Security Solutions for Communications Platforms in the Ubiquitous Age

KITAKAZE Jiro

Abstract

The communications environments of enterprises are expanding toward ubiquitous environments in which communications are available "anytime, anywhere." Meanwhile, the issues related to security are being focused on compliance management, internal control and risk management. This paper discusses the concept of the security management that will be necessary following the proposed further development of communications environments and introduces some specific solutions.

Keywords

security, compliance, ubiquitous, communications

1. Introduction

The means of communication in the activities of enterprises has been expanding rapidly, from the traditional means such as telephony and fax to messaging systems based on various IT technologies such as e-mailing, web conferencing, teleconferencing and instant messaging.

Following the integration of such means into communications tools that function entirely on the IP network platforms the scope of communications has also been expanding rapidly regardless of the boundaries between enterprises. Included in this trend are specific uses inside a single enterprise to use in all of the ubiquitous environments including at the vanguard position of sales, the domains of various types of businesses: distribution, architecture, medical care, education, etc.,) as well as in fabs, employees' homes and inside moving vehicles. This trend has led to an environment in which the communications platforms are becoming more important than ever in the activities of enterprises.

On the other hand, the changes in communications environments as seen above are also changing the concept of security among enterprises from the traditional security measures focusing on defense issues to management-type security measures. It is now a matter of urgency for any enterprise to recognize the importance of this change and to adopt early measures to support its promotion.

In the following sections, we will introduce the concept of the security measures that are required from the viewpoint of compliance and risk management in the context of the advancement of communications platforms and the proposed solutions.

2. Changes in the Communications Environments of Enterprises

The main means of enterprise communications used to be the telephony and facsimile (fax), but the introduction of the Internet (particularly E-mailing) in the 1990's has significantly changed the circumstances.

The fax has been an important means of transmission in emergencies, but most of its use has now shifted to E-mailing. At present, E-mails are also used widely for less-urgent messaging that once was the domain of telephony.

Concurrently with this trend the communications of enterprises have also been diversified widely, as may be seen in the transfer of images via the web conferencing systems, the instant messaging enabling more intermediate messaging than e-mailing and the collaboration tools that can handle document compilation and development work in addition to providing communications based on collaboration between remote locations.

However, the flood of various communications tools has also resulted in issues such as the complexity of selection or operation of tools. These issues are accelerating efforts to support the Unified Communications (UC), in an attempt to integrate the communications tools around the IP telephony environment and to thus make them more efficient. Since all of the tools run on IP network platforms as described above, their usage does not remain exclusively in the in-house intranet environments of enterprises but will be expanded rapidly to fill the ubiquitous environments both inside and outside the enterprises.

3. Issues of Security Measures

The efforts for UC and the expansion of ubiquitous environments have also introduced a new aspect to the security issues of the new communications platforms. The recent security issues imposed on enterprises and the newly changed environments are as follows.

(1) Efforts from the Viewpoints of Compliance and Internal Controls

The Japanese Corporation Law and Financial Instruments and Exchange Law have made it mandatory for large and listed companies to make efforts to put internal controls into operation.

Following the above, it is now evident that the most important security measures related to internal controls (particularly the IT-related general controls) are the “access control,” “log collection & analysis” and “content management & workflow/authorizations” (**Fig. 1**).

(2) Issues Related to the Use of Communications Tools

The advancement of communications tools has made it necessary to evaluate the security risks in the use of the various tools and to apply effective remedial countermeasures. For example, the P2P software is one of these very convenient tools, but it also poses a threat in that it may produce critical risks leading to leaks of corporate information (the representative software of this kind is the infamous Winny). When various means of communication are linked and integrated as is seen today, it is expected that building a continual verification and evaluation system for their security will become a more important issue in the future.

(3) Importance of Identify (ID) Management

The importance of ID management started to be recognized around 2000, when the use of IT systems was accelerating and has been discussed actively since that time. In those days, the opening up of core task systems led to a chaotic increase in web systems and their user accounts as all kinds of systems from groupware to mailing systems developed. The Windows [(R)] network and other platform networks as well as physical entrance/exit management systems had their own user IDs and were managed individually. These circumstances caused a serious situation in that the ID information that should have originally been managed as a unique attribute of each person was not controlled at all (**Fig. 2**).

The main issues that become evident in such a situation include the following;

1) The illegal use of IDs and impersonations;
2) leak of passwords;
3) An increase in the amount of labor required to carry out ID and password management.

These problems led to grave problems with regard to security and management.

For the “access control,” “log management” and “approval/workflow” that are important measures from the viewpoints of internal control and compliance, the loss of credibility of the ID information as their key information meant that those important measures did not function at all. This situation also became a grave problem with regard to the security measures being taken by enterprises.

In order to deal with the above problems, active attempts

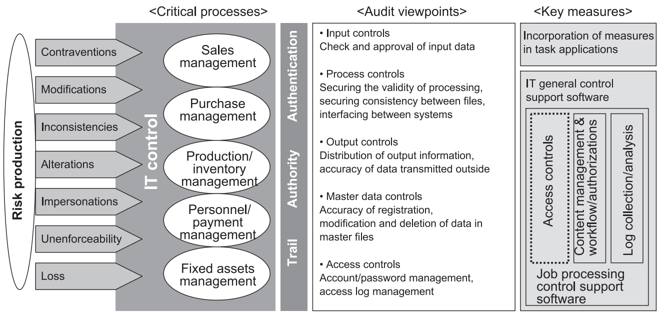
<Critical processes>
<Audit viewpoints>
<Key measures>
Risk production
Contraventions
Modifications
Inconsistencies
Alterations
Impersonations
Unenforceability
Loss
IT control
Sales management
Purchase management
Production/ inventory management
Personnel/ payment management
Fixed assets management
Authentication
Authority
Trail
• Input controls
Check and approval of input data
• Process controls
Securing the validity of processing, securing consistency between files, interfacing between systems
• Output controls
Distribution of output information, accuracy of data transmitted outside
• Master data controls
Accuracy of registration, modification and deletion of data in master files
• Access controls
Account/password management, access log management
Incorporation of measures in task applications
IT general control support software
Access controls
Content management & workflow/authorizations
Log collection/analysis
Job processing control support software

Fig. 1 Viewpoints and key measures in audit of IT-related general governance.

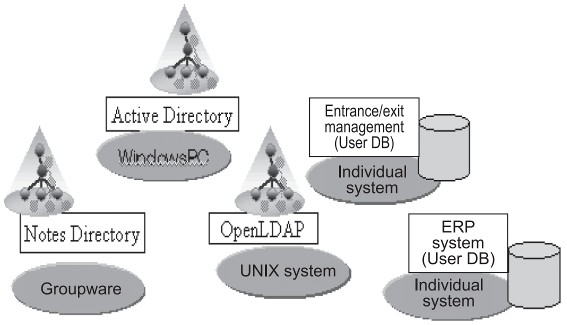

Fig. 2 Situation in which individual ID information is distributed in multiple systems.

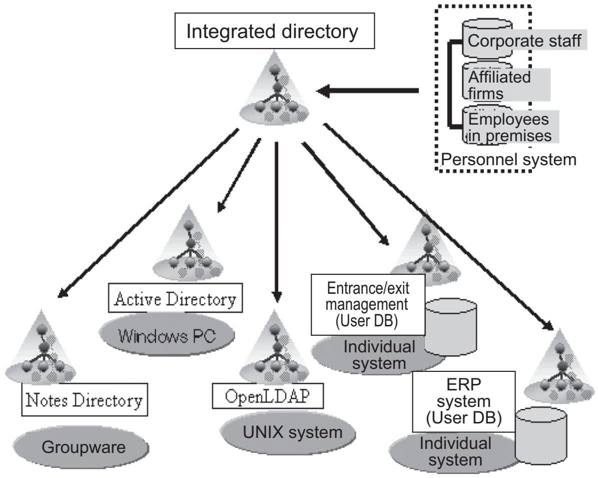

Fig. 3 Approach using an integrated directory.

were made to integrate the databases managing IDs in a server, called the directory system. Nevertheless, these attempts also led to a chaotic coexistence of various ID management systems including the Active Directory (AD) aimed mainly at managing the IDs of Windows [(R)] PC networks, the vendor-specific directory systems of individual groupware programs (e.g. Lotus Notes Domino Directory, etc.,) the directory systems for repository of job application IDs, and the ID management systems used in security cards for entrance/exit management (IC cards). In this situation, we have to admit that there are few successful cases of ID management operations using completely integrated directory systems (**Fig. 3**).

As a large variety of communication tools continues to be announced and their integration progresses, ID management is increasing in importance as a management target for linking the system user access log management and individual users. Currently, this is one of the highest-priority issues in the security measures of enterprises.

4. Introduction of the Latest Security Solutions

In the following we introduce some of our latest security solutions.

(1) Integrated ID Management

With regard to the security measures for solving the above problems, the most important management & workflow/authorizations" as described in subsection 3-(1). ID management is the key to these measures because the basis of access control are the attributes (ID and the authority and other properties accompanying it) of individuals. The trail management linked to the ID information is the most important item of the internal control and compliance measures (**Fig. 4**).

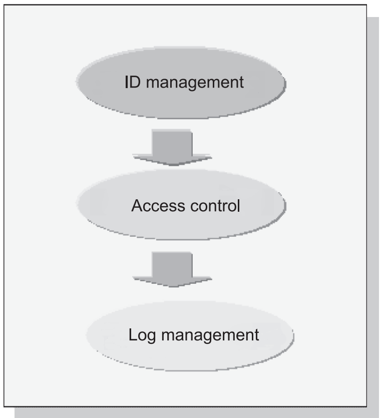

Fig. 4 Big three elements of security management.

However, the approach via the integrated directory aiming at the integrated management of IDs produces significant problems in the continued use of daily-growing systems as discussed in subsection 3-(3). Therefore, we have contrived a new approach, which is a concept of integrated management that is capable of the centralized provisioning and management of ID information distributed in multiple locations.

Fig. 5 shows a diagram of integrated management using the integrated ID management system "WebSAM SECUREMASTER/EIM" of NEC.

The integrated ID management approach provides data distribution connectors to Windows [(R)] Active Directory [(R)] and IBM-Lotus Notes Domino Directory as well as to various job applications (EXPLANNER, Flow Lites, etc.), entrance/exist management systems, groupware (StarOffice 21, etc.) and LDAPs (Open LDAP, Sun Java System Directory Server, LDAPv3, etc.). It thus enables registration, updating and deletion of user IDs and passwords according to the DB information of personnel affairs. In addition to the user management functions above, SECUREMASTER/EIM also provides password management and approval/workflow functions in order to achieve centralized operation of accurate ID information and password management.

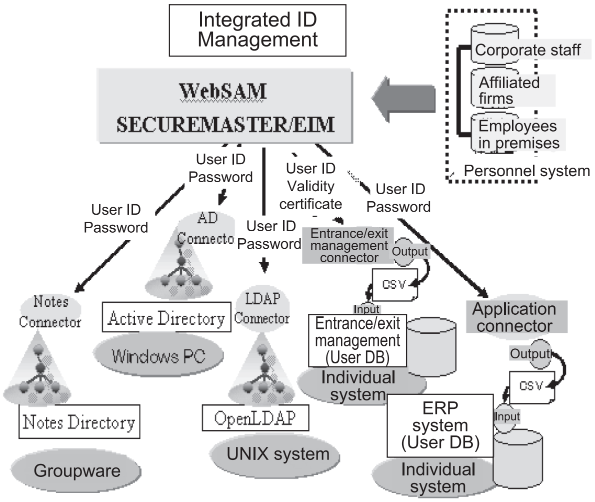

Fig. 5 Integrated ID management system provided by NEC.

Also, in addition to its ID management function, SECUREMASTER/EIM also includes a function for the storage of user information by functioning as a directory system. It can therefore be used also in the management of ID information in distributed directories and individualized systems.

Thanks to its features described above, SECUREMASTER/EIM has already been introduced in many situations. These include the user ID information management of a large-scale entrance/exit system and in the integrated operation of the LDAP Server used as a wireless LAN authentication system as well as for Active Directory use in Windows (R) PC authentications.

(2) Network Archiving

One of the security measures that is expected to increase in importance as a platform of Unified Communications in which various means of communications coexist is that of trail management. The construction of the trail management platform is a key solution in the control of IT associated with internal control (IT general control).

Actions for enforcing trail management require “log collection/analysis” measures. However, “network archiving” measures for recording, storing and analyzing communications data on the networks are also needed. Network archiving not only records and supplements communications packets, but it also provides a function for restoration on a per-application basis.

For example, it is capable of restoration of the browser display at the time of web site accessing as well as restoration of a mail message from the communication packets of a mail. This capability can contribute to reducing the time required to perform trail management work such as report compilation and analysis of trail data in the case of an incident.

The issues described above are very important from the viewpoint that the simple collection and storage of logs and packets do not achieve the original purpose of internal control. For the present, the introduction of network archiving is being started from the Internet connection portals, which are the gateways for information exchange with the enterprises outside (**Fig. 6**).

It is expected that the trail management solution using network archiving will be quite effective and important in the Unified Communications platforms featuring integrated

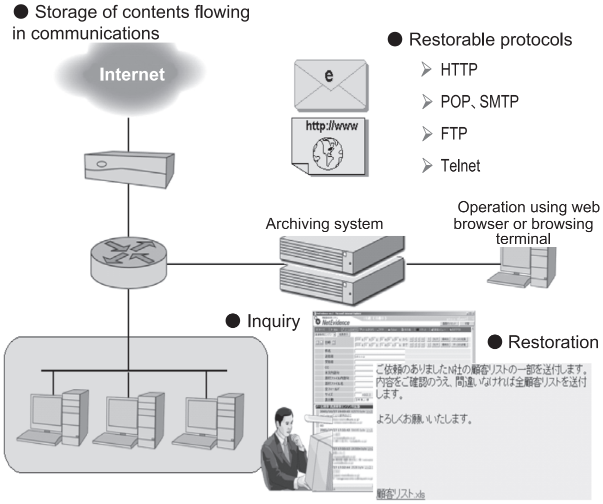
● Storage of contents flowing in communications
Internet
e
http://www
● Restorable protocols
HTTP
POP、SMTP
FTP
Telnet
Archiving system
Operation using web browser or browsing terminal
● Inquiry
● Restoration
ご依頼のありましたN社の顧客リストの一部を送付します。
内容をご確認のうえ、間違いなければ全顧客リストを送付します。
よろしくお願いいたします。
顧客リスト.xls

Fig. 6 Example of an application of network archiving.

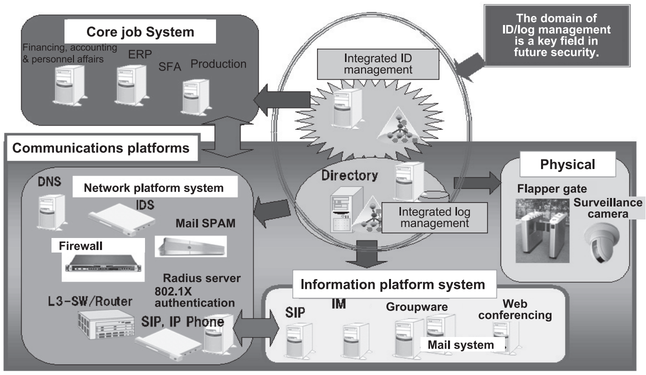

Fig. 7 Security supporting communications.

operations of various communications tools. **Fig. 7** shows a diagrammatic representation of the integrated management of various systems as discussed above.

5. Summary

It was the need to improve the efficiencies of office jobs that triggered the recent interest in Unified Communications. This interest has more recently grown to include improvements in the efficiencies of processes that have previously been based on human interventions by means of the direct command of communications tools by various job applications.

With the security measures to support the platforms for the new usages of communications, the most important issues are the three fundamentals of “integrated management,” “trail management (log management and archiving) and “authentication” as well as the access control system that is based on them (**Fig. 8**).

The above concept is currently being applied confidently to the LAN switch that supports the network platforms. A mechanism called the Network Access Control (NAC) (which is an intelligent LAN switch) is also beginning to be introduced. While the access control has previously been possible only on a per-application (or per-server) basis, the access control of this mechanism is provided by the network platform. Therefore, it is expected that it will be able to enhance the control capability for the entire system, reduce the labor for individual management and improve the security level (**Fig. 9**).

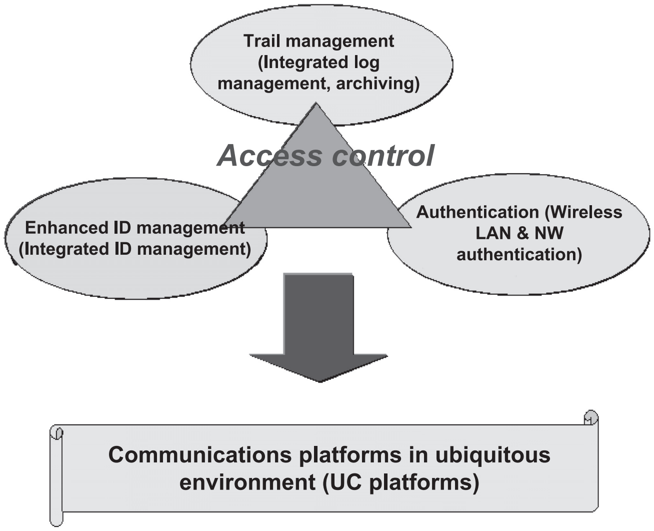
Trail management (Integrated log management, archiving)
Access control
Enhanced ID management (Integrated ID management)
Authentication (Wireless LAN & NW authentication)
Communications platforms in ubiquitous environment (UC platforms)

Fig. 8 Security in support of communications.

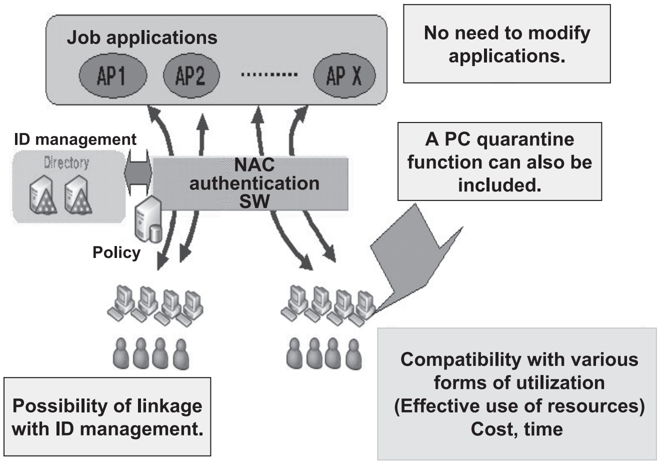
Job applications
AP1
AP2
AP X
No need to modify applications.
ID management
Directory
NAC authentication SW
A PC quarantine function can also be included.
Policy
Compatibility with various forms of utilization (Effective use of resources) Cost, time
Possibility of linkage with ID management.

Fig. 9 Network Access Control (NAC).

6. Conclusion

In the above, we discussed compliance and internal controls and also introduced security measures to support their effective implementation. At NEC, we offer a security management system for providing effective measures to meet specific needs. We also provide a wide range of services such as support in defining the requirements for taking related measures in enterprises and support for the verification and installation of connections to existing security systems as well as providing system integration services.

For the present, Japanese enterprises appear to be rather passive in their efforts toward such security measures, waiting for the preparation of a suitable legal system and the establishment of regulations inside industry. However, in the study for the preparation and use of new communications platforms, it is already an essential matter to make positive efforts toward new security measures. An approach to the new security measures of foreseeing the future one step ahead will be the source of big advances in the use of IT to support the projected activities of enterprises some years into the future.

At NEC, we are determined to continue to provide security solutions that can lead to innovations based on the UC of enterprise communications via our UNIVERGE products.

*Active Directory is a trademark or registered trademark of the Microsoft Corporation in the United States, Japan and other countries.

*IBM, IBM Notes Directory, Notes Director and Notes are trademarks or registered trademarks of the International Business Machines Corporation in the United States, Japan and other countries.

*SUN Java System Directory Server is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries.

*Other brand names and product names mentioned in this paper are trademarks or registered trademarks of their respective owners.

Author's Profile

KITAKAZE Jiro
General Manager,
UNIVERGE Solutions Promotion Division,
Enterprise Solutions Operations Unit,
NEC Corporation