

HIRT: Annual Report 2008

Hitachi Incident Response Team (HIRT)

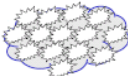

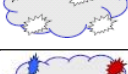

<http://www.hitachi.com/hirt/>

Kashimada 890, Saiwai, Kawasaki, Kanagawa, 212-8567 Japan

1 Introduction

Table 1 provides a summary of a transition of incidents from 2000 onwards. This table is subjective and does not cover all incidents. However, as far as the transition of incidents over several years is concerned, a new type of security breach arises in a short cycle time, and remains constant once established. In addition, the technology is inherited and nurtured through such security breaches for better or worse. From 2008 onwards, a virus started to spread via USB memory sticks (hereinafter called the USB memory virus), which represents a recurrence of the virus infection via floppy disk phenomenon and can be described as history repeating itself.

Table 1: Transitions of incidents from 2000 onwards

Period	Features	Impact model
2000 -2001	Single occurrences of homogeneous impact over a wide area Website defacement	
2000 -2005	Chain reaction of homogeneous impact over wide area. Dissemination of mails with viruses attached Spread of network worms	
2005-	Local impact of a similar kind Web site attacks through SQL injection Information leakage caused by Winny and Share Phishing, Spyware, Bot viruses, etc.	
2006-	Local impact of various kinds Targeted attacks	

These changes in the nature of incidents have caused a change in the view of those fighting against them. With the advent of Internet worms in 1988, the importance of sharing information concerning the causes of incidents and countermeasures thereto was recognized, and the “incident response” model, in which measures are taken in accordance with a pre-determined plan, began to take hold. From 2001 to 2003, network worms appeared and countermeasures to them spawned the “incident operations” model. Incident operations represent a series of security activities implemented to predict and prevent damage caused by incidents and adopt measures to reduce the expansion of the damage once such incidents have occurred.

To promote proactive measures against vulnerabilities, as well as reactive measures against incidents, as part of information security activities, such changes have meant an increasing need for CSIRTs (Computer Security

Incident Response Teams) to not only have the basic abilities to “predict and alert from a technical point of view”, “make technical adjustments” and “collaborate with external communities on the technical aspects” but also provide the following function based on their experience:

Implementing measures at an early stage in an effort to “catch any sign of future threats”

Hitachi Incident Response Teams (HIRT), as a organization with the above-mentioned abilities and roles, takes the lead in adopting proactive measures against vulnerabilities in products and services, as well as reactive measures against incidents, such as virus activities and information leakage, and assumes responsibility for establishing activities, mechanisms and systems to enhance Hitachi brand in the security field, as a unified point of contact for IRT activities in the Hitachi group.

This document gives you an overview of the threats and vulnerabilities in 2008, as well as HIRT activities, as the HIRT annual report for 2008.

2 Overview of activities in 2008

This section focuses on HIRT activities in 2008.

2.1 Overview of threats and vulnerabilities

In 2008, there was a recurrence of well-known means of attacks, such as DNS cache poisoning, USB memory viruses, network worms abusing MS08-067, and SQL injection, or of those that prevailed previously. Furthermore, websites are also used as download sites, from which sequential malware repeatedly downloads programs that provide other functions.

As shown in Figure 1, the total number of vulnerabilities entered in the National Vulnerability Database (NIST NVD) in 2008 is 5,634. (CERT/CC reported 6,058). Vulnerabilities in web application software products, including Cross-site Scripting (XSS), SQL Injection, Directory Traversal and Cross Site Request Forgery (CSRF), account for approximately 40% of the total, or 2,315. (See Figure 2)[1]. Of the vulnerabilities in websites in operation reported to IPA, Cross-site Scripting (XSS) and SQL Injection account for approximately 60%, with the number of vulnerabilities reported increasing every year. (See Figure 3)[2].

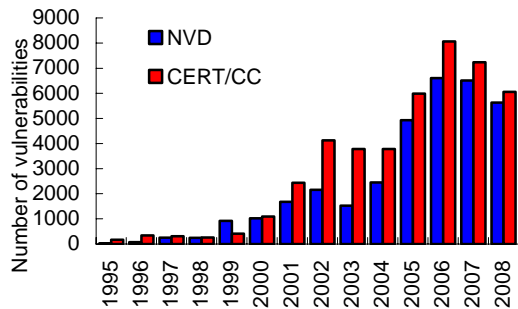


Figure 1: Changes in the number of vulnerabilities reported (Source: NIST NVD)

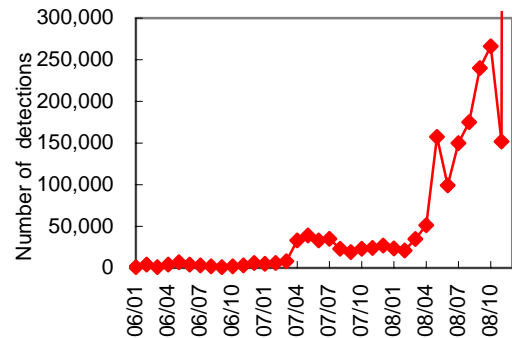


Figure 4: Changes in the number of SQL injection attacks detected (Source: LAC)

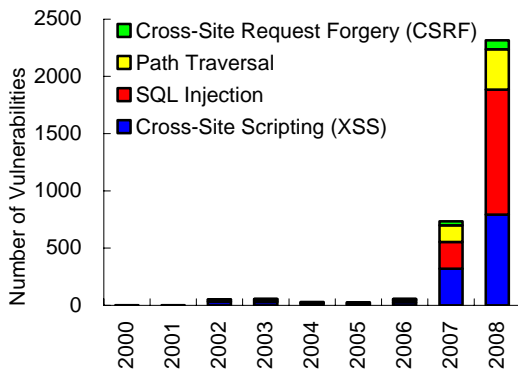


Figure 2: Changes in the number of vulnerabilities reported for web application software products (Source: NIST NVD)

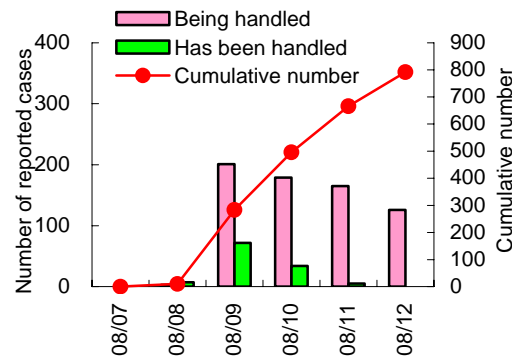


Figure 5: Number of DNS cache poisoning vulnerabilities reported and countermeasures taken (Source IPA, JPCERT/CC)

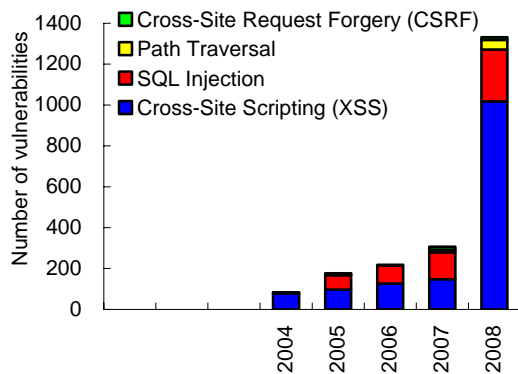


Figure 3: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC)

With more SQL injection attacks detected from 2007 onwards, as shown in (Figure 4)[3], proactive measures against vulnerabilities must be further promoted lest websites should become a base for malicious activities.

DNS cache poisoning is a method for attacking a server that provides a DNS service (DNS server) by having it memorize forged information. Once this attack is successful, the DNS server provides the forged information it has memorized, thus inducing users, who expect to being connected to the right web server with the right host name, to a web server where an attacker is waiting to trap them. The potential threat of DNS cache poisoning has already been pointed out and an effective cache poisoning method had already become public in July 2008, further emphasizing the need to ensure the widespread of countermeasures to protect the DNS service, an underlying Internet service. (Figure 5).

For the USB memory virus that started to spread from 2008 onwards, more infection events are reported, as shown in (Figure 6)[4], which indicates that USB memory sticks have become established as physical media. The convenience of the automatic replay and execution provided by USB memory sticks and the security thereof should be reviewed with preventive measures in mind.

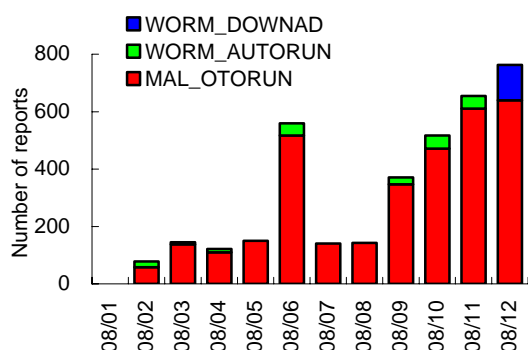


Figure 6: Number of USB memory virus infection events reported (Source: Trend Micro)

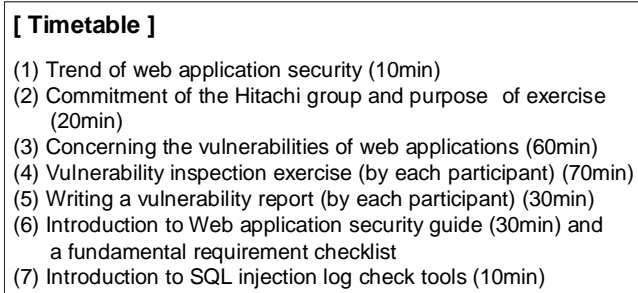


Figure 7: Hands-on class in HIRT open meetings (Web application security)

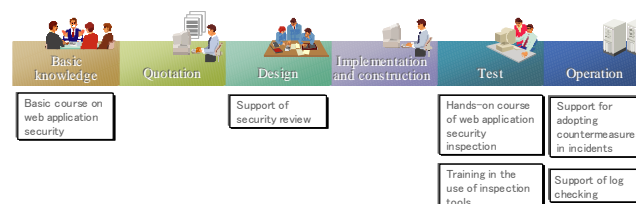


Figure 8: Systematizing HIRT support activities (Web application security)

2.2 HIRT activities

This subsection describes the HIRT activities in 2008.

(1) Establishing Hands-on class in HIRT open meetings

A HIRT open meeting is an activity to let people know the HIRT community built on a trusting relationship. The meeting is held in accordance with the policy of “providing members of the HIRT/CC with the opportunity to exchange their opinions on HIRT activities”, “providing a venue for the share of information to let the Hitachi group know about the activities of the HIRT/CC and listen to opinions from people outside the HIRT/CC, and “inviting people to participate in the HIRT community built on a trusting relationship”.

In 2008, targeting the establishment of Hands-on class in HIRT open meetings for web application development, which commenced in 2007, (See Figure 7), we held a total of nine meetings, in which altogether approximately 200 people participated.

(2) Systematizing product and service security activities

In order to give feedback in the form of know-how obtained through proactive measures against vulnerabilities as well as reactive measures against incidents, to product development processes, we started considering the systematization of HIRT support activities suitable for each process. For web application security, for which HIRT support activities precede, we are considering systematization that incorporates the Hands-on class in HIRT open meetings described in item (1). (See Figure 8).

For embedded products, we have started support activities focusing on security inspection, including how security evaluation should be or needs to be performed and how evaluation tools should be used, in order to develop product development processes that take security into account. In particular, for tools used for security inspection, we try to prevent any recurrence of known vulnerabilities by not only developing or providing product specific security inspection tools, such as Session Initiation Protocol (SIP), but also using “TCP/IP-related well-known vulnerability verification tools”[5] provided from IPA for developers of products implementing TCP/IP, and are now adopting more specific security measures for intelligent home appliance, embedded products and control systems in the Hitachi group.

In addition, in order for people to widely accept product and service security activities, it is important for an organization to be mindful [6]; not only viewing security activities from technical aspects but also constantly from the perspectives of “What circumstances are we facing?” “What kind of problem do we have?” or “What measures can we take?” so that it can take actions immediately whenever necessary. With this in mind, we invited Professor Aki Nakanishi, the Faculty of School of Business Administration, Meiji University, as an instructor to hold a lecture meeting concerning high reliability organizations resilient to contingencies, such as failures or accidents, in April 2008.

[Timetable]
(1) Overview of HIRT-08043 (10min)
(2) DNS mechanism and related tools (20min)
- whois service
- nslookup command
(3) Use of inspection tools and notes (30min)
- Cross-Pollination Check
- DNS-OARC Randomness Test
(4) Configuration for Recursive query(20min)
- Countermeasures on BIND DNS servers
- Countermeasures on Windows DNS servers
(5) Introduction to HIRT-FUP activities and a request for cooperation (5min)

Figure 9: HIRT open meeting on DNS cache poisoning countermeasures

(3) Supporting countermeasures against DNS cache poisoning vulnerability

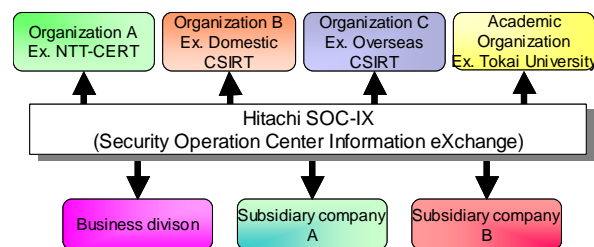
To reduce the threat from DNS cache poisoning vulnerability associated with the DNS service, we issued a security alert in August 2008. Unfortunately, only a limited amount of information is available about DNS behavior and related tools, although many network services provided on the Internet rely on DNS. To cope with this situation, we held an HIRT open meeting “Roles of DNS and Use of Related Tools” in December as a countermeasure to DNS cache poisoning vulnerability, in order to describe DNS behavior and how to use tools. (See Figure 9). To help promote DNS cache poisoning countermeasures in Japan, the materials prepared for the HIRT open meeting were provided as a reference, based on which “Countermeasures against DNS Cache Poisoning vulnerability” [7], issued from the IPA in January, 2009, was created.

(4) Holding JWS2008

In March 2008, we, along with domestic FIRST member teams, invited the FIRST Technical Colloquium, a FIRST technical meeting, to Tokyo (March 25 - 28, 2008). During the meeting, we held a Joint Workshop on Security 2008, Tokyo (JWS2008) [8], with a view to providing an opportunity to exchange opinions to promote the creation of an ideal and reactive system, built on the strong trusting relationship among domestic CSIRTs.

(5) Participation in the domestic COMCHECK Drill 2008

The domestic COMCHECK Drill 2008, called “SHIWASU”, was held by the Nippon CSIRT Association on December 4, 2008, with a view to ensuring that domestic CSIRTs and in-house information security departments of various organizations could communicate with each other. In the drill, the participants were organized into a star topology, with a commander at the center and the points of contact for organizations surrounding it, to make a contact with each other via mail, assuming that an incident has occurred.



Creating a framework or mechanism for exchange information, such as observation data, has the following advantages:

- It allows analysis using a large amount of various observation data.
- It allows you to use observation data you do not have
- It allows you to use technology and know-how in fields in which each CSIRT excels.

Figure 10: Schematic view of the Hitachi SOC-IX

(6) Strengthening partnership with the CSIRT community

As part of activities to strengthen partnership among organizations, we met with NTT-CERT [9] on a regular basis to exchange information to help improve CSIRT activities and allow the mutual use of a malware capturing system (Nepenthes). For the malware capturing system, in an attempt to reflect the partnership among organizations, we released the research outcome from data compiled focusing on the behavior of infected PCs at the Computer Security Group, Information Processing Society of Japan. [10].

To cope with persistent information leakage via file exchange software, we consider it necessary to establish a partnership with external organizations. On this purpose, we continued to investigate the file exchange network environment with the Systems Development Laboratory, Hitachi Ltd. while obtaining assistance from the Association of Copyright for Computer Software and Secure Trusted Network Forum P2P Research Group; both of which participate in the “Development of Technology to Detect Information Leak through Networks and Block Automatic Circulation of Leaked Information”, a project run by the Ministry of Internal Affairs and Communications. [11][12].

As a new instance of partnership among organizations, we sent relevant organizations a virus-attached email purporting to be a Call for Papers (CFP) for a symposium held by the Computer Security Group, Information Processing Society of Japan, as well as providing a demonstration [*] in which people can virtually and safely experience receiving virus-attached email, in order to reveal how a targeted attack is done [13].

2008 was a year where “Hitachi Security Operation Center Information eXchange (SOC-IX)”, a framework that allows organizations to share and jointly use the information required to analyze threats, including observation data, albeit slowly. (See Figure 10).

*) The demonstration is a flash movie that can be operated with buttons (for starting demonstration and rewinding a little). It triggers no actual virus infection.

Table 2: Reports released in Publications on HIRT website

Number	Title
HIRT-PUB08008	Investigation report on information leakage caused by file exchange software in 2008
HIRT-PUB08007	Malware circulating in P2P file exchange software environment
HIRT-PUB08005	Countermeasure of Cache poisoning vulnerability for DNS servers
HIRT-PUB08002	Information Security Day for 2008
HIRT-PUB08001	Presuming the number of P2P file exchange software nodes using the crawling method

(7) Others

- In cooperation with the Systems Development Laboratory, Hitachi, Ltd., we summarized the outcome of the “Development of Technology to Detect Information Leakage through Networks and Block Automatic Circulation of Leaked Information”, a project run by the Ministry of Internal Affairs and Communications, into a report to release in the HIRT Publications on our website. (See Table 2).
- We contributed articles concerning proactive measures against vulnerabilities to the ITpro Computer Security Incident Response Team (CSIRT) Forum of Nikkei Business Publications.

3 HIRT

To give you an in-depth understanding of HIRT, this section describes the organizational model adopted, the HIRT/CC, a coordinating unit, and the activities currently promoted by the HIRT/CC.

3.1 Organizational model

We have adopted an organizational model consisting of four IRTs. (See Figure 11 and Table 3). The four IRTs consist of three IRTs; each of which corresponds to an aspect of the Hitachi group and the HIRT Coordination Center (HIRT/CC), an IRT that provides coordination among the three. The first aspect is that which develops products related to information systems (Product Vendor IRT). The second is one that builds a system or provides a service using those products (SI Vendor IRT). The third aspect is one that administers Hitachi’s information systems as an Internet user (Internal User IRT). Such classifications not only clarify the role each IRT has to play but also promote security activities effectively and efficiently in partnership among the IRTs. HIRT refers to incident operation activities within the entire Hitachi group in a broader sense, and the HIRT/CC in a narrower sense.

As shown in Table 4, we experienced four phases before four IRTs had been established. After the roles and functions of the three IRTs had been roughly decided, the HIRT/CC was formed as a coordinator for the internal and

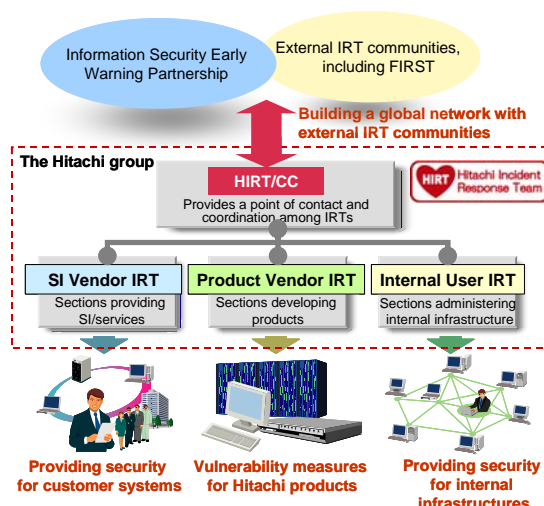


Figure 11: Four IRTs as an organizational model

Table 3: Role of each IRT

Category	Role
HIRT/CC	Corresponding sections: HIRT/CC - Provides a point of contact to external CSIRT organizations, such as FIRST, JPCERT/CC and CERT/CC. - Provides coordination among the SI Vendor, Product Vendor and Internal User IRTs.
SI Vendor IRT	Corresponding sections: Sections providing SI/services - Promotes CSIRT activities for customer systems. - Provides customer systems with equivalent security against reported vulnerabilities to that for internal systems.
Product Vendor IRT	Corresponding sections: Sections developing products - Provides support to promote vulnerability measures for Hitachi products and the release of information concerning such measures - Promptly investigates whether a reported vulnerability has an impact on Hitachi products, notifies users of the impact, if any, and provides a security fix.
Internal User IRT	Corresponding sections: Sections administering internal infrastructures - Provide support to promote security measures for internal networks lest Hitachi websites should be used as a base for making unauthorized access.

external IRTs. In addition, each phase has a trigger that causes a corresponding IRT to be formed. For example, Multiple Vulnerabilities in Many Implementations of SNMP [14], as reported by CERT/CC, worked as a trigger to form the Product Vendor IRT in the second phase, while in the third, the start of an “Information Security Early Warning Partnership” worked as a trigger to establish the SI Vendor IRT.

Table 4: Phases until the organization was formed

Phase	Overview
April 1998	We started CSIRT activities as a project to establish a Hitachi CSIRT framework.
1 st phase Establishing the Internal User IRT (1998 - 2002)	In order to run a Hitachi CSIRT on a trial basis, we formed a cross-sectional virtual team within the Hitachi group to start mailing list based activities. Most of the members comprised internal security experts and those from sections administering internal infrastructures.
2 nd phase Establishing the Product Vendor IRT (From 2002 -)	In order to start conducting activities seriously as a Hitachi CSIRT, the sections developing products played a central role in establishing an organizational structure of the Product Vendor IRT with related business sites through cooperation from internal security experts, the sections administering internal infrastructures, the sections developing products and the Quality Assurance Department.
3 rd phase Establishing the SI Vendor IRT (From 2004 -)	We started to form an SI Vendor IRT with the sections providing SI/services. In order to swiftly implement proactive measures against vulnerabilities, as well as reactive measures against incidents, via partnership with Internet communities, we started to form HIRT/CC, which provides a point of contact for external organizations and enhances coordination among Internal IRTs.
October 2004	We established the HIRT/CC.

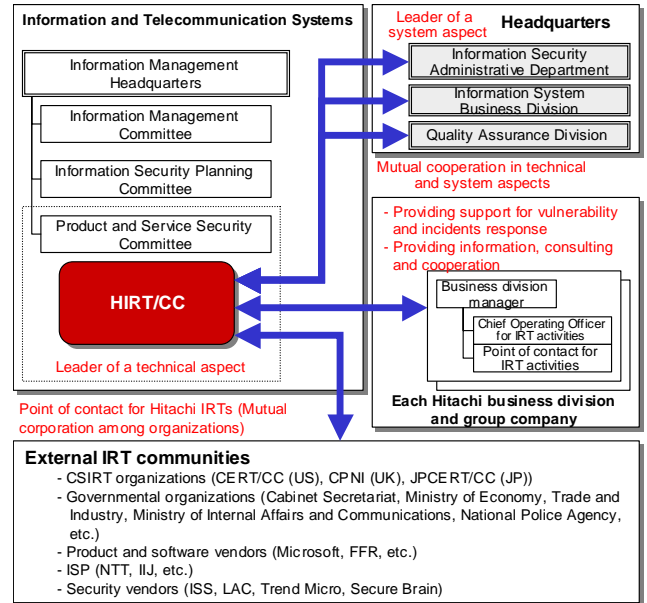


Figure 12: Positioning of the HIRT/CC

3.2 Positioning of the HIRT/CC

The HIRT/CC is an executive arm of the Product and Service Security Committee under the Information and Telecommunication Systems. Its main activities include promoting security measures in terms of organizational system and technology through mutual cooperation with the Information Security Administrative Department, Information System Business Division, and Quality Assurance Division, helping each business division and group company implement proactive measures against vulnerabilities, as well as reactive measures against incidents, and promoting security measures through partnerships among organizations as a point of contact for CSIRT activities in the Hitachi group (Figure 12).

The organization of the HIRT/CC features the combination of vertical and horizontal collaboration of people and units. More specifically, this model has achieved a flat and cross-sectional organizational system for implementing measures and coordinating ability through distribution of functions by creating a virtual

organization consisting of dedicated personnel and those who are assigned to HIRT as an additional task.

Such organization is based on the concept that the performance of duties by each section and cooperation among sections are necessary to solve security issues, given the great diversification among components in the information systems.

3.3 Main activities for HIRT center

The main activities of the HIRT center currently being promoted include CSIRT activities for internal organizations (See Table 5) and those for external organizations (See Table 6).

As for internal CSIRT activities, we issued know-how obtained through the collection and analysis of security information as security alerts and advisories, and are promoting activities to provide feedback to product development processes in the form of guidelines and supporting tools.

Table 5: (Internally) promoting projects

Category	Overview
Collecting, analyzing and providing security information	<ul style="list-style-type: none"> ➤ Promoting Information Security Early Warning Partnership (Information concerning proactive measures against vulnerabilities, as well as reactive measures against incidents/horizontal deployment of know-how) ➤ Building a wide area observation network based on the Hitachi Security Operation Center Information eXchange (SOC-IX) ➤ Developing and deploying technical know-how to protect against malware
Promoting proactive measures against vulnerabilities, as well as reactive measures against incidents for products/services	<ul style="list-style-type: none"> ➤ Improving the infrastructure to provide Hitachi security information in one-stop leveraging HIRT security information portal. ➤ Developing a framework for sending internal security information
Enhancing security technology for products/services	<ul style="list-style-type: none"> ➤ Enhancing web application security ➤ Establishing more specific security measures for intelligent home appliance, embedded products and control systems. ➤ Developing and deploying technical know-how for proactive measures against vulnerabilities ➤ Developing development and management processes (Guidelines for development, testing and operation and maintenance)
Developing a framework for research activities	<ul style="list-style-type: none"> ➤ Developing a framework for joint research with the Systems Development Laboratory (for P2P observation, etc)

Table 6: (Externally) promoting projects

Category	Overview
Strengthening the domestic partnership for CSIRT	<ul style="list-style-type: none"> ➤ Deploying proactive measures against vulnerabilities based on the Information Security Early Warning Partnership ➤ Promoting activities related to the Nippon CSIRT Association
Strengthening the overseas partnership for CSIRT activities	<ul style="list-style-type: none"> ➤ Establishing a partnership with overseas CSIRT organizations and overseas product vendor IRTs through lectures at and participation in FIRST conferences and symposiums ➤ Promoting UK WARP related activities. ➤ Adopting vulnerability-related standards, such as CVE, CVSS and CPE
Developing a framework for research activities	<ul style="list-style-type: none"> ➤ Establishing a joint research between Tokai University (Professor Hiroaki Kikuchi) and HIRT. ➤ Participating in academic research activities, such as a workshop to develop human resources for research on malware countermeasures

Table 7: Classification of security information issued by HIRT

ID number	Usage
HIRT-FUPyynn	Priority: Urgent Distributed to: Only relevant sections Is used to notify relevant sections of a vulnerability when an HIRT member has found such vulnerability in a Hitachi group product or a website, or received such information.
HIRT-yynn	Priority: Middle – High Distributed to: No restriction Is used to widely call attention to proactive measures against vulnerabilities, as well as reactive measures against incidents.
HIRT-FYIynn	Priority: Low Distributed to: No restriction Is used to notify people of HIRT open meetings or lecture meetings.

As for the internal issue of security alerts and advisories, we have broken down HIRT security information into two types since June 2005: HIRT security information that aims to distribute security alerts and hot topics widely and HIRT-FUP information used to request relevant sections to take reactive measures, to take its priority and the needs into account (See Table 7 and Figure 13). To convey information efficiently, we reduce the number of issues of information by aggregating the same, and release the information in collaboration with the Information Security Administrative Department and Quality Assurance Division.

We are now promoting activities to expand the Hitachi group's commitment to product and service security to Internet users via our security portal website, as a proactive measure against vulnerabilities, as well as reactive measures against incidents.

In particular, for issuing security information on proactive measures against vulnerabilities, as well as reactive measures against incidents, to external entities, we also adopt an approach in which an "Emergency Level" of information is determined and a "Website Level" at which the information is to be published is selected, in addition to just routinely publishing security information via our security portal website. (See Figure 14).

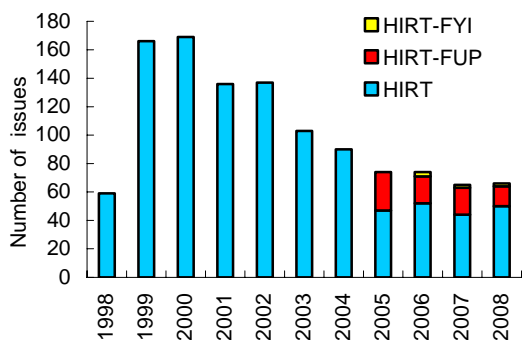


Figure 13: Number of issues of security information by ID number

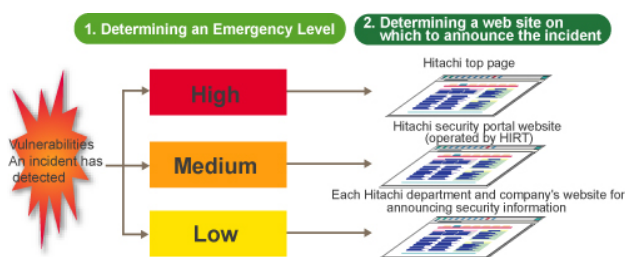


Figure 14: Conceptual view of issuing information based on “Emergency Level” x “Website Level”

4 Activity summary from 1998 to 2007

This section describes the activities for each year from 1998 when the HIRT project started.

4.1 Year 2007

(1) Starting Hands-on security training in HIRT open meetings

We held HIRT open meetings focusing on Hands-on security training twice in March and June 2007 in order for web application developers to implement the guideline “Web Application Security Guide” more practically.

(2) Founding the Nippon CSIRT Association

In order to develop a system based on a strong trusting relationship among CSIRTs that can successfully and promptly react to events that single CSIRTs find it difficult to solve, we founded the Nippon CSIRT Association with IIJ-SECT (IIJ), JPCERT/CC, JSOC (LAC), NTT-CERT (NTT) and SBCSIRT (Softbank) in April 2007. [15].

(3) Joining UK WARP

In order to strengthen the overseas partnership on CSIRT activities, we joined the Warning, Advice and Reporting Point (WARP), promoted by the Centre for the Protection of National Infrastructure (CPNI), a British government security organization, in May 2007. [16].

(4) Strengthening the partnership with the CSIRT community

As an activity to strengthen partnership among organizations, we met regularly with NTT-CERT[9] since 2006 in order to exchange information to improve CSIRT activities. In order to establish a mutually cooperative relationship with NTT-CERT to observe the Bots, in 2007, we considered the joint use of observation data.

(5) Lecture meetings

- August 2007: “Inspection of Vulnerabilities Using Static Analysis” by Dr. Yuji Ukai, Fourteen Forty Research Institute

4.2 Year 2006

(1) Providing a unified point of contact for vulnerability reporting

In November 2006, in order to circulate vulnerability-related information properly in the Hitachi group and thereby promote measures against vulnerabilities in Hitachi software products and websites, we provided a unified point of contact for receiving reports on vulnerabilities found in software products and web applications.

(2) Enhancing Web application security

In October 2006, as part of web application security measures in the Hitachi group, we created guidelines and checklists and provided support for their implementation in the Hitachi group. We updated “Web Application Security Guide (Development) V2.0” by adding new vulnerabilities, such as LDAP injection and XML injection, and a method for checking the existence of such vulnerabilities.

(3) Calling attention to information leakage caused by P2P file exchange software

Antinny is a virus that has penetrated widely via “Winny”, file exchange software that appeared in August 2003. The virus causes infected PCs to leak information and attack particular websites. In April 2006, HIRT issued a security alert entitled “Prevention of Information Leakage Caused by Winny and Proactive Measures against It” based on previous experience of threats.

(4) Starting product security activities for intelligent home appliance and embedded products

We have started product security activities for intelligent home appliance and embedded products. HIRT focused on the Session Initiation Protocol (SIP), a call control protocol used for Internet telephony, and summarized related security tools and measures into a report.

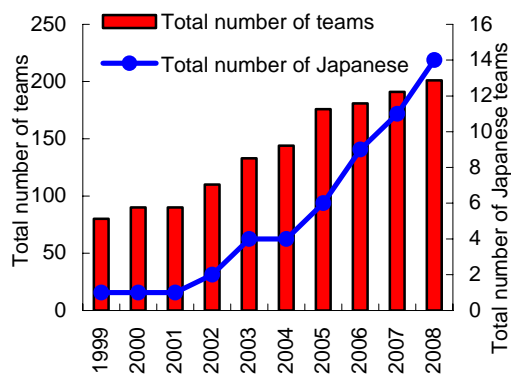


Figure 15: Changes in the number of members of FIRST

(5) Strengthening partnership with the CSIRT community

In March 2006, we introduced Hitachi's CSIRT activities in a workshop held by NTT-CERT to exchange information to improve CSIRT activities with each other.

(6) Lecture meetings

- May 2006: "Security for embedded systems", by Dr. Yuji Ukai, eEye Digital Security
- September 2006: "Measures against Botnets in Telecom-ISAC Japan", by Mr. Satoru Koyama, Telecom-ISAC Japan

(7) Other activities

- Started adding a digital signature to technical documents (PDF files) issued from HIRT.[17]

4.3 Year 2005

(1) Joining FIRST

In January 2005, to boost experience in CSIRT activities while creating an organizational structure to address incidents in partnership with CSIRT organizations overseas, we joined the Forum of Incident Response and Security Teams (FIRST), an international community for computer incident handling teams. [18].The preparation period extended for about one year, since any team wishing to join the community must obtain recommendations from two member teams before doing so.

As of January 2009, fourteen teams from Japan had joined the community. They include CFC (Info-Communications Bureau, the National Police Agency), HIRT (Hitachi), IIJ-SECT (IIJ), IPA-CERT (Information-technology Promotion Agency), JPCERT/CC, JSOC (LAC), KKCSIRT (Kakaku.com), NCSIRT (NRI Secure Technologies), NISC (National Information Security Center), NTT-CERT(NTT), Rakuten-CERT (Rakuten), RicohPSIRT (Ricoh), SBCSIRT (Softbank) and YIRD (Yahoo). (See Figure 15).

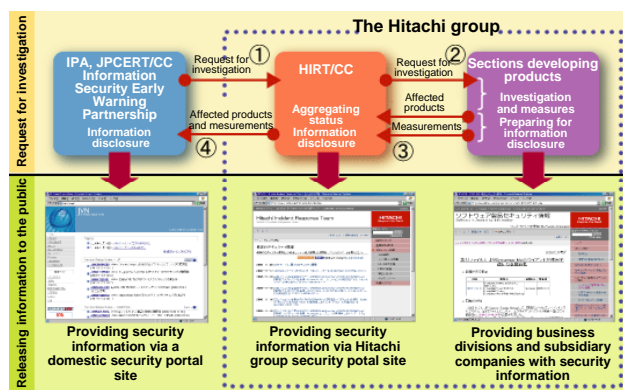


Figure 16: Providing security information on the security information portal

(2) Setting up a security information portal site

In September 2005, in order to provide Internet users with comprehensive information on security problems applicable to the products and service of the Hitachi group, we set up a security information portal site within which the security information provided through the websites of Hitachi business divisions and group companies is integrated. (See Figure 16). We also created "Guidance for Providing Security Information from Websites to External Users, V1.0".

Security information portal site:

Japanese: <http://www.hitachi.co.jp/hirt/>

English: <http://www.hitachi.com/hirt/>

(3) Strengthening the domestic partnership for CSIRT activities

In order to strengthen the domestic partnership for CSIRT activities, we hold meetings with domestic teams that are members of FIRST, and individual meetings with NTT-CERT and Microsoft Product Security Team (PST), and established an emergency call network to be used, for example, when a website is found to have been tampered.

4.4 Year 2004

(1) Participating in the Information Security Early Warning Partnership

The Information Security Early Warning Partnership started in July 2004 when the "Standard for Handling Information Related to Vulnerabilities in Software, etc." was implemented.[19][20]

The Hitachi group registered itself as a product development vendor to the Partnership, using HIRT as a point of contact, and started publishing Hitachi's vulnerability handling status on JP Vulnerability Notes (JVN).[21]

Table 8: Information on point of contact

Name	“HIRT”: Hitachi Incident Response Team.
Address	890 Kashimada, Saiwai, Kawasaki City, Kanagawa, 212-8567
E-mail	hirt@hitachi.co.jp
PGP key	KeyID = 2301A5FA Key fingerprint 7BE3 ECBF 173E 3106 F55A 011D F6CD EB6B 2301 A5FA pub 1024D/ 2003-09-17 HIRT: Hitachi Incident Response Team hirt@hitachi.co.jp

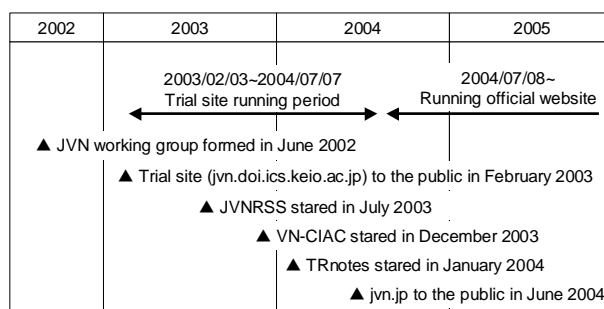


Figure 17: Building and running a JVN trial site

(2) Enhancing web application security

In November 2004, we created the “Web Application Security Guide (Development), V1.0” and distributed it throughout the Hitachi group. The guide summarizes typical problems that need to be considered when designing and developing web applications, and provides an overview of measures taken to solve such problems.

(3) Lecture meetings

- January 2004: “Security business affairs after Blaster in the US”, by Mr. Tom Noonan, President and CEO of Internet Security Systems (ISS)

4.5 Year 2003

(1) Starting web application security activities

We started to consider a method for enhancing web application security and developed the “Procedure for Creating a Security Measure Standard for Web Application Development V1.0” with business divisions.

(2) Disseminating vulnerability information from NISCC throughout Hitachi

Following the dissemination of vulnerability information from CERT/CC in 2002, we started obtaining/publishing information in accordance with the NISCC (currently, CPNI) Vulnerability Disclosure Policy. It was 006489/H323 of January 2004 when information on a Hitachi product was first published in NISCC Vulnerability Advisory after starting the activity. [22].

(3) Providing a point of contact for external organizations

In line with the more active reporting and releasing of information concerning the discovery of a vulnerability ([23], [24], and [25]), we provided a point of contact, as shown in Table 8, that initiates actions when vulnerabilities or malicious actions in Hitachi products and Hitachi-related websites are pointed out.

4.6 Year 2002

(1) Disseminating vulnerability information from CERT/CC throughout Hitachi

SNMP vulnerability [14] reported from CERT/CC in 2002 affected a wide range of software and devices. This provided an opportunity to start the Product Vendor IRT and obtaining/publishing information based on the CERT/CC Vulnerability Disclosure Policy.[26] It was VU#459371 of October 2002 when Hitachi product information was first published in the CERT/CC Vulnerability Notes Database after commencing this activity.[27]

(2) Assisting JPCERT/CC in building Vendor Status Notes

We provided support to build and operate a trial website, JPCERT/CC Vendor Status Notes (JVN) (<http://jvn.doi.ics.keio.ac.jp/>), in February 2003, as an attempt to improve the domestic circulation of security information. (See Figure 17)[28][29]. With the implementation of the “Standard for Handling Information Related to Vulnerabilities in Software, etc.” in July 2004, the roles of the trial site were transferred to Japan Vulnerability Notes (JVN), a site releasing information on reported vulnerabilities (<http://jvn.jp/en/index.html>).

4.7 Year 2001

(1) Investigating the activities of worms attacking web services

We investigated the activities of worms attacking web services in 2001, CodeRed I, CodeRed II and Nimda, from June 15, 2001 to June 30, 2002, based on the log data from the websites on the Internet. For CodeRed II and Nimda (Figure 18), which caused significant damage in Japan, the log reveals that the time span between the time at which the attack was first logged and the date on which attacks occurred most frequently was only approximately two days, indicating that damage caused by the worms had spread rapidly and widely.

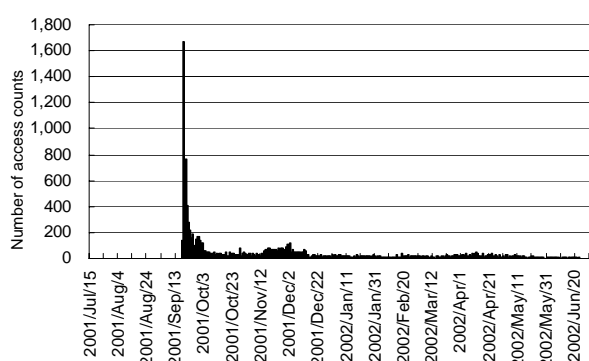


Figure 18: Changes in the number of Nimda log counts found during the observation period (for Nimda)

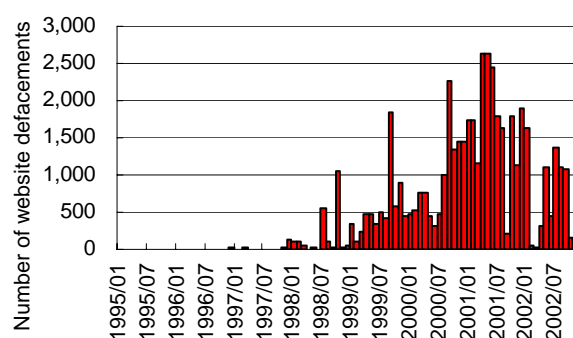


Figure 19: Changes in the number of websites defacements

4.8 Year 2000

(1) Investigating the severity metrics for vulnerabilities

In order to measure the severity level of vulnerability exploited for destructive or security-compromising activities, we investigated the severity metrics used by relevant organizations and summarized the results into a report.

CERT/CC publishes notes called “Vulnerability Notes” [30] for each vulnerability. It provides the Severity Metric indicating the severity of vulnerability. [31] Common Vulnerabilities and Exposures (CVE) classifies information security vulnerabilities into “Vulnerabilities” and “Exposures” and focuses on the former [32]. The former is defined as mistakes in software to violate a reasonable security policy and the latter as environment-specific, configuration issues or mistakes in software used to violate a specific policy. The National Institute of Standards and Technology (NIST) uses whether or not a CERT advisory and CVE identifier number has been issued as a guide to determine the severity of vulnerability, and classifies vulnerabilities into three levels in the ICAT Metabase [33], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [34] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

4.9 Year 1999

(1) Launch of the hirt.hitachi.co.jp domain

To improve the provision of security information to the Hitachi group, we created an internal domain for HIRT projects to set up a website (hirt.hitachi.co.jp) in December 1999.

(2) Investigation of website defacement

Website defacement was a major type of incidents since it occurred for the first time in the US in 1996 until the network worm era started (2001 - 2004). We conducted a research on webpage defacing from 1999 to 2002 to find out how malicious activities were performed. (See Figure 19).

4.10 Year 1998

(1) Starting to provide HIRT security information

In April 1998, we started to provide information on security measures mainly using an internal mailing list and an internal website for HIRT projects. This information is based on the security information issued by CERT/CC, JPCERT/CC, and product vendors (Cisco, HP, Microsoft, Netscape, Sun Microsystems, etc.).

(2) Lecture meetings

On June 25 - 26, 1998, we provided “Network security” training for Hitachi. We invited an US security expert who had also participated in the US Security Conference DEFCON [35] as a speaker as an instructor.

5 Conclusion

As described initially, as far as the transition of incidents over several years is concerned, new security breaches arise in short cycle time, and remain constant once established. In addition, the technology is inherited and evolved through such security breaches for better or worse. Under these circumstances, security problems must be addressed and solved through cross-organizational collaboration, namely, a combination of organizations’ abilities to observe, analyze and respond to the situation systematically.

In future, HIRT will continue to promote proactive measures against vulnerabilities using the Information Security Early Warning Partnership, establish a partnership with other organizations so that CSIRTs can mutually cooperate to combat new threats, and develop a cooperative relationship that can improve proactive measures against incidents.

Acknowledgments

The Hitachi Incident Response Team (HIRT) was awarded with the “Commerce and Information Policy Bureau Chief Prize, Ministry of Economy, Trade and Industry (Information Security Promotion Section)” at the 2008 Information Technology Promotion Period Commemorative Ceremony held on October 1, 2008 by the Information Technology Period Promotion Conference. The conference featured the participation of the Ministry of Economy, Trade and Industry, Cabinet Office, the Ministry of Internal Affairs and Communications, the Ministry of Finance, the Ministry of Education, Culture, Sports, Science and Technology, and the Ministry of Land, Infrastructure, Transport and Tourism. [36]. We express our deep gratitude towards the people concerned within and outside Hitachi who supported us in promoting HIRT activities.

(February 19, 2009)

References

- 1) NIST NVD (National Vulnerability Database), <http://nvd.nist.gov/>
- 2) Information-Technology Promotion Agency, Japan: Vulnerabilities >> Quarterly Reports, http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html
- 3) LAC Corporation: Number of Detected SQL Injection Attacks (Up to December 2008) (2009-01-08), <http://www.lac.co.jp/info/alert/alert20090108.html>
- 4) Trend Micro Incorporated: Report on Internet Threat, http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html
- 5) Information-Technology Promotion Agency, Japan: Verification Tools for Well-known TCP/IP-related Vulnerabilities (2009/1), http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html
- 6) Information-Technology Promotion Agency, Japan: High Reliability Organization Requirements for Critical Infrastructures (2008/2), http://www.ipa.go.jp/security/event/2007/infra-sem/pdf/20080220MEIJI-Nakanishi_sama.pdf
- 7) Information-Technology Promotion Agency, Japan: Countermeasures against DNS Cache Poisoning (2009/2), http://www.ipa.go.jp/security/vuln/DNS_security.html
- 8) Recording Site for Joint Workshop on Security 2008, Tokyo (2008/3), <http://www.nca.gr.jp/jws2008/index.html>
- 9) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), <http://www.ntt-cert.org/>
- 10) Considerations on Classification on How PCs Are Infected with Malware, Information Processing Society, CSEC Research Report Vol. 2008 No. 21. (2008/3)
- 11) Investigation Results on Information Leakage in 2008 Caused by File Exchange Software (2008/12), <http://www.hitachi.co.jp/hirt/publications/hirt-pub08008/index.html>
- 12) Malware Circulating in P2P File Exchange Software Environment (2008/12), <http://www.hitachi.co.jp/hirt/publications/hirt-pub08007/index.html>
- 13) Virtual Demonstration of Virus-attached Mail That Pretended to Be a Call for Papers (CFP) for CSS2008 (2009/1), <http://www.sdl.hitachi.co.jp/csec/css2008-cfp-malware/malware-demo.html>
- 14) CERT Advisory CA-2002-03, “Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)” (2002/2), <http://www.cert.org/advisories/CA-2002-03.html>
- 15) CSIRT - Nippon CSIRT Association, <http://www.nca.gr.jp/>
- 16) WARP (Warning, Advice and Reporting Point), <http://www.warp.gov.uk/>
- 17) GlobalSign Adobe Certified Document Services, <http://www.globalsign.com/adobe-cds/index.htm>
- 18) FIRST (Forum of Incident Response and Security Teams), <http://www.first.org/>
- 19) Ministry of Economy, Trade and Industry, Notification No. 235: Standard for Handling Information Related to Vulnerabilities in Software, etc., (2004/7), <http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf>
- 20) Information-Technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline (2008/7), http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html#Partnership
- 21) JVN (Japan Vulnerability Notes), <http://jvn.jp/>
- 22) NISCC: NISCC Vulnerability Advisory 006489/H323: Vulnerability Issues in Implementations of the H.323 Protocol (2004/1), <http://www.kb.cert.org/vuls/id/JSHA-5V6H7S>
- 23) Organization for Internet Safety: Draft Security Vulnerability Reporting and Response Process (2003/7), <http://www.oisafety.org/resources.html>
- 24) Information-Technology Promotion Agency, Japan: Research Reports on Policy for Security Vulnerability Information Disclosure, <http://www.ipa.go.jp/security/awareness/vendor/vulnerability200309012.pdf>

- 25 LAC Corporation: Policy for Vulnerability Reporting and Disclosure (2003/8),
http://www.lac.co.jp/info/advisory/pdf/vulnerability_reporting_and_disclosure.pdf
- 26) CERT/CC Vulnerability Disclosure Policy,
http://www.cert.org/kb/vul_disclosure.html
- 27) US-CERT: Vulnerability Note VU#459371: Multiple IPsec implementations do not adequately validate authentication data” (2002/10),
<http://www.kb.cert.org/vuls/id/459371>
- 28) Considerations on JPCERT/CC Vendor Status Notes DB: JVN, CSS2002 (2002/10),
<http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf>
- 29) Deploying JP Vendor Status Notes (JVN) for Dissemination of Security Information Throughout Japan (2005/5), <http://www.hitachi.com/rd/sdl/people/jvn/>
- 30) CERT/CC Vulnerability Notes Database,
<http://www.kb.cert.org/vuls>
- 31) CERT/CC Vulnerability Note Field Descriptions,
<http://www.kb.cert.org/vuls/html/fieldhelp>
- 32) CVE (Common Vulnerabilities and Exposures),
<http://cve.mitre.org/>
- 33) ICAT, <http://icat.nist.gov/>
- 34) CVSS (Common Vulnerability Scoring System),
<http://www.first.org/cvss/>
- 35) DEFCON, <http://www.defcon.org/>
- 36) 2008 Information Technology Period Promotion - Awarding companies that have contributed to the promotion of information technology in 2008 (2008/10), <http://www.jipdec.or.jp/gekkan/ceremony/prize02.html>

Author

Masato Terada

After launching HIRT activities in 1998 on a trial basis, he launched a research site (<http://jvn.doi.ics.keio.ac.jp/>), a predecessor of JVN (<http://jvn.jp/>), in 2002 and acted as a point of contact for HIRT in order to promote external CSIRT activities, including participation in FIRST, an international CSIRT organization in 2005. Presently, he works as a technical member of the JPCERT Coordination Center, a researcher of the Information Technology Promotion Agency, Japan, and vice chief of the steering committee for the Nippon CSIRT Association.