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

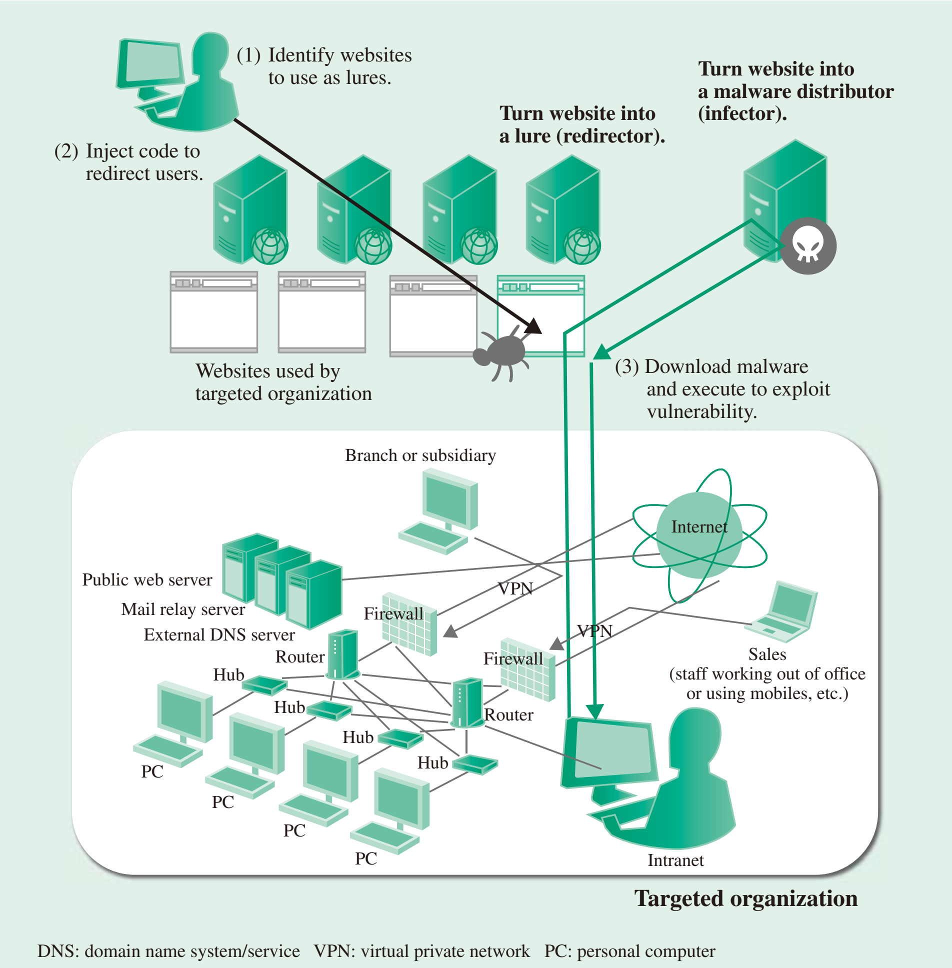

(1) Identify websites to use as lures.
(2) Inject code to redirect users.
Turn website into a lure (redirector).
Turn website into a malware distributor (infector).
Websites used by targeted organization
(3) Download malware and execute to exploit vulnerability.
Branch or subsidiary
Internet
Public web server
Mail relay server
External DNS server
VPN
Firewall
VPN
Router
Firewall
Hub
Hub
Router
Hub
Hub
Sales (staff working out of office or using mobiles, etc.)
PC
PC
PC
PC
Intranet
Targeted organization
DNS: domain name system/service VPN: virtual private network PC: personal computer

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

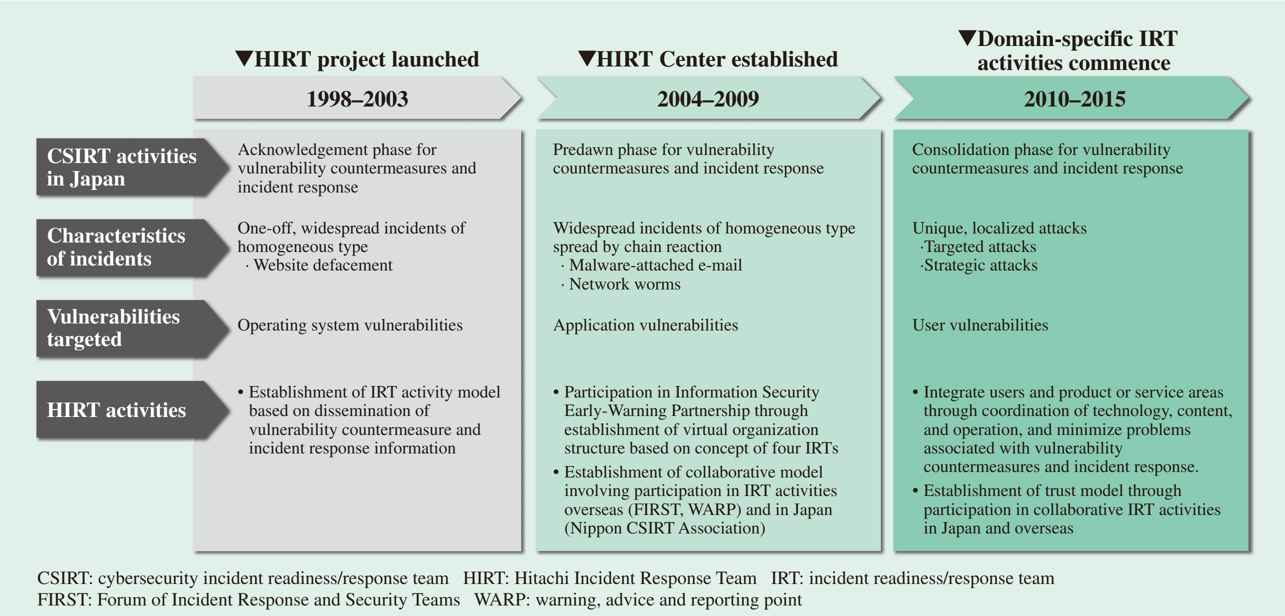
CSIRTs

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



	▼HIRT project launched	▼HIRT Center established	▼Domain-specific IRT activities commence
	1998–2003	2004–2009	2010–2015
CSIRT activities in Japan	Acknowledgement phase for vulnerability countermeasures and incident response	Predawn phase for vulnerability countermeasures and incident response	Consolidation phase for vulnerability countermeasures and incident response
Characteristics of incidents	One-off, widespread incidents of homogeneous type · Website defacement	Widespread incidents of homogeneous type spread by chain reaction · Malware-attached e-mail · Network worms	Unique, localized attacks ·Targeted attacks ·Strategic attacks
Vulnerabilities targeted	Operating system vulnerabilities	Application vulnerabilities	User vulnerabilities
HIRT activities	• Establishment of IRT activity model based on dissemination of vulnerability countermeasure and incident response information	• Participation in Information Security Early-Warning Partnership through establishment of virtual organization structure based on concept of four IRTs • Establishment of collaborative model involving participation in IRT activities overseas (FIRST, WARP) and in Japan (Nippon CSIRT Association)	• Integrate users and product or service areas through coordination of technology, content, and operation, and minimize problems associated with vulnerability countermeasures and incident response. • Establishment of trust model through participation in collaborative IRT activities in Japan and overseas

CSIRT: cybersecurity incident readiness/response team HIRT: Hitachi Incident Response Team IRT: incident readiness/response team
FIRST: Forum of Incident Response and Security Teams WARP: warning, advice and reporting point

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

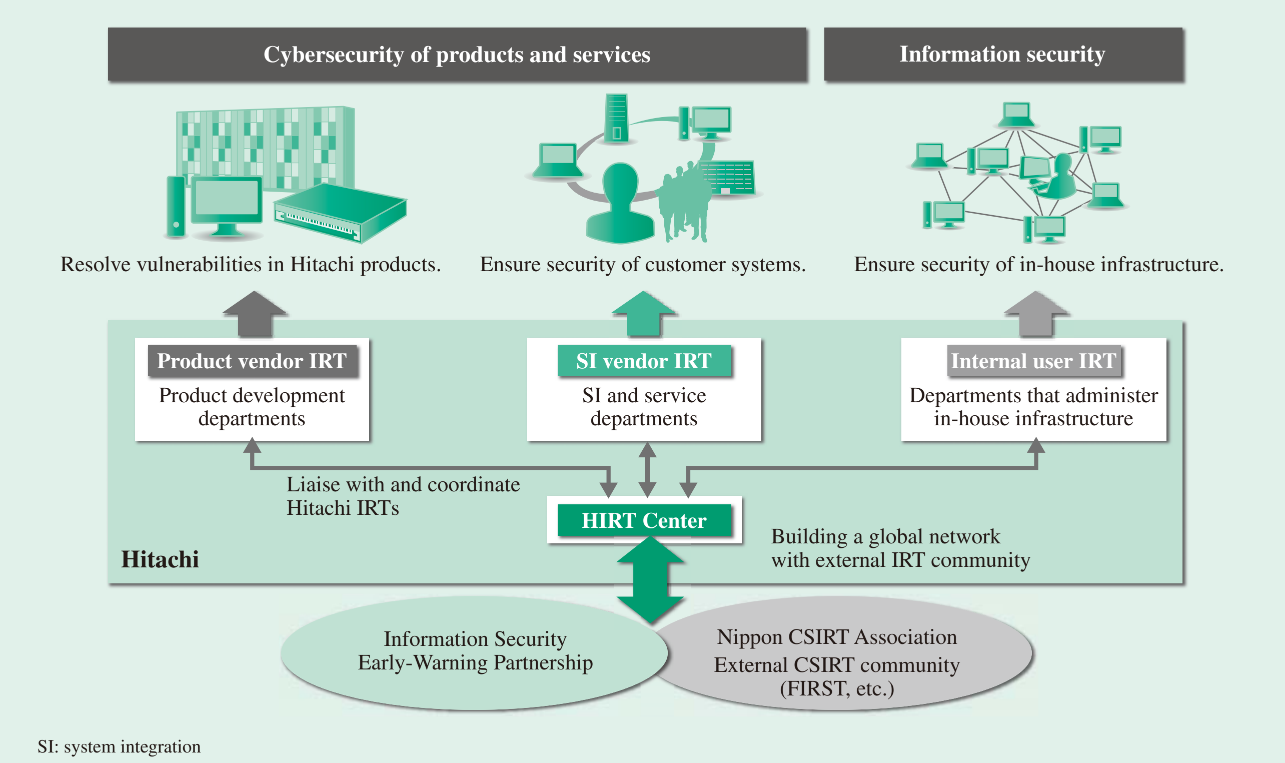

Cybersecurity of products and services
Information security
Resolve vulnerabilities in Hitachi products.
Ensure security of customer systems.
Ensure security of in-house infrastructure.
Product vendor IRT
Product development departments
SI vendor IRT
SI and service departments
Internal user IRT
Departments that administer in-house infrastructure
Liaise with and coordinate Hitachi IRTs
HIRT Center
Building a global network with external IRT community
Hitachi
Information Security Early-Warning Partnership
Nippon CSIRT Association
External CSIRT community (FIRST, etc.)
SI: system integration

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

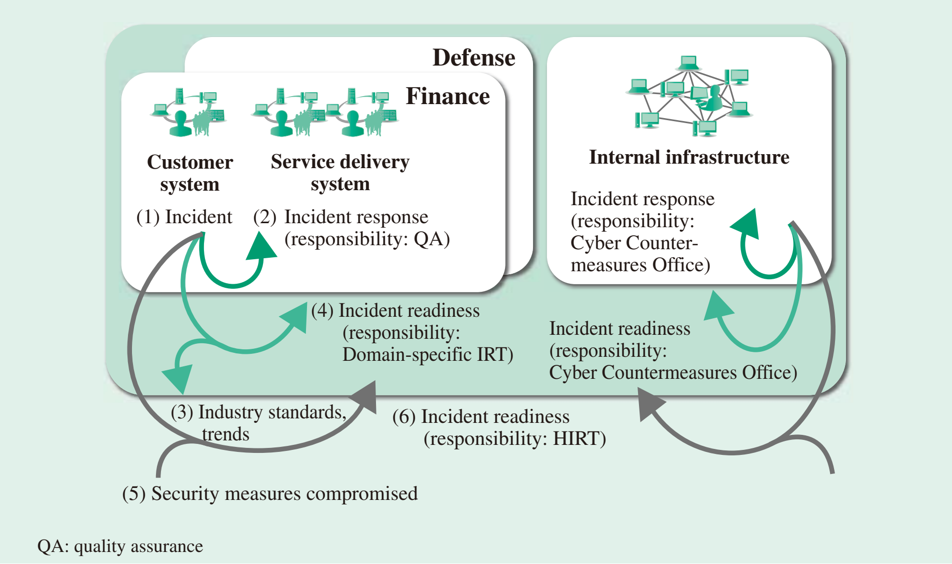
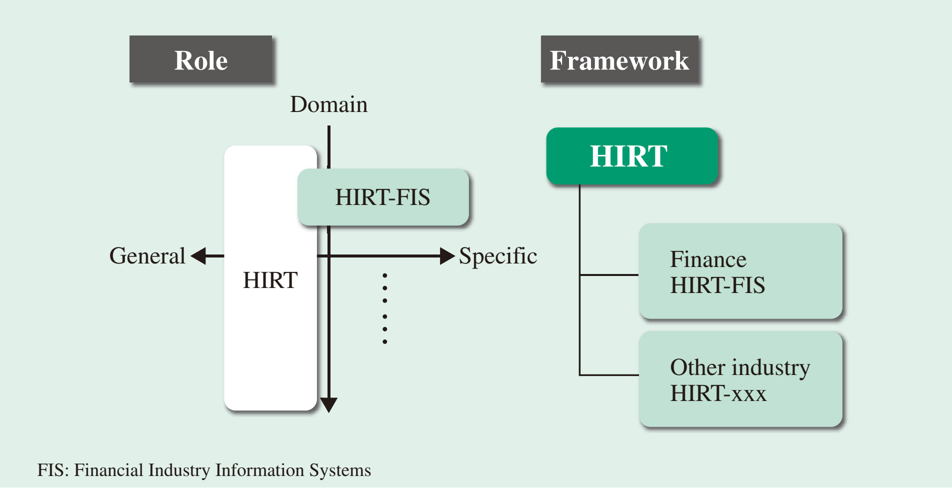

Defense
Finance
Customer system
Service delivery system
(1) Incident
(2) Incident response (responsibility: QA)
Internal infrastructure
Incident response (responsibility: Cyber Countermeasures Office)
(4) Incident readiness (responsibility: Domain-specific IRT)
Incident readiness (responsibility: Cyber Countermeasures Office)
(3) Industry standards, trends
(6) Incident readiness (responsibility: HIRT)
(5) Security measures compromised
QA: quality assurance

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.



FIS: Financial Industry Information Systems

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.