Security Measures for Cloud Computing

Cloud computing is a new processing scheme to realize the flexibility and agility of computing that is not possible in traditional systems. However, cloud computing presents new security problems, such as security and reliability, to the user. This section introduces the security initiatives implemented in the Fujitsu Cloud Computing Service.

Security in the Fujitsu Cloud Computing Service

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

Security Governance

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

Compliance

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

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

Policies and procedures are defined in relation to maintaining and storing cloud service data, and data preservation measures are implemented such as reliable information leak and information tampering prevention in accordance with these. For example, in order to prevent leaking of information when disposing of information in the on-demand virtual system service, all
of the storage areas that had been used are securely erased by overwriting with zeros when returning a customer virtual system that had been entrusted by the customer and when disposing of physical storage. Furthermore, the data that is saved in the storage is protected by powerful storage encryption schemes that comply with various international guidelines.

**Security Measures**

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

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

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

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

**Security Emergency Response System (Fujitsu Cloud CERT)**

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

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