Featured Articles

Physical Security for Companies that Maintain Social Infrastructure

Shinsuke Kanai
Kenji Nakamoto
Akio Takemoto
Masatoshi Furuya

OVERVIEW: While the companies that maintain social infrastructure have gained many benefits from advances in information and communications technology and its widespread adoption, they also face new threats. Modern corporate management demands security measures for both the physical and cyber realms. For reasons of corporate group governance, there has been a growing trend in recent years toward the group-wide consolidation of system management, with increasing adoption of both the private and public cloud models. There has also been interest in the use of techniques for ultra-high compression and decompression in surveillance camera systems to allow transmission over narrow bandwidths. The food safety sector, meanwhile, has recognized the potential for establishing video traceability infrastructure, utilizing bar codes or other forms of identification.

INTRODUCTION

THE major earthquake that struck eastern Japan in March 2011 caused considerable damage to the social infrastructure on which people's quality of life and corporate business activity depend. The consequences continue to disrupt the lives of many people. Furthermore, because the earthquake made it difficult for many of the companies that suffered damage to continue in business, it also resulted in indirect interruptions to the operations of some of the companies that did business with these directly affected companies. This demonstrates how companies are part of the infrastructure of society (see Fig. 1).

The causes of interruptions to corporate activity are not limited only to earthquakes. Nor are they limited only to things that relate to a company's own business, such as leaks of personal information, data falsification, false accounting, false advertising, or inadequate food hygiene management. Along with these, they also include various other serious threats, including malicious behavior by staff, malicious postings on the Internet, or company-targeted terrorism. Physical security for companies can be defined as "preemptively establishing physical systems to prevent, track, and rapidly recover from threats with the potential for business interruption."

This article describes developments in the field of physical security products, such as access control or surveillance cameras, that consolidate and automate problematic administration at the corporate groups that maintain social infrastructure, a ultra-high compression and decompression technique for video that is useful for transmission over narrow bandwidths,

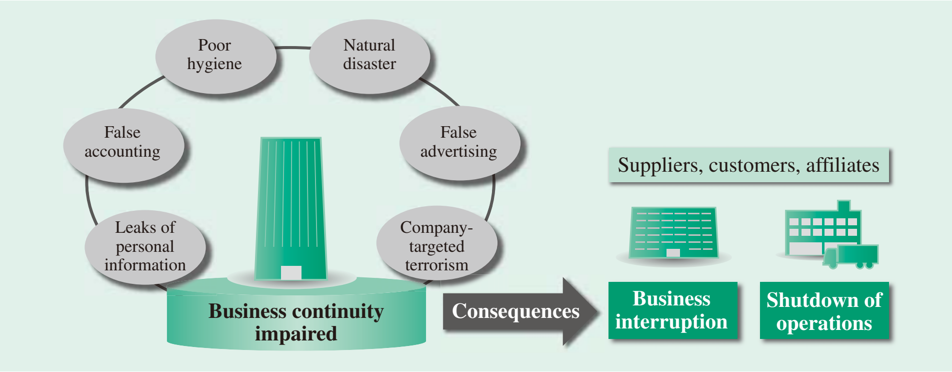

Fig. 1—Consequences of Business Interruption to Companies Involved in Social Infrastructure.
The inability of a particular company to maintain its operations will have consequences for its customers and suppliers, among others. Companies are also part of the infrastructure of society.

and infrastructure for physical security and traceability in the food safety sector that is seen as having potential in the future.

STANDARDIZED GROUP-WIDE CORPORATE PHYSICAL SECURITY

For the companies and other organizations that handle confidential, commercial, technical, or personnel information, or that maintain important social infrastructure, it has become an accepted practice to restrict access to work areas and other key locations at their offices and to control where people are able to go. Nowadays, doors are kept locked when not in use and it is rare for outsiders to gain access to a workplace without permission. Visitors are received away from the workplace at a reception room. The main mechanisms used for this purpose are identification devices such as non-contact smartcard readers and finger vein recognition systems, together with other equipment such as electric locks and automatic doors or gates. Staff can use a card or their finger vein pattern to open the doors to those rooms to which they are permitted access.

Because many such companies are subject to intense global competition, one of the most important aspects of their business is timely integration, reorganization, and rationalization, including of group companies. A consequence of this is that transfers and other changes of workplace occur frequently for staff throughout the group, who may number in the thousands or more. If each workplace were to use a different way of controlling access, not only would it be inconvenient for staff and management, there would also be considerable cost each time changes were made. An effective solution is to centralize personnel information across the group and to provide automatic links between the personnel information and access control systems.

Meanwhile, because criminal acts typically involve someone gaining unauthorized access in a way that does not leave a record, such as “tailgating” (entering behind an authorized person), it is difficult to determine what has happened from the access control system’s records alone. Given that people’s memory of events becomes more uncertain as time passes, it is critical to locate surveillance cameras at key thoroughfares where they cannot be evaded, and to store all video that contains movement for at least several months. However, while installing more cameras makes it easier to determine what has happened by reviewing the video, it also results in more data to be stored.

Since 2008, Hitachi has been adopting standardized physical security based on this concept throughout the group, including at its headquarters and at all branch offices, sales offices, factories, laboratories, and company hospitals.

TRENDS IN PHYSICAL SECURITY PRODUCTS

Private Cloud Model

Past systems have mainly used “local model” configurations that are structured around individual workplaces. However, it is not an easy task to provide the environment and support systems needed for 24-hour operation of servers, recorders, and other equipment independently at each workplace. It is particularly difficult at sales offices with a small staff.

In response, Hitachi recommends the use of in-house data centers to centralize system administration for physical security at a number of workplaces and group companies, using systems with a configuration based on a private cloud model shared by each workplace. Use of a private cloud model not only allows centralized management of servers, recorders, and other equipment, it also facilitates automatic links to personnel information systems. However, care is required when centralizing the transmission and archiving of video. Because it is enough to be able to view live or recorded video when needed, it is not necessarily a requirement to consolidate all video at one place in realtime. Unless it causes administration problems, Hitachi recommends that recorders be distributed across the company (see Fig. 2).

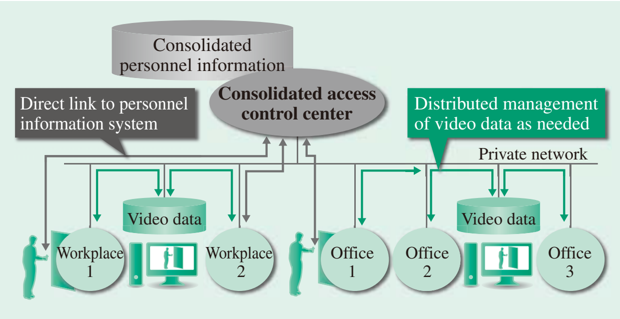
Consolidated personnel information
Direct link to personnel information system
Consolidated access control center
Distributed management of video data as needed
Private network
Video data
Video data
Workplace 1
Workplace 2
Office 1
Office 2
Office 3

Fig. 2—Configuration of Physical Security Based on Private Cloud Model.
In addition to centralizing management of servers, recorders, and other equipment based on a private cloud model, this also facilitates the provision of automatic links to personnel information systems.

Public Cloud Model

Many companies adopt an information security policy of not connecting their corporate physical security systems to their internal network, meaning there is no automatic link to their personnel information systems.

For customers who adopt this policy, Hitachi offers its integrated facilities management solution. The facilities management solution uses a configuration based on a public cloud model to allow centralized system administration covering multiple workplaces. This model uses servers and application services hosted at a public cloud center managed by Hitachi. By outsourcing the maintenance and management of the servers used for centralized administration of multiple workplaces based on this model, the customer can be sure of always having easy access to the latest application services.

In addition to the facilities management solution for offices, Hitachi also supplies an information system for condominiums.

REQUIREMENTS FOR SURVEILLANCE CAMERA SYSTEMS

Criminal acts that occur in a physical environment are often planned. Perpetrators use the Internet to plan the crime or check the targeted site or other information beforehand, and take a preliminary look at the site, escape routes, and other locations. To obtain crime-solving clues, criminal investigations in recent years have increasingly been utilizing forensic analyses of networks and other information technology (IT) equipment, and cross-checking with analysis of video surveillance records from the scene. The use of surveillance cameras is becoming increasingly important.

Along with locating surveillance cameras where people cannot reach them, it is also important to provide them with adequate anti-tampering functions. For example, it is essential that they be fitted with alarms that will be triggered if someone covers them with spray or some other form of blindfold, or if someone interferes with their power supply, communications, or camera orientation. In the case of locations where people frequently interfere with the camera orientation, it is necessary to consider installing a domed camera; a panoramic view, tilt, and zoom (PTZ) camera that can be operated remotely; or a 360° omnidirectional camera.

Hitachi recommends its video management system that incorporates effective anti-tampering functions and functions for detecting or searching recorded video for suspicious people or behavior. These functions can automatically detect movements that indicate an attempt at unauthorized access; people who are hiding their faces in a suspicious way; or people bringing in, taking out, or swapping suspicious packages or leaving them unattended, for example. Hitachi also intends to consider applications that can detect or search for instances in which someone is carrying packages that are clearly different in type or quantity between the time they enter and leave a room. At sites such as data centers, this function should be used in conjunction with other measures such as checking in packages or inspecting them on arrival or departure. At places that are not sufficiently visible to people, the system would issue a verbal warning to any suspicious person from a speaker-equipped camera.

Analog cameras have been widely used in the past due to limits on the storage capacity of recorders and on network bandwidth, and because they are easy to set up. Because of the need for surveillance to extend from large areas down to tiny details such as fingertip movements, use of high-resolution Internet protocol (IP) cameras with resolutions in the megapixel range has become increasingly common in recent years. However, it is necessary to avoid compressing images by so much that the high-resolution video is unable to be restored to its original quality level due to limits on transmission and storage. In response, Hitachi has been working on research and development of a technique for ultra-high compression and decompression intended for use in narrow-bandwidth transmission. This technique allows the storage of long-duration video from large numbers of cameras at a high resolution and frame rate, even when bandwidth and recorder storage capacity are limited, and that also supports high-speed video searching. It is anticipated that this will lead to progress on the centralization and backup of video management.

FOOD SAFETY AND PHYSICAL SECURITY TRACEABILITY

Guaranteeing food safety is vital to ensuring that people can participate healthily in society. The companies and retailers involved in the growing, processing, manufacturing, distribution, and consumption of food (the “food chain”) all have an important role to play as part of the infrastructure of society. In the case of countries that experience frequent terrorism, this concern extends to subjecting all guests and visitors to hotels, particularly those used by important people, to body checks by metal detector.

When considered in terms of physical security, food processing plants that mainly deal with processing and other manufacturing are characterized by having large sites that are visited by numerous vendors, and by employing staff under a wide variety of employment arrangements. If a plant is undefended, it is easy for someone planning a crime to gain access and difficult to identify their behavior as suspicious once they do so. For these reasons, it is good practice to make the plant difficult to enter without authorization through measures such as limiting the number of points of entry as far as possible, having guards check people and vehicles on entry and exit, and enclosing the site in a fence with intruder detection sensors or other defenses (see Fig. 3).

For hygiene reasons, however, such as measures for preventing contamination by foreign material, it is not possible to install access control using non-contact smartcards or other methods at the production areas inside a factory. For example, along with metal detector body checks conducted prior to entry to a production area, it is necessary to adopt measures involving the use of high-resolution surveillance cameras both inside and outside the production area to record faces, fingertip movements, and other features. If something does happen, it is vital to have measures in place to present these records as evidence. In recent incidents of harmful food contamination in Japan, considerable time had often elapsed between the date of production and the detection of the contamination at the point of consumption. At a minimum, recorded video should be kept from the date of production up until the food's use-by date. Also, it is not uncommon for food processing plants to present a difficult environment for camera operation, including hot and humid conditions or freezing temperatures. It is recommended that suitable checks be made regarding the operating temperature range prior to installation, and that cameras be inspected regularly.

Interest in the use of video recording for food traceability has grown in recent years. As noted above, the presence of harmful contaminants in food is often not detected until the point of consumption, meaning that the contamination could have occurred at any point along the food chain. By recording the time and location each time the bar code attached to the food is scanned as it moves along the food chain, if something subsequently happens, it will be possible to go back

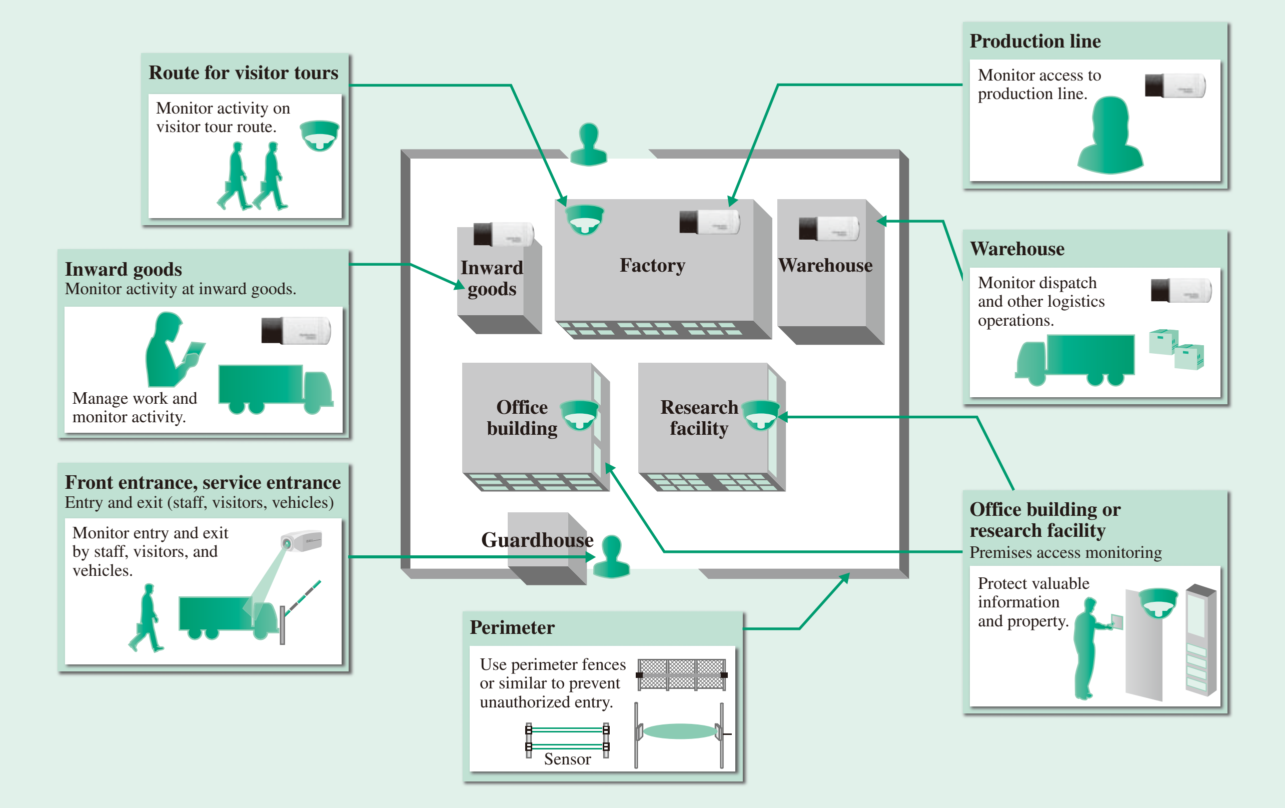
Route for visitor tours
Monitor activity on visitor tour route.
Inward goods
Monitor activity at inward goods.
Manage work and monitor activity.
Front entrance, service entrance
Entry and exit (staff, visitors, vehicles)
Monitor entry and exit by staff, visitors, and vehicles.
Inward goods
Factory
Warehouse
Office building
Research facility
Guardhouse
Perimeter
Use perimeter fences or similar to prevent unauthorized entry.
Sensor
Production line
Monitor access to production line.
Warehouse
Monitor dispatch and other logistics operations.
Office building or research facility
Premises access monitoring
Protect valuable information and property.

Fig. 3—Physical Security at Food Processing Plant.
This access control solution for factories supports physical security at food processing plants and other facilities.

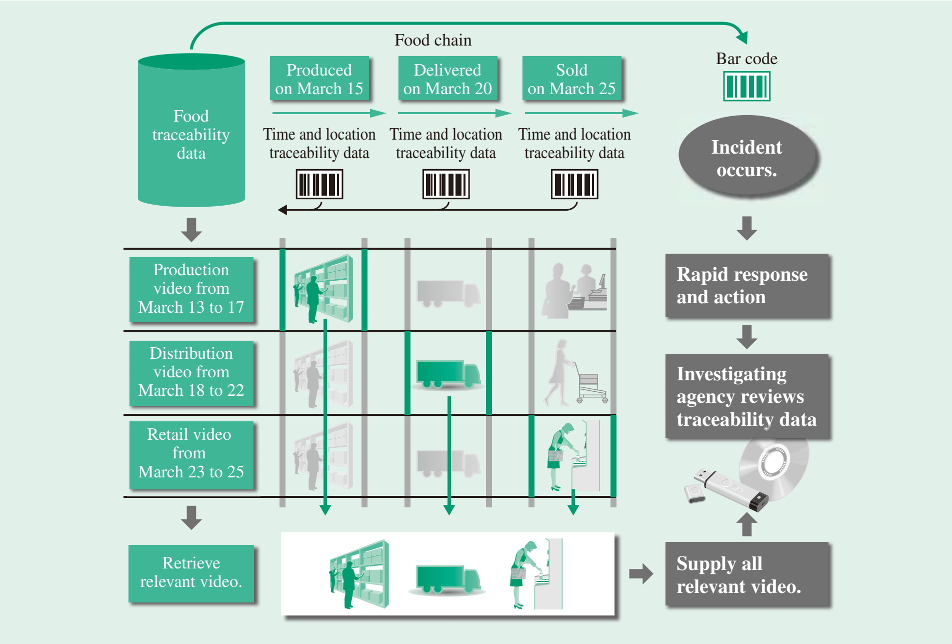
Food chain
Food traceability data
Produced on March 15
Delivered on March 20
Sold on March 25
Time and location traceability data
Time and location traceability data
Time and location traceability data
Bar code
Incident occurs.
Production video from March 13 to 17
Distribution video from March 18 to 22
Retail video from March 23 to 25
Rapid response and action
Investigating agency reviews traceability data
Retrieve relevant video.
Supply all relevant video.

Fig. 4—Block Diagram of Video Traceability.
There is a need to establish the infrastructure for video traceability along the entire length of the food chain.

and review all of the recorded video for those times and places. This is much more efficient than reviewing all of the video. It is anticipated that infrastructure will be established for video traceability so that video of all of the main control points along the food chain is able to be viewed over a network (see Fig. 4).

CONCLUSIONS

This article has described developments in the field of system models for the group-wide standardization of physical security for corporate groups, which has an important role underpinning both companies and social infrastructure, with an emphasis on the functional requirements for surveillance cameras. The article has also used food safety as an example, explaining the need for physical security at all of the companies and retailers involved in the food chain, and how it is anticipated that the industry will work together to establish the infrastructure for video traceability.

Hitachi believes that the wider adoption and encouragement of corporate physical security, and advances in the associated technology, will also contribute to the success of the Tokyo Olympics in 2020.

ABOUT THE AUTHORS

Shinsuke Kanai

Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in solution business in integrated security.

Kenji Nakamoto

Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in solution business in integrated security.

Akio Takemoto

Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in security business in cameras.

Masatoshi Furuya

Energy System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in business planning related to security.