

# *MistyGuard Solution: An Easy-to-Use Information Security Software*

Authors: *Atsuo Tanaami\** and *Tetsuo Hayama\*\**

## 1. Introduction

Mitsubishi Electric Information Systems Corporation has upgraded its MistyGuard Solution software, file encryption software CRYPTOFILE PLUS, PC log-on software MISTYLOGON Lite, and corporate confidential information management software DROSY Enterprise Edition, for organizations and individuals wishing to implement information security solutions which are much easier to use than the previous ones.

Following the enforcement of the Act on the Protection of Personal Information, corporations have started to consider how to manage the personal information that they keep and have actively introduced self-protection measures to protect personal information. In 2005, there were many incidents of corporate confidential information being leaked via P2P file sharing software and it became a major social issue, as such incidents threatened business continuity. Information security measures were once believed to be necessary only for highly confidential information, but today such measures are indispensable to corporations.

Under such circumstances, MDIS provides users with not only information security tools but also MistyGuard solutions that focus on ease-of-use for organizations and individuals.

This report summarizes easy-to-use MistyGuard solutions.

## 2. Considerations for Corporate Information Security Measures

### 2.1 Information security measure I (Prevention of information leakage)

Corporate information security measures differ from one company to another. Many corporations use encryption of hard disk drives and files as security measures for PCs. Such encryption is designed to protect the information stored in the PC, USB memory devices, or other types of digital media carried by their employees during business trips or the like in case of loss or theft. Some corporations have also introduced tools to record operations such as historical access to data or to prohibit unauthorized persons from reading data from their PCs in case of actual incidents.

### 2.2 Information security measure II (IT governance)

Typical incidents of information leaks that have been

publicized since the Act on the Protection of Personal Information was enforced were information leaks from PCs via file-swapping software. The information leaks occurred after PCs became infected with viruses via file-swapping software, highlighting the fact that tools to encrypt hard disk drives are not a reliable means of securing information to prevent such incidents.

Such incidents seriously threaten business continuity and so are addressed as part of corporate governance measures (IT governance).

Examples of measures against incidents involving file-swapping software

- (1) Prohibition of PC use for non-business purposes
- (2) Designation of banned software
- (3) Mandatory use of "Microsoft Windows Update" function (suppression of vulnerability)
- (4) Mandatory updating of virus check patterns (suppression of vulnerability)
- (5) Transition to authorization system for removing PCs or digital media from their designated positions

### 2.3 Considerations for implementing information security measures

Information security measures often cause difficulties and affect primary business operations, as the measures place top priority on safety rather than operational efficiency.

On the other hand, the responsibility of information users for risks related to information security incidents has grown remarkably. Information needs to be protected by information security tools so that users can, without fear, use devices containing data out of their designated positions. In addition, the load on administrators also needs to be minimized. Effective information security tools that meet such needs are necessary.

## 3. Easy-To-Use MistyGuard Solution

To solve such problems, the MistyGuard Solution provides simple information security solutions that are easy to understand and use.

### 3.1 Encryption software for automatically updating security settings: CRYPTOFILE PLUS

CRYPTOFILE PLUS is a program for encrypting PC data, which is a fundamental information security measure, and serves as the core software of the MistyGuard Solution. Unlike other security programs

which encrypt and decrypt the entire hard disk upon each startup and shutdown of the PC, CRYPTOFILE PLUS performs encryption and decryption sequentially upon each time of writing and reading to/from the hard disk. CRYPTOFILE PLUS does not keep the user waiting for as long as 10 minutes upon starting up or shutting down the PC. The software can also prohibit data from being written to a removable disk, and can record the history of file operations.

With the old versions of CRYPTOFILE PLUS, when changing the security settings (policies) for encryption operation and access to removable disks, reinstallation of CRYPTOFILE PLUS and decryption of encrypted files were required. In contrast, the new version of CRYPTOFILE PLUS requires only the preparation of the policy update file followed by distribution of the file from the server for automatic update of the security settings on each PC (see Fig. 1). The policy update file is encrypted with the policy group key generated upon implementing CRYPTOFILE PLUS to prevent unauthorized manipulation, thus preventing users from altering the security settings.

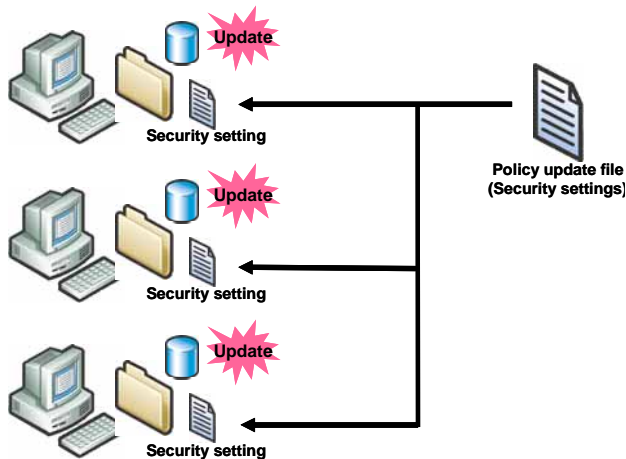


Fig. 1 Policy update of CRYPTOFILE PLUS

### 3.2 PC log-on security for protecting data and PC with USB flash memory equipped with fingerprint recognition device: MISTYLOGON Lite

The previous version of PC log-on security MISTYLOGON required a special server for administration.

With MISTYLOGON Lite which does not require a server for administration, administrative functions are provided on the PC, so the PC can be logged onto only by fingerprint recognition technology using a USB flash memory equipped with a fingerprint recognition device (see Fig. 2). With log-on information (such as ID and password) and fingerprint data associated in advance, the fingerprint recognition operation allows the user to log on to the computer automatically. The fingerprint recognition device can register fingerprints of up to two fingers of the user, to allow for recognition errors due to

the condition of one finger.



Fig. 2 Fingerprint recognition screen of MISTYLOGON Lite

To change the log-on password periodically, the user can activate the administrator tool by the fingerprint recognition and then update the associated log-on information (see Fig. 3).

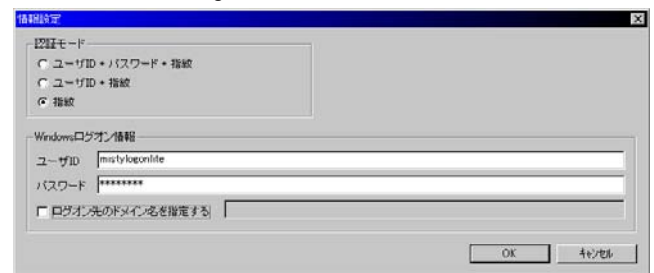


Fig. 3 Association of log-on information on MISTYLOGON Lite

The USB flash memory of MISTYLOGON Lite equipped with the fingerprint recognition device can be used as a digital medium to remove data safely from the computer. The fingerprint recognition function allows the user to log on to the USB flash memory and access data (for writing or reading), thus ensuring safe data removal.

The program also records the log-on history in a log and the logs collected by the administrator can be viewed.

MISTYLOGON can be equipped with an optional feature that allows the user to log on with a smart card and the fingerprint recognition device in addition to the USB flash memory equipped with the fingerprint recognition device.

### 3.3 Corporate confidential information management software: DROSY Enterprise Edition

DROSY Enterprise Edition is a solution for safely sharing confidential information within a corporation. The users and types of operation in conjunction with

confidential documents encrypted by DROSY functions are limited (authorization and protection). The protected documents remain encrypted all the time and confidentiality cannot be broken even if the documents are leaked from the computer by illegal file-swapping software or the like.

Two major problems existed with introducing and implementing the previous versions of the software. The first problem was associated with the document protection method; the protection process took a long time because particular documents to be protected had to be specified. With the new version, however, the protection folder on the DROSY server automatically protects all the documents stored in that folder, thus greatly reducing the time required for the document protection process. This protection folder is associated with sub-folders, which can directly be used as a shared folder (see Fig. 4).

The second problem was related with the management of identity information (management of user-identification data). With the old version of the software, DROSY managed the users independently. With the new version, the program together with Active Directory defines the log-on users of Windows PC as DROSY users and integrates the user authentication operation, thus reducing the user management load on the administrator. Furthermore, the user groups of Active Directory can be imported as they are.

#### 4. Application Examples of MistyGuard Solution

This section introduces application examples of MistyGuard Solution including the three products introduced above.

Figure 5 shows an example in which the user can automatically log on to CRYPTOFILE PLUS, DROSY, and Active Directory at the same time by logging on to the PC by using the USB flash memory of MISTY-LOGON Lite equipped with a fingerprint recognition device. In this case, Active Directory consolidates the entire user management, access to the shared file server is controlled by the domain user management function, and some of the files are protected by DROSY.

Other application examples include a log management system to collect the history of log-on and log-off to PCs and file operations, and controlled access records from controlled-access management equipment (Mitsubishi Integrated Building Security System “MEL-SAFETY”), and a system for file encryption and sharing confidential information by using CRYPTOFILE and DROSY in a MetaFrame environment using thin clients. Mitsubishi provides all these applications with the easy-to-use MistyGuard Solution working efficiently in harmony with existing systems.

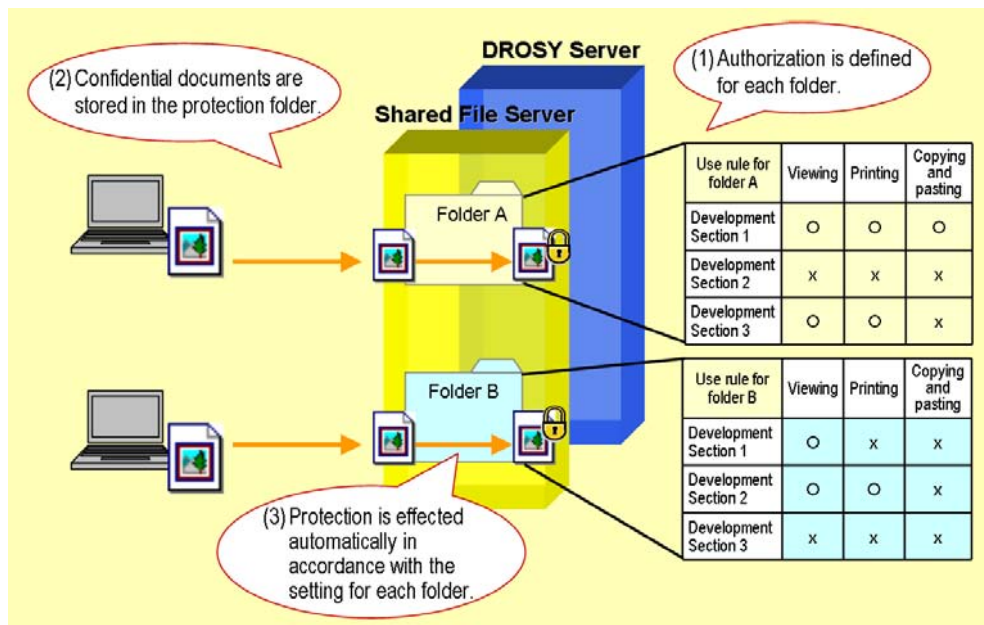


Fig. 4 Automatic conversion of confidential information by file server folder control of DROSY Enterprise Edition

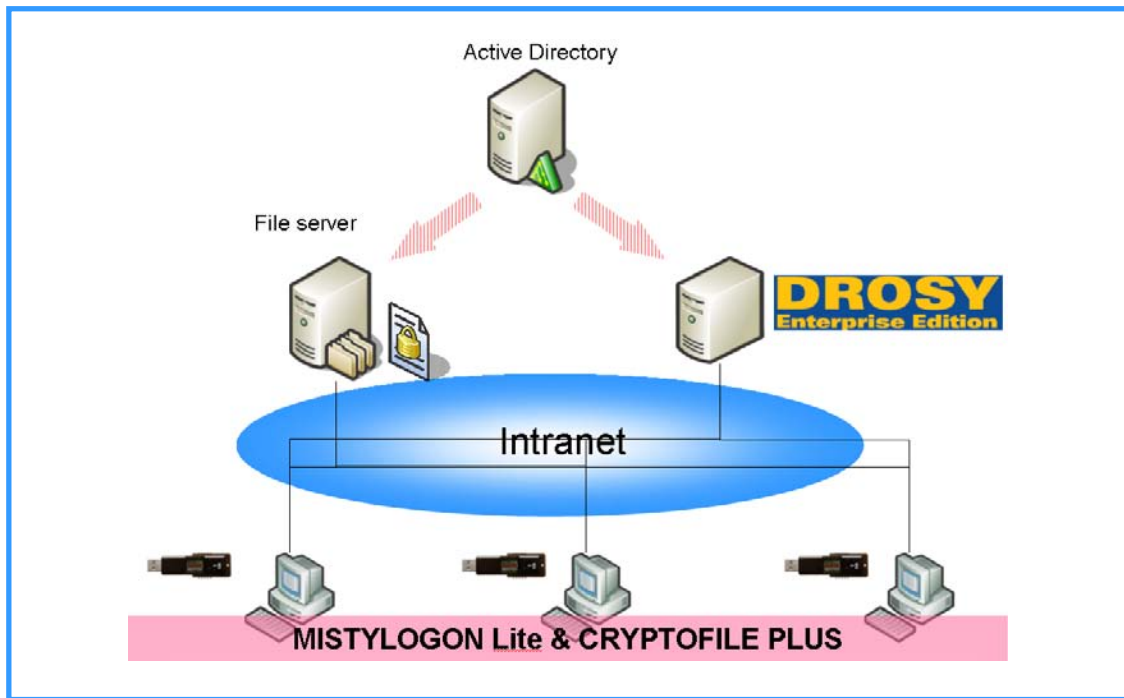


Fig. 5 Application example of MistyGuard Solution