Secure File Transfer Service for the NTT Group

Hirofumi Abe†*, Hiroaki Isaka, Koji Morishita, and Takahiko Nagata*

Abstract

The "occrue" service, which began in January 2009, is a means of sharing important information and high-volume data such as customer information, facilities information, and administrative information among the NTT Group companies and their clients by using a scalable secure file transfer platform system.

1. Need for a secure file transfer service

The NTT Group is developing an extensive range of business that involves the exchange of various kinds of private information, such as customer, facility, data, and administrative information. In the NTT R&D Division, patent information and confidential information related to system development and maintenance management is exchanged. One widely used tool for information transfer is email. Although this is highly convenient and can be sent anywhere in the world, there are major problems such as security vulnerabilities—for example information leaks caused by sending to unintended recipients—and eavesdropping of unencrypted messages (**Fig. 1**). Moreover, files attached to email are generally limited to a size of a few megabytes. Although files that exceed that limit can be transferred using Internet services, some of those services have uncertain safety levels and their use creates a risk of information leaking. Furthermore, while there is increasing use of encryption and password-protected documents in email attachments, there remains the risk of the encryption being broken by cryptoanalytic tools or other means.

The NTT Information Sharing Platform Laboratories has been working on the development of a Scalable Secure File Sharing System (SSS) [1] since 2005. This service can send and receive files as large as 100 GB with authentication of the sending and receiving users, encryption of the transmitted data, and restriction of recipients to a closed transmission path. All this is done transparently as far as users are concerned (**Fig. 2**). To implement secure file transfer for NTT Group companies and their clients, we collaborated with NTT Communications and NTT Comware to develop the "occrue" service. In this article, we describe the service, its special features, and the sharing rules.

2. Internal control for secure file transfer

SSS was previously intended for safe and reliable file transfer for end users (Fig. 2). That left it to the end user to take security measures. However, the security managers of the various companies expanded on that system to create internal control that allows one-stop management of end users and organization policies (**Fig. 3**). This ensures that the end user automatically follows the policy set by the security manager before sending a file, so secure file transfer is consistent with the scope of that policy. In particular, in cases where there is risk of an information leak, such as when sending a file to a guest in the system or when performing traceability control for information sent outside the company, the circumstances of file transfer can be controlled by specifying the means of internal control.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan

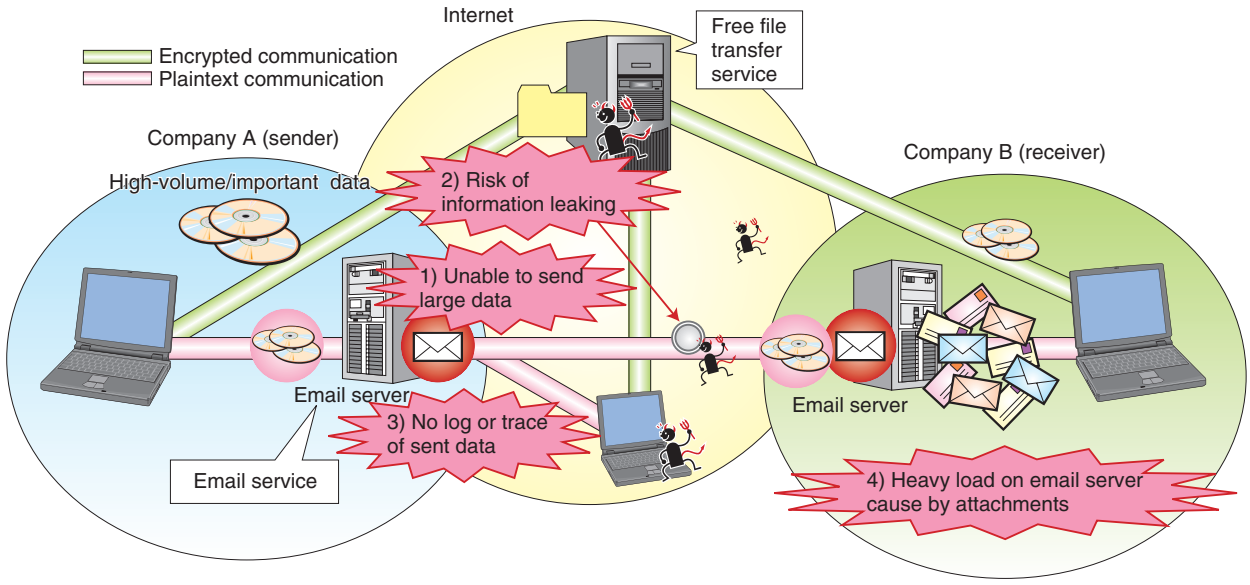

Fig. 1. Problems with email and Internet file transfer services.

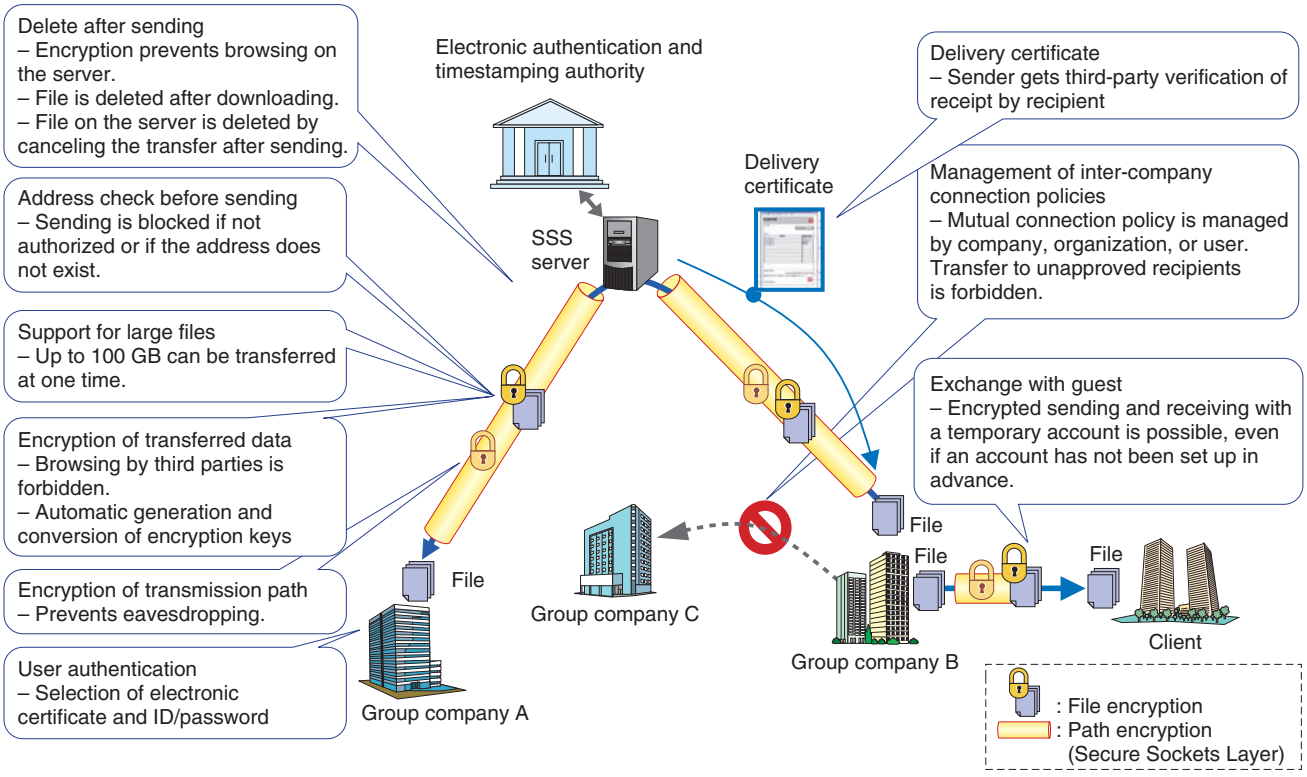

Fig. 2. Overview of secure file transfer service.

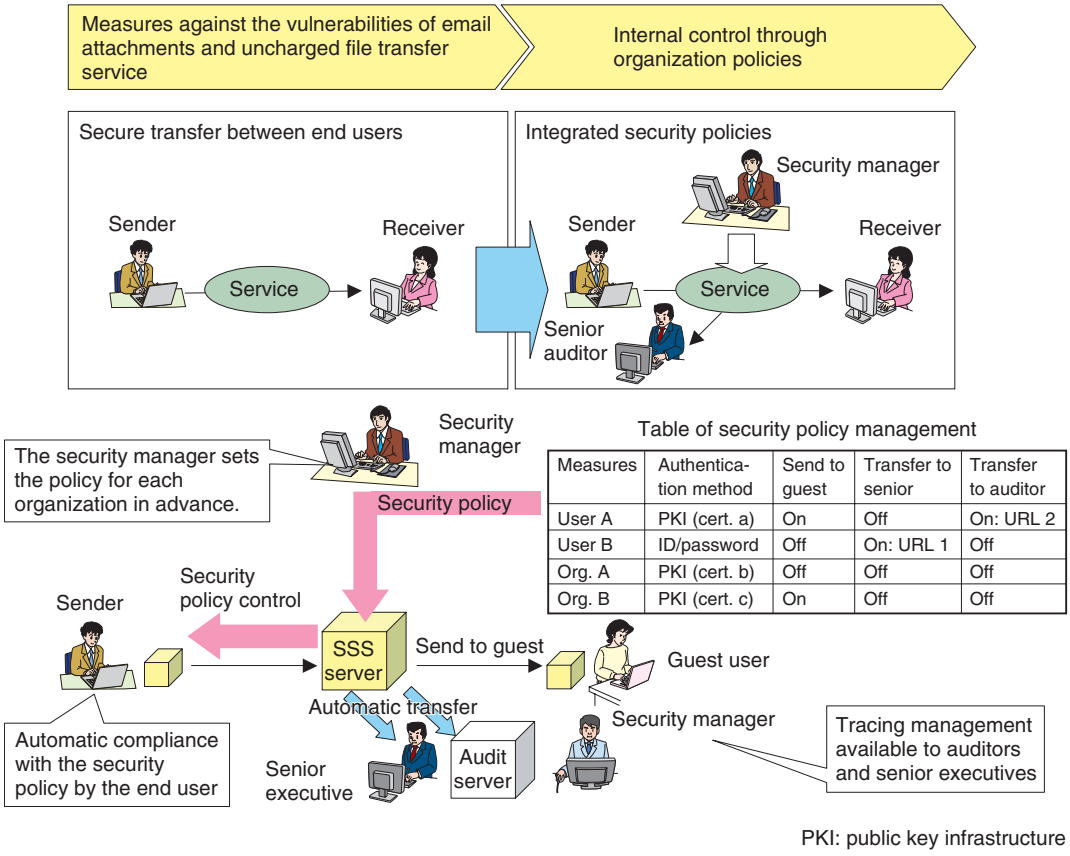

Fig. 3. Extension for internal control.

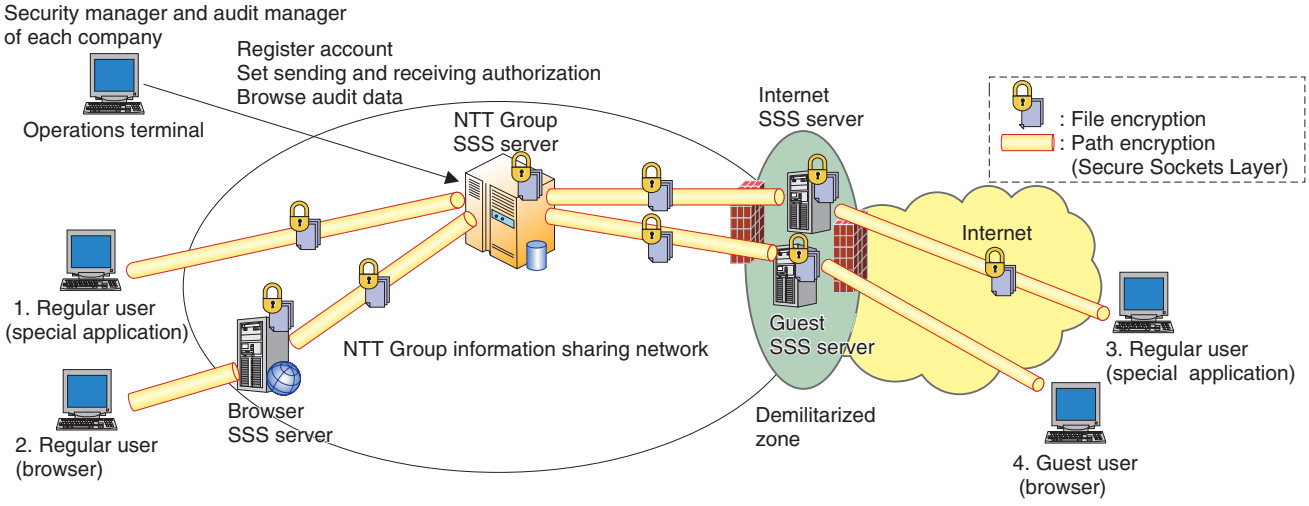

Fig. 4. Overview of the occrue service.

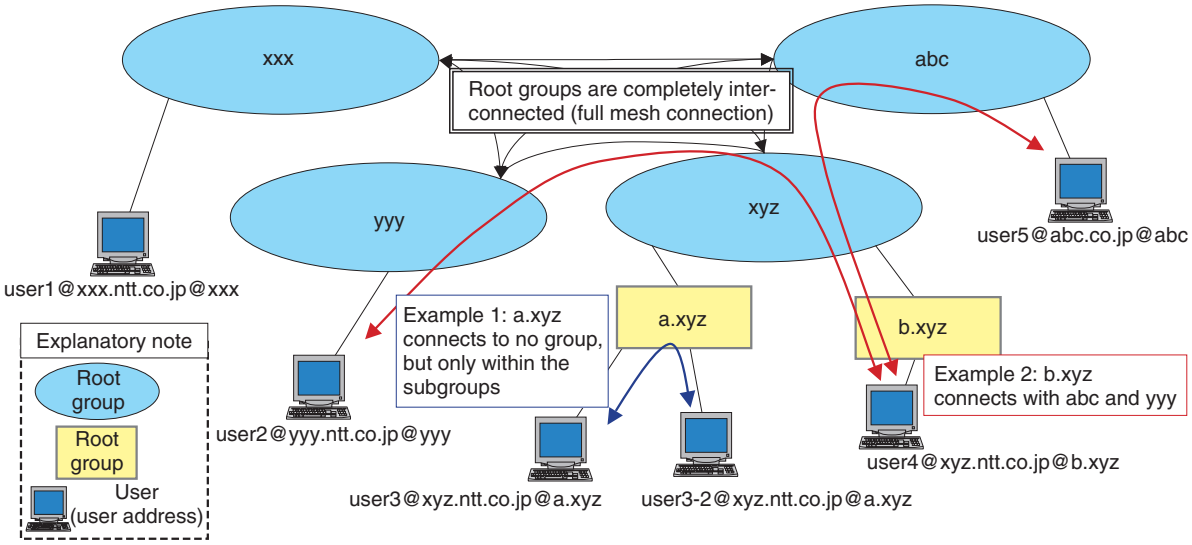

Fig. 5. Mutual connection among NTT Group companies.

Secure file transfer user address standard

The user address used in secure file transfer is specified below.

<user name>@<full group name>
(1) (2)

(1) User name:
This is a "secure file transfer user name" that uniquely identifies a user (client) (The user's email address is used.) or an "alias" used for the same communication.

(2) Full group name:
This is the Group for specifying data management, the scope of file sending and receiving, and the routing for secure file transfer. When it is the root group itself, a subgroup of the root group may be specified.

Example: user1@xxx.ntt.co.jp@xxx
(1) (2)

Example: user4@xyz.ntt.co.jp@b.xyz
(1) (2)

Point of caution: One user is assigned a unique user address.

Fig. 6. User address structure.

3. Occrue service and sharing rules

An overview of the occrue service is presented in **Fig. 4**. This service provides secure information transfer from one end to the other end, including the network, through the use of an SSS server placed on the NTT Group information sharing network [2]. It focuses on secure information transfer among NTT Group companies, issuing regular occrue user accounts for NTT Group employees and collaborators and temporary ad hoc occrue accounts for guest users (mainly clients and customers). The regular accounts connect via the NTT Group information sharing network, and authentication by a client certificate is provided for stronger personal authentication. Guest user accounts, on the other hand, can connect via the Internet with a one-time password.

The occrue service implements root groups for companies, which are similar in concept to email domains. Root groups serve as units for mutual connections among companies, account management, sending and receiving authorization, contracts, and so on. Groups include root groups and subgroups. Subgroups can be defined hierarchically below root groups. This service provides full-mesh connection between root groups for data transfer among NTT Group companies, but subgroups are assumed to provide local connection for the companies cooperating with each Group company. Each Group company can define the connection rules according to its own policy (**Fig. 5**).

The user addresses for this service have two parts: the user name and the full group name. For the user name, we use the user's company email address. The full group name is defined as the root group and the company-assigned subgroup (**Fig. 6**).

4. Future plans

We aim to improve security by increasing the utility to each company in the Group even more and will develop applications for interworking with commercial email programs. Specifically, we intend to reduce the inconvenience to the user by automatically invoking the SSS client when an email arrival notice is received and to improve usability by integrating the data sent and received in a dual management system of the email program and SSS client.

References

[1] K. Yoshida, M. Tanikawa, K. Takaya, K. Morishita, and H. Fujiwara, "Scalable Secure File Sharing System," NTT Technical Review, Vol. 4, No. 10, pp. 60–65, 2006. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200610060.pdf
[2] occrue Department, "occrue Service Specifications 1.0," 2008.

Hirofumi Abe
Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees from the Faculty of Instrumentation Engineering, Keio University, Kanagawa, in 1994 and 1996, respectively. He joined NTT in 1996 and is currently engaged in the development of an information security platform.

Hiroaki Isaka
Senior Researcher, Application Platform SE Project, NTT Information Sharing Platform Laboratories
He received the B.S, M.E., and Ph.D. degrees in physical chemistry from Waseda University, Tokyo, in 1985, 1987, and 1998, respectively. He joined NTT Basic Research Laboratories in1987. He moved to NTT Communications in 1999. From 1999 through 2007, he was with CommerceNet Japan and Rosettanet Japan promoting an RoHS-compliant EDI standard. He moved to NTT Information Sharing Platform Laboratories in 2007 and has managed the engineering and development team of SSS since then. He is a member of Chemical Society of Japan.

Koji Morishita
Research Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.
He joined NTT in 1985 and engaged in research on IP networking structure and the measurement of service quality. He is currently engaged in the development of an information security platform.

Takahiko Nagata
Research Engineer, Application Platform SE Project, NTT Information Sharing Platform Laboratories.
He received the B.E. and M.E. degrees from the Faculty of Instrumentation Engineering, Hiroshima University in 1993 and 1995, respectively. He joined NTT in 1995 and is currently engaged in the development of an information security platform.