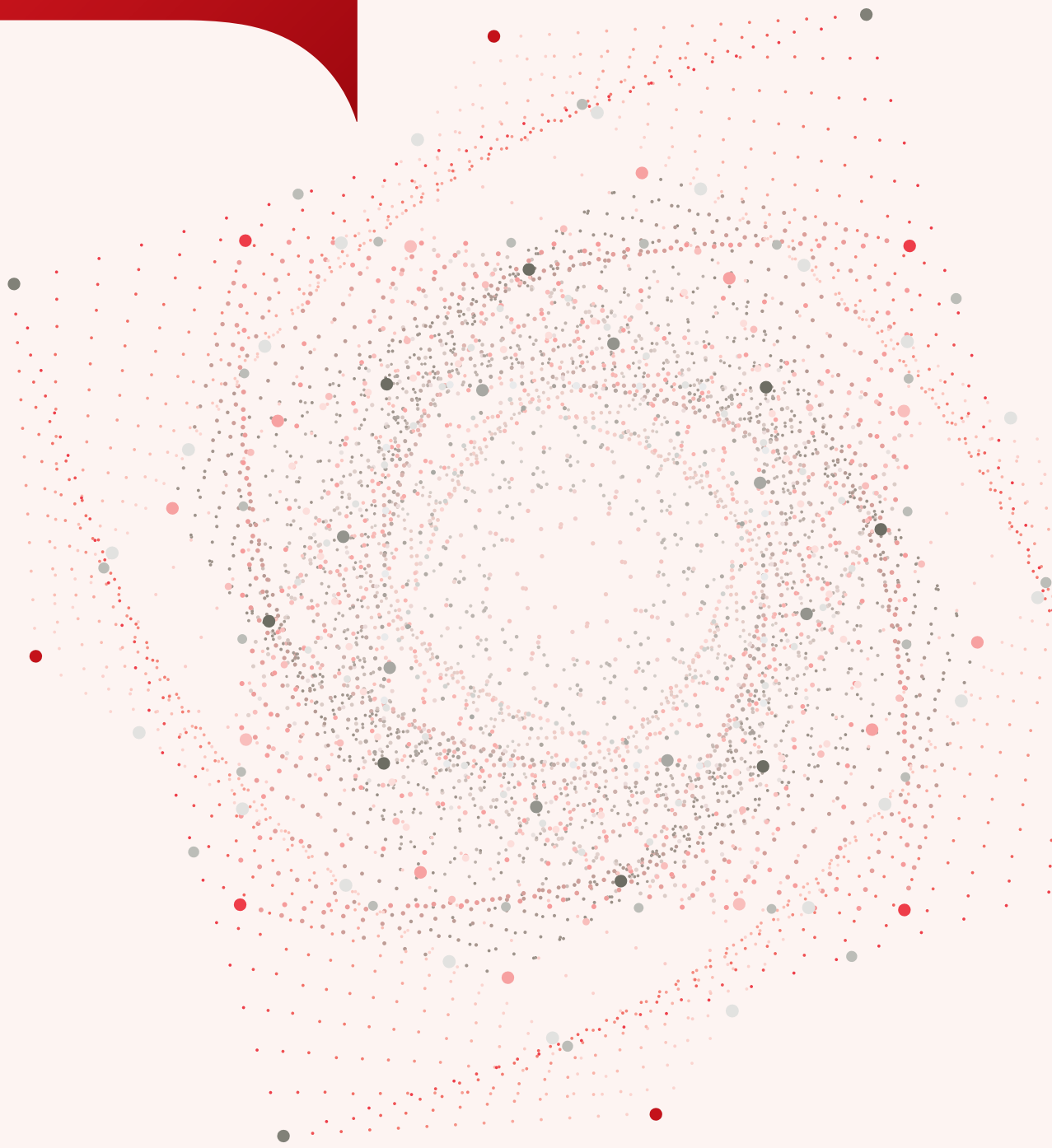
Fujitsu Group Information Security Report 2016

FUJITSU



shaping tomorrow with you

CONTENTS

Fujitsu Group Information Security Report 2016

Report Summary

Target Period and Scope of the Report

This report covers the period up to March 2016 and focuses on efforts in information security by the Fujitsu Group.

Report Publication Date

This report was published in August 2016.

Cover design: the design is a graphic visualization of the annually increasing traffic volume of big data, expressing the growing need for information security.

Fujitsu Information Security: Our Vision and Reality

"Creating a safe, pleasant, networked society" and Information Security

The Fujitsu Group established the "FUJITSU Way" as the Group's philosophy and principles. We are strongly aware of the change in the role and responsibility of the corporation in society, and established the following corporate philosophy to indicate the significance of the existence of the Fujitsu Group.

Corporate Vision

Through our constant pursuit of innovation, the Fujitsu Group aims to contribute to the creation of a networked society that is rewarding and secure, bringing about a prosperous future that fulfills the dreams of people throughout the world.

ICT (Information and Communication Technology) connects the world's people and creates a variety of ideas and opportunities. On the other hand, we are confronted by new issues due to the rapid proliferation of ICT. Preparation against the increasing number of cross-border cyber-attacks and assured protection of private and confidential information are items companies and organizations should respond to urgently. At the Fujitsu Group, we use technologies nurtured through our own systems operations as a base for responding to these types of problems while collaborating with a variety of related organizations.

The Fujitsu Group has a vision of a "Human Centric Intelligent Society" where anyone can use ICT to draw out their maximum potential in a safer, more abundant, sustainable society. We think it is our social responsibility as a global ICT company to use the power of ICT to contribute to the realization of a sustainable earth and society and maintain and reinforce a safe and secure digital society.

Guided by this vision, we in the Fujitsu Group observe internal rules based on the FUJITSU Way Code of Conduct to ensure correct management and use of data. At the same time, to make sure we maintain confidentiality as a key aspect of our social responsibility, we have established the "Fujitsu Group Information Security Policy," which applies both in Japan and internationally, and are working to promote information security.

Furthermore, the Fujitsu Group also has a unified information security management system in place to thoroughly manage information and enhance information security. On the other hand, given that we are developing businesses across an expansive range of fields, we have also put in place an information security management system at the business division level. This is to ensure that we can swiftly address varying information management and information security issues, as required by the characteristics of individual businesses.

This "Information Security Report 2016" presents the Fujitsu Group's information security-related activities. We trust that this report will give you a stronger understanding of our commitment to information security.

Tatsuya Tanaka

Representative Director
President
Fujitsu Limited

Fujitsu Group's Information Security

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

Corporate Governance and Risk Management

Corporate Governance

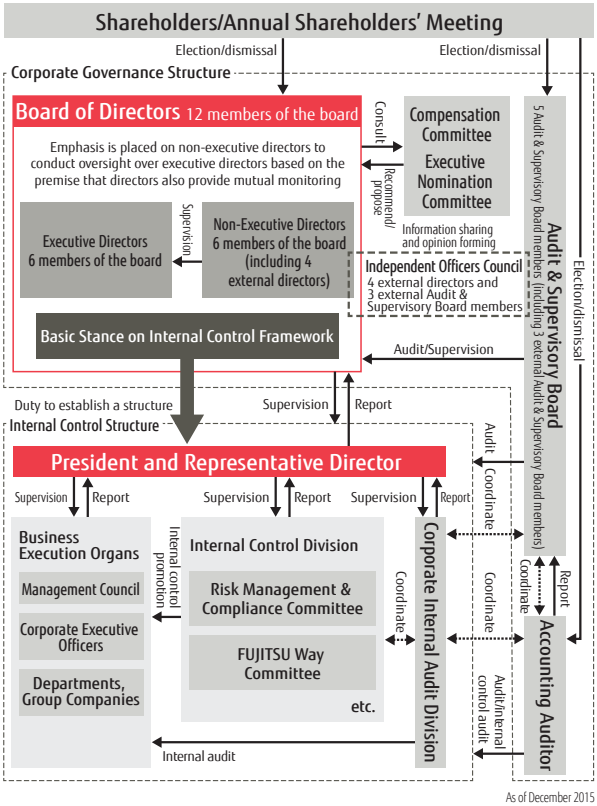
The main emphasis of Fujitsu's corporate governance is on having the non-executive directors provide oversight and advice to executive directors in their management execution role within the Board of Directors, while adopting the Audit & Supervisory Board system.

Specifically, while assuming mutual supervision between directors and oversight of directors by the Board of Directors, Fujitsu makes a clear distinction between the management execution role and the management oversight role on the Board of Directors and, moreover, makes sure that there are at least as many non-executive directors responsible for management oversight as there are executive directors responsible for management execution.

In addition, in selecting candidates for non-executive directors, consideration is given to the candidate's backgrounds and insight into Fujitsu's business so that effective advice that reflects a diversity of viewpoints can be obtained.

Furthermore, Audit & Supervisory Board members provide audits and oversight from the outside of the Board of Directors, and Fujitsu has established the Executive Nomination Committee, the Compensation Committee, and the Independent Officers Council of its own accord, thereby augmenting the Board of Directors. The overall approach is designed to raise corporate value through effective corporate governance.

Corporate Governance Structure

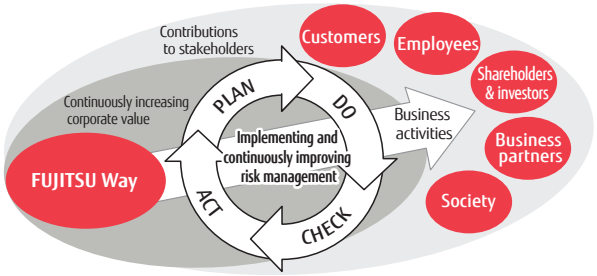


As of December 2015

Risk Management

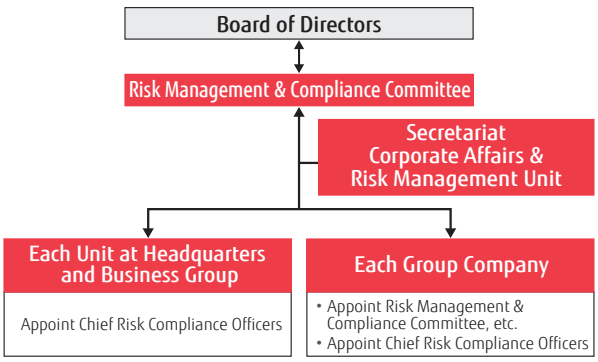
Through its global activities in the ICT industry, the Fujitsu Group continuously seeks to increase its corporate value, and to contribute to its customers, local communities and all other stakeholders. Management places a high priority on properly assessing and dealing with risks that threaten the achievement of our objectives, taking steps to prevent the occurrence of these risk events, and establishing measures to minimize the impact of such events if they do occur, and prevent their reoccurrence. Moreover, we have built a risk management and compliance system for the entire Group and we are committed to continuously implementing and improving it.

Implementing and Continuously Improving Risk Management



With the aim of integrating and strengthening its global risk management and compliance structures, the Fujitsu Group has established a Risk Management and Compliance Committee as an internal control committee that reports to top management. The Risk Management & Compliance Committee appoints a Chief Risk Compliance Officer for each department and company throughout the Group, and encourages them to cooperate together both to guard against potential risks and to mitigate risks that materialize, thereby forming a risk management and compliance structure for the entire Group.

Risk Management & Compliance Structure



Promotion of Information Security

Ensuring Information Security

Bearing in mind that ICT constitutes a fundamental part of the Fujitsu Group's business, the Fujitsu Group maintains information security throughout the Group and also proactively strives to maintain and improve its customers' information security through Fujitsu's products and services, and thereby contributes to the Corporate Philosophy that articulates our desire for "a network society that is rewarding and secure."

■ Fujitsu Group Information Security Policy

Fujitsu has newly established the "Fujitsu Group Information Security Policy" to conform to the "Cybersecurity Management Guidelines" announced in December 2015 by Japan's Ministry of Economy, Trade and Industry and the Information-Technology Promotion Agency. The Fujitsu Group Information Security Policy is a global security policy that covers the entire Fujitsu Group, in accordance with decisions made by the Risk Management & Compliance Committee that reports directly to the Board of Directors.

Fujitsu Group Information Security Policy (Excerpt) (Global Security Policy)

I. Purpose

The purpose of this Fujitsu Group Information Security Policy (this "Basic Policy") is to set forth basic matters, such as measures and frameworks, regarding Fujitsu Group's information security in accordance with the "Cybersecurity Management Guidelines" formulated by the Ministry of Economy, Trade and Industry of Japan, as well as to declare, both internally and externally, that the Fujitsu Group will not only maintain the information security throughout the Group but also proactively strive to maintain and improve our customers' information security bearing in mind that ICT constitutes a fundamental part of Fujitsu Group's business, and thereby implements the Corporate Philosophy set forth in FUJITSU Way.

● Fujitsu Group Information Security Policy (Full Text)
http://www.fujitsu.com/global/about/csr/management/security/

■ Information Security Organization

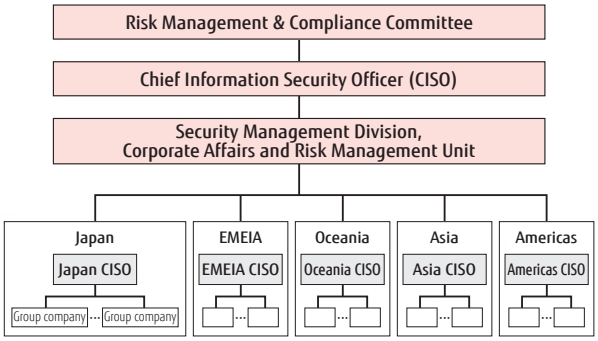
In order to further strengthen its security measures in response to the recent trend of increasingly numerous and sophisticated cyber attacks, Fujitsu has appointed a Chief Information Security Officer (CISO) under the Risk Management and Compliance Committee and has reviewed its security organization structure, thereby ensuring the establishment and implementation of information security measures.

Varied Measures to Ensure Information Security

In accordance with the Fujitsu Group Information Security Policy, Fujitsu not only establishes internal policies and procedures and conducts employee training, but also proactively takes advantage of ICT in order to maintain and improve its information security globally.

In addition, Fujitsu has expert teams to appropriately respond to information security incidents.

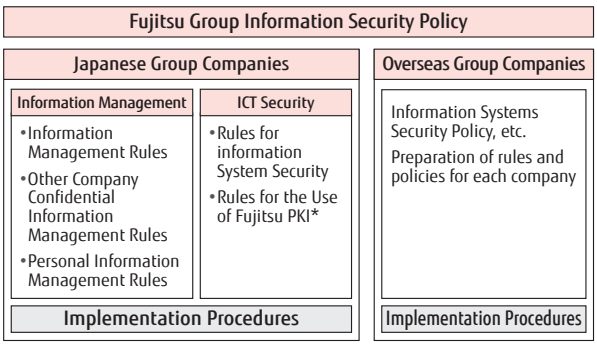
〓 Information Security Organization



■ Establishment of Internal Policies and Procedures

Each Fujitsu Group company establishes its internal policies and procedures regarding information management and ICT security based on the "Fujitsu Group Information Security Policy" and implements information security measures accordingly.

〓 Framework of Information Security Rules



* PKI (Public Key Infrastructure): Rules relating to the use of systems for personal identification and encoding.

■ Training and Raising Awareness Regarding Information Security

Since FY 2008, the Fujitsu Group has promoted a common slogan "Declaration for thorough information management! Information management is the lifeline of the Fujitsu Group."

Fujitsu Limited and its domestic group companies have been working to increase information security awareness at the individual employee level by displaying posters at respective offices and affixing information security awareness stickers to all business PCs used by employees. Furthermore, e-Learning courses are held for all our employees, including executives, every year in order to further establish information security awareness.

Similarly, measures such as employee training are continuously conducted at overseas group companies in order to raise employee awareness regarding information security.

The sticker affixed to business PCs

■ Enhancing Security with ICT

Fujitsu has also taken steps to enhance security by utilizing ICT. For example, Fujitsu has introduced a tool called "ShieldMailChecker," developed by Fujitsu Social Science Laboratory Limited, to all domestic group companies in order to prevent information leakage caused by erroneous email transmission to external parties.

■ Activities by Information Security Promoting Organizations at the Business Group Level

Business units and group companies that provide system integration services within the Fujitsu Group have established information security promoting organizations, which implement a higher level of information management and enhanced security.

Many of these organizations have actively obtained ISMS (Information Security Management System) certification*1 (43 organizations certified as of June 2016), and promote secure management of confidential information such as customer data.

■ Responding to Cyber Attacks

In order to maintain the security of the Fujitsu Group's globally integrated intranet, Fujitsu monitors its network 24 hours a day, 365 days a year, through its GSOC (Global Security Operation Center), which is comprised of security teams at main offices around the world. Information security incidents, such as malware infection, will be reported promptly to the administrator located at the source of the incident with instructions regarding risk elimination, and appropriate countermeasures will be planned. Furthermore, Fujitsu coordinates with external organizations such as government ministries and agencies in order to work together on early detection and resolution.

In addition, newly developed systems will undergo prior review by our security control division in accordance with relevant information security policies to ensure that adequate measures are taken against cyber attacks and any issues are resolved.

■ Information Security Presentation for Business Partners

As a result of dramatic changes in the ICT environment in recent years, the risk of information leaks has never been higher. In response, the Fujitsu Group has held information security presentations not only for Group employees but also for domestic business partners to which we outsource software development and services, and has worked to share information on challenges and to thoroughly implement prevention measures.

- Example of presentations held in FY 2015
  http://www.fujitsu.com/global/about/csr/activities/society/procurement/

Personal Data Protection Initiatives

Fujitsu has established the "Personal Data Protection Policy" and "Rules for Management of Personal Data." Based on these rules, we give training on how private information should be handled and carry out surveys in an ongoing effort to strengthen the protection given. In August 2007, we acquired company-wide PrivacyMark*2 certification and have since renewed this certification every two years. Domestic Group companies are also acquiring PrivacyMark certification individually as necessary and are 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 websites.

*1 ISMS (Information Security Management System) certification: A system for verifying compliance with the ISO/IEC 27001 international standard for information risk management.

*2 PrivacyMark: A certification system relating to the handling of private information, The system is operated by the Japan Institute for Promotion of Digital Economy and Community.

IT Security Efforts

In situations where ICT is applied, a large volume of data related to business is collected and made easily accessible. This is accompanied by various risks such as the risk of information being leaked, damaged, or unavailable.

For this reason, the Fujitsu Group has positioned IT security, which seeks to ensure the secure management of information when using ICT, as a common Group-wide theme, and is working towards this end.

Pursuing IT Security to Support Business Operations

At the Fujitsu Group, IT security aims to support business operations, without interfering with the convenience or efficiency of business.

If rules for information security measures are too excessive, employees will struggle to understand and observe them, making compliance impractical.

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

In addition, security threats are constantly changing in step with advancement in ICT. To maintain effective measures against such threats, we believe that cutting-edge technology is needed to develop and implement technical measures, as well as to analyze and address problems. To this end, we have put in place a dedicated team of IT security specialists.

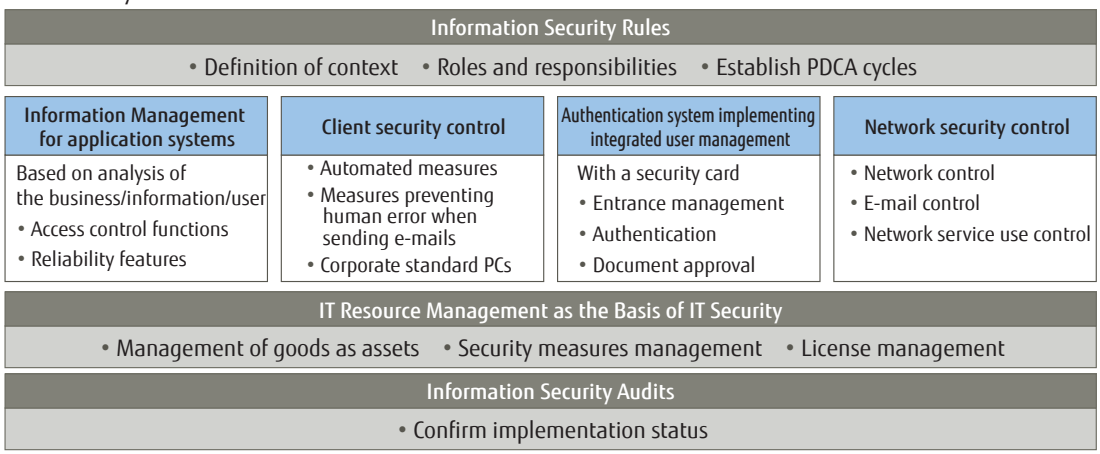
In addition, technical countermeasures developed and implemented are put into practical application and tested for effectiveness and efficacy before being presented to customers and fed back in products*.

* Products include FENICS II Universal Connect

IT Security Framework

The Fujitsu Group implements IT security measures based on IT security-related rules. For each measure designed according to the context of information use, there are information management functions for business systems, client security controls, integrated user management authentication systems, and network security controls. IT resource management is the foundation of all these elements. Furthermore, IT security audits are conducted to entrench and improve on these measures.

IT Security Framework



IT Security-Related Rules

Fujitsu's IT security-related rules have the following three features, as set forth in Items 1–3 below.

1. Definition of context

The main contexts for ICT use are listed below. The IT security-related rules stipulate IT security measures that must be implemented in each context.

- Business systems that accumulate and process business information mainly on servers
- Offices and other worksites where PCs and other equipment are used
- Intra- and inter-office networks

2. Roles and responsibilities

The rules establish roles and responsibilities with respect to implementing IT security measures, and designate individuals responsible for implementing those measures in each business system and department. The rules also stipulate the authority of divisions supervising the implementation of measures.

3. Establish PDCA cycles

The rules govern the elements that compose each part of the PDCA cycle, including implementation of IT security measures, awareness-raising and education, promotion, incident response, evaluation and improvement in a bid to entrench and improve the measures.

Information Management in Business Systems

The Fujitsu Group uses ICT in a variety of operations, including finance and accounting, human resources and general affairs, sales, purchasing, systems engineering operations, production and logistics, and product development management. The information maintained and handled has security requirements that vary according to task and responsibility. By analyzing these requirements, we have implemented and applied an access control feature to control access to information based on the user's position and qualifications, and a reliability feature to meet the importance and continuity requirements of the business.

Client Security Control

An important information security issue is how human errors can be effectively dealt with. Relying only on human attentiveness in using ICT applications will not necessarily prevent information security incidents. Of course, education and awareness programs should be employed to draw attention to information security, but even then, information leakage and other incidents will occur beyond the reach of the ICT-based measures.

Based on this reality, we focused on the client business processes involving human action, and replaced the measures dependent upon human attentiveness with ICT enabled solutions after checking for feasibility.

■ Automated security measures for PCs

Application of security patches and updates for operating systems, applications, and virus definition files are automated.

■ Measures to prevent human error when sending e-mails

Information leakage can easily result from sending an e-mail or attachment to an incorrect e-mail address. To reduce the risk of information leakage, e-mail addresses are automatically checked, and the sender is required to reconfirm when e-mails are addressed to external persons.

■ Introduction of Fujitsu standard PCs

Corporate standard PCs are those with identified models and specifications for internal corporate use. PCs with installed security measures, such as hard disk encryption, preset BIOS passwords, preset screen savers, installed resource management software, and installed anti-virus software, are issued to all departments. In doing so, PC model selection, installation, and operation become standardized and there is a reduction in costs. This frees users from the responsibility of implementing security measures and aids the success of such measures.

■ Safe use of client devices outside the office

Client devices such as PCs and smartphones can be used outside the office, such as at home or while out on business. Such remote access raises the risk of information leaks if the device is stolen or lost, therefore, it's an important objective to thoroughly inform employees of cautionary practices regarding remote devices through monthly "Security Check Days" and annual information security training.

ICT measures that could be introduced include a "Virtual Desktop Service" and "Smart Device Application," which protect against information withdrawal and keep important information secure when accessed through a remote client device.

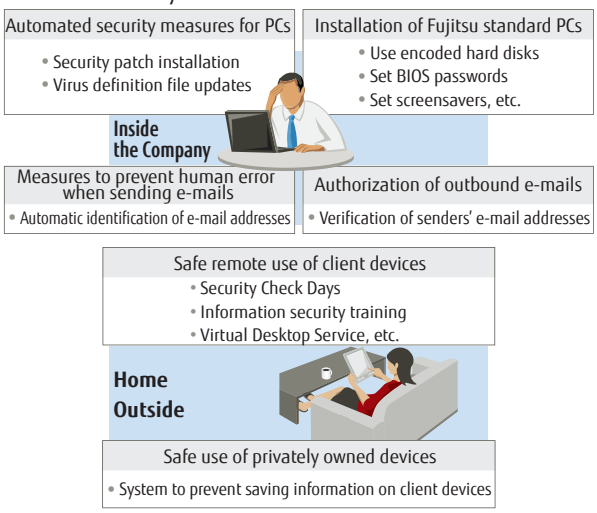
■ Safe use of privately owned devices (PCs, smartphones, etc.)

The Virtual Desktop Service and FENICS II Universal Connect are employed to enable safe use of privately owned devices like PCs and smartphones. These services ensure that internal information displayed on client devices cannot be saved on the devices to avoid the collection or leaking of confidential information due to user carelessness. Using this system with a personal device from home means that personal information and the internal network connection are separated within the device, ensuring the safe management of work information.

■ Management of e-mails sent outside of the Company

This system confirms whether a sender is authorized to send e-mail outside of the Company. It also prevents users who do not need external e-mail communication from sending e-mail to outsiders, thus preventing leakage of information.

Client Security Control



IT Resource Management as the Basis of IT Security

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

The IT Resource Management System maintains the following information.

■ Hardware resources: server and PC models, specifications

■ Software resources: software and software versions used on each server and PC

■ Application status of security patches

By managing software and software versions, the installation of software matching the license agreement is automated. In addition, the administrator can view the status of software resources and progress of security patch installation and instruct on remedial actions.

The IT Resource Management System is built on Systemwalker Desktop Patrol, a security management product of the Systemwalker family of integrated operation management software products, and integrates management of IT resources, security status, and software licensing.

Authentication System Implementing Integrated User Management

The Fujitsu Group provides each employee with an IC card, called a "Security Card," for authenticating employees and for other applications.

The name and a photograph of the employee are printed on the face of the Security Card. In addition, the IC chip stores the name, employee number, and employee PKI (Public Key Infrastructure) certificate and key. This data is unique for each employee in the Fujitsu Group.

Because the Security Card is managed by the Human Resources Division and is issued at hire and returned at termination or retirement, the user is guaranteed to be a legitimate employee. In addition, the card is invalidated if lost to prevent abuse.

The primary applications of the Security Card are as follows:

Entrance management

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

Authentication

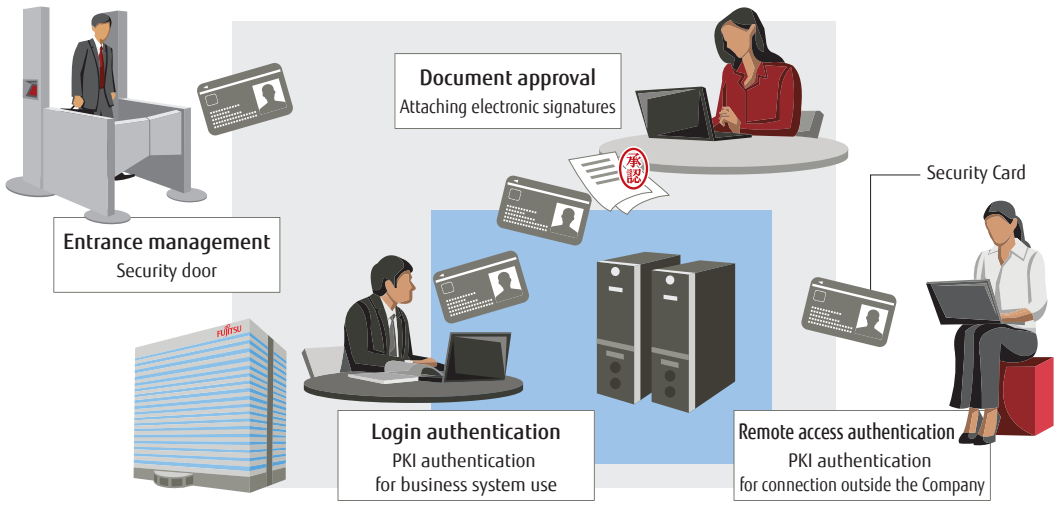
Employees are required to use the Security Card when accessing business systems that require authentication. Authentication by PKI at login to business systems enables secure identification and authentication of employees along with simple operation.

Business systems can also be accessed from off premises, e.g., on business trips. In this case, the remote connection is authenticated by PKI, and the employee is securely identified.

Document approval

The Security Card is also used in approval of electronic documents. Approvers use the PKI feature to add their electronic signatures to the electronic documents. This action indicates that the approver has confirmed and approved that document and has the same effect as affixing an approval seal to a paper document.

Using the Security Card



Network Security Control

The Internet is indispensable to business as a means for business communication, for publicity and information provision, and for utilizing the large amount of external information. On the other hand, the serious threats originating in the openness and mechanisms of the Internet cannot be ignored. At the Fujitsu Group, a team of specialists armed with the latest technologies creates measures to combat these threats and conducts integrated management of Internet gateways across the globe with the aim of minimizing the burden on employees and ensuring security.

Network control

The following policies are in place for the network.

- Control of Internet connections and intranet construction and operation
  - Installation and operation of gateway systems, such as firewalls, by a team of experts
  - Screening and authorization of individual connections in business groups
- Maintaining security during operation
  - Measures against unauthorized access (server configuration, checking the status of device management, and monitoring and preventing unauthorized transmissions)
  - High availability measures including performance management and dependable system design
- Support for mobile devices
  - Implementing and operating a secure business environment for using remote PCs and smart devices* to access the intranet

  * Smart devices: Smartphones and tablets
- Adapting to shifting threats
  - Analyze trends, gather information and formulate countermeasures against new threats that are difficult to address with existing techniques, such as targeted e-mail attacks and Advanced Persistent Threat (APT)
  - Research on attacking techniques and responses
  - Awareness and training programs for users

Controlling e-mail servers

E-mail is currently indispensable for business execution. The following measures are in place for managing e-mail security.

- E-mail control
  - Installation and operation of e-mail servers by a specialist team
- Maintaining security during operation
  - Anti-virus measures
  - Anti-spam measures
  - High availability measures including performance management and dependable system design

Network service use control

The Internet environment outside the Group provides many network services such as file transfer and online meetings. Use of these services is selectively approved with necessary conditions based on the evaluation of business merits and requirements and improved client security controls. On the other hand, use of specific network services identified to have risks of information leakage is prohibited. In addition, to prevent accidental use, communication using these services is continually monitored.

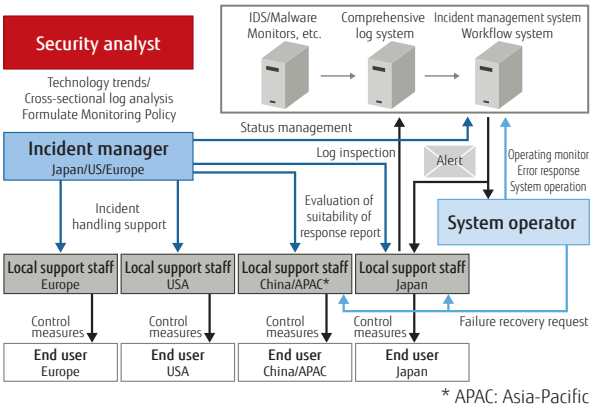
Intranet use control

The Fujitsu Group controls its intranet use because it recognizes that control of intranet use is an important factor of global controls under the "Fujitsu Group Information Security Policy." A priority information security measure is to attain and maintain common security standards regardless of country or territory. Consequently, intranet construction and use in Group companies worldwide are controlled based on security measures, common policies and management measures.

The Security Operation Center (SOC) conducts global control, supports the single global intranet and handles network incidents. Hundreds of millions of network alerts are detected daily among Group companies worldwide. We respond to these rapidly, determining their risk level and whether to handle them as an incident. Characteristics of the alerts are as follows:

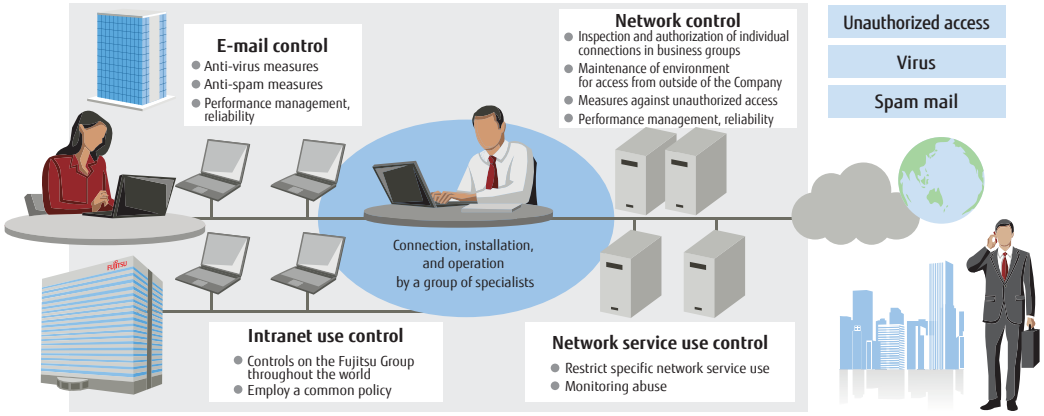
- Globally standardized risk guidelines and response processes
- Automatic evaluation of large volumes of data or logs
- SOC technicians stationed in all areas enable 24-hour response regardless of time zones
- Shorter response time due to a workflow system supporting connections between the incident manager and system operator
- Threat detection and new policy formulation conducted by specialist security analysts

SOC: Network Incident Handling



* APAC: Asia-Pacific

Network Security Control



IT Security Audits

An Audit Division, independent of the divisions implementing the foregoing IT security measures, performs audits of IT security measures based on an audit plan for a given fiscal year. The audits are conducted based on methods appropriate to the audit's target. Methods include having the auditor conduct an on-site visit to visually confirm the management status of devices and settings, inspecting reports on the results of inspections carried out by the divisions implementing IT security measures, and inspecting technical vulnerabilities via the network. The audited divisions use the audit findings to improve IT security measures.

Fujitsu Group Initiatives for Sound Protection of Customers' Information Assets

The organizations and Group companies in the Fujitsu Group that provide system integration service are called upon to maintain an even higher level of information management than the rest of the Fujitsu Group because they have many more opportunities to handle customer information assets and personal data. That is why Fujitsu's Information Security Council Secretariat (Council Secretariat) provides its information security management system based on a security management framework to all related organizations and Group companies. Related organizations and Group companies apply the framework and promote policies.

Our Approach to Establishing an Organization to Promote Information Security

Cyber-attack threats have become sophisticated and diversified, resulting in global debate about various types of business regulations. Consequently, Fujitsu launched the Security Steering Committee in 2013 to share information on cyber security and discuss our business policies.

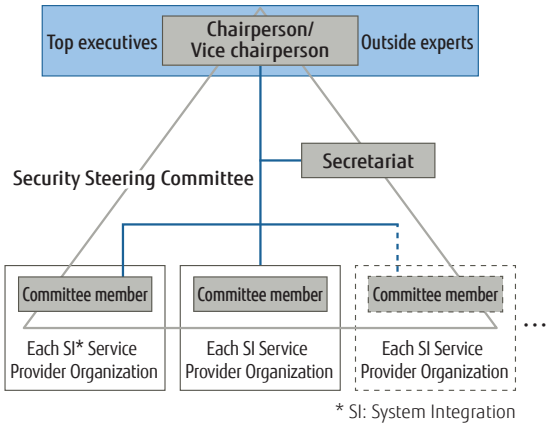
The Security Steering Committee is comprised of directors overseeing the various businesses undertaken by the System Integration Service Business; directors in charge of Japanese sales, marketing, and overseas sales divisions; and outside experts called upon to ensure impartiality.

Fujitsu abides by the principles of the "Fujitsu Technology and Service Vision." Reliability of information is important for a "Human Centric Intelligent Society," so it is vital to create a system where information utilization can continue on the assumption that accidents happen. The committee discusses and approves policies for projects requiring a global-level response, starting with countermeasures to the threat of cyber-attacks and observance of laws governing international cloud centers, as well as handling personal information.

The Security Steering Committee promotes activities to enhance the security quality of Fujitsu's system integration and services. The committee is a substructure of the Information Security Council (Council), which decides on the direction of the Fujitsu Group's security activities and is one of the Information Security Policy participating organizations (participating organizations).

In addition, the committee promotes security personnel training for system integration and services for the entire Fujitsu Group.

Security Steering Committee Structure



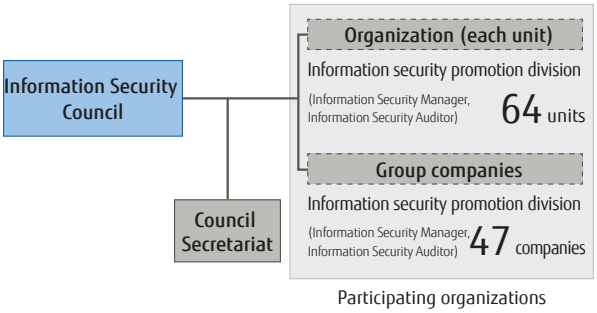
* SI: System Integration

Development and Execution of Security Governance

Targeted attacks on specific corporations and groups, website attacks, and personal information leaks have been increasing even further in recent years. This has created the need to implement risk management from a corporate management perspective. To this end, Fujitsu is pressing ahead with security initiatives under information security governance.

The System Integration Service Provider Organization and Group companies take part in the Council. Participating organizations formulate security plans, introduce security measures, promote information security activities and conduct internal audits based on the Security Management Framework (SMF; See the next page for details). They also strive to improve the management framework and security measures by confirming and evaluating the status of daily information security activities and security incidents and accidents.

Information Security Council Structure



Participating organizations

Information Security Management Promotion System

Participating organizations have established the "Information Security Council Activities Guidelines" with the goal of sound protection of customer and internal information to better handle information including customer information assets and confidential information. Based on these guidelines, participating organizations maintain and promote information security. Quarterly promotion meetings are held for information security managers and information security auditors from participating organizations to exchange information and opinions on security policies. The head of the participating organizations shall be the person responsible for promoting information security.

Furthermore, the Council Secretariat provides participating organizations with various assistance, as necessary, including support for effective measures and advice on enhancement initiatives needed to promote information security activities. This promotes the continuation of information security activities among participating organizations.

Conversely, each participating organization promotes the information security activities stipulated by the Council and maintains information security standards.

SMF (Security Management Framework)

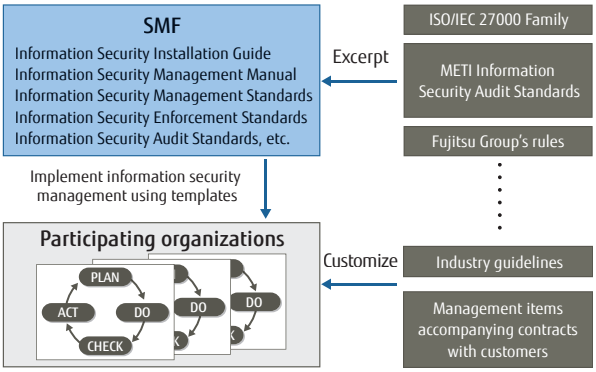
The Council Secretariat provides participating organizations with the SMF as a template to implement information security management. The SMF incorporates the ISO/IEC 27000 family, the Ministry of Economy, Trade and Industry (METI) Information Security Audit Standards, and other Japanese and international standards, in addition to the Fujitsu Group's rules. The SMF consists of documents on the information security management system and the information security audit system. When carrying out their operations, participating organizations must follow the customers' industry guidelines and fulfill the security requirements such as items regarding management in their contract with the customer. Each participating organization uses the SMF template to prepare its own information security-related documents and subsequent operations.

The SMF takes steps to respond to recently increasing cyber-attack risks and information leak risks from unauthorized internal activity by following the latest security countermeasure standards and extending their scope. The SMF draws on all manner of rules and guidelines related to information security controls that have been announced around the world, based on the regulations of the Fujitsu Group, thereby maintaining a consistent level while promulgating them through all participating organizations.

As an example, in handling the Social Security and Tax Number System that was officially implemented from 2016, Fujitsu Group has prepared its own guidelines and check sheet to enable participating organizations to formulate detailed rules for meeting the requirements for handling the system.

The relationships between the SMF, Fujitsu Group's rules, international standards, industry guidelines, and so forth are shown in the following diagram.

Relationship between the SMF and Fujitsu Group's Rules, International Standards, Industry Guidelines, etc.



Security Improvement Efforts

Human Resources Development

Information Security Manager Training is provided to information security managers and information security promoters for promoting and managing information security at participating organizations.

Since fiscal 2012 the Council Secretariat operated an e-learning program that was also offered to encourage information security managers to continuously hone their own skills. For members of participating organizations, there is also an Information Security Course. This comprises a basic version and individual-theme versions set each year, to meet the demand from participating organizations.

Furthermore, in response to demand for developing internal auditors, the Council Secretariat has also launched Information Security Auditor Training.

The Council actively encourages information security auditors to acquire auditor qualifications certified by the Japan Information Security Audit Association (JASA) to increase the quality of information security audits within the Fujitsu Group and move them along their career path. As of fiscal 2015, 142 employees had acquired auditor qualifications and were actively engaged in internal audits and committee audits.

Number of people in training

Training course name	Number of people
Information Security Manager Training (Group)	679
Information Security Manager Training (e-learning)	692
Information Security Auditor Training	1,330

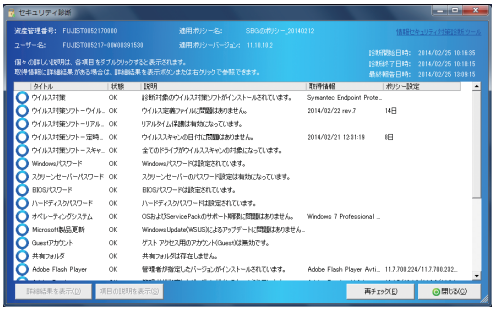
Periodic Security Checks

On "Security Check Days" implemented by the Fujitsu Group each month, personnel confirm the security settings of PCs and smart devices, as well as the administration of removable media devices. At the Council, the information security measure diagnostic tool (IT Policy N@vi) is installed in all PCs to diagnose the security measures and operational status of each PC. When a PC is started, diagnostic items* are automatically checked, with the results displayed on the PC monitor. Furthermore, by having the information security managers of each organization easily confirm the results of all PCs, Fujitsu has effectively increased the penetration of security measures.

The Council provides a security check sheet for smart devices that conforms to the Company-wide policy. The check sheet is used by various participating organizations to ensure smart device security.

* Diagnostic items: 26 items including OS, viruses, passwords, encryption, and prohibited configuration items

Information Security Measure Diagnostic Results Screen (in Japanese)



Information Security Audits

The Council defines two types of information security audits: internal audits conducted by the participating organizations themselves and external audits of the participating organizations conducted by the Council Secretariat from an independent perspective.

By having regular internal and external audits of the participating organizations, we confirm the penetration and entrenchment of information security management practices and the operational status and entrenchment of information security measures, which provides guidance for making improvements.

External audits are conducted yearly under themes stipulated by the Council Secretariat and audit plans are proposed. The Council Secretariat takes the lead in forming an audit team comprised of members who hold JASA auditor qualifications. This plays a role in the career track of the security auditors described above, and helps to improve the quality of internal audits at each organization. The audit team confirms the promotion of information security management, identifies any deficiencies, and proposes improvements, among other activities, to maintain and improve security across all participating organizations. Outstanding measures in audited organizations will be introduced as examples at the Council and utilized to raise the level of security across all participating organizations.

In other activities, experts from the Council Secretariat implement special audits of specific projects, as well as participating organizations. This is to set themes individually to address individual requests from participating organizations and to meet operational requirements.

Social Media Training

SNS* has become quite popular as a communication tool in our daily life. With the increase in the number of users of SNS, for business or private purposes, the question of where corporate responsibility lies when problems occur has emerged.

In the face of these situations, Fujitsu has published the guidelines, Rules and Manners for Participating in Social Media. Based on these guidelines, the Council Secretariat has prepared an educational program titled Information Security Course for Social Media and delivers this to members.

The course explains the risks in using SNS and gives examples that guide learners on proper uses of the media.

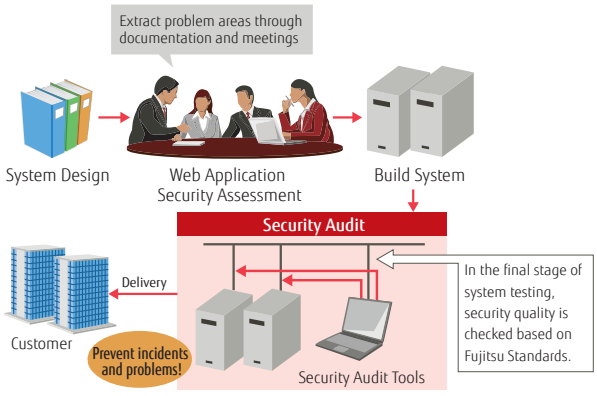
* SNS: Social Networking Service

Security Audits for Systems Delivered to Customers

The Fujitsu Group formulates security standards that should be satisfied in Internet-connected systems delivered to customers.

A pre-delivery security audit where specialized security departments objectively verify whether these systems meet guidelines is obligatory as part of quality inspections.

Security Audits for Systems Delivered to Customers



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

Regarding web application security audits in particular, security assessments are performed at the systems design stage to rapidly extract and resolve any security problems related to web applications.

This ensures that the systems delivered to customers have been confirmed to meet a consistent security level established by the Fujitsu Group, while helping to prevent security incidents caused by unauthorized access from outside. Following the inception of security audits for systems delivered to customers, Fujitsu has confirmed a sharp decline in incidents caused by insufficient security configuration in the systems integration process.

Initiatives toward the Improvement of Security Quality Including Cloud-based Services

It is important for service providers to respond to the ever-changing security threats to enable customers to be able to use services such as cloud-based services with a sense of safety and security. Fujitsu, as a service provider, clearly defines the security response that should be implemented, formulates guidelines and standards and conducts audits. In addition, Fujitsu has established a dedicated organization that will respond to incidents. It is also engaged in third-party evaluation and makes information available to the public.

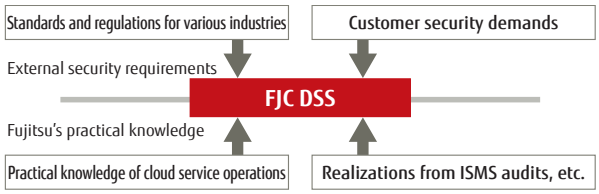
Initiatives through Countermeasure Standards for Cloud-Based Services

The reduction in security-related apprehensions and latency problems, expectations for the reduction and visualization of operating costs and business continuity coupled with the increase in cloud-based services operated in data centers within Japan herald the arrival of the cloud first era in which the public cloud becomes the preferred option.

Numerous organizations including METI, CSA and ENISA have published cloud security guidelines. The international standard ISO/IEC 27017, which is based on METI guidelines, was issued in December 2015. However, the requirements of these guidelines are set in such a way that cloud service users can freely select the strength of security that they want to adopt, causing a disparity in the level of security measures for each cloud service provider.

Therefore, Fujitsu created its own security standards, the Fujitsu Cloud Data Security Standard (FJC DSS), by integrating these external security requirements, customers' security requirements and its own practical knowledge. Fujitsu will also implement the standard in its cloud services. This ensures that cloud services offered by Fujitsu meet a consistent security quality.

FJC DSS Development Policies



Initiatives through Guidelines and Audits

Fujitsu has established Service Security Response Guidelines, which include items that should be implemented in service development and operation processes to ensure the security quality of services offered to customers.

Divisions providing services put into practice the security measures based on these guidelines. Moreover, before launching a service, the audit department audits the status of security measures and ensures its quality.

During service operations, the security audit department continually conducts regular security audits. The security quality is maintained and continuously improved by taking corrective measures if necessary.

Fujitsu Cloud CERT Initiatives

Fujitsu Cloud CERT (Computer Emergency Response Team), a team that specializes in the security of services including cloud-based services, performs the following activities on a global scale in order to support customers' businesses and protect the cloud environment from various security threats.

1. Information security operations

For customers to securely use Fujitsu cloud-based services, Fujitsu Cloud CERT implements security measures, including point of contact detection of various external attacks and monitoring of the cloud service infrastructure, and operates under a 24-hour, 365-day system.

2. Emergency response

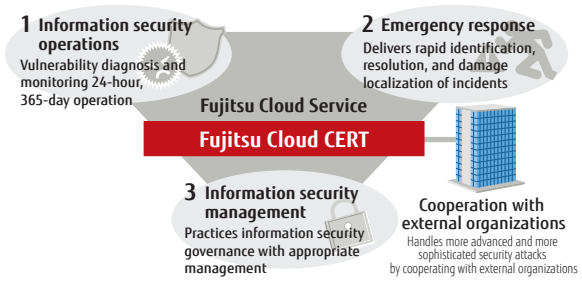
Fujitsu Cloud CERT has established response procedures that will be implemented when an incident occurs to achieve rapid and accurate identification, resolution, and damage localization of the incident.

3. Information security management

Fujitsu Cloud CERT properly manages the "people," "goods," and "information" in Fujitsu Cloud services to protect the important information of the customers. Moreover, Fujitsu Cloud CERT is a member of security-related organizations such as the Nippon CSIRT Association and FIRST* and plays an active role in improving global cloud security.

* FIRST: Forum of Incident Response and Security Teams

Activities of Fujitsu Cloud CERT

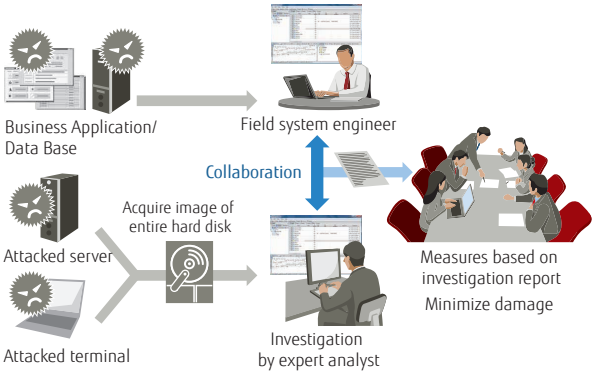


Fujitsu Answers Customers' Needs from Real-Time Monitoring to Breach Investigation

Our expert analysts use digital forensic techniques to investigate unauthorized access and breach status, even in global multi-cloud environments. These investigations identify evidence of unauthorized access, such as file tampering and unauthorized programs, from data on servers and terminal hard drives that have been subject to attack. They then investigate the vulnerabilities that enabled the attack, and the extent of impact from the unauthorized activity.

The analysts also identify traces of unauthorized access by recovering logs and deleted files, revealing the full extent of a cyber-attack. Moreover, they go beyond simple digital forensics, working in close collaboration with field system engineers to handle analysis of business applications and data bases as well.

Breach Investigation Process



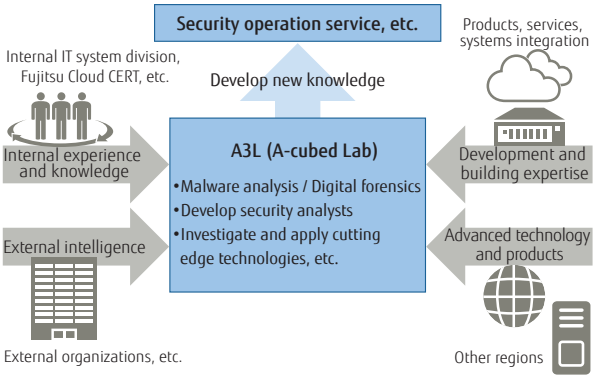
Investigations Drawing on the Fujitsu Group's Combined Knowledge and Use of Research Facilities

The FUJITSU Advanced Artifact Analysis Laboratory ("A3L"—A-cubed Lab)* was established in November 2015 to keep track of increasingly sophisticated cyber-attacks and concentrate and reinforce expert analysis technologies. The facility will discover new attack methods by using incident analysis, malware analysis, and threat information, and transfer this knowledge into services.

Clarifying the true aims and targets of attackers will enable preventative measures to be put in place to counter potential attacks before they occur. Specifically, the A3L will conduct artifact analysis (analysis of attack methods such as malware and targeted email), and collect cyber threat intelligence for sharing and utilization.

* A3L: FUJITSU Advanced Artifact Analysis Laboratory

Making Use of Investigation and Research Facilities

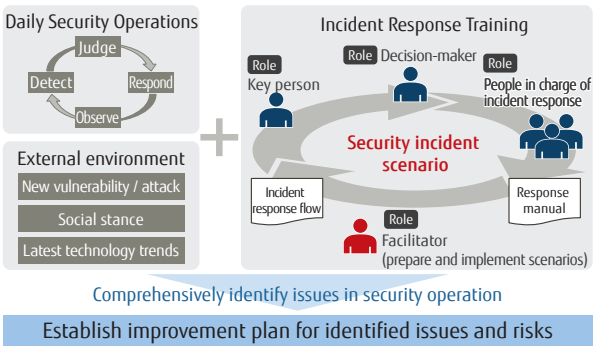


Strengthening Security Endurance through Incident Response Training

Fujitsu conducts incident response training to bolster security operation endurance, improving the operating environment in response to event statistics detected during operation and changes in the external environment and attack methods.

Incident response training involves selecting a scenario to use in a given situation from multiple envisaged scenarios matched to actual situations. The scenario is then played out as a form of academic practice. Issues and risks identified through incident response training are then discussed to form improvement proposals. Continuous improvements are made to the flow, documentation and communication protocols between related organizations used to respond to each type of incident.

Incident Response Training Process



Product Security

The security enhancement initiatives of Fujitsu's software product development divisions include responding to vulnerabilities in open source software and methods for verifying vulnerabilities in order to produce products that are resilient against cyber-attacks. These initiatives are described below.

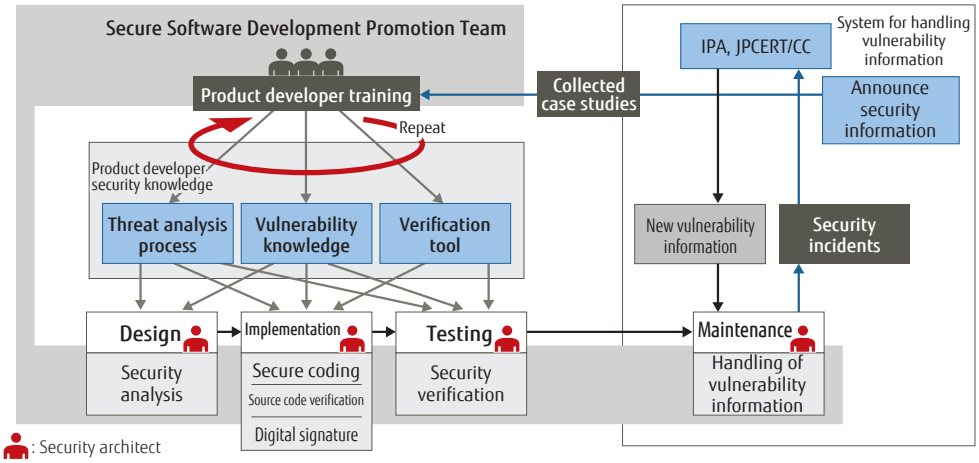
Software Security Quality Enhancement Initiatives

To improve the security quality of its software products including firmware, Fujitsu conducts the activities shown in the diagram below, led by the Secure Software Development Promotion Team. Specifically, Fujitsu incorporates the following four activities into its development process to ensure security quality:

1. In the design process, Fujitsu conducts security analysis (threat analysis) and uses the results to improve the design.
2. In the implementation process, Fujitsu conducts coding to avoid any built-in vulnerabilities (secure coding), verifies source code using verification tools, and adds digital signatures to programs as necessary.
3. In the testing process, Fujitsu conducts security verification using verification tools and runs tests from a security perspective.
4. In the maintenance process, Fujitsu monitors security vulnerabilities, rapidly provides security patches, and publicly discloses security information in coordination with the Information-technology Promotion Agency (IPA) and the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

For each process, Fujitsu deploys security architects with technical knowledge of security in each division, in order to entrench proper security responses in development activities. About 10% of all developers are certified as security architects.

Security Process for Software Products



Ensuring Security in Shipped Products Using Open Source Software

One part of the maintenance process referred to above involves ensuring the security of products using open source software, which is described here. Accompanying the increasing diversity of software product requirements is the growing variation of open source software that Fujitsu products use. That makes it crucial to provide rapid support for each open source software vulnerability. Fujitsu system engineering and product development divisions jointly created the Open Source Software Vulnerability Response System to comprehensively and effectively prevent response failures and provide rapid support.

Overview of the Open Source Software Vulnerability Response System

1. Fujitsu employs the Vulnerability Countermeasure Information Database JVN iPedia*1 as an information source about open source software vulnerabilities. This database covers vulnerabilities which have been given a number by the National Vulnerability Database (NVD)*2.
2. Based on information stored in the product repository, applicable open source software for each product is specified in the system for vulnerability information. This enables all open source software being used in products to be investigated for vulnerabilities.
3. Vulnerability information collected by the Open Source Software Vulnerability Response System is cross-checked against open source software divided by product in the product repository and immediately communicated to developers, starting the vulnerability response process.

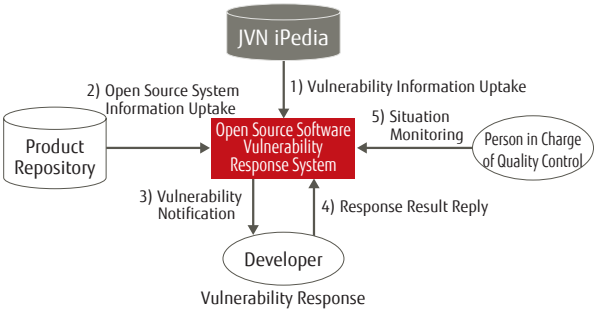
4. Security is positioned as a high-priority issue and open source software vulnerabilities are given a high priority and investigated. Those responsible for product quality control in the product development divisions check the response status and issue appropriate instructions if they find the response to be lagging.

Various types of information publicly available on the Internet are used as source material.

*1 Vulnerability Countermeasure Information Database JVN iPedia is a vulnerability database jointly managed by JPCERT/CC and the IPA. It covers all vulnerability information registered in the NVD since 2007.

*2 The National Vulnerability Database is a vulnerability database managed by the U.S. National Institute of Standards and Technology.

Overview of the Open Source Software Vulnerability Response System



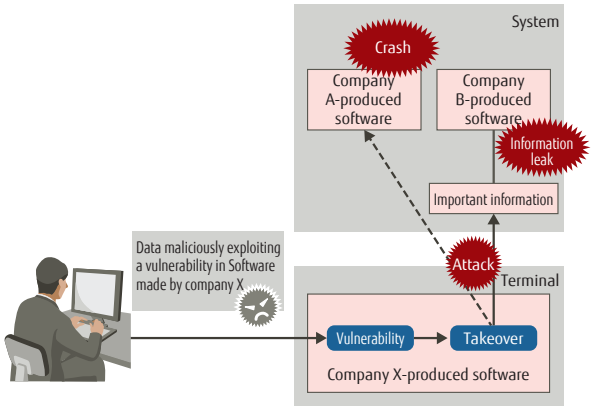
Providing Strong Products Equipped against Cyber-Attacks

During our testing process, Fujitsu conducts security verification using tools. In this section, we explain how fuzzing tools are used to test for vulnerabilities in security verification.

Expanding Cyber-Attacks

Cyber-attacks are a major issue for management in contemporary companies. Many cyber-attacks maliciously exploit software vulnerabilities to unleash their attacks.

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



Attackers deploy advanced persistent threats (APTs)*1 targeting vulnerabilities in the software used on terminals that use the Internet, email, and so forth, to attack and take over the terminal.

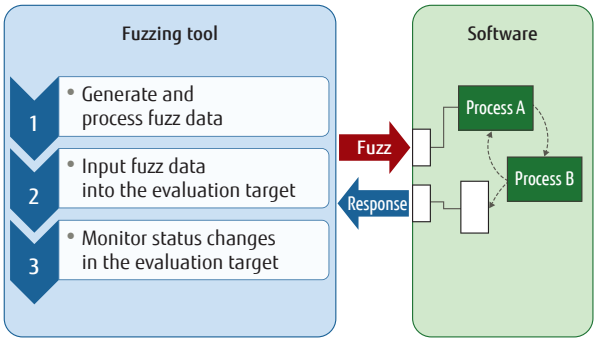
Next, using the acquired terminal as a foothold, they launch an attack on internal systems not connected to the Internet.

To minimize the impact of such cyber-attacks, the component system software must be prepared with high resilience against cyber-attacks.

Fuzzing

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

How Fuzzing Works



Effect of Introducing Fuzzing

Introducing fuzzing enables us to detect and respond to software vulnerabilities that have been difficult to spot with conventional detection tools. Fuzzing is particularly effective for verifying vulnerabilities to service disruption attack*2 and buffer overflows*3.

Prior Verification of Cyber-Attacks by Fuzzing

Fujitsu's software product development process includes a verification step using our fuzzing tools developed in-house. This is part of our efforts to ensure that our products that are resilient against cyber-attacks.

*1 Advanced Persistent Threat (APT): APTs are a type of cyber-attack that is targeted at a particular body of data within an organization. They are often conducted by methods such as sending an email with a virus attachment to the computers of the organization members.

*2 Service disruption attack: A deliberate action intended to render a computer such as a server or network resource unable to provide service. Also referred to as a Denial of Service (DoS) attack. A variety of this attack, known as a Distributed Denial of Service (DDoS) attack, draws in multiple computers to the attacker side.

*3 Buffer overflow: one of several problems that can cause "memory area destruction" in a program, or the phenomenon caused by it.

Information Security Personnel Training

Recently, increasingly advanced and sophisticated cyber-attacks are becoming a major social issue. One of Fujitsu's initiatives to protect customer's information assets from this threat is to promote development of security personnel with advanced security skills. In this section, we introduce our Security Meister*1 Certification System for certifying specialists in protecting information systems from cyber-attacks and our Security Architect Training for certifying personnel who are responsible for improving the security quality of software in the development stage.

The Security Meister Certification System

The Necessity of Training Professional Information Security Personnel

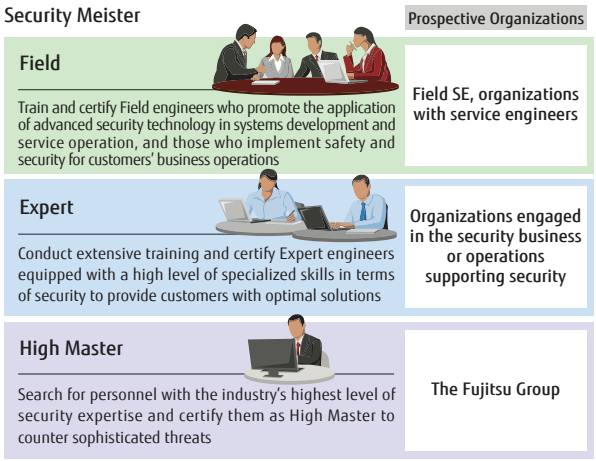
Threats related to cyber-attacks such as serious damage brought about by targeted attacks on companies and organizations are becoming diversified and sophisticated. With this in mind, one of Fujitsu's efforts to protect the information assets of its customers from those threats involved launching a system to search within the Fujitsu Group for engineers with a high level of security skills so that they can be trained and certified, and eventually dispatched in the field.

The Security Meister Certification System

Security specialists who can protect information systems from cyber-attacks will undergo systematic and continuous training, and be certified as Security Meisters. In this system, specialists are grouped into three categories, namely Field, Expert, and High Master, according to the functions and requirements of the job. There is a plan to train and certify 2,000 engineers by the end of fiscal 2017.

*1 The Security Meister Certification System is the official name of Fujitsu's personnel training system. The word "Meister" is of German origin, referring to a person who has extensive theoretical knowledge and practical skills in their profession.

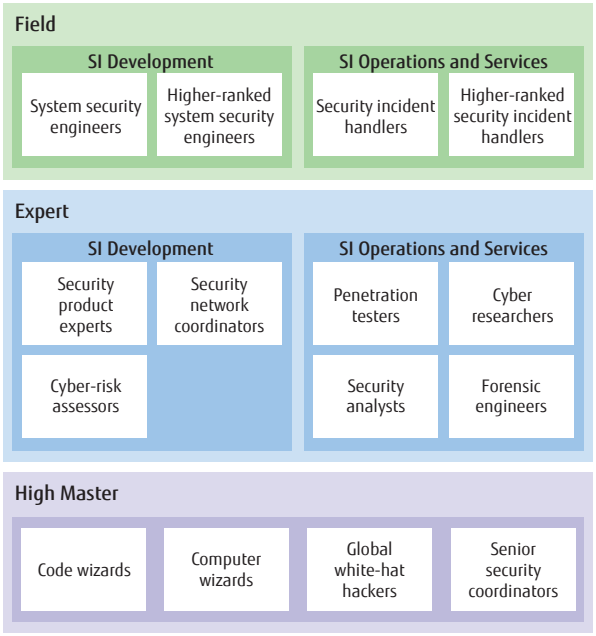
Three Security Meister Categories



Defining the Types of Security Engineers

The Security Meister Certification System defines the types of security engineers who can adapt to the needs of ICT development and operations today. The 15 types of security engineers grouped into three categories defined by the various requirements of ICT development and operations are outlined in the model below.

Security Meister Model



In realizing this model, Fujitsu takes into consideration its consistency with Japan's IT skill standards and various security personnel models available overseas. Furthermore, High Master is defined as being equivalent to a white-hat hacker*2 or Top Gun*3.

The following are examples of types of security engineers with their respective definitions. A System Security Engineer in the Field category is assigned to the Systems Development Division and is in charge of on-site security design and implementation of technical security countermeasures.

A Security Incident Handler is assigned to the Systems Operation Division and is in charge of the system security operation design and implementation of security countermeasures concerning information security incidents that occur on-site.

A Computer Wizard in the High Master category is assigned to the Development Division of embedded systems, can conduct original research and share and disseminate information by leveraging their technical capabilities. This kind of personnel utilizes cutting-edge security technology, is self-motivated and expected to participate in and give presentations at external organizations' events (including research and security seminars for local engineers).

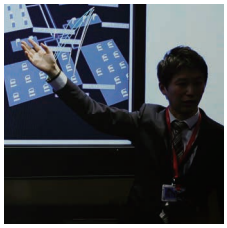
*2 White-hat hacker: A person with high level IT skills that they apply for correct objectives.

*3 Top Gun: Security engineer with an advanced level of expertise.

Establishment of Training Programs

As part of establishing training programs for security engineers with emphasis on practical applications, Fujitsu has opened specialized training courses that correspond to each type of security engineer. A training program conducted in a cyber-range (virtual training area) has been newly set up. Fujitsu makes these training courses available to each of its customers.

A training scene



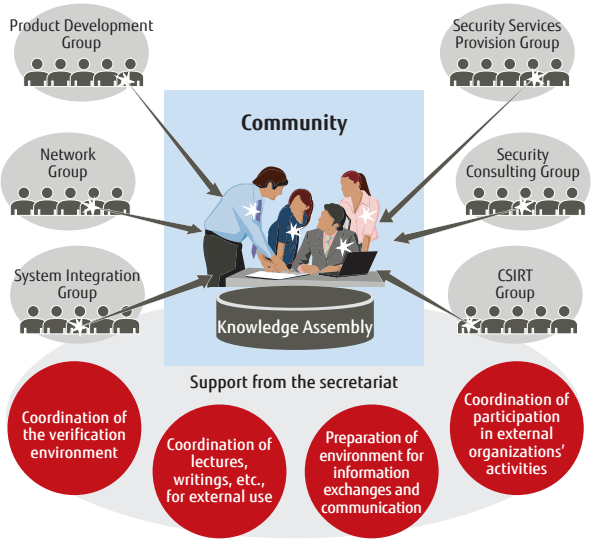
Searching for Capable Security Personnel and Increasing Their Number

Fujitsu is promoting the discovery of personnel with security skills and growth in the number of security engineers. Fujitsu also strives to consolidate knowledge and information from various divisions within the Company and has formed a Security Meister Community for the effective utilization of gathered resources. Experts sharing their knowledge within the community will result in the enhancement of their skills after they have been certified.

A security contest that includes hacking techniques is also being held internally. The security contest also utilizes the cyber–range, allowing 40 engineers to showcase their technical capabilities as they compete against each other at the same time.

In this manner, Fujitsu offers its customers safety and security as it proactively conducts security-related training.

Security Meister Community



Software Product Developer Training

Security training in the software product development divisions involves General Training for general product development and testing staff and Security Architect Training for development of professionals.

Security Architect Training

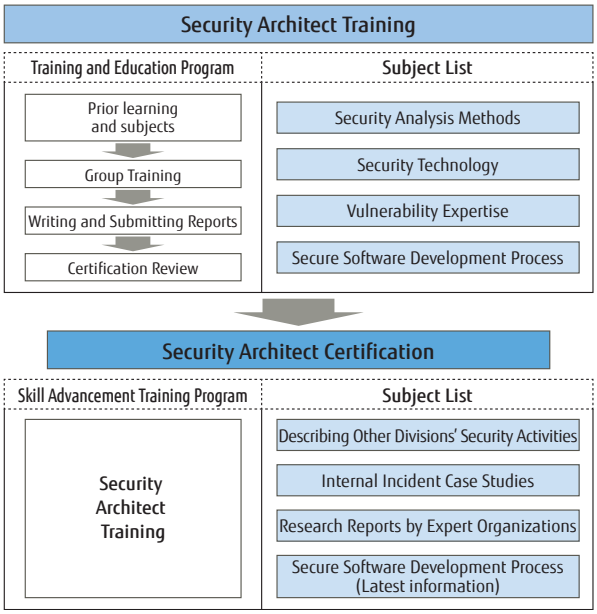
Security architects are those who have obtained professional qualifications within the Company to promote security response activities, enhance security quality in software products, and operate the Security Architect Certification System, which includes training programs given in software product development divisions.

The training program for security architects has a curriculum executed in four phases over several months for candidates recommended by each development division. The four phases are: (1) Prior learning and subjects, (2) Group training (exercise style), (3) Producing issue (threat analysis) reports, and (4) Certification review. Following certification as a security architect, training programs are held regularly with details such as those shown in the figure on the right, at a rate of once or twice a year, to hone architects' skills.

- Describing Other Divisions' Security Activities
- Internal Incident Case Studies
- Research Reports by Expert Organizations
- Secure Software Development Process (Latest information)

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

Overview of Security Architect Training



Research and Development into Security Technology for Supporting a Safe Lifestyle

Cyber-attacks are becoming more intense and more sophisticated every day, threatening the safety of company systems. On the other hand, discussion of new services with strict personal identification confirmation has started, on the assumption that the private sector will be able to use the Social Security and Tax Number System. There is a demand for reliable personal authentication technology that will also protect personal information. Fujitsu Laboratories Ltd. is developing the latest technologies to resolve these challenges. This report provides an introduction on technology using artificial intelligence (AI) to identify sophisticated cyber-attacks more efficiently and technology for safe encryption of biometric information.

Application of AI Technologies to Detecting Cyber-Attacks

Background

As cyber-attacks increase in intensity, networks from the public and private sectors are being attacked in various ways. In recent years, in particular, concealed amid the large volume of known attack methods such as vulnerability scans and Denial of Service (DoS) attacks, sophisticated attacks such as advanced persistent threats (APTs) have also been carried out. Monitoring and analysis of logs output from network equipment and so forth is considered to be an effective method for detecting these sophisticated attacks. However, as sophisticated attacks occur only rarely, it is extremely difficult to detect an attack by manual analysis of the enormous logs.

Fujitsu Laboratories has developed security log analysis technologies in which AI technologies are used to visualize threats that are difficult to find manually. These technologies enable log analysts to efficiently identify the sophisticated attacks hidden among the large volume of known attacks.

Newly Developed Technologies

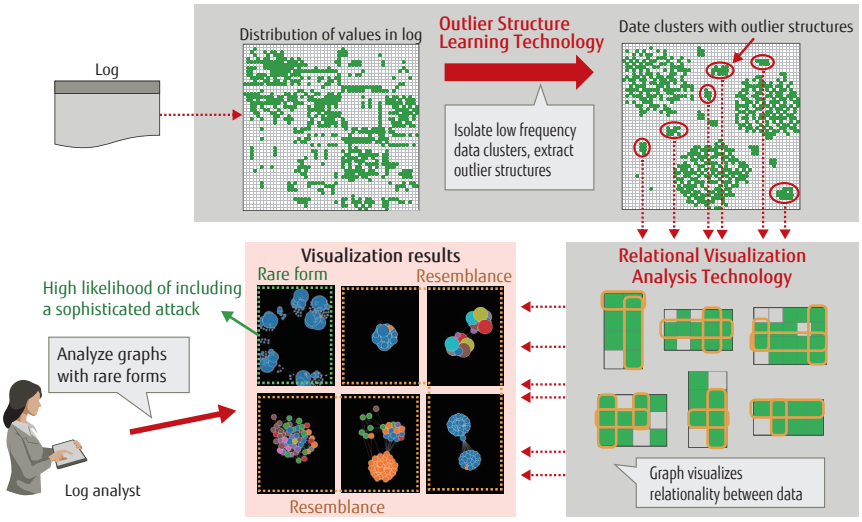
To enable identification of sophisticated attacks, Fujitsu Laboratories developed two technologies: the Outlier Structure Learning Technology and Relational Visualization Analysis Technology.

The Outlier Structure Learning Technology analyzes large-scale logs to extract an outlier structure—a small cluster of data with rare values. As sophisticated attacks occur with such low frequency, there is a high likelihood that they will be included in this outlier structure.

The Relational Visualization Analysis Technology is used to create a visualization of data clusters having outlier structures. Visualized outlier clusters have characteristics that appear when shown in graphic form depending on the type of attack. These characteristics can be used to categorize data clusters with outlier structures by attack type.

Log analysts can analyze the visualized results and efficiently extract the sophisticated attacks from among the data clusters.

Security Log Analysis Technology Employing AI: Processing Flow



1. Outlier Structure Learning Technology

Outlier Structure Learning Technology focuses on the frequency of data characteristics that appear in logs and extracts small data clusters that have rare characteristics. Conventional technology performed categorization and extraction of the log focusing only on the characteristics that appeared frequently within the log. Consequently, even if attacks occurring in large volumes could be detected, it was difficult to extract small-scale, irregular attacks concealed among them.

Outlier Structure Learning Technology focuses on characteristics that rarely appear in the log, separates data clusters that share characteristics that appear infrequently and repeatedly integrates the multiple data clusters of infrequent characteristics that have been segmented. This enables the extraction of "outlier structures," which are small-scale data clusters that share rare characteristics within a log.

2. Relational Visualization Analysis Technology

Next, clusters with outlier structures are plotted on a graph to visualize relationality between the data.

Data clusters with outlier structures also contain many known attacks that occur infrequently. Visualizing those attacks revealed similarities in their graphic forms. Focusing on this characteristic enables log analysts to extract the rare graphic form shapes. Data clusters with rare graphic shapes correspond to attacks with characteristics that differ from others, making it easier to identify sophisticated attacks.

Relational Visualization Analysis Technology compares the results of visualization and extracts data clusters with rare graphic forms. This enables the narrowing down of data clusters with a high likelihood of being a sophisticated attack, enabling log analysts to efficiently identify such attacks.

Verification in an Actual Environment Log

Verification was carried out on the developed technology by applying it to a log obtained from an actual environment. Extracting data clusters with outlier structures and comparing the visualization results enabled the extraction of two-to-three data clusters with rare graphic forms. A detailed analysis of these clusters showed they contained a sophisticated attack. Previously, the laboratory had taken about three months to identify this attack. The newly developed technology identified the attack in about one day. This verified that the developed technology enables efficient identification of sophisticated attacks from logs.

Initiatives Going Forward

Currently, this technology is undergoing trial operations under the supervision of Fujitsu Cloud Services. Looking ahead, after refining the analysis accuracy, the technology will contribute to the safe operation and management of Fujitsu Cloud Services.

Technology to Encrypt Biometric Data

Background

The volume of IDs, passwords and other personal confidential data is increasing along with the growth of Internet services. All of this confidential data, being difficult to remember, is increasingly managed with encryption, such as by using AES, the current standard encryption technology. With current technologies, it has been necessary for users to manage cryptographic keys to decrypt encrypted data by storing cryptographic keys on an IC card or by validating cryptographic keys through password authentication. This therefore elicits a need for a technology that can securely encrypt and manage an individual's confidential data using biometric data for personal authentication that is inseparable from the individual as a key.

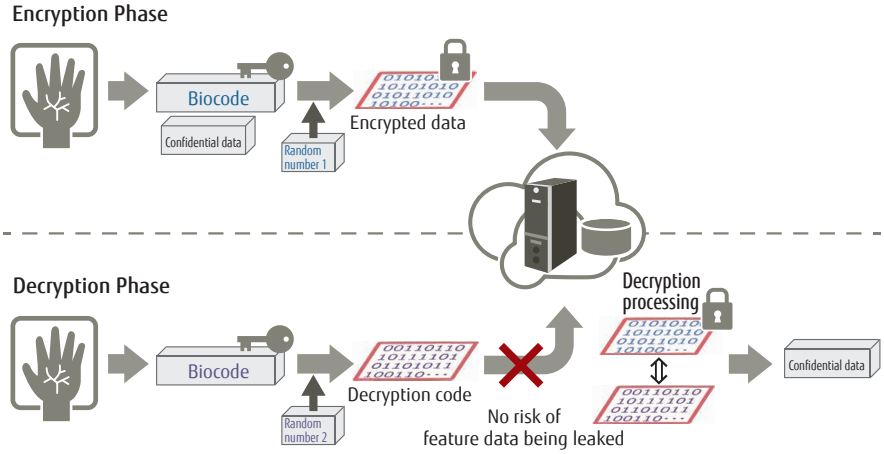
Meanwhile, conventional methods of technology using biometric data as a cryptographic key commonly use Feature Data*1 extracted from biometric data as the key and therefore used same feature data for decryption. However, using this data online through open networks such as clouds required even safer encryption technologies to prevent leaks of biometric data.

Fujitsu Laboratories developed a technology that applies biocode technology*2 to extract feature data as a 2048-bit code from a palm vein image, then converts confidential data with the biocode to encrypt it. The biocode used for the encryption key is also converted to a random number to protect it, enabling expanded use in cloud-based services through open networks.

*1 Feature Data: Data obtained from a person's biological features.

*2 Biocode technology: A 2048-bit binary code extracted from a palm vein image, created by technology unique to Fujitsu Laboratories. A summary of this technology can be found in the Fujitsu Group Information Security Report 2014.

Flow of Encryption and Decryption Using Biocode



Newly Developed Technology

We have developed two technologies for application in biocode technology making use of palm veins: technology to protect biometric data using random numbers, and technology to decrypt confidential data using error-correcting codes.

1. Technology to Protect Biometric Data Using Random Numbers

In encryption, biocode converted to a random number is added to confidential data to generate encrypted data, which is registered in the server.

A decryption code is used as the key when decrypting encrypted data. For decryption, the decryption code is converted into secure data by the device and sent from the device to the server. The decryption code is generated by first converting the biocode using a random number. As the system can randomly select different random numbers for encryption and decryption, a different, secure decryption code can be generated every time.

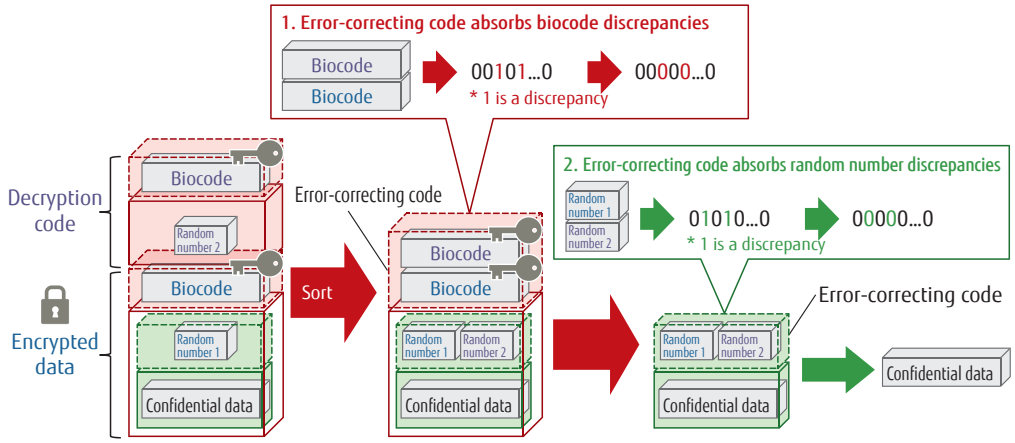
2. Technology to Protect Biometric Data Using Error-Correcting Codes

Variations in one's motion or position when inputting biometric data, and the use of a different random number each time can generate slight discrepancies. The discrepancies can be absorbed because they are converted using an error-correcting code. Error-correcting code is widely used as a supplementary technology for data loss generated during transmission.

The decryption process using error-correcting code involves two steps. In step 1, the discrepancies caused when calculating the decryption biocode for the encrypted biocode are corrected. In step 2, the discrepancies caused by calculating the random number used for decrypting the random number added during encryption are similarly corrected, enabling recovery of the confidential data.

In this way, as the biometric data input for encryption and decryption are sufficiently similar, so long as they are both from the same person, the confidential data can be retrieved from the encrypted data using error-correcting technology.

Recovery of Confidential Data Using Error-Correcting Code



Effect

With the ability to use biometric data for encryption and decryption, the cryptographic key management that had been needed for existing encryption technologies becomes unnecessary. Consequently, as servers holding encrypted data do not have the encryption data at the same time, they can be operated more securely. Moreover, as biometric data used during encryption and decryption is converted using random numbers, the unconverted biometric data will not flow into the network. This means that the use of encryption technology using biometrics can now be expanded to cloud services.

Future Plans

With this technology, we aim to continue improving the speed of decryption processing and expanding the types of data that can be encrypted, while also examining the technology's applicability to a number of potential use cases, such as the Social Security and Tax Number System. We will also examine ways to develop biocode utilizing the feature of the person encrypting being the only person capable of decrypting, and work to expand the types of applicable biometrics, such as fingerprints.

Information Security Enhancement Measures in Cooperation with Business Partners

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

Amid these activities, the Fujitsu Group and its business partners build long-term bonds of trust, each enhancing its own abilities as a valued partner and together creating continuous and mutually prosperous relationships, all under the Fujitsu Way corporate policy.

The Fujitsu Group aims to eliminate information security incidents together with its business partners. To this end, the Group continuously implements measures to maintain and strengthen information security, such as education, awareness raising, audits, and information sharing.

Information Security Promotion Initiatives in Fiscal 2015

Education and Raising Awareness

■ Information security seminars

To prepare for the full-scale rollout of the Social Security and Tax Number System beginning in 2016, Fujitsu revised the "Information Management Procedure for Business Partners" (agreement relating to information security between the Fujitsu Group and its partners) in September 2015. We held training sessions in 2015 to explain the revisions and cover themes such as case studies of Advanced Persistent Threat (APT) and the importance of improving IT literacy.

- Fiscal 2015: 1,300 participants from 950 business partners (in places including Sendai, Tokyo, Kawasaki, Chiba, Nagoya, Osaka, Takamatsu, Fukuoka and Okinawa.)

■ Out-of-office training and workshops at business partners' premises

At the request of its business partners, Fujitsu dispatched trainers to provide them with group training sessions (out-of-office training).

Also, for business partners seeking to improve their leaders' abilities, we provided group workshop-style training sessions to reaffirm the role of a leader and improve skills in risk response (out-of-office workshops).

- Fiscal 2015
  - Out-of-office training
    40 companies/1,400 participants
  - Out-of-office workshops
    10 companies/170 participants

Business Partner Selection and Evaluation, and Confirmation of Information Security Status

Selection of new business partners involves confirmation of information security readiness, and is limited to those business partners who consent to contractual requirements concerning information security management and the handling of personal data.

Existing business partners are also obliged to submit an annual written survey of the status of their information security measures, and outsourcing suppliers are selected based on requirements such as compliance with the Act on the Protection of Personal Information.

Furthermore, in selecting business partners each year, we conduct personal visits and inspect the status of information security compliance based on the contract. If the inspection reveals a need for correction, we provide a correction plan proposal and implementation guidance.

- Fiscal 2015 Surveys 190 companies

Information Sharing and Presenting On-Site Support Tools

For the purpose of sharing the latest news on information security, Fujitsu has published the Information Security Plaza and awareness posters for business partners since April 2009.

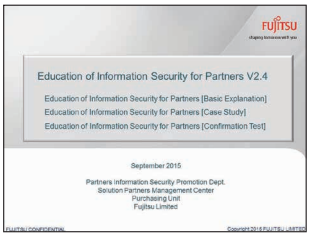
Fujitsu provides project information security plans at the start of projects to establish a consensus on project information security requirements and share it among all members, enabling rapid discovery of and response to issues. In addition, we also provide a "compliance status check sheet" to be used for self-checking.

■ January 2016 issue of Information Security Plaza

Support for Overseas Business Partners

Opportunities have increased for business through cooperation with overseas business partners aimed at such objectives as supporting customers' overseas expansion, securing development resources, and responding to global products.

Fujitsu concludes "Information Management Procedure for Business Partners" agreements with overseas business partners as it does with Japanese partners, regulating the handling of information provided by Fujitsu in accordance with the conditions of each country. It also conducts regular information security audits and training.



Third Party Evaluation/Certification

The Fujitsu Group is working to acquire third-party evaluations and certifications in its information security initiatives.

PrivacyMark Registration

The PrivacyMark registration status within Fujitsu and Fujitsu Group companies from the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) is as follows:

FUJITSU LIMITED
IT MANAGEMENT PARTNERS LIMITED
FUJITSU ADVANCED ENGINEERING LIMITED
FUJITSU ADVANCED SYSTEMS LIMITED
FUJITSU APPLICATIONS, LTD.
FUJITSU ADVANCED PRINTING & PUBLISHING CO., LTD.
FUJITSU HUMAN RESOURCE PROFESSIONALS LIMITED
AB SYSTEM SOLUTIONS LIMITED
FUJITSU FIP CORPORATION
FUJITSU FOM LIMITED
FUJITSU FSAS INC.
OKINAWA FUJITSU SYSTEMS ENGINEERING LTD.
FUJITSU KAGOSHIMA INFORNET LIMITED
FUJITSU KYUSHU SYSTEMS LIMITED
FUJITSU QUALITY & WISDOM LIMITED
FUJITSU COMMUNICATION SERVICES LIMITED
FUJITSU COWORCO LIMITED
FUJITSU CIT LIMITED
G-SEARCH LIMITED
FUJITSU SHIKOKU INFORTEC LIMITED
FUJITSU SYSTEMS APPLICATIONS & SUPPORT LIMITED
FUJITSU SYSTEMS EAST LIMITED
FUJITSU SYSTEMS WEST LIMITED
FUJITSU RESEARCH INSTITUTE
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
FUJITSU SOFTWARE TECHNOLOGIES LIMITED
TOTALIZATOR ENGINEERING LIMITED
TOYAMA FUJITSU LIMITED
FUJITSU TRAVELANCE LTD.
FUJITSU NIIGATA SYSTEMS LIMITED
FUJITSU PERSONAL SYSTEM LIMITED
FUJITSU PUBLIC SOLUTIONS LIMITED
FUJITSU BANKING INFORMATION TECHNOLOGY LIMITED
BANKING CHANNEL SOLUTIONS LIMITED
FUJITSU BROAD SOLUTION & CONSULTING INC.
PFU LIMITED
FUJITSU FRONTECH LIMITED
FUJITSU FRONTECH SYSTEMS LIMITED
BEST LIFE PROMOTION LTD.
FUJITSU HOME & OFFICE SERVICES LIMITED
FUJITSU HOKURIKU SYSTEMS LIMITED
FUJITSU MARKETING LIMITED
FUJITSU MISSION CRITICAL SYSTEMS LIMITED
FUJITSU YAMAGUCHI INFORMATION CO., LTD.
UCOT INFOTECHNO CO., LTD.
FUJITSU LEARNING MEDIA LIMITED
FUJITSU YFC LIMITED

ISMS Certification

Fujitsu and Fujitsu Group companies with divisions that have acquired ISMS certification based on International Standards ISMS (ISO/IEC 27001) for Information Security Management Systems are as follows:

FUJITSU LIMITED
FUJITSU IT MANAGEMENT PARTNER CO. LTD.
FUJITSU ADVANCED ENGINEERING LIMITED
FUJITSU FIP CORPORATION
FUJITSU FSAS INC.
FUJITSU KAGOSHIMA INFORNET LIMITED
FUJITSU KANSAI-CHUBU NET-TECH LIMITED
FUJITSU KYUSHU SYSTEMS LIMITED
FUJITSU SHIKOKU INFORTEC LIMITED
ZIS INFORMATION TECHNOLOGY CORPORATION
FUJITSU SYSTEMS APPLICATIONS & SUPPORT LIMITED
FUJITSU SYSTEMS EAST LIMITED
FUJITSU SYSTEMS WEST LIMITED
FUJITSU GENERAL LIMITED
FUJITSU RESEARCH INSTITUTE
FUJITSU SOCIAL SCIENCE LABORATORY LIMITED
FUJITSU DEFENSE SYSTEMS ENGINEERING LIMITED
TOYAMA FUJITSU LIMITED
NIFTY CORPORATION
FUJITSU NETWORK SOLUTIONS LIMITED
FUJITSU PUBLIC SOLUTIONS LIMITED
BANKING CHANNEL SOLUTIONS LIMITED
FUJITSU BROAD SOLUTION & CONSULTING INC.
PFU LIMITED
FUJITSU FRONTECH LIMITED
FUJITSU MARKETING LIMITED
FUJITSU MISSION CRITICAL SYSTEMS LIMITED
FUJITSU MIDDLEWARE LIMITED
FUJITSU LEASING CO., LTD.
FUJITSU YFC LIMITED

Information Security Rating Certification

Information security ratings indicate the level of security, mainly in terms of whether information leaks and other security incidents could occur. Information here refers to technical data, trade secrets, and personal information handled by companies and other organizations.

The ratings are given by I.S.Rating Co., Ltd. The Fujitsu Group information security ratings are shown to the right.

Company Name	Rating Scope	Rating Mark
FUJITSU LIMITED	Tatebayashi System Center	AAA_{is}
	Akashi System Center	AAA_{is}
FUJITSU FIP CORPORATION	Yokohama Data Center	AAA_{is}
	Chubu Data Center	AAA_{is}
	Kyushu Data Center	AA^{+}_{is}
FUJITSU FSAS INC.	Tokyo LCM Service Center	AA^{+}_{is}

ISMS Auditor Certification

In 2002, the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) began full operation of an information security management system (ISMS) compliance evaluation system in Japan. The personnel certification institutions that register evaluations of auditors in Japan are the Japanese Registration of Certificated Auditors (JRCA) and International Register of Certified Auditors (IRCA) Japan.

The certification classifications for auditors include "ISMS Lead Auditor," "ISMS Auditor," and "ISMS Provisional Auditor." The number of people who hold ISMS auditor certifications at Fujitsu and Fujitsu Group companies is shown as follows.

<155 people>

JASA Auditor Certification

The NPO Japan Information Security Audit Association (JASA) is a certification organization for auditors who implement information security audits based on the "Information Security Audit System" issued by the Ministry of Economy, Trade and Industry in April 2003. The categories of qualifications are "CAIS*-Lead Auditor," "CAIS-Auditor," "CAIS-Assistant," and "CAIS-Associate."

Fujitsu and Fujitsu Group companies have the largest number of individuals who are qualified as JASA auditors. The number of such auditors is shown as follows.

<142 people>

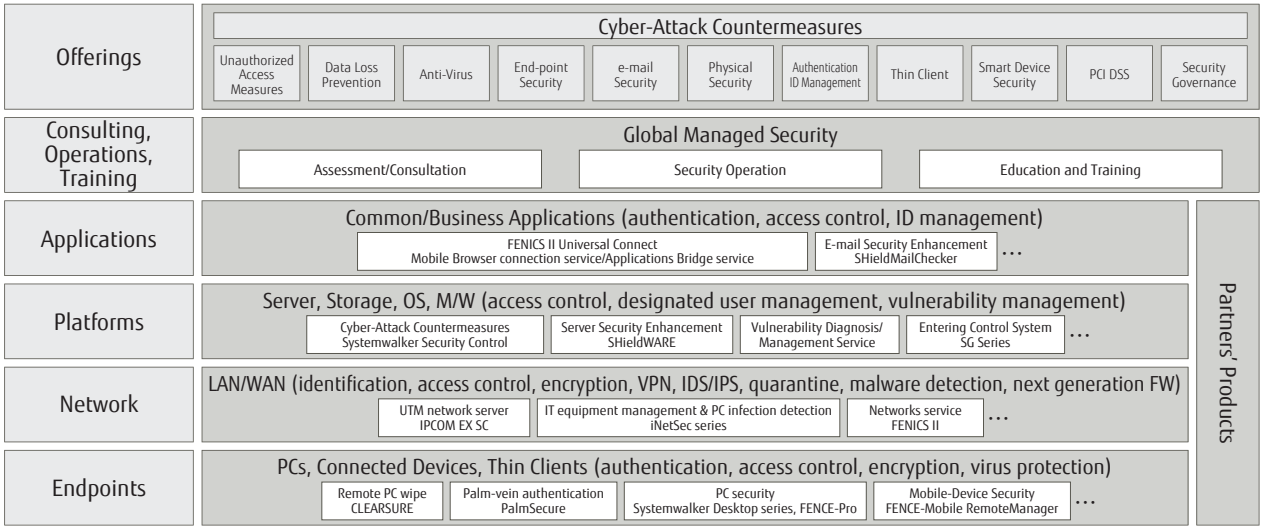
* CAIS: Certified Auditor of Information Security

FUJITSU Security Initiative

Fujitsu continuously works on achieving safe and secure ICT to continue supporting customers and sustainable business.

The growing popularity of cloud computing and smart devices has seen the regions utilizing ICT expand and cyber-attacks grow more sophisticated and cunning by the day, so taking measures against the attacks to ensure safe and secure utilization of ICT has become a significant issue. Through appropriate countermeasures and operations, Fujitsu, which is comprised of approximately 300 companies worldwide, currently deals with several hundred million security events logged per day to detect threats in its own Intranet. To apply this expertise to the security measures of its customers and deliver integrated support, including enhanced systems and operations as well as education and training of companies' personnel, Fujitsu has organized a line of products and services that follow its new "FUJITSU Security Initiative."

FUJITSU Security Initiative



Security Solutions

Currently, the environment encompassing information security is exposed to a variety of security risks, starting with external threats such as viruses and illegal access, and including cyber-attacks and data loss incidents which are increasing in conjunction with the widespread use of smart devices. Fujitsu's track record of practical experience provides security solutions based on consistent beliefs and thorough in-house implementation under "the Fujitsu Enterprise Security Architecture (ESA)" and "our Security Management Framework (SMF)." Providing solutions requires integrating the necessary security solutions and conforming to the ESA in order to effectively support companies' investments from a functional aspect. Presenting reference models based on internal practices enables customers to implement highly reliable solutions drawn from our track record.

Main Models Offered	For further details on security, please visit the following website (Japanese only): http://www.fujitsu.com/jp/solutions/business-technology/security/secure/index.html
Global Managed Security	Visualizes problem areas with the existing organization and processes, and while continuing to make use of conventional counter measures, provides optimal countermeasure solutions for the customer to respond to cyber-attacks, based on practical knowledge cultivated through numerous business talks and operation of in-house systems.
Security Governance	Supports the realization of "information security governance" in the organization based on continuous security measures from the perspective of overall company activities including ICT.
Cyber-Attack Countermeasures	Provides optimal measures to guard against new cyber-attack methods, while taking full advantage of conventional measures.
Smart Device Security	Provides solutions for customers' security concerns when using smart devices for business purposes.
Unauthorized Access Measures	Realizes a security cycle including surveillance 24 hours a day, 365 days a year, as well as planning, establishing measures, implementing measures, auditing, and monitoring.
Data Loss Prevention	Provides functions for drafting and establishing information management policies and encryption functions for protecting personal information and preventing information leaks.
Anti-Virus	Provides services including protection, virus removal, monitoring, and recovery support as anti-virus measures.
End-point Security	Creates an environment that protects customer systems from threats such as leaks of confidential information and virus damage at end-points (terminals of client-connected systems).
e-mail Security	Provides total security assistance needed to use e-mail securely, such as anti-virus measures and preservation of audit trails.
Authentication ID Management	Provides assistance for authentication and user information management, which are the foundations of information security, through various products and services, including biometric authentication, electronic certificates, and directories.
PCI DSS	Provides security measure solutions for helping to ensure compliance with the PCI DSS (Payment Card Industry Data Security Standard).
Thin Client	Provides total client virtualization using cutting-edge devices and secure networks. Also supports work style reforms by enabling mobile use of an extensive range of user devices.
Physical Security	Provides comprehensive solutions for physical security issues in the office.

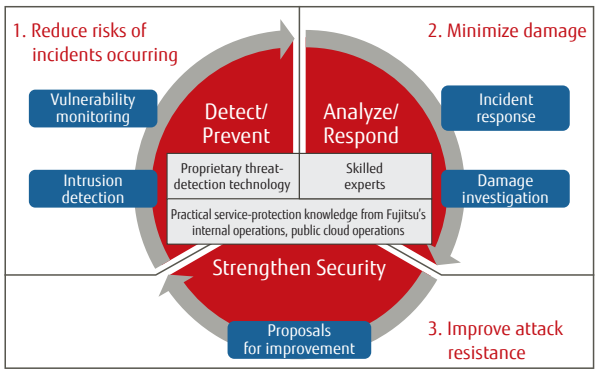
FUJITSU Security Solution–Global Managed Security Service

This service provides total security operation assistance to customers developing their businesses globally. It begins with a setup service, in which the customer's existing system is audited and weak spots are identified. This is necessary before engaging in the security management service, which handles cyber-attacks by providing services that are difficult for customers to perform by themselves, such as 24-hour, year-round real-time monitoring, incident response, and long-term security-management assistance such as training.

Global Managed Security Service

■ Service Concept

The service provides various functions necessary to the three operation processes that are vital elements of cyber-attack response: "detect/prevent," "analyze/respond," and "strengthen security."



■ Service Features

1. Accurate malware detection using proprietary technology

It is essential to introduce highly accurate detection equipment to detect unknown malware. Fujitsu uses a completely new attack detection technology called Malicious Intrusion Process Scan,*1 which is capable of detecting cyber-attacks in progress.

2. Skilled experts

To minimize the damage from a cyber-attack, companies need to continuously develop highly skilled human resources capable of resisting cyber-attacks, which are growing more sophisticated day by day.

Fujitsu develops human resources such as security analysts and forensic engineers through its Security Meister Certification System. These experts are deployed to operate this service.

3. Full use of in-house experience and knowledge

The knowledge and expertise that the Fujitsu Group has accumulated regarding security is concentrated at A3L*2 and used in developing this service.

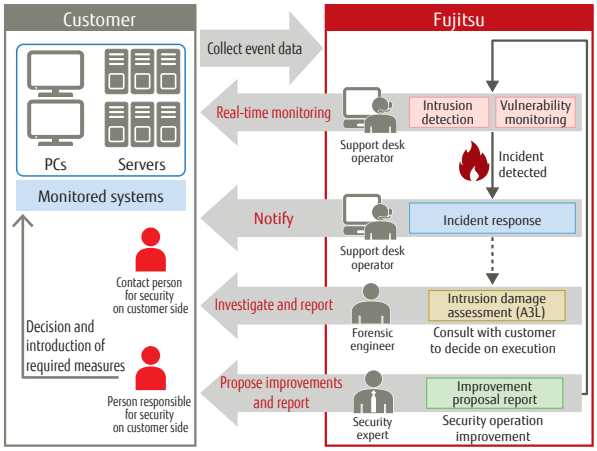
- Investigation and application of the latest technologies
- Expertise acquired from development and construction activities of services and system integrators
- Results from internal implementation in Fujitsu Cloud CERT

*1 Malicious Intrusion Process Scan: A new Fujitsu proprietary technology that markedly improves the detection rate of unknown malware by focusing on the behavioral processes of the attackers rather than those of the malware.

*2 A3L: FUJITSU Advanced Artifact Analysis Laboratory

■ Service Overview

Fujitsu provides a security operation service for responding to cyber-attacks by helping customers with aspects they find difficult to manage without help, such as 24-hour, year-round real-time monitoring, accurate incident response, and continuously strengthening security operations.



Related services

Service	Contents
FUJITSU Security Solution Hidden Malware Survey Service (PC log analysis)	Using technologies from Fujitsu Laboratories, this service can easily investigate malware-infected PCs and the damage status. A service engineer uses Fujitsu's proprietary inspection tools onsite to check for the presence and spread of malware.
FUJITSU Security Solution Malware Survey Service (Network log analysis)	With this survey service, sensors are installed on the customer's network to detect targeted cyber-attacks, and traffic on the customer's network is monitored to look for malware infections or potential infections. Results are reported to the customer.
FUJITSU Security Solution Targeted E-mail Attack Drill Service	In line with training objectives, this service covers developing and carrying out training plans, including examinations of the contents of mock attack e-mail messages. Support includes information on issues that arise during training and support for handling the issues based on past experience, trends in training results and suggestions for improving them.
FUJITSU Security Solution Incident Response Training Service	This service provides training in responding to incidents based on current trends in cyber-attacks, as well as changes in day-to-day security management, the external environment, and attack methods.
FUJITSU Security Solution Security Violation Investigation Service	This service provides a detailed investigation and analysis of a customer's data (HDD images, logs, etc.). By acquiring an accurate understanding of the scope of unauthorized activity by an attacker, such as whether or not an intrusive attack has occurred, the reason for the attack and countermeasures, and the extent of the damage, the service helps customers to clarify their response policy.

Published by
FUJITSU LIMITED

Corporate Affairs & Risk Management Unit
Shiodome City Center, 1-5-2 Higashi-Shimbashi, Minato-ku, Tokyo 105-7123, Japan
TEL: +81-3-6252-2198

Security Management Service Business Unit
Fujitsu Solutions Square, 1-17-25 Shin-kamata, Ohta-ku, Tokyo 144-8588, Japan
TEL: +81-3-6810-6682

FUJITSU LIMITED

http://www.fujitsu.com/global/