Coordinated Implementation of Facilities and Information Security Systems

HAYANO Shin-ichiro, TANIKAWA Tadashi, KITAKAZE Jiro

Abstract

In response to the increasing risk of information leakage, this paper proposes a new direction, incorporating the concept of area security management. In the past, management for people, goods, PCs, networks and information content was implemented individually, however, if all management was coordinated based on "integrated ID management," it would be possible to manage "when," "by whom," and "what is done to" information. For example, by limiting the locations where information is accessed, coordinating PCs and entrance/exit controls, taking logs and processing videos, efficient management with greater security can be achievable.

Keywords

access control, security, facilities security, IC card, information leakage

1. Introduction

As the computerization of information increases, the notion of innovating business using ICT (Information and Communication Technologies) is growing. It has become easy to process and transport large amounts of information, however, this result in a greater risk for information to be leaked. Furthermore, enhancing information security has become important issues in order to protecting personal information, preventing the leaking of trade secrets, responding to rules and regulations by consolidating a foundation for internal control to support business operations[1].

This paper describes a new security system capable of managing not only information but also people and objects transporting information. The system operates in an efficient manner by mutually coordinating the management of people, objects and information, which results in a raised level of information security.

2. Trends of Information Security Management

Conventional information security management generally consists of a model intended to prevent persons from outside taking information out of a company or organization. The primary concern of security strategies had been intruder prevention, by preventing information leakage outside of a company, barring external persons from entering an office area or not allowing viruses from entering an enterprise network. However, analyses indicate that in many cases, employees are playing a role in the leaking of information; for example, through the theft or loss of a PC, or through the usage of flawed file conversion softwares at home. Moreover, it is necessary for corporate organizations that handle large amounts of personal information or data centers, where critical data is handled in an integrated manner, to implement security management different from ordinary office areas, more specifically, by limiting the persons with access to data and the taking of logs of persons accessing data.

For these reasons it will be important in the future to divide the work place into multiple areas based on security levels, as shown in **Fig. 1**, and to implement entrance/exit control, known as physical security, to each area in order to manage information relating to "where" people are and "when" that is. This is done for security measures suitable for each individual area. It will also be very important to ensure that information relating to "when" and "by whom," as well as "what is done to" information can be managed, by linking the people with the information they handle, so that if an incident occurs, it would be easy to trace it.

Fig. 2 shows a diagram that represents an arrangement of items required to manage in the aforementioned manner. First of all, it must be possible to manage the movement of people and objects by controlling entrance/exit access at various areas, not just for buildings or offices, along with presence management (positional information of people and objects, as well as information relating to their status). Second, client PCs used to handle information must be managed so that connection of such computers with privately owned PCs or PCs installed with file exchange software can be barred. Third, terminal authentication must be performed for the management of

Coordinated Implementation of Facilities and Information Security Systems

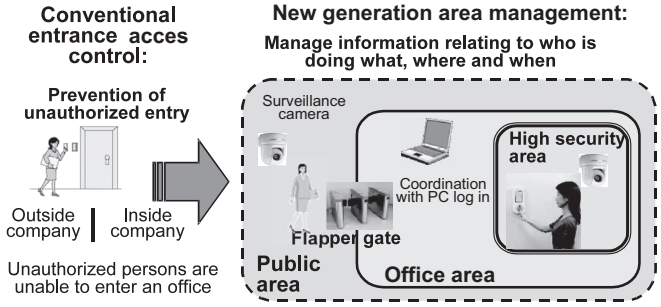

Fig.1 New generation security management.

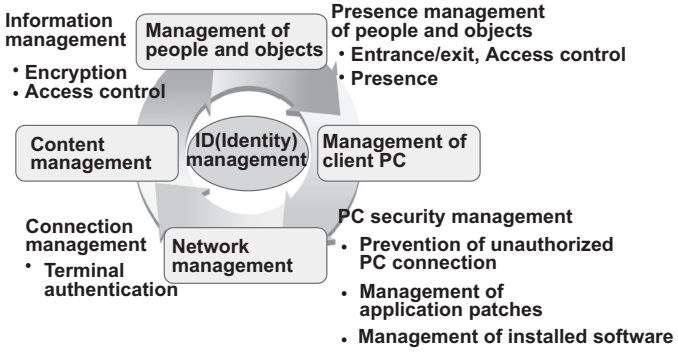

Fig. 2 Security management unifying people, objects and networks.

networks in order to manage information relating to "which" terminal is being used and "where." Fourth, encryption and access authorization control must be performed to manage content, in order to manage the people who handle and read the information. Finally, persons must be identified and the ID used for setting authorization must be managed to build a system that integrates an overall system capable of providing information relating to "who" is doing "what" and "when." By implementing such a system it is also possible to prevent unauthorized use on multiple levels. For example, unauthorized access to internal information from outside of a controlled area, or the connection of devices to make unauthorized copies of data on a network can be rendered impossible.

Through such a management system activities that lead to information leakage can be suppressed, incidents can be detected in the early stages and they can easily be tracked and inquiries made into these incidents.

3. Coordinating Implementation of Security Relating to Persons, Objects, Networks and Information

This section describes how implementation of security relating to persons, objects and information can be coordinated and how a sophisticated management system can be built. Although management systems relating to persons, objects and information have already been implemented in the past, such systems were managed separately. For example, since entrance/exit control was implemented only to management of duty it was difficult to detect access to corporate internal systems by outsiders.

Management systems for information were also implemented for individual systems and for this reason, in some cases when such systems could be made available for one system, it was necessary for them to apply for and obtain a new ID to access another system. Moreover, since the IDs that specified particular individuals were individually managed by each system, a person could have multiple IDs that varied from one system to another, even if the person assigned with such IDs and using such systems was the very same person. For this reason it was not easy to correlate the actions of an individual, when the actions were by the same individual on different systems.

In such situations, the IDs and authorized rights for the same individual were managed by multiple systems, requiring more effort to manage them. This could have also potentially triggered incidents, since the mismatching of identities and authorities could have easily occurred between different systems, as such systems were not coordinated. For example, it was possible for a system to retain information relating to persons already retired or who had resigned, with the details of individuals that were current, prior to their release from employment at a company or an organization.

In order to coordinate these systems, it was necessary to first of all implement an integrated ID management system and also to coordinate personnel or human resources systems with other systems in order to create an environment wherein personnel authentication could be unified, as shown in **Fig. 3**. Coordinating implementation of security systems relating to persons and objects, such as entrance/exit security, as well as security systems relating to information, such as management of access to information, along with security relating to networks, the entire group of systems had to be linked together by an IP network, with an integrated ID management system at the core. Non-contact-type IC cards are the latest trend for such purposes. Since implementation of all systems are coor-

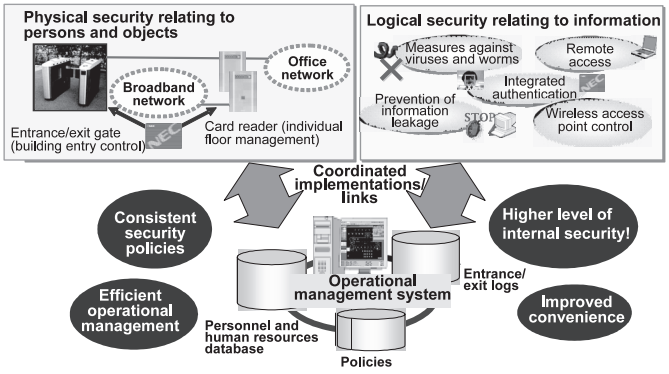

Fig. 3 Coordinated implementation of security relating to persons,objects and information.

dinated in such a manner and because the management of policies is conducted by an integrated ID management system, it is possible to implement changes at one location, thereby making the operation and management of the overall system more efficient with fewer errors. Furthermore, since all authentications are linked, it is possible for a user to simply scan his or her IC card once to be authenticated for all systems. By utilizing the function for passing on authentication information from one system to another, it is also possible to implement security enhancements without placing any burden on the user, such as logging off a PC when the user leaves the work area.

4. Practical Examples of Coordinated Implementation of Security for Persons, Objects and Information

Fig. 4 shows a practical example of coordinated implementation for persons, objects and information. The underlying foundation for such a system is entrance/exit control using IC cards. Flapper gates that prevent entry by multiple persons installed at each area and automatic doors, as well as card readers, restrict access to enter and exit, making it possible to manage information relating to "who," "where" and "when." Entrance/exit control is coordinated with the integrated ID management, which makes it possible to instantly reflect to entrance/exit control any changes with personnel or human resources. Through such implementations it becomes possible to put in place entry restrictions based on official responsibilities, as well as to conduct appropriate entrance/exit control for

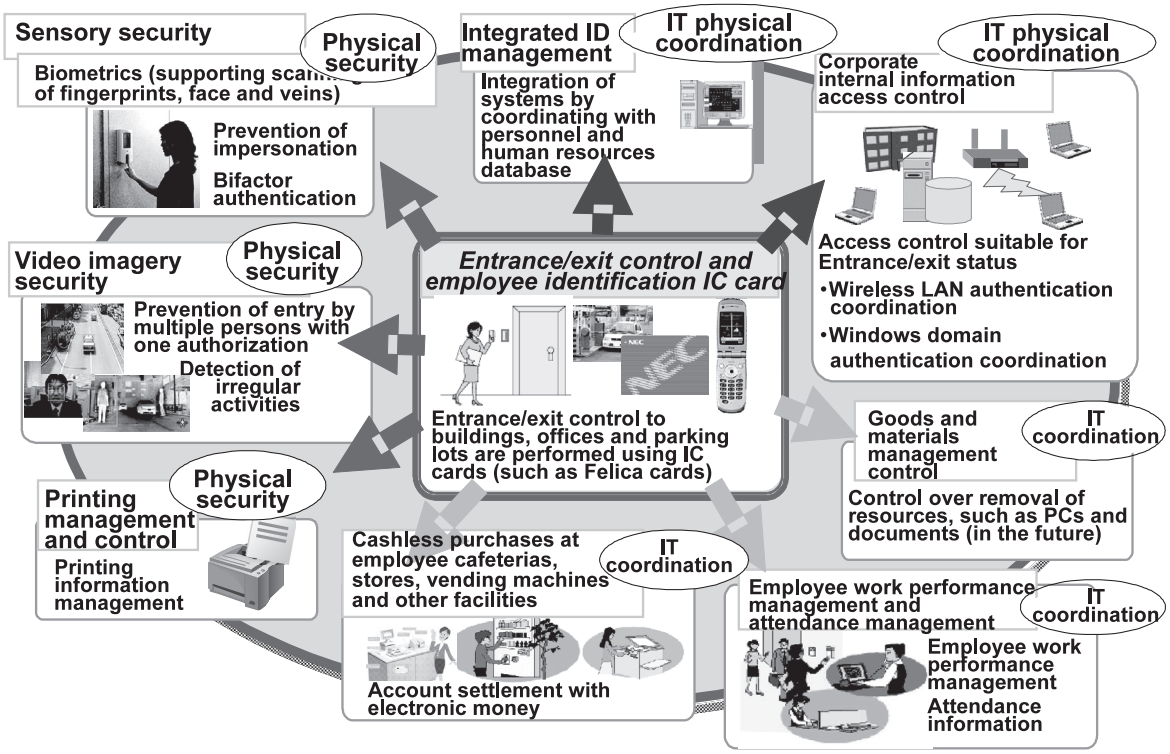

Fig. 4 Security coordination with employee identification IC card.

persons who have just joined or left a company and perform time management of employees in an efficient manner.

By coordinating the implementation of IT systems and authentication for networks access to information can also be controlled, raising the level of security for such purposes as well. Transfer of authentication information to PCs can be restricted by entrance/exit control information, to allow only persons belonging to a particular office to access certain PCs, to automatically log off a PC when its user leaves the area, to permit only those individuals who have entered the room to access wireless LAN or to take logs of areas accessed by individuals. It is also possible to take logs on locations where information was accessed. However, if more than one person enters an area with authorization for only one person, the second person is not able to gain access to any PCs in the area. Also, printing from a printer at a particular location using an IC card would be possible, by coordinating the implementation of printers, documents can be printed only when an appropriate IC card is scanned. This prevents outsiders from gaining contact with information, therefore prevents unauthorized access.

It is not necessary to replace all systems at the same time when implementing the overall system. It is possible to partially implement the system with individual component systems as required or as they are updated. The critical point is the selection of the integrated ID management system and IC cards. Both of these items must be procured with consideration for functions that can accommodate future expansion. However, when a plan is made to change an integrated ID management system or IC cards, it is possible to minimize the costs involved in future changes to the system by carefully considering the extent to which such a system or card should be coordinated in the overall system.

5. Example of Coordinated Implementation Using Video Images

Surveillance by video images have been in use for some time, but in recent years there has been an increase in video images utilized to enhance security, by digitizing and transmitting video images over IP networks. Furthermore, video image processing makes it possible to detect moving objects and non-moving objects, as well as area surveillance and facial authentication, improving security functions and reducing surveillance costs through coordinated implementation of the video system with other systems. The diagram depicted in **Fig. 5** shows the implementation of a system coordinated with entrance/exit access control. The information on the card authentication (ID, OK, NG, etc.) detected by the entrance/exit control can be stored with correlating video images in order for them to be available for the efficient identification of suspicious persons and analysis of incidents. In the past only video images were recorded and all video images had to be verified manually whenever verification was needed. When many cameras were involved an enormous amount of man-hours were required to perform manual verifications, which made timely responses difficult. With the addition of ID and entrance/exit information to the video image, it is possible to narrow down video images that need to be verified, thereby dramatically reducing the man-hours required for such verifications.

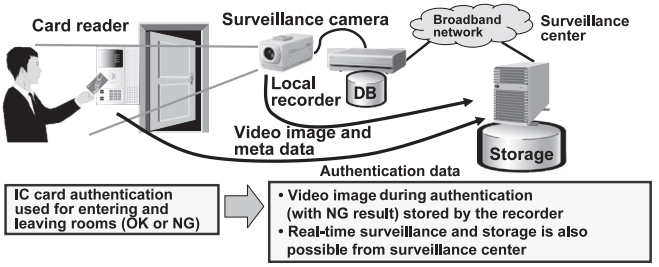

Fig. 5 Enhancement of security using video images.

In addition to facial authentication using video image processing for IC card authentication, security can be enhanced by authenticating the identity of a person, by detecting and recording suspicious persons and suspicious objects, as well as by detecting entry by multiple persons with an authorization for only one person, even at locations where the installation of flapper gates is difficult, by using video image analysis, before setting off an alarm whenever any irregularity is detected.

A portion of video image processing, which had in the past been handled by a server, can now be performed by a camera that has been configured into the system. Results of video image processing by such a camera are sent to the server as meta information, along with video images. The server can perform a more detailed analysis on the selected images, as meta information can narrow down the relevant video images. This makes it possible to avoid concentration of a load on the server when the number of cameras is increased in the future.

6. Conclusion

This paper described methods for improving the efficiency of operational management for the security of persons, objects and information. This is done by managing "who," "when"

and "where," as well as "what" was done, by implementing systems in a coordinated manner, with the integrated ID management system at the core. We expect further developments with technologies for remote detection of IDs in the future, through such means as RFID and anticipate PCs capable of transporting large amount of information and advancement in security management that includes the management of recording media relocations.

Reference

1) JYOHO TSUSHIN HAKUSHO HEISEI 17 NENBAN, SOMUSHO (Information and Communication White Paper, 2005 Edition, Ministry of Public Management, Home Affairs, Posts and Telecommunications,) June 2005.

Authors' Profiles

HAYANO Shin-ichiro
Senior Manager,
Enterprise Solutions Planning Division
NEC Corporation

TANIKAWA Tadashi
Manager,
Broadband Security Promotion Department,
UNIVERGE Solutions Promotion Division,
Enterprise Solutions Operations Unit,
NEC Corporation

KITAKAZE Jiro
Senior Manager,
Broadband Security Promotion Department,
UNIVERGE Solutions Promotion Division,
Enterprise Solutions Operations Unit,
NEC Corporation

●The details about this paper can be seen at the following.
Relevant URL:
http://www.nec.co.jp/univerge/solution/pack/index.html