Overview

Disaster Management and Security Solutions to Usher in the IoT Era

Takeshi Miyao
Toshihiko Nakano, Ph.D.

1. The Bright and Dark Sides of the IoT Era

The emergence of the Internet of Things (IoT) is bringing about a world in which objects of all different sorts are being connected to the Internet. It involves the use of smartphones, sensors, cameras, and other devices to transform the activities of people and things into data and link it to the Internet. With its ability to model the real world in digital form and perform analysis and simulation in cyberspace, the IoT is able to uncover new value at an unprecedented rate and provide it as feedback to the real world. This is set to bring major changes that will extend to the structure of industry as well as the infrastructure of society itself. Thus while the emergence of the IoT gives rise to new value, it also means the emergence of new threats.

In the past, infrastructure such as electric power and railways were not under threat of attack because the systems they used were isolated from external networks. With the use of the IoT to provide more sophisticated services, however, they have now become exposed to security threats. Moreover, new challenges and threats are emerging to which individual companies or other organizations have not previously been exposed. These include the way in which the establishment of large supply chains and other ecosystems, which was made possible by the growing interconnectedness of systems, puts entire systems at risk through the use of security weak points as an attack gateway.

To create a resilient society for the IoT era by building lifestyle platforms that enable people to go about their lives in safety and security, it is essential that adequate security measures be implemented based on an awareness of both the usefulness and threats that come with the IoT.

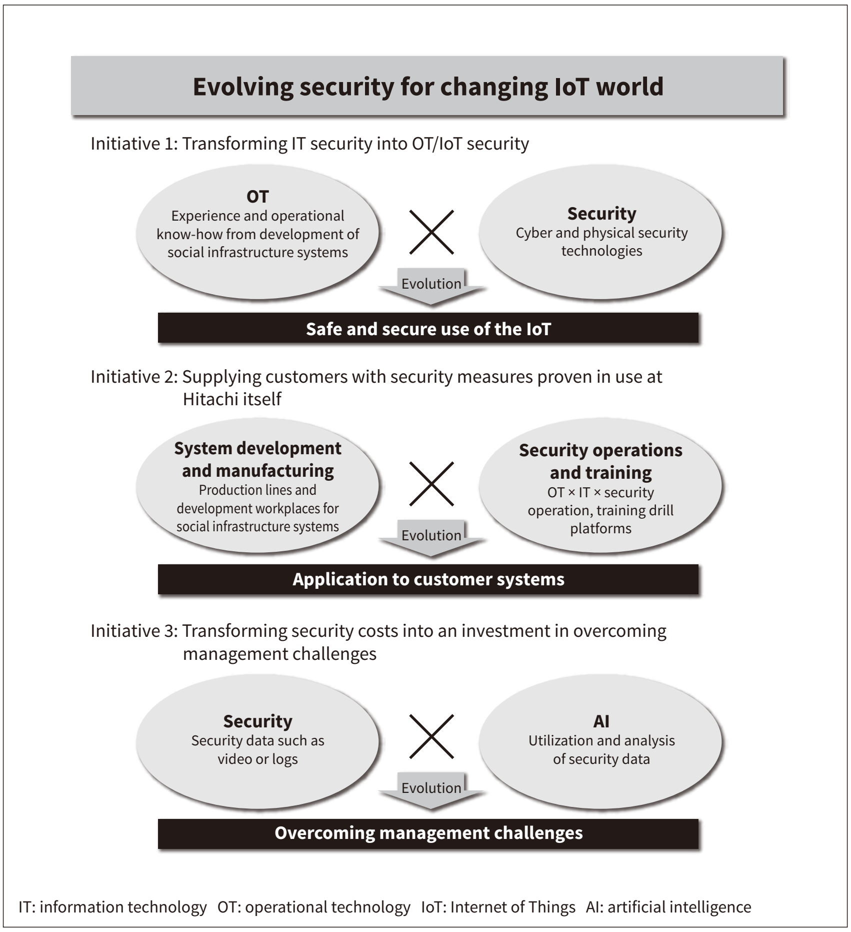
2. Measures for Disaster Management and Security that Evolve in Step with the IoT

To enable customers to move their businesses forward in the era of the IoT, Hitachi supplies solutions that use the IoT for data analysis and resolving management challenges. Underpinning these is Hitachi's Lumada IoT platform. As an IoT platform that provides an open and step-by-step approach, Lumada links a wide variety of different customer systems and data sources to perform sophisticated analyses, thereby accelerating the progress of the business by uncovering valuable insights for business improvement and business creation.

To ensure that the progress of a business is safe and secure, the security needed for the IoT era is provided as one of the core technologies in Lumada. To keep

Figure 1 — Hitachi's Security Vision

To protect customer systems and services in a changing IoT world, Hitachi has embarked on the three different security initiatives shown in the figure.


Evolving security for changing IoT world
Initiative 1: Transforming IT security into OT/IoT security
OT
Experience and operational know-how from development of social infrastructure systems
Security
Cyber and physical security technologies
Evolution
Safe and secure use of the IoT
Initiative 2: Supplying customers with security measures proven in use at Hitachi itself
System development and manufacturing
Production lines and development workplaces for social infrastructure systems
Security operations and training
OT × IT × security operation, training drill platforms
Evolution
Application to customer systems
Initiative 3: Transforming security costs into an investment in overcoming management challenges
Security
Security data such as video or logs
AI
Utilization and analysis of security data
Evolution
Overcoming management challenges

IT: information technology OT: operational technology IoT: Internet of Things AI: artificial intelligence

customer systems and services safe in this changing era, Hitachi is seeking to advance security through a vision of "evolving security for changing IoT world." The following sections describe how it plans to go about this (see **Figure 1**).

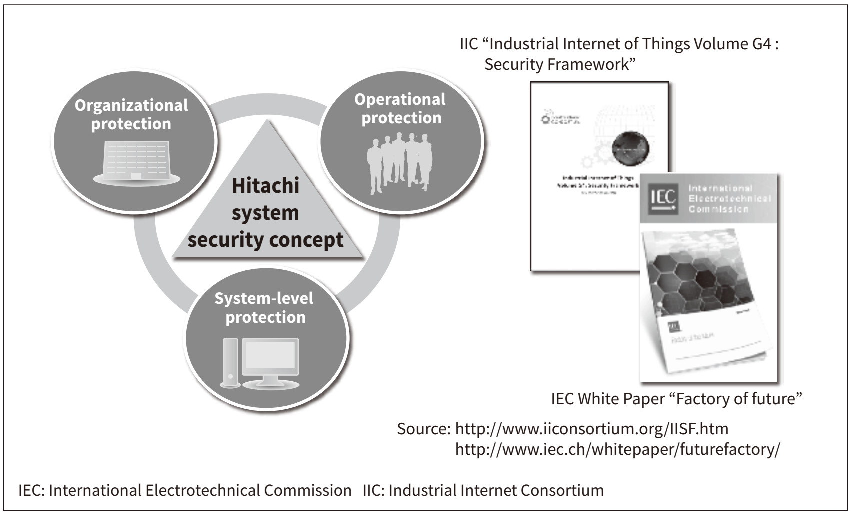
2. 1 Initiative 1: Transforming IT Security into OT/IoT Security

Hitachi has built and supplied social infrastructure systems for customers that include electric power, railways, gas, water, manufacturing, telecommunications, finance, and the public sector. It sees this experience and its past successes as crucial elements in implementing security measures. Security measures for social infrastructure systems are only worthwhile if based not only on security technology but also on an understanding of how systems are operated and how best to protect them given that this is how they are used. Of particular importance in operational technology (OT)/IoT security are safety and business continuity. It is important that systems function correctly and that services are provided safely and continuously, with the application of experience from infrastructure development being a key point in security implementation.

2. 2 Initiative 2: Supplying Customers with Security Measures Proven in Use at Hitachi Itself

Hitachi has put in place a diverse set of environments for trialing security measures. In the case of information technology (IT) systems, Hitachi has experience with operating IT infrastructure for approximately 300,000 in-house users. This experience includes the Hitachi Incident Response Team, the establishment of which in 1998 made Hitachi the first company in Japan to have an in-house computer security incident response team.

For OT security, equipment for security testing and training set up at Omika Works provides a venue for collaborative creation with customers through security training drills.


IIC "Industrial Internet of Things Volume G4 : Security Framework"
Organizational protection
Operational protection
Hitachi system security concept
System-level protection
IEC White Paper "Factory of future"

Source: http://www.iiconsortium.org/IISF.htm
http://www.iec.ch/whitepaper/futurefactory/

IEC: International Electrotechnical Commission IIC: Industrial Internet Consortium

Figure 2 — Hitachi's Security Approach and Involvement in International Standardization

To ensure the safety and security of its customers, Hitachi has adopted a security approach of providing "protection at the system, organizational, and operational levels." Hitachi is also contributing to the international standardization of OT/IoT security, including through the inclusion of the Hitachi system security concept in a white paper by an international standardization body.

For physical security, Hitachi is using and testing walkthrough-style finger vein authentication for premises access control.

In this way, enhancements to security technology are being achieved through in-house testing and the results supplied to customers.

2. 3 Initiative 3: Transforming Security Costs into an Investment in Overcoming Management Challenges

Through the application of artificial intelligence (AI) and analytics to security, Hitachi is transforming the cost of security into an investment in overcoming management challenges such as productivity improvement.

Security monitoring, for example, is labor-intensive because of the need for ongoing checks of a large amount of log data, work that is difficult to perform unless staff have skills in security. By using AI for log analysis, however, the work can be made more efficient.

In another example, the application of AI to the large amounts of simultaneous video data that is collected enables monitoring in real time, something that is difficult to achieve by the human eye. There is also potential for using the analysis of people's actions to make safety and productivity improvements.

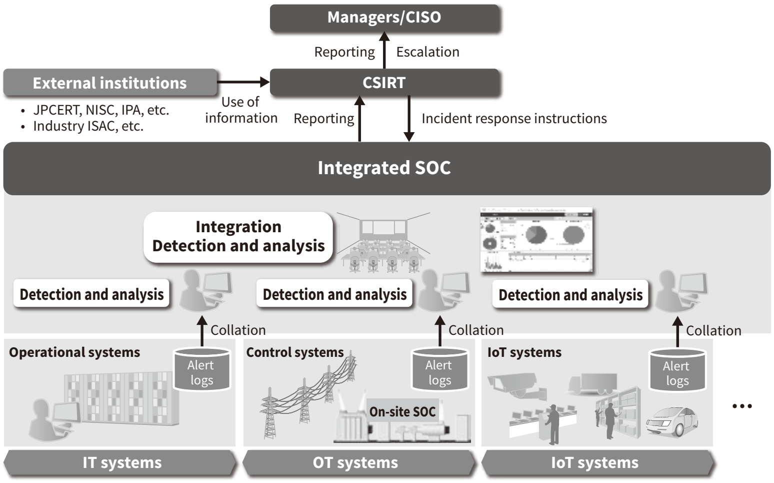
The use of AI to detect warning signs and analyze actions makes it possible to anticipate security incidents. Because the costs of restoring halted systems and services and recovering management quality after an incident are so large, this enhances business continuity and maintains management quality by detecting minor anomalies and responding to them preemptively.

3. Hitachi Disaster Management and Security Solutions that Support Safety and Peace of Mind

To ensure the safety and security of its customers, Hitachi has adopted a security approach of protection at the system, organizational, and operational levels. Along with the development of security systems, Hitachi also provides management systems to keep the functions of these systems in continuous operation and measures for the monitoring and detection of anomalous behavior. It has also developed the Hitachi system security concept to implement and support this work. The concept was proposed to an international standardization body in a white paper and was subsequently adopted. In accordance with its security approach, Hitachi supplies solutions that cover the entire value chain from early-stage security consulting through to system implementation and operational monitoring. Hitachi is also proposing initiatives in which cyber and physical security are combined by transforming solutions for IT systems into solutions for OT and IoT systems (see **Figure 2**).

In particular, to adapt to the IoT era, Hitachi has developed solutions for integrated security, area security, and IoT security respectively.

Here, "integrated security" means solutions that comprehensively and efficiently overcome the



CISO: chief information security officer JPCERT: Japan Computer Emergency Response Team
NISC: National Center of Incident Readiness and Strategy for Cybersecurity
IPA: Information-technology Promotion Agency, Japan ISAC: information sharing and analysis center
CSIRT: computer security incident response team SOC: security operation center

Figure 3 — Overview of Integrated Security

Integrated security provides solutions that overcome the operational challenges inherent to the IoT era, and that are inclusive of CSIRTs and managers. These challenges include security operation and monitoring that covers OT and IoT systems as well as IT systems, merging and boosting the efficiency of the organizations that handle security, and the sharing and utilization of intelligence information.

operational challenges that are an inherent part of the IoT era, including through the use of AI. These challenges encompass security operation and monitoring that extends to OT and IoT systems as well as IT systems, merging and boosting the efficiency of the organizations that handle security, and the sharing and utilization of intelligence information (see **Figures 3 and 4**).

"Area security," meanwhile, means solutions that strengthen security and move the business forward (including business improvement, overcoming management issues, and new business creation) in many different social infrastructure areas that support people's way of life, including power plants, airports, railway stations, public places, factories, and theme parks.

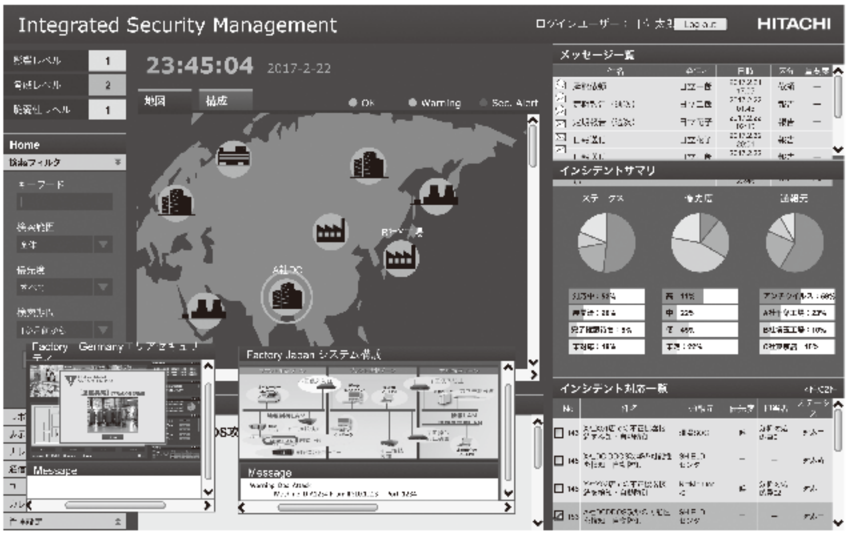
"IoT security" means security solutions aimed at overcoming important security challenges that did not exist in the past but have arisen along with the emerging IoT era. Hitachi is proposing these solutions based on its own unique perspective on IoT systems.

4. Collaborative Creation with Customers and Overcoming Management Challenges

Hitachi is adapting security to the changing IoT era in order to protect the services provided by customers

Figure 4 — Example Integrated SOC Monitoring Screen

The monitoring screen shown here is based on a model of manufacturing plants spread around the world. Alerts and logs from OT, IT, and IoT systems are collated and comprehensive information is displayed together with use of AI.



and their business operations. This involves striving to overcome the genuine challenges faced by management by joining with customers to think about how to move their services forward based on a knowledge of how they build and operate the services they provide.

Security is more than just a cost. Instead it is part of an organization's investment in its own operations that contributes to productivity and quality improvements by overcoming challenges. To optimize investment and keep it to an absolute minimum, Hitachi draws on its know-how in the building and operation of social infrastructure systems to suggest the level of security measures that is best from short-, medium-, and long-term perspectives. It also supplies platforms that can minimize initial investment by starting small and building systems progressively.

Hitachi looks at security from the perspective of a business operator and is standing beside customers to move their businesses forward.

5. Conclusions

This article has described Hitachi's approach to work on disaster management and security solutions for the IoT era.

For a description of specific solutions or research and development work based on these ways of thinking, and examples of their application for disaster management and security, please refer to the articles in this issue of *Hitachi Review* that cover these topics in detail.

References

1) IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, "IoT Security Guidelines ver. 1.0 (Jul. 2016)," http://www.soumu.go.jp/main_content/000428393.pdf in Japanese.

2) T. Miyao et al., "Hitachi's Social Infrastructure Defenses for Safety and Security through Collaborative Creation with Customers," Hitachi Review, 65, pp. 302–307 (Sep. 2016).

Authors

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

Toshihiko Nakano, Ph.D.
Security Businesses Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Development of security for social infrastructure systems. *Society memberships*: The Institute of Electrical Engineers of Japan (IEEJ).