Hitachi Review
Volume 63 Number 5 July 2014

HITACHI
Inspire the Next

Social Infrastructure Security

www.hitachi.com/rev

Hitachi Review
Volume 63 Number 5 July 2014

From the Editor

Social infrastructure systems deliver services in many areas that underpin our social activity. These operate ceaselessly, 24 hours a day, 365 days a year, extending from electric power, water, gas, and other services that we use directly in our daily lives through to services such as the public transportation and facilities that sustain the activity of people and businesses. Meanwhile, numerous threats that put the provision of these services at risk have been emerging in recent years. Along with accidents or faults, a diverse range of threats including natural disasters and freak weather conditions as well as armed attacks and cyberterrorism are on the rise. Social infrastructure security is about providing the means to protect our way of life from these threats.

The provision of social infrastructure security requires envisaging all possibilities and devising countermeasures to cover these, without leaving any gaps. To achieve this in practice, Hitachi seeks to implement security measures for dealing with all threats by considering them in terms of: (1) Adaptability for providing all-encompassing preventive measures, (2) Responsiveness for responding quickly and appropriately when an incident does occur, and (3) Cooperativeness for maintaining security through collaboration between different organizations.

This edition of *Hitachi Review* describes Hitachi's views on how best to provide social infrastructure security, and presents technologies, products, and solutions that implement these ideas. While security impinges on many areas, the articles in this issue break the field down into: (1) Physical security for ensuring the security of various different types of facilities or equipment, defending against armed or other forms of violent attack, and preparations for dealing with natural disasters; (2) Information security for keeping information safe from viruses and other malware attacks; and (3) Control security for defending against attacks on the control systems and embedded systems that underpin social infrastructure. Regardless of the sector involved, Hitachi recognizes the importance of devising preventive measures that take account of various different angles, adopting the concept of damage limitation (accurate information sharing and timely command and control to minimize the damage when an incident does occur), and the use of exercises to improve the ability to deal with unanticipated events.

Along with providing a better understanding of how Hitachi views social infrastructure security, I hope that this issue will prove beneficial to your business and to making the world a safer place.

Editorial Coordinator,
Social Infrastructure Security Issue

Toshiaki Arai
CTO
Defense Systems Company
Hitachi, Ltd.

Social Infrastructure Security

The social infrastructure that underpins our daily lives and business activity is expected to deliver services non-stop, regardless of any disruptions that may occur.
Given the growing diversity in recent years of threats with the potential to interrupt the operation of this infrastructure, such as natural disasters or cyber-attacks, security measures able to deal with all manner of situations are essential.
With its many years of experience working in the field of social infrastructure, Hitachi is also striving to enhance its security.
Through a range of solutions that satisfy the need for future security to be adaptive, responsive, and cooperative, Hitachi is helping make the infrastructure of society safer and more secure.

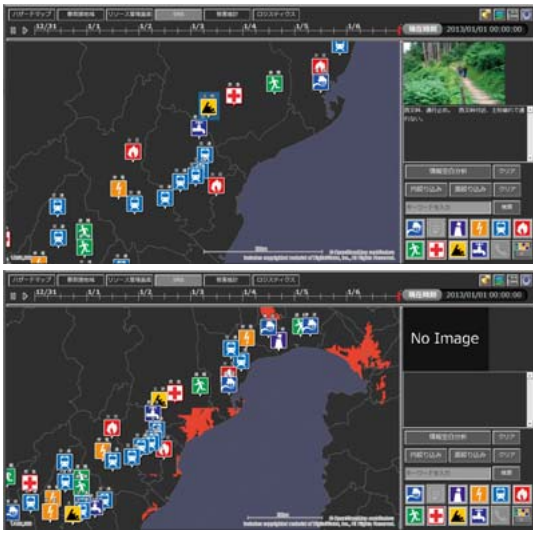

Security solutions for airports or railway stations (image)

Physical security solutions for factories (image)

Marine defense and underwater security solutions (image)


Predictive diagnosis service for social infrastructure maintenance (image) (left) and its use in a demonstration project (right)

Multimodal malware analysis system with multiple types of sandboxes (analysis environments)



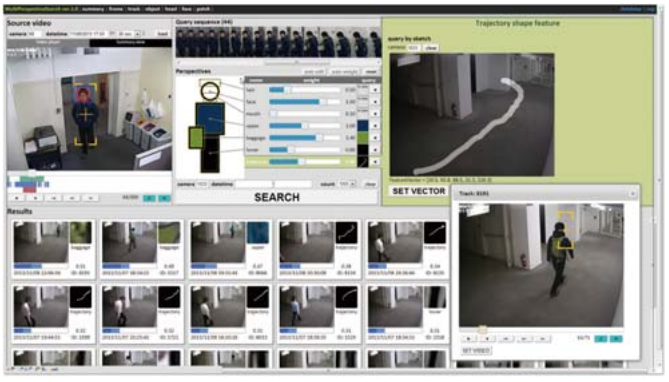
Use of SNS information during major disasters (example screen shot)

Hand luggage inspection machine with built-in explosives detection
(Hitachi Power Solutions Co., Ltd.)

* This technology was developed under the “R&D Program for Implementation of Anti-Crime and Anti-Terrorism Technologies for a Safe and Secure Society” of the “Funds for Integrated Promotion of Social System Reform and Research and Development” of the Ministry of Education, Culture, Sports, Science and Technology.

Unconscious authentication technique combining facial image and finger vein recognition

Traceable physical security (example screen shot of integrated viewer)



Example user screen of multi-perspective search system

Expert Insights

Recent Cyber-attacks and How Organizations Can Respond

Ryoichi Sasaki

Professor
Department of Information Systems and Multimedia Design
Tokyo Denki University

Graduated from The University of Tokyo and entered Hitachi, Ltd. in 1971 where he worked at the Systems Development Laboratory on topics that included techniques for improving system reliability and security technology. He took up his current post in April 2001.
Doctor of Engineering (University of Tokyo); Chairman, Japan Society of Security Management; Advisor on Information Security, National Information Security Center; Visiting Professor, National Institute of Informatics.
His publications include “Introduction to Internet Security” (Iwanami Shinsho, 1999) and “Concept of IT Risk” (Iwanami Shinsho, 2008), both in Japanese.

Along with attacks from hackers motivated as much as anything by their own amusement, the increasing diversity of cyber-threats also encompasses a growing number of sophisticated attacks from spies and the like seeking to obtain confidential information. A well-known form of this latter threat is the following type of targeted e-mail attack.

Step 1: Initial intrusion: An e-mail with a virus-infected file attachment is sent to the personal computer (PC) of a key person at the targeted organization. Opening the file causes the PC to become infected.

Step 2: Escalation of intrusion: An attempt is made to penetrate servers on the local network from the infected PC.

Step 3: Mission accomplished: Confidential information is stolen from the infected PC or servers.

A targeted e-mail attack differs from a conventional spam attack in various ways. These include, (1) The content of the e-mail is chosen specifically for the individual targeted so as to encourage them to open the file, (2) The small number of such attacks means that the anti-virus provider may not be aware of the virus’s existence, and therefore virus scanning may be unable to detect and remove it, and (3) Once a PC is infected, it can make ongoing attempts to access servers on the local area network (LAN) with the aim of acquiring information.

Just because you believe that no spy would have reason to mount a targeted e-mail attack on your own company is no cause for complacency. It is not unknown for such attacks to start, not by attacking the target directly, but by stealing information from affiliated companies or customers that can then be used to penetrate the real target company.

A growing trend in recent times has been the use of “water hole attacks” that attempt to infect computers with a virus by illicitly tampering with websites frequented by users at the targeted organization. To make it difficult to detect which websites have been compromised, a common practice is to only attempt infection in response to access from specific Internet protocol (IP) addresses, such as those of government agencies.

As we approach the Tokyo Olympics in 2020, we can expect cyber-attacks on Japan to become increasingly sophisticated and diverse. Equipping our organizations with the capabilities to put comprehensive countermeasures in place is a matter of urgency.

Technotalk

People and Systems Working in Harmony to Make Social Infrastructure More Resilient

Makoto Takahashi, Ph.D Professor, Management of Science & Technology Department, Graduate School of Engineering, Tohoku University
Shuji Senoo Senior Director, Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd.
Masahiro Mimura, Ph.D. Department Manager, Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd.
Toshihiko Nakano, Ph.D. General Manager, Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd.
Toshiaki Arai, Ph.D. CTO, Defense Systems Company, Hitachi, Ltd.

Cyber-attacks and other threats to information security have been growing in recent years. Meanwhile, rising concerns about natural disasters and terrorism have made the provision of comprehensive countermeasures against events such as these an issue for society. Along with putting measures in place to counter growing threats, maintaining the safety of social infrastructure systems also requires appropriate measures for minimizing damage. Hitachi has built up a portfolio of security technologies in fields ranging from social infrastructure to physical security. Through total security solutions that utilize these technologies, Hitachi intends to help create a society that is safer and more secure.

Defense in Depth to Deal with the Unexpected

Arai: Along with the growth in threats to the safety and security of society, concern about the security of social infrastructure is also growing. Professor Takahashi currently heads the Tohoku Tagajo Headquarter of the Control System Security Center, of which Hitachi is a member. Can you please explain which aspects of social infrastructure security you are looking at in particular?

Takahashi: My main research topic is the security of large systems such as nuclear power plants or air traffic control systems that, if disrupted, have a major impact on society. I am looking in particular at how to improve the overall security of systems, including human factors. The idea of the "unexpected" was a key legacy of the Great East Japan Earthquake. However much you allow for various different situations, it will not prevent the unexpected from happening. Whatever capabilities you build into your systems, there will always remain some aspects where you must rely on the adaptability and flexibility of people to deal with the unexpected. My research looks at how these human factors can make

Makoto Takahashi, Ph.D

Professor, Management of Science & Technology Department, Graduate School of Engineering, Tohoku University

Graduated in 1986 with a degree in nuclear engineering from the School of Engineering, Tohoku University, and earned a doctoral degree in nuclear engineering from the Graduate School of Engineering, Tohoku University in 1991. After appointments that included assistant professor at the Graduate School of Engineering, Tohoku University in 2000, he took up his current position in 2011. He is also currently the head of the Tohoku Tagajo Headquarter of the Control System Security Center. He is a director of the Atomic Energy Society of Japan and of the Human Interface Society. He specializes in cognitive engineering, system engineering, and human error analysis.

Shuji Senoo

Senior Director, Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1984. After working as a system engineer in the public sector division of Hitachi that develops systems for local government and other government agencies, he commenced his current security-related work in 2002.

overall systems safer.

Senoo: In the case of cyber-security where new viruses and other forms of malware are continually emerging, there is no hope of being able to anticipate all risks in advance. Taking the unexpected as a given, it is important to focus on damage limitation, which means looking at how to reduce the unexpected and how to minimize damage when it does occur.

Mimura: Targeted attacks have recently become a problem for cyber-security. These are attacks that target specific devices by exploiting little-known vulnerabilities. Because the tendency in the past was to spread viruses far and wide, vulnerabilities could be identified and patched quickly. Targeted attacks on the other hand, because they are directed at a limited number of targets, are difficult to spot and are capable of doing large amounts of damage before being detected. Along with the elimination of vulnerabilities, "risk hedging" techniques that minimize damage also have an important role in dealing with this new type of threat.

Takahashi: In this sense, I also believe that a "defense in depth" approach is important. This is a fundamental concept in the military realm. Rather than erecting protective measures in duplicate or triplicate, what it means is ensuring that if one line of defense fails, other lines will continue to function. By adopting this practical approach as the basis of our planning, I believe that we can minimize the ultimate damage.

Extending Range of Regular Exercises, and Use of Information during Emergencies

Arai: Conducting command and control system training exercises is also important for reducing risks caused by human factors. Especially in the case of the emergencies that arise during a large disaster, a change in attitude is also crucial because of the different operations that are required compared to normal situations, such as working diligently through the observe, orient, decide, and act (OODA) loop.

Takahashi: In the case of large systems, simulators are used to perform exercises under near-real-world conditions. While these can include one-in-tens-of-million situations with multiple simultaneous incidents, their value depends on the details of the exercise itself. As scenario-based exercises are ineffective at delivering the unexpected, a worthwhile approach is to conduct planned exercises in which the scenario after a certain point is left undisclosed. Also, however many exercises are conducted, because the availability of information during an actual disaster can be a matter of life or death, it is also important to put measures in place for utilizing information during an emergency.

Senoo: The USA is proceeding with the adoption of a standard model for information sharing called the National Information Exchange Model (NIEM) so that preexisting infrastructure for sharing information between government, agencies, municipalities, and other participants will be available during an emergency such as a disaster or terrorist attack, and to establish the mechanisms for the smooth flow of information between the various systems involved. Japan is also looking at open data practices that encourage the availability and use of public information collected and held by government agencies. However, numerous issues still remain. Together with the use of technologies such as those for preventing tampering, I believe that making public data available in a form that facilitates secondary use is essential to conducting

Masahiro Mimura, Ph.D.

Department Manager, Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1997. After working on the research and development of financial systems and of biometric and other security technologies and systems, he commenced work in 2012 on the research and development of financial and public sector solutions together with software productivity techniques used by these solutions, and of system security technology.
Dr. Mimura is a member of the Information Processing Society of Japan (IPSJ).

Toshihiko Nakano, Ph.D.

General Manager, Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1980. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

operations appropriately during a disaster or other emergency.

Security Risks for Control Systems

Arai: Another human consideration is that, while progress has been made on information security management systems (ISMSs) and other measures for preventing information leaks and other unauthorized tampering with corporate information systems, there is a need for rethinking attitudes to the security of control systems.

Nakano: Whereas control systems in the past were closed systems and not seen as under threat from cyber-attacks, factors such as the use of general-purpose platforms, networking, and portable storage media mean that risks are growing. I believe we have an obligation to help raise general knowledge of security and risk awareness in the control systems field.

Senoo: Security requires more than just experts with specialist knowledge. The problem is that protection functions will only work if the staff responsible for day-to-day activities have a basic understanding of security. Otherwise, their naivety will leave them prone to opening files attached to targeted e-mail attacks, for example. The challenge for businesses, I believe, is to ensure that security knowledge is spread widely, not just among system engineers (SE) and other non-technical personnel.

Mimura: The idea that security involves work and cost is also deep-rooted, I believe. Along with emphasizing the importance of security, other areas I think we should be working on include adopting countermeasures against cyber-attacks that minimize the amount of human intervention required, and the use of information technology (IT) for automation and to support administrators.

Takahashi: An important factor when an actual cyber-attack occurs is to be able to determine quickly whether it is in fact a cyber-attack rather than simply an operational problem caused by a fault in the system. While one system-based technique is to use predefined signatures to detect attacks automatically, another important approach is to have countermeasures that provide a common operational picture (COP) and other appropriate information to the people who administer the system, and to support them in situation assessment, decision making, and other related tasks.

Senoo: Because security is a new field in the case of control systems in particular, there is no way of knowing what unexpected threats may arise. Accordingly, we are focusing on ways of issuing warnings as quickly as possible and providing assistance to administrators. One example is a solution we have developed that uses decoy servers in a system to detect virus intrusion and infection at an early stage, and that alerts administrators accordingly to prevent the infection from spreading. In the social infrastructure sector, in particular, where system availability is critical, the system is being built to operate continuously over long periods.

Nakano: Compliance with the IEC 62443 international standard for security is starting to become more common in the control system sector. I believe we need to contribute to this standardization process with a view to standardizing highly reliable techniques built up over time, with the aim of ensuring security everywhere from individual components up to entire systems, operations, and society.

Toshiaki Arai, Ph.D.

CTO, Defense Systems Company, Hitachi, Ltd.

Joined Hitachi, Ltd. in 1978. Prior to taking up his current position, Dr. Arai worked on information system research and development at the then Systems Development Laboratory.

Utilizing Human Factors to Enhance Resilience

Takahashi: A recent interest of mine has been the field of resilience engineering. While resilience normally refers to a system's ability to withstand or recover from a shock, the concept is also becoming important for security. Past security measures have sought to identify the cause when an incident occurs so that measures can be adopted to prevent it from happening again. While I certainly do not want to discredit that approach, there are also cases when, rather than focusing on rare examples of failure, it is better to analyze why practices work successfully in an ever-changing environment, and to implement them accordingly. Also essential to the progress of security technology, I believe, is an approach that focuses on why practices work and establishes processes for preventing incidents by enhancing resilience through human factors, such as people's ability to make accurate predictions, to respond, and to act with flexibility.

Nakano: In the event of a major disaster or other incident of a sort that happens only once in a lifetime, there is always a potential for panic, even among people who have been through numerous training exercises. What is needed to deal with such situations, I suspect, is to study past examples of success and failure, and to have systems that can supply the best possible information in a timely manner to assist people in decision making.

Takahashi: Getting people and systems to work in harmony will be increasingly important in the future. One example might be for machines and other systems to leave decisions to people during normal situations, but also to read their state of mind from biometric or other data and provide them with assistance in situations where they appear to be reaching the limit of their capabilities, the point where they are potentially becoming unreliable. If systems like this become possible, that would be the ideal. We have embarked on research into the basic technology for such systems, which we call adaptive interfaces.

Arai: Having people and machines working harmoniously together will also be critical for physical security within Japan, which will become increasingly important as we approach the Tokyo Olympics in 2020. Hitachi has strengths in IT and is hoping to use these skills to contribute to better physical security, by combining surveillance cameras and image recognition, for example.

Senoo: There will also be uses, I believe, for biometric authentication techniques such as finger vein recognition. There have also been moves in recent times to analyze information such as people's movements ("pedestrian flow") or position information from mobile phones, and to use this for security or to improve services. If Japan as a nation can clarify its policies on privacy and information use, it will make it easier for us to develop the technologies for this use.

Mimura: Hitachi sees adaptability, readiness, and harmony as being the three key concepts needed for social infrastructure security. Adaptability means the idea of implementing security measures at all layers within a system, from the individual components up to the middleware that ties them together and the applications that run on this middleware. Meanwhile, because there is still a risk of these being compromised due to infection by a virus, the concept of readiness means being able to respond promptly to any situation. Likewise, harmony means taking steps to share information obtained about viruses or other vulnerabilities as quickly as possible with the rest of the community, including the Information-technology Promotion Agency, Japan (IPA) and the Japan Computer Emergency Response Team (JPCERT). While this already happens, I believe we should go even further and establish mechanisms for more pooling and sharing of the information needed to improve security right across society, not just for IT systems and physical security, but also for the control systems that underpin social infrastructure. I see these key concepts as also being important for security in other areas.

Arai: Hitachi supplies total security solutions based on technologies that support security in a wide range of fields, from IT and control systems to physical security. Drawing on our discussion today, I hope we can contribute to enhancing the safety and security of society. Thank you for your time today.

Overview

Hitachi's Concept for Social Infrastructure Security

Masahiro Mimura, Ph.D.
Toshiaki Arai, Ph.D.
Toshihiko Nakano, Ph.D.
Ryuichi Hattori
Atsutoshi Sato

GROWING IMPORTANCE OF SOCIAL INFRASTRUCTURE SECURITY

SOCIAL infrastructure includes the facilities, equipment, and systems that underpin social activity by people and economic activity by business. It provides the public with government, finance, healthcare, and other services, including electric power, gas, water, and railways (see Fig. 1). Accordingly, social infrastructure is expected to operate non-stop, 24 hours a day and 365 days a year, or to provide core essential services under all circumstances. This is one of the key characteristics of social infrastructure systems.

Furthermore, rather than existing independently within the social infrastructure, these services are inherently interdependent. For example, railways need electric power to operate, while the staff of power companies commute to work by rail. In this way, the infrastructure of society constitutes a single enormous interlinked system, with active use being made of information and communication technology (ICT) to ensure its smart operation. One such example would be a smart city in which ICT, environmental technologies, and other techniques are combined to make effective use of electric power.

In Japan, the term "security" has generally been used to refer to information security, in the sense of keeping information confidential. When the application of the term is extended to cover social infrastructure, however, the meaning should include the need to protect the social infrastructure from a variety of threats so that it can continue to deliver services unimpeded. Hitachi uses the term "social infrastructure security" to refer to this wider sense, and has formulated a concept that expresses the future requirements for the security of social infrastructure based on ongoing changes in society and technology. This article reviews current trends in the field of social infrastructure, identifies the security requirements, and explains Hitachi's concept for social infrastructure security.

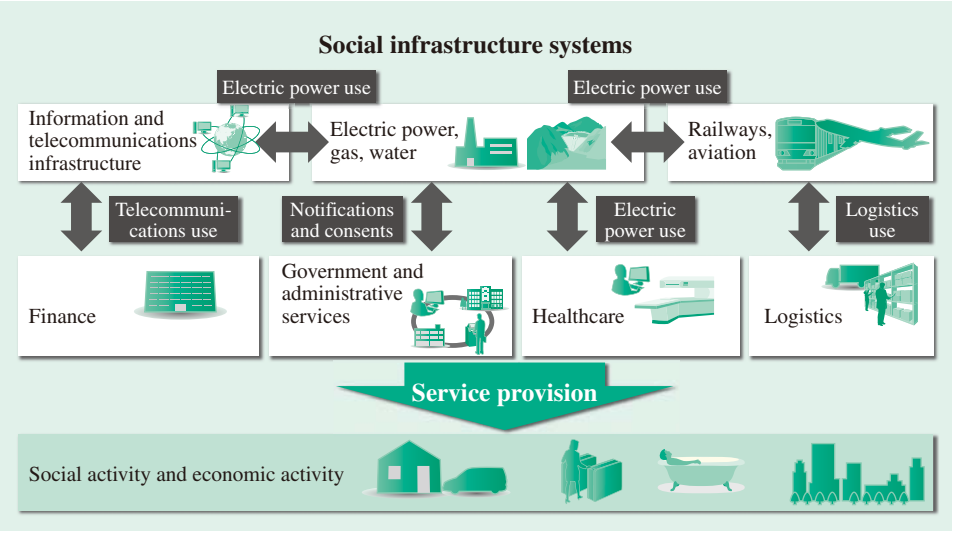


Fig. 1—Social Infrastructure Systems.
Made up of the facilities, equipment, and systems that underpin social activity by people and economic activity by business, the social infrastructure forms an enormous interlinked system comprised of mutually interdependent sub-systems.

TRENDS IN SOCIAL INFRASTRUCTURE SECURITY

Three trends influencing social infrastructure security are the growing diversity of threats, the importance of incident response measures, and increasing interdependence (see Fig. 2).

Growing Diversity of Threats

The threats faced by social infrastructure in the 21st century have included unanticipated natural disasters, accidents, and attacks, with attacks being targeted not just at particular facilities or equipment but at ICT in general (cyberspace, in other words). The attack by the Stuxnet virus on power plants in 2010, for example, can be seen as a new form of threat to key facilities that utilize ICT.

Similarly, a review of the nature of cyber-attacks indicates their high level of sophistication, such as those that exploit little-known vulnerabilities to mount targeted attacks on particular organizations or people, or watering hole attacks that work by infiltrating malware into websites visited by large numbers of the public. Also anticipated is the emergence in the future of cyber-attack services provided by people with the specialist skills needed to do so, thereby making it easy for people who lack those skills to execute attacks.

Meanwhile, natural disasters have been becoming more frequent and larger in scale over recent years. Major hurricanes such as Katrina in 2005 and Sandy in 2012, for example, have resulted in urban flooding, widespread power blackouts, paralyzed transportation systems, and interruptions to banking and local government services[(1)]. In Japan, recent years have seen examples of house collapses, flooding, and other damage resulting from events such as tornados or localized heavy rain (called "guerrilla rainstorms" in Japan).

With these threats to the social infrastructure becoming more diverse, there is a need to prepare for previously unanticipated types of threat.

Importance of Incident Response Measures

Security is typically based on a defense in depth approach. This involves putting in place a number of defenses against particular attacks or disasters so that at least one of these measures will be enough to prevent damage from occurring. An example from the field of cybersecurity is to protect information systems that hold confidential information by combining both internal measures, which prevent infection by viruses seeking to steal this information, and outbound measures, which prevent such information from leaving the system. This is a case of making the most of available information to establish preemptive measures.

However, with social infrastructure now facing an increasingly diverse range of threats, as noted above, it is not practical to expect that countermeasures can be put in place to deal with all possible future threats or disasters. Given the potential for damage from such unanticipated causes to occur even if countermeasures against foreseeable events are established based on the defense in depth philosophy, there is a need to consider incident response measures that can be implemented after the damage occurs. One example of this is the concept of damage limitation, meaning the mounting of a quick response to an attack or disaster in order to limit the magnitude and spread of its consequences, even if unable to prevent the damage resulting from the event itself.

That the importance of this type of incident response measure is coming to be recognized is evident in recent developments in the area of international standardization. One example from the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27000 series of international standards for information security management is ISO/IEC 27031:2011 (Guidelines for information and communication technology readiness for business continuity) published in 2011, which provides guidelines for

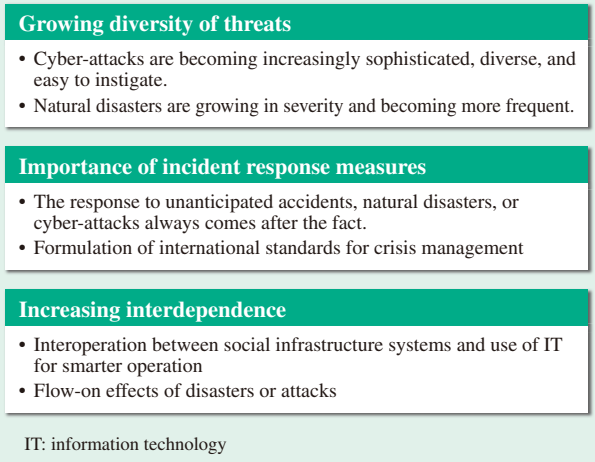


Fig. 2—Trends in Social Infrastructure Security.
Three trends influencing social infrastructure security are the growing diversity of threats, the importance of incident response measures, and increasing interdependence.

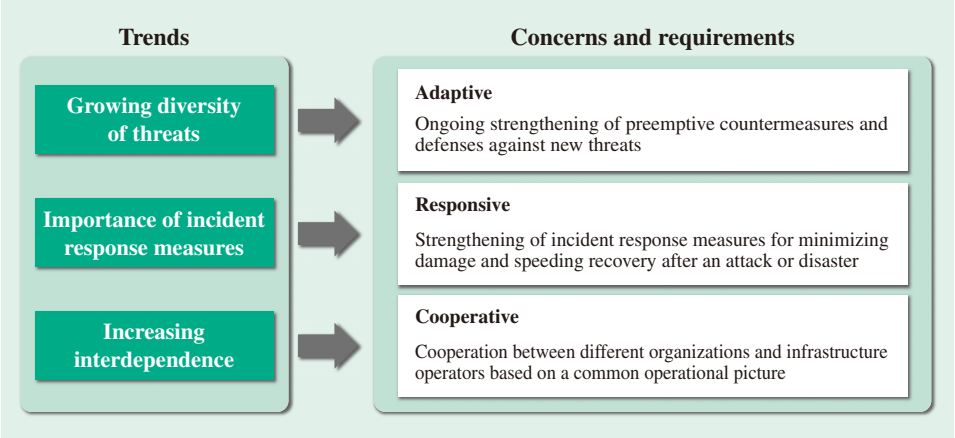


Fig. 3—Requirements for Social Infrastructure Security. Hitachi recognizes that social infrastructure security needs to be adaptive, responsive, and cooperative.

business continuity plans (BCPs). Based on the recognition that information security is not absolute and that accidents will happen, the standard contains guidelines for maintaining information services. Similarly, ISO 22320 (Societal security—Emergency management—Requirements for incident response) aims to improve emergency readiness by specifying the minimum requirements for implementing effective emergency measures.

Increasing Interdependence

As noted earlier, the way that social infrastructure services work in tandem with each other means that the social infrastructure can be thought of as a single enormous interlinked system. The current trend is toward the use of information technology (IT) to achieve ever tighter integration between different services with the aim of improving their convenience and efficiency. Examples include the sharing of track by different railway companies and supply chains that extend throughout the world. Each of these provides benefits such as greater convenience for consumers or productivity for businesses, and it is anticipated that future developments will provide social infrastructure with a high level of cross-industry interoperation, such as in smart cities. Along with the growing sophistication of multi-function services, this increasing interdependence between services also brings with it greater potential for the flow-on effects of attacks or disasters to cause damage in other areas. Examples include a railway accident in one place that interferes with all services that share the same line, or the way in which a localized natural disaster triggered a cascade of problems around the world that affected the cost of hard disk drives (HDDs) and the finished products that use them, as occurred after the 2011 floods in the Kingdom of Thailand[(2)].

REQUIREMENTS FOR SOCIAL INFRASTRUCTURE SECURITY

This section lists the requirements of social infrastructure security that follow from the factors (trends) discussed earlier in this article (see Fig. 3). Specifically, these requirements are that security measures be adaptive to allow the ongoing strengthening of preemptive countermeasures and other defenses against the increasing diversity of new threats, responsive enough both to minimize damage when attacks or disasters occur and to speed up the subsequent recovery process, and cooperative in the way that different organizations and operators work together to deal with attacks or disasters based on a common understanding of the situation. The following sections describe these requirements in more detail.

Adaptability

In broad terms, there are two ways of approaching the task of establishing ongoing countermeasures against the increasingly diverse threats posed by attacks or disasters.

The first is to add preemptive countermeasures to the system being defended each time a new threat is identified. This uses the plan, do, check, and act (PDCA) cycle, a widely used technique in security management. It is a way of dealing with the discovery of new threats through an ongoing process involving the identification of a new threat, determining how to counter it, planning how to implement countermeasures, and then proceeding with the implementation and assessment.

The second is to provide protection for each layer of the system being defended. Systems in general, not just social infrastructure systems, can be treated as being comprised of virtual (cyberspace), physical,

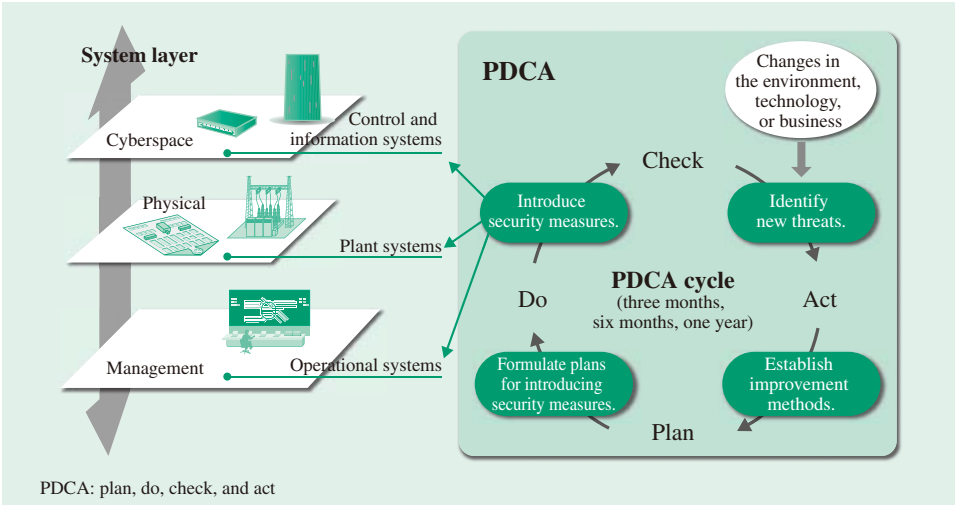


Fig. 4—Adaptability.
Use of the PDCA cycle in the virtual (cyberspace), physical, and management layers to make ongoing strengthening of preemptive countermeasures and defenses against new threats.

and management layers. To provide countermeasures against the different forms of attacks or disasters that affect social infrastructure systems, it is not necessarily enough to defend a single layer only. If the philosophy of defense in depth is to be adopted, measures should be provided at all three layers to defend against each form of attack of disaster.

In an environment in which new and diverse threats continue to emerge, the concept of adaptability means working through the PDCA cycle for each layer of the system to provide ongoing countermeasures (see Fig. 4).

Responsiveness

The growing importance of incident response measures means that, along with preemptive countermeasures with the adaptability to prevent attacks or disasters, as described above, the concept of responsiveness is also essential to minimize as far as possible the damage that occurs after an attack or disaster, and to speed the recovery. The following section describes a process, different to PDCA, that can be used to achieve this (see Fig. 5).

The first requirement is for the means to observe continuously what is happening in a system and its surrounding environment so as to detect any changes. Which aspects of the system to monitor depends on the application. In the case of cybersecurity, this might be to look for new vulnerabilities or virus infections. In the case of a disaster, examples might include monitoring for changes in the number of people at evacuation centers, or for the interruption or restoration of services such as electric power, gas, and water.

Once a change has been identified, the next requirement is orientation, meaning assessing the new situation to determine or predict the extent of damage. In the above examples, this might involve using information about the virus or other

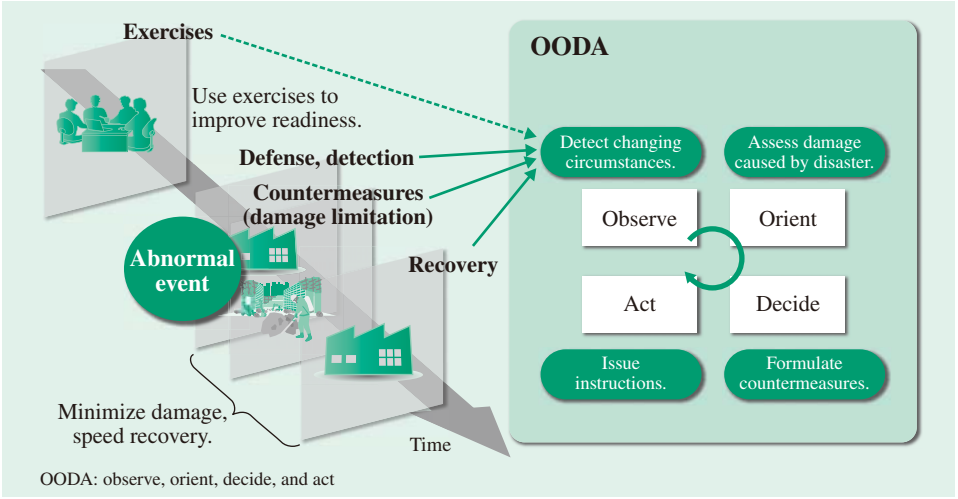
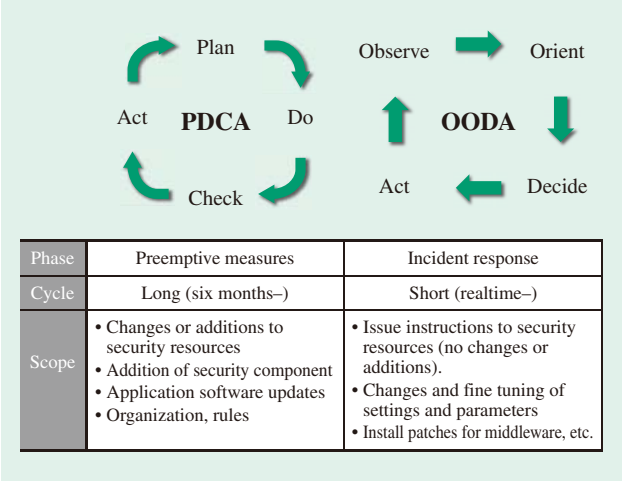


Fig. 5—Responsiveness.
This means strengthening incident response measures to minimize damage and speed recovery after an attack or disaster. It involves providing support for the OODA process for responding promptly to changing circumstances.



Phase	Preemptive measures	Incident response
Cycle	Long (six months–)	Short (realtime–)
Scope	• Changes or additions to security resources • Addition of security component • Application software updates • Organization, rules	• Issue instructions to security resources (no changes or additions). • Changes and fine tuning of settings and parameters • Install patches for middleware, etc.

Fig. 6—PDCA and OODA.
The PDCA cycle is a process for periodically reviewing and improving security measures. In contrast, the OODA loop is a process for minimizing damage by responding promptly when an attack occurs.

vulnerability to predict the potential for information to have been compromised (risk), or using information about service outages and the number of people at an evacuation center to predict whether the center is likely to suffer additional problems.

Utilizing information about damage and associated predictions, the next step is to decide what to do about it. Responses might include temporarily shutting down a system deemed at risk of information leaks, or the emergency distribution of drinking water or heaters. The final step is to act on the decision.

This sequence of steps was originally devised in the 1970s by the U.S. Air Force as a model for realtime decision making[3]. Around the year 2000, it was also studied as a process for command and control. Unlike the PDCA cycle for improving systems or operations by identifying problems and implementing system or operational countermeasures over a long timescale, this technique focuses on achieving the best response utilizing those system or operational resources that are immediately available.

Techniques such as PDCA that provide a systematic response over a long time period are too slow for improving incident response after an attack or disaster. Instead, what is needed is the responsiveness to minimize damage and facilitate a speedy recovery by working through the observe, orient, decide, and act (OODA) loop of monitoring and assessing the situation then deciding what to do and acting on the decision on a realtime or near-realtime timescale.

While this can be achieved by providing IT to support the tasks that make up the OODA loop, IT cannot replace all human activities. This applies particularly to the task of decision-making. Accordingly, achieving a high level of responsiveness requires that steps also be taken to speed up human activities. This should be able to be achieved by using exercises to improve people's readiness by allowing them to practice working through the OODA loop under simulated conditions.

Fig. 6 shows the differences between PDCA and OODA.

Cooperativeness

While the growing interdependence of social infrastructure systems is providing greater convenience, there are concerns that damage in a particular sub-system caused by an attack or disaster will have an impact on other sub-systems, resulting in more extensive damage throughout the social infrastructure. What is needed to deal with this is to

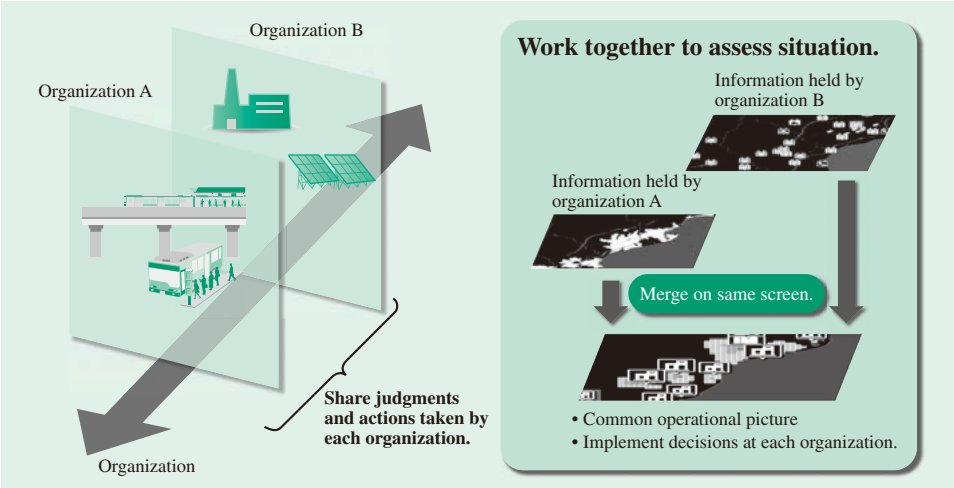


Fig. 7—Cooperativeness.
Cooperativeness allows coordinated measures to be implemented by sharing information among different organizations or infrastructure operators and presenting it from different perspectives.

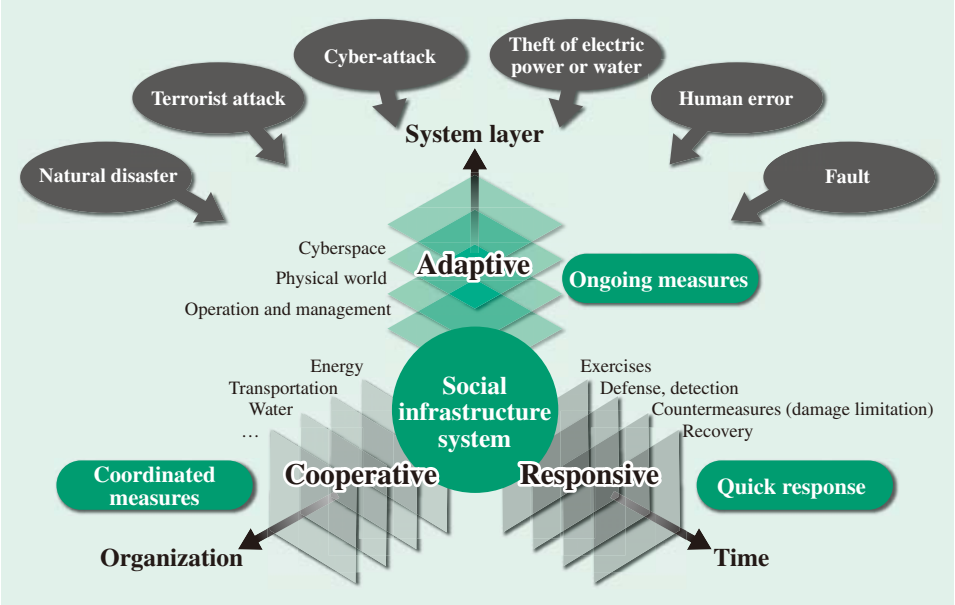
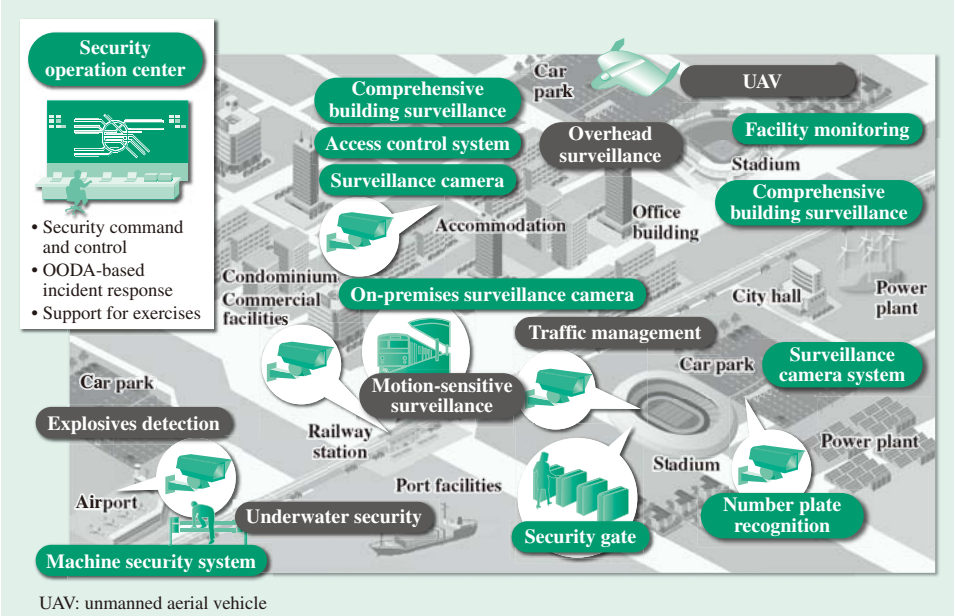


Fig. 8—Hitachi's Concept for Social Infrastructure Security. The security of social infrastructure is achieved through measures taken with respect to the system layer, time, and organization.

apply the concept of cooperativeness to the orient and decide steps of the OODA loop described above by having the different sub-systems (meaning different organizations or infrastructure operators) establish an accurate assessment of each other's situations (see Fig. 7). This in turn requires the standardization of the meaning of terminology used to indicate the situation at each organization, mechanisms for exchanging machine-readable information, and the centralized presentation and management of information from different organizations. This is what the defense sector calls a "common operational picture" (COP), and is recognized as a key function of command and control[4].

HITACHI'S CONCEPT FOR SOCIAL INFRASTRUCTURE SECURITY

This article has already described the need for social infrastructure security to be adaptive, responsive, and cooperative. Hitachi has combined these to develop a concept for future social infrastructure security based on three trends that are influencing social infrastructure (the growing diversity of threats, the importance of incident response measures, and increasing interdependence) (see Fig. 8). It also categorizes the concepts by their countermeasures or other responses in terms of their system layer, time, and organization.



UAV: unmanned aerial vehicle

Fig. 9—Citywide Solution for Safety and Security. The solution provides border security checks for the aircraft, ships, vehicles, and people that enter a city.

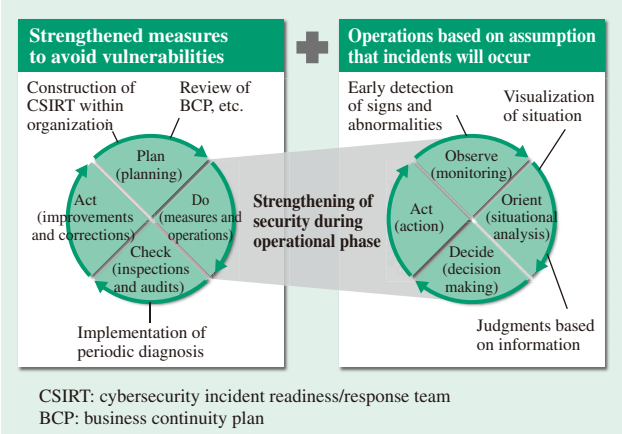


Fig. 10—Managed Security Service Concept.
These services use the PDCA cycle and OODA loop to provide more effective and faster-acting security measures for cyberspace.

Social infrastructure systems are expected to have a high level of availability, not only during routine operation but also by providing the minimum level of services needed during an emergency, a fact that leaves them open to a very wide variety of threats. Widespread measures are needed to protect social infrastructure systems from these threats. Hitachi sees its combined concept that focuses on security measures being adaptive, responsive, and cooperative as providing a context in which to investigate measures for social infrastructure security.

SECURITY PRODUCTS, SOLUTIONS, AND SERVICES

Hitachi also offers solutions based on its social infrastructure security concept that include security products for physical and cyberspace.

For physical security, Hitachi supplies citywide safety and security solutions that conduct border security checks on the aircraft, ships, vehicles, and people that enter a city (see Fig. 9). Specific examples include airport and railway station security solutions that monitor the behavior of suspicious individuals at facilities such as these, and marine defense solutions that detect, identify, and classify shipping. These solutions provide the adaptability to allow various different layers of preemptive countermeasures.

Managed security services that combine responsiveness with adaptability are commonplace in the field of cybersecurity (see Fig. 10). In addition to strengthening countermeasures to eliminate vulnerabilities by working through the PDCA cycle of establishing or reviewing CSIRTs[(a)] (plan),

(a) CSIRT
Cybersecurity incident readiness/response team. A team responsible for responding to information security incidents at a company or other organization.

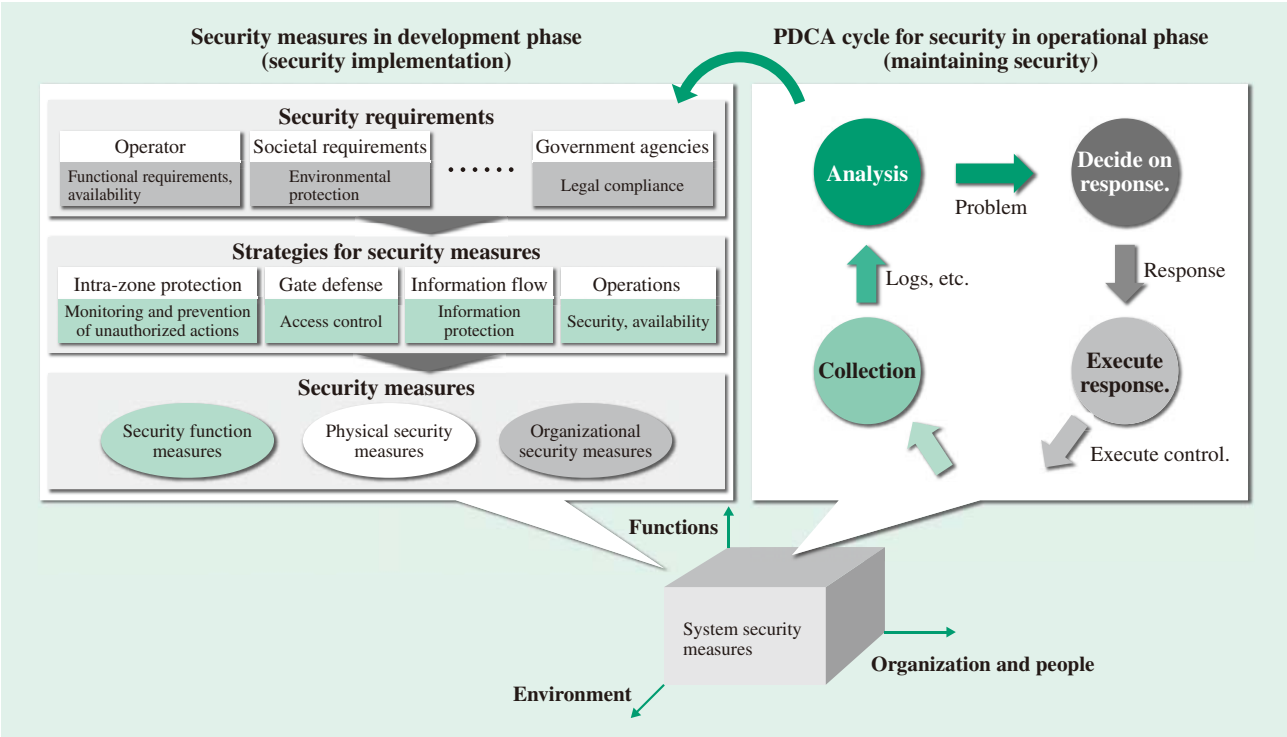


Fig. 11—2 × 3 Security Implementation Model.
The model seeks to ensure the security of social infrastructure systems across their entire lifecycle by assessing security during two phases and in terms of three different criteria.

implementing countermeasures and operations (do), conducting inspections and audits (check), and making improvements or revisions (act), these services also utilize the OODA loop concept of observation, orientation, decision, and action to ensure prompt and sensible decision-making and policies. This results in more effective and faster-acting security measures.

For control system security, IEC 62443(b) provides indices for assessing system robustness in terms of how they be adaptive, responsive, and cooperative, stipulating the requirements and associated measures for satisfying these indices at the control system and control component layers respectively. Based on the 2 × 3 security implementation model for ensuring the security of social infrastructure systems across their entire lifecycle, this involves ensuring that security measures with the required security level and adaptability are incorporated during the development phase, and using the security PDCA cycle to satisfy the responsiveness and cooperativeness requirements in the operational phase (see Fig. 11).

(b) IEC 62443
A series of international standards for control system security. While industry-specific standards have also been formulated for control system security, there is a growing trend toward consolidating these under the generic IEC 62443 series of standards.

MAKING SOCIAL INFRASTRUCTURE EVEN SAFER AND MORE SECURE

This article has described Hitachi's concept for social infrastructure security requirements together with solutions for implementing the concept on control systems and in the physical and virtual (cyberspace) worlds.

In the future, Hitachi intends to continue contributing to making social infrastructure systems safer and more secure by supplying products, solutions, and services based on this concept.

REFERENCES

(1) H. Nishimura, "Damage due to Hurricane Katrina," Technical Report of The Institute of Electronics, Information and Communication Engineers 106, 220, pp. 13–16 (2006) in Japanese.
(2) M. Shimizu, "Effects of Flooding in Thailand on HDD Supply Chain," Future SIGHT, No. 55, pp. 32–36 (2012) in Japanese.
(3) T. Grant, "Unifying Planning and Control Using an OODA-based Architecture," Proceedings of SAICSIT (2005).
(4) H. Minners, "Conceptual Linking of FCS C4ISR Systems Performance to Information Quality and Force Effectiveness Using the CASTFOREM High Resolution Combat Model," WSC 2006 (2006).

ABOUT THE AUTHORS

Masahiro Mimura, Ph.D.
Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of solutions, security, and productivity technology for corporate information systems. Dr. Mimura is a member of the Information Processing Society of Japan (IPSJ).

Toshiaki Arai, Ph.D.
Defense Systems Company, Hitachi, Ltd. He is currently engaged in the management of technology at the Defense Systems Company in his role as CTO.

Toshihiko Nakano, Ph.D.
Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Ryuichi Hattori
Business Planning Department & Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in the planning of service businesses, primarily dealing with security.

Atsutoshi Sato
Brand Promotion Unit, Information Design Department, Design Division, Hitachi, Ltd. He is currently engaged in design work for social infrastructure systems and smart city projects.

Featured Articles

Citywide Safety and Security Solutions

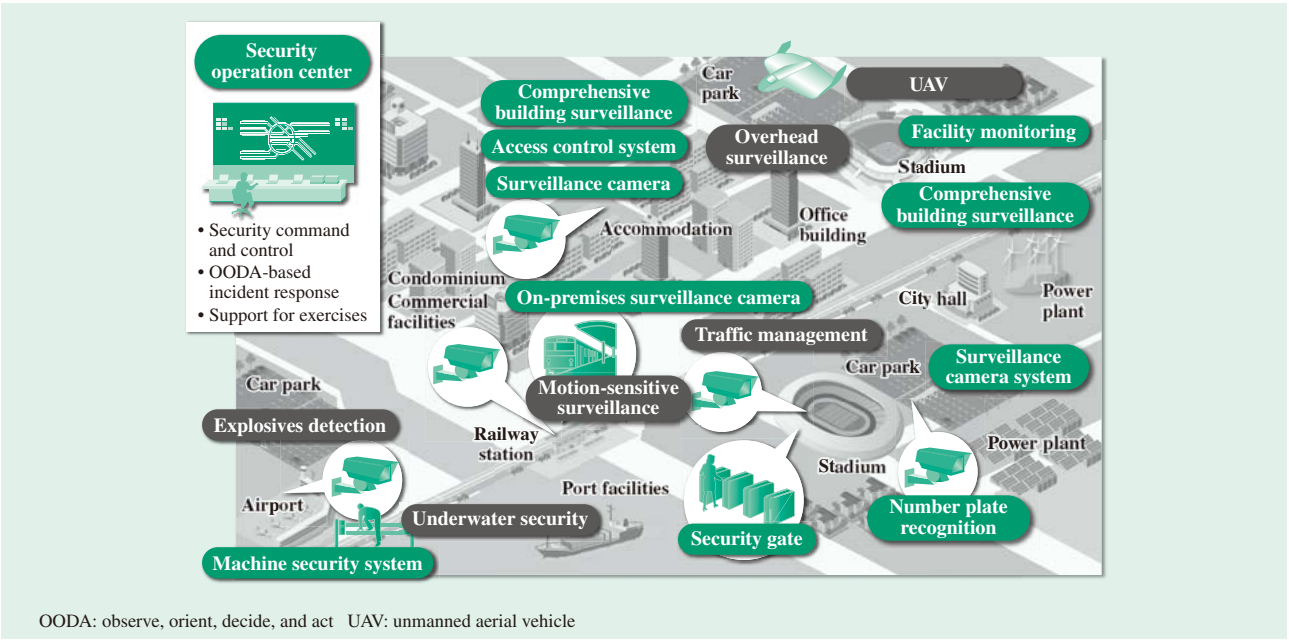
Ikuhiro Ono
Futoshi Sagami
Kenji Nakamoto

OVERVIEW: To provide people with a convenient and comfortable way of life, the social infrastructure systems that support the functions of a city have become increasingly advanced and complex, forming an enormous interdependent system. Meanwhile, threats such as natural disasters, epidemics, crime, and cyberterrorism that have the potential to impact on the reliable operation of these social infrastructure systems continue to grow, placing greater demands on social infrastructure security to protect people's safety and security. Hitachi has been drawing on its know-how in defense and social infrastructure security systems, and on its experience with their implementation, to consider what form the social infrastructure security systems of the future should take. From this base, Hitachi is contributing to the provision of social infrastructure that is even safer and more secure.

INTRODUCTION

CITIES provide an environment in which complex systems such as those used at energy facilities or by transportation agencies or financial institutions can work together in sophisticated ways to facilitate a comfortable and convenient way of life. Meanwhile, natural disasters like the Great East Japan Earthquake of 2011, the 9/11 terrorist attacks in the USA in 2001, the severe acute respiratory syndrome (SARS) outbreak in China in 2003, and the increased risk in recent years of cyber-attacks on important infrastructure have raised concerns about the potential for events like these to have a major impact[1].

Whereas facilities have in the past tended to implement their own independent security measures, it is now recognized that the future will require system concepts that take account of the entire system. The



OODA: observe, orient, decide, and act UAV: unmanned aerial vehicle

Fig. 1—Overview of Social Infrastructure Security.
Security measures are needed to protect people's safety and security from an increasing number of threats in a variety of forms in cities where complex systems work together in sophisticated ways.

fear of terrorist acts staged to draw international attention to the ideals of their perpetrators mean that large national events in particular require countermeasures against such threats[2].

This article provides an overview of how Hitachi's concept for social infrastructure security that focuses on security measures being adaptive, responsive, and cooperative works in practice, and describes security solutions that implement this concept (see Fig. 1).

HOW HITACHI'S SOCIAL INFRASTRUCTURE SECURITY CONCEPT WORKS IN PRACTICE

This section describes the new value added when the concept is applied to social infrastructure systems, giving an overview of how this works in practice.

Having identified the growing diversity of threats, the importance of incident response measures, and increasing interdependence as three trends influencing the field of social infrastructure security, Hitachi has adopted a concept for social infrastructure security that focuses on the need for future security measures to be adaptive, responsive, and cooperative.

By also incorporating the observe, orient, decide, and act (OODA) loop concept, this concept goes beyond the existing practice of business continuity planning (BCP) for maintaining operations during an emergency to establish business continuity management (BCM) in which the response to an incident can adapt to actual circumstances. Along with improving the efficiency of existing activities under non-emergency conditions, it also enables the provision of new services through the coordination of systems and organizations (see Fig. 2).

The following presents an overview of a system that incorporates this concept.

To ensure cooperation between organizations, the system acts as a common platform for security services such as operational management, identification (ID) management, and providing a common operational picture (COP) to allow greater coordination of social infrastructure system applications. Responsiveness is achieved by deciding on incident response measures that work through the OODA loop to minimize damage when an incident occurs in a social infrastructure system. These practices can also be used to decide whether an incident is limited to certain systems only, or whether it is interrelated.

By applying this structure to both physical security and cybersecurity, it is possible to build an integrated system that extends beyond the physical and virtual (cyberspace) realms (see Fig. 3).

SOLUTIONS BASED ON HITACHI CONCEPT

This section describes urban security solutions that implement the concepts described above. Other articles describe solutions for other forms of security, including cyber and control system security.

Cities have typically developed transportation systems that link them to the outside world, and it is more efficient for them to perform border security checks on the aircraft, ships, vehicles, and people that enter the city. The following sections describe solutions from this vantage point.

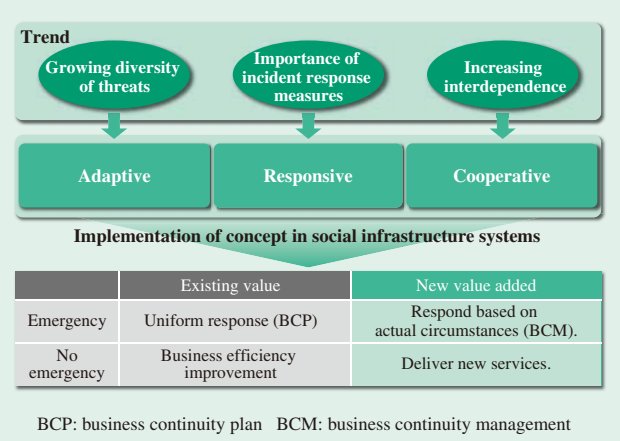


Fig. 2—New Value Added by Implementation of Hitachi's Concept.
Hitachi's concept for social infrastructure security that focuses on security measures being adaptive, responsive, and cooperative can add new value both during an emergency and at other times.

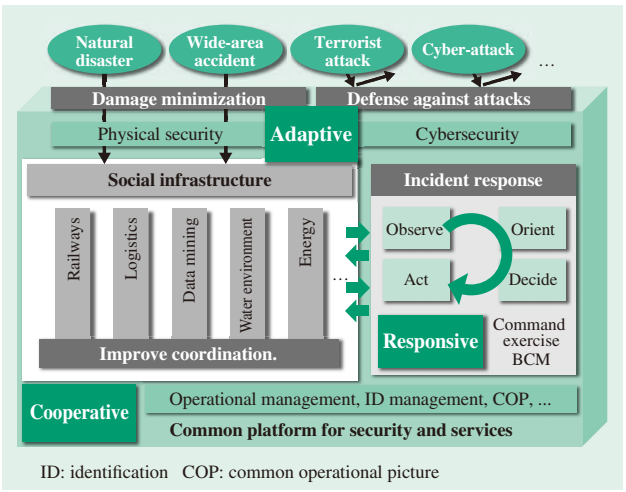


Fig. 3—System Outline.
The diagram shows an example system that implements Hitachi's social infrastructure security concept.

Total Security Solution for Airports

There has been a notable improvement in service at airports in recent years thanks to a reduction in the time required for passengers to check in and board.

Although airport security has been considerably strengthened since the 9/11 terrorist attacks in the USA in September 2001, terrorist attacks on transportation and other targets around the world continue unabated, with examples including the London bombings in July 2005, the attempted car bombings and terrorist attacks on airport facilities in the UK in June 2007, and the bombing at Domodedovo Airport in 2011.

Airports are divided into zones that include both public areas where large numbers of people congregate and restricted areas where only authorized personnel are permitted. Together with their operational collaboration with police, fire, and other agencies, airport companies also need to manage shopping and other areas inside terminal buildings where people congregate, ensure boarding procedures operate smoothly, and deal with more sophisticated and ferocious criminal activity. That is, an important requirement for airports is that they can quickly identify and track criminals or other suspicious individuals while also keeping nearby passengers and airport staff safe without imposing an overbearing security presence.

To maintain the safety and security of airports, Hitachi is progressively introducing services in the form of large-scale monitoring solutions for total security that combine imaging solutions for efficient image searching and tracking with other solutions such as those that predict the behavior patterns of criminals (see Fig. 4).

Marine Defense Solution

The importation of drugs, guns, and other contraband from overseas is believed to have played a part in violent crime in Japan over recent years. There are also fears that international terrorist organizations are engaged in activities such as using ships to launch attacks on land-based sites or other vessels, the illegal importation of arms or materials used for weapons of mass destruction, and the smuggling of terrorists across borders.

In the “1974 International Convention for the Safety of Life at Sea (SOLAS 74)” document that became effective in July 2002, Japan established a requirement that an automatic identification system (AIS) be fitted to, (1) All vessels of 300 t gross or more that ply international waters, (2) All passenger vessels that ply international waters, and (3) All vessels of 500 t gross or more, regardless of whether they ply international waters. Because AIS automatically sends and receives vessel information, including the vessel’s

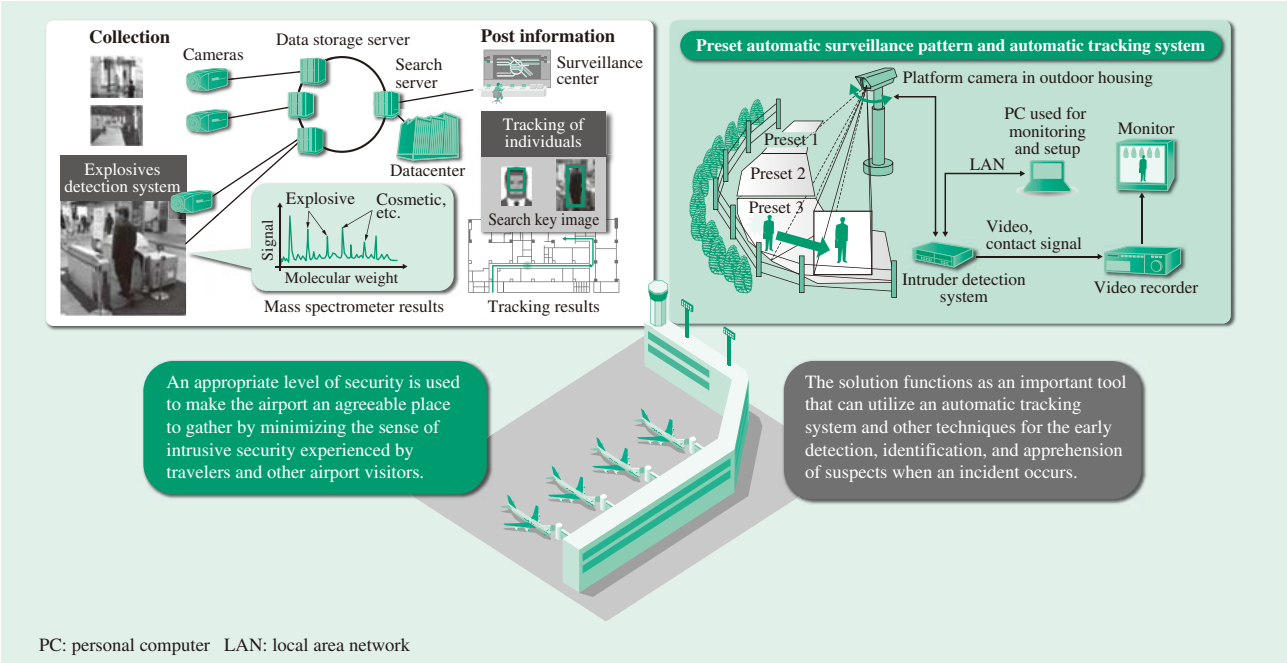


Fig. 4—Total Security Solution for Airports.
The solution is an important tool that can provide an appropriate level of security during normal times without imposing an overbearing security presence, while also being able to utilize an automatic tracking system and other techniques for the early detection, identification, and apprehension of suspects in the event of an emergency.

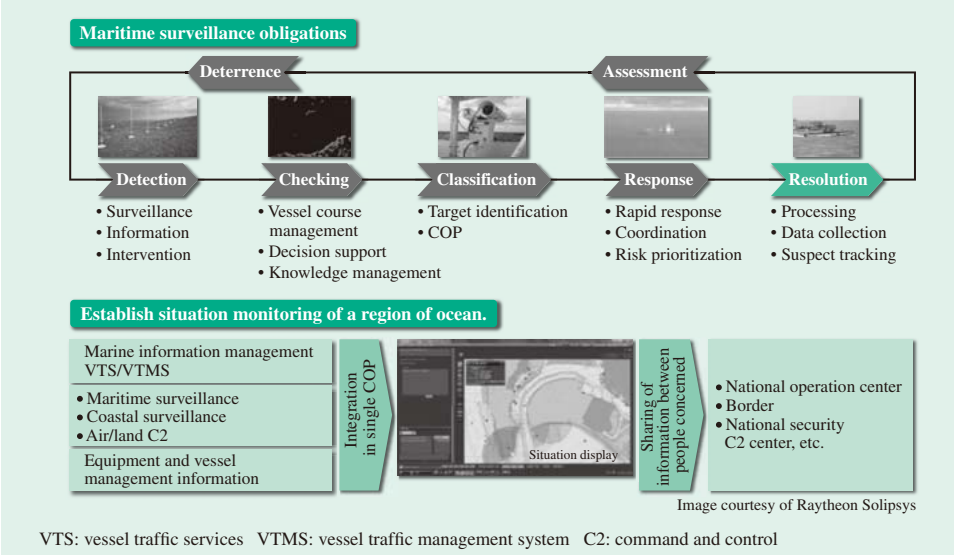


Fig. 5—Marine Defense Solution.
The solution supports marine defense by establishing situation monitoring of a region of ocean.

identification code, type, location, course, speed, progress, and other safety information, it allows shore-based agencies to keep track of vessel movements[5].

The issues with AIS, however, include the existence of small vessels that are not required to fit it and the fact that AIS information cannot be used to keep track of those vessels that are obliged to install it because sailors can disable it deliberately, this being permitted to allow large working fishing vessels to keep the location of fishing grounds secret[6].

Hitachi's marine defense solution is a total system that supports all aspects of marine surveillance from the detection of vessels through to identification, classification, response, and resolution. For the detection, identification, and classification phase, the solution can collect vessel traffic services (VTS) and AIS information and correlate it with other sensor data, including that from coastal radar and specific absorption rate (SAR) information from aircraft, to identify ships or other vessels and provide a highly accurate situation assessment. By installing radar and cameras on small boats, it can also track and monitor suspicious craft outside areas covered by radar. This information can then be shared by displaying it all together in a single COP. The solution also provides functions for using chat and whiteboards to prioritize risks or coordinate responses in the response and resolution phase (see Fig. 5).

Underwater Security Solution

Airports, power plants, oil storage facilities, and other important infrastructure are located along the coast of Japan, making it very important that these facilities have adequate security against underwater threats.

Because electromagnetic radiation, including both visible light and radio waves, attenuates rapidly in seawater, sonar security systems that work acoustically are the best way to detect underwater intrusions. Hitachi has reduced the installation cost by combining both passive sonar for long-range tracking and imaging sonar for short-range targeting, seeing this as also providing an effective system configuration in security terms.

Between FY2005 and FY2007, Hitachi participated in research into underwater security sonar systems by the Underwater Technology Research Center, Institute of Industrial Science at The University of Tokyo. The three-year research program demonstrated through sea trials that the system they had developed was suitable in practice for underwater intrusion monitoring (see Fig. 6).

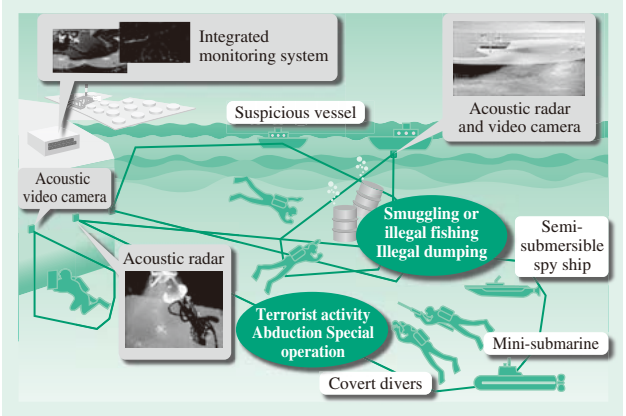


Fig. 6—Concept of Operation of Underwater Security Sonar System.
The diagram shows the concept of operation of the underwater security sonar system.

Railway Station Security Solution

An incident in May 2012 in which a man was seriously injured by a knife attack at Shibuya Station on the Fukutoshin Line of Tokyo Metro Co., Ltd. was resolved by the arrest of the assailant some days later by the Metropolitan Police Department, who had treated the case as one of attempted murder. Crucial to the arrest was video footage from the surveillance cameras installed at Tokyo Metro stations and security cameras installed in the streets around Shibuya Station.

While the installation of surveillance cameras at stations for crime prevention is ongoing, there is a need to take their deterrent effect a step further. That is, to integrate them into security systems. The use of high-speed image processing to keep nearby people safe by preemptively detecting and tracking suspicious individuals will be among the roles of future security systems. Given that large numbers of passengers packed onto the limited platform space is one of the features of railways in Japan, security systems that impede mass transit are impractical. What are feasible, however, are measures such as the use of surveillance video technology and sensing to provide warning of threats to passengers and station staff (see Fig. 7).

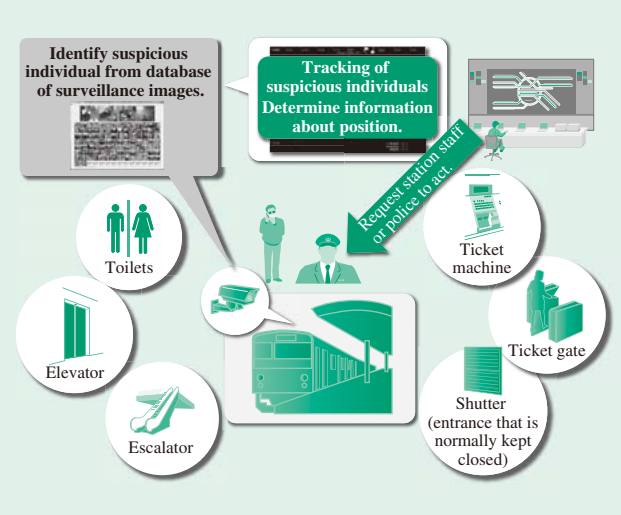


Fig. 7—Railway Station Security Solution.
Suspicious individuals can be detected and tracked using surveillance video technology and sensing.

Facility Security Solution

Facility security is used at facilities with a wide diversity of layouts and people present, including event halls, large retail premises, office buildings, factories, research institutions, datacenters, condominiums, and elderly care facilities. Likewise, the investigation and implementation of security depends on the type of facility, including both locations that are open to the public and locations used only by specific people.

The Great East Japan Earthquake reinforced to local government in Japan, businesses, and other organizations the importance of confirming people's safety when an emergency occurs.

Progress has been made on integration with security systems to make further advances in this field. This involves combining the confirmation of people's safety with access control systems to allow the rapid confirmation of who is present at a factory or other facility. This combination is recognized as being beneficial for confirming people's safety when a fire or other incident occurs at a factory, regardless of the scale.

Hitachi has experience in the building and installation of locally managed systems for large buildings, datacenters, and other facilities. Hitachi also supplies solutions through the public cloud for premises such as condominiums, small offices, or elderly care facilities that are operated by businesses that cannot afford a large investment. The benefits of using the public cloud can include minimizing the investment required by users of such facilities, cutting the cost of administration, and making operation more efficient. For example, the 24-hour, 365-day provision and management of common-use equipment or smartcard-based access to condominiums is difficult to achieve without relying on an administration office that operates both day and night. It can be provided at low cost, however, by utilizing Hitachi's public cloud and support infrastructure. The public cloud has also attracted attention from people with an interest in this area for its ability to perform low-cost operating system upgrades by treating the public cloud itself as a management service.

In a future initiative, Hitachi aims to achieve even greater efficiency than in the past while still maintaining a high level of security through the centralized management of areas of a certain scale, such as business districts or building complexes, rather than individual large buildings or condominiums, using the public or private cloud depending on the location. This is an even more advanced form of the "area management" being promoted by the Ministry of Land, Infrastructure, Transport and Tourism, and involves managing everything centrally through a private cloud or public cloud, including not only security management but also the efficient use of energy[7].

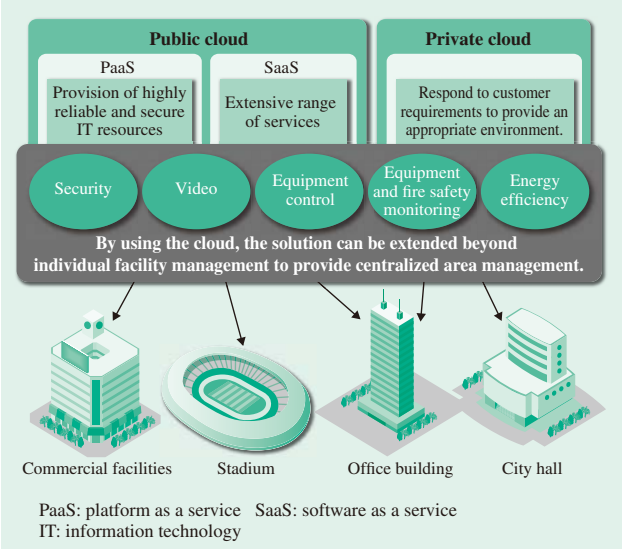


Fig. 8—Facility Security Solution.
By using the cloud, the scope of the solution can be extended beyond individual facilities to provide centralized area management.

Among the future possibilities for this initiative is the use of big data, something that is difficult to achieve under conventional configurations, by performing area management on a private cloud that allows centralized management of information. It is anticipated that this could be used for a new type of security measure that records people who are involved in incidents in the area so that, should these people enter the area again, administrators can be informed and a trace placed on the people concerned, and the implementation of management practices for identifying potential incidents before they occur and taking preventative steps (see Fig. 8).

CONCLUSIONS

This article has provided an overview of how Hitachi's concept for social infrastructure security works in practice, and described security solutions that implement this concept.

Hitachi believes that the solutions described here can contribute to making society safer and more secure.

REFERENCES

(1) Information-technology Promotion Agency, Japan, "Report on Analysis of Specific Targeted Cyber-attacks and their Countermeasures," (Jan. 2012), https://www.ipa.go.jp/files/000024536.pdf in Japanese.
(2) The Tokyo Organising Committee of the Olympic and Paralympic Games, "Candidature File, Theme 11 Games Safety, Security and Medical Services."
(3) Water Supply Division, Health Service Bureau, Ministry of Health, Labour and Welfare, "Information Security Guidelines for Water Industry (Revised Version)," http://www.mhlw.go.jp/topics/bukyoku/kenkou/suido/houkoku/dl/guideline.pdf in Japanese.
(4) Japanese Industrial Standards JIS Q 22320, "Societal Security—Emergency Management—Requirements for Incident Response" (2013) in Japanese.
(5) Japan Coast Guard, "Navigation Support System Utilizing AIS," http://www.kaiho.mlit.go.jp/syoukai/soshiki/toudai/ais/ais_index.htm in Japanese.
(6) The Japan Association of Marine Safety, "Role of AIS in Safe Vessel Operation," Sea and Safety, No. 545 (2010), http://nikkaibo.or.jp/pdf/545_2010.pdf in Japanese.
(7) Ministry of Land, Infrastructure, Transport and Tourism, "Support Information for Area Management," http://tochi.mlit.go.jp/tocsei/areamanagement/web_contents/shien/index_01.html in Japanese.

ABOUT THE AUTHORS

Ikuhiro Ono
Business Development Center, Business Advancement Division, Defense Systems Company, Hitachi, Ltd. He is currently engaged in system commercialization in the crisis management and disaster prevention fields.

Futoshi Sagami
Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the security system integration business.

Kenji Nakamoto
Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the security system integration business.

Featured Articles

Disaster Prevention and Response Support Solutions

Junji Ogasawara
Koichi Tanimoto
Osamu Imaichi, Dr. Eng.
Masayoshi Yoshimoto

OVERVIEW: With national and regional agencies updating their plans for dealing with large, wide-area disasters based on the lessons from the Great East Japan Earthquake, there is also growing demand for the systems that support disaster prevention and response to incorporate countermeasures against such major disasters. In the case of large, wide-area disasters, realtime and ongoing decision making is a particular challenge because circumstances are continually changing. Hitachi is developing disaster prevention and response support solutions that incorporate operational concepts for emergency situations. To overcome the problem of delayed decision making during a large, wide-area disaster due to gaps in available information, Hitachi is also proposing a rapid situation assessment system that utilizes information from SNSs and other sources to help quickly collect information and determine what is happening.

INTRODUCTION

TAKING note of the lessons from the severe damage that resulted from disasters such as the Great Hanshin Awaji Earthquake in 1995 and the Niigata-ken-Chuetsu Earthquake in 2004, ongoing work is being done to establish organizations and schemes and provide facilities and systems for damage limitation in Japan. Following the Great East Japan Earthquake in March 2011, it is anticipated that further nationwide measures for mitigating disasters will be undertaken in parallel with ongoing recovery and reconstruction in the affected regions. In particular, there is an urgent need to adopt measures for dealing with events such as a Nankai Trough Earthquake or an earthquake directly under Tokyo, both of which have been predicted, and revisions are being made to plans for dealing with large, wide-area disasters under the leadership of the Central Disaster Prevention Council[(1)] of the Japanese Government. As a consequence, there is growing demand for incorporating countermeasures against large, wide-area disasters into the disaster prevention systems that support the response to a disaster.

This article describes the disaster prevention and response support solutions being developed by Hitachi, and also a rapid situation assessment system that utilizes information from social networking services (SNSs) and other sources immediately after the disaster strikes to help quickly collect information and determine what is happening. This proposed system is intended as a way of overcoming the problem of ensuring realtime and ongoing decision making during a large, wide-area disaster in which circumstances are continually changing.

DISASTER PREVENTION AND RESPONSE SUPPORT SOLUTIONS

Concept

During a disaster, response activities must operate in a constantly changing environment. In particular, mounting a rapid and accurate response is difficult if the disaster has caused large amounts of damage over a wide area with numerous unforeseen events.

For this reason, the disaster prevention and response support solutions are based on the concept of implementing the observe, orient, decide, and act (OODA) loop, a decision making methodology from the defense sector that was devised by U.S. Air Force Colonel John Boyd based on insights from aerial combat. It achieves fast and accurate decision making by performing a repeated cycle of observation, orientation, decision, and action. It differs from the conventional plan, do, check, and act (PDCA) cycle in that monitoring and situation assessment are ongoing at all steps in the cycle to allow a flexible response to a continually changing situation.

The disaster prevention and response support solutions aim to provide services that implement a continuous OODA loop from the time the disaster strikes until recovery is achieved (see Fig. 1).

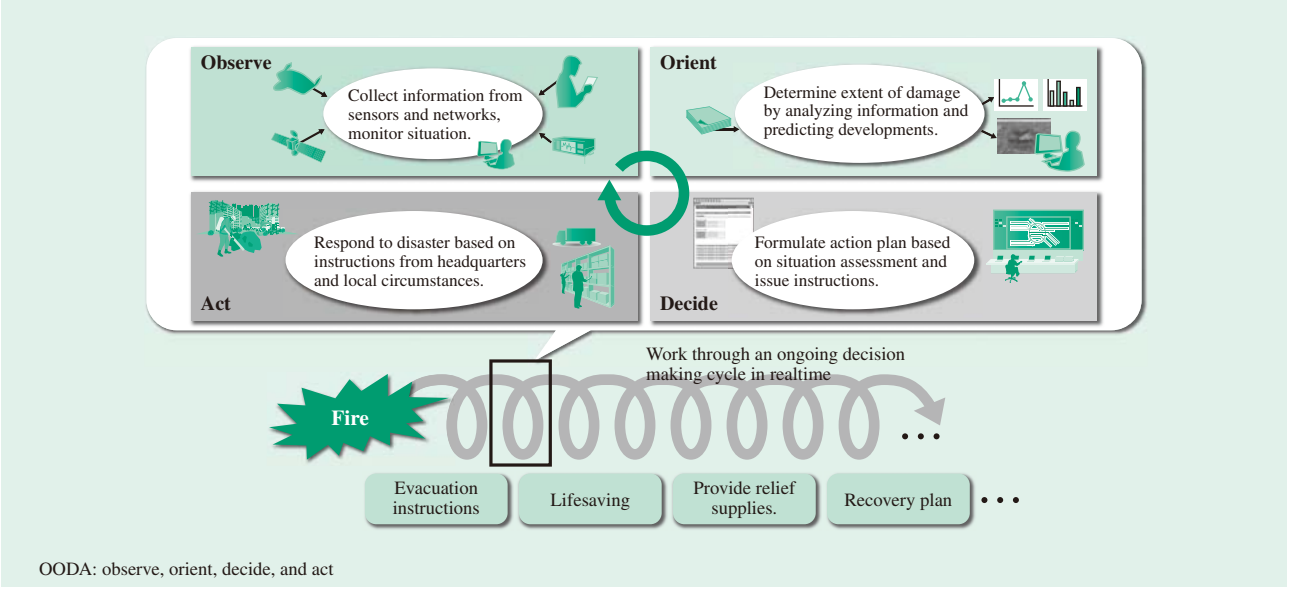


Fig. 1—OODA Loop for Disaster Response.
The OODA loop achieves fast and accurate decision making by performing a repeated cycle of observation, orientation, decision, and action.

Overview of Disaster Prevention and Response Support Solutions

Fig. 2 shows an overview of the disaster prevention and response support solutions.

Based on the OODA loop described above, Hitachi provides the following solutions that assist with working through the OODA cycle quickly and accurately during a large, widearea disaster.

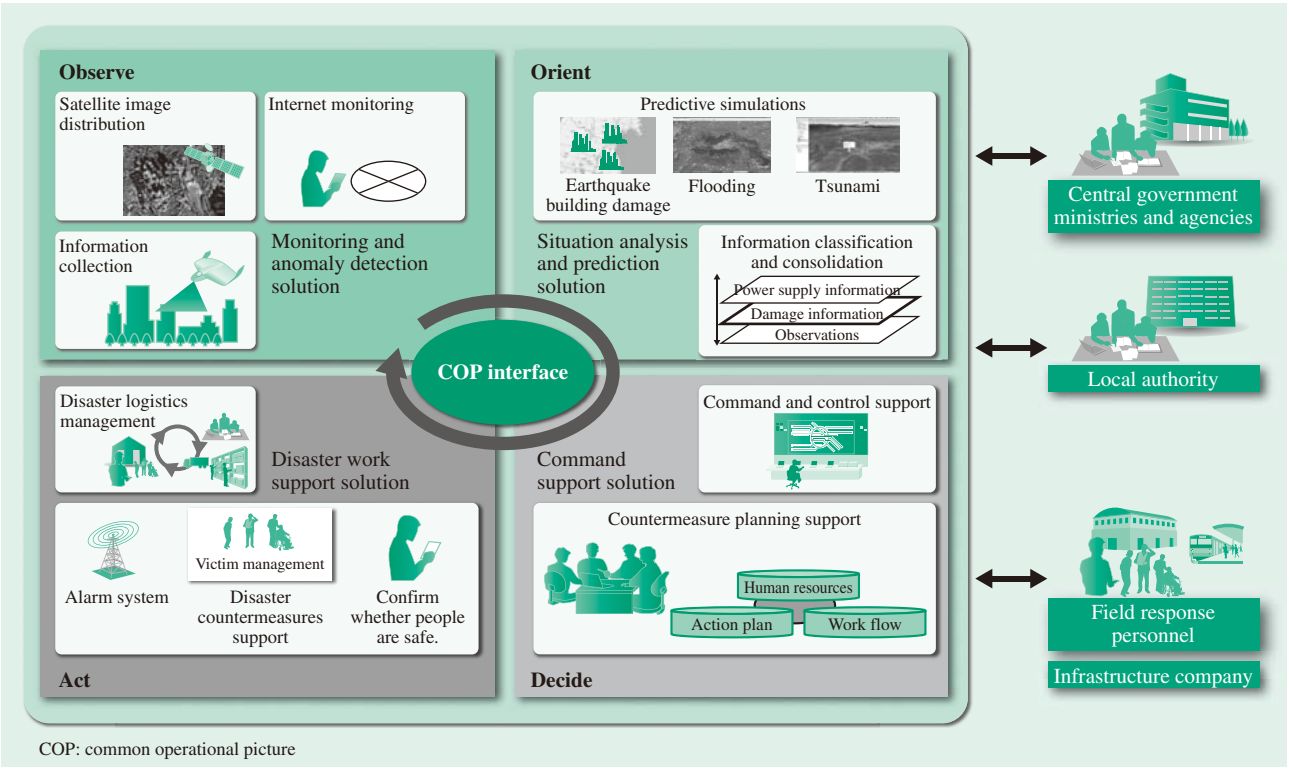


Fig. 2—Disaster Prevention and Response Support Solution.
The monitoring and anomaly detection, situation analysis and prediction, command support, and disaster work support solutions help implement the OODA loop to support fast and accurate decision making during a disaster.

(1) Monitoring and anomaly detection solution

This solution collects information from sources such as seismometers, river level gauges, surveillance cameras, unmanned aerial vehicles, satellites, and Internet SNSs, and integrates it on a geographic information system (GIS) to detect anomalies by assessing the situation and identifying what has changed.

(2) Situation analysis and prediction solution

This solution provides functions for collating and classifying the information collected by the monitoring and anomaly detection solution and other systems, thereby enhancing its value as intelligence for use in situation analysis and prediction (see Fig. 3). The solution also uses simulation techniques for earthquake building damage, flooding, tsunamis, or the movement of people to conduct risk simulations and provide information to help determine the current situation and assess changing circumstances and possible future developments.

The solution classifies and collates information from sensors such as river level gauges to calculate the rise in river levels, and incorporates information about upcoming weather conditions to perform flooding simulations. This can be used to generate intelligence, such as warning that a particular district is at risk of a levee breach in an hour's time, for example. Intelligence like this facilitates fast and accurate decision making on evacuation alerts.

(3) Command support solution

This solution supports effective and efficient command and control for relief and recovery. For example, it provides the disaster response headquarters with a map of the disaster situation that they can refer to as they assign people, organizations, goods, and other resources in accordance with the evolving situation on the ground. This solution builds a database from which the data required for the tasks associated with the event and their execution can be accessed quickly based on an event model of the time when the disaster strikes, a disaster response model (work flow), a data model that specifies the relationships between data, and a disaster management model that links these other models together. This allows the "push" delivery of information based on users' circumstances and responsibilities (see Fig. 4). For the people or organizations assigned the task of distributing relief supplies, for example, the solution supplies the information needed to complete this task, namely the information associated with the distribution of relief supplies (road damage status, where to distribute supplies, recommended routes, and so on).

(4) Disaster work support solution

This solution provides functions for managing the activities of local authorities (confirming the safety of staff, evacuation site management, issuing victim certificates, and so on) as well as requests for relief

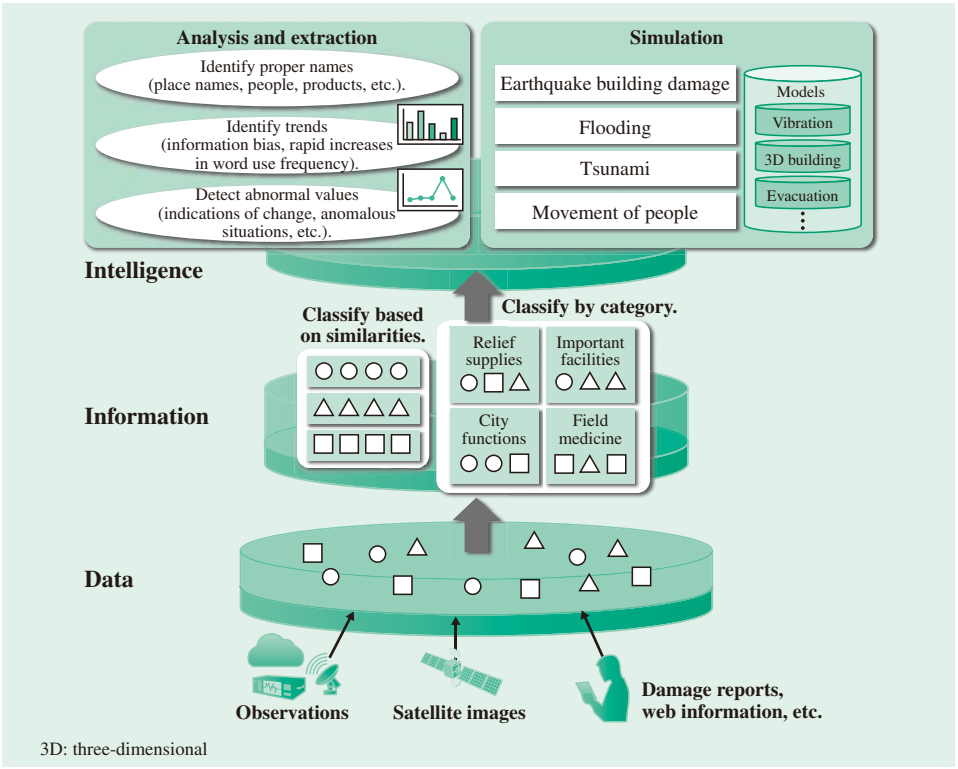


Fig. 3—Situation Analysis and Prediction Solution.
The solution categorizes and collates data and uses trend analysis, simulation, and other techniques to supply information that is useful for fast and accurate decision making.

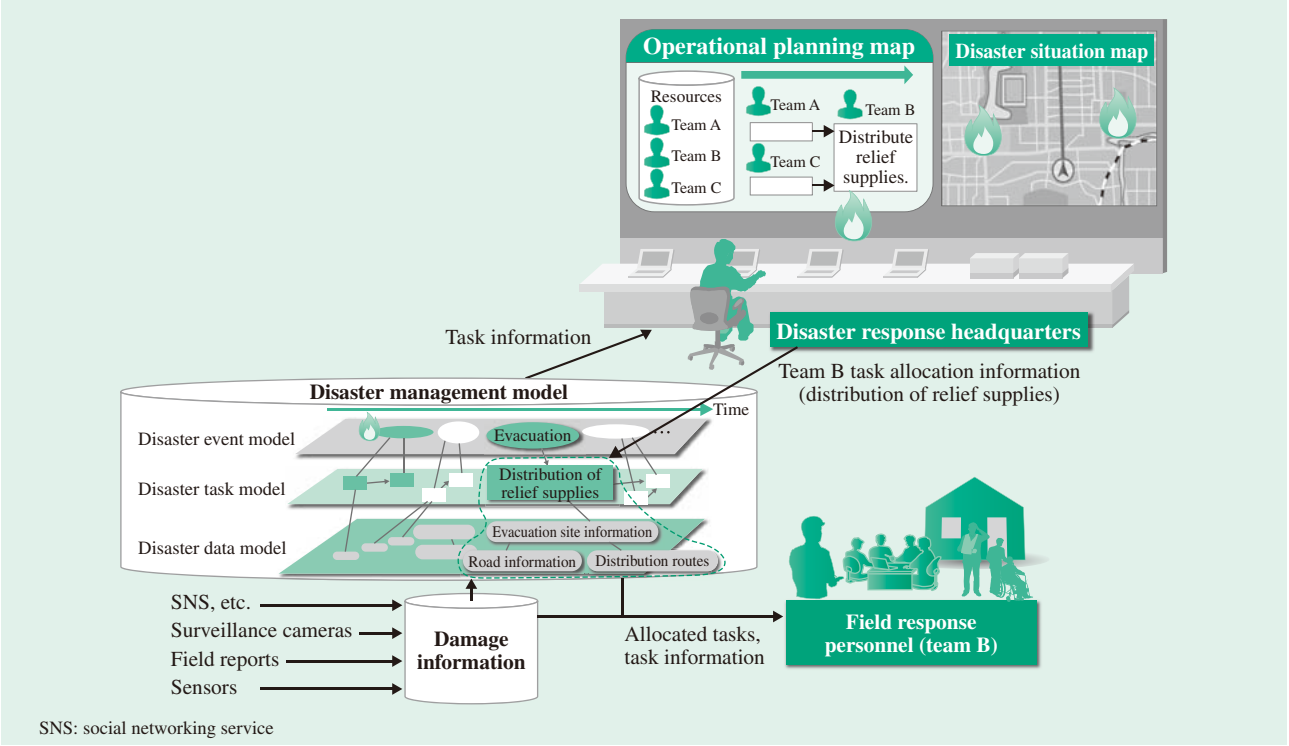


Fig. 4—Command Support Solution.
This solution is used to prepare an activity plan and support the assignment of personnel, organizations, goods, and other resources. When a task is assigned to a person or organization, the information required to complete that task is extracted from the database and supplied to the person or organization using "push" style delivery.

supplies, stock control, dispatch instructions, and other aspects of logistics.

RAPID SITUATION ASSESSMENT SYSTEM

Challenges of Decision Making during Disasters

As noted above, the key to successful disaster response is to work through the OODA loop decision making cycle as quickly as possible based on the actual situation. However, there are numerous obstacles to achieving this during a large, wide-area disaster. Damage at local government, fire department, police, or other local agencies, for example, may result in a lack of information for making decisions. At the Cabinet Office, one of the problems during the Great East Japan Earthquake was that the government needed to mount an emergency response despite a lack of information caused by the impairment of local government functions due to damage to their buildings or injuries to staff[2].

This information vacuum in the immediate aftermath of a disaster can result in fatal delays in decisions for the most urgent lifesaving response activities. As it is recognized that survivability falls off rapidly once 72 hours have elapsed since a disaster, the important factor is how to work through the OODA loop quickly during this 72 hour period.

In response, Hitachi has developed a rapid situation assessment system to enhance the observation and orientation functions of its disaster prevention and response support solutions. The system looks to SNSs such as Twitter*, blogs, and bulletin boards to provide the information that can fill in these temporal and spatial gaps in information during a disaster.

Strategy for Using SNS Data

The characteristics of SNS data mean it provides the following benefits.

(1) SNSs can be used from mobile phones or other devices with hardware and software familiar to large numbers of users, including the general public and public agencies. They are currently used by about 30% of local government disaster prevention and management agencies, with a further group of nearly 20% considering their adoption[3].

(2) The collection of realtime information on communication between the public in the immediate aftermath of a disaster can indicate the status of

* Twitter is a registered trademark of Twitter, Inc.

affected areas (how the situation is developing, including actions by the public). As base station batteries running out after the power fails is the major cause of interruptions to mobile phone and other telecommunications infrastructure[4], mobile networks in affected areas can be expected to remain available for about half a day after a disaster strikes.

(3) The system can utilize systems and networks that are already available and widely used.

The disadvantages, meanwhile, are as follows.

(1) Information includes incorrect reports and rumors.

(2) Huge volume of data can bury important information and make it difficult to find.

For these reasons, accepting that incorrect reports and rumors will be present, the new system collects SNS data continuously in realtime and uses it to augment information from more reliable sources.

System Overview

Fig. 5 shows an overview of the rapid situation assessment system.

The system consists of SNS data collection, SNS data analysis, and common operational picture (COP) interface functions. It collects SNS data from sources such as Twitter and provides users with screens that help them assess the situation. The following sections describe these functions in detail.

(1) SNS data collection function

The SNS data collection function crawls the Internet to collect SNS data (raw data) from social media services and other targeted web pages. It also subjects the collected data to metadata and natural language analyses[5] to determine the time, location, identity of poster, and classification tag (disaster-related key words such as earthquake, tsunami, fire, or evacuation). The raw SNS data is stored in a database together with this extracted information, which is used for indexing. This classification then provides a basis for presenting the information on a map via the COP interface function, where it can be used to detect events such as fires, determine the extent of damage (such as halted trains or the location of injured people), and determine how the response is progressing (such as the deployment of fire fighters).

(2) SNS data analysis function

The SNS data analysis function consists of reliability analysis and anomaly detection.

The reliability analysis uses the criteria listed in (a) to (e) below to score the reliability of the SNS data so that information deemed to be reliable can be utilized for purposes such as situation assessment.

(a) Analysis of information source (person)

This assigns a reliability score based on the ID or other account information for the person who supplied the information. Information from local government personnel, for example, is given a high score whereas that from the general public is given a lower score. For example, it uses the account name included in Twitter data to determine whether or not a tweet is from an official local government account. If it is, it is given a

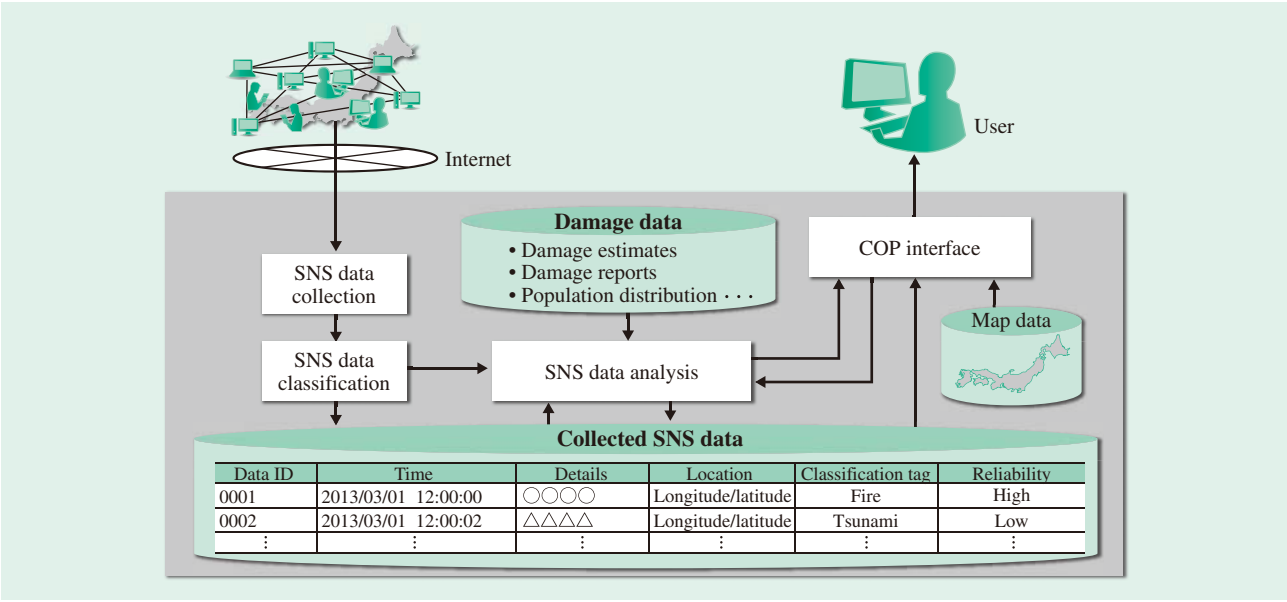


Fig. 5—Rapid Situation Assessment System.
The system collects, classifies, and displays SNS data to fill in gaps in information after a disaster occurs, and to provide a rapid assessment of the overall situation.

high reliability score and saved in the database. The identity of official accounts is available because local governments publish this information.

(b) Analysis of information source (location)

This assigns a reliability score based on the location from which the SNS information was posted, as indicated by global positioning system (GPS) or other location data. For example, information is given a high score if the location matches the content (such as place names contained in the data).

(c) Analysis of information type

This assigns a reliability score based on the type of information. For example, text is given a low score whereas videos or photographs are scored highly.

(d) Analysis of information timing

This assigns a reliability score based on how current the information is. For example, information is given a high score (timeliness) at the time it is posted, but this falls as time passes.

(e) Analysis of correlation with other information

This assigns a reliability score based on correlation with other information. For example, information is given a higher score the more other posts of the same type (such as those indicating a fire, for example) are collected from the same vicinity. Information is also scored more highly if it is highly ranked by other users.

Anomaly detection analyzes the collected SNS data as follows.

(a) Trend analysis, time-domain change analysis

Trend analysis identifies frequently occurring words and collates and condenses SNS data from each region. Time-domain change analysis identifies sudden increases or decreases in the frequency of particular words, and detects changes in data volumes.

(b) Information gap analysis

This performs comparisons on the disaster data in the database (such as damage estimates, damage reports, or population distributions) to generate data on information gaps (such as anomalous areas that are producing less data than would be expected) and similar. A location from which no data is being generated is likely to be so badly damaged that information can no longer be posted.

(3) COP interface function

After being subjected to the analyses described in (1) and (2) above, the SNS data is displayed on a map where it can be used to aid decision making. Fig. 6 and Fig. 7 show examples of screens displayed by the system. This function uses map and population density data published by the Ministry of Land, Infrastructure, Transport and Tourism.

TRIAL OPERATION

The system's classification and data visualization functions were tested using tweets collected via the Streaming Application Programming Interface (API) supplied by Twitter, Inc.

Typhoon 18 on September 16, 2013 caused heavy rain damage in the area around Kyoto in Japan. Information about flooding started coming in about midnight, with posts by the public about specific damage in upstream areas, such as high river levels or surface flooding on roads, appearing at around 3:50 AM (see Fig. 8). According to the damage report from the Fire and Disaster Management Agency[6], the disaster response headquarters under the jurisdiction of Kyoto Prefecture were set up at 5:00 AM. This suggests that the information collated and presented by this system would have been useful for making this decision, and for quickly assessing the situation once the headquarters was established.

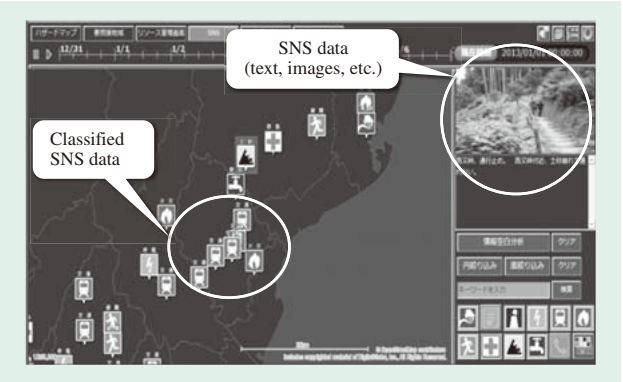


Fig. 6—Rapid Situation Assessment Screen.
The screen displays SNS data classified by the type of event (earthquake, tsunami, fire, etc.).

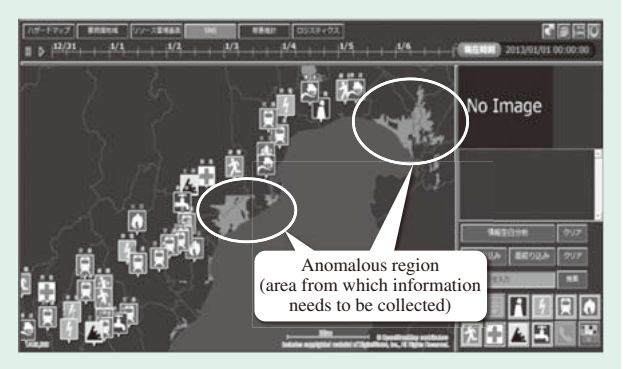


Fig. 7—SNS Data Analysis Screen.
The system performs comparisons on disaster data (such as damage estimates, damage reports, or population distributions) to identify anomalous regions, such as areas that are producing less data than would be expected.

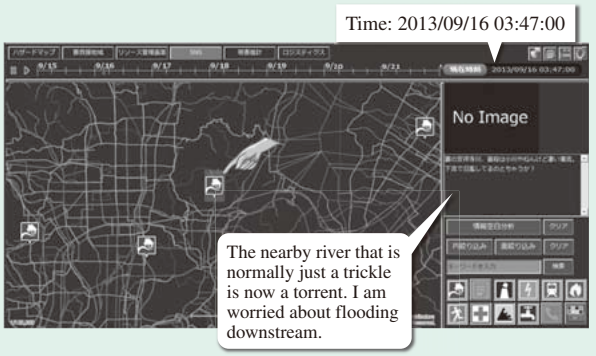
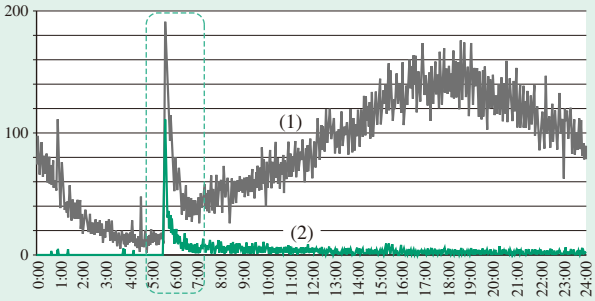
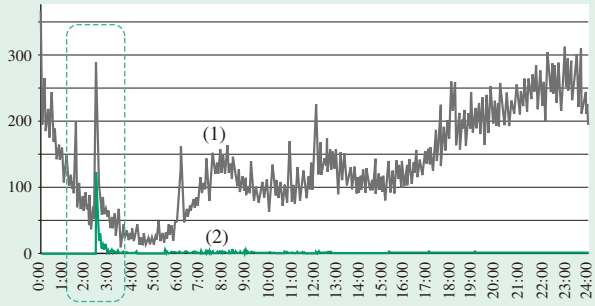


Fig. 8—Screen Displaying SNS Data on Wind or Water Damage. The screen utilizes SNS data to show specific damage information such as abnormal river levels or surface flooding on roads.

Fig. 9 shows the trend in the number of tweets before and after an earthquake on April 13, 2013 at Awaji Island in Hyogo Prefecture that was measured with an intensity of six lower, and an earthquake on September 20, 2013 in Fukushima Prefecture that was measured with an intensity of five upper. In both cases, a rapid rise occurred in the number of earthquake-related tweets identified by the system after each earthquake, indicating that SNS data provides a valuable source of information to help assess the situation immediately after a disaster, which is the primary objective of this system.



Location	Time	Epicenter	Size	Maximum intensity
Awaji Island	2013/04/13 05:33	N:34.251 E:134.497	M6.3	Intensity 6 lower
(1) No. of GPS-tagged posts (in Japan)				120,071
(2) No. of earthquake-related GPS-tagged posts				3,088



Location	Time	Epicenter	Size	Maximum intensity
Fukushima	2013/09/20 02:25	N:37.100 E:140.700	M5.9	Intensity 5 upper
(1) No. of GPS-tagged posts (in Japan)				195,141
(2) No. of earthquake-related GPS-tagged posts				1,271

GPS: global positioning system

Fig. 9—Quantity of Earthquake-related SNS Posts when Earthquake Occurs.
The graphs plot the number of earthquake-related posts on the SNS detected by the system before and after an earthquake.

CONCLUSIONS

This article has described the disaster prevention and response support solutions being developed by Hitachi, and also a rapid situation assessment system that utilizes information from SNSs and other sources immediately after the disaster strikes to help quickly collect information and determine what is happening. This proposed system is intended as a way of overcoming the problem of ensuring realtime and ongoing decision making during a large, wide-area disaster in which circumstances are continually changing.

To help create a safe and secure society, Hitachi intends to continue its research and development aimed at combining the different types of information collected when a disaster strikes, and at identifying information that will be of use during the emergency response. By supplying systems that provide effective support for decision making and activities on the ground during a disaster, Hitachi believes it can help reduce the damage that these disasters cause.

REFERENCES

(1) Central Disaster Prevention Council, Cabinet Office, Government of Japan, http://www.bousai.go.jp/kaigirep/chuobou/ in Japanese.
(2) Cabinet Office, Government of Japan (Disaster Management), "Main Issues with Disaster Emergency Response during Great East Japan Earthquake" (Jul. 2012), http://www.bousai.go.jp/jishin/syuto/taisaku_wg/5/pdf/3.pdf in Japanese.
(3) Gifu Prefecture Policy Committee, "Current Status and Issues Associated with Disaster Management in Gifu Prefecture" (Nov. 2012) in Japanese.
(4) Ministry of Internal Affairs and Communications, "Damage to Information and Telecommunications Sector in Great East Japan Earthquake, and Progress to Date on Recovery" (Jun. 2011) in Japanese.
(5) O. Imaichi et al., "HCRL at NTCIR-10 MedNLP Task," Proceedings of the 10th NTCIR Conference (2013).
(6) Fire and Disaster Management Agency, "Damage from Typhoon 18 (Report 11) (Oct. 2013) in Japanese.

ABOUT THE AUTHORS

Junji Ogasawara

Business Development Center, Business Advancement Division, Defense Systems Company, Hitachi, Ltd. He is currently engaged in planning and development of disaster prevention and crisis management business.

Koichi Tanimoto

Infrastructure Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of disaster prevention and crisis management systems.

Osamu Imaichi, Dr. Eng.

Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of information extraction and information retrieval. Dr. Imaichi is a member of the Association for Natural Language Processing and The Japanese Society for Artificial Intelligence.

Masayoshi Yoshimoto

Experience Oriented Approach Promotion Center, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in research and development of service design.

Featured Articles

Crisis Management System for Large-scale Disasters

Kazuhiko Tanimura
Kentaro Yoshikawa

OVERVIEW: The Great East Japan Earthquake has prompted a widespread reevaluation of how to go about crisis management. The Japanese government incorporated the standardization of disaster response into its "Basic Policies for Economic and Fiscal Management and Reform." Progress on the standardization of "incident response" is also occurring at the international level, with the publishing of the ISO 22320/JIS Q 22320 standard. Meanwhile, the multilateral provision of international aid following major disasters has become commonplace, with the scope of assistance expanding beyond natural disasters to also include terrorist attacks or major accidents. This has made the use of standardization to improve crisis management essential. Hitachi utilizes its crisis management technologies and products and its know-how built up through its defense and disaster prevention businesses to make social infrastructure even safer and more secure, and it is also conducting studies aimed at supplying new standards-compliant social infrastructure security solutions.

INTRODUCTION

THE Great East Japan Earthquake posed a major challenge because it required a diverse range of organizations to work together in many different situations in response to the disaster. These included national and local government, the Self-Defense Forces, the US military, fire departments, police, healthcare institutions, and private companies. This has prompted a widespread reevaluation of how to go about crisis management, with the inclusion in the government's June 2013 "Basic Policies for Economic and Fiscal Management and Reform"[(1)] of a plan to improve national resilience by proceeding with "studies toward standardization of disaster responses to facilitate wide-area aid." Also, because international relief work with participation by multilateral organizations has become common during major disasters in recent years, the formulation of the ISO 22320/JIS Q 22320 international standard[(2)] ("Societal Security - Emergency Management - Requirements for Incident Response") has been a vital development. The introduction to the standard notes the need for an approach that encompasses multiple nations and organizations.

Because large and complex disasters that cover a wide area cause damage to numerous organizations and districts, resulting in varying degrees of impairment to those organizations and their functions, it is difficult for the people on the ground who are dealing with the situation to exchange damage information and establish mutual understanding. Problems reported during the Great East Japan Earthquake included delays in getting assistance and rescue work underway, delays in decision making, and lack of clarity in the command and control structure. Overcoming these problems will require an upgrading of capabilities during normal times, including the standardization of disaster response in a way that systematizes response know-how, and training exercises that follow the framework laid out by the standard.

This article describes a US crisis management system and the international standard for incident response, and gives an overview of a crisis management solution designed with reference to these.

CRISIS MANAGEMENT SYSTEMS IN USA

The terrorist attacks of September 2001 prompted the USA to establish a National Incident Management System (NIMS)[(3)] in 2004. The NIMS is a comprehensive crisis management system that covers the entire country and collates the concepts and principles of crisis management for different types of incidents and organizations. It includes the following stipulations.

(1) Preparedness

This expresses the necessity of improving preparedness for disasters before they happen by putting in place measures such as planning, procedures, training and exercises, and qualifications.

(2) Communications and information management

This expresses the importance of interoperability and the need for communication and information systems that can provide a common operational picture (COP) to everyone involved in the response to an incident.

(3) Resource management

This expresses the need for flexible and standardized mechanisms for things like typing, inventory, distribution, and management.

(4) Command and management

This expresses the need for providing a flexible and standardized framework for crisis management, and the importance of the concepts of command, coordination, and public information.

INTERNATIONAL STANDARD FOR CRISIS MANAGEMENT

The ISO 22320/JIS Q 22320 international standard was issued in November 2011 and adopted as a Japanese Industrial Standards (JIS) in October 2013. It stipulates the minimum requirements for mounting an effective response to a crisis. These requirements are summarized below.

(1) Command and control

Specifies command coordination, organizational structures and procedures, and resource management within an organization.

(2) Activity information

Specifies how to handle things like work processes and data capture and management to provide timely, relevant, and accurate information.

(3) Coordination and cooperation

Specifies command coordination processes as well as coordination and cooperation between organizations and between different parts of the same organization.

CRISIS MANAGEMENT SOLUTION

While the USA's NIMS provides a viable framework for the effective implementation of crisis management, its adoption is not enough on its own to provide complete crisis management. When the requirements of the international standard are considered as well, it is also essential to undertake preparations, such as conducting exercises based on a particular scenario, and to utilize information and communication technology that provides efficient support for these preparations. The following section describes a solution that supports the NIMS requirements.

Preparation: Improving Disaster Response Capabilities in Advance

Training exercises are particularly important for mounting an appropriate response when incidents occur.

Exercises include seminars for conducting basic training, skills exercises that use a training simulator or other resources to train people in system operation, table top exercises (TTXs) that involve discussing a problem around a table and devising solutions, command exercises using simulation-based role playing to provide training in decision making, and field training exercises (FTXs) that practice mounting an actual response on the ground. Along with having clear objectives, it is important that a framework be established for each exercise. These are then put together in the form of a separate scenario package for each objective. These scenario packages specify the scenario for the exercise and include the process to be followed during its execution.

It is recognized that there is currently a shortage of exercises intended primarily for command staff in particular (command exercises). By providing a more comprehensive range of this type of exercise, the intention is to foster leaders able to deal appropriately with unexpected events, and to optimize crisis management manuals and other plans or operational procedures by incorporating the lessons learned during exercises (see Table 1 and Fig. 1).

Table 1. Exercise Programs

There is currently a shortage of exercises intended primarily for command staff (command exercises).

Exercise type	Purpose	Example
Seminars	Basic training and knowledge acquisition	• Classroom training • e-learning, etc.
Skills exercises	Repetitive exercises such as training on operating procedures	• Driving simulator • Flight simulator, etc.
TTXs	Group exercise to discuss a problem and devise solutions	• Small group activities • OJT, etc.
Command exercises	Exercises based on role-playing for command staff	?
FTXs	Exercises at the actual site of an incident	• Civil defense exercises, etc.

TTX: table top exercise FTX: field training exercise OJT: on-the-job training

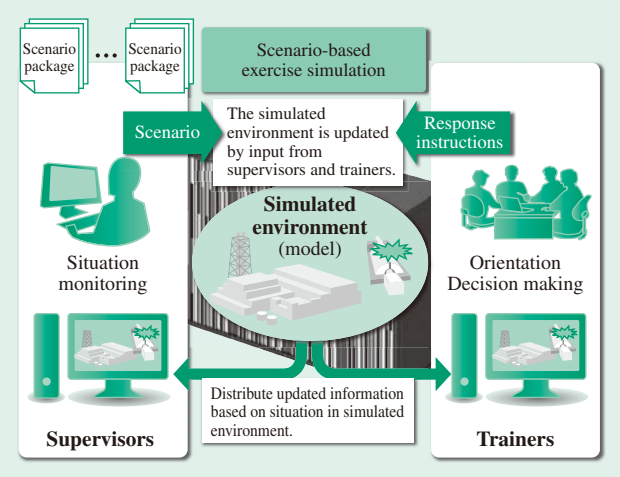


Fig. 1—Overview of Exercise Functions.
Exercises are made more effective by basing them on scenarios prepared for different objectives and conducting them in realistic simulated environments.

Communications and Information Management

(1) COP

It is essential that the people involved in the response to a large and complex disaster extending over a wide area share incident information. COP is a technology for achieving this. By allowing everyone involved to share in the evolving situation in realtime, command staff can issue appropriate orders instructing what to do next and people working on the ground can make assumptions about how to prepare for their upcoming tasks. When sharing information, only providing people with what is relevant to their role or duties saves them from being swamped by a flood of information.

The ways in which information might be displayed on a COP include showing incident information overlaid on a map, tasking lists (realtime display of tasks, events, and progress based on groupings formed during an emergency), and aerial or satellite images of the affected area (see Fig. 2).

(2) Interoperability

Incident response utilizes radio, information, and other systems belonging to the organizations involved in the response; government agency systems; and local civil defense, police, or firefighting radio systems or other audio disaster prevention systems. It also requires the wide-area coordination of the many information systems belonging to relevant agencies. Because of the diverse range of systems that manage the required information, an important role is played by the communications infrastructure that implements this wide-area coordination and provides a base for ensuring the interoperability of different systems (see Fig. 3).

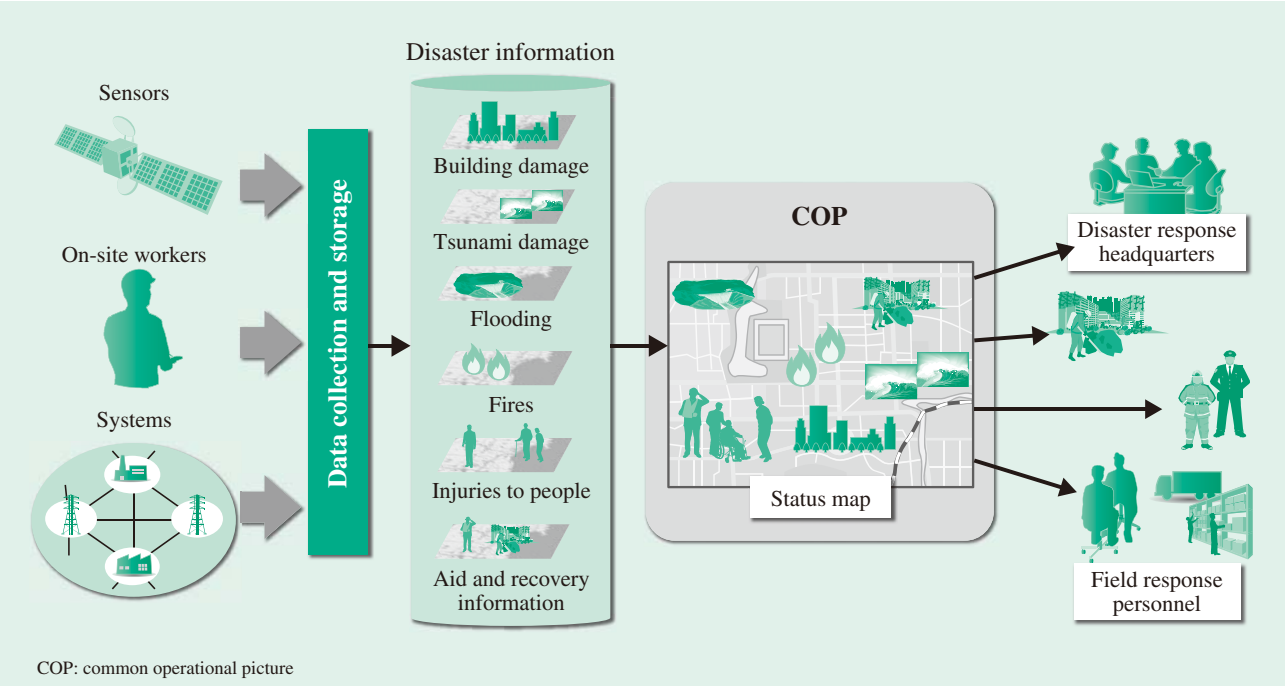


Fig. 2—COP.
COP technology is used to classify and combine information required for incident response so that information can be shared between the people involved in realtime.

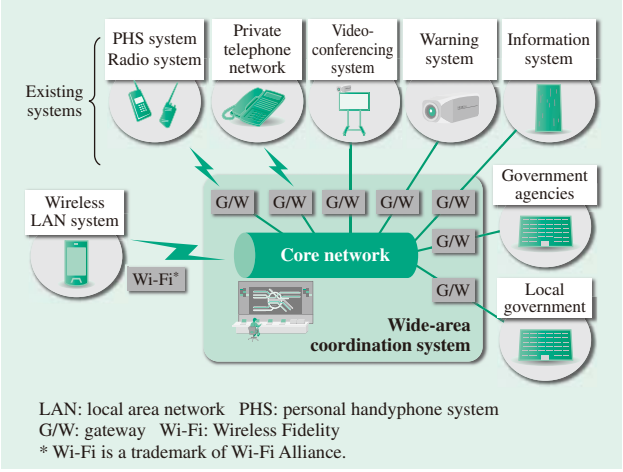


Fig. 3—Wide-area Coordination System.
It is important to have communications infrastructure that can provide wide-area coordination and act as a base for ensuring interoperability between different systems.

Resource Management: Flexible Mechanisms

Emergency logistics management supports the management of inventorying, procurement, and distribution of relief supplies; the presentation of this information on a map; and the dispatching of requested supplies. It provides flexible resource management, including the use of functions such as the forecasting of demand for supplies so that those in charge can decide to dispatch relief supplies to areas that have suffered so much devastation that they are not in a position to issue their own requests (see Fig. 4).

Command and Management: Flexible and Standardized Framework for Crisis Management

The observe, orient, decide, and act (OODA) decision making methodology devised by the US military for use in emergencies involves the use of a COP to help commanders orient themselves, identify and understand confused activity at an early stage, and shorten the time taken for decision making. Working through this OODA loop as quickly as possible in response to an unexpected event or severe accident can mitigate damage and prevent it from spreading. The plan, do, check, and act (PDCA) process is widely used for responding to events. However, whereas PDCA involves a slower paced cycle of steps suited to putting countermeasures to an incident in place beforehand, the OODA cycle is an emergency measure for dealing with unexpected events and is suited to the response needed immediately after an incident has occurred (see Fig. 5).

CONCLUSIONS

This article has described a US crisis management system and the international standard for incident response, and has given an overview of a crisis management solution designed with reference to these.

Hitachi is utilizing its know-how in fields such as command and control (C2), exercises, and cyber-security obtained through experience in its defense and

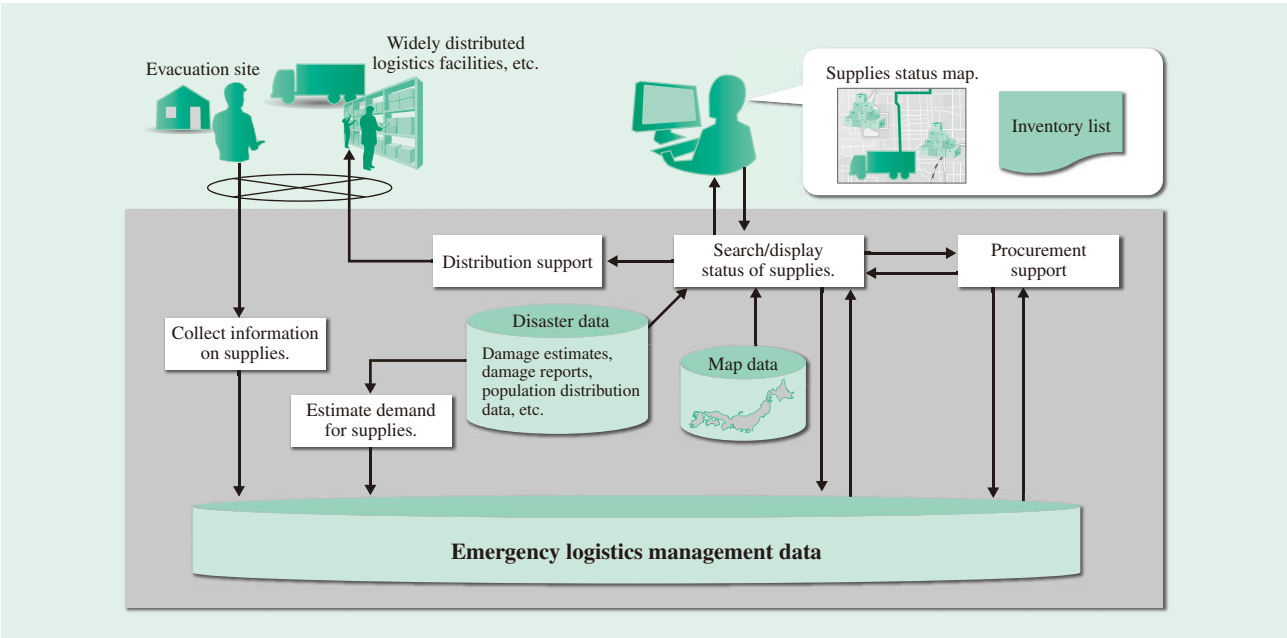


Fig. 4—Flexible Emergency Logistics.
This manages warehousing and distribution of relief supplies during a disaster.

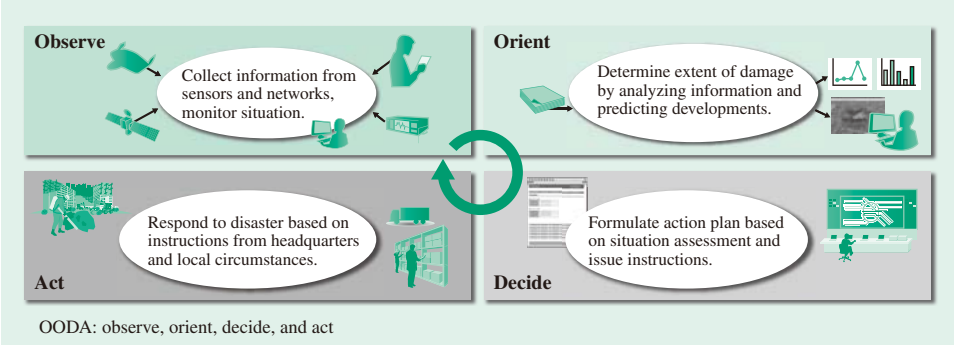


Fig. 5—OODA Loop.
The OODA loop implements command and control as a cycle of observation, orientation, decision, and action.

disaster prevention businesses to investigate new social infrastructure security technologies with reference to developments in international standardization.

Utilizing an approach like the C2 concept from defense systems is an effective way to mount an efficient operation in response to a severe accident. Conducting routine exercises is also important, and these should be used as guidance when actual incidents happen or in other situations such as demonstrations relating to public safety and security. In addition to the solution described in this article, Hitachi also has numerous other technologies applicable to crisis management. Among these are enterprise asset management that includes techniques for using sensor information for anomaly prediction or detection and preventive maintenance, wearable devices, containerized data centers, and disaster response robots.

Through its ability to supply one-stop solutions that extend from control systems to the information systems used for social infrastructure, Hitachi is seeking to further improve safety and security throughout the infrastructure of society.

REFERENCES

(1) Cabinet decision, "Basic Policies for Economic and Fiscal Management and Reform" (Jun. 14, 2013).
(2) JIS Q 22320: 2013 "Societal Security - Emergency Management - Requirements for Incident Response," http://kikakurui.com/q/Q22320-2013-01.html in Japanese.
(3) Federal Emergency Management Agency, National Incident Management System, http://www.fema.gov/national-incident-management-system

ABOUT THE AUTHORS

Kazuhiko Tanimura
Business Development Centre, Business Advancement Division, Defense Systems Company, Hitachi, Ltd.
He is currently engaged in system commercialization in the fields of command and control and crisis management.

Kentaro Yoshikawa
Business Development Centre, Business Advancement Division, Defense Systems Company, Hitachi, Ltd.
He is currently engaged in the planning and sales of disaster information systems.

Featured Articles

Physical Security for Companies that Maintain Social Infrastructure

Shinsuke Kanai
Kenji Nakamoto
Akio Takemoto
Masatoshi Furuya

OVERVIEW: While the companies that maintain social infrastructure have gained many benefits from advances in information and communications technology and its widespread adoption, they also face new threats. Modern corporate management demands security measures for both the physical and cyber realms. For reasons of corporate group governance, there has been a growing trend in recent years toward the group-wide consolidation of system management, with increasing adoption of both the private and public cloud models. There has also been interest in the use of techniques for ultra-high compression and decompression in surveillance camera systems to allow transmission over narrow bandwidths. The food safety sector, meanwhile, has recognized the potential for establishing video traceability infrastructure, utilizing bar codes or other forms of identification.

INTRODUCTION

THE major earthquake that struck eastern Japan in March 2011 caused considerable damage to the social infrastructure on which people's quality of life and corporate business activity depend. The consequences continue to disrupt the lives of many people. Furthermore, because the earthquake made it difficult for many of the companies that suffered damage to continue in business, it also resulted in indirect interruptions to the operations of some of the companies that did business with these directly affected companies. This demonstrates how companies are part of the infrastructure of society (see Fig. 1).

The causes of interruptions to corporate activity are not limited only to earthquakes. Nor are they limited only to things that relate to a company's own business, such as leaks of personal information, data falsification, false accounting, false advertising, or inadequate food hygiene management. Along with these, they also include various other serious threats, including malicious behavior by staff, malicious postings on the Internet, or company-targeted terrorism. Physical security for companies can be defined as "preemptively establishing physical systems to prevent, track, and rapidly recover from threats with the potential for business interruption."

This article describes developments in the field of physical security products, such as access control or surveillance cameras, that consolidate and automate problematic administration at the corporate groups that maintain social infrastructure, a ultra-high compression and decompression technique for video that is useful for transmission over narrow bandwidths,

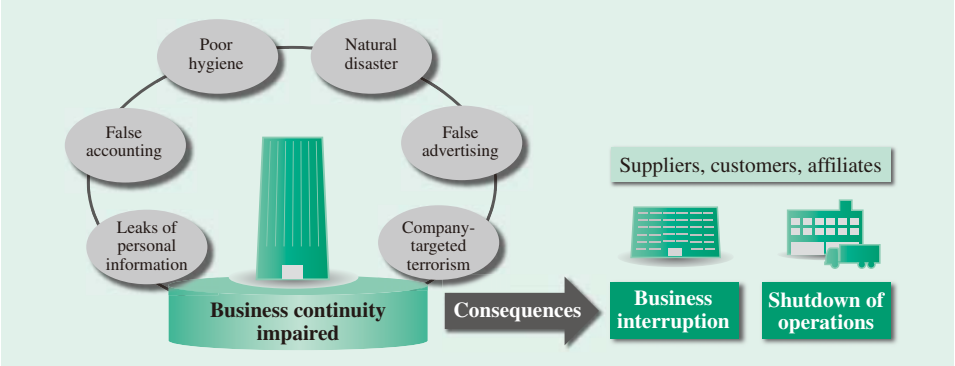


Fig. 1—Consequences of Business Interruption to Companies Involved in Social Infrastructure.
The inability of a particular company to maintain its operations will have consequences for its customers and suppliers, among others. Companies are also part of the infrastructure of society.

and infrastructure for physical security and traceability in the food safety sector that is seen as having potential in the future.

STANDARDIZED GROUP-WIDE CORPORATE PHYSICAL SECURITY

For the companies and other organizations that handle confidential, commercial, technical, or personnel information, or that maintain important social infrastructure, it has become an accepted practice to restrict access to work areas and other key locations at their offices and to control where people are able to go. Nowadays, doors are kept locked when not in use and it is rare for outsiders to gain access to a workplace without permission. Visitors are received away from the workplace at a reception room. The main mechanisms used for this purpose are identification devices such as non-contact smartcard readers and finger vein recognition systems, together with other equipment such as electric locks and automatic doors or gates. Staff can use a card or their finger vein pattern to open the doors to those rooms to which they are permitted access.

Because many such companies are subject to intense global competition, one of the most important aspects of their business is timely integration, reorganization, and rationalization, including of group companies. A consequence of this is that transfers and other changes of workplace occur frequently for staff throughout the group, who may number in the thousands or more. If each workplace were to use a different way of controlling access, not only would it be inconvenient for staff and management, there would also be considerable cost each time changes were made. An effective solution is to centralize personnel information across the group and to provide automatic links between the personnel information and access control systems.

Meanwhile, because criminal acts typically involve someone gaining unauthorized access in a way that does not leave a record, such as "tailgating" (entering behind an authorized person), it is difficult to determine what has happened from the access control system's records alone. Given that people's memory of events becomes more uncertain as time passes, it is critical to locate surveillance cameras at key thoroughfares where they cannot be evaded, and to store all video that contains movement for at least several months. However, while installing more cameras makes it easier to determine what has happened by reviewing the video, it also results in more data to be stored.

Since 2008, Hitachi has been adopting standardized physical security based on this concept throughout the group, including at its headquarters and at all branch offices, sales offices, factories, laboratories, and company hospitals.

TRENDS IN PHYSICAL SECURITY PRODUCTS

Private Cloud Model

Past systems have mainly used "local model" configurations that are structured around individual workplaces. However, it is not an easy task to provide the environment and support systems needed for 24-hour operation of servers, recorders, and other equipment independently at each workplace. It is particularly difficult at sales offices with a small staff.

In response, Hitachi recommends the use of in-house data centers to centralize system administration for physical security at a number of workplaces and group companies, using systems with a configuration based on a private cloud model shared by each workplace. Use of a private cloud model not only allows centralized management of servers, recorders, and other equipment, it also facilitates automatic links to personnel information systems. However, care is required when centralizing the transmission and archiving of video. Because it is enough to be able to view live or recorded video when needed, it is not necessarily a requirement to consolidate all video at one place in realtime. Unless it causes administration problems, Hitachi recommends that recorders be distributed across the company (see Fig. 2).

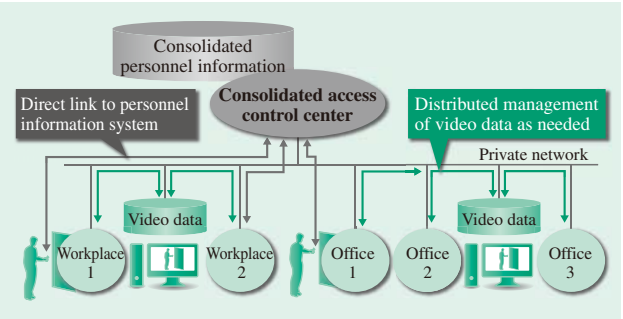


Fig. 2—Configuration of Physical Security Based on Private Cloud Model.
In addition to centralizing management of servers, recorders, and other equipment based on a private cloud model, this also facilitates the provision of automatic links to personnel information systems.

Public Cloud Model

Many companies adopt an information security policy of not connecting their corporate physical security systems to their internal network, meaning there is no automatic link to their personnel information systems.

For customers who adopt this policy, Hitachi offers its integrated facilities management solution. The facilities management solution uses a configuration based on a public cloud model to allow centralized system administration covering multiple workplaces. This model uses servers and application services hosted at a public cloud center managed by Hitachi. By outsourcing the maintenance and management of the servers used for centralized administration of multiple workplaces based on this model, the customer can be sure of always having easy access to the latest application services.

In addition to the facilities management solution for offices, Hitachi also supplies an information system for condominiums.

REQUIREMENTS FOR SURVEILLANCE CAMERA SYSTEMS

Criminal acts that occur in a physical environment are often planned. Perpetrators use the Internet to plan the crime or check the targeted site or other information beforehand, and take a preliminary look at the site, escape routes, and other locations. To obtain crime-solving clues, criminal investigations in recent years have increasingly been utilizing forensic analyses of networks and other information technology (IT) equipment, and cross-checking with analysis of video surveillance records from the scene. The use of surveillance cameras is becoming increasingly important.

Along with locating surveillance cameras where people cannot reach them, it is also important to provide them with adequate anti-tampering functions. For example, it is essential that they be fitted with alarms that will be triggered if someone covers them with spray or some other form of blindfold, or if someone interferes with their power supply, communications, or camera orientation. In the case of locations where people frequently interfere with the camera orientation, it is necessary to consider installing a domed camera; a panoramic view, tilt, and zoom (PTZ) camera that can be operated remotely; or a 360° omnidirectional camera.

Hitachi recommends its video management system that incorporates effective anti-tampering functions and functions for detecting or searching recorded video for suspicious people or behavior. These functions can automatically detect movements that indicate an attempt at unauthorized access; people who are hiding their faces in a suspicious way; or people bringing in, taking out, or swapping suspicious packages or leaving them unattended, for example. Hitachi also intends to consider applications that can detect or search for instances in which someone is carrying packages that are clearly different in type or quantity between the time they enter and leave a room. At sites such as data centers, this function should be used in conjunction with other measures such as checking in packages or inspecting them on arrival or departure. At places that are not sufficiently visible to people, the system would issue a verbal warning to any suspicious person from a speaker-equipped camera.

Analog cameras have been widely used in the past due to limits on the storage capacity of recorders and on network bandwidth, and because they are easy to set up. Because of the need for surveillance to extend from large areas down to tiny details such as fingertip movements, use of high-resolution Internet protocol (IP) cameras with resolutions in the megapixel range has become increasingly common in recent years. However, it is necessary to avoid compressing images by so much that the high-resolution video is unable to be restored to its original quality level due to limits on transmission and storage. In response, Hitachi has been working on research and development of a technique for ultra-high compression and decompression intended for use in narrow-bandwidth transmission. This technique allows the storage of long-duration video from large numbers of cameras at a high resolution and frame rate, even when bandwidth and recorder storage capacity are limited, and that also supports high-speed video searching. It is anticipated that this will lead to progress on the centralization and backup of video management.

FOOD SAFETY AND PHYSICAL SECURITY TRACEABILITY

Guaranteeing food safety is vital to ensuring that people can participate healthily in society. The companies and retailers involved in the growing, processing, manufacturing, distribution, and consumption of food (the “food chain”) all have an important role to play as part of the infrastructure of society. In the case of countries that experience frequent terrorism, this concern extends to subjecting all guests and visitors

to hotels, particularly those used by important people, to body checks by metal detector.

When considered in terms of physical security, food processing plants that mainly deal with processing and other manufacturing are characterized by having large sites that are visited by numerous vendors, and by employing staff under a wide variety of employment arrangements. If a plant is undefended, it is easy for someone planning a crime to gain access and difficult to identify their behavior as suspicious once they do so. For these reasons, it is good practice to make the plant difficult to enter without authorization through measures such as limiting the number of points of entry as far as possible, having guards check people and vehicles on entry and exit, and enclosing the site in a fence with intruder detection sensors or other defenses (see Fig. 3).

For hygiene reasons, however, such as measures for preventing contamination by foreign material, it is not possible to install access control using non-contact smartcards or other methods at the production areas inside a factory. For example, along with metal detector body checks conducted prior to entry to a production area, it is necessary to adopt measures involving the use of high-resolution surveillance cameras both inside and outside the production area to record faces, fingertip movements, and other features. If something does happen, it is vital to have measures in place to present these records as evidence. In recent incidents of harmful food contamination in Japan, considerable time had often elapsed between the date of production and the detection of the contamination at the point of consumption. At a minimum, recorded video should be kept from the date of production up until the food's use-by date. Also, it is not uncommon for food processing plants to present a difficult environment for camera operation, including hot and humid conditions or freezing temperatures. It is recommended that suitable checks be made regarding the operating temperature range prior to installation, and that cameras be inspected regularly.

Interest in the use of video recording for food traceability has grown in recent years. As noted above, the presence of harmful contaminants in food is often not detected until the point of consumption, meaning that the contamination could have occurred at any point along the food chain. By recording the time and location each time the bar code attached to the food is scanned as it moves along the food chain, if something subsequently happens, it will be possible to go back

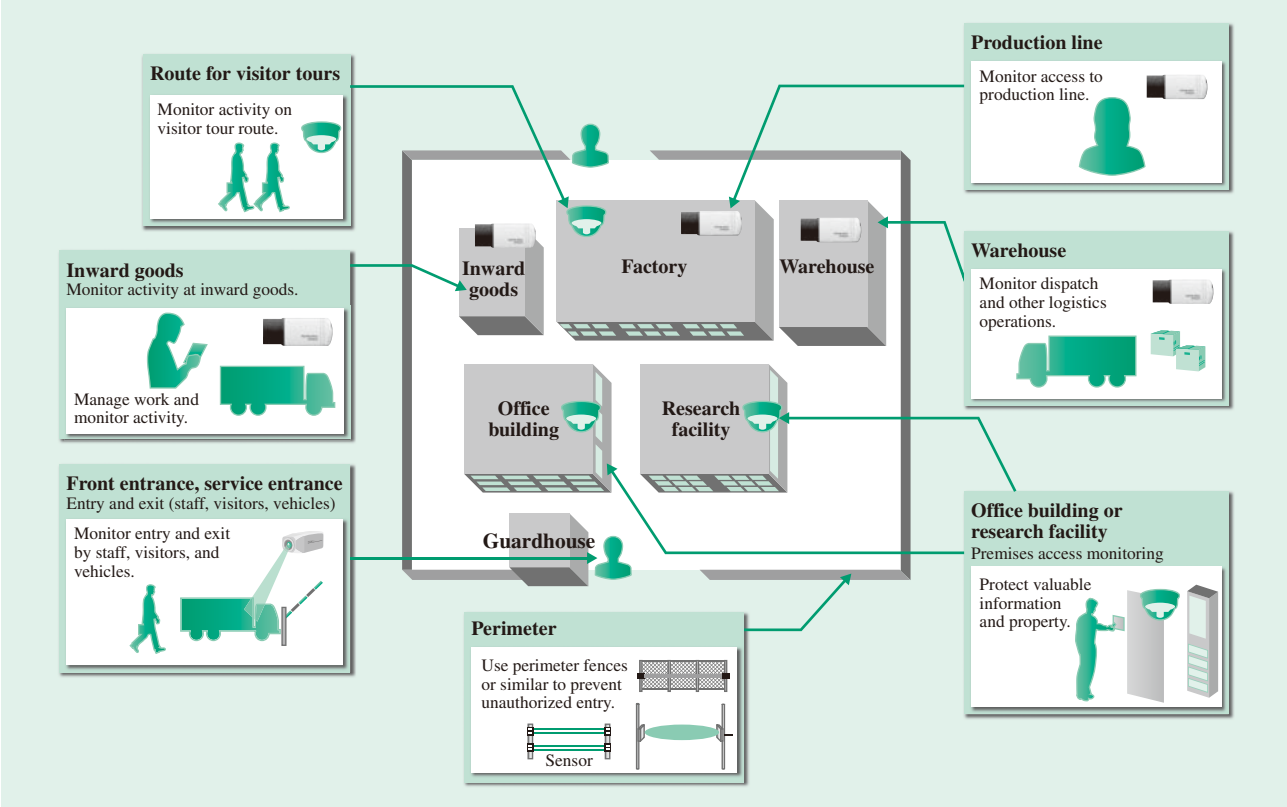


Fig. 3—Physical Security at Food Processing Plant.
This access control solution for factories supports physical security at food processing plants and other facilities.

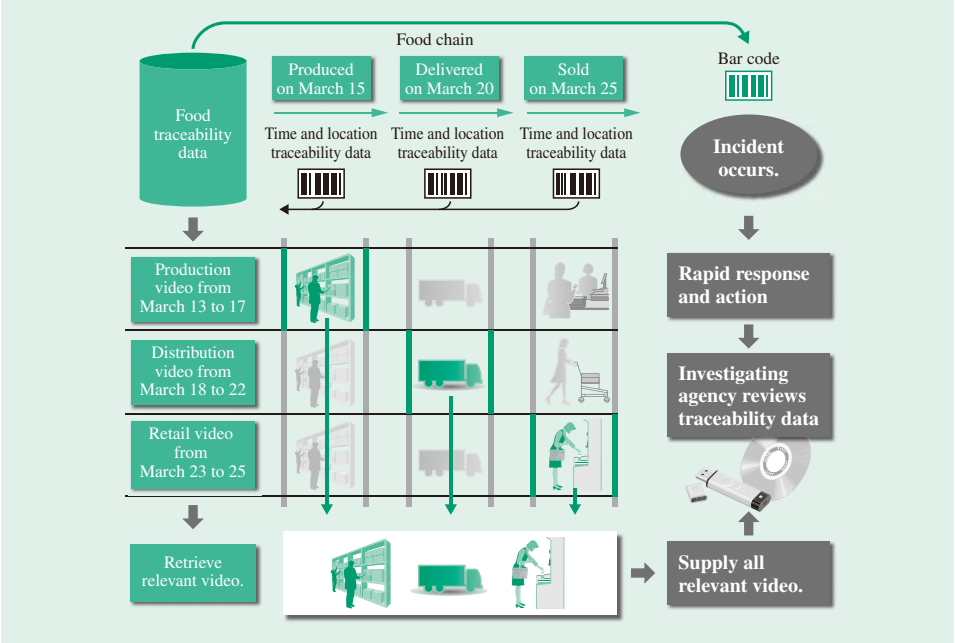


Fig. 4—Block Diagram of Video Traceability.
There is a need to establish the infrastructure for video traceability along the entire length of the food chain.

and review all of the recorded video for those times and places. This is much more efficient than reviewing all of the video. It is anticipated that infrastructure will be established for video traceability so that video of all of the main control points along the food chain is able to be viewed over a network (see Fig. 4).

CONCLUSIONS

This article has described developments in the field of system models for the group-wide standardization of physical security for corporate groups, which has an important role underpinning both companies and social infrastructure, with an emphasis on the functional requirements for surveillance cameras. The article has also used food safety as an example, explaining the need for physical security at all of the companies and retailers involved in the food chain, and how it is anticipated that the industry will work together to establish the infrastructure for video traceability.

Hitachi believes that the wider adoption and encouragement of corporate physical security, and advances in the associated technology, will also contribute to the success of the Tokyo Olympics in 2020.

ABOUT THE AUTHORS

Shinsuke Kanai
Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in solution business in integrated security.

Kenji Nakamoto
Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in solution business in integrated security.

Akio Takemoto
Security System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in security business in cameras.

Masatoshi Furuya
Energy System Engineering Department, Security & Energy Solutions Division, Urban & Energy Solutions Division, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in business planning related to security.

Featured Articles

Traceable Physical Security Systems for a Safe and Secure Society

Tatsuhiko Kagehiro, Ph.D.
Kenichi Yoneji
Harumi Kiyomizu
Yuki Watanabe, Dr. Info.
Yohei Kawaguchi
Zisheng Li, Dr. Eng.
Hisashi Nagano
Yusuke Matsuda

OVERVIEW: In an era of terrorism and serious criminal activity, a strong reliance is being placed on security systems that keep society safe and secure. This in turn requires ways of determining the security of people and property, and the ability to extract relevant information from accumulated data quickly. In response, Hitachi has been studying the functions required to combine high security with convenience, two objectives with conflicting characteristics, at major public facilities where these systems are likely to be installed. The concept of "traceable physical security" is used to ensure people's safety. Hitachi has also built a "multi-perspective search" system that can search collected image data using a variety of different attributes as keys.

INTRODUCTION

WHILE the number of victims of terrorist incidents has been declining over time, the proportion of fatalities has been increasing steadily since 2009, reaching about 30% in 2011. This is because the increasing severity of individual attacks has resulted in more severe consequences. As a result, there is strong demand for enhancing security systems to prevent this.

In many cases, surveillance cameras are used as the primary means of physical security. In 2008, Hitachi announced a large surveillance system that can connect numerous surveillance cameras together via a network and manage them centrally, and that can also perform high-speed searches of large amounts of collected image data[(1)].

Hitachi also introduced finger vein identification in 2003 to provide a new mode of biometric authentication. The technology is widely used in a diverse range of applications, including access control, personal computer (PC) login, and banking systems.

Hitachi has also been working on the research and development of explosives detection systems that use mass spectrometry, including verifying their robustness in demonstration projects and building up a track record of practical use. The use of this technology in a hand luggage inspection system for airports was announced in September 2013[(2)].

At public facilities, physical security is utilized to ensure the safety of people and property and, where possible, to prevent criminal activity before it happens. However, combining a high level of security with convenience is problematic. Because the cumbersome procedures associated with strengthening security measures tend to detract from convenience, it is difficult to apply such measures more widely. This means it is necessary to find invisible means of authentication that the public will not find intrusive, and to improve convenience for the people who are not deemed to pose a threat. This article uses the term "unconscious authentication" to refer to methods for authenticating users without their being aware of the process (but who have given their prior consent for this to occur).

Meanwhile, when an incident does happen, there is a need for the rapid extraction of footage that might help resolve the incident from collected surveillance camera video data. Because eyewitness and other information is fragmentary by nature, there is a recognized need for video surveillance systems that can perform rapid searches based on numerous different attributes.

This article describes traceable physical security systems for a safe and secure society, and multi-perspective search.

TRACEABLE PHYSICAL SECURITY

Measures such as biometric authentication and hand luggage inspection are used to ensure the security of people and property at public facilities. However, these measures can be inconvenient if they require checks or

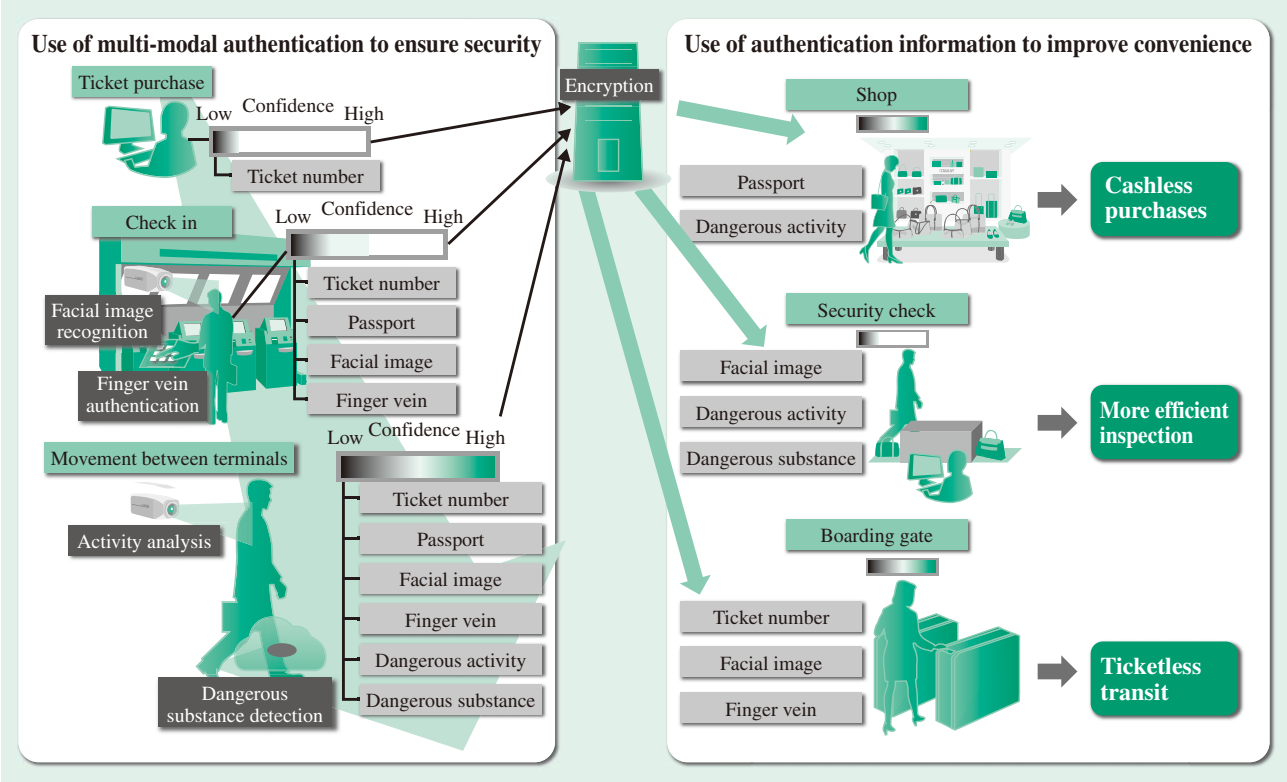


Fig. 1—Concept of Traceable Physical Security.
The requirement is to combine use of multi-modal authentication for security with the use of the authentication information to improve convenience.

other actions that interrupt the flow of people, causing queues to form. Accordingly, the ideal solution is to use unconscious authentication techniques for visitor screening. If it is possible to use a number of different modes of authentication or inspection, and to modify the level of security applicable to individuals as needed, convenience can be enhanced by expediting services for members of the public who pose no threat. This concept is called "traceable physical security," and is summarized in Fig. 1. The implementation of traceable physical security involves a combination of touch panel finger vein authentication and facial image recognition for biometric authentication, together with explosives detection systems capable of sampling from multiple points for hand luggage inspection and the use of surveillance cameras for hand luggage tracking.

Biometric Authentication

A variety of biometric authentication techniques exist based on different biological attributes, with facial recognition being the most commonly used mode for unconscious authentication. In practice, however, the accuracy of facial image recognition remains inadequate for use as a single-mode unconscious authentication technique. Accordingly, an alternative option is to achieve the level of accuracy required in practice by using it to identify individuals in combination with an authentication mode such as finger vein recognition that has proven its accuracy in practical use.

However, finger vein recognition cannot currently be described as an unconscious authentication technique because it requires the user to place their finger in or on a scanner. In response, Hitachi has looked at the possibility of reading a user's finger vein pattern without their being aware of the process by doing it as part of some other activity. The device shown in Fig. 2 generates infrared light to read a person's finger vein pattern while they use a touch panel of the sort that might be found on an automated teller machine (ATM), ticket dispenser, or check-in kiosk. The device consists of a projector and camera contained inside a housing. The display image is projected onto frosted glass, and the built-in camera is used to detect where on this image the user touches their fingertip to the glass. By identifying where the user touches the glass, the system acts as a touch screen input device. The user's finger vein pattern is read by the built-in camera by shining infrared light onto their finger from an above-mounted light-emitting diode (LED) when they touch the glass.

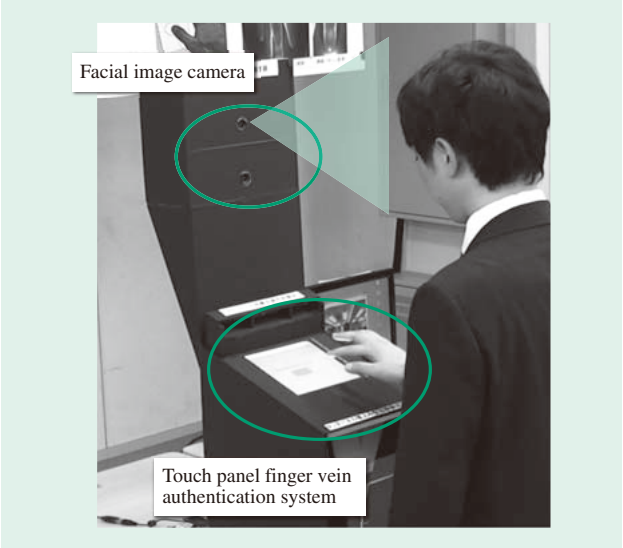


Fig. 2—Touch Panel Finger Vein Authentication System.
Finger vein authentication is performed while the user operates a touch panel, during which time a facial image is also captured.

As the user is unaware of this happening, the system can perform unconscious authentication while they use the touch panel.

Once finger vein recognition has completed, an image of the user's face is captured by a camera mounted at the top of the housing, and the facial image linked to the user's identity. This allows people within the surveillance area to be identified with a high level of accuracy, with the facial image captured when the person entered the facility used as a template. Because recognition is performed on a recently acquired facial image, this also has the advantage of minimizing the impact of factors such as aging or cosmetics. This facial image recognition technique has already been used in applications that include simple gate management and signage.

Explosives Detection System with Multi-point Sampling

This system uses the principle of mass spectrometry to detect substances such as ingredients contained in explosives adhering to people or property. Hitachi has previously developed gateway-style detection systems. However, these are unable to detect suspicious substances in open spaces. The new system, in contrast, sequentially draws air samples into the mass spectrometer from a number of pipes installed around the area being monitored to identify the location of suspicious substances. Unfortunately, a drawback with this approach is that the time taken to sample all pipes one after the other makes it difficult to detect substances quickly. To overcome this, the samples are taken from a number of pipes at the same time, using a different combination of pipes each time. The resulting mass spectrometry signal is then subject to a signal processing technique called "compression sensing." This technique can identify the location of a dangerous substance from a short-duration signal and thereby achieve rapid detection of substances in the area being monitored without requiring a large number of expensive mass spectrometers.

Hand Luggage Tracking

To ensure safety, there is a need to identify the route taken through the facility by each item of hand luggage and the people who handle it. Accordingly, Hitachi has studied an approach to ensuring safety based on the results of hand luggage tracking using this system.

At important facilities, it is common to require the inspection of hand luggage when someone enters a restricted area. This involves placing the item on a belt conveyor and checking it using an X-ray machine, explosives detection system, or other sensors. By installing a camera on top of this inspection system to photograph the luggage, it is possible to obtain comparatively reliable images of the item being checked. These luggage images can then be used as a basis for presenting a visual representation of the route traveled by the item up to this point. The surveillance cameras installed at the facility are used to perform continuous detection of movements by people or hand luggage, and this information can be used to register the image data for objects that resemble hand luggage in a similar image search engine. This search engine is then used to perform a search based on the color characteristics of the hand luggage image captured at the luggage inspection system to identify matching image sections that are then used to recreate the route taken by that particular item. The safety of the luggage can then be assessed by comparing this route with the results from the explosives detection system with multi-point sampling described above. The image data from the route taken by the luggage can also be used to check for suspicious actions such as the luggage being handed from one person to another.

Integrated Viewer

The results from the authentication, detection, and recognition systems described above are collated in an information system and displayed in turn on an integrated viewer (see Fig. 3). The viewer can display a map overlaid with the locations of people as they

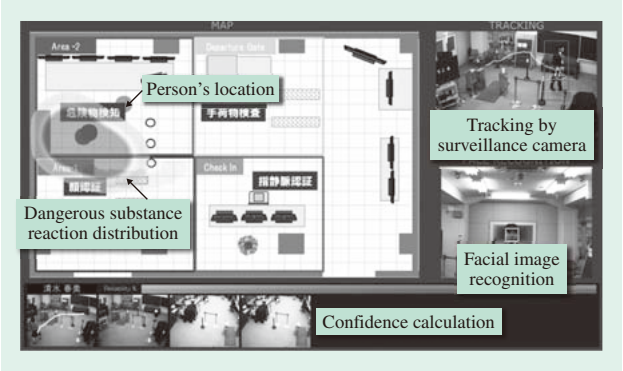


Fig. 3—Integrated Viewer.
The viewer displays the location of people at a facility, estimated distribution of dangerous substances, surveillance camera video, and facial image recognition.

Fig. 4—Authentication Viewer.
The screen displays authentication results from each area in turn.

Fig. 5—User Screen for Multi-perspective Search.
The screen displays the result of a search performed using attributes of the upper body, lower body, luggage, and route traveled as keys.

are tracked though each area of the facility, and with the estimated distribution obtained by explosives detection. It can also be used to view video from surveillance cameras. The authentication viewer shown in Fig. 4, meanwhile, can display the results of authentication for a visitor at each area within the facility. It can also show the authentication mode used to identify them in each case, the attribute information obtained, and a confidence estimate based on these authentication results. In this way, the system provides centrally managed information on who is present at the facility, their current location, and confidence estimate (degree of suspicion).

MULTI-PERSPECTIVE SEARCH

Information needs to be assessed rapidly when an incident occurs in order to minimize damage and prevent any further criminal activity. This requires an ability to quickly retrieve the necessary information from the large amounts of image data collected by surveillance cameras. There was also a recognized need for general-purpose search functions able to utilize fragmentary and diverse information from witness reports as search keys. In response, Hitachi has developed a technique for searching collected video based on attributes such as a person's clothing or movements. This is called "multi-perspective search." Fig. 5 shows an example screen.

In addition to comparing facial images, the multi-perspective search also considers the color of the head, mouth, upper body, lower body, and hand luggage, and the route traveled. For example, it is possible to search for a person wearing a blue shirt and black trousers and carrying a green bag on their back, and who passed through a corridor. This works by tracking a person in the collected image data and using the results to register the characteristics of each partial image in the search engine. The colors of each part are then specified to the search engine as keys so that it can search for images that contain the matching colors. The route traveled by the person (obtained by the tracking function) is also registered in the search engine and linked to the corresponding images. When the operator requests a search using a particular route as a key, the search engine returns video for the similar route. This makes it possible to conduct an investigation using a variety of information provided by witnesses by combining these search results.

CONCLUSIONS

This article has described traceable physical security systems for a safe and secure society, and multi-perspective search.

The use of more sophisticated physical security systems is seen as having potential for helping

prevent terrorism and serious criminal activity. To meet this demand, Hitachi has implemented traceable physical security systems that combine unconscious authentication, detection systems, and other components, and also multi-perspective search, which can perform a diverse variety of searches on collected video. Hitachi intends to continue trialing these prototypes with a view to their commercialization. Among the challenges facing security systems are those of privacy and information leaks. In the future, Hitachi also plans to incorporate information protection technologies and to formulate strict operational rules to ensure that these problems do not arise in actual operation.

REFERENCES

(1) Hitachi News Releases, "Development of Technology for Selective Display of High-priority Images from Multiple Networked Cameras, with High-speed Search for Similar Images in a Database" (Feb. 2008), http://www.hitachi.co.jp/New/cnews/month/2008/02/0201.html in Japanese.
(2) Hitachi News Releases, "Development of Explosives Detection Technology to Automatically Detect Explosive Substances Adhering to Carry-on Luggage" (Sep. 2013), http://www.hitachi.com/New/cnews/130925a.html

ABOUT THE AUTHORS

Tatsuhiko Kagehiro, Ph.D.
Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of image processing and recognition technology. Dr. Kagehiro is a member of The Institute of Electronics, Information and Communication Engineers (IEICE), the Information Processing Society of Japan (IPSJ), and the Auditory and Visual Information Research Group (AVIRG).

Harumi Kiyomizu
Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. She is currently engaged in the research and development of image processing and recognition technology. Ms. Kiyomizu is a member of the IEICE.

Yohei Kawaguchi
Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in research into signal processing. Mr. Kawaguchi is a member of the IEEE, the IEICE, and The Acoustical Society of Japan.

Hisashi Nagano
Medical Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of mass spectrometry. Mr. Nagano is a member of The Japan Society for Analytical Chemistry and the Japan Explosives Society.

Kenichi Yoneji
Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of image processing and recognition technology. Mr. Yoneji is a member of the IEICE and The Institute of Image Information and Television Engineers.

Yuki Watanabe, Dr. Info.
Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of similar image search technology.

Zisheng Li, Dr. Eng.
Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of medical image processing and pattern recognition technology. Dr. Li is a member of the IEICE.

Yusuke Matsuda
Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd. He is currently engaged in the research and development of image recognition and biometric authentication technology. Mr. Matsuda is a member of the IEICE.

Featured Articles

Facility Monitoring Services for More Efficient Maintenance of Social Infrastructure

Masaki Ogihara
Masafumi Uematsu
Daisuke Shibata
Sachio Minami

OVERVIEW: Japan's social infrastructure underwent rapid development during the period when the economy was growing strongly. The aging of this infrastructure has now become an issue, with a need to reduce the lifecycle costs of facilities while still delivering safe and secure services to users. Facility monitoring services include condition monitoring, which uses M2M technology to collect data from sensors and other sources, and predictive diagnosis, which uses data mining techniques to analyze this collected data. The benefits of these services include the early detection of anomalies at facilities that use these services and preventive maintenance for aging facilities. They also facilitate management of the lifecycle of social infrastructure to extend its life and reduce total costs.

INTRODUCTION

THE construction of roads and bridges, public buildings, and various other forms of infrastructure proceeded at a rapid pace throughout Japan during the period starting about 50 years ago in the 1960s when Japanese economy was growing strongly. Since then, although this infrastructure has undergone earthquake-strengthening and other measures to make it more resilient to disasters, what to do about the widespread aging of social infrastructure remains an important issue. However, given the difficulty of financing the construction of replacement infrastructure, there is a need to ensure that users are kept safe and secure from threats such as disasters or accidents happening at existing facilities.

The operation and maintenance of social infrastructure is generally based on corrective maintenance, which means performing periodic inspections that are primarily conducted visually, and then following these up with more detailed investigations or repairs if any problems are found. However, in addition to supplying safe and secure services to their users, infrastructure operators also face the challenge of how to reduce the lifecycle cost of facilities. To overcome this challenge, it will be important for future facility management to implement preventive maintenance, which differs from the corrective maintenance of the past in that it performs repairs after obtaining an accurate understanding of the condition of the facility.

An essential requirement for implementing preventive maintenance will be the effective combination of technologies and know-how comprising information and communication technology (ICT), data analysis, and engineering to perform inspections more efficiently and to obtain more accurate assessments of the condition of facilities. There is also growing demand for one-stop services provided in the form of systems (see Fig. 1).

In response, Hitachi has launched a new business offering cloud-based, one-stop facility monitoring services that provide machine-to-machine (M2M)[*1] technologies for data collection using sensors and radio-frequency identification (RFID), big data technologies for analyzing the collected data,

*1 Systems in which machines exchange information directly via a network, without human intervention.

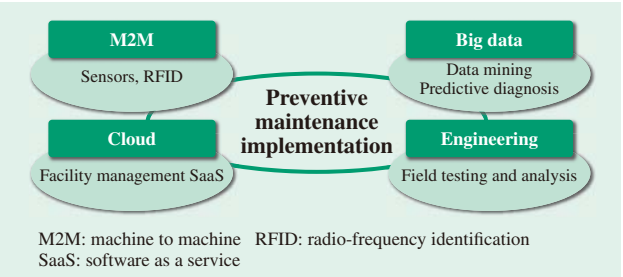


Fig. 1—Technologies Used to Implement Preventive Maintenance.
There is growing demand for one-stop services that provide the technologies and know-how required to implement preventive maintenance.

and engineering know-how built up through past experience.

This article gives an overview of Hitachi's facility monitoring services, and describes their features, example applications, and future developments.

OVERVIEW OF FACILITY MONITORING SERVICES

Hitachi launched its facility monitoring services in October 2013. Targeted primarily at roads, railways, water supply and sewage systems, and dams, they are provided through Intelligent Operations for Facilities, one of a range of services provided by Hitachi's smart information business.

The two services being offered are a condition monitoring service that uses M2M technology for the efficient collection of sensor data and provides realtime access to information on status changes at facilities, and a predictive diagnosis service that uses data mining technology to analyze the collected data.

FEATURES OF FACILITY MONITORING SERVICES

The facility monitoring services have the following four features (see Fig. 2).

(1) Use of a variety of sensors to detect status changes at facilities

Sensors for measuring parameters such as characteristic frequency or angle of tilt are selected to suit the specific requirements of the social infrastructure being monitored. They are then installed at the facility to measure and assess its soundness in various different ways.

(2) Use of wireless devices (RFID) for data collection

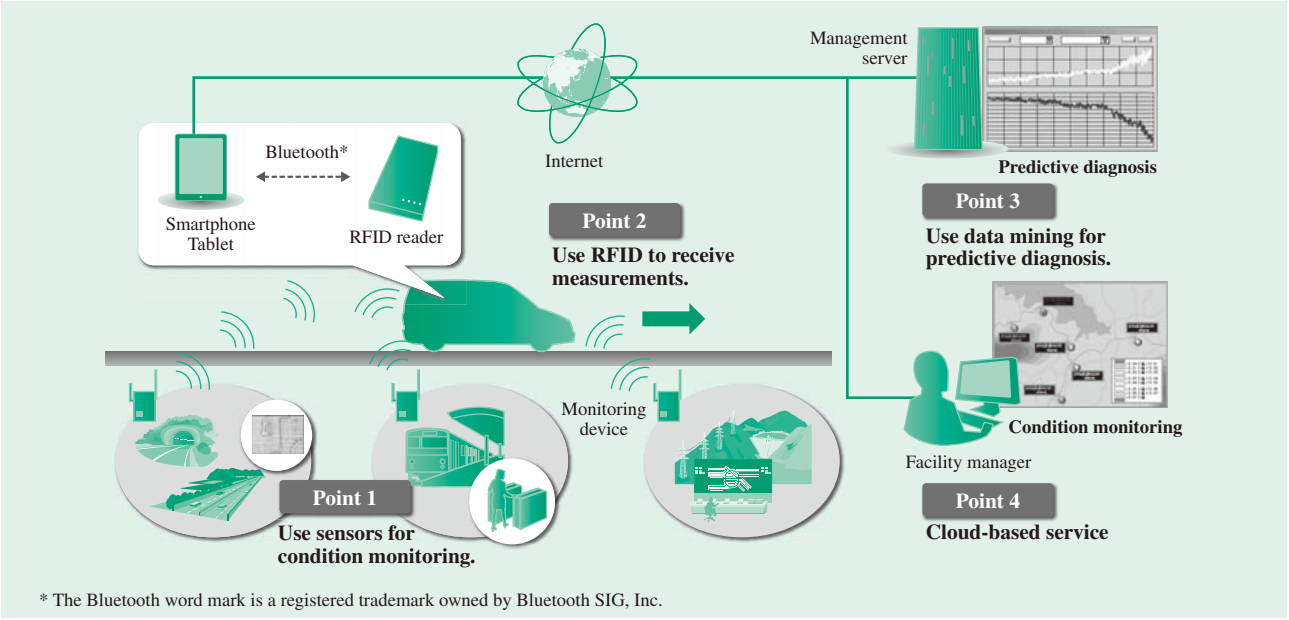
RFID can be used to receive measurement data from sensors remotely or when moving at high speed. The data can also be forwarded to a server in realtime via devices such as smartphones or tablets.

(3) Use of data mining for predictive diagnosis

Hitachi uses data mining techniques it has developed itself to supply a predictive diagnosis service that uses collected sensor data as a basis for learning what constitutes normal conditions and for identifying correlations with abnormal events. By analyzing changes at a facility, the service can diagnose symptoms of aging or other anomalies.

(4) Provision as a cloud-based preventive maintenance service

This is a condition monitoring service that manages collected data based on facility records to provide functions such as the archiving of monitoring data and alarm generation when a change occurs. This can provide early identification of risks to a facility by the realtime detection of changes at the facility when a disaster or accident occurs (such as a rockfall or landslide).



* The Bluetooth word mark is a registered trademark owned by Bluetooth SIG, Inc.

Fig. 2—Features of Facility Monitoring Services.
Hitachi cloud services utilize sensors, RFIDs, and other M2M technologies to monitor equipment and other facilities and assess their condition.

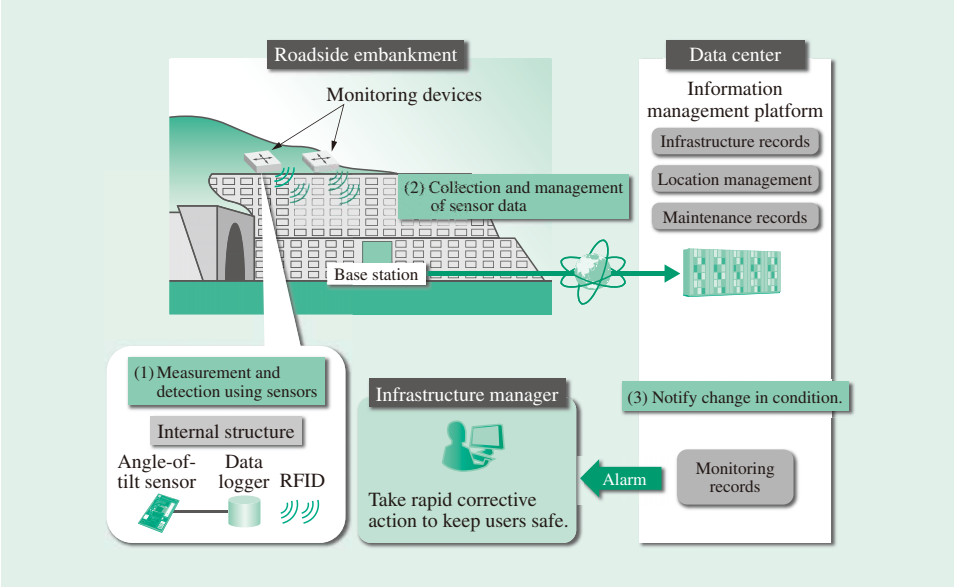


Fig. 3—Example of Condition Monitoring Service.
This example is for a roadside embankment. The condition monitoring service monitors for situations such as landslides and issues realtime alarms.

EXAMPLES OF FACILITY MONITORING SERVICES

As noted above, the facility monitoring services include condition monitoring and predictive diagnosis. The following sections describe examples of each of these taken from the highway management sector.

Example Condition Monitoring Service

Utilizing sensors, RFIDs, and other M2M technologies for the efficient collection of data, the condition monitoring service facilitates a rapid response to rarely occurring accidents or disasters, such as rockfalls or landslides, by monitoring the condition of social infrastructure and providing early detection of events such as these.

The example below describes how the service is used for an embankment built as part of road construction (see Fig. 3).

As shown in Fig. 3, angle-of-tilt sensors are installed at various points on the embankment to make periodic measurements of any changes in its shape. At locations where the installation of fixed-wire sensors would be impractical, or where road rules or other regulations would result in increased costs, RFID is used to transmit measurements to a base station. The data is then kept on a server to which it is forwarded in realtime via an existing fixed-wire network. If the server detects that a measurement has exceeded a predefined threshold, an alarm is sent to the person responsible via e-mail or some other method. This gives the person a chance to take prompt corrective action to prevent a rockfall or landslide.

Example Predictive Diagnosis Service

The predictive diagnosis service supports more sophisticated lifecycle management of social infrastructure to help extend its life and reduce total costs. It analyzes data collected by a variety of different methods, including the condition monitoring service, to provide the information required to assess the soundness of social infrastructure or other equipment and to detect any anomalies.

One example is the potential for detecting signs of problems on jet fans (which are used in highway infrastructure) by fitting them with characteristic frequency sensors and analyzing the collected data to determine their condition.

The system uses characteristic frequency sensors to measure the condition of blades (or bearings), ceiling mountings, and other components on jet fans that are installed inside tunnels to provide ventilation. This data is then collected via an RFID reader and smartphone in an inspection vehicle that makes routine visits to the site. The data is sent via the telephone network to a server for storage. At the server, data mining techniques are used to compare the measurements with data from normal operating conditions collected when the service first commenced and detect signs of problems from anomalous data or event intervals. Based on the results of this comparison, the idea is to take steps to counteract the aging of the jet fans and reduce lifecycle costs by making repairs or taking other remedial measures before parts deteriorate with age or problems arise due to fittings coming loose (see Fig. 4).

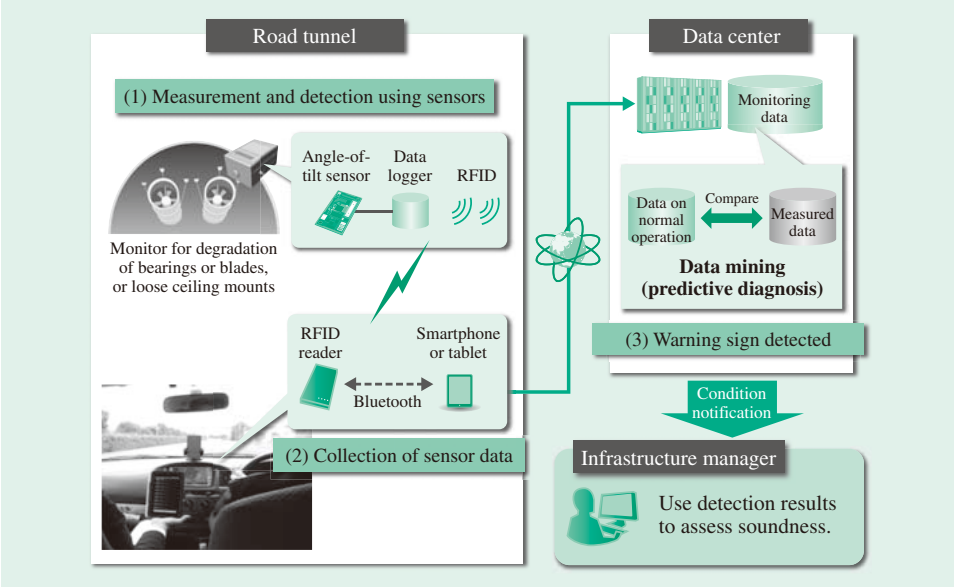


Fig. 4—Example of Predictive Diagnosis Service.
In this example, a vehicle makes routine visits to collect sensor measurements. The predictive diagnosis service uses data mining techniques developed by Hitachi to detect warning signs of aging or other deterioration.

Examples of Sensors and What they are Used to Measure

To provide condition monitoring and predictive diagnosis, the facility monitoring services select the sensors that best suit the social infrastructure being monitored.

As condition monitoring is used for structures such as embankments, road signs, or railway tracks that require realtime detection of changes triggered by an accident or other disaster, suitable sensors are likely to include those for measuring angle of tilt or anchor loads.

Similarly, as predictive diagnosis is used for structures such as jet fans or bridges that require follow-up observation or the detection of deterioration due to age by measuring long-term changes in their condition, suitable sensors are likely to include characteristic frequency and strain gauges.

Current system development work for facility monitoring services is focused on sensors for which there is strong demand, including those for measuring angle of tilt and characteristic frequency (see Fig. 5).

FUTURE DEVELOPMENTS

Based on past experience, the initial deployment of facility monitoring services is in the highway management sector. Hitachi also aims to deploy the services for Japanese local government road maintenance, where there is a need for efficiency improvements; for the maintenance of other types of social infrastructure with similar requirements; and overseas.

Deployment in Other Fields

Hitachi intends to expand the range of sensors supported by its facility monitoring services beyond those already mentioned. As a low-cost alternative to the expensive standalone systems used in the past, and with the ability to perform centralized monitoring of multiple sites, these cloud-based services are expected to be increasingly used for applications such as highway management by local government. When considering the operation and maintenance requirements shared by infrastructure such as bridges, tunnels, levees, dams, and airports, a committee studying the use of monitoring

Condition monitoring service

Realtime notification of changes detected when an accident or other disaster occurs.

Measurements	Events detected	Sensors used
Embankment	Monitor for landslides	Angle of tilt, rain gauge
Embankment (anchors)	Tensile forces on earth anchors, failures	Anchor load cells
Signs, streetlights	Collapse or fatigue failure of columns	Angle of tilt, characteristic frequency
Railway track	Deformation, subsidence, or listing of rails	Angle of tilt, settling

Predictive diagnosis service

Take measurements of long-term changes in condition and use to detect anomalies or deterioration due to age.

Measurements	Events detected	Sensors used
Jet fans	Deterioration or loosening of mountings	Characteristic frequency
Bridges (bracing, etc.)	Tensile forces in bracing	Characteristic frequency, tensile force
Bridges (piers)	Management of scouring	Characteristic frequency
Joints	Couplings coming loose	Strain gauge

Fig. 5—Example of Sensors Used.
Different sensors are used depending on what is to be measured and what conditions are being looked for.

technology for social infrastructure led by the Ministry of Land, Infrastructure, Transport and Tourism has highlighted the importance of inspecting sites that are (1) difficult to inspect visually or (2) difficult to access.

Hitachi believes that the solution to these issues lies in one of the features of its services, namely the use of wireless data collection. In the case of railways, for example, where special-purpose vehicles are used to take measurements to check for the warping of rails or faults in signaling or other equipment, Hitachi believes that monitoring techniques that combine sensors and wireless devices will be useful for sites such as the undersides of bridges that cannot be inspected visually.

Along with more efficient working practices and improved safety, the advantages of using facility monitoring services to perform more sophisticated operation and management are also expected to include benefits to management. In the case of the equipment used in industries such as steel or chemicals, there is also the risk of interruptions to production resulting from the failure of aging equipment. However, if the use of data mining techniques for predictive diagnosis makes it possible to repair the equipment before the deterioration manifests, this risk can be avoided and the life of plants extended (reducing operation and maintenance costs).

Overseas Applications

While the focus for facility monitoring services in Japan has been on measures for dealing with aging infrastructure, there is also scope for its use overseas on newly constructed facilities, particularly in emerging nations.

Sensor installation is less costly if done during construction. Hitachi also anticipates that measuring a facility under normal conditions before it enters use will allow its soundness to be assessed with greater certainty after it becomes operational.

Solutions that are unique to Hitachi, with its fusion of IT and infrastructure technologies, will have extensive applications in emerging economies, not only in infrastructure such as roads and railways, but also in water treatment plants, industrial equipment, and other facilities.

CONCLUSIONS

This article has given an overview of Hitachi's facility monitoring services, and described their features, example applications, and future developments.

Use of sensors, RFIDs, and other Hitachi M2M technologies has expanded the scope for collecting large volumes of measurement data that would have been difficult to obtain in the past. Furthermore, linking the cloud, big data, and various other technologies together with products and services has created solutions that only Hitachi, with its fusion of IT and infrastructure technologies, can deliver.

With its facility monitoring services, Hitachi believes it can contribute to creating safe and secure societies, not just through its business know-how built up from past experience in the social infrastructure sector, but also by seeking new applications for its services in the global market.

REFERENCE

(1) Hitachi Facility Monitoring Services, http://www.hitachi.co.jp/products/it/traceability/service/monitoring_service.html in Japanese.

ABOUT THE AUTHORS

Masaki Ogihara
Security Services Department, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in overall management of facility monitoring services.

Masafumi Uematsu
Security Services Department, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in management of software design and development for facility monitoring services.

Daisuke Shibata
Security Services Department, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in management of hardware design and development for facility monitoring services.

Sachio Minami
Security Services Department, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in design and development of the overall architecture and applications for facility monitoring services.

Featured Articles

Trends in Cybersecurity and Latest Countermeasures

Satoshi Takemoto
Makoto Kayashima, Ph.D.
Kunihiko Miyazaki, Ph.D.
Yasuko Fukuzawa, Ph.D.

OVERVIEW: For the IT systems that underpin social infrastructure, advances are taking place in the fields of information systems, industrial control systems, and cyber-physical systems that are based on the high-level integration of these information and control systems. On the other hand, unauthorized access is becoming increasingly sophisticated and extensive, with even industrial control systems that were once considered secure against these threats now being exposed to serious cyber-attacks. Hitachi supplies a comprehensive range of cybersecurity, including information security solutions provided by Hitachi and managed security services, security for industrial control systems that is also intended for cyber-physical systems, incident response by Hitachi Incident Response Team, and malware analysis for preventing targeted attacks and other evolving threats. Hitachi is also working on advanced research and development aimed at ensuring safe and secure social infrastructure.

INTRODUCTION

IN recent years, there have been rapid advances in information technology (IT) systems, particularly in the fields of cloud computing and mobile digital devices, therefore cybersecurity technologies are playing an increasingly important role. While the spread of cloud computing is bringing benefits such as the on-demand availability of extensive resources, there are concerns such as data leaks or unauthorized access by cloud system administrators. In the case of cyber-physical systems that combine information and control systems, while these are opening up the prospect of new social infrastructure developments such as smart grids or smart cities, cyber-attacks on industrial control systems that were once considered secure against these threats are revealed. Reported examples include the Stuxnet malware that infiltrates industrial control systems and causes control devices to behave abnormally, and unauthorized access to automotive embedded systems, medical devices, or other equipment that poses a risk to human life. One way of going about this has been the use of social engineering whereby attacks take advantage of people's psychological vulnerabilities or mistakes to inflict damage.

Meanwhile, supply chains being established for things like parts procurement or the development of IT systems and the products used to build them are increasingly taking advantage of open technologies and commercial off-the-shelf products, and of trends such as globalization. This raises the problem of how to ensure security throughout the supply chain when the development and management related to security is performed by both local and overseas suppliers.

Given these developments, Hitachi is working to supply comprehensive services, products, and technologies related to cybersecurity. Specific examples include information security solutions provided by Hitachi[(1)], which supply products ranging from consulting to security measures and operational services; a managed security service; security for industrial control systems that is also intended for cyber-physical systems; incident response and countermeasures against the vulnerabilities of products and solutions by the Hitachi Incident Response Team (HIRT); and multi-environment dynamic analysis systems for the automatic analysis of environment-dependent malware (please refer to other Hitachi publications for more information about these).

This article describes advanced research and development being undertaken with a view to its use in security services and products supplied by Hitachi, including a security verification technique that uses formal methods, technologies for implementing secure cloud computing environments, and security evaluation techniques for embedded systems.

SECURITY VERIFICATION TECHNIQUE USING FORMAL METHODS

Formal methods are techniques based on mathematical logic that are used to mechanically verify that programs or other specifications do not contain defects or inconsistencies. There is particular interest in formal methods in fields that require high levels of safety and reliability, with their use in development recommended by international standards in industries such as aviation, railways, or automobiles, for example. Hitachi's involvement in the field includes the release of software[(2)] that supports the efficient use of formal methods, and research and development of formal verification techniques for automotive control software[(3)].

A feature of formal methods is their ability to demonstrate comprehensively that no defects are present within a particular scope. This makes the technique valuable for security verification where there is a need to guarantee safety even under conditions where it is not known what sort of people will attempt an attack. A typical example of a security verification technique that uses formal methods would be one used to verify the safety of a cryptographic protocol.

Cryptographic protocols provide a way of establishing secure communication by combining a variety of cryptographic functions (including encryption and electronic signatures). Examples include Transport Layer Security (TLS) and the Security Architecture for the Internet Protocol (IPsec). These play an essential role in maintaining the security of Internet and various other communications.

Verifying that a cryptographic protocol is secure is not easy. While the individual cryptographic functions (components) that make up the protocol must themselves be secure, this on its own is insufficient.

The following shows the procedure for the Needham–Schroeder public-key protocol for sharing keys.

(1) A → B: $\{Na, A\}_{Kb}$
(2) B → A: $\{Na, Nb\}_{Ka}$
(3) A → B: $\{Nb\}_{Kb}$

Here, N*x* is a random number generated by agent X, K*x* is the public key belonging to X, and $\{\cdot\}_{Kx}$ means to encrypt the data enclosed in parentheses using K*x*.

Executing the protocol using this procedure results in the secret exchange of keys Na and Nb between A and B. This protocol had been believed to be secure for nearly 20 years after it was first proposed in 1978. In 1996, however, Gavin Lowe found that a man-in-the-middle attack involving someone intercepting the communications between A and B could discover Na and Nb. This attack could be achieved without breaking the $\{\cdot\}_{Kx}$ encryption function used as a component of the protocol.

Even for a comparatively simple specification like this one, the difficulty of verifying the security of the protocol arises because it operates in parallel between a number of agents and in a non-deterministic way. It is typically difficult to check all possible situations without overlooking or omitting any.

In his research into the above attack, Lowe used a formal method tool (model checker) called failures-divergence refinement (FDR) to confirm the attack and verify the security of the updated protocol. A number of verification methods and tools based on formal methods such as model checking and theorem proving have been developed or proposed, and work is progressing on assessing the security of protocols in actual use such as WiMAX[*1] or European standards for railway communications.

Meanwhile, the interrelationships between verification methods and tools for cryptographic protocols that use these formal methods are not always well understood, and it has not been clear how the results of assessment should be interpreted in practice.

In response, Hitachi has since 2006 been involved in the international standardization of security assessment for cryptographic protocols. As a result of Hitachi's work as project editor of ISO/IEC JTC 1/SC 27/WG 3 in conjunction with partners such as the National Institute of Information and Communications Technology (NICT) and the National Institute of Advanced Industrial Science and Technology (AIST), the ISO/IEC 29128 standard (Verification of Cryptographic Protocols) was published in 2011. This standard specifies the common items required to be described when assessing a protocol (the protocol specification, intruder model, security requirements, and self-assessment). It also defines four protocol assurance levels (PALs) that indicate the degree of verification: PAL1 (informal argument), PAL2 (formal paper-and-pencil proof), PAL3 (tool-aided bounded verification), and PAL4 (tool-aided unbounded verification).

In December 2013, NICT, Hitachi, Ltd., KDDI R&D Laboratories, Inc., and Nippon Telegraph and Telephone Corporation (NTT) established the

*1 WiMAX is a trademark or registered trademark of the WiMAX Forum.

"Cryptographic Protocol Evaluation toward Long-lived Outstanding Security" (CELLOS) consortium for cryptographic protocol evaluation technology[4]. The consortium aims to encourage the wider adoption of secure cryptographic protocols through the international collection and dissemination of reliable information on the security of cryptographic protocols, discussion about information and communication technology (ICT) systems, and the publishing of security information resulting from these activities. This will include participation by universities, research institutions, and interested companies from Japan and other countries so that activities can be undertaken through an international cooperative framework that extends beyond Japan.

TECHNIQUES FOR IMPLEMENTING SECURE CLOUD COMPUTING ENVIRONMENTS

The use of cloud computing provides numerous benefits, including on-demand access to extensive resources. However, because users who store their data in the cloud are not able to check the cloud systems themselves, they need some other way to protect against information leaks due to people (including possibly system administrators) accessing their data without authorization. In response, Hitachi is researching and developing technologies based on encrypted data such as electronic signatures using biometric data and privacy-preserving information processing.

Electronic Signature Technology Using Biometric Data

Conventional authentication enhanced techniques have included the use of hardware tokens such as smartcards and the use of public key infrastructure (PKI). While these help improve security, there are problems in terms of inconvenience and of poor cost-benefit. Another problem with the conventional techniques is that they have used anti-tampering devices such as smartcards or have been based on a centralized model that requires strict management of authentication data. In response, Hitachi has developed a public biometrics infrastructure (PBI)[5] that uses public templates*2. PBI works by converting the biometric templates into a form from which the original data cannot be recovered, thereby making it secure for the data to be published without risk to privacy, but still allowing it to be used for purposes such as authentication or electronic signatures (see Fig. 1).

*2 This technology incorporates results from the "R&D on Cloud Security Technologies for Disaster Preparedness and Emergency Response" project sponsored by the Ministry of Internal Affairs and Communications.

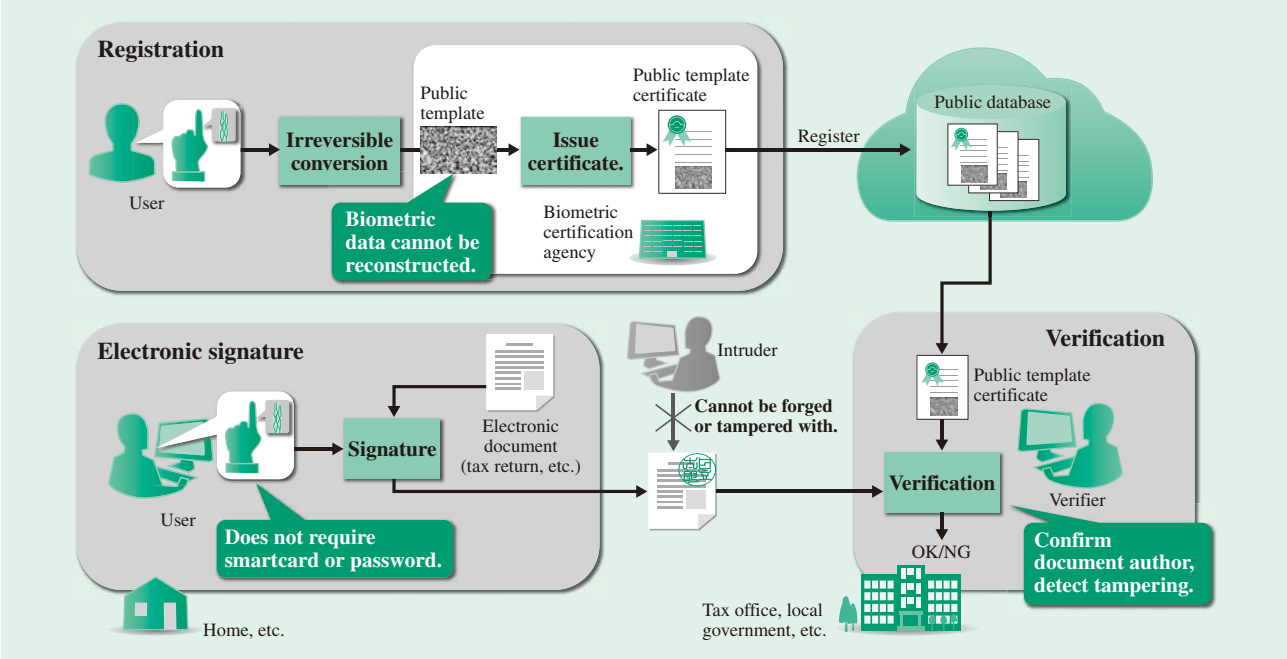


Fig. 1—Biometric Authentication Platform with Public Templates.
The platform facilitates the migration of payment, e-government, and other systems that require strict user authentication to the cloud, and the linking of identities (IDs) across other related systems at low cost.

Using a new electronic signature scheme that tolerates errors in the private key, PBI can verify (authenticate) a signature using error correction and an appropriate threshold setting provided the error in the analog data that is invariably generated each time the biometric data is retrieved is within a given range. Because it is not possible to recover the original biometric data from the public key (public template) used to verify the electronic signature, anyone can perform signature verification (authentication) without risk of the biometric data being leaked or forged. Furthermore, by reducing the security of the newly developed scheme to that of the Waters signature*3 scheme, the security of which has already been proved mathematically, it has been proven that the Hitachi scheme cannot be broken by any form of attack.

Use of this scheme makes it possible to implement systems that require strict user authentication (such as payment or e-government systems) on the cloud, and to link identities (IDs) across other related systems at low cost.

Technologies for Privacy-preserving Information Processing

Data encryption has commonly been used to ensure the confidentiality of the data used by a system. However, because the data needs to be decrypted for use, this provides an opportunity for system administrators, malware, or others to read the data.

To minimize this risk, Hitachi has developed an encryption technique[6] that supports fast searching*4 (see Fig. 2). The technique achieves efficiency based on common-key encryption, and ensures high security that allows comparisons of encrypted data to be performed using homomorphic encryption.

Hitachi has also utilized this technique to develop and commercialize a privacy-preserving analysis technique[7] that can obtain the frequencies with which a number of keywords appear in an encrypted database, and then compare these to find correlation rules.

SECURITY EVALUATION TECHNIQUES FOR AUTOMOTIVE EMBEDDED SYSTEMS

In recent years, networks, devices, operating systems (OSs), and other components that are widely used in IT have also started to find uses in automotive and other embedded systems. Accordingly, the importance of countermeasures against cyber-attacks is also growing in this field. Examples have already been demonstrated in which automotive embedded systems are manipulated remotely via a network. Because attacks on vehicles have the potential to put human life at risk, there is a need to offer automotive security at an early stage.

In Europe, which has led the way in the study of automotive security, the 7th Framework Programme for Research and Technological Development (FP7) has proposed standards for hardware security modules (HSMs) and has also embarked on an investigation into the security evaluation in automotive embedded systems that incorporate HSMs.

*3 A digital signature scheme proposed by Brent Waters in 2005. The scheme has been shown to fulfill the requirements of EUF-CMA (probability of existentially unforgeable under chosen-message attacks), a widely accepted definition of the security of electronic signature schemes, under the Computational Diffie-Hellman (CDH) assumption (a mathematical assumption).

*4 This technology incorporates results from the "R&D on Cloud Security Technologies for Disaster Preparedness and Emergency Response" project sponsored by the Ministry of Internal Affairs and Communications.

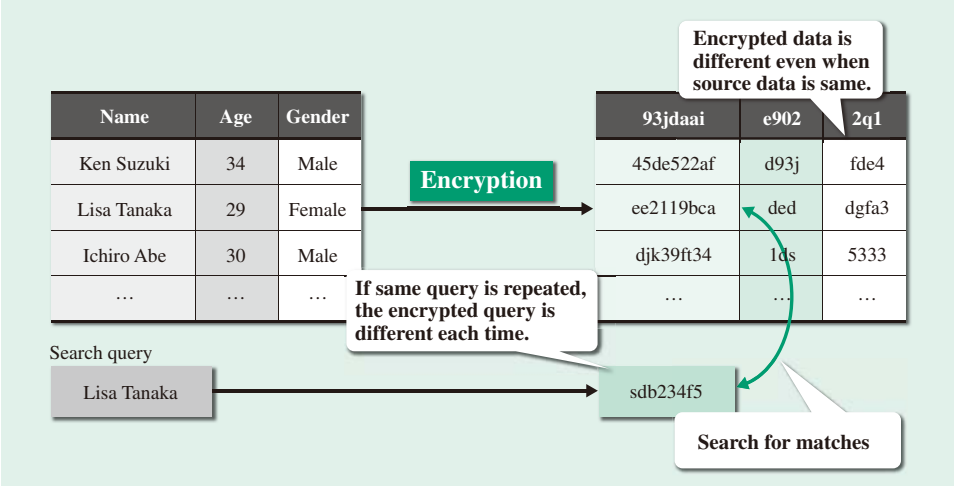


Fig. 2—Features of Searchable Encryption Technique. The technique combines common-key encryption and homomorphic encryption to achieve both high speed and security.

Accordingly, Hitachi has applied security evaluation techniques based on the safety analysis techniques for plants it developed during the 1980s to automotive embedded systems. In Japan, Hitachi is participating in the standardization of security evaluation techniques and has proposed methods for threat analysis and risk assessment.

The following sections describe the threat analysis and risk assessment methods that form the core of these security evaluation techniques for embedded systems for vehicles.

Definition of Target System of Evaluation

Security threats can be described in terms of, "which threat agents exist, and what adverse action they perform on which assets" in the target system of evaluation.

In addition to information, which has conventionally been treated as an asset to be protected, the assets in automotive embedded systems also include embedded system firmware and the functions that control mechanisms such as the engine or brakes. A system model is produced from the nature of the assets and from data flow diagrams that specify data flows in relation to these assets.

The threat agents are those people involved at any point along the lifecycle of a vehicle, which includes its manufacture, its use by the owners who purchased the vehicle new or second-hand, and ultimately its disposal. This is because confidential information held by automotive embedded systems is stored and accessed not only during the normal usage phase but also at other phases such as during manufacturing, delivery, or servicing.

With respect to what adverse actions are performed (the threats), all of the things that can happen for each entry point are studied, and are also considered in terms of types of failure called confidentiality, integrity, or availability that can occur for each type of asset. For example, it is important that the functions of an automotive IT system operate as correctly as expected, and failure of integrity or availability must be prevented. Similarly, it is important that the information exchanged between central servers and vehicle-mounted intelligent transport system (ITS) devices is protected from disclosure and modification, and failure of confidentiality or integrity must also be prevented.

Identification of Threats

For the target of evaluation, the threats are identified from four perspectives (see Table 1).

By applying to these perspectives, the system model, lifecycle, and adverse actions, which are studied in defining the target system of evaluation described in the previous section, it can be exhaustively identified what threat agents exist and what adverse action they perform on which assets at what phases.

Risk Assessment

The risk that threats pose to an IT system has been typically assessed by deriving from the value of the assets and the attack cost, which depends on how the threats are carried out. This is an effective approach when there are numerous examples of attacks, and a consensus can be reached about the cost of the attack method, including factors such as the execution time needed to undertake the attack and the capabilities of the person launching it.

In the case of automotive embedded systems, while a number of example attacks have been identified at the research level, there is not the same wide range of attack method variations that exist for IT systems. As a consequence, we consider that it is difficult to estimate the cost of attack methods. Therefore, Hitachi has developed a threat risk assessment method that is based on the common vulnerability scoring system (CVSS) used to score the severity of IT system vulnerabilities.

This method assigns an asset value to each asset in terms of confidentiality, integrity, and availability and then it calculates a score for risk from the degree of ease in mounting an attack, which is derived from the metric that reflects how close the threat agents need to get to the assets and from the existence of barriers that they break through to access to them. Even in cases such as automotive embedded systems where there is a lack of accumulated know-how about security threats, the method can calculate a risk value analytically from the definitions of the threats and the system of evaluation. It can also incorporate consideration of factors such as risk to life into the risk assessment by treating functions as assets and, for the purpose of

Table 1. Perspectives for Identification of Threats
The system model, lifecycle, and adverse actions, which are studied in defining the target system of evaluation, are applied to these perspectives.

Perspective	Explanation
Where	Identify entry points for attacks.
Who	Identify threat agents.
When	Identify lifecycle phases for attacks.
What	Identify adverse actions.

valuation, raising the estimated asset value in the case of functions for which loss of integrity or availability has serious consequences.

CONCLUSIONS

This article has described developments in the field of cybersecurity for the IT systems used to support social infrastructure, and advanced research and development being undertaken with reference to these.

In the future, Hitachi intends to continue contributing to the provision of safe and secure social infrastructure by supplying new security solutions and developing technologies for use in these solutions.

REFERENCES

(1) Hitachi Secureplaza Security Solution, http://www.hitachi.co.jp/Prod/comp/Secureplaza/index.html in Japanese.
(2) Hitachi News Releases, "Release of Highly Reliable and Efficient Software Development Technology for Social Infrastructure" (Feb. 2013), http://www.hitachi.com/New/cnews/130212a.html
(3) Hitachi News Releases, "Development of Highly Reliable Verification Technology for Automotive Control Software Using Formal Methods" (Apr. 2013), http://www.hitachi.co.jp/New/cnews/month/2013/04/0416a.html in Japanese.
(4) Hitachi News Releases, "Establishment of Cryptographic Protocol Evaluation Toward Long-Lived Outstanding Security (CELLOS) Consortium" (Dec. 2013), http://www.hitachi.com/New/cnews/131219b.html
(5) Hitachi News Releases, "Successful Development of Biometric Digital Signature Technology" (Feb. 2013), http://www.hitachi.com/New/cnews/130218.html
(6) Hitachi News Releases, "Searchable Encryption Technology Supporting the Prevention of Information Leakage on Cloud Systems" (Mar. 2012), http://www.hitachi.co.jp/New/cnews/month/2012/03/0312.html in Japanese.
(7) Hitachi News Releases, "Development of Privacy-preserving Analysis Technology for Analyzing Data in Encrypted Form" (Jan. 2014), http://www.hitachi.co.jp/New/cnews/month/2014/01/0121b.html in Japanese.

ABOUT THE AUTHORS

Satoshi Takemoto
Advanced Cybersecurity Technology Department, Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in the creation and launch of a new security business.

Makoto Kayashima, Ph.D.
Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research on information security. Dr. Kayashima is a member of the Information Processing Society of Japan (IPSJ), The Institute of Electronics, Information and Communication Engineers (IEICE), and The Japanese Society for Artificial Intelligence.

Kunihiko Miyazaki, Ph.D.
Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research on formal methods and information security. Dr. Miyazaki is a member of the IPSJ and the IEICE.

Yasuko Fukuzawa, Ph.D.
Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd. She is currently engaged in research on information security and cryptography. Dr. Fukuzawa is a member of The Institute of Electrical Engineers of Japan (IEEJ), IPSJ, and IEICE.

Featured Articles

Trends in Security Incidents and Hitachi's Activities
—About HIRT Activities—

Masato Terada, Dr. Eng.
Masashi Fujiwara
Akiko Numata
Toru Senoo
Kazumi Ishibuchi
Mari Miyazaki

OVERVIEW: As cyber-attacks continue to evolve, the types of security incident they trigger are becoming more diverse. They are also having an increasingly significant impact on social infrastructure that has been built using the Internet on a platform of information or control systems. This has raised the importance of measures for dealing with these incidents, including the establishment of CSIRTs and handing down of techniques. The HIRT is a CSIRT team that handles incident operations throughout Hitachi. Through vulnerability countermeasures (work aimed at eliminating vulnerabilities that threaten cybersecurity) and incident response (work aimed at defending against and resolving cyber-attacks when they occur), the HIRT plays a leading role in cybersecurity at Hitachi.

INTRODUCTION

SOCIAL infrastructure that has been built using the Internet on a platform of information or control systems faces new threats that need to be defended against through an ongoing combination of both vulnerability countermeasures and incident response. The Hitachi Incident Response Team (HIRT) operates throughout Hitachi, helping ensure the safety of customers and the public and the provision of reliable social infrastructure by preventing security incidents that could potentially result from new threats, and by responding quickly when an incident does occur.

This article describes recent trends in security incidents, and Hitachi's cybersecurity incident readiness/response team (CSIRT) activities in which the HIRT Center plays a central role.

TRENDS IN SECURITY INCIDENTS

Cyber-attacks have continued to evolve since the VBS/Loveletter virus of 2000, with the vulnerabilities exploited by these attacks expanding beyond operating systems to also include applications. Malware is also evolving by building on past techniques, which include malware-attached e-mail, network worms, and bots. In addition, web malware (such as Gumblar) and USB malware, attacks that exploit vulnerability in the Internet users' psychology and behavior and use it for advantage, have become common since around 2008.

Targeted attacks such as advanced persistent threats (APTs) have been raising concerns since 2010, and have been utilized for objectives that go beyond the theft of information. The Stuxnet malware spread in July 2010 targeted nuclear power facilities and disrupted the operation of control equipment by accessing it via data acquisition [supervisory control and data acquisition (SCADA)] software[(1)].

The features of 2013 in terms of incidents were that website compromised actions became regular occurrences and damage by malicious programs that targeted online banking became serious. In particular, these cyber-attacks on websites form part of a category of targeted attacks called "watering hole attacks." These involve tampering with websites that are highly likely to be used by the organization being targeted, using these sites as a lure in the same way animal predators take advantage of a watering hole to lure prey (see Fig. 1).

The attack works by redirecting users of the lure website to another website that contains the malware, making it technically similar to the methods used by other web malware such as Gumblar that also redirects users to a different website. Other methods include list attacks that utilize lists of account information to attempt login to many different sites, and domain name system/service (DNS) and network time protocol (NTP) reflection attacks, a category of distributed reflected denial of service (DrDoS) attack that utilizes differences in request and response data sizes[(2)]. As

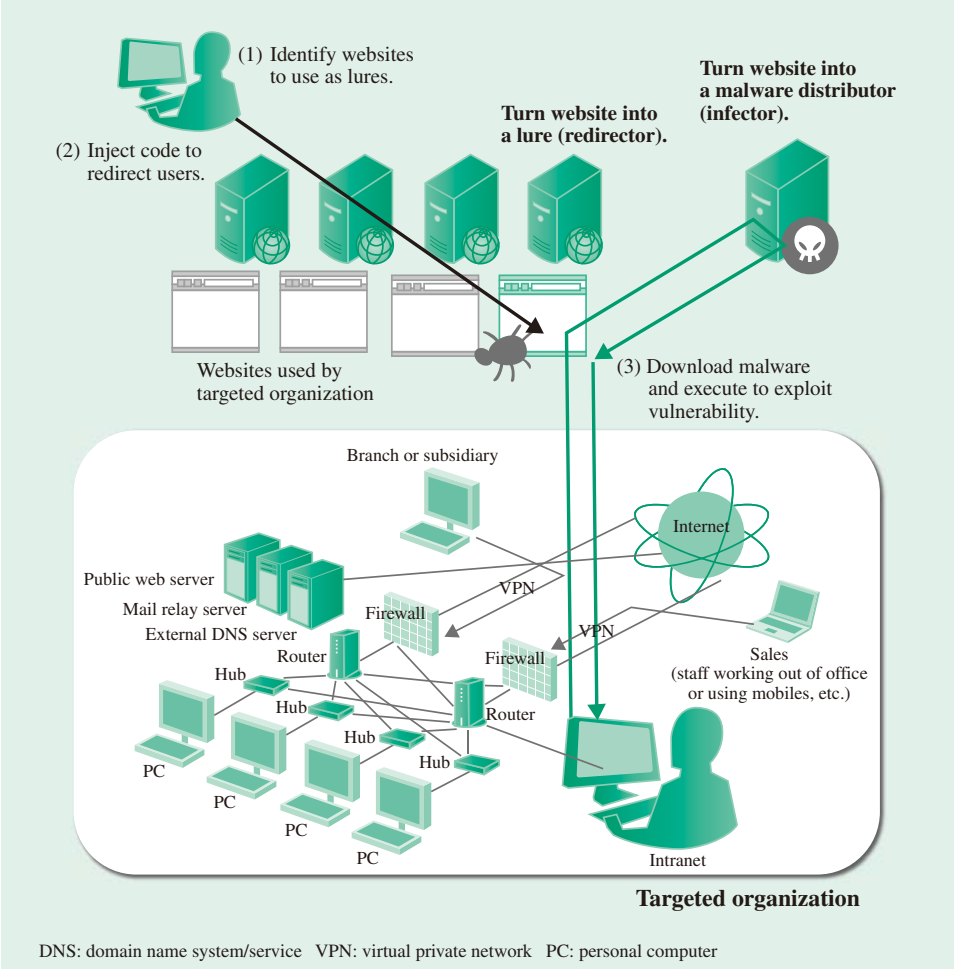


Fig. 1—Watering Hole Attack. A watering hole attack is so named because it lies in wait for users from the targeted organization to visit particular websites, in much the same way as a lion uses a watering hole as a lure for its prey.

DNS and NTP, respectively name resolution and time synchronization services, are vital to the functioning of the Internet, it is essential that everyone cooperate to limit this threat.

CSIRT ACTIVITIES AT HITACHI

CSIRTs

The activities of CSIRTs set up to counter cyberthreats in Japan since 1998 can be divided into three phases (see Fig. 2).

The first "acknowledgement" phase drew on the example of activities being initiated by CSIRTs in the USA, and involved the introduction of the concept of incident response, meaning responding to events in accordance with a predetermined plan. The second "predawn" phase was the time in which Japan's own CSIRT activities got underway, utilizing empirical feedback on the network worms that were circulating in this period from 2001 to 2003. This phase saw the establishment of a framework for CSIRT activities in Japan that reflected local circumstances, including the launch of the Information Security Early-Warning Partnership in 2004; the release of the Japan Vulnerability Notes (JVN), a vulnerability information database; and the establishment of the Nippon CSIRT Association in 2007. An emerging trend in 2012, in the third phase of CSIRT activities, was toward the use of CSIRTs to provide specialist incident response functions for dealing with cyberthreats. Prompted in large part by the diverse range of security incidents that occurred during 2011, this represented a consolidation phase in the activity of CSIRTs and can be seen as a landmark year in the progress of the field.

HIRT

The HIRT was launched in April 1998 as a research project aimed at establishing CSIRTs at Hitachi. So that the HIRT could operate as a CSIRT, this work included ensuring that, in dealing with vulnerability countermeasures and incident response, the HIRT would have the capabilities to identify and communicate information about threats at a technical level, to manage technical coordination, and to undertake

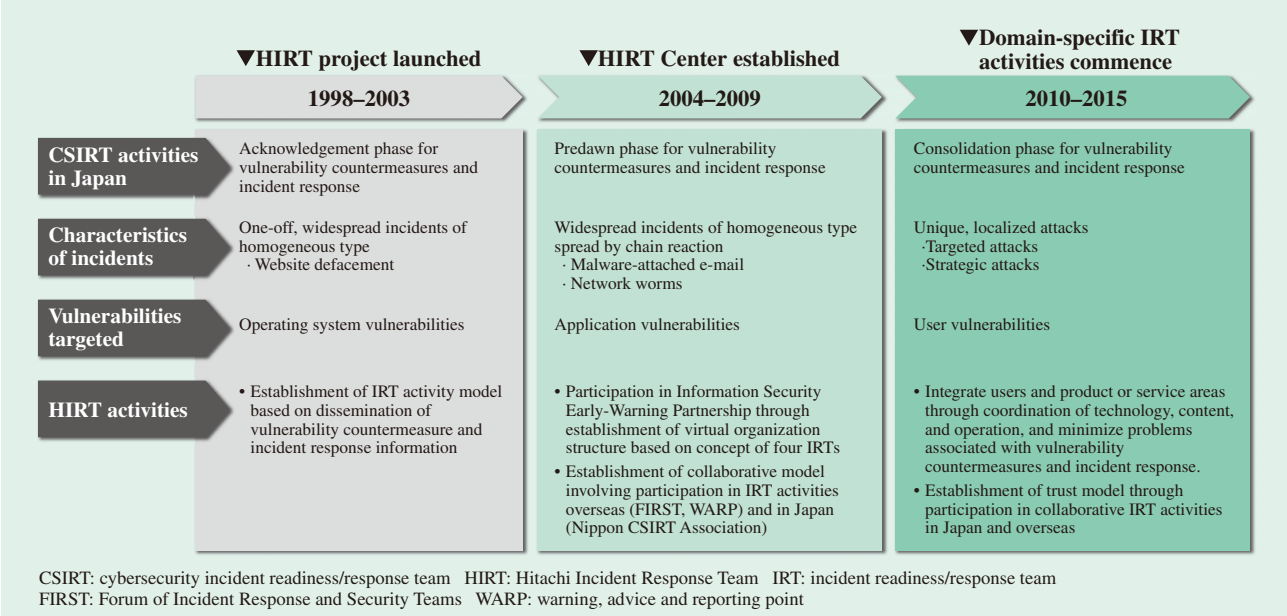


Fig. 2—Overview of Evolution of Incidents and HIRT Response.
The activities of the CSIRTs that deal with cyber-attacks in Japan continue to grow along with the evolution of those cyber-attacks.

technical collaboration with the external community. Furthermore, its mission was set forth as being to utilize experience from incident operations (security measures conducted to predict and prevent the damage caused by security incidents, and to limit the extent of damage that results when an incident does occur) to identify emerging threats and take action as early as possible. Along with its being equipped with these capabilities and assigned this mission, the HIRT also has the role of acting as the point of contact between Hitachi and other CSIRTs in the external entities.

CSIRT Activity Model at Hitachi

In its role as a CSIRT, the HIRT has the job of supporting cybersecurity at Hitachi through its work on vulnerability countermeasures (activities aimed at eliminating threats to cybersecurity) and incident response (activities aimed at defending against and resolving cyberthreats when they occur). It is also tasked with helping ensure the safety and security of social infrastructure by utilizing its practical experience of incident response and other activities to improve incident readiness.

In operating as a CSIRT, the HIRT has adopted an organizational model based on four incident readiness/response teams (IRTs) (see Fig. 3). Hitachi has three of these IRTs: a product vendor IRT that deals with the development of information systems, control systems, and other products; a system integration (SI) vendor IRT that deals with the use of these products in system implementation or service provision; and an internal user IRT that deals with the administration of Hitachi's own use of the Internet.

In this way, by establishing a HIRT Center to coordinate the different IRTs, the four IRTs constitute an organizational model that provides a clear definition of each IRT's role so that they can work together on cybersecurity measures. Note that the term "HIRT" is used both in the broad sense of incident operations conducted throughout Hitachi and in the narrow sense of the HIRT Center.

ACTIVITIES CONDUCTED BY HIRT CENTER

The main task of the HIRT Center is to conduct in-house IRT activities that deal with the administrative and technical aspects of cybersecurity measures in cooperation with the departments charged with their administration, and to support vulnerability countermeasures and incident response at the different business divisions and group companies. The external IRT activities of the HIRT Center also involve collaborating on cybersecurity measures by acting as Hitachi's point of contact with the external community for matters relating to CSIRTs.

Activities of In-house IRTs

The activities of in-house IRTs include passing on knowledge obtained through the collection and analysis of cybersecurity information in the form

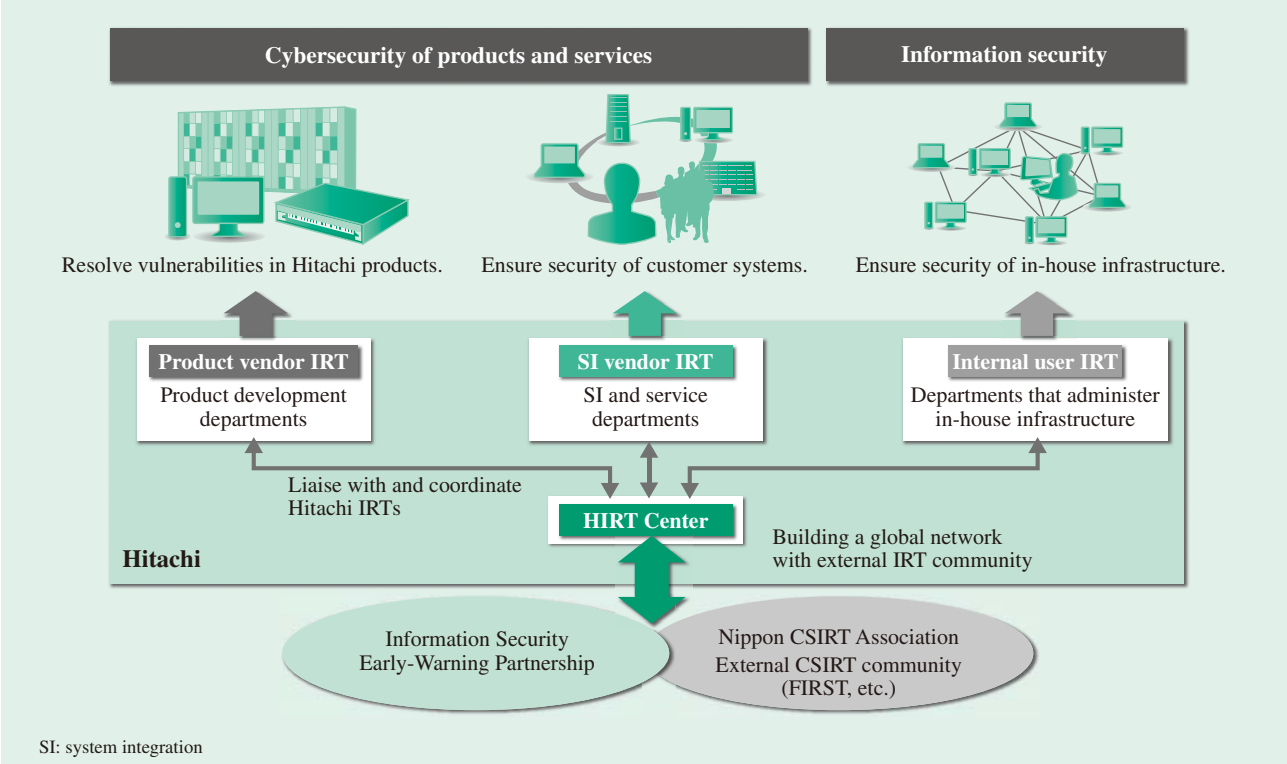


Fig. 3—Four IRTs for Vulnerability Countermeasures and Incident Response.
Hitachi has adopted an organizational model for its vulnerability countermeasure and incident response activities that is based on a four-IRT structure.

of advisories, and providing feedback to product and service development processes in the form of guidelines or support tools.

(1) Collection, analysis, and dissemination of security information

The interdepartmental dissemination of know-how and other information relating to vulnerability countermeasures and incident response.

(2) Provision of infrastructure for utilizing information

The provision of infrastructure for the utilization of information in the collection, analysis, and dissemination of cybersecurity information.

(3) Security technology improvement for products and services

Enhancements to web application security, implementation of security measures for digital consumer electronics and other products that incorporate embedded systems or control systems, and the establishment of development and management processes.

(4) Provision of infrastructure for research work

Establishment of collaborative arrangements with research institutions to facilitate technical developments aimed at achieving rapid deployment of countermeasures.

Activities with External IRTs

Along with an increasing number of cyber-attacks that keep their symptoms and damage hidden, progress is being made on establishing cooperative arrangements that allow CSIRTs from different organizations to work together to resolve problems by obtaining a broad overview of cyber-attacks, and to help each other operate more effectively.

(1) Better coordination of CSIRT activities in Japan

This includes the provision of infrastructure for utilizing information using JVN and the JVN Resource Description Framework Site Summary (JVNRSS)[3], work on countering vulnerabilities based on the Information Security Early-Warning Partnership, and collaboration between CSIRTs at different organizations through the Nippon CSIRT Association.

(2) Better international coordination of CSIRT activities

This includes work on establishing arrangements for collaboration with overseas CSIRTs, involvement in the work of warning, advice, and reporting points (WARPs) in the UK, and compliance with the standardization of the cybersecurity information exchange framework (CYBEX).

TABLE 1. Project to Improve Hitachi's CSIRT Activities
The project's objective is to establish incident operations throughout Hitachi.

Category	Measures
Phase 1 (2010 to 2011)	**Improve collaboration with business division and group company IRTs.** • Provide support through collaboration between HIRT center and business division and group company IRTs. • Utilize HIRT open meetings to establish an operational framework for IRT collaboration and mechanisms for sharing technical know-how. • Disseminate information about solutions for problems identified in security review consultations.
Phase 2 (2012 to 2013)	**Strengthen partnership with IRT support staff.** • Trial collaboration with IRT support staff (at business divisions and group companies) • Bottom-up implementation of IRT activities initiated by IRT support staff
Phase 3 (2014 to 2015)	**Establish a virtual, interdepartmental incident response system.** • Undertake support activities by the HIRT Center, IRTs, and IRT support staff. • Develop the HIRT (in the broad sense of a virtual organization model) by combining the user collaboration model (phases 1 and 2) and organizational collaboration model (phase 3).

(3) Provision of infrastructure for research work

This involves the training of researchers and practitioners with specialist knowledge through joint research with academic institutions and by participating in academic activities, such as training workshops for researchers in the field of malware countermeasures.

Main Activities

In 2010, Hitachi launched a project to improve its CSIRT activities with the aim of establishing incident operations throughout the group (see Table 1). This section covers the period up to phase 2, looking in particular at a trial of domain-specific (industry-specific) IRT activities and work on vulnerability countermeasures for control system products.

Trial of Domain-specific IRT

(1) Three-tiered cycle for incident response and readiness

While responding to incidents when they occur clearly has an important role in dealing with cyber-attacks, taking account of incidents and related developments to improve readiness is also essential. Accordingly, Hitachi has chosen to adopt a domain-specific approach to readiness involving a three-tiered cycle of incident response and readiness based on considerations specific to the business domain concerned, with clear demarcation of the roles of each division and how they are to work together (see Fig. 4).

(2) HIRT-FIS: Advanced endeavor in the financial domain

The Financial Industry Information Systems HIRT (HIRT-FIS) was established in October 2012 in the financial information systems division. In its role as a domain-specific subsidiary HIRT, the aim for the HIRT-FIS was to establish a prototype of a professional CSIRT specifically for the finance industry (see Fig. 5). This initiative was also part of the implementation of the three-tiered cycle for incident response and readiness. In particular, recognizing that measures for countering cyber-attacks need to take account of industry trends and other specific circumstances, the aim of the HIRT-FIS was to take the lead in studying and implementing CSIRT activities tailored to the financial sector. In the future, Hitachi

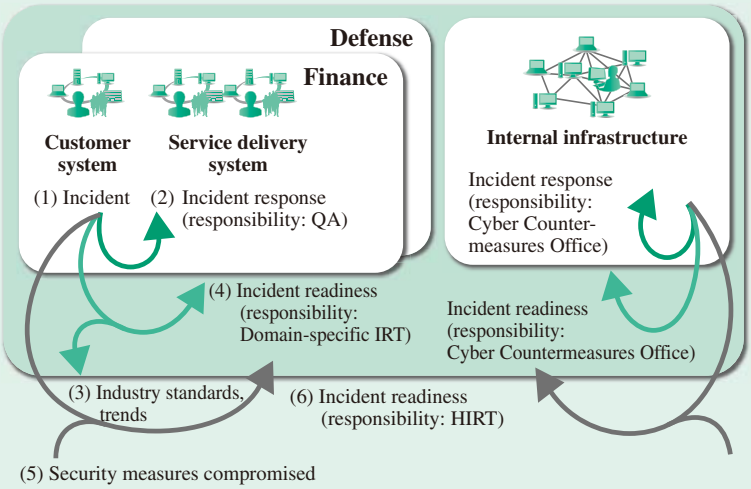


Fig. 4—Three-tiered Cycle for Incident Response and Readiness.
In addition to dealing with cyberthreats by responding to incidents when they occur, this also involves improving readiness by learning from the experience of actual incidents and by taking account of changing circumstances from the perspective of specific business domains.

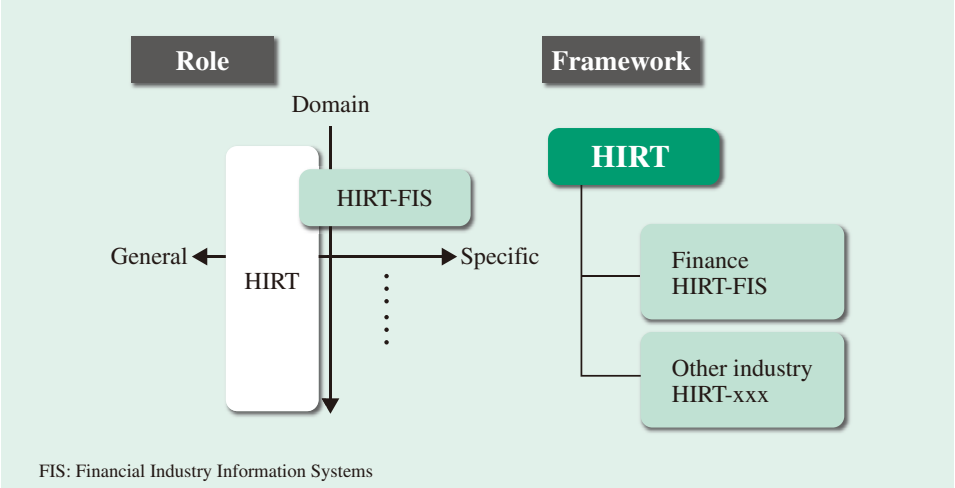


Fig. 5—Role of and Framework for Domain-specific IRT Activities.
The HIRT-FIS is one of the measures adopted to implement the three-tiered cycle for incident response and readiness and is intended as a prototype of a professional CSIRT tailored specifically to the finance industry.

intends to review progress and establish further domain-specific subsidiary IRTs for sectors such as control systems or defense.

Vulnerability Countermeasures for Control System Products

Hitachi is proceeding with three initiatives based on an approach that utilizes experience from past HIRT activities and applies it in the control systems sector.

(1) Utilize HIRT security information in the collection of security information related to control systems, including the latest trends, product vulnerabilities, and incident case studies.

(2) Establish arrangements for the HIRT to act as a primary point of contact for the external community in relation to vulnerability handling and incident handling.

(3) In addition to dealing with vulnerabilities in terms of specifications, source code, and configurations, embark on investigations aimed at establishing preliminary examples for control equipment and control systems with the aim of implementing vulnerability countermeasures for control equipment and other control systems that have specific applications in mind.

CONCLUSIONS

This article has described recent trends in security incidents, and Hitachi's CSIRT activities in which the HIRT Center plays a central role.

Along with the ongoing damage caused by known threats, damage is also being done by emerging threats from new types of cyber-attack. Also becoming clear is the damage caused by cyber-attacks that results from the degree of impact that organizations have on each other. This makes it essential to utilize CSIRTs for specialist and practical collaboration between organizations.

The HIRT takes note of changing circumstances and is working on measures for the rapid deployment of countermeasures as part of the process of identifying upcoming threats. Hitachi also believes that it can contribute to the creation of safe and secure social infrastructure through the activities of its CSIRTs for specific industries or other sectors, and by training the academics who will form the next generation of the CSIRT community.

REFERENCES

(1) Information-technology Promotion Agency, Japan, "IPA Technical Watch: Report on APT," http://www.ipa.go.jp/about/technicalwatch/20101217.html in Japanese.

(2) JPCERT/CC, "DDoS Attacks Using Recursive DNS Requests," https://www.jpcert.or.jp/at/2013/at130022.html in Japanese.

(3) M. Terada et al., "Proposal of JP Vendor Status Notes Database (JVN)," IPSJ Journal **46**, pp.1256–1265 (May 2005) in Japanese.

ABOUT THE AUTHORS

Masato Terada, Dr. Eng.
Hitachi Incident Response Team, Services Creation Division, Information & Telecommunication Systems Company and Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in CSIRT collaboration activities for the incident operation of cybersecurity. Dr. Terada is a member of the Information Processing Society of Japan (IPSJ).

Masashi Fujiwara
Hitachi Incident Response Team, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in the vulnerability handling and incident response for Hitachi products and the Internet application service.

Akiko Numata
Hitachi Incident Response Team, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. She is currently engaged in establishment of internal education framework for the vulnerability handling and incident response.

Toru Senoo
IT Platform Division Group and Hitachi Incident Response Team, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in the establishment of the vulnerability countermeasure process for the Industrial Control Systems.

Kazumi Ishibuchi
IT Platform Division Group and Hitachi Incident Response Team, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in cyber intelligence as a cybersecurity information analyst.

Mari Miyazaki
CSIRT Group, General System Department, Financial Project Management Unit, Financial Information Systems Division, Information & Telecommunication Systems Company, Hitachi, Ltd. She is currently engaged in CSIRT activities as HIRT-FIS (Financial Industry Information Systems HIRT) staff.

Featured Articles

Control System Security for Social Infrastructure

Toshihiko Nakano, Ph.D.
Katsuhito Shimizu
Tsutomu Yamada
Tadashi Kaji, Dr. Info.

OVERVIEW: The wider use of networking in social infrastructure in recent years has exposed their control systems to greater security risks. In response, ongoing work is being done by international standards bodies and other industry associations on determining security requirements for control systems. Along with taking note of trends in cyber-attacks and social infrastructure requirements such as long operating life, Hitachi supplies solutions and products for satisfying these requirements. Hitachi has also been coordinating measures for improving the security of control systems through its participation in the Control System Security Center, a collaboration between industry, government, and academia set up for this purpose, since it was first established.

INTRODUCTION

THE threat of cyber-attack is a consequence of greater use being made of networks in social infrastructure over recent years. This makes it essential for social infrastructure systems also to adopt security measures against a broad range of cyber-attacks.

As these security measures need to be implemented in ways that do not leave any gaps, but also that do not impose an excessive overhead, ongoing study being undertaken at international standards bodies includes both security requirements and the criteria to consider in security assessments. The International Electrotechnical Commission (IEC), for example, in its IEC 62443 security standard for control systems[(1)], has stipulated security requirements, the requirements for analyzing impacts on health, safety, and the environment (HSE), and security assurance levels (SALs) for assessing the strength of security measures. The International Telecommunication Union (ITU), meanwhile, is working on the development and standardization of its Cybersecurity Indicator[(2)] and Global Cybersecurity Index[(3)] assessment criteria. Elsewhere, the European Telecommunications Standards Institute (ETSI) is also developing assessment criteria called Information Security Indicators[(4)].

These assessment criteria tend to provide an assessment or numerical indicator for the strength of security measures as they exist at a particular time (usually the design stage). However, a key prerequisite for the control systems used in social infrastructure is that they remain in operation over a long period of time. Because of this long timescale, social infrastructure tends to contain a mix of different types of system. Also, rapid advances in the technology of cyber-attacks mean that it is not uncommon for previously unanticipated attacks to become suddenly commonplace.

Given this background, security measures implemented in social infrastructure systems at the design stage cannot be assumed to provide adequate security, and therefore it is necessary to ensure that measures can be upgraded as required over the long operating life of social infrastructure in response to advances in the technology of cyber-attacks. Taking note of developments in cyber-attacks and the long operating life and other characteristics of social infrastructure, Hitachi has identified three new security requirements for social infrastructure, namely that security measures be adaptive, responsive, and cooperative.

This article describes the levels of security required in social infrastructure; strategies for achieving these levels of security; work on implementing measures at the system and component level; the activities of the Control System Security Center (CSSC), which was set up to ensure the security of control systems; and the work being done by Hitachi.

LEVELS OF SECURITY REQUIRED IN SOCIAL INFRASTRUCTURE

This section looks at the security levels defined in IEC 62443. It also describes the requirements identified by Hitachi for security measures to be adaptive, responsive, and cooperative, and the level required in each case, defining the required levels.

(1) Required level of security

IEC 62443 defines the SAL criteria for assessing the strength of security measures (see Table 1).

Looking at current trends in attacks against social infrastructure systems, it is clear that these systems are the subject of systematic attacks with a high level of malicious intent. This means they require level 3 or 4 security measures.

(2) Required level of adaptability

Adaptability defines the flexibility of measures for responding to a diverse range of attacks.

The requirement in the past has been to incorporate security measures that can deal with the types of attack anticipated at the design stage. However, factors such as the evolution of attack methods mean that new forms of attack will continue to appear. Accordingly, the ability to respond to types of attack not anticipated at the design stage has also become necessary.

Table 2 lists the levels used to represent the extent to which this adaptability requirement is satisfied.

Because control systems used in social infrastructure will very likely face types of attack not anticipated at the design stage, they require a higher level of adaptability than information and other systems. This means that their security measures need to achieve level 3, and they also require organizational initiatives aimed at upgrading this to level 4 in the future.

(3) Required level of responsiveness

Responsiveness defines how quickly a response can be mounted to an attack.

Whereas the emphasis in the past was on security measures for preventing attacks, what is needed to deal with the sophisticated attacks of recent times is the ability to quickly detect when such an attack has taken place and to instigate effective countermeasures.

Table 3 lists the levels for this responsiveness requirement.

As control systems used for social infrastructure need to deliver services continuously, they must respond quickly when a security attack occurs. This means they need to satisfy the level 3 requirement for responsiveness, whereby they can respond to an attack without interrupting service delivery. To deal with relentlessly evolving attacks, they also require organizational initiatives aimed at upgrading to level 4 in the future.

(4) Required level of cooperativeness

Cooperativeness defines the degree to which security measures are influenced by other systems with which they coexist.

Table 1. Security Levels

These levels indicate the strength of security measures as they exist at a given point in time.

Level	Description
1	Protection against casual or coincidental violation
2	Protection against intentional violation using simple means
3	Protection against intentional violation using sophisticated means
4	Protection against intentional violation using sophisticated means with extended resources

Table 2. Adaptability Levels

These levels indicate how flexibly countermeasures can cope with a diverse variety of threats.

Level	Description
1	No measures for dealing with security threats
2	Measures in place for dealing with security threats identified during the design stage
3	Measures in place for dealing with new security threats
4	Establishment of management systems for dealing with new threats

Table 3. Responsiveness Levels

These levels indicate how quickly a response can be mounted when a threat occurs.

Level	Description
1	No measures for detecting threats
2	Measures in place for detecting threats
3	Measures in place for countermeasures after threat occurs
4	Establishment of management systems covering time from threat occurring to countermeasures being implemented

Table 4. Cooperativeness Levels

These levels indicate the influence of other interdependent systems.

Level	Description
1	No measures for preventing negative influences
2	Measures in place for preventing negative influences
3	Measures in place for taking advantage of positive influences
4	Establishment of management systems for ongoing assessment of influences of one system on another

These influences can be both positive (such as the sharing of threat information to allow the detection of previously unknown threats) and negative (such as an attack from another system that has been infected by malware).

Levels are defined representing the extent to which this cooperativeness requirement is satisfied (see Table 4).

Because social infrastructure systems have a long operating life, they coexist with a wide variety of other systems, not all of which will have the same level of security measures. In such a situation, use of level 2

security measures that maintain system-wide security is required to prevent attacks against the weakest parts.

STRATEGIES FOR ACHIEVING CONTROL SYSTEM SECURITY

Hitachi has been in the practice of using a "2 × 3 security implementation model" to model its approach to maintaining security throughout the lifecycle of social infrastructure systems[5]. This model is based on the idea of achieving the ongoing provision of all-encompassing security by dealing with threats across two different lifecycle phases (development and operation), and in terms of three different perspectives (functions, environment, and organization and people) (see Fig. 1).

In terms of the security requirements, this seeks to utilize security measures in the development phase to satisfy both the required level of security and the adaptability requirement, and to establish a plan, do, check, and act (PDCA) cycle for security during the operational phase to satisfy the responsiveness and cooperativeness requirements. In particular, the development process needs to take account of operational phase considerations if a system is to be provided with level 3 or higher responsiveness and level 2 or higher cooperativeness as this requires continuous monitoring of system security to detect security incidents, and the establishment of operational security infrastructure that can respond to any incidents that are detected without interrupting services.

SECURITY IMPLEMENTATION AT SYSTEM LEVEL

Based on the 2 × 3 security implementation model, this section describes development-phase security measures applicable to control system development, and also operational-phase security measures.

Development Phase

An important part of control system development is to assess potential security threats and determine which security measures to incorporate. Hitachi has established system implementation guidelines that specify the relevant procedures, and which utilize the security concepts advocated in IEC 62443. These guidelines are used to provide appropriate security

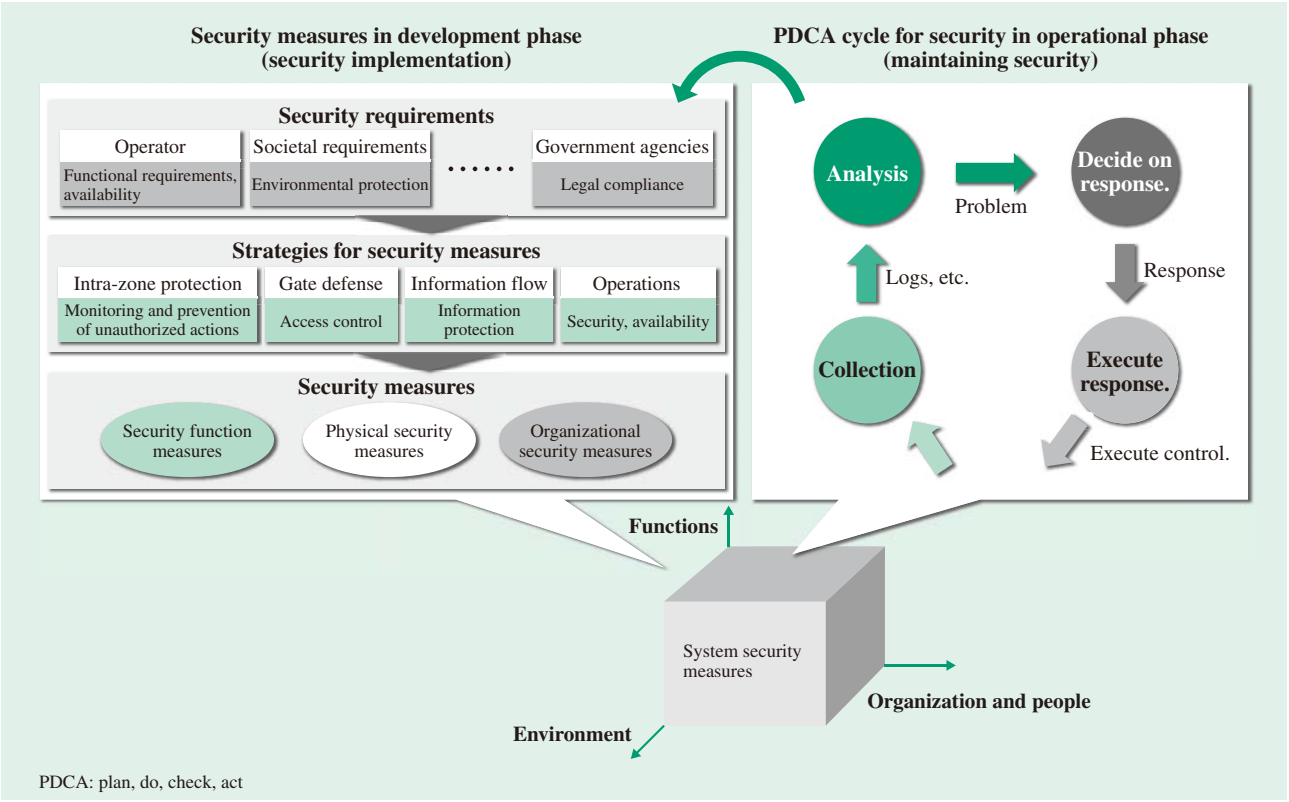


Fig. 1—2 × 3 Security Implementation Model.
This model provides all-encompassing security by dealing with threats across two different lifecycle phases (development and operation), and in terms of three different perspectives (functions, environment, and organization and people).

measures based on factors such as the importance of the system and its customer requirements.

Specifically, they cover the following procedures.

(1) Partitioning of the system into zones in which the same security policies apply based on a risk analysis of the system.

(2) Identification of "conduits" (interconnections) between zones.

(3) Formulation of security measures

(a) Measures for preventing unauthorized information entering a zone via a conduit (provision of conduit gates)

(b) Measures for preventing unauthorized operations within a zone

(i) Network measures

(ii) Device measures

The following section describes the security measures specified by these system implementation guidelines to satisfy the required levels (described above) in the case of the information and control zone (see Fig. 2).

(1) Security measures for conduit gates (measure 1)

The main purposes of security measures for conduit gates are to prevent unauthorized intrusions into the zone and leaks of information from the zone.

For a system to achieve security level 3 or 4, conduit gates must identify necessary communications and block unnecessary communications. Factors to consider when determining whether or not a communication is necessary include not only where the communication is being sent to or received from, but also its direction and content. To achieve level 3 adaptability, it must be possible to incorporate logic for determining such things as whether or not communication in necessary or whether it is suspicious. To achieve level 3 responsiveness, it is necessary to monitor communications continuously, and to allow the control system operator to decide how to respond when a suspicious communication is detected. Based on these considerations, the system is developed in accordance with the security policies for each zone.

(2) Security measures for preventing unauthorized actions within a zone: network (measure 2)

The main purposes of intra-zone network security measures are to prevent unauthorized users or malware that have entered the zone from accessing functions or information, and to detect unauthorized users.

To achieve security level 3 or 4, components within a zone must be identified and the connection of unnecessary components blocked. Hitachi supplies products for this purpose.

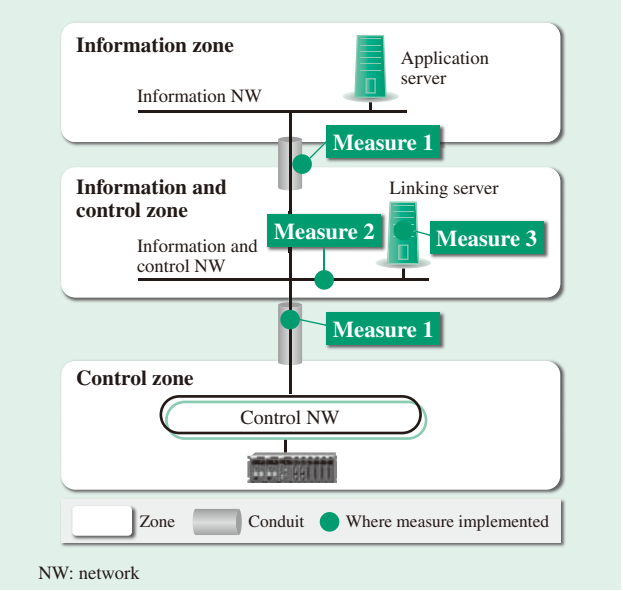


Fig. 2—Security Implementation Points for Control Systems. The control system is partitioned into zones and security measures implemented for the zone entry and exit points and for networks (information and control networks and components inside each zone).

Achieving level 4 responsiveness requires continuous monitoring within the zone and generation of an alarm to the security operation system whenever a suspicious action is detected. In a new approach to intra-zone monitoring, Hitachi has developed a solution that uses a decoy server. Located within the zone, the decoy server has deliberately downgraded security functions so that its becoming infected by malware will provide an early warning of any intrusion by malware into the zone.

(3) Security measures for preventing unauthorized actions within a zone: devices (measure 3)

The main purpose of security measures for control components within a zone is to prevent access to information or functions by any malware that has infected a device.

This requires functions for preventing operations by software other than that authorized for use in the control component, and the use of control components with enhanced security.

These security enhancements to control components are described later in this article.

Operational Phase

This section describes the security measures required for control systems during their operational phase, specifically measures for responding rapidly to security incidents, and formal security management

practices for dealing with risks such as the emergence of new threats.

(1) Measures for responding rapidly to security incidents

When a security problem is detected at a conduit gate, on an intra-zone network, or in a component within the zone, it is necessary to determine quickly whether the problem is the result of an actual security incident or simply a misdetection, and to respond accordingly. In addition to setting up a security operation center (SOC) for information systems, Hitachi has established an incident response team to build up its expertise in dealing with incidents. However, industry knowledge is also needed to determine whether a problem is due to an actual incident.

Hitachi has know-how in both incident response and business system implementation and operation, and is applying it in the development of security operation systems and services.

(2) Formal security management systems

Formal security management systems are essential if a control system is to achieve level 4 adaptability and responsiveness. Hitachi has focused in particular on cybersecurity management systems (CSMSs). CSMSs are intended to maintain ongoing security by having the operator of a control system undertake risk management for that system. For a system operator to maintain security, they need to collaborate with the system integrator and other product vendors. Hitachi has long strived to deliver highly reliable and secure control systems, and is also working on CSMSs.

INITIATIVES AT THE CONTROL COMPONENT LEVEL

To build secure control systems with level 3 or higher security, it is important that the components used in the system be able to operate safely and reliably. In addition to hardening control components (making them more secure) and strengthening security functions, Hitachi is also developing products for enhancing the security of control components that cannot implement their own security measures.

Hitachi is currently working toward Embedded Device Security Assurance (EDSA) certification[(6)], a certification system for the security assurance of control components that is administered by The International Society of Automation (ISA) Security Compliance Institute (ISCI). The certification process considers the following three criteria.

(1) Functional security assessment (FSA): This assesses the implementation of security functions

(2) Software development security assessment (SDSA): This covers each phase of software development

(3) Communication robustness testing (CRT)

INITIATIVES BY CSSC AND HITACHI

The CSSC was set up in March 2012 as a collaboration between industry, government, and academia with the aim of strengthening control system security. Its main objectives are the research and development of control system security technology, security auditing of control equipment, and the use of simulated plant to raise awareness and for personnel development. In the case of the security auditing of control equipment, CSSC is looking closely at EDSA certification, including joining ISCI as an associate member, and is working towards obtaining certification as an auditor.

Hitachi has been a member of CSSC since its establishment and is collaborating with the organization on joint research into measures for improving the security of control systems, the use of simulated plant for security training on control systems, and the security auditing of control equipment. As a member of CSSC, Hitachi intends to continue its active participation in the research and development of technology for enhancing control system security, and also other related measures.

CONCLUSIONS

This article has described the new security requirements for control systems used in social infrastructure systems, and the security technologies for satisfying these requirements.

Control system security measures have an important role in the protection of social infrastructure systems. To counter continually evolving threats, Hitachi intends to work with organizations such as the CSSC in Japan and overseas, as well as researching and developing the required technologies and supplying products that incorporate these technologies. Hitachi is also seeking to supply total services that extend from security risk analysis for control systems to system implementation and operational support. In doing so, Hitachi will contribute to the creation of secure social infrastructure that everyone can use with confidence.

REFERENCES

(1) IEC, "Industrial Network and System Security," IEC 62443 (2013).
(2) ITU-T, "A Cybersecurity Indicator of Risk to Enhance Confidence and Security in the Use of Telecommunication/ information and Communication Technologies," Recommendation ITU-T X.1208, 1204.
(3) ITU-D, "Global Cybersecurity Index," http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
(4) ETSI, "Information Security Indicators," http://www.etsi.org/images/files/ETSITechnologyLeaflets/InformationSecurityIndicators.pdf
(5) T. Kaji et al., "Cyber Security Technologies for Social Infrastructure Systems," Hitachi Review **62**, pp. 397–401 (Sep. 2013).
(6) ISCI, "Embedded Device Security Assurance (EDSA)," http://isasecure.org/ISASecure-Program.aspx

ABOUT THE AUTHORS

Toshihiko Nakano, Ph.D.
Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Katsuhito Shimizu
Control System Platform Design Department, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the design and development of servers and controllers for information and control systems.

Tsutomu Yamada
Department of Energy Management Systems Research, Hitachi Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of embedded computer architecture, network systems and cybersecurity for industrial control systems. He is a Professional Engineer, Japan (Information Engineering). Mr. Yamada is a member of the IEEE, the International Society of Automation (ISA), The Institute of Electronics, Information and Communication Engineers (IEICE), and The Society of Instrument and Control Engineers (SICE).

Tadashi Kaji, Dr. Info.
Infrastructure Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of information security technology. Dr. Kaji is a member of the IEEE Computer Society.

Featured Articles

Managed Security Services to Address Increasingly Sophisticated Cyber-attacks

Yoshitaka Narishima
Shinichi Kasai
Takayuki Sato
Masaki Mori
Akihiko Fujita

OVERVIEW: Companies and organizations have been facing increasingly severe security risks in recent years as cyber-attacks have grown more complicated and sophisticated. Also, as cloud services have spread, the connection of information appliances and control system devices to the Internet has added to the complexity of the information systems that must be protected. Managed security services are a group of integrated services that provide everything from consulting to operations and the application of security measures. These services include technical assistance in the handling of incidents by applying Hitachi's knowledge, and security event monitoring services that apply know-how in both construction and operations, thereby enabling the provision of solutions that are tailored to the information systems that are being protected and contributing to the safety and security of the social infrastructure.

INTRODUCTION

INFORMATION technology (IT) is increasingly being utilized to achieve an advanced social infrastructure that provides greater user convenience. As the role of IT systems grows in this type of social infrastructure, the importance of ensuring safety and security is becoming more and more important.

Companies and organizations have been facing stark security risks in recent years as cyber-attacks have grown more complex and sophisticated. This includes more advanced targeted e-mail attacks and larger distributed denial of service (DDoS) attacks, among others. Cyber-attacks target specific organizations or individuals and relentlessly attempt to steal confidential or personal information and to cripple IT system services, which even lead to exact money.

The information systems that must be protected used to be set up within the organizations, but due to the spread of cloud services, they can now be located outside the organizations and on the Internet. With internal corporate information systems sometimes linked to cloud services as well, the boundaries between security regions are becoming less clear, and the administration of security increasingly complicated. Also, in addition to personal computers (PCs) and other such IT devices, information appliances, control system devices, and other devices are now being connected to the Internet. This makes much larger number of system environments vulnerable to the cyber-attacks, making the scale of the threats even greater.

Against the background of these threats, taking security measures based on defense in depth in order to protect information systems from cyber-attacks, the necessity is also growing for the immediate detection of incidents when an attack occurs, so that events can be handled rapidly to hold damage to a minimum. To this end, monitoring systems must be strengthened, with advanced log management systems that constantly monitor the complex IT systems, as well as an organization comprised of engineering staff with the technical skills required to take necessary measures quickly. Also, the necessity for outsourcing security operations and security measures has been spreading as the operational burdens placed on information system departments has been increasing along with the required security expertise.

This article discusses managed security services, which are a set of comprehensive security measures designed to protect social infrastructures and information systems from more complicated and sophisticated cyber-attacks.

MANAGED SECURITY SERVICES

Offerings from Hitachi include managed security services that oppose cyber-attacks and other threats. These security solutions, everything from consulting to the application of security measures and operational services, provide total support for companies in the social infrastructure field and a variety of other industries and business categories, as well as for public agencies and local governments.

These services manage security during the operational phases of IT systems with expanded needs in outsourcing security measures and operations, and not only do they "protect IT," they offer an integrated set of security services designed for the "protection via IT." Managed security services comprise three categories: "managed security governance," "managed channel security," and "managed platform security," which can propose and provide the right solution for the information system being protected, as well as the responsible office and department in the organization (see Fig. 1).

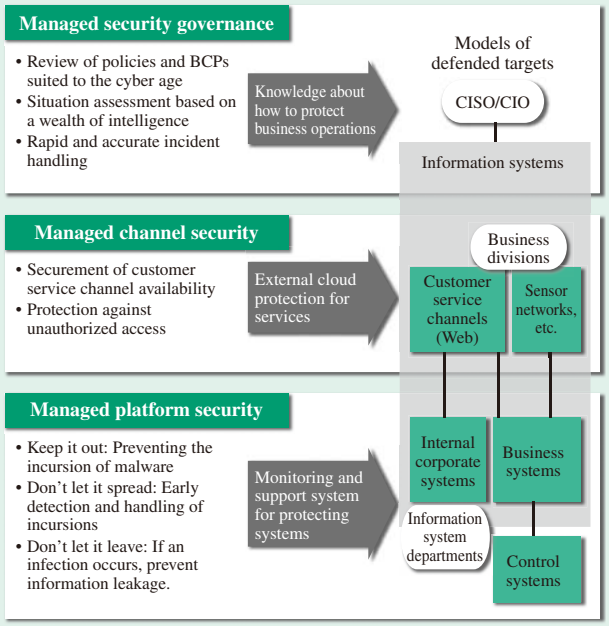
The features of each of these three service categories are described below.

Achieving Dynamic Security Management

In order to strengthen measures against vulnerabilities in managed security services, in addition to improvements based on the "PDCA cycle," with planning that involves constructing cybersecurity incident readiness/response teams (CSIRT) within organizations and reviewing business continuity plans (BCPs) (plan), measures and operations (do), inspections and audits (check), and improvements and corrections (act), the "OODA loop" concept is also adopted in order to achieve decision making that is both rapid and rational, through a series of steps that includes monitoring (observe), situational analysis (orient), decision making (decide), and action (act). This method is used to strengthen dynamic security management in the operational stage, to establish information security policies based on the assumption that incidents will occur, and to implement stronger and more rapid security measures (see Fig. 2).

Applying the Incident-handling Know-how of a Team of Professionals

The Hitachi Incident Response Team (HIRT), which acts as a CSIRT with responsibility for cyber-attack



Category	Service menu	Feature overview
Managed security governance	Security consulting service	• Security policy formulation support • Security risk analysis support • Business continuity management formulation support
	Security diagnosis service	• IT infrastructure vulnerability diagnosis • Malware inspection
	Intelligence service	• System vulnerability information provision • Harmful rumor surveys regarding specific sites • Incident response support
	CSIRT technical support service	• CSIRT operation support within organizations • Targeted attack mail training
Managed channel security	Website protection service	• Web application firewalls • Website DDoS measures
	Website check service	• Web system vulnerability diagnosis • Tampering detection
Managed platform security	E-mail security service	• Anti-virus, anti-spam • Content filtering
	Web security service	• URL filtering during Web browsing • Anti-virus
	Security event monitoring service	• Integrated log management • Log correlation analysis
	Virtual server protection service	• Virtual UTM operation support

BCP: business continuity plan CISO: Chief Information Security Officer CIO: Chief Information Officer IT: information technology
CSIRT: cybersecurity incident readiness/response team DDoS: distributed denial of service URL: uniform resource locator UTM: unified threat management

Fig. 1—List of Menu Options for Managed Security Services.
The systems defended by each category of managed security services are shown above. The table lists the service menu options available in each category.

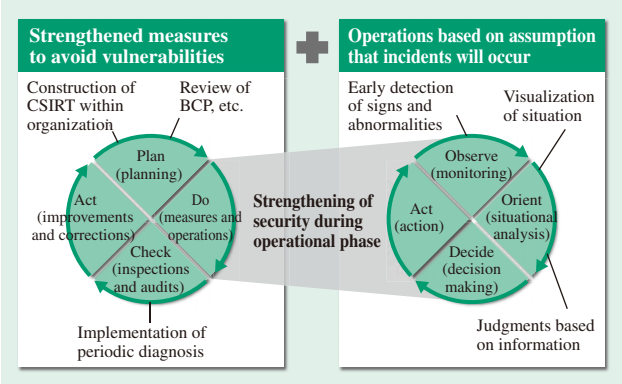


Fig. 2—Relationship between PDCA Cycle and OODA Loop. In addition to the continual improvements of the PDCA (plan, do, check, act) cycle, operations based on the OODA (observe, orient, decide, act) loop are adopted in order to strengthen security in the operational (do) phase.

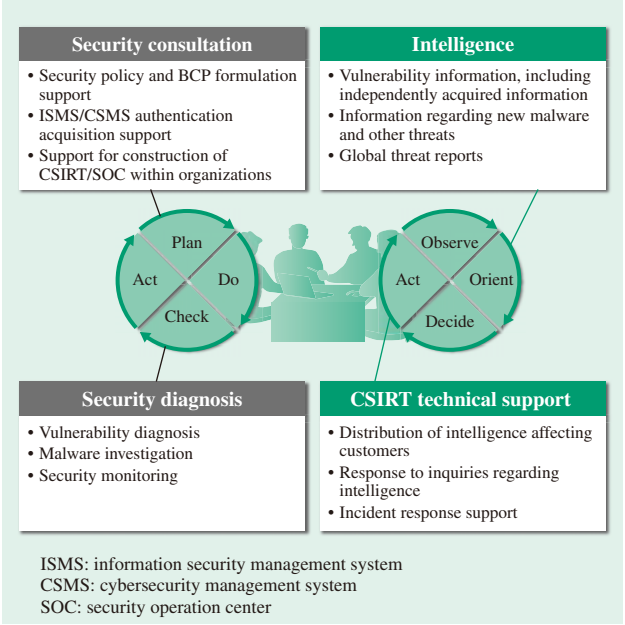


Fig. 3—Managed Security Governance Menu Configuration. This diagram shows the service menus provided for managed security governance, and the relationship between the menus and the PDCA cycle and OODA loop.

measures, is a team of professionals within Hitachi with extensive know-how in handling incidents. HIRT cooperates with global partners to analyze and monitor intelligence on behalf of the customer's internal CSIRT, while offering various services including a "CSIRT technical support service" that provides related information and necessary responses, as well as an extremely advanced security operation and management system that is active 24 hours a day and 365 days a year.

Flexible Support for Cloud Environments

Complex security measures and operations are provided for multiple system environments including on-premises environments, cloud environments, distributed cloud environments, and others. Also, by providing services such as "virtual server protection services" and "security event monitoring services" that enable detailed individual security measures that have been difficult under cloud environments in the past, flexible support for cloud environments is achieved.

CATEGORIES AND SERVICE MENUS

Service menu options that warrant attention are described below for each of the three categories of managed security services.

Managed Security Governance

Managed security governance, which protects business operations, is comprised of professional consultation services and other services based on the knowledge accumulated as part of Hitachi's internal information system management, in addition to knowledge accumulated as part of activities supporting customer businesses (see Fig. 3).

The process of continual improvement activities through the PDCA cycle in information security management is an effective way to ensure information security in social infrastructures and IT systems. Security consulting services support the formulation of an organization's security policies and the analysis of security risks based on the ISO/IEC 27001 international standard for information security management. Organized and systematic security management is promoted by providing and working to establish these types of security management efforts for customers.

Mechanisms and systems that can rapidly handle incidents are necessary to deal with increasingly sophisticated cyber-attacks. By quickly acquiring valuable information such as newly discovered cyber-attack techniques and vulnerabilities, cyberterrorism information, and so on, it is possible to hold an advantage when it comes to implementing cyber-attack measures as well. Intelligence services exist that gather this type of threat information using a global intelligence network, in order to provide the information in a rapid and comprehensive manner. In addition to technical information, the intention behind each attack is also provided along with surrounding conditions, so that the scale of the threat can be determined with greater specificity. Information such

as zero day vulnerabilities newly discovered in known vulnerability information as well as vulnerability information used to predict future threats is also provided and added to the information content that corresponds to the organization's system.

Finally, based on the gathered threat information and the log management system described below, the way incidents are actually handled is key, and the CSIRT inside the organization is responsible for fulfilling this role. The necessity of this type of system has increased in recent years, and a variety of different organizations including financial institutions have been constructing systems. A CSIRT technical support service provides operational support including incident handling and cyber-attack analysis for newly launched organizations. In the future, as cyber-attacks evolve even further, it is expected that still higher levels of security expertise will be required, and the need for these types of support services will increase.

Managed Channel Security

Managed channel security is a service that protects the customer's services by defending public websites from threats in an external cloud.

This service has become indispensable for business, and due to the fact that the public websites that are used in actual business involving the provision of corporate information and various business deals are always exposed to the Internet, they are ideal targets for attackers. There have been many cases recently of vulnerabilities in websites being exploited to tamper with the sites. Although in the past these types of attacks mainly involved displaying a flag or some other image, recently websites have been tampered with in ways that are not visible, with viruses injected in many cases. Users accessing such a site are unknowingly infected with the virus, and personal information and other information is stolen as a result. Not only is the organization with a website that has been tampered with a victim, it can also conceivably be seen as the party perpetrating the harm to its Web users, and so the strengthening of security is an urgent issue. Website protection services continuously defend public websites with DDoS attack measure services to protect websites from attacks coming from large-scale, globally distributed platforms, as well as Web Application Firewall (WAF) services.

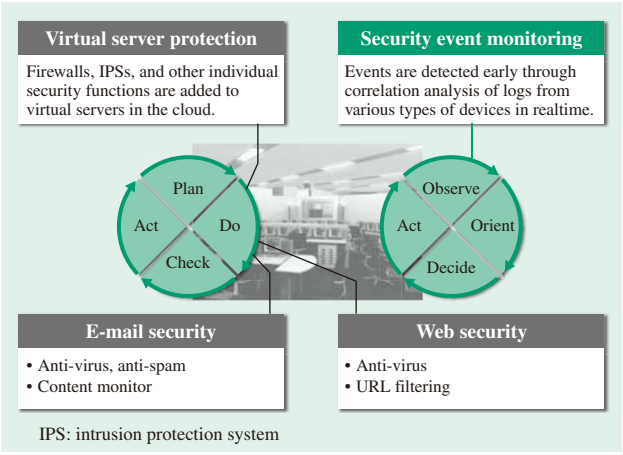


Fig. 4—Managed Platform Security Menu Configuration. This diagram shows the service menus provided for managed platform security, and the relationship between the menus and the PDCA cycle and OODA loop.

Managed Platform Security

Managed platform security is a service that defends the customer's information and control systems from threats (see Fig. 4).

Based on the "defense in depth" concept, multiple layers of defenses include "internal measures" designed to prevent incursions by malware, "proliferation measures" designed to quickly detect any incursions and prevent them from proliferating, and "outbound measures" designed with goals that include preventing information from leaking in the case of an infection. Although outbound measures that do not allow information leaks are also important, internal measures must act as the first line of defense by reducing the incursion of targeted attack e-mail and other such threats inside the organization. The e-mail security service is a Software as a Service (SaaS) type service that provides multiple functions, including highly accurate anti-spam functions, as well as anti-virus functions that combine multiple commercial virus scanners with a proprietary artificial intelligence engine. Each advanced detection function enables the reduction of unwanted e-mail within the organization, thereby improving organizational work efficiency. It is also possible to take advantage of the SaaS features to reduce the time required to adopt security measures, cut costs, and decrease the burden of management.

The use of cloud solutions such as Hitachi Cloud Computing Solutions is growing. Benefits to the adoption of cloud solutions include a reduction in both cost and development time. On the other hand, concerns in the area of security are acting as an obstacle to usage. With a managed security service, in addition to the security provided by each cloud platform, functions such as firewalls and intrusion protection systems (IPSs) are also provided as virtual

server protection services, with detailed settings and log analysis that are the same as for an on-premises environment.

In these types of systems as well, where on-premises environments are mixed with cloud environments utilizing virtualization technology, it is necessary to monitor each type of device on a regular basis in order to quickly detect security abnormalities, and to tie this in to the handling of incidents. Security event monitoring services provide comprehensive monitoring of systems in hybrid environments that include cloud services, detecting incidents at an early stage while offering advanced and rapid incident handling support by a team of professionals, in collaboration with Hitachi's Security Operation Center (SOC).

CASE STUDIES AND EFFECTS OF ADOPTION

Managed security services are provided as a set of services offering comprehensive security measures. Examples of adopted service menu options are described below.

E-mail security services are used by financial institutions as well as many other types of companies. A large number of customers have reported that the internal workload placed on their companies was decreased after the services were adopted, due to the high rate of detection. The support system, which is active 24 hours a day and 365 days a year, has been given high marks for providing customer service for incidents whenever they occur. Also, since the time required to adopt the services is short, there are even cases where the services are adopted as a measure while a targeted e-mail attack is already occurring.

Security event monitoring services used to be adopted with the goal of acquiring and storing logs in compliance with internal regulations and other such standards, but recently they have been adopted with increasing frequency in order to proactively detect cyber-attacks. It is possible to detect suspected incidents essentially in realtime by applying optimal detection rules based on past results using large amounts of collected logs. Also, by additionally using support services provided by expert engineers, not only is it possible to greatly reduce the time required to handle incidents after detection, the progression of damage can also be held in check. As a result, the effects of damage are either eliminated or minimized (see Fig. 5).

CONCLUSIONS

This article discussed managed security services, which are a set of comprehensive security measures designed to protect social infrastructures and information systems from increasingly complicated and sophisticated cyber-attacks.

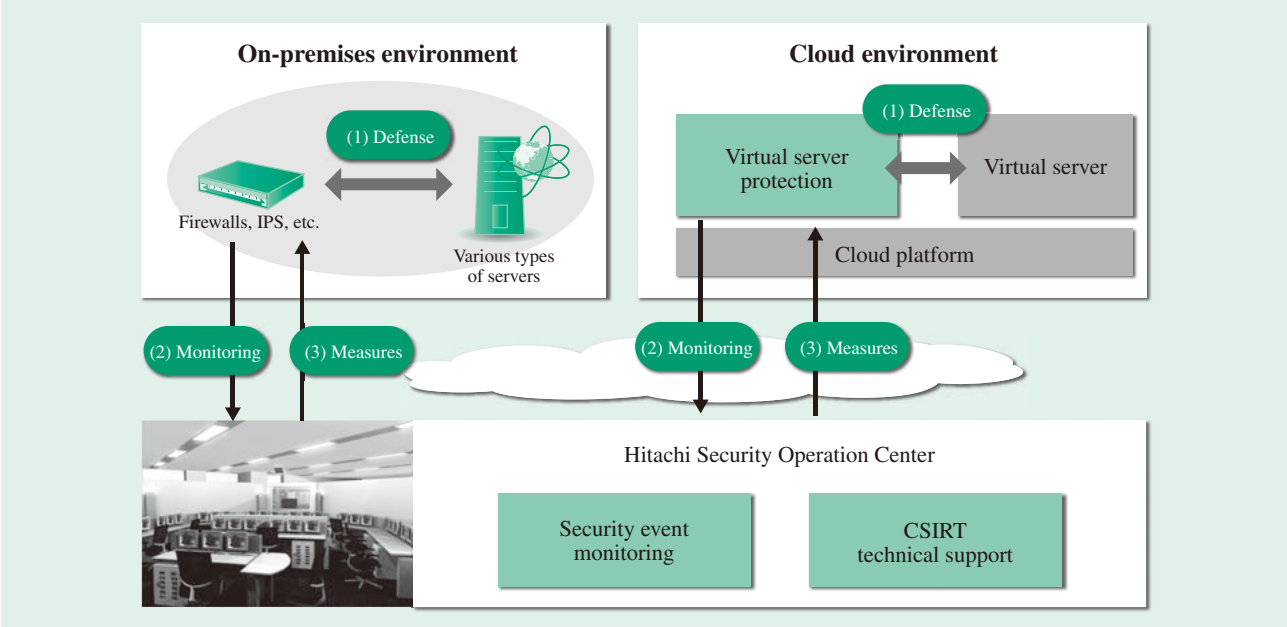


Fig. 5—Security Event Monitoring Service Overview.
These services can be provided for both on-premises and cloud environments. This diagram shows the relationship between defense, monitoring, and measure security operations available as outsourcing services.

Hitachi is itself dealing with a wide range of security issues as a group of companies, from diversifying system environments to cyber-attacks that are growing more advanced. As part of this process, group members with specialized skills use their knowledge to select countermeasures, and the security measures that represent the best practices are implemented. Efforts to expand menu options for managed security services will continue through the utilization of know-how that has actually been applied and the latest technologies. These efforts are aimed at achieving social innovation, and are based on infrastructure technology that has been cultivated over many long years, advanced IT, and security measures. This is why in addition to corporate systems, Hitachi is strengthening security measures that can be applied to social infrastructure systems including control systems as well.

Hitachi will continue to work towards solutions on all sorts of issues in partnership with its customers, thereby contributing to the achievement of a safe and secure society.

REFERENCE

(1) "Information Security Advisory Board: Recommendations to the Ministry of Internal Affairs and Communications Regarding the Promotion of Information Security Policies" (Apr. 2013), http://www.soumu.go.jp/main_content/000217000.pdf in Japanese.

ABOUT THE AUTHORS

Yoshitaka Narishima
Systems Department1, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in proposal and implementation of security services.

Shinichi Kasai
Systems Department1, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in proposal and implementation of security services.

Takayuki Sato
Systems Department1, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in development and proposal, and implementation of security services.

Masaki Mori
Secureplaza Business Promotion Department, Security Solution Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd. He is currently engaged in sales of security solutions, including security services.

Akihiko Fujita
Network Services Division, Cloud ICT Service Business Group, Hitachi Systems, Ltd. He is currently engaged in development and proposal, and implementation of security services.

Featured Articles

Automatic Malware Analysis Technology to Defend against Evolving Targeted Attacks

Hirofumi Nakakoji
Tetsuro Kito
Tomohiro Shigemoto
Naoki Hayashi
Shingo Yamashita

OVERVIEW: As the malware used in targeted attacks has grown more advanced in recent years, the number of cases where existing inbound measures have failed to detect attacks and allowed incursions into the organization has increased. In a situation such as this, it is necessary to clarify the characteristics of the intruding malware so that countermeasures can be taken quickly to prevent the damage from expanding. A dynamic analysis method is used in order to clarify the malware's characteristics, by running the malware in a special analytical environment for behavior observation. Recently, however, types of malware that avoid analysis in analytical environments by restricting execution environments have been growing more common. Malware also exists that attaches to confidential information in a parasitic fashion, and this makes it difficult to simply outsource the malware for external analysis work. In response, the multimodal malware analysis system executes malware under a variety of different analytical environments, so that malware that only runs under a specific environment can still be automatically analyzed. By operating this system in a standalone capacity, it is possible to clarify the characteristics of malware within one's own organization, without the need to rely on external services.

INTRODUCTION

EVER since the world's first computer virus was confirmed in the 1970s, computer administrators have spent the last almost half of a century in confrontation with constantly evolving computer viruses. In the present era, with the wide range of different viruses that exist, any software developed with malicious intent is referred to by the general term "malware," including the computer viruses that generally represent the entire category. As for the targeted attacks and other cyber-attacks that have been making waves recently, malware is being used by increasingly professional criminals as a tool for purposes such as the extraction of money and confidential information, or the destruction of infrastructure systems. To this end, the malware is itself becoming even more advanced, diversified, and sophisticated, and this makes it more difficult to protect against malware using traditional inbound measures such as firewalls and pattern matching.

On the defending side as well, training in targeted attack measures is being conducted among employees as part of a defense strategy against targeted attacks, and operational measures such as improving the security literacy of employees are also being carried out as well as technical solutions. Thanks to the success of these initiatives, information system departments are receiving more reports and samples from employees who have received suspicious e-mail, and this has increased opportunities to acquire unknown malware that existing security measures could not detect, that is, samples that seem to be malware. The information system department then determines whether or not the sample is malware from the perspectives of incident prevention and countermeasures and, if the sample was indeed malware, clarifies the functions of the malware while considering how to respond if the employee's system was infected. It is important to take internal and outbound measures at an early stage in order to prevent damage from occurring or spreading.

This article describes the multimodal malware analysis system that can efficiently clarify the behavior of malware by automating the process that used to be performed manually by malware analysts with advanced and specialized knowledge.

ISSUES IN MALWARE ANALYSIS

Analysis by an expert is necessary to determine if a sample is malware, and what functions the sample possesses as such. A static analysis method employs reverse engineering and other techniques to analyze samples without executing them, while a dynamic analysis method actually executes the samples under a special analytical environment in order to observe their behavior. Although static analysis has the benefit of enabling the detailed clarification of every one of the sample's functions, it is extremely costly because it requires someone with a deep understanding of programs, operating systems (OSs), hardware, and other mechanisms to decipher each individual line of code. Dynamic analysis, on the other hand, can be used to analyze samples that employ obfuscation (code encryption, etc.) without the need to work directly on the samples, and so analysis can be performed relatively quickly in comparison with static analysis. Although dynamic analysis has the advantage of allowing for the confirmation of behavior that is not clarified through static analysis alone (such as behavior after new malware is downloaded from the Internet and executed), it also suffers from a shortcoming whereby the behavior of functions that do not activate themselves during observation cannot be clarified. Usually, when a sample is analyzed, the properties of the sample, the goals of analysis, and the experience of the analyst will be used as a basis to determine how to combine and implement static and dynamic analyses in complementary ways.

Analytical software that supports dynamic analysis has been developed recently, and the open-source software (OSS) Cuckoo Sandbox[(1)] can be downloaded from the website. This type of software employs virtualization technology to safely execute samples within a sandbox (analytical environment), and enable detailed results of observing network communications and application programming interface (API) calls to be acquired, which is why most of the experts who analyze such samples use it in their work. Security vendors are also providing sample behavior analysis services such as ThreatExpert[(2)]* so that the results of analysis can be acquired by submitting samples over the Internet.

As described above, it has become comparatively easier than before for the defending side to analyze samples, thanks to the evolution of technology and tools. Recently, however, the developers of malware have been incorporating mechanisms into the malware they create to avoid detection and analysis, whereby the malware detects the configuration of hardware and software, including the virtual or debugging environment, the version of the OS, installed applications, and so on. The detected information is used by an environment-dependent malware, whose existence has been confirmed, to determine whether or not it is within the environment of its attack target, so that it can change its behaviors accordingly. It has also been confirmed that "downloader" malware exists that downloads secondary malware from a malware distribution server prepared by the attacker, so that the attack can be carried out in stages. There are also malware distribution servers that conceal themselves by checking the Internet Protocol (IP) address of the accessing malware, only distributing secondary malware if the IP address matches that of the target organization, and distributing legitimate content otherwise.

There are many cases where the behavior of malware equipped with this type of mechanism cannot be clarified using existing dynamic analysis software that only works under a specific, previously prepared environment. Also, since malware distribution servers will act as legitimate servers with respect to outsourced external analysis services whose IP addresses do not match that of the organization targeted for attack, the analysts will not be able to clarify the malware's behavior. The existence of malware that acts as parasites in Portable Document Format (PDF) documents and other files that can include confidential information has also been confirmed, and so increasing numbers of companies are hesitant to rely on external services for sample analysis, since the malware is connected to the confidential information. This increases the need for an ability to clarify the characteristics of malware in-house.

In order to resolve these types of issues, the Yokohama Research Laboratory of Hitachi, Ltd. is working on the research and development of technology that can automatically analyze samples under multiple types of analytical environments using dynamic analysis and determine whether or not a sample behaves as malware, as well as the characteristics of the sample.

MULTIMODAL MALWARE ANALYSIS SYSTEM

The multimodal malware analysis system improves the success rate of analysis of environment-dependent malware by employing multiple types of

* ThreatExpert is a trademark of Symantec International Corporation.

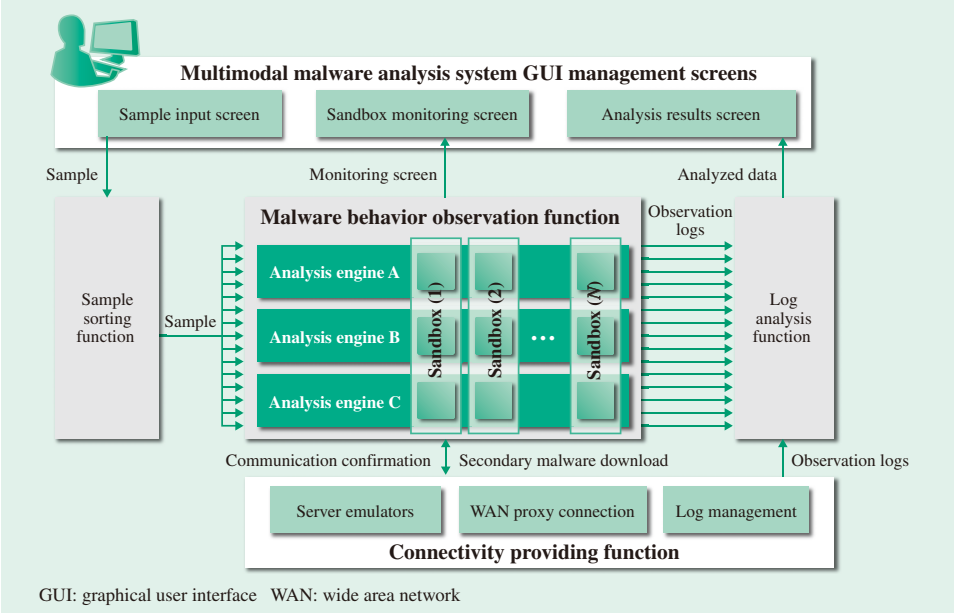


Fig. 1—Multimodal Malware Analysis System Architecture. Multiple types of sandboxes (analytical environments) are prepared to ensure that it is easy for malware to infect and operate, and obtained behavior observation logs are automatically analyzed based on previously acquired analysis know-how in order to create reports. This mechanism automates and speeds up the analytical work previously performed by experts using advanced techniques, while simultaneously achieving a high success rate.

analysis engines and sandboxes during analysis. The architecture of this system is shown in Fig. 1.

When an analyst analyzing a sample that appears to be malware uses the system's sample input screen to input (upload) a sample, that sample is copied by a sample sorting function and simultaneously input into multiple sandboxes configured for use by the malware behavior observation function. Each copy of the input sample is automatically run in the sandboxes, the behavior is observed, and results are output to logs. A log analysis function then gathers the extremely large logs output by the malware behavior observation function (in some cases, millions of lines can be generated for a single sample, amounting to several gigabytes of data), analyzes statistics for the states of activities performed by the samples in each sandbox (file access, registry access, network access, and so on), and extracts files generated by the samples along with any uniform resource locators (URLs) it connects to over the network. Since these processes are automatically run in parallel, the time required for analysis can be greatly reduced, and analysis jobs can be run in overnight batches.

The features of this system are described below.

Malware Behavior Observation Function

The multimodal malware analysis system improves the success rate of environment-dependent malware analysis by analyzing samples in several dozen types of sandboxes. The group of sandboxes is configured using combinations of different analysis engines, hardware, software types and versions, settings, and so on. Although the success rate of environment-dependent malware analysis increases with larger numbers of sandbox variations, since there are limitations in physical machine resources and licenses, preparing every possible combination is not practical.

The sandbox configurations of this system were defined based on the following five selection elements: (1) analysis engine, (2) hardware, (3) architecture, (4) OS, (5) application (see Table 1).

Of these selection elements, three types of analysis engines are used for the multimodal malware analysis system, including the aforementioned Cuckoo Sandbox. Since different virtual machines are supported by different types of analysis engines, the use of multiple types of analysis engines can be expected to be effective not only in terms of analytical performance, but in terms of analyzing malware with virtualization function detection functions as well.

Since there are such an extremely large number of variations, including types and versions of both operating systems and applications, this leads to combinatorial explosion when one considers the various combinations that are possible. This system is designed to infect sandboxes with malware in order to clarify as much of the behavior as possible, and so the selection of environments that are easy for malware to infect and operate in from the perspective of the malware developer (in other words, environments that are most likely to be affected by attacks) is given priority. This is why the OS configurations are designed to differentiate between major operating systems and service packs starting with Windows

TABLE 1. Execution Environment Selection Elements
The five selection elements defined for each execution environment are the analysis engine, hardware, architecture, operating system (OS), and applications.

Analysis engine	Hardware	Architecture	OS	Application
Analysis engine A	• Physical machine • Virtual machine (VMware*1 ESXi)	• 32 bit (×86) • 64 bit (×64)	• Windows*3 XP (SP x) • Windows Vista*3 (SP x) • Windows 7 (SP x)	• Microsoft*3 Office xxxx • Adobe*4 Reader*4 xx • Internet Explorer*3 xx • Adobe Flash*4 Player xxx.x • JRE x.x • Windows Media*3 Player xx
Analysis engine B	• Virtual machine (Oracle*2 VM VirtualBox)			
Analysis engine C	• Virtual machine (VMware Workstation)			

JRE: Java*2 Runtime Environment
*1 VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions.
*2 Oracle and Java are registered trademarks of Oracle and/or its affiliates.
*3 Microsoft, Internet Explorer, Windows, Windows Vista, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
*4 Adobe, Adobe Reader, and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

XP, which is reported as being frequently infected by malware. In the application configurations as well, applications with a large number of vulnerabilities (in other words, applications for which vulnerability information has been published a large number of times), are given priority during selection. Information in the JVN iPedia Vulnerability Countermeasure Information Database(3) from January 1, 2012 to August 16, 2013 is used to investigate the number of instances of vulnerability information being published.

Connectivity Providing Function

Recent types of malware are known for using network connection functions to connect to a malware distribution server and download secondary malware, or to connect to a Command and Control (C&C) server in order to receive remote control operations. Also, it has been confirmed that there are some types of malware that attempt to avoid analysis by verifying network communications immediately after infection, to ensure that they have not been copied into an analytical environment.

The multimodal malware analysis system has the connectivity providing functions shown in Fig. 1. This includes functions that emulate servers inside the sandbox in order to respond to various requests from samples directed at major server types including Web servers, File Transfer Protocol (FTP) servers, and Domain Name System (DNS) servers, as well as Wide Area Network (WAN) proxy connection functions (under development) to communicate with malware distribution servers and C&C servers through a proxy connection to the Internet. This allows the behavior of downloader malware to be reproduced with a high degree of accuracy, from when the malware downloads files from specific Web servers through the execution of those files.

Log Analysis Function

The log analysis function identifies the behaviors unique to malware from the extremely large amounts of log data acquired from several dozen different types of sandboxes. The function design (formal knowledge) of the identification algorithms was based on the advanced malware analysis know-how (implicit knowledge) from malware analysis specialists with excellent track records. A number of analytical functions are introduced below:

(1) Determination of the presence or absence of a debugger detection function
(2) Determination of the presence or absence of process injection
(3) Determination of the presence or absence of timed execution
(4) Determination of an external network connection

The behavior detected here often appears as part of the series of illicit activities conducted by malware. For this reason, determining whether or not these behavior patterns are present is a useful method of extrapolating whether or not a sample is actually malware. Inventive techniques based on analytical know-how are also applied as part of each item's determination methods. For instance, during the determination of the existence of an external network connection, multiple types of API calls including minor network connection methods used to avoid detection by malware analysts are monitored, and determination takes a multifaceted approach by analyzing data such as communications traffic and connectivity providing function logs.

Display of Analytical Results

The multimodal malware analysis system has both a function that displays a summary of the operational results of samples in several dozen types of sandboxes, and a function that consolidates and displays a list

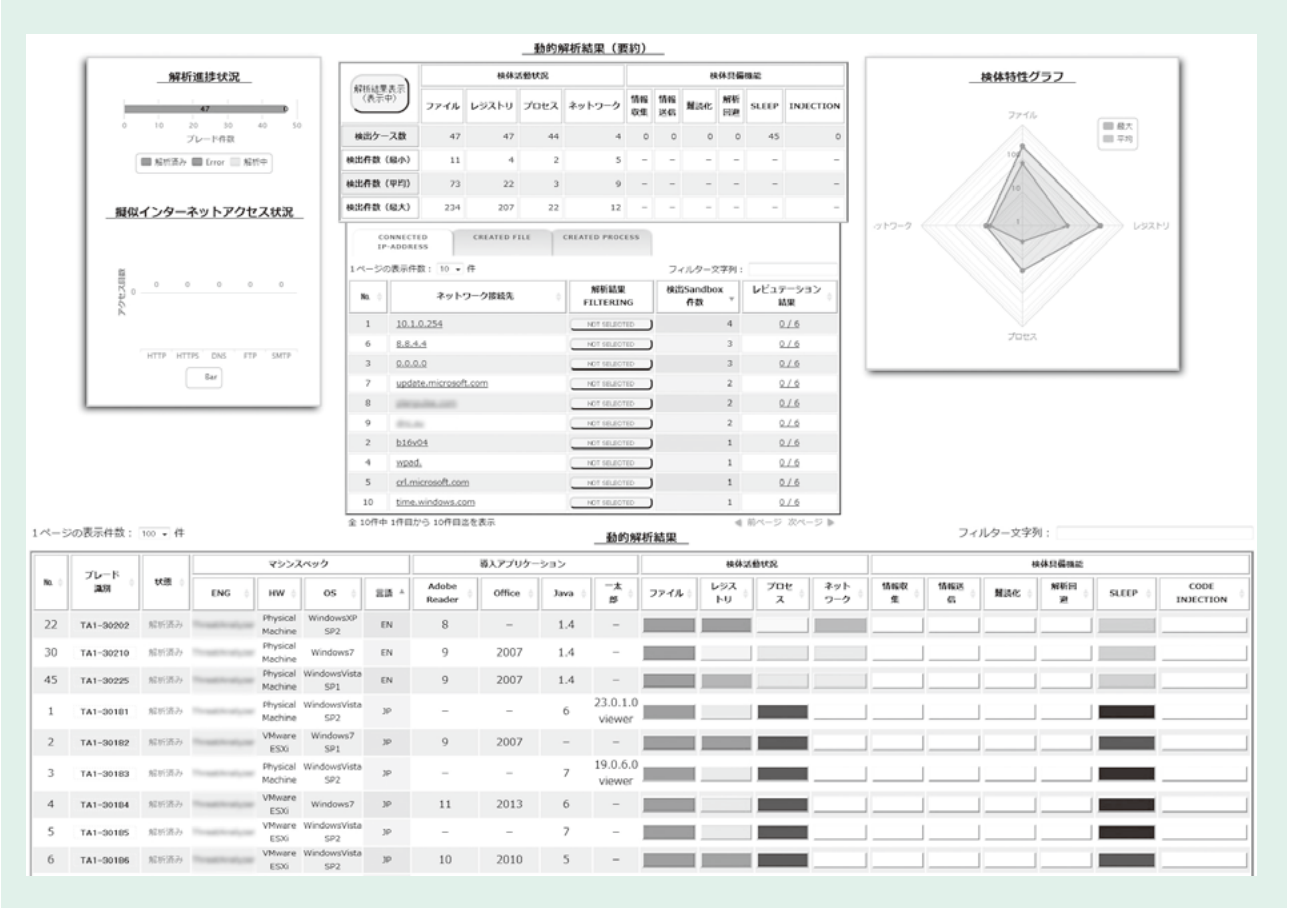


Fig. 2—Sample Analysis Results Screens.
A screen that displays a summary of the malware operational results of several dozen types of sandboxes is provided (top), along with a screen that displays a consolidated list of analytical results for each separate sandbox (bottom).

of analytical results for each separate sandbox (see Fig. 2).

This screen can be used to verify the followings: The URLs connected to by samples; created files; generated process information; the detection results obtained by matching the samples against 16 types of antivirus software pattern files. If a sample is malware, then it is a simple matter to grasp the state of antivirus software support, the URLs that it might connected to over the network if an employee's computer terminal is infected with that malware, any traps placed on employee terminals (malware-related files), and so on. By taking countermeasures such as using this information and a firewall, proxy, or some other method to prohibit communications with the connected URLs, and adding disinfection information to the pattern files of antivirus software, it is possible to utilize defense in depth whereby internal measures and outbound measures are applied if an infection or outbreak occurs in an employee's terminal due to malware slipping past the inbound measures.

MULTIMODAL MALWARE ANALYSIS SYSTEM VERIFICATION

The following is a report of analysis results obtained by using a prototype multimodal malware analysis system in order to analyze several hundred types of samples that appear to be unknown malware, not detectable using the antivirus software of a certain security vendor's antivirus software.

Approximately 80 types of sandboxes were used for this verification work, and it took around 15 minutes per sample to complete the analyses (this was the time required to test a single sample in 80 different sandboxes). Approximately 73% of all the tested samples connected to an external server that appeared to be related to an illegitimate site, and this reconfirms the fact that malware in recent years is characterized by the property of using network connections. Also, by analyzing the malware in sandboxes that reproduce the multiple types of analytical environments that characterize the multimodal malware analysis system,

it was possible to verify the existence of environment-dependent malware that manifests under the following conditions:
(1) Samples that only activate themselves under environments where Microsoft Office 2007/2010 is installed
(2) Samples that only activate themselves under Windows XP
(3) Samples that only activate themselves under a physical environment
(4) Samples that only activate themselves under a physical environment running Windows 7 (except with Service Pack 1)
(5) Samples that do not activate themselves under VMware ESXi or VMware Workstation, but do activate under Oracle VM VirtualBox

In other words, this shows that samples with these properties are difficult to analyze using dynamic analysis under an environment that does not match the proper operating conditions.

Through this verification work, it was confirmed that it is possible to automate malware analysis and clarify the illicit behavior of unknown malware, as well as execute and clarify the behavior of environment-dependent malware. Also, by extracting the number of sandboxes where malware manifests its network connections and other behavior, as well as commonalities in sandbox environment configurations where the behavior manifests, it is possible to derive how easy it is for the malware to manifest, in addition to the environmental conditions under which the environment-dependent malware executes. This type of information can be applied as clues during the construction of analytical environments for use in more detailed analysis.

CONCLUSIONS

This article described the multimodal malware analysis system that automatically clarifies the behavior of suspicious files used in targeted attacks using dynamic analysis, by reporting on the details of the malware's activities.

This system is integrated into a half-rack, all-in-one system designed to operate in a standalone capacity. Since the system can be used as a standalone system for analyzing the behavior of malware, it can analyze downloader malware that only downloads secondary malware from a specific IP address, and samples that are treated as confidential information can be kept within the organization during analysis. By installing this system in the organization's information system department or security operations center, not only is it possible to greatly reduce the cost of malware analysis work performed by experts, this also allows organizations without experts to easily clarify malware threats. This can be expected to have a beneficial effect on defense in depth measures against the latest targeted attacks and other types of cyber-attacks by making it easier to grasp the state of damage, among other benefits.

A safe and secure information technology (IT) environment will be achieved through further reductions in analysis time, expanded log analysis functions, and continued research in automated countermeasures based on information regarding the properties of malware as obtained by this system.

REFERENCES

(1) Claudio "nex" Guarnieri & Cuckoo Sandbox Developers, "Automated Malware Analysis—Cuckoo Sandbox," http://www.cuckoosandbox.org/
(2) ThreatExpert Ltd., "ThreatExpert—Automated Threat Analysis," http://www.threatexpert.com/
(3) JPCERT/CC and IPA, "JVN iPedia—Vulnerability Countermeasure Information Database," http://jvndb.jvn.jp/en/

ABOUT THE AUTHORS

Hirofumi Nakakoji

Enterprise Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of measures against cyber-attacks. Mr. Nakakoji is a member of the Information Processing Society of Japan (IPSJ).

Tetsuro Kito

Enterprise Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of measures against cyber-attacks. Mr. Kito is a member of the IPSJ.

Tomohiro Shigemoto

Enterprise Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of measures against cyber-attacks. Mr. Shigemoto is a member of the IPSJ.

Naoki Hayashi

Enterprise Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of measures against cyber-attacks.

Shingo Yamashita

Defense Information Systems Division, Hitachi Advanced Systems Corporation. He is currently engaged in development of information security products.

Featured Articles

Trends and Developments in Security Standards for Secure Social Infrastructure Systems

Tsutomu Yamada
Tadashi Kaji, Dr. Info.
Toshihiko Nakano, Ph.D.

OVERVIEW: Consolidation of standards suitable for control systems is an urgent task that must be accomplished if control system security is to be improved. When it comes to control system security standards, the consolidation of industry standards is happening more quickly, but international standards are also being formulated with four out of the 13 documents of the IEC 62443 series of standards already published. Also, ISASecure EDSA and CSMS certification are standards for certifying conformance with security rules by control systems and control devices. The rapid acquisition of international certifications in terms of security is also important from the perspective of strengthening international competitiveness, and the Ministry of Economy, Trade and Industry is implementing a pilot project in order to enable the acquisition of these certifications from inside Japan. Hitachi is contributing to standardization activities aimed at the utilization of these standards.*

INTRODUCTION

GOVERNMENT agencies and industries in various countries are carrying out foundational activities aimed at improving the security of the control systems that support social infrastructures. In the past, on-site information has been utilized in operations and management in order to increase efficiency and productivity in social infrastructures and on factory floors. Also, aimed at increasing both affinity with information systems and development efficiency, information technology (IT) has been incorporated into many control systems, both in terms of operating systems (OS) and the field of network technology. At the same time, the Stuxnet computer virus, which was discovered in 2010, was created targeting specific control systems. This reminded many responsible parties, industries, and government agencies with a connection to control systems about the importance of security.

However, the additional installation of information system security technologies to control systems is often problematic. This is because since only limited computing power is available in controllers and various other types of devices, modifying configurations has a major impact on processing overhead. In general, the availability and integrity of the protected assets are given priority in control systems, and so the confidentiality that is emphasized in information systems has a relatively lower priority. Also, the facilities and external environments must also be protected, including the control devices themselves, in addition to information.

In other words, measures must be suited to the control systems if control system security is to be strengthened. Since control systems are used in countries around the world, it is effective to apply standards that can be evaluated from a shared, international perspective as security countermeasures and guidelines. This is why government agencies from various nations, standards bodies, and industry groups are working to formulate standards and guidelines in the area of control system security.

This article provides a general overview of control system security standards, representative standardization efforts, and trends as well as the current state of various types of certification systems aimed at improving security.

INTERNATIONAL AND INDUSTRY STANDARDS

Overview

When it comes to security standards, the ones in the field of IT are leading the way. For instance,

* ISASecure is a trademark of ASCI.

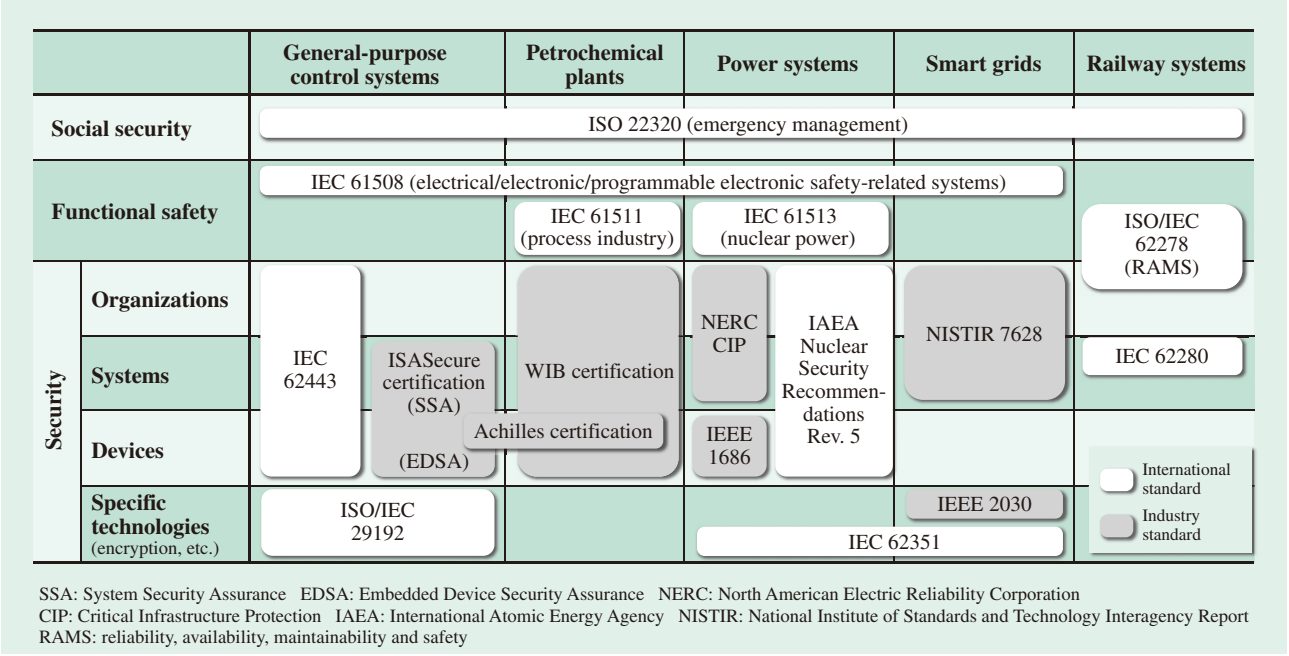


Fig. 1—Overview of Standards Related to Control System Security.
The diagram indicates which standards in each field are international, and which are industry standards.

Common Criteria (ISO/IEC 15408[1]) is utilized in the procurement of security related products. In order to counter the same threats as exist in the IT field, many control system security standards reference physical security standards[2] as well as IT security standards. Of these interrelated standards, this article will focus in particular on trends in control system security standards.

Fig. 1 shows an overview of international and industry standards regarding control system security. The diagram indicates which standards in each field are international, and which are industry standards. In addition to security standards, functional safety standards with a close relationship to the safe operation of control systems are included.

Starting in the 2000s, standards came together comparatively quickly in each industry, in response to the demands of control system user. In the diagram, this would be the ISASecure standard[3], the WIB standard[4], and Achilles certification[5]. In many cases, certification frameworks have also been provided along with the standards. These companies and organizations are in the business of guaranteeing that products that comply with the standards achieve a certain level.

As a related trend, the president of the USA is moving forward with security efforts in the area of countering the threat of cyber-attacks[6]. The National Institute of Standards and Technology (NIST) has also issued a cybersecurity framework[7]. While this framework is not legally binding, it does act as a guideline for ensuring corporate security, and the trend towards treating this guideline as a de facto standard must be noted.

Although they are lagging a bit behind the industry standards, international standards are being launched. At present, work is being done on consolidating the IEC 62443 standards, which address control systems overall. Also, in order to protect the crucial infrastructure of power systems, the US government has prepared the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)[8] as a security standard for the power industry, and the standard has already gone into effect.

Hitachi has established guidelines for the secure construction of control systems based on the specifications demanded by these standards. In order to construct a system whereby continuous security measures are possible, these guidelines are utilized while following the security implementation policy for control systems as described in the featured article “Control System Security for Social Infrastructure” (see p. 277 in this issue).

IEC 62443

IEC 62443 is a series of international standards that is drawing attention. The overall framework is shown in Table 1.

TABLE 1. General Framework of IEC 62443 Standards
The general framework of IEC 62443 standards is provided below.

Standard No.	Standard name	Overview
IEC/TS 62443-1-1 (published)	Terminology, concepts and models	Terms, concepts, and model definitions
IEC/TR 62443-1-2	Master glossary of terms and abbreviations	Terms and abbreviations
IEC 62443-1-3	System security compliance metrics	System safety evaluation criteria
IEC/TR 62443-1-4	IACS security life cycle and use case	IACS security life cycle and use cases
IEC 62443-2-1 (published)	IACS security management system - Requirements	IACS security management system requirements
IEC 62443-2-2	IACS security management system - Implementation guidance	IACS security management system implementation guidelines
IEC/TR 62443-2-3	Patch management in the IACS environment	Guidelines regarding patch management methods for IACS
IEC 62443-2-4	Requirements for IACS solution suppliers	Security practices for IACS equipment vendors
IEC/TR 62443-3-1 (published)	Security technologies for IACS	List of security technologies that can be used in IACS
IEC 62443-3-2	Security levels for zones and conduits	Safety assurance levels for zone and conduit concepts
IEC 62443-3-3 (published)	System security requirements and security assurance levels	System security levels and corresponding function requirements
IEC 62443-4-1	Product development requirements	Component development process rules
IEC 62443-4-2	Technical security requirements for IACS components	Component security function requirements

IACS: Industrial Automation and Control System

IEC 62443 is comprised of a total of 13 documents. The IEC 62443-1-x series comprises general standards, and deals with basic concepts, models, and terminology. The IEC 62443-2-x series is for asset owners, and deals with security policies as well as the systems used to manage organizations and people. The IEC 62443-3-x series is for system integrators, and deals with the technology requirements of control systems. The IEC 62443-4-x series is for equipment vendors, and deals with the security requirements of the control devices that constitute a system.

An overview of the standards in the IEC 62443 series that have already been published is provided below.

(1) IEC/TS 62443-1-1[9]

Stipulates basic security requirements for control systems. The seven requirements are access control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability.

(2) IEC 62443-2-1[10]

Describes risks that the asset owner must manage in systems, and the cybersecurity management system (CSMS).

(3) IEC/TR 62443-3-1[11]

General catalog of security technologies. Describes certification, filtering and access controls, encryption and data certification, managed audit monitoring, software management for personal computers (PC) and other devices, and physical security.

(4) IEC 62443-3-3[12]

Defines four security levels of detailed function requirements for protecting system security according to the seven requirements mentioned above.

Four of the IEC 62443 documents listed in this table have already been published, and the remaining documents are still being formulated at present by the International Electrotechnical Commission (IEC) Technical Committee (TC) 65/Working Group (WG) 10. In order to continuously improve the security of control systems, Hitachi is working with members of the IEC National Committee while contributing to the documentation process.

CERTIFICATION STANDARDS

Clarification of the criteria used to evaluate security coverage and robustness is advisable for asset owners when security is to be adopted for control systems. A security certification framework is an effective way to evaluate security functions. Representative examples of frameworks include ISASecure and CSMS certifications.

ISASecure

The ISA Security Compliance Institute (ISCI)[3] is a subordinate body of the International Society of Automation (ISA)[13] industry group headquartered in the USA. ISASecure is a framework for certifying that the security criteria established by the ISCI are met. The ISCI prepares certification programs for everything that is certified, including Embedded Device Security Assurance (EDSA) certification for control devices, and System Security Assurance (SSA) certification for control systems. Standards have been already been published and certification has begun for EDSA[14], but not yet for SSA.

EDSA certification involves the following three categories of inspection (see Fig. 2):

(1) Communication Robustness Testing (CRT)

Verifies the control device's communication

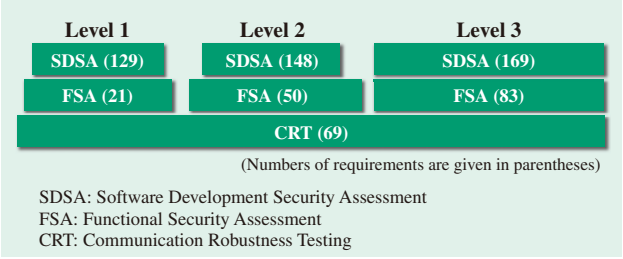


Fig. 2—Numbers of EDSA Certification Requirements. Security test requirements are stipulated based on the certification level to be acquired.

protocols [Ethernet, Address Resolution Protocol (ARP), Internet Protocol (IP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP)]. Specialized tools certified by the ISCI are used to verify normal operation during the protocol inspection.

(2) Functional Security Assessment (FSA)

Verifies the control device's security functions.

(3) Software Development Security Assessment (SDSA)

Verifies the processes used to develop control devices.

With EDSA certification, the CRT uses the same tests at all levels to verify compliance, whereas the FSA and SDSA verifies test items according to the three levels.

CSMS

The CSMS is a management system whereby the asset owner manages risk to a control system while continuously maintaining security. In the case of information systems, this is associated with the control system version of the information security management system (ISMS) established with ISO/IEC 27001. Certification standards are expected to be enacted based on IEC 62443-2-1.

Fig. 3 shows the flowchart for achieving CSMS as illustrated by example in IEC 62343-2-1 Annex B[10]. The achievement of CSMS starts with justifying the CSMS program with the management team [see (1) in the diagram]. Next, threats, probability of realization of threats, vulnerability types, and results are presented [see (2) and (3) in the diagram]. Furthermore, based on the organization's risk tolerance, appropriate policies and organizations are established in order to execute countermeasures [see (4) in the diagram], and countermeasures are selected and adopted [see (5) in the diagram]. After adoption, whether or not the organization conforms with CSMS policies and procedures is verified, as well as effectiveness and the need for any changes in targets [see (6) in the diagram].

CSMS certification involves verifying whether or not the asset owner can implement the flowchart for managing security maintenance.

VARIOUS TRIAL CERTIFICATIONS

From the perspective of strengthening competitiveness, in order to successfully deploy control systems overseas, it is important to rapidly acquire certifications that are accepted internationally. Therefore, the Ministry of Economy, Trade and Industry is leading a pilot project in order to enable the domestic acquisition of the two aforementioned certifications in Japan.

Agencies within Japan already provided a framework for the information system security standards ISMS and ISO/IEC 15408, and the goal is to prepare the same type of framework for control systems as well. The Control System Security Center (CSSC) technological research association is conducting a pilot EDSA certification program. The Japan Information Processing Development Center (JIPDEC) has a pilot certification program for CSMS certification.

Certification criteria and guidelines are being prepared for both EDSA and CSMS certification. Hitachi is cooperating with responsible organizations in the establishment of both types of certification, and provides security solutions for customer systems while applying these standards.

CONCLUSIONS

Establishing security standards for control systems and achieving certification will help raise levels of security even further. Hitachi is contributing to standardization activities in order to develop the infrastructure of security technology.

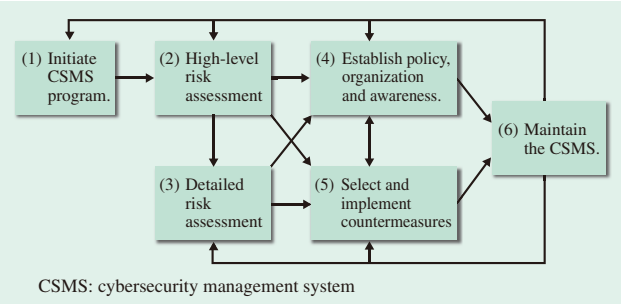


Fig. 3—CSMS Achievement Flowchart. Procedures are stipulated for control system risk assessment and security maintenance management.

Since it will take some time before security in control systems is seen from the perspective of international standards, other measures must also be implemented. To this end, it is important to comply with international and industry standards while at the same time engaging in research and development supporting the latest security technology and providing solutions.

REFERENCES

(1) ISO/IEC, "ISO/IEC 15408, Information Technology—Security Techniques—Evaluation Criteria for IT Security—"
(2) U.S. Department of Defense, DoD Manual 5100.76-M, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives."
(3) ISA Security Compliance Institute, http://www.isasecure.org/
(4) WIB, http://www.wib.nl/
(5) Wurldtech, Wurldtech Certification, http://www.wurldtech.com/product_services/certifications/
(6) President's Council of Advisors on Science and Technology, "Report to the President Immediate Opportunities for Strengthening the Nation's Cybersecurity" (Nov. 2013).
(7) NIST, "Framework for Improving Critical Infrastructure Cybersecurity" (Feb. 2014).
(8) NERC, CIP Standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
(9) IEC: IEC/TS 62443-1-1, "Terminology, Concepts and Models" (July 2009).
(10) IEC: IEC 62443-2-1, "Establishing an Industrial Automation and Control System Security Program" (Nov. 2010).
(11) IEC: IEC/TR 62443-3-1, "Security Technologies for Industrial Automation and Control Systems" (July 2009).
(12) IEC: IEC 62443-3-3, "System Security Requirements and Security Levels" (Aug. 2013).
(13) ISA, http://www.isa.org/
(14) ISCI, "ISASecure Program Description," http://www.isasecure.org/ISASecure-Program.aspx

ABOUT THE AUTHORS

Tsutomu Yamada

Department of Energy Management Systems Research, Hitachi Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of embedded computer architecture, network systems and cybersecurity for industrial control systems. He is a Professional Engineer, Japan (Information Engineering). Mr. Yamada is a member of the IEEE, the International Society of Automation (ISA), The Institute of Electronics, Information and Communication Engineers (IEICE), and The Society of Instrument and Control Engineers (SICE).

Toshihiko Nakano, Ph.D.

Control System Security Center, Omika Works, Infrastructure Systems Company, Hitachi, Ltd. He is currently engaged in the development of security for social infrastructure systems. Dr. Nakano is a member of The Institute of Electrical Engineers of Japan (IEEJ).

Tadashi Kaji, Dr. Info.

Infrastructure Systems Research Department, Information Service Research Center, Yokohama Research Laboratory, Hitachi, Ltd. He is currently engaged in research and development of information security technology. Dr. Kaji is a member of the IEEE Computer Society.

Topics

Using *Capture the Flag* Events as Training Opportunities

INTRODUCTION

Capture the flag (CTF) is a traditional children's outdoor game in which two teams attempt to protect their own flag, while at the same time trying to locate their opponent's flag, capture it, and return it to their own home base in order to win the game. An increasingly popular adaptation of this game has spawned an entire subculture within the computer security community. At Defcon[1], the capture the flag competition is one of the longest running of many well-known competitions, having been introduced in 1996 at Defcon 4.

CAPTURE THE FLAG VARIATIONS

There are two primary variations of CTF as played in computer security circles. Each offers competitors a chance to put into practice skills from all facets of the computer security field with the ultimate goal of retrieving "flags" that may be delivered to the contest organizers in order to demonstrate that a particular challenged has been solved or a particular goal met.

Perhaps the most well-known version of CTF is the version that has come to be known as the "Defcon-style" CTF. The Defcon CTF is a *full-spectrum* CTF played by a limited number of teams in a live, head-to-head event. At Defcon, the scale of this game has grown from eight teams to its current size of 20 teams that compete at a live event over the course of three days in Las Vegas, Nevada every summer. In a full-spectrum CTF, the event organizers provide each team with identical server images pre-configured with custom software developed by the organizers. Each team's server is connected into an isolated game network dedicated to the competition. Each team is required to simultaneously administer and defend their own server while attempting to penetrate the defenses crafted by each of the other teams in order to capture flags which are turned in to the organizers in exchange for points.

The rules for a full-spectrum CTF are intentionally unrestrictive in order not to limit the creativity of each team in building novel defenses. In order to prevent teams from shutting down vulnerable software as a means of defending it, teams are typically graded on their ability to continue providing these "services" to the public, which includes the organizers who periodically test whether each team's software remains accessible both to the organizers and to other teams. There is an expectation that teams patch any flaws that they find in their assigned software rather than simply shutting the software down.

As teams find flaws in their own software and come to understand how they may themselves be vulnerable to attack, they also understand that every other team playing the game is also vulnerable to the same attack. Consequently, teams attempt to use each flaw to penetrate their opponent's servers and, following each successful penetration, retrieve a flag from their opponent. Flags are placed on each team's server by the organizers and are periodically replaced in order to provide new flags to capture throughout the game. This periodic rotation of flags forces teams to repeatedly demonstrate that they can maintain access into their opponent's servers and allows for the gradual evolution of both defenses and offenses as the game progresses.

The Defcon CTF has become so popular that hundreds of teams attempt to qualify to play in the Defcon CTF every year with many of these teams spending months of preparation time in the hopes of earning a trip to Las Vegas. Increasingly the Defcon CTF is becoming an international event. Prior to

2006 competitors at Defcon consisted solely of American teams. In 2006, the first international team, from South Korea, qualified and participated in the Defcon CTF. In 2013, two-thirds of the participating teams at the Defcon CTF were international teams including teams from Japan, South Korea, China, Russia, and mixed European teams.

A number of other full-spectrum CTFs have developed since the first Defcon CTF. Most of these are open primarily to academic institutions with the most well-known of these being the University of California, Santa Barbara's iCTF (International CTF) competition which has become the largest scale full-spectrum CTF in existence. In 2013, the iCTF hosted 90 teams from around the world in an eight-hour live event.

The second variation of CTF is based on the concept of solving puzzles in order to be awarded points. In a puzzle CTF, organizers develop a number of security-related challenges and make them available to participants for solving. Participants do not interact with one another; instead teams race to be the first to solve puzzles and to gather the most points.

The infrastructure to host a puzzle CTF resembles a traditional web site on which the puzzles are posted more than a live network battle ground. This makes it somewhat easier to host puzzle CTFs and allows far more teams to participate in a live puzzle-style event. In many cases 500 or more teams may be competing simultaneously to see who can win the event. A puzzle-style event is used as a qualifying event for the Defcon CTF, allowing hundreds of teams the opportunity to compete for a chance to compete in the live Defcon event.

Because they lack a head-to-head component, puzzle-style events often offer a wider variety of challenges across a larger number of security-related skills than full-spectrum events. Categories present in puzzle-style events often include reverse engineering, cryptography, forensics, packet analysis, web security, network reconnaissance, and many others.

Between these two types of events, CTF has become so popular that it is possible to find a CTF of one type or the other taking place almost every week of the year. In fact an entire online community has emerged and is tracked by sites such as ctftime.org[3], which offers both a comprehensive calendar of events as well as results tracking and team ranking. The ranking system in particular highlights both the popularity of CTF and the increasingly competitive nature of the events.

BEYOND THE COMPETITIONS

While CTF events themselves are great fun for all participants, there is much more to CTF than just solving challenges. CTF offers a small window into the computer security field and the games and the excitement surrounding the games are both a great way to introduce new people to the computer security field, identifying talented individuals within specific security disciplines, and a way for established security professionals to showcase their skills.

One of the great opportunities available through CTF is to be able to introduce computer security to young students as a non-traditional introduction to the computer science field. When appropriately packaged, a CTF for young students can both demonstrate the dynamic nature of the computer security field and gently introduce young people to the security problems they are faced with through their everyday interaction with technology. In particular, the media often speaks of the dangers

that are present when using social media. Younger users often see social media as a convenience, a necessity, and an expectation without understanding the risk they may be exposing themselves to through reckless use of such technologies. A well designed CTF can go a long way towards raising awareness and increasing interest in computer security at ages where traditional computer programming may be too difficult to introduce.

As CTF evolves, or more specifically as organizers consider how they might evolve their games, one of the most important ways that CTF can become even more useful is to package CTF as a complete training opportunity in which the organizers provide training in CTF-specific skills, which mirror the skills of everyday security practitioners, leading up to an actual CTF event. Since the organizers typically have complete visibility into their CTF infrastructure, they are uniquely situated to utilize the data they collect, to include packet capture and event timelines, in order to conduct after-event training with participants in which feedback on procedures may be provided along with addressing any shortcomings noted during the event. Used in such a manner, CTF can be a valuable tool both in the workplace as a training opportunity and for the general public as a recruiting tool.

CONCLUSIONS

Japan like many nations faces a critical shortfall in the workplace for skilled computer professionals. Many studies show that it is increasingly difficult to reach younger students and motivate them to pursue education and jobs in the computer field and more specifically in the computer security field. CTF is used in many organizations as a motivational tool as well as a great source of pride when an organization's teams perform particularly well in large competitions. In the United States, companies boast of successful participation in CTF and individuals proudly list CTF on their resumes when applying for jobs in the security field.

As a means of introducing anyone to the computer security field CTF provides a highly interactive way to generate both involvement and interest. While CTF alone is certainly not going to solve the personnel shortage faced by many companies and nations, in a field that lacks innovative ideas for stimulating interest, CTF certainly looks like a good place to start.

REFERENCES

(1) Defcon Computer Security Conference, http://www.defcon.org.
(2) University of California, Santa Barbara iCTF, http://ictf.cs.ucsb.edu/
(3) CTF Time, https://ctftime.org/

ABOUT THE AUTHOR

Christopher Eagle

Christopher Eagle (Chris Eagle) is a Senior Lecturer of Computer Science at the Naval Postgraduate School (NPS) in Monterey, CA. A computer engineer/scientist for 28+ years, his research interests include computer network operations, forensics and reverse engineering. He has been a speaker at conferences such as Black Hat, Defcon, Infiltrate, and Shmoocon and is the author of "The IDA Pro Book," the definitive guide to IDA Pro. He is a multiple winner of the Defcon Capture the Flag Competition and was the organizer of that competition from 2009-2012. He is currently working with DARPA to build their Cyber Grand Challenge competition.