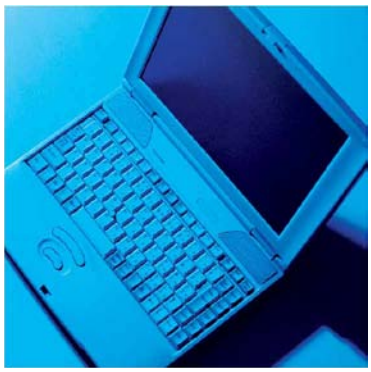
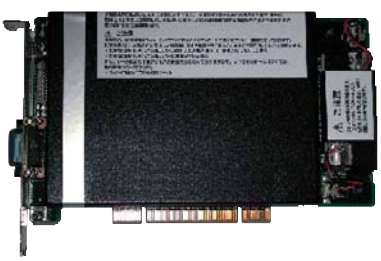
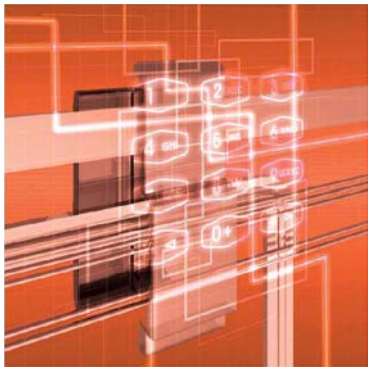
ISSN 1345-3041
MITSUBISHI ELECTRIC Jun. 2007／Vol.118

ADVANCE

Information Security System and Service Infrastructure







MITSUBISHI ELECTRIC
Changes for the Better

Jun. 2007 / Vol. 118
MITSUBISHI ELECTRIC ADVANCE
Information Security System and Service Infrastructure

Cover Story

The photo on the cover shows an example of information network security equipment.

The photo in the upper right shows a USB flash memory equipped with a fingerprint recognition device.

The photo in the middle shows a VPN board applicable to a wire speed of 10 Gbps.

The photo in the lower left shows a PCI half-size Tamper-resistance Encryption Board with high-speed RSA Encryption and a hardware random number generator.

• **Editorial Inquiries**
Makoto Egashira
Corporate Total Productivity Management
& Environmental Programs
Fax +81-3-3218-2465

• **Product Inquiries**
Technology Management Group
Planning & Coordination Dept.
Information Technology R&D Center
Fax +81-467-41-2142

Mitsubishi Electric Advance is published on line quarterly (in March, June, September, and December) by Mitsubishi Electric Corporation.

CONTENTS

Technical Reports

Overview

Author: *Tsuyoshi Motegi**

IT Platform for Information Security Management

As information technology advances and spreads, the risks associated with information security are increasing. Various new and diverse unknown security risks are reported each day, so it is no longer sufficient to introduce a set of uni-functional security products for protecting systems. Rather, we need a more sophisticated *Information Security Management Platform* which continuously maintains enterprise information security levels after installing products.

We focused on two aspects of environmental changes, internal and external, which directly or indirectly introduce information security risks around an enterprise. In order to reduce the risks caused by internal changes, we developed *(1) the Policy-based Security Management System* which monitors and controls the changes in the configuration of computers and applications, *(2) the Identity Lifecycle Management System* which permits changes in the organization and its people, and *(3) the Integrated Management System for Various Log Data* which exhaustively records and tracks the changes themselves. For external changes, we also developed *(4) the Information Security Forecast System* which captures the first signs of unknown security risks, and enables actions to be taken in advance.

For years, Mitsubishi Electric Group has been providing systematic security solutions which integrate physical and information security components and technologies. In this feature article, we propose the IT Platform for Information Security Management System which continuously allows enterprises not only to maintain but also to improve their security levels in the midst of internal and external changes.

**Information Technology R&D Center*

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

*Mitsubishi Electric Information Systems Corporation **Information Systems & Network Service Group

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.

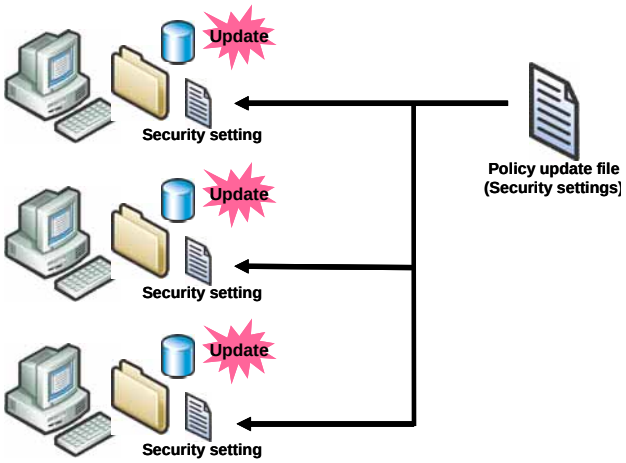


Fig. 1 Policy update of CRYPTOFILE PLUS

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).

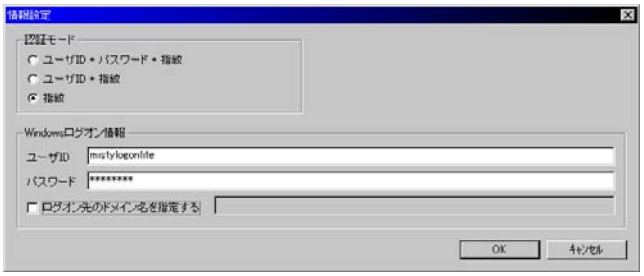


Fig. 3 Association of log-on information on MISTYLOGON Lite

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 “MELSAFETY”), 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.

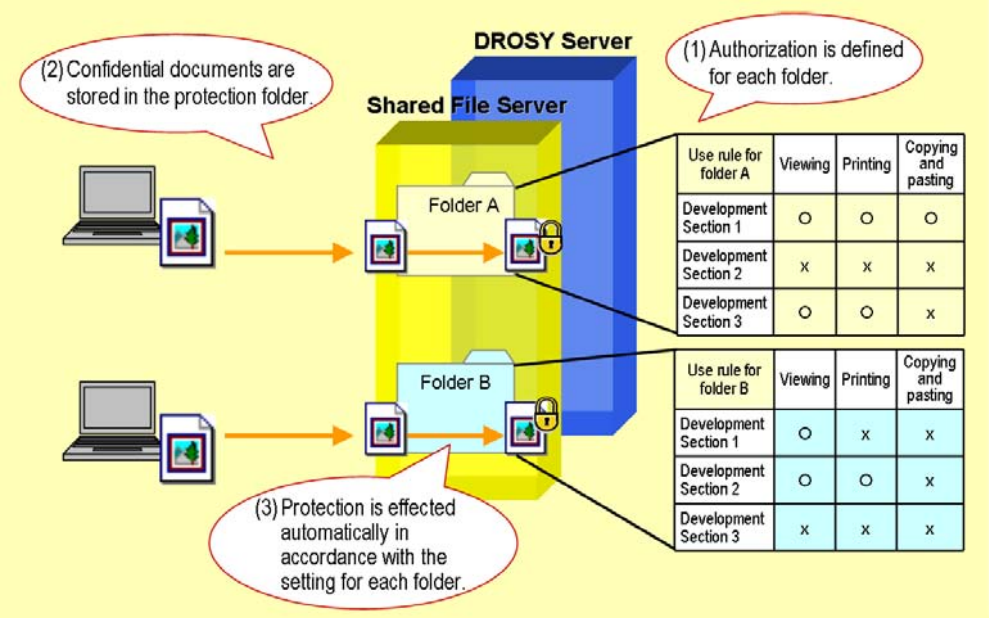


Fig. 4 Automatic conversion of confidential information by file server folder control of DROSY Enterprise Edition

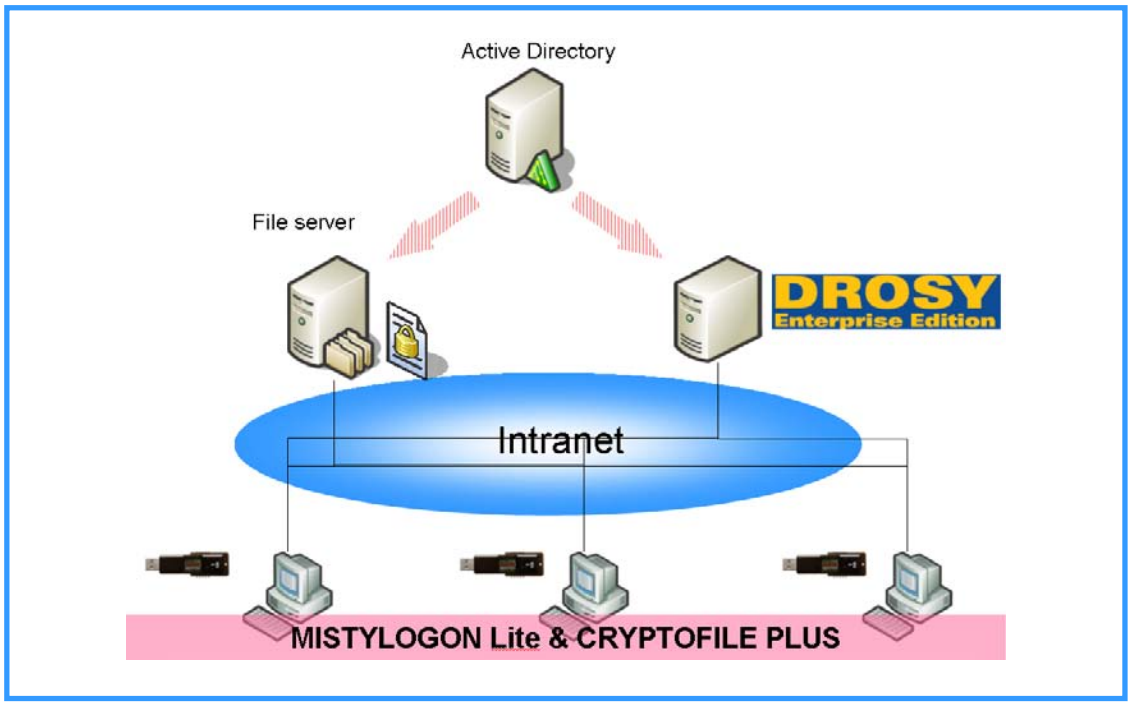


Fig. 5 Application example of MistyGuard Solution

Identity Lifecycle Management Technology

Authors: *Seiichi Kondo** and *Tatsuya Tsurukawa**

1. Introduction

In an integrated identity management system for shared use by the types of security components of a corporate information system and business operation system, the lifecycle should be managed in accordance with the organizational structure of the corporation in order to reduce operating costs associated with types of variations, to maintain and improve the security level, and to ensure digital traceability.

2. Identity Management and Problems

An identity management system manages information concerning identity and access privileges assigned to users. As shown in Fig. 1, the identity information is uniformly managed by the database for safe and efficient user authentication and authorization. The identity information is distributed to the controlled access management system and business applications, etc. The identity information is also used for authorization concerning user authentication and access privileges employed in various systems such as PC log-on, removable devices control, file encryption, and single sign-on for Web based applications.

Lifecycle management of the identity management system is required to deal with the following variations which may arise after the system has been introduced due to the company's activities.

(1) Variations in information of identity and access policy
User attribute information which is the basis of access control changes in accordance with employment, retirement, transfer, promotion, and reorganization. And also security targets such as devices, contents are added or removed, and policy improvement is done in accordance with internal or external factors.

(2) Variations in authentication device that identifies users
Smart cards identifying employees and visitors are increasingly being used for various types of applications. However, these cards are at risk of loss, contamination, damage, failure, and theft. To ensure operational safety, a quick response and appropriate measures in accordance with the security policies are necessary.

(3) Changes in user information of identity in log stored for a long time
Security Standard ISO/IEC 27001:2005 specifies regarding the acquisition of audit logs that an audit log containing the records of user activities, exception handling, and information security events shall be recorded and the log shall be stored for an agreed period in case of future investigations and for monitoring access control. Generally, such logs are held for a long time, and precise association with information concerning identity, devices, and contents which often change during the storage period becomes an important issue.

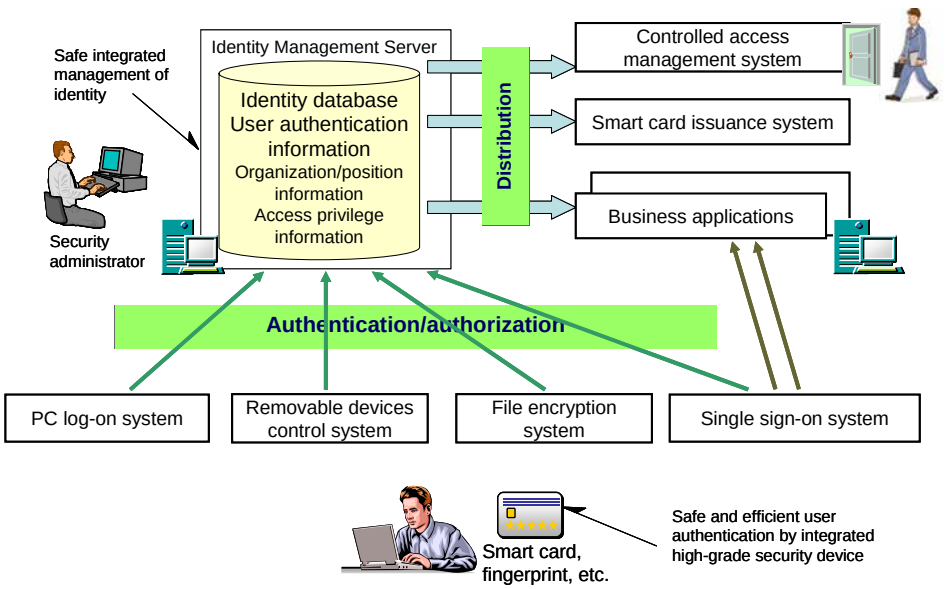


Fig. 1 Architecture of identity management system

*Information Technology R&D Center

This report introduces solutions to such problems in the following sections 3 to 5.

3. Identity Management for Corporations

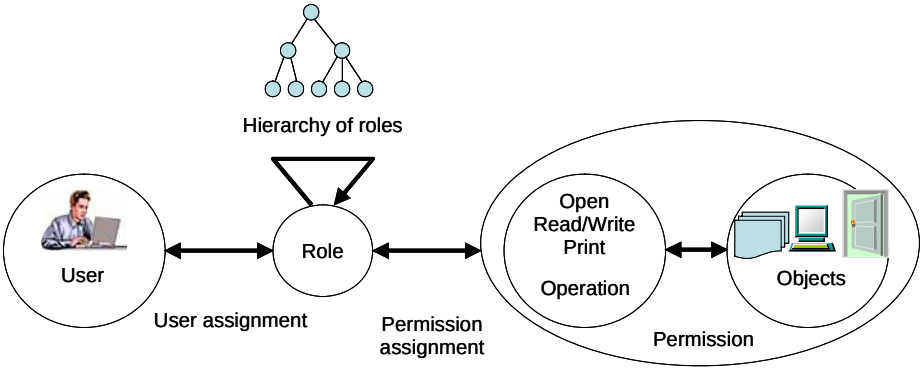
The RBAC (Role-Based Access Control) model[1] is widely used for access control with security objects such as devices and contents separated from users. In RBAC, changes in user information and security objects are localized by connecting the users and permission for operating security objects indirectly via a role. A hierarchical RBAC employs a hierarchical role. As discussed in Section 2 (a) above, corporations generally define roles on the basis of personnel information such as their organizations and positions, so there is an issue that changes in personnel details significantly affect the settings between roles and users.

To solve this problem, we propose the structure shown in Fig. 2 (b), in which the users and the organization associated with the personnel information are assigned independently from the roles. The relationships between roles and the organization and between roles and users are indirectly designated by rules defined by logical formula instead of directly connecting them. As a result, the influence of changes in personnel information on roles can be localized.

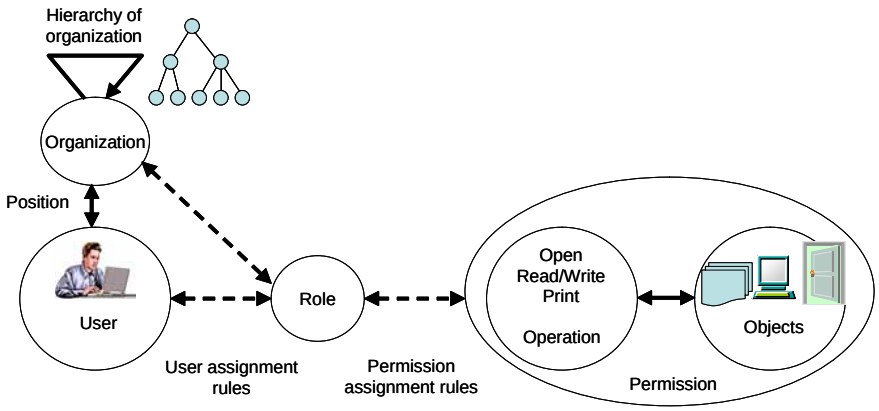
4. Smart Card Implementation Management

Corporations today increasingly use smart cards as employee IDs for controlling access to corporate facilities, logging on to PCs, approval, print-out authorization, etc. As discussed in Section 2 (2), it is necessary to change the access privileges, change to substitute cards, and output audit logs quickly and accurately whenever the details of smart card users change due to personnel relocations or business trips, and whenever smart cards are affected by loss, contamination, damage, failure, theft, or expiration of validity as shown in Fig. 3. Especially when smart cards are changed to substitute cards, how to maintain conformance between the official cards and substitute cards with respect to the combinations of conditions of cards is the key issue.

We propose the system shown in Fig. 4 in which smart card implementation rules are defined in a state chart to construct the implementation system without needing a program. The implementation rules are defined and operated as follows.



(a) Hierarchical RBAC



(b) Hierarchical organization RBAC

Fig. 2 Role-based access control (RBAC)

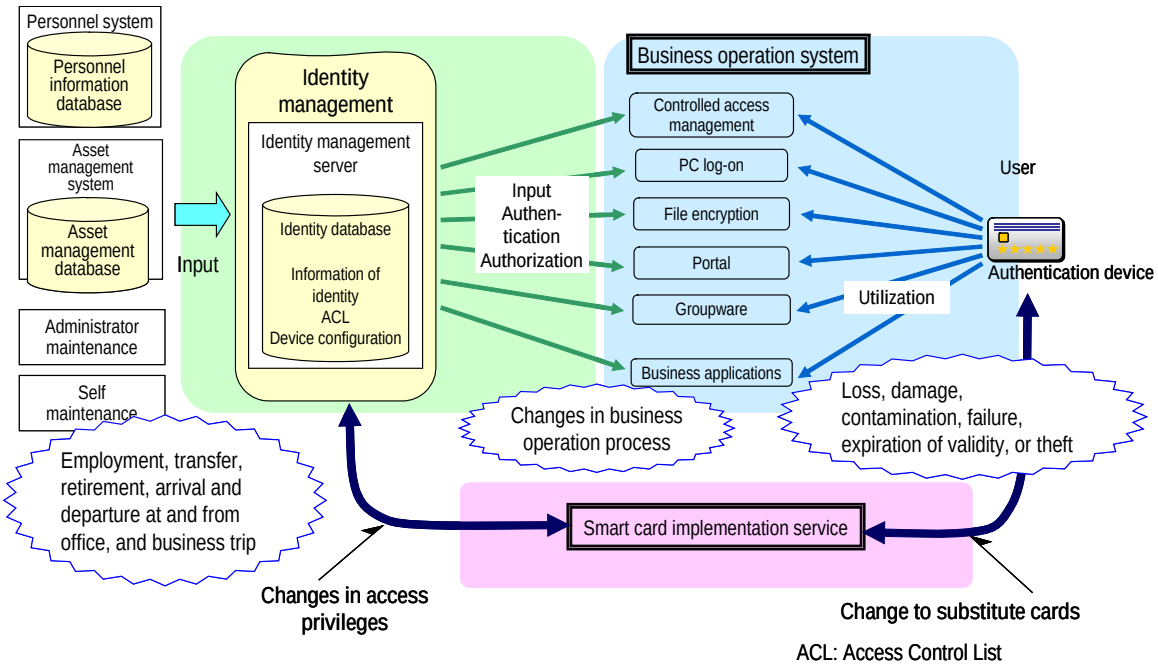


Fig. 3 Example of smart card management system

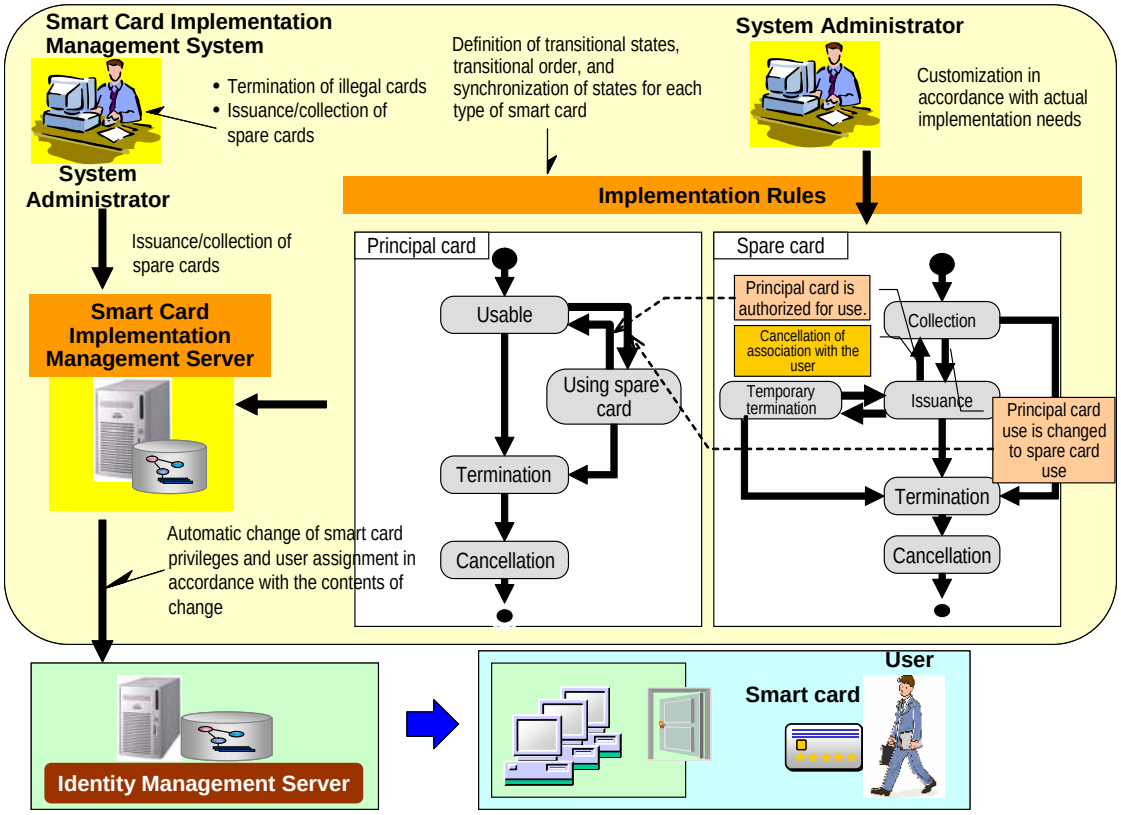


Fig. 4 System example using implementation rules

(1) The changes in the conditions of cards for employees, cards for nonemployees/residents, cards for visitors, and spare cards in case of accident are defined dynamically and independently from the program in the state chart as shown in Fig. 4.

(2) The changes in access privileges due to changes in the conditions or the restriction that the cards cannot be used simultaneously with the corresponding spare cards are defined as actions.

(3) The actions in accordance with the changes in the conditions are automatically executed according to the implementation rules defined in items (1) and

(2) above.

This configuration of implementation rules, which is independent of the program, has the following effects.

- Improved security level
  Conformance of conditions among two or more cards and automation of the function interlocked with the access privilege control prevent users from improper use, whether deliberate or accidental.
- Application of implementation rules to different environments
  Required implementation rules of smart cards can be used for different divisions without a program.

5. Digital Traceability

This section examines digital traceability which governs logs stored for a long time under a change of user information, as mentioned in Section 2 (3). Today, various systems collect and store the logs output by various application programs as well as the systems themselves, so that the causes of any information leaks could be analyzed. However, disagreement of user identifiers recorded in the logs for respective sources often prevents multiple logs from being analyzed in an integrated manner. To resolve this, digital traceability can improve log analysis by combining the identity management system which provides the identity lifecycle management function in response to changes in employment, transfer, and retirement of employees over a long time, as one of its characteristic functions.

Focusing on the user identifiers recorded in the logs, the problems in using them are listed below.

- Difficult to uniformly analyze multiple logs

Because the user identifiers are recorded with identifiers unique to each log, it is difficult to execute a uniform analysis spanning different logs.

- Attribute information of users cannot be used for analysis.

The attribute information (e.g., names and divisions) associated with the respective user identifiers is usually not recorded, and so cannot be used for analysis.

Figure 5 shows an example of a system configuration using digital traceability. The logs are collected from terminals, servers, and physical security equipments and stored in the log management server. The system also has an identity management server providing identity management function, and a management terminal that retrieves and displays the logs from the log management server.

- Inquiry and reflection of unified identifiers

The log management server, after collecting logs, makes inquiries with the identity management server to obtain the unified identifiers associated with the log-specific user identifiers stored in each log and reflects them in the logs for storage.

Logon account or E-mail address are examples of the log-specific user identifier above and the unified identifier above means the identifier which can uniquely identify the particular user like an employee No.

Inquiring and reflecting unified identifiers to all log records enables links between user identifiers recorded

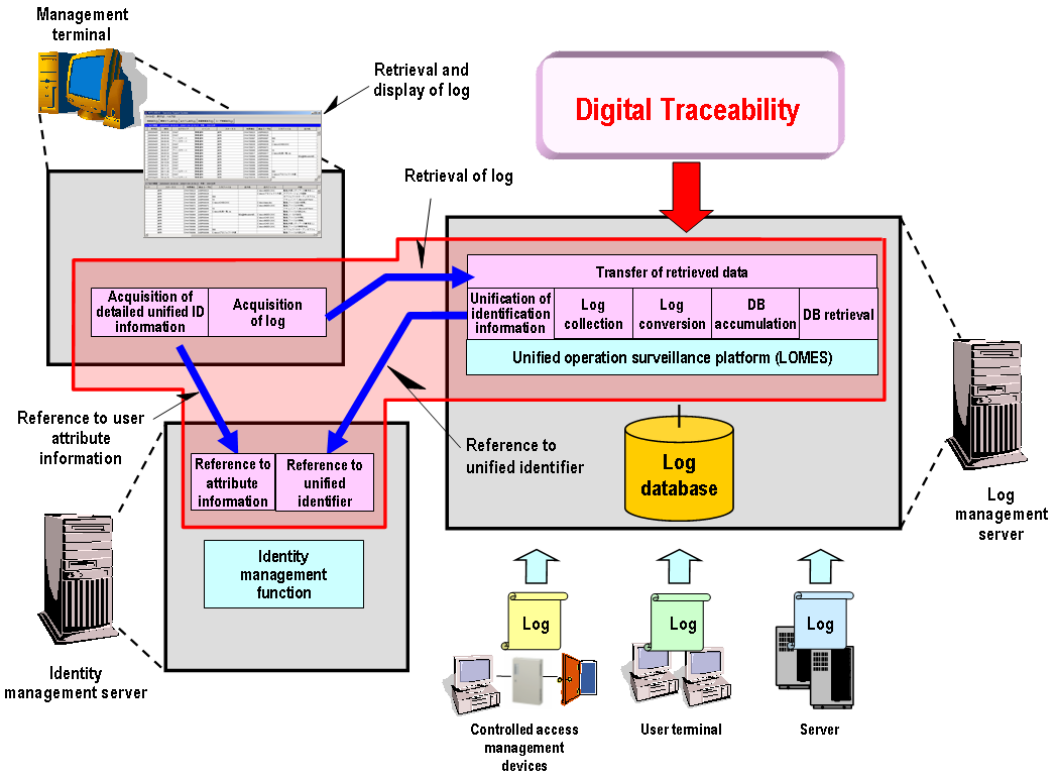


Fig. 5 Example of system configuration with digital traceability system

differently in each log and then makes uniform log analysis available.

- Analysis using attribute information

After retrieving and displaying a log on the management terminal, it can inquire a part of the attribute information associated with the unified identifier and it also can display them additionally (see Fig. 6). If all the attribute information is reflected in the accumulated log, the log becomes large and inefficiently consumes the capacity for the log database. However, it reflects them after retrieving and narrowing down the log, thus solving the problem and allowing the system to use the attribute information efficiently during log analysis.

Likewise, in combination with the identity management server, log analysis with referencing corresponding personnel affair information can be available by inquiring and displaying them as necessary (see Fig. 7). Even if the log to be analyzed is old and the corresponding user has retired, past logs still can be analyzed with the relevant personnel information based on the date and time of the log record.

We have stated the integrated management of identity and the lifecycle management for diversified changes of it, they are necessary to enable the governance of information systems.

We are going to seek "comfort" enabling convenience, "safety" by system automation, and "development" by providing identity history to logs in the identity implementation management.

Reference

R. S. Sandhu, D., et al.: Role-Based Access Control Models, IEEE Computer, 29(2): 38-47 (1996)

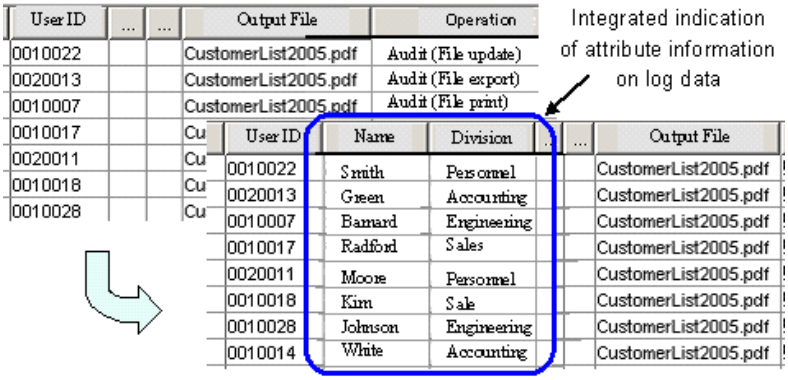


Fig. 6 Integrated indication of attribute information

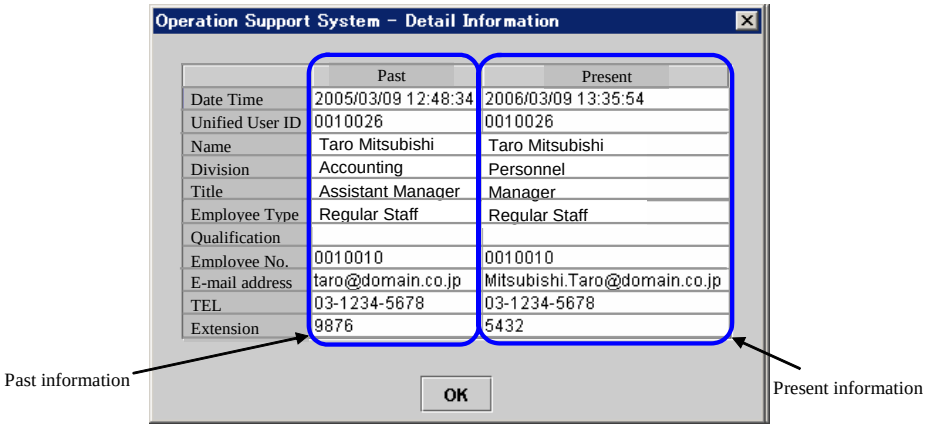


Fig. 7 Indication of past and present personnel information

LogAuditor Enterprise: Integrated Management System for Various Log Data

Authors: *Mitsunori Kori** and *Takashi Fujimura***

1. Introduction

LogAuditor Enterprise provides integrated management of various logs generated by information systems for a company's internal control and security management. Mitsubishi Electric has used its high-speed processing technologies to achieve integration, high-speed accumulation and searching of logs of different formats, while reducing the storage capacity required, which were hard to realize in the past. Analysis templates for outputting audit reports are also available.

2. Problems Related with Log Management

Amid the increasing interest in internal control and security management among corporations, the logs generated by various information systems need to be stored as evidence. However, the volume of such logs may reach tens of terabytes per year. And whereas logs used to be managed for each information system, today integrated management is required for reducing management costs and increasing the efficiency of problem analysis.

In conventional log management, a general-purpose RDB (Relational Database) was often used. However, since RDBs were developed for applications based on OLTP (On-Line Transaction Processing), they have various formats and are not suitable for efficiently processing logs that contain huge volumes of data[1]. As the types and volumes of logs have increased, log management using RDB involves the following problems.

- The data formats must be unified beforehand and logs of formats not specified in advance are difficult to handle.
- The time required for processing related to log accumulation or log search is too long.
- The cost of long-term storage is very high.

3. LogAuditor Enterprise

LogAuditor Enterprise solves these problems and provides integrated management of various large logs. LogAuditor Enterprise generally consists of LogAuditor/PSF (Power Staging Facility) which imports logs, LogAuditor/LDB (Log Database) which stores and monitors logs, and LogAuditor/AQL (Analytical Query Language) which is a log analysis engine. A Microsoft Excel add-in is provided as a front end for analysis. Table 1 shows the operating environment of LogAuditor Enterprise.

Table 1 Operating environment of LogAuditor Enterprise

Server	Microsoft Windows Server 2003
Client	Microsoft Windows XP Professional Microsoft Windows 2000 Professional

LogAuditor/PSF collects and processes various types of a company's internal log data, and has the following features:

- Fine and detailed data processing and edit functions
- High productivity and maintainability
- Major RDBs and CSVs as data sources can be applied.

LogAuditor/LDB[2] is a new type of database that can accumulate given logs, and has the following features:

- Logs, regardless of type, can be gathered and stored in a manner that allows the original logs to be restored completely. Particular log types need not be specified in advance.
- High-speed accumulation of terabyte-size logs and high-speed searching by regular expression specification
- Storage volume is reduced by data compression. Time-series management such as back-up or deletion of logs based on ranges such as daily or the like (patent pending)

LogAuditor/AQL is a database management system suitable for data compilation and analysis, and has the following features:

- Logs are held as structured data suitable for compilation and analysis
- High-speed data search and compilation
- Reduced required storage volume by data compression
- Conformance to standard SQL (Structured Query Language)

The analysis front end is an add-in tool that directly

[1] LogAuditor is a trademark owned by Mitsubishi Electric Information Technology Corporation.

[2] Microsoft, Excel, Windows, Windows Server 2003, Windows XP, and Windows 2000 are trademarks owned by Microsoft Corporation, U.S.A.

*Information Technology R&D Center **Mitsubishi Electric Information Technology Corporation

produces analysis reports by Microsoft Excel, and has the following features:

- Preparation and use of analysis templates
- Flexible atypical analysis and easy-to-use wizard type operation method
- Seamless operation from Excel and automatic generation of summary sheets
- Drill-through function to move from summary values to breakdown analysis data
- Linking of primary log data

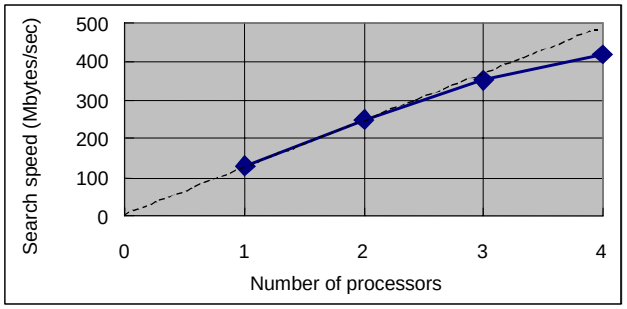


Fig. 2 Log full search performance (LogAuditor/LDB)

4. High-Speed Processing Technology of LogAuditor Enterprise

LogAuditor/LDB and LogAuditor/AQL offer high-speed processing of large logs thanks to Mitsubishi's unique large-scale data high-speed processing architecture SISA (Scalable Intelligent Storage Architecture).

In both LogAuditor/LDB and LogAuditor/AQL, logs are automatically compressed to reduce the required storage volume to about 1/10 or less of the standard. In addition, storage input/output is reduced by data compression, thus increasing the speed of accumulation and searching. Figure 1 shows an example of the reduction of data volume when a PC operation log is stored in LogAuditor/LDB. Compared to the RDB, the storage volume is reduced to about 1/23.

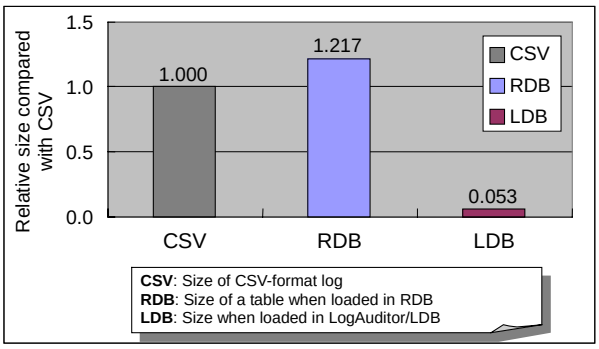


Fig. 1 Reduction of data by data compression (LogAuditor/LDB)

Both LogAuditor/LDB and LogAuditor/AQL execute compression, extension, and searching by parallel processing using multiple processors, distribute the data to multiple storage devices, and perform input/output operations in parallel. As a result, the system is highly scalable in accordance with the log volume. Figure 2 shows an example of the full search performance of LogAuditor/LDB with PC operation logs.

LogAuditor/LDB can extract logs by judging the log types upon log accumulation, without having to specify the log types prior to log accumulation. In the conventional character-string pattern matching method, the complicated pattern matching process was too slow for judging the type of log. But with Mitsubishi's own sDFA (size-reduced Deterministic Finite Automaton)[3] (patent pending) technology, a high speed of approximately 100 million characters/sec. is attained regardless of the search condition, thus solving the speed-related problem (see Fig. 3). Indexing is often used for boosting the speed of database searching, but indexing is unsuitable for log management because it decreases the accumulation speed and increases the storage volume. With LogAuditor/LDB, all requirements regarding accumulation speed, storage volume, and search speed are satisfied by high-speed character-string pattern matching technology.

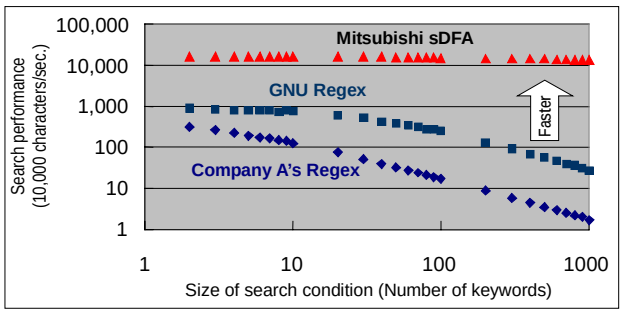


Fig. 3 Comparison of text search performance

5. Application Examples of Integrated Log Management Solution

As a solution making use of LogAuditor Enterprise, we provide an "Analysis Template" which outputs audit reports for internal control based on the corporate business operation flow execution log, PC operation log, file server access log, and the like. Analysis Template outputs Microsoft Excel type audit reports in accordance with the definitions of the structure of the integrated log DB, structure of the data mart for log analysis, and the log import style.

It is difficult to intuitively grasp a huge volume of information contained in a log. For example, an increase in the number of accesses to confidential files or its relationship with the execution status of business operation flow cannot easily be identified by viewing the logs of the file server and business applications. The audit reports are designed to present tables and graphs as reports by visualizing the intangible log data (see Fig. 5). Access to confidential files and business operation status with respect to users are clearly recognized and can be used for verifying or reviewing security management measures. Furthermore, causes can be analyzed in detail from a required position in the audit report by using the "Search back in log breakdown" function.

Integrated Log Management Solution is useful for information security management, internal control, information infrastructure management, information system implementation management, and many other fields.

6. Outlook

We plan to expand the scalability and improve the Analysis Template to handle larger logs and diversified log types.

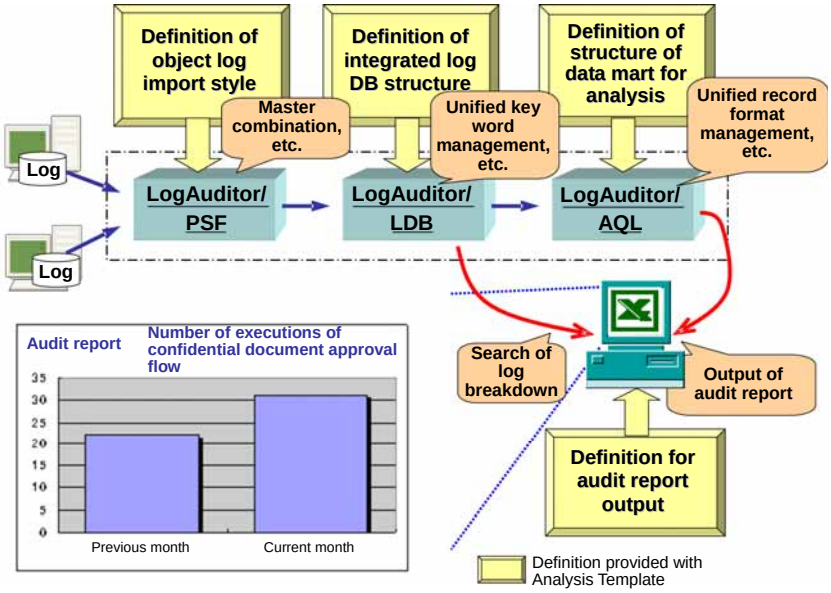


Fig. 4 Structure of analysis template

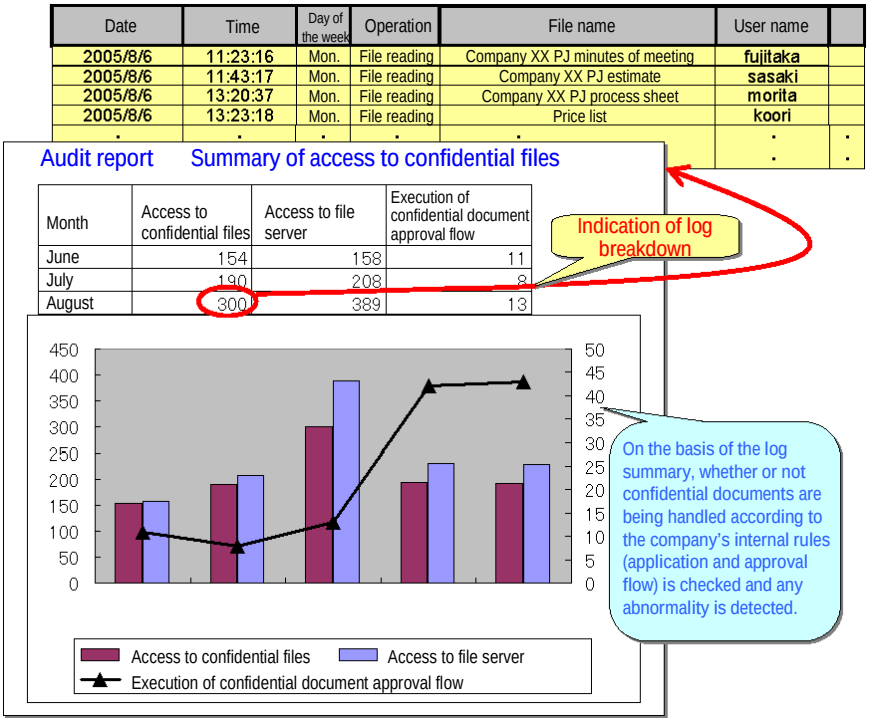


Fig. 5 Example of audit report

References:

(1) Sah, A.: A New Architecture for Managing Enterprise Log Data, Proc. of LISA 2002, 121 to 132 (2002)
(2) T. Nakamura, et al.: Realization of Large-Scale Log Database, 68th Information Processing Society National Conference, ID-2 (2006)
(3) T. Nakamura, et al.: High-Speed Pattern Matching Method for Large-Scale Regular Expressions, 67th Information Processing Society National Conference, 4F-5 (2005)
(4) T. Fujimura, et al.: Compliance Promotion Solution to Support Information Risk Management and Internal Control, Mitsubishi Electric Corporation Technical Report, 80, No. 4, 281 to 284 (2006)

EVERSIGN: Preserving the Long-Term Authenticity of Electronic Records

Authors: *Kazuya Miyazaki** and *Manabu Tanaka***

1. Introduction

Abiding by the e-Document Law and J-SOX Law (Japanese SOX law: Financial Products Dealings Act of 2006) requires that the authenticity of electronic records can be maintained for an extended period of time. In order to meet this requirement, a technology for securing the long-term validity of digital signatures is necessary. The EVERSIGN system mechanically constructs data complying with the long-term signature format, which is a standard format for this purpose, according to a predetermined schedule.

2. Mechanism of Signature Validity Extension

A digital signature is used to secure the authenticity of an electronic record. A digital signature refers to an electronic signature based on Public Key Infrastructure (PKI), and bases its trust on a public key certificate issued by the certification authority. The public key certificate contains mechanisms for the validity period and revocation, and the validity of the digital signature depends on the validity period and revocation of the public key certificate (Fig. 1). In other words, if the public key certificate exceeds the validity period or is revoked, the validity of the digital signature is also lost.

This is because a signature could be forged due to leakage of the signature key or vulnerability of algorithms if the public key certificate were allowed to exceed the validity period. This is also true of revocation because a signature could be forged using the leaked key.

A digital signature can contain time information, which is usually based on the system clock of the personal computer used to generate the digital signature. Since this time can be freely changed by the personal computer manager, it cannot generally be considered to be a reliable time. Thus, when a signature is re-verified, it is impossible to distinguish whether it is an authentic signature created within the validity period or a forged signature created after the validity period. If revocation takes place, it is also impossible to distinguish whether it is a signature before or after revocation. In addition, since even revocation information is not issued after the validity period, it will be impossible to confirm even whether or not revocation takes place.

Therefore, since the validity of a digital signature is usually lost in about one to three years, it is impossible to retain healthcare records for five years, tax documents for seven years and other documents that must be retained for 30 years or longer while maintaining their authenticity.

Signature validity extension is a technology that overcomes the validity period and revocation of public key certificates and vulnerability of cryptographic technology used for digital signatures in order to maintain the long-term validity of digital signatures. The requirements[1] for signature validity extension are shown below (Fig. 2).

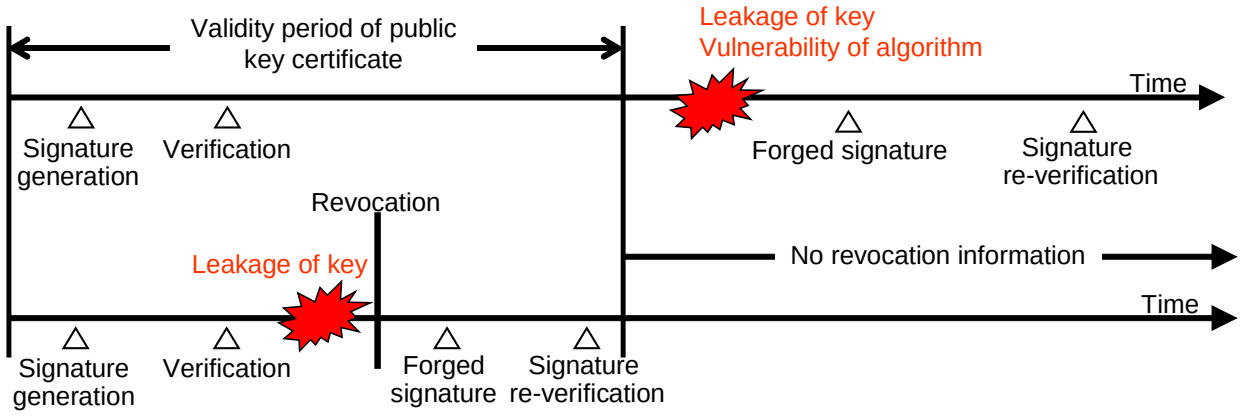


Fig. 1 Limit of digital signature

*Information Technology R&D Center **Mitsubishi Electric Information Systems Corporation

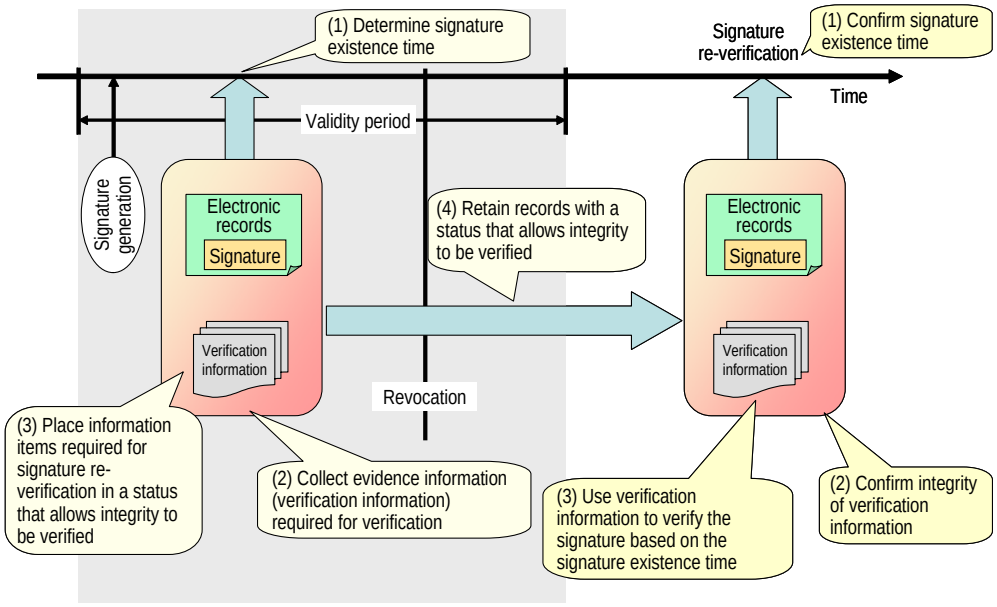


Fig. 2 Requirements for signature validity extension

Requirement (1): Determine digital signature existence time: Assign a reliable time to a digital signature to enable confirmation of the relationship between the digital signature and its validity period and revocation.

Requirement (2): Collect evidence information (verification information) required for verification of a digital signature: Collect revocation information items such as the sets of public key certificates from the signer to the route certification authority and CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol)[2] responses for those public key certificates.

Requirement (3): Place information items required for digital signature re-verification in a status that allows integrity to be verified: Place the original electronic records and verification information in a status that allows integrity to be verified.

Requirement (4): Retain records with a status that allows integrity to be verified as indicated in (3) above: Maintain the status in which integrity of records can be verified as indicated in (3) over the required retention period.

If requirements (1) to (4) are satisfied, then the following confirmation steps (1) to (3) can be used to distinguish whether the original signature is true or false:

Confirmation (1): Confirm the signature existence time.

Confirmation (2): Confirm that electronic records attached their signatures and verification information have not been tampered with.

Confirmation (3): Use verification information to perform verification based on the signature existence time.

3. Long-term Signature Format

One way of satisfying the requirements described in the previous chapter is to use the long-term signature format (Fig. 3). The long-term signature format is a global standard as RFC3126[3], etc. This method satisfies the requirements as follows:

Requirement (1): Assign a standard time stamp to a signature value (ES-T signature time-stamp).

Requirement (2): Store verification information items such as the set of public key certificates and CRL and OCSP responses (ES-C and ES-X verification information references and verification information).

Requirement (3): Assign a time stamp to electronic records with signature (ES), signature time stamp, verification information reference, and the entire verifi-

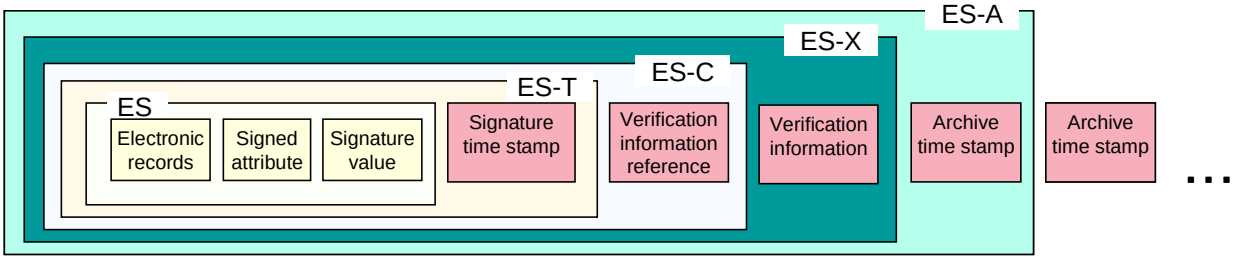


Fig. 3 Long-term signature format

cation information (ES-A archive time stamp).

Requirement (4): Overlap a time stamp on the entirety in order to maintain long-term tamper-resistance (outside archive time stamp).

The method that uses the long-term signature format with a time stamp to meet requirements (3) and (4) has the following features that make it superior to the method that assumes the safety of the system and operation to obtain the same effect (e.g., electronic original management system):

(1) Standard PKI technology allows anyone to verify the validity.
(2) Processing to construct and extend a long-term signature can be performed by anyone and can be taken over by others in the middle of processing.
(3) Trust is based on only the trust point in standard PKI without needing to consider the safety of the system and operation, which are currently difficult to confirm.
(4) Since time stamp services are always provided using the cryptographic technology whose safety has been confirmed at the relevant point of time, obsolescence of the technology is not a concern.

4. Signature Validity Extension System MistyGuard "EVERSIGN"

Constructing the long-term signature format requires that the signature time stamp, verification information including revocation information and archive time stamp be collected at their respective appropriate timings and be appropriately stored in the long-term signature format. Management of the timings is extremely complex, and so cannot be left to individual users.

When the constructed long-term signature is to be verified, it is also necessary to verify the original signature, signature time stamp, verification information, archive time stamp, etc. respectively after assuming the fixed time (e.g., time indicated by each time stamp) and to determine whether the signature is true or false after confirming the consistency between the time indicated by the time stamp and validity period and revocation information.

The Mitsubishi signature validity extension system MistyGuard "EVERSIGN" is a server-type system that automatically constructs the long-term signature format by only registering a document with signature according to a fixed protocol. Such operation is achieved by the EVERSIGN server that contains a scheduler to automatically execute processing based on the settings regarding various timings and where various data items on time stamp services, etc. are collected. The constructed long-term signature data can also be collected by the user according to the fixed protocol.

A report on the results of long-term signature verification can also be obtained by using the verification protocol to issue the request to the EVERSIGN server.

The EVERSIGN client library can be used to incorporate the exchange of requests and responses with the EVERSIGN server in various applications. Normally, the structure is such that the long-term retention function is expanded by interfacing with various document management systems and record management systems instead of using EVERSIGN on a standalone basis.

5. Long-term Signature Format Interoperability Test

From October to December 2005, the long-term signature format interoperability test was performed by ECOM[4]. This test aims to confirm the conformance to the "long-term signature profile" established by ECOM and the interoperability between products of companies. This profile was established to minimize the redundancy and ambiguity of the standard long-term signature format. By complying with this profile, it is possible to construct and verify a long-term signature with the objective of long-term retention.

A total of 13 companies participated in the test with their products or prototypes including the prototype from Mitsubishi Electric Information Technology R&D Center and the product EVERSIGN from Mitsubishi Electric Information Systems.

The following two types of tests were performed:

(1) Offline validation test: Conduct tests on the prepared sets of ES format data (ES-T, ES-X Long, ES-A), verification information and setting information to verify the validity using the actual products of the companies.
(2) Online matrix generation and validation test: Confirm whether long-term signature test data generated by the actual products of the companies can be read normally and verified correctly by the actual products of other companies.

The actual products of the companies including two Mitsubishi Electric-related actual products passed the test and were confirmed to comply with the long-term signature profile established by ECOM.

6. Application Example

EVERSIGN has been incorporated and used in the electronic record management system of a certain social infrastructure system company since May 2006. This system provides a retention management function for the workflow and electronic records and computerized documents to make electronic contracts between the company that has installed the system and the company that conducts transactions with it. EVERSIGN has functions for generating the long-term signature format, extending the validity and verifying the validity

of the electronically signed contracts and other transaction records between the companies conducting transactions from the document storage server at the heart of the system. To comply with the revised Electronic Ledger Preservation Law of the e-Document Law, this system uses the certificate of specified certification operation and the PFU time stamp service certified by the Nippon Information Communications Association. As of June 2006, which was immediately after operation started when the number of initial companies using the system was limited, the system was used about 3,000 times per month on the basis of registered documents. However, the number of companies using the system will increase in future and the scope of application of the system is expected to expand significantly.

From this fall, the system will also be used for a nationwide electronic contract document retention service provided by a financial institution. Both the number of companies using this system and the number of documents handled are expected to exceed those for the system that is currently in use. The system has the same basic configuration as that mentioned earlier, but will be provided as an ASP (Application Service Provider) service that can be used among multiple companies. The OCSP-based revocation verification system will be used as the mechanism of public key certificate verification.

7. Conclusion

In future, enforcement of J-SOX Law (Japanese SOX law: Financial Products Dealings Act of 2006) will raise the importance of securing the authenticity and adequacy of documents and records and their retention. Mitsubishi Electric technology and products are expected to make a significant contribution.

References

(1) Kazuya Miyazaki et al.: Mechanism and Practice of Electronic Record Retention, CHUOKEI-ZAI-SHA (2005)
(2) RFC2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP (1999)
(3) RFC3126: Electronic Signature Formats for Long-term Electronic Signatures (2001)
(4) Next-Generation Electronic Commerce Promotion Council of Japan: Long-term Signature Format Interoperability Test Report (2006)

Integrated Security Management Service

Authors: *Akira Tanaka** and *Fujii Seiji***

1. Introduction

This paper describes the managed security monitoring service that MIND has provided since 1998 and the integrated security management service that MIND started as a business in fiscal 2005. It then describes the information security forecast system that MIND and Mitsubishi Electric Information Technology R&D Center are jointly developing as an expansion of these services, with the aim of releasing the system in fiscal 2007.

2. MIND Managed Security Service

This service provides a total security package ranging from construction, operation, monitoring and support of the system to be monitored, to the collection and analysis of security information. This service is run from the Integrated Control Center where security expert engineers monitor security operations 24 hours/365 days a year. This service consists of professional operations, education and information provision, consulting, and construction, all of which constitute the life cycle of information security.

3. Integrated Security Management Service

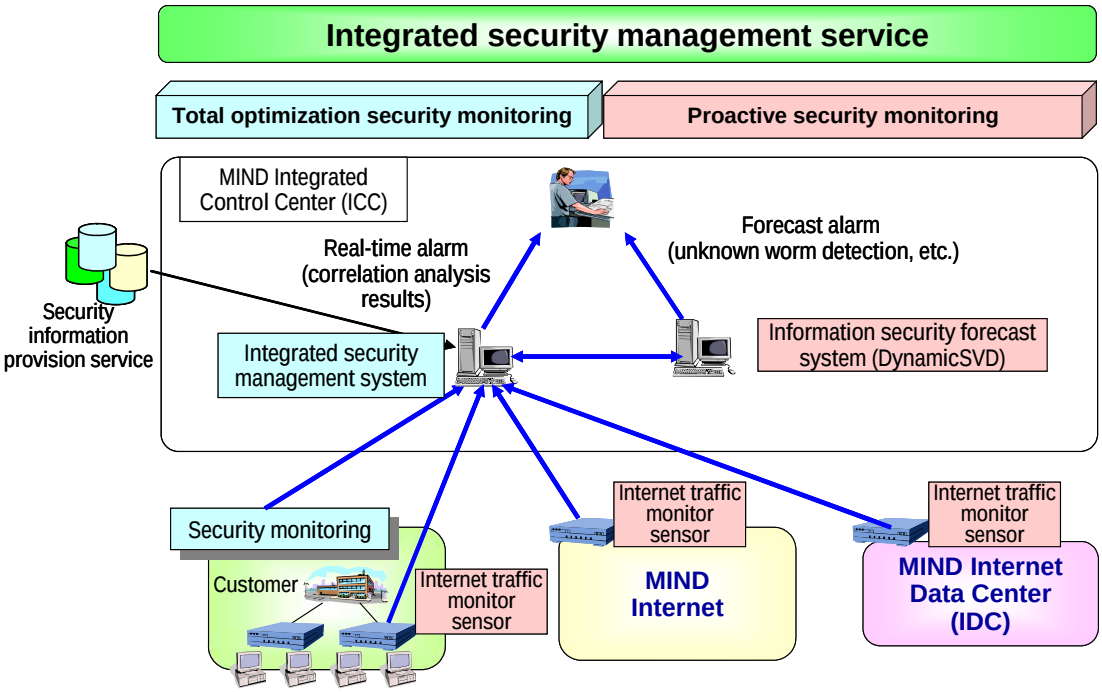
An overview of the integrated security management service is shown in Fig. 1. The integrated security management service was started as an improvement on the MIND managed security service. In this integrated service, a total optimization security monitoring service was started in fiscal 2005, and a proactive security monitoring service is now being developed, toward introduction in fiscal 2007.

3.1 Total optimization security monitoring

A typical company has many IT systems, and needs to maintain and improve the entire security management level. The integrated security management service was designed in response to increasing demands for monitoring system operations broadly throughout a company as well as conventional optimization of individual systems.

In order to achieve these services, individually managed security information items (Intrusion Detection System [IDS]/Intrusion Prevention System [IPS] alarm/log, firewall log, system security setting, vulnerability information and security diagnosis results, etc.) are gathered by the Security Information Management (SIM) system.

The correlation analysis function of SIM was used



ICC: Integrated Control Center
IDC: Internet Data Center

DynamicSVD: Dynamic Singular Value Decomposition

Fig. 1 Integrated security management service

*Mitsubishi Electric Information Network Corporation ** Information Technology R&D Center

to define the expertise of security expert engineers accumulated in past service operations as rules of this function, and then the gathered security information items are automatically monitored and analyzed based on the rules.

3.2 Proactive security monitoring

In this planned service, proactive monitoring provides added value by using the security log and system information gathered, to achieve total optimization.

Security measures such as firewalls offer immediate protection against unauthorized access and known worm-type virus attacks via the Internet. As shown in Fig. 2, however, if an unknown attack can be detected immediately it occurs, effective measures can be quickly taken to prevent the damage from spreading.

To achieve proactive monitoring of unknown attacks, an information security forecast system is being researched and developed.

4. Information Security Forecast System

The information security forecast system consists of the new algorithm DynamicSVD (Dynamic Singular Value Decomposition), a function for taking quick action based on the evaluation by the algorithm, and a function that interfaces with SIM.

4.1 Information security forecast function

The information security forecast function learns the normal network traffic status and detects abnormal traffic to help DynamicSVD ensure early detection of invalid traffic that occurs just prior to an unauthorized access. DynamicSVD has the following features:

(1) High-speed processing

The information security forecast algorithm DynamicSVD was developed based on the Incremental SVD that speeds up Singular Value Decomposition (SVD) developed by Mitsubishi Electric Research Laboratories, Inc. (MERL), which is Mitsubishi Electric's research and development center in the U.S. This algorithm enables real-time analysis of even time-series data such as network monitoring data.

(2) Improved detection accuracy

With SVD, continuous analysis of network monitoring data adversely affected the performance of attack detection. To prevent this deterioration of detection performance, data is analyzed while deleting unnecessary past network monitoring data.

(3) Verification result

In order to verify the validity of DynamicSVD that has the above features, the following network monitoring data items were analyzed using DynamicSVD to verify that an unknown attack can be detected:

(a) Lincoln Laboratory (U.S.) IDS evaluation data
(b) JPCERT/CC Internet traffic monitor data
(c) MIND Internet traffic monitor data

Figure 4 shows the result of analyzing MIND Internet traffic monitor data in (c). The analysis using DynamicSVD achieved detection in just one third of the time required by the threshold method.

4.2 Future development

Customers demand security monitoring that can promptly detect unknown attacks and respond quickly. This section describes the function that is being developed to achieve this.

(1) Early detection

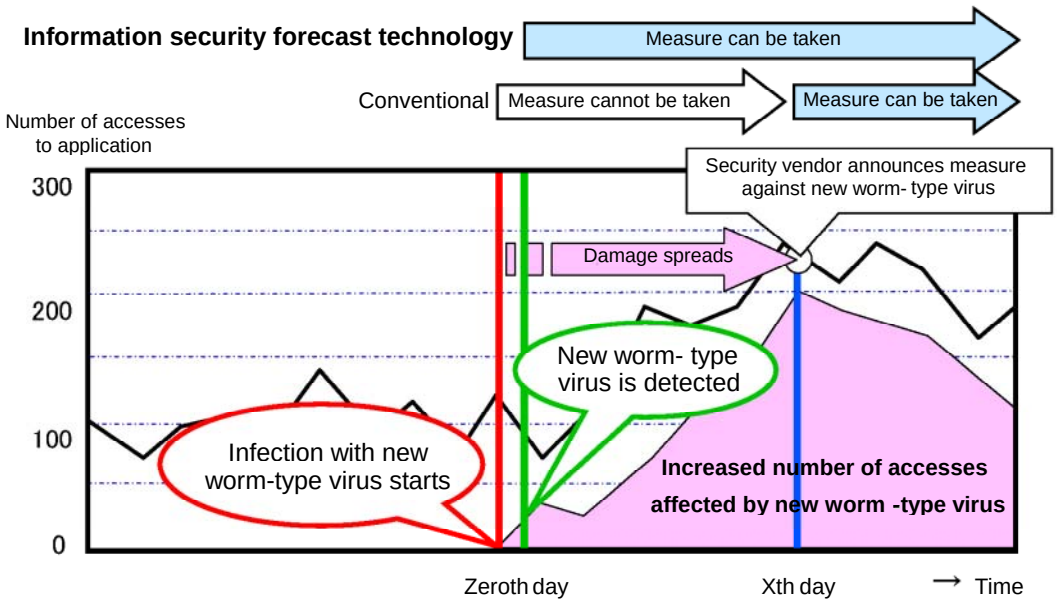
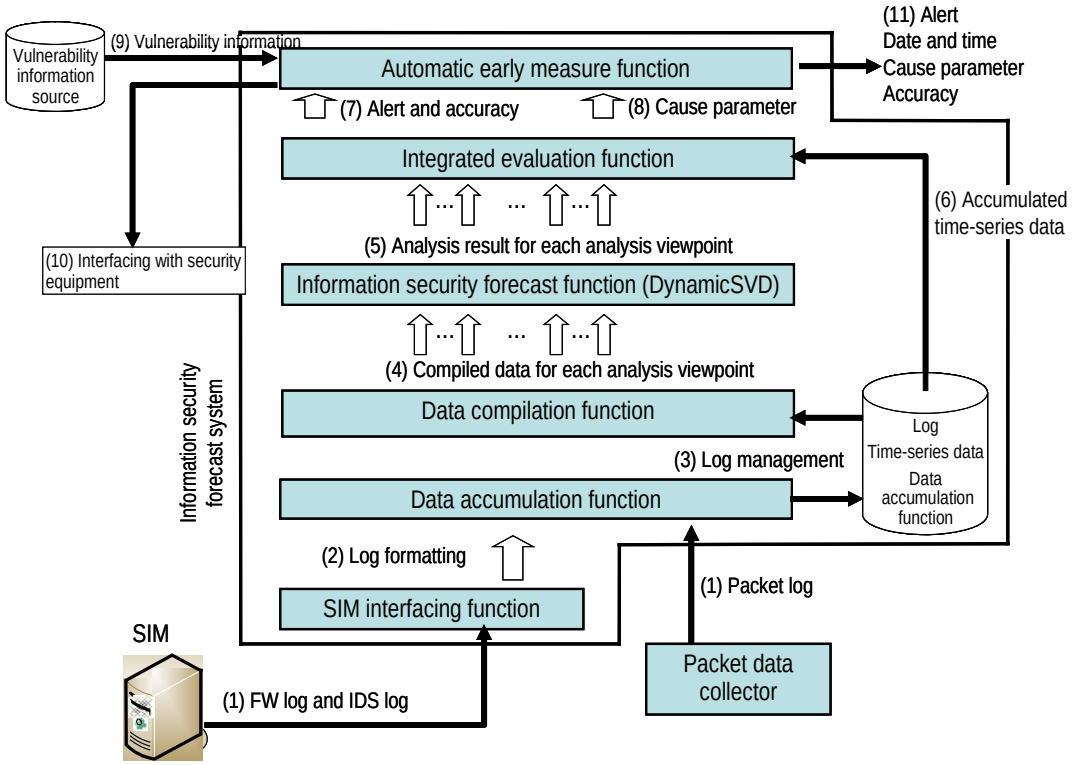


Fig. 2 Timing of unknown worm detection



SIM: Security Information Management
DynamicSVD: Dynamic Singular Value Decomposition
IDS: Intrusion Detection System
FW: Firewall

Fig. 3 Data flow diagram of information security forecast system

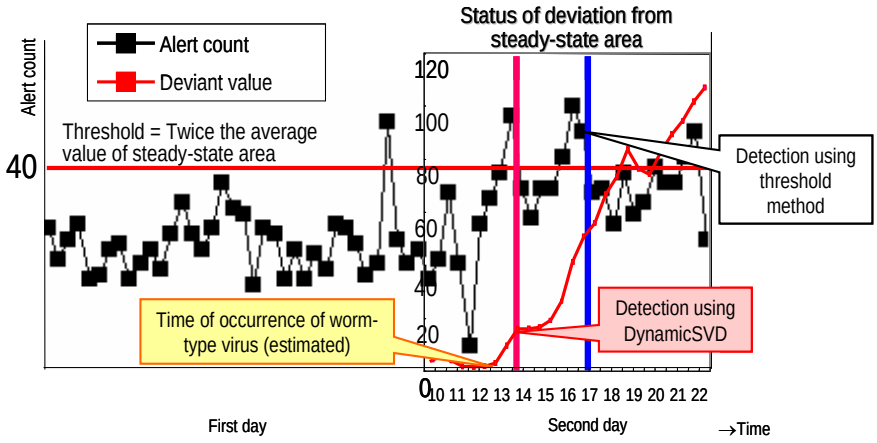


Fig. 4 Difference in detection time between methods for detecting unauthorized access

In order to use the information security forecast system for the integrated security management service, interfacing with SIM is required. We therefore developed the SIM interfacing function to collect a huge amount of SIM logs without hindering operation of the security monitoring system.

(2) Specified measure

In order to take action quickly, the cause of the abnormality and information on how to correct it are required. We are developing an automatic early measure function that uses the security equipment installed at the monitored target to take measures according to the information provided by the integrated evaluation function and publicly available vulnerability information.

References

(1) Hiroyuki Sakakibara et al.: Proposal of Unauthorized Access Analysis System Using Internet Traffic Monitor, the 68th National Convention of Information Processing Society of Japan 2006, 5E-3 (2006)

(2) Norio Hirai et al.: Proposal of Unauthorized Access Analysis System Using Internet Traffic Monitor – Analysis Technique for Network Log to Detect an Abnormality Caused by Worm Attack, the 68th National Convention of Information Processing Society of Japan 2006, 5E-4 (2006)
(3) Hiroyuki Sakakibara et al.: Unauthorized Access Analysis System Using Internet Traffic Monitor, the 38th Computer Security Group Research Seminar of Information Processing Society of Japan, 2007
(4) Kazuhiro Ono et al.: Evaluation Technique for Network Abnormality Detection Using Principal Component Analysis, Symposium on Cryptography and Information Security 2007, 1F2-1 (2007)


MITSUBISHI ELECTRIC CORPORATION