrastructure standard operation service

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



全体の説明はこちらをご覧ください。

タイトル	状態	説明	取得情報
○ ハードディスクパスワード	OK	ハードディスクパスワードは設定されています。	
○ Windowsパスワード	OK	Windowsパスワードは設定されています。	
○ スクリーンセーバー パスワード	OK	スクリーンセーバーのパスワード設定は有効になっています。	
○ ゲスト アカウント	OK	ゲスト アクセス用のアカウント(Guest)は無効です。	
○ 共有フォルダ情報	OK	共有フォルダは存在しません。	
○ ウイルス対策	OK	チェック対象のウイルス対策ソフトのサポート期限に問題はありません。	Symantec AntiVirus CE 10.1.6.6010
○ ウイルス対策 － ウイルス定義	OK	ウイルス定義ファイルに問題はありません。	2010/03/30 rev.9
○ ウイルス対策 － リアルタイム保護	OK	リアルタイム保護は有効になっています。	
○ ウイルス対策 － 定時スキャン	OK	ウイルススキャンの日付に問題はありません。	2010/03/30
△ ウイルス対策 － スキャン対象	注意	全てのドライブがスキャン対象になっていません。	
○ Winny,Share等の禁止ソフト	OK	Winny,Share等の禁止ソフトは発見されませんでした。	2010/03/31 (最終チェック日)

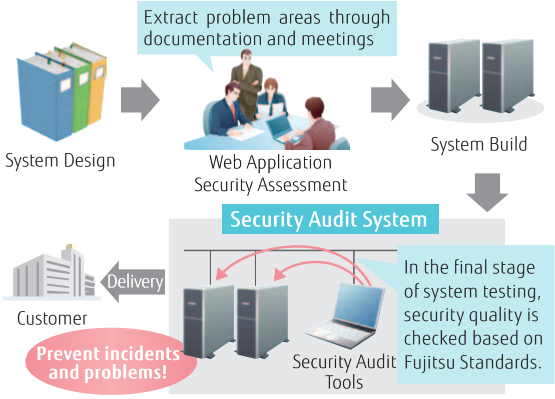
個々の詳しい説明は、各項目をダブルクリックすると表示されます。
取得情報に詳細結果がある場合は、右クリックで参照ができます。

Copyright (C) 2006-2008 FUJITSU SHIKOKU SYSTEMS LIMITED

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 (hereinafter customer delivered systems). It is mandatory that a security specialist department objectively verify that the contents of the "Security Requirements" are fulfilled before delivery to the customer.

▼Security audits for systems delivered to customers


Extract problem areas through documentation and meetings
System Design
Web Application Security Assessment
System Build
Security Audit System
Delivery
Customer
Prevent incidents and problems!
In the final stage of system testing, security quality is checked based on Fujitsu Standards.
Security Audit Tools

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

In regard to web applications, to resolve problems in the upper process, security assessments 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 implementation of the customer system security audit.

Information security audits

The SBG periodically performs internal audits and audits by the SBG security committee on each division and group company to check the operational status and adherence to information security management and security measures.

In the internal audits, audits are conducted mainly by auditors who have completed the "information security auditor training". In the audits by the SBG security committee, audits are performed by auditor teams consisting of members from the security committee and qualified JASA auditors who do not belong to the organization being audited.

In addition, special auditing themes are set up and security audits are individually conducted by specialists in the security committee on particular projects, divisions, and group companies within the Fujitsu Group as needed.

Visualization of Information Security Activities

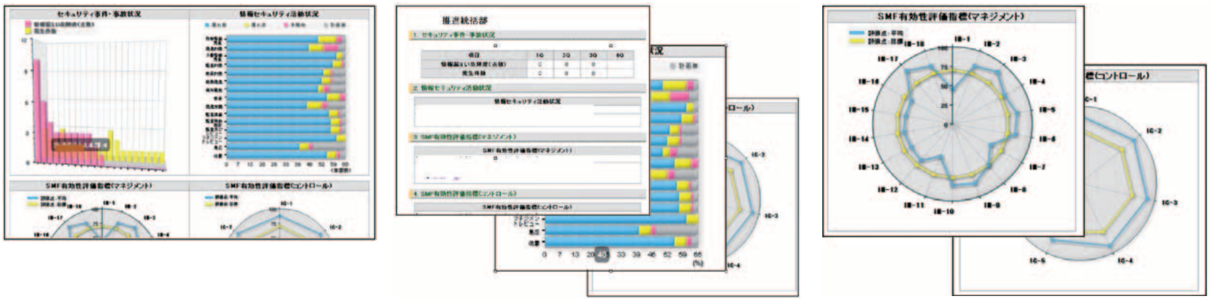
Information security activity includes activity on the management side and activity on the measures for PC security side.

It is effective for the SBG Security Committee to evaluate to what level these activities are being performed using quantitative metrics.

The SBG periodically collects and performs risk evaluation on incident and accident information, and calls for measures to prevent reoccurrence.

Furthermore, the status of information security activities are measured and evaluated with several evaluation metrics, and the evaluation results are presented visually to be understood uniformly. More specifically, this is visualized and 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

As a major client device, Personal Computers are exposed to many security threats as the end points within a company. During the development of client devices at Fujitsu, we strive to provide security functions that allow you to implement the best safety measures for threats envisioned in each usage scenario.

Approach to Security Criteria in Client Devices

PCs are client devices that work an important role as an endpoint for handling information resources within a company, including confidential and personal information. Since they are used by numerous people in a variety of environments, PCs are exposed to countless security threats, including the loss or theft of the computer, unauthorized access, data tampering, and computer viruses, all of which require appropriate preventative measures. Fujitsu thus strives to provide security functions that allow you to implement the best safety measures for the various threats that are envisioned in each usage scenario, including when turned off, when starting up and logging in, during use, and when being disposed.

When Turned Off

When not in use, there is a possibility of loss or theft of the computer or hard disk. Computers are equipped with a cable lock for preventing theft of the computer, a hard disk unit with an encryption function so that data cannot be viewed if the computer is stolen, and a remote erase function for locking or invalidating data on the hard disk remotely in the event of loss or theft.

While Starting Up and Logging In

There is always a threat of unauthorized use and impersonation when logging into a system. In addition to the password authentication provided by BIOS and the OS, authentication can also be strengthened using the ownership-based authentication of smartcards or by biometric authentication using fingerprints and palm vein patterns.

While In Use

The possibility of leaking encryption keys from unauthorized removal of data by the user or by viruses exists while the computer is in use. We provide functions for restricting the use of USB and printer ports, security chips that offer hardware protection of encryption keys, and anti-virus software for implementing measures to prevent viruses.

When Being Disposed

There exists a risk of data being leaked from hard disks that have not been properly disposed. We provide a hard disk erase function that overwrites original data on the disk with invalid data multiple times, so that no traces of the original data remain and the data cannot be recovered after it is disposed.

▼ Threats and measures envisioned for each PC usage scenario

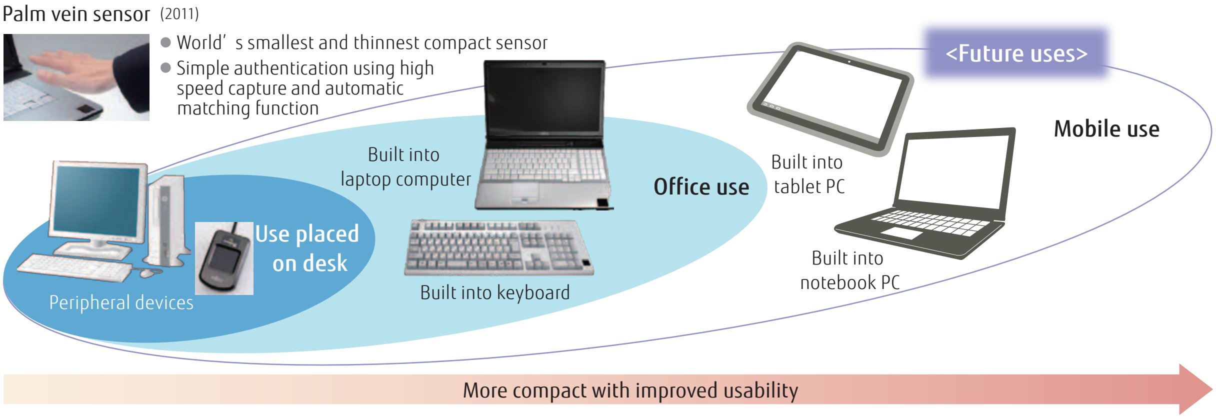
Operation	Threat		Measures	
			PC/Windows standard functions	Strengthened Functions provided by Fujitsu
When off	Loss or theft of computer or hard disk	Measures for loss and theft	• Hard disk password	• Security Lock Slot • Remote erase (CLEARSURE)
		Encryption	• Volume encryption (BitLocker)	• Full-Disk encryption (Self-Encrypting HDD)
Starting up/ logging in	Use by unauthorized users Leaking of passwords	BIOS password	• Startup password • BIOS setup password	• Security panel (five buttons for Power ON password) • Palm vein authentication • Fingerprint authentication
		Strengthened authentication	• Windows password • Application password	• Palm vein authentication • Fingerprint authentication • Smartcard authentication
While in use	Unauthorized removal of data Theft/forgery	Encryption	• Folder encryption (Windows EFS)	• Security chip
		Operation restrictions	———	• PortShutter("lock-out" certain ports from unauthorized use)
	Virus infection	Anti-virus	• Windows Update • DEP(Data Execution Prevention)	• Anti-virus software
When being disposed	Data theft	Data erasure	———	• HDD erase utility (Permanently delete data)

Approach to Palm Vein Authentication

Although passwords are generally used for personal authentication, it also allows for exposure through the theft of a password and inconveniences when having forgotten the password. As a result, attention is being focused on biometric authentication which utilizes characteristics which only the authentic user possesses. From among these technologies, palm vein authentication is using technology developed exclusively by Fujitsu and has the advantages of being robust against loss, theft, and forgery. ID theft can also prove to be difficult since the technology utilizes palm vein patterns which are normally invisible, and thus has been started to be used by financial institutions and is widely spreading to the medical, government, and public service sectors.

Initially having a built-in palm vein authentication unit, while offering high-level personal authentication, required equipment and devices of a certain thickness to fit within the chassis. Since the system required the palm of the hand to remain momentarily still over the sensor during authentication, this became a problem when expanding the environments in which the technology could be used. However, technology was then developed to make this advanced personal authentication technology even more portable and easier to use, and in 2011 the world's smallest no-contact palm vein sensor offering both compactness and increased usability was put into practical use. This made it possible to embed the technology into keyboards and build into laptop computers as well as drastically improving usability to deliver authentication by simply waving the palm of your hand. In the future, we are working on developing an even more compact palm vein sensor that can be built into tablet PCs and notebook PCs so that it can be used for biometric authentication to further suit the needs of our customers.

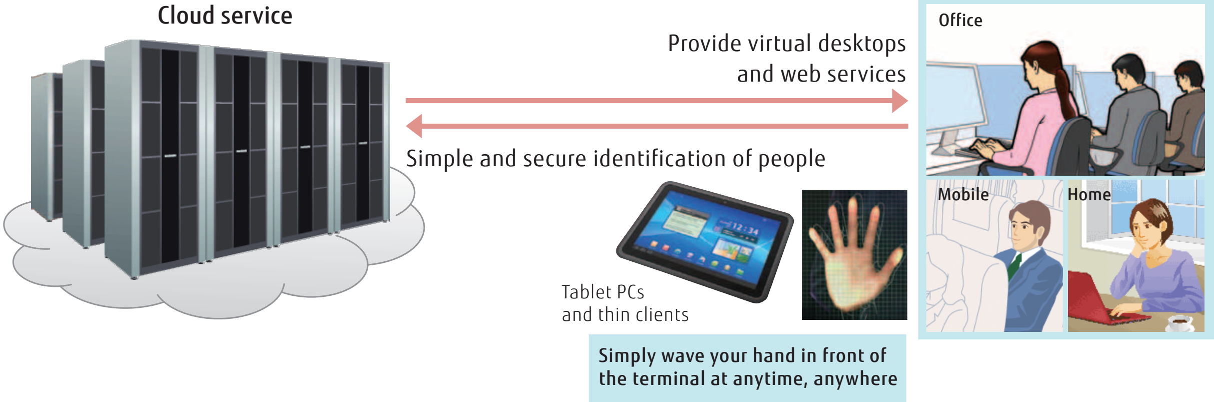
▼ Evolution of usage scenarios for palm vein authentication


Palm vein sensor (2011)
● World’ s smallest and thinnest compact sensor
● Simple authentication using high speed capture and automatic matching function
<Future uses>
Mobile use
Built into laptop computer
Office use
Built into tablet PC
Use placed on desk
Built into keyboard
Built into notebook PC
Peripheral devices
More compact with improved usability

Workplace solutions of client security in the Feature

With cloud computing, resources are placed on virtualized servers with the expectation of systems that can be used from a wide variety of locations. Data in the cloud can be accessed by anyone, however, and personal authentication is even more important for identifying authentic users. One solution is for allowing safe use of the cloud environment by employing personal authentication in the cloud service by using biometric authentication (which has no risk of loss or theft). Fujitsu is constantly striving to improve security functions for front-end client devices in ICT environments to suit the evolving needs of our customers.

▼ Envisioned usage of biometric authentication in the cloud and thin clients


Cloud service
Provide virtual desktops and web services
Simple and secure identification of people
Office
Mobile
Home
Tablet PCs and thin clients
Simply wave your hand in front of the terminal at anytime, anywhere

Approach of Fujitsu FSAS

Fujitsu FSAS Incorporated aims to be a leading IT infrastructure company based on the corporate message of "More Secure & More Creative".

Within the Fujitsu Group, Fujitsu FSAS is trying to utilize our front-line point of customer contact to become an irreplaceable partner for total one-stop service to suit our customers' needs.

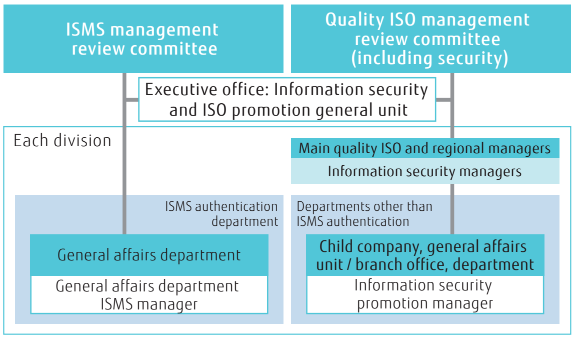
Because of this, we place importance on personnel development, and implement a variety of initiatives for improving technical skills and information security.

Fujitsu FSAS undertook an external accreditation audit by I. S. Rating Co., which rates the strength of information security, with the Tokyo LCM Call Center awarded the first "AA$_{is}$" for a call center in fiscal 2011, providing even more secure, safe, and stable service to our customers.

Information Security Framework

The ISMS authentication department is the service execution department that is entrusted with customer information, and aims to build and operate processes modeled on ISMS requests, to continuously execute PDCA, and to improve security.

Departments other than ISMS authentication execute PDCA in compliance with level 3 SMF measures of the Fujitsu SBG Security Committee based on the ISO/IEC 27000 family.


ISMS management review committee
Quality ISO management review committee (including security)
Executive office: Information security and ISO promotion general unit
Each division
Main quality ISO and regional managers
Information security managers
ISMS authentication department
General affairs department
General affairs department ISMS manager
Departments other than ISMS authentication
Child company, general affairs unit / branch office, department
Information security promotion manager

Information Security Policy

In addition to measures implemented by the system as information security measures, educational activities are undertaken for training of personnel and public security awareness.

(1) Security measures for file servers with shared information

■ Access control using Active Directory Rights Management Services + Rightspia + SharePoint®

Customer information is encrypted, with access rights granted at the library, folder, and file levels.

Note: Rightspia is an add-on for the Active Directory Rights Management Services that implements rights limitations on viewing, printing, and performing other operations on Microsoft® Office documents, and provides the same interfaces and functions to PDF documents.

(2) Measures for preventing dissemination of information on systems permitted to be taken outside the office

The system restricts use after work has finished with the sole purpose of preventing the dissemination of information by requiring approval by a superior and a defined period of validity. Furthermore, tracking management has been implemented with the use of a carry out authorization log.

(3) Managing PCs taken outside the office

■ PCs exclusively for use outside the office and PCs that are prohibited for taking outside the office are strictly separated

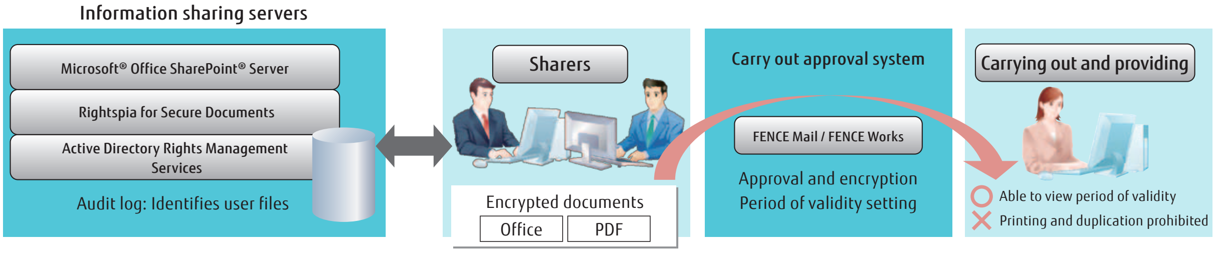
PCs exclusively for taking outside the office are constructed using the formula of requiring "thin client + no emailer installed + automatic data deletion tool", with all data on the PC immediately erased the following morning to ensure no data remains on the PC.

(4) PC security measures

A diagnostic tool "DOEXPRESS Security" is installed on all PCs, and automatically diagnoses whether security patch updates, passwords, etc. are configured correctly. (Carried out monthly)

In the Fujitsu LCM Service Center, unauthorized PC connections to network systems are prohibited by a network quarantine system.

▼ Security measures on file servers that share information


Information sharing servers
Microsoft® Office SharePoint® Server
Rightspia for Secure Documents
Active Directory Rights Management Services
Audit log: Identifies user files
Sharers
Encrypted documents
Office
PDF
Carry out approval system
FENCE Mail / FENCE Works
Approval and encryption
Period of validity setting
Carrying out and providing
○ Able to view period of validity
✕ Printing and duplication prohibited

Personnel Development Policy

Fujitsu FSAS continuously conducts annual education and training activities as part of a range of activities against information security accidents. This makes each and every employee think, and raises awareness of information security.

(1) Self-check

- Every day, use the internal company web to perform a check of e-mail left on mobile phones, security settings, and the whereabouts of cards loaned to the customer.
- Carry out a check of whether or not work information exists on non-work-related PCs.
  (Twice per year: Detection expert)

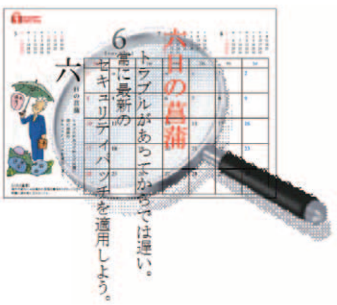
(2) Information security video education

Video education is "Education by realization" which stimulates people into thinking about security by viewing dramatically constructed security incidents and is an improvement over standard educational methods (textual information only).

- Theme of educational material: Loss and theft resulting from consuming alcohol

(3) Posters and desk calendars

These continually alert employees with the aim of preventing information security incidents from occurring.


6
六
六日の菖蒲
トラブルがあらわれてからでは遅い。
常に最新の
セキュリティパッチを適用しよう。

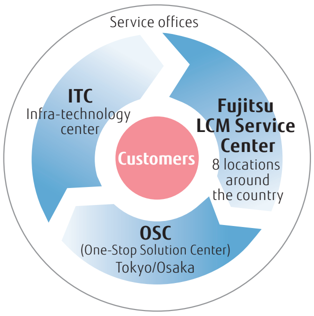
Advanced Information Security Infrastructure for Supporting Services

A watertight framework for supporting the IT systems of our customers is provided through the establishment of "ITC (Infra-technology center)" for supporting the building of infrastructure, "Fujitsu LCM Service Center" for supporting operations, and "OSC (One-Stop Solution Center)" for troubleshooting support.

(1) Support that is closely tied with the region

The following measures are implemented with an emphasis on supporting customers in each region.

- In the rare event that problems occur, the service engineers in charge of the region rush from the nearest center to deliver rapid response.
- Service is provided using a "24-hour, 365-day" system that includes not only support during business hours, but also nights and holidays when system administrators tend to be absent.
- Information security inspections are carried out on Fujitsu CE partners (600 major offices including small and medium offices and local partners) throughout the country to ensure that a high security level is maintained.



(2) Robust physical security measures

At the LCM Service Center and OSC, which provides centralized management of customer data, information is managed using complete security measures.

■ Entrance/exit management

- Areas are separated by purpose, and appropriate room access restrictions are imposed.
- The state of people entering and exiting rooms is also monitored and recorded with only employees registered in advance allowed to enter and exit rooms using palm vein authentication devices.

■ Surveillance and video recording using surveillance cameras

- Surveillance cameras are installed in locations that require a high security level, such as entrances, exits, and server areas.

Note: Information security management system:
IS 93196 / ISO/IEC 27001:2005

Note: I. S. Rating certification ID codes:
10000310116C1102; Rating code (AAis) (Tokyo LCM Service Center)

(3) High quality service

IT service management systems have been acquired at LCM service centers in 8 locations throughout the country, providing secure regionally tied in service.

Note: ITSMS 508018 / ISO/IEC 20000-1:2005

Fujitsu FSAS provides "secure, safe, and stable" services 24 hours a day, 365 days a year on our customers' front lines together with 850 service centers and approximately 8,000 service engineers throughout the country from the Fujitsu Group CE and Fujitsu CE partners.

Security and Safety Measures by Nifty

Nifty Corporation (hereinafter Nifty) provides "@nifty" the Internet service, "Shufumo" free service for housewives through mobile phones and smartphones, also the "Nifty cloud" public cloud computing service.

As information security measures, Nifty adopt the international standard ISO/IEC 27001, and follow it strictly in all companies. In addition to protect credit card information, we also adopt PCI DSS the security standard of the global standards of the card industry. Nifty fully complied to the standard. Nifty provide secure and safe services to our customers by combining these two international security standards to protect our total of 11,840,000*1 customer information.

The total number of Nifty members is approximately 11,840,000*1

Nifty provides a product lineup which includes an optical fiber (FTTH) connection service, high speed mobile communications such as WiMAX and web services with a total membership of 11,840,000 customer*1.

The "Shufumo" free service for mobile phones and smartphones provides summary of high-interest information for housewives which includes pamphlets issued by supermarkets throughout Japan, and is welcomed by more than 1,400,000*2 members. The "Nifty Cloud" public cloud computing service has already got more than 1,000*3 customer.

Holding large amount of customer information, Nifty provides the Internet services over the open the Internet environment. Consequently our information security measures had to meet international standards.

*1: As of November 2011
*2: As of January 2012
*3: As of October 2011

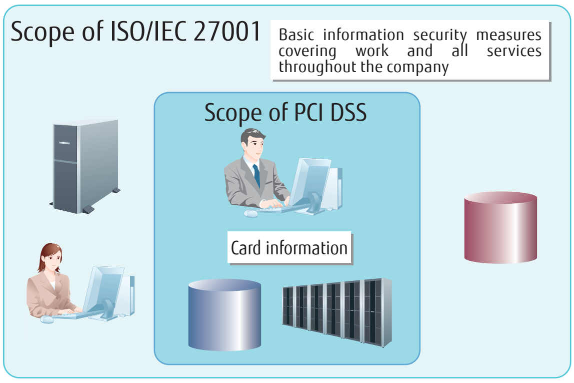
Implementing Multilayer Security Measures That Combine the Two Standards

Nifty implements multilayer measures by combining two information security related international standards. The implementation of multilayer measures is based on the idea of a fail-safe, where even if there are weaknesses, those weaknesses are covered by other measures.

The combination of international standards employed for the multilayers are the ISO/IEC 27001 international standard for information security management and the PCI DSS (Payment Card Industry Data Security Standard) global security standards from the credit card industry. Multilayered measures are implemented by total compliance with the PCI DSS for credit card information which requires an even higher level of protection in addition to the implementation of basic information security measures on all operations and services throughout the company using ISO/IEC 27001.

Using this combination of two different international standards makes it possible to implement efficient and effective security measures for customer information that contains personal information and other information resources, even for credit card information.

▼Implementing multilayered protection by following two standards


Scope of ISO/IEC 27001
Basic information security measures covering work and all services throughout the company
Scope of PCI DSS
Card information

ISO/IEC 27001 security measures have been implemented for all services and companies, and PCI DSS additionally covers credit card related systems and tasks.

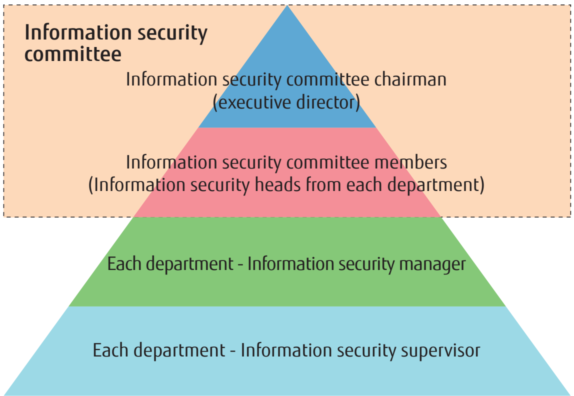
Adoption of the ISO/IEC 27001 international standards for information security management

ISO/IEC 27001, which is the base of the security measures that are combined into the multilayered structure, requires establishing information security policies, identifying the information resource held by a company, and managing and protecting these from organizational, human, physical, and technical perspectives.

As an organizational response, an "Information Security Committee" was established for promoting information security measures throughout the entire company. This committee has the responsibility for implementing the "Management Review" required by ISO/IEC 27001 and also for providing basic proposals for the information security measures across the company as well as other plans.

Furthermore, they also appoint the supervisors, managers, and personnel in charge of information security in each department, and organize a system that implements periodic security checks. In the security checks that are held every month, the basic measures determined by the rules are checked and the efficacy is increased by confirmation by the manager. Furthermore, efforts are made to share information at the whole company level and to prevent reoccurrences even in the event that an implementation measure is skipped.

▼ Nifty information security framework


Information security committee
Information security committee chairman (executive director)
Information security committee members (Information security heads from each department)
Each department - Information security manager
Each department - Information security supervisor

Analyze various security incidents to utilize for training materials

Security training is served periodically for all employees to enable executing security measures by themselves. The content of the training includes basic topics such as the importance of the information security and to publicize rules in the company and to let every employees to comply the rules, also includes case study of other company which caused a mass leak of their customer information. The training features importance of managing accounts and passwords appropriately and the risks when you access a system in the company from outside. Also it provides clearly necessary measures to prevent security incidents. Furthermore we focus on an effort in human resource development for qualification of the information security management such as an assistant ISMS auditor.

Zone offices to strengthen physical security

Nifty relocated their head office at the end of 2011. At this new premises the office layout was designed with information security measures in mind, with the physical security greatly strengthened compared to the security that was previously in place. The office layout was designed using a method called "zoning" where the rooms are separated to match the importance of the information resources that are handled. In each of the zoned rooms, the employees that can enter and the information that is handled are restricted, and the opportunities for unauthorized personnel to come into contact with information resources is reduced.

Hierarchical measures from development to operation

Nifty maintains an environment that provides safer services by hierarchically constructing multiple security measures. For example, the zoning used in the office layout is also applied to the ICT infrastructure. Considering the importance of information, we manipulate and manage appropriate access control of networks and servers of the whole ICT infrastructure. We established a procedure when we develop and release services. It requires a quality test before releasing and periodical vulnerability test after releasing. We regard quality of a product as a total one in every stages from development to operation. Nifty maintains and improves information security by hierarchical measures.

Credit card information is strongly protected by PCI DSS

Nifty adopted PCI DSS as the information security measure for protecting credit card information, and verifies total compliance with a compliance confirmation review by a review company certified by the PCI SSC (Payment Card Industry Security Standards Council). PCI DSS requires over 250 rules and measures for systems that process or save credit card numbers, or where credit card numbers are transferred. For example, this requires specific measures that are more strict than ISO/IEC 27001 described earlier, such as installing firewalls, encrypting databases, and conducting periodic intrusion testing. Nifty therefore strictly employs measures such as zoning and quality testing for ICT infrastructure and operations that handle credit card information. Furthermore, more effective security is implemented by periodically auditing these measures. This provides a secure environment for customers to use credit cards.

Other Security Measures

At the same time as working on information security measures according to the aforementioned global standards ISO/IEC 27001 and PCI DSS as an "approach to safety and security", Nifty also implements efforts such as "Internet Service Provider Safety and Security Mark", "Personal information protection policies", and "@nifty junk mail measures policy". Refer to the Nifty website to view details on these approaches.

Approach of Fujitsu Technology Solutions (Fujitsu CEMEA & I)

Fujitsu has restructured Fujitsu Services (UK) and Fujitsu Technology Solutions on the management level, and is currently driving its business in the 3 areas of UK and Ireland, CEMEA & I (Continental Europe, Middle East, Africa & India), and Nordic regions. This report accounts for CEMEA & I, based out of Germany.

The internal security organization of Fujitsu CEMEA & I is responsible for Governance in IT-Security, Information Security, BCM for ICT systems, ICT Risk- & Crisis management and Data Privacy to all countries, locations, departments, business function, third parties, projects and employees and for maintaining the Corporate ISO/IEC 27001 Certificate in Fujitsu CEMEA & I.

Features of Fujitsu Technology Solutions

The goal of FTS Internal Security Services is to prevent and reduce loss, manipulation, forgery and disclosure of the company's internal and external confidential information. This is assured by designing and implementing technical and organizational security measures, guidelines and policies.

This organization is part of the CIO organization of Fujitsu CEMEA & I and is based in Germany. For all countries in which Fujitsu CEMEA & I operates, a security manager is in place to deal with policies, guidelines and issues in security. This allows us to immediately address security issues that occur in each country.

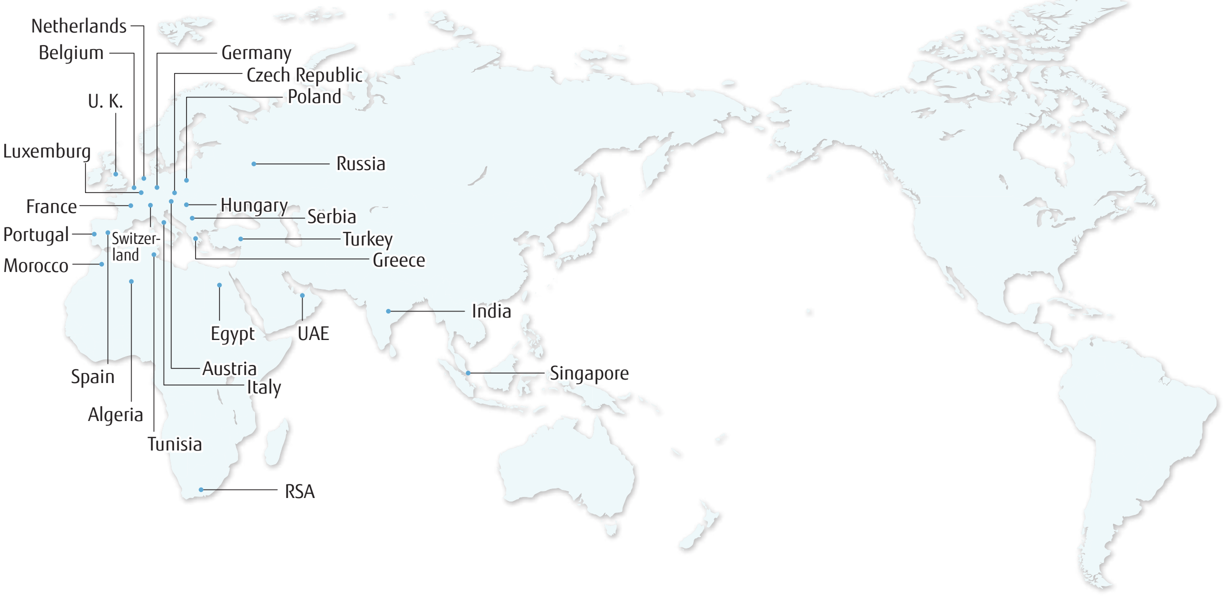
The organizational aspects of Security Governance by the CIO follows existing policies and guidelines. On the technical front, the organization is responsible for analyzing, conceiving, testing, and planning technical measures. This includes network, server and client security, vulnerability management, assessment management, reviews of security measures, internal security forensics and security incident management.

The operational tasks of our primary services are:

- Malware Protection for all used systems,
- Firewall Management for all DeMilitarized Zone (DMZ) with external view and internal firewalls cross the organization,
- Proxy Management (including web filtering),
- Public Key Infrastructure (PKI) and Encryption (HDD, E-mail)
- Authentication (Hardware/Software Token)
- Microsoft® Rights Management
- Intrusion Detection/Intrusion Prevention Systems (IDS/IPS) within all DMZ operated within Fujitsu CEMEA & I. Since the beginning of 2012 the Fujitsu Cloud (German part) is protected by IDS/IPS as well.

Besides what is listed above, FTS Internal Security Services is also responsible for Fujitsu Technology Solutions GmbH's legal compliance with the German Privacy Protection Law and advises Fujitsu CEMEA & I in matters of privacy protection.

▼ Fujitsu CEMEA & I Locations



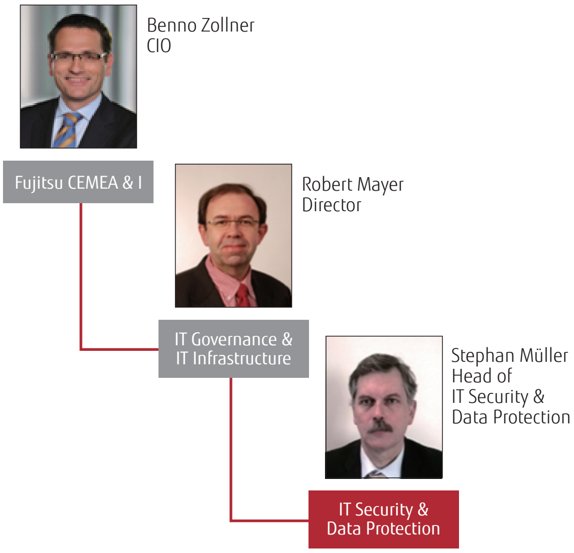
Structure and Status of Information Security Management

Since February 2012 the security function has been integrated into the CIO organization of Fujitsu CEMEA & I. The Fujitsu CEMEA & I security organization has set up activities, responsibilities and duties to assess and achieve compliance to internal and external security requirements.

To achieve these goals, a cross-organization security community has been put in place, lead by the Fujitsu CEMEA & I HQ Office in Munich. The organization is headed by Benno Zollner CIO, Robert Mayer Director IT Governance & IT Infrastructure and Stephan Müller Head of IT Security & Data Protection.

Information security measures and activities have been primarily influenced by the Fujitsu Global Information Security Policies, in addition to the FTS own Policy framework, ISO/IEC 27001, J-SOX, ISAE 3402 etc. and customer requests. All relevant controls are in place and documented.

Security Responsibility in Fujitsu CEMEA & I


Benno Zollner
CIO
Fujitsu CEMEA & I
Robert Mayer
Director
IT Governance & IT Infrastructure
Stephan Müller
Head of IT Security & Data Protection
IT Security & Data Protection

Various Information Security Measures

Patch management process

Fujitsu CEMEA & I has a strict update policy in place to ensure security for all standard clients and servers used by Fujitsu CEMEA & I, and to make sure they are using the most up-to-date patch. Emergency patch rollout begins within 5 business days. The rollout of out-of-band patches starts within 24 hours after being released. All business critical server systems are scanned four times a year by security and any vulnerabilities are found, analyzed, and remedied.

Preventing cyber attacks

All systems within the Fujitsu CEMEA & I DMZ are protected with firewalls, intrusion prevention and intrusion detection systems. Regularly Qualys vulnerability scans are done on all business critical systems. Findings are then discussed and checked with the system owners.

Activities in cooperation with the government and public institutions

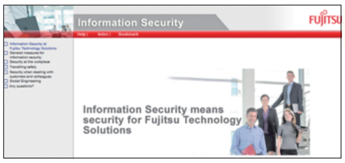
Fujitsu CEMEA & I Security and Data Protection maintains a strong cooperating relationship with FIRST, ISF, Federation of German CERTs, GDD (Society of Data Privacy and Data Security) and major enterprises including Siemens and BSH (Bosch Siemens Hausgeräte)

Information Security Awareness

The Fujitsu CEMEA & I security organization offers security related e-Learning, presentations, images and flyers to the entire company. Additionally, awareness training is conducted regularly across the company.

Security Awareness within Fujitsu CEMEA & I

Web based training


Information Security

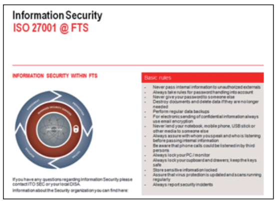
Help | Index | Bookmark

- Information Security at Fujitsu Technology Solutions
- General measures for information security
- Security at the workplace
- Travelling safely
- Security when dealing with customers and colleagues
- Social Engineering
- Any questions?

Information Security means security for Fujitsu Technology Solutions

Security images

Security flyer


Information Security
ISO 27001 @ FTS

INFORMATION SECURITY WITHIN FTS

If you have any questions regarding Information Security please contact ITO SEC or your local DISA.
Information about the Security organization you can find here:

Basic rules

- Never pass internal information to unauthorized externals
- Always take rules for password handling into account
- Never give your password to someone else
- Destroy documents and delete data if they are no longer needed
- Perform regular data backups
- For electronic sending of confidential information always use email encryption
- Never lend your notebook, mobile phone, USB stick or other media to someone else
- Always assure with whom you speak and who is listening before passing internal information
- Be aware that phone calls could be listened in by third persons
- Always lock your PC / monitor
- Always lock your cupboard and drawers; keep the keys safe
- Store sensitive information locked
- Assure that virus protection is updated and scans running regularly
- Always report security incidents

Formal Obligation Management (FOM)

By utilizing these tools, employee obligations can be collected automatically and give employees an individual overview about all given obligations. It is an important step to show compliance internally and publicly. This reduces paper consumption and is the step towards a paperless work process.

Research and Development into Security Technology for Supporting a Safe Lifestyle

Cyber attacks have become a problem, and the need for security technology in companies where smartphones are now rampant is continually growing. In order to manage these new risks, resilient, refined, and advanced security must be implemented. Fujitsu Laboratories is promoting research and development of leading edge technology in response to the demand for more advanced security measures.

Approach to Security Technology at Fujitsu Laboratories

Fujitsu Laboratories is conducting research on protecting the information used by companies from a wide variety of threats. The scope of this research covers a wide range from systems security technology for supporting a safe and secure society, to various component technologies. For example, the security of systems and products from Fujitsu has been greatly increased by using secure development processes that eliminate vulnerabilities in systems and products, anonymizing technology for protecting the privacy information that is becoming more and more important into the future, and tamperproofing technology for protecting chips that also have a security function.

This report introduces large scale biometric authentication technology and homomorphic encryption that allows operations to be performed on encrypted data as modern efforts in leading edge technology.

Authentication Systems for 10 Million People Using Palm Vein Patterns and Fingerprints

In recent years, biometric authentication technology has become more widespread as a technology to prevent attacks through "impersonation" that cause information leaks in companies and financial institutions. Among such technology, palm vein authentication was developed first in the world by Fujitsu Laboratories. This technology is currently utilized widely around the globe in such means as personal authentication in the ATMs of financial institutions due to its high level of authentication performance, PC access management in companies, and for room entry/exit management. Furthermore, because of its high authentication processing speed, fingerprint authentication has become widespread as a simple and accurate personal login authentication system that is built into PCs and mobile phones.

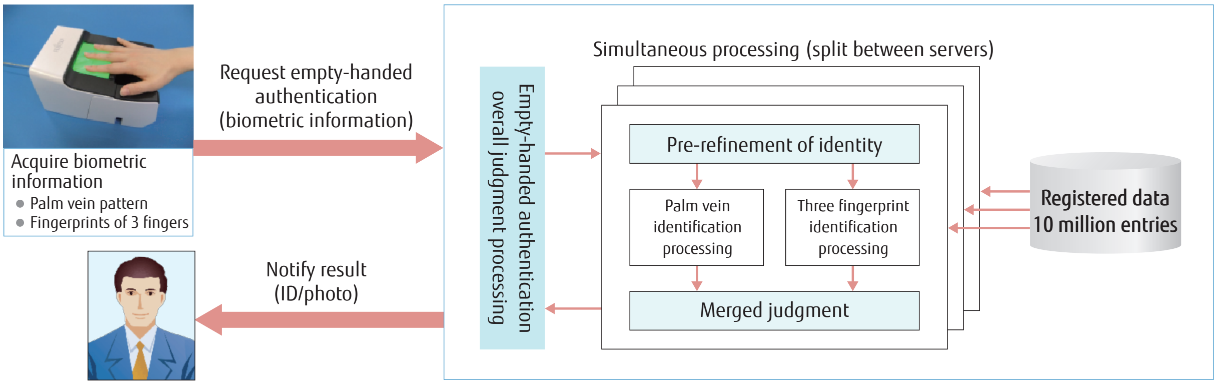
One of the features of biometric authentication is that it is an empty-handed authentication service that requires only biometric information, and the spread of biometric authentication is expected to accelerate even more due to the convenience of being able to use a service using your body alone. Attention is being drawn to the ability for such technology to quickly and accurately authenticate a particular person from among 10 million to 100 million people covered by a large company or government service, and is a key factor in the spread of this technology.

Fujitsu Laboratories was the first in the world to develop biometric authentication technology that combines palm vein information with fingerprint information from three fingers. We were able to develop and implement this technology in prototype system so that it can identify in 2 seconds a particular person from among the data of 10 million people by using both palm vein and fingerprint information.

Four pieces of technology were developed: 1) technology to simultaneously and stably acquire data from palm veins and fingerprints on three fingers; 2) technology to quickly refine the data to identify with 1/1000 precision; 3) technology to accurately and stably identifying a particular person by merging the palm vein and multiple fingerprints; and 4) technology to increase the simultaneous identification process.

Using this technology makes it possible to construct a biometric authentication system for performing empty-handed authentication for small scale room entry and exit management and for larger scale systems supporting the social infrastructure. Furthermore, this technology can be easily installed by simply adding palm vein authentication to the already widespread fingerprint sensors. Fujitsu Laboratories is investigating applying this technology to a wide variety of usage scenarios and environments.

▼ Prototype system of empty-handed authentication technology on a scale of 10 million people



Acquire biometric information
● Palm vein pattern
● Fingerprints of 3 fingers
Request empty-handed authentication (biometric information)
Notify result (ID/photo)
Empty-handed authentication overall judgment processing
Simultaneous processing (split between servers)
Pre-refinement of identity
Palm vein identification processing
Three fingerprint identification processing
Merged judgment
Registered data 10 million entries

Leading Edge Cryptanalysis Technology

Encryption technology is an element of information security that is necessary for the protection of all kinds of digital information. Encryption technology of recent years uses mathematical problems that are difficult to solve (for instance, integer factorization, discrete logarithm problems, and shortest vector problems) to implement mechanisms that allow only the person who holds the secret key (represented by numbers) to correctly decrypt information, and to guarantee that a valid signature is attached. However, if this kind of mathematical problem becomes solvable, encryption that depends on that problem will immediately become unsafe to use. This is because the difficulty of the problem needs to be accurately known in order to safely use the encryption.

Fujitsu Laboratories is currently conducting security evaluations of RSA encryption that is widely used in internet shopping. In terms of the integer factorization problem that is the fundamental basis for RSA encryption's dependability, we succeeded in factorizing a 176 digit composite number using software in cooperation with universities and other institutions, to achieve a world record for the size of a factorized composite number. We were also the first in the world to develop a dedicated high-speed hardware unit for integer factorization, and succeeded in rigorously evaluating RSA encryption by using cryptanalysis technology with the highest performance that could be implemented using current technology. This result was able to confirm that 2048-bit RSA encryption will be safe for at least the next 10 years.

We also perform cryptanalysis experiments on the elliptic curve cryptography which is anticipated to replace RSA encryption. These results contribute to a smooth generational changeover of encryption technologies to ensure the security of encryption in the future.

We have also developed our own unique SC2000 encryption algorithm that offers high security and processing performance essential for building a electric government.

Encryption technology is advancing every day. Through these activities, Fujitsu Laboratories is greatly contributing to the safe usage of Fujitsu systems and products by accurately grasping the security and processing performance of encryption. Evaluation of encryption is only possible if you have the highest-level, leading edge cryptanalysis technology. Fujitsu Laboratories is also developing and maintaining encryption technology that can withstand such cryptanalysis technology, and is continuing to provide safe and practical encryption technology to our customers around the world.

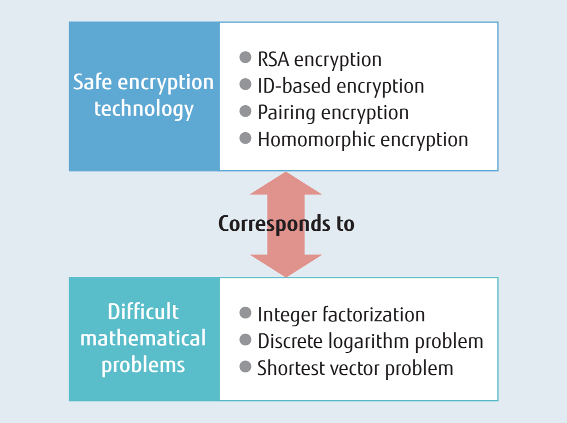
▼Fujitsu Laboratories approach to encryption technology

2000	Developed SC2000 symmetric key cryptography, which was added to the list of cryptography recommended for electric government of Japan
2005	World record integer factorization (176 digits)
2006	Developed dedicated hardware for integer factorization
2009	Experimented on cryptanalysis of elliptic curve cryptography and compared the strength with RSA cryptography
2012	World record for cryptanalysis encryption based on the discrete logarithm problem (278 digits)

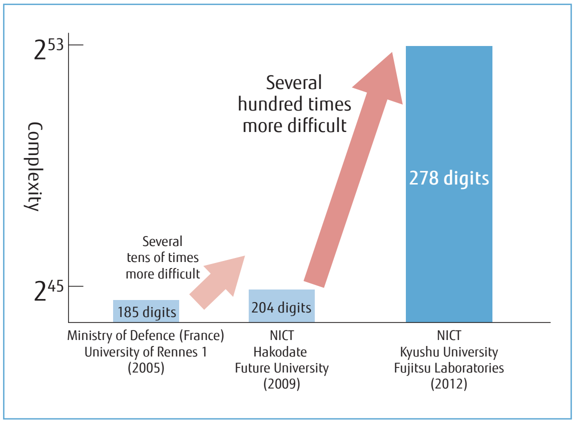
(1) Achieve world record - Breaking the discrete logarithm problem

We have conducted large-scale cryptanalysis experiments in cooperation with universities and other institutions on the discrete logarithm problem that is used as the basis for the security of encryption technologies that have drawn attention as the next generation of cryptography. Such new technology includes an ID-based encryption where the user ID can be used as-is as the encryption key and pairing-based cryptography that established a world record in 2012 by successfully breaking a 278-digit problem. (The previous record was 204 digits)

▼Mathematical problems and safety of encryption technology



▼World record for cryptanalysis encryption based on the discrete logarithm problem



(2) Processing concealed data - Homomorphic encryption

In the last few years, the new "homomorphic cryptography" encryption technology which can perform a variety of data processing and services on still-encrypted data has been gaining attention. Although homomorphic encryption has been expected to be applied to the cloud and other applications, claims that it is not practical have emerged, primarily because processing performance severely drops if security is too high. Fujitsu Laboratories has been developing homomorphic encryption that has sufficient security at practical speeds by implementing a variety of attacks such as "lattice attacks" on the "shortest vector problem" which is the cornerstone for security of homomorphic encryption, as well as checking its endurance against all currently known attacks.

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 supplier 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 that occur at the suppliers' location, there is a trend of reduced incidence with the introduction and thorough implementation of countermeasures in the following cases:

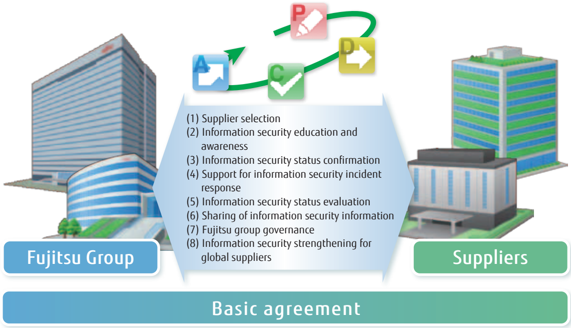
(1) Information leaks to the Internet by file sharing software

(2) Loss and theft due to carelessness

(3) Missending of e-mails and faxes

In fiscal 2011, measures were implemented in addition to existing measures to handle sudden changes in the environment, such as the spread of new technologies such as cloud services and smart devices, the expansion of global business, social networking services (SNS), and the growth of nomad workers.

▼Security improvement measures in cooperation with suppliers


P
D
C
A
(1) Supplier selection
(2) Information security education and awareness
(3) Information security status confirmation
(4) Support for information security incident response
(5) Information security status evaluation
(6) Sharing of information security information
(7) Fujitsu group governance
(8) Information security strengthening for global suppliers
Fujitsu Group
Suppliers
Basic agreement

(1) Supplier selection

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

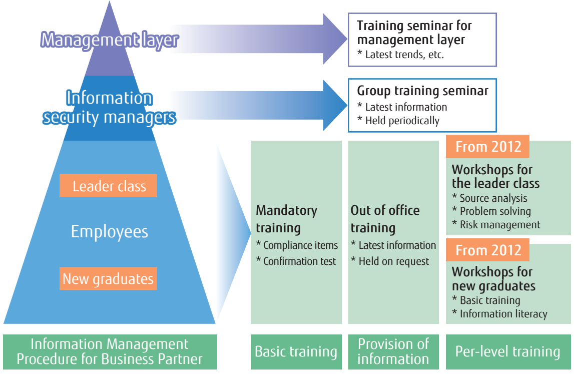
In addition, the Fujitsu Group supervises subcontractors entrusted with personal information and other suppliers with respect to the Act on the Protection of Personal Information.

(2) Information security education and awareness

In addition to education and awareness training aimed at subcontracted suppliers, we also strive for level-based education for reducing information security risks. Furthermore, 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.

▼Training and education system for suppliers

● Promotion of education by level and by purpose



■Conducting information security seminars for suppliers

Part one "Latest trends and countermeasures in information security"

- Case studies and features of recent information security accidents
- Points to note when cloud systems and smart devices are used for contracted business, and other topics

Part two "Basics and concepts for ensuring information security"

- Importance of ensuring information security
- Measures for ensuring adherence, and other topics

● November 2011 Approx. 1,300 people Approx. 1,100 companies

In the questionnaire results, approximately 99% answered affirmatively.

Furthermore, the education material was provided to suppliers.

パートナー様向け
情報セキュリティ研修会2011

第一部

情報セキュリティの最新動向と対策

2011年11月

富士通株式会社
ソリューション調達本部
パートナー総合センター
パートナー情報セキュリティ推進部

パートナー様向け
情報セキュリティ研修会2011

第二部

情報セキュリティ確保の基本と考え方

～ 形式より実効性 ～

2011年11月

富士通株式会社
ソリューション調達本部
パートナー総合センター
パートナー情報セキュリティ推進部

Conducting out of office training for suppliers

"The knowledge of pros in information security"
Instructors are dispatched to conduct training seminars for supplier employees at the request of suppliers

- Fiscal 2011 Approximately 60 companies and approximately 1,400 people received training

Information security training seminars are held for the management layer in the main suppliers for Fujitsu FSA (Fujitsu Software Association)

- Fiscal 2011 Held 4 times

Information security education inside Fujitsu

e-Learning was conducted on all employees with the aim of giving an understanding of the scope of behavior and thoroughly understanding information management. Furthermore, the same content is planned to be expanded to the group companies in fiscal 2012.

- Approx. 16,000 employees in October 2011

(3) 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 followup on corrective actions when a supplier experiences an information security incident.

- Fiscal 2011 audit about 150 companies (about 1,100 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

(4) 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.

(5) 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.

(6) 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.
- It has been issued 6 times in 2011, with the latest issue providing information such as points of caution regarding SNS. Furthermore, educational posters were provided to prevent information security accidents.

(7) Fujitsu Group Governance

In the Fujitsu Group, measures to strengthen the information security at our suppliers are promoted throughout the entire group.

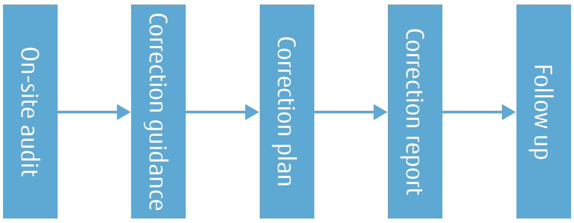
More effective preventative measures are implemented and promoted to suppliers by intra-group cooperation over each measure and by sharing information such as case studies of information security accidents.

(8) Strengthening information security in global suppliers

Recently, opportunities for offshore development through cooperation with global suppliers mainly in China have been growing with the aim of limiting development costs and supporting global products. Fujitsu is striving to maintain information security by exchanging "Information Management Procedure for Business Partner" with global suppliers that define the handling of entrusted information the same as for domestic suppliers.

Part of these efforts is to implement on-site information security auditing to check the state of handling of entrusted information in global suppliers. Furthermore, revision planning, guidance to implementation, and checking of revision planning are performed based on the results of the check. During audits, checks that include specific operations are conducted not only by the information security managers in each company, but also with the project managers and employees present.

- Fiscal 2011 audits 4 companies
- Main items audited
  - Management of working employees
  - Management of entrusted information (procurement, use, and disposal or return)
  - Management of devices that use removable media, etc.
  - Information security measures for development environments such as laptop computers
  - Room entrance and exit management
  - Periodic checking of information security status and mechanisms for improvement
  - Build a cooperative system with Fujitsu



Safe and Secure Solutions from Fujitsu

Safe and Secure Solutions from Fujitsu that Focus on the Age of the Cloud - SafetyValue

In recent years, companies have been demanding a new risk management architecture. The realization of this architecture requires increasing the business continuity by changing from businesses that pursue "selection and centralization" to "distribution and sharing", and at the same time requires a transformation into a business that ensures "efficiency". Fujitsu provides the "SafetyValue" safe and secure solutions that continue to support the businesses of our customers through ICT based on the concept of "the current need for sustainable businesses".

Features of SafetyValue

Aiming to Deliver Sustainable Business

The purpose of sustainable business is to maintain and improve future operations while aiming to deliver a sustainable society by establishing both environmental and economic activities. Fujitsu proposes optimal solutions for delivering sustainable business to our customers in terms of the three perspectives of "customer-oriented", "improved usefulness", and "environmental contribution".

■ Features of SafetyValue

- Customer-oriented

  Proposes the best solutions for resolving customer problems in terms of the three perspectives of business continuity, security, and energy.

- Improved usefulness

  Delivers an environment where information resources can be used efficiently while carefully protecting customer resources.

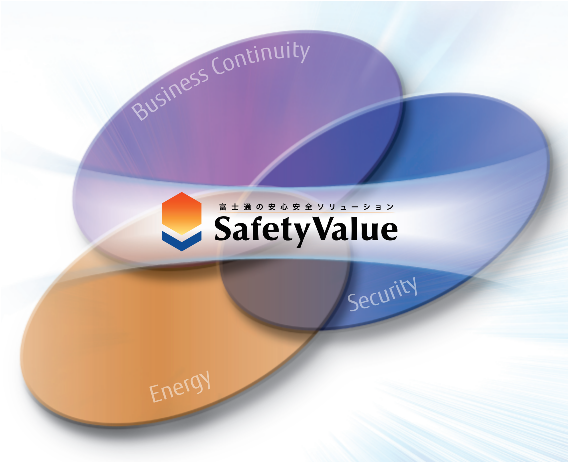
- Environmental contribution

  Assists with building an office environment that delivers diverse work styles and efficient management aiming for the most efficient use of energy.

"SafetyValue" solution framework

"SafetyValue" is built based on the three pillars of "business continuity", "security", and "energy" that originate from the business challenges of our customers. It also improves the convenience of safely and efficiently using information resources, and promotes building an office environment that offers both optimal usage of energy and a diverse range of work styles. This report introduces "security" related solutions.

▼ Three pillars for delivering sustainable business



Business Continuity

We provide a complete range of services including establishing and implementing business continuity planning and operational management, to support for continual improvement activities, and deliver robust business continuity measures. This utilizes our in-house hands-on expertise and the latest cloud computing technology provide powerful assistance for the business continuity efforts of our customers.

Security

We will propose the most appropriate solutions, not only for handling the new security risks that appear from virtualization and the move towards the cloud, but also for supporting innovation for better work styles improved productivity by ICT.

Energy

Proposes total solutions for establishing plans and increased transparency, to improvements in ICT for not only the business continuity and security in the company activities, but also efficiency of energy usage which requires consideration.

Thinking About Security in the Cloud Age

Solutions offered in the field of security

The next generation of information security measures for the age of the cloud must be examined by considering the effectiveness and efficiency of each security measure.

Fujitsu assists with the establishing of optimal information security governance based on the cost-effectiveness required when the customer invests in a corporate strategy.

We also provide information security measures that both protect customer information resources and improve usability with ICT, by providing solutions that handle a variety of security risks such as the information leak incidents that accompany the growing use of smartphones and tablets, internal crimes, and attacks over the internet.

Solutions for 14 Areas of Information Security (April 2012)

Security	
Security Controls	Supports the realization of "information security governance" in the organization based on continuous security measures from the perspective of overall company activities including ICT
Smart Device Security	Provides security measures that take an overall view of the systems required when utilizing smart devices for work.
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)
Thin Clients	Provides total coverage from dedicated thin client PCs, tablet PCs, and building network environments to virtualizing clients
Physical Security	Provides integrated resolutions for security products in the office through integration with authentication with palm vein patterns and IC cards, video compression technology, etc.

Fujitsu Cloud Security Solutions

Amongst the cloud services that attract attention, there is demand for security measures for systems that have been complicated by virtualization and integration. By migrating to the cloud, threats that are specific to the cloud (virtualized environment) have also emerged.

The Fujitsu Cloud offers a lineup of cloud security solutions from the three perspectives of "protecting the virtual environment from the outside", "protecting within the virtual environment", and "protecting using policies" for protecting against these threats.

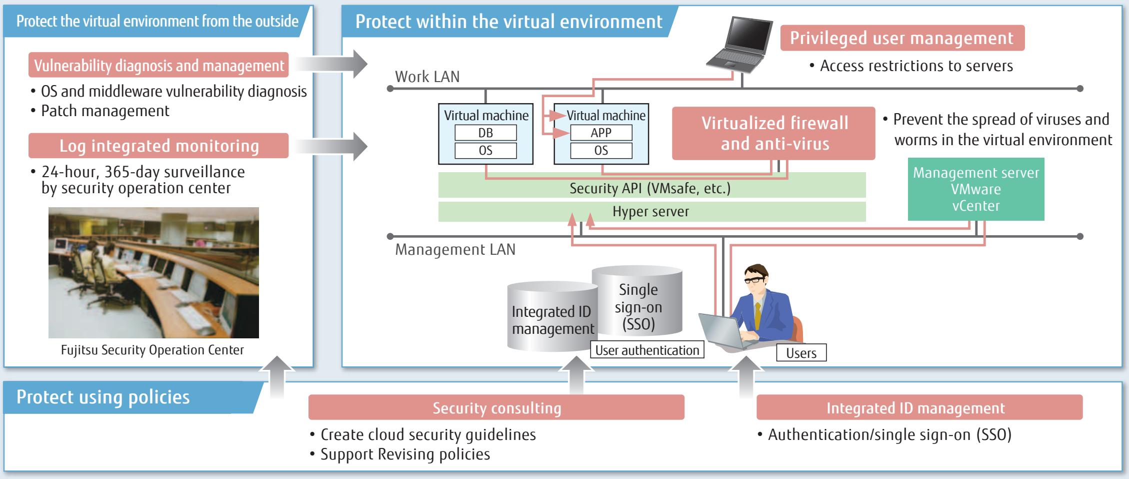
Fujitsu Cloud Security Measures - Three "Protections" -

Protection 1
Protect the virtual environment from the outside

Protection 2
Protect within the virtual environment

Protection 3
Protect using policies

Schematic diagram of the cloud (virtualized environment) security measures


Protect the virtual environment from the outside
Vulnerability diagnosis and management
• OS and middleware vulnerability diagnosis
• Patch management
Log integrated monitoring
• 24-hour, 365-day surveillance by security operation center
Fujitsu Security Operation Center
Protect within the virtual environment
Privileged user management
• Access restrictions to servers
Work LAN
Virtual machine
DB
OS
Virtual machine
APP
OS
Virtualized firewall and anti-virus
• Prevent the spread of viruses and worms in the virtual environment
Security API (VMsafe, etc.)
Hyper server
Management server
VMware
vCenter
Management LAN
Integrated ID management
Single sign-on (SSO)
User authentication
Users
Protect using policies
Security consulting
• Create cloud security guidelines
• Support Revising policies
Integrated ID management
• Authentication/single sign-on (SSO)

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.

FUJITSU LIMITED
FUJITSU ADVANCED ENGINEERING LIMITED
FUJITSU ADVANCED SOLUTIONS LIMITED
FUJITSU APPLICATIONS, LTD.
FUJITSU ADVANCED PRINTING & PUBLISHING CO., LTD.
FUJITSU HUMAN RESOURCE PROFESSIONALS LIMITED
AB SYSTEM SOLUTIONS LIMITED
FUJITSU FIP CORPORATION
FUJITSU FOM LIMITED
FUJITSU FSAS INC.
FUJITSU OKAYAMA SYSTEMS ENGINEERING LTD.*1
OKINAWA FUJITSU SYSTEMS ENGINEERING LIMITED
FUJITSU KAGOSHIMA INFORNET LTD.
FUJITSU KANSAI SYSTEMS LIMITED*1
FUJITSU KYUSHU SYSTEMS LIMITED
FUJITSU COMMUNICATION SERVICES LIMITED
FUJITSU COWORCO LIMITED
FUJITSU CIT LIMITED
G-SEARCH LIMITED
FUJITSU SHIKOKU INFORTEC LIMITED
FUJITSU SHIKOKU SYSTEMS LIMITED*1
FUJITSU SYSTEM SOLUTIONS LIMITED*2
FUJITSU RESEARCH INSTITUTE
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
FUJITSU SOFTWARE TECHNOLOGIES LIMITED
FUJITSU CHUGOKU SYSTEMS LIMITED*1
FUJITSU CHUBU SYSTEMS LIMITED*1
TOTALIZATOR ENGINEERING LIMITED
FUJITSU TRAVELANCE LTD.
FUJITSU TOHOKU SYSTEMS LTD.*2
TOYAMA FUJITSU LIMITED
FUJITSU NAGANO SYSTEMS ENGINEERING LIMITED*2
FUJITSU NIIGATA SYSTEMS LIMITED
FUJITSU NISHI-NIHON APPLICATIONS, LTD.*1
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*2
FUJITSU MARKETING LIMITED
FUJITSU YAMAGUCHI INFORMATION CO.,LTD
UCOT CORPORATION
FUJITSU LEARNING MEDIA LIMITED
LIFEMEDIA, INC.
FUJITSU YFC LIMITED

*1: Became Fujitsu Systems West Limited from 1st April 2012.
*2: Because Fujitsu Systems East Limited from 1st April 2012.

ISMS Certification

Fujitsu and Fujitsu Group companies that have organizations that acquired the ISMS certification based on International Standards ISMS (ISO/ IEC 27001) for Information Security Management Systems 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 LTD.
FUJITSU KANSAI-CHUBU NET-TECH LIMITED
FUJITSU KYUSHU SYSTEMS LIMITED
FUJITSU COMMUNICATION SERVICES LIMITED
FUJITSU SHIKOKU SYSTEMS LIMITED*3
ZIFTEC
FUJITSU SYSTEM SOLUTIONS LIMITED*4
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
FUJITSU RESEARCH INSTITUTE
FUJITSU CHUBU SYSTEMS LIMITED*3
FUJITSU DEFENSE SYSTEMS ENGINEERING LIMITED
FUJITSU TOHOKU SYSTEMS LTD.*4
FUJITSU NAGANO SYSTEMS ENGINEERING LIMITED*4
NIFTY CORPORATION
FUJITSU NETWORK SOLUTIONS LIMITED
FUJITSU PUBLIC SOLUTIONS LIMITED
FUJITSU BROAD SOLUTION & CONSULTING INC.
PFU LIMITED
FUJITSU MARKETING LIMITED
FUJITSU MISSION CRITICAL SYSTEMS LTD.
FUJITSU MIDDLEWARE LIMITED
FUJITSU MOBILE-PHONE PRODUCTS LIMITED
FUJITSU LEASING CO., LTD.
FUJITSU YFC LIMITED

*3: Became Fujitsu Systems West Limited from 1st April 2012.
*4: Became Fujitsu Systems East Limited from 1st April 2012.

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	AAA_{is}
FUJITSU FIP CORPORATION	Yokohama Data Center	AAA_{is}
	Chubu Data Center	AAA_{is}
	Kyushu Data Center	AA^{+}_{is}
FUJITSU FSAS INC.	Tokyo LCM Service Center	AA_{is}
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED	Software Service Department	A^{+}_{is}
PFU LIMITED	Applies to entire company	A^{+}_{is}

IT Security Evaluation Certification

Following representative ICT 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)

Note: For details, inquire separately.

ISMS Auditors

The Japan Information Processing Development Corporation (JIPDEC) began full operation of an information security management system (ISMS) compliance evaluation system within Japan from 2002. Within Japan, the personnel certification institutions that register evaluations of auditors are the Japanese Registration of Certificated Auditors (JRCA) and IRCA Japan (International Registration of Certified Auditors).

The certification classifications for auditors include "ISMS Lead Auditor", "ISMS Auditor", and "ISMS Provisional Auditor". In Fujitsu and group companies, certified auditors are active in internal audits within our company and information security consulting work at the request of our customers. The number of people who hold ISMS auditor certifications in Fujitsu and group companies is as follows.

<qualified ISMS auditor number: 136>

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: 141>

FUJITSU LIMITED
Information Security Center

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

This Brochure was produced by waterless printing and utilizes VEGETABLE OIL INK on FSC®-certified Paper.