Fujitsu's Approach to Cloud-related Information Security

● Masayuki Okuhara ● Takuya Suzuki ● Tetsuo Shiozaki
● Makoto Hattori

Cloud computing opens up a variety of possibilities but at the same time it raises new concerns about information security. To enable users to safely enjoy the benefits of cloud computing, it is necessary to consider both general measures for information security that have conventionally been employed and information security measures tailored to cloud computing. To address these concerns and enable customers to use Fujitsu's cloud services with peace of mind, Fujitsu is implementing various measures such as establishing information security controls within the Fujitsu Group and introducing advanced information security technologies. This paper describes Fujitsu's security governance of cloud services, its approach to compliance-related issues, and the measures it has implemented to maintain information security.

1. Introduction

The birth of cloud computing as a new computing model opens up new possibilities inconceivable under existing models. At the same time, computing in the cloud is forcing providers of cloud services to reassess information security measures implemented for existing models. This paper discusses how information security is changing with the shift to cloud computing and introduces Fujitsu's approach to providing information security for its cloud services and thus a highly secure and dependable computing infrastructure.

2. Changes in information security

In the cloud, account information and data for many users reside on the same information and communications technology (ICT) resources. Users and providers of cloud services must therefore adopt measures to deal with the variety of threats inherent in such a format.

According to the report of the "Study Group on Infrastructure for Cloud Computing Society"[1] of the Information-technology Promotion Agency, Japan (IPA), typical cloud-related security threats can be summarized as follows.

1) Attacks from outside against ICT resources in the cloud

Given that a large number of information assets are concentrated in the cloud, the effects of cyber terrorism, malicious scans, and distributed denial of service (DDoS) attacks can be considerable. This makes attacks on cloud resources attractive to hackers.

2) Attacks to the outside using the cloud as a steppingstone

In this type of attack, an attacker uses the ICT cloud resources normally used by authorized cloud users as a tool for mounting attacks on sites outside the cloud.

3) Attacks on cloud users from ICT resources within the cloud

Economic denial of service (EDoS) attacks that maliciously use ICT resources to cause monetary losses and information leaks caused

by unauthorized data transfers can also occur within the cloud.

4) Incidents internal to cloud service providers

Malicious actions by individuals within the service provider organization or mistakes in operation by service providers can create security incidents.

5) Malicious use of cloud ICT resources

In this type of attack, users with malicious intentions make use of ICT resources in the cloud for mounting attacks or engaging in some sort of criminal behavior. It has been reported, for example, that ICT resources in the cloud can be used to crack passwords or break codes in a relatively short time at low cost.

6) Incidents in the cloud not related to attacks

Cloud services can also be halted or obstructed by data-center power outages, software or hardware faults, and other unexpected incidents.

In the cloud, there is an area in which information security measures must be robustly implemented from the same technical viewpoint as conventional systems, that is, to protect networks, servers, Web applications, etc. In this area, ideas surrounding information security are essentially unchanged. At the same time, there are aspects of cloud computing that require a radical change in thought when it comes to information security, as summarized by the following two points.

First, measures must be taken to deal with information security risks in relation to new technologies like the virtualization typical of cloud computing. In the cloud, the presence of an information security problem on the virtualization platform that controls the virtualization system can pose a threat to all of the virtual systems residing on that platform. Furthermore, to prevent information from leaking between virtual systems residing on the same platform, these systems must be completely separated and protected.

Second, measures must be taken to deal with information-security risks on the management level as the boundaries between system users, system owners, and cloud service providers change. In the cloud, the boundary between the user's environment and the ICT resources accessible over the network is different from that in on-premise systems, which means that the approaches to operations and security risk management and to information security management have to change.

Thus, in the cloud, both conventional and new ways of thinking about information security must be adopted, and measures must be implemented accordingly. To this end, it is important that users and cloud service providers be aware of their respective scope of responsibility and that they cooperate with each other.

The following sections describe Fujitsu's approach to resolving these cloud-related information security issues.

3. Security governance

A key feature of cloud services is that a number of geographically separated data centers cooperate to provide optimal services in a joint manner. It is therefore necessary that a uniform and controlled information security standard be implemented among these data centers, which can be located anywhere in the world. Fujitsu has established a "Basic Policy on Information Security in Cloud Services" applicable to all data centers including those of overseas group companies. This basic policy provides security governance as described below for all cloud services provided at these data centers.

1) Information security system and roles and responsibilities

The information security system and associated roles and responsibilities must be clarified if information security measures are to be appropriately and accurately implemented.

Although Fujitsu cloud services are managed in units of "regions" as abstractions of

real data centers, Fujitsu has established a global information security system that encompasses these regions in countries throughout the world and has set up a cloud security committee with a Fujitsu board member as chairperson to provide a forum for evaluating risk and making security-related decisions.

Additionally, Fujitsu is constructing a system within the Fujitsu Group for comprehensively and exhaustively dealing with the information security risks of cloud services. This system is made possible through cooperation between the development and operating groups of the cloud-service platform and security departments within the Fujitsu Group.

2) Risk evaluation

Fujitsu considers it an obligation to evaluate security risks for all systems constructed on a cloud-service platform and implemented and operated in accordance with Fujitsu policies. The only systems that are allowed to operate are those that have cleared security criteria—before initial launching in the case of a new system or at the time of a configuration upgrade in the case of an existing system—defined by an independent group of security experts within the Fujitsu Group.

3) Information security management process

Fujitsu has set up an information security management process in units of the abstract regions described above. Each region has the responsibility of maintaining and improving information security standards in accordance with its information security management policy. The cloud security committee is responsible for governing the information security management activities of all regions.

4. Compliance

As described above, the roles of stakeholders (system users, system owners, cloud service providers) and the boundaries between them in the cloud model are considerably different from those in the conventional computing model. It is therefore important to clearly define the division of roles and the scope of responsibilities, which in the past were somewhat vague. In response to this need and to enable its customers to use its cloud services with peace of mind, Fujitsu is addressing compliance-related issues in the following ways.

1) Laws/regulations and agreements

To make it clear that Fujitsu treats with utmost care the important information entrusted to it by its customers, as dictated by laws and regulations, and that Fujitsu is committed to protecting customer rights and interests, the conditions under which Fujitsu accesses virtual systems deployed by customers are clearly specified in agreements and elsewhere. Fujitsu also describes in agreements how it handles confidential information such as customer-specific data that customers register or input in virtual systems. Furthermore, Fujitsu also clarifies in agreements the actions it will take in the event that a customer who has concluded a service agreement with Fujitsu is found to have been intentionally using cloud services in an unauthorized manner.

2) Compliance and auditing

Customer compliance with laws and regulations when using cloud services is a serious matter, and auditing must be performed to determine if and how compliance is being achieved. This makes it essential that logs be appropriately kept so that user access and operations can be examined afterwards. Fujitsu's cloud services provide functions that support customer compliance. For example, the Fujitsu Global Cloud Platform "FGCP/S5" service[2] in Japan ("Global Cloud Platform [GCP] service" overseas) logs the operations performed by Fujitsu system operators and users with manager-level authority, and Fujitsu keeps these logs for seven years to serve as an audit trail.

3) Fujitsu lifecycle management (data governance)

Fujitsu has established policies and

procedures for storing and managing data in cloud services. They are used as a basis for implementing data-preservation measures including those for preventing information leaks and information tampering. For example, to prevent information leaks when a customer releases a virtual system or when physical storage is being disposed of in the FGCP/S5 service, all storage areas that the customer had been using are wiped clean by completely overwriting them. Data saved on storage devices are also protected by a robust 128-bit AES-equivalent storage encryption system.

4) Human resources

Cloud-related security incidents originating in malicious intentions or operating mistakes by personnel associated with the cloud service provider are taken as matters of grave concern. At Fujitsu, all employees who are capable of accessing data in cloud services receive thorough briefings and periodic training on organization policies, procedures, and processes related to security and on their individual roles in protecting data. System engineers, meanwhile, receive technical training on the servers, networks, and other infrastructure components that support the cloud service platform, on secure development techniques, and on the various types of applications provided in the cloud. At the same time, service managers who manage quality across all provided services receive training on Information Security Management System (ISMS) policies and on Information Technology Infrastructure Library (ITIL) concepts and practices to enhance their skills in information security management and data-center service management. Finally, specialist organizations within Fujitsu such as its Computer Emergency Response Team (CERT), which responds to cloud-related incidents, work together with the technical departments that develop the cloud service infrastructure, the monitoring center, and the research laboratories to maintain information security. These organizations also interface with outside expert organizations to enhance information security and deal appropriately with incidents.

5) Vulnerability assessment and patch management

To protect customer systems in the cloud from external attempts to exploit vulnerabilities and gain unauthorized access, Fujitsu performs information security inspections using vulnerability diagnosis software before the launching of customer systems constructed by Fujitsu or customer systems entrusted to Fujitsu for operation. The cloud service platform itself is periodically subjected to vulnerability inspections and penetration tests by specialist organizations, and the signatures of anti-virus software for protecting Web communications and E-mail are regularly updated. Fujitsu has also established policies and procedures with regard to patch management, and it gives priority to security patches provided from vendors for their software while assessing their potential impact.

6) Information security incident management

Fujitsu has established policies, processes, and procedures on the management of information security incidents so that any incident can be rapidly and correctly identified and reported. Plus, in 2010, a Fujitsu Cloud CERT was set up to support the administration of information security for cloud services. This team, which drew up the previously mentioned "Basic Policy on Information Security in Cloud Services," performs security monitoring and security diagnosis of service environments and responds to security-related emergencies in cooperation with departments within the Fujitsu Group and organizations outside the company (**Figure 1**).

5. Information security measures

Fujitsu has implemented the following measures to maintain information security so that customers can use cloud services with peace of mind.

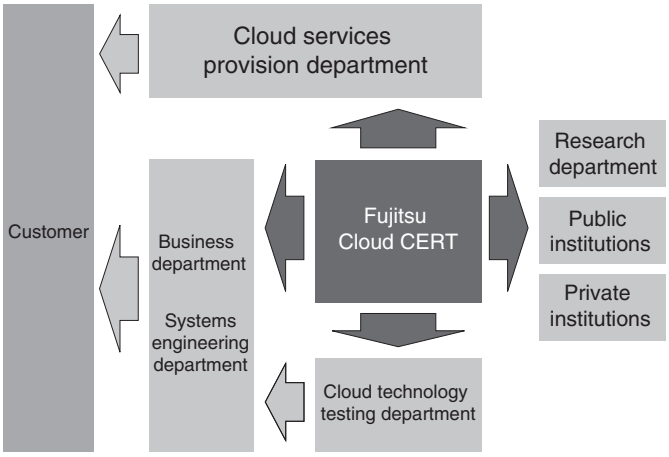

Figure 1
Role of Fujitsu Cloud CERT.

1) Identity and access management

For its cloud services, Fujitsu assigns a unique user identification number (ID) to each system manager at customer companies and prevents unauthorized use of user IDs through a rigorous authentication process. For example, when using a Web portal to make configuration changes, deploy virtual systems, or check operating conditions in the FGCP/S5 service, the user—once user registration has been completed—first downloads a digital certificate for purposes of individual authentication and then logs in using that certificate. The user then applies this digital certificate together with a personal identification number (PIN) of 16 characters or more to complete a two-factor authentication process that eliminates the risk of unauthorized certificate use by another party. Other functions have been implemented to prevent the unauthorized use of user IDs. For example, there is a function that automatically rejects a user who has failed to log in after a certain number of consecutive attempts and a function that requests the user to log-in again with a digital certificate after a session has timed out.

2) Data security

A basic rule of operations at Fujitsu is that an employee performing technical operations on the cloud platform must be identifiable. For example, an employee performing an operation on the FGCP/S5 service must be authenticated by a client certificate. It is also a rule of operations that digital certificates used by customers and those used by Fujitsu staff are strictly divided. This type of client certificate is issued by a digital signature system that appears on the list of ciphers recommended for use in e-government procurement in Japan. Fujitsu is presently using a digital signature system employing the Secure Hash Algorithm-256 (SHA-256) function. Fujitsu also maintains a list of expired certificates to prevent their malicious use.

3) Network security

Fujitsu provides a variety of measures to protect customer systems constructed in the cloud from network security risks. The FGCP/S5 service, for example, logically separates the network environments established for each customer by using a firewall function provided as standard. Furthermore, the internal segments of a customer's system can be logically divided into a maximum of three tiers of virtual networks. This means that a network configuration consisting of three segments—a segment that can be directly accessed from the Internet, a demilitarized zone (DMZ), and an internal segment—can be constructed in the cloud so

that virtual application servers and virtual database servers performing important business operations cannot be directly accessed from the Internet.

Additionally, the virtual firewalls do more than simply control access on the basis of IP addresses and the protocol in use. They can also perform source network address translation (SNAT), which converts the source IP address and port number into a designated IP address and port number, and destination network address translation (DNAT), which converts the destination IP address into a designated IP address. These functions provide for flexible address conversion, enabling segments directly connected to the Internet to be separated from internal segments.

In addition to the above, customers' communications for managing their virtual systems are encrypted using a Secure Sockets Layer Virtual Private Network (SSL-VPN).

4) Monitoring (obtaining and protecting audit logs)

Fujitsu achieves integrated management of cloud services by installing consoles in data centers to consolidate data on cloud platform operations. In the FGCP/S5 service, a variety of daily logs are centrally managed using lifecycle management software (Systemwalker Centric Manager), which enables problems in the system to be visualized and countermeasures to be efficiently implemented.

5) Data center operation

With the aim of optimizing services and maintaining and enhancing quality on an ongoing basis in data centers that support cloud services, Fujitsu systemizes, evaluates, and improves operations and services in accordance with a plan-do-check-act (PDCA) cycle. As a result of these efforts, Fujitsu's advanced Tatebayashi System Center became, in February 2010, the first data center in Japan to be given an "AAAis" information security rating (the highest evaluation in this category) from I. S. Rating Co., Ltd.[3)]

6) Service continuity

Fujitsu has established an incident response plan to deal with incidents that have the potential of hindering the continuity of cloud services. This plan is reviewed periodically as well as whenever a major change occurs in the organization or operating environment.

In addition, maintenance tools and materials covering about 98% of operating equipment and devices are stored on the premises of Fujitsu data centers. Support staff are present at data centers on a 24 hours a day, 7 days a week basis, and a system is followed whereby operators, infrastructure operation staff, and on-site support staff respond immediately to the occurrence of a system problem.

6. Conclusion

This paper described Fujitsu's approach to cloud-related information security. Fujitsu recognizes that cloud computing is still a new field, and it promotes ongoing discussions of security requirements. With the aim of complying with requirements in this new era of computing, Fujitsu will continue to reevaluate and strengthen the information security of its cloud services. The latest trends in cloud security at Fujitsu are described on a public site,[4)] which we sincerely hope our readers will visit.

References

1) Information-technology Promotion Agency, Japan (IPA): Report of the "Study Group on Infrastructure for Cloud Computing Society." March 2010. (in Japanese).
http://www.ipa.go.jp/about/research/2009cloud/index.html
2) Fujitsu: Fujitsu Global Cloud Platform FGCP/S5. (in Japanese).
http://fenics.fujitsu.com/outsourcingservice/saas/plat/sop/
3) Fujitsu: Tatebayashi System Center acquires AAAis rating for information security. (in Japanese).
http://fenics.fujitsu.com/idc/tatebayashi/aaa/
4) Fujitsu: Fujitsu- Approach to information security for the cloud.
http://jp.fujitsu.com/solutions/cloud/concept/pdf/cloud-security-wp-us.pdf

Masayuki Okuhara
Fujitsu Ltd.
Mr. Okuhara is engaged in security planning and operations for cloud businesses.

Tetsuo Shiozaki
Fujitsu Ltd.
Mr. Shiozaki is engaged in security planning and operations for cloud businesses.

Takuya Suzuki
Fujitsu Ltd.
Mr. Suzuki is engaged in the planning, proposing, and publicizing of security businesses.

Makoto Hattori
Fujitsu Ltd.
Mr. Hattori is engaged in the planning, proposing, and publicizing of security businesses.