Security Solutions Provided by Fujitsu's Middleware Products

● Takahisa Hatakeyama ● Tatsuji Shimoe ● Yoshie Yamanaka
● Hideyuki Kageyama

(Manuscript received January 12, 2007)

In recent years, companies have increasingly been asked to take more social responsibility. From the standpoint of business continuity and complying with regulations, it has become more important to establish information security governance. This paper describes the solutions provided by the TRIOLE middleware products that conform to the Fujitsu enterprise security architecture (ESA) and efficiently improve system information security governance. Japanese companies will be obliged to comply with the Japan's new Financial Instruments and Exchange Law, which includes the Japanese equivalent of the US Sarbanes-Oxley Act, starting in 2008. The ESA-conforming TRIOLE middleware products will facilitate building of a secure system in compliance with laws and regulations, including the Japanese Sarbanes-Oxley act.

1. Introduction

In recent years, companies have increasingly been asked to take more social responsibility. Installation and replacement of IT systems has required judgment from a viewpoint of management. It has especially become important to ensure information security from the perspective of information security governance based on business continuity and compliance instead of accident response.

In Japan, the Act on the Protection of Personal Information went into effect in 2005, and the Japan's new Financial Instruments and Exchange Law, which includes the Japanese equivalent of the US Sarbanes-Oxley Act, will come into effect in 2008. Japanese companies are required to prepare for internal control and IT governance, and it has become important to establish information security governance as a mechanism to prevent and audit fraud.[1] This paper describes the technical architecture of the middleware products that support information security governance in accordance with Fujitsu's enterprise security architecture (ESA),[2] which was released in November 2006. It also describes the solutions provided by TRIOLE middleware products that efficiently improve information security governance.

2. Security architecture and concepts of TRIOLE middleware

Fujitsu's ESA is based on the analyzed and organized security requirements that are common to all companies. It focuses on information security governance and classifies the security functions commonly required for companies into the following four areas:

1) Identity management and authentication: Managing user IDs and passwords and confirming user authorization
2) Access control: Strictly managing access so appropriate users can use appropriate resources such as data and services.

3) Audit trail: Identifying the cause of a detected security breach and confirming that no fraud has occurred by collecting, maintaining, and managing the evidence (logs).
4) Centralized security administration: Centralizing security management to achieve consistency and uniformity throughout an entire organization.

When various ISV products conform to the ESA and Fujitsu's middleware products, the following two benefits can be obtained:

1) The system security functions commonly required for companies can be improved just by installing the ISV products.
2) When product vendors independently provide the security functions for the above four areas, there may be inconsistencies, which might, for example, cause a malfunction when products of different vendors are used together. ESA-conforming products, on the other hand, can be easily and safely linked because they have a common interface.

Fujitsu provides a security-enhanced suite of middleware products that conform to the ESA.

The following sections describe the solutions provided by these Fujitsu middleware products, which improve three areas of system security: identity management and authentication, access control, and audit trail.

3. Identity management and authentication

3.1 Authentication solution

To build an authentication system in the open environment, appropriate methods must be selected in consideration of several factors. These factors and related Fujitsu products are described below.

3.1.1 Authentication scopes and methods

1) Local authentication involving a PC only

Authentication can be done at the individual PC level by using, for example, fingerprint authentication, BIOS authentication with a security button, or Windows logon.

2) Network authentication

Access to or from the network is authenticated using a proxy, RADIUS, or 802.1X (EAP-TLS). To support network authentication, Fujitsu provides Interstage Security Director,[3] SafeAuthor, and IPCOM.[4]

3) Application authentication

The use of Web applications that are operated with a browser has recently increased, and many companies are now using a Web single sign-on (SSO) function for these applications. The Web SSO function makes all Web-based applications and services available with a single authentication, whereas without this function each job must be authenticated individually.

Fujitsu provides Interstage Application Server to support Web SSO.

It is necessary to set and operate authentication policies by combining 1), 2), and 3) above.

3.1.2 Authentication method security level

Basic authentication using an ID and password cannot completely prevent spoofing, so various authentication technologies are used to enhance the security level. Particularly important services should be operated using security policies based on a high-level authentication method. For example, Fujitsu internally implements and operates its public key infrastructure (PKI) system to achieve high-security operation. This system is integrated with a PKI by using a smart card to apply secure socket layer (SSL) V3 client authentication to Web SSO systems. Fujitsu provides local governments and companies in Japan with the following TRIOLE security solutions based on the Fujitsu PKI system and has achieved many excellent results with them:

1) Systemwalker PKI Manager (certificate authority product)
2) Web SSO function of Interstage Application Server
3) Safety Domain (software for smart cards)

Recently, case studies of advanced system integration have shown that Web SSO systems are being integrated with biometrics systems. For example, a financial institution has used palm vein authentication based on Fujitsu's PalmSecure integrated with a Web SSO system to build a new security system. In this system, simply holding a palm over the scanner displays the initial window of the application menu. As just described, integration know-how for combining various products to meet customer requirements is extremely important in providing authentication solutions. Therefore, authentication solutions have many variations.

Figure 1 shows an example application of the identification authentication solution.

3.2 Next-generation authentication protocols

In recent years, approaches based on the SOA and Web services that advanced from Web computing have attracted much attention. More and more companies have adopted these approaches, which have expanded the market. The following international standards are being developed for authentication and authorization of these SOA and Web services:

1) Security assertion markup language (SAML)

SAML[5] is a standard specification for exchanging security information using SOAP/XML defined by the standards body OASIS. The existing Web SSO function protocols have no mutual connectivity because they are vendor-specific. As a result, SAML has been used by more and more companies because of its mutual connectivity with the standardized credential for SSO and confirmation protocol for access control. Fujitsu will support SAML in the next few years.

2) Extensible access control markup language (XACML)

XACML[6] is a policy description language specification for controlling access to Web services. As with SAML, its standard specification is defined by OASIS.

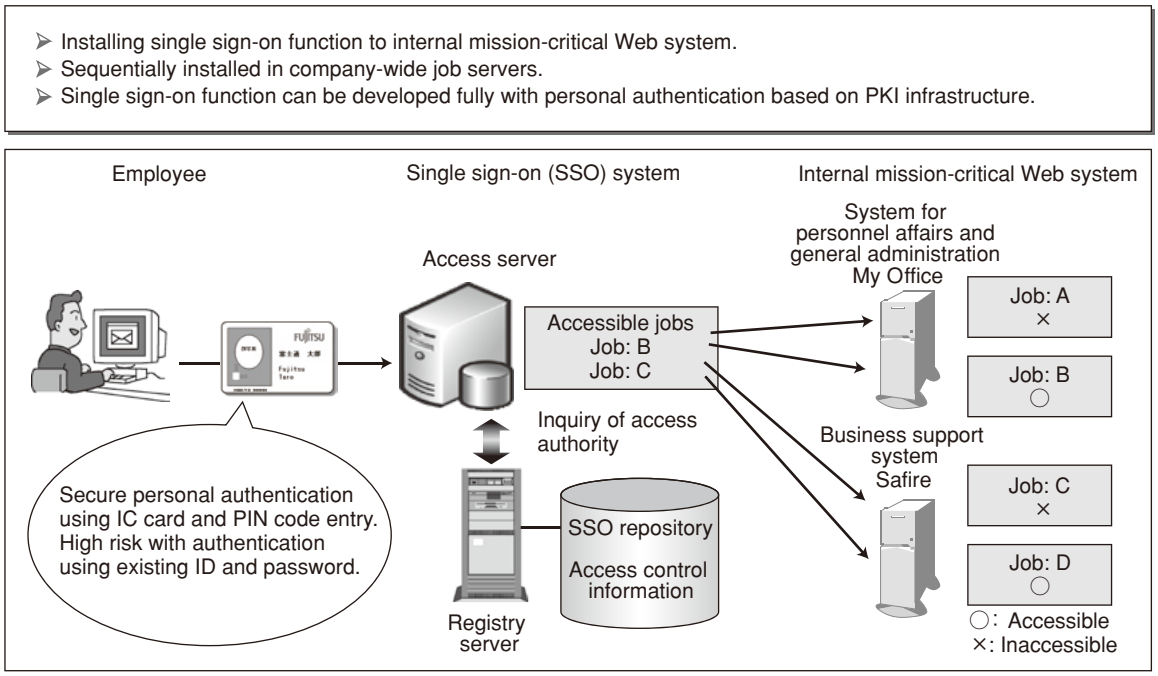

Figure 1
Example application of identification authentication solution using SSO to internal mission-critical system.

XACML can describe an access control policy by combining rules, policy statements, and policy set statements. Although various policy description languages have been considered so far, XACML is the overriding standard specification for the present circumstances. The authentication and authorization model is well known as the common architecture of the access control policy mechanism. **Figure 2** gives an outline of the relationships among the following components based on various authorization models such as the Internet Engineering Task Force (IETF) policy model:

- Policy administration point (PAP)

  Manages (generates, verifies, and distributes) the policy.
- Policy decision point (PDP)

  Determines the accessibility based on the policy.
- Policy information point (PIP)

  Provides user and resource IDs and attribute information required to determine the accessibility in PDP.
- Policy enforcement point (PEP)

  Controls the accessibility according to the accessibility determination in PDP.

It is expected that this authentication and authorization model will be adopted on a growing number of systems that support SOA and Web services, and Fujitsu will consider supporting the authentication and authorization systems that will be created as a result.

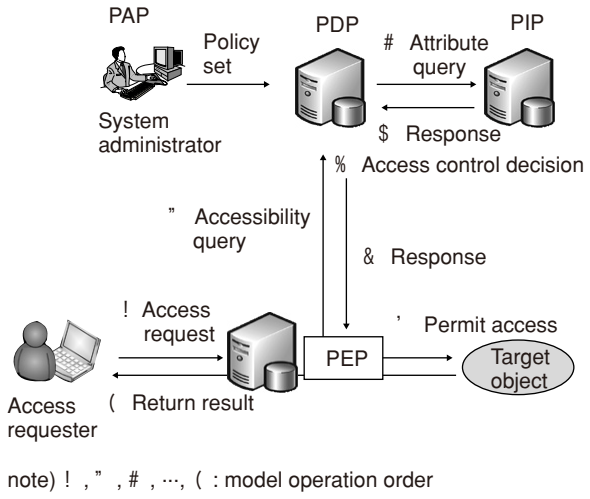

Figure 2
Authentication and authorization policy model.

3.3 Identity management

The term "identification" means recognition and specification of people, devices, and programs. Information used to identify users, applications, devices, and systems is called ID information.

The term "authentication" means a function or action to confirm that the users and components (e.g., devices and programs) are who and what have been envisioned by other parties such as information service providers. ID information is used for authentication.

Distributed environments and open systems have various ID information items. Authentication using ID information forms the core of security, and the importance of centralized management of ID information has been rediscovered in internal IT control. Identity management middleware is used to perform centralized management of ID information.

The typical problems with internal IT control are as follows:

1) Incomplete work separation
2) Inadequate access control for OSs, DBs, and application systems
3) Many users can execute privileged user processing.
4) ID information items of retired personnel and the access authorities for IDs are not deleted.
5) Access authorities for jobs are left unused and unattended.

Identity management systems are attracting attention as a means of solving these problems. Fujitsu has already provided identity management products as security control solutions, and these have been successfully used to build and integrate many systems. Fujitsu will further support these identity management

products, focusing on the standardization trend as appropriate.

4. Access control

Information systems are now important social infrastructures, and countermeasures against illegal access and disclosure of information handled on IT systems have become key issues.

For example, data managed by a server and data stored on a PC can be accessed from a system endpoint PC. Extracted data can easily be copied to the outside through portable media such as USB memories, CDs, DVDs, e-mail, or printed documents.

To ensure confidentiality and privacy, Fujitsu provides the Systemwalker Desktop series to prevent unauthorized disclosure of information from PCs.

The Systemwalker Desktop series consist of the seven products shown in **Figure 3**. They are based on the concept that the status of resources should be confirmed and the following security measures should be taken:

1) Security patch application
2) File encryption
3) PC operation restriction
4) Log collection and analysis
5) File operation restriction

In addition, the mission of the Systemwalker Desktop series is to prevent illegal data access from PCs from the standpoints of internal control and IT governance. To fulfill this mission, the Systemwalker Desktop series support access control functions to stop the following illegal accesses from unauthorized PCs:

1) Illegal network access
2) Illegal PC access
3) Illegal file access

4.1 Access control functions provided by Systemwalker Desktop series

The following three Systemwalker Desktop series products provide access control functions:

1) Systemwalker Desktop Keeper

Performs PC operation restriction in accordance with the PC user authority

2) Systemwalker Desktop Rights Master

Performs data access control for secure use of data managed using a file server

3) Systemwalker Desktop Inspection

Performs network access authority control according to the PC security level (quarantine network system)

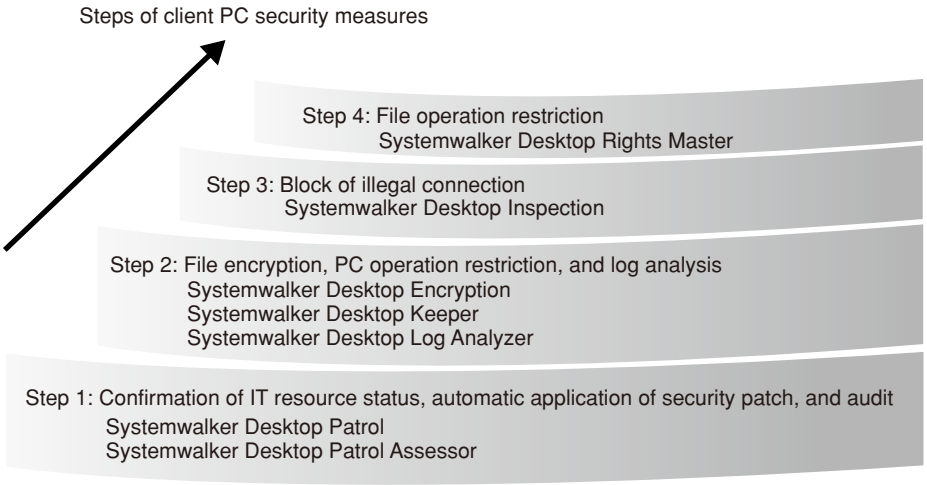

Figure 3
Steps of client PC security measures.

The access control technologies provided by the Systemwalker Desktop series[7] are described below.

4.2 PC operation restriction: Systemwalker Desktop Keeper

With the recent improvement of the IT environment, highly-portable notebook PCs and external media such as USB memories, CDs, and DVDs that enable data to be easily copied from desktop PCs have become widespread, and this has heightened the risk of unauthorized information disclosure.

Systemwalker Desktop Keeper has further enhanced OS-level access controls to control the following operations made on data-handling PCs:

1) Starting specified applications
2) Starting specific services and processes
3) Logon. For example, inhibiting logon by users that belong to specific groups
4) Copying windows using the PrintScreen key
5) Writing data to specified drive units
6) Printing data from specified applications
7) Attaching files in e-mails

Systemwalker Desktop Keeper links with the authentication server (Microsoft Active Directory) to apply the above operation restrictions for each terminal or user according to the user's position, work type, job, and other details. Because authorities are set and managed for each user or group to be authorized, PC operations according to a policy can be controlled for each department, job, or person.

Systemwalker Desktop Keeper also collects PC operation logs, and making this known to users can deter them from illegally accessing PCs.

4.3 Data access control: Systemwalker Desktop Rights Master

Systemwalker Desktop Rights Master (DTRM) provides the following solutions for confidential documents:

1) Secure protection with encryption (AES-128)
2) Recording of access controls and audit trails for each user operation, for example, browsing and file printing
3) Controlling time-limits of accesses to target files

These functions can stop disclosure of data to third parties and inhibit operations from unauthorized users unless connections are made to the license distribution server of DTRM on the intranet. These functions have securely protected confidential documents.

DTRM uses the Fujitsu-developed universal distributed access control (UDAC)[8] technology as a digital rights management (DRM) mechanism to control access to individual files.

The UDAC technical proposals and information distribution services that use this technology have been promoted in a UDAC consortium that consists of IT companies and content-business companies. This consortium has publicized the PKI-based key exchange and other specifications.

DTRM uses the UDAC technology to independently handle the license information about the encrypted files and their access information. Therefore, it allows protected files to be freely copied and distributed between PCs under DTRM and also allows operations under permission conditions that are based on license information (e.g., access count and period).

Moreover, encrypting documents using AES-128 and communication protocols for each license acquisition can localize a security problem such as hacking of protected files. The confidential document protection function can prevent damage caused by hacking from spreading throughout the entire system.

4.4 Quarantine network system: Systemwalker Desktop Inspection

Traditionally, measures against illegal access, hacking, and other vulnerabilities include a firewall for protection against attacks from outside, an intrusion detection system (IDS), and antivirus software. Recently, technologies for

protecting against illegal access to a corporate network from unauthorized PCs and from authorized PCs that have no security measures are attracting attention. As PCs become an integral part of everyday life, it is becoming increasingly common for people to take business-use PCs outside, for example, on business trips, and also connect private PCs to corporate networks without permission. The information disclosures and virus infections caused by these practices have not been negligible, and these technologies have been promoted to mitigate these risks.

To stop illegal connections, the validity of the PC user and the PC should be confirmed (authentication). It should also be confirmed that the security patches of PCs and the definition file of their antivirus software are up to date (security measures check). If any impropriety or deficiency is detected, the connection should not be permitted. While it is not so difficult to take these actions for PCs that have a fixed connection to a corporate network to be managed, they are not so easy to take for mobile PCs that are taken outside. There are two main reasons for this. First, the existing technologies require preliminary software installation, registration, and setup for monitoring and cannot take appropriate action for mobile PCs. The other reason is that the existing technologies have no mechanism for forcibly blocking access from deficient PCs.

To help solve these problems, Fujitsu provides a quarantine network system that monitors PC networks to block and isolate illegal PC communications. This system combines a dynamic virtual LAN (VLAN) based on IEEE802.1X authentication, authentication with a network equipment dynamic access list, and an access control mechanism. The system controls the network connections of PCs according to the check results for the PCs' security measures.

In the Fujitsu quarantine network system, Systemwalker Desktop Inspection, which is the management server, links with the network server IPCOM L series and secure switch SR-S series. The IPCOM L series can control the network by using the dynamic access control list. The SR-S series supports a dynamic VLAN function based on IEEE802.1X authentication (**Figure 4**).

The quarantine network system checks the user authentication and MAC address authentication and also checks whether the security policies are satisfied when connecting to a client PC. The security policies include policies about the security patch application status, the update status of the antivirus software definition file, and the installation status of optional software. The system then determines whether the PC can be connected to the corporate network. The job servers that can be connected to the corporate network can be limited for each user. Unless the security policies are satisfied, connection permission can be limited to the update server instead of merely rejecting a connection request. The quarantine network system can automatically apply a required security patch and virus pattern for a PC whose connection has been rejected by linking with Systemwalker Desktop Patrol for the update server. Systemwalker Desktop Patrol provides an automatic application function for security patches and virus patterns. As just mentioned, the quarantine network system enables autonomous maintenance of the corporate network security level.

5. Audit trail

The increase in illegal accesses to information systems and the resultant information disclosures are worldwide problems. According to data released by the Department of Justice (DOJ), an estimated 3.6 million households (about 3% of all U.S. households) experienced some sort of personal information theft in the first half of 2004. The total amount of damages was anticipated to reach 3.2 billion dollars. The number of damages concerning personal information continued to rise throughout 2004 and subsequent years. Under these circumstances, it is the social

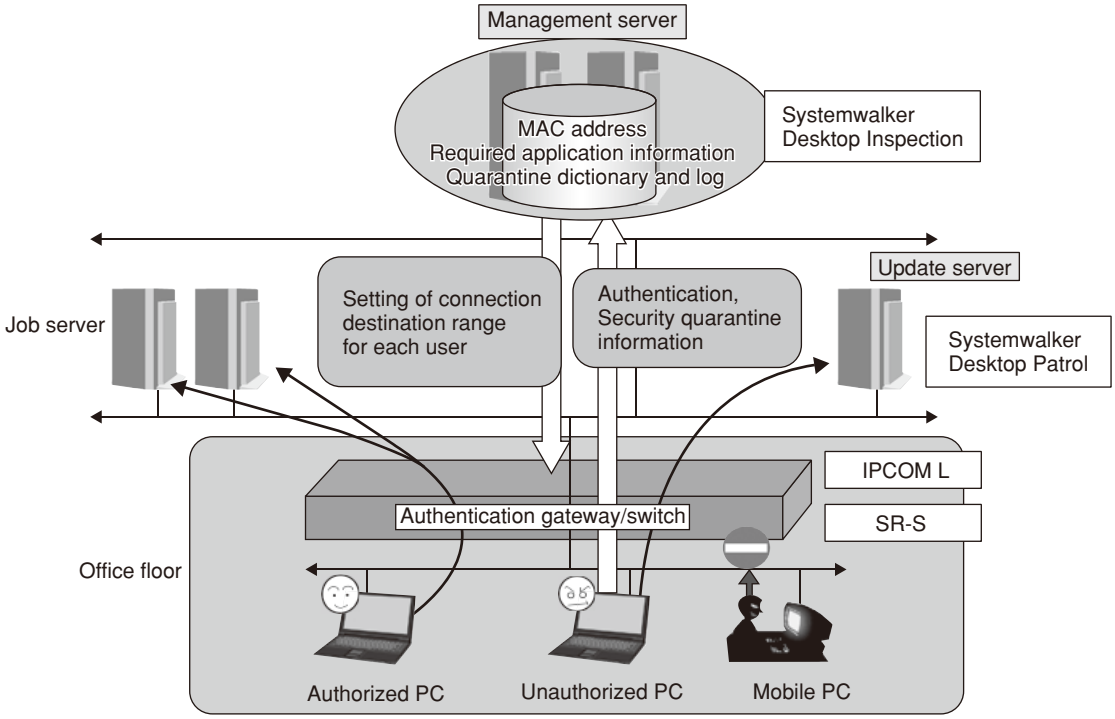

Figure 4
Quarantine network system.

and moral responsibility of individual companies to take adequate security measures.

Because problems such as illegal access cannot be prevented completely, early problem detection and handling are necessary. To do so, the detailed operation status of information systems should be recorded, managed, and analyzed as an audit trail (audit log). Then, based on this trail, appropriate measures should be established and taken.

Fujitsu provides audit log management and analysis solutions that use Systemwalker Centric Manager as the core component. These solutions are based on the trail management architecture, which is one of Fujitsu's ESAs.

This section describes the considerations and solutions in the following audit log management and analysis phases:

- Log collection and management
- Log audit and analysis

5.1 Log collection and management

The logs to be collected are generally determined according to the information system security policies. Many different logs, ranging from OS logs to middleware and application logs, should be collected. The audit log management function of Systemwalker Centric Manager supports the collection of logs in a variety of output formats, including the following:

1) OS log (e.g., syslog, loginlog, sulog for UNIX, event log for Windows)
2) Access log of the Web server (Interstage Application Server, Apache, and IIS)
3) Operation and activation logs of Systemwalker Centric Manager
4) Client operation log of Systemwalker Desktop Keeper
5) Audit log of the database server (Symfoware)
6) Access log of the storage unit (ETERNUS NR1000 series[9])
7) Logs of the form processing software products (Interstage List Works, Interstage

List Creator, and Interstage List Manager)

Managing logs distributed to servers on a server or application basis is very costly, and the collected audit logs can contain gigabytes or even terabytes of data. Therefore, a mechanism that can safely and securely manage large audit logs over the long term is required.

To achieve this mechanism, the audit log management function of Systemwalker Centric Manager[10] collects audit logs on the job servers and sends them to the IT operation management server for centralized management. In addition, this function periodically stores the audit logs into storage units such as ETERNUS for longterm storage (**Figure 5**).

Systemwalker Centric Manager also provides the following functions required to manage the audit logs:

1) Automatic log collection
2) Encrypted communication at collection to ensure secure and reliable log collection
3) To reduce the network load, collection of only logs that have been added. Also, a split transfer function
4) Identification of the collected audit log (e.g., by date, server, and application unit)

5.2 Log audit and analysis

It is important to analyze logs on a routine basis. Aggregating the processing contents for each date, day of the week, and time of day and also analyzing trends makes it easier to detect unusual events that may be signs of failures. Periodic analysis allows the users to audit the information system status.

The audit log analysis function provided by Systemwalker uses the aggregation and search engine of Interstage Navigator[11] to enable batch searching and aggregation for multiple logs under complicated conditions (**Figure 6**).

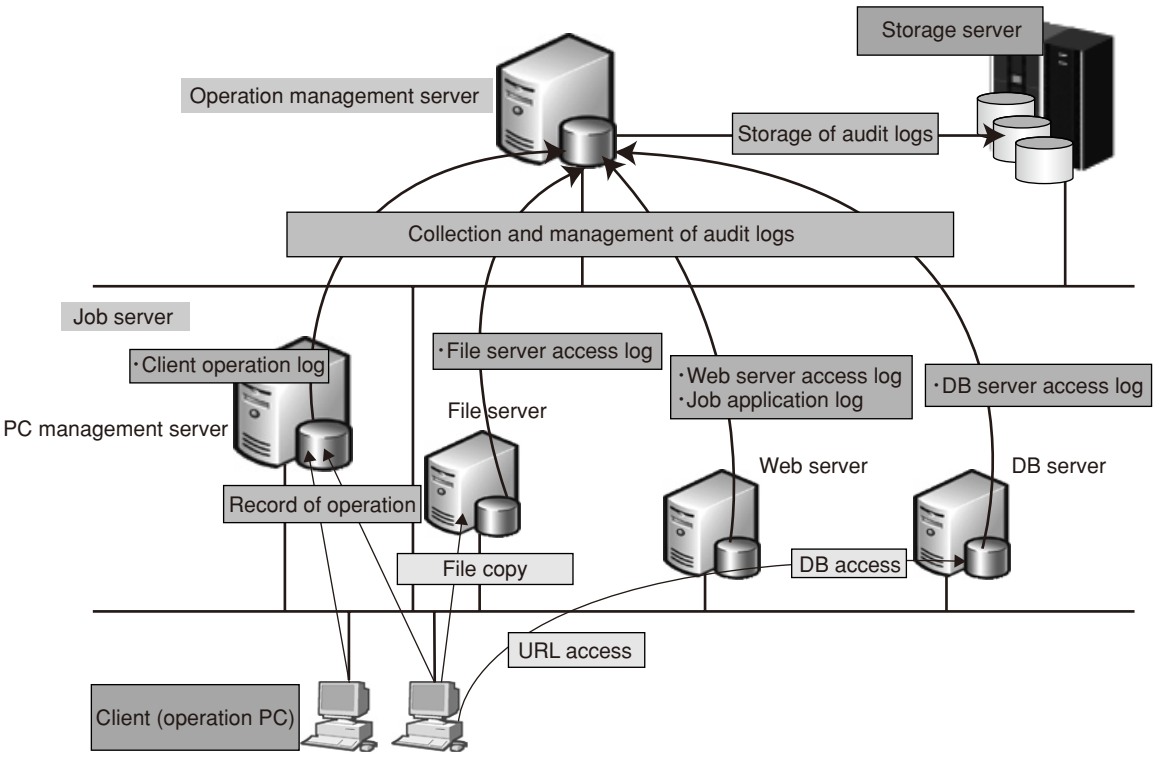

Figure 5
Collection and storage of audit logs from entire system.

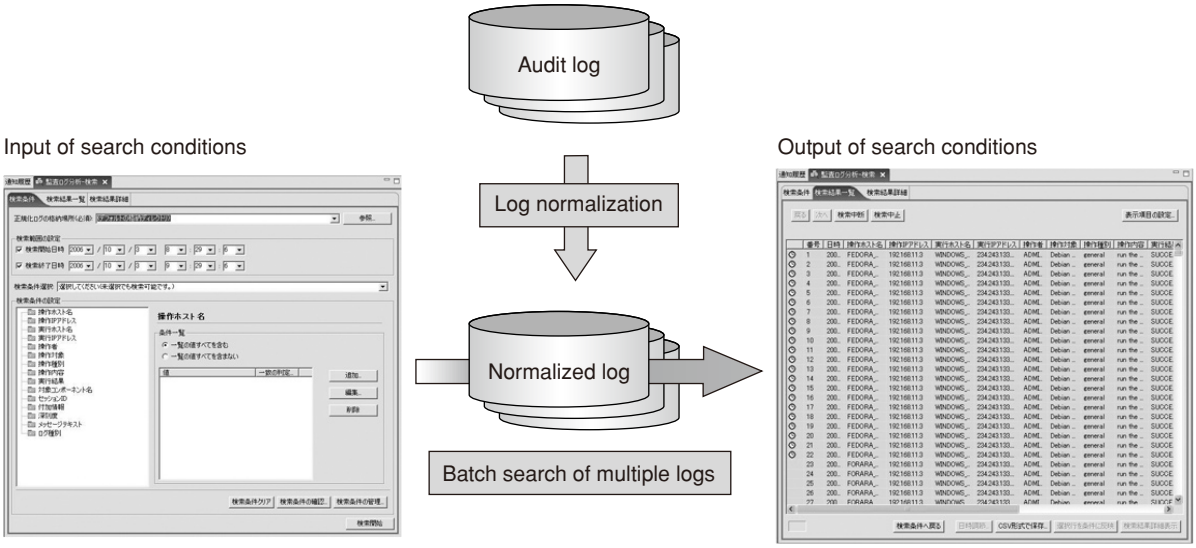

Figure 6
Log normalization and search.

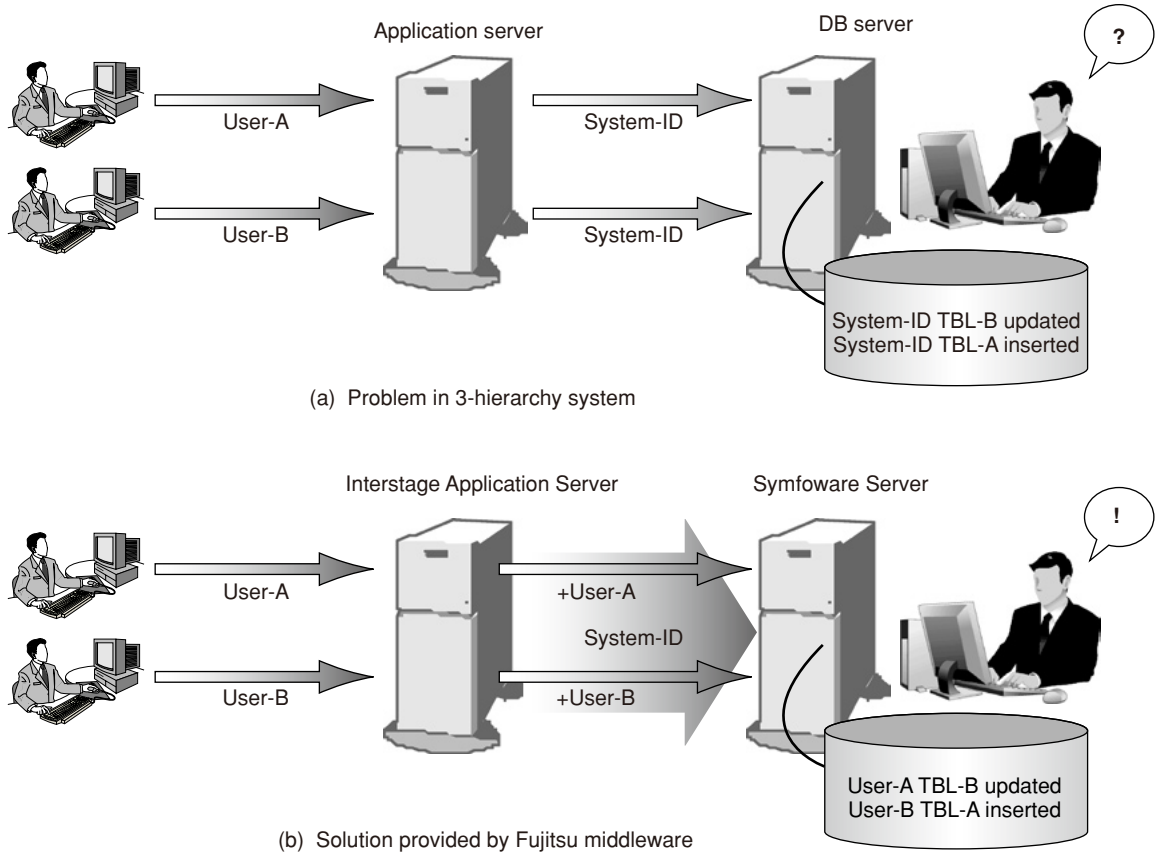

Figure 7
Problem and solution in 3-hierarchy system.

The basic requirements for the audit log analysis function are that it:

1) Normalizes logs and absorbs the differences in output formats between logs to enable batch searches and aggregation of multiple logs.
2) Provides standard templates for search conditions. The templates must be customizable as necessary.
3) Provides standard templates for aggregation reports. The templates must be customizable as necessary.

The user ID and IP address are the common search keys for associating multiple logs in which a series of processes are recorded and then analyzing them. In fact, log association may be difficult.

In general 3-hierarchical Web systems, the application server accesses the DB server using the application server-specific ID instead of the user ID. This is done to improve performance, for example, by reducing the number of logins to the DB system. Accordingly, the audit log output by the DB server has no information to identify the user [**Figure 7 (a)**].

To solve this problem, it is necessary to make a link between the application server and DB server in order to transfer the user ID. In the Fujitsu middleware solution, the application server Interstage Application Server[11] links with the DB server Symfoware[12] to transfer the user ID. This system enables the user ID to be stored correctly in the DB server audit log so the associated logs can be analyzed [**Figure 7 (b)**].

5.3 Summary of audit trail

The Fujitsu middleware solution focusing on Systemwalker Centric Manager has an audit trail architecture. As mentioned above, this solution enables safe and secure audit trail management and analysis, which can improve the efficiency of the PDCA cycle of information system security management.

Fujitsu will further enhance the functions of this solution to provide various audit log management and analysis solutions.

6. Conclusion

This paper described Fujitsu's middleware solutions for ESA security areas. Installing Fujitsu's ESA-conforming products facilitates linkages between products and enhances information security governance of an entire system.

Fujitsu will continue to provide ESA-conforming products to improve information security governance.

References

1) T. Hatakeyama et al.: Infrastructure for Security Compliance Management System. (in Japanese), *FUJITSU*, **57**, 2, p.115-121 (2006).
2) T. Shiozaki, M. Okuhara, and N. Yoshikawa: Fujitsu Enterprise Security Architecture. *FUJITSU Sci. Tech. J.*, **43**, 2, p.153-158 (2007). *http://www.fujitsu.com/downloads/MAG/vol43-2/paper01.pdf*
3) Fujitsu: Interstage Security Director. *http://www.fujitsu.com/global/services/software/interstage/products/sdirector/Features.html*
4) Fujitsu: IPCOM S Series Functions Overview. *http://www.fujitsu.com/downloads/SG/fapl/ipcom/ipcoms_functions.pdf*
5) SAML2.0 Assertions and Protocols. *http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf*
6) XACML2.0 Specification Document. *http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf*
7) Fujitsu: Systemwalker Desktop Series. (in Japanese). *http://systemwalker.fujitsu.com/jp/solution/solution_31.html*
8) UDAC Consortium. *http://www.udac-consortium.org/index_e.html*
9) Fujitsu: ETERNUS. *http://www.fujitsu.com/global/services/computing/storage/*
10) Fujitsu: Systemwalker. *http://www.fujitsu.com/global/services/software/systemwalker/*
11) Fujitsu: Interstage. *http://www.fujitsu.com/global/services/software/interstage/*
12) Fujitsu: Symfoware. *http://www.fujitsu.com/global/services/software/symfoware/*

Takahisa Hatakeyama, *Fujitsu Ltd.*
Mr. Hatakeyama received the B.S. and M.S. degrees in Marine System Engineering from the University of Osaka Prefecture, Sakai, Japan in 1986 and 1988, respectively. He joined Fujitsu Ltd., Kawasaki, Japan in 1988, where he has been engaged in research and planning of network and security software.

Tatsuji Shimoe, *Fujitsu Ltd.*
Mr. Shimoe received the B.S. degree in Chemistry from Sophia University, Tokyo, Japan in 1980. He joined Fujitsu Ltd. Japan in 1981, where he has been engaged in research and development of distributed computing and security-related systems. He qualified as a CISSP in 2006.

Yoshie Yamanaka, *Fujitsu Ltd.*
Ms. Yamanaka received the B.S. degree in Physics from Toho University, Chiba, Japan in 1988. She joined Fujitsu Ltd. in 1988, where she was engaged in research and development of computer graphic systems. Since 2000, she has been engaged in research and development of security solutions. She is also developing client security systems.

Hideyuki Kageyama, *Fujitsu Ltd.*
Mr. Kageyama received the B.E. degree in Civil Engineering from Meijo University, Nagoya, Japan in 1988. He joined Fujitsu Aichi Engineering Ltd. in 1988. Then, he moved to Fujitsu Ltd., Nagoya, Japan in 2005, where he has been engaged in development of enterprise management software. He received the Telecommunication Management Research Award of the IEICE in 2002.