Integrated ID Management in the Age of Internal Governance

TANAKA Nobuyoshi, KUWATA Masahiko

Abstract

Enterprises have previously managed user information separately for each information system. As a result, they are currently encountering the need to integrate their ID information on the basis of strict management of access to information systems and confidential information. This policy is required in order to solve the problems inherited from the previous management systems, as well as to enhance the internal governance that is required by both the social circumstances and the legal regulations. Based on experiences in the introduction of a variety of integrated ID management systems both inside and outside of NEC, we are ready to contribute to the efficient preparation of corporate integrated ID management systems with our consultation services and utilities such as SECUREMASTER. With the future in mind, NEC is planning to provide a whole range of integrated ID management infrastructures that can help enterprises create added value by mutually combining existing values of their own and achieve integrated services that feature a large variety of combinations.

Keywords

internal governance, integrated ID (identity) management, ID information provisioning, personal identity authentication, single sign-on, access management, access control, access log, computer forensics

1. Introduction

Enterprises have been implementing various jobs into information systems one after another aiming at improving job efficiency and making a more efficient use of information. However, as the information systems were built and introduced individually from other systems, the methods of managing user information have become variable between systems and enterprises now encounter many problems, including the following:

1) The maintenance of user information should be performed individually and repeatedly for every one of the large number of systems.

2) The ID and password of a user differs depending on the system in use and the user often forgets or loses them. ID and password management is often faulty in this regard.

To solve the above problems, it is necessary to integrate the management of user information as a common infrastructure for all of the systems.

On the other hand, social considerations have been forcing enterprises to enhance their internal governance by preventing information leakage, applying thorough compliance and by properly handling the increasing number of dispatched and limited-term employees. In the enhancement of internal governance for the more secure use of information systems, it is important to eliminate unauthorized use and manage access to the information systems and confidential corporate information more strictly. The basis for strict personal identity authentication and access management of users is the management of the identity (ID) that represents the authority of each user.

Moreover, with regard to the legal regulations, the Japanese SOX law will be enforced for the fiscal year starting on April 1, 2008. This law has been established by adding prescriptions on the governance of IT based on the SOX Act in the U.S.A. When this law was applied to auditing in the U.S. inadequacies in ID and access management were discovered in many enterprises. These were later forced to commit significant funding in order to thoroughly improve their businesses. To avoid similar problems from being repeated in auditing based on the Japanese SOX Law, it is important to arrange the foundations for ID and access management at the beginning.

2. Integrated ID Management as the Foundation of Internal Governance

In order to implement strict personal identity authentication and ID management for the enhancement of internal governance, an enterprise must solve the following problems that may have been passed on from previous ID management systems.

1) A specific user cannot be identified because a shared ID is used.

2) The users are managed per system so every user has more than one ID and password for use in different information systems. As a result, many users are unable to remember their IDs and passwords and often paste a memo on the

terminals or use passwords that are easy to remember (and easier to be guessed by third parties).

3) The user attribute information (information determining authorizations such as for organizations, posts, employment categories) is managed per system so that the attribute information of a single user is not consistent between systems (this may for example occur when the attribute information of the user is not updated in a system after personnel changes). If the authorization for users to use systems is set incorrectly, the chances of unauthorized use will increase.

4) The IDs of retired employees cannot be invalidated immediately.

To solve these problems, it is necessary to apply integrated management of the user ID information (including authentication information such as the ID and password and the attribute information) that has been managed independently for each system as shown in **Fig. 1**. This is to ensure that user authentication is always executed using a personal ID that is managed integrally, regardless of the system used. In addition, it is also necessary to manage the ID information strictly throughout the lifecycle from generation to deletion and to minimize the attribution of authorizations to individuals throughout this period. This is because expanding the number of authorizations above the required levels increases the risk of abuse and operational mistakes.

These procedures are realized by applying an integrated ID management system. To receive auditing by proving the optimum use of confidential corporate information, an integrated ID management system should be introduced thus; 1) manage all of the individual users strictly without exception; 2) apply strict personal identity verification based on personal IDs; 3) apply control for permitting access only to the minimum required information/systems, and; 4) record and analyze who accessed which part of what information/system and when was it done.

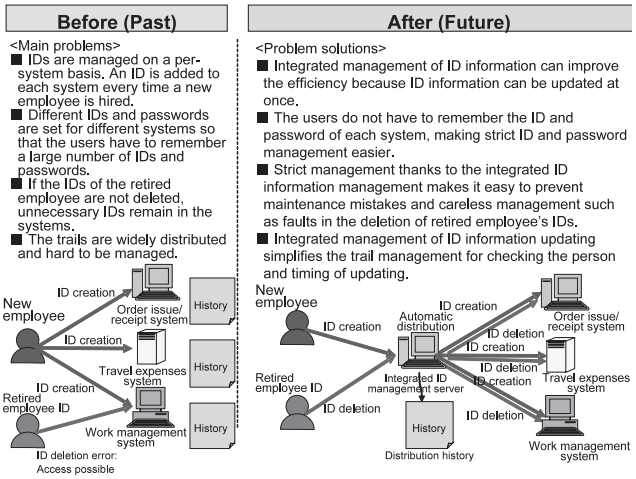


Fig. 1 Solution of problems by the introduction of integrated ID management.

3. Requirements for the Effective Introduction of an Integrated ID Management System

An effectively integrated ID management system meets the following requirements.

a) Database and data referencing/updating GUI that can facilitate integrated management of the ID information of individual users.

b) Registration, modification, deletion, suspension and restoration of IDs and system usage authorizations following the lifecycles of users from employment (ID generation) to retirement (ID deletion).

c) Improvements in the efficiency of workflow processing for applications and approvals of the ID and system usage authorizations for each user.

d) Provision of ID information of individual users to the systems (i.e. the management of the ID information of the users of different systems are centralized into an integrated ID management system, which sends the ID information to systems for ensuring synchronization between them).

e) Single sign-on (SSO) to the systems and access control according to the usage authorizations.

f) Recording, collection, referencing, inquiry, analysis and auditing of access logs.

The introduction of an integrated ID management system that meets the above requirements will bring about the following effects.

1) Integration of maintenance procedures for the same ID information that has hitherto been required to be repeated for each system will enable a reduction in management costs. The prevention of maintenance mistakes and careless management procedures can also improve the accuracy of ID information.

2) Every user needs remember only one pair of ID and password and will keep it secret more strictly.

3) The infrastructures facilitating the management of common personal IDs for systems and access management can reduce the development costs of integrating the ID information.

4) Registrations of users and user authorities can be verified and approved whthout omission by the person in charge of management, so strict management is possible.

5) The range of system usage by each user can be restricted with less difficulty in the minimum required range approved by the person in charge of management.

6) The system usage trails of individual users can be accurately recorded, so that auditing can be performed easily.

4. Integrated ID Management Solutions Provided by NEC

At NEC, we have been introducing and enhancing an integrated ID management system for our 150,000 group employees since 2000 and ahead of our competitors. We have also achieved the introduction of integrated ID management systems for more than 50 of our customers. This rich experience is the source of expertise that NEC provides for the customers.

Our expert staff in the field of integrated ID management offers total support for system introduction by matching the environment of each customer. This is achieved from the consulting, planning and system proposal stages to those of requirements definitions, design, construction and operations.

In the following sections, we will introduce some of the integrated ID management solutions of NEC by focusing on the linkages between consultation, products and the physical (entrance/exit) security that is one of the typical characteristics of NEC solutions.

4.1 Consulting

The key to the successful introduction of an integrated ID management system lies in the depth of study in the upstream process; including planning, requirements definitions and basic design.

When we first introduced integrated ID management inside NEC, we repeated trials and errors and often encountered difficult issues. Subsequently, when we reviewed this experience, we identified that the main cause of these issues was an insufficiency in the study of the upstream process. In other words, we discovered that careful requirements definitions and basic design make it possible to avoid backtrackings for system reviews. When integrating ID management, it is essential to fully analyze existing system environments and to connect the results to the requirements definitions and basic design. This is a field in which rich experience is the key.

The important study subjects for the upstream process of systems introductions are as follows.

For the requirements definitions:

1) Definition of the positioning and role of the integrated ID management system.
2) Determination of the data items subject to management as the ID information.
3) Clarification of the purpose of data usage and statement of applications used (job systems).
4) Approval authority and application/approval flow.

For the basic design:

5) Standardization of common code systems, including; personal IDs, organization code, post code, etc.
6) Data source determination and design of data updating operations for maintaining data accuracy.
7) Linkage with the personnel department.
8) Linkages with applications (job systems)
9) Security maintenance.

We advance efficient research programs for the solution of these issues in accordance with customer characteristics.

4.2 Integrated ID Management Products

NEC provides SECUREMASTER, an integrated ID management product, which features total coverage of the issues that customers might encounter when implementing an integrated ID management.

While many similar products are available from outside Japan, SECUREMASTER is a Japanese integrated ID management product that can manage jobs that are specific to Japanese enterprises and organization structures that feature deep hierarchical levels. We have also prepared substantial technical support teams in Japan to offer timely, flexible responses to the relevant issues.

The composition of SECUREMASTER is as described below. The configuration of the product is as shown in **Fig. 2**.

The SECUREMASTER meets the requirements of an integrated ID management system that are enumerated in Section 3 of this paper. The relationships are as shown in Fig. 2.

(1) Enterprise Identity Manager

This is the ID information management/provisioning product providing functions as summarized in **Fig. 3**.

(2) Enterprise Directory Server

This is the LDAP (Lightweight Directory Access Protocol)* directory server product that provides functions as

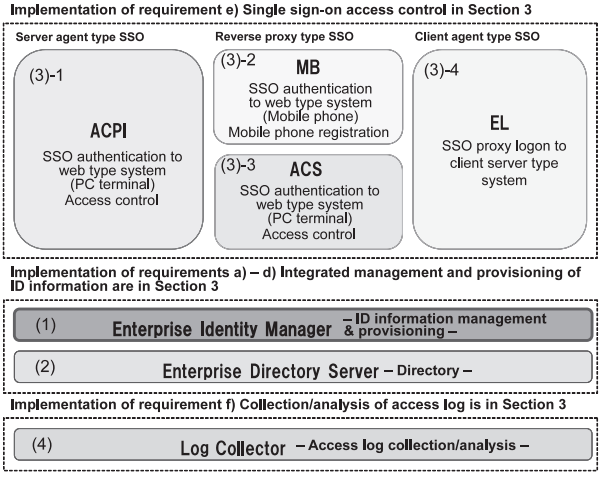


Fig. 2 Configuration of the integrated ID management product, SECUREMASTER.

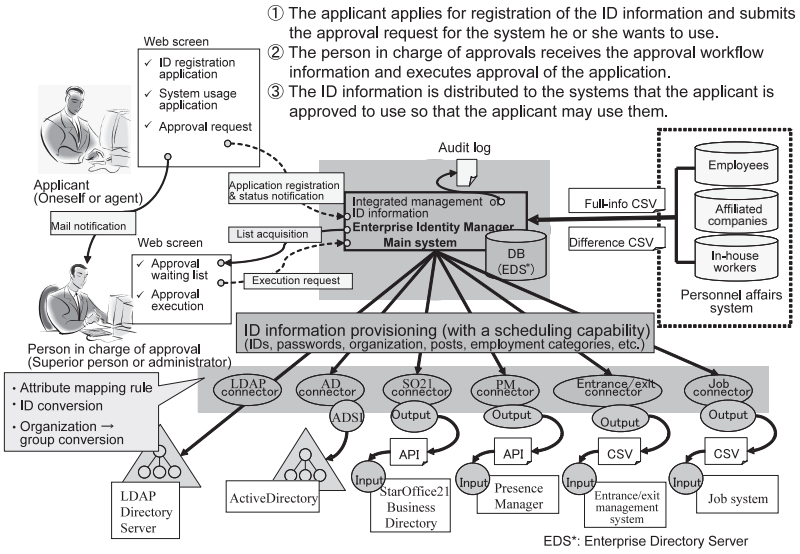


Fig. 3 Functions of the Enterprise Identity Manager.

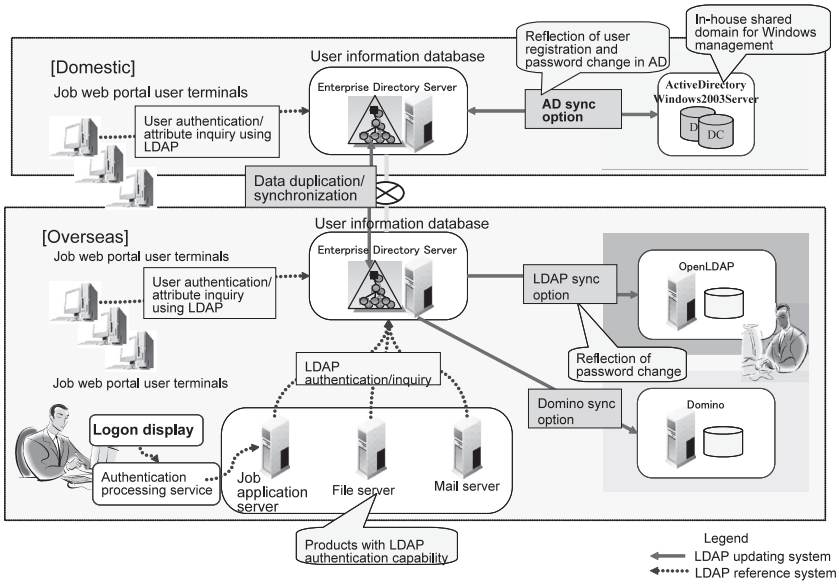


Fig. 4 Functions of Enterprise Directory Server.

summarized in **Fig. 4**. In the integrated ID management system, it assumes the role of the database storing the ID information.

(3) SECUREMASTER/ACPI, MB, ACS, EL

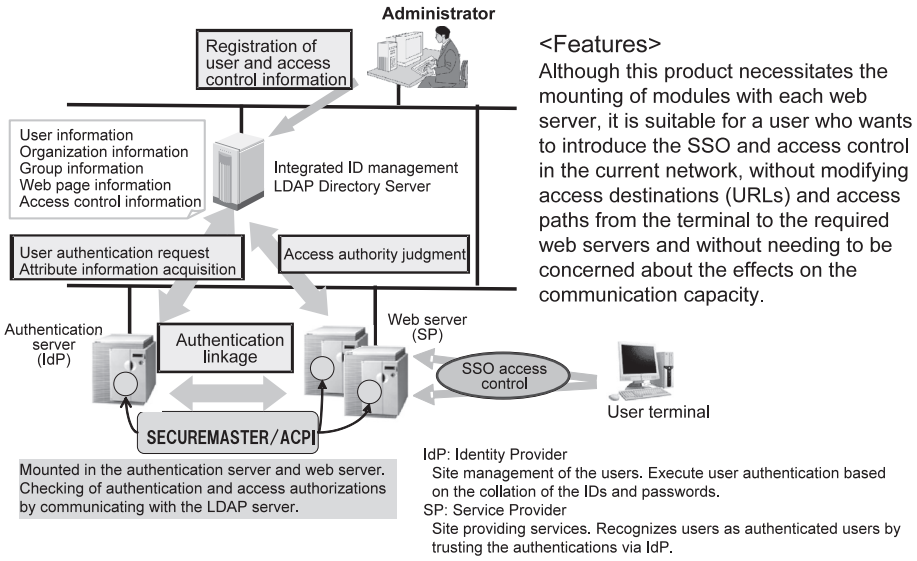
These are the SSO and access control products. The functions of the ACPI, MB, ACS and EL and their positioning are shown in **Figs. 5, 6 and 7**.

These products can be selected or combined according to the environment of each customer. The strong points of each product are as shown in the figures.

(4) Log Collector

This is the log collection/analysis support product providing functions as summarized in **Fig. 8**.

In the integrated ID management system, the recording and au-



<Features>
Although this product necessitates the mounting of modules with each web server, it is suitable for a user who wants to introduce the SSO and access control in the current network, without modifying access destinations (URLs) and access paths from the terminal to the required web servers and without needing to be concerned about the effects on the communication capacity.

Fig. 5 Functions of SECUREMASTER/ACPI.

<Features>
Although the access destination (URL) and access path from the terminal to the web server of this product involves the reverse proxy server and is therefore required to take into account the network configuration and its effects on communication capacity, it is suitable for a user who wants to introduce the SSO and access control without mounting modules in the web server independently of the operating environment of the web server.

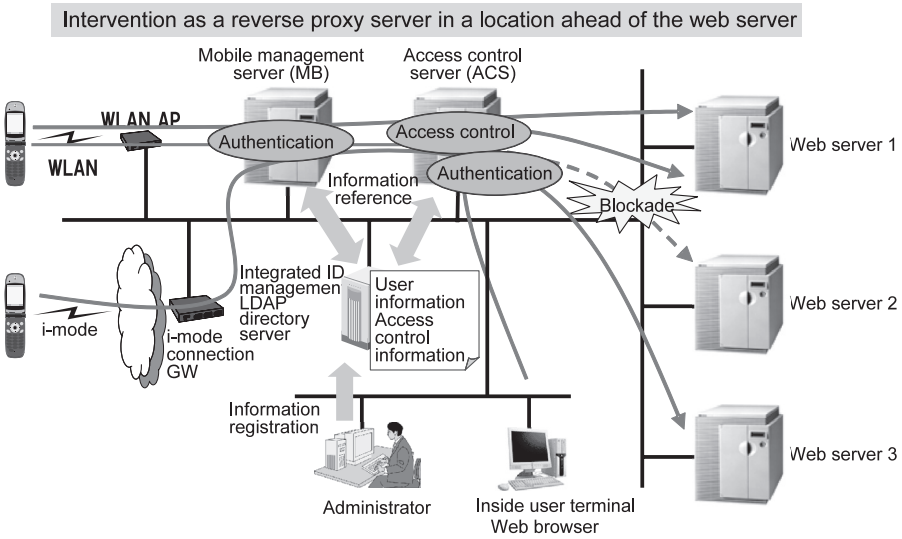


Fig. 6 Functions of the SECUREMASTER/MB, ACS.

<Features>
Although this product is not capable of web content access control using URLs like the web type SSO and access control products, it is suitable for a user who wants to introduce SSO for a wide range of systems that cannot be handled with web type products, such as client server type applications, standalone applications on terminals and mainframe terminal emulators.

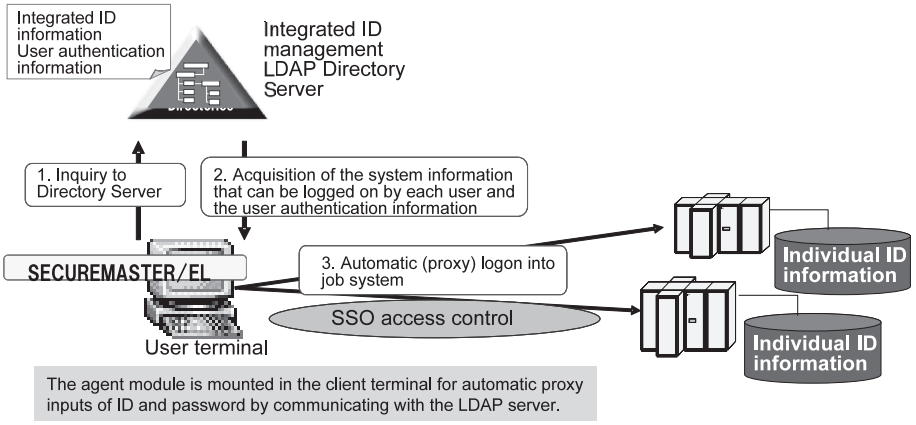


Fig. 7 Functions of the SECUREMASTER/EL.

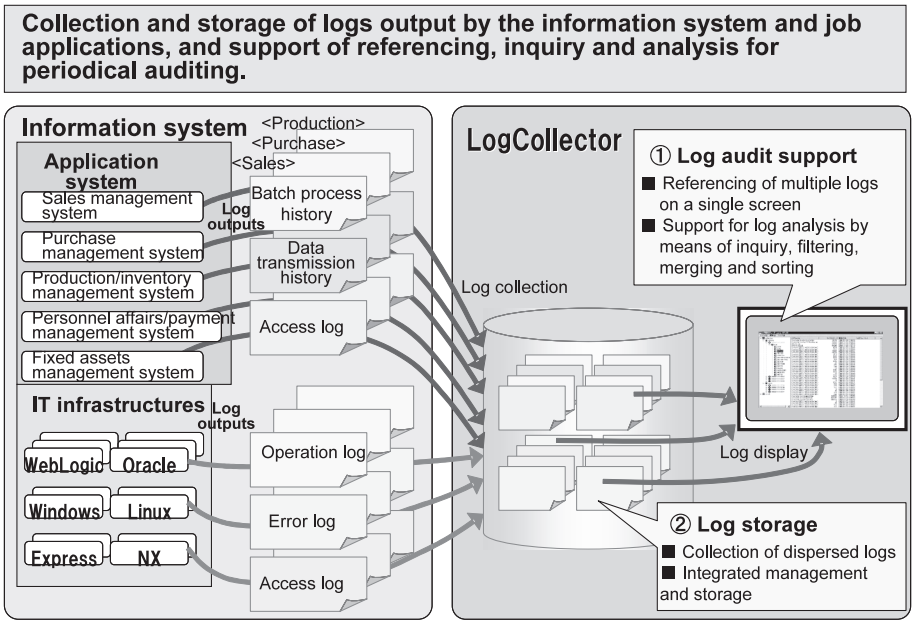


Fig. 8 Functions of Log Collector.

diting of system usage trails are important for knowing when a specific user who can be connected to an integrated personal ID may access which information systems at which timings, and the Log Collector is a tool for facilitating these operations.

4.3 Linkage with Physical (Entrance/Exit) Security

NEC also provides a solution that links the integrated ID/access management system with the office entrance/exit management system.

Linkage of these two systems makes possible; 1) personal authentication at the entrance/exist management system of the employees managed by the integrated ID management system using their ID cards (IC cards); 2) restriction of entrances/exits of employees according to their organizations, posts and jobs, etc., and; 3) permission for the use of office PCs and connection to the network only for those employees that have been authenticated by the entrance/exit management system.

5. Future Usage of Integrated ID Management Infrastructures

Preparation of the integrated ID management infrastructures is necessary without delay in order to enhance the current quality of internal governance. At NEC, we also believe that integrated ID management infrastructures can lead to continuing development of customers' businesses as described below.

To win in an age of severe competition at the global level, it is important that enterprises or service providers combine and integrate their individual core competences in order to create an overall competence.

For example, a travel company notices that the sale via the Internet of a regional company's specialty has become active and decides to collaborate with such a company in marketing that specialty. These are "the service proposing and selling the travel plans to that region" and "the service selling a regional specialty," thus providing the combination as an integrated service allowing each user (consumer) to make purchases using a single ID and with a single sign-on. The opportunities that users find in combination are thus increased. In other words, by integrating the respective markets, the two companies can advance them to a new, larger integrated market.

Such linkage of information systems/services between enterprises or service providers should be able to respond flexibly to the rapidly changing user needs and execute dynamic, speedy linkages by varying the collaborator as required. This will ensure the flexible linkage of various enterprises and services, creation of new values by combining existing values and the implementation of integrated services based on a large variety of combinations.

For this purpose, the information systems/services of the enterprises and service providers should be arranged to be equipped with a standard linkage interface that can enable flexible linkages with unspecified numbers of companies. The preparation of integrated ID management systems is the basis of the user management in such linkages and should be advanced aiming at an ID and access management system that can handle dynamic linkages.

6. Conclusion

This paper has introduced the role of the integrated ID management system and our SECUREMASTER utilities and demonstrated that the introduction of an integrated ID management environment for enterprises will contribute to the enhancement of the internal IT governance which is likely to be a requirement for enterprises of the future. We also pointed out the importance of requirements definitions and the basic design of ID management integration systems.

As a result of hard experience gained in the introduction of a wide range of integrated ID management systems inside and outside the company, we at NEC are now capable of efficiently advancing deep study into requirements definitions and basic design. The fact that we own our original products also helps us to provide enhanced and integrated ID management solutions that are suitable for Japanese enterprises. What we aim at for the future is to provide integrated ID management infrastructures that allow various enterprises and services to establish linkages by dynamically varying their partners in order to create new values by combining their existing ones and providing integrated services in the form of various combinations.

At NEC, we are determined to enhance our products and offer improved consultations designed to contribute to the preparation of integrated ID infrastructures of customers so that they may continue to effectively develop their businesses.

Authors' Profiles

TANAKA Nobuyoshi
Senior Manager,
First System Software Division,
Systems Software Operations Unit,
NEC Corporation

KUWATA Masahiko
Engineering Manager,
First System Software Division,
Systems Software Operations Unit,
NEC Corporation