Highly Secure, User-Friendly Physical Security for Tatebayashi System Center

● Hijiri Kawakita

The system departments in companies and government offices where information technology (IT) is rapidly evolving face various issues as they come to own an increasing number of servers. In particular, they must procure appropriate equipment and implement disaster-prevention and security measures to ensure stable server operation. However, arranging for robust electrical and air conditioning facilities that can withstand earthquakes, fires, and other calamities and implementing strict security measures on one's own can be extremely costly. Consequently, the demand for data centers has been growing in various industries and the data center market has been expanding in recent years. To remain competitive in this market, Fujitsu places considerable importance on physical security at its system centers so that customers can rest assured that their IT resources are safe and secure. This paper introduces the advanced physical security features of the new annex of Fujitsu's Tatebayashi System Center, located in Gunma Prefecture in Japan, which opened in November 2009.

1. Introduction

The growing demand for the outsourcing of information technology (IT) resources is being driven by a variety of problems affecting operations management such as the difficulty in securing space for an increasing number of servers and the need to procure diverse equipment to ensure stable operations. At the same time, there is a growing need for corporate information storage systems with the aim of strengthening internal controls and establishing business continuity plans.[1)] A data center can provide the user with the following advantages.

1) Cost savings compared with securing one's own server space, a stable power supply and air conditioning system, seismic-isolation facilities, and a system for strictly controlling entry into and departure from rooms within one's own company
2) Reduced risk by entrusting the IT resources and operation of facilities to specialists
3) Use of up-to-date equipment in a secure environment appropriate for Cloud computing and software-as-a-service (SaaS) applications without the need to own that equipment

In this way, data center use can be extremely advantageous to a company that aims for flexible business development. Fujitsu's system centers provide high-quality facility management services including stable air-conditioning and power-supply systems and robust security measures to assure customers that their IT resources are safe and secure. These security measures include physical security, which means that access to the IT resources of customers will be accurately and strictly controlled and that unauthorized entry will be prevented even in an environment in which room-access-control doors, server rooms, and even the network are shared

by multiple customers.

This paper introduces the advanced physical security features at the new annex of the Tatebayashi System Center, located in Gunma Prefecture in Japan, which opened in November 2009.

2. Security plans

When considering physical security for an entire site including buildings, one must plan for the installation of security gates, monitoring cameras, and sensors to prevent crime and unauthorized activities. In the plan for the new annex of the Tatebayashi System Center, the first step was to establish security levels within the building and define the flow of people so that locations where such devices should be installed would not be overlooked and security measures would not be duplicated.

2.1 Establishing security levels and defining people flow

The plan divided the site and reception desks, corridors, staircases, server rooms, machine rooms, etc. within the building into various areas on the basis of building boundaries and doorways and established security levels for those areas in an upward, stepwise manner. Moreover, it defined the routes leading to server rooms and other rooms housing critical equipment within the building in terms of people flow according to the classes of users, because, in addition to customers and company technicians, users may also include maintenance personnel, service company employees, and data center employees, and they use different routes.

2.2 Planning security measures

The people flow was used to plan either automatic or ordinary doors for places where the security level changes and where the people flow diverges or converges. Biometric palm-based authentication was chosen to control the opening and closing of those doors through accurate individual authentication. It was considered that setting up automatic or ordinary doors at locations where the security level or people flow does not change would not provide any crime-prevention effect while making operations less user-friendly, so such locations were designed to allow free passage unless other conditions such as legal obligations or air conditioning requirements took priority. Plans for monitoring cameras and sensors were based on similar thinking.

In the above way, an appropriate degree of security could be planned for by first establishing security levels and people flow and then designing actual security measures. In actuality, people-flow control performed on a user-by-user basis is a major feature of the Tatebayashi System Center, and on February 18, 2010, overall security operations at this data center received the highest possible information security rating (AAA) from I. S. Rating Co., Ltd.

3. Security measures in practice

Security measures at a commercial enterprise typically consist of manned monitoring at reception desks and disaster control centers as well as access-right checks at security gates by smart-card authentication. In the case of a data center, however, a server room is shared by a number of customers whose critical information resources are operated and managed in units of server racks. Therefore, since customers with different approaches to security and operations share a server room, there has been a growing demand to apply even stricter security measures to people who work in such rooms. In recent years, we have seen the appearance of anti-tailgating gates, such as flapper gates and circle gates, and elevators in which the floor to stop at can be set for each individual to prevent people from reaching floors unrelated to their work. There has also been an increase in the use of biometric authentication based on the recognition of veins, irises, or other physical characteristics at doorways to sensitive facilities or rooms to

provide tighter entry and exit checks.[2] The Tatebayashi System Center has placed particular importance on admission application and reception management as the initial checkpoints for visitors as well as on server-rack security as the final line of defense for information resources. This section describes integrated physical security at the Tatebayashi System Center beginning with these systems and continuing with room access control and location management, anti-tailgating and anti-impersonation measures, and monitoring by network cameras and video-trail management.

3.1 Admission application and reception management

3.1.1 Admission application system

An admission application system is an important checkpoint for screening a visitor beforehand and allowing him or her entry into the building. The admission application system at the Tatebayashi System Center pays particular attention to a function for accurately registering the applicant/visitor and a function for sharing information about the visitor's work day and type of work to be performed with center employees.

The admission application system includes two important functions: one enables the applicant to request entry into a server room by specifying what is to be done by whom and when and where such work will be done and the other enables designated personnel to check the application, obtain approval from a supervisor, and notify the visitor that permission to enter the building has been granted. As part of this process, information about the server room in which the visitor plans to work and about the type of work to be performed can be shared beforehand with center employees concerned.

The admission application system also uses an in-house public key infrastructure (PKI) authentication scheme linked with personnel information as part of the login and visitor registration. This scheme makes it possible to guarantee that the applicant/visitor is an employee of the company or a related company. It also enables information about the applicant/visitor to be automatically updated even in the face of personnel or organizational changes thereby solving the information maintenance problem. At present, access to the admission application and reception system is limited to Fujitsu personnel, which means that the registration of customers and outside visitors is carried out through company employees or operation managers. There are plans, however, to add a function that would enable admission application to be performed directly over the Internet.

However, the use of such a common, batch-type management system means that the entry of maintenance personnel in the event of an emergency or occasional, unscheduled entry by employees cannot be supported.[3] For this reason, an emergency admission function that limits the entry period and requires subsequent approval from a supervisor has been implemented separately from the normal admission application. This function enables individuals to apply for admission on the spot at times of emergencies, at night, or on holidays and to enter the building quickly as long as the application is in order.

3.1.2 Reception management system

Reception at the Tatebayashi System Center plays an important role as a manned checkpoint for entry to the premises. This checkpoint registers palm-vein data for individual authentication, checks the purpose of the visitor's work and confirms his or her identity, and lends out a security card or radio-frequency (RF) tag to the visitor.

In this regard, there was a need for a dedicated visitor terminal that would enable visitors to register themselves even without reception support. This terminal would have to have a straightforward, user-friendly screen

display for performing registration procedures. To this end, an intuitively easy-to-operate touch panel was chosen and a visitor-oriented registration device for registering biometric palm-vein data accurately and quickly was prepared. A variety of measures have also been taken to make the admission process as short as possible such as a mechanism for registering the palm-vein data of only one hand and the use of previously registered vein data within the period that building entry has been allowed.

In addition, a receptionist must be able to confirm visitors' identities and lend out security cards even under busy conditions when many visitors are trying to register. For this reason, a touch-panel format was chosen for the receptionist's terminal and a function for inputting the identities (IDs) of security cards and RF tags using a barcode reader was prepared. These measures enable fast and accurate reception processing.

3.2 Server rack security

Here, we introduce server rack security at the Tatebayashi System Center. In the past, server racks were locked by keys or combination locks, which were lent out and managed by employees using a paper ledger, or keys and security codes were managed by customers themselves. However, while such a system could effectively lock server-rack doors, key management was still dependent on human skills so the risk of lost keys or unauthorized use was always present.

The Tatebayashi System Center is equipped with special server racks featuring electronically locked handles on the front and back doors. Security for these server racks housing customer servers and network equipment is achieved by locking and unlocking the rack doors through operations performed at a key station (**Figure 1**). This scheme not only limits operation to only preapproved server racks but also simplifies operations greatly by eliminating the complications of physical key management and enabling automatic recording of key usage. To unlock a rack, the user goes to a key station and operates a palm-vein authentication device and a keypad terminal to select the rack to work on and receive permission to unlock it. The user then moves over to that rack before the permission expires and pushes the handle's switch to unlock the electronic key and open the door enabling work to begin. To lock the rack, the user again performs operations at the key station, but in this case, a function is provided to automatically lock the server rack's door after a certain time has elapsed after the door has been closed. This prevents unauthorized use of the rack in the event that the user forgets to lock it.

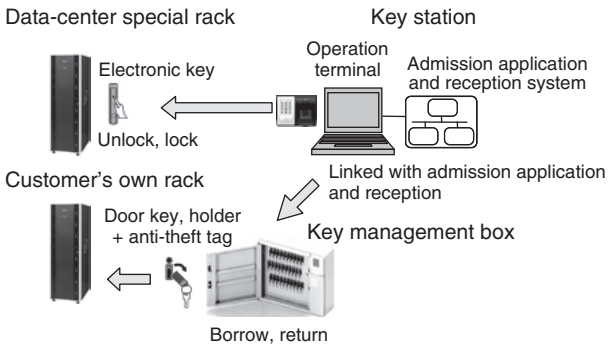

Figure 1
Server rack security scheme.

A key management box is also set up near the key station to lend out and manage keys for locking and unlocking server racks brought in by customers. In this case, the user uses the key station to unlock the door to the adjacent key management box and release the key holder's lock so that the key in question can be borrowed. Then, on completing the desired work, the user again opens the key management box by the same procedure as above and returns the key to its holder. If the key is not returned to the key management box, an anti-theft tag attached to the key will cause an alarm to sound if the key is carried through a security gate (Figure 1).

Server racks and key management boxes that can be controlled from key stations are

linked with the admission-application and reception systems. A server rack or key for which permission has not been provided beforehand cannot be selected, which prevents that key from being borrowed. In addition, by uniformly managing the operation history of the key station and the video obtained by monitoring cameras to record a trail of key borrowing and returning, and by deterring unauthorized rack operations by monitoring cameras and linking recorded video with rack operation history, it has become possible to accurately determine who worked on what rack at what time.

3.3 Room access control and location management

3.3.1 Room access control

For introducing user-friendly biometric authentication, security gates at the Tatebayashi System Center, which are placed at various locations throughout the building, combine RF tags and biometric authentication equipment so that a user need only hold up the palm of one hand to be authenticated and gain access. The mechanism behind this process is as follows. When a user approaches a security gate, the ID stored on the RF tag carried by the user is automatically read by the RF-tag receiver indicating to the system that someone is near the gate. Next, the palm-vein data obtained when the user places his or her palm over the equipment is compared with previously stored data using the RF-tag's ID as a search key. If authentication is successful, the gate is unlocked and the user is granted passage (**Figure 2**).

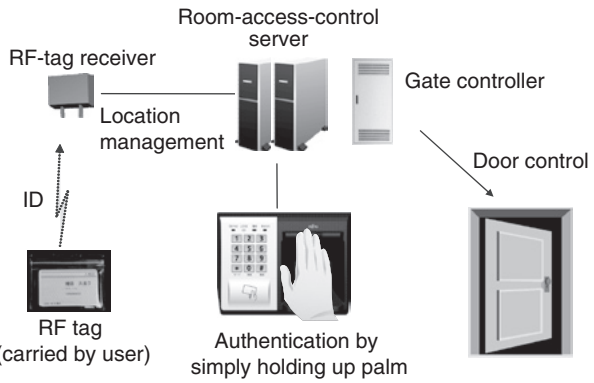

Figure 2
Smart biometric security gate system.

3.3.2 Location management

In addition to the security gates described above, RF-tag receivers are placed at locations where the flow of people concentrates such as corridors and elevator halls so that user locations can be detected in real time. This location management function enables actual behavior patterns to be recognized such as a user's presence in an area of no concern to him or her or failure to enter a room despite being authenticated by biometric authentication equipment. Looking forward, there are plans to use such RF-tag-based human-location detection technology not only for security purposes but also for the sake of user safety and convenience.

3.4 Checking for tailgating and impersonators

The Tatebayashi System Center incorporates a function for preventing tailgating and impersonators in the anteroom leading up to the server room (**Figure 3**).

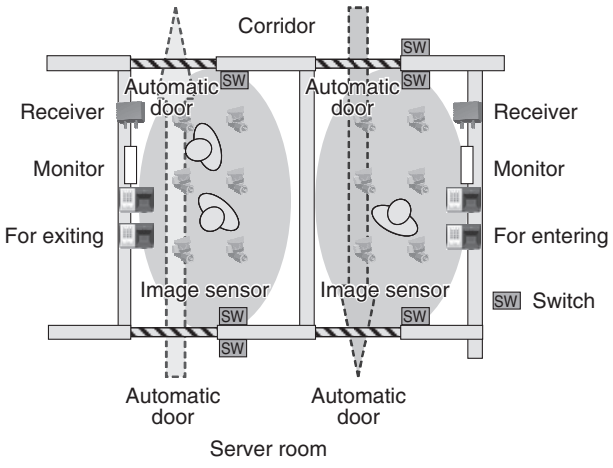

Figure 3
Checking for tailgating and impersonators (separated type).

Once all people of a group intending to enter a server room have entered the anteroom and the automatic door has closed, an image sensor is used to count the number of people and RF tags are used to determine exactly how many people are in the anteroom. If the number of people counted using the image sensor and the number of RF tags fail to match, the system judges that tailgating might have occurred and it denies the group entry to the server room. Likewise, if the anteroom includes a person who is determined through RF-tag detection to have no right to enter that server room, then entry is denied. However, if the results of these checks turn out normal and all users in the anteroom pass a palm-vein authentication test, then the automatic door on the side of the server room will open, allowing entry into the room.

At the Tatebayashi System Center, this mechanism for preventing tailgating and impersonators is provided not only on the anteroom for entering but also on exiting the server room, which leads to accurate and thorough room access control in both directions.

3.5 Monitoring by network cameras and video-trail management

In the world of surveillance, network cameras are becoming mainstream thanks to their ease of installation, low price, and good quality. The Tatebayashi System Center was the first to construct a video monitoring system based on a large-scale Internet protocol (IP) network consisting of more than 300 cameras. This IP network is used for video-gathering, realtime-monitoring, video-storage, and video-playback purposes, and the application of appropriate packet control prevents the generation of block noise or frame loss, leading to a high-quality video monitoring and storage system. The system performs video monitoring without any blind spots at security gates or inside server rooms, focuses the monitoring on scenes consisting of human figures, and records as primary raw data in a high-quality format at several frames per second. In addition, recorded video is recompressed according to the H.264/AVC protocol, enabling long-term storage in excess of one year. Video data is archived on hard disks so that it can be searched and retrieved quickly at any time to play back specific scenes. Also provided is a video-trail management function that links the recorded video with the room-access history and plays back that video in the event of an unforeseen incident (**Figure 4**).

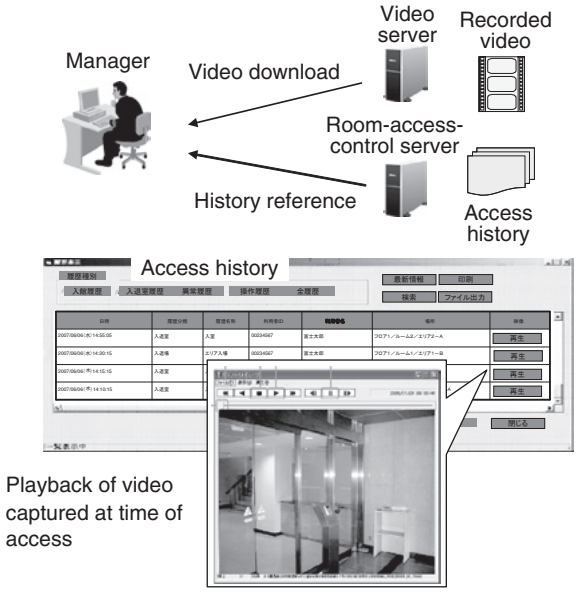

Figure 4
Scheme for access history linkage between security gate and monitoring system.

For more details on checking for tailgating and impersonators and monitoring by network cameras and video-trail management, please refer to "Advanced Physical Security Using Imaging Technology,"[4] in Special Issue 2 Video Processing and Solutions in the January 2009 issue of *FUJITSU*.

4. Outlook for next-generation data centers

In future data centers, the spread of Cloud computing and SaaS will enable system environment configuration, server resource

allocation, and other management tasks to be performed remotely. As a result, there will be fewer occasions to enter a server room to set up servers, add equipment, and perform other work than in the past.

Thus, as data center operations progress toward a labor-saving format by remote management and ultimately toward an unmanned environment, the requirements of physical security will also come to change. In the future, more emphasis will be placed on robustness and confidentiality, checks on carried articles will be intensified, captured video will be subjected to image processing, and monitoring will be made more efficient to minimize risk. In short, the trend will be toward greater use of visual countermeasures. Furthermore, since the number of employees and workers at the data center will decrease, more measures that take efficiency and safety into account will become necessary.

For example, data centers may come to apply methods similar to those used at airport security gates, such as the use of metal detectors or X-ray imaging equipment to strengthen checks of carried articles or a mechanism using a full-body scanner to enhance the detection of media concealed in pockets or wedged in documents. These techniques all involve imaging, and in the future, we can expect the application of image processing to lead to more advances such as the automatic detection of unauthorized articles to prevent such articles from being overlooked.

Moreover, as the outsourcing business goes global, the requirements of physical security demanded by customers will come to include those not considered for domestic outsourcing. Given the same conditions as exist overseas, there will also be a need for site-security measures to protect buildings and infrastructure from unlawful entry and terrorist activities.

Here, however, while data center employees and users may comprehend the need and role of such security measures, a feeling of being overly controlled may take root, which could lead, in some cases, to unpleasant feelings and a drop in work efficiency. However, if such security measures were to guarantee safety and security while being user-friendly in their implementation, users would come to fully understand the need for them. For example, we can consider a disaster-prevention function that, in the event of an incident like an earthquake or fire, checks on the status of users and safely evacuates them from the premises, or a function for slowing down the opening/closing speed of automatic doors when a user in a wheelchair enters a room and guiding that user to an appropriate target area. Implementing functions like these should solve the problem described above.

In this way, the field of next-generation data centers that will deal with advanced IT will demand physical security that excels in high-security, user-friendliness, and safety. This trend will need to be watched closely from here on.

5. Conclusion

We introduced the advanced and robust physical security features of the Tatebayashi System Center showcasing actual examples of their implementation. When choosing a data center, customers often cite user-friendliness, robustness, availability, reasonable rates, and safe & secure operations as prime conditions. To ensure that Fujitsu System Centers become their first choice, we will continue to strengthen physical security at the Tokyo, Akashi, and Tatebayashi System Centers and to work on the implementation of advanced security features at the system centers of related group companies.

We can also expect the market for high-security products in the future to include the data centers of other companies that are looking to strengthen internal controls, as well as banks, securities companies, call centers that handle personal and confidential information, research laboratories, and pharmaceutical companies.

The security measures that should be taken by such institutions are quite similar in terms of objectives and solutions, and there are many "components" that can be used in common at the execution level. With this in mind, we plan to organize and modularize the technologies and know-how used at the Tatebayashi System Center in a form conducive to horizontal expansion and to explore opportunities for business expansion.

Hijiri Kawakita
Fujitsu Ltd.
Mr. Kawakita is a systems engineer and has been engaged in the design and development of physical security, mainly for Internet data centers.

References

1) M. Takahashi et al.: Here is the Secret to Using Scarce Data Centers. (in Japanese), Mitsubishi Research Institute Club, Vol. 4, No. 10, pp. 32–35 (2007).
2) A. Okawa: State of Data Center Security. (in Japanese), *A&S JAPAN*, No. 11, pp. 52–56 (2009).
3) R. Kubo: Linking of Access Control Systems with Other Systems. (in Japanese), *A&S JAPAN*, No. 11, pp. 20–25 (2009).
4) H. Shinbori et al.: Advanced Physical Security Using Imaging Technology. (in Japanese), *FUJITSU*, Vol. 60, No. 1, pp. 64–68 (2009).