Dependable Security Service That Takes Advantage of Internal Control Methodology

SHIMIZU Miou, MIYACHI Hitoshi, SAKAGAMI Takeshi, SEKI Masaki

Abstract

Cloud computing, by its very nature, is exposed to a wider range of security threats than conventional enterprise systems. To ensure security, NEC Cloud IaaS features built-in controls to monitor and detect external threats at the operation center. NEC is also cooperating with security specialists to improve the safety of our systems and has obtained internal control assurance reports including SOC 2. This will help reduce the need for customers to deal with internal control audits.

This paper outlines the security services used by NEC Cloud IaaS to protect our customers' data from security breaches.

Keywords

cloud computing, internal control, security service, SOC 2, internal control assurance report, NEC Cloud IaaS, American Institute of Certified Public Accountants (AICPA), ID and access management

1. Introduction

More and more organizations today are moving their IT systems into the cloud, looking to take advantage of the reduced costs, enhanced flexibility, and ease of updating that cloud services make possible.

This rapid expansion of cloud services brings with it new risks. Instituting measures to cope with actual and potential internal and external threats, as well as to adhere to regulatory compliance, is absolutely critical. As computer resources are often shared with other users under the management of cloud service providers, users may find it difficult to assess the actual level of security - the extent to which the security systems in place protect the confidentiality, integrity, and availability of their data.

In this paper, we will discuss the NEC Cloud IaaS cloud platform service's security measures, the commitment to internal control that the company has implemented as a cloud service provider, and the security services it provides to help cloud users perform internal control of their own systems.

2. NEC Cloud IaaS Security Measures

(1) Our concept of security

The NEC Cloud IaaS has been designed to meet all our original cloud security standards and cloud security guidelines (CSA CCM, ISO/IEC27001-27002, FISC, JASA, PCI DSS, etc.). In addition, it has been configured to meet the rigorous security standards issued by other industrial and standardization organizations. At the same time, we are continually working to update our standards to ensure that each service offered in the NEC Cloud IaaS is protected by the highest level of security.

To ensure that the security policies specified for the NEC Cloud IaaS are observed in practice, our internal controls are evaluated once each year by an internationally recognized third party.

We also strive to ensure early detection of threats and vulnerabilities by cooperating and exchanging information with our in-house specialist Computer Security Incident Response Team (CSIRT) and information systems divisions.

(2) Commitment to the internal control assurance reporting system

In order to improve their own internal controls, cloud users need to be familiar with the internal controls implemented by their cloud service provider. However, it can be difficult to fully understand the complex mechanism underlying the cloud, thereby making it more difficult to accurately assess the strength and reliability of the cloud's security.

By having a third-party organization analyze our security from an objective standpoint and provide internal control assurance reports, we are able to obtain an accurate assessment of the effectiveness of the internal controls applied to the infrastructure we build and operate. This means that in order to evaluate the internal controls used in the NEC Cloud IaaS, cloud users simply need to obtain the third-party report. There is no need for customers to try and determine the effectiveness of the internal controls by directly analyzing the NEC Cloud IaaS themselves.

We have adopted a system called Service Organization Control (SOC) Reports established by the American Institute of Certified Public Accountants (AICPA) for the NEC Cloud IaaS. Currently, we are working to obtain the following two certificates (schedule to be available in April 2015).

1) SOC 1

These are assurance reports for internal control of commissioned business pertaining to financial statements and can be used for financial statement auditing of cloud users.

2) SOC 2

These reports are for assurance of internal control pertaining to wider-ranging system risks, while SOC 1 is restricted to assuring the reliability of financial statements. They can be used by cloud users for their own internal control.

In particular, SOC 2 can be applied to internal controls related to overall information security, making it ideal for users who wish to assess the security of the NEC Cloud IaaS.

The assessment information is presented to existing and new customers based on non-disclosure agreements.

(3) Acquisition of other external certifications

In addition to these, we have obtained certifications for the NEC Cloud IaaS from other external certification organizations pertaining to policies, processes, and controls that NEC has built and is operating.

• ISMS (JIS Q 27001)

• PrivacyMark (JIS Q 15001)

Because the NEC Cloud IaaS platform provides many mission-critical services to our customers, it is essential that we maintain the highest level of security in order to ensure the safety and privacy of the data stored in our cloud, as well as the connections used to access and transmit that data.

We have designed the NEC Cloud IaaS in such a way that operation staff will be able to build an optimal system for infrastructure operation and to implement appropriate controls on user access, task monitoring, and so on.

Additionally, to further improve security control levels, we have established an independent internal auditing division to perform periodic audits and make recommendations for improvements.

3. Internal Control of Cloud Users

The NEC Cloud IaaS offers ID and access management services developed based on NEC's extensive experience in internal control system construction, the expertise of our team of security specialists, as the ID and access management technology developed in collaboration with Encourage Technologies Co., Ltd. Capable of strengthening the security and internal control of companies and organizations that use the NEC Cloud IaaS, this ID and access management technology has been implemented in the platform system which offers the services of the NEC Cloud IaaS.

This service offers the following functions to prevent information leakage, insider attacks, as well as any other weaknesses in the system.

3.1 ID and Access Management (work trace management)

The ID and access management service delivers functionality that meticulously records the operation details of the customer's system such as direct operation of databases and alteration of applications, enabling periodic inspections and audits to be performed. All the details of operations made by the customer's staff are recorded with movies of screen transitions, as well as text.

This functionality automatically records the system operation screens of each individual and simultaneously collates them with operation history information such as operation logs. This data is then stored, enabling real-time detection and reporting of breaches and other suspicious activity, thereby preventing security incidents in advance by detecting and reporting misconducts in real time before they happen. The results are recorded so that they can be searched and played back, allowing the data to be utilized for internal and exterior audits. Taking advantage of this functionality helps reduce security risks such as information leakage or data breaches - whether they stem from a weakness in the system or from wrongful or erroneous operation, as well as providing the tools and data needed for more comprehensive and reliable system inspections and audits.

This functionality is the result of joint development with Encourage Technology - Japan's top vendor of system trace audit tools - for their ESS REC.

Function details 1:

Access permission without password entry

When an operator with access permission accesses the server under the administration of the ID and access management server, the ID and access management server automatically changes that server's password and automatically facilitates connection using the newly changed password. This process is repeated every time an access is made.

The server under the administration can only be set with a password automatically allocated by the ID and access management function. Access via any route other than the ID and access management server is prohibited (**Fig. 1**).

Operators can only access servers for which they have access permission, and it is virtually impossible to use that server as a stepping stone to access other servers.

Function details 2:

Detailed operation recording with movies and text

When administrating a system, there is no getting around the fact that special privileges (privileged ID) are required in order for a user to be able to directly work with applications and databases. However, this makes it necessary to take steps to mitigate the risks posed by the potential abuse of these privileges or by careless mistakes that can lead to loss or destruction of data.

Of particular importance is establishing effective controls over authorized personnel who possess high levels of technological expertise. In order to maintain effective control over usage of privileged IDs by system administrators with advanced technological knowledge, it is important that, in addition to the utilization of IT-based solutions, emphasis be placed on the development of a means to immediately detect unauthorized use of user privileges or errors caused by user carelessness.

Detailed operation records are an effective and important means (**Fig. 2**) of objectively judge the validity of tasks in system operations.

Closely inspecting and auditing operational details and results makes it easier to spot anomalies such as operations being executed that have no apparent justification or that appear to have been executed in error. Once an invalid operation has been detected, appropriate countermeasures can be implemented.

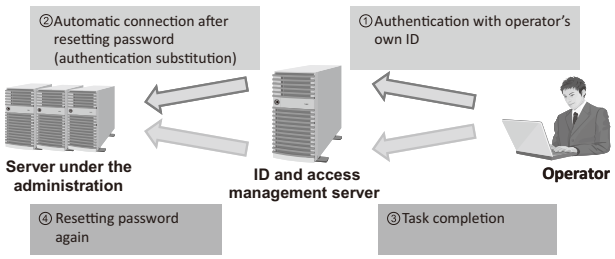

Fig. 1 Access permission without password entry.

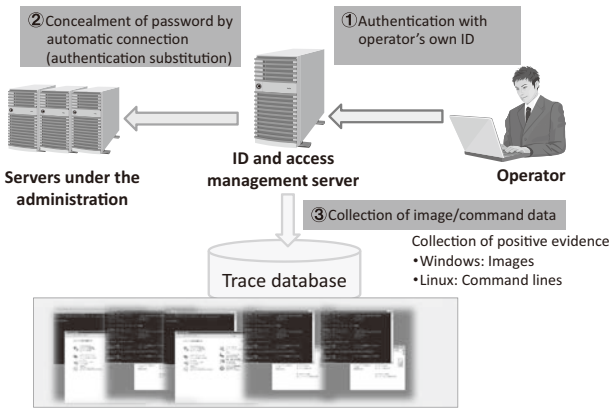

Fig. 2 Detailed operation recording with movies and text.

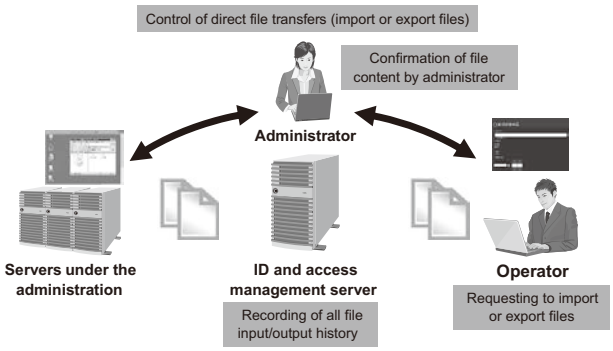

Fig. 3 Control of file transfers.

Function details 3:

Control of file transfers

When access to a server is managed by the ID and access management server, this also includes control over file imports and exports. Preventing files from being transferred without permission (either to or from the server), information leakage can be prevented.

Importing or exporting files is managed by the ID and access management server the first time a user attempts to do so. Subsequently, file transfer is possible when the administrator gives permission.

Files that have been imported or exported are all recorded in the server's history, preventing an operator from taking confidential information out of the server without the administrator's permission (**Fig. 3**).

Function details 4:

Incorrect login management function (log collation)

The ID and access management service includes an incorrect login management function (log collation) to enhance security capability. This function gathers login history from servers to detect the presence or absence of incorrect accesses. This makes it possible to perform early detection should illegal external access or unauthorized internal access occur.

Moreover, if a prohibited or unauthorized operation is performed, the alert function for prohibited commands immediately detects it and alerts the administrators. This makes it possible to immediately cope with any prohibited operations, as well as alerting the administrators to any unauthorized operation executed by an authorized operator, enabling them to deal with it without delay.

4. Conclusion

In this paper, we have reviewed the security measures implemented in NEC Cloud IaaS, as well as the other security services that provide robust constructions to our customer's systems by employing NEC's extensive experience in internal control system construction.

We are committed to providing the NEC Cloud IaaS with the functionality necessary to easily and efficiently reinforce standardized internal controls in our customers' systems.

Authors' Profiles

SHIMIZU Miou
Executive Specialist
Service Delivery Division

MIYACHI Hitoshi
Manager
Service Control Department
Service Delivery Division

SAKAGAMI Takeshi
Assistant Manager
Service Control Department
Service Delivery Division

SEKI Masaki
Assistant Manager
Service Control Department
Service Delivery Division

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.9 No.2 Special Issue on Future Cloud Platforms for ICT Systems

Vol.9 No.2
June, 2015

Special Issue TOP

NEC Information