Secure PC environment roaming technology for ubiquitous office

Shigeyoshi Iizuka Kei Uwazumi Kiyoshi Nakahama Shinya Nakajima Katsuhiko Ogawa
NTT Cyber Solutions Laboratories
1-1 Hikari-no-Oka Yokosuka-shi Kanagawa 239-0847 Japan

ABSTRACT

Since businessmen who are outside their homes or offices often want to netsurf for information retrieval and/or making documents, it is becoming popular to access public computers in sites such as rental offices and Internet cafes. However, there are two major problems with using such computers. One is the excessive time and effort needed to recreate the user's preferred desktop environment. The other problem is security. Our Shared PC concept eliminates these problems. The Shared PC represents a kind of ubiquitous office that can be safely created and used simply by inserting a personal IC card into a PC. The user's own PC environment, held at a server as encrypted files, is deciphered and restored using a private key stored in the IC card. Security is ensured because the local hard disk holding the user's personalized environment is formatted at the end of each session. This paper presents the Shared PC architecture and a field trial.

KEYWORDS

ubiquitous, environment roaming, personal computer roaming, IC card, security

1 INTRODUCTION

Computers are useful only if they support the user. One key to their success is the personalization of the desktop. Like our living room, we tend to spend much time in rearranging the objects (icons and menus) in the room (desktop) so that we can quickly find and use things. Urgent items are often put in a special place and their presence acts a reminder. While notebook PCs are becoming more common, they pose new problems such as security and the lack of data protection; drop the notebook and the more recent work may be lost for ever. What is needed is a way of accessing our personalized environment from outside the home or office.

While public computers are available, their security and user-friendliness are suspect. Excessive time and effort are needed to recreate the user's personalized environment. They lack security systems that can prevent the disclosure of personal information. In order to eliminate these problems, we developed the PC environment roaming technology. Section 2 elucidates the problems of public personal computers and the requirements that must be satisfied to solve them. The proposed PC environment roaming system "Shared PC" is detailed in Section 3, and the results of a field trial are given in Section 4.

2 REQUIREMENTS

In this section, we describe two major problems of public computers and requirements that will yield their resolution.

2. 1 PROBLEMS

There are two major problems with public computers. One is the time and effort required to set them up prior to their use. That is, if you want to be productive, it is necessary to personalize the appropriate software for the tasks demanded, and considerable time is needed for this. The other problem is security. Since public computers are shared by many users, the obvious concern is the disclosure of personal information. User information such as files, password information, and cookie information must be imported or entered and then deleted from the PC. The passwords memorized by the public PC are a major problem. For example, company secrets may be accessed via the Internet by unauthorized users if password information is 'accidentally' saved on a public computer. If these problems are solved, it will be possible to use a public computer comfortably at a going-out place.

2.2 REQUIREMENTS

We believe that public computers can become successful only if three requirements are satisfied.

- Mobility : the user needs to carry only a lightweight ID system.
- Security : no personal information remains on the public computer. User files cannot be read even by the system administrator of the server.
- Usability : the user's personalized desktop is recreated in full.

We developed the "PC environment roaming technology" to satisfy the above requirements.

3 SHARED PC SYSTEM

We developed the "Shared PC system"[1] which satisfies the requirements described above. This section describes the features, architecture, and realization of the Shared PC system, PC environment roaming, backup method and usage procedure.

3.1 FEATURES

The Shared PC system will promote the use of public computers. The key to its success will be its use of the PC environment roaming technology which provides the user with her own personalized environment with complete safety. The requirements are satisfied by the following feature of the Shared PC system.

- The user needs to carry only an IC card for authentication.
- Since all user information is completely deleted when the session ends, and files are transferred in the encrypted state, security is complete.
- Popular application programs can be used without stress, and the user's personalized environment is made available.

3.2 ARCHITECTURE

The Shared PC system consists of Shared PC clients and a Shared PC server, which is called server hereafter. The server keeps the user's personalized environment and is connected to the Internet. The system architecture is shown in Fig. 1.

3.3 REALIZING PC ENVIRONMENT ROAMING

There are two major approaches to realizing PC environment roaming. One is the streaming type of which “Metaframe”[2] of Citrix is typical. Streaming systems run the applications on the server. While the specification of a client may be low, the load placed on the server is large. Therefore, throughput depends on the zone of network, so multimedia applications may be slower than normal. Accordingly, we adopted the download type, which is the other type. One example is the “Roaming User Profiles”[3] of Microsoft Windows2000 server. This technology puts the user's profile directory on the server and so provides the user with the same environment. However, while system introduction is easy, the service is quite restricted; only the subordinate files of the directory, specified by Microsoft, can be provided, and the domain is closed. Moreover, the use of the Roaming User Profiles is limited to the same domain, so its security level is not high. On the other hand, the Shared PC system places no limits on the domain, and can reproduce any environment. The realization method of PC environment roaming in the Shared PC is shown in Fig. 2. The server holds the user's applications and the difference files, which allow the user's personalized environment to be completely reproduced by downloading and installing them when desired.

3.4 DIFFERENTIAL BACKUP METHOD

If the backup of all data is performed at the end of the session, it needs much time. Then, in order to shorten the shutdown delay, the Shared PC backs up the files at fixed intervals while in use. The backup agent in the Shared PC checks for changes in the file information in the hard disk at fixed intervals. We explain details of the backup method using Fig. 3. Assume that the Shared PC creates difference files F1, F2, and F3 at Time(t－Δt), these files are then backed up to the server at Time(t－Δt). F3 is updated later, which becomes F3’. And F4 is created after Time(t－Δt) but before Time(t) on the Shared PC. The backup agent on the Shared PC compares the time stamps of the files at Time(t), and sends only F3’ and newly created F4 to the server.

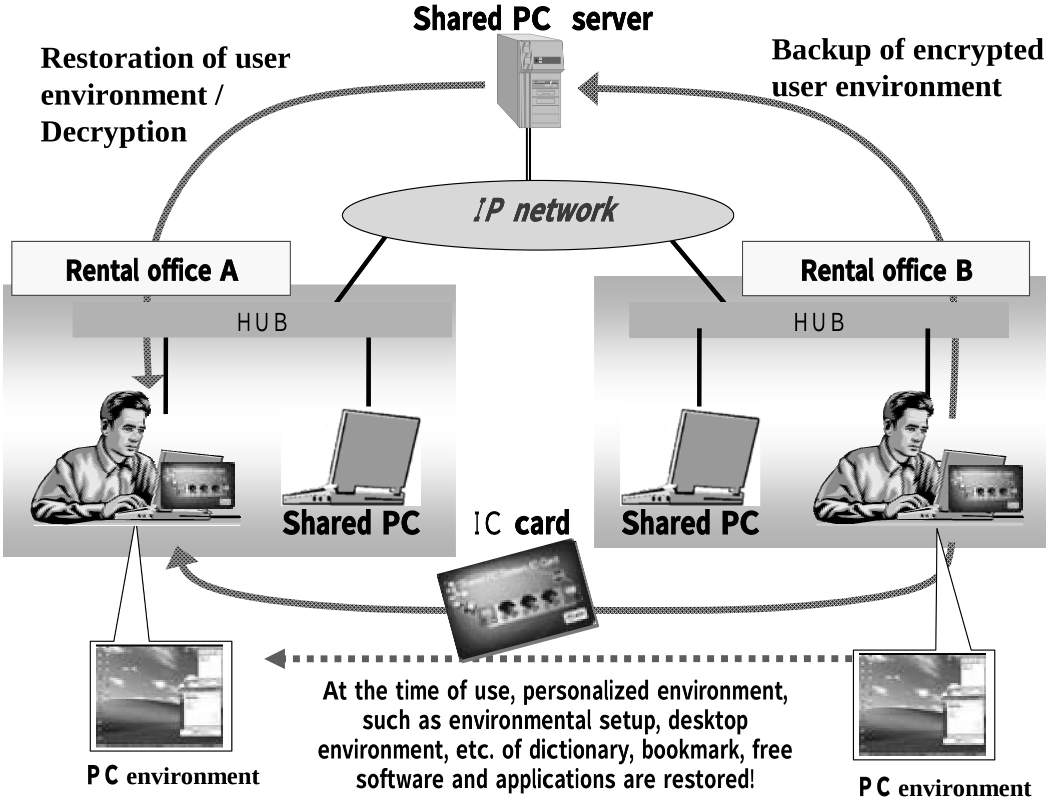
Shared PC server
Restoration of user environment / Decryption
Backup of encrypted user environment
IP network
Rental office A
Rental office B
HUB
HUB
Shared PC
IC card
Shared PC
PC environment
At the time of use, personalized environment, such as environmental setup, desktop environment, etc. of dictionary, bookmark, free software and applications are restored!
PC environment

Fig.1 Architecture of the Shared PC

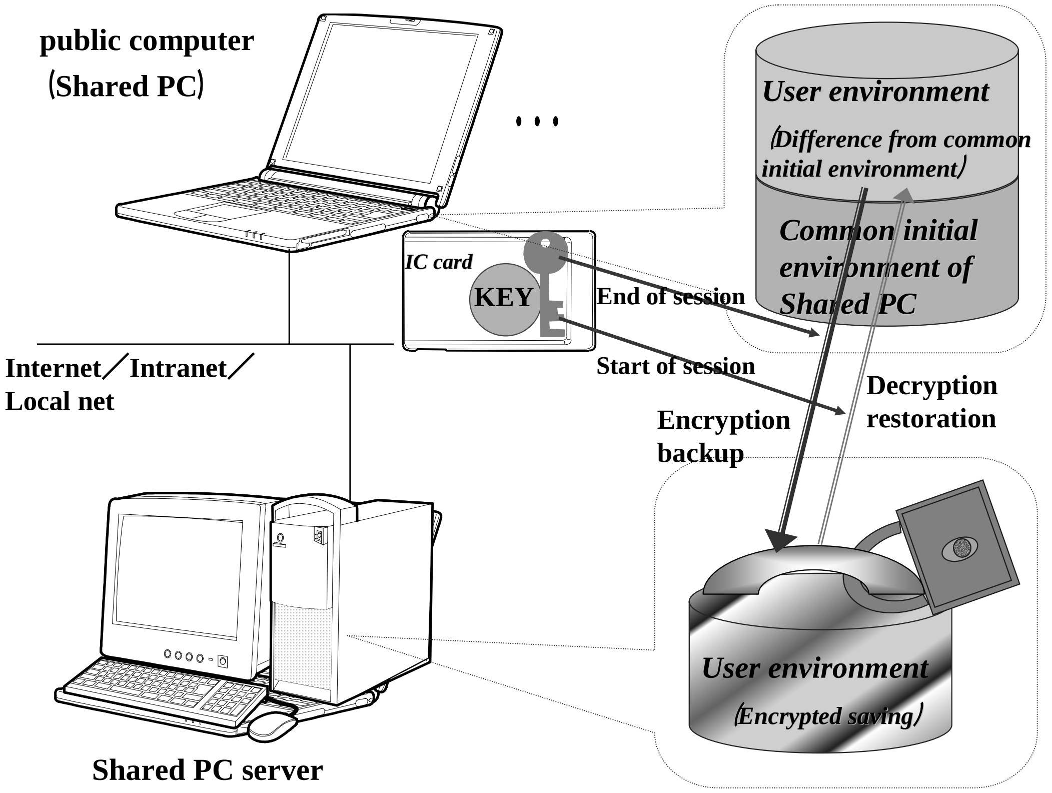

Fig.2 PC Environment Roaming Method

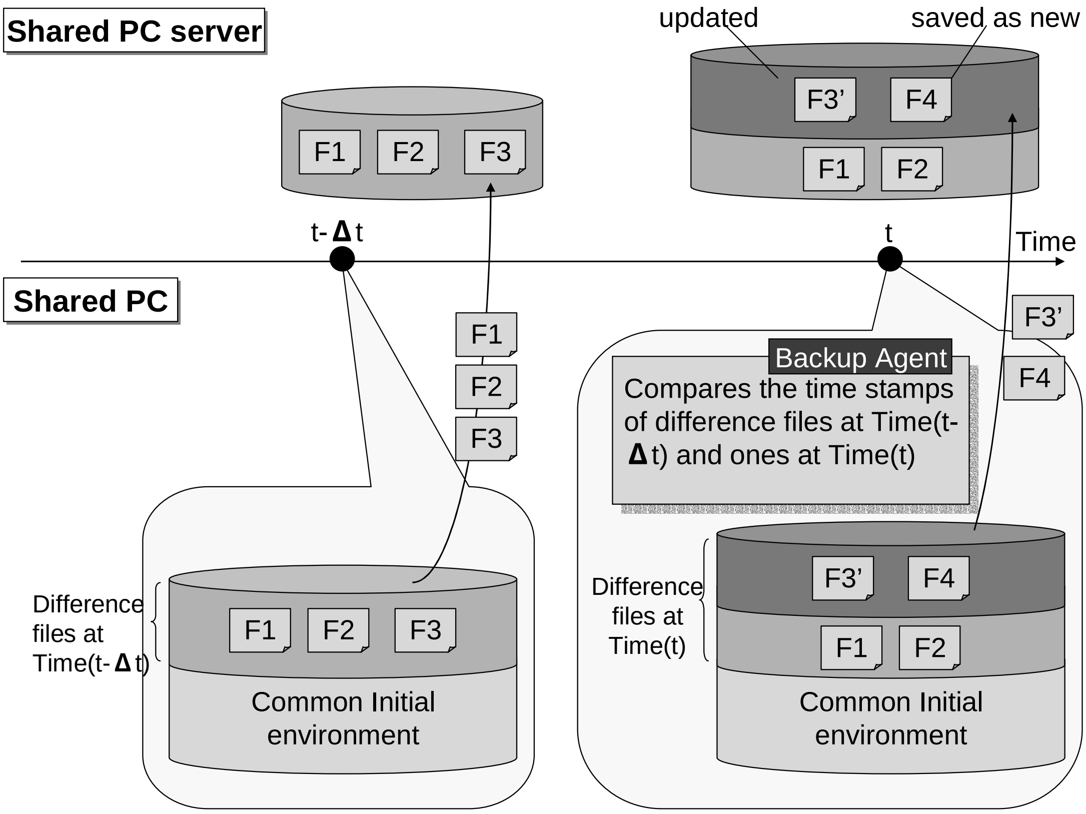
Shared PC server
updated
saved as new
F3'
F4
F1
F2
F1
F2
F3
t-Δt
t
Time
Shared PC
F1
F2
F3
F3'
F4
Backup Agent
Compares the time stamps of difference files at Time(t-Δt) and ones at Time(t)
Difference files at Time(t-Δt)
F1
F2
F3
Common Initial environment
Difference files at Time(t)
F3'
F4
F1
F2
Common Initial environment

Fig.3 Details of Backup

3.5 SAFE PC ENVIRONMENT WITH HIGH SECURITY

First, we adopted SSL to the backup process, and the common key system (FEAL32X) to encrypt data. This means that the data held on the server is encrypted and is transferred over the public network in encrypted form. Each Shared PC user is identified by her unique IC card. The card holds a key that decrypt the data held on the server as well as encrypting the data prior to backup. The user performs user authentication by inputting her password (PIN). Therefore, even the server administrator cannot open a user's files. Moreover, when a session ends, all user data and settings are automatically and completely deleted. This keeps all user data and information private.

3.6 USAGE

The Shared PC system is used as described below. Note that step (0) is performed just once when joining the system.

(0)Registration (Online signup)

The user registers with the Shared PC system and indicates her password. The user is given an IC card in which the password is embedded and uses it to create and encrypt the difference files with the server.

(1)Personalized Environment Restoration

When the user wants to use the Shared PC, she inserts her IC card into a reader attached to the computer and identifies herself by entering her password. The system then restores the user's personalized environment.

(2)Difference Files Backup

The system encrypts and backs up the difference files during the session.

(3)Termination

At the end of the session, the locked system files and any remaining difference files are backed up.

(4)Security Cleanup

This means that user data cannot be retrieved even if restoration software is used. This is possible because each Shared PC has two partitions. Volume C is the ‘user domain’ and volume D is the ‘system domain’. The user’s personalized environment is installed in volume C. The system OS of the Shared PC is installed in volume D. These volumes permit dual boot operation. The ‘user domain’ established the Windows PC environment. The ‘system domain’ performs attestation for running the Shared PC and communicating with the server.

4 FIELD TRIAL

In order to perform verification for service including the service, security, management, and system of the Shared PC, we performed the trial in the actual field. In this section, we describe an outline, result, and evaluation of the application trial to the public computer of the Shared PC.

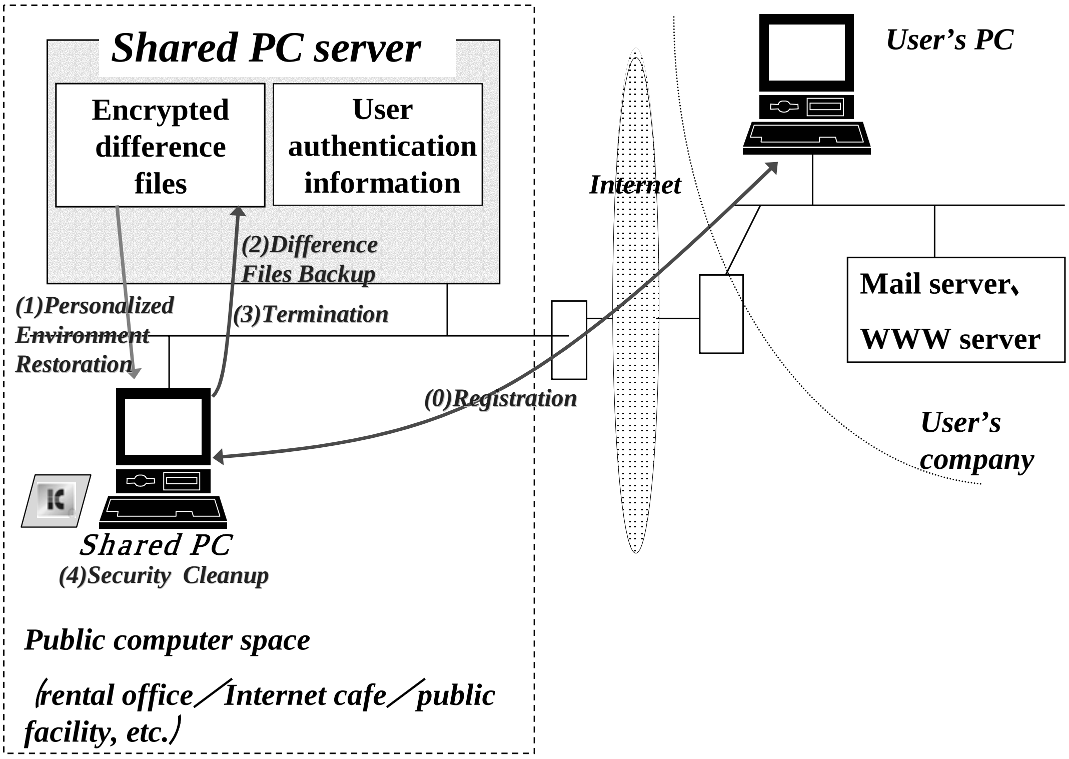
Shared PC server
Encrypted difference files
User authentication information
(2)Difference Files Backup
(1)Personalized Environment Restoration
(3)Termination
Internet
User’s PC
Mail server、WWW server
(0)Registration
User’s company
IC
Shared PC
(4)Security Cleanup
Public computer space
(rental office／Internet cafe／public facility, etc.)

Fig.4 Usage Procedure

Table 1 Equipment Specifications

PART		SPECIFICATION
Shared PC	CPU	PentiumⅢ 1GHz
	memory	256MB
	OS	Windows98 SE
	Line	Optical Fiber (100Mbps) (Share with 10 computers in a rental office)
Shared PC server	CPU	PentiumⅢ 1.26GHz
	memory	256MB
	OS	TurboLinux
	Line	Optical Fiber (100Mbps)

4.1 OUTLINE

An outline of the trial is shown below. The trial was conducted in two actual commercial rental offices.

- Two Shared PCs were installed in each rental office
- The trial period was four months.
- The subjects were 62 clients of the rental offices.

The system configuration of this trial and the specifications are shown in Table1.

4.2 RESULT AND EVALUATION

First, the following results were brought about the operating frequency in an trial period.

• Average session duration	:73min 32sec
• Average use time per person	:7.1 times
• Average use time per day	:4.3 times

The subjects were asked to respond to a questionnaire; 25 complete replies were obtained. The staffs of the rental offices were queried as to the stability of the system in use.

We discuss the results below.

(1) Service

The questionnaire raised the following questions to evaluate satisfaction with the system.

Q1: The good points of Shared PC

Q2: The weak points of Shared PC

Q3: What ability do you want to add to Shared PC

Q4: Was it easy to use Shared PC?

Q5: Did Shared PC increase work efficiency

Q6: Do you want to use Shared PC again?

Q7: Which item is most important in the appeal of the “PC environment roaming service”? （Number of usage sites, Secure network connection to the company or home, low cost, speed of network.）

The answers provided to these questions are shown in a Fig.5. First, about Q1, 80% of the subjects replied “the simplicity of using just an IC card”. About Q2, 76% of the subjects replied “Much time is required when starting”. This seems unavoidable given the need to form the users personalized environment and then reboot into it. About Q3, 72% of the subjects noted that they wanted to be able to shift from present environment of their own computers at home or in the office. The serviceability of the Shared PC was highly rated in that Q4 through Q6 received only 10%~15% negative replies. Moreover, about Q7, at least half the subjects selected “the number of usage sites” as the most important. It turns out that users wanted to be able to use the Shared PC system from wherever they go.

(2) Security

We examined Volume C contents after several sessions using the latest disk recovery programs and could find no user data. Given the complexity of the modern PC operating system, we will need to conduct extensive checks to confirm the security of the Shared PC system.

Additionally, the answer of Q7 showed that “security” is noted as the second important item. It indicates that the user cares about security in use of public computer. So the importance of security has been checked anew.

(3) Management

Interviews with the rental office staff showed that the Shared PC system is easier to manage than the conventional approach. With the regular computers, the staff has to delete the user's history, files, etc. However it seems that some information cannot be deleted so security is not perfect. The Shared PC system, on the other hand, makes it unnecessary for the staff to delete user history and data; this is done automatically and is done rigorously.

(4) System

During the trial, no unusual system operation or failure occurred. We did notice that some subjects did not follow the specified shut down procedure but this problem is rather easy to prevent.

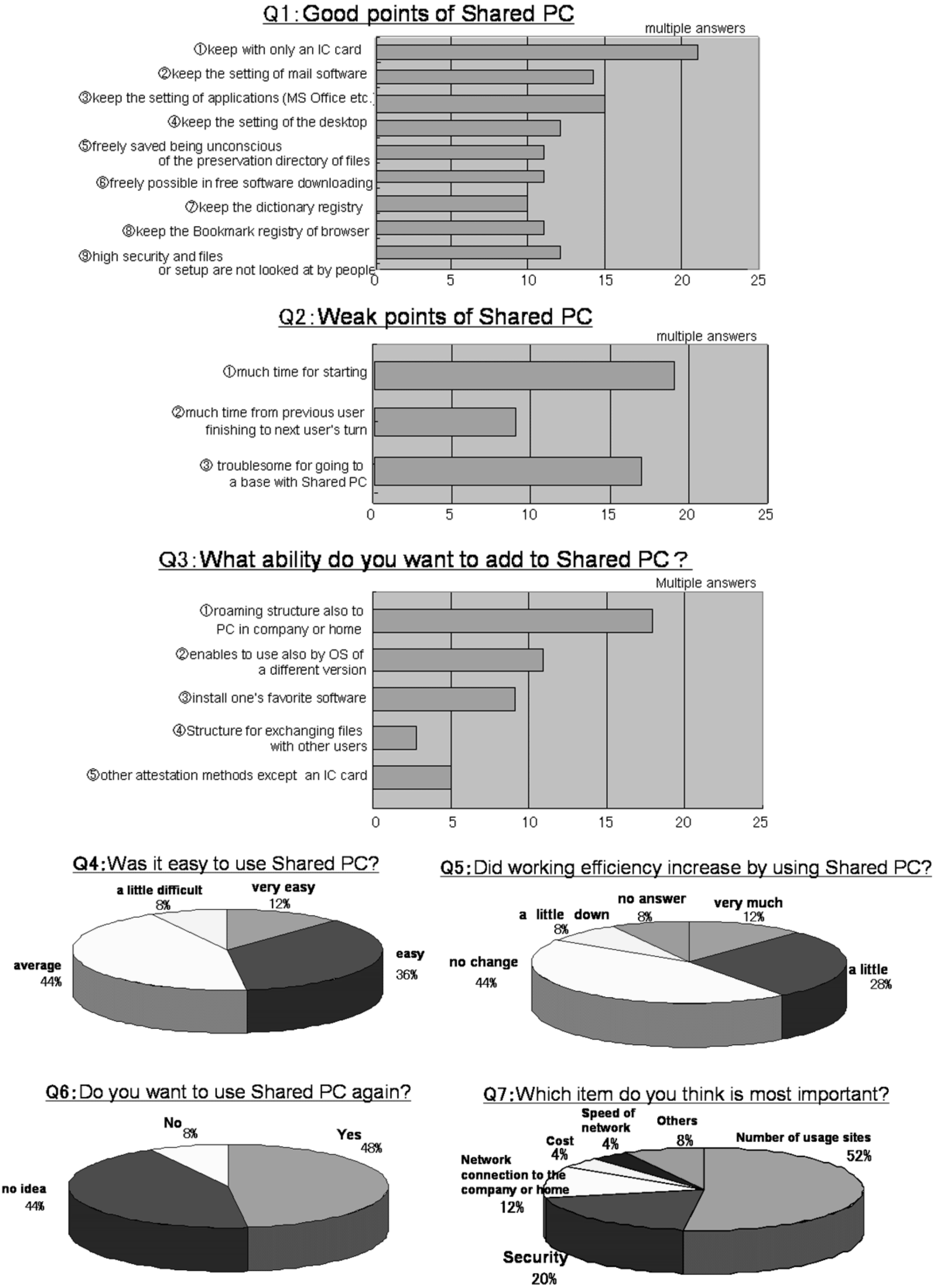

fig.5 Questionnaire Result

5 CONCLUSION

This paper tackled the two problems that prevent the widespread use of public computers: the time and effort needed to reconstruct the user's personalized environment, and poor security. We developed the three main requirements of ‘Mobility’, ‘Security’ and ‘Usability’ for resolving the problems. Our PC environment roaming technology “Shared PC” was shown to fulfill the requirements. The Shared PC system requires the user to simply insert an IC card into the public computer to allow it use. Since the system encrypts all files and decrypts them only when the public computer is actually being used, and reformats the user's partition at the end of the session, complete security is provided to the user. We described the results of an extended field trial; Shared PC units were installed in two commercial rental offices. The results of the trial indicate that the PC environmental roaming service offered by the Shared PC was well accepted. The key benefits were simple log on via the user's IC card and provision of user's personalized environment. We noted that subjects who used the system often rated the system more highly. Areas for improvement include reducing the time taken to complete the startup.

We will conduct further research into personal computer environment roaming between different personal computer models; the current system demands that all client terminals be the same model. Moreover, we want to consider not only the security of personal computers, but also the security of the usage site.

ACKNOWLEDGEMENT

Many thanks to Yoshihiko Kitano of KOKUYO Corp. for great cooperation in trial.

REFERENCES

[1]K.Nakahama, K.Uwazumi; Shared PC for Ubiquitous Office Construction, NTT REVIEW, vol.14, No.5, pp.15-17, Sep. (2002)

[2] http://www.citrix.com/

[3] http://www.microsoft.com/windows2000/