Ubiquitous Thin Client and Teleworking

Takaaki Ozeki

The implementation of thin clients is accelerating as they are considered to be the "trump card of strategies against information leaks" in the IT environment of business enterprises. Thin client systems have as their basic architecture "Server Based Computing" (SBC), which offers a mechanism for managing data at data centers, also the data cannot be retrieved from the terminals of individuals. This is an important aspect that prevents the leaking of information in teleworking operations. Another feature of thin clients, "the availability of one's own personal computer environment from any terminal" (location-free) is also a major advantage for realizing an easy to use teleworking environment.

A thin client USB-type is introduced as a "ubiquitous thin client" in this paper. Using this USB-type thin client enables users to utilize their own desktop personal computer or any laptop personal computer, available anywhere, as a thin client in a simple manner, making it possible for teleworking in a secure manner.

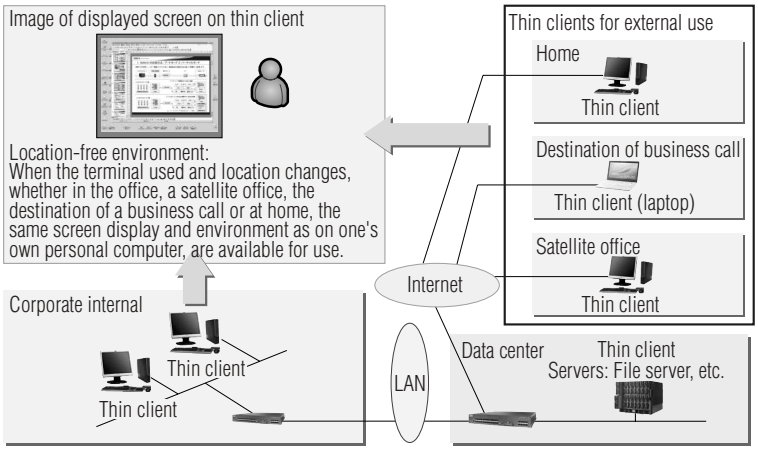

Fig. 1 Location-free

Ubiquitous thin client

A feature of thin clients is "the availability of one's own personal computer environment at any terminal", which means that when thin client terminals are arranged in the manner shown in **Fig. 1**, a user can log onto his or her "own personal computer environment" from any of these thin client terminals. This demonstrates that the configuration depicted in **Fig. 1** is an environment that presents a "location-free" setup, so to speak, which enables users to do their work using different thin client terminals at different locations as if they were always using their own personal computers.

The method involving the placement of dedicated thin clients at all locations, including homes, in order to actually carry out teleworking is not very realistic however, when the transition from existing personal computer environments to new environments, as well as the implementation costs involved, are taken into consideration. In view of the consequences of such a situation we developed a USB-type of ubiquitous thin client, "Safario," which is a tool for using the existing personal computers as thin client terminals in a secure yet simple manner.

A user simply inserts the Safario into the USB port of an existing personal computer and starts using the personal computer as a thin client terminal. This combination of "personal computer plus Safario" can replace the category of "thin clients for external use" depicted in **Fig. 1**.

Features of the Safario relevant to providing thin client environments suitable for teleworking are described in the next chapter.

Features of ubiquitous thin client Safario

Safario is a "ubiquitous thin client solution" developed with the intention of achieving remote access in a secure yet simple manner. Safario is comprised of the following three components (**Fig. 2**):

a. Safario token (USB memory-type device)

This USB-type thin client device internally incorporates the operating system and applications. This device enables the instant use of a personal computer as a thin client terminal simply by connecting it to the USB port of an existing personal computer. Furthermore, this device functions as a "token" for certifying that it is an authorized thin client device through an internally incorporated certificate authenticated through a coordinated linkup with the Safario Gateway and Safario Manager, which are described in the following section.

b. Safario Gateway (software)

The Safario Gateway is installed at the entrance to

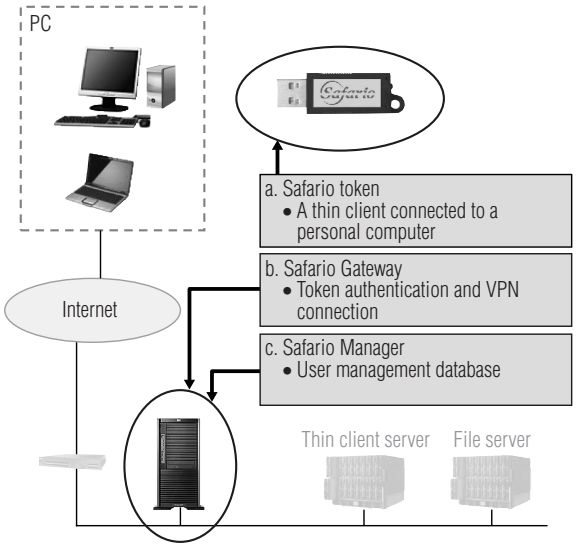

Fig. 2 Three components of Safario

the corporate internal network. The personal computer of a user is able to gain access to the corporate internal network from the internet via a Safario token that links it to the Safario Gateway. In this process, when a connection request is received from a Safario token, the Safario Gateway authenticates the authorized user by accessing the database managed by the Safario Manager, which is described in the next section. Furthermore, a virtual private network (VPN) connection with encrypted data is configured on the communication path between the Safario token and the Safario Gateway.

c. Safario Manager (software)

This tool is used for managing the users of Safario tokens. It prepares a database that correlates the Safario tokens with users. This database is used for authenticating Safario tokens and users, as described earlier. If a user loses a Safario token, the lost token can be registered for "prohibited use" with the Safario Manager to prevent unauthorized use by others.

Safario provides a ubiquitous thin client environment securely and simply through the functions of the three components described above. In terms of further outlay considerations, lower cost systems have been made available for USB-type thin clients of other companies. The functional features of Safario, which will be necessary for teleworking, are described in the following segment.

(1) Security as a thin client

The Safario token operates as an independent thin client with the necessary operating system as well as applications all built in. It is also able to operate without the use of any hard disk in the personal computer. For this reason the operating environment of Safario will never be impacted by any virus that infects personal computers. Furthermore, the leaking of information can be prevented, since the loading of data onto an external storage device is prohibited when Safario is in use.

In this manner, it is possible to utilize existing personal computers as thin client terminals and to realize secure teleworking through the use of Safario (**Fig. 3**).

(2) Security of communication path

When a thin client terminal is used externally, it is usually connected to the corporate internal network via the internet. The connection via the internet has been identified as an issue, since the data can potentially be tapped into through the communication path. Therefore, the VPN is most commonly used for the encryption of communications through a connection between a terminal at an external location and a corporate internal network.

Since Safario already provides the VPN connectivity as a basic function, there is no need to arrange for equipment to use VPN (lower cost) to realize teleworking securely and simply. This is an aspect that is considered to be a feature of Safario (**Fig. 3**).

(3) Two methods available for startup

Two methods, "Boot mode" and "Virtual mode," are available for starting up Safario. This feature of Safario is not available with other USB-type thin clients. The "Boot mode" method of starting up Safario is executed by inserting it into the USB port of a personal computer

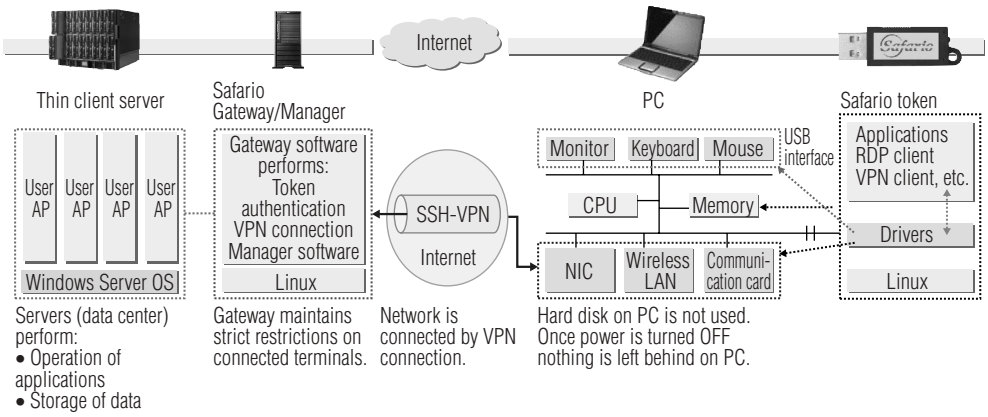

Fig. 3 Security of Safario

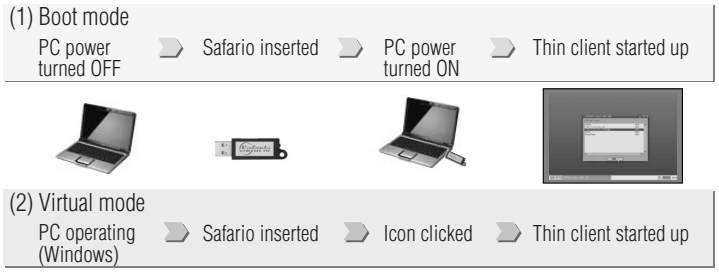

Fig. 4 Two startup modes (Boot mode and Virtual mode)

before turning on the power of the personal computer. The "Virtual mode," on the other hand, is a method for starting up Safario automatically by simply inserting it into a personal computer that is already running on a Windows operating system. The characteristics of these two methods are described below (**Fig. 4**).

a. Boot mode

This is an operating mode in which Safario starts up without the use of any portion of the hard disk on the personal computer. In this mode Safario is theoretically equivalent to a "dedicated thin client terminal." Furthermore, the features of this mode include the speed at which Safario starts up and terminates operations, which is overwhelmingly faster than the Windows operating system.

This booting mode for starting up Safario, however, may not be available in some personal computer models, depending on the particular model in use, due to the difference in basic specifications. In such cases, utilization of the "Supplementary CD-ROM" supplied with Safario will render most personal computers usable for starting up Safario.

b. Virtual mode

This mode allows the thin client to be used simultaneously with a Windows operating system on a personal computer. The thin client environment in this mode runs on an operating system inside Safario and it is different from the Windows operating system. For this reason, it is not accessible from applications running on the Windows operating system. Even if the Windows operating system becomes infected with a virus, it will not impact Safario due to this feature. Furthermore, since data can not be loaded onto an external destination on business calls from the thin client environment of Safario, the leaking of information is not possible.

If in the unlikely event a type of virus is concealed on the Windows operating system, such as a key logger or screen logger, there is a threat that the key operations or screen displays on Safario could be tapped. Incidentally, these types of viruses are related to Winny, which often creates problems. In order to avoid such unforeseen threats, Safario is equipped with a function for checking to see whether or not appropriate antivirus software has been installed on the Windows operating system before starting up in the Virtual mode. It is possible to set Safario so that the Virtual mode is not started if

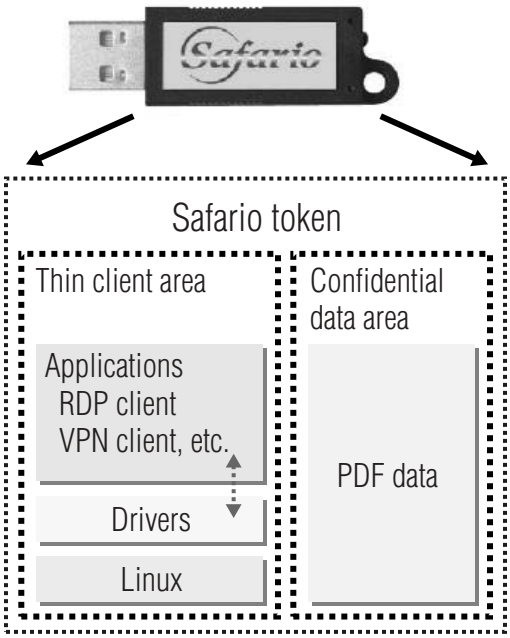

Fig. 5 Confidential data area

appropriate antivirus software is not installed on the Windows operating system.

By selecting one of these two startup modes in an appropriate manner it is possible to attain the benefits of a more convenient thin client environment suitable for particular conditions of teleworking.

(4) Confidential data area (Fig. 5)

The third feature within the Safario token is a memory region that can be used to encrypt and store the necessary PDF data obtained from corporate internal file servers. Furthermore, because the stored PDF data can only be read on Safario, the potential for a leak outside the company is completely eliminated. Since this PDF data can be accessed even in an environment where access to the network is not available, it can also be used for presentations to clients at their location.

Case examples of Safario implementations

In this chapter, case examples of teleworking through the implementation of Safario are introduced with the effectiveness of such an application evaluated. Figure 6 depicts an example of the work operations performed in our company using Safario. A desktop-type thin client terminal is used for the work operations inside the company, whereas a combination of "laptop PC + Safario" is used as a thin client terminal for mobile work performed externally. Furthermore, work at home is performed with a combination of "personal computer at home + Safario" similar to that of a thin client terminal. Since a thin client system had already been in use in our offices, implementation for this case example involved the new addition of Safario to the existing facility. More specifically, a Safario Gateway and Safario Manager (one

server hardware unit, using Linux as the operating system) were installed to the segment, where access was made from external locations to the corporate internal network, which completed the addition of a Safario system.

Existing laptop personal computers in use, running on Windows XP operating systems, are used as thin client terminals by connecting a Safario token. It is not possible to start Safario using the Boot mode with some laptop personal computers and in such cases the Virtual mode is used. The network for mobile use provides adequate communication speeds, access to which is gained using a high-speed communication card and publicly available commercial wireless LAN. Since only the "data for the difference in screen display information" is transmitted by thin clients, the operating sensation of the terminals is not inferior to that of the operating environment in the office. Furthermore, since a VPN connection is used for communication paths that are connected via the internet, there is no need to worry about information leaks occurring on the communication path.

The Safario token is connected to the personal computer at home, converting it into a thin client terminal, for use at home. Risks relating to the security of personal computers used at home pertain to the existence of any virus infection of the personal computer itself. Since Safario does not use any part of the hard disk on the personal computer when it is started in the Boot mode and, even in the unlikely event that the personal computer is infected by a virus, its effects do not impact the work and the work is secure while Safario is used. Also, when the personal computer at home is used in the Virtual mode, Safario starts up only after it verifies that the antivirus software installed on the personal computer's main unit is adequate, making it is possible to use the terminal with virus related risks avoided.

As described above, teleworking is possible in a secure and simple way, using a thin client system employing Safario.

A survey was conducted with the users who utilized Safario in this case example. The main results are described below:

"Did you experience any problem or inconvenience when connecting to the network?"

- "None" (95%); "Setting up the wireless LAN connection took some time" (5%).

"How was the starting up speed of Safario?"

- "Extremely fast" and "Fast" (90%).

"Did you experience any problem or inconvenience with authentication?"

- "None" (100%).

"How does it feel (speed) using a thin client?"

- "Fast" and "No problems" (80%).

"How fast was the start up and terminating speed?"

- "Extremely fast" and "Fast" (100%).

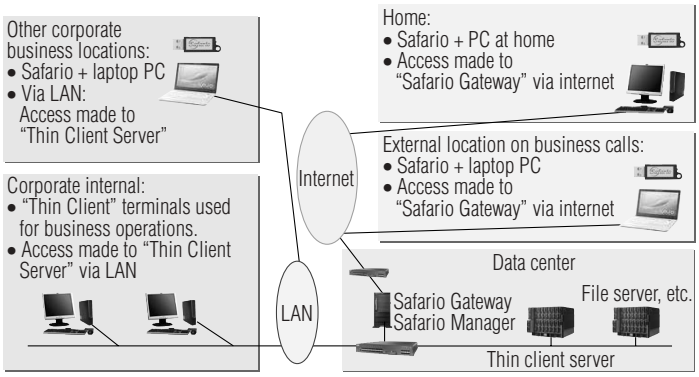

Fig. 6 Example of Safario application

"Other impressions"

- "The aspects of assured and enhanced security while maintaining convenience for work operations using Safario are excellent features in comparison with the situation nowadays, in which increasing restrictions are put on the use of personal computers for the purpose of enhancing security".

Many users who actually used Safario voiced their opinions indicating how extremely convenient it was to use.

Conclusion

It is essential for tools intended to facilitate teleworking to assure high levels of security against information leaks and to provide the same levels of operability as those available in the company. Economical efficiency is also an important factor when implementation is considered.

This paper introduced Safario as an effective tool for the promotion of teleworking, with consideration for the aforementioned factors and to facilitate the use of existing personal computers in safe, simple yet economical thin clients. We do hope that the descriptions provided by this paper serve as a reference for the promotion of teleworking.

References

1) Ozeki, Takaaki: "Requirements for Implementation of Thin Clients as Security Terminals," Oki Technical Review, Issue 205, Vol. 73, No. 1, pp. 20-25, January, 2006.

Authors

Takaaki Ozeki: Oki Consulting Solutions Co., Ltd., ICT Solutions Group.