Cloud-based File Encryption Service - ActSecure Cloud Secure File Service -

KAGEYAMA Tetsuya, SUZUKI Akio

Abstract

This paper introduces the Cloud Secure File Service. This is a SaaS service that encrypts the electronic files of an enterprise as a countermeasure against information leakages. The service is based on the InfoCage FileShell of file encryption software. It provides a management server function in the cloud environment and offers file encryption based on the DRM technology in collaboration with the Azure Information Protection service of Microsoft and the clients installed by the enterprise user. While previous systems specifically had freedom of customization but had to use labor in designing policy and building and operating a management server, this service is designed as enterprise user friendly by the strategy of offering the in-house operations knowhow of NEC and by providing a pre-built cloud environment.

Keywords

security, information leak countermeasure, file encryption, cloud, service

1. Introduction

In their publication, the "10 Major Security Threats 2017," the Information-technology Promotion Agency of Japan (IPA) rank the threats related to information leakages as of the 1st and 5th magnitude. As seen with some cases of service outages caused by information leakages, such threats are increasingly mounting harmful social effects (**Table**).

Table Information security ranking in 10 Major Threats (IPA).

2016 ranking	2017 ranking	Threats of organization
1st	1st	Information leakage via targeted attacks
7th	2nd	Damage by ransomware
3rd	3rd	Theft of user information from web services
4th	4th	Service shutdown by denial-of-service attacks
2nd	5th	Information leakage by insiders and subsequent service outages
5th	6th	Website falsifications
9th	7th	Unauthorized login to web services
Out of ranking	8th	Disclosure of vulnerabilities of IoT devices
Our of ranking	9th	Commercialization of cyberattacks (underground services)
8th	10th	Unauthorized use of Internet banking credentials and credit card information

Most of the cases of information leakages from organizations are caused by "targeted attacks" or "internal fraud." Considering the complication of targeted attacks and the amended personal information protection act, the risk of leakage of an organization's confidential information (both technical and personal) is tending to increase further. The escalation of risks in the business management sector is also increasingly evident.

NEC has been providing an information leakage prevention countermeasure in the form of the file encryption software InfoCage File Shell since 2010, which has already been used by 500,000 persons, including many from within the NEC Group. Recently, NEC has started to market the "Cloud Secure File Service based on the InfoCage FileShell." This is a SaaS type security service ActSecure.

2. Mechanisms and Issues of InfoCage FileShell

The base product of the service introduced here, the InfoCage FileShell is a software product that enables permanent file protection using DRM (Digital Rights Management: a digital copyright management technology). More specifically, it employs RMS (Rights Management Services) issued by Microsoft (hereafter MS) to provide a DRM platform in the Windows environment. The document protection functions using MS RMS include the Office IRM (Information Rights Management) also issued by MS. The InfoCage FileShell features the following function extensions from the Office IRM to provide the user with a file protection mechanism without imposing the need to execute special operations (**Fig. 1**).

- Compatibility with apps other than MS Office
- Thorough application of uniform protection rules in-house (provision of a controlled environment)
- Document protection linked with document management server
- Auto application of protection rules to files distributed in personal local environments
- Provision of extended log system

Construction of management servers environment in the customer's network is required to implement file protection with the InfoCage FileShell. As a result, it has been adopted by large to medium-scale enterprises that are capable of building and operating such an environment. Nevertheless, the information leakage threats occur regardless of the business scale. NEC has therefore developed a SaaS type security service based on the InfoCage FileShell so that an assortment of customers can utilize the file protection mechanism available with the InfoCage FileShell. The service became available in June 2017 (**Fig. 2**).

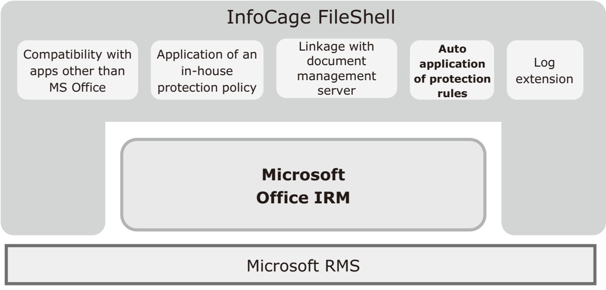
InfoCage FileShell
Compatibility with apps other than MS Office
Application of an in-house protection policy
Linkage with document management server
Auto application of protection rules
Log extension
Microsoft Office IRM
Microsoft RMS

Fig. 1 Relationship between InfoCage FileShell and MS RMS.

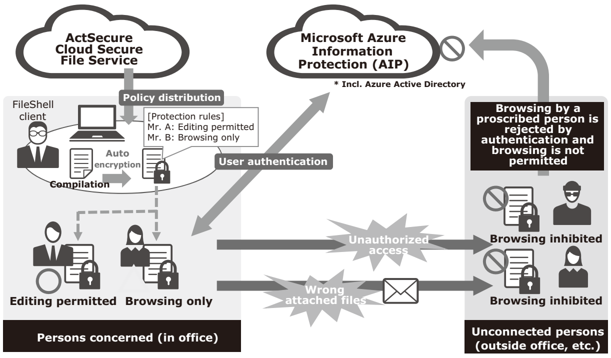
ActSecure Cloud Secure File Service
Microsoft Azure Information Protection (AIP)
* Incl. Azure Active Directory
Policy distribution
FileShell client
[Protection rules]
Mr. A: Editing permitted
Mr. B: Browsing only
Auto encryption
Compilation
User authentication
Browsing by a proscribed person is rejected by authentication and browsing is not permitted
Browsing inhibited
Unauthorized access
Wrong attached files
Browsing inhibited
Editing permitted
Browsing only
Persons concerned (in office)
Unconnected persons (outside office, etc.)

Fig. 2 Outline of ActSecure Cloud Secure File Service.

3. Technical Features of Service

The service introduced in this paper has three features that differ from those of the InfoCage FileShell.

- No need of building management servers in the customer environment
- Azure Information Protection (AIP) used as the authentication platform and provided within the service
- Management policy based on the in-house expertise of NEC

The first feature is that this service frees the customer from the need of preparing management servers (management server, RMS server and database) that is required in installing the InfoCage FileShell. This facility contributes to a reduction in the introduction period as well as of the costs associated with server installations and the workload associated with server operations.

The second feature is that this service includes MS RMS, which the InfoCage FileShell utilizes as the authentication platform. The result is that as with the first feature, this frees the customer from building and managing an environment for using the service.

The third feature is that NEC itself has introduced the InfoCage FileShell and uses it as an information leakage countermeasure and feeds back the acquired knowledge within the service. Specifically, the service prepares the file protection policy required for the operation in advance and has the customer follow its rules in order to reduce the burden of developing a policy. The following sections will describe these features in more detail.

3.1 Provision of a Cloud Environment Service for FileShell Servers

The InfoCage FileShell is composed of agents and the management server that supervises it. The management server is composed of the client management function and database. The implementation of management servers in the cloud environment has made it unnecessary to install a management server in the customer network. Additionally, the entire system is organized to enable efficient, centralized and integrated management, e.g., by integrating the provided functions that can be shared among several enterprise users in the cloud environment.

While the InfoCage FileShell works in linkages with MS

RMS, this service substitutes this operation by utilizing the AIP from the same MS. Since the AIP is a cloud service, the RMS server does not need to be built. Management-related servers other than the AIP are built using NEC's Cloud IaaS cloud service platform by considering the safety, availability and efficiency.

The service platform introduced in this paper is designed and built safely and securely by complying with NEC's in-house secure operations and development guidelines and by adopting periodical security diagnoses in addition to the system configuration and settings.

3.2 Details of Linkage with Azure

As described above, this service adopts MS AIP as the authentication platform and provides it within the framework of the service. The customer does not need to perform any preparation work, including the Azure setting, except for filing the necessary information. While the AIP requires entry of an ID password for authentication, this service introduces a proxy authentication (single sign-in) mechanism in advance, so as to avoid the necessity of Azure authentication at every file access and provides a safe file encryption environment with a reduced usage burden for the customer.

3.3 NEC's Operation Knowhow in Service

The InfoCage FileShell is capable of customizing policy at the time of introduction, including that of handling encrypted files (extensions to be protected, folders to be encrypted automatically and of controlling apps etc.), according to the departmental and organizational needs of the customer. However, the service introduced here is provided in a simpler form, using a unique policy by limiting the setting flexibility and linking with the customer's inherent system, so that it can be used safely and efficiently by many customers. Our policy is defined based on the operations achieved by hundreds of thousands of machines in-house at NEC and our experience in the sale of the InfoCage FileShell to 500,000 IDs. This has enabled us to offer support to the wide range of OS and environments used by customers and encouraging use by as large a variety of customers as possible.

Service policy of Cloud Secure File

- Only one encryption policy can be used per contracting enterprise.
- The authority of clients is limited to the following three functions:

  Privileged administrator with permission to decrypt:

  General use with operational authorization other than for decryption:

  Restricted user, permitted only to browse files.

In the case of a public service, it is naturally impossible to satisfy all of the requirements of individual customers. However, NEC has defined and provided a policy that can be accepted by as many customers as possible, based on past operational and marketing experience.

4. Enabling Safe Operations in the Cloud Service

In the provision of the cloud service, we have each customer express the precise conditions of use and we are then able to provide a cloud environment that has the each customer's information. We have prepared a consultation service that receives modification requests and inquiries from customers and executes changes or answers questions. In addition, to prepare for an accidental occurrence of fault in the cloud environment, we maintain a system that monitors the equipment day by day and, in case of a problem, informs the customer and attempts recovery. Furthermore, we also conduct the operations that are required for providing functions via the Internet by collecting the latest security countermeasure information as desired. At the time of implementation as a cloud-based service, we also add a function for checking the number of IDs reported by each customer and that for holding periodical communications with each client in order to provide a safe and secure service.

5. Future Perspectives

We are planning to add the functions already implemented by the InfoCage FileShell to the ActSecure Cloud Secure File Service. The service will also be enhanced in the future, e.g., by adding higher-level services permitted under the policies of individual customers.

With the ActSecure SaaS type security service, we have already provided services other than the Cloud Secure File Service introduced here. These are: the cloud mail security service that provides transmission/reception functions for countermeasures to deal with spam mail, viruses, targeted attacks and wrong transmissions, the cloud WAF (Web-Application Firewall) service that protects web servers in the application layer, the cloud sandbox service that provides the sandbox function of UTM (Unified Threat Management) products remotely and the cloud DDoS (Distributed Denial of Service) service that provides protection against DDoS attacks.

Security measures of enterprises encounter various settings in addition to surveillance of Internet communications and devices. These include, information handling,

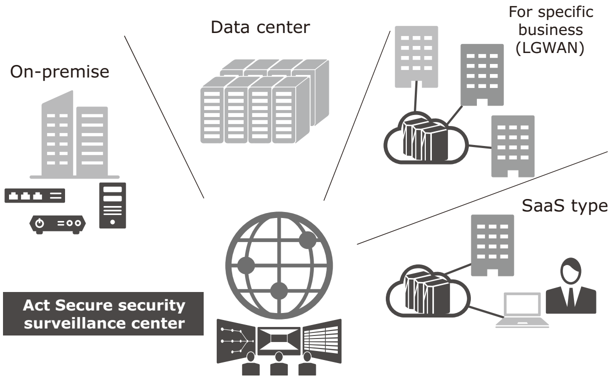
Data center
For specific business (LGWAN)
On-premise
SaaS type
Act Secure security surveillance center

Fig. 3 ActSecure Total Security Service.

in-house security management and incident responses. In the future, we will provide a variety of services that will contribute to the security measures of enterprises as an ActSecure Total Security Service (**Fig. 3**) at any time.

* Microsoft and Windows are registered trademarks of Microsoft Corporation in the U.S. and other countries.
* All other company names and product names that appear in this paper are trademarks or registered trademarks of their respective companies.

Authors' Profiles

KAGEYAMA Tetsuya
Manager
Smart Networks Division

SUZUKI Akio
Senior Expert
Smart Networks Division

The details about this paper can be seen at the following.

Related URL:

InfoCage FileShell
http://www.nec.com/en/global/prod/infocage/fileshell/

NEC Cloud IaaS
http://www.nec.com/en/global/solutions/cloud/infrastructure_service.html

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.12 No.2 Cybersecurity

- Building Futureproof Security to Support Business Safety and Reliability -

Social trends & NEC's approach

Cybersecurity solutions

Applications of AI technology to cybersecurity

In-house efforts provide safety and security for customers

\Orchestrating a brighter world NEC
NEC Technical Journal
Cybersecurity
- Building Futureproof Security to Support Business Safety and Reliability -
Vol.12 No.2

Vol.12 No.2
January 2018

Special Issue TOP