Overview

Security Solutions Assisting Social Infrastructure Digitalization

Takeshi Miyao
Junichi Tanimoto

1. Digitalization and Security Threats

The rise of the Internet of Things (IoT) is creating a world in which any object can be connected to the Internet. Using smartphones, sensors, and cameras, the behaviors of objects and people are being converted to data and connected to the Internet. By digitally modeling the real world and analyzing and trialing it in cyberspace, digitalization can uncover new value and feed back results to the real world at an unprecedented rate. It is on the brink of creating major changes that will reshape the world's industries and social infrastructure itself.

While the changes being brought by this digitalization will create new value, this positive aspect will come at the price of new security threats.

Governments and industry bodies are responding to this societal challenge by working on problem-solving initiatives. For example, Japan's Ministry of Economy, Trade and Industry is working on identifying the challenges facing cybersecurity and drafting relevant policies by creating an organization of industry leaders and Internet innovators called the Study Group for Industrial Cybersecurity[(1)]. Collaborative public/private-sector efforts are also on the rise, with the Japan Business Federation releasing a statement entitled A Call for Reinforcement of Cybersecurity To Realize Society 5.0. It sets forth approaches to solving cybersecurity problems by outlining the issues for industry to tackle and making government policy recommendations[(2)].

These moves come in the wake of security threats that have surfaced recently, such as the WannaCry ransomware attack that wreaked worldwide havoc in 2017.

2. Hitachi Initiatives and Security Vision

Hitachi was one of the victims of the WannaCry ransomware attack and suffered actual damage as a result. Responding to the attack has revealed the need for the following two activities:

(1) Reviewing how large-scale systems are used in the IoT era

(2) Examining business continuity plans from the standpoint of both natural disasters and cyberattacks

The fact that IoT devices were the entry points for the attack on Hitachi led to a number of realizations: Control units running on infrastructure systems are just as exposed to security threats as IT devices. When incidents occur, it is important to consider how to respond to them from a business continuity perspective instead of just creating protections against cyberattacks. Planning how to create preventive measures in advance is also important. Turning these realizations

Table 1 — Challenges for Carrying out Cyberattack-ready Business Continuity Plans

Putting lessons learned from the ransomware attack into practice will require responses involving the areas of governance, organizations, technology, and human resources.

Governance	Creating business continuity plans anticipating cyberattacks as well as natural disasters; carrying out risk assessments
Organizations	Enabling business continuity decisions when incidents arise by creating cross-departmental structure enabling collaboration between information/site departments
Technology	Helping to monitor, detect, analyze, and deal with incidents; creating security systems designed for business continuity and rapid recovery
Human resources	Staff training providing expertise in both security and business and control systems

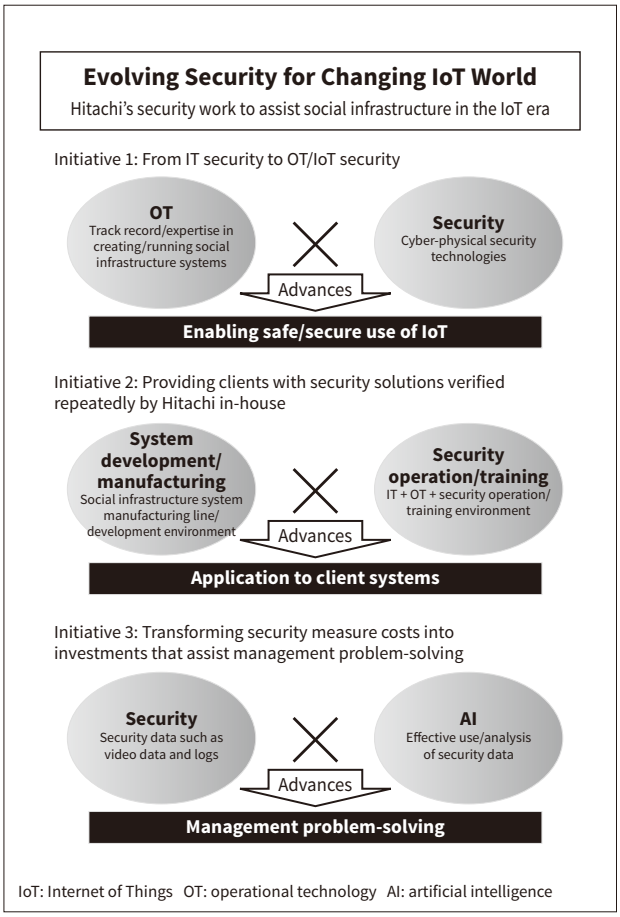
into actual security measures will require responses involving the areas of governance, organizations, technology, and human resources (see **Table 1**).

Governance measures will need to augment business plans created to anticipate natural disasters to develop plans that include contingencies for cyberattacks. For organizational measures, an important requirement will be enabling business continuity decisions when incidents occur by creating a cross-departmental structure enabling collaboration between the information departments in possession of the security technology and the front-line departments doing the actual work. For technology measures, the key will be to contain self-replicating viruses by helping to monitor, detect, analyze, and deal with them, and creating security systems designed for business continuity and rapid recovery. The major requirement for human resources measures will be staff training that provides expertise in both security and business and control systems, enabling responses that make sense from a business continuity standpoint when incidents occur.

To deal with the issues above, Hitachi has created a vision of security entitled Evolving Security for Changing IoT World. This vision is designed to create security advances using the initiatives described below (see **Figure 1**).

Figure 1 — Hitachi's Security Vision

The diagram illustrates the three initiatives Hitachi is using to make advances in security designed to help ensure business continuity for infrastructure.



2. 1
Initiative 1: From IT Security to OT/IoT Security

Hitachi has created several infrastructure systems for customers in areas such as power, rail transport, gas, water, manufacturing, ICT, finance, and public utilities. The experience and track record it has accumulated in these areas are important resources for implementing security measures. But creating useful social infrastructure system security measures requires more than just an understanding of the security technologies themselves. It is also essential to understand how systems are operated and how those operations should be protected. Safety and business continuity are the key elements of operational technology (OT)/IoT security. It is important for systems to work

normally and to provide services securely and continuously. Applying infrastructure-building experience to security is crucial.

2. 2
Initiative 2: Providing Clients with Security Solutions Verified Repeatedly by Hitachi In-house

Hitachi has constructed and possesses a wide range of security verification environments. It verifies IT security by operating IT infrastructure used internally by about 300,000 Hitachi Group users, performing security operations and monitoring on a routine basis. Hitachi also provides a security operations center (SOC) service to clients in 45 countries. It is provided through four worldwide bases and supports four languages (English, French, Spanish, and Japanese). Hitachi is also working to improve its in-house infrastructure in response to the lessons learned from the recent ransomware attack.

By developing and manufacturing social infrastructure systems, Hitachi is building up a track record and expertise in OT security as well, through repeated verification in-house.

2. 3
Initiative 3: Transforming Security Measure Costs into Investments that Assist Management Problem-solving

By applying artificial intelligence (AI) and analytics technology to security, Hitachi is transforming security from something previously only considered a cost, into an investment in management problem-solving enabled by means such as improvements in business efficiency.

For example, monitoring operations involve the labor-intensive task of continually checking massive volumes of log information, and are difficult to handle by staff who are unskilled in security. Applying AI technology to log analysis can increase the efficiency of that work.

Similarly, real-time monitoring of large volumes of simultaneously generated video data is difficult for human operators, but can be done in real time using AI technology. This technology can be used to analyze human behaviors to increase security and improve work efficiency.

AI technology-driven predictive detection and behavior analysis will make it possible to have responses to security incidents ready in advance. System and service shutdowns after incidents incur massive costs for restoring and recovering of routine quality. Detecting small anomalies and responding to them proactively will increase business continuity and preserve management quality.

3. Cyber-physical Security Solutions

To benefit from the lessons learned from the recent ransomware attack, Hitachi is implementing its security vision by starting to provide security solutions that incorporate both cyber and physical elements.

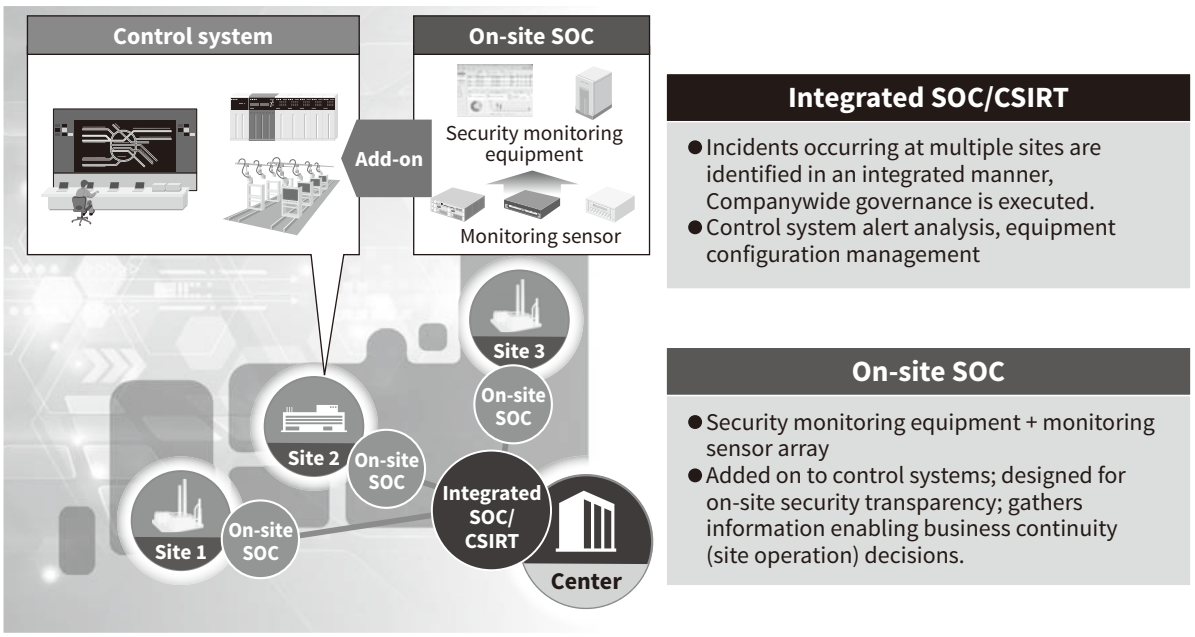
To execute business continuity plans that anticipate cyberattacks and protect IoT devices from these attacks, Hitachi is providing solutions for integrated security monitoring, IoT security (IoT device management), and area security.

Integrated security monitoring is a solution designed to assist with the business continuity of infrastructure business areas. The security operations it implements cover both IT systems and OT/IoT systems. It starts by defining the division of duties between the central organization and site organizations. The central organization's duties are to execute governance, monitor conditions at multiple sites, and gather intelligence information and security staff. The duties of the sites are to assess business continuity (site operation) by adding security monitoring to previous monitoring operations, and to work on site security transparency. To carry out these duties, Hitachi has started providing solutions in the form of integrated SOC/Computer Security Incident Response Team (CSIRT) and on-site SOCs (see **Figure 2**).

The challenge facing IoT device management done for IoT security is determining how to execute security responses under conditions of long life cycles with 24-hour operation, which makes shutdowns difficult. The recommended solution for this is a zone design approach (see **Figure 3**) that anticipates equipment such as devices to prevent intrusion and detects unauthorized connections being installed in a way that includes control equipment unsuited to issuing

Figure 2 — Center and Site Duties for Integrated Security Monitoring

Hitachi provides an integrated SOC/CSIRT solution for performing center duties, and an on-site SOC solution for performing site duties.



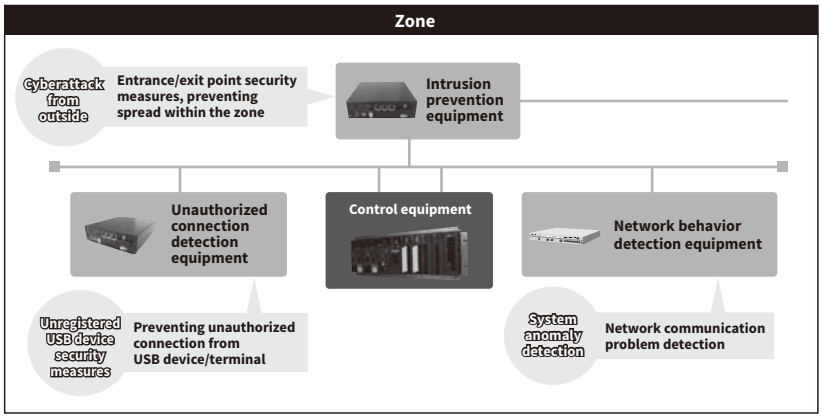
SOC: security operations center CSIRT: Computer Security Incident Response Team

patches. **Figure 4** illustrates an example system configuration for the manufacturing industry.

Area security is a solution that protects a given region (area) by applying technologies such as video and biometric authentication to gather and store security information for crime/disaster prevention applications. It can be used to enable greater transparency in the entire area, to improve security through image analysis and AI coordination, and to help ensure security and optimize business operations (management problem-solving efforts). Hitachi's finger vein recognition technology is one of the elemental technologies used in this solution. It has been well received for benefits such as its authentication accuracy and authentication speed, and is being used increasingly overseas for physical security applications.

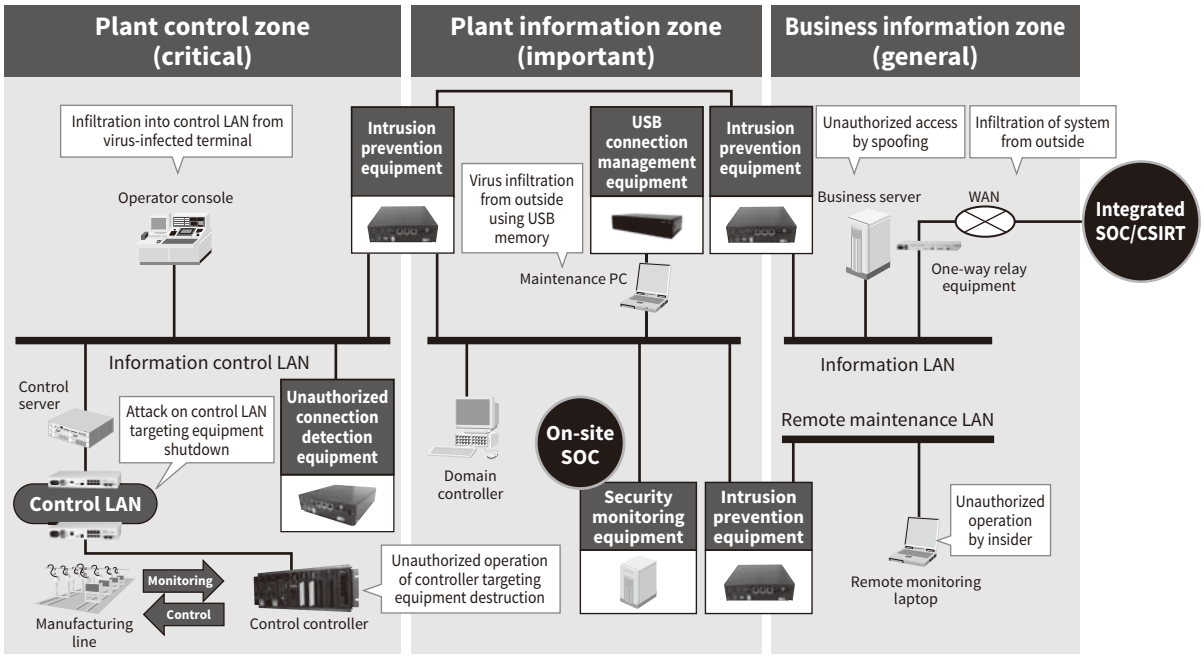
Figure 3 — Example of the Zone Design

Security in the zone is ensured by installing equipment such as intrusion prevention devices and detecting unauthorized connections in a way that includes control equipment that is unsuited to normal security measures such as operating system updates and issuing of security patches.



USB: universal serial bus

Figure 4 — Example of Integrated Security Monitoring for the Manufacturing Industry
The example system configuration shown here applies the zone design and integrated security monitoring to the manufacturing industry.



LAN: local area network WAN: wide area network

4. Human Resources Training and Integrated Cyber Security Training

Initiatives to train security staff are becoming widespread. One example is the Industrial Cyber Security Center of Excellence (ICSCoE) created in April 2017 by the Information-technology Promotion Agency, Japan (IPA). Actual curriculum-based staff training began in July, and Hitachi is also taking part to provide staff training[(3)].

Staff members are being trained through practical exercises at Hitachi, Ltd. Omika Works that develops and manufactures infrastructure systems. Here, programs that create and use systems simulating the actual systems of infrastructure providers are being used to check and verify improvements in cyberattack-ready business continuity plans covering organizational administration and system operation. Omika Works has also started providing Integrated Cyber Security Training Services for staff training designed to create experts in both security technologies and business and control systems.

5. Collaborative Creation and Management Problem-solving with Clients

Hitachi will continue making advances in security adapted to digitalization, working to protect the services and business areas provided by its clients. This work involves efforts to find genuine solutions to management issues by uncovering how the services provided by the client are created and run, and then working with the client to review and refine them.

Security is not simply a cost. By assisting client problem-solving, it helps increase efficiency and improve quality, creating management returns as a form of investment. To help clients minimize and optimize their investments, Hitachi will continue to draw on its expertise in creating and running corporate infrastructure systems to pitch solutions that outline how far to take security measures over the short, medium, and long terms. The platforms it provides allow clients to start implementing security on a small scale with a low initial investment, enabling progressive system expansion in the future.

Hitachi will continue to work alongside clients to create business advances by approaching security from a corporate manager's perspective.

6. Conclusions

This article has looked at Hitachi's work on the security issues that infrastructure systems need to address in an era of increasing digitalization.

The cyber and physical elements of specific solutions that have arisen from this work are described in detail in the other articles of this feature issue.

References

1) Ministry of Economy, Trade and Industry News Releases, "Study Group for Industrial Cybersecurity to Hold Its First Meeting (December 2017)," (Dec. 2017), http://www.meti.go.jp/english/press/2017/1226_004.html
2) Japan Business Federation (Keidanren), "A Call for Reinforcement of Cybersecurity To Realize Society 5.0 (December 12, 2017)," (Dec. 2017), http://www.keidanren.or.jp/en/policy/2017/103_summary.pdf
3) Information-technology Promotion Agency, Japan (IPA) Press Release, "Industrial Cyber Security Human Resources Development Facility Startup in July, Recruitment of Students Begins February 20," (Feb. 2017), https://www.ipa.go.jp/about/press/20170208.html in Japanese.

Authors

Takeshi Miyao
Security Businesses Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* General management of security businesses.

Junichi Tanimoto
Security Businesses Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Planning of security businesses.