HIRT: Annual Report 2012

Hitachi Incident Response Team (HIRT)
http://www.hitachi.com/hirt/

Kashimada 1-1-2, Saiwai, Kawasaki, Kanagawa, 212-8567 Japan

1 Introduction

2012 was a year in which CSIRT (Computer Security Incident Readiness/Response Team) took a major step forward amid the third or settlement phase (Figure 2) of unfolding CSIRT activities, which is based on the regional characteristics of Japan (what may be termed "localization"). The backdrop to this was the varied slew of security incidents that occurred in 2011 and the tendency for those under cyber attack to utilize CSIRTs as specialist capabilities for dealing with the incidents. This tendency can be glimpsed from the specialized and pragmatic collaboration utilizing CSIRTs mentioned in the Information Security Measure Promotion Council's *Forms to be Taken by Public-Private Collaboration Regarding Information Security Measures*, published on January 19, 2012 [1].

> I. Countermeasures regarding information sharing, etc., that the government should take with regard to targeted attack
> (Omission of middle part of a text)
> In public-private collaborations, rather than sharing in-formation among organizations in a vague manner, it is important for each organization to set up a specialist team with the capability to make emergency responses to information security incidents (hereinafter referred to as "CSIRT" (Computer Security Incident Response Team), etc.), and for specialized and pragmatic collaboration to be carried out among the CSIRTs, etc., inside the various organizations, both public and private.

From the very words "targeted attack" that come up in the *Forms to be Taken by Public-Private Collaboration*, one is apt to think of an invasive action that is targeted at a particular organization only. In most cases however, targeted attack - typified by the APT (Advanced Persistent Threats) that have been in the limelight since 2010 - are of a chain type (stepping-stone type) in which the outcome of one invasive action is utilized for the next action (targeted attack), leading up to a invasive action on a particular organization that is the ultimate target (Figure 1).

Therefore, security measures and incident responses for such attacks are designed to counter attacks that to a considerable extent act on, or are acted on by, other organizations. This is an approach that is not considered in the "entry-dispersion-exit countermeasure" type multi-layered defense of organizational-internal systems, and we believe that it is here that the significance of specialized, pragmatic collaboration among organizations via CSIRTs resides.

We consider that the requirements for CSIRTs in carrying out vulnerability countermeasures and incident responses are to possess the capabilities for "predicting and alerting from a technical point of view", "making technical coordination" and "collaborating with external communities on the technical aspects". We are not envisioning special requirements here.

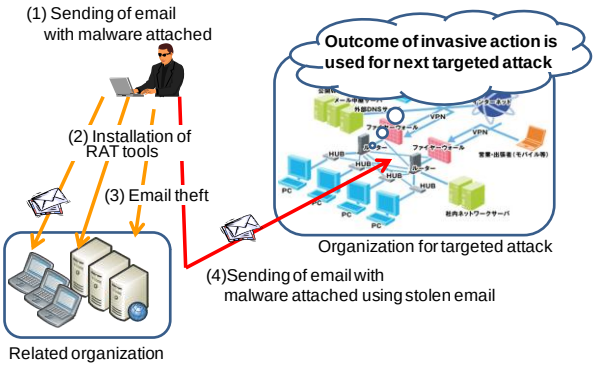


Figure 1: Chain type (stepping-stone type) targeted attack.

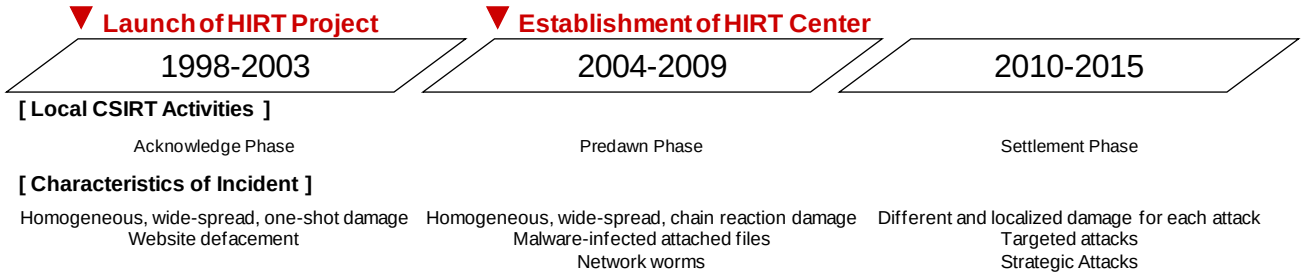


Figure 2: Positioning of CSIRT activities and development of incidents in Japan.

The role of CSIRTs is to make use of their experience in incident operation (the series of security measure actions implemented in order to predict and prevent damage from incidents and to lessen the expansion of damage after incidents occur) so as to "catch any sign of future threats and take actions as early as possible".

As an organization that possesses these capabilities and roles, HIRT (Hitachi Incident Response Team) leads the way in countermeasures for product and service vulnerability countermeasures and incident responses for malware infection and information leakage, besides being responsible - as the Hitachi Group's integrated CSIRT liaison organization - for implementing activities, mechanisms and framework for enhancing Hitachi's brand image in the field of security.

This report will introduce a summary of the vulnerabilities and threats and the activities of HIRT in 2012.

2 Overview of activities in 2012

This section focuses on HIRT activities in 2012.

2.1 Overview of Threats and Vulnerabilities

(1) Overview of Threats

The known threats like targeted attack, website compromised actions and USB malware (e.g. Conficker) have continued to cause damage. Features of 2012 were that denial-of-service attacks and website compromised actions by "hacktivists" became steady occurrences, and that inside Japan there manifested remote-control viruses (in October 2012), pop-up type phishing (also in October 2012) and other security incidents that impacted ordinary users.

- **Targeted attack**

APT (advanced persistent threats) has been attracting attention since 2010 as targeted attack. Table 1 shows forth cases of targeted attacks that are categorized as chain type (stepping-stone type).

In the U.S., a "Cyber Kill Chain" approach is under consideration to deal with such chain type targeted attack. This approach has the following features, as reported by Lockheed Martin at the ICIW (International Conference on Information Warfare and Security) in 2011 [2].

✓ Dividing the counter-actions into stages

This is an application of the U.S. Air Force's Kill Chain (F2T2EA) military concept to cyber attack countermeasures, and takes the form of a 7-stage attack counter-action model (Table 2).

✓ Implementing counter-actions from the initial stage onward

Whereas formerly the start point in most counter-actions was the detection of malware after entry (left chart of Figure 3), this approach also accommodates counter-actions that take as their start point the stage where the targeting email or similar is sent (right chart of Figure 3). Specific instances of such counter-actions are the J-CSIP (Initiative for Cyber Security Information Sharing Partnership for Japan) [3] promoted by the Ministry of Economy, Trade and Industry since 2012 and the Cyber Intelligence Information Sharing Network [4] promoted by the National Police Agency.

✓ Utilizing attack observables (what can be observed through an attack) and attack indicators (things for detecting an attack)

By progressively characterizing the attacker - What is it trying to execute? How is it trying to do it? and so on - the attacker's patterns, behavior, TTP (Tactics, Techniques and Procedures), intentions and so forth are made clear, and a campaign analysis is carried out.

Table 1: Cases of chain type (stepping-stone type) invasive actions.

Time	Outline
April 2011	In April 2011, customer information (email addresses, etc.) was stolen from the email system of Epsilon company. In the same month, messages that directed to illicit sites were transmitted to the stolen email addresses.
May 2011	In March 2011, RSA SecurID-related information was stolen from EMC Corporation. In mid-May, an invasive action on Lockheed Martin occurred that made ill use of the RSA SecurID-related information.
August 2011	On August 26, email was stolen from the Society of Japanese Aerospace Companies. On the same day, malware was inserted into the stolen email, which was then used as targeted email against the Society's member companies.

Table 2: Stages of counter-action against APT.

#	Stage	Outline
1	Reconnaissance	Surveying targets for attack, via websites, mailing lists and so forth
2	Weaponization	Preparing methods (such as injecting in an office document or PDF) for executing the exploit code
3	Delivery	Delivering the exploit code via email, websites, USB memories and so forth
4	Exploitation	Execution of the prepared exploit code under the target environment
5	Installation	Installing a RAT [*a] or back door, etc., in the target environment
6	Command and Control(C2)	Establishing remote control communication paths from the RAT or back door, etc., to the command server
7	Actions on Objectives	Execution of the ultimate objective - theft, disruption, etc. - or expansion of invasive action in the organization's internal network

[*a] RAT: stands for Remote Access Trojan or Remote Administration Tool. Program for operating a system that has been penetrated from a remote location. Used for stealth/theft activities and so on.

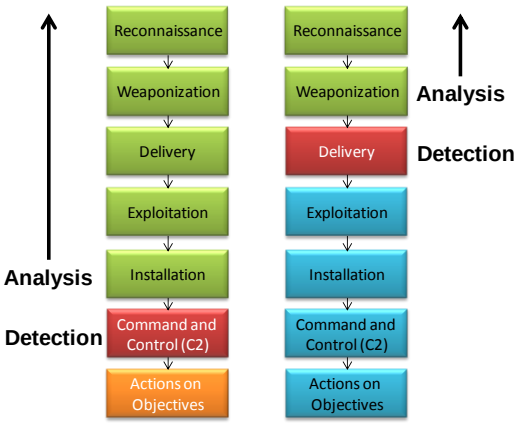


Figure 3: Shift in start points for counter-actions.

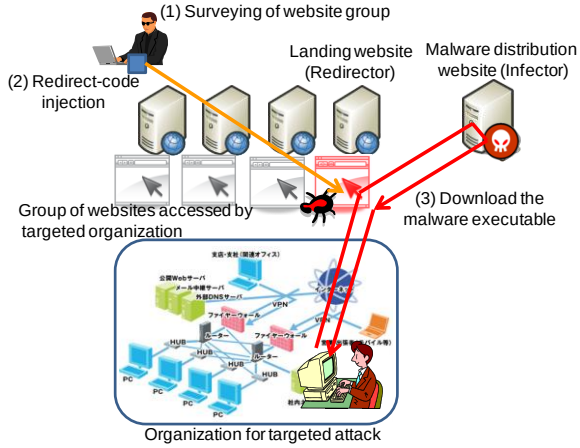


Figure 4: Watering Hole Attack.

- **Watering Hole Attack**

In the year 2000, malware was circulated by means of email attachments. By 2008, malware was circulated by means of websites. A similar development has taken place in targeted attack.

In 2011, targeted attack via email manifested themselves. In 2012, there was a rapid expansion in the ruse whereby tricks are stowed in a group of websites that people in a targeted organization are highly likely to visit, and those websites are then used as landing sites (redirectors) (Table 3). These are called "Watering Hole Attack" because lying in wait for users at a targeted organization to visit a landing website (redirector) is similar to a lion ambushing its prey at a watering hole (Figure 4). The gambit used here is that the landing websites redirect visitors to malware distribution websites. Technically this is a similar mechanism to the type of malware that redirects to a website - malware typified by Gumblar.

- **Conficker**

Conficker emerged as a worn that exploited Vulnerability in Windows, "Server Service Could Allow Remote Code Execution (MS08-067)" in around November 2008. In December 2008, by modification of Conficker (enhanced with the feature to infect via a USB memory stick), infection spread to the closed networks via a physical meditational means. Since 2009, the number of reports on the USB malware infection in Japan has been decreasing (Figure 5) [5]. However, according to the report of the Conficker Work Group, the number of computers infected with Conficker is about 2 million on the IP address base (Figure 6) [6].

(2) Overview of Vulnerabilities

The total number of vulnerabilities entered in the NIST NVD (National Vulnerability Database) [7] was 5,279 in 2012. 20 percent (1,029) of these were vulnerabilities in web software application products (Figure 7). Looking at the breakdown, it continues to be the case that cross-site scripting (XSS) and SQL injection account for about 80 percent of the vulnerabilities (Figure 8). XSS and SQL injection also account for some 60 percent of the vulnerabilities in operational websites that were reported to the IPA, with some 600 cases a year of these vulnerabilities being reported (Figure 9) [8].

The ICS-CERT (Industrial Control System-CERT) has issued 29 alerts and 81 advisories concerning vulnerabilities (Figure 10). Eight of the advisories (accounting for 10 percent) pointed out that credentials such as passwords and private keys were hard coded. Also, a large majority of the alerts issued in January 2012 concerned the PLC (programmable logic controller) vulnerabilities that were identified in a report at the SCADA Security Scientific Symposium held in mid-January.

Table 3: Cases of Watering Hole Attack.

Time	Outline
Since 2009	Elderwood Project [9] [Infector] Exploiting Adobe Flash Player vulnerabilities (CVE-2012-0779, CVE-2012-1535), an Internet Explorer vulnerability (CVE-2012-1875) and an XML core service vulnerability (CVE-2012-1889)
May 2012	Amnesty International Hong Kong (amnesty.org) [Infector] Exploiting an Internet Explorer vulnerability (CVE-2012-1875)
June & July 2012	VOHO campaign [10] [Redirector] Prince George's County, Rockland Trust and etc. [Infector] Toronto Curling Association, etc. Exploiting a Java vulnerability (CVE-2012-1723) and an XML core service vulnerability (CVE-2012-1889)
December 2012	Council on Foreign Relations [Infector] Exploiting an Internet Explorer vulnerability (CVE-2012-4792)

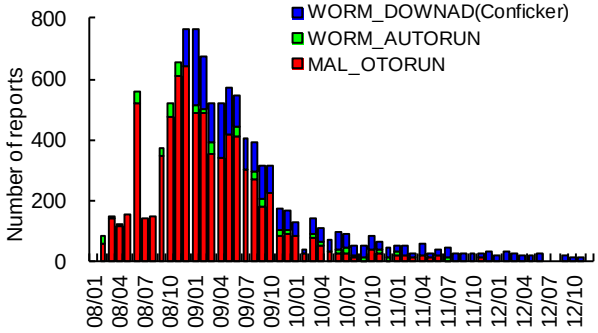


Figure 5: Number of Infection of USB Malware (per month).

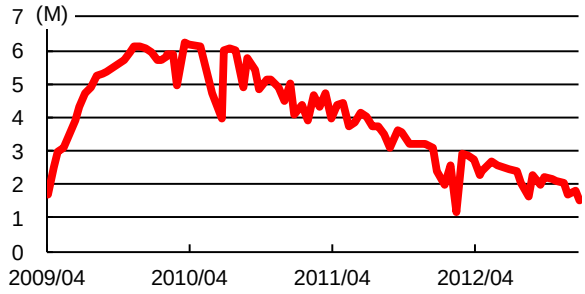


Figure 6: Number of Infection of ConfickerA+B (per day).

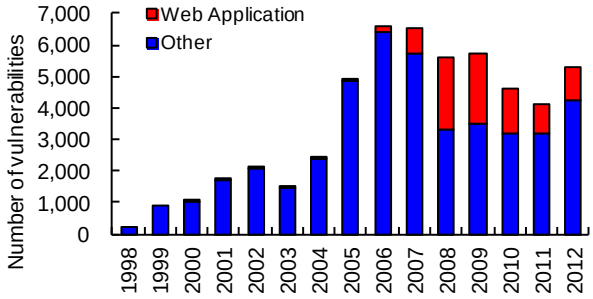


Figure 7: Number of Vulnerabilities Reported (Source: NIST NVD).

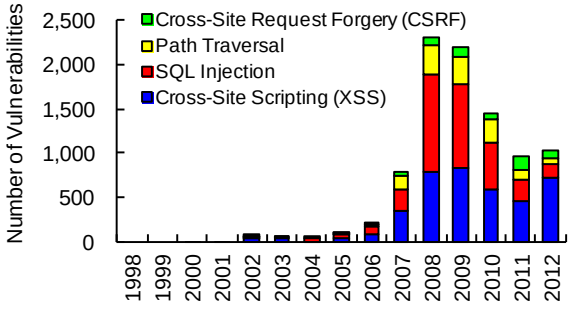


Figure 8: Changes in the number of vulnerabilities reported for software products of web application (Source: NIST NVD).

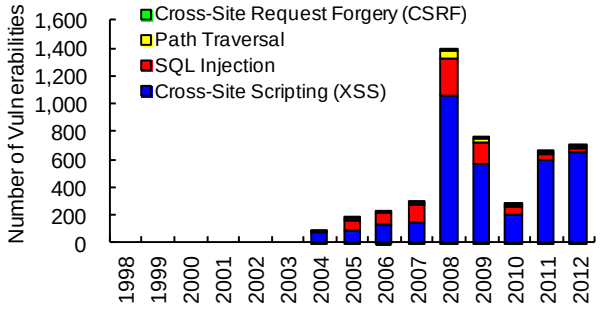


Figure 9: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC).

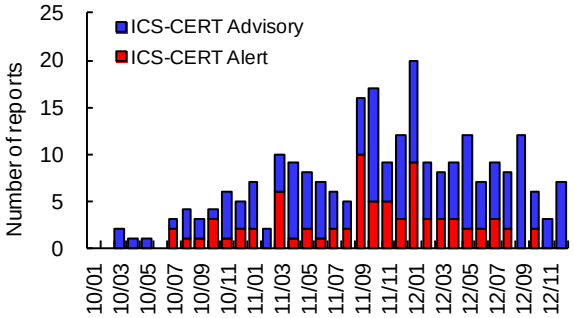


Figure 10: Change in the number of control system vulnerabilities reported (Source: ICS-CERT).

2.2 HIRT Activities

This subsection describes the HIRT activities in 2012.

(1) Start of improvement of Hitachi Group CSIRT activities (Phase 2)

In 2010, we started improvements of Hitachi Group CSIRT activities with the goal of "installing incident operation into the whole Hitachi Group" (Figure 12). 2012 was the third year of the improvements and in it we started Phase 2 (Figure 11), which is to strengthen collaboration inside the Hitachi Group through the HIRT supporting staff (staff who work with the HIRT Center to actively promote IRT activities).

- **Drawing up a list of check points to be re-verified in FY 2011**

Carrying on from FY 2010, we compiled into a list of check points the issues that had emerged through security reviews, incident response support and other operations. For FY 2011, we drew up as check points the issues during system construction, at the start of service provision and for maintenance.

- **Disseminating Countermeasure Information through HIRT OPEN Meeting**

We continued with rounding out the countermeasure dissemination through HIRT OPEN Meeting, and in addition we had the IRT supporting staff assist as instructors in mainly hands-on seminars (

Table 4) [*b] as part of moving forward with Phase 2. Through these activities, we expanded the IRT supporting staff who are able to assist in each field.

(2) Start of Advanced HIRT OPEN Meeting

As a part of the strengthening of collaboration with HIRT supporting staff, we started holding periodic (once or twice per term) Advanced HIRT OPEN Meeting that is coordinated with existing ML for horizontal dissemination of IRT activities. The Advanced HIRT OPEN Meeting handles subjects such as targeted attacks that have actually occurred, and attack methods, undetermined information and so forth that have come under attention. They further have the objective of creating sites for practicing "face-to-face information exchange instead of faceless information exchange", and thereby offering the IRT supporting staff opportunities to experience aspects of IRT activities while broadening their horizons.

(3) Trial IRT activities for individual domains

- **Three-tiered cycle for Incident Response and Readiness**

In countering cyber attacks, incident responses (after-the-fact counter-actions) are of course important for resolving vulnerability cases when they occur, but it is also indispensable to promote readiness (before-the-fact counter-actions) based on incidents and trends. Accordingly, by taking an "Three-tiered cycle for Incident Response and Readiness" approach (Figure 13) that incorporates the perspectives of individual business domains, we are promoting readiness (before-the-fact counter-actions) for individual business domains while clarifying the role-sharing and collaboration with the sections.

- **HIRT-FIS: Advanced endeavor in the financial domain**

On October 1, 2012, we organized up HIRT-FIS (Financial Industry Information Systems HIRT) inside our financial section. Positioned as a subset of HIRT for a particular field, HIRT-FIS is one of the endeavors for putting into effect the three-tiered cycle for Incident Response and Readiness and aims to be a path breaking CSIRT professional team tailored to the financial domain. Its background is that we considered that in the area of cyber attack countermeasures, there was a need for responses in line with the background circumstances and trends in particular domains, and are therefore taking the lead in studying and moving ahead with CSIRT activities tailored to domains (Figure 14).

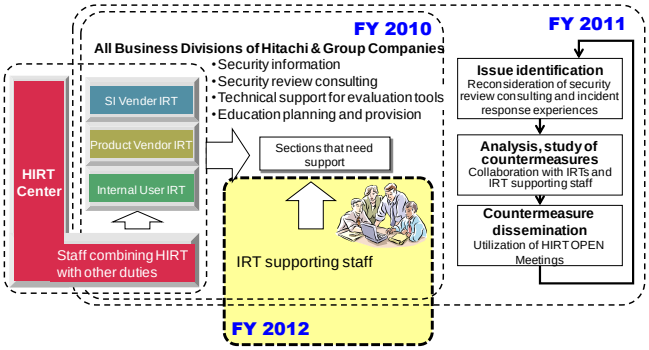
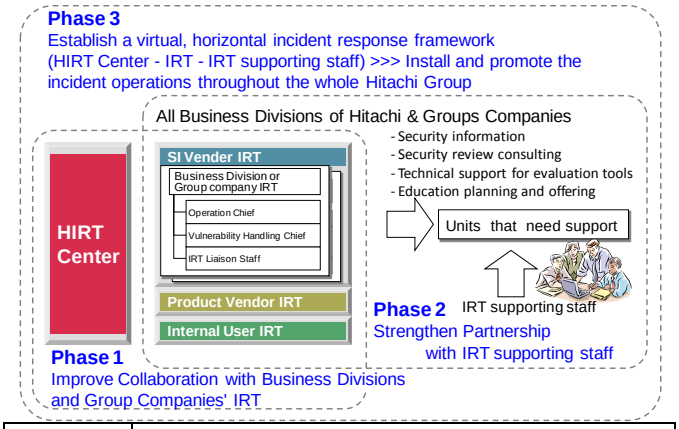


Figure 11: Phase 2 activities.



Category	Concrete Measures
Phase 1	Improve Collaboration with IRT of Business Divisions and Group Companies - Promote support activities with the collaboration between the IRT of Business Divisions and Group Companies - Establish an IRT coalition framework and mechanism to share technological know-how using the HIRT OPEN Meetings - Disseminate information about solutions/countermeasures for the problems discussed in the security review consultation.
Phase 2	Strengthen Partnership with IRT supporting staffs - Trial collaboration with IRT supporting staffs (of business divisions and group companies) - Bottom up the IRT activities with the IRT supporting staffs as a starting point
Phase 3	Establish Virtual, Horizontal Incident Response System - Promote various support activities by the HIRT Center, IRTs and IRT collision support members - Develop a HIRT in a broad sense (virtual organization model) by combining the user collaboration model (Phase 1,2) and entity collaboration model (Phase 3).

Figure 12: Scenario on a Virtual, Horizontal Incident Response System.

[*b] HIRT Open Meeting
HIRT Open Meeting is an activity is to popularize the HIRT community on the basis of relationships of trust. The meetings are held in line with policies of "offering an opportunity for HIRT Center members to share information about HIRT activities", "offering an open event for people of the Hitachi Group to learn about the HIRT Center's activities for the HIRT Center members to share information with and get opinions from non HIRT Center members", and "providing an opportunity to call for participation in the HIRT community on the basis of relationships of trust".
HIRT Open Meeting (Technical Meeting)
Technical Meeting is for designers, system engineers and persons willing to share their technical expertise come together to share and learn the technical know-how necessary to build security into products and services.

Table 4: HIRT OPEN Meeting (Technical meeting) in 2012.

Month	Outline
March	[External instructor] Nobuo Miwa (S&J Consulting) *Framework for Promoting Security Measures in Organizations*
May	[IRT supporting staff] Hands-on: Forensics at a compromised SSH system
July	[IRT supporting staff] Hands-on: Guide to Drawing Up Basic Security Specifications - Group discussion using Worksheet 1 -
August	[External instructor] Haruto Kitano (Oracle Corporation Japan) *Elements and Implementation of Database Security*
September	Seminar of countermeasures for external server vulnerabilities checking
	[External instructor] Daisuke Inoue (National Institute of Information and Communications Technology) *Trends in Cyber Attacks and the Cutting Edge of Cyber Security Research*
October	Cyber Attack Countermeasures at a Defensive Perspective
November	[External instructor] Tetsutaro Uehara (The Research Institute of Information Security (NPO)) *A Look Back Over Remote Control Incidents, the Firstserver Problem and the Leap-Second Problem*

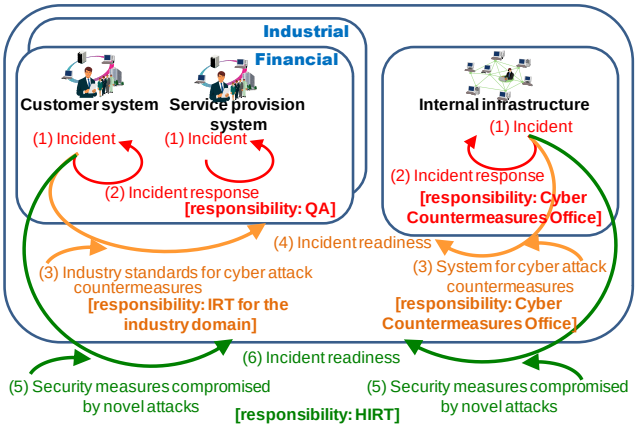


Figure 13: System view of "Three-tiered cycle for Incident Response and Readiness" approach.

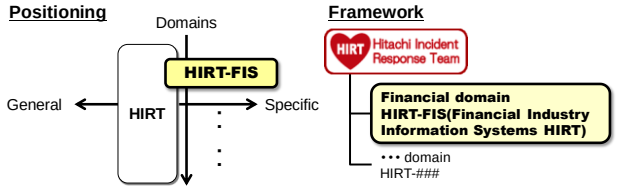


Figure 14: Positioning and framework of IRT activities for individual industry domains

(4) Scoring CVSS to security information at the HIRT website

We have begun scoring basic CVSS (Common Vulnerability Scoring System) values to the information that is published by the HIRT website. These values are indicated alongside the titles of the information. In cases where one security information item covers multiple vulnerabilities, we select the largest value among the CVSS score items.

[Example]
Cross-site scripting (XSS) vulnerability in Hitachi IT Operations product
(CVSS:4.3)

(5) Strengthening of Partnership with the CSIRT community

- **Holding of CSIRT Workshop 2012**

Together with NTT-CERT, OKI-CSIRT and JPCERT/CC, we held on February 29, 2012 the CSIRT Workshop 2012 as an opportunity for exchange of opinions on corporate CSIRT, targeting corporate staff interested in CSIRT activities[11]. Besides presenting examples of CSIRT implementation and CSIRT organization activities in Japanese companies, this workshop featured a lecture titled "The Government's Endeavors for Strengthening Public-Private Collaboration and Collaboration with Private CSIRTs and the Like", given by an official from the National Information Security Center.

- **Holding of FIRST Technical Colloquium 2012 Kyoto**

Together with the FIRST member teams in Japan, we held a FIRST Technical Colloquium at the Kyoto International Community House from November 13 to 15, 2012 [12]. The FIRST Technical Colloquiums are gatherings held in various regions roughly 3 or 4 times a year.

This Technical Colloquium had the theme phrase "Incident Response: Collaboration and Sharing" and was utilized as a site for working toward building a framework for swift and optimal responses based on strong relationships of trust among CSIRTs. Also, on the "Summit Days" when attention was focused on particular topics, we had exchanges of views on "Future of Global Vulnerability Reporting".

- **Launching of FIRST VRDX-SIG**

In order to continue with study of "Future of Global Vulnerability Reporting", which was raised at the FIRST Technical Colloquium 2012 Kyoto, we launched a Vulnerability Reporting and Data eXchange SIG (Special Interest Group) inside FIRST.

- **Participation in MWS (anti Malware engineering workshop) 2012**

Through our participation in MWS we are supporting research activities for malware countermeasures, and

through such support activities we are also aiming to contribute to the fostering of academic human resources that will feed into the next-generation CSIRT community.

(6) Other Activity

- Created a guidebook for new FIRST members [13]
- Gave a report on a "Feasibility study of scenario-based self-training material for incident responses" at the 24th Annual FIRST Conference [14]
- Contributed a paper on vulnerability countermeasures titled "Must-Read Vulnerability Information" to the ITpro CSIRT Forum held by Nikkei Business Publications, Inc. [15]
- Published a report on HIRT's activities on our security information portal (Table 5).

Table 5: Reports Published on the Security Information Portal.

Number	Title
HIRT-PUB12001	Topics in 2011 Regarding Problems for Transition from Old-Generation Encryption (commonly known as "Encryption Problems 2010")

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 that consists of four IRTs (Figure 15 and Table 6). There are three IRTs for the case with Hitachi Group itself; Product Vendor IRT; SI Vendor IRT, and Internal User IRT; each corresponding to one of the IRT's aspects: the Product Vendor IRT corresponds to the aspect of developer of products such as information systems and control systems, the SI Vendor IRT to that of a system integrator/service provider that uses those products, and the Internal User IRT to that of an internet user that operates and manages its own enterprise. By adding to these a fourth IRT - the HIRT/CC (HIRT Coordination Center), which carries out coordination work among the others - a model is obtained which we considered would be able to implement efficient and effective security measure activities that achieve collaboration among the IRTs, while making clear their individual functions. The name "HIRT" signifies the incident operation activities promoted by the Hitachi Group as a whole, in the broad sense, and signifies the HIRT/CC (HIRT Center) in the narrow sense.

In fact, four phases (set forth in Table 7) had to be gone through in order to put the four IRTs in place. For each phase, there was an "impetus" that encouraged organizational formation. For instance, the impetus for the second phase - establishing of the Product Vendor IRT - was the fact that the vulnerability in SNMP [16] reported by CERT/CC had affected large numbers of Hitachi products. The impetus for the third phase - establishing of the SI Vendor IRT - was the commencement of the Information Security Early Warning Partnership. The HIRT Center was set up to play the role of coordinator inside Hitachi and with external entities, after the other three IRTs had largely taken shape.

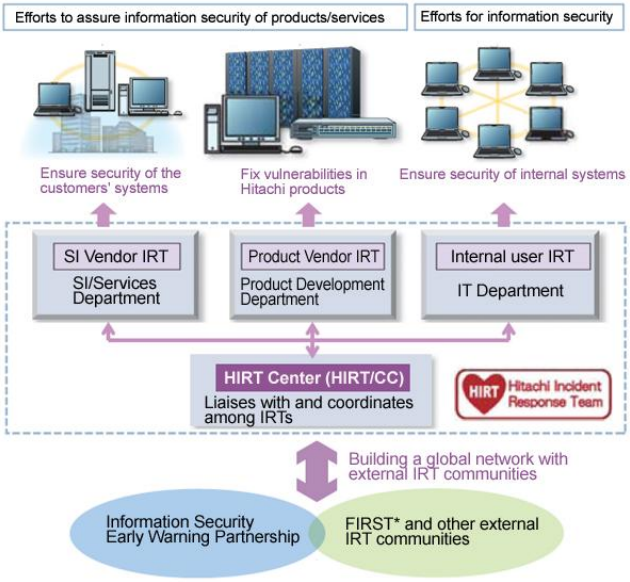


Figure 15: Four IRTs as an organizational model.

Table 6: 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 countermeasures - 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.

Table 7: Phases until the organization was formed.

Phase	Overview
April 1998	We started CSIRT activities as a project to establish a Hitachi CSIRT framework.
1st 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.
2nd 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.
3rd 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.

3.2 Position of HIRT/CC

The HIRT/CC is positioned under Information and Telecommunication Systems Company and has the role of not only a coordinator within and with the entities outside Hitachi but also a leader in promoting security technology. The main area of activity is to support the Product and Service Security Committee technically, to promote security efforts from the technical and institutional aspect in cooperation with the IT and Security Strategy Division, Information Technology Division and Quality Assurance Division.

Moreover, it also includes helping each business division and group company implement proactive security 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 16).

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 if 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 of HIRT Center

The main activities of the HIRT center currently being promoted include CSIRT activities for internal organizations (Table 8) and those for external organizations (Table 9). The internally-oriented CSIRT activities comprise issuing alerts and advisories that embody the know-how obtained through gathering and analyzing security information. Besides those, we are currently engaged in activities to feed such knowledge back into product development processes in the form of various guidelines and support tools.

HIRT security information in internally-oriented alerts and advisories has been broken down into two types since June 2005. One is HIRT security information that aims to distribute alerts and hot topics widely, and the other is HIRT-FUP information, which is used to request individual sections to take counter-action.This distinction is for the sake of information propagation and priority ranking. (Table 10 and Figure 17). To communicate information efficiently, we condense it to reduce the number of information items and release it in tandem with the IT & Security Strategy Division and the 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.

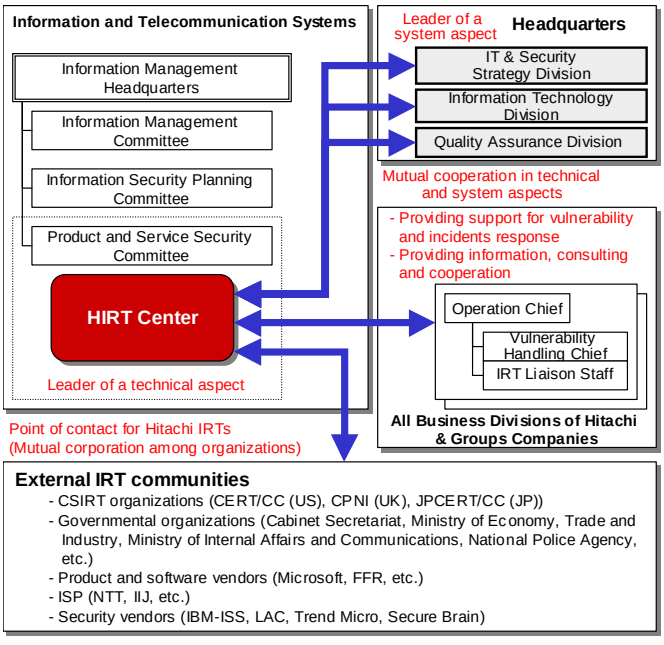


Figure 16: Position of HIRT Center.

Table 8: (Internally) promoting projects.

Category	Overview
Collecting, analyzing and providing security information	- 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)
Promoting proactive measures against vulnerabilities, as well as reactive measures against incidents for products/services	- Reinforcing the security foundation within the Hitachi Group through education for sections addressing security within the companies - Accumulating and deploying technical know-how for countermeasures against vulnerabilities and incident response - Promoting the publication of security information from external websites using the Security Information Integration Site
Enhancing security technology for products/services	- Improving the process to provide security (each guideline for development, inspection and operation) - Enhancing and expanding support and processes though internal support activities - Enhancing web application security
Developing a framework for research activities	- Developing a framework for joint research with the Yokohama Research Laboratory (for P2P observation, etc)

Table 9: (Externally) promoting projects.

Category	Overview
Strengthening the domestic partnership for CSIRT activities	- 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	- Improving partnerships with overseas CSIRT organizations/product vendor IRTs through lectures or events at FIRST conferences - Promoting UK WARP related activities. - Countermeasures against vulnerabilities, such as CVE and CVSS, and standardization of incident response (ISO, ITU-T) [*c]
Developing a framework for research activities	- Establish 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 (MWS) [17]

[*c] Work had begun in 2007 in ISO SC27/WG3 to develop an international standard "Vulnerability Disclosure (29147)". Work had begun in 2009 in ITU-T SG17 Q.4 to develop an international standard "Cyber security Information Exchange Framework (X.cybex)".

Table 10: Classification of security information issued by HIRT.

ID number	Usage
HIRT-FUPyynnn	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-yynnn	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-FYIyynnn	Priority: Low Distributed to: No restriction Is used to notify people of HIRT OPEN Meetings or lecture meetings.

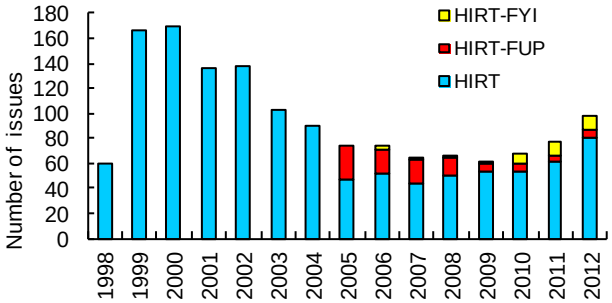


Figure 17: Number of issues of security information by ID number.

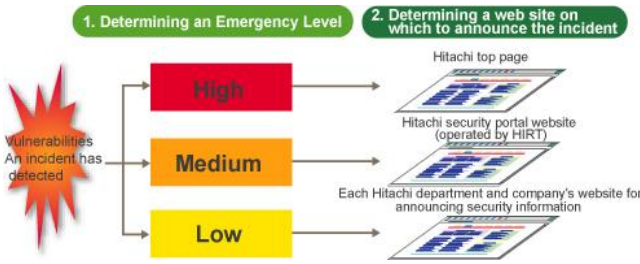


Figure 18: Conceptual view of issuing information based on "Emergency Level" x "Website Level".

In particular, for issuing security information for vulnerabilities and 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 (Figure 18).

4 Activity Summary from 1998 to 2011

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

4.1 The Year 2011

(1) Improvement of Hitachi Group CSIRT Activities (Phase 1)

2011 was the second and concluding year of Phase 1, and in it we concentrated our efforts on entrenching the support activity cycle (issue identification, analysis, countermeasure deliberation and deployment) that links with the Divisions and the Group company IRTs.

- Drew up a list of check points to be re-verified in FY 2010
- Expanded HIRT OPEN Meeting (Technical Meeting)

(2) Disseminating Information on Vulnerability in Control System Products

We elected to deal with vulnerability in control system products on a monthly basis, because the number of vulnerabilities reported for such products had increased, and in order to routinely determine the trends in the vulnerabilities reported.

(3) Strengthening of Partnership with the CSIRT Community

We carried out information transmission in cooperation with the Nippon CSIRT Association's Incident Information Utilization Framework Working Group.

- Web Malware "mstmp" exploiting Mash-up

(4) Lectures

- July 2011: "Defining Security Requirements for Web Application Development" by Hiroshi Tokumaru, HASH Consulting Corporation
- September 2011: "Difficulties and Actual Practice in the Information Leakage Countermeasure Field - Tracking Down Malicious Data Diffusion Crimes" by Toshifumi Tokuda, IBM Japan
- December 2011: "Circumstances Surrounding Android (Trends in the Android Malware)" by Norihiko Maeda, Kaspersky Labs Japan

(5) Other activities

- Cooperated with the standardization activities for ITU-T's Cybersecurity Information Exchange Framework ("CYBEX")

4.2 The Year 2010

(1) Start of Improvement of Hitachi Group CSIRT Activities (Phase 1)

We began activities for Phase 1 of the improvement of Hitachi Group CSIRT activities, with the goal of "installing incident operation into the whole Hitachi Group". In 2010, the initial year of Phase 1, we concentrated our efforts on regular holding of liaison meetings (operational and technical meeting) for the vulnerability-related information handling officers and IRT liaison staff.

- Operational Meetin (once/term): for the vulnerability-related information handling officers and IRT liaison staff, held with the objectives of sharing and passing on the operational know-how necessary for IRT activities
- Technical Meeting (2-4 times/term): for designers, system engineers and persons able to assist with disseminating technological expertise, held in order to disseminate the technological expertise necessary for building security into products and services.

(2) Strengthening of Partnership with the CSIRT Community

In December 2012, we provided support for the holding of the Nippon CSIRT Association's International Partnership Workshop Also, in cooperation with the Nippon CSIRT Association's Incident Information Utilization Framework Working Group, we carried out information disseminated [18]:

- A website with the information about Gumblar countermeasure
- Information on the SSL attack by the Botnet PushDo
- Information about Stuxnet

(3) Other activity

- In July 2010, we provided backing for the organizing of an "Academy CERT Meeting" in collaboration with JPCERT/CC, to help Indonesia's academic CSIRT activities [19].
- "Survey on Malware Circulating Within the P2P File Exchange Environment" [20]
  Since 2007, many Antinny-type known malwares that are liable to cause information leakage have been swarming on the "Winny" P2P file-sharing environment (Figure 19).

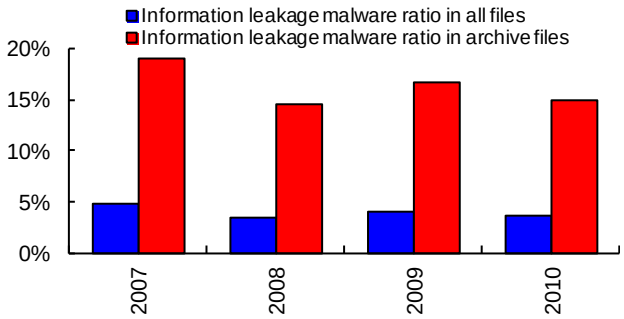


Figure 19: Change in Malware Circulating in Winny That Causes Information Leakage.

4.3 The Year 2009

(1) Start of Product/Service Security Feedback

To give feedback to the product development processes about the know-how we learned from the experience of vulnerability fighting and incident response, we started to provide support for each process (Figure 20).

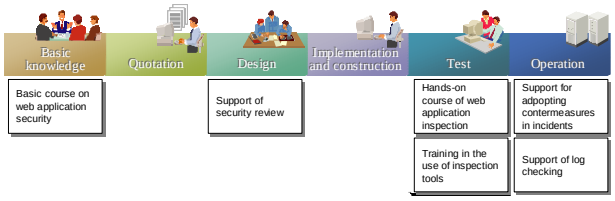


Figure 20: Systematizing HIRT support activities (Web application security).

(2) Providing Security Engineer Training

As part of the security engineer training program utilizing the CSIRT activities, we accepted a trainee and trained him for six months with the focus on web system security.

(3) Lectures

- July 2009: "Web Application Security" by Hiromitsu Takagi, National Institute of Advanced Industrial Science and Technology (AIST)
- July 2009: "NTT-CERT Activity" by, Takehiko Yoshida, NTT-CERT

(4) Other Activities

- "Survey on Malware Circulating within the P2P File Exchange Environment" [21]
- February 2009: Gave an web application development exercise for NTT Group at a workshop organized by NTT-CERT
- In cooperation with the Incident Information Utilization Framework Working Group of Nippon CSIRT Association, information dissemination using cNotes (Current Status Notes) [22] which tries to visualize the observational data.

4.4 The Year 2008

(1) Supporting countermeasures against DNS cache poisoning vulnerability

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. 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" [23] issued from the IPA in January, 2009, was created.

(2) Holding JWS2008

March 25-28, 2008, we held the FIRST Technical Colloquium, a FIRST technical meeting, and Joint Workshop on Security 2008, Tokyo (JWS2008), a domestic CSIRT technical workshop, with a team of domestic FIRST members [24].

(3) Participation in the domestic COMCHECK Drill 2008

With a view to ensuring that in-house information security departments of various organizations could communicate with each other, we participated in a domestic COMCHECK Drill (Drill name: SHIWASU, was held by the Nippon CSIRT Association on December 4, 2008).

(4) Award with the Commerce and Information Policy Bureau Chief Prize, Ministry of Economy, Trade and Industry (Information Security Promotion Section)

In the 2008 Information Technology Promotion Monthly Period memorial ceremony held by Information Technology Promotion Conference (Ministry of Economy, Trade and Industry, Cabinet Office, Ministry of Internal Affairs and Communications, Ministry of Finance Japan, Ministry of Education, Culture, Sports, Science and Technology, Ministry of Land, Infrastructure and Transport) on October 1, 2008. We were awarded with the "Commerce and Information Policy Bureau Chief Prize, Ministry of Economy, Trade and Industry (Information Security Promotion Section)" [25].

(5) Lectures

- April 2008: "Management of High Reliability Organizations" by Aki Nakanishi, the Faculty of Business Administration, Meiji University.

(6) Other Activity

In order to partially reveal the actual circumstances of targeted attack as a part of efforts to develop a new inter-organization collaboration, we provided related organizations with a malware-attached e-mail, which faked itself as Call for Papers (CFP) for the symposium held by the Computer Security Symposium 2008 of Information Processing Societies Japan as a sample.

4.5 The Year 2007

(1) Starting Hands-on Security Training at HIRT OPEN Meetings

In 2007, to promote the practical use of the guideline "Web Application Security Guideline", we provided a hands-on, exercise-based HIRT OPEN Meeting twice in March and June for the web application developer.

(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 [26]. As of December 2012, 31 teams have been joined (Figure 21).

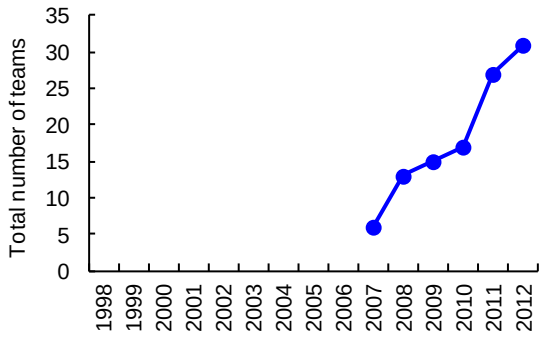


Figure 21: Change in Number of Nippon CSIRT Association Members.

(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 [27].

(4) Lectures

- July 2008: "Vulnerability Assessment through Static Analysis" by Yuji Ukai, Fourteenforty Research Institute, Inc.

4.6 The 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 security measures of web application 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.

(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) Lectures

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

(7) Other Activities

- Starting to sign a digital signature to technical documents (PDF files) issued from HIRT [28]

4.7 The 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 [29]. 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 December 2012, a total of 269 teams have joined this community. The following 23 Japanese teams have joined: CDI-CIRT (Cyber Defense Institute), CFC (Cyber Force Center of the National Police Agency's Info-Communications Bureau), DeNA CERT (DeNA), FJC-CERT (Fujitsu), HIRT (Hitachi), IIJ-SECT (IIJ), IPA-CERT (Information-technology Promotion Agency), JPCERT/CC , JSOC (LAC) , KDDI-SOC (KDDI) , KKCSIRT (Kakaku.com), MBSD-SIRT (Mitsui Bussan Secure Directions) , MIXIRT (Mixi) , MUFG-CERT (Mitsubishi UFJ Financial Group), NCSIRT (NRI Secure Technologies), NISC (National Information Security Center) , NTT-CERT (NTT) , NTTDATA-CERT (NTT Data) , Panasonic PSIRT (Panasonic) , Rakuten-CERT (Rakuten), RicohPSIRT (Ricoh), SBCSIRT (Softbank) and YIRD (Yahoo) (Figure 22).

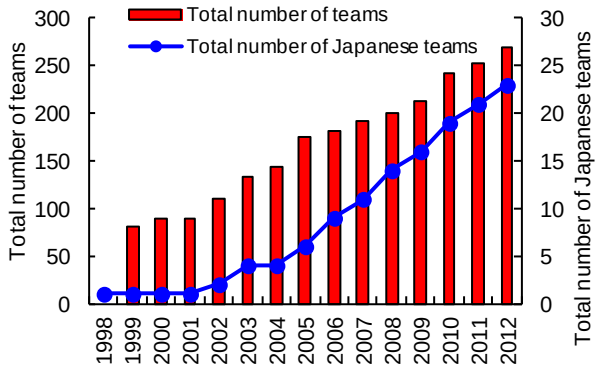


Figure 22: Changes in the number of members of FIRST.

(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 (Figure 23). 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/

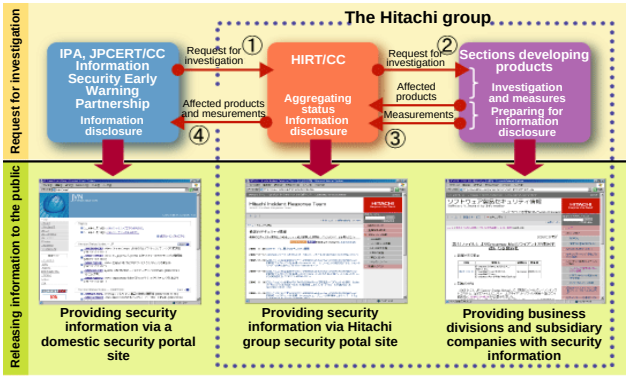


Figure 23: Providing security information on the Hitachi security information portal.

(3) Strengthening the Domestic Partnership for CSIRT Activities

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) to exchange opinions, and have established a contact network to be used, for example, when a website is found to have been tampered with.

4.8 The 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 [30][31].

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) [32].

(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) Lectures

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

4.9 The 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. 006489/H323 of January 2004 for security information on a Hitachi product was first published in NISCC Vulnerability Advisory after starting the activity [33].

(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 [34], we provided a point of contact, as shown in Table 11, that initiates actions when vulnerabilities or malicious actions in Hitachi products and Hitachi-related websites are pointed out.

4.10 The Year 2002

(1) Disseminating Vulnerability Information from CERT/CC throughout Hitachi

SNMP vulnerability [16] 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 [35]. VU#459371 of October 2002 for security information on Hitachi product was first published in the CERT/CC Vulnerability Notes Database after commencing this activity [36].

(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 (Figure 24) [37][38]. 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).

Table 11: 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

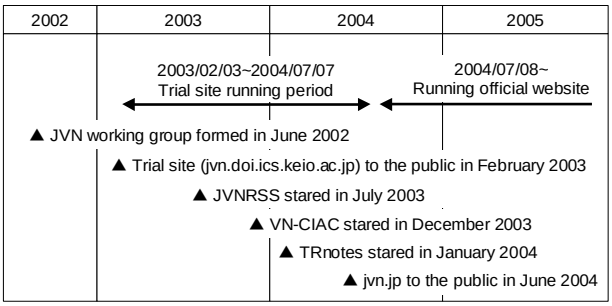


Figure 24: Building and running a JVN trial site.

4.11 The 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 25), 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.

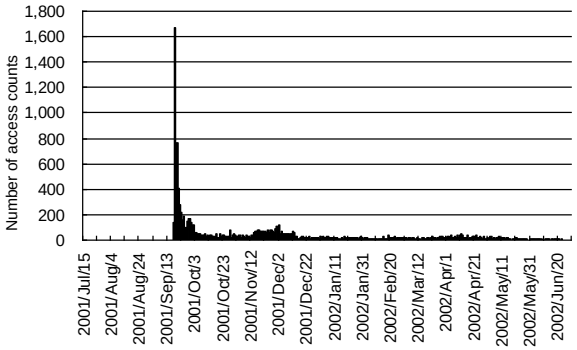


Figure 25: Changes in the number of Nimda log counts found during the observation period (for Nimda).

4.12 The 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" [39] for vulnerability. It provides the Severity Metric indicating the severity of vulnerability [40] Common Vulnerabilities and Exposures (CVE) classified information security vulnerabilities into "Vulnerabilities" and "Exposures" and focuses on the former [41]. 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 [42], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [43] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

4.13 The 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 (Figure 26).

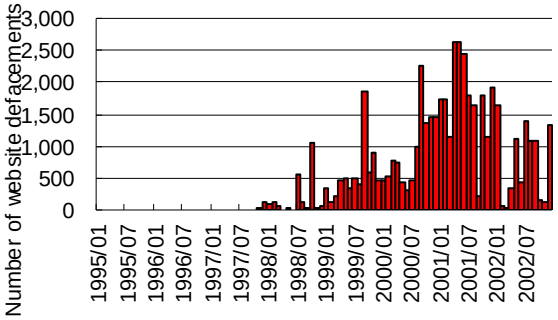


Figure 26: Changes in the number of websites defacements.

4.14 The 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) Lectures

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 [44] as a speaker as an instructor.

5 Conclusion

Damage from known threats is ongoing. Meanwhile, threats from new cyber attack activities have emerged and are giving rise to damage. Further, it has become evident that damage from cyber attack activities is to a considerable extent designed to act on other organizations or to be acted on by other organizations. Given such circumstances, it is essential to realize specialized and pragmatic collaboration among organizations by means of CSIRTs.

In line with changes in the incident occurrence situation, HIRT will be proceeding with activities to disseminate countermeasures early as part of its efforts to "catch any sign of future threats". We intend also to experiment with new forms of collaboration utilizing CSIRT, in such ways as promoting CSIRT activities tailored to particular industry types and other fields, and making contributions to the cultivation of academic human resources that will lead to the formation of the next-generation CSIRT community.

(May 14, 2013)

References

1) National Information Security Center: Forms to be Taken by Public-Private Collaboration Regarding Information Security Measures, http://www.nisc.go.jp/conference/suishin/ciso/dai4/pdf/1-1.pdf
2) Eric M. Hutchings et al.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains (ICIW2011)
3) Information-technology Promotion Agency, Japan: Cyber Information Sharing Initiative (J-CSIP) http://www.ipa.go.jp/security/J-CSIP/
4) National Police Agency: Updated Information On Cyber Intelligence During the First Half of FY2012 http://www.npa.go.jp/keibi/biki3/20120823kouhou.pdf
5) Trend Micro Incorporated: Report on Internet Threat, http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html
6) Conficker Work Group - ANY - Infection Tracking, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
7) NIST NVD (National Vulnerability Database), http://nvd.nist.gov/
8) Information-Technology Promotion Agency, Japan: Quarterly Reports, http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html
9) Symantec: "The Elderwood Project", http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf
10) EMC: "The VOHO Campaign: An In-Depth Analysis", http://www.emc.com/collateral/hardware/solution-overview/h11146-the-voho-campaign-so.pdf
11) CSIRT Workshop 2012, http://www.hitachi.co.jp/hirt/topics/20120229.html
12) Kyoto 2012 FIRST Technical Colloquium, http://www.first.org/events/colloquia/kyoto2012
13) FIRST Japan Teams, http://www.facebook.com/first.japan.teams
14) Feasibility study of scenario-based self-training material for incident responses, 24th FIRST Annual Conference(2012/6), http://www.first.org/conference/2012/program/index.html
15) ITpro Security, http://itpro.nikkeibp.co.jp/security/
16) 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
17) anti Malware engineering workshop, http://www.iwsec.org/mws/2012/
18) Nippon CSIRT Association: incident response, http://www.nca.gr.jp/2010/incidentresponse.html

19) SGU MIT Workshop Academy CERT Meeting (2010/7), http://idsirtii.or.id/academy-cert-meeting/
20) Malware Circulating in P2P File Exchange Software Environment (2011) (2011/9), http://www.hitachi.co.jp/hirt/publications/hirt-pub11003/index.html
21) 2009 Survey on information leakage via P2P File Exchange Software Environment (2009/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html
22) cNotes: Current Status Notes, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi
23) Information-Technology Promotion Agency, Japan: Countermeasures against DNS Cache Poisoning (2009/2), http://www.ipa.go.jp/security/vuln/DNS_security.html
24) Recording Site for Joint Workshop on Security 2008, Tokyo (2008/3), http://www.nca.gr.jp/jws2008/index.html
25) 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/archives/project/gekkan/2008/ceremony/prize02.html
26) CSIRT - Nippon CSIRT Association, http://www.nca.gr.jp/
27) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
28) GlobalSign Adobe Certified Document Services, http://jp.globalsign.com/solution/example/hitachi.html
29) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
30) 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
31) Information-technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline (2004/7), http://www.ipa.go.jp/security/ciadr/partnership_guide.html
32) JVN (Japan Vulnerability Notes), http://jvn.jp/
33) 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
34) Information-Technology Promotion Agency, Japan: Research Reports on Policy for Security Vulnerability Information Disclosure (2003/9), http://www.ipa.go.jp/security/awareness/vendor/vulnerability200309012.pdf
35) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
36) 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
37) Considerations on JPCERT/CC Vendor Status Notes DB: JVN, CSS2002 (2002/10), http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf
38) Development of JVN to Support Dissemination of Security Information (2005/5), http://www.hitachi.co.jp/rd/portal/story/jvn/index.html
39) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
40) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp
41) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/
42) ICAT, http://icat.nist.gov/(not available)
43) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
44) DEFCON, http://www.defcon.org/

[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, Telecom ISAC a steering committee member, and vice chief of the steering committee for the Nippon CSIRT Association.