# Development of Systemwalker Desktop Products Suite for Implementing Privacy Protection Measures

● Makoto Shimosaki ● Toru Murai ● Shingo Ohnishi

*(Manuscript received October 30, 2006)*

**In recent years, information has frequently been leaked from corporations and local governments. One factor cited for this problem is that the monitoring and prevention of such leaks do not extend as far as the endpoint PCs. Accordingly, corporations and local governments are now looking at measures such as IT asset management, restrictions on user operations, and the management of audit trails at endpoint PCs. Fujitsu's Systemwalker Desktop products suite enables endpoint PCs to be managed according to directives issued by operations managers. This paper describes various development initiatives for this suite.**

## 1. Introduction

In recent years, information has been frequently leaked from corporations and local governments. Leaks of personal information can result in large compensation payments and loss of social credibility for corporations and local governments. Therefore, the implementation of measures to prevent information leaks has become a concern for corporate management.

Personal information is leaked because it has a monetary value and there is widespread use of inexpensive, light, and portable media such as USB flash memory. Information can be easily obtained from endpoint PCs, and there is a high risk of information being taken offsite, stolen, or lost. The fact that the monitoring and prevention of information leaks do not extend to endpoint PCs is also cited as a reason for these incidents. In many cases, in-house personnel are responsible for these leaks.

Consequently, the extension of such monitoring and prevention to endpoint PCs is becoming a necessity for corporations and local governments.

This paper introduces the Systemwalker Desktop products suite.[1)-3)] Section 2 introduces the Systemwalker Desktop products. Section 3 examines information leaks and how to prevent them. Section 4 describes measures for preventing information leaks by using the Systemwalker Desktop products suite, and Section 5 presents our conclusion.

## 2. Systemwalker Desktop products

We believe that information leaks should be prevented in four steps. First, it is very important to carefully manage IT assets. In order to do so, operations managers must know the number of endpoint PCs, the update status of security patches, and the virus definitions of anti-virus software. In this paper, "operations managers" refers to those who manage the information systems of corporations or local governments. These persons must ensure that up-to-date security patches are applied to all endpoint PCs. Fujitsu's Systemwalker Desktop Patrol[4)] provides functions for these tasks.

Second, it is necessary to prepare for cases of personal information being leaked outside (e.g., through theft by outsiders and access to information by outsiders using lost or stolen notebook PCs or USB flash memories). Therefore, it is necessary to encrypt data. Systemwalker Desktop Encryption provides functions for such tasks.

Third, information leaks due to operational errors or inappropriate acts by in-house personnel must be prevented. To do this, it is necessary to collect user operation logs at endpoint PCs so that operations managers can obtain evidence about specific incidents. The collection of these logs will also have a psychological deterrent effect on the users of endpoint PCs. Systemwalker Desktop Keeper[5] provides functions for these tasks.

Fourth, advanced and detailed prevention measures such as placing restrictions on user operations, preventing unauthorized access, and controlling user access by file units must be taken. Systemwalker Desktop Keeper, Systemwalker Desktop Inspection, and Systemwalker Desktop Rights Master provide functions for these tasks.

This paper introduces the mechanism of Systemwalker Desktop Patrol for applying security patches and the mechanism of Systemwalker Desktop Keeper for restricting user operations and managing audit trails.

## 3. Preventing information leaks

In recent years, the number of endpoint PCs in many corporations and local governments has increased to 10s of thousands. As a result, the operations managers responsible for these PCs cannot grasp the update status of their security patches and the virus definitions of their anti-virus software. In operating environments, security patches are often not applied to endpoint PCs. An investigation of the environment of one of our customers revealed that up-to-date security patches had not been applied to about 66% of the endpoint PCs.

At endpoint PCs, users can easily install software that may cause information leaks and may copy confidential files to external storage media (e.g., a hard disk, floppy disk, CD, DVD, or USB flash memory), print out files, and take the documents offsite. In such an environment, important information may be taken offsite and media containing vital information may be lost without the knowledge of the operations managers, who therefore cannot prevent leaks of information at the endpoint PCs. An analysis of incidents occurring in 2005 conducted by the NPO Japan Network Security Association showed that about 42% of the incidents involved loss or misplacement, about 17% involved operational and administrative errors, and about 7% involved inappropriate acts by in-house personnel. Therefore, in-house personnel were responsible for as much as 66% of all incidents reported.[6]

We found there are two main issues to be addressed regarding this situation. First, relying on the ethics of endpoint PC users cannot effectively prevent information leaks. Second, operations managers are unable to ascertain the effects of preventive measures because they cannot assess and understand the situation regarding endpoint PCs, even if the measures have been taken. Therefore, they cannot analyze the risks of information leaks or plan effective measures.

## 4. Measures for preventing information leaks

For the first issue, we consider it necessary to take measures without operations being performed by endpoint PC users, for example, providing functions to prevent the copying of business files to external storage media and automatically applying security patches. By using these functions, operations managers can take measures based on operation policies to resolve this issue.

For the second issue, we must develop a method of ascertaining the effects of measures that have been taken. For example, the status of applied security patches and the operation logs at endpoint PCs must be collected and sent to the management server for subsequent analysis.

To provide a solution for preventing information leaks, we have developed Systemwalker Desktop products with the following functions:

1) IT asset management for understanding the security situation

This function enables operations managers to manage the IT assets — especially installed software — of thousands of endpoint PCs. This is very important because IT assets are a major cause of information leaks.

With this function, the operations managers can automatically apply security patches to endpoint PCs and analyze the results of a patch application from the management console.

2) Restrictions on user operations and management of audit trails

The operations managers can restrict user operations such as the printing of files and copying of files to external storage media and also collect operation logs at endpoint PCs so they can manage audit trails. Restriction and logging of user operations at endpoint PCs are based on operation policies defined by the operations managers. Operation logs are collected and sent to the management server so the operations managers can use them to understand and improve the security situation.

## 4.1 Automatic application of security patches

Systemwalker Desktop Patrol provides a function for the automatic application of security patches. **Figure 1** shows the mechanism of this function. To manage more than 1000 PCs, relay servers are usually employed to balance the load. The processing flow is as follows:

1) Definition of operation policies by the operations managers

The operations managers define the types of information (e.g., hardware information, operating system information, software information) to be collected at endpoint PCs for IT asset management and the collection frequency (e.g., daily or

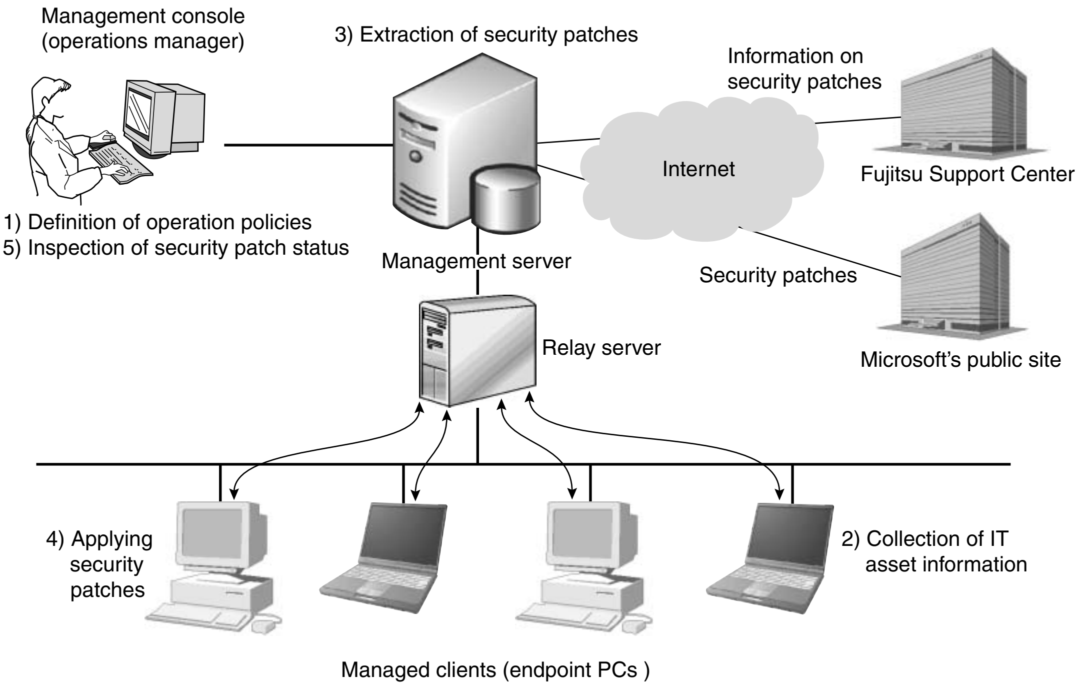

Management console
(operations manager)
3) Extraction of security patches
Information on security patches
Internet
Fujitsu Support Center
1) Definition of operation policies
5) Inspection of security patch status
Management server
Security patches
Relay server
Microsoft's public site
4) Applying security patches
2) Collection of IT asset information
Managed clients (endpoint PCs )

Figure 1
Mechanism of automatic application of security patches.

every Monday). These operation policies are automatically distributed to the endpoint PCs.

The operations managers also specify the security patches to be applied to endpoint PCs, then the specified security patches are automatically downloaded.

2) Collection of IT asset information at endpoint PCs

Based on the operation policies distributed to endpoint PCs, information concerning IT assets is collected at the endpoint PCs and sent to the management server.

3) Extraction of security patches to be applied

The management server collates the operation policies and information stored on the management server concerning the software installed on each endpoint PC. Then, the management server extracts the necessary security patches to be applied to each endpoint PC and distributes them to the PCs based on the extraction results.

4) Applying security patches to endpoint PCs

The distributed security patches are applied to endpoint PCs, then the application status of those PCs are updated at the next collection of IT asset information.

5) Inspection of the security patch status

The operations managers can check from the management console whether security patches have been applied to the endpoint PCs. In this way, the status of security patches for the entire system can be inspected.

Therefore, endpoint PC users need not perform any related operations. Moreover, the mandatory application of security patches can be managed under the guidance of the operations managers.

The operations managers can also inspect the update status of the virus definitions of anti-virus software from the management console.

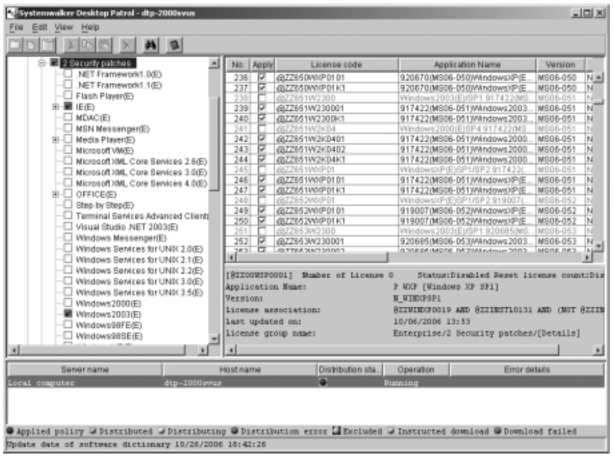
Additionally, the Fujitsu Support Center regularly distributes information about security patches. This information is a kind of security patch list and includes the conditions for applying patches, information for downloading patches from Microsoft's public site to the management server, and so on. Systemwalker Desktop Patrol automatically interprets this information, so the operations managers only need to specify the necessary security patches from the management console. Then, the patches are automatically applied to the endpoint PCs. This makes it easy for operations managers to manage the system.

**Figure 2** shows the management console for specifying the security patches to be applied. The window consists of three fields: the upper-left field showing the names of software, the upper-right field showing the list of security patches for the software selected in the upper-left field, and the lower field showing the status of the management server and relay server. The operations managers only need to check the boxes in the upper-left and upper-right fields.

Although there are other products for automatically applying security patches to endpoint PCs, these products require the operations managers to manually download security patches to the management server and define the application conditions.

## 4.2 Restrictions on user operations and management of audit trails

Systemwalker Desktop Keeper provides



☑ 2 Security patches
☐ .NET Framework1.0(E)
☐ .NET Framework1.1(E)
☐ Flash Player(E)
☑ IE(E)
☐ MDAC(E)
☐ MSN Messenger(E)
☐ Media Player(E)
☐ Microsoft VM(E)
☐ Microsoft XML Core Services 2.6(E)
☐ Microsoft XML Core Services 3.0(E)
☐ Microsoft XML Core Services 4.0(E)
☐ OFFICE(E)
☐ Step by Step(E)
☐ Terminal Services Advanced Client
☐ Visual Studio .NET 2003(E)
☐ Windows Messenger(E)
☐ Windows Services for UNIX 2.0(E)
☐ Windows Services for UNIX 2.1(E)
☐ Windows Services for UNIX 2.2(E)
☐ Windows Services for UNIX 3.0(E)
☐ Windows Services for UNIX 3.5(E)
☐ Windows2000(E)
☑ Windows2003(E)
☐ Windows98FE(E)
☐ Windows98SE(E)

| No. | Apply | License code | Application Name | Version | |
|---|---|---|---|---|---|
| 236 | ☑ | @ZZ650WXP0101 | 920670(MS06-050)WindowsXP(E... | MS06-050 | N |
| 237 | ☑ | @ZZ650WXP01K1 | 920670(MS06-050)WindowsXP(E... | MS06-050 | N |
| 238 | ☐ | @ZZ651W2300 | Windows2003(E)SP1:917422(MS... | MS06-051 | N |
| 239 | ☑ | @ZZ651W230001 | 917422(MS06-051)Windows2003... | MS06-051 | N |
| 240 | ☑ | @ZZ651W2300K1 | 917422(MS06-051)Windows2003... | MS06-051 | N |
| 241 | ☐ | @ZZ651W2K04 | Windows2000(E)SP4:917422(MS... | MS06-051 | N |
| 242 | ☑ | @ZZ651W2K0401 | 917422(MS06-051)Windows2000... | MS06-051 | N |
| 243 | ☑ | @ZZ651W2K0402 | 917422(MS06-051)Windows2000... | MS06-051 | N |
| 244 | ☑ | @ZZ651W2K04K1 | 917422(MS06-051)Windows2000... | MS06-051 | N |
| 245 | ☐ | @ZZ651WXP01 | WindowsXP(E)SP1/SP2:917422(... | MS06-051 | N |
| 246 | ☑ | @ZZ651WXP0101 | 917422(MS06-051)WindowsXP(E... | MS06-051 | N |
| 247 | ☑ | @ZZ651WXP01K1 | 917422(MS06-051)WindowsXP(E... | MS06-051 | N |
| 248 | ☐ | @ZZ652WXP01 | WindowsXP(E)SP1/SP2:919007(... | MS06-052 | N |
| 249 | ☑ | @ZZ652WXP0101 | 919007(MS06-052)WindowsXP(E... | MS06-052 | N |
| 250 | ☑ | @ZZ652WXP01K1 | 919007(MS06-052)WindowsXP(E... | MS06-052 | N |
| 251 | ☐ | @ZZ653W2300 | Windows2003(E)SP1:920685(MS... | MS06-053 | N |
| 252 | ☑ | @ZZ653W230001 | 920685(MS06-053)Windows2003... | MS06-053 | N |

```
[@ZZ00MSP0001]  Number of License 0     Status:Disabled Reset license count:Dis
Application Name:             P WXP [Windows XP SP1]
Version:                      N_WINXPSP1
license association:          @ZZWINDCP0019 AND @ZZINST10131 AND (NOT @ZZIN
last updated on:              10/06/2006 13:53
license group name:           Enterprise/2 Security patches/[Details]
```

| Server name | Host name | Distribution sta... | Operation | Error details |
|---|---|---|---|---|
| Local computer | dtp-2000svus | ● | Running | |

● Applied policy ● Distributed ● Distributing ● Distribution error ▨ Excluded ● Instructed download ● Download failed

Update date of software dictionary 10/26/2006 18:42:26

Figure 2
Management console for specifying security patches.

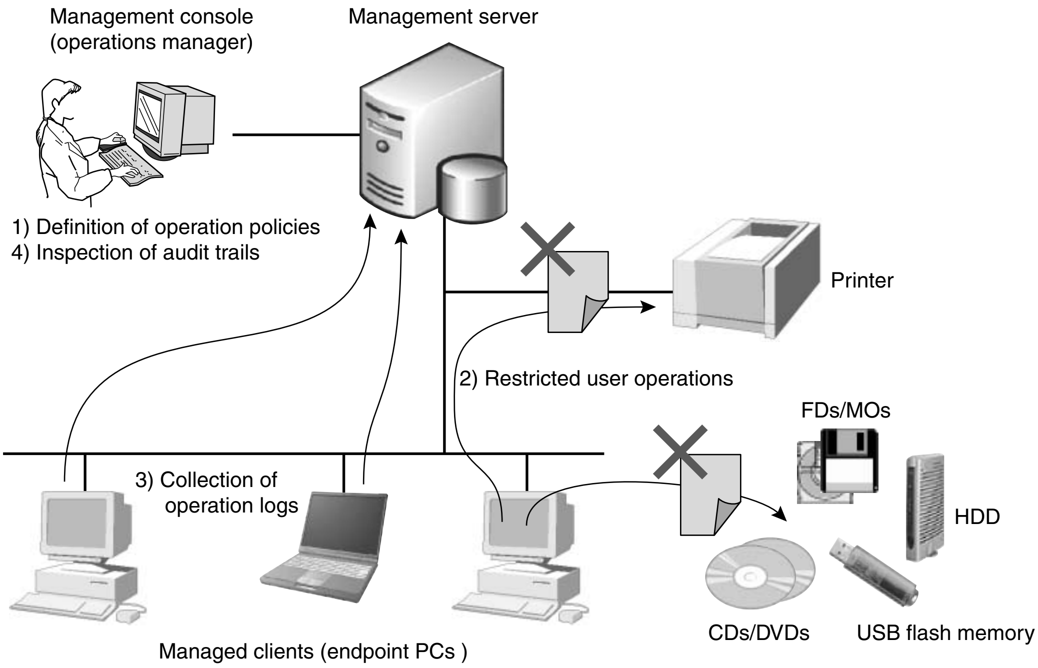

Management console
(operations manager)
Management server
1) Definition of operation policies
4) Inspection of audit trails
Printer
2) Restricted user operations
FDs/MOs
3) Collection of operation logs
HDD
CDs/DVDs
USB flash memory
Managed clients (endpoint PCs )

Figure 3
Mechanism of user operation restrictions and management of audit trails.

functions to prevent files from being written to external storage media and to encrypt files prior to writing so that unencrypted files cannot be taken offsite.

Systemwalker Desktop Keeper also collects user operation logs at the endpoint PCs and sends the logs to the management server for audit trails.

**Figure 3** shows the mechanism of these functions. The processing flow is as follows:

1) Definition of operation policies by the operations managers

The operations managers define the operation policies (e.g., restrictions on writing to external storage media, authorized writing with mandatory encryption, and restricted file printing). The operation policies are automatically distributed to the endpoint PCs.

2) Restrictions on user operations at endpoint PCs

Restrictions are imposed on the endpoint PCs according to the distributed operation policies. If an endpoint PC user attempts to write a file to a prohibited external storage media, the process is prevented at the driver level or the file is forcibly encrypted and then written to the media. If an endpoint PC user attempts to print the file, the process is prevented at the application level.

3) Collection of operation logs

When endpoint PC users execute certain operations defined by operation policies, the operation logs are collected and sent to the management server.

4) Inspection of audit trails (operation logs)

On the management console, the operations managers can check which files the users have attempted to copy to an external storage medium, which files have been encrypted and taken offsite, and who has attempted to print files.

By analyzing this information, the operations managers can make suggestions for improving the security situation.

## 5. Conclusion

This paper introduced the Systemwalker Desktop products suite for implementing privacy protection measures in compliance with Japan's privacy protection laws. We presented practical information about the mechanism of Systemwalker Desktop Patrol for applying security patches and the mechanism of Systemwalker Desktop Keeper for restricting user operations and managing audit trails.

In the next issue of FSTJ, we will introduce the technologies of Systemwalker Desktop Rights Master and Systemwalker Desktop Inspection.

In the future, we plan to extend the capabilities of this suite, for example, by adding internal control functions.

## References

1) Fujitsu: Solution to prevent the information leak. (in Japanese).
*http://systemwalker.fujitsu.com/jp/solution/solution_31.html*

2) Nikkei Business Publications: Security solutions of FUJITSU, Preventing the information leak. (in Japanese).
*http://info.nikkeibp.co.jp/nbpp/fujitsu_security/02/index.html*

3) Fujitsu: Introduction case of Kanto Electrical Safety Inspection Association. (in Japanese).
*http://systemwalker.fujitsu.com/jp/casestudies/companies/kdh/index.html*

4) Fujitsu: Systemwalker Desktop Patrol.
*http://www.fujitsu.com/global/services/software/systemwalker/products/dtp/*

5) Fujitsu: Systemwalker Desktop Keeper.
*http://www.fujitsu.com/global/services/software/systemwalker/products/dtk/*

6) NPO Japan Network Security Association: 2005 Information Security Incident Survey Report. Ver.1.0, July 31, 2006.
*http://www.jnsa.org/result/2005/20060803_pol01/2005incidentsurvey_060731en.pdf*

**Makoto Shimosaki**, *Fujitsu Ltd.*
Mr. Shimosaki received the M.S. degree in Informatics from Kyushu University, Fukuoka, Japan in 2001. He joined Fujitsu Ltd., Yokohama, Japan in 2001, where he has been engaged in development of enterprise management products.

**Toru Murai**, *Fujitsu Ltd.*
Mr. Murai received the M.S. degree in Physics from Niigata University, Niigata, Japan in 1988. He joined Fujitsu Ltd., Yokohama, Japan in 1988, where he has been engaged in development of enterprise management products.

**Shingo Ohnishi**, *Fujitsu Ltd.*
Mr. Ohnishi received the B.E. degree in Engineering from Doshisha University, Kyoto, Japan in 1987. He joined Fujitsu Aichi Engineering Ltd., Aichi, Japan in 1987 and then moved to Fujitsu Ltd., Yokohama, Japan in 1999, where he has been engaged in development of enterprise management products.