Physical Security Systems

OVERVIEW: Since the terrorist attacks of September 11, 2001, in the United States, various steps have been taken around the world to raise the level of security, including anti-terrorist steps, at key facilities and public places where people gather. In that context, the needs are increasing for physical security systems and related equipment. Centered on security systems it developed in the past, Hitachi, Ltd. is now developing new products such as detectors for detecting dangerous objects, personal authentication systems, and inspection equipment using X-ray equipment. The discussion in this paper is centered on security systems Hitachi previously developed but it also presents a summary of the current situation concerning sensors for detecting unauthorized facility access, personal authentication systems, and surveillance cameras, all used in security systems.

INTRODUCTION

SINCE the terrorist attacks in the U.S. on September 11, 2001, terrorist threats have increased around the world. As a result, security measures have been bolstered at key transport facilities such as airports and harbors, as well as at places where people gather, i.e. various events and celebrations.

In that backdrop, Hitachi established a physical security equipment business under the theme “Comfort and Safety.” The new business is centered on security systems that Hitachi has developed, installed, and maintained up to the present. Hitachi has also been involved in the field of cyber security, and has much experience in developing and installing many such systems. In fact, Hitachi is one of the few manufacturers able to combine its expertise in the twin fields of cyber security and physical security to provide solutions for total security systems.

Among physical security systems, the emphasis in this paper is on security systems in place at key...
NEEDS OF KEY FACILITIES FOR SECURITY SYSTEMS

Some key facilities in Japan have had security systems with sophisticated levels of security for years. In many countries the security level at key facilities, centered on the U.S., has been raised recent years. Even facilities that formerly did not use security systems are now planning to install them.

Next, let us describe a security system commonly used in Japan.

OUTLINE OF SECURITY SYSTEM

This is an access-egress control system that
Unauthorized Access Surveillance System

The unauthorized access surveillance system uses various kinds of sensors for surveillance of unauthorized access. It is necessary to select the most appropriate sensors depending on the surrounding environment, the prevailing weather of the particular location, and other factors. Table 1 provides a comparison of surveillance cameras and Table 2 provides a comparison of selected cards.

### Table 2. Comparison of Surveillance Cameras

This table compares selected surveillance cameras. Cameras should be chosen according to their use environment.

<table>
<thead>
<tr>
<th>Camera type</th>
<th>Single-pole rotation, solid-body type camera</th>
<th>Tri-pole rotation solid-body type camera (high magnification rate)</th>
<th>Tri-pole rotation solid-body type camera</th>
<th>Day-and-night-vision single panel solid-body type camera</th>
</tr>
</thead>
<tbody>
<tr>
<td>Camera type</td>
<td>Visible light color</td>
<td>Visible light camera</td>
<td>Visible light camera</td>
<td>Near infrared rays, and visible light color</td>
</tr>
<tr>
<td>CCD element</td>
<td>1/3” CCD</td>
<td>1/2” CCD × 3</td>
<td>1/2” CCD</td>
<td>1/2” CCD</td>
</tr>
<tr>
<td>Resolution</td>
<td>480 TV lines</td>
<td>850 TV lines</td>
<td>800 TV lines</td>
<td>480 TV lines</td>
</tr>
<tr>
<td>Visible light sensitivity</td>
<td>Ordinary 1.5 lx</td>
<td>0.009 lx</td>
<td>0.009 lx</td>
<td>0.3 lx (Visible light color)</td>
</tr>
<tr>
<td></td>
<td>Recording 0.02 lx</td>
<td>0.00007 lx</td>
<td>0.00007 lx</td>
<td>0.02 lx (Near infrared rays)</td>
</tr>
<tr>
<td>Lens</td>
<td>Zoom lens 16 times 4.5 – 72 mm</td>
<td>33 times 11 – 363 mm</td>
<td>17 times 7 – 119 mm</td>
<td>18 times 8.6 – 154 mm</td>
</tr>
<tr>
<td>Camera stand</td>
<td>Electric high-speed rotation camera stand</td>
<td>Electric high-speed rotation camera stand</td>
<td>Electric high-speed rotation camera stand</td>
<td>Electric high-speed rotation camera stand</td>
</tr>
<tr>
<td></td>
<td>Automatic high-speed rotation, horizontal maximum 180°/s</td>
<td>Automatic high-speed rotation, horizontal maximum 49°/s</td>
<td>Automatic high-speed rotation, horizontal maximum 90°/s</td>
<td>Automatic high-speed rotation, horizontal maximum 45°/s</td>
</tr>
<tr>
<td>Lighting</td>
<td>Built-in option</td>
<td>Fitted to outside option</td>
<td>Fitted to outside option</td>
<td>Near infrared ray lighting</td>
</tr>
<tr>
<td>Mass</td>
<td>13.5 kg</td>
<td>About 70 kg</td>
<td>About 20 kg</td>
<td>About 20 kg</td>
</tr>
<tr>
<td>Features</td>
<td>Tracking through high-speed rotation</td>
<td>Fitting for night surveillance</td>
<td>Fitting for night surveillance</td>
<td>Near infrared rays give it high concealment</td>
</tr>
<tr>
<td>Aim of installation</td>
<td>Limited to night surveillance of preset area</td>
<td>For wide-area night surveillance</td>
<td>For wide-area night surveillance</td>
<td>For night surveillance of concealment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 3. Comparison of Selected Cards

This chart compares selected types of cards. In the future, the use of smart cards is expected to be mainstream, because of their data security capabilities.

<table>
<thead>
<tr>
<th>Card Type</th>
<th>Prevention of counterfeiting</th>
<th>Data volume</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar code</td>
<td>x</td>
<td>x</td>
<td>☎</td>
</tr>
<tr>
<td>Electromagnetic cards</td>
<td>△</td>
<td>△</td>
<td>☎</td>
</tr>
<tr>
<td>IC cards</td>
<td>☎</td>
<td>☎</td>
<td>△</td>
</tr>
</tbody>
</table>

◎ : good  △ : not so good  × : bad

Unauthorized Access Surveillance System

The unauthorized access surveillance system includes a surveillance system for preventing unauthorized access to specific facilities from outside and a system for checking the credentials of persons entering the facility via authorized gates. A third system oversees and integrates the first two systems.

The unauthorized access surveillance system has detector sensors located near the fence or other barrier that marks the perimeter of the facility’s property, as well as surveillance cameras for viewing the areas the sensors cover.

The access-egress control system has equipment installed at the gates or doors where visitors are authorized to enter or leave the facility. It includes ID card readers for confirming the information on ID cards concerning the credentials of persons entering the facility.

The control room is fitted with television monitors for monitoring the various systems, computers for displaying various information, and a control console containing the various operation buttons and switches.
comparison of unauthorized access sensors. Even among sensors based on the same principle, there is a need to consider adding to them a sensor check function, or a detector function to prevent tampering.

Various types of surveillance cameras are available, as seen in the comparison in Table 2. Cameras should be selected and used depending on the lighting conditions at their locations as well as the objects they are monitoring. It is also necessary to design the cameras appropriately, such as selecting the camera cases and the platforms to which they will be fitted.

It is important to check the related surveillance camera as soon as feasible after a sensor unit transmits a signal. Among the various methods of doing so Hitachi uses a network based on autonomous distributing for ensuring fast transfer of signals. Utilizing frame memory, meanwhile, a method is used for memorizing still images when a sensor transmits signals.

A wide spectrum of reasons can be input for causing the sensors to transmit signals. For confirming that the sensors are working properly, moreover, a system is used that checks each sensor at least once a day. All such data are stored as log files and can be accessed at any time.

### Table 4. Comparison of Personal Authentication Equipment

This table compares selected personal authentication devices. Hitachi has developed an easy-to-use device that is also difficult to trick with counterfeits.

<table>
<thead>
<tr>
<th>Confirmation of organism</th>
<th>Size of device</th>
<th>Weight of features of object being examined</th>
<th>Areas of application</th>
<th>Future tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint minutia</td>
<td>Per square centimeter</td>
<td>Points per feature</td>
<td>Access/egress control</td>
<td>Access control, wet skin, dry skin</td>
</tr>
<tr>
<td>Hand geometry</td>
<td>Per every 10 square centimeters</td>
<td>Size of palm, length, proportion</td>
<td>Access/egress control</td>
<td>Miniaturization of device</td>
</tr>
<tr>
<td>Iris</td>
<td>About 3 × 3 × 10 cm (camera)</td>
<td>Pattern of iris</td>
<td>Access/egress control</td>
<td>Access control</td>
</tr>
<tr>
<td></td>
<td>About 30 mm × 15 mm (microphone)</td>
<td>Voice wavelength, speed of sound generation, for visitor access/egress/leaving early control</td>
<td>Access/egress control</td>
<td>Susceptibility to health condition</td>
</tr>
<tr>
<td>Face</td>
<td>Square centimeter (tablet)</td>
<td>Order of lines, writing speed, and shape of letters for access control</td>
<td>Access control</td>
<td>Countermeasures for forged signatures</td>
</tr>
<tr>
<td>Signature lines</td>
<td>Per square centimeter</td>
<td>Shape of vein</td>
<td>Access/egress control</td>
<td>Susceptibility to health condition</td>
</tr>
</tbody>
</table>

### Access/egress Control Systems

Access/egress control systems fit into either of two general categories: card systems, and gate systems.

Table 3 shows a representative type of card system. Magnetic cards were mostly used at first in these control systems but IC cards, with their large capacity and high level of security for stored data, can be expected to become the mainstream products in the future. For methods such as those using disposable cards, many types of two-dimensional disposable barcode cards are available and can be expected to be used. As introduced in another article of this issue, there is new type of a card used as an access control system that combines RFID (radio-frequency identification) and infrared radiation.

Next, let us discuss access/egress control gates. These gates are particularly effective when the number of authorized persons entering/leaving a facility increases above a certain level, thus making manual control difficult. There are various types of gates. Those providing the highest level of security use extra-strength doors, while the simplest gates are like the passenger wickets at train stations. The most important point concerning gates is that their functions differ widely depending on whether they are manned or not. If a gate is unmanned, the card used will have to include
a function for authorizing passage of each person, and
the gate will have to be designed so that it cannot be
easily bypassed, such as by climbing over it.

Fig. 2 shows an access/egress control gate with a
function for checking the carrying out of valuables. In
the future, the system is expected to be utilized for
goods control using RFID.

For the purpose of identifying the persons passing
through an unmanned gate, personal authentication
devices can be used.

Table 4 compares selected personal authentication
devices. Hitachi has developed an easy-to-use device
that is also difficult-to-trick with counterfeits. It
enhances live finger recognition, for example, by using
finger vein authentication.

Hitachi decided to develop a device that enhances
live finger recognition by using finger-vein authenti-
cation because it provides a low error rate and meets
with little resistance from users. The use of this device
is expected to expand in the future.

Personal authentication devices will become more
familiar to a wider audience as they are gradually used
more often in financial institutions and for purposes
such as verifying passports.

An important point in access/egress control systems
is the ability to know at all times where persons are
inside a facility after having been granted access.
Knowing the location of persons inside a facility:
(1) prevents double usage of their cards, and
(2) allows a quick search and pinpointing of each
person’s whereabouts if an emergency situation
develops.

In order to know the whereabouts of all persons
inside a facility at all times, the central system utilizes
an autonomous distributed management system for
high-speed processing.

Control Room

The control room includes television monitors for
confirming images sent from the unauthorized entry
surveillance system cameras. Each person in the
control room should be in charge of no more than 3–4
television monitors, and the monitors should always
display images from the surveillance cameras in
predetermined cycles. When a sensor transmits a
signal, the system automatically switches to the images
being sent from the related surveillance cameras.

In the most up-to-date systems, frame memory is
used for constantly memorizing images from each of
the cameras cyclically. When a sensor transmits a
signal, the constant cyclic monitoring is stopped, the
image on the related monitor at the time the sensor
signal was sent is confirmed, and the cause of the signal
is correctly determined.

Related to the access/egress control system, the
console in the control room is fitted with buttons for
operating each gate and has monitors connected to
surveillance cameras that monitor the gates and their
surrounding areas. It is especially important to
establish a method for confirming whether or not an
ID card belongs to a specific person when an error is
generated at a control gate related to confirmation of
a person’s access qualifications.

SYSTEMS IN FUTURE

Devices for Detecting Dangerous Objects

Key facilities are expected to increase their level
of security in the future, and they might add explosives
and chemicals among the hypothetical threats. For
those reasons, it will become more important in future
systems to include devices for detecting dangerous
objects.

Ideally, bulk-type X-ray devices and trace-type
devices for detecting dangerous objects should both
be utilized. Hitachi is developing products in both
categories, and in the future will provide solutions that
integrate new products into security systems used up
to now. The bulk-type X-ray devices and trace-type
devices are introduced in another article of this issue.

X-ray Equipment for Use in Inspecting Motor
Vehicles

As a product for more effective inspection of motor
vehicles that enter the precincts of key facilities,
Hitachi is currently developing X-ray equipment for viewing an entire vehicle at one time.

Other Equipment

Other equipment that might be mentioned is an image-processing sensor included in the group of sensors for surveillance of unauthorized entry.

When image-processing sensors are used outdoors, special care should be taken in choosing the installation location in areas where it frequently snows or is foggy. Such installations are not easy but when successful the sensors are quite effective.

Also, as the use of electronic passports and electronic driving licenses becomes more widespread, the use of personal authentication systems is also expected to increase. Hitachi is therefore continuing its development of such systems.

CONCLUSIONS

As described above, Hitachi has developed a variety of security systems including bulk-type X-ray using new technology and trace-type devices for detecting dangerous objects. Moreover, in the field of access/egress control, we have developed an access-control system that utilizes RFID and infrared radiation and a finger-vein authentication system making Hitachi one of the new manufacturers that can provide a total physical security system.

It was said in the past that systems and their equipment became more difficult to use when the level of security was increased. For its part, Hitachi will continue to develop systems and equipment that will be easy to use even as the level of security is increased.