

DataBridge: Technology to Transfer Data Securely and Efficiently Between Terminals Connected to Different Networks

Hiroyuki Adachi, Nagatoshi Nawa, Fumihiro Yokose, Kimio Tsuchikawa, and Akira Inoue

Abstract

NTT Access Network Service Systems Laboratories is working on enhancing operational efficiency and reducing operational errors. In this article, we introduce our product called DataBridge, which enables data to be transferred securely and efficiently between terminals connected to different networks.

Keywords: data transfer, security, operational efficiency

1. Introduction

Companies use various operation systems (OpSs) to improve operational efficiency and ultimately reduce costs. For the most part, OpSs are applied to typical operations in which the volume of business is large rather than to atypical operations in which the business volume is comparatively small. Atypical operations occur less frequently, but their total business volume is not insignificant because there are many types of such operations. To further improve operational efficiency, we need more than ever to address the issue of improving the efficiency of operations that are difficult for OpSs to handle.

NTT Access Network Service Systems Laboratories is proposing *client side cooperation* as a solution to this issue. This solution enables OpSs to cooperate with each other through terminals rather than through system servers or networks. It has a minimal impact on OpSs and can be applied flexibly according to operations because it is applied on the client side. We have developed DataBridge as one of the elemental technologies of client side cooperation.

2. DataBridge outline

It is often the case that networks used within a corporation cannot be interconnected mainly because of security constraints. Networks for OpSs are designed to transfer only necessary data, and mission-critical tasks will not be affected even if OpSs are not connected to the Internet. However, in some atypical operations such as sending e-mail with attached files that are stored only in OpSs, there is a need to exchange data between different networks.

In such cases, data are currently transferred by manual operations such as using universal serial bus (USB) flash drives, or by printing the information on paper and manually inputting it. DataBridge allows transfer of data between terminals that are not interconnected via a network, based on the concept of client side cooperation. It ensures that data will be transferred securely and efficiently, which is not the case with the conventional approach of using USB flash drives or manually inputting data printed on paper, as shown in **Fig. 1**.

In general there is a trade-off relationship between

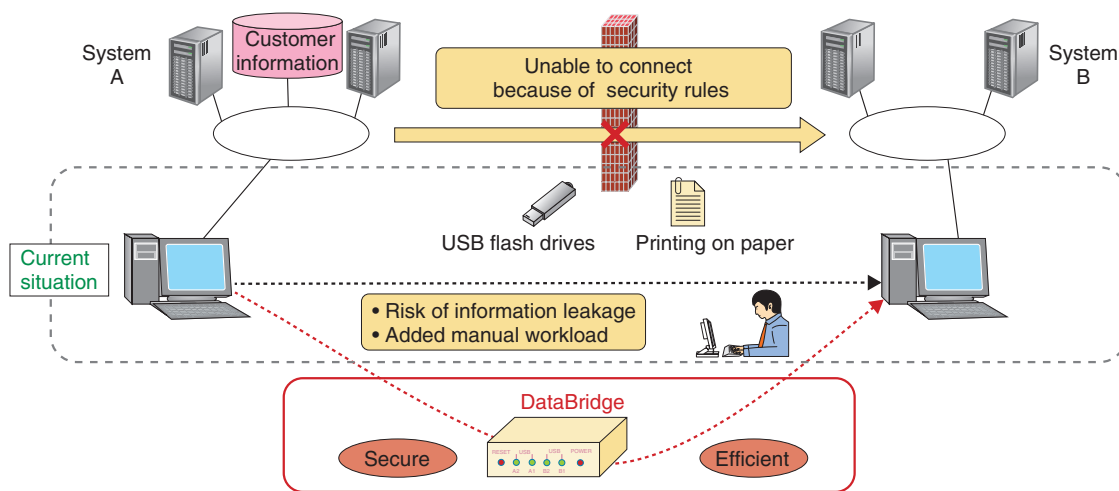


Fig. 1. Schematic of DataBridge.

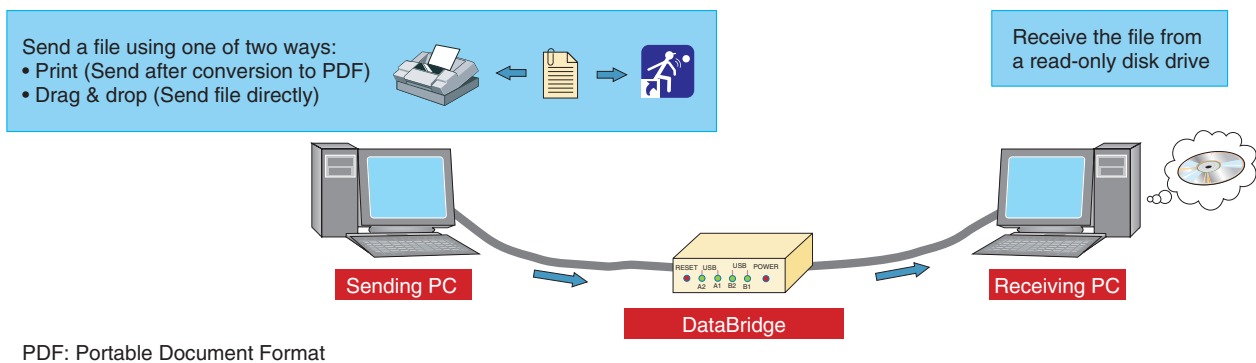


Fig. 2. Utilization of DataBridge.

security and convenience. However, using the various functions of DataBridge enables users to obtain the most suitable balance with respect to security criteria and business content.

3. DataBridge mechanism

DataBridge is software for general purpose personal computers (PCs). It enables PCs to be used as a data bridge after the software has been installed in them. (Hereinafter, a PC installed with DataBridge software is referred to as “DataBridge”). DataBridge has two USB client ports, one for sending and one for receiving. It also has a function that filters the data input to the sending port so that the user gets only appropriate data from the receiving port (Fig. 2).

A user only needs to connect two USB cables in order to utilize DataBridge—one from DataBridge to the sending PC and one from DataBridge to the receiving PC. DataBridge ensures the two networks are never connected to each other because it transfers data without an IP (Internet protocol) connection. The sending PC recognizes DataBridge as a virtual printer, and the receiving PC recognizes it as a read-only removable drive. Users who specify DataBridge as a printer when printing applications (e.g., Excel or OpS) can then get portable document format (PDF) files on the receiving PC.

With this feature, DataBridge provides the following advantages to users.

- (i) It transfers only data that are permissible to extract from the system on paper.

Table 1. Examples of setting items.

Setting item		Explanation
Data transfer restrictions		Per-day data volume and number of transfers can be limited to prevent unduly large data transfers. Unrestricted volume and number of transfers can also be set.
Availability period		Available time and days can be set to prevent off-hours usage.
Automatic deletion time frame		Time frame for automatic deletion of DataBridge-stored data can be set.
Policy expiration date		Policy expiration date can be set to enable periodic policy reviews. Data cannot be transferred after policy expires. Unlimited-duration policy can also be set.
Available terminals		Available sending PCs and receiving PCs can be registered.
Authorized users		Authorized users can be registered.
Unit recognition information		Identification names can be set for identifying which DataBridge unit was used when using multiple units in parallel.
File filters	File name filters	Keywords can be set as file name filters. File names containing keywords enable DataBridge to allow or disallow data transfers.
	Application filters	Applications available for transfer can be set.

(ii) It can remove viruses from files.

(iii) It can transfer data in a single direction.

These advantages enable users to transfer data securely. When users convert files to the PDF format, it becomes difficult to reuse the data. Therefore, DataBridge has a function that allows users to transfer files directly without converting them to PDF, as long as the abovementioned items (i) and (ii) are unnecessary. (The administrator can freely configure enable/disable settings.)

4. DataBridge features

4.1 Security features to ensure safe and appropriate data transfer

DataBridge provides functions for transferring *appropriate* data; the meaning of appropriate is determined based on the conditions listed in **Table 1**.

DataBridge can filter files by checking file names and types; thus, it functions as a file type filter by checking whether file extensions coincide with the file contents. DataBridge can even extract and check archived files in formats such as zip and lha.

It also has functions to ensure that usage is limited to authorized users and connected PCs. The administrator registers the MAC (media access control) address of PCs so that only registered PCs can use the system. Its user recognition function displays a dialog box in which the user name and password are entered. It can also recognize users by using Windows login information.

By combining these functions, the administrator can set different rules for different people, depending on the positions they hold within their company or

organization.

Some examples of usage and restrictions are:

- Managers can use DataBridge at any time via all connected PCs.
- Rank-and-file users can use it only from 9 a.m. to 5 p.m. and only via their own PCs.
- Dispatched employees can transfer only Excel files for which the file name includes the word *application*.

Because data stored in DataBridge may not be taken from the office, DataBridge encrypts the stored data and automatically erases the data if it detects a disconnection or power-off of the USB cable being used. The erased data can never be restored.

4.2 Automatic usage history record for audits

It is important to ensure that the administrator is able to check whether data have been transferred appropriately. If this check is done using a manual operation, it imposes a heavy burden on both the person recording the usage history and the person checking it. To prevent this, DataBridge automatically records the usage history showing who used the system and when, as well as what files were used and from which PC and to which PC data were transferred. This usage history is basically stored inside DataBridge but can be transferred outside of it, which is useful when multiple DataBridge units are used in parallel.

4.3 Comparison with USB flash drives

USB flash drives are used for transferring data between terminals that are not interconnected over a network, and they present risks of unauthorized use

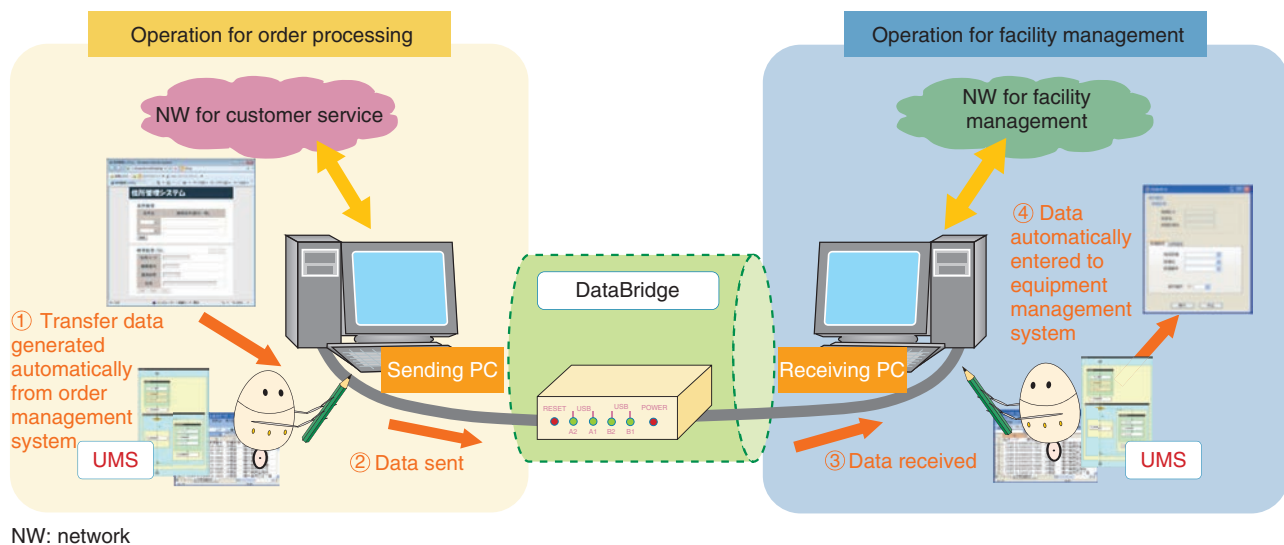


Fig. 3. Automated operation by combining DataBridge and UMS.

and information leakage. DataBridge prevents these risks by limiting the ways data are transferred and by recording the usage history.

4.4 Cooperation with UMS

The Unified Management Support System (UMS) is a software program that automates a variety of operations being executed on a single terminal. Like DataBridge, it is an example of client side cooperation technology [1, 2]. Combining DataBridge and the UMS makes it possible to automate operations that span across terminals that are not interconnected via a network, as shown in Fig. 3.

5. Summary and future plans

We have developed DataBridge, which enables users to transfer data easily and securely between

terminals connected to different networks without any need to modify existing networks or systems. DataBridge is currently being used in the NTT Group. The DataBridge technology was transferred to NTT Software Corporation, where the plan is to further develop and commercialize it.

References

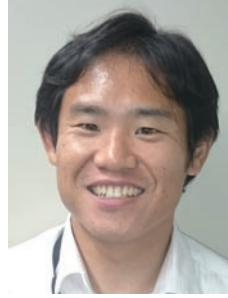
- [1] F. Yokose and A. Inoue, "UMS: Software to Automate Operators' Actions," NTT Technical Review, Vol. 9, No. 8, 2011. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201108ra4.html>
- [2] H. Adachi, K. Hotta, F. Yokose, T. Toyoda, and A. Inoue, "UMS: Software for Automating Operators' Actions to Rapidly Improve Operational Efficiency at Low Cost," NTT Technical Review, Vol. 12, No. 2, 2014. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201402fa1.html>



Hiroyuki Adachi

Engineer, Access Network Operation Project, NTT Access Network Service Systems Laboratories.

He received the M.E. in physics from Osaka City University in 2011. He joined NTT WEST in 2011 and worked in the Nagoya Branch until 2013, after which he moved to NTT Access Network Service Systems Laboratories. He is currently engaged in research and development of operation support systems of access networks.



Kimio Tsuchikawa

Senior Research Engineer, Access Network Operation Project, NTT Access Network Service Systems Laboratories.

He received the M.E. in applied physics from Nagoya University in 2002. He joined NTT in 2002 and is currently engaged in developing operation support systems for access networks.



Nagatoshi Nawa

Senior Research Engineer, Access Network Operation Project, NTT Access Network Service Systems Laboratories.

He received the M.E. in information engineering from the University of Tokyo in 1994. He joined NTT in 1994 and is currently engaged in developing operation support systems for access networks.



Akira Inoue

Senior Research Engineer, Supervisor, Access Network Operation Project, NTT Access Network Service Systems Laboratories.

He received the M.E. in mechanical engineering from Osaka University in 1994. He joined NTT in 1994 and is currently engaged in researching navigation technologies for future networks. He received the Academic Encouragement Award from the Institute of Electronics, Information and Communication Engineers (IEICE) in 2002. He is a senior member of IEICE.



Fumihiro Yokose

Network Business Headquarters, Strategic Network Management Department, NTT EAST.

He received the M.E. in electrical engineering from the University of Electro-Communications, Tokyo, in 2007. He joined NTT Access Network Service Systems Laboratories from 2007 to 2014. He moved to NTT EAST in July 2014.