Overview

Hitachi's Social Infrastructure Defenses for Safety and Security through Collaborative Creation with Customers

Takeshi Miyao
Toshihiko Nakano, Ph.D.

ADVANCES IN SOCIAL INFRASTRUCTURE SYSTEMS AND ASSOCIATED GROWTH IN THREATS

THE social infrastructure that underpins daily life and business is required to ensure service continuity even during times of difficulty. Many different types of services, including government, finance, and healthcare as well as electric power, gas, water, and railways, are expected to provide 24-hour/365-day uninterrupted operation, or at least to maintain a bare minimum of essential services at all times.

Social infrastructure systems are steadily advancing and seeking to improve efficiency, increasingly operating over wide areas, with interoperation between different providers and use of systems based on the Internet of Things (IoT). Meanwhile, it is also true that the incidence of damage-causing attacks on social infrastructure systems is rising, with an increase in the number of terroristic incidents taking place overseas and a greater diversity of cyber-attacks.

This article presents an overview of what Hitachi is doing to coordinate social infrastructure to protect it against security threats by sharing ideas with social infrastructure companies based on Hitachi's concept of collaborative creation.

ENVIRONMENT SURROUNDING SOCIAL INFRASTRUCTURE

Security Measures Taken by Japanese Government and Industry Bodies

Measures taken by the Japanese government to deal with cyber-attacks on social infrastructure involve the different government ministries and agencies coordinating their activities primarily through the National center of Incident readiness and Strategy for Cybersecurity (NISC)[a]. This includes the Basic Act on Cybersecurity[b, (1)] enforced in January 2015, the fourth edition of Principles for Formulating of "Safety Standards, Guidelines, etc." concerning Assurance of Information Security of Critical Infrastructures[(2)] in May 2015 and Cybersecurity Management Guidelines issued by the Ministry of Economy, Trade and Industry issuing[c, (3)] in December 2015. In industry, meanwhile, the Japan Business Federation (Keidanren) issued its Second Proposal for Reinforcing Cybersecurity Measures[(4)] in January 2016, and work continues on implementing cybersecurity in accordance with these laws and guidelines.

Trends in International Standardization for Security

Work is progressing on formulating international standards for control system security to protect social infrastructure as well as for traditional information system security. Examples include the work done on control system security standardization by the International Electrotechnical Commission (IEC), which is formulating the general-purpose IEC 62443 security standard for control systems. This standard, particularly IEC 62443-2-1, includes rules

(a) National center of Incident readiness and Strategy for Cybersecurity (NISC)
An organization established in January 2015 through the reorganization of the National Information Security Center based on the Basic Act on Cybersecurity enacted in November 2014. Along with handling overall coordination of cybersecurity policy based on the cybersecurity strategy of the Japanese Cabinet, the center is engaged in activities that bring together the public and private sectors aimed at leading the world in establishing a robust and vigorous cyberspace.

(b) Basic Act on Cybersecurity
A Japanese law with provisions that include clarifying the basic concepts and governmental obligations and establishing the core activities and organizational structure for dealing with cybersecurity, with the aim that cybersecurity policy should proceed in a comprehensive and effective manner. The law was passed and enacted by a plenary session of the House of Representatives in November 6, 2014 and came into full effect on January 9, 2015.

(c) Cybersecurity Management Guidelines
These guidelines treat cybersecurity as a management problem for companies, stipulating "three rules" for protecting companies against cyber-attacks that need to be acknowledged by the managers of companies for which the use of IT is essential, and "ten important considerations" whereby management should appoint a chief information security officer (CISO) or other such person to be responsible for information security measures.

on cyber security management systems (CSMSs) for control systems. Along with risk assessment, these cover the staging of drills, physical security, and the establishment of a security organization for CSMSs. Japan has led the world in establishing a certification system for CSMSs, which is now in operation.

Awareness of Challenges Facing Social Infrastructure Companies

The growing diversity and sophistication of cyber-attacks pose threats to the security of organizations that deliver social infrastructure services. The response to these security threats involves utilizing guidelines and other standards to take action with respect to both management and systems. In the case of systems, this means undertaking a risk assessment to evaluate the security threats to social infrastructure systems and the consequences if an incident does occur, and prioritizing the steps to be taken based on the size of the risk. Along with these system-based measures, action on management considerations is also important. While the trend at social infrastructure companies has been to establish company-wide security coordination organizations with responsibility for security measures, they are also looking at ways of achieving a shared awareness with the operational departments responsible for actual security implementation, specific coordination measures, and industry-wide coordination with other companies. In this environment, security measures and their implementation have come to be recognized as genuine issues for management due to the need for coordination between planning departments, information technology (IT) departments, and operational departments, and also the need for activities that involve the wider industry.

HITACHI'S SECURITY CONCEPT

From System-based Measures to Organizational and Operational Responses

While system-based measures are an important prerequisite for protecting social infrastructure against security threats, they are insufficient on their own. The growing sophistication of methods used to mount cyber-attacks makes continuous improvement of systems essential. Also important is to establish the infrastructure needed to quickly identify the location of a problem when an incident does occur, and to respond and recover.

Based on its concept of protection at the system, organization, and operational levels, Hitachi is seeking to implement this concept using its hardening – adaptive, responsive, cooperative approach. This seeks to protect social infrastructure by having a strong platform for implementing security measures (hardening) and using this as a base for continuously strengthening and implementing pre-emptive countermeasures and defenses against new threats at the system level (adaptive), minimizing the damage that results from attacks and shortening the recovery at the operational level (responsive), and coordinating with other organizations and companies at the organizational level (cooperative) (see Fig. 1).

Application to Security of Experience with Building Social Infrastructure Systems

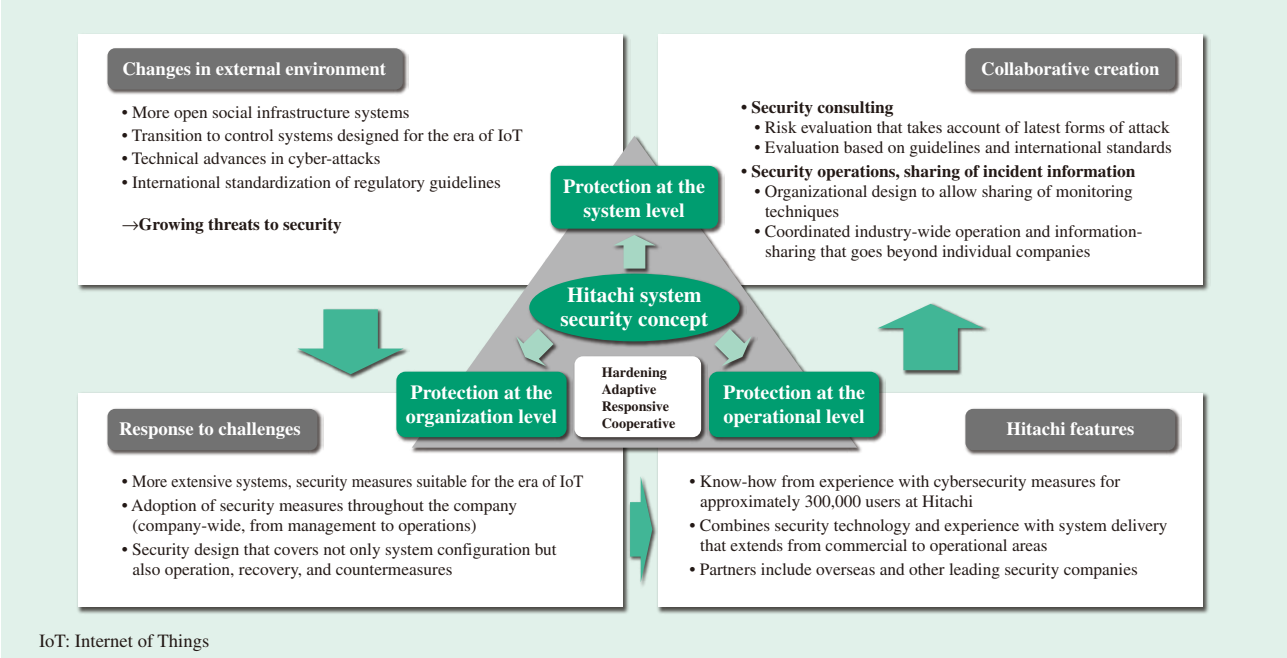
Hitachi has experience with building social infrastructure systems and supplying them to companies in such sectors as electric power, gas, water, railways, finance, and government. What social infrastructure companies require if they are to supply high-quality services are high system reliability and availability. While recent threats of cyber-attack are one of the factors putting quality at risk, they are not everything. Security risks do not exist in isolation and should be assessed and dealt with in conjunction with other sources of risk, such as equipment failure, human error, or natural disaster. Accordingly, the question becomes how to incorporate security measures into overall system operation. Hitachi believes it is essential to make security integral to the service operator's entire operation, including the assignment of security implementation functions to the operational departments responsible for the operation of social infrastructure systems.

Defenses in Depth and Predictive Detection Techniques that Combine Cyber and Physical Features

Social infrastructure systems are increasingly connected indirectly to external networks such as the Internet. Accordingly, while there may be no direct intrusions into social infrastructure systems, the potential still remains for an intruder to gain access by connecting via a number of gateways.

For this reason, defenses in depth and predictive detection practices are being adopted to protect social infrastructure systems.

Defenses in depth involve placing a number of gateways on multiple layers between the social infrastructure system and the outside world. Whether it be in cyberspace or physical space, having multiple



IoT: Internet of Things

Fig. 1—Hitachi Security Concept.
Based on its concept of protection at the system, organization, and operational levels, Hitachi is helping create safe and secure social infrastructure systems through collaborative creation with social infrastructure companies in response to changes in the external environment.

layers of gateways minimizes the risk of system intrusion and makes access more time-consuming, providing more time for the warning signs to be detected (see Fig. 2).

Predictive detection detects signs of a threat, such as when any of the multiple layers of gateways come under attack, or some of these gateways being breached, even if the intrusion has not gotten as far as the social infrastructure system itself. Hitachi has developed techniques for detecting signs of intrusion that utilize things like malware[(d)] detection or whitelist[(e)] systems and combine a number of different techniques. In particular, it is possible to utilize physical security techniques to detect unauthorized behavior from remotely launched cyber-attacks by using techniques

(d) Malware
An abbreviation of *malicious software*, meaning software used in malicious attacks such as computer viruses, spyware, and Trojans. Recent years have seen an increase in targeted attacks such as those that seek to steal confidential information from a specific organization.
(e) Whitelisting
A method used to protect devices against cyber-attack by only permitting certain approved programs to be used. Security is maintained by prohibiting the execution of any unknown malware that gains access to the system. This is in contrast to blacklisting, whereby code or other data that has previously been identified as malicious is detected and excluded.

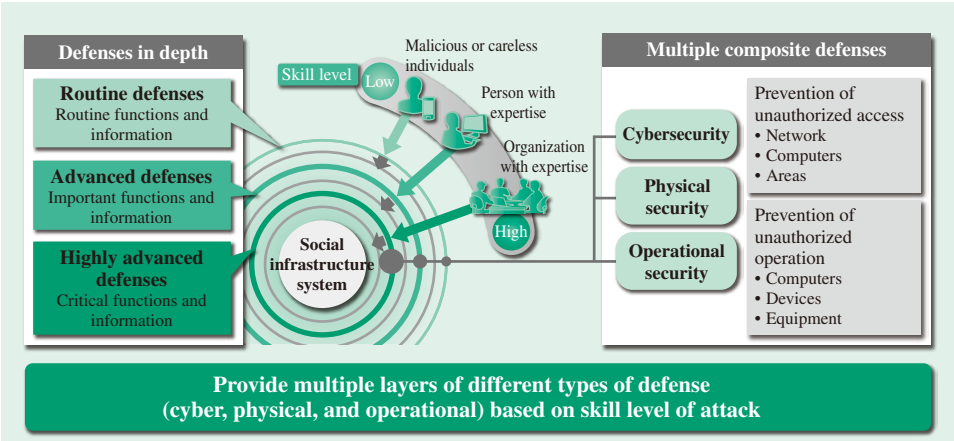


Fig. 2—Multi-layer Defenses.
This means providing multiple layers of defense for social infrastructure systems, with overlapping cyber, physical, and operational measures.

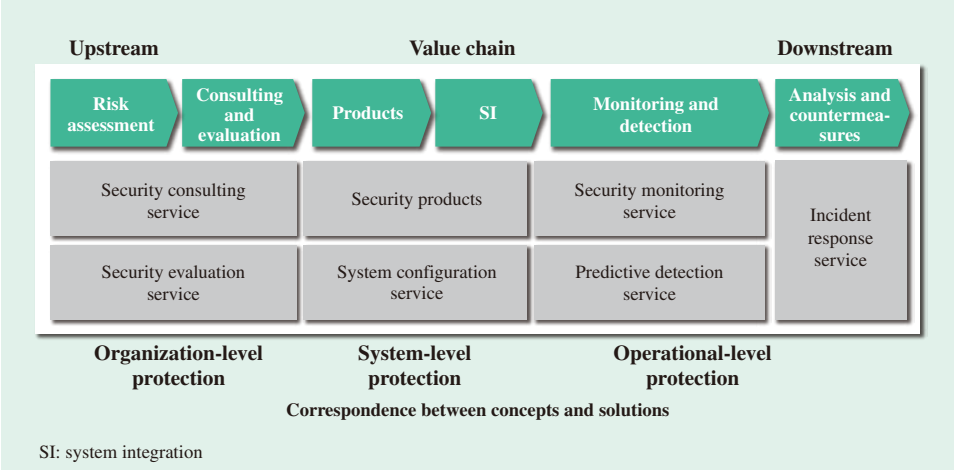


Fig. 3—Hitachi's Security Solutions.
Hitachi supplies solutions in accordance with its concept while also taking a value chain perspective.

that identify the operational staff who work on social infrastructure systems and determine whether the operations they perform are valid by ensuring that specific actions are consistent with those performed by the operator concerned.

Operational Experience from within Hitachi

Hitachi supplies IT infrastructure services to approximately 300,000 internal users of its own, including routine responses and countermeasures against external cyber-attacks. This is the largest IT infrastructure in Japan, with continuous 24-hour/365-day monitoring by specialist security staff. In 1998, Hitachi became the first company in Japan to establish its own internal Computer Security Incident Response Team (CSIRT), and this team continues to handle security operations to this day. Hitachi draws on this operational experience in providing solutions to social infrastructure companies.

Collaborative Creation with Customers

Hitachi operates its Social Innovation Business through collaborative creation with customers. Security is one of the important aspects of this business, and Hitachi works alongside customers to devise and implement responses to the security challenges facing social infrastructure companies in terms of systems, organizations, and operations.

HITACHI'S SECURITY SOLUTIONS

Solutions Based on Hitachi's Security Concept

Based on its concept of protection at the system, organization, and operational levels, Hitachi's approach is to work alongside social infrastructure companies in addressing their security issues. To this end, it supplies security solutions in accordance with this concept while also applying the idea of a value chain to these solutions (see Fig. 3). The upstream end of the value chain involves offering security consulting services that manifest the concept of protection at the organization level. For protection at the system level, Hitachi supplies products that protect social infrastructure systems against security threats and configures them as systems. At the downstream end of the value chain, Hitachi supplies security monitoring, detection, information-sharing, and countermeasures for protection at the operation level. A feature of all this is that Hitachi adopts the standpoint of a social infrastructure operator and supplies solutions that establish a total value chain. The following sections present an overview of specific solutions.

Security Consulting

Hitachi's security consulting includes risk assessment and consulting based on international standards. Along with a thorough knowledge of security technology, the important factors in providing these services include business knowledge about the social infrastructure to be protected and expertise in system configuration and operation. Hitachi has an extensive track record in the supply of social infrastructure systems together with the experience of operating its own in-house IT infrastructure services. A feature of security consulting by Hitachi is its ability to draw on this know-how in the services it supplies to customers.

Products and System Configuration

Hitachi supplies security products for both the cyber and physical realms. In terms of cybersecurity, for example, it provides products and system configuration

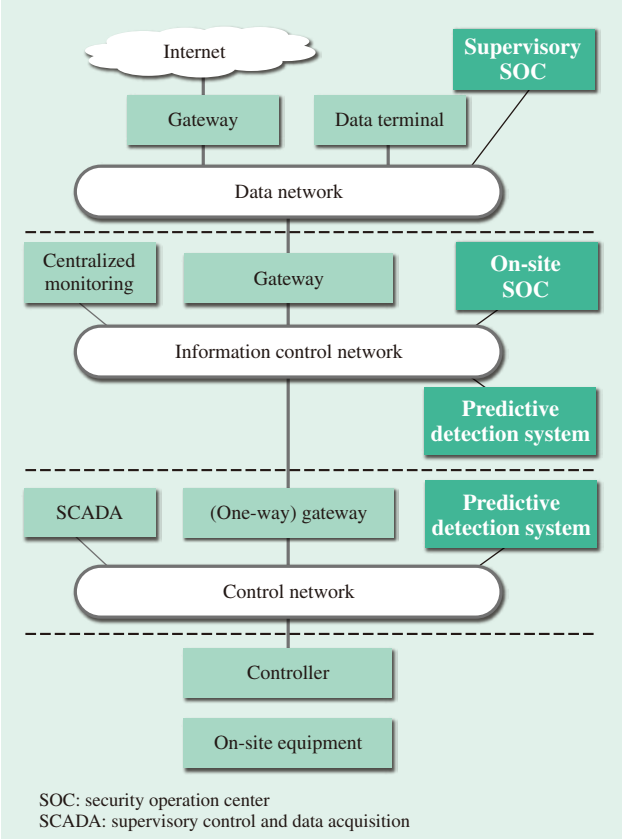


Fig. 4—Security Monitoring Architecture.
On-site SOCs, predictive detection systems, and supervisory SOCs interoperate to form a security operation, monitoring, and detection architecture for control systems.

services including a cloud security service for protecting customer systems, network security for preventing unauthorized access at the network layer, and data security for keeping information safe.

In terms of physical security, Hitachi supplies access control systems that use finger vein authentication(f), video surveillance solutions that use cameras, and an explosives trace detection system for incorporation into security gates. A product that combines both cyber and physical features is a undirectional network device that can protect social infrastructure systems by physically blocking unauthorized cyberspace access from the outside world.

Security Operations Service

Even once a system has been implemented that satisfies the security requirements, protecting social infrastructure requires ongoing monitoring. It is necessary to design reliable security practices that identify threats to security at an early stage and take prompt action. Essential to achieving this are the timely collection of operational data, reliable situation assessment, determination of the correct response, and its rapid implementation.

Hitachi supplies services for establishing security operation centers (SOCs) to perform these steps, operating them on the customer's behalf, supporting analysis by specialists in security technology and experts with operational know-how from Hitachi's own SOCs, and staff training on how to deal with security threats, including the staging of drills.

Hitachi is also developing services for setting up SOCs in social infrastructure systems, particularly for control systems, and for operating them on the customer's behalf. In the case of control systems, because Hitachi has monitoring systems such as supervisory control and data acquisition (SCADA) systems, the requirements include functional demarcation with security monitoring, and functions such as data logging for predictive detection, situation assessment, and identification of causes, and backup and recovery to restore systems quickly. Accordingly, Hitachi intends to expand its security operations services that support the operational departments of social infrastructure companies (see Fig. 4).

Protection of Safe and Secure Social Infrastructure Systems

With the emergence of the IoT, security threats are rising relentlessly along with advances in social infrastructure systems.

Based on its concept of protection at the system, organization, and operational levels, Hitachi is contributing to the creation of safe and secure social infrastructure systems through collaborative creation with many different organizations, including social infrastructure companies, while also drawing on its experience built up by supplying these systems.

(f) Finger vein authentication
A biometric technique for using part of a person's body to verify their identity. Authentication of an individual is performed by identifying the structural pattern of finger veins in an image obtained by shining near-infra-red light through the subject's finger and then comparing it against a set of prerecorded patterns.

REFERENCES

(1) National center of Incident readiness and Strategy for Cybersecurity (NISC), Related Laws and Regulations, http://www.nisc.go.jp/law/ in Japanese.
(2) National center of Incident readiness and Strategy for Cybersecurity (NISC), Activities, Related materials regarding critical infrastructures, http://www.nisc.go.jp/active/infra/siryou.html in Japanese.

(3) Ministry of Economy, Trade and Industry, "METI Formulates the Cybersecurity Management Guidelines," http://www.meti.go.jp/english/press/2015/1228_03.html

(4) Japan Business Federation (Keidanren), "Second Proposal for Reinforcing Cybersecurity Measures," https://www.keidanren.or.jp/en/policy/2016/006.html

ABOUT THE AUTHORS

Takeshi Miyao

Security Business Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of security businesses.

Toshihiko Nakano, Ph.D.

Security Business Division, Social Innovations Business Division, Hitachi, Ltd. He is currently engaged in the development of security solutions. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan(IEEJ).