

“DIGUARD NET”: Security System Integration Platform

Authors: Masahito Matsushita* and Shinji Kitagami**

1. Introduction

To ensure strict security control at lower cost in companies, we have developed “DIGUARD NET,” a security system integration platform. DIGUARD NET seamlessly links security appliances (access control, video surveillance, etc.) and security governance systems, “internal control,” (identity management, security log management, etc.) that have been installed individually.

2. Architecture of DIGUARD NET

DIGUARD NET provides the middleware and APIs (Application Programming Interfaces) which make it possible to cooperate with various security appliances, internal control systems and building facilities (Figure 1).

The architecture of DIGUARD NET consists of three layers: (1) the application layer, (2) the DIGUARD NET middleware layer, and (3) the security appliance layer (Figure 2).

In the application layer (1), we developed DIGUARD NET APIs to form cooperative security applications. The API features set in the application layer are abstractions for various security appliances and internal control systems. As the differences of individual security appliances and systems are eliminated by the APIs, DIGUARD applications become systematically

more independent. And it is possible to reduce the cost of modifying program code when the new appliances are installed.

In the middleware layer (2), DIGUARD NET middleware is located. Its functions are to translate various security appliances’ protocol and convert a customer’s information system data to the DIGUARD data format.

In the security appliance layer (3), it has the appliances, such as access control units, surveillance cameras and recorders system, and so on. The interfaces and protocols for existing security appliances (no-DIGUARD) are translated by the DIGUARD NET middleware and APIs.

3. Access Control Solution

Managing the flow of people and products is a critical issue to strengthening physical security. Detection of illegal acts such as spoofing, tailgating, and illegal unlocking by an insider requires a complex system that closely integrates the video surveillance system, physical sensor, information system, etc.

DIGUARD NET provides a mechanism for uniform handling of varieties of Mitsubishi’s security appliances. Particularly in the application layer, the APIs for controlling the appliances and systems are standardized and arranged by function, so the system can be constructed

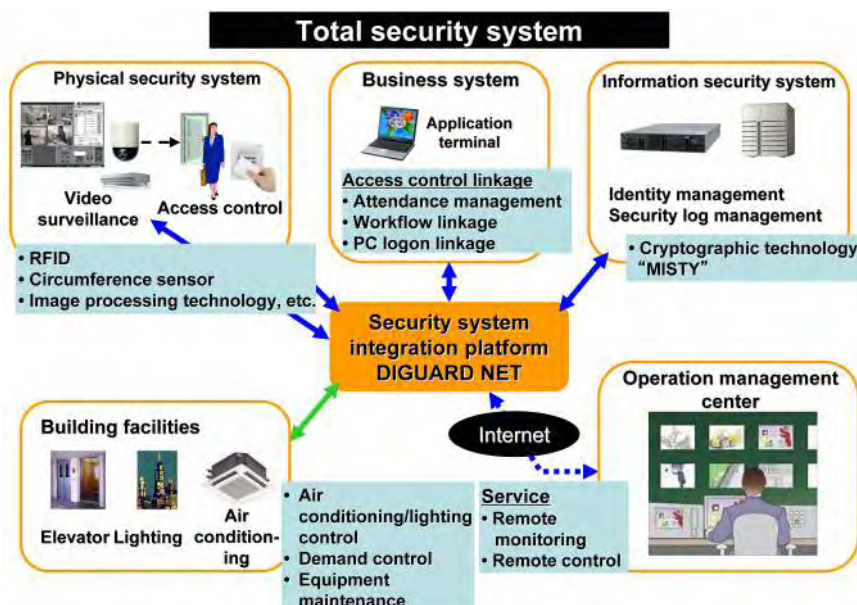


Fig.1 “DIGUARD NET”, a security integration platform

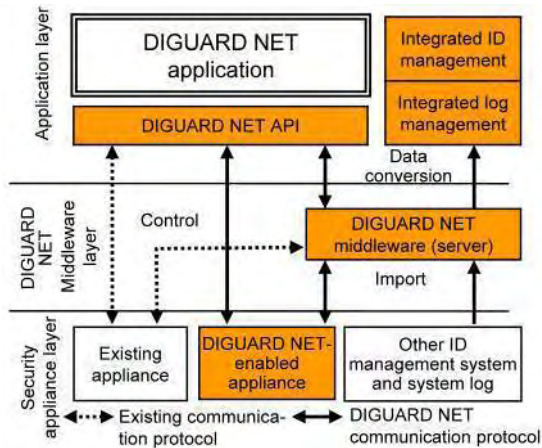


Fig.2 Basic architecture of DIGUARD NET

without considering the differences among appliances.

Figure 3 shows an example of the system configuration in which the access control system and video surveillance digital recorder are linked through DIGUARD NET. In this system, the digital recorder is DIGUARD NET-enabled and can be controlled from the application software of the access control system. Examples of linkage functions include: a function that links and plays back the video recorded in the recorder from the access history recorded in the access control system, and a function that displays the live video of the intruded area when illegal access is detected.

4. Video Surveillance Solution

In video surveillance systems, it is difficult to identify the required scene from the recordings although video recorders can effectively store evidence (recorded videos) for a long period.

To improve searching of a recorded video, the video surveillance system has to be linked with security systems such as access control, and uses information from other systems. Such cooperative system conventionally had to be developed for each project, but DIGUARD NET allows them to be developed efficiently.

Figure 4 shows a configuration example of DIGUARD NET-linked system focusing on video surveillance. In this example, the other system operates as an external event source for the video surveillance system. The video surveillance system obtains the events such as access operation and illegal operation that occur in the access control system and status changes such as locking&unlocking, long-time door open, and appliance errors, for example, via DIGUARD NET. It then saves these information items as external events together with time of occurrence, camera information, etc. and uses them for recalling the recorded videos.

Figure 5 shows the screen image of the integrated surveillance monitor terminal achieved based on the monitor terminal of the digital type video surveillance

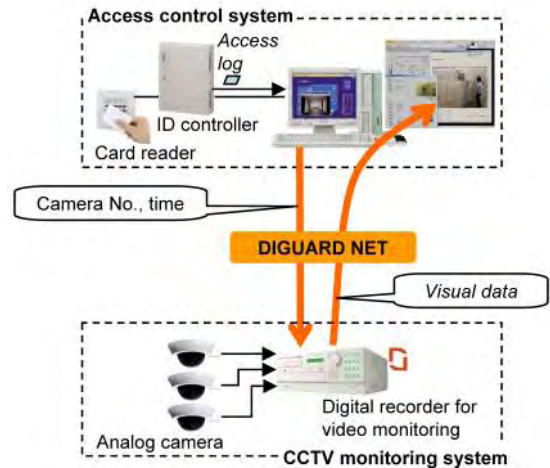


Fig.3 Linkage system focusing on access control system.

5. Internal Control Solution for Security Governance

The Control Objectives for Information and Related Technology (COBIT) framework that achieves the internal control includes identity management that integrates and manages the user information and access privilege of each system and a mechanism that accumulates and audits system logs.

However, in order to continuously maintain and take measures to improve-governance against various threats, the entire company must unify its governance mechanism.

DIGUARD NET enables security-related management information to be safely exchanged between the security governance, internal control system and access control and video surveillance systems. In addition to the conventional information system, security governance (identity management and security log management) of the entire company including access control and video surveillance can be achieved.

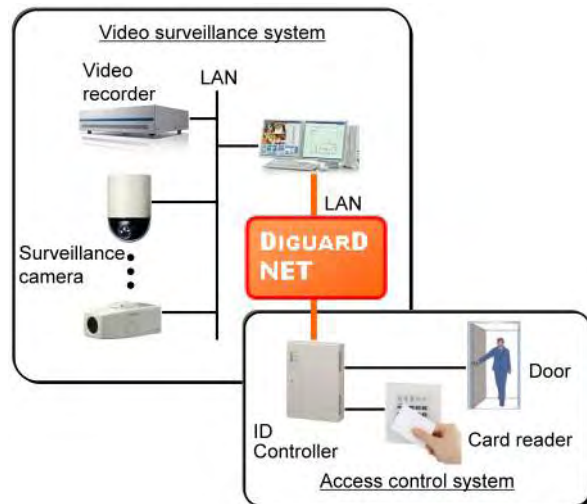


Fig.4 Linkage system focusing on video surveillance

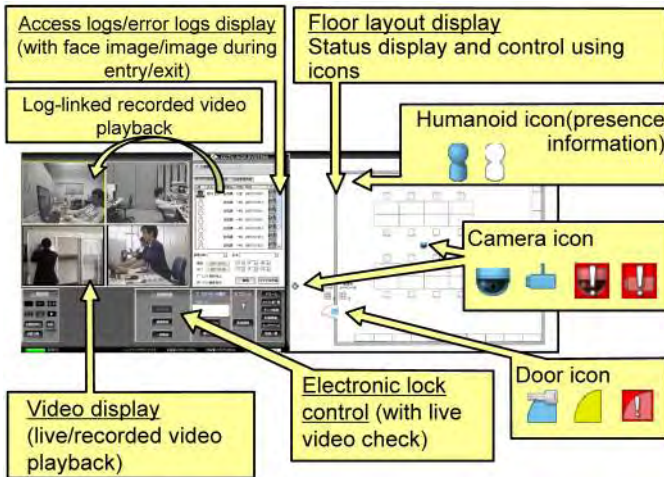


Fig.5 Screen example of the video surveillance/access control cooperative system

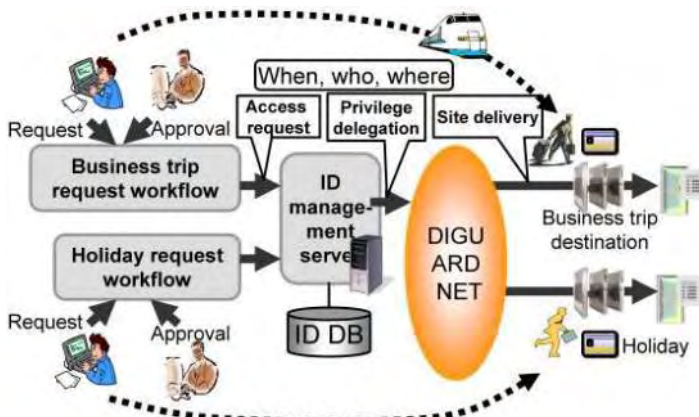


Fig.6 Workflow and access control linkage system

5.1 Identity management (ID management)

Examples of security governance through identity management include: promptly resetting privileges after a staff reorganization, temporary delegation of privileges to personnel on business trips and holiday, and the consistency check between access information and attendance information.

The identity management server imports information about privileges upon joining, retirement, personnel changes, reorganization, etc. from the human resource system, and delivers privilege information determined according to the access control policy governed by corporate rules, etc. to the site where the access control system is installed.

Figure 6 shows an example of the workflow linkage system that temporarily delegates privileges. The identity management server imports information about a user who is granted access as a result of a business trip request workflow, working overtime request workflow, etc., determines whether privilege delegation is valid, and delivers smart card authentication information, period, and accessible location to the access control system.

5.2 Security log management

Access control systems and various information systems recently output and store large amounts of security logs for the purpose of preserving evidence. These logs have conventionally been managed for each appliance and system. However, DIGUARD NET enables various logs to be collected from multiple security appliances and information systems in a unified procedure for integration and management. This reduces management costs and makes log analysis more efficient.

Figure 7 shows the configuration of the integrated security log management system using DIGUARD NET. The integrated log management server collects logs from access control and video surveillance systems and various information systems connected to DIGUARD NET for centralized management.

The server also saves access control and information system logs and snapshot images of video surveillance linked with the time and ID. This enables logs to be searched for a specific time, person, and appliance, and associated images to be displayed when investigating an incident.

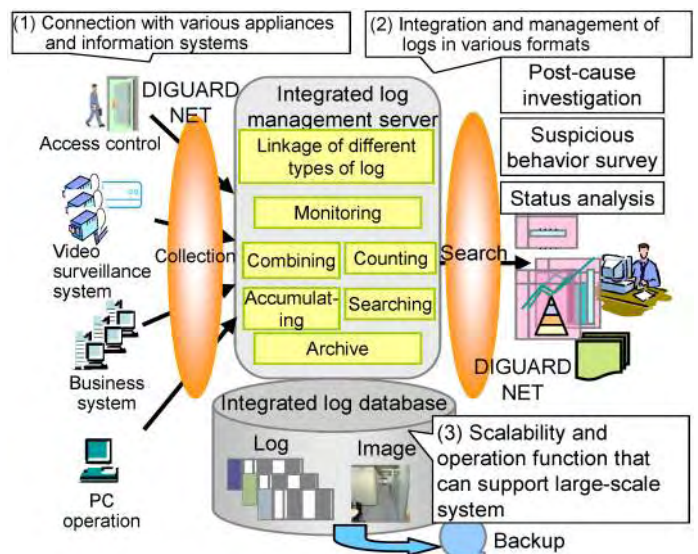


Fig.7 Integrated security log management system