Security Enhancement for Information System Platform through Utilization of Server Based Computing Technology at Suruga Bank

Momoko Kaneko

Maintaining information security is becoming the social responsibility of corporations, as successive incidents of information leaks have occurred at major corporations. The “Act on the Protection of Personal Information” was put into effect in April 2005, which required particular appropriate handling of personal information by corporations.

Since the personal information of bank customers must be handled at financial institutions, it has become essential for these institutions to implement security management for personal data according to the guidelines of the Financial Services Agency, which requires further security enhancements.

At the Suruga Bank Ltd., (hereinafter referred to as the “Suruga Bank”), consideration for a platform for their information system begun with a central feature for an information leak countermeasure, along with consideration for the upgrading of their information system PC (personal computer). Even though the bank started as a regional business that covered primarily the Shizuoka and Kanagawa areas it implemented an IT strategy ahead of all others, making a significant step towards becoming a business engaged in the retail financial business serving consumers on a nationwide scale. Furthermore, they are a “concierge bank” for whom customers are number one, a bank that deals with each customer’s needs in good faith with a mission to “materialize dreams” and assists customers in “putting realization dates to dreams”.

This paper will describe the features and effectiveness of the information system platform created for the Suruga Bank, which utilizes the SBC (Server Based Computing) technology that has drawn attention as a new system platform in recent years, due to its features, such as the high level of security it offers as well as ease of management.

Background of system implementation

The information system at the Suruga Bank had already been built on a client-server system with approximately 1,500 personal computer units operating with Windows NT 4.0 Workstation.

The building of an optimum system that satisfied the four requirements, “effectively uses existing assets”, “improves operational management”, “enhances personal computer security environments” and “upgrades personal computers to the latest models”, was required. These requirements given by the bank not only prompted us to consider assuring security for the information system as a whole, but also to be concerned about improving the operational efficiency through such means as reducing TCO (Total Cost of Ownership), when examining the creation of a new information system platform.

Features of system

A domain environment, already built with Active Directory for the information system platform at Suruga Bank, allowed centralized management of the personal computers of users. Infrastructures, such as broadband networks, were also already being maintained.

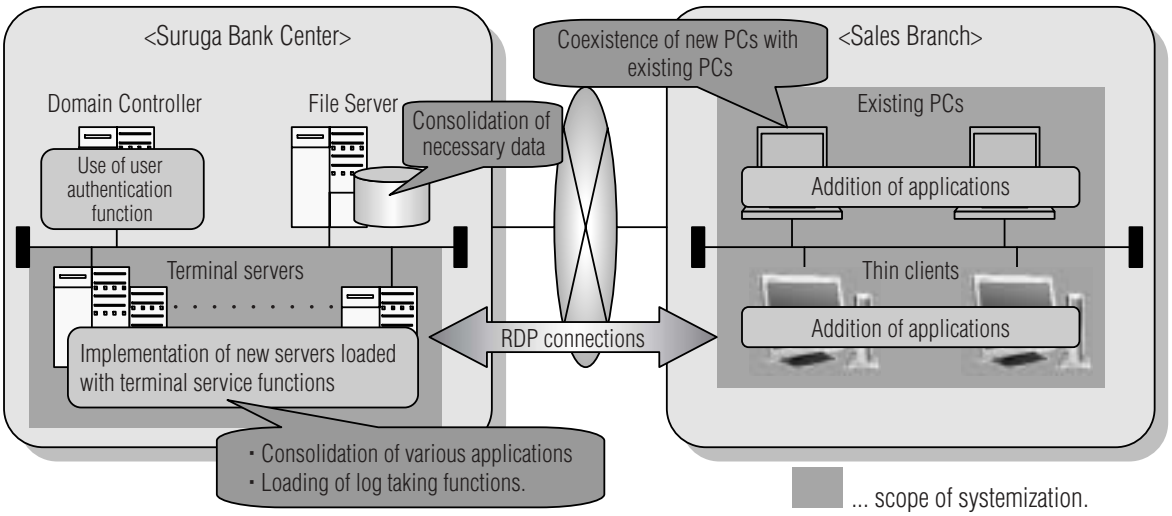

Fig. 1 System configuration after implementation

The terminal service of Microsoft Windows Server 2003 (described below) was adopted for the system to maximize the use of these existing assets while satisfying the security requirements of the bank (**Figure 1**).

Security was further enhanced not merely by implementing the terminal service but also through the development of new applications.

Features of the system are described below.

(1) Implementation of terminal service

In order to implement new sets of applications it was necessary to install or upgrade the applications on all the information system's personal computers set up at individual locations. Furthermore, the users of personal computers could potentially install their own individual applications as well, which presented issues for managing maintenance and operations.

Various types of applications and data can all be installed and managed on servers with a terminal service. These applications installed on servers can be executed from personal computers at remote locations through transactions involving minimal input and output information (key information and mouse information, as well as screen information, etc.) (**Figure 2**).

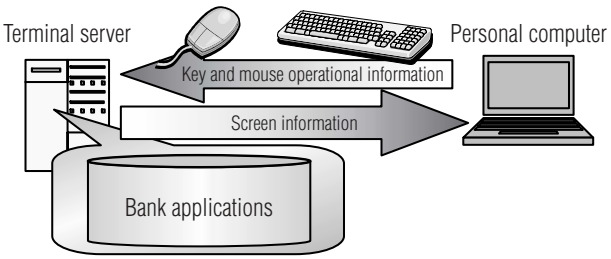

Fig. 2 Terminal service operation conceptual diagram

As a result of the features described above personal computers have become dedicated terminals that use screen displays, thereby enabling the system to provide user environments similar to those available in the past.

A platform was built that makes it possible to manage all together the various applications on servers, which were previously installed on individual personal computers.

Furthermore, through the control of all user environments of personal computers on servers, it became possible for users to use the same environment at all times, regardless of the particular personal computer in use.

(2) Enhancement of security

Ordinary terminal services impose no restrictions on the operation of personal computers, which allowed any of their functions to be used freely. For this reason, there have been unresolved security issues, such as the fact that files can be saved to individual personal computers.

Consequently, new applications were developed and combined with functions of terminal services to substantiate the security requirements at the bank.

- **Restrictions on functions of personal computers**

A dedicated login application was developed as a means to impose restrictions on personal computer environments. Through this application only a dedicated screen (**Figure 3**), displayed after logging in, becomes available for operations by the users of personal computers, concealing all other aspects of the personal computer environment.

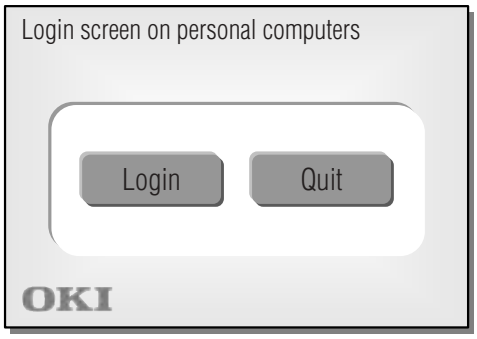

Fig. 3 Image of initial screen on personal computers

- **Output control of printouts**

Strict control for printouts is required, since printouts can contain various types of personal information, such as customer information. Therefore, we made it possible to control the output of printouts by embedding applications for detecting and recording output processes from personal computers in terminal servers (**Figure 4**).

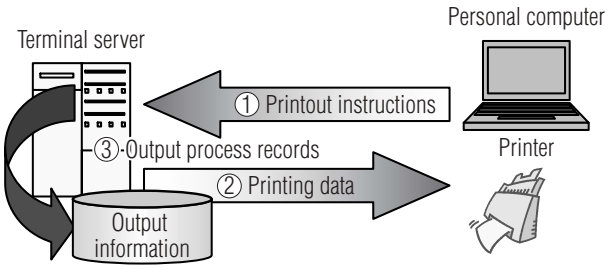

Fig. 4 Printout control conceptual diagram

Through this it became possible to manage the records of all printing from personal computers at the center.

- **Restriction on access to various data**

Strict control is required for various data that contains personal information, requiring an environment that can implement access controls different for the individual users of personal computers.

File servers at sales branches were consolidated at the Suruga Bank, to centralize data and to control access to this data.

By also using this control of authority for terminal servers it became possible to impose restrictions on the access to data (**Figure 5**).

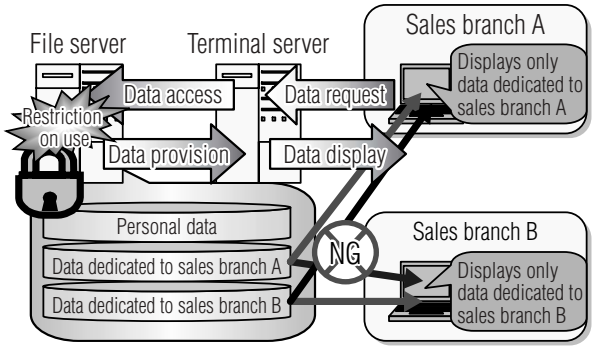

Fig. 5 Access control conceptual diagram

- **Use of printers under unified login environment**

Through the implementation of the terminal service it became possible to use personal computers with identical environments from various locations. The issue regarding the fact that identical environments were not available for using printers, however, still remained.

An application developed for printer displays was embedded in the servers. We created an environment that is identical at start up at all times, wherein only the printers displayed are adapted to the specific location from which printing is being attempted, even when personal computers of different locations are used temporarily, for example on a business trip (**Figure 6**).

(3) Replacement of personal computers

This system enhanced security for existing personal computers. Since a portion of these personal computers were progressively becoming outdated, however, it was necessary to consider the replacement of such personal computers as well.

As a consideration for the system, therefore, thin clients were primary candidates, rather than ordinary personal computers. Thin clients do not have any hard disks and are terminals dedicated to screen displays. They are terminals for personal data protection strategies since their features prevent them from storing information within these devices. They also have attracted a lot of attention in recent years.

By building this system we established in advance an environment for implementing thin clients at Suruga Bank. For this reason we were able to replace ordinary personal computers with thin clients without the necessity of yet another project.

Advantages of system implementation

With this system a high level of security was obtained for the new information system platform at Suruga Bank, while effectively utilizing existing assets. Furthermore, an optimum system that satisfies the requirements of the bank was created, while a high degree of effectiveness was exhibited in its performance, with regards to operational management and processing speeds of client personal computers.

(1) Improvement of security management

Through implementation of the SBC technology and consolidation of various data in the center, the storing of data in files on personal computers ceased and the amount of personal information in the hands of various sales branches and corporate organizations was reduced. The reduction of information subject to control contributes to the prevention of information leaks. Furthermore, the incorporation of various applications provided as additional functions attributed to the realization of various security enhancements.

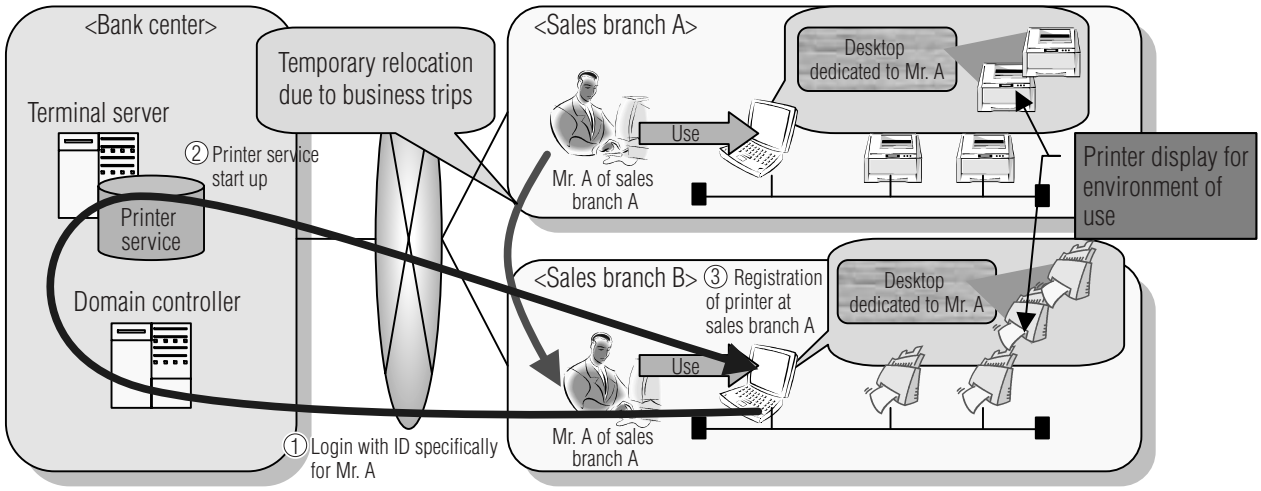

Fig. 6 System configuration after implementation

Issues for the system have been resolved through the minimization of threats, such as malicious tampering of data or the leaking of data subject to protection, including personal information, by locking the local environments of existing personal computers, as well as through the placement of access restrictions on various data.

Furthermore, a printing log collection function is effective for monitoring and keeping a check on the unauthorized printing or unauthorized use of files.

Since the unification of the login environment it became possible to conduct individual security management on the users as well. This includes, for example, the "management of acquired printing logs for individual users" or "restriction of access to the files on individual users".

In terms of environment the implementation of thin clients as new personal computers reduced the threat of data leaks through the theft of personal computers.

(2) Alleviation of operational load and management

The centralization of applications can lead to a reduction in the load of operational management.

Additional and eliminated applications on terminal servers at the center are reflected on all personal computers. Furthermore, since all application licenses are registered on servers, a simplified maintenance and license management, as well as a reduction of the TCO have been achieved.

(3) Improvement of client performance

The system made it possible to shift the operating environment of applications to servers, thus the mechanism allowed the processing of applications to be dependant on the capabilities of the servers. For this reason an environment was created in which the latest applications can be used at a satisfactory speed while improving the performance of client computers, even if client personal computers are running on an older operating system, such as Windows NT4.0.

This means that it is possible to use the latest environment with a performance that supersedes existing environments using existing personal computers. We were, therefore, able to build a system with great advantages to the users.

Conclusion

The system started operations in March 2005 and has been evaluated positively by the bank as an example of success for building an information system platform that features security enhancement.

Furthermore, the fact that the start of operations was achieved in approximately three short months since the beginning of full-scale considerations, resulted in a positive evaluation by users for the building of a platform in such a short period of time. This, however, would not have been possible without cooperation from Suruga Bank, the user of the system.

The implementation of thin clients, which started at the launch of the system, is showing favorable progress and implementation is expected to eventually spread to all sales branches.

Furthermore, a plan to unify the "login environment" with accounting terminals can be conducted in the future with minimal investment using this system. The system is expected to play a major role as a flexible information system platform for that purpose as well.

Authors

Momoko Kaneko: Financial Solutions Company, Financial Systems Div., Banking Solutions SE Dept.-2

TIPS Basic Terminology Descriptions

SBC (Server Based Computing)

A mechanism for centralizing the management and operation of client applications on servers by placing applications and data on servers and substituting the processing functions of clients with those of servers.

Client-server system

A mechanism for operations with the roles of computers divided into functions for servers and functions for clients.

RDP (Remote Desktop Protocol)

A unique protocol for terminal services. This protocol is based on TCP/IP, which is used to transmit user input information from the mouse and keyboard of client personal computers to servers or to transmit screen display information from servers to clients.

TCO (Total Cost of Ownership)

The total costs relating to implementation, maintenance and management of a computer system.

Terminal service

A function for executing applications and management tools on servers by using a Windows desktop that is virtually configured on terminal servers from a client's personal computer.

Active Directory

A mechanism for centralizing the management of information relating to hardware resources that exist on a network, such as servers, clients and printers, as well as the attributes of users who use them, along with their access authorities.