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.

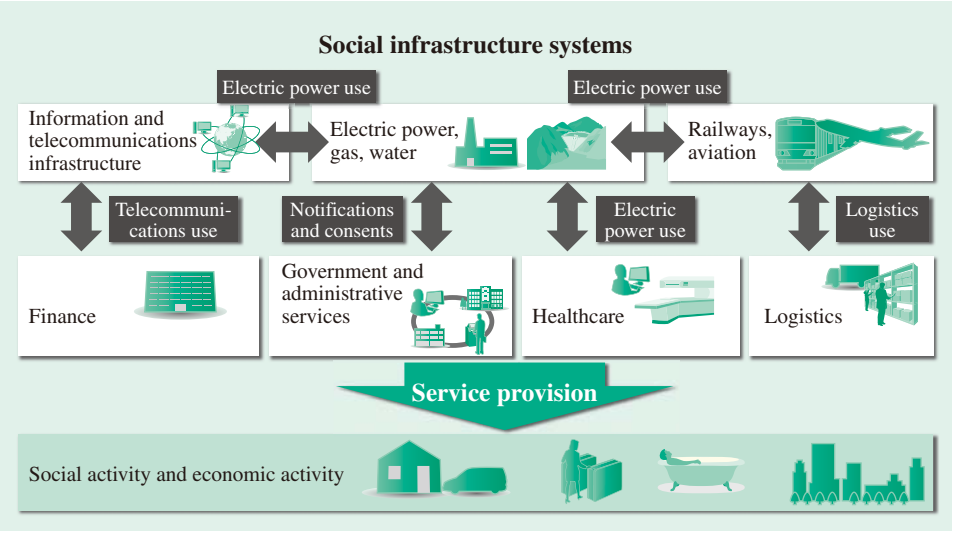


Fig. 1—Social Infrastructure Systems.
Made up of the facilities, equipment, and systems that underpin social activity by people and economic activity by business, the social infrastructure forms an enormous interlinked system comprised of mutually interdependent sub-systems.

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

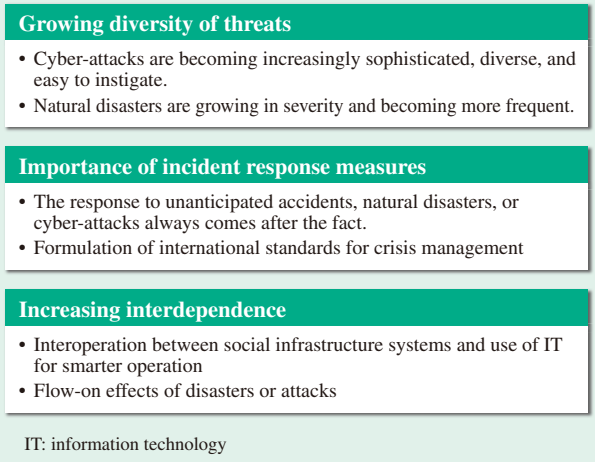


Fig. 2—Trends in Social Infrastructure Security.
Three trends influencing social infrastructure security are the growing diversity of threats, the importance of incident response measures, and increasing interdependence.

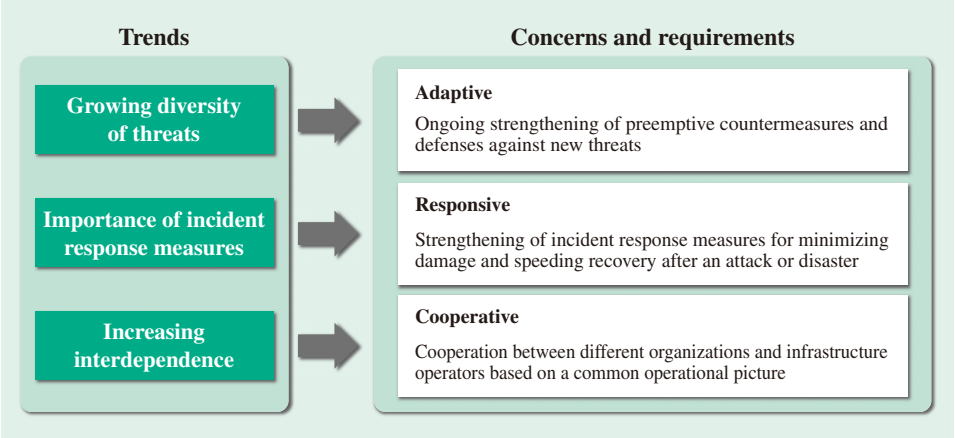


Fig. 3—Requirements for Social Infrastructure Security. Hitachi recognizes that social infrastructure security needs to be adaptive, responsive, and cooperative.

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,

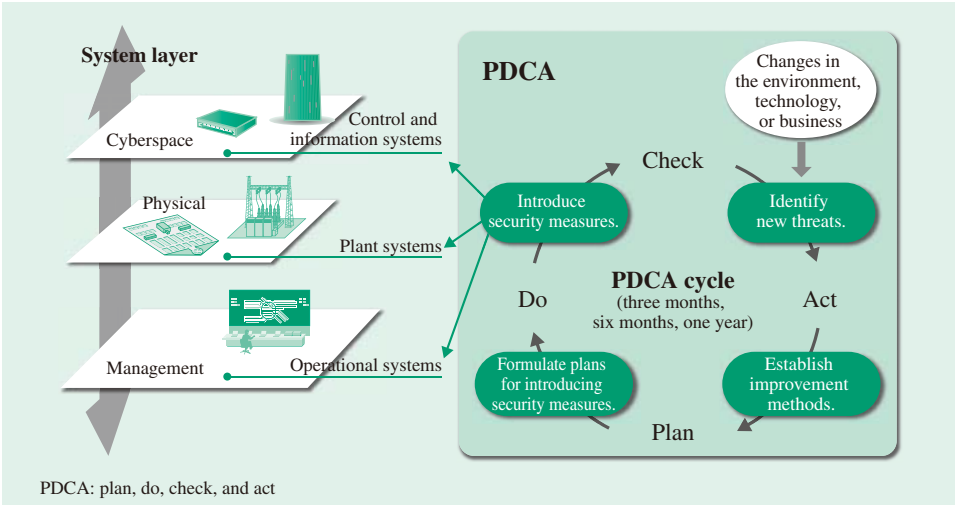


Fig. 4—Adaptability.
Use of the PDCA cycle in the virtual (cyberspace), physical, and management layers to make ongoing strengthening of preemptive countermeasures and defenses against new threats.

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

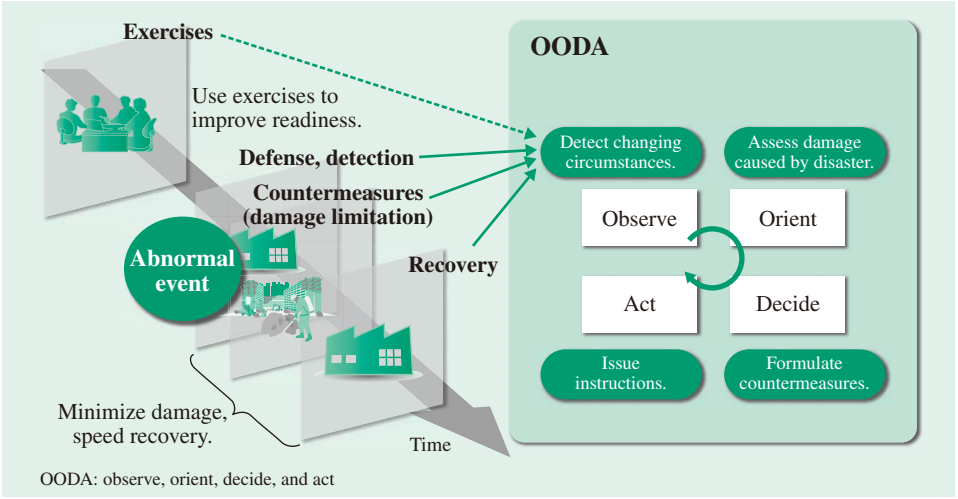
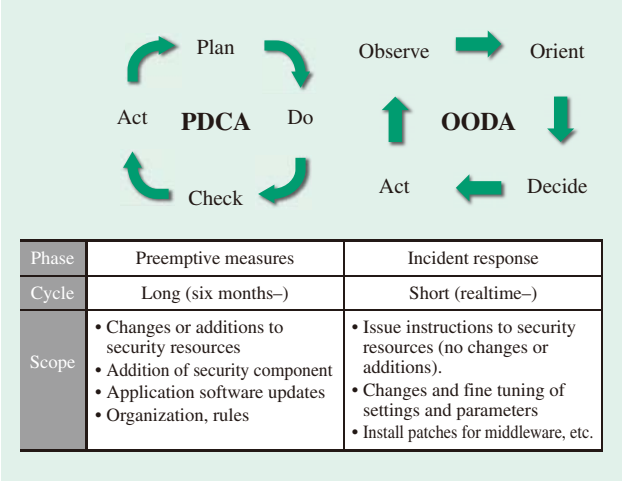


Fig. 5—Responsiveness.
This means strengthening incident response measures to minimize damage and speed recovery after an attack or disaster. It involves providing support for the OODA process for responding promptly to changing circumstances.



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

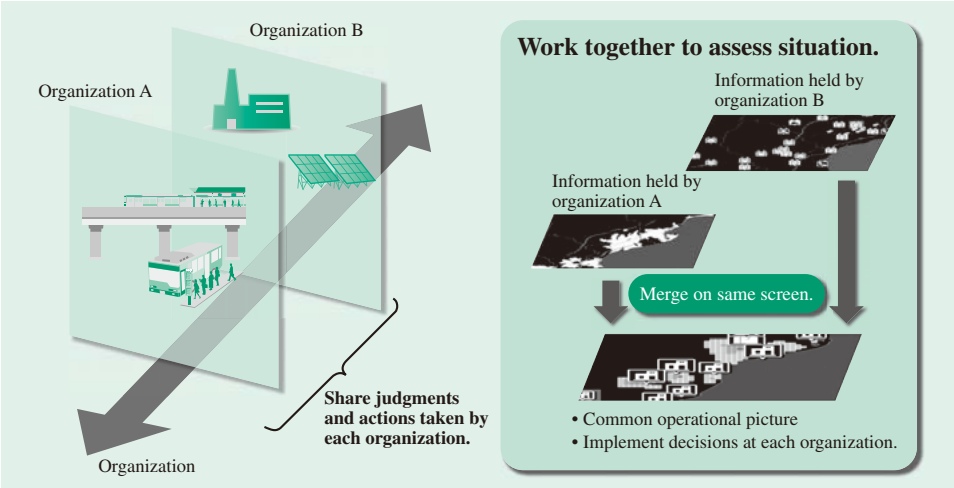


Fig. 7—Cooperativeness.
Cooperativeness allows coordinated measures to be implemented by sharing information among different organizations or infrastructure operators and presenting it from different perspectives.

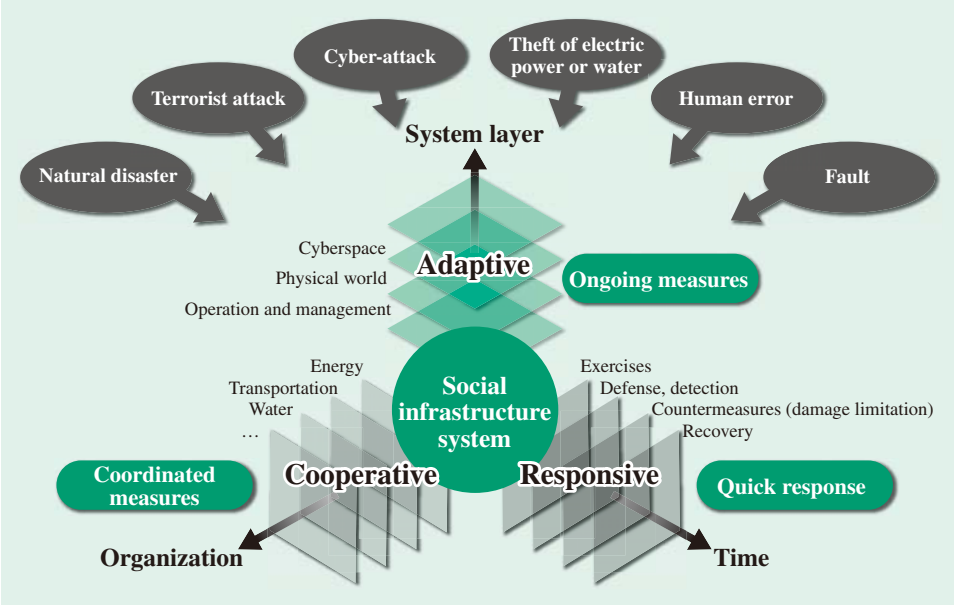
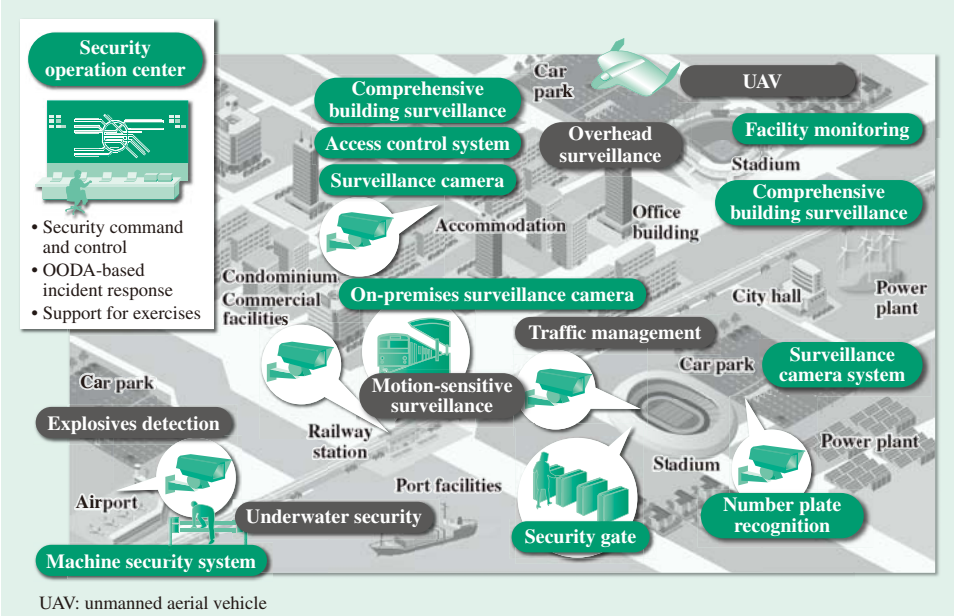


Fig. 8—Hitachi's Concept for Social Infrastructure Security. The security of social infrastructure is achieved through measures taken with respect to the system layer, time, and organization.

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.

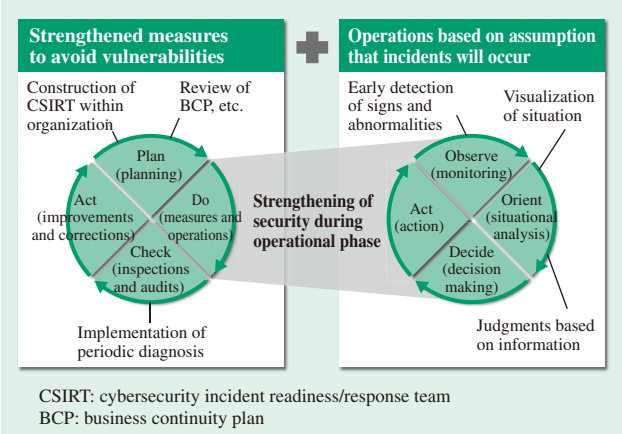


Fig. 10—Managed Security Service Concept.
These services use the PDCA cycle and OODA loop to provide more effective and faster-acting security measures for cyberspace.

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.

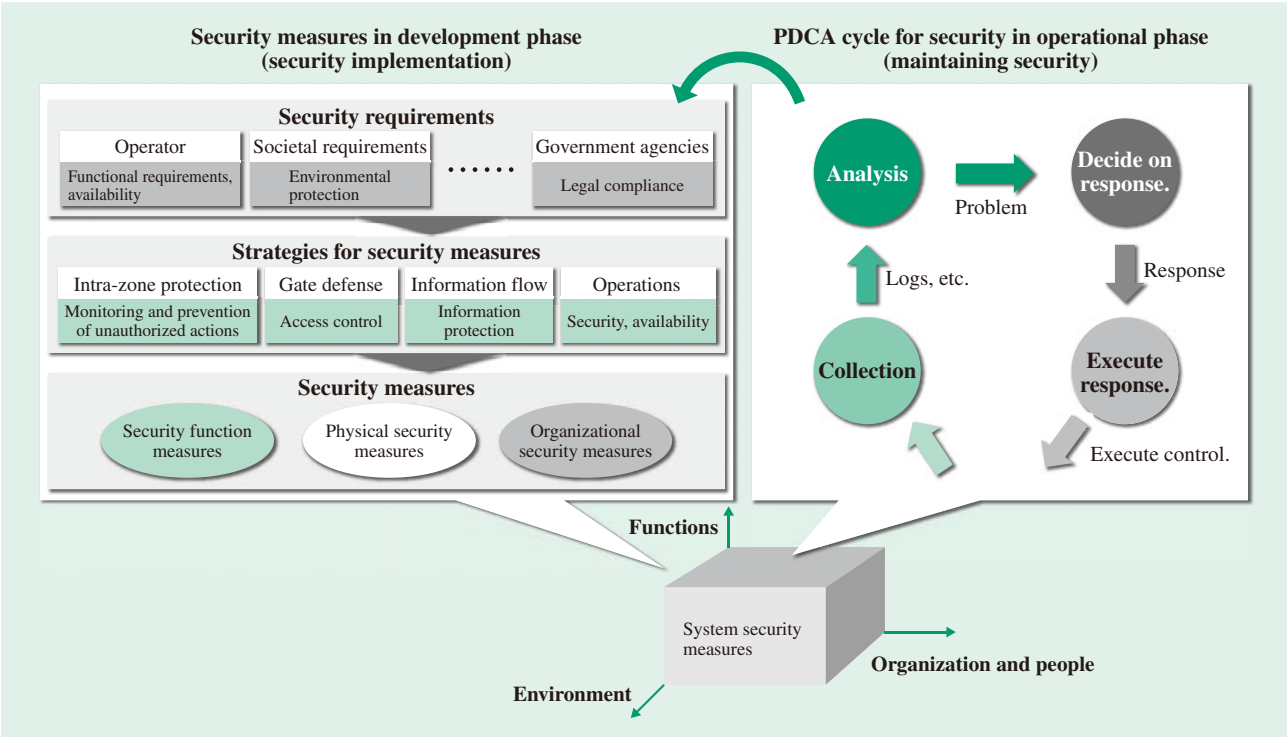


Fig. 11—2 × 3 Security Implementation Model.
The model seeks to ensure the security of social infrastructure systems across their entire lifecycle by assessing security during two phases and in terms of three different criteria.

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.