Hitachi Review
Volume 65 Number 8 September 2016

HITACHI
Inspire the Next

Security for Safe and Secure Social Infrastructure

www.hitachi.com/rev

Hitachi Review
Volume 65 Number 8 September 2016

From the Editor

Social infrastructure systems provide uninterrupted 24-hour/365-day services such as the electric power, gas, and water that underpin daily life and business activity. The social infrastructure systems that deliver these services 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 internationally and a greater diversity of cyber-attacks.

Work on security is being undertaken by government and industry bodies. In Japan, government agencies are working together through the National center of Incident readiness and Strategy for Cybersecurity (NISC) to formulate rules and guidelines, and statements on security have been issued by industry bodies.

With reference to this situation and to these rules and guidelines, this feature issue of *Hitachi Review* describes Hitachi's views on what form security should take to keep society safe and secure by protecting social infrastructure from security threats, the concepts involved with achieving this, and various technologies, products, and solutions, including examples of their use in the field of social infrastructure.

Based on its concept of protection at the system, organization, and operational levels, Hitachi supplies total solutions for social infrastructure that extend from consulting on the upstream end of the value chain to system implementation and security operations. In its solutions, Hitachi draws on its advanced security technologies, which combine the cyber and physical realms, on its many years of experience supplying social infrastructure systems, and its experience of operating information technology (IT) infrastructure for its own workforce of approximately 300,000 people.

I hope that this feature issue of *Hitachi Review* will give readers get a better understanding of the security concepts proposed by Hitachi, and that it will contribute to building safe and secure social infrastructure systems through collaborative creation with many organizations, starting with social infrastructure companies.

Editorial Coordinator,
"Security for Safe and Secure Social Infrastructure" Issue

Takeshi Miyao

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

Security for Safe and Secure Social Infrastructure

Contents

Security for Safe and Secure Social Infrastructure

While progress is being made on using information to build a more advanced social infrastructure, it is concerning that cyber-attacks on information systems have now spread to social infrastructure systems.
Hitachi combines knowledge acquired through the supply of social infrastructure control systems over many years with technology and know-how built up in its information technology and defense and security businesses to supply security solutions that provide total protection for social infrastructure across both the physical and cyber realms. Based on the 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 customers and many other organizations.

Expert Insights

Achieving a High-quality Internet

Hideki Sunahara, Ph.D.

Professor of Media Design/Advanced Research Center, Keio University Graduate School
Director of Cyber Security Research Center

Born in Hyogo Prefecture in 1960, he earned a Ph.D. in Computer Science from Keio University in 1988. After working as a tutor in the Department of Computer Science and Information Mathematics at the University of Electro-Communications, he was appointed assistant professor at the Nara Institute of Science and Technology's Information Technology Center in 1994, professor from 2001, and professor at the Graduate School of Information Science from 2005. He was appointed to his current position in April 2008.
Involved in building the Internet in Japan and in associated research with the team of Jun Murai (Professor on the Faculty of Environment and Information Studies, Keio University) on the JUNET project from 1984, and the WIDE Project from 1988. Launched the Live E! Project for sharing of environmental information over the Internet with Hiroshi Esaki (Professor at the University of Tokyo) in 2005. Currently, researching security and privacy to create a secure and safe Internet-based society, and promoting the Information Bank Project about the safe management of personal information.

Not a day goes by without news of a security incident, whether it be an information leak, unauthorized access, or malware. Recent cases have also emerged of ransomware, which holds information for ransom and demands money. In February of this year, the operations of a Los Angeles hospital were disrupted by ransomware that infected its PCs. Apparently the hospital ended up paying the ransom to resolve the incident. When we hear stories like this, engineers like me always wonder whether we cannot solve this problem, but I have come to the conclusion that it is not something we can overcome using technology alone. This is because, through the analysis of various different incidents, I have found that it is people who are the weakest link. In other words, unless people change, incidents like this will continue.

In this case, in what way should people change? One thing that I believe to be crucial is an awareness that nobody is unaffected by Internet security. It is important that people understand that security matters to them and that it is not enough simply to establish a security department at the organization, appoint a chief information officer (CIO), and delegate responsibility to someone else. I do not believe it is necessary to understand how systems are implemented or how complex incidents were perpetrated. On the other hand, just understanding that your routine behaviors have security implications is, I believe, enough to change matters significantly. If everyone is paying attention, they should be able to notice when something is out of the ordinary. Provided that someone notices, it can then be left to the specialists to assess the situation and determine what has happened.

This means that action is needed to raise everyone's awareness. I think of this as education. While the training of specialists is essential, what we also need to do nowadays is to provide ongoing education for everyone else. Improving Internet security equates to improving the quality of the Internet that we use as part of the social infrastructure. While technology development and the establishment of public policy are necessary for achieving this, I also believe that providing education in parallel with such work will create a high-quality Internet.

Japan will host major international sports events in 2020. By that time, I believe the Internet will have become an even more important part of the social infrastructure. For Japan to take the lead in improving the quality of the Internet at this time, we should be working on initiatives in the three areas of technology, policy, and education.

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.

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

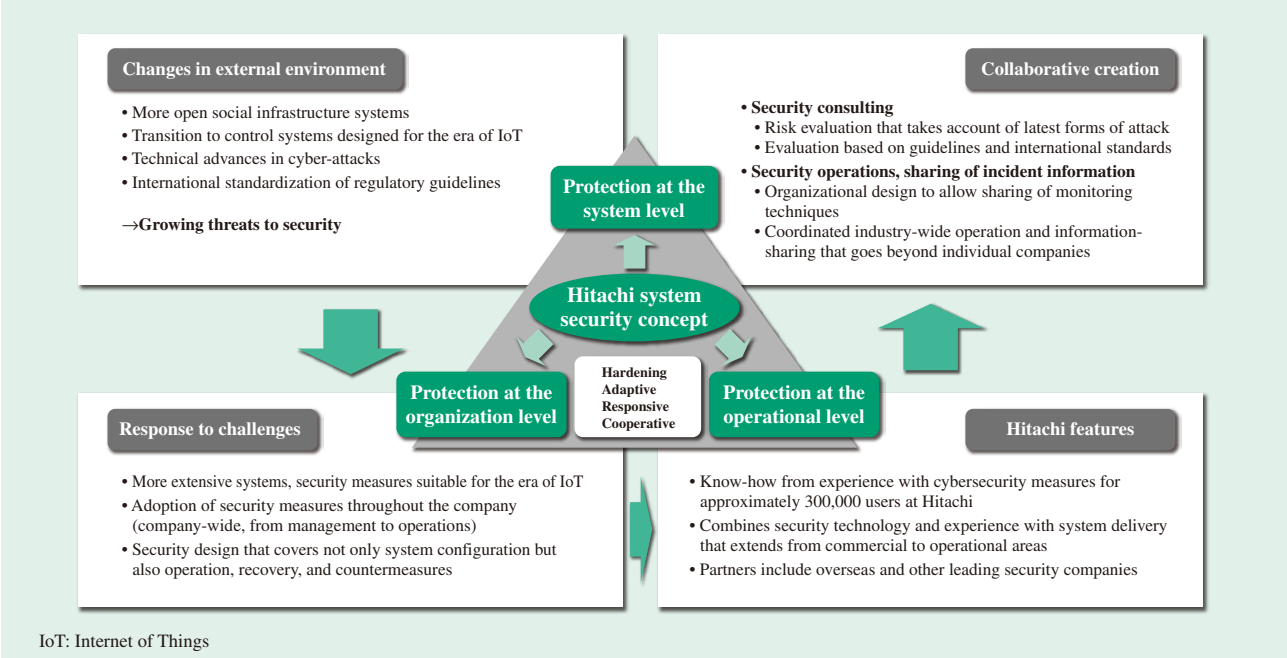
Hitachi has experience with building social infrastructure systems and supplying them to companies in such sectors as electric power, gas, water, railways, finance, and government. What social infrastructure companies require if they are to supply high-quality services are high system reliability and 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.

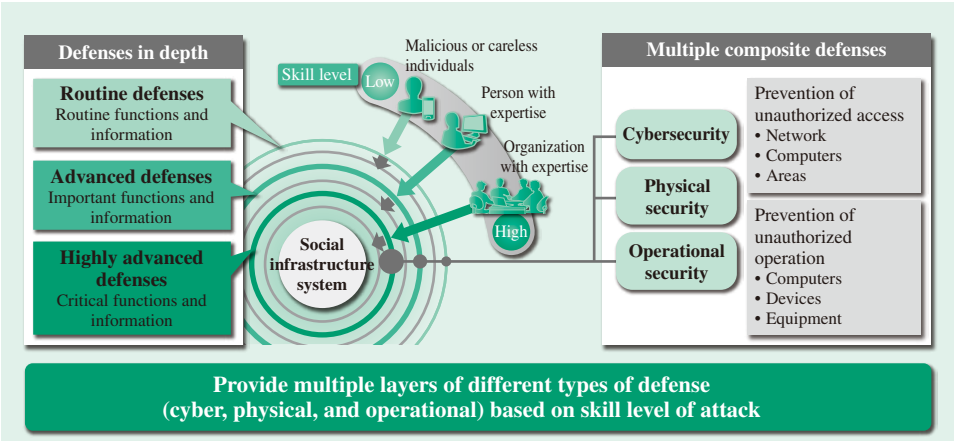


Fig. 2—Multi-layer Defenses.
This means providing multiple layers of defense for social infrastructure systems, with overlapping cyber, physical, and operational measures.

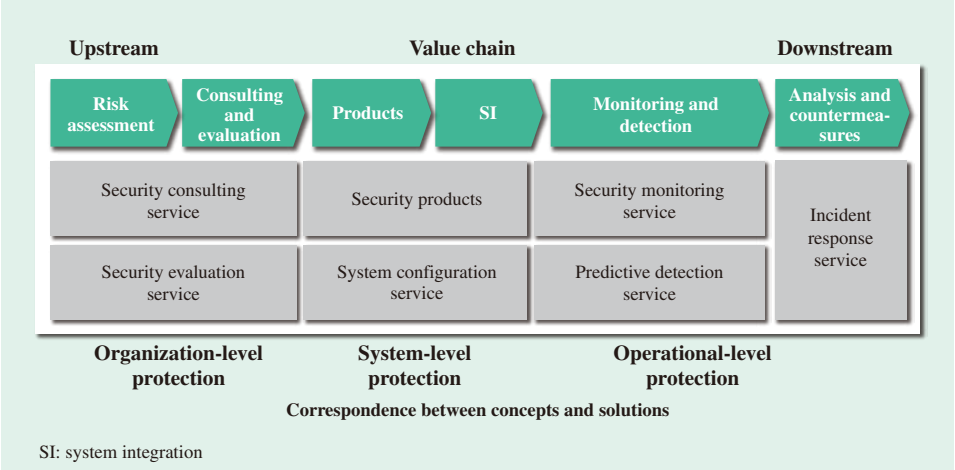


Fig. 3—Hitachi's Security Solutions.
Hitachi supplies solutions in accordance with its concept while also taking a value chain perspective.

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

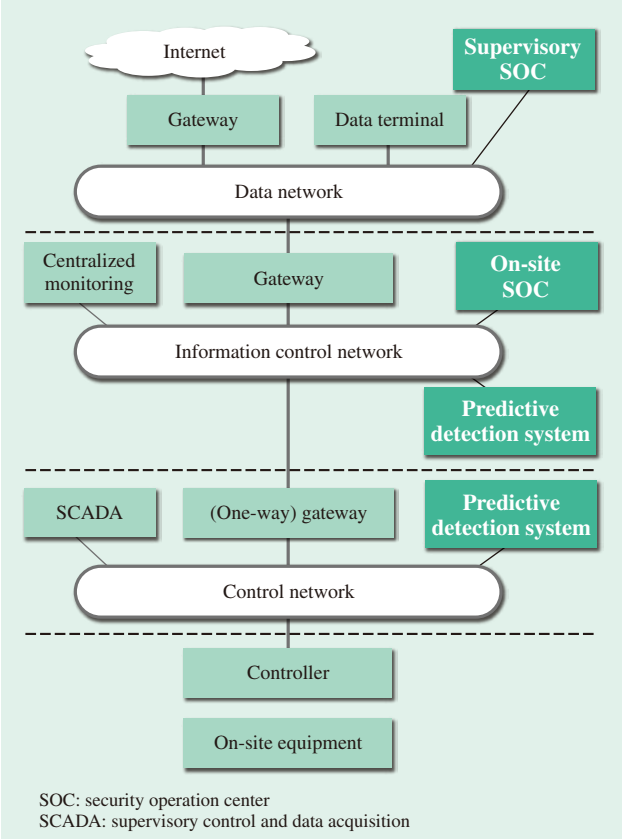


Fig. 4—Security Monitoring Architecture.
On-site SOCs, predictive detection systems, and supervisory SOCs interoperate to form a security operation, monitoring, and detection architecture for control systems.

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).

Featured Articles I

Power Sector Examples

Hitachi's Approach to Security for Power Control Systems

Masahiro Murakami
Hideki Hanami
Hiromichi Konno
Ryuichi Okamoto
Mitsuaki Ishiba

OVERVIEW: The power market reforms in Japan, which include wide-area operation, retail market deregulation, and the separation of generation and transmission, are expected to widen the scope of the networks that connect power systems in the future. Accompanying this is growing interest in security measures for power control systems together with recognition of the importance of these measures. Hitachi is drawing on its experience with power control systems built up over many years to investigate security measures that make the most of technologies for control and for information security by identifying what form power control security should take and analyzing security risks in terms of control, people (behaviors), and information. This article describes Hitachi's approach to power control security and presents a case study of its work.

INTRODUCTION

THE power market reforms in Japan, which include wide-area operation, retail market deregulation, and the separation of generation and transmission, will lead to a wider scope of operation for the communication networks that connect power systems, including the transmission of information about power use as well as the power itself from consumers to generators. Safety is the top priority for power equipment, and together with the ongoing requirement for security of supply, this means that there is a need for security measures that can deal with increasingly sophisticated attackers.

This article describes Hitachi's approach to power control security in terms of contributing to the security of the power supply, and presents a case study of its work[1].

SECURITY THREATS TO THE POWER INFRASTRUCTURE

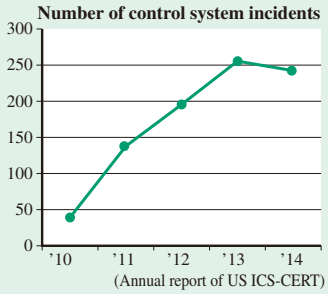
Increasing Ingenuity and Diversity of Cyber-attacks

Numerous instances of damage resulting from cyber-attacks on critical infrastructure around the world, such as nuclear power plants and power transmission and distribution systems, have been reported since the 2010 cyber-attack on nuclear facilities in the Islamic Republic of Iran (see Fig. 1).

Damage-causing attacks on critical infrastructure are increasing in frequency and ingenuity

- Growing prevalence of cyber-threats against control systems
- Optimization of attacks based on investigations that take account of targets

➡ Actual incidents of damage



Instances of cyber-attacks on critical infrastructure

Date	Target (location) Damage inflicted	Cost
2010/7	Nuclear facilities (Islamic Republic of Iran) Equipment damage	NR
2012/3	Financial institutions (worldwide) Information theft	$80M
2012/8	Oil company (Middle East) Equipment damage	NR
2013/3	Broadcaster, financial institution (South Korea) System shutdown	$800M
2015/6	Public agency (Japan) Information theft	NR
2015/12	Power plant (Ukraine) System shutdown	NR

US: United States ICS-CERT: Industrial Control Systems Cyber Emergency Response Team NR: not reported

Fig. 1—Security Incidents on Critical Infrastructure.
Attacks on critical infrastructure are increasing and their effects are expanding.

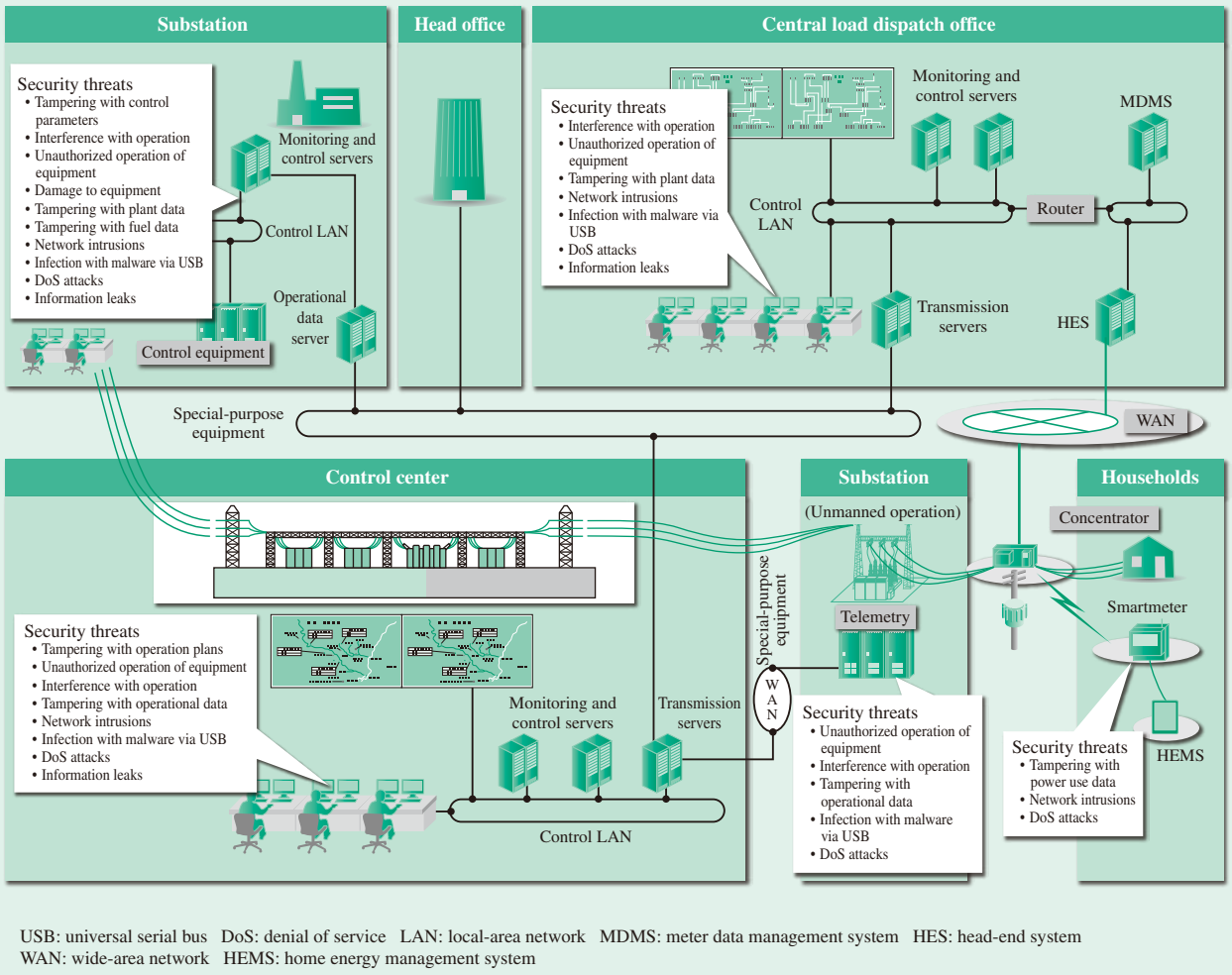


Fig. 2—Typical Security Risks for Electric Power Control Systems.
Critical infrastructure is connected to a large number of networks, each of which poses security threats. The consequences of a serious incident extend from localized damage such as faulty equipment operation to damage to important facilities such as power plants or substations, carrying a risk of damage spreading to the wider power system.

The methods used in recently reported cyber-attacks on critical infrastructure are seen as exposing critical infrastructure to the threat of highly malicious and ingenious cyber-attacks, with instances in which, rather than a simple cyber-attack such as one that seeks to exploit information, the aim has been to gain access to control systems and acquire and decode control information to identify specific equipment and prevent it from being controlled properly.

Risks Faced by Power Control Systems

Potential cyber-attacks on power control systems include both physical attacks, such as intrusions by people with malicious intent, and sophisticated cyber-attacks, such as intrusions that use universal serial bus (USB) or other media and control network intrusions from the Internet that enter via data networks.

In the past, power control systems in Japan were at very low risk of cyber-attack from the Internet due to the use of proprietary technology and special-purpose closed control networks. Nowadays, however, these systems are increasingly connected via firewalls or other security equipment to information systems for purposes such as big data applications or greater convenience. As a result, they are at increased risk of attack by people with expertise in advanced cyber-attack technology.

The sorts of cyber-attacks that might occur on a power control system go beyond the exploitation of control information or denial of service (DoS) attacks on networks to also include attacks aimed at disrupting the reliable operation of critical infrastructure by means such as tampering with control signals or unauthorized operation of equipment (see Fig. 2).

HOW HITACHI VIEWS POWER CONTROL SYSTEM SECURITY

Security Concepts

In addition to complying with international and industry standards, it is important for power companies in particular to demarcate the required security measures into different levels based on the importance (in terms of safety and potential for damage) of the equipment concerned.

The Hitachi system security concept under which security is required to be adaptive, responsive, and cooperative has been adopted by Hitachi and has also been applied to power control systems.

To repel sophisticated modern cyber-attacks, it is becoming increasingly important to undertake adequate security design and provide detection and defense functions in the development phase, and to implement security measures, establish infrastructure for dealing with cyber-attacks, share information through collaboration with other relevant organizations such as Industrial Control Systems Cyber Emergency Response Teams (ICS-CERTs), and stage routine drills to enable the correct response when an attack occurs in the operational phase.

It is necessary during the operational phase not only to maintain the security levels assigned in the development phase, but also to maintain and enhance the security system by collecting the latest security knowledge. This is achieved by collecting and analyzing data from various points around the system to assess the state of system security, detect problems quickly, and respond appropriately when needed (see Fig. 3). That is, to strengthen security measures by utilizing the observe, orient, decide, act (OODA) loop to achieve quick and accurate decision-making as well as using the plan, do, check, act (PDCA) cycle of planning, improvement, and adjustment[2), (3)].

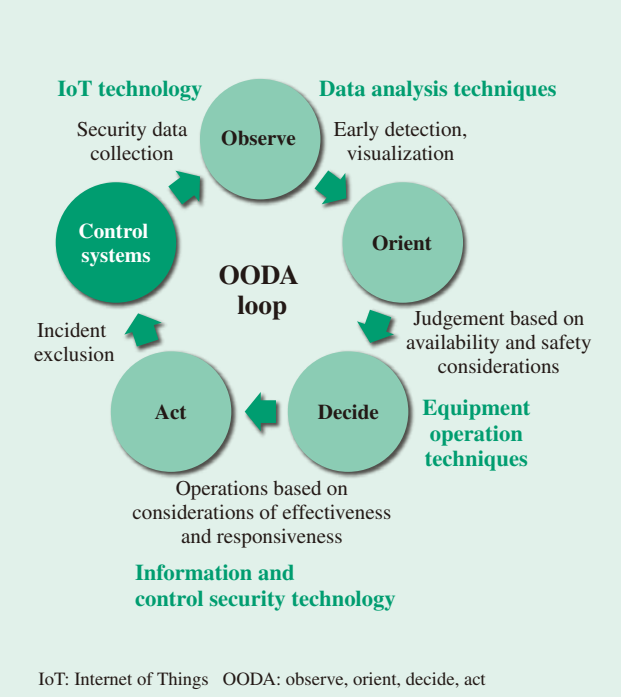


Fig. 3—Security Concept for Improving Availability of Power Control Systems.
The concept involves using the OODA loop to protect critical infrastructure from cyber-attack.

Introduction of Security Maps

Of greatest importance when providing security measures for critical infrastructure is to determine what needs to be protected and to ensure secure protection in order to maintain operation while also preserving robustness. Accordingly, Hitachi believes it is essential to consider the possibility of both physical and cyber-based attacks on power control systems, and to determine in advance for each item of equipment how to respond to an incident and the criteria for action.

This response requires the preparation of security maps in which the overall power system is split into zones and the potential consequences are assessed for each zone based on a risk analysis that considers both control security (a risk analysis based on control considerations) and system security, covering physical attacks on system equipment as well as cyber-attacks on networks and other information technology (IT) equipment.

Formulation of Security Policies

The next steps are to break the system down into the individual control systems, including central load dispatch offices and power plants, and to formulate individual security policies in accordance with the guidelines defined in the security map (see Fig. 4).

To produce these policies, Hitachi drew on its knowledgeable experience in power control systems, first to assess possible attack patterns by considering how attackers might go about attacking each system, then to collate specific defense measures for system equipment by considering how the system could be defended against each of these attacks.

In this way, Hitachi believes it is contributing to the reliable operation of power control systems by formulating responses for each item of equipment in the power system in a security map and security policies.

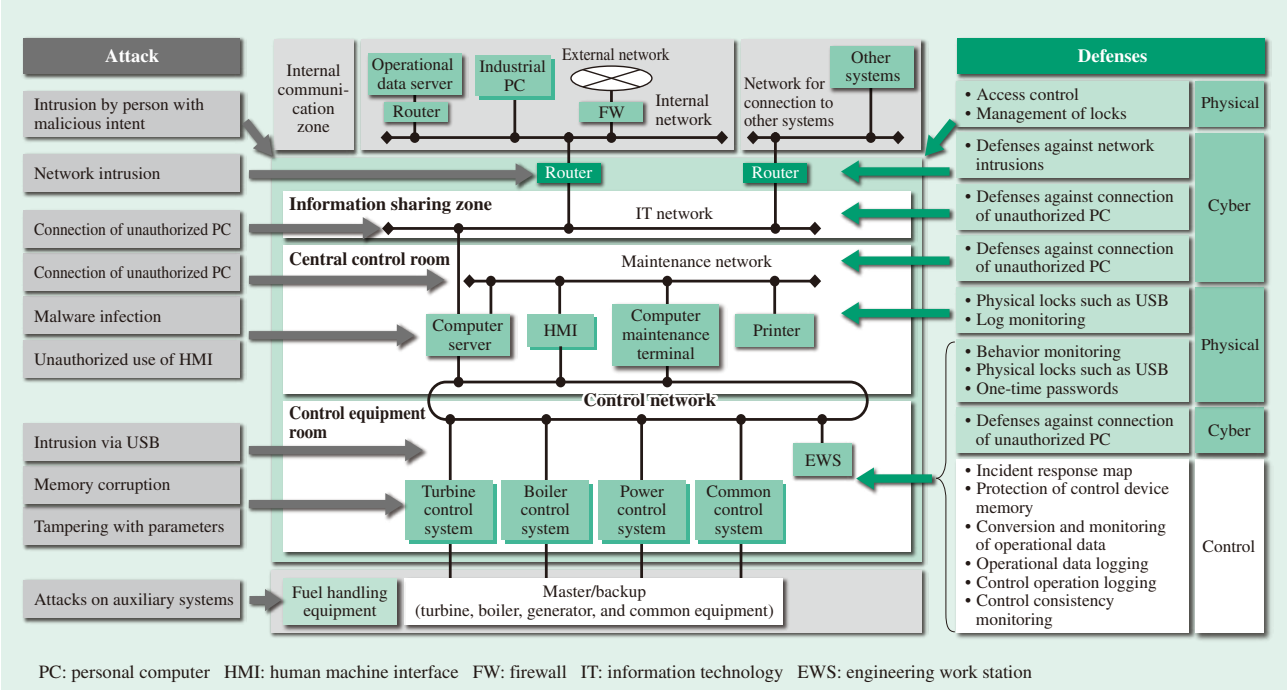


Fig. 4—Control System Security Policies.
By formulating security policies for control systems, power systems are protected by identifying all the different means of attack and implementing ways to detect and defend against them.

SECURITY SOLUTIONS

Power Grid Monitoring and Control Systems

Power grid monitoring and control systems have in the past run on closed control networks. It is anticipated that this will change in the future toward greater use of open control networks, bringing with it increasing opportunities for network interconnection with the outside world. Because such an environment carries a risk of large-scale power outages due to cyber-attacks on power grid monitoring and control systems, appropriate measures are needed. While the security measures on past power grid monitoring and control systems have included measures for preventing unauthorized access by installing firewalls at points of interconnection with systems at other sites or the various support systems, the threat of modern-day cyber-attacks and the increase in concerns about them have led to a growing trend toward stronger security measures, including intrusion detection systems (IDSs), whitelist control, and access control using identification (ID) cards.

Power Plants and Monitoring and Control Systems

Nuclear power plants in Japan have traditionally implemented physical security measures as required by the Act on the Regulation of Nuclear Source Material, Nuclear Fuel Material and Reactors. In the future, safety measures for workers will be tightened in the light of the accident at Fukushima Daiichi Nuclear Power Station. Similarly, while cybersecurity will continue to include use of conventional practices such as firewalls and data diodes, measures will also be strengthened to bring them up to international standards, with reference to factors such as previous work on security measures in the USA that has gone as far as to formulate design-basis threats and consider deep safeguards.

Likewise, with thermal and hydro power plants, control systems have traditionally been protected against external threats by the use of zoning, whereby systems are split into control and IT zones, and the installation of firewalls and other security devices at interfaces with the outside world.

A variety of measures are required for the control systems at some thermal and hydro power plants because they include equipment from different vendors. This makes it necessary to adopt practices that are not vendor-specific and to implement security measures with reference to the International Electrotechnical Commission (IEC) 62443 international standard for control security. In addition to control-based measures that cover protection, control, and operational data monitoring, Hitachi is strengthening security by

hardening through the use of equipment with Embedded Device Security Assurance (EDSA) certification and using a combination of physical and cyber-security.

Physical Security

As restricting physical access to important equipment and monitoring and control systems helps reduce cybersecurity risks as well as its obvious role in preventing unsafe activities, physical and cybersecurity complement each other. Access restriction involves assigning people to categories and limiting those who are able to access equipment to the bare minimum, while at the same time preventing people from bringing in dangerous goods and controlling possession of mobile media and other devices.

Because power plants are characterized by occupying large sites and buildings, locating where people are is important for security management and also useful for guiding staff in the event of an emergency.

With transmission and distribution equipment being spread across a wide area, Hitachi uses centralized management for access control and login authentication for control systems, and operates it in tandem with physical security.

CONCLUSIONS

The power control systems that support the electricity infrastructure are required not only to help optimize operations through the monitoring and control of transmission, distribution, and generation equipment, but also to counter new threats such as physical and cyber-based attacks while maintaining a reliable supply of power.

Along with power control systems, Hitachi also has expertise in power supply systems and technologies for control, physical security, and cybersecurity. This enables it to establish ways to deal with attacks on customer equipment using multiple layers of different types of defense. Hitachi is able to improve the resilience of both the hardware and software used in control equipment and to provide ongoing defense against increasingly sophisticated cyber-attacks on control and information systems through support supplied by its own Computer Security Incident Response Teams (CSIRTs), and it intends to contribute to the reliable supply of power and solving management challenges by protecting customer equipment.

REFERENCES

(1) Ministry of Economy, Trade and Industry, "2015 White Paper on Manufacturing Industries (Monodukuri)," http://www.meti.go.jp/report/whitepaper/mono/2015/honbun_html/index.html in Japanese.
(2) T. Nakano et al., "Control System Security for Social Infrastructure," Hitachi Review **63**, pp. 277–282 (Jul. 2014).
(3) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).
(4) ZDNet Japan, "Establishment of Ecosystems Required by IT Companies," (Feb. 2015), http://japan.zdnet.com/article/35060584/ in Japanese.
(5) H. Horii et al., "Power System Technologies for Reliable Supply of Electric Power and Wide-area Grids," Hitachi Review **62**, pp. 53–59 (Feb. 2013).
(6) Hitachi, Ltd., Autonomous Decentralized System, http://www.hitachi.co.jp/products/infrastructure/product_solution/platform/middleware/autonomy_dispersion/index.html in Japanese.
(7) H. Kuwahara, "Experience Teach us the Future of Autonomous Decentralized Systems," International Symposium on Autonomous Decentralized Systems/Keynote Address, pp. 169–175 (1997).

ABOUT THE AUTHORS

Masahiro Murakami

Power Generation Plant & Power Grid Control Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the power infrastructure O&M services design business utilizing the Internet of Things (IoT).

Hiromichi Konno

Power Generation Plant & Power Grid Control Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the power infrastructure O&M services design business utilizing the IoT.

Mitsuaki Ishiba

Nuclear Power Control and Instrumentation Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the nuclear power control systems design business.

Hideki Hanami

Nuclear Power Control and Instrumentation Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the design and development of nuclear power control systems and security systems.

Ryuuichi Okamoto

Power Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the power grid systems design business.

Featured Articles I

Process Industry Examples

Control Security Support in Hitachi Instrumentation Systems

Shigenori Kaneko
Kazunobu Morita
Tomoyuki Sunaga
Hitoshi Murakami
Makiko Murakami
Katsumi Hanashima

OVERVIEW: Many industries typically have long upgrade cycles for plant production lines and production control systems, and are often still using old machines. In the past, systems were protected by having no connections to external networks, however, since external connections have become unavoidable due to the growing use of big data and the IoT, systems are becoming increasingly vulnerable to security threats. To address this issue, Hitachi has proposed a method of improving security that uses templates to reduce the workload on production sites. The concept behind this method divides security measures into three whitelists that prioritize affinity with production lines and production control systems.

INTRODUCTION

TO increase productivity in plants and factories, many industries are increasingly using the Internet of Things (IoT) as a way to improve construction of new equipment, extend the life or improve the utilization of existing equipment. The IoT is being used for big-data analysis of operation data, and for gathering equipment and system statuses in the form of data.

Inevitably, control systems will need to be connected to external systems for things such as sending equipment data to the cloud server for big-data analysis of operation data, and using wireless or carrier lines for IoT compatibility.

Japan's government has responded by enacting the Basic Act on Cybersecurity, which specifies 13 key infrastructure areas. Cybersecurity measures are considered key requirements for the production equipment of various industries. However, sites prioritize response measures that are taken to keep equipment operating and to ensure productivity. Standard response measures that start with upstream consulting, and then involve system threat analysis, security system installation, and parameter setting increase the site workload, making them difficult to implement.

When instrumentation systems contain production lines or production control systems and are used as production equipment, Hitachi feels it is important to define templates of security measures for them. These templates are used to propose and implement systems, aiming to provide security solutions that do not increase site workload. Hitachi's work in this area is gaining momentum. This article looks at these solutions.

FEATURES AND ISSUES FOR PRODUCTION LINES AND PRODUCTION CONTROL SYSTEMS

The instrumentation system for a production line or production control system has a system configuration mainly composed of a client/server-based manufacturing execution system (MES), a distributed control system (DCS) with a human-machine interface (HMI), an engineering station (ENGS), a controller, and the network that links these components.

The conventional idea that this system is safe because it is offline has been largely abandoned today. And even if the system is connected through a firewall, there are high risks of cyber-attacks via remote monitoring systems and office automation (OA) systems, and of direct attacks and malware infiltration. These risks are the result of big data usage and IoT compatibility. They can be caused not only by connecting control systems to external systems, but also by network-based remote monitoring, connection to OA systems, and the use of removable memory media such as universal serial bus (USB) memory (see Fig. 1).

To devise templates for security measures to combat these risks, Hitachi compiled a list of system features and issues. It found the following three points are key for templates:

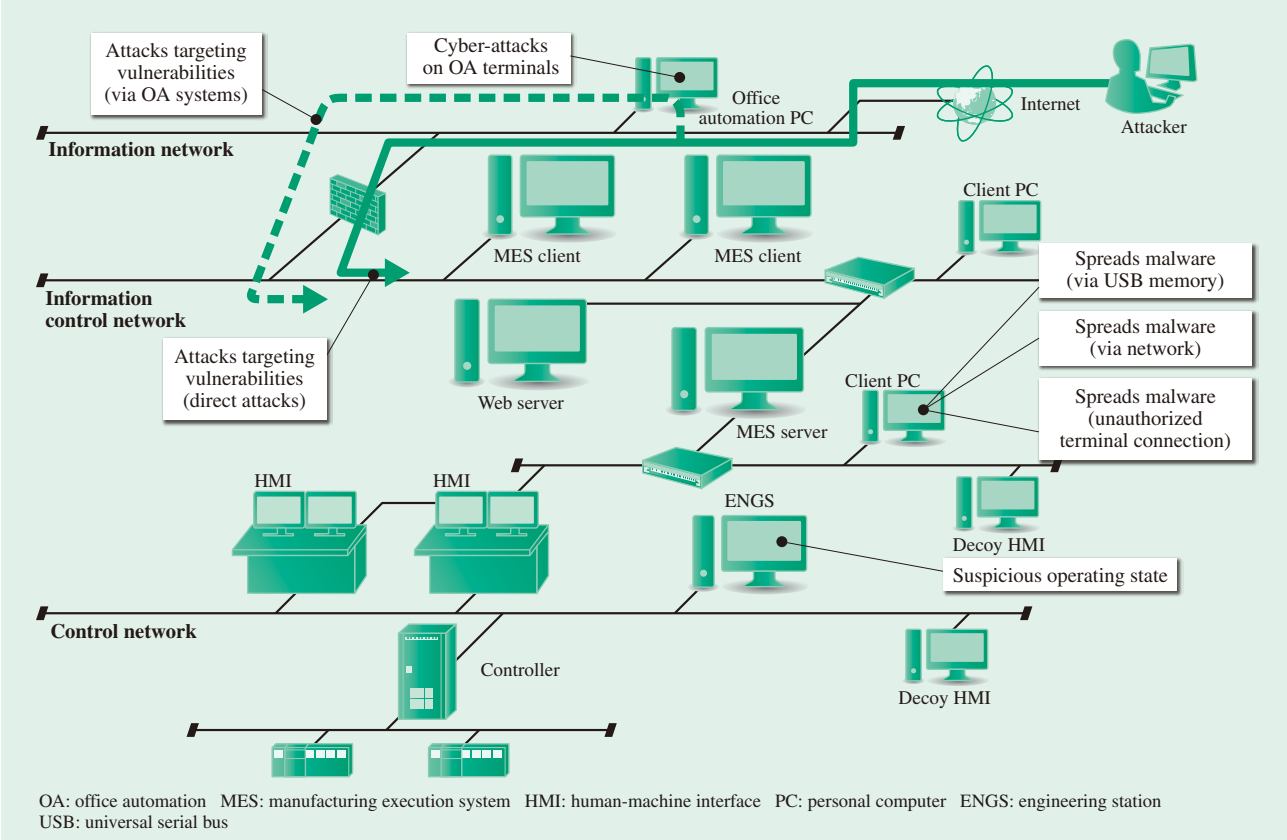


Fig. 1—Production Line/Production Control System Overview and Security Threats.
A standard production line/production control system is defined and made into a template to analyze threats and create templates for security measures. The security level can be selected and the system gradually improved in accordance with the budget and system.

(1) Long system life

While the hardware and software comprising IT systems have maintenance/service periods of five to seven years, production lines and production control systems are used for longer terms of 10 to 20 years.

This longer life results in the problem of software and operating systems (OS) exceeding their support period and continuing to be used without providing security patches for them.

(2) Inability to shut systems down

Three elements are considered important for information security response measures—confidentiality, integrity, and availability. Among these elements, the availability of not being able to shut a system down is often prioritized, resulting in the problem of not being able to make frequent upgrades (requiring restarts) using security patches or security tools.

(3) Frequently critical delayed responses

Some systems are time-critical types that do not permit delayed responses, so a delayed response in applying a security patch or installing a tool could ultimately be fatal for them. Another problem is the difficulty of adding programs after a system has been put into operation, because upgrades must be carefully examined to determine their effect on system response.

SECURITY REQUIREMENTS AND SECURITY CONCEPTS FOR PRODUCTION LINES AND PRODUCTION CONTROL SYSTEMS

Below is a discussion of requirements derived from the features and issues listed in the previous chapter.

Security Requirements

(1) Systems that are offline

The first requirement is an extension of previous security concepts—it must be possible to provide responses to offline systems operating in an offline network environment not connected to any external system. Although external connection is becoming mandatory, there are still many systems in offline environments. These systems cannot update signature and pattern files in real time, so they must maintain a secure state in the environment in which they were adopted.

(2) Systems that have long lives

The second requirement is that tools installed in OSs must work on legacy OSs. To enable use for long periods, they must also work on OSs that have exceeded their support periods.

(3) Systems that are given priority because they cannot be shut down

The third requirement is that systems are not permitted to be shut down and restarted. Since system shutdowns are directly linked to the continuity of the business itself, system shutdowns and restarts for purposes such as software updates must be kept to a minimum.

(4) Systems that are time-critical

The fourth requirement is that delayed responses must not occur. A delayed response in applying a security measure has a very high risk of developing into a critical problem.

Security Measure Concepts

To satisfy the requirements above for the purpose of continuing business without shutting down production lines or production control systems, a multi-stage defense approach is an effective way to implement containment measures. This approach presupposes the risk of malware infiltration, while reducing the infiltration risk and rapidly detecting infiltration to prevent its spread to peripheral equipment. Hitachi has proposed the following three whitelisting concepts:

(1) Whitelisting applications

(2) Whitelisting devices connected to networks

(3) Whitelisting control network communication

SECURITY MEASURE PROPOSALS FOR PRODUCTION LINES AND CONTROL SYSTEMS

(1) Whitelisting applications

Hitachi has enabled responses with affinities to systems conforming to templates by limiting the applications that run on the system, and by using whitelist-based security products that circulate in the market and have been checked for compatibility (see Fig. 2).

(2) Whitelisting devices connected to networks

Networks are whitelisted by limiting the devices that may be connected to the network (see Fig. 3). Hitachi has released a product that detects unauthorized connections. It can be installed outside the network and after-the-fact, enabling installation with affinity to both new and existing systems (see Fig. 4).

(3) Whitelisting control network communication

Control networks contain physical production lines or production control systems, enabling communication recipients to be determined in advance,

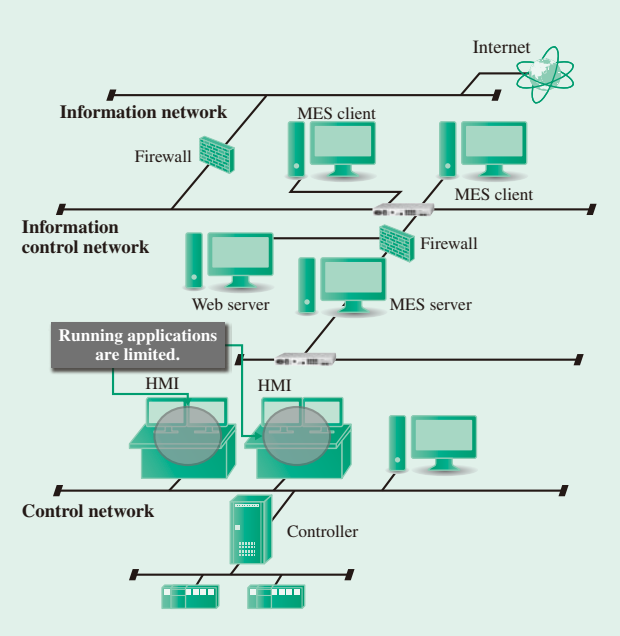


Fig. 2—Whitelisting of Applications.
The applications that run on the HMI are limited to protect the system.

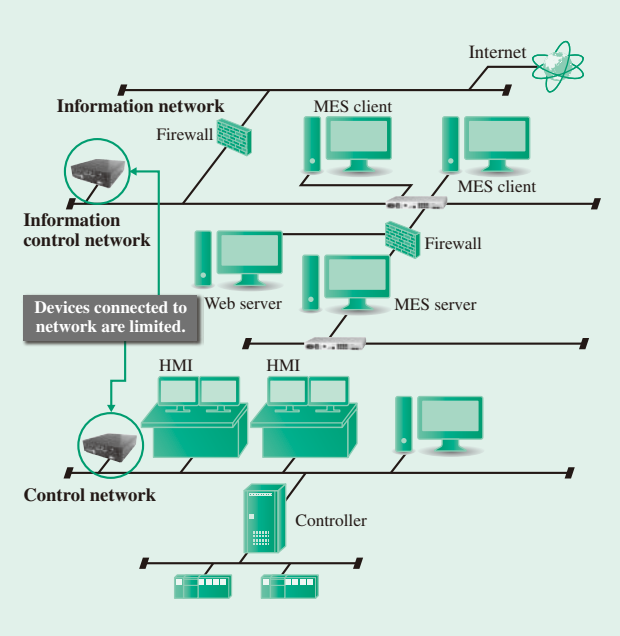


Fig. 3—Whitelisting of Devices Connected to Network.
The devices that can be connected to the network are limited to protect the system.

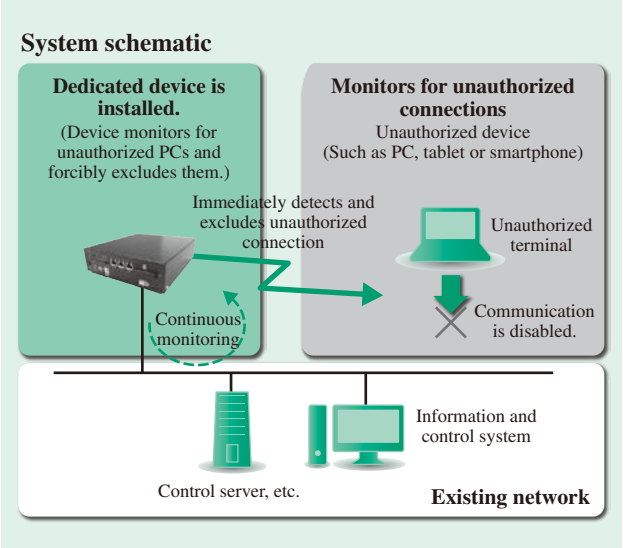


Fig. 4—Unauthorized Connection Detector.
This detector detects and automatically excludes attempts to connect unregistered devices to the network, to prevent the threat of cyber-attacks.

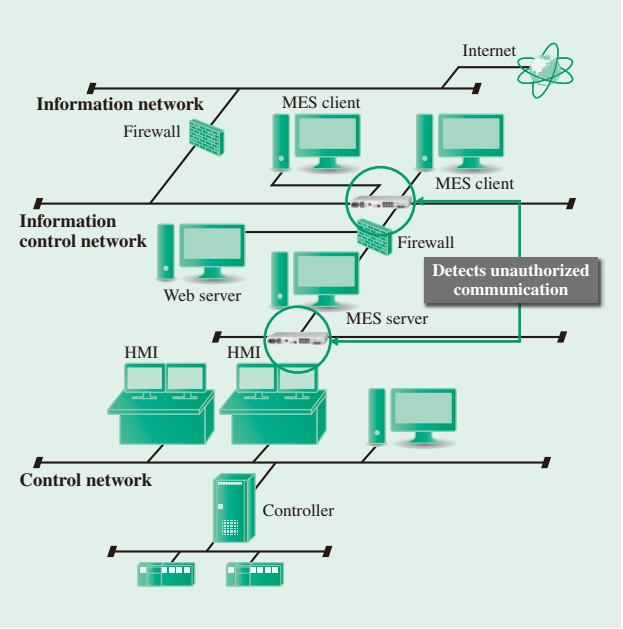


Fig. 5—Whitelisting of Control Network Communication.
A tool for detecting unauthorized communication is added to the network to protect the system.

and detection of unauthorized communication. These characteristics can be used to enable communication whitelisting (see Fig. 5).

Unauthorized communication can be detected using the network switch for industrial control systems product released by Hitachi (see Fig. 6), or a product provided by a specialist security vendor. To ensure affinity between these products and the protected systems, it may be possible to define control network types in terms of the templates proposed by Hitachi, enabling easy installation at the site. These types can be defined by evaluating and investigating combinations of systems, taking into account whether they are new or existing systems.

Fig. 6—Network Switch for Industrial Control Systems.
It has been made more environmentally resistant, enabling installation in site equipment. In addition to providing typical network functions, it detects and automatically excludes unregistered communication.

CONCLUSIONS

This article has discussed some examples of template-based security measures that take site workload into account and enable easy installation, while conforming to the characteristics of the protected production line or production control system.

Hitachi will continue to value Hitachi company technology, while providing security ecosystems that serve as total solutions for protecting client systems. These solutions are created by appropriately combining different security products, and are used to protect products such as Hitachi's integrated instrumentation system, and Hitachi's digitally integrated monitoring control system.

REFERENCES

(1) H. Osonoi et al., "Information and Control Platform for Utilization of Plant Data," Hitachi Review **65**, pp. 70–76 (Jun. 2016).
(2) S. Okubo et al., "Plant Monitoring and Control System for Building Secure Systems," Keiso **58**, No. 12, pp. 34–37 (Dec. 2015) in Japanese.

ABOUT THE AUTHORS

Shigenori Kaneko

Control System Platform Development Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of component products for control systems. Mr. Kaneko is a member of the Information Processing Society of Japan (IPSJ), The Society of Instrument and Control Engineers (SICE), and the Society of Project Management (SPM).

Kazunobu Morita

Industrial Manufacturing Solution Division, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd. He is currently engaged in the industrial production solutions business.

Tomoyuki Sunaga

Industrial System Engineering Department, Industrial Manufacturing Solution Division, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd. He is currently engaged in coordinating industrial instrumentation systems.

Hitoshi Murakami

Management & Development Group, Instrument & Control Systems Sales Division, Instrument & Control Systems Division, Hitachi High-Tech Solutions Corporation. He is currently engaged in business planning for industrial instrumentation systems.

Makiko Murakami

Control System Platform Development Department, Control System Platform Development Division, Services & Platforms Business Unit, Hitachi, Ltd. She is currently engaged in the development of middleware software for industrial instrumentation systems.

Katsumi Hanashima

Control System Platform Development Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in coordinating middleware software development for industrial instrumentation systems.

Featured Articles I

Water and Sewage Industry Examples

Security Technology for Wide-area Monitoring and Control Systems

Tadao Watanabe
Kosuke Yamaguchi
Hideyuki Tadokoro, P.E.Jp
Takahiro Tachi

OVERVIEW: Water and sewage are important parts of the social infrastructure, and a variety of initiatives are being considered for overcoming the business challenges they face. One such challenge is the consolidation of their operations, with reports having been prepared in Japan that consider organizational consolidation from a variety of perspectives[1]. When considering the opportunities for interconnecting existing systems that come with consolidation, cybersecurity measures are essential. With security threats becoming more diverse, the changing business environment represented by consolidation means that security measures need to be considered when connecting what were previously closed systems through reconstruction, etc. Hitachi is working on security measures for its monitoring and control systems, paying attention to security trends in the water and sewage industries.

INTRODUCTION

FOLLOWING a period of rapid economic growth, the coverage of water and sewage infrastructure in Japan is at a historically high level, namely 97.7% for water (in FY2013)[2] and 77.6% for sewage (in FY2014, excluding Fukushima Prefecture)[3]. The future maintenance of water and sewage infrastructure is a major challenge for the industry. Moreover, operating conditions are expected to become increasingly difficult as the demographics associated with the aging population and low birth rate indicate falling demand for water in the future. With small and medium-sized organizations facing workforce shortages, many operators are struggling with how to inherit technical skills.

There has been considerable activity aimed at encouraging the consolidation of the scope of organizations, which is an effective way to sustain safe and secure water and sewage service. In the water industry, such initiatives were under consideration by 22 prefectural-level local governments as of December 2015, with the establishment of working groups included among the numerous amalgamation proposals[4]. In the sewage industry, the revised Sewerage Act enacted in May 2015[5] encouraged consolidation projects by freeing up the rules on the establishment of working groups for discussing ways to go about regional coordination between different sewage system operators.

In the field of monitoring and control systems, meanwhile, the consolidation of plant operations will be brought about through the interconnection of existing systems or the installation of new integrated systems. It has become possible to target the optimization of operations at a regional level in place of past practices, which were limited to optimizing the operation of individual plants. This means seeking to achieve system-wide optimization by reallocating water and electric power between organizations to maintain reliable operation and lower energy costs, and by using realtime control. The interconnection of existing monitoring and control systems opens up the prospect of not only optimal control that takes account of the entire system but also improved reliability by allowing central control rooms to provide backup for each other and the ability to manage operations with a smaller workforce through system integration.

Based on this background, this article considers the trends in cybersecurity at water and sewage system operators and describes the security technologies provided by Hitachi's monitoring and control system.

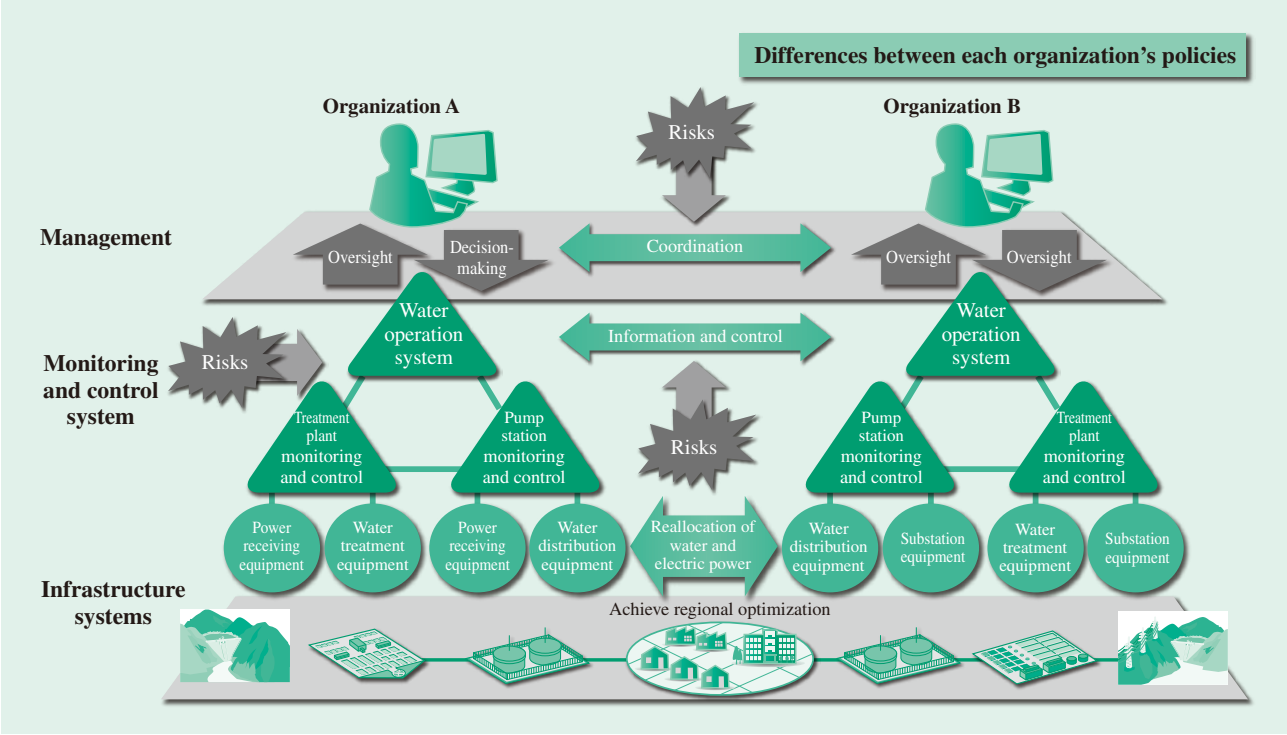


Fig. 1—Security Risks Resulting from System Integration.
The interconnection of systems is essential to achieving optimal operation at a regional level. When different organizations are working together, it is essential to consider security measures on the assumption that the security policies of each organization will be different, including the risks posed by interconnection points.

SECURITY TRENDS

Status of Security in Water and Sewage Industry

An issue raised by interconnection is security. In the case of interconnections between different organizations, risk assessments need to be based on the assumption that the respective security policies of each organization will be different. When a number of different monitoring and control systems are connected via a network, security measures are essential to deal with such risks as the infiltration and spreading of malware via interconnection points (see Fig. 1). It is also recognized that security measures are becoming more complex due to the increasing diversity of security threats and of the methods used to mount attacks (see Fig. 2). Accordingly, when considering security measures, it is important to make a theoretical determination of what type of measures to adopt together with their relative priorities based on a clear understanding of the risks in terms of frequency of incidents and their effects on plant operation.

In October 2015, an experts' committee at The Institute of Electrical Engineers of Japan, Investigating R&D Committee on Survey on the Current Situation and Issues of Security Practices for Water Facilities in Japan, looking at the status and challenges associated with security technology at water and sewage facilities undertook a questionnaire-based survey of security at water and sewage system operators[6]. The survey considered the changes that occurred since the previous survey conducted in 2007. What it found was a small increase in opportunities for interconnection between systems due to changes in the business environment. It also found that there had been no change in how secure systems were, with isolation from external networks being the primary mechanism. However, there is potential for these past assumptions to be overturned as the consolidation of water and sewage systems progresses in the future. It seems likely that demands for security measures will accompany consolidation.

Guidelines for Operation

To date, the issuing of guidelines on security measures that indicate their necessity and importance has been driven by the government.

The Ministry of Health, Labour and Welfare issued "Information Security Guidelines for Water Industry," in October 2006. This document contained basic

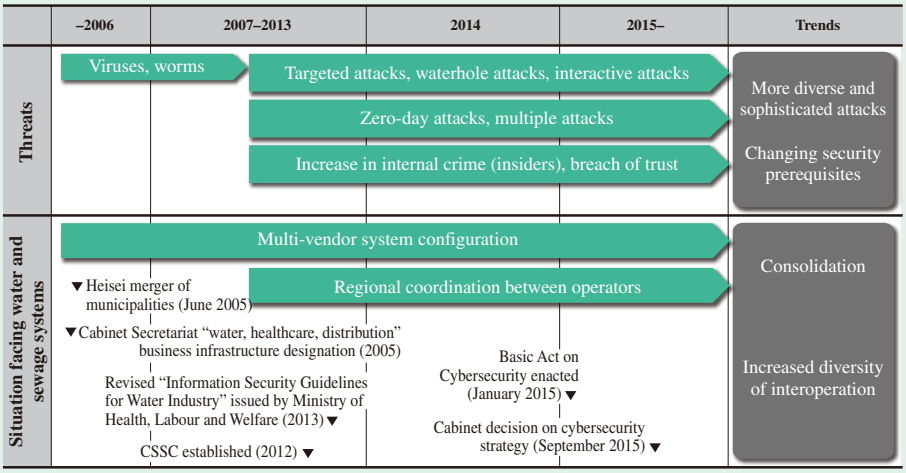


Fig. 2—Security Trends.
As threats become more diverse and sophisticated, the prerequisites for security measures are changing. Security measures are becoming an issue for water and sewage systems due to their consolidation and interoperation of different systems.

instructions that included measures for preventing interruptions to the water supply, which is an important part of the infrastructure. These guidelines were revised in March 2008, and a third edition was published in June 2013 with updates on how to deal with new threats, such as targeted attacks, and changes in how telecommunications technology is used, such as smart devices[7].

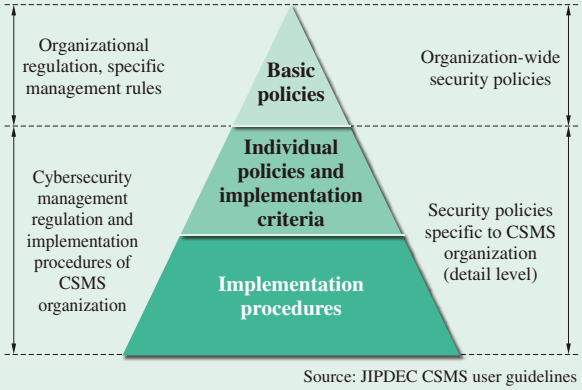
The Basic Act on Cybersecurity enacted in January 2015 called for autonomy on the formulation of criteria for security measures and the staging of drills and exercises by operators of critical infrastructure, including water. Similarly, a cabinet decision on cybersecurity strategy[8] issued based on the new law in September 2015 called for the government, operators of critical infrastructure, and relevant companies to work together voluntarily in giving consideration to national crisis management and security in order to take action on increasingly sophisticated cyber-attacks.

Internationally, meanwhile, following on from industry-specific standards for electric power, petrochemicals, and railways, progress is being made on formulating the International Electrotechnical Commission (IEC) 62443 standard covering all aspects of control systems.

The IEC 62443-1-x series of standards deals with common concepts and terminology. The IEC 62443-2-x series deals with security policies and organizational management systems for the owners of control systems. The IEC 62443-3-x series deals with the technical requirements for control systems for those who implement the systems. The IEC 62443-4-x series is for equipment manufacturers and deals with security requirements for control equipment.

The plan, do, check, act (PDCA) cycle for dealing with system security requirements and changes to the structure of monitoring and control systems is essential for maintaining the security of control systems. Cyber security management system (CSMS) certification provides a framework for this use of PDCA. CSMS certification is the control system equivalent of an information security management system (ISMS) as defined in ISO/IEC 27001 for information systems, and was announced in April 2014 by JIPDEC as a set of certification criteria based on IEC 62443-2-1[9] (see Fig. 3).

It is anticipated that water and sewage system operators will be expected in the future to manage security in accordance with CSMS.



CSMS: cyber security management system

Fig. 3—Organizational Overview of CSMS Certification.
The security policies of organizations that operate control systems are linked to the security policies and information management rules of their parent organization. The formulated security policies must be approved by the relevant manager.

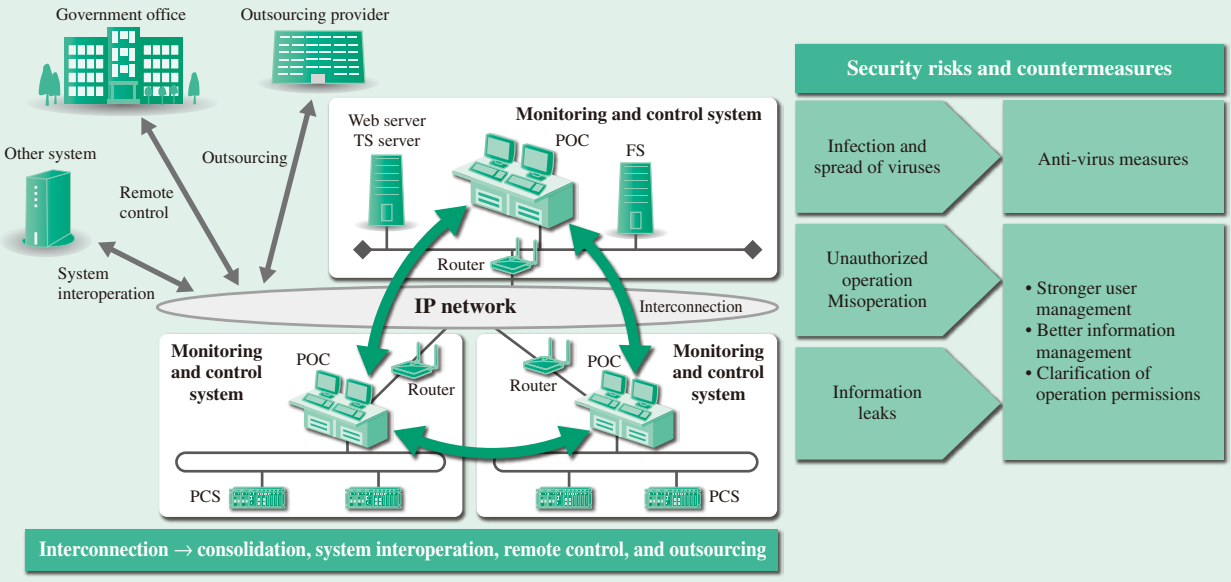


Fig. 4—Interoperation of Monitoring and Control Systems and Security Risks.
Advances in IP networking can help with consolidation by enabling the interconnection of monitoring and control systems. However, this means there is a need for ways of dealing with the security risks that come with interconnection.

SECURITY MEASURES IN MONITORING AND CONTROL SYSTEMS

The interconnection of monitoring and control systems both encourages the integration of monitoring to enable operation with a small number of staff and makes it possible to use outsourcing to achieve rapid fault response and to deal with shortages of technical staff. The possibilities include further efficiencies through interoperation with the systems of adjacent system operators, and skills transfers achieved through the accumulation of know-how and its wider deployment. It also offers a way to create new value by sharing information with other industries and systems.

Given this background, Hitachi's monitoring and control system provides wide-area monitoring and control based on a new domain-based concept that encourages the use of distributed servers connected to a closed Internet protocol (IP) network spanning multiple sites that can be used for cross-system monitoring[10]. Web, terminal service (TS), and other servers can also be installed to provide monitoring and control over a more open IP network.

Anti-virus measures	Whitelist		Prevents execution of viruses that have gained unauthorized access to the system by prohibiting execution of other than a predefined list of programs
Prevent unauthorized operation or misoperation	User management	User authentication	Excludes unauthorized users by login/password authentication of users and an automatic logoff function
		Emergency login	Provides a temporary login for equipment operation in times of emergency by pressing a special key combination
	Information management (traceability)	Operation logs	The user name and the device used to perform each operation is recorded in plant operation logs, which can be viewed using a search function.
		Portable media	A record is kept of removal to external media or printing of data, which can be viewed using a search function.
	Execution control based on user accounts	Operation permissions	The scope of equipment jurisdiction is specified for each user. Equipment can be designed as required with input and output signals to suit plant operation.
		Equipment jurisdiction	Each operational function is assigned a level (routine operation, control parameter modification) based on user permissions.

Fig. 5—Security Functions of Hitachi's monitoring and control system.
To provide reliable system operation and an environment for safe equipment operation, the monitoring and control system is equipped with anti-virus, user authentication, and user operation permission features to protect system assets and functions against security risks.

Whereas past monitoring and control systems were based on a closed architecture, the interconnections associated with system enhancements bring a variety of security risks (see Fig. 4). Hitachi's monitoring and control system, described below, has ways of dealing with these security risks (see Fig. 5).

Whitelist-based Anti-virus Measures

When monitoring and control systems are connected to other systems, there is the risk that a virus infection on one machine could quickly spread to the other connected machines.

Hitachi's monitoring and control system uses whitelist-based anti-virus measures to prevent the infection and spread of viruses. This prevents infection by an unknown virus because it only permits the execution of a predefined list of programs. Because whitelisting does not require an Internet connection to get virus definition updates (unlike blacklisting), it is suitable for use on closed systems and has the advantage of not compromising system stability or responsiveness by having to run routine scans.

On the other hand, whitelisting has no way of eliminating pre-existing viruses. Accordingly, the monitoring and control system uses it in conjunction with virus scanning using a blacklist that is updated by portable universal serial bus (USB) memory to provide dependable measures for preventing the infection and spread of viruses.

User Management and Traceability

The growing use of remote control and outsourcing means that the physical security of the locations from which monitoring and operation are performed may no longer be adequate, creating a requirement for user and information management in response to the risk of unauthorized people operating the systems or stealing data.

User management involves the use of an identity (ID) and password for authentication when accessing the system to prevent login by other than authorized users. To prevent intrusion by an unauthorized person when a user forgets to log off, the monitoring and control system also has a function to automatically log users off if they do not perform any action for a predetermined length of time. Together with improved password management criteria, the system also includes password management functions for specifying how long passwords remain valid and for disabling users who enter an incorrect password more than the permitted number of times.

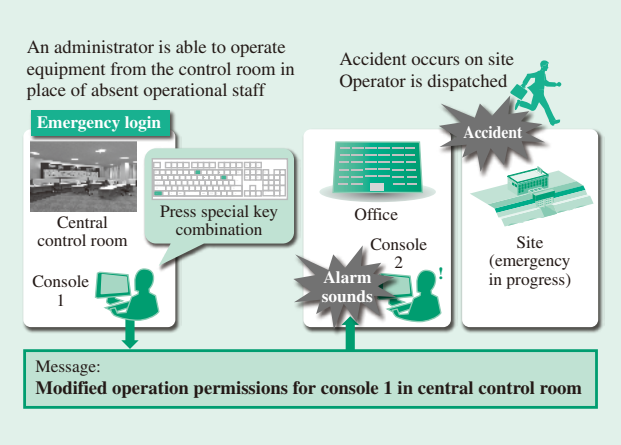


Fig. 6—Emergency Login.
An emergency login function that provides temporary access to equipment operation is provided to deal with the situation when operational staff with operation permissions are absent during an accident or natural disaster.

Another function is provided for the case when operational staff are not present in the central control room to deal with on-site response and other matters when a major accident or disaster occurs, and permitting emergency login by administrators who are able to handle control room operations on their behalf. It provides a temporary login that permits the sorts of equipment operation required in an emergency, enabled by pressing a predefined key combination on the keyboard. An alarm tone sounds continuously during an emergency login to make it clear that emergency operation is in progress (see Fig. 6).

Information management includes a function for appending the user name and the device the user is using to operation logs in order to enable any unauthorized or mistaken operations to be identified afterward. Records are also kept of the removal or printing of system data to ensure that the identity of anyone who removes data can be determined along with the time and the device they used.

Use of User Accounts for Execution Control

Because interconnected monitoring and control systems are used by operational staff at different sites, as shown in Fig. 4, there is a risk of misoperation of equipment outside a user's jurisdiction.

The use of user accounts for execution control makes it possible to combine operation permissions, which specify the level of operations the logged in user is allowed to perform, with an equipment jurisdiction that specifies the range of equipment the user is allowed to operate (see Fig. 7).

User	Operation level	Equipment jurisdiction (group of input/output signals)				
		Power receiving equipment	Water treatment plant	Off-site equipment A	Off-site equipment B	…
User A	Operator	○	×	×	×	
User B	Operator	×	○	×	×	
User C	Operator	×	×	○	○	
User D	Technician	○	○			
User E	Technician	×	×	○	○	
User F	Administrator	○	○	○	○	

Operation / Level	Operation permissions					
	Plant operation			Reporting		Trend graphs
	Machinery operation	Upper and lower alarm settings	PID tuning	Report generation	Data correction	Pen settings
Operator	○	×	×	○	×	×
Technician	○	○	×	○	○	×
Administrator	○	○	○	○	○	○

PID: proportional – integral – differential

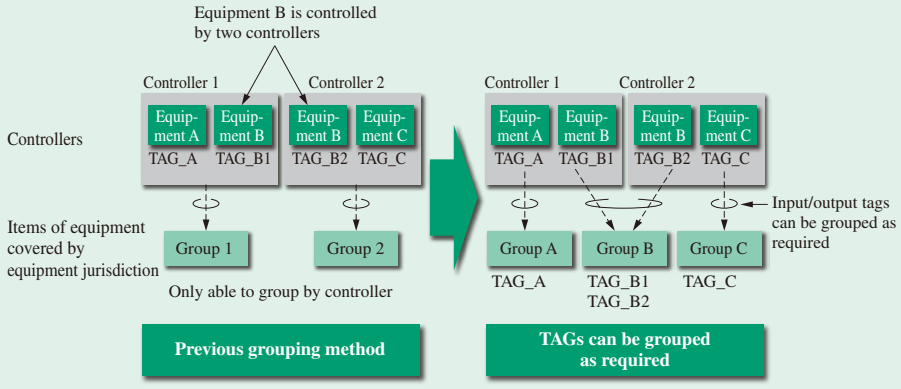
Fig. 7—Level Settings for Operation Permissions.
The system allows equipment jurisdiction and operation permissions to be specified for individual users.

Operation permissions work by predefining the level of operations permitted to operators, technicians, administrators, and other staff, and then assigning each type of user to one of these levels. It is possible, for example, to configure the system such that operators are only permitted to operate equipment, technicians are permitted also to change upper and lower limit alarm settings, and administrators are permitted to perform all of these operations as well as to modify control parameters. The function can be used to assign different operation levels to ordinary and expert operators. Permissions can also be assigned at the level of individual users, such as whether they are permitted to correct report data or specify pen settings for trend graphs.

The equipment jurisdiction function prevents incorrect equipment operation. It works by grouping input and output signals and can be used to specify in detail the scope of monitoring and operation permitted to each operator. The way input and output signals were grouped in the past only allowed grouping to be specified at the level of individual controllers, making it difficult to use in cases when the same controller was used for different equipment or the same equipment was handled by multiple controllers. Because the new method allows all input and output signals handled by the system to be grouped independently, it allows fine-grained control of the scope of monitoring and operation permitted to operators (see Fig. 8).

CONCLUSIONS

This article has described the need for cybersecurity measures in response to the trend toward consolidation of operations, and the security technologies provided by Hitachi's monitoring and control system to meet this need.



TAG: input/output signal tag

Fig. 8—Grouping of Input/Output Signals.
Input and output signals can be grouped as required to provide fine-grained control of the scope of monitoring and operation permitted to an operator.

Hitachi believes that appropriate security measures will improve the convenience of interconnection and lead to the ongoing development of safe and secure water and sewage infrastructure. Hitachi intends to continue developing products with superior security technology and supplying solutions.

REFERENCES

(1) Local Public Enterprise Management Office, Local Public Finance Bureau, Ministry of Internal Affairs and Communications, "Implementation Case Studies of Consolidation Efforts, etc. by Water Utilities," http://www.soumu.go.jp/main_content/000382947.pdf in Japanese.

(2) Ministry of Health, Labour and Welfare, "Trends in Water Supply Coverage," http://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000122560.pdf in Japanese.

(3) Ministry of Land, Infrastructure, Transport and Tourism, "Sewage Treatment Utilization Rate," http://www.mlit.go.jp/common/001103039.pdf in Japanese.

(4) Ministry of Health, Labour and Welfare, "The Need for Water Supply Consolidation, December 2015 Water Supply Division Investigation," http://www.mhlw.go.jp/file/05-Shingikai-10901000-Kenkoukyoku-Soumuka/0000112382.pdf in Japanese.

(5) Sewerage Act, http://law.e-gov.go.jp/htmldata/S33/S33HO079.html in Japanese.

(6) Investigating R&D Committee on Survey on the Current Situation and Issues of Security Practices for Water Facilities in Japan, "Security Management System for Water Facility: A Survey on the Current Situation of Security Practices for Water Facilities in Japan," IEEJ Technical Reports No. 1362 (Oct. 2015) in Japanese.

(7) Ministry of Health, Labour and Welfare, "Information Security Guidelines for Water Industry (the third version)" (Jun. 2013), http://www.mhlw.go.jp/file/06-Seisakujouhou-10900000-Kenkoukyoku/0000046638.pdf in Japanese.

(8) Cabinet Decision, "Cybersecurity Strategy," (Sep. 2015), http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

(9) JIPDEC, "Publishing of Documents Relating to Cyber Security Management System (CSMS) Auditing and Certification for Control Security," http://www.isms.jipdec.or.jp/csms/csmspublish.html in Japanese.

(10) T. Watanabe et al., "Information and Control Systems to Support Planning, Operation, and Maintenance Activities for Sustainability of Water Supply and Sewage Facilities," Hitachi Review **63**, pp. 500–507 (Sep. 2014).

ABOUT THE AUTHORS

Tadao Watanabe

Public Control Systems Engineering Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of monitoring and control systems for water supply and sewage.

Kosuke Yamaguchi

Public Control Systems Engineering Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of monitoring and control systems for water supply and sewage.

Hideyuki Tadokoro, P.E.Jp

Public Control Systems Engineering Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the research and development management of water supply and sewerage operation and control systems. Mr. Tadokoro is a member of The Institute of Electrical Engineers of Japan (IEEJ), the Society of Instrument and Control Engineers (SICE), and The Society of Environmental Instrumentation Control and Automation (EICA).

Takahiro Tachi

Water Solutions Division, Water Business Unit, Hitachi, Ltd. He is currently engaged in general management of research and development on water environments. Mr. Tachi is an expert member of the International Organization for Standardization (ISO) Technical Committee 224, Working Groups 7 & 9, and a member of EICA, and the Catalysis Society of Japan (CATSJ).

Featured Articles I

Financial Industry Examples

Incident Response Team Activities in Finance

Mari Miyazaki
Hiroyuki Hatanaka
Katsunori Takahashi
Momoko Nagata

OVERVIEW: With DDoS attacks and the spread of malware infiltration targeting Internet banking, there is a growing threat of cyber-attacks in the financial industry, one of the country's key infrastructure sectors. Against this background, financial institutions have responded by working rapidly to establish response measures for cyber-attacks, and are increasingly sharing cyber-attack-related information among themselves. Hitachi has a Group-wide incident response team called HIRT, with a financial sector subset called HIRT-FIS that promotes incident readiness activities for the financial sector. Hitachi also operates a joint internet banking center, which has continually provided security measures to combat today's constantly changing threats since the service started.

INTRODUCTION

SOFTWARE vulnerabilities, security incidents, and security accidents are being reported on a daily basis and represent major threats not only to key infrastructure companies, but also to the organizations in charge of the systems of those companies. Hitachi, Ltd.'s Financial Information Systems Division has helped create safe and secure financial systems through activities such as revising the Security Guidelines on Computer Systems for Banking and Related Financial Institutions (hereafter, FISC Security Guidelines) published by the Center for Financial Industry Information Systems (FISC), and constructing and operating systems designed in conformance with these guidelines.

However, recently, the repeated occurrence of unauthorized funds transfers done through Internet banking using malware, and the increase in activities taking advantage of the dissemination of vulnerability intelligence are creating a demand for fresh approaches at financial sites. This article discusses Hitachi's work on security measures in the financial sector.

SECURITY TRENDS IN THE FINANCIAL INDUSTRY

Financial Services Agency Activities

In April 2015, Japan's Financial Services Agency (FSA) revised some of its guidelines relating to system risks and Internet banking such as its Comprehensive Guidelines for Supervision of Major Banks, etc. and its Financial Inspection Manual.

The revisions call strongly for ensuring the security of Internet banking, and for developing cybersecurity management measures such as Computer Security Incident Response Teams (CSIRTs). They also make reference to specific technical measures in the form of intrusion detection systems, distributed denial of service (DDoS) attack response measures, and detection/blocking of improper communication.

In July 2015, the FSA released its Policy Approaches to Strengthen Cyber Security in the Financial Sector. In line with these policies, hearings were conducted to determine the state of work on cybersecurity management measures at financial institutions, and the efficacy of these measures.

FISC Activities

In June 2013, FISC established the Council of Experts on Countermeasures Against Cyber Attacks on Financial Institutions. The council consisted of experts from industry and academia (with members from government taking part as observers). It investigated the current state of cyber-attacks on financial institutions along with future efforts, and ultimately created a report of its findings. The report was used to investigate revisions in the FISC Security Guidelines (Revised Supplement to the Eighth Edition)

published by FISC, to which new items pertaining to the establishment of cyber-attack response measures were added.

In July 2015, FISC started a new initiative, administering the FISC Cyber Security Reference Information. This initiative consists of releasing useful notes and reference information when an event such as a security incident occurs, to ensure that the FISC Security Guidelines are interpreted properly.

Information-sharing Community Activities

Recently, financial institutions have been increasingly coordinating their cyber-attack-related information by joining information-sharing communities.

The Financials Information Sharing and Analysis Center Japan (Financials ISAC Japan) organization was created for sharing cybersecurity-related information among Japanese financial institutions. It originated from security study groups from major financial institutions, and began operation in November 2014.

According to the Financials ISAC Japan website, the organization has a total of 222 members (full members and associate members) as of the end of April 2016. Financials ISAC Japan shares information on incidents and vulnerabilities, and organizes working group activities on individual topics related to specific key issues.

Financial institutions that have created in-house CSIRTs are joining the Nippon Computer Security Incident Response Team Association (NCA). The NCA is a community created in 2007 to enable information sharing and coordination among Japanese CSIRTs. As of April 2016, it has a total of 137 member teams, of which 27 are CSIRTs in financial institutions. Membership is expected to continue to grow in the future.

This is how the culture of sharing cybersecurity-related information is rapidly being formed among Japanese financial institutions.

SECURITY INITIATIVES IN INTERNET BANKING

Responding to Unauthorized Funds Transfer Losses

The situation surrounding Internet banking has changed dramatically over the past few years. Publicly-released materials from Japan's National Police Agency show that losses to Japanese financial institutions from unauthorized funds transfers have been rapidly increasing since about 2013, with the amount of losses surpassing 3 billion yen for the first time in 2015. There is no doubt that measures to combat losses from unauthorized funds transfers are currently considered the most crucial area of security measures among banks.

Since beginning operation in 1999, Hitachi's joint internet banking center has responded to a widely evolving array of cyber-attacks by continually providing security measures to combat these ever-changing threats. While it is difficult to predict unknown threats that could occur in the future and take action beforehand, effective security measures for threats that have been identified so far are scheduled for wholesale and retail release in FY2016. Through these releases, the joint internet banking center plans to complete its release of functions for security measures conforming to the Japanese Bankers Association's "Understanding" on Improving/Strengthening Security Measures released by the Japanese Bankers Association.

Hitachi's joint internet banking center also works on early detection and prevention of losses from unauthorized funds transfers through operations-based measures. If a depositor suffers a loss from an unauthorized transfer, the joint internet banking center investigates whether similar unauthorized funds transfer losses have occurred in the past at any other banks, and immediately contacts those banks if suspicious transactions are found. It also monitors account access in anticipation of similar unauthorized funds transfers occurring in the future. If a monitored account is accessed, the relevant institution is contacted immediately to enable early discovery.

FISC Compliance

To provide comprehensive security measures for Internet banking, Hitachi is working on facility-, operations-, and technology-based security measures in conformance with the FISC Security Guidelines.

In the area of equipment, it has created data center facilities that offer high reliability, safety, and confidentiality, and conform to official standards such as those set by the International Organization for Standardization (ISO) (see Fig. 1).

In the area of operations, Hitachi has created operations management standards, and uses internal and external audits to check the efficacy of management standards and investigate items for implementation.

In the area of technology, it is working to protect information resources and public servers connected to the Internet through multiple network- and application-level measures, and is investigating efficacy through periodic vulnerability checks.

Location/building

- Highly safe region and ground environment with few natural disasters
- The spread foundation structure employed can withstand earthquakes of up to magnitude 7 on the Japanese scale (as large as the 2011 Great East Japan Earthquake).
- Close to police stations/fire stations
- Equipment conforms to financial industry FISC standards

Power/air conditioning equipment

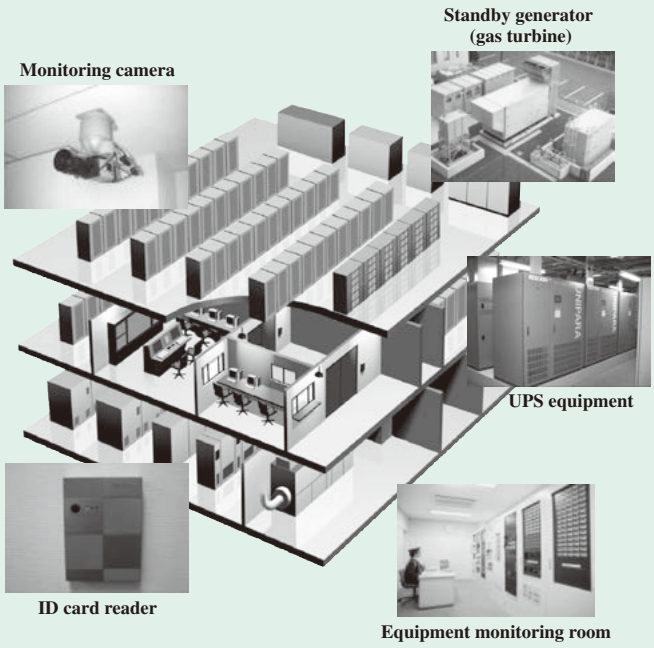
- Powered directly by underground cables from the power station
- Power equipment redundancy eliminates power failures.
- Equipment such as UPS and a standby generator ensure power failure readiness.
- The air-cooled air conditioning equipment shuts off the water supply during disasters.

Information security

- Security management conforming to ISMS certification standard
- Operation and management system conforming to ISO 9000 quality control systems

Other

- A hardware maintenance team is stationed in the same building.



FISC: Center for Financial Industry Information Systems UPS: uninterruptible power supply ISMS: information security management system
ISO: International Organization for Standardization ID: identification

Fig. 1—Data Center Equipment at Hitachi's Joint Internet Banking Center.
Data center equipment conforming to industry standards and official standards such as FISC standards, ISO 27001, and ISO 9000 enables high reliability, safety, and confidentiality.

CSIRT ACTIVITIES IN THE FINANCIAL SECTOR: HIRT-FIS

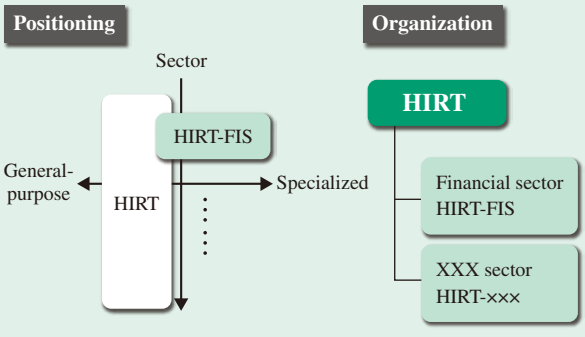
The Hitachi Incident Response Team (HIRT) is Hitachi's CSIRT. In October 2012, a subset of HIRT called Financial Industry Information Systems HIRT (HIRT-FIS) was created for the financial sector (see Fig. 2).

HIRT-FIS engages in incident readiness activities in the financial sector, aiming to serve as a professional CSIRT team specializing in the sector, while keeping abreast of industry-specific conditions and trends through FSA and FISC regulations and guides.

Activities within the Organization

To respond to cyber-attacks, it is vital to keep abreast of current threats and be quick to study and implement responses. HIRT-FIS makes daily checks of publicly-released incident information, and posts it on its intranet site.

The aim of these activities is to provide the latest security information to Hitachi sales representatives and system engineers (SEs) who are involved with the



HIRT: Hitachi Incident Response Team
HIRT-FIS: Financial Industry Information Systems HIRT

Fig. 2—HIRT-FIS Positioning.
HIRT-FIS is located within the Financial Information Systems Division, as the financial sector subset of HIRT.

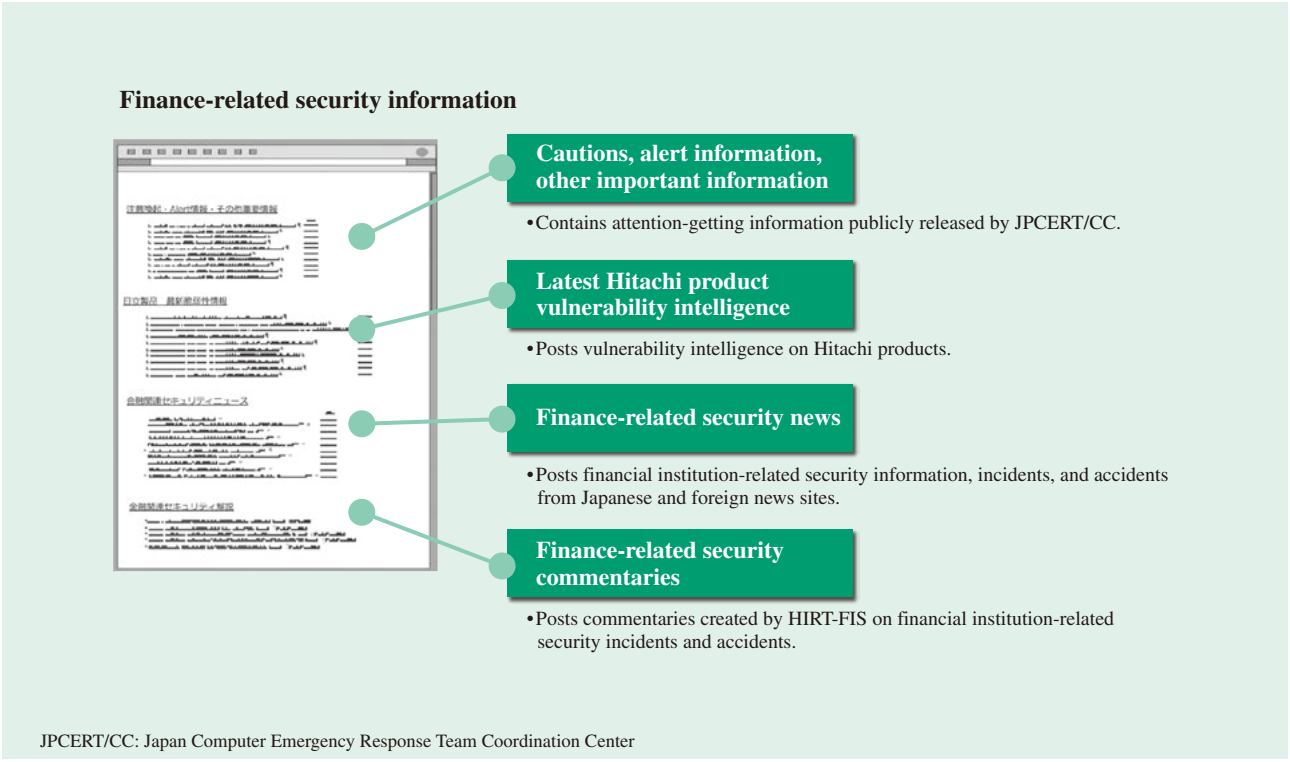


Fig. 3—HIRT-FIS Portal.
HIRT-FIS posts finance-related security information on its intranet site.

financial industry, to enable as early a start as possible for activities to reduce anticipated threats. Information is posted in the following four categories (see Fig. 3):
(1) Cautions, alert information, other important information

Mainly consists of alert information publicly released by the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

(2) Latest Hitachi product vulnerability intelligence

Consists of vulnerability intelligence publicly released by Hitachi.

(3) Finance-related security news

Consists of incident information related to financial institutions in Japan and abroad.

(4) Finance-related security commentaries

Consists of commentaries created on topics of high concern.

This information is used to help respond to inquiries received from other Hitachi departments, to assist with reviews of documentation such as security designs and security operation procedures, and to assist with evaluations of vulnerability check results.

HIRT-FIS is also responsible for creating security guides for SEs, disseminating information in-house through an email newsletter, and training financial sector security staff.

Coordination Activities among Organizations

HIRT acts as Hitachi's CSIRT office for dealing with external organizations, providing assistance with cybersecurity measures. It also works on improving CSIRT coordination among organizations through the NCA. This activity is designed to enable coordination among CSIRTs at different organizations, providing a more sweeping view of cyber-attacks for use in problem-solving, and enabling mutual assistance with activities.

As HIRT's financial subset, the role of HIRT-FIS in this activity is to coordinate financial institution CSIRTs.

CONCLUSIONS

This article has described the state of cybersecurity for financial systems, the security work being done by Hitachi's joint internet banking center, and the work being done by HIRT-FIS.

Financial institutions have traditionally changed staff roles through a rotation system, including staff who work with information systems. However, financial institutions are flexibly altering their human resources policies, making changes such as handling the highly specialized jobs done by security staff as

special appointments. These changes indicate that cybersecurity response measures are taking firm hold in the financial industry, and that the environment for coordination among highly specialized CSIRTs is becoming more active.

Initiatives related to the services Hitachi provides, and initiatives engaged in by specialist security departments are the two pillars of Hitachi's security activities, and Hitachi believes these activities will help ensure safe and secure financial systems in partnership with financial institutions.

REFERENCES

(1) The Center for Financial Industry Information Systems Website, https://www.fisc.or.jp in Japanese.
(2) Financial Services Agency Website, http://www.fsa.go.jp in Japanese.
(3) Financials ISAC Japan Website, http://www.f-isac.jp in Japanese.
(4) Nippon CSIRT Association Website, http://www.nca.gr.jp in Japanese.
(5) National Police Agency Website, https://www.npa.go.jp in Japanese.

ABOUT THE AUTHORS

Mari Miyazaki
CSIRT Group, General System Department, Financial Project Management Unit, Financial Information Systems Division, Financial Institutions Business Unit, Hitachi, Ltd. She is currently engaged in CSIRT activities as HIRT-FIS staff.

Hiroyuki Hatanaka
Planning Group, Financial Channel Solution Department 1, Financial Channel Solution Business Unit, Financial Channel Solutions & Payment Services Division, Financial Institutions Business Unit, Hitachi, Ltd. He is currently engaged in the planning of financial channel solutions.

Katsunori Takahashi
CSIRT Group, General System Department, Financial Project Management Unit, Financial Information Systems Division, Financial Institutions Business Unit, Hitachi, Ltd. He is currently engaged in CSIRT activities as HIRT-FIS staff.

Momoko Nagata
CSIRT Group, General System Department, Financial Project Management Unit, Financial Information Systems Division, Financial Institutions Business Unit, Hitachi, Ltd. She is currently engaged in CSIRT activities as HIRT-FIS staff.

Featured Articles I

Citywide Protection Examples

Global Work on Protecting the Safety and Security of Cities

Ryota Masuda
Saneyuki Fujita
Makoto Namai
Justin Bean

OVERVIEW: Although life in cities equipped with a variety of social infrastructure and facilities is convenient, residents are exposed to a large number of threats, such as terrorism, crime, and urban disasters. Hitachi has compiled the requirements for protecting cities from these threats, and provides solutions for ongoing implementation of appropriate responses. This article describes some examples of the work that Hitachi has done in the USA and Singapore on technology and solutions in this area with features such as an integrated monitoring center that enables monitoring and response measures for entire cities, a vehicle screening system, and an explosives trace detection system. Hitachi will continue to help create safe and secure cities by providing robust and advanced security products and services.

INTRODUCTION

CITIES are convenient places to live since they are equipped with social infrastructure such as electricity, water, and public transport, along with a variety of facilities such as housing, offices, and commercial facilities. However, while residents enjoy the benefits of urban life, they are also exposed to a large number of threats including various crimes such as the seemingly endless series of international terrorist acts and enduringly common crimes such as phone fraud. There are also new types of natural disasters such as urban flooding caused by intense localized thundershowers.

Japan will soon host events that will be closely followed around the world (in 2019 and 2020), making it crucial for the country to determine how best to protect the safety and security of its cities as a whole. This article looks at Hitachi's work on addressing this issue.

SECURITY SOLUTIONS FOR PROTECTING CITIES

Hitachi has compiled a set of security requirements needed to protect cities from threats such as natural disasters, cyber-attacks, and terrorism, with the three concepts[1] of "Adaptive," "Responsive," "Cooperative". Hitachi provides security solutions by continually implementing appropriate security measures in compliance with the International Organization for Standardization (ISO) 22320 international crisis management standard (see Fig. 1).

Specifically, it performs multifaceted monitoring of social infrastructure by using monitoring cameras, access control systems, along with satellites, unmanned aerial vehicles, network monitoring, and other sensors to assess the ever-changing situation in both the physical and cyber realms. It provides action support through physical means such as robots and security gates, while analyzing and predicting information obtained by these means using geographic information systems (GIS), imagery analysis, and simulation technology. These activities and know-how based on the observe, orient, decide, act (OODA) process support rapid and accurate decision making. They also support prompt action through the automatic detection of warning signs identified by real-time processing of large amounts of collected monitoring data. The system can be configured and installed quickly thanks to a flexible choice of hardware configuration based on the nature of the operation and existing equipment. (see Fig. 2).

Integrated Monitoring Centers that Protect Cities

Recent urbanization has resulted in the growth and diversification of the facilities and infrastructure composing cities, creating a need for integrated use

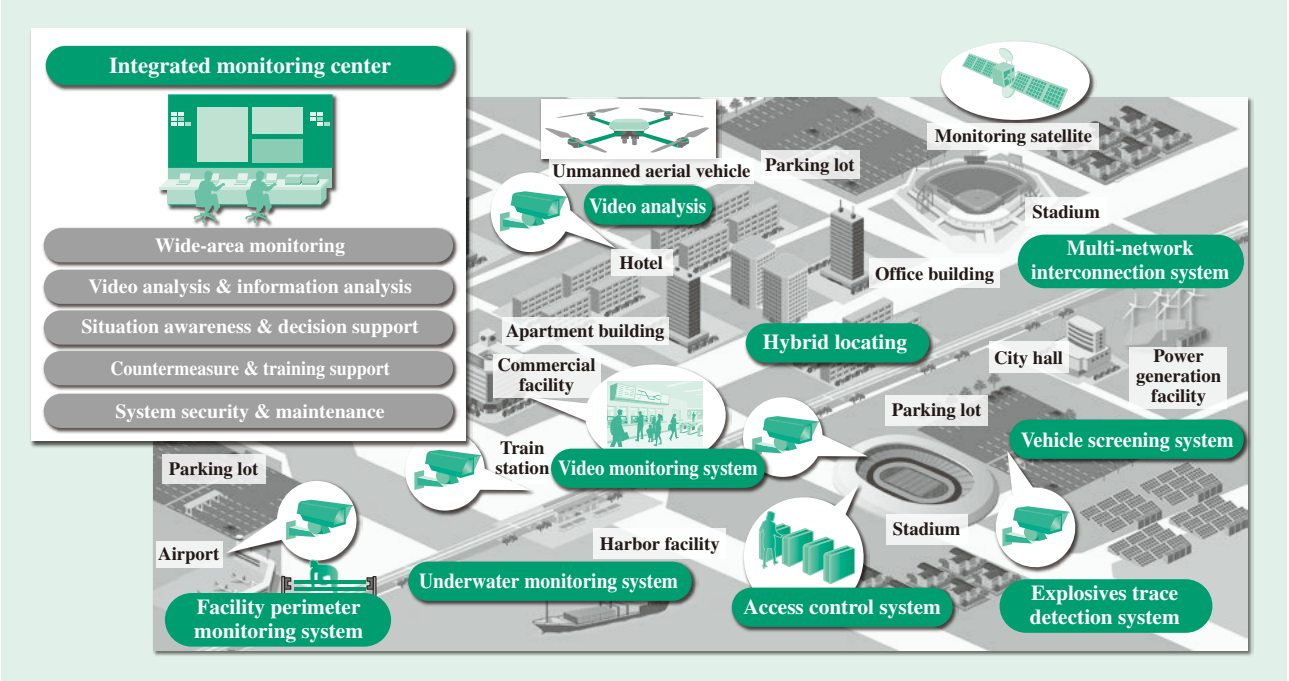


Fig. 1—Overview of Security Solution for Protecting Cities.
The security solution includes an integrated monitoring center that collects information from widely dispersed sensors (monitoring cameras and sensors in facilities and infrastructure control systems), which achieves situation awareness throughout the entire city. By analyzing and processing the collected information, the security solution achieves wide-area monitoring that assists with precise and rapid countermeasures.

of sensors and information to monitor facilities and areas that have so far been monitored individually. Hitachi provides integrated monitoring centers that perform integrated monitoring of an entire city as a single area, creating safe, secure, and comfortable lives for residents in areas including various facilities.

The centers achieve wide-area monitoring using various types of sensors interconnected by a common interface. The information from these sensors is analyzed to detect abnormalities in real time for use in preventing crime and in counter-terrorism. Decision support systems driven by GIS technology-

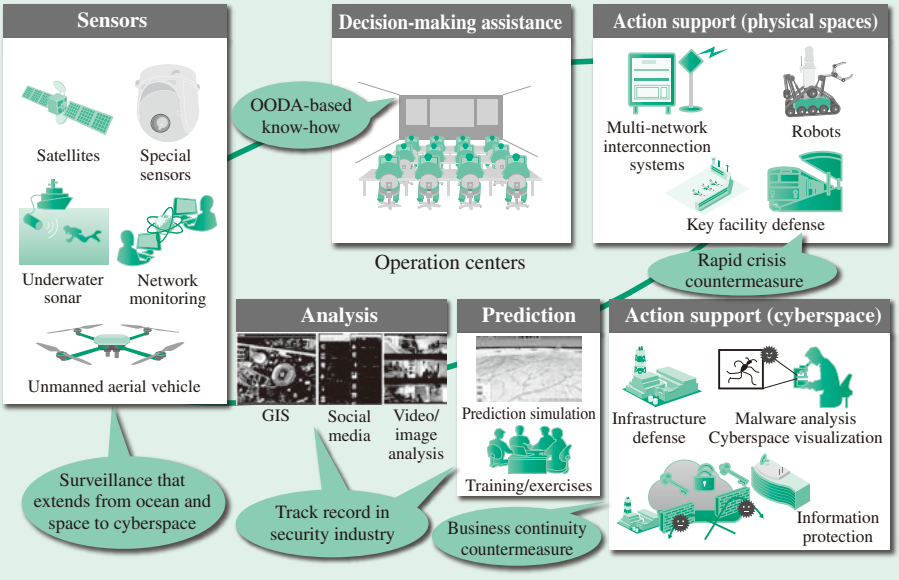


Fig. 2—Component Technologies of Security Solutions for Protecting Cities.
In multiple dimensions, from underwater to up in the sky, Hitachi can provide a variety of solutions that support both physical spaces and cyberspace.

based visualization and the OODA process enable precise situation awareness and decision making. Coordination with mobile terminals and various communication devices enables rapid processing of sharing information with sites and issuing of response instructions.

By detecting dangerous acts, suspicious persons, and suspicious items, the centers enable accident prevention, and by detecting people who have sudden illness or who need nursing care, they enable more rapid responses to situations and better service.

In addition to the normal operations of monitoring, analysis, decision making, and response, the centers also use simulation technology to help improve training and operation. Cybersecurity technology that prevents unauthorized access to sensors and integrated monitoring center systems ensures system safety.

Hitachi provides a complete lineup of services for these integrated monitoring centers and other large-scale monitoring systems, ranging from installation consulting to system integration.

Vehicle Screening System

At checkpoints on public roads and access control points at entrances to key facilities, officials check vehicle interiors and vehicle numbers, and inspect for hazardous items under vehicles. Hitachi provides a vehicle screening system that enables rapid and precise inspections under vehicles (see Fig. 3).

Using this system enables faster checks under vehicles than hand-mirror checks, enabling smoother vehicle passage. Under-vehicle inspection images can also be recorded and saved, enabling later use of the image data if needed.

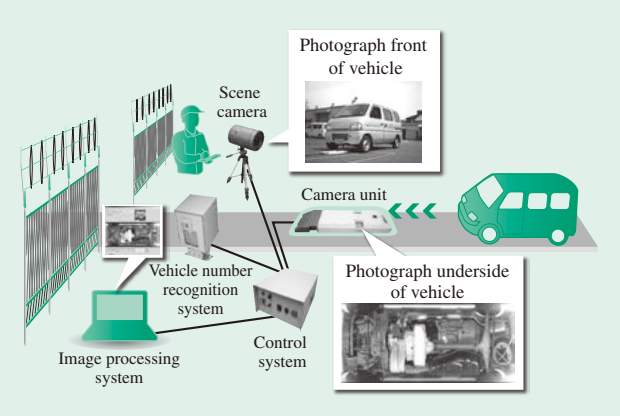


Fig. 3—Overview of Vehicle Screening System.
The system can be installed easily without preliminary construction, and enables smoother inspections for abnormalities under vehicles than hand-mirror inspections.

The vehicle screening system consists of a camera unit, control system, scene camera, vehicle number recognition system, and image processing system. The highly portable camera unit is designed with a size that enables passage of vehicles with low minimum ground clearances. The system has very high utility, enabling use just by placing it on the road, with no need for preliminary construction during installation.

The system was used for security since the Asia-Pacific Economic Cooperation (APEC) forum in 2010[2]. Its use at key facilities and a major international sports event in 2020 is anticipated in the future.

Multi-network Interconnection System

The facilities and infrastructure composing cities today each have their own communication networks, and are not sufficiently interconnected. To enable rapid and precise responses to situations, there is a need for information-sharing between integrated monitoring centers and sites, and information coordination among facilities and organizations. Means of communication that connect these communication networks together are becoming increasingly important. There is also a renewed recognition of the need for response measures that anticipate communication failures during major disasters.

Hitachi provides a multi-network interconnection system that provides wide-area voice and data communication by integrating different means of communication such as existing-infrastructure communication facilities, mobile phones, and radios (see Fig. 4).

The multi-network interconnection system provides seamless wireless and wired communication, incorporating unique communication protocols resembling radios that identify terminals by frequency or modulation type, and enabling normally impossible communication such as calls between radio and telephone equipment. By using the Internet protocol (IP) to integrate information from broadband wireless transmission equipment and existing communication infrastructure, the multi-network interconnection system can easily provide high-speed data communication of video information, etc. in addition to voice.

The system is a portable type that fits in a rack, so it can be transported by car, enabling easy construction of proprietary communication infrastructure in areas of communication failure during major disasters.

The system was used to enable rapid recovery of the communication infrastructure of Japan Air Self-Defense Force (JASDF) Matsushima Air Base, which

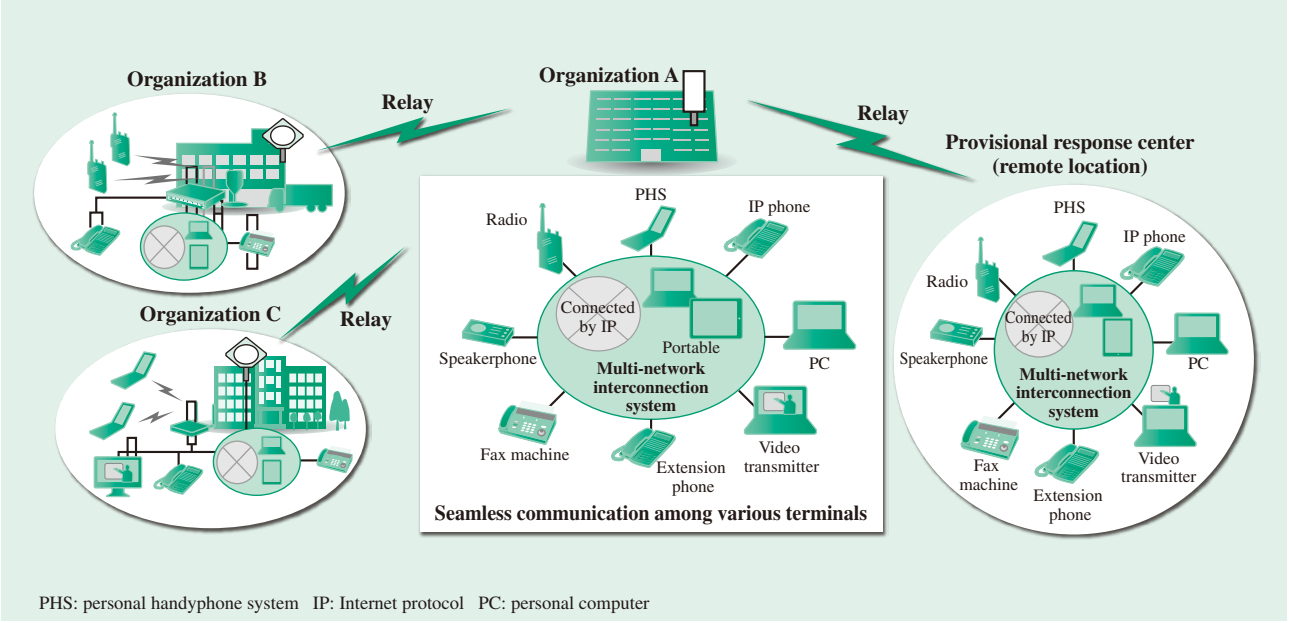


Fig. 4—Overview of Multi-network Interconnection System.
The system seamlessly connects both wireless and wired communication devices that use various communication protocols, such as mobile phones and radios. It enables easy construction of proprietary communication infrastructure.

was damaged during the Great East Japan Earthquake of 2011, and has since been used to construct various communication infrastructure[3].

Explosives Trace Detection System

Hitachi, Ltd. started developing a security gate with built-in explosives trace detection system in 2010 using "R&D Program for Implementation of Anti-Crime and Anti-Terrorism Technologies for a Safe and Secure Society", Funds for Integrated Promotion of Social System Reform and Research and Development of the Ministry of Education, Culture, Sports, Science and Technology, Japan[4]. This project was done in collaboration with University of Yamanashi and Nippon Signal Co., Ltd., and in 2014, Hitachi developed a prototype of the security gate which detected explosive particles with low false positive rate (<0.1%) within 3 sec after a subject passes through the gate. Those features were realized by using a high throughput particle concentrator and high efficient ionization source (See Fig. 5). The gate enables the inspection of all subjects passing through the gate, which cannot be realized by conventional wipe-sampling systems.

In 2015, Hitachi started a project for the commercialization of such gate for nuclear plants and plan to complete it in 2016. By expanding a lineup of physical security systems, Hitachi will contribute to realize the secure cities.

EXAMPLES OF OVERSEAS ACTIVITIES

Activities in the USA

In the USA, Hitachi provides the Hitachi Visualization Suite, public safety solutions that enable customers to grasp the situation rapidly and precisely through real-time displays created by integrating video from surveillance cameras with information from various

Fig. 5—Security Gate with Built-in Explosives Trace Detection System.
The explosives trace detection system was developed by Hitachi, Ltd., University of Yamanashi, and Nippon Signal Co., Ltd. in collaboration on the R&D Program for Implementation of Anti-Crime and Anti-Terrorism Technologies for a Safe and Secure Society and Funds for Integrated Promotion of Social System Reform and Research and Development from the Ministry of Education, Culture, Sports, Science and Technology, Japan.

Fig. 6—Map displayed by Hitachi Visualization Suite, Public Safety Solutions.
A video from surveillance camera is displayed on a map, along with information from various systems (such as the location where the crime was reported and license plates of nearby cars) and sensor information (such as gunshots). The display integrates these various types of information and enables public safety departments to get clear grasp of the situation.

systems and sensors. These solutions have been delivered to about 80 municipal police departments including the Austin Police Department as well as stadium/event agencies, and contribute citizen's safety.

For example, if a citizen calls the police to report a crime, the report details and reporter location are displayed on a map. This information is accompanied by video from surveillance cameras installed nearby, along with information from sensors (such as gunshot detection sensors). This enables police to get better situation awareness. Then police can assign their resources more efficiently and effectively (see Fig. 6). In addition, the system features Predictive Crime Analytics, which use historical data to give the police a likelihood that a type of crime will occur at a given time and place before it happens, to help the officers be in the right place at the right time to prevent the crime from happening.

Activities in Singapore

In Singapore, one of the safest countries in the world, the Economic Development Board and the Ministry of Home Affairs jointly set up the Safety & Security Industry Programme Office (SSIPO) to promote innovation capabilities in the safety and security industries. The SSIPO identifies challenges arising from homeland security and urbanization and creates opportunities for industry partners to develop and test new solutions in a live environment in Singapore.

Hitachi showcased its pioneering and cutting-edge technology on urban security solutions called Similar Face Search during the first testbed led by SSIPO in 2013-2014[(5)]. Also, its video content analysis and biometrics technologies will be candidates for validation through the second testbed planned by SSIPO from 2016 to 2020.

CONCLUSIONS

This article has described some of the work being done by Hitachi on protecting the safety and security of cities. It will continue to provide robust, advanced, and high-utility security products and services to support the safety and security of cities.

REFERENCES

(1) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).
(2) National Police Agency, "2010 APEC Security," Focus Issue No. 279 (Mar. 2011), https://www.npa.go.jp/archive/keibi/syouten/syouten279/p22.html in Japanese.
(3) T. Sato et al., "Flexible Communication Infrastructure Using Existing Systems and Terminals," Hitachi Review **62**, pp. 174–179 (Apr. 2013).
(4) Hitachi News Release, "Development of Real-time Human Tracking Technology by Linking Walk-Through Style Explosive Detection Equipment and Surveillance Camera Network" (Dec. 2010), http://www.hitachi.com/New/cnews/101202.html
(5) Hitachi Asia Ltd. News Release, "Hitachi Asia Partners with AGT International-O'Connor's Consortium for Singapore's Safe City Test Bed Project," (May 2014), http://www.hitachi.com.sg/press/press_2014/20140528a.html

ABOUT THE AUTHORS

Ryota Masuda

Security Business Division, Service Strategy Division, Social Innovation Business Division, Hitachi, Ltd. He is currently engaged in security solutions for social infrastructures.

Saneyuki Fujita

Business Development Center, Business Advancement Division, Defense Systems Business Unit, Hitachi, Ltd. He is currently engaged in business development for the social infrastructure security sector.

Makoto Namai

Nuclear Power Control and Instrumentation Systems Engineering Department, Power Information & Control Systems Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the design of a physical security system.

Justin Bean

Hitachi Data Systems Corporation. He is currently engaged in the marketing of smart city solutions.

Featured Articles II

Security Platforms

Hitachi's Security Solution Platforms for Social Infrastructure

Toshihiko Nakano, Ph.D.
Takeshi Onodera
Tadashi Kamiwaki
Takeshi Miyao

OVERVIEW: Recent years have seen an increase in the number of security threats to social infrastructure systems, including targeted attacks directed at more specific objectives and attacks that affect the public. Advances in IoT technology, meanwhile, are increasing the potential for cyber-attacks from a wide range of sources. Insider and terroristic incidents are also on the rise. Hitachi uses the Hitachi system security concept as a basis for considering the security requirements for protecting social infrastructure systems, and is working on the development of a security solution platform that combines various measures required by management, operations, and on-site systems. To provide safe social infrastructure systems that everyone can be confident of using, Hitachi intends to supply solutions that can be precisely tailored to changes such as the proliferation of security threats and open architectures.

INTRODUCTION

SECURITY threats to social infrastructure systems are increasing in both the cyber and physical realms. In cyberspace, this includes an increase in targeted attacks directed at more specific objectives and attacks on the equipment used to control social infrastructure systems. Advances in Internet of Things (IoT) technology are accelerating use of system interoperation and increasing the potential for cyber-attacks from a wider area to have an impact on functions that are intimately involved in operations. In the physical realm, meanwhile, insider and terroristic incidents are also on the rise.

Taking note of the trends in these threats, the characteristics of the social infrastructure systems to be protected, and developments in techniques for open innovation starting with the IoT, Hitachi proposed its views on the security requirements for social infrastructure systems, a subject being worked on at the International Electrotechnical Commission (IEC)[1], an international standards body. The proposal was expressed as the Hitachi system security concept, requiring that these systems be adaptive, responsive, and cooperative. The requirements were presented and adopted in a whitepaper entitled *Factory of the Future*[2] on how factories will look in the future and

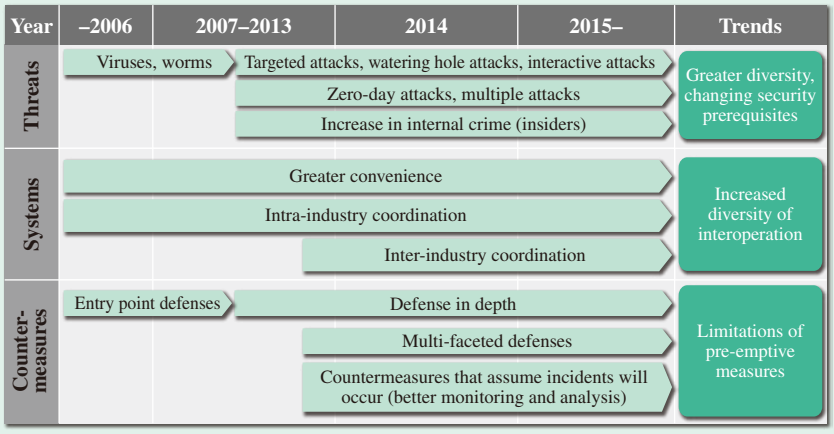


Fig. 1—Security Trends.
Along with security threats becoming more diverse in recent years, interoperation between social infrastructure systems is also increasing and taking on various forms. This demands new thinking about how to provide countermeasures.

the technologies that will be required. Hitachi is promoting the development of a variety of security solution platforms based on this concept.

This article contains an overview of security trends in social infrastructure systems that includes examples of the types of social infrastructure systems being considered, and presents a profile of a security solution platform based on the Hitachi system security concept[3] for the security requirements of social infrastructure systems.

TRENDS IN SECURITY

This chapter gives an overview of trends in threat identification, system configuration, and countermeasures that are essential to the security of social infrastructure systems (see Fig. 1).

While security threats are continually changing, the nature of attacks has become more diverse in recent years, including zero-day attacks in cyberspace and attacks that have both a cyber and a physical aspect. Insider incidents, in which an attack is perpetrated by someone involved with the system, also need to be considered. In terms of the system configurations on which all this is based, growing use of symbiotic autonomous decentralized architectures in which systems are interconnected in ways that transcend industries, applications, and nations is anticipated due to such developments as the proliferation of the IoT and supply chains. Fig. 2 shows examples of social infrastructure systems that interoperate over an open architecture. In addition to operating in ways that go beyond their locations, these systems utilize a variety of services for making the best use of planning, operational, and other data. A point to note about these social infrastructure systems is that each one operates autonomously, and so it is important that each system also maintains its own security in an autonomous way. As a result, maintaining security is also essential for the social infrastructure as a whole.

Unfortunately, greater use of interoperation makes it more difficult to predict the incidence and consequences of security threats accurately, making pre-emptive countermeasures increasingly problematic. Two important factors in considering how to respond to such security trends are to formulate security measures on the assumption that threats will manifest and to maintain on-site safety. This means ensuring the safety of those things that social infrastructure systems are intended to protect (including people, goods, information, and the environment), making it essential that systems provide protection on multiple fronts and incorporate security measures that satisfy this requirement for both the cyber and physical realms.

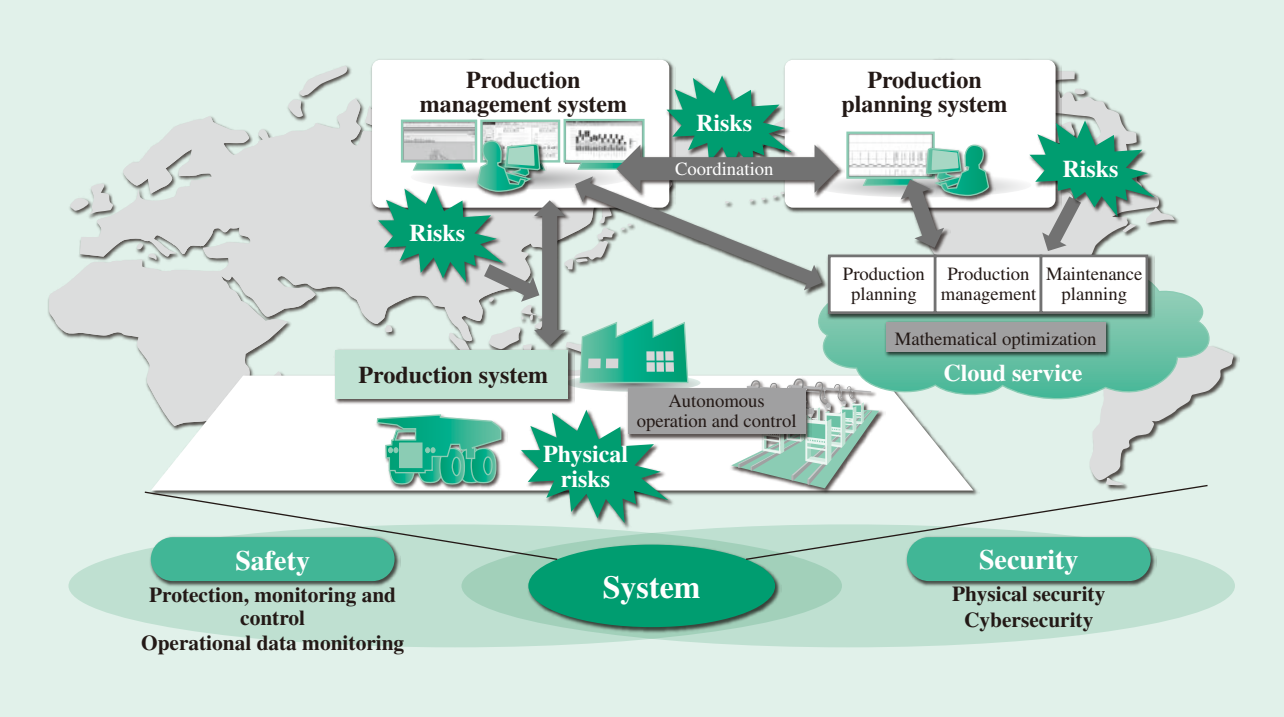


Fig. 2—Maintaining Safety and Security of Social Infrastructure Systems.
Systems interoperate across an open architecture, so maintaining safety and security is important.

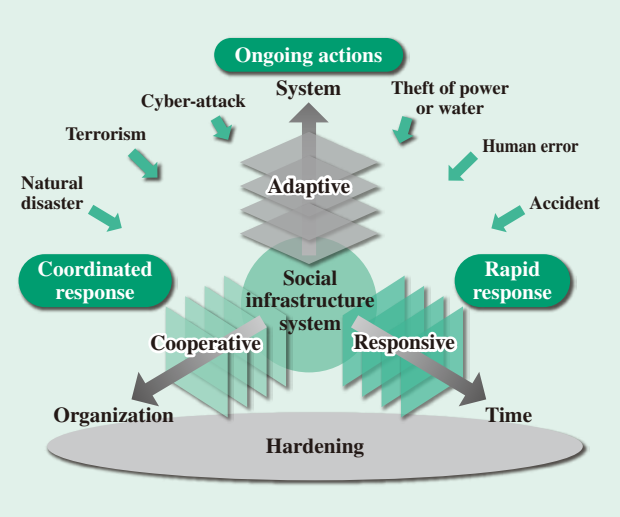


Fig. 3—Hitachi System Security Concept.
Hitachi has proposed the Hitachi system security concept for the requirements needed to maintain security on social infrastructure systems.

HITACHI SYSTEM SECURITY CONCEPT

This chapter describes the Hitachi system security concept proposed by Hitachi.

Hitachi expresses the requirements for maintaining the security of social infrastructure systems in terms of this Hitachi system security concept (see Fig. 3). Specifically, this means being more resilient to anticipated threats using the configuration of the systems concerned as a base (hardening). With this base, the concept also describes new requirements for security in terms of being adaptive, so that security measures, too, can change as needed in response to continually changing threats and system configurations; being responsive, so as to take actions to minimize the impact on social infrastructure systems when a security threat does arise; and being cooperative in the sense of multiple organizations working together to identify security threats at an early stage.

Recognizing that these requirements are important for the implementation of social infrastructure systems and need to be shared throughout the world, the requirements have been discussed at the IEC, an international standards body, where they were presented and adopted in a whitepaper entitled *Factory of the Future* on how factories will look in the future and the technologies that will be required. Table 1 lists the details of what is required for each requirement.

TABLE 1. Hitachi System Security Concept Implementation
The table lists what is needed to implement each aspect of the Hitachi system security concept.

Type of countermeasure	Summary
Making systems more resilient (Hardening)	Divide the system into separately managed zones, and detect unauthorized intrusions or behavior in each zone
Ongoing adaptation to threats (Adaptive)	Routinely assess system risks with reference to threat trends and update or strengthen measures for making system more resilient
Rapid response to threats (Responsive)	Continually monitor and analyze status of measures for making system more resilient and respond quickly if a threat gets into the system
Share information about threats (Cooperative)	Prepare for incidents by sharing information about threats and risks with stakeholders, including operational and management staff, other companies in same industry, and customers (risk communication)

SECURITY SOLUTION PLATFORMS

This chapter describes security solution platforms that implement the Hitachi system security concept that was summarized in the previous chapter.

To provide systems that combine safety and security, Hitachi supplies not only standard security solutions, but also security solutions that take advantage of the services and other business knowledge provided by the systems themselves. Hitachi supplies security solution platforms that are optimized for specific social infrastructure systems using common security solutions as a base (see Fig. 4).

In addition to solutions for the security of on-site systems, these security solution platforms provide solutions that take account of everything from security management at the planning stage to daily security operations. The following gives an overview of the solutions provided by Hitachi.

(1) Adaptive solutions

To be adaptive, it is important for organizations to put a security management system in place. Accordingly, Hitachi supplies consulting for establishing in-house security management systems that comply with standards such as the IEC 62443 and the International Organization for Standardization (ISO) 27000 series. To ensure that management is undertaken correctly, this includes assistance with security risk analysis as well as assessing the status of security on existing systems.

(2) Cooperative solutions

In terms of being cooperative, there is a mechanism in place for linking information between organizations inside and outside a company to protect systems from security threats. By having organizations inform

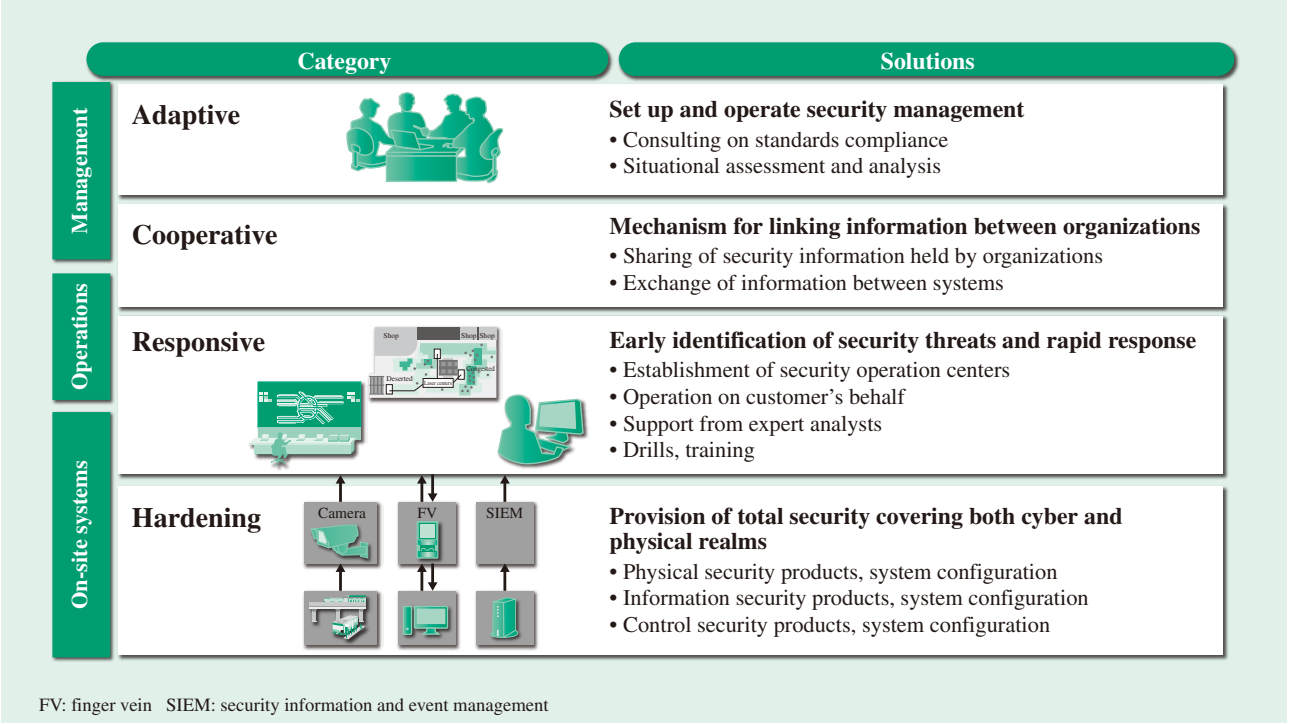


Fig. 4—Security Solution Platform.
The security solution platform implements the Hitachi system security concept.

each other about things like new security threats and how to deal with them, this exchange of information enables the security management systems referred to above to take advantage of the latest information. The exchange of information is also needed to make systems responsive, as discussed below. Attackers are continually looking in a systematic manner for new methods and routes of attack. This makes it essential that the defenders, too, collect and share information about the characteristics of attacks widely across a number of organizations. It is particularly important to share images and other information from the physical realm as well as from cyberspace. Hitachi supplies solutions that establish the infrastructure and support the practice of sharing information on both the cyber and physical realms.

(3) Responsive solutions

In terms of being responsive, the essential factors in enabling the early identification of security threats and a rapid response are to collect on-site information in a timely manner, to have effective ways of assessing situations, to formulate the correct responses, and to implement them quickly. Hitachi supplies support for establishing security operation centers to perform these steps, operating them on the customer's behalf, and conducting analyses using specialists in security technology and experts with operational know-how from Hitachi's own centers, and also training staff on how to deal with security threats, including the staging of drills.

(4) Hardening solutions

To protect on-site systems by making them more resilient, it is necessary to equip them with the means to protect the targets of security threats in ways that combine both cyber and physical defenses. Hitachi supplies security products and system configurations for the protection of physical spaces and in the form of solutions for protecting cyberspace.

Other articles in this edition of *Hitachi Review* describe solutions for information security, control security, physical security, and IoT systems.

CONCLUSIONS

This article has described Hitachi's security solution platforms for maintaining the safety and security of social infrastructure systems.

Security threats to social infrastructure systems are having a greater impact than ever on the activities of organizations and people, and on society. Meanwhile, advances in society and the development of IoT technology are linking the activities of organizations and people together into more extensive networks. As a result, it is becoming more difficult to predict

the incidence of security threats or the routes that attacks or infection will take. This makes it important that security measures be undertaken by people and organizations working together in networks rather than just as individual entities. To achieve this, security guidelines and the infrastructure for information sharing are being put in place by governments and organizations. Progress is also being made on turning these into international standards and on establishing certification programs.

Hitachi intends to continue contributing to the creation of safe and secure social infrastructure systems through collaborative creation with numerous organizations as well as by accurately identifying changes and supplying the best possible solutions.

REFERENCES

(1) IEC, http://www.iec.ch/
(2) IEC, "White Paper: Factory of the Future," http://www.iec.ch/whitepaper/futurefactory/
(3) T. Nakano et al., "International Standardization Activities for Hitachi System Security Concept and Social Infrastructure Security Based on It," Hitachi Review **65**, pp. 64–69 (Jun. 2016).

ABOUT THE AUTHORS

Toshihiko Nakano, Ph.D.
Security Business Division, Social Innovation 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).

Takeshi Onodera
Information System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the business development of service platforms.

Tadashi Kamiwaki
Security Business Division, Social Innovation Business Division, Hitachi, Ltd. He is currently engaged in the development of security business.

Takeshi Miyao
Security Business Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in supervising security business operations.

Featured Articles II

Information Security
Hitachi's Solution for Defending against Cyber-attacks

Takehiro Kawashima
Yuji Motokawa
Kazuya Yonemitsu
Hiroyuki Hamada
Kazuhiro Kawashima, Ph.D.

OVERVIEW: Along with the trend over recent years toward social infrastructure being connected to public and wide-area networks to take advantage of the IoT, the growing technical sophistication and seriousness of cyber-attacks has raised concerns about the threat they pose. Hitachi's cybersecurity solutions offer a range of options covering all aspects of customers' countermeasure phase with respect to three points, defenses in depth, early detection, and rapid response. Hitachi protects customers from cyber-attacks by supplying solutions that cover everything from preliminary planning, such as its assessment service, to monitoring and operational management, such as its SOC service, and incident response, such as its support for establishing a CSIRT. Given the expectation that the threat of previously unknown cyber-attacks will rise rapidly in the future, Hitachi is seeking to maintain and improve the security of social infrastructure through a wide range of activities that include establishing information exchanges that enable mutual defense through intelligence-sharing and the training and deployment of security staff.

INTRODUCTION

A steady series of social innovations that make use of cyberspace have arisen since the start of the 21st century. However, this has also been accompanied by a spread of malicious uses of cyberspace in crime and terrorism. This trend poses a threat to the safety and security of social infrastructure, making cybersecurity an essential part of future social innovation.

This article summarizes Hitachi's solutions for dealing with cyber-attacks with reference to recent trends in these attacks.

TRENDS IN CYBER-ATTACKS IN RELATION TO SOCIAL INFRASTRUCTURE

Recent Trends in Cyber-attacks

There has been an expansion and growing diversity in cyber-attacks over recent years on a variety of fronts, including the range of targets and the methods used. While attacks by individuals in the nature of vandalism were common in the past, there has been an increase in cases of specifically-targeted cyber-attacks.

Examples include financially-motivated attacks by criminal organizations on individuals, companies, and public institutions with the aim of stealing personal or corporate information, and attacks on social infrastructure undertaken for the purpose of "hacktivism" or cyber-terrorism. Because attacks targeting companies can damage their value if countermeasures are inadequate, it is no exaggeration to say that cybersecurity is now a corporate management issue.

Because these attacks have clear intentions and targets, they can choose the methods that best suit the target. In a typical targeted attack, a method is chosen that is most likely to work on the targeted individual. Because of the wide variety of different technical methods that can be adopted to suit the target, it is difficult in practice to completely eliminate intrusions.

Risk of Cyber-attack on Social Infrastructure

Social infrastructure is being required to connect to public and wide-area networks due to its growing need to use the Internet of Things (IoT), and for better maintenance and convenience. This means that previously isolated control systems now sometimes have indirect connections to the outside via information technology (IT) networks or portable media. With instances of damage-causing cyber-attacks on social infrastructure having already taken place overseas[1], it would be no surprise for such incidents to occur in Japan.

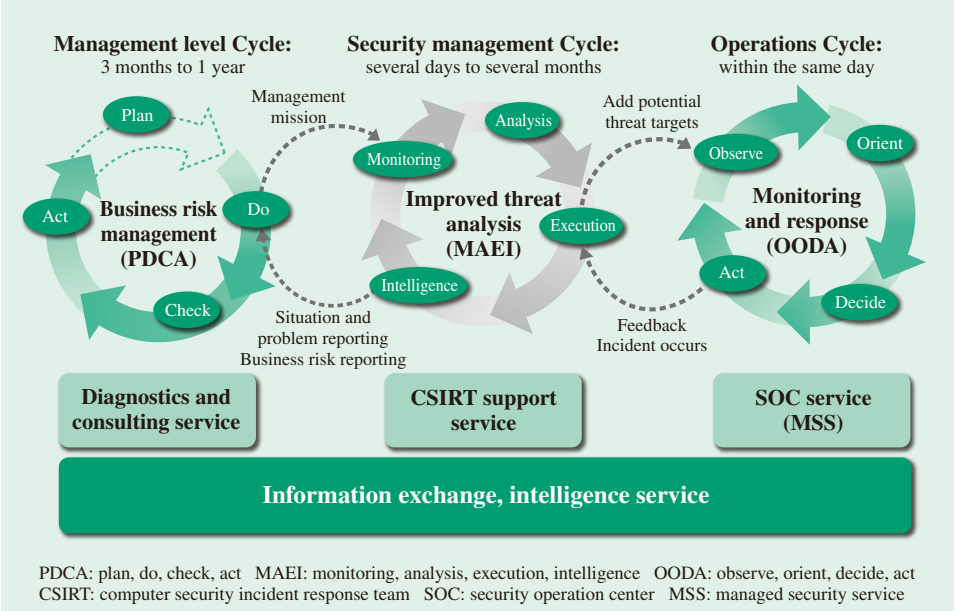


Fig. 1—Relationship between Cycle of Security Measures and Associated Services.
The security measures at an organization have a different cycle at each level. These cycles are linked, and among them, a CSIRT handles security management. Hitachi's security solutions offer one-stop service for each level.

HITACHI'S INVOLVEMENT IN CYBERSECURITY

Trend of Cybersecurity Measures by Hitachi

Cybersecurity for organizations (both corporate and non-corporate) means more than just the installation of security functions (products such as anti-virus software), requiring rather a process of change involving ongoing situational analysis to determine the appropriate security measures for the organization at each point in time.

The optimal approach to security in 1990 was a process of evolution whereby extra layers of border defenses were added at the boundary between the organization and the outside world. In 1996, Hitachi went on to establish a security operation center (SOC) service for providing border defenses to customers in its role as a leader in the field of managed security services (MSSs*) in Japan. Subsequently, Hitachi undertook to analyze threats as they changed over time and with changes in technology, and in the intentions of attackers and criminals. This led to ongoing changes in the nature of MSSs themselves, including entry point and exit point defenses and other methods for dealing with practices such as attacks on on-line retailers and other web applications, phishing scams, distributed denial of service (DDoS) attacks, and targeted attacks, and an expansion in the scope of monitoring to include things like IoT devices. Meanwhile, the increasing complexity of cybersecurity meant that ways of providing security measures at customer sites were also needed. Specifically, from the standpoint of business continuity management (BCM), there was a need for computer security incident response teams (CSIRTs) that tie together the cybersecurity considerations of management and operations (see Fig. 1).

Hitachi is continually upgrading all aspects of its cybersecurity solutions, including services that support CSIRT activities by customers that are an extrapolation of MSSs, information exchanges that link people and organizations, and the provision of the intelligence required by the exchanges.

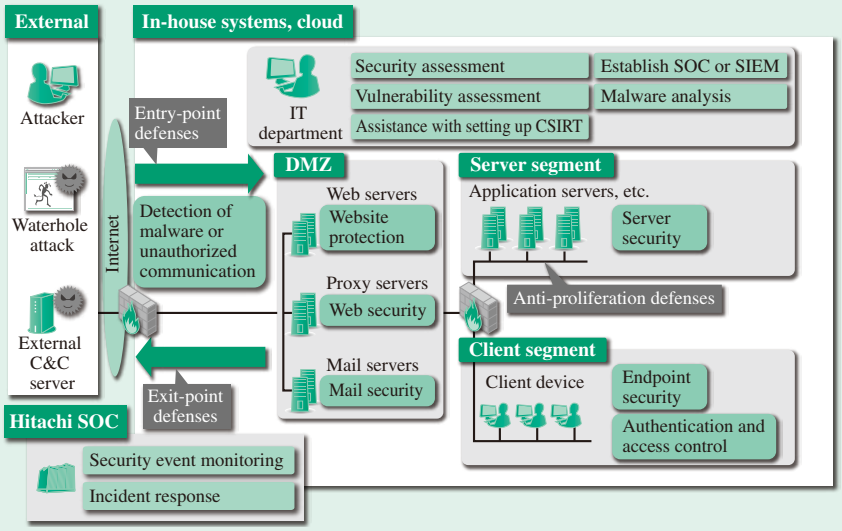
Hitachi Cybersecurity Solutions

Hitachi's cybersecurity solutions take cyber-attacks and malware intrusions for granted and are based around three points: defenses in depth, early detection, and rapid response.

Rather than using localized measures at entry points only, for example, defenses in depth minimize risk and prevent incidents with multiple layers of defense at entry points, exit points, and inside the organization. It means using multiple techniques covering the detection of malware or unauthorized communications, entry- and exit-point measures for the web and e-mail, and internal measures such as server endpoints to prevent spreading (see Fig. 2).

Early detection means implementing measures for minimizing damage through the early identification of the signs of an attack. It is important to establish monitoring practices by determining the sequence of an attack or identifying malware activity using techniques such as event monitoring or setting up an SOC.

* A service for detecting security abnormalities and protecting IT systems through the monitoring and operation of security equipment.



IT: information technology DMZ: demilitarized zone C&C: command and control
SIEM: security information and event management

Fig. 2—Defenses in Depth Solutions for Cybersecurity. The risks of cyber-attacks can be minimized and incidents prevented by establishing multiple layers of defense covering entry points, exit points, and internal proliferation.

An important factor in achieving a rapid response is to establish capabilities for responding to cyber-attacks and other information security incidents at the organization. The establishment and operation of a CSIRT is one example of such a measure. Hitachi supplies solutions for these points that combine everything from preliminary planning to countermeasures and protection together with monitoring and operational management, to post-incident follow-up (see Fig. 3).

Example of Countermeasures against Cyber-attack: Assessment Service

Planning which types of countermeasures to use is an important part of the job, and involves assessing the current situation to identify things like the assets to be protected, the potential threats, and the extent to which countermeasures are already in place.

The rest of this section describes an example of an assessment service that proposed countermeasures based on an assessment of the current situation (see

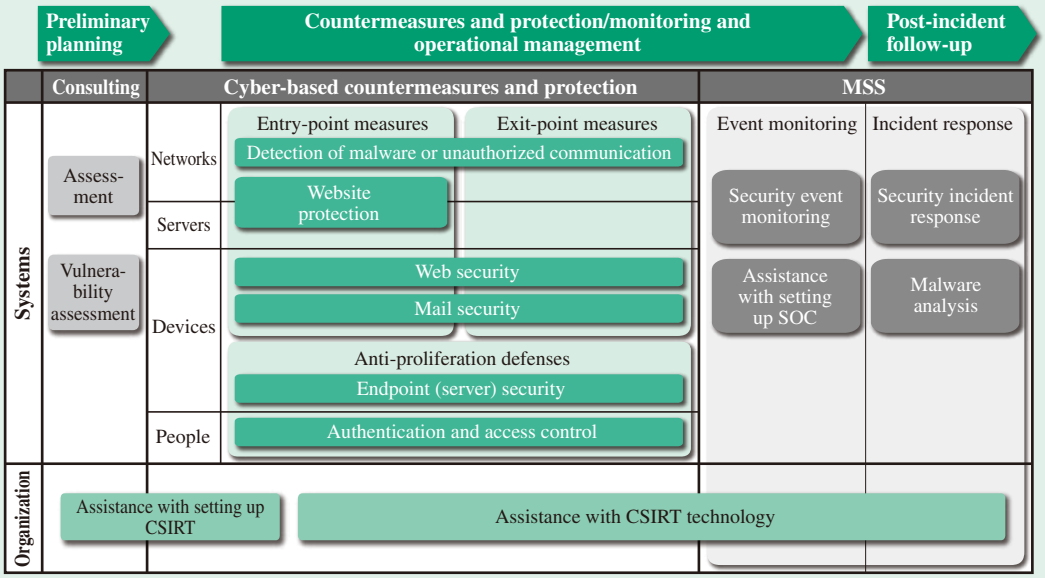


Fig. 3—Solutions according to Each Countermeasure Phase of the Customer.
Hitachi supplies comprehensive solutions that cover each countermeasure phase from preliminary planning to countermeasures and protection together with monitoring and operational management, to post-incident follow-up.

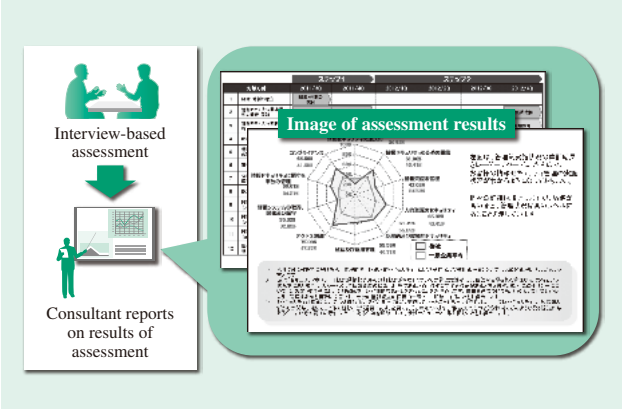


Fig. 4—Image of Assessment Service Results.
The results of the assessment service are presented in the form of proposed measures based on an assessment of the current situation.

Fig. 4). The service involves consultants with expertise in defending against sophisticated cyber-attacks who undertake theoretical evaluations to decide how to go about providing countermeasures in the future.

Hitachi provides the assessment service using proprietary evaluation methods by categorizing the actual methods used by cyber-attacks. A feature of the service is that the assessments are conducted from the perspective of specialists based on their extensive experience, including not only technical staff who specialize in security assessments, but also those with specialist skills in networks, databases, and hacking, etc. Network engineers, for example, are able to point out problems with the structure of the customer's network and security problems with the network's entry points, exit points, and internal parts by surveying a map of the customer's network and conducting simple interviews about the nature of the customer's work.

The assessment results indicate the security problems that were identified and present a list of proposed high-priority countermeasures to address them. These latter come in two types: proposals that require a certain amount of investment, such as installing L7 firewalls on important segments or proxies with a URL filtering function, and proposals that can be introduced with minimal investment, such as changes to the network structure or establishing a process for emergency response by the CSIRT.

The customer is able to formulate and implement a plan for security measures that are highly practical and effective by using these assessment results as a basis for prioritizing measures and adopting them in order of their cost-benefit.

OUTLOOK FOR CYBERSECURITY OF SOCIAL INFRASTRUCTURE

Intelligence-sharing to Protect Social Infrastructure

Hitachi has experience with activities such as setting up SOCs with capabilities for log correlation analysis using security information and event management (SIEM) for customers in the social infrastructure and industrial sectors, and assisting them with the establishment of CSIRTs. To make better use of the associated security monitoring platforms, it is important to take action before the damage due to a cyber-attack spreads by sharing intelligence on the latest threats and vulnerabilities between SOCs, CSIRTs, and others in ways that transcend the boundaries between companies and organizations. This is the key idea behind group defense (see Fig. 5).

Specifically, this involves consolidating intelligence on an information exchange, including information on cyber-attacks obtained by social infrastructure operators or Hitachi's SOCs, information on threats and vulnerabilities provided by security vendors, and other technical information obtained by security technicians working together. This information can then be analyzed to provide reports and countermeasure services to the SOCs and CSIRTs at each company. Doing so enables social infrastructure operators to prevent newly proliferating cyber-attacks before they strike.

By providing these services, Hitachi's aim for the future is to establish comprehensive and ongoing security services for social infrastructure that extend from the establishment of security systems and their routine monitoring, operation, and training to responding when an incident occurs.

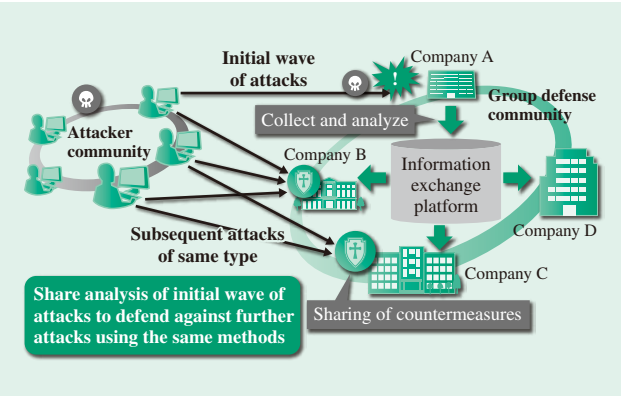


Fig. 5—Intelligence-sharing Structure.
The sharing of intelligence gained from analysis of the initial wave of attacks prevents further attacks using the same methods.

Cybersecurity Human Resource Development

A survey by the Information-technology Promotion Agency, Japan (IPA) concluded that the quality and number of information security staff was insufficient for the increasing severity of cyber-attacks(2). Hitachi has long been aware of workforce issues and engages in both internal and external activities that cover everything from human resource development to increasing community activation and the establishment of career paths.

Activities linked to people outside the Hitachi Group include initiatives aimed at increasing the supply of human resources, such as public security seminars(3) run as collaborations between industry and academia; assisting with SECCON, Japan's largest security competition, and the Computer Security Symposium and anti-malware Engineering Workshop (CSS/MWS); and initiatives aimed at encouraging the research community like participating in a joint university team at the MWS Cup 2015 (team winners).

Internally, Hitachi is proceeding with career path planning and human resource development for different IT skill levels and specialties (administration, technical, and so on) (see Fig. 6). Specific activities that are expediting human resource development include visualization of human resources by conducting information security specialist examinations aimed at uncovering and evaluating personnel and offering them training and employment, providing knowledge through set courses in information security and practical skills, and creating educational opportunities using the information security community.

Through these activities, Hitachi aims to establish a human resource development cycle to underpin its cybersecurity solutions by expanding its workforce of security engineers with Information Technology Skill Standard (ITSS) level 4 or higher to 1,000 people by FY2018, including 100 security evangelists with abilities in the analysis of malware and similar.

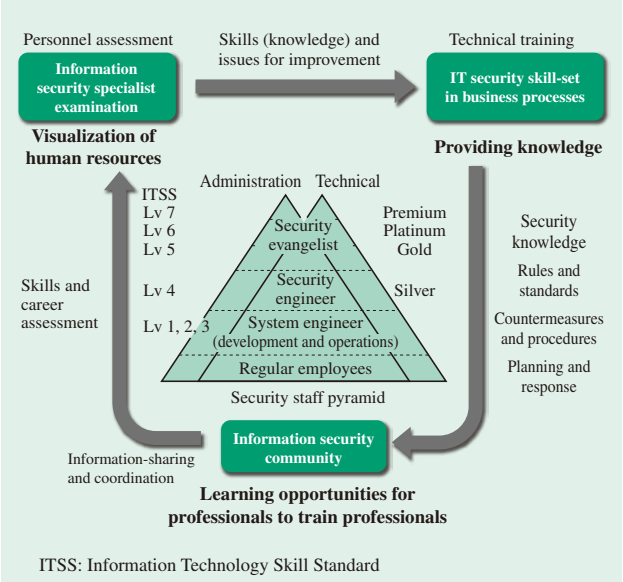


Fig. 6—Security Human Resource Development Cycle at Hitachi.
Hitachi has established a human resource development cycle by undertaking security training on the basis of personnel assessment, technical training, and information-sharing and coordination.

CONCLUSIONS

There is potential in the future for increasingly serious attacks on social infrastructure using previously unknown means and timed to coincide with national or other events. Accordingly, Hitachi intends to strengthen its security business to maintain and improve social infrastructure security. Cybersecurity is a never-ending process.

REFERENCES

(1) SANS Industrial Control Systems Security Blog, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
(2) Information-technology Promotion Agency, Japan, Report on "Basic Survey on Training of Information Security Personnel" (Jul. 2014), https://www.ipa.go.jp/security/fy23/reports/jinzai/ in Japanese.
(3) Hitachi Systems News Release, "Strengthening Efforts to Address Shortage of Information Security Personnel through University-Industry Cooperation and Collaborative Creation" (Jan. 2016), http://www.hitachi-systems.com/news/2016/20160125.html in Japanese.

ABOUT THE AUTHORS

Takehiro Kawashima

Business Planning Department, IoT & Cloud Services Business Division, Service Platform Business Division Group, Information and Communication Technology Business Division, Hitachi, Ltd. He is currently engaged in the planning of service business, primarily dealing with security.

Kazuya Yonemitsu

Total Security Solution Department, Security Solution Division, Cross Industry Solution Business Division, Hitachi Solutions, Ltd. He is currently engaged in consulting on information security. Mr. Yonemitsu is a member of the Japan Information-Technology Engineers Examination Committee (ITEE Committee).

Kazuhiro Kawashima, Ph.D.

Advanced Cyber Security Technology Department, Advanced Security Technology Operations, Cyber Security Business Division, Service Platform Business Division Group, Information and Communication Technology Business Division, Hitachi, Ltd. He is currently engaged in the development of information security human resources.

Yuji Motokawa

Cloud ICT Service Business Group, Hitachi Systems, Ltd. He is currently engaged in the coordinating of cyber-security engineering. Mr. Motokawa is the Vice President of the ISACA Tokyo Chapter, and a secretary of the NPO Japan Network Security Association (JNSA).

Hiroyuki Hamada

Security Solutions Department, IoT & Cloud Services Business Division, Service Platform Business Division Group, Information and Communication Technology Business Division, Hitachi, Ltd. He is currently engaged in the development of cyber-security solutions.

Featured Articles II

Control Security

Security Solutions that Protect the Life Cycle of Control Systems

Satoshi Okubo
Kohei Yamaguchi
Tetsuaki Nakamikawa, P.E.Jp
Hiroki Uchiyama, Ph.D.

OVERVIEW: As the control systems used in social infrastructure become more general-purpose and connected to a greater range of networks, security problems are continually being found. However, since long-term stable operation is a priority for control systems, it is not easy to use security measures such as security patches. So, there is a need for security management that monitors for vulnerabilities and provides early detection and handling of attacks that target vulnerabilities. To respond to this need, Hitachi is ensuring the safety and security of social infrastructure by creating security solutions that help reduce the workload needed for control system security management and ensure security across the entire control system life cycle.

INTRODUCTION

SOCIAL infrastructure systems (such as power, railways, gas, and water), and vehicle control systems have conventionally been considered immune from cyber-attacks since they use their own operating systems and protocols, and are installed in environments that are not accessible from the Internet or other external networks. However, the use of general-purpose operating systems such as Windows*1 and Linux*2, and general-purpose protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) has recently been on the rise as a cost-cutting measure. Connections to information systems such as production control systems have also become increasingly common as a way of improving efficiency, resulting in control systems (for which security was previously not a concern) requiring the same security measures as information systems.

Control systems have different requirements from typical information systems, namely availability and long-term maintainability. These different requirements make it difficult to apply security technology and products designed for information systems to control systems as-is. For example, when a vulnerability or other security problem is discovered in a control system, it is not easy to use patches or other security measures that might have unknown effects on the system's operation. Installing security products can also change the system configuration after restarting, resulting in known vulnerabilities becoming actualized or new vulnerabilities being discovered, thereby preventing complete handling of the problem.

A certification system has been created for security management of information systems, in the form of information security management systems (ISMSs) defined by the ISO/IEC 27001 standard(1). The aim of an ISMS is to protect information resources (client information and confidential information). It calls for tasks such as security risk analysis, risk handling (preventive measures), creation of an operation organization/system, and creation of procedures for responding to incidents (detection measures, response measures). The organization also needs to create a security life cycle loop (review current situation → prevent → detect → respond). In the future, this type of security management will likely be needed not just for information systems, but also for control systems.

This article discusses the need for control system security management to ensure the safety and security of social infrastructure systems, Hitachi's security management concept, and solutions for assisting it.

*1 Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.
*2 Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

TABLE 1. Differences between an ISMS and a CSMS
The differences between the requirements of an ISMS and a CSMS are listed below.

Difference	ISMS	CSMS
Protected assets	Information assets	Information assets, personal/physical assets, operation (IACS)
Anticipated threats	Damage to CIA of protected assets	Damage to CIA of protected assets, as well as damage to HSE
Protected life cycle	Mainly operations	All areas of system life cycle

ISMS: information security management system
CSMS: cyber security management system
CIA: confidentiality, integrity, availability
IACS: industrial automation and control systems
HSE: health, safety, environment

NEED FOR CONTROL SYSTEM SECURITY MANAGEMENT

As control system security management becomes increasingly important, its requirements are being set forth in security standards for control systems, and in guidelines created by governments. This chapter looks at some of the developments taking place in this area.

Security Standards

IEC 62443[(2)] has been created as a security standard for general-purpose control systems. The standard consists of 13 standard groups that specify requirements for businesses, for system integrators, and for component vendors. Among these standard groups, IEC 62443-2-1[(3)] defines cyber security management systems (CSMSs). Table 1 shows the differences between an ISMS and a CSMS. As with ISMSs, the world's first certification system for CSMSs was created in 2014[(4)], and certification by social infrastructure providers may increase in the future.

Government Guidelines

Japan's Ministry of Economy, Trade and Industry (METI) has teamed up with Information-technology Promotion Agency, Japan (IPA) to create cybersecurity guidelines for the chief executives of information technology (IT) system or service providers, or of companies that depend on IT for their corporate strategy[(5)]. The guidelines list the following four items as key management items:
(1) Demonstrating leadership, organization-building
(2) Setting a framework for cybersecurity risk management
(3) Attack-prevention measures that understand the risks
(4) Preparations in readiness for cyber-attacks

The creation of control system standards and guidelines in Japan and abroad reflects how IT-dependent social infrastructure providers need to implement security management over the long term.

CONTROL SYSTEM SECURITY MANAGEMENT CONCEPT

Social Infrastructure Security Concept

A number of security requirements are needed to protect social infrastructure from threats such as natural disasters, cyber-attacks and terrorism. Hitachi has distilled these requirements into four properties–hardening, adaptive, responsive and cooperative. They form the basis of Hitachi's system security concept[(6)].
(1) Hardening: Acquiring the defensive ability to withstand the attack skills of attackers
(2) Adaptive: Continually improving preventive/defensive measures against new threats
(3) Responsive: Improving after-the-fact handling ability to minimize damage and recovery time after an attack has occurred
(4) Cooperative: Different organizations or businesses working together with a common understanding of the situation

Approach to Control System Security Management

Hitachi applies its system security concept to implement control system security management by continually improving responses to new threats through the plan, do, check, act (PDCA) cycle (see Fig. 1).
(1) Identify new threats

New threats that need to be investigated due to events such as system configuration changes are uncovered, and their effects on the system to be protected are identified by means such as risk analysis.
(2) Propose improvement methods

The risk analysis results from (1) are used to investigate improvement methods for the anticipated risks.
(3) Set implementation plan

A plan for implementing the improvement methods investigated in (2) is set.
(4) Implement security measures

The security measures set in (3) are implemented.

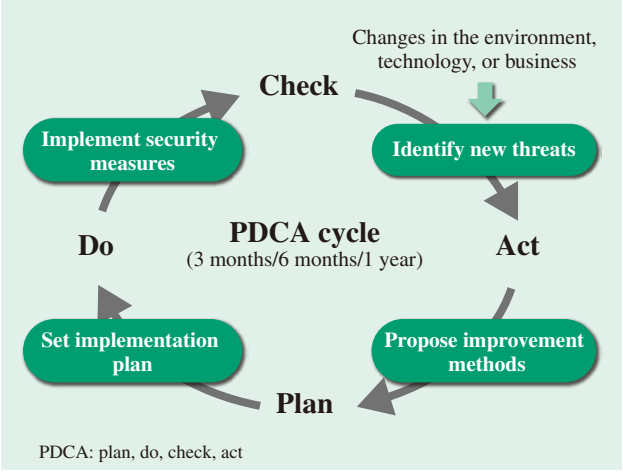


Fig. 1—Measures Driven by Security Operation Management PDCA.
Responses to new threats are continually improved through the PDCA cycle.

CONTROL SECURITY SOLUTIONS ASSISTING SECURITY MANAGEMENT

To provide security measures for a control system, the system must first be divided into zones according to the security level required by each zone, and then security measures must be provided for each zone's portal and the communication channels linking the zones.

Hitachi's control system security measures draw on the system security concept to propose two solutions: (1) Assist in preventing unauthorized cyber access, and (2) Assist in preventing unauthorized system operation (see Fig. 2).

Assist in Preventing Unauthorized Cyber Access

Assisting in preventing unauthorized cyber access is a solution that prevents unauthorized access via cyberspace at the portal of each zone (hardening), and prevents the spread of security problems after unauthorized access has been detected (responsive).

Devices that prevent unauthorized access block unauthorized data packets that do not match a predefined whitelist. Installing these devices at the portals of the control system to be protected enables prevention of unauthorized control system access. Hitachi has a tool that can generate the whitelist previously mentioned by using an access log during system trial operation. These benefits make it easy to install the solution in a control system. If a security problem (such as malware infiltration) occurs in another system connected to the control system, devices that prevent unauthorized access can prevent the problem from spreading to the control system by blocking communication data packets from the other system.

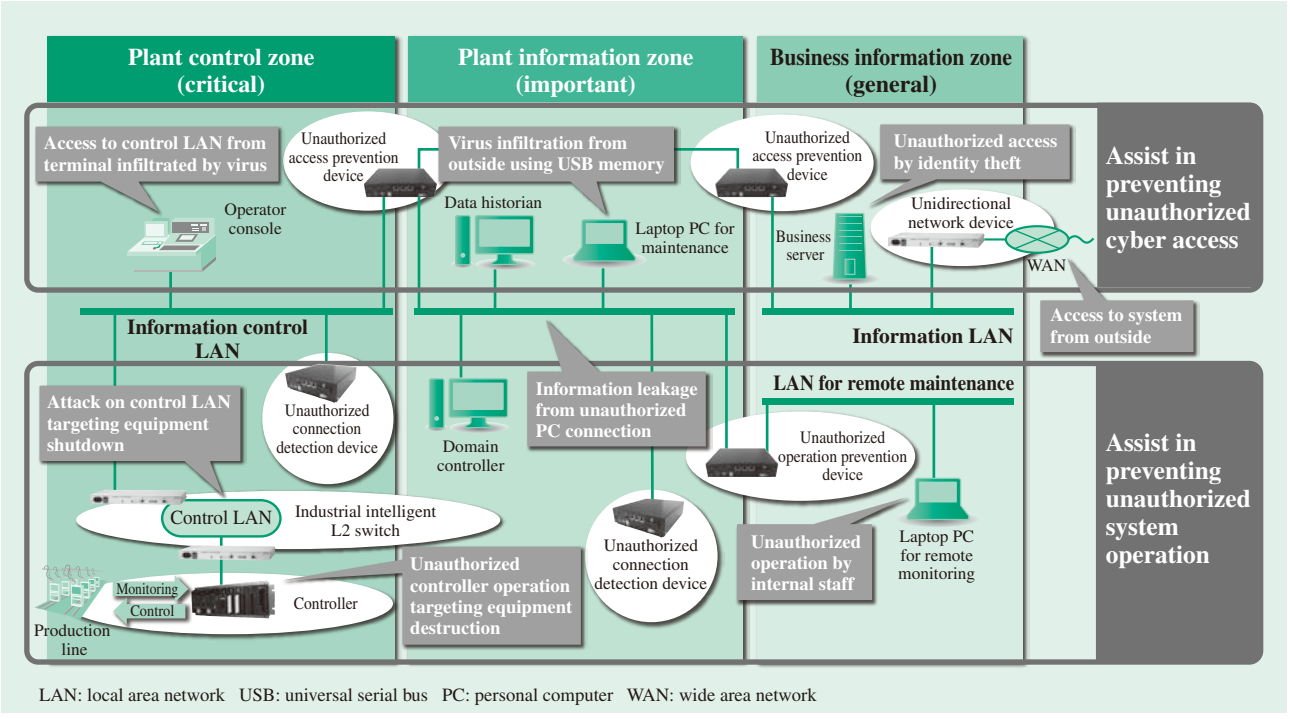


Fig. 2—Control System Security Solutions.
Two control system security solutions are provided by combining a wide range of security products for control systems.

Fig. 3—Unidirectional Network Device.
This device's software-free implementation reduces the risk of configuration errors and reduces the workload during operation.

Fig. 4—Unauthorized Connection Detection Device.
This device prevents the threat of cyber-attacks by detecting and automatically eliminating network connection attempts by unregistered devices.

In addition, Hitachi's unidirectional network device provides a software-free data diode function (a function that permits communication in one direction only, like a diode) so that when transmitting information from a core system to the outside world, unauthorized access from the outside world can be physically blocked, protecting the core system. It also reduces the workload during operation by providing benefits such as not needing software upgrades and an extended life (see Fig. 3).

Assist in Preventing Unauthorized System Operation

In the future, control systems are expected to have various Internet of Things (IoT) devices connected to them via networks. Installing a wireless network at a manufacturing site increases the chance of an unauthorized device (such as an IoT device the administrator is unaware of, or an employee's personal terminal) being connected to a control system, creating new risks of malware infiltration or information leakage. Assistance in preventing unauthorized system operation is provided by solutions that defend control systems from threats caused by this type of unauthorized device connection within the system (hardening), and detect and eliminate unauthorized operations on authorized devices such as malware infiltration (responsive).

Hitachi's unauthorized connection detection device has a function that detects when a non-preregistered device has connected to the network, and excludes it from the network. It can also support connections via wireless networks, preventing unauthorized devices from connecting to control systems (see Fig. 4).

Measures for handling the targeted attacks that have recently been on the rise must assume that it is difficult to completely prevent unauthorized access to systems, such as infiltration by malware that is not perceived as a cyber-attack, and not handled by antivirus software. To detect cyber-attacks, behavior detection products with a proven track record for information systems can be used in coordination with the aforementioned unauthorized connection detection device to detect devices that perform unauthorized operations, and eliminate them from the network.

In addition, measures of increasing robustness against cyber-attacks are also used to minimize the effects of cyber-attacks that manage to penetrate network defenses.

Hitachi has developed a controller that is certified under the Embedded Device Security Assurance (EDSA) certification system for security assurance of control components administered by the International Society of Automation (ISA) Security Compliance Institute (ISCI), and provides increased resistance to cyber-attacks (see Fig. 5).

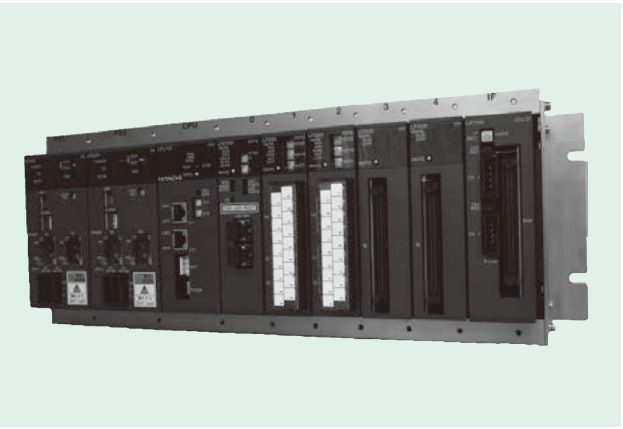


Fig. 5—Controller with EDSA Certification.
The controller demonstrates resistance to cyber-attacks by satisfying preset security requirements.

CONCLUSIONS

This article has examined the need for control system security management that reflects the developments taking place in Japan and abroad, and has presented Hitachi's security concept and the solutions used to support it.

With the use of the latest IT and coordination with information systems and IoT devices, control systems are expected to continue growing as platforms that support social infrastructure. The risk of cyber-attacks is expected to grow as well. To help ensure safe and secure social infrastructure systems, Hitachi will continue to develop control security technologies and provide high added-value solutions.

REFERENCES

(1) JIPDEC, ISMS Conformity Assessment Scheme, http://www.isms.jipdec.or.jp/english/isms.html
(2) International Electrotechnical Commission (IEC), IEC TS 62443-1-1, "Terminology, Concepts and Models," (Jul. 2009).
(3) International Electrotechnical Commission (IEC), IEC 62443-2-1, "Establishing an Industrial Automation and Control System Security Program," (Nov. 2010).
(4) JIPDEC, CSMS Conformity Assessment Scheme, http://www.isms.jipdec.or.jp/csms.html in Japanese.
(5) Ministry of Economy, Trade and Industry, "Cybersecurity Management Guidelines Version 1.0," in Japanese.
(6) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).

ABOUT THE AUTHORS

Satoshi Okubo
Control System Platform Security Center, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of security components for industrial control systems.

Kohei Yamaguchi
Control System Platform Security Center, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of security components for industrial control systems.

Tetsuaki Nakamikawa, P.E.Jp
Control System Platform Development Department, Control System Platform Division, Services & Platforms Business Unit, Hitachi, Ltd. He is currently engaged in the development of control system components. Mr. Nakamikawa is a member of the Information Processing Society of Japan (IPSJ).

Hiroki Uchiyama, Ph.D.
Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of security technology for control systems. Dr. Uchiyama is a member of The Institute of Electrical Engineers of Japan (IEEJ) and the IPSJ.

Featured Articles II

Physical Security

Integrated Physical Security Platform Concept Meeting More Diverse Customer Needs

Tatsuhito Sagawa
Tomokazu Murakami, Ph.D.
Taisuke Kano
Wataru Ito
Masakazu Nakayama
Ichiro Ote

OVERVIEW: To flexibly adapt to the growing and changing risks to public infrastructure and companies posed by threats such as terrorism in the lead-up to an international sports event to be held in Tokyo in 2020 and threats to food safety from contamination, organizations from throughout the Hitachi Group are currently making a collaborative effort to create a platform for physical security. The platform will be created around a core of functions that integrate multiple security systems such as video surveillance and access control systems. It will enable various physical security solutions, providing features such as system scalability, video analysis functions tailored to specific applications, and cloud system support. However, its applications will not be limited to just ensuring safety and security. In readiness for the IoT era, it will also enable active use as a platform for providing video analysis data and various other types of data to systems such as big data analysis systems, and production control systems in plants. These applications will extend the platform's physical security uses to customer business improvements such as optimizing operations in companies.

INTRODUCTION

RECENTLY there has been a seemingly unending succession of cases involving threats to public safety and security such as terrorism in public facilities and food contamination in plants. To prevent these acts, solutions to satisfy customer needs must be provided using various types of physical security systems.

The Hitachi Group is comprised of several companies that work with physical security systems such as video surveillance systems, video analysis systems, access control systems, and vehicle access control systems. Each of these companies has refined its expertise and abilities in the channel it specializes in. To link these companies together and provide single solutions to customers requires customized development tailored to each customer, making it a challenge to provide solutions in a timely manner. So, it became apparent that there was a need for an integrated physical security platform to link various systems together.

Companies in the physical security industry have been increasingly active recently in acquiring or collaborating with competitors. In today's dramatically changing market environment, Hitachi is looking to use its integrated physical security platform to focus the combined abilities of Group companies on providing a wide lineup of solutions tailored to customer needs. This article discusses the concepts behind this integrated platform and the creation of the various solutions built on it.

PLATFORM OVERVIEW

Fig. 1 shows an overview of the integrated platform proposed by Hitachi. Centered around a security system that combines surveillance cameras and sensors, the platform provides a comprehensive package of site data acquisition, management, analysis, and presentation functions for aims such as improving plant or distribution site productivity, and commercial facility customer flow analysis.

Platform Objectives

When meeting a site's information usage needs, the optimum solution will vary in form according to the business operations it is being provided for. In terms of system configuration for example, facilities can range

from large facilities handling large numbers of cameras (such as airports), to small facilities dispersed over a wide area (such as coin-operated parking lots). In terms of functions, the information to be acquired can also vary. For example, the security industry needs to acquire information on the behaviors of an indeterminately large number of people, the manufacturing industry needs information on workers and production equipment operating conditions, and the logistics sector needs information on workers and shipment tracking.

There are a number of key attributes required for providing solutions that match customer needs in a timely and optimum manner: (1) convenience enabling flexible adaptation to the implementation format, (2) functionality that can meet a wide range of business improvement needs, and (3) expandability enabling both video surveillance and adaptation to multiple applications in the future.

Hitachi's integrated platform has been proposed as a general-purpose platform designed to provide these attributes.

Technological Characteristics

The integrated platform technologies created to achieve the aforementioned convenience, functionality, and expandability are as follows:

To provide convenience, the system architecture has been designed to support both on-premises and cloud-based systems, with a common interface (I/F) connecting the cameras and sensors. It supports scalability in numbers of cameras, and has functions to support various modes of use, such as map displays and smartphone linkage.

To provide functionality, Hitachi's integrated platform incorporates the workflow design concept, using a method that enables various video analysis functions and data analysis functions to be selected and combined. Video analysis functions operate as plug-ins, creating an environment that enables flexible configuration of functions meeting customer needs. For example, the number of people detected by an access control device can be compared with the number detected by a surveillance camera, to detect unauthorized tailgating access.

To provide expandability, Hitachi's integrated platform includes a data processing platform that gathers and records data acquired from sensors, and functions that can be used as an Internet of Things (IoT) platform. Functions that work together with a manufacturing execution system (MES) can also be developed to provide solutions for plants, and statistical analysis functions can be provided using an interface for communicating with business intelligence (BI) tools such as Pentaho*.

* An open-source BI tool created for professionals.

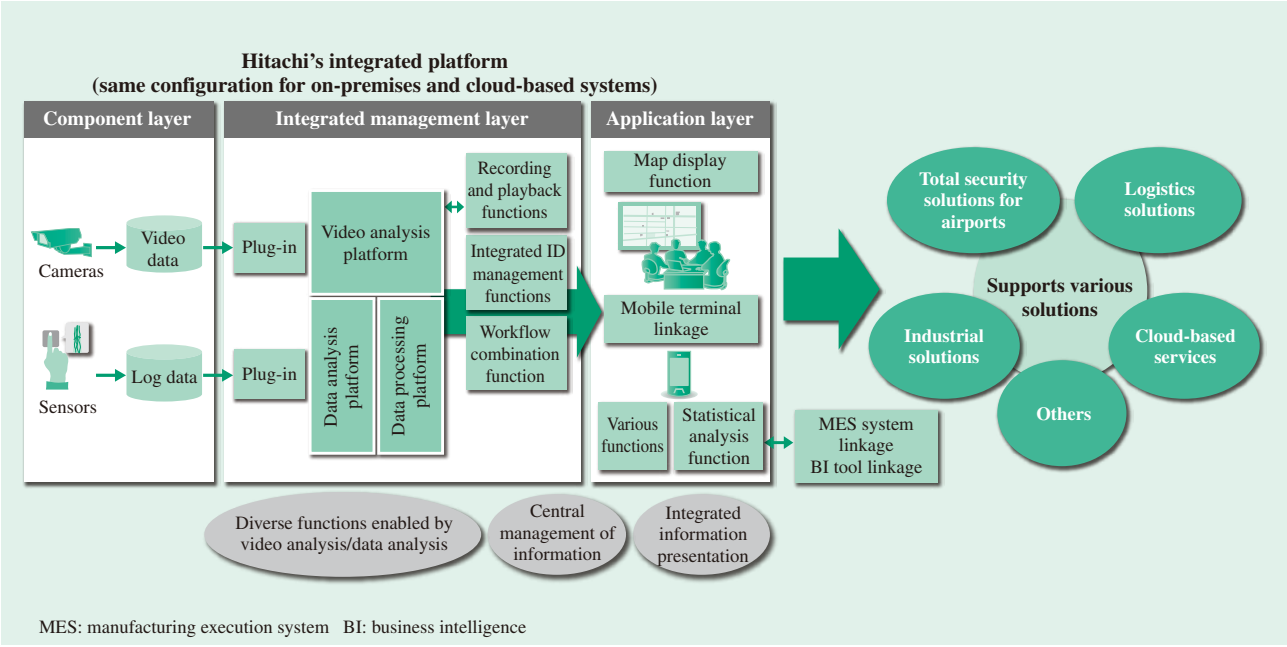


Fig. 1—Overview of Hitachi's Integrated Platform.
The platform proposed by Hitachi is characterized by features such as central management of information, diverse functions provided by video analysis and data analysis, and integrated information presentation.

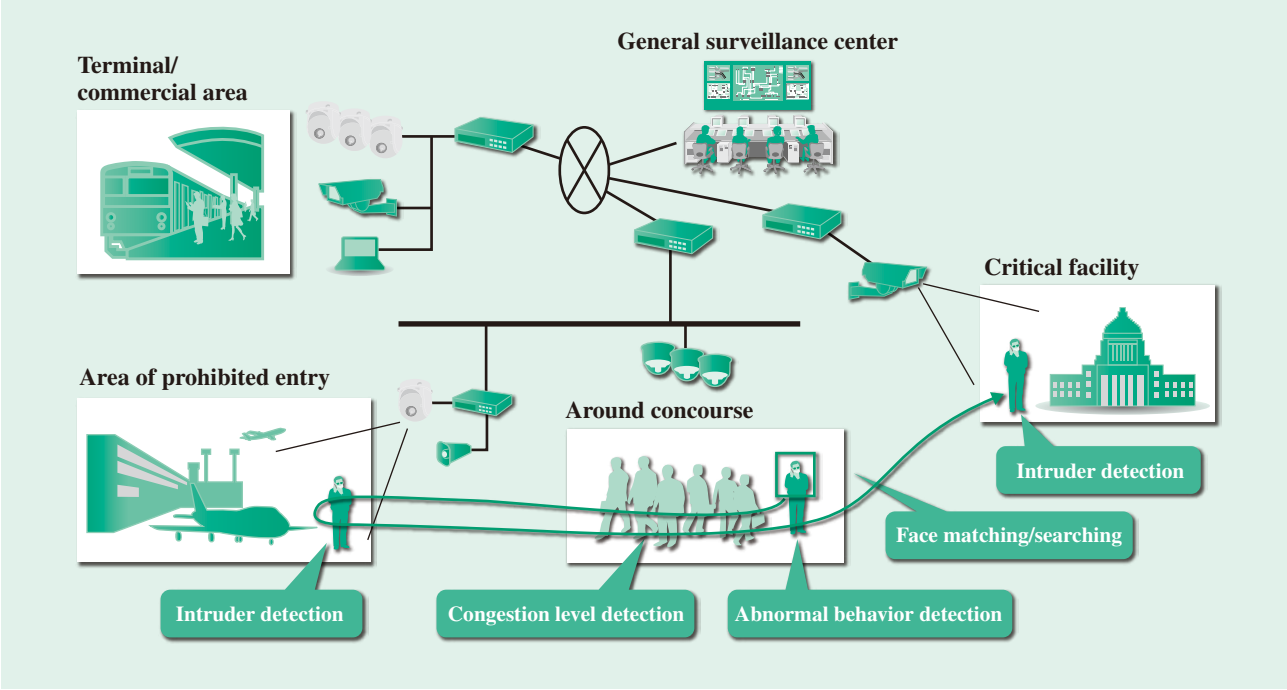


Fig. 2—Total Security Solution in Airports.
Airports have various facilities including areas of prohibited entry, critical facilities, and commercial facilities. The types of video analysis needed therefore vary greatly, requiring a total security solution.

SOLUTIONS LINEUP

Total Security Solutions for Airports

The network video surveillance system enables a large amount of video data from locations such as security/restricted areas in multiple terminal buildings, commercial areas, and airport peripheral facilities to be gathered by a general surveillance center. The video from these locations can be used to perform various image analysis functions on Hitachi's integrated platform, such as face matching/searching, congestion level detection, intruder detection, and abnormal behavior detection. These analysis functions can be used to ensure the safety and security of facility users, and to improve service. In times of disasters, they can also help create total security solutions that use information from various sources to provide appropriate operation management and evacuation guidance. Fig. 2 shows an example of a total security solution system configuration. Typical video analysis functions are listed below, along with examples of solutions that use them.

(1) Face matching

Live Face Matching is a Hitachi solution that detects when people that have been registered in advance are captured by a camera. It can be used to help find terrorists or wanted criminals in airport facilities, to prevent terrorist acts or to reduce crime. When used with ID cards in access control systems for controlled areas, it can also help improve the security level by preventing identity theft.

(2) Congestion estimation

Hitachi's congestion estimation solution can be used to analyze areas with high concentrations of airport facility users to help prevent incidents or accidents by providing user guidance during times of canceled flights, or by detecting passengers or articles left behind. It can also detect lines at check-in counters and security gates to help improve the efficiency of security operations, or improve service by using digital signage to guide users according to the congestion levels in restaurants or other airport facilities.

Industrial Solutions

Fig. 3 shows an example of a physical security solution designed for a plant. It uses Hitachi's integrated platform to implement external access control measures, along with internal control measures for employees.

Conventional physical security systems were implemented by installing individual systems for each function (such as vehicle access, biometric authentication-based access control, and video surveillance). However, when these systems are implemented individually, the surveillance work (the

work of checking alert/event times and locations using surveillance camera video) requires individual management of alert/event history information and surveillance video. This approach therefore requires information to be checked separately on different systems, resulting in poor operational efficiency, and risks such as key surveillance video being missed. To address this situation, Hitachi's integrated platform enables centralized management of surveillance information from multiple systems (such as intruder surveillance systems and access control systems). This approach enables more efficient surveillance operation, with display of surveillance camera video for relevant times and locations using information in the alert/event history.

Hitachi also plans to use the integrated platform to provide linkages to video analysis technologies for functions such as presence sensing, status and attribution recognition, and behavior understanding and prediction. In addition to simple video surveillance, these functions will enable autonomous surveillance that can detect events automatically and assist operation by using behavioral analysis to predict what will happen next. In the future, the uses of Hitachi's integrated platform will not be limited to security applications, since it is planning to release solutions designed to solve various business challenges. Examples include a solution designed to improve business efficiency by analyzing employee work operations to provide visual demonstrations of work know-how, and a quality control solution that provides correlation analysis of production control information and video analysis results.

Logistics Solutions

The recent explosive growth of electronic commerce (e-commerce) has increased the number of packages handled by the logistics industry, and the growth trend is expected to continue. However, Japan's declining birthrate and aging population have resulted in a shrinking of the labor force that has caused an increase in hiring of mainly foreign temporary workers, creating instability in the areas of rule compliance and safety management.

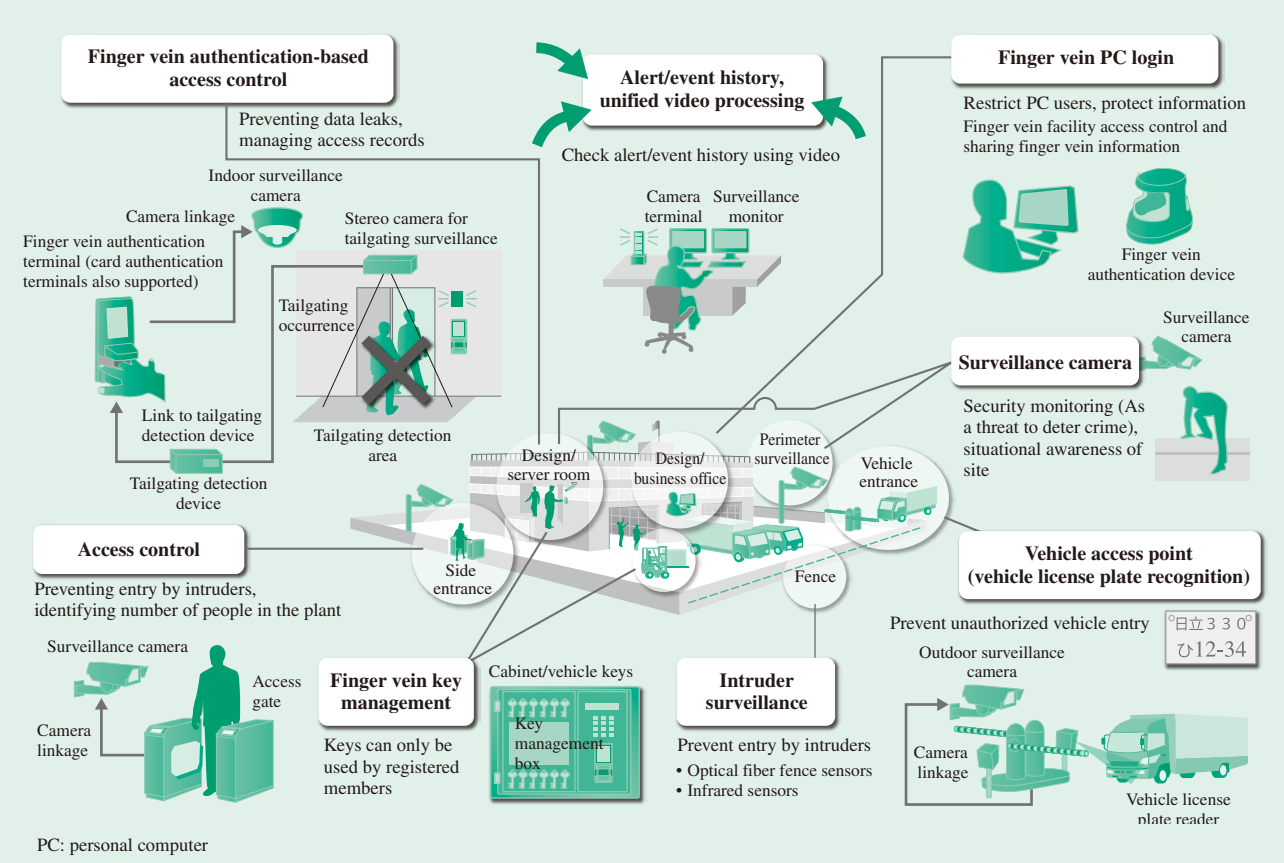


Fig. 3—Physical Security Solution in Plants.
Linking multiple security systems for integrated/central management of user information, alerts, history, and video lowers the management/surveillance workload and enables better business efficiency and quality through history/video correlation analysis.

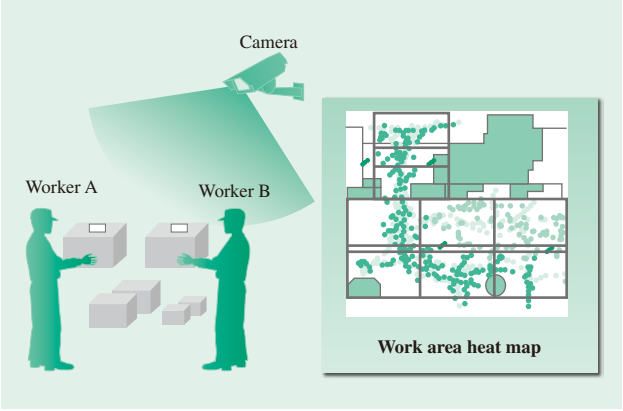


Fig. 4—Work Area Surveillance in Distribution Warehouse.
Worker movement flows analyzed using surveillance camera video can be displayed on work area maps for use in various investigations.

By providing integrated linking of surveillance cameras, video analysis systems, and analysis tools, Hitachi's integrated platform can be used to propose various solutions to address these issues. For example, video analysis of images from surveillance cameras installed in distribution warehouse work areas can be used to identify worker action zones and movement flows, enabling analysis to determine whether the work layout is efficient and safe for workers (see Fig. 4).

Solutions can also be used to enable supervisors to carry out improvement measures. For example, video analysis can be used to detect workers and transport equipment such as forklifts and pallet jacks, preventing collisions between them by sounding alarms. Behavior analysis can be used to determine whether work operations conform to rules, and the results used to create reports when infractions are found.

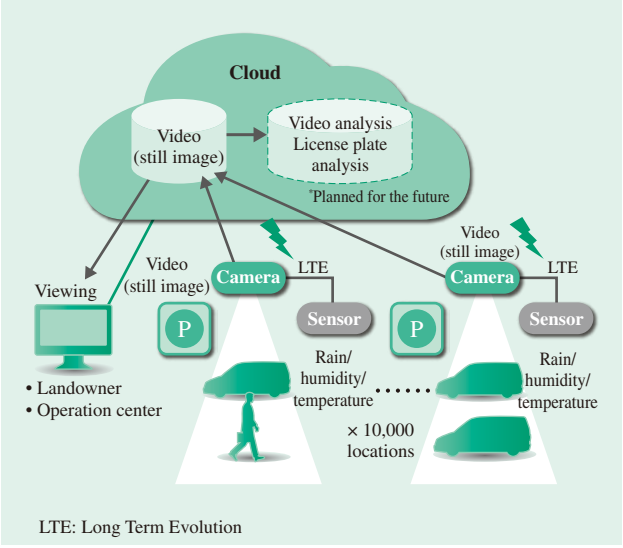


Fig. 5—Cloud-based Video Management System for Coin-operated Parking Lot.
Cameras installed in the parking lot are connected to a cloud system with an LTE connection. Video is collected for uses such as identifying parking lot usage conditions and preventing crime.

CLOUD-BASED SERVICES

When operating chains of establishments or operating in certain locations, customers may have small establishments that require cloud-based services on networks. Coin-operated parking lots are described here as an example (see Fig. 5).

Coin-operated parking lots are generally unmanned. Along with ensuring neighborhood security and preventing crimes in the parking lot, video surveillance and control are important operation goals that can be met using video analysis to identify illegal lot users and monitor suspicious behavior. Cloud systems are characterized by generally being designed for use with Long Term Evolution (LTE*) connections to connect the cloud system to the installed cameras or other sensors. (LTE is a pay-as-you-go public wireless network system.) So, unlike on-premises systems in local area network (LAN) environments, cost considerations prevent unlimited transfer of video data. Accordingly, methods are used to reduce the amount of data sent, such as sending still images periodically or sending still images whenever an event is detected (such as when a vehicle or person is detected, or a sensor is triggered). For fixed-interval video management, the video can be stored within the camera, and loaded into the system remotely when needed. Real-time video analysis in cloud systems creates a systematic time lag, so instead of monitoring video from the system, it may be more effective to use in-camera video analysis functions to send video to the cloud system when events are generated. In the future, cloud systems with embedded platforms may be able to use analysis functions installed as plug-ins to analyze accumulated video data analysis information and event logs in a correlated manner to provide added-value information tied to marketing and operational improvement.

CONCLUSIONS

This article has provided some examples of solutions driven by the integrated platform now being created

* LTE is a trademark of ETSI.

through the combined efforts of several Hitachi Group companies, and has described how the platform may be used in the future.

In the future, Hitachi will expand the range of linked Group companies, such as through ties to Hitachi's proprietary explosives trace detection system. It will also consider teaming up with competitor systems. Working as a cross-organizational host within the Hitachi Group, and as a tool for providing advanced solutions to customers, it will be the driving engine behind resolutions to customer business issues and collaborative creation with customers.

ABOUT THE AUTHORS

Tatsuhito Sagawa

Security Engineering Department, Industrial Manufacturing Solution Division, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd. He is currently engaged in the business of security solutions.

Tomokazu Murakami, Ph.D.

Media Systems Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the development of image recognition and processing techniques. Dr. Murakami is a member of The Institute of Electronics, Information and Communication Engineers (IEICE), the Institute of Image Information and Television Engineers (ITE), and The Virtual Reality Society of Japan (VRSJ).

Taisuke Kano

Physical Security Solution Division, Physical Security Solution Department, Hitachi Industry & Control Solutions, Ltd. He is currently engaged in the design of physical security solutions.

Wataru Ito

Engineering Development Department, Business Planning Center, Video & Communication Systems Division, Hitachi Kokusai Electric Inc. He is currently engaged in the development of an image processing and recognition technology. Mr. Ito is a member of the Information Processing Society of Japan (IPSJ) and The Society of Instrument and Control Engineers (SICE).

Masakazu Nakayama

Facility Solution Service Department, Facility Solutions Division, Hitachi Systems, Ltd. He is currently engaged in the system integration of physical security for facilities.

Ichiro Ote

Business Management Department, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd. He is currently engaged in the business of security solutions.

Featured Articles II

IoT Security

IoT System Security Issues and Solution Approaches

Shinsuke Tanaka
Kenzaburo Fujishima
Nodoka Mimura, Dr. Eng.
Tetsuya Ohashi
Mayuko Tanaka

OVERVIEW: By connecting various devices to a network and enabling data gathering and analysis, the IoT is expected to contribute to the creation of new customer value. Critical infrastructure that affects people's lives and economic activities will also become an area in which the IoT is used, so security measures for IoT systems are very important. On the other hand, a dramatic increase in the number of connected devices will create technical problems such as attacks with a broader scope of influence and attacks that last longer. So, a shortage of security operations administrators will also be a problem. This article focuses on availability, which is one of the key requirements for IoT security for critical infrastructure. The article presents approaches for proceeding quickly from problem detection to provisional measures to ensure availability, and detection technology developed by Hitachi that has high sensitivity and a low rate of false positives.

INTRODUCTION

WITH the recent spread of the Internet of Things (IoT), the number of network-connected devices is increasing dramatically. The connected devices are not limited to information devices. They comprise an increasingly diverse list of items, including life-related items such as vehicles and medical equipment, and items with potentially large impacts on society such as power stations and nuclear facilities.

Since the IoT consists of various network-connected devices, when one device is infiltrated by malware, it can become the starting point for the spread of the infiltration to other devices that could ultimately threaten critical infrastructure that should ordinarily be protected. Actual past security incidents have demonstrated that vulnerabilities in the communication software of devices connected to critical infrastructure such as work-use personal computers (PCs) and surveillance cameras have been targeted to enable unauthorized access from outside. These devices have been used as starting points for making critical infrastructure operate abnormally[(1)].

This article looks at the security issues involved in adopting the IoT, along with approaches for resolving these issues.

IoT SYSTEM FEATURES AND SECURITY ISSUES

Devices that previously had no communication functions are being connected to a network by IoT systems. These systems enable the discovery of phenomena that were previously unseen, providing new insights. When data gathered from connected devices is analyzed, new knowledge can be acquired. These features make the IoT a promising tool for increasing efficiency by reducing costs or increasing sales. However, in its discussion of security threats in the IoT era, the IoT Acceleration Consortium (a collaborative program with members from industry, academia, and the government) has underscored the need for measures to handle the following three issues: (1) the increasing number of network-connected IoT devices, (2) long life cycles, and (3) the difficulty of perfect manual surveillance[(2)].

In the discussion of the first issue, the increasing number of potential targets for attacks due to the increase in number of IoT devices, as well as the growing scope of influence of attacks have been pointed out. In the discussion of the second and third issues, it has been pointed out that IoT systems require little human involvement, so they can easily lapse into

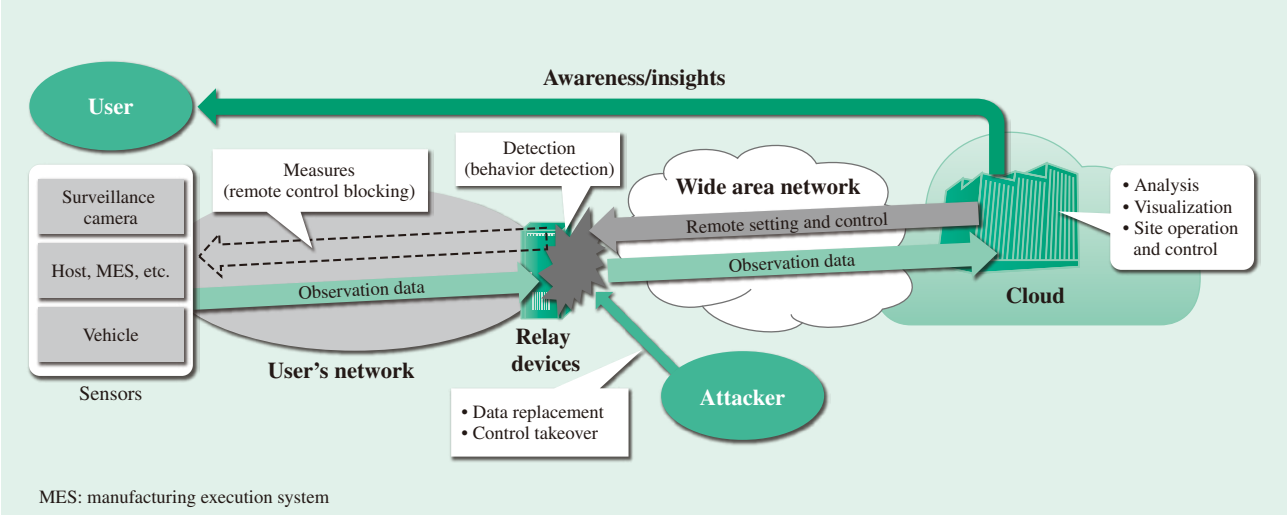


Fig. 1—Layered Architecture of an IoT System.
Relay devices are installed between the sensors and the cloud, and sensor information is gathered by the relay devices. Sensor problems are detected by the relay devices.

a situation where there is a shortage of administrators that makes attack detection difficult, and that long life cycles, over 10 years long, result in attacks that continue for long periods of time. The approaches that Hitachi has conceived to resolve these issues are described below.

APPROACHES TO RESOLVING ISSUES

To respond to the increase in network-connected IoT devices, Hitachi has adopted a layered architecture with relay devices installed between sensors and the cloud. These relay devices are used to gather large volumes of sensor information (see Fig. 1). They can take a variety of forms, such as gateways, switches and routers, depending on the client system.

When responding to the issues of long life cycles and the difficulty of manual surveillance, the two key points are: detecting problems as soon as they occur, and taking provisional measures to prevent the spread of damage while the system continues to operate.

Importance of Immediate Detection

Fig. 2 illustrates the importance of immediate detection using a model for calculating the cost of IoT security damage.

Security damage consists of direct damage and indirect damage. Direct damage includes the primary damage caused directly by the incident (the labor and equipment repair costs needed to handle the incident), and the profits lost due to equipment shutdown. Indirect damage includes the secondary damage caused by the spread of damage such as payment of compensation, damage caused by rumors, and loss of public trust.

Unlike incidents in information technology (IT) systems, incidents occurring in IoT systems can take several months to be discovered. When an incident occurs, the primary damage first starts increasing. Subsequently, the incident is discovered at time t_1, the cause is identified and then provisional measures are taken at time t_2, and finally the system is restored at time t_3. The secondary damage continues increasing

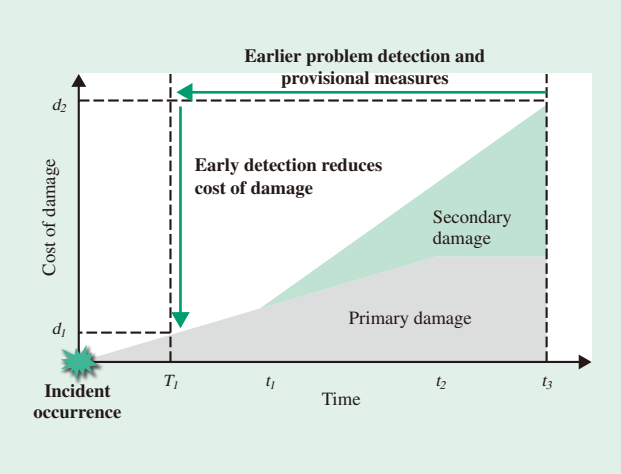


Fig. 2—Model for Calculating Cost of IoT Security Damage.
The cost of IoT security damage is the sum of the cost of the primary damage caused directly from the incident occurrence, and the cost of the secondary damage that occurs as the damage spreads. Carrying out problem detection and provisional measures at time T_1 can reduce the cost of the damage.

for a while after the provisional measures are carried out at time t_2. So, if problem detection and provisional measures can be carried out at time T_1 ahead of the natural discovery time t_1, the cost of the damage can be reduced from d_2 to d_1. The technology required for immediate detection is described in the next chapter.

Requirements for Provisional Measures

Provisional measures are needed immediately after problem detection. The methods used for provisional measures include isolating the location where the incident occurred, defending against further attacks, and reducing damage. Unlike IT systems, critical infrastructure systems often cannot be shut down when incidents occur, so the availability of the entire system must be the top priority when handling incidents.

Incident handling also requires business knowledge of the client systems that use the IoT, such as production lines and power systems. In other words, the same incident can require different handling measures for different systems, and customization involving thorough knowledge of how the client systems work.

Process Flow from Problem Detection to Provisional Measures

This section outlines the methods used to enable early problem detection and rapid provisional measures to ensure the availability of critical infrastructure.

For known problems with previously-created response methods, the process flow from problem detection to provisional response measures can be automated to enable rapid handling and ensure availability.

However, since there are no previously-created response methods for unknown problems, causes must be identified by means such as log analysis, response measures must be proposed for eliminating the causes, and the effectiveness of the proposed measures must be verified. The process flow from problem detection to provisional response measures, therefore, takes time. An effective way to shorten this time is to investigate response measures for hypothetical problems in advance, verify their effects, and create a manual of provisional response procedures.

Approach to Implementing Provisional Response Measures

If damage from incidents such as malware infiltration is expected to spread, one effective way to avoid the worst-case scenario (a complete system shutdown caused by the spread of damage) is to temporarily isolate only the location where the problem occurred from the system (as a provisional measure). To minimize the scope of the temporary isolation resulting from this provisional measure, the problem detection resolution should ideally have at least the same granularity as the isolation. The entire system should therefore be observed in overview to determine the scope of isolation of the location where the problem occurred.

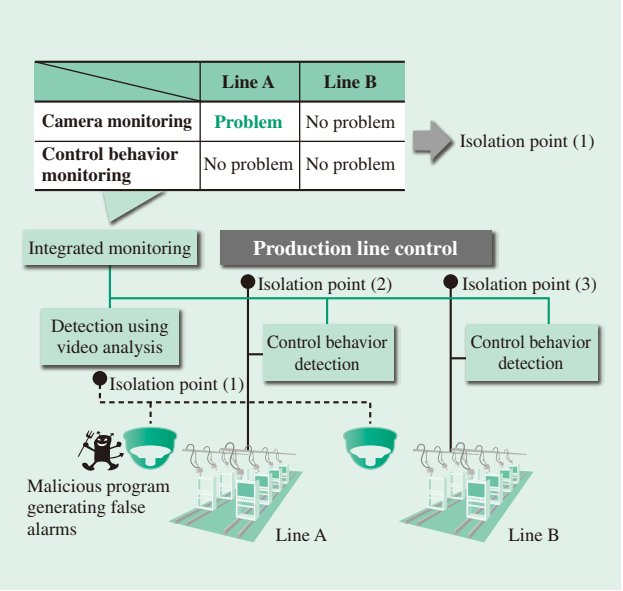


Fig. 3—Behaviors when Detecting Problems on Production Lines. The example above illustrates how two production lines can be monitored using a camera and control behavior to detect and isolate problems.

As an example, Fig. 3 illustrates how the behavior of two production lines (line A and line B) can be monitored by two methods—camera monitoring and control behavior monitoring.

First, consider a situation in which a malicious program is introduced into the camera for line A and generates false alarms indicating problems in line A. In this case, there is no problem with the control of line A itself, so the system is isolated at isolation point (1) to prevent the spread of damage. However, if a problem is found in both the camera and the control behavior of line A, then a problem in line A itself is deemed to have occurred, so the system is isolated at isolation point (2).

Creating a manual beforehand that specifies how to isolate the system depending on the nature of the problem in this way makes it possible to create provisional measures based on business knowledge. The provisional measures specified in this manual can then be implemented as programs at the isolation points, enabling them to be automated.

This method and the detection technology presented in the next chapter can be combined to enable the process from problem detection to provisional measures to be accomplished as rapidly as possible.

TECHNOLOGY FOR IMMEDIATE DETECTION

The security of critical infrastructure networks has conventionally been ensured by isolating the networks from the outside. However, these networks are becoming integrated with information networks to enable business innovation, and recently there have been demands to connect them to external networks to enable coordination with IoT-driven remote maintenance and other services (see Fig. 4).

Conventional cybersecurity measures have used methods such as antivirus software that detects viruses using definition files, and intrusion detection systems (IDSs) that detect intrusions using signatures that express the features of known cyber-attacks. While all of these methods are effective at detecting known attacks, their inability to detect zero-day attacks is a problem.

Anomaly detection technology has become an important means of solving this problem. This technology defines normal data in advance, and detects any deviation from it as a problem. Properly defining normal data requires operations administrators who have a thorough understanding of the network configuration and all areas of the customer's business, as well as the ability to configure complex settings. However, currently, there are not enough human resources who possess these skills. Moreover, there has been a recent increase in attacks that work by skillfully misusing standard built-in commands of operating systems (OSs) or software that was not developed for attack purposes, making them difficult to distinguish from normal data.

Hitachi has responded by developing a technology that provides high-sensitivity detection of behaviors on information networks that could be misused for attack purposes, even if they are behaviors that were previously considered normal (such as the execution of standard OS commands). To allay fears that the increased sensitivity of this technology might increase the rate of false positives, Hitachi has used a cyber kill chain model* to reduce false positives by evaluating risks not only in terms of points (single phenomena), but also in terms of planes (relationships and co-occurring states among points), focusing on serial changes[3]. This technology consists of three main functions:

(1) Server/PC internal operation monitoring function

Installed on an individual server or PC for protection. Monitors events such as universal serial bus (USB) memory insertion/removal and program startup to detect suspicious behaviors.

(2) Traffic anomaly detection function

Presents a visual representation of the traffic flowing over the network, and detects suspicious communications such as by identifying whether standard OS commands could have been misused for attack purposes, or whether backdoor communication has taken place. When installing function (1) on a device is difficult, function (2) provides an effective way to monitor the device's behavior using network traffic.

(3) Evaluation function using cyber kill chain

Evaluates risks in an integrated manner using the suspicious behavior and suspicious communication detected by functions (1) and (2).

This technology can be used to detect previously undetectable skillful attacks, and solve the problem of the operations administrator shortage.

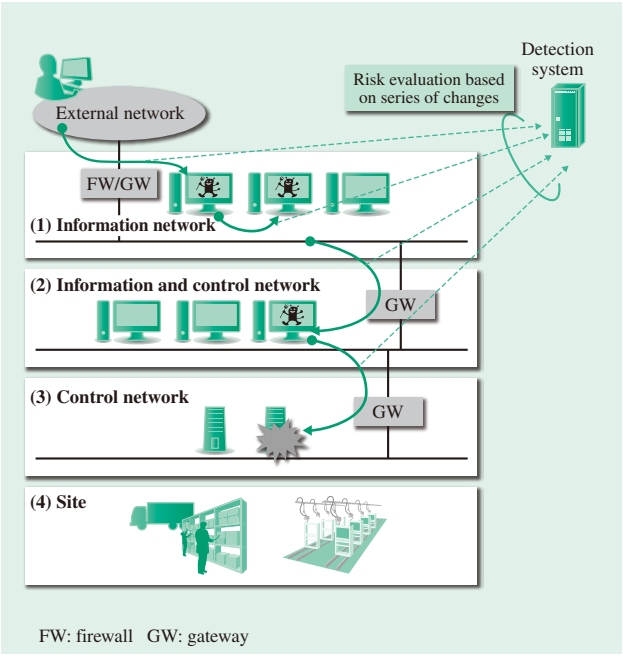


Fig. 4—IoT Value Chain Configuration.
Integrating systems from information networks through control networks, and then connecting them to external networks can improve business efficiency.

* A systematic approach to targeted attacks consisting of seven steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.

CONCLUSIONS

This article has discussed the security issues that have arisen as a result of the adoption and spread of IoT systems, the approaches for solving these issues, and the detection technologies serving as the elemental technologies of these approaches.

This work was supported by the Council for Science, Technology and Innovation (CSTI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber-Security for Critical Infrastructure" (funding agency: NEDO). In the future, Hitachi plans to apply the detection technologies described in this article to layered networks (information and control networks, and control networks), to carry out research and validation aimed at improving them, and then expects to put the knowledge obtained through these activities to use in new products.

REFERENCES

(1) IPA Website, "Vulnerability Countermeasure Guidelines for Control System Operators," https://www.ipa.go.jp/files/000044733.pdf in Japanese.
(2) IoT Acceleration Consortium Website, "IoT Security Trends," http://www.iotac.jp/wg/security/ in Japanese.
(3) N. Kawaguchi et al., "Detection of Advanced Persistent Threat Based on Cascade of Suspicious Activities over Multiple Internal Hosts," Transactions of Information Processing Society of Japan **57**, No. 3 (Mar. 2016) in Japanese.

ABOUT THE AUTHORS

Shinsuke Tanaka
Security Business Operation Center, IoT Business Operation, IoT & Cloud Services Business Division, Service Platform Business Division Group, Information and Communication Technology Business Division, Hitachi, Ltd. He is currently engaged in the business development of IoT security solutions.

Kenzaburo Fujishima
Network Research Department, Center for Technology Innovation – Information and Telecommunications, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of IoT systems, IoT security, and related technologies especially for critical infrastructure.

Nodoka Mimura, Dr. Eng.
Network Research Department, Center for Technology Innovation – Information and Telecommunications, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of IoT security solutions. Dr. Mimura is a member of The Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), and IEEE.

Tetsuya Ohashi
Platform 1st Dept., IoT Development Operation, IoT & Cloud Services Business Division, Service Platform Business Division Group, Information and Communication Technology Business Division, Hitachi, Ltd. He is currently engaged in the development of network and security solutions.

Mayuko Tanaka
Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. She is currently engaged in the research and development of measures against cyber-attacks.

Featured Articles II

Security Research and Development

Research and Development of Advanced Security Technology

Tadashi Kaji, Ph.D.

OVERVIEW: The damage done by cyber-attacks in recent years is spreading to all areas of society due to the targeting of IoT systems used in social infrastructure as well as IT systems. In response to these circumstances, Hitachi has been promoting the continuing research and development of cybersecurity as part of its mission of building and operating safe and secure social infrastructure. This article describes the research and development being undertaken to implement Hitachi's system security concept. The aim of this research is to achieve quick responses to cyber-attacks in cooperation with system stakeholders through the design and development of robust IoT systems that people can use for a long time to come with peace of mind.

INTRODUCTION

CYBER-ATTACKS on information technology (IT) systems are becoming more sophisticated. With corporate activity having become more dependent on IT, the potential for damage due to an attack on IT systems is a direct business risk.

Security countermeasures are also becoming essential for control systems, an area that was previously outside the scope of cyber-attacks, due the emergence of Internet of Things (IoT) systems that use IT for interconnecting devices. This makes it important for research into cybersecurity to take on new issues.

This article presents an overview of new research and development being undertaken in response to these circumstances, including an explanation of the security concept being promoted by Hitachi.

HITACHI'S SYSTEM SECURITY CONCEPT

Security countermeasures are essential for the IT and IoT systems used in social infrastructure, not just to protect information, but also in terms of the ability of social infrastructure to continue providing services despite being exposed to a variety of threats. Meanwhile, the increasing number of devices connected to networks means that targets that were not previously at risk of attack are now increasingly likely to suffer damage. Another new development is that IT and IoT systems are using interoperation to implement various functions.

Accordingly, Hitachi believes that action needs to be taken in response to the following three trends to ensure the information security of IT and IoT systems.

(1) Growing diversity of threats
(2) Importance of incident response
(3) Greater interdependence

To deal with these trends, Hitachi has been promoting its Hitachi system security concept since 2013[1] (see Fig. 1).

The implementation of security functions for components and security operation management

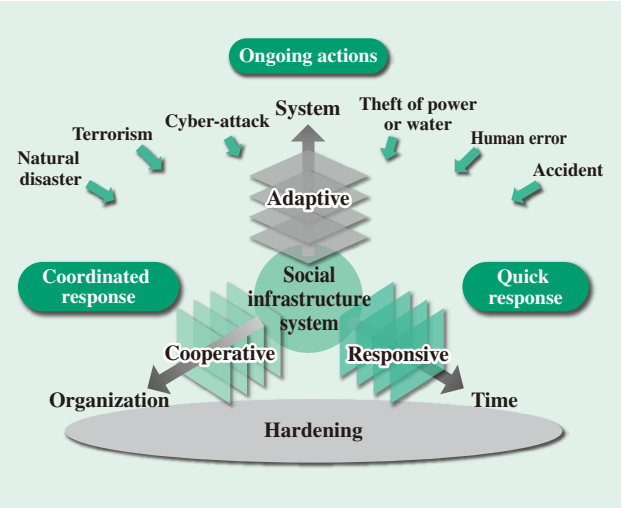


Fig. 1—Hitachi System Security Concept.
Along with the traditional idea of hardening, the Hitachi system security concept also highlights improvements to security in terms of it being adaptive, responsive, and cooperative.

for systems are both important for improving the information security of IT systems. The Hitachi system security concept identifies where improvements are needed to deal with the above three trends in terms of both functions and management.

FEATURES OF THE HITACHI SYSTEM SECURITY CONCEPT

This section gives an overview of the sort of security the Hitachi system security concept is seeking to achieve.

Building Robust Systems

A cyber-attack is an action that compromises the confidentiality, integrity, and availability of the assets in a system that are to be protected. To counter such an action, it is necessary to make the system more secure.

The first requirement for preventing cyber-attacks on an IT system is to identify and authenticate users and only permit access once identity is verified. Common methods used on past systems have included user name and password authentication whereby the user's identity is confirmed by having them enter a password that only they know, or having the user present a smartcard containing information identifying them that is protected by a personal identification number (PIN) so that only they can access it.

Unfortunately, there have been numerous instances on current IT systems of damage caused by "social engineering" methods that deceive users into revealing their passwords or phishing sites that covertly harvest passwords. Given the existence of various other methods, including being able to guess passwords easily or copy passwords that have been written down in a notebook, for example, or malicious use of sites for resetting passwords, any system that is based on existing systems cannot necessarily be described as secure.

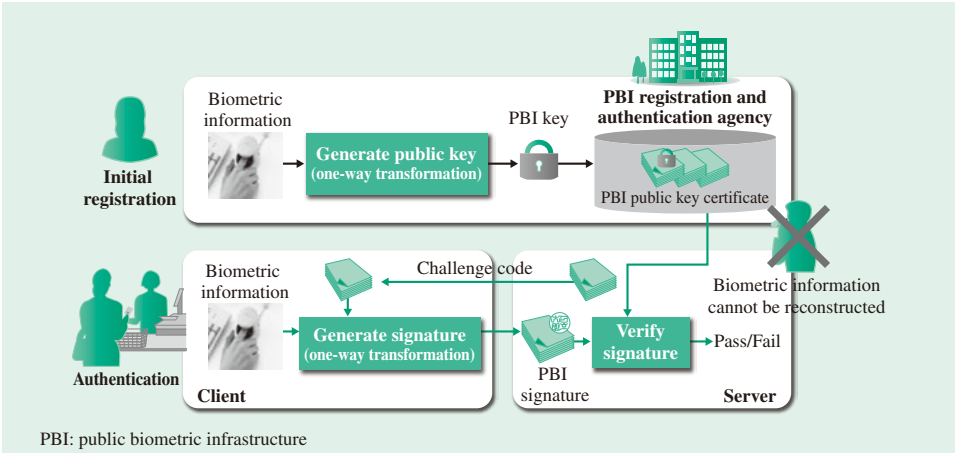
In response, Hitachi has developed a public biometric infrastructure (PBI) (see Fig. 2) for more secure personal identification that combines biometric information that cannot be stolen by an attacker with what is currently the most secure form of public key infrastructure (PKI).

Even more than IT systems, IoT systems with interconnecting devices have strong requirements for lower costs and are often implemented on low-cost hardware, even at the expense of processing performance. Accordingly, it has been difficult to include security functions for encryption that provide secrecy of communication paths and the exchange of authentication between communicating parties on current IoT systems. Hitachi has responded by developing resource-saving encryption techniques that target the hardware used by IoT systems and that are able to operate using minimal resources compared to past techniques.

Guarantee with respect to Long-term Availability

Unlike personal computers (PCs) or smartphones, the devices used in IoT systems sometimes need to remain in use for a decade or more in order to keep system costs down. By contrast, the methods used by cyber-attacks are evolving in ingenuity on a daily basis, such that there is a need for ongoing security countermeasures such as installing software patches when a new system vulnerability is identified.

Unfortunately, whether software is commercial or open source, software maintenance is only available for a limited time. As the support periods for IT systems are typically about five years, in order to provide a long-term guarantee, it is important that they



PBI: public biometric infrastructure

Fig. 2—How PBI Works. PBI provides a means of personal identification that prevents an attacker from impersonating a user by using a PBI key generated by a one-way transformation of biometric information.

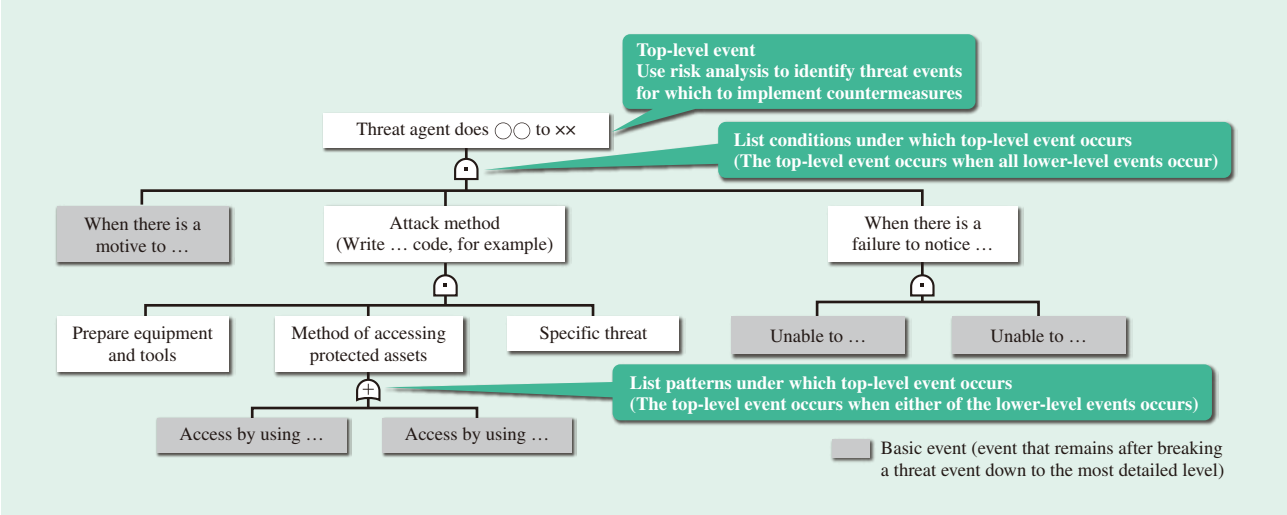


Fig. 3—Determine Threat Countermeasure Objectives Using Fault Tree Analysis.
Fault tree analysis is used to investigate how to counter the basic events that lead to threat events by considering the factors involved in terms of motivations, methods, and the conditions under which the threat events can occur.

are designed to allow for ongoing countermeasures as well as eliminating vulnerabilities. To achieve this, Hitachi has developed security design techniques intended specifically for IoT systems.

Devices used in IoT systems have sensors and actuators, which means they can interact with the physical realm as well as cyberspace. The focus of past IT systems has been on protecting information in cyberspace, with security design based on preventing information from being stolen or tampered with by third parties. This leaves room for doubt as to whether the techniques used on IT systems are suitable, in their current form, for the security design of IoT systems and devices. In the case of IoT devices that have potential implications for human life if subject to a cyber-attack, such as vehicles with a network connection, it is necessary to treat the device's control functions as an important aspect that needs to be protected along with information.

Hitachi has developed security design techniques specifically for IoT systems that build on those for IT systems and are characterized by identifying threats and considering countermeasures on the basis that the scope of protection also covers device functions. These techniques are based on standard security design procedures and are made up of four phases, namely, defining the scope to be considered, identifying security issues, formulating countermeasure objectives, and selecting security requirements. A feature of this process is that the things that the selected security requirements are intended to prevent can be logically explained by identifying the security issues and formulating the countermeasure objectives in an analytical and comprehensive manner.

Specifically, the particular task of identifying threat events among the security issues is performed with respect to the assets to be protected (including functions) in a comprehensive manner from the perspectives of *where*, *who*, *when*, *why*, and *what*. It can also produce logically explainable countermeasure objectives by conducting a detailed analysis of the attacker's motivations and methods and the conditions under which an attack can be launched for all of the identified threat events using the fault tree analysis method, and studying ways of countering the end events of the tree (see Fig. 3).

Achieving Quick Responses

IT systems have been exposed to a variety of cyber-attacks over the past half-century. As a result, IT vendors have built up expertise in security design and strengthened capabilities for responding quickly when an attack happens (incident response).

To avoid detection during an intrusion, targeted and other recent cyber-attacks have featured increased use of advanced and highly-engineered malware that only runs on systems with the targeted operating system (OS) or application installed. It has also been claimed that half of such malware is undetectable by existing anti-virus techniques based on pattern-matching.

Accordingly, to enable a response to be mounted against such malware at an early stage, Hitachi has been researching techniques for the automatic and rapid evaluation of malware behavior by executing

this highly-engineered malware under a wide range of different conditions and recording how it behaves. This helps achieve faster incident response by implementing exit point defenses, for example, based on behaviors identified by this technique, such as the transmission of information by the malware to a site controlled by the attacker, in which case connections to that site can be blocked (see Fig. 4).

Sharing Information to Improve Security

While convenience is improved through interoperation between IT and IoT systems, there are concerns about it increasing the overall harm to the system due to the damage resulting from an attack or incident on one subsystem leading to damage to other subsystems. To prevent this, it has become necessary to respond in a coordinated manner utilizing the *orient* and *decide* steps of incident response described above.

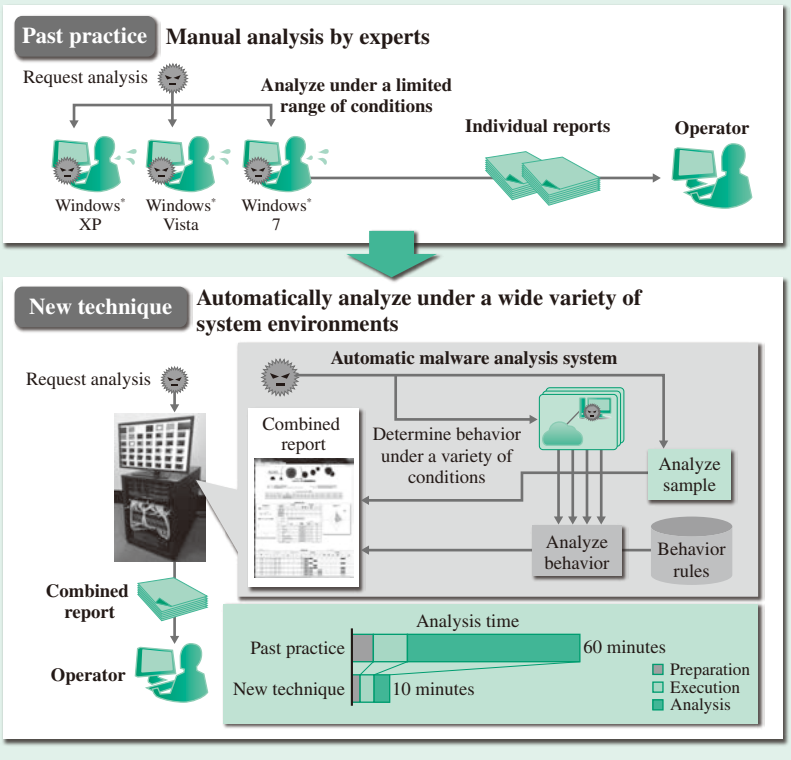
Hitachi has proposed its symbiotic autonomous decentralization concept for encouraging new growth by supplying value created by linking different systems and other mechanisms to all of the stakeholders in the associated systems[(2)].

In the case of symbiotic autonomous decentralized systems, obtaining an accurate understanding of what is happening across various different organizations or operators (subsystems) requires the sharing of information between organizations such as information sharing and analysis centers (ISACs) or incident response teams. In order to respond quickly, it is also important to be able to process incident response information automatically. The Cyber Threat Intelligence (CTI) Technical Committee (TC) of the Organization for the Advancement of Structured Information Standards (OASIS) is currently formulating the Structured Threat Information Expression (STIX*), Trusted Automated Exchange of Indicator Information (TAXII*), and Cyber Observable Expression (CybOX*) standards specifying key information formats for IT systems, and work has just started on adapting these standards for use on IoT systems.

STANDARDIZATION ACTIVITIES

Moves to formulate a variety of standards for IoT system security are accelerating. For industry, work is proceeding on the IEC 62443 security

* STIX, TAXII, CybOX and the CybOX logo are trademarks of The MITRE Corporation.



* Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Fig. 4—Malware Automatic Analysis Technique.
This technique automatically analyzes malware under a wide variety of system environments to determine the behavior of malware that varies depending on the environment.

standard for control systems, primarily through the International Electrotechnical Commission (IEC). For areas that deal primarily with networks and IT, standards bodies such as the IEEE, oneM2M, the International Organization for Standardization (ISO), and International Telecommunication Union Telecommunication Standardization Sector (ITU-T) are working together to formulate security standards.

Hitachi's involvement to date in security standardization for IT and IoT systems has included contributing to the establishment of security concepts and to implementing security functions that take account of the characteristics of IoT systems.

In the former case, Hitachi is contributing to the IEC to improve security by guaranteeing long-term availability, achieving a quick response, and information sharing as well as building systems that are resilient, in step with trends in IoT and IT systems. Hitachi is also working with the Control System Security Center, a Japanese technology research organization, to conduct research and development using standards, with work proceeding on raising awareness and a program of security exercises.

In the latter case, Hitachi has proposed a lightweight (able to run on minimal resources) encryption algorithm to ISO and IEC with the aim of enabling security functions to be implemented on IoT devices that need to deliver realtime performance despite limited central processing unit (CPU) and memory capacity. As a lightweight encrypted communications protocol is also required for IoT devices to verify each other's identity and to gain access to secure communication links, Hitachi has proposed a standard technique to the ITU-T and is participating in the formulation of standard techniques at oneM2M.

CONCLUSIONS

Because IT and IoT systems will serve as platforms for the social infrastructure of the future, it is critical that they utilize the latest technology to provide for all eventualities, including cyber-terrorism. This article has provided an update on the latest research on security for IT and IoT systems in the context of the Hitachi system security concept.

Current techniques for building resilient systems provide the basis for maintaining the cybersecurity of IT and IoT systems with low cost and long life. It is also important to identify threats during system development and maintain the most effective countermeasures over a long period of time, to mount a quick response during system operation, and to strengthen defenses against increasingly sophisticated cyber-attacks by sharing security information between stakeholders. Hitachi intends to continue contributing to the creation of safe and secure social infrastructure by working on the research and development of the latest technologies based on these considerations.

REFERENCES

(1) M. Mimura et al., "Hitachi's Concept for Social Infrastructure Security," Hitachi Review **63**, pp. 222–229 (Jul. 2014).
(2) N. Irie et al., "Information and Control Systems –Open Innovation Achieved through Symbiotic Autonomous Decentralization–," Hitachi Review **65**, pp. 13–19 (Jun. 2016).

ABOUT THE AUTHOR

Tadashi Kaji, Ph.D.
Security Research Department, Center for Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. He is currently engaged in the research and development of cyber security technology. Dr. Kaji is a member of the IEEE Computer Society.

Hitachi Review

Hitachi Review Volume 65 Number 8 September 2016

ISSN 0018-277X
Hitachi Review is published by Hitachi, Ltd.
Visit our site at www.hitachi.com/rev
Address correspondence to: The Editor, Hitachi Review, Advertising Dept., Corporate Brand & Communications Div., Hitachi, Ltd.
Shin-Otemachi Building, 2-1, Otemachi 2-chome, Chiyoda-ku, Tokyo, 100-0004 Japan
Editor-in-Chief: Akira Banno

Date of Issue: September, 2016
Printed in Japan by Hitachi Document Solutions Co., Ltd.

XR-E066