Priority Measures

From the perspective of defense in depth, the Fujitsu Group has streamlined its information security priority areas and is aggressively promoting the three priority measure areas of information management, cybersecurity, and physical security.

Three Priority Measures Based on the Concept of "Defense in Depth"

Recent cyberattacks, often experienced as "advanced persistent threats(APTs)" have become more sophisticated, diverse, and complex than in the past, so conventional single-layer security measures are no longer able to completely defend against these.

The Fujitsu Group has adopted the concept of "defense in depth," a multilayer defense mechanism that utilizes several different defense measures instead of one, as its basic concept for information security. Defense in depth has three goals: "Prevent attacks by raising multiple defensive barriers," "Rapidly detect attacks by establishing multiple detection functions," and "Minimize damage after infiltration." By appropriately deploying these, we can prevent attacks and minimize damage.

The Fujitsu Group has adopted three priority security measures to protect internal information, namely "information management," which aims to protect information, "cybersecurity," which is centered on measures that protect systems against cyberattacks, and "physical security," which prevents unauthorized access to offices, factories, and other facilities.

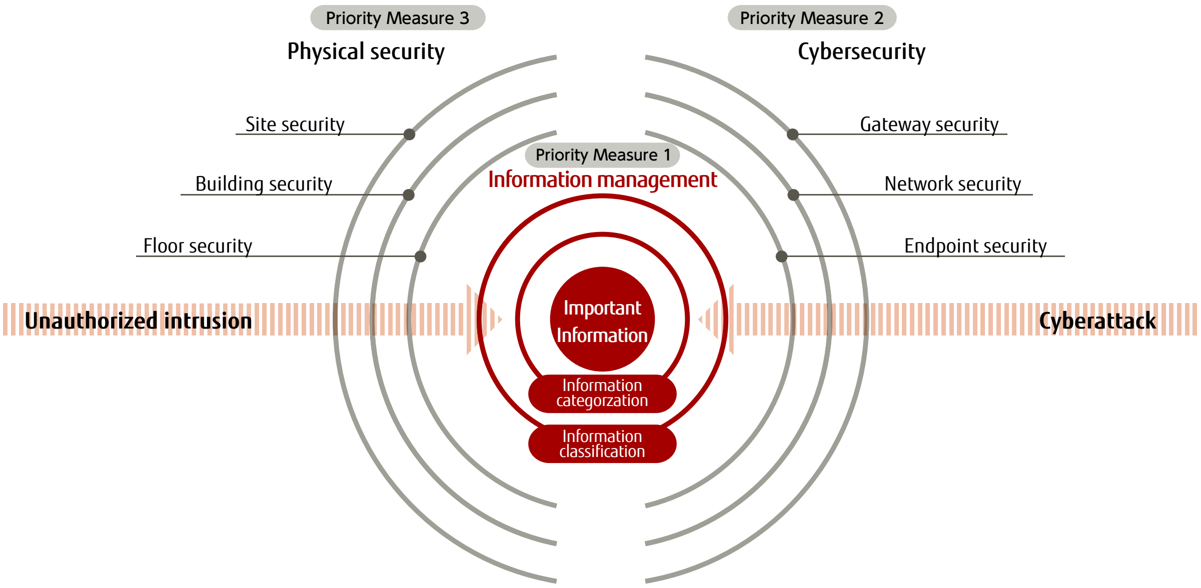
Priority Measure 1: Information Management Security

Information Classification

The Fujitsu Group in Japan has established a set of rules for handling information circulated internally called the Information Management Policy, by which we categorize, appropriately manage, and utilize internally circulated information. In other countries as well, we categorize and manage information according to the situation of each country in a similar manner.

Internal-use-only information and restricted information are managed in accordance with the Information Management Policy, whereas third-party confidential information is managed in accordance with the Third-party Confidential Information Management Policy.

Defense in Depth Conceptual Image



Information Categories

Information Categories			Examples	Personal Information Examples
Public Information			Catalogs, manuals, press releases, public website, etc.	Executive officer information posted on the public website, etc.
Confidential Information	Fujitsu Confidential Information	Internal-use-Only Information	Information other than restricted information • Internal rules, etc.	Organizational chart
		Restricted Information	Information that should not be disclosed to unrelated parties • Information on under development technologies	Human resources information, customer lists, etc.
	Third-party Confidential Information			Personal information received as a result of contracted work

Public Information Public information refers to disclosed items, including public websites, catalogs, and manuals.

Confidential Information Confidential information is categorized into Fujitsu Confidential Information and Non-Fujitsu Confidential information, where Fujitsu Confidential Information is further categorized as Internal-use Only Information and Restricted Information.

Internal-use-Only Information Internal-use only information refers to information that must not be disclosed outside the company, including internal rules and internal reports, etc.

Restricted Information Restricted information refers to information that should not be known to unessential personnel, such as human resource information, information on under development technologies, and customer lists.

Third-party Confidential Information Third-party confidential information refers to information subject to confidentiality by agreement, such as confidential information acquired from customers and other companies through contract agreements, non-disclosure agreements, licensing agreements, and such.

Personal Information Personal information refers to personal information independently acquired by Fujitsu and personal information held by customers that is received by and for which access has been granted to Fujitsu coinciding with services entrusted by the customer for contracted development. Personal Information includes Japan's social security and taxation number.

■ Information Categorization (Public Information, Confidential Information Categories)

Information handled inside the company is categorized as shown in the figure above. We also rank the seriousness with which information should be handled in terms of legal requirements, value, and importance, etc., and, in Japan, we categorize information on four levels, namely public information, internal-use only information, restricted information, and third-party confidential information.

We have defined rules for how information of each category should be handled and protected. Our domestic group companies in Japan conduct on-site audits once per year to determine if the PDCA cycle for managing important information in accordance with these rules is being implemented. Our overseas group companies also categorize information similarly to how we do domestically.

Priority Measure 2: Cybersecurity

The Fujitsu Group implements separate measures at different layers in accordance with the network characteristics in preparation for cyberattacks. Through defense in depth security that combines gateway security measures, which include firewalls and advanced persistent threats(APTs) measures, network security measures, which include unauthorized access detection, and endpoint security measures, which include malware countermeasures and security patch management, we are working to protect against increasingly sophisticated, diverse, and complex cyberattacks.

■ Gateway Security Measures

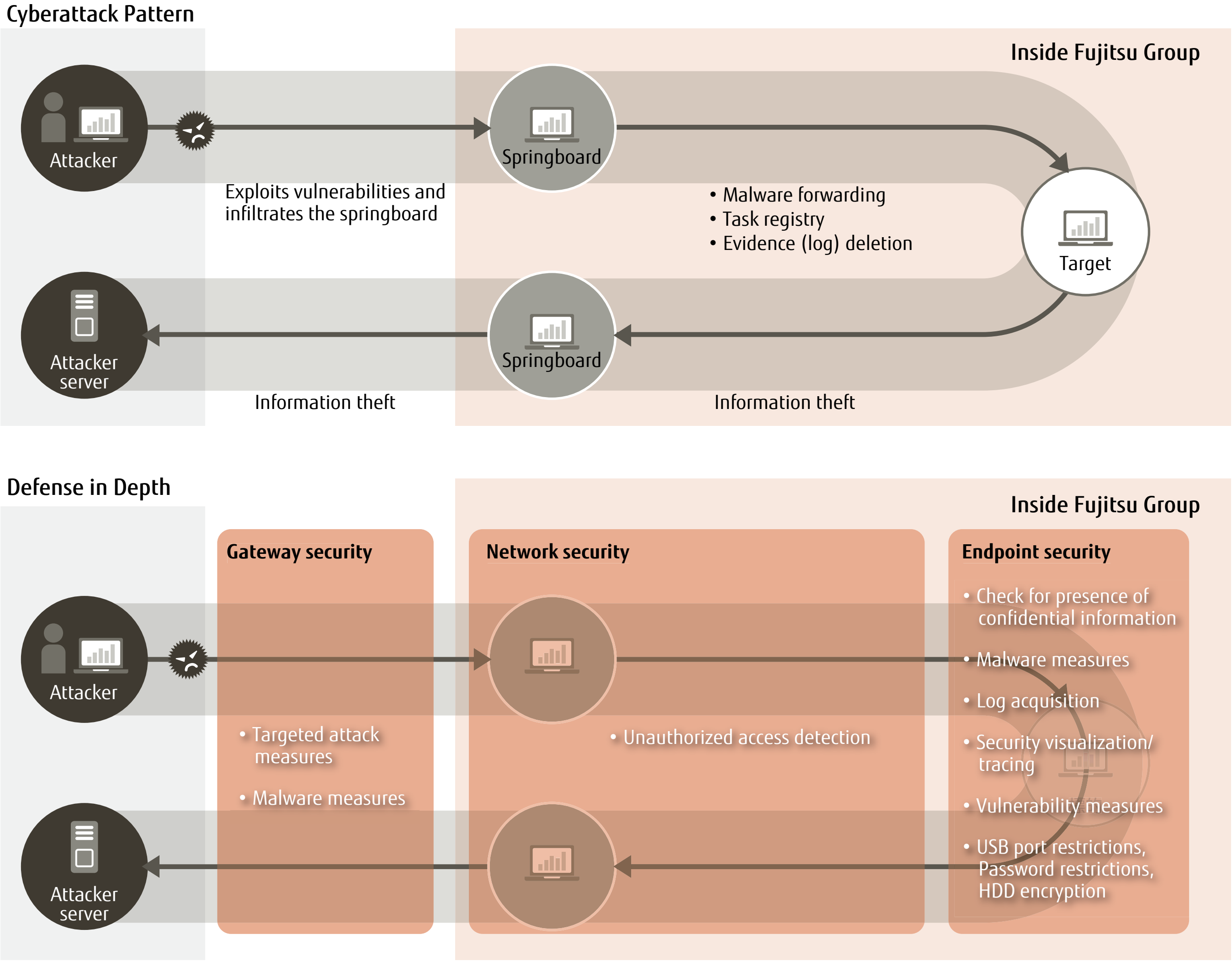
When preventing cyberattacks, it is essential to prevent intrusion from outside. The Fujitsu Group has installed a gateway at the border between the external internet environment and the Fujitsu Group internal information networks, thereby blocking unessential communications from outside to ensure security. Specifically, we have adopted a firewall to protect against unauthorized access to the border with the internet layer, an unidentified malware detection system as a advanced persistent threats(APTs) countermeasure, and monitor e-mail and web communications as entrance/exit measures.

■ Network Security Measures

Whereas conventional cyberattack countermeasures are focused on gateway measures that block intrusion from outside, the recent advancement of cyberattacks, including advanced persistent threats(APTs) has made it increasingly difficult for this approach to fully protect against intrusion from cyberspace. This has made internal measures that rapidly detect threats in the internal network essential.

The Fujitsu Group has installed devices that detect unauthorized internal communications as a measure to detect suspicious communications on its internal networks, and is also demonstrating new technologies under development by implementing these internally as a step towards commercialization and actual operations.

Cyberattack and Defense in Depth Cybersecurity Measures



Endpoint Security Measures

The recent increase in targeted e-mail attacks and other cyberattacks targeting endpoints such as personal information terminals has led to a stronger demand for countermeasures than in the past.

The Fujitsu Group is also adopting and implementing the concept of "defense in depth" for endpoint security, including for employee personal computers and mobile terminals. We have taken the necessary security measures by separating endpoints into individual layers, including malware countermeasures, log acquisition, and HDD encryption. In accordance with the shared global Fujitsu Group Information Security Policy, we manage security by limiting network

Main Endpoint Security Measures

Layer	Security Measures
Data	Confidential information check
Security tools	Malware countermeasures
Logs	Log acquisition
Security patch	Security visualization and tracking
OS	Vulnerability measures
Device	USB port restrictions, password restrictions, HDD encryption

access from personal computers with operating systems for which support is no longer provided.

As an information leak countermeasure, we also apply restrictions so that confidential information, including customer data, cannot be saved to personal computers or written to external media.

Priority Measure 3: Physical Security

We take measures to provide security at sites including factories and on office floors, not just at the entrances of offices. In accordance with the concept of defense in depth, we also apply security measures here that clearly separate the line of flow for employees and visitors in order to strictly control entry and exit. In addition, using security cards and surveillance cameras allows us to capture detailed information for entry and exit, while at the same time enhancing our tracking capability during emergencies. We also take similar physical security measures in other countries in accordance with the situation of each country.

Policy

- Only authorized personnel are allowed on sites, inside buildings, and on floors.
- Regardless of whether the individual is an employee or not, we always capture and record the entry and exit of all personnel.

■ Site Security

In addition to entry and exit security gates at which passage is checked by guards, we detect intrusion via external fence sensors and surveillance cameras to strictly control access, thereby ensuring that only authorized personnel may enter.

■ Building Security

We have implemented entry and exit control at building entrances using security gates and security cards to prevent unauthorized entry.

■ Floor Security

We have separated work areas in which internal networks have been installed from other work areas, and further restricted entry and exit to these areas in order to prevent those without authority from accessing important information. Even when there is an attending employee, for example, anyone other than a Fujitsu Group employee is prohibited from entry to ensure security. Specifically, during entry and exit, security cards are used to authenticate the individual, where palm vein authentication is used when we feel it is necessary to further increase the level of security.

Palm Vein Authentication Security Gate (European Office)