Technotalk

Overall View and Collaborative Creation Activities for a Safe and Secure Society

Kenji Watanabe, Ph.D. Professor of Graduate School of Engineering, Head of Disaster & Safety Management, Nagoya Institute of Technology
Toshihiko Nakano, Ph.D. Security Business Division, Social Innovation Business Division, Hitachi, Ltd.
Akihiro Ohashi General Manager, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd.
Ichiro Ote Business Management Department, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd.
Tadashi Kaji, Ph.D. Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd.
Takeshi Miyao General Manager, Security Business Division, Services & Platforms Business Unit, Hitachi, Ltd.

Threats to the security of social infrastructure systems are on the rise against a background of increasingly sophisticated cyber-attacks and a changing security environment inside and outside of Japan. Social infrastructure, meanwhile, plays a fundamental role in the functioning of society and is called on to maintain service continuity while dealing with a variety of incidents. In response to these challenges, Hitachi supplies security solutions for social infrastructure based on its concept of protection at the system, organization, and operational levels. It intends to continue contributing to the creation of a safe and secure society by supplying total services extending from consulting to products, system configuration, and security operations.

Security Measures that also Encompass Human Systems

Miyao: As the risks facing social infrastructure become more diverse, concerns about security are rising. Professor Watanabe has been engaged for many years in research into practical risk management, having worked in areas such as international standardization and the development of policies for the cybersecurity of important infrastructure. Professor, how do you view the current state of security for social infrastructure?

Watanabe: I was prompted to become involved in research into risk management, business continuity management (BCM), and cybersecurity by major business interruption risks such as natural disasters as well as terrorism and other forms of disorder that I encountered during the time I spent working as a banker in the USA. This is why my research has come to focus on the importance of human systems, which was brought home to me by my first-hand experience of emergency response. There is no point building redundancy into a system if the people on the ground when an incident strikes are unable to take advantage of it.

The nature of risk over recent years has been diverse, extending from terrorism and other criminal acts to natural disasters, infectious disease, system faults, and disruptions in transport services. While being able to deal with all of these different risks and keep services operating is the basis of business continuity management, it is not enough to rely solely on technological measures, including for cyber and physical security. I believe that genuine emergency response can only be achieved by revising and improving human systems, such as business processes, work rules, and operations.

Miyao: Dr. Nakano has been involved in a variety of work on international standardization. Please tell us about recent trends in this area.

Nakano: An emerging topic of importance in the world of standardization is security for the Internet of Things (IoT). Compliance with the security requirements stipulated in international standards is crucial if we are to supply safe and secure services despite the connection of large numbers of devices that are outside our control. Meanwhile, the ISO/IEC 27000 series of standards for information security, IEC 62443 standards for control system security, and other existing standards are being expanded to reflect changes in society. While use of these international standards and management systems such as cyber security management systems (CSMSs) is becoming more widespread, I believe the next step we need to take is to incorporate things like BCM and service

quality assurance into standards, as described by Professor Watanabe.

Taking an All-encompassing View of Resilience

Watanabe: It will be important to take a multidisciplinary approach to future security. This means taking account of information and control security, risk management, and BCM to improve resilience across the entire company. While the definition of organizational resilience remains vague in some respects, to us it means resilience to attack, learning and growing from adversity, and finding new directions. Based on the assumption that it is impossible to prevent incidents entirely, security demands things like flexibility and the ability to recover.

Taking a multidisciplinary approach also applies across organizations. Even if an organization keeps itself secure, if it is part of a value chain, attacks can target weaknesses and use them to gain access. As Dr. Nakano noted, it is also essential that standardization be used to ensure a minimum level of security.

Kaji: To maintain the level of security, it is important to be aware of the risks you face and their potential impacts. In research and development, we are putting a lot of effort into development on the basis that risk analysis based on the latest techniques used by attackers together with risk assessment techniques for accurate prioritization form one of the pillars of security research and development.

Miyao: I understand work is also being done on formulating guidelines for dealing with risks.

Nakano: In the electric power sector, progress is being made on formulating security guidelines for electric power control systems. Factors to be considered in these guidelines include the establishment of management practices for considering risks, the sharing of information and coordination across the industry, and risk analysis, with work in this area being undertaken with reference to the power market reforms taking place in Japan. I anticipate that work will proceed on guidelines for numerous other forms of social infrastructure in the future. Having the entire industry, including operators, vendors like ourselves, and government agencies, work together on producing guidelines will also help build a common understanding of security matters.

Watanabe: The formulation of standards and guidelines is valuable not only for the end result but also for the process, which brings together various stakeholders in discussion. In other words, guidelines are not something that are decided on once and for all. Rather, what is needed is a system for reviewing and auditing operations and progressively updating the guidelines. I believe that establishing mechanisms for sharing information such as on how to identify security incidents is something the industry should be doing on its own initiative.

Protection at the System, Organization, and Operational Levels

Miyao: Hitachi supplies security solutions to its social infrastructure customers, and customer attitudes have been changing, particularly over recent years.

Ohashi: That's right. Until a few years ago, control systems that were not connected to a network were assumed to be immune to cyber-attacks, the threat of cyber-attacks has been of increasing concern over recent times as information and control functions

Kenji Watanabe, Ph.D.

Professor of Graduate School of Engineering, Head of Disaster & Safety Management, Nagoya Institute of Technology

Graduated from Kyoto University in 1986. Joined Fuji Bank (now Mizuho Bank). After working at PricewaterhouseCoopers, he was appointed associate professor at Nagaoka University of Technology in 2003 and took up his current position in 2010. His other appointments include Council Chair of the Critical Infrastructure Protection Council, membership on a Cabinet Office Study Panel on Measures to Facilitate the Establishment and Operation of a Business Continuity Plan, ISO/Security Committee at the Industrial Science and Technology Policy and Environment Bureau of the Ministry of Economy, Trade and Industry, and an expert on ISO/TC292 (security and resilience). He has a doctorate in engineering and an MBA.

have become more integrated, and we are receiving a rising number of inquiries regarding security. I am aware of a change in attitudes accompanying the trend toward the use of the IoT in applications such as infrastructure maintenance.

Ote: Concerns about physical security are also rising. In particular, moves to increase the number of street surveillance cameras have been gathering pace in the lead up to the international sports events to be held in Tokyo in 2020. Surveillance camera video is vital for resolving incidents in an increasing number of cases and I believe there is a shift in public attitudes more toward the idea that the public is being protected rather than being monitored.

Against a background of incidents of food contamination, there has also been a shift at food processing plants and similar facilities toward preventing insider sabotage as well as preventing external intruders. Hitachi aims to provide an overall secure environment by supplying security solutions that combine access control systems, surveillance cameras, and other devices, and are able to collect and analyze access logs, perform image-based monitoring, and divide building interiors into zones with different security levels.

Miyao: As Professor Watanabe commented earlier, security nowadays cannot be achieved by a single organization acting alone. Hitachi is seeking to grow through collaborative creation with customers in many different industries, with the supply of security solutions for social infrastructure being one such collaborative creation initiative.

Hitachi's concept for social infrastructure security is protection at the system, organization, and operational levels. We have adopted the term "hardening - adaptive, responsive, and cooperative" to express the requirements for achieving this. The idea is to protect social infrastructure by building adaptive systems that run on hardened security platforms and on which threat countermeasures are progressively improved, by implementing practices that can respond to incidents, and by sharing information and cooperating with other organizations.

Watanabe: Adopting operating practices that maintain compatibility between control systems and security systems is something that infrastructure companies find difficult, I believe. While there is an urgent need to train people with skills in both areas, Hitachi has experience and know-how that it has built up in the construction of social infrastructure systems, and it also understands business processes. I hope to see you make use of this knowledge to support security practices that are built into actual operations. By doing so, and if a centralized overview of different parts of the social infrastructure can be obtained, it should also be possible to identify multiple simultaneous incidents quickly.

Identifying Incidents and Providing Appropriate Notification

Miyao: As Professor Watanabe noted, detection plays an important role in protecting social infrastructure systems. Major advances have also been made in surveillance technology. Please tell us what you are working on in the research division.

Kaji: We are engaged in joint research into techniques for monitoring and analyzing the operation of control and communication equipment and control networks through involvement in work on the Cyber-Security for Critical Infrastructure, one of the projects of the government's Cross-ministerial Strategic Innovation Promotion Program (SIP). We are also seeking to

Toshihiko Nakano, Ph.D.

Security Business Division, Social Innovation Business Division, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1980. Having worked on the development of security platform software and artificial intelligence for information and control systems, he is currently engaged in the development of security solutions for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Akihiro Ohashi

General Manager, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1986. Having worked on the development of control equipment for various types of social infrastructure, he is currently engaged in managing the development of control systems that combine control and information. Mr. Ohashi is a member of the Information Processing Society of Japan (IPSJ).

detect incidents with as much accuracy as possible from the large quantities of data associated with widespread corporate activities, making use of knowledge acquired through Hitachi's work on its strengths in big data analytics, artificial intelligence (AI) technology, and social infrastructure control.

Watanabe: Another thing I am looking for as a user is an indication of what impact the things that are detected will have on business. It is helpful for decision-making if questions such as how blocking a particular form of access to improve security will affect business operations, for example, can be answered in ways that make sense to management as well as those in the workplace.

Kaji: In fact, we have started on such research. While the timeliness of management decision-making is crucial to minimizing the spread of damage, problems arise when management is not provided with the information it needs to make these decisions, or when the information is not provided in a form that aids decision-making. There have also been cases of security specialists being aware of vulnerabilities at their company, but not being able to budget for countermeasures because they have not communicated these clearly enough to management. We are looking for ways to present the effects that incidents have on operations and to report using terminology that management can understand.

Establishing and Instantiating Security Knowledge

Miyao: The judgment of people in the workplace is important for social infrastructure. What practices are available that can help with on-site decision-making?

Nakano: Because operators perform their work in accordance with detailed manuals, it is important to provide them with training so that they are able to do what the manual tells them when specific situations arise. What is needed to respond effectively to security incidents in the workplace is to foster people with the ability to produce manuals that incorporate security knowledge and other skills, and to equip these people with the knowledge they require to produce the manuals. Practices are required to enable the collation and utilization of information such as sample hazard maps and examples of past incidents and how they have been dealt with, with vendors like Hitachi playing a role in establishing this base of knowledge and seeing that it is put to use.

Watanabe: What you are saying is that Hitachi is in a position to put its capabilities to work at customer workplaces and in areas such as human resource development, including know-how and skills obtained from dealing with actual cybersecurity incidents.

Ohashi: The creation of manuals is an ongoing process, and it is important to work through the plan, do, check, act (PDCA) cycle at an organizational level and to establish a virtuous circle that encompasses everything from systems and operations to the organization.

While there is a tendency to think of control systems as applying to machinery because they started out as a means to automate tasks that were originally performed by people, the underlying purpose is to achieve automation by linking activities together. We have been working with customers to improve control systems in order to achieve more advanced forms of this type of automation, and as another step in this process, I believe we should also be trying to create control systems that enhance customer operations, including security.

Ichiro Ote

Business Management Department, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1983. Having worked on the development of core and solution software for personal computers (PCs), PC servers, and digital consumer electronics, and in product planning for security equipment, he is currently engaged in business planning for security solutions.

Tadashi Kaji, Ph.D.

Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd.,

Joined Hitachi, Ltd. in 1996. Having worked on the research and development of security for distributed object systems and corporate information systems, he was appointed to his current position in 2015. Dr. Kaji is a member of the IEEE.

Transforming Security from a Cost to an Investment

Watanabe: While I suspect most companies still think of security measures as a cost, do you have any ideas for solutions that can turn this view around?
Ote: One example would be utilizing production line security to turn process improvements into added value. Video from surveillance cameras installed on production lines can be transformed into structured data by collecting and analyzing it using image processing. This information is being utilized in a variety of solutions, such as big data analytics, for things like productivity or quality improvement, for example. The idea is that providing solutions that are used routinely for process improvement while still being available when needed for security-related damage prevention adds value to physical security while also allowing more intensive collaborative creation with customers.
Nakano: The utilization of data can transform security from a cost to an investment. This form of value is a message we need to effectively communicate.
Kaji: With cybersecurity, the ability of log analysis to monitor the behavior patterns of staff can be utilized for purposes such as improving productivity. You can also think of providing cybersecurity as a way of using big data analytics for operational improvements.
Ohashi: In the case of machinery, operations that differ from normal operations can be used to detect faults as well as security incidents. The payback on investment can be improved by using data for both risk management and machine maintenance.
Miyao: As mentioned earlier, thinking in terms of making improvements to corporate workplaces and management, including security, gives rise to multiple benefits.
Watanabe: To improve awareness of security among management, I believe it would be worthwhile for Hitachi to take on initiatives such as security conferences or working groups. This is because there is widespread interest in sharing experiences from different industries and companies.
Nakano: That's right. In this regard I understand that Professor Watanabe's university has set up a model plant and educational curriculum, and is successfully providing training in cybersecurity in partnership with infrastructure companies.
Watanabe: This initiative relates primarily to business continuity and has provided a wealth of insights thanks to its being accompanied by lively opinion-sharing, especially with important regional infrastructure companies. Being a grass-roots activity conducted as part of research and teaching, the hope is that knowledge and insights gained through training can be promulgated within companies and communities, and that the participation of students will help foster people who are able to work in the security industry. While security is a field that lacks definitive answers, I hope that we can help improve the resilience of society as a whole by conducting practical security training together with ongoing measures that incorporate scientific analysis.
Nakano: This sort of joint training encourages the overall view we spoke of at the beginning. We intend to transcend the boundaries between organizations and between the cyber and physical realms, and to think about and deal with security as a large all-encompassing social system. To achieve this, I believe we need to make the most of Hitachi's capabilities, with its knowledge of information systems, social infrastructure control systems, business activities, and security.
Watanabe: There are few companies in the world that possess all of those attributes. I look forward to seeing Hitachi put those strengths to work for the benefit of social infrastructure security.
Miyao: As security threats grow, Hitachi seeks to be more than just a vendor that builds systems by engaging in collaborative creation with social infrastructure companies and thinking about security together in partnerships. Thank you for your time today.

Takeshi Miyao

General Manager, Security Business Division, Services & Platforms Business Unit, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1987. His work has included control system product development for electric power, railways, gas, and other industries. Having worked at the Ministry of Economy, Trade and Industry, he is currently engaged in the security business for social infrastructure systems.