Visionaries 2015

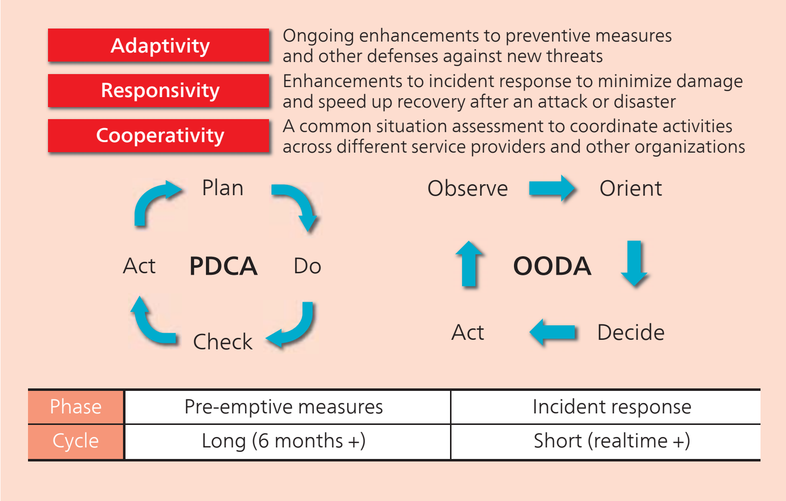
Achieving Agile Strength

— Social Infrastructure Security —

The sophistication and convenience of social infrastructure such as energy and transportation are enhanced through interoperation.
This also means that the social infrastructure is a vast multi-faceted system comprising many different organizations and systems.
Currently, social infrastructure faces rapidly growing threats, such as natural disasters or cyber terrorism, while the consequences of incidents are also expanding in scope.
In its involvement in social infrastructure security, Hitachi brings together safety and security technologies it has built up in many different fields.
Moves are underway to optimize all aspects of security based on the concept of making it adaptive, responsive, and cooperative.

Accepting that Damage will Occur

For all its convenience and comfort, modern society is vulnerable to a variety of risks. The social infrastructure that underpins our daily lives and business activity includes electric power, gas, water, railways, roads, public facilities, and telecommunication networks, and the scope of these services has grown through greater interoperation. The corollary of this, however, is that when a problem arises, its consequences spread more widely. Such problems are not necessarily the result of equipment faults or human error. Abnormal weather or other natural disasters are predicted to progressively increase in severity in the future due to global climate change. Along with the growing worries about armed terrorist attacks that come with globalization, the rise in cyber terrorism associated with the spread of information technol-



Adaptivity: Ongoing enhancements to preventive measures and other defenses against new threats

Responsivity: Enhancements to incident response to minimize damage and speed up recovery after an attack or disaster

Cooperativity: A common situation assessment to coordinate activities across different service providers and other organizations

Phase	Pre-emptive measures	Incident response
Cycle	Long (6 months +)	Short (realtime +)

Hitachi bases its requirements for social infrastructure security measures around the three concepts of adaptivity, responsivity, and cooperativity. Adaptivity relates to the PDCA cycle, and responsivity to the OODA decision-making process used in military activities.

ogy (IT) can no longer be dismissed as a problem that only concerns other people.

The infrastructure that underpins society, 24 hours a day, 365 days a year, needs to be able to continue to provide essential services even in the event of a problem. Unfortunately, it is no longer realistic to take steps to deal with all of the growing and increasingly diverse range of potential threats. What is needed is a flexible approach that accepts that some damage will be inflicted when an unanticipated disaster or attack occurs, but that seeks to react appropriately to prevent the damage from being exacerbated or spreading more widely, and to quickly restore services.

Hitachi has identified three particular requirements for security measures that take account of these special circumstances surrounding social infrastructure: "adaptivity," "responsivity," and "cooperativity." Toshiaki Arai (CTO, Defense Systems Company, Hitachi, Ltd.), who coordinates work on security technology across the Hitachi Group, explains the concepts as follows.

"Adaptivity means working through an ongoing process of identifying new threats; devising countermeasures; and planning, implementing, and evaluating those countermeasures in order to make them more effective. In other words, it relates to measures that can be taken prior to an incident. Responsivity, on the other hand, is about enhancing the ability to react to an incident. It is about focusing on the best measures to take given the available resources, and seeking to minimize damage and speed up recovery after a disaster, attack, or other incident has occurred. Cooperativity, meanwhile, is about increasing interoperation. This means sharing information between different organizations and service providers so that they can be aware of each other's circumstances and take account of these in their subsequent actions."

With system-level robustness as a base, Hitachi employs the concepts embodied by these three terms in its work on wide-ranging security measures that encompass both the physical and cyber realms.

Combining Convenience and Safety

To put these concepts into practice in the realm of physical security, Hitachi products include city-wide safety and security solutions that conduct border security checks on the aircraft, ships, vehicles, and people that enter a city through the interoperation between the associated systems, and also disaster response support solutions that utilize sensor data and simulation techniques.

In the past, physical security has been provided by standalone systems that serve different facili-

Toshiaki Arai

Tatsuhiko Kagehiro

ties and areas. In cities with sophisticated interoperation and coordination of social infrastructure systems, however, even greater benefits can be obtained by tracking the movement of people and goods through the interoperation and coordination of different security systems.

One example is a traceable physical security system developed to provide security at large public facilities and areas. Tatsuhiko Kagehiro (Senior Researcher, Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd.), who coordinated the development, describes the features of the system as follows.

"Our aim was to combine convenience with a high level of safety. While the problem with improving security in the past has been the extra effort and work associated with things like authentication and inspection, this system is able to authenticate people that are entering a site, for example, without compromising convenience, by using touch panel operation together with finger vein authentication and the capturing of facial images."

It can also be used, for example, in the provision of information or services to individuals by checking against personal information that has been obtained with their consent. Also, safety checks on individual items of baggage can be performed by combining a baggage tracking system with devices that can quickly identify the location of explosives by using mass spectrometry to detect the presence of explosive ingredients within the area being monitored. The baggage tracking system works by recording images of items people have with them as part of the baggage inspection procedure and then uses these images to track the movement of the items on surveillance cameras located across the facility.

In the event of malicious activity like planting explosives, it is necessary to find the suspicious individuals quickly by searching large amounts of surveillance camera data based on information from witnesses or other sources. Multi-perspective searching is a valuable tool in such cases.

Mr. Kagehiro says, "Utilizing similar image retrieval, a technique on which we have already been working, we are able to quickly find images with a high degree of similarity in stored image data, even when using fragmentary search conditions comprising not only the face but also upper body, lower body, baggage color, or route traveled."

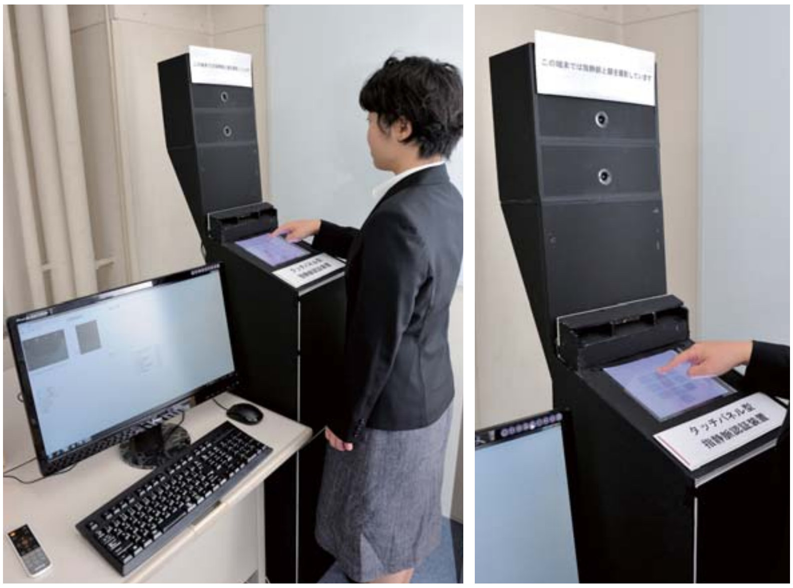
It is anticipated that this system will dramatically improve the efficiency with which people can be tracked from surveillance camera images.

Defending against Attacks through Early Detection and Response

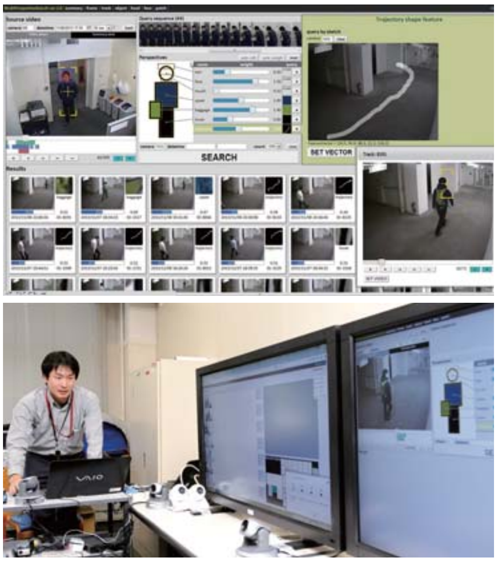
The field of cybersecurity can be broadly divided into information systems and control systems.

Shuji Senoo (Senior Director, Advanced Security Technology Operations, Services Creation Division, Information & Telecommunication Systems Company, Hitachi, Ltd.), an expert in the latest technology for information security, makes the following comments about measures for dealing with cyber-attacks, which are becoming more sophisticated and organized year by year.

"The steady stream of new malware, such as targeted attacks on individuals, means that it is now



Prototype touch panel finger vein authentication system. The system provides enhanced convenience by performing authentication without the user' s awareness (but with their prior consent) by identifying their finger vein pattern as they use the touch panel, while at the same time taking a facial photograph.



Multi-perspective search utilizing a similar image retrieval technique. Yuki Watanabe (Intelligent Media Systems Research Department, Central Research Laboratory, Hitachi, Ltd.), who was part of the development team, emphasizes the system' s effectiveness in applications such as suspect tracking.

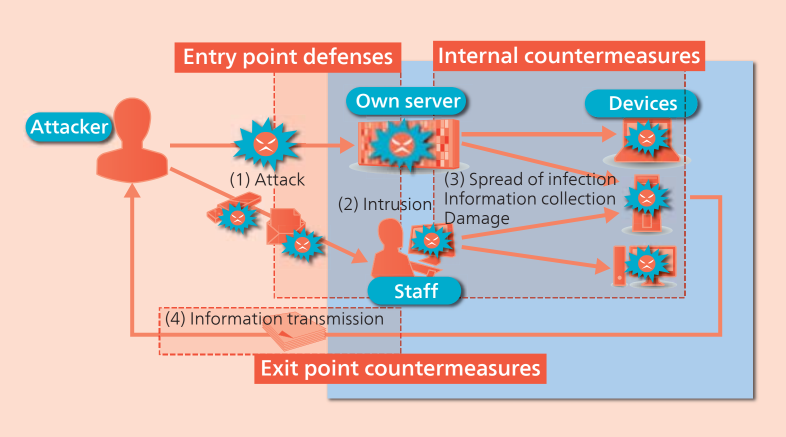
practically impossible to prevent all intrusions into a system. Accepting this, I believe that the basis for information security at present is to consider how to achieve early detection and response based on the concept of the observe, orient, decide, and act (OODA) loop. For example, in addition to conventional entry point defenses, the prompt execution of internal detection and response is crucial, as is the interception of unauthorized transmission of information at exit points to prevent practical losses."

Based on this approach, Hitachi's information security solutions provide multi-layered (defense in depth) monitoring and protection that combines techniques such as a monitoring service for detecting and preventing unauthorized access or malware, and the automatic monitoring and blocking of unauthorized connections to personal computers (PCs). The characteristics of detected malware are determined by a proprietary technique that automatically executes it in a variety of environments to analyze its structure so that this knowledge can be utilized in the subsequent response.

The control systems that support social infrastructure such as power plants and other key industries also face a growing risk of cyber-attacks, having become increasingly integrated with information systems in recent years. Toshihiko Nakano (General Manager, Control System Security Center, Infrastructure Systems Company, Hitachi, Ltd.), describes the characteristics of the control security for which he is responsible as follows.

"Hitachi has participated in the Control System Security Center (CSSC), which was established as a collaboration between industry, academia, and government, since its inception, working on enhancements to control security. The potential for security threats is growing in the control sector, making it important to consider how defenses can be strengthened at a system-wide level."

Hitachi was among the first companies to start developing controller products with ISASecure*1 EDSA Certification*1 in order to reduce the risk of cyber-attacks via a network. On particularly important systems, high security is achieved by providing one-way bridges that block access from external networks. To prevent security threats due to the connection of unauthorized devices to the network, Hitachi also supplies systems for detecting and forcibly disconnecting unauthorized PCs. Another solution installs decoy servers in a system for the early detection of malware intrusions, and to capture and analyze the malware. Operating these in tandem with unauthorized access detection systems makes it possible to respond quickly to both known and unknown threats.



It has recently come to be accepted in information security that preventing all malware intrusions is impossible. Given this situation, organizations need to implement internal and exit point countermeasures in addition to their conventional entry point defenses.

Controller (ISASecure EDSA certified)

System for detection and forcible disconnection of unauthorized PCs

One-way bridge

Devices for protecting against cyber-attacks on the control systems of vital industrial infrastructure. Hitachi supplies these as part of its solutions for countering attacks.

Information and control are the foundations of social infrastructure systems. Based on the technologies described here, Hitachi supplies comprehensive security services that cover everything from risk analysis and consulting to system configuration and operational support.

System-wide Optimization of Security

In addition to important business data, social infrastructure security also involves handling a variety of personal information, such as finger vein and other biometric information. Masahiro Mimura (General Manager, Enterprise Systems Research Department, Yokohama Research Laboratory, Hitachi, Ltd.), who is engaged in research into finance and public sector security technologies, describes some of the advanced techniques for protecting such information as follows.

Shuji Senoo

[1] EDSA is an abbreviation of Embedded Device Security Assurance. EDSA is a security certification program for embedded systems in control equipment. It is run by an international certification agency made up primarily of members of the International Society of Automation.
See "Trademarks" on page 146.

Developing Technology and People to Improve Social Infrastructure Security

Professor Seiichi Shin

The Control System Security Center (CSSC) based in Tagajo City in Miyagi Prefecture was established in March 2012 as an industry-academia-government partnership that undertakes security certification, research and development, training, and awareness raising activities with the aim of strengthening security for the control systems that underpin social infrastructure. CSSC President, Seiichi Shin (Professor, Control Systems Program, Department of Mechanical Engineering and Intelligent Systems, Graduate School of Informatics and Engineering, The University of Electro-Communications) specializes in control engineering and is recognized as a leader in the field of microcomputer control.

"In the past we have strived to make the world a more convenient place by linking various different things together. As a result we have achieved a level of social infrastructure that is unsurpassed anywhere in the world, with trains that run on time, safe drinking water, and a power system that is not prone to blackouts. While it goes without saying that it is the diverse technologies of companies like Hitachi that help maintain this world in which all of these things continue to function correctly as a matter of course, security in particular has become an important factor in recent years.

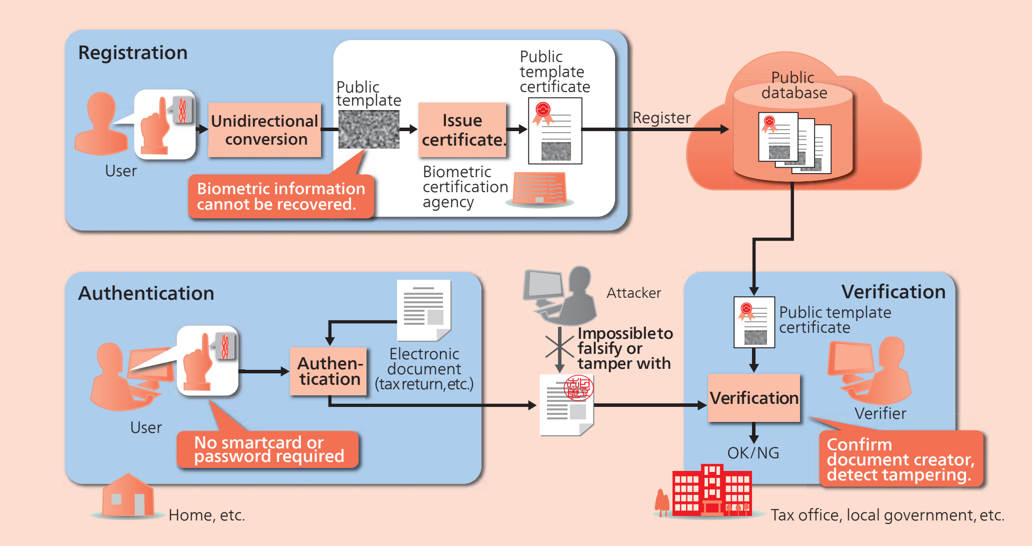
Once the preserve of mischief makers, cyber terrorist activity has become a form of organized crime undertaken for commercial motives, with the control systems in social infrastructure increasingly being targeted. Defending against this requires not only security technology but also policies and management capabilities for deploying the technology to good effect.

In this, international standards and their certification systems have important roles to play. Security certification was one of the founding objectives of CSSC and we are the certification agency for EDSA in Japan. We also seek to support the export of Japan' s excellent social infrastructure systems by keeping up with technical trends in international standards and encouraging their adoption by Japanese companies.

To improve social infrastructure security in terms of both awareness and actions, the CSSC also conducts cyber-attack drills for the operators of thermal power plants, electricity network control, sewage treatment plants, building control systems, assembly plants, gas plants, and petrochemical plants. We collaborate on global information sharing and on research and development with other agencies, including cybersecurity promotion agencies in Europe, America, and Asia.

People are another important consideration. At both CSSC and The University of Electro-Communications, we are striving to train people with an understanding of both information security and control systems, a combination that will be increasingly needed in the future. The safety and security of social infrastructure is underpinned by ethical considerations as well as by technical capabilities. To attract the best people with high levels of both qualities, I hope that those who work in this field will receive their due respect. I ask this because it will in itself result in higher levels of safety and security for society as a whole.

Cybersecurity is already widely recognized as a military technology, and Japan is the only country in the world where critical infrastructure is protected by the private sector. I look forward to Hitachi playing a central role in helping improve social infrastructure security."


Registration
User
Unidirectional conversion
Public template
Issue certificate.
Public template certificate
Biometric certification agency
Biometric information cannot be recovered.
Register
Public database
Authentication
User
Authen-tication
Electronic document (tax return, etc.)
No smartcard or password required
Home, etc.
Attacker
Impossible to falsify or tamper with
Verification
Public template certificate
Verification
Verifier
OK/NG
Confirm document creator, detect tampering.
Tax office, local government, etc.

The PBI public template biometric authentication platform facilitates the shifting to the cloud of systems that require rigorous user authentication, and provides a low-cost way to use the same identification across a number of related systems.

Toshihiko Nakano

"The public biometric infrastructure (PBI) is a technique for authentication and identification that works in conjunction with an encryption key and stores biometric information in a form that can safely be made public by converting it to a template from which the original information cannot be recovered. We also have privacy-preserving information processing techniques that can rapidly search, compare, and analyze data in encrypted form."

PBI combines the convenience of being able to use your own biometric information (such as finger vein patterns) for authentication with a reduced risk of information disclosure. The privacy-preserving information processing techniques are able to process large quantities of data while maintaining a high level of security. Future advanced security technology will reduce the risk of handling important social infrastructure information on the cloud. In other words, Hitachi's concept of social infrastructure security is of a platform for society that maintains security without compromising public convenience and without users needing to concern themselves with particular details.

As described above, attempting to increase security on its own not only results in more complex equipment operation and other procedures, it also tends to demand ongoing vigilance. Atsutoshi Sato (Information Design Department, Design Division, Hitachi, Ltd.), a specialist in information design, reinforces Mr. Mimura's comments by describing the approach needed for future security measures as follows.

"A society in which people are always feeling stressed about security is unlikely to be a comfortable place to live. I believe that, by utilizing our design capabilities, we can identify the ideal security measures that will maintain the required level of security without compromising comfort."

Equipment, for example, can be made easier to use, and human error can be avoided, by providing better user interfaces. Providing effective presentation of alarm and warning levels helps the transition between emergency and non-emergency situations. Hitachi is seeking to utilize methods such as ethnography*[2] and the experience-oriented approach*[3] to achieve this.

The infrastructure that underpins society needs to keep not only individual systems but also the overall infrastructure secure. Along with adopting approaches to design like these, Hitachi is seeking to achieve this by supplying safety and security technologies built up over a wide range of fields together with services that consolidate the operation of these technologies, and also by participating in standardization work to raise standards and facilitate the further development of security. Underlying these activities is the concept of the total optimization of security.

With its social infrastructure security, Hitachi intends to support the creation of a society that enjoys behind-the-scenes protection from diverse threats and that is capable of agile but strong resistance to unanticipated dangers.

Masahiro Mimura

Atsutoshi Sato

*2 A method for observing user workplaces to identify latent needs at the earliest stages of human-centric design. Through close observation of people' s actual behavior and fact-based analyses of the collected data, it can obtain an overview of what people are actually doing together with things like their tacit assumed values and their unfulfilled needs or wants.

*3 A methodology for consensus-building in the very earliest stages of system development (concept development and planning stages), with an emphasis on user experiences. The experience-oriented approach has been formalized by Hitachi based on the experience design method.