Hitachi Incident Response Team
2014.05.26 11:04:14 +09'00'

HIRT: Annual Report 2013

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

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

1 Introduction

Since the VBS/Loveletter virus of the year 2000, cyber attacks have developed continually and the vulnerabilities they target have broadened out from operating systems to applications. Malicious programs too have evolved while varying their forms - malware-attached emails, network worms, bots and so forth. From around 2008, methods that take advantage of users' psychological and behavioral vulnerabilities to draw them into the vortex of a cyber attack activity have become common. Such methods include redirecting-type malware (typified by Gumblar) and infection via USB memory sticks.

Targeted attacks - typified by the APTs (Advanced Persistent Threats) that have been in the limelight since 2010 - are not solely attacks with the objective of stealing information. The Stuxnet malware that circulated in July 2010 was a malicious program that targeted nuclear power facilities and induced operational abnormalities in their control systems via SCADA (Supervisory Control And Data Acquisition) software.

As for online banking trojan, it progressively varies its forms of attack and continues to evolve while passing on its techniques in the form of toolkits (Figure 1).

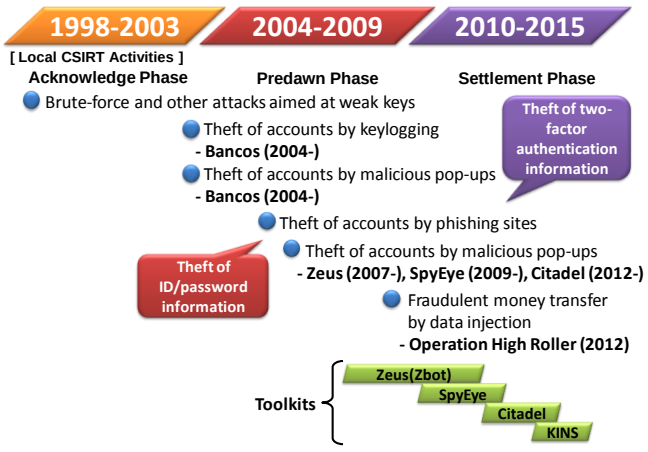


Figure 1: Activities of online banking trojan.

Social infrastructures, which have been constructed utilizing the internet on a base of information systems, control systems and so forth, are facing new threats and need to overcome them through vulnerability countermeasures and incident responses on a day-to-day basis. Alongside that, the role of CSIRTs is showing a broadening-out from information security countermeasures to cyber security measures that will protect social infrastructures. This development can be seen from the fact that organizations naming themselves Cyber Security Incident Response Team rather than Computer Security Incident Response Team are gradually increasing.

The specific role of HIRT (Hitachi Incident Response Team) as a CSIRT remains, as before, to lead the cybersecurity measure activities of the Hitachi Group, through vulnerability countermeasures - activities to eliminate vulnerabilities that could pose a threat for cyber security, and incident responses - activities to avert and resolve cyber attacks when they occur.

Further, 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 collaboration" and "collaborating with external communities on the technical aspects". We are not envisioning special requirements here. It is a matter of making use of experience in incident operation (the series of security measure activities 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 leads the way in vulnerability countermeasures for products and services and in incident responses for malware infection damage and information leakage, besides shouldering duties as the Hitachi Group's integrated CSIRT liaison organization.

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

2 Overview of activities in 2013

This section focuses on the threats and vulnerabilities, and HIRT's activities, in 2013.

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.

The features of 2013 in terms of incidents were that website compromised actions became steady occurrences

Copyright © Hitachi Incident Response Team(HIRT). 2013. All rights reserved.

and damage by malicious programs that target online banking became serious. Meanwhile, the following attack methods manifested: malware that assumes authenticated proxies in targeted attacks; password list attacks in which account information is archived and used for attempting unauthorized accesses at various sites to steal personal information, etc.; and amplification attacks (also known as reflector attacks) that use amplification of request/response messages.

- **Steady occurrence of website invasive actions**

Incidents of website alteration in Japan with the intention of infecting the sites with redirecting malware have been continuing since March 2013. Looking at the number of reported cases, one sees that these alterations are occurring in larger quantities than the Gumblar incidents that took place in 2009 (Figure 2). All kinds of files inside a website are targets for such alteration - HTML files, JavaScript (.js) files, PHP (.php) files, CSS (.css) files and so on. Also, most of the alteration cases have occurred in sites that run on cloud services or rental services. In particular, sites have been compromised because the vulnerabilities of their old-version CMSs (such as Wordpress, Movable Type, Joomla!, Drupal) or management tools (such as Parallels Plesk Panel) were exploited.

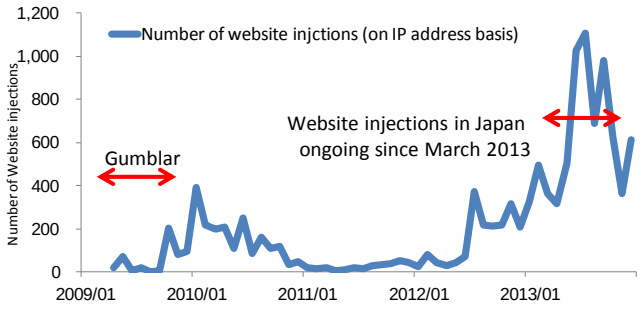


Figure 2: Number of reported cases of website injections. (Source: JPCERT/CC).

- **Damage by malicious programs that target online banking**

According to a National Police Agency Report, there were a total of 1,315 cases of fraudulent money transfer damage in Japan in 2013, affecting 32 banks and amounting to some 1.406 billion yen in total damage (Figure 3)[1]. A salient trick in fraudulent money transfers is to infect bank users' personal computers with malware that steals the ID and password they use for transactions. In roughly 50% of the cases, money was taken out from an ATM after being transferred using a traded account, and in roughly 20%, money was transferred overseas via a fund transfer service provider.

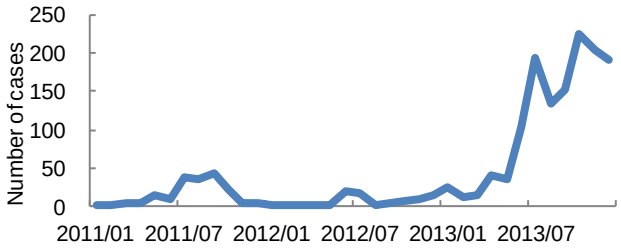


Figure 3: Monthly cases of fraudulent money transfer damage. (Source: National Police Agency)

- **Targeted attacks**

Remote Access Trojan / Remote Administration Tool known as RAT is used as programs for remotely controlling systems that have been penetrated in targeted attacks. Since about 2013, RATs with capabilities for getting past an authenticated proxy server and communicating with the outside world, by for example stealing proxy server authentication information, have been gradually spreading (Figure 4).

Also, Watering Hole Attacks have continued to occur, sometimes taking the form of zero-day attacks (Table 1). Watering Hole Attacks began to be reported around 2012; they are ambush-style attacks that stow tricks in a group of websites that people in a targeted organization are likely to visit, and develop this into a targeted attack.

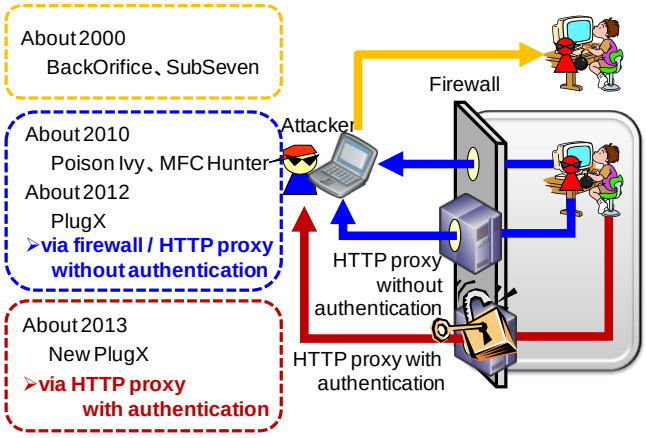


Figure 4: Development of Remote Access Trojan / Remote Administration Tool (RATs).

Table 1: Cases of Watering Hole Attack.

Time	Outline
May 2013	United States Department of Labor Internet Explorer vulnerability (CVE-2013-1347 (April 2013)) exploited
October 2013	Invasive action called "Operation DeputyDog" targeting Japan [2] Internet Explorer vulnerability (CVE-2013-3893 (September 2013)) exploited
November 2013	Invasive action called "Operation Ephemeral Hydra" [3] Internet Explorer vulnerability (CVE-2013-3918 (November 2013)) exploited

Copyright © HIRT. 2013. All rights reserved.

- **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. Although the number of reports of infection damage has been decreasing since 2009, about 1.2 million computers (on an IP address basis) remain infected with Conficker according to observations by the Conficker Work Group (Figure 5) [4].

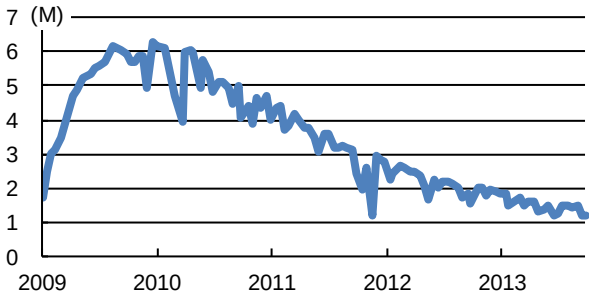


Figure 5: Number of Infection of ConfickerA+B (per day). (Source: Conficker Work Group)

- **Password List Attacks (List-Based Attacks)**

Since April 2013 numerous cases have occurred in Japan of account information (ID and password) lists, obtained by some means or other, being archived and unauthorized log-ins being attempted using such account information list archives. Users who use account information across multiple websites are highly likely to fall victims to this attack method. According to the IPA (Information Promotion Agency, Japan), the success rate for unauthorized log-ins is provisionally estimated at 0.15 to 1.35% from the cases that have occurred [5].

- **Reflector Attacks**

In 2013 there manifested the threat of DrDoS (Distributed Reflective Denial of Service) attacks, which exploit UDP services. DrDoS is an attack method whereby a packet is transmitted, from a spoofing IP address, to a service that offers a high request/response message amplification factor (a high value for response size / request size) and will serve as a springboard (Figure 6). DNS (open resolver) and NTP servers, which can be sent any inquiry over the internet, have been particularly exploited as such springboards for attacks. In March 2013, DrDoS attack peak traffic on the order of 300 Gbps was reported (Figure 7).

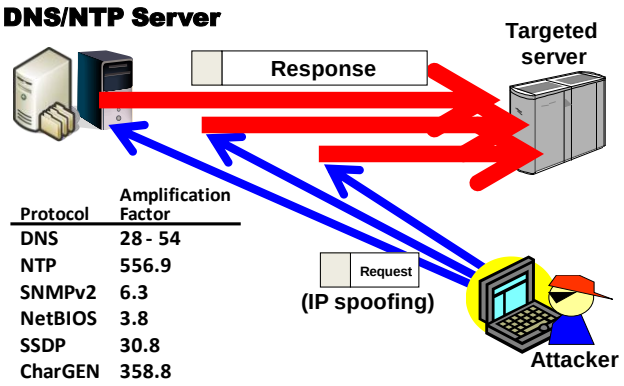


Figure 6: Reflector attack.

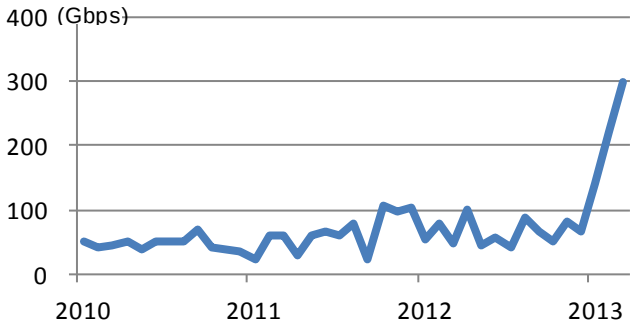


Figure 7: Trend in DrDoS attack peak traffic. (Source: Arbor Networks)

(2) Overview of Vulnerabilities

- **Overall Trend**

The total number of vulnerabilities entered in the NIST NVD (National Vulnerability Database) was 5,186 in 2013 [6]. About 20% (984) of the vulnerabilities were in web software application products (Figure 8). Breaking these down, cross-site scripting (XSS) and SQL injection account for about 80%, which is a continuing trend (Figure 9). Likewise, some 60% of the vulnerabilities in operational websites that were reported to the IPA are accounted for by cross-site scripting (XSS) and SQL injection, and this too is a continuing trend, with close to 600 a year of these vulnerabilities being reported (Figure 10) [7].

- **Control System Products**

The ICS-CERT (Industrial Control System-CERT) issued 10 alerts and 85 advisories concerning vulnerabilities (Figure 11). 23 of these were vulnerabilities that allowed denial-of-service attacks due to inadequate verification of input data (CWE-20), and another 15 related to vulnerabilities in products that implement the DNP3 (Distributed Network Protocol) that is used at electric power, water supply and similar facilities.

Copyright © HIRT. 2013. All rights reserved.

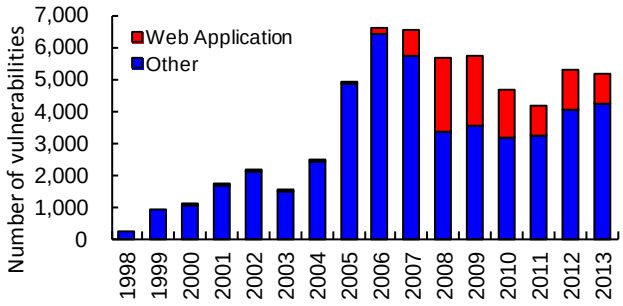


Figure 8: Number of Vulnerabilities Reported (Source: NIST NVD).

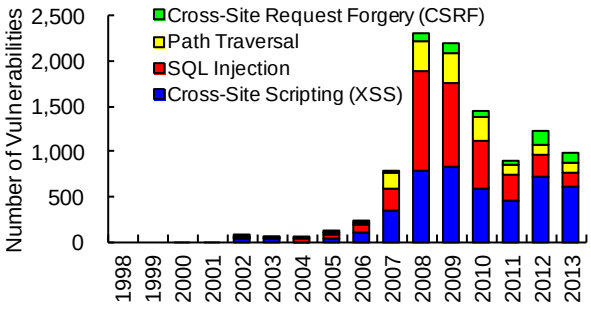


Figure 9: Changes in the number of vulnerabilities reported for software products of web application (Source: NIST NVD).

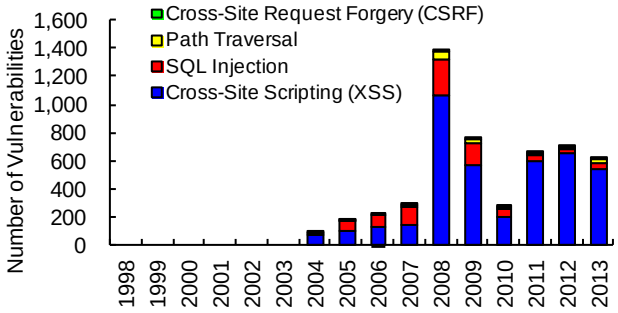


Figure 10: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC).

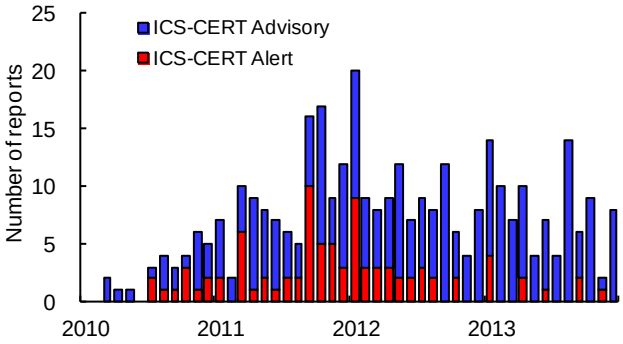


Figure 11: Change in the number of control system vulnerabilities reported (Source: ICS-CERT).

- **Broadband Routers**

Among the vulnerabilities present in broadband routers, two problems manifested as threats: (a) broadband routers mistakenly operating like a DNS server (open resolver) and responding to any inquiry from the internet, and (b) access to broadband router management screens from the internet being mistakenly allowed. Cases have been reported in which account information (PPPoE ID and password) stolen in such management screen accessing was subsequently used to mount password list attacks [8].

2.2 HIRT Activities

This subsection describes the HIRT activities in 2013.

(1) Improvement of Hitachi Group CSIRT activities (Phase 2)

In 2010, we started improvements of Hitachi Group CSIRT activities with the goal of "instilling incident operation into the whole Hitachi Group" (Figure 12). In 2013 - the fourth year of the improvements and the final year of Phase 2 - we moved ahead with entrenching loci for passing on techniques for cyber security countermeasures, in concert with the HIRT supporting staff (staff who work with the HIRT Center to actively promote IRT activities).

For the passing on of techniques, we divided the techniques into three categories: (1) **analysis (reverse engineering)** of the operation of the malware and so forth used in cyber attacks, (2) **investigation (forensics)** to determine the phenomena from the recorded traces, and (3) **assessment (penetration)** to clarify the vulnerabilities that are liable to become targets of cyber attacks. Regarding analysis, we tried out technique pass-on loci using level division into experiencing, fundamentals, application and specialization, while for investigation, we made use of a HIRT OPEN Meeting (Technical Meeting) (Table 2) [*a].

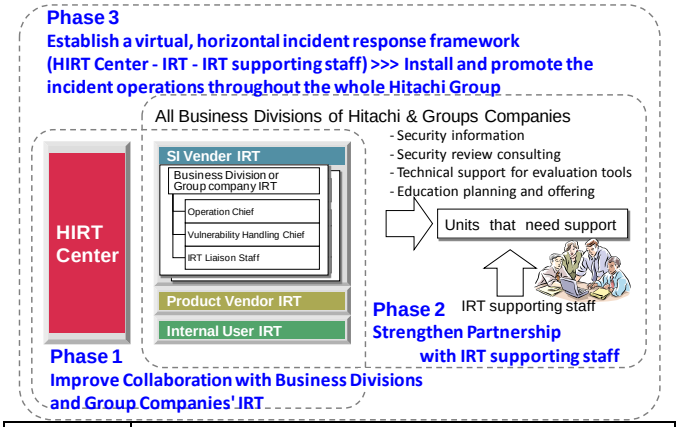
(2) Trial IRT activities for individual domains

- **Moving ahead with readiness activities at HIRT-FIS**

In order to put into practice the three-tiered cycle for incident response and readiness (Figure 13) that incorporates the perspectives of individual business domains, HIRT-FIS (Financial Industry Information Systems HIRT) engaged as main actor in internal/external readiness activities for the financial domain.

[*a] 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.

Copyright © HIRT. 2013. All rights reserved.



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 and 2) and entity collaboration model (Phase 3).

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

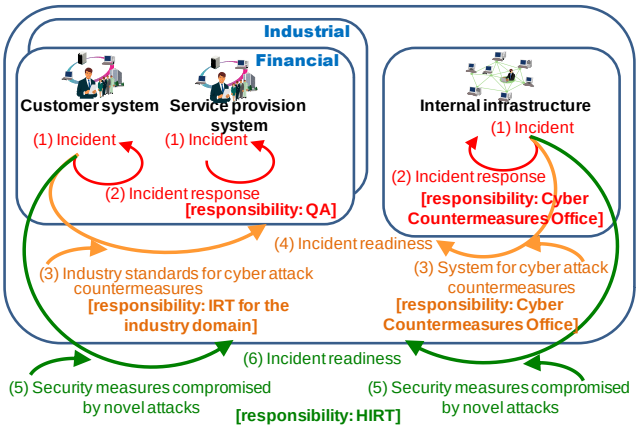


Figure 13: System view of "Three-tiered cycle for Incident Response and Readiness" approach.

In the HIRT-FIS internal activities, they proceeded with gathering and analyzing financial-related security information and issuing HIRT-FIS reports. In the external activities, they held view-exchange meetings with financial-related CSIRTs, and tried out weekly dissemination of HIRT-FIS Security Notes in order to put out feelers for collaboration with financial-related CSIRTs (Figure 14). The HIRT-FIS Security Notes are simple reports that cover subjects such as financial-related security incidents that have arisen in Japan or overseas, relevant regulations and so forth.

Table 2: HIRT OPEN Meeting (Technical meeting) in 2013.

Month	Outline
January	Advanced HIRT OPEN Meeting
February	Hands-on: Forensics for Windows (Basics meeting)
March	Cyber Attack Countermeasures from a Defense Perspective
	Hands-on: Forensics for Windows (Hands-on meeting)
June	[External instructor] Masaru Matsunami (Sony Digital Network Applications, Inc.) *Security for Android Apps and Security Activities for Software Development Worksites*
July	Group discussion on "operational security" for incident response
	Advanced HIRT OPEN Meeting
September	Seminar on technical countermeasures during vulnerability checking of external servers
	[External instructor] Lauri Korts-Pärn (Cyber Defense Institute, Inc.) *Control System Security: Suggestions for Proactive Approaches Toward the Generation When Information and Control Systems Fuse*
December	Advanced HIRT OPEN Meeting

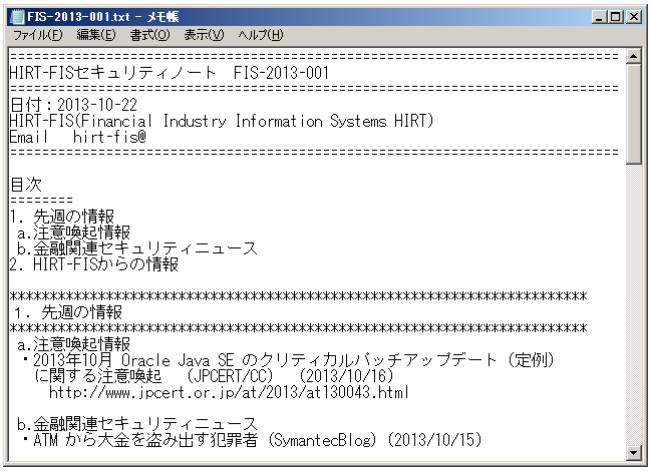


Figure 14: Example of the HIRT-FIS Security Notes that are disseminated weekly to financial-domain CSIRTs.

Copyright © HIRT. 2013. All rights reserved.

- **Vulnerability countermeasures for control systems**

We carried out three efforts using the approach of extending into the field of control systems the empirical experience from the HIRT activities implemented to date.

✓ Utilization of HIRT security information
We gathered information relating to latest trends, product vulnerabilities, incidents, etc., in control systems.

✓ Establishment of framework with HIRT as basic point of contact for external organizations
We established a framework for vulnerability handling and incident handling (Figure 15).

✓ Proceeding with vulnerability countermeasures that look toward dissemination
We approached vulnerability countermeasures from the three perspectives of specifications, codes and settings, and in addition we began deliberations on creating precedents in control devices and systems.

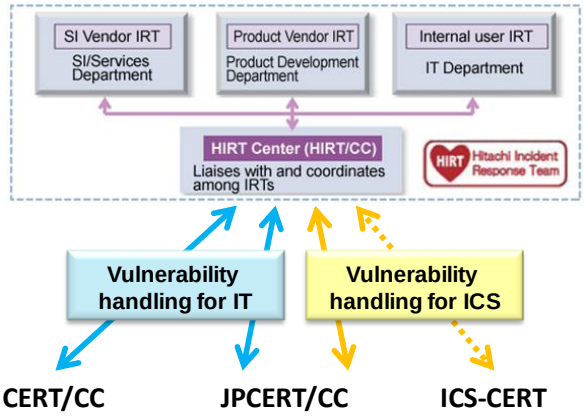


Figure 15: Framework for vulnerability handling.

(3) Strengthening of Partnership with the CSIRT Community

As concrete activities for strengthening our partnership with the CSIRT community, we continued with the gatherings with NTT-CERT [9] that we have been holding periodically since 2006, at which we exchanged information for improving CSIRT activities. Also, we carried out information dissemination in cooperation with the Nippon CSIRT Association's Incident Information Utilization Framework Working Group [16].

- Regarding the domestic web page alteration incidents ongoing since March 2013

(4) Winning of (ISC)^2 Asia-Pacific ISLA 2013

We won the 2013 Senior Information Security Professional Award for ISLA (Information Security Leadership Achievements) from (ISC)^2, which runs the CISSP information security certification and is highly appraised for its contributions to the vulnerability countermeasure activities pertaining to the JVN (Japan Vulnerability Notes), in which HIRT is involved [10].

(5) Other Activity

- Participation in MWS (anti Malware engineering workshop) 2013.
We took part in this workshop with the aim of supporting research activities for malware countermeasures and contributing, through such support, to the formation of the next-generation CSIRT community.
- Contributed an article on vulnerability countermeasures titled "*Vulnerability Information to Keep in Mind*", to the ITpro CSIRT Forum held by Nikkei Business Publications, Inc. [11].

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 16 and Table 4). 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 3) 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 [12] 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.

Copyright © HIRT. 2013. All rights reserved.

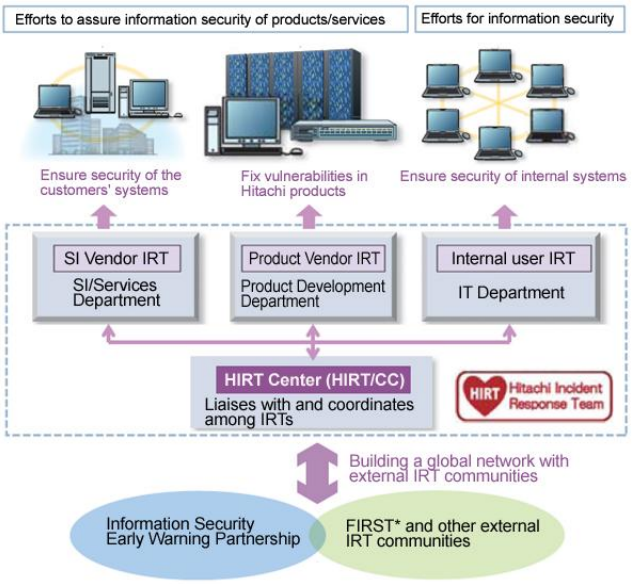


Figure 16: Four IRTs as an organizational model.

Table 3: 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) <Establishment>	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 -) <Establishment>	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 -) <Establishment>	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.
4th phase (October 2004) <Establishment>	We established the HIRT/CC.
1st phase (2010-2011) <Improvement>	Improvements of Hitachi group CSIRT activities **Goal: instilling incident operation into the whole Hitachi Group**
2nd phase (2012-2013) <Improvement>	

Table 4: 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.

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 17).

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.

Copyright © HIRT. 2013. All rights reserved.

3.3 Main Activities of HIRT Center

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

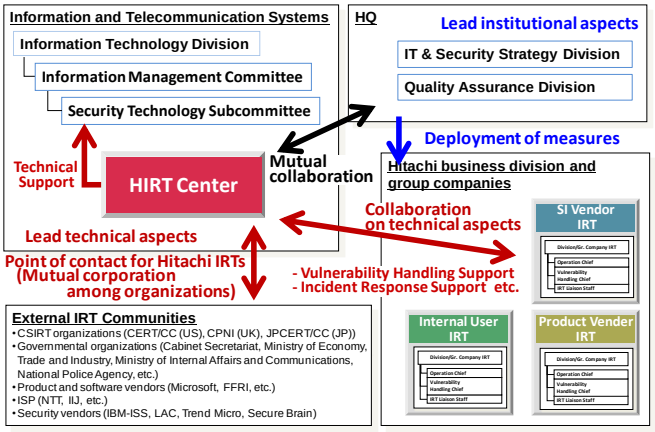


Figure 17: Position of HIRT Center.

Table 5: (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	- Strengthening of collaboration with IRT contact points of business divisions and group companies (Phases 1 and 2 - Passing on of techniques for the incident operation - Promoting the publication of security information from external websites using the Security Information Integration Site
Enhancing security technology for products/services	-- Establishment of processes for building-in of security (approach from the three perspectives of specifications, codes and configurations, and in addition move ahead with creating precedents in control devices and systems)
Developing a framework for research activities	- Developing a framework for joint research with the Yokohama Research Laboratory

Table 6: (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) [*b]
Developing a framework for research activities	- Establish a joint research between Meiji 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) [13]

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 7 and Figure 18). 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.

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 19).

[*b]Under ISO SC27/WG3, work began in 2007 to develop a "Vulnerability Disclosure" international standard (29147), and in 2010 to develop a "Vulnerability Response Procedure" international standard (30111). These international standards were completed in February 2014 and November 2013 respectively. Work to develop a "Cyber Security Information Exchange Framework (X.cybex)" international standard covering CVE (Common Vulnerability and Exposures), CVSS (Common Vulnerability Scoring System) and so forth began in 2009 under ITU-T SG17 Q.4.

Copyright © HIRT. 2013. All rights reserved.

Table 7: 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 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.

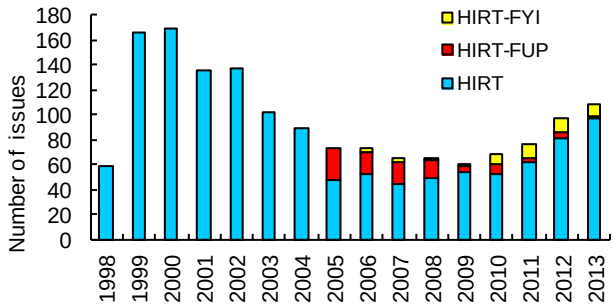


Figure 18: Number of issues of security information by ID number.

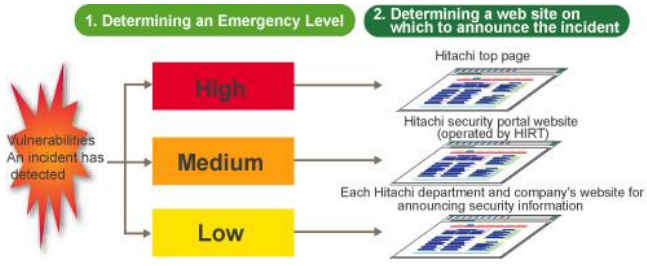


Figure 19: Conceptual view of issuing information based on "Emergency Level" x "Website Level".

4 Activity Summary from 1998 to 2012

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

4.1 The Year 2012

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

2012 was the third year of the improvements and in it we started Phase 2, which is to strengthen collaboration inside the Hitachi Group through the HIRT supporting staff.

- Disseminating Countermeasure Information through HIRT OPEN Meetings
- Start of Advanced HIRT OPEN Meetings

(2) Trial IRT activities for individual domains

We started trial IRT activities for individual domains, in order to take the approach of the three-tiered cycle for incident response and readiness that incorporates the perspectives of individual business domains (Figure 13).

Also, as an advanced endeavor in the financial domain, we set up HIRT-FIS inside our financial section on October 1, 2012 (Figure 20).

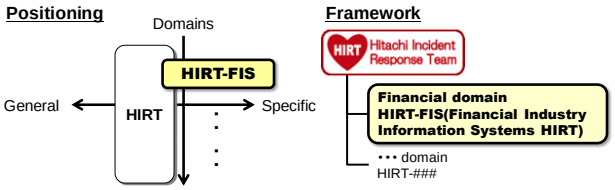


Figure 20: Positioning and framework of IRT activities for individual industry domains

(3) Strengthening of Partnership with the CSIRT community

- On February 29, 2012 we held the CSIRT Workshop 2012 as an opportunity for exchange of opinions on corporate CSIRT, targeting corporate staff interested in CSIRT activities [14].
- Together with the FIRST member teams in Japan, we held the FIRST Technical Colloquium 2012 Kyoto at the Kyoto International Community House from November 13 to 15, 2012 [15].
- 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.

(4) Lectures

- March 2012: "Framework for Promoting Security Measures in Organizations" by Nobuo Miwa, S&J Consulting
- August 2012: "Elements and Implementation of Database Security" by Haruto Kitano, Oracle Corporation Japan

Copyright © HIRT. 2013. All rights reserved.

- September 2012: "Trends in Cyber Attacks and the Cutting Edge of Cyber Security Research" by Daisuke Inoue, National Institute of Information and Communications Technology
- November 2012: "A Look Back Over Remote Control Incidents, the Firstserver Problem and the Leap-Second Problem" by Tetsutaro Uehara, The Research Institute of Information Security (NPO)

4.2 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")

4.3 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 entrenching the liaison meetings (operational and technical meetings) for the vulnerability-related information handling officers and IRT liaison staff.

- Operational Meeting (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 [16]:

- 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 [17].
- "Survey on Malware Circulating Within the P2P File Exchange Environment" [18]
- 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 21).

Copyright © HIRT. 2013. All rights reserved.

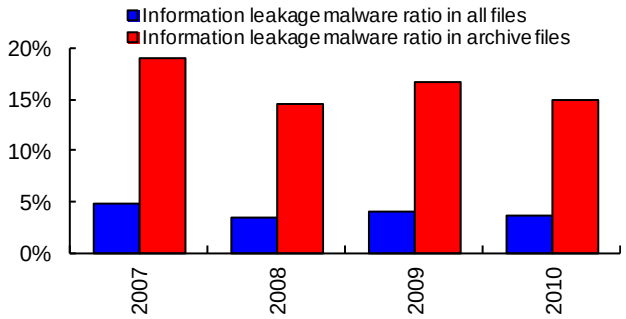


Figure 21: Change in Malware Circulating in Winny That Causes Information Leakage.

4.4 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 22).

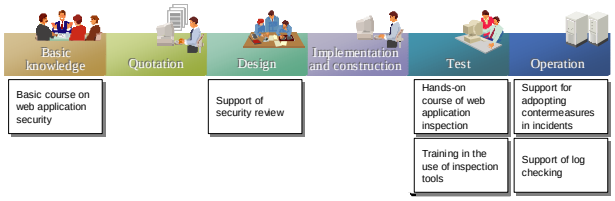


Figure 22: Systematizing HIRT support activities (Web application security).

(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" [19]
- 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) [20] which tries to visualize the observational data.

4.5 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" [21] 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 [22].

(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)" [23].

(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.

Copyright © HIRT. 2013. All rights reserved.

4.6 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 [24]. As of December 2012, 31 teams have been joined (Figure 23).

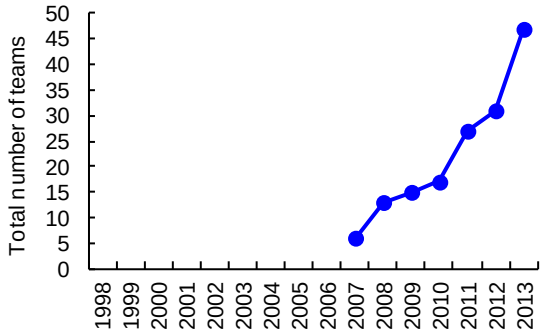


Figure 23: Change in Number of Nippon CSIRT Association Members.

(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 [25].

(4) Lectures

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

4.7 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 [26]

4.8 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 [27]. 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.

Copyright © HIRT. 2013. All rights reserved.

As of December 2013, a total of 289 teams have joined this community, including 23 Japanese teams (Figure 24) [*c].

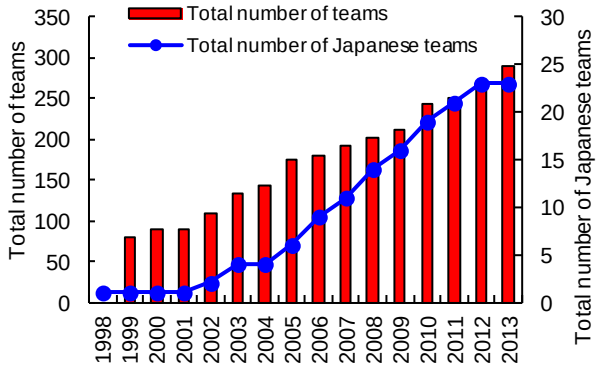


Figure 24: Changes in the number of members of FIRST.

(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 25). 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/

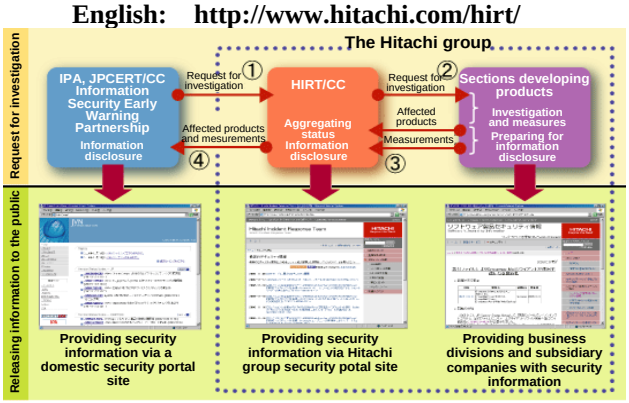


Figure 25: Providing security information on the Hitachi security information portal.

(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.

4.9 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 [28][29].

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) [30].

(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)

4.10 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 [31].

[*c] 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-CSIRT (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).

Copyright © HIRT. 2013. All rights reserved.

(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 [32], 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.

Table 8: Information on point of contact.

Name	"HIRT": Hitachi Incident Response Team.
Address	Kashimada 1-1-2, Saiwai, Kawasaki City, Kanagawa, 212-8567 Japan
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

4.11 The Year 2002

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

SNMP vulnerability [12] 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 [33]. 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 [34].

(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 26) [35][36].

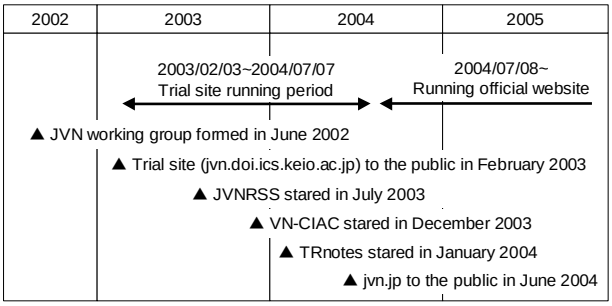


Figure 26: Building and running a JVN trial site.

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/).

4.12 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 27), 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.

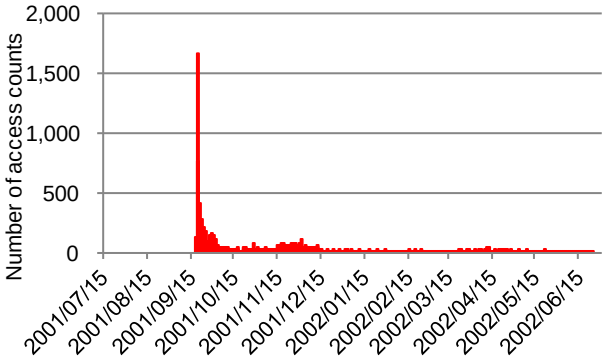


Figure 27: Changes in the number of Nimda log counts found during the observation period (for Nimda).

4.13 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" [37] for vulnerability. It provides the Severity Metric indicating the severity of vulnerability [38] Common Vulnerabilities and Exposures (CVE) classified information security vulnerabilities into "Vulnerabilities" and "Exposures" and focuses on the former [39]. 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

Copyright © HIRT. 2013. All rights reserved.

determine the severity of vulnerability, and classifies vulnerabilities into three levels in the ICAT Metabase [40], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [41] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

4.14 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 28).

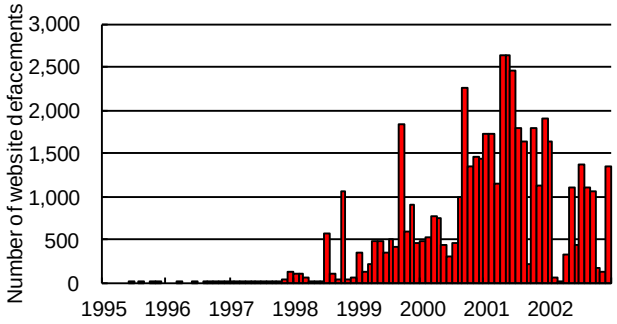


Figure 28: Changes in the number of websites defacements.

4.15 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 [42] as a speaker as an instructor.

5 Conclusion

Due to the borderless, global nature of the cyber world, the social infrastructure that has been constructed utilizing the internet is facing a novel kind of threat – the threat of cyber attack.

Given such circumstances, it is essential to realize CSIRT activities that give attention to national and regional cyber security measures. We believe that the role of CSIRTs is starting to broaden out from information security measures to cyber security measures that will protect social infrastructure.

Firmly apprehending the situational change from information security measures to cyber security measures, HIRT will be proceeding with activities to disseminate countermeasures early as part of its efforts to "catch any sign of future threats". We will also be contributing to the realization of safe and reassuring internet-based social infrastructure, in such ways as promoting CSIRT activities tailored to particular industry types and other fields, and fostering academic loci that will lead to the formation of the next-generation CSIRT community.

(March 21, 2014)

References

1) National Police Agency: Occurrence of Fraudulent Money Transfer Crimes Relating to Internet Banking in 2013, http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf
2) FireEye: Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets, http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html
3) FireEye: New IE Zero-Day Found in Watering Hole Attack, http://www.fireeye.com/blog/technical/2013/11/new-ie-zero-day-found-in-watering-hole-attack.html
4) Conficker Work Group - ANY - Infection Tracking, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
5) Information-Technology Promotion Agency, Japan: Alerts for August 2013, https://www.ipa.go.jp/security/txt/2013/08outline.html
6) NIST NVD (National Vulnerability Database), http://nvd.nist.gov/
7) Information-Technology Promotion Agency, Japan: Quarterly Reports, http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html

Copyright © HIRT. 2013. All rights reserved.

8) Telecom-ISAC Japan: Investigation of Vulnerable Broadband Router Situation and Countermeasures Therefor, https://www.telecom-isac.jp/news/news20130830.html
9) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/
10) (ISC)^2: Information Security Leadership Achievements (ISLA)プログラム, https://www.isc2.org/japan/isla.html
11) ITpro Security, http://itpro.nikkeibp.co.jp/security/
12) 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
13) anti Malware engineering workshop, http://www.iwsec.org/mws/2013/
14) CSIRT Workshop 2012, http://www.hitachi.co.jp/hirt/topics/20120229.html
15) Kyoto 2012 FIRST Technical Colloquium, http://www.first.org/events/colloquia/kyoto2012
16) Nippon CSIRT Association: incident response, http://www.nca.gr.jp/2010/incidentresponse.html
17) SGU MIT Workshop Academy CERT Meeting(2010/7), http://academy-cert-indonesia.blogspot.jp/2010/06/academy-cert-meeting.html
18) Malware Circulating in P2P File Exchange Software Environment (2011) (2011/9), http://www.hitachi.co.jp/hirt/publications/hirt-pub11003/index.html
19) 2009 Survey on information leakage via P2P File Exchange Software Environment (2009/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html
20) cNotes: Current Status Notes, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi
21) Information-Technology Promotion Agency, Japan: Countermeasures against DNS Cache Poisoning (2009/2), http://www.ipa.go.jp/security/vuln/DNS_security.html
22) Recording Site for Joint Workshop on Security 2008, Tokyo (2008/3), http://www.nca.gr.jp/jws2008/index.html
23) 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
24) CSIRT - Nippon CSIRT Association, http://www.nca.gr.jp/
25) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
26) GlobalSign Adobe Certified Document Services, http://jp.globalsign.com/solution/example/hitachi.html
27) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
28) 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
29) Information-technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline (2004/7), http://www.ipa.go.jp/security/ciadr/partnership_guide.html
30) JVN (Japan Vulnerability Notes), http://jvn.jp/
31) 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
32) 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
33) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
34) 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
35) Considerations on JPCERT/CC Vendor Status Notes DB: JVN, CSS2002 (2002/10), http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf
36) Development of JVN to Support Dissemination of Security Information (2005/5), http://www.hitachi.co.jp/hirt/csirt/jvn/index.html
37) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
38) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp
39) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/
40) ICAT, http://icat.nist.gov/(not available)
41) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
42) 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.

Copyright © HIRT. 2013. All rights reserved.