Featured Articles II

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

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

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

INTRODUCTION

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

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

TRENDS IN CYBER-ATTACKS IN RELATION TO SOCIAL INFRASTRUCTURE

Recent Trends in Cyber-attacks

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

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

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

Risk of Cyber-attack on Social Infrastructure

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

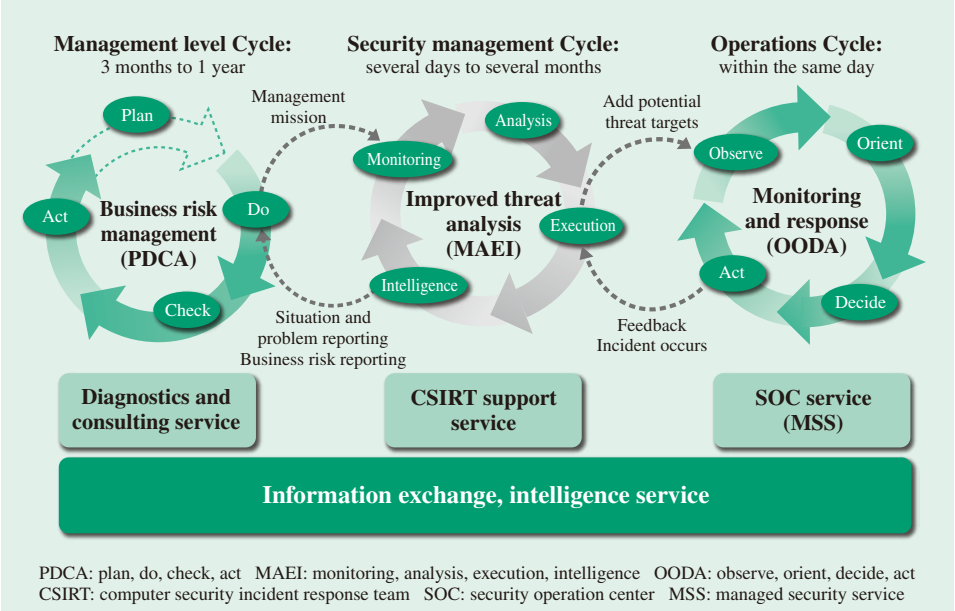


Fig. 1—Relationship between Cycle of Security Measures and Associated Services.
The security measures at an organization have a different cycle at each level. These cycles are linked, and among them, a CSIRT handles security management. Hitachi's security solutions offer one-stop service for each level.

HITACHI'S INVOLVEMENT IN CYBERSECURITY

Trend of Cybersecurity Measures by Hitachi

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

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

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

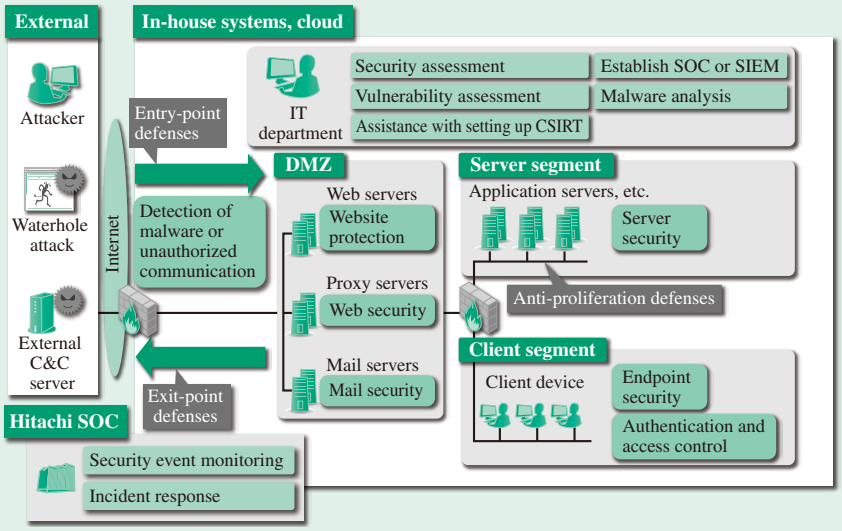
Hitachi Cybersecurity Solutions

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

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

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

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



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

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

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

Example of Countermeasures against Cyber-attack: Assessment Service

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

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

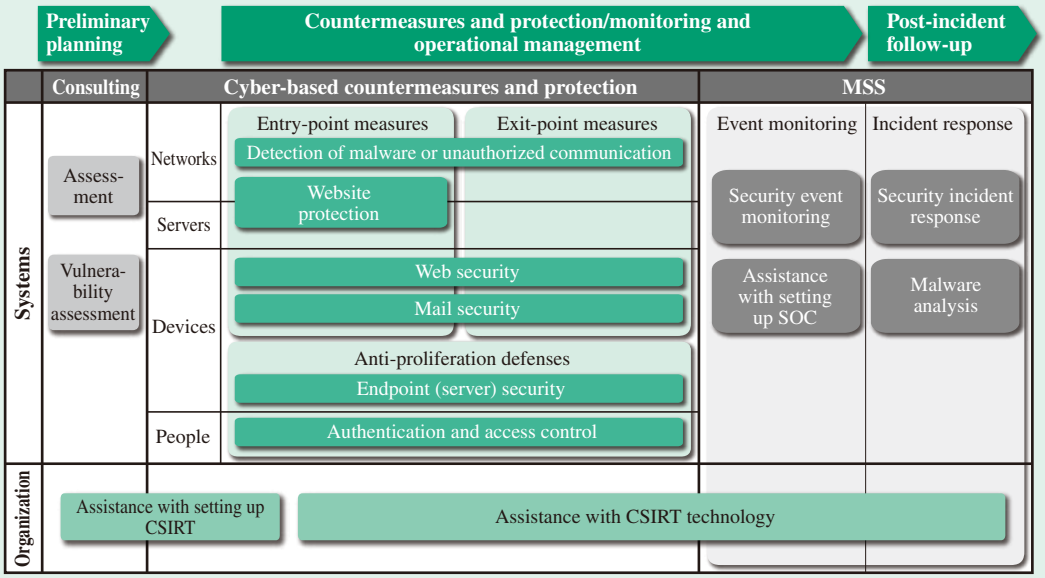


Fig. 3—Solutions according to Each Countermeasure Phase of the Customer.
Hitachi supplies comprehensive solutions that cover each countermeasure phase from preliminary planning to countermeasures and protection together with monitoring and operational management, to post-incident follow-up.

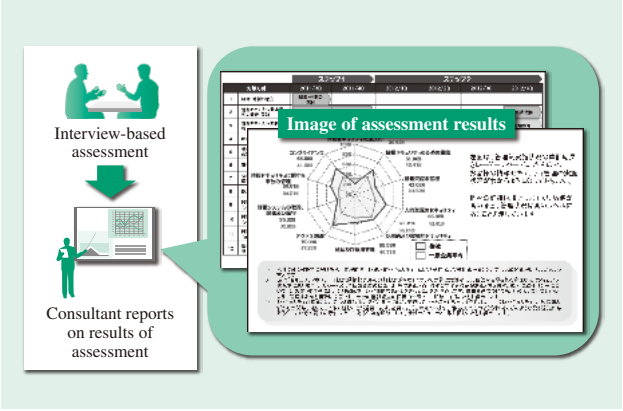


Fig. 4—Image of Assessment Service Results.
The results of the assessment service are presented in the form of proposed measures based on an assessment of the current situation.

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

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

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

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

OUTLOOK FOR CYBERSECURITY OF SOCIAL INFRASTRUCTURE

Intelligence-sharing to Protect Social Infrastructure

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

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

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

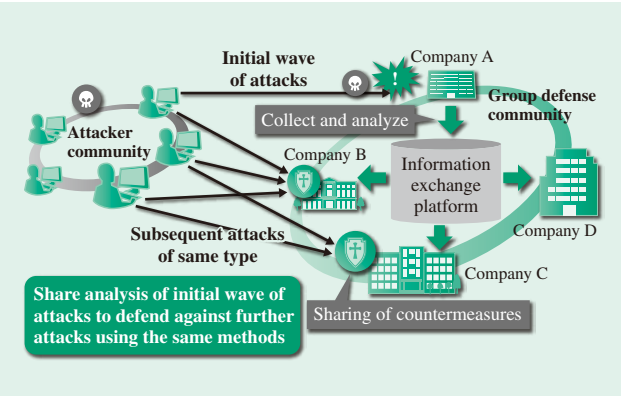


Fig. 5—Intelligence-sharing Structure.
The sharing of intelligence gained from analysis of the initial wave of attacks prevents further attacks using the same methods.

Cybersecurity Human Resource Development

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

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

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

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

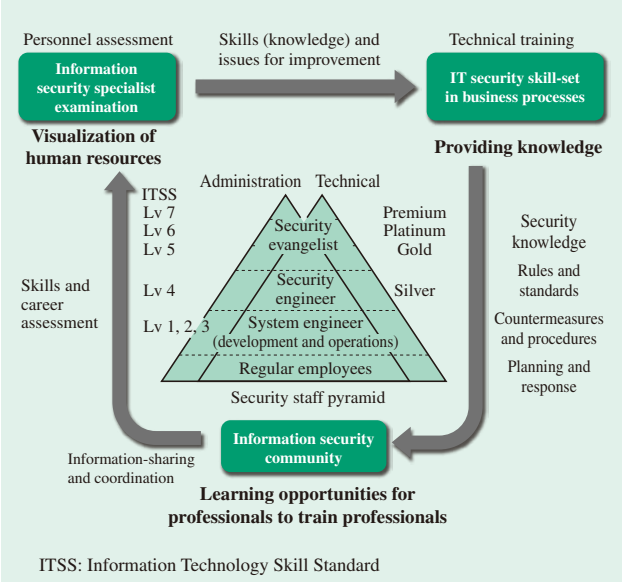


Fig. 6—Security Human Resource Development Cycle at Hitachi.
Hitachi has established a human resource development cycle by undertaking security training on the basis of personnel assessment, technical training, and information-sharing and coordination.

CONCLUSIONS

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

REFERENCES

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

ABOUT THE AUTHORS

Takehiro Kawashima

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

Kazuya Yonemitsu

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

Kazuhiro Kawashima, Ph.D.

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

Yuji Motokawa

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

Hiroyuki Hamada

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