HIRT: Annual Report 2011

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

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

1 Introduction

The year 2011 saw the occurrence of a diversity of security incidents and developed into a transitional period in which cyber attack countermeasures were put under review (Table 1).

Table 1: Typical security incidents.

Time	Outline
March 2011	Circulation of virus emails, riding on the back of the earthquake
April 2011	Unauthorized accessing of Japanese enterprises' overseas websites, resulting in information leakage
August 2011	Unauthorized accessing of internet banking sites
September 2011	Targeted attacks on defense industry enterprises
November 2011	Denial-of-service attacks on clouds

Particularly salient were the incidents of April 2011, which forced a rigorous implementation of security measures that needed to be taken (especially vulnerability countermeasures), and the incidents of September 2011, which forced a fresh consideration of introducing of security measures (especially Egress countermeasures) grounded in information security.

Alongside of this, attention in the area of security measures in Japan in 2011 was focused on "Egress countermeasures" that will achieve multi-layered defense of organization-internal systems. Whereas the emphasis in security measures hitherto had been placed on "Ingress countermeasures" that protect against intrusion, the emphasis with multi-layered defense that incorporates "Egress countermeasures" is on promoting countermeasures from three perspectives:

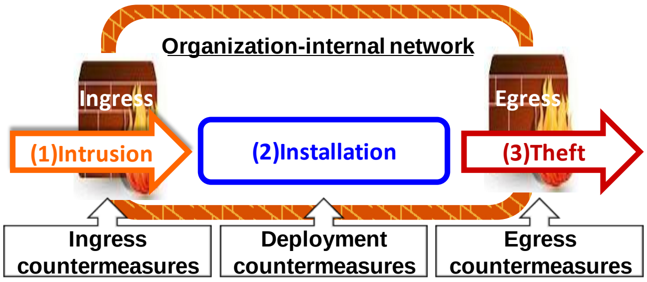


Figure 1: Multi-layered defense of an organization-internal system.

- Ingress countermeasures - strengthening intrusion prevention;
- Deployment countermeasures - preventing the spread of an invasive action in an organization-internal network, so as to guard against intrusion; and
- Egress countermeasures - preventing progression of invasive action, or leakage of information, and so forth etc., via back door communication, so as to guard against intrusion.

We believe that in the times ahead, such changes in countermeasures will have no small impact on inter-organizational collaboration - especially information exchange - among CSIRTs (Computer Security Incident Readiness/Response Teams).

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 adjustments" and "collaborating with external communities on the technical aspects". We are not envisioning special requirements here. The role of CSIRTs is to make use of their experience in incident operations (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 "implement measures at an early stage in an effort to catch any sign of future threats".

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 in the field of security. This report will present an overview of the vulnerabilities and threats, and HIRT's activities, in 2011.

2 Overview of activities in 2011

This section focuses on the threats and vulnerabilities, and HIRT's activities, in 2011.

2.1 Overview of Threats and Vulnerabilities

(1) Overview of Threats

In Japan there occurred a varied slew of security incidents, including targeted attacks and website invasive actions. Of those, the known threats like USB memory type malware (e.g. Conficker) have continued to cause damage.

A feature of 2011 was that security incidents relating to digital certification, which could be termed the basis of the digital society, became steady occurrences. These were incidents such as fraudulent issuance of digital certificates by means of invasive activities (March and August 2011) and use of stolen digital certificates in malware (November 2011).

- **Targeted attacks**

Figure 2 shows a scenario for one of the targeted attacks reported in 2011 that had stealing information as objective. The distinctive features of this attack include the targeted email that uses social engineering (to be discussed later); system intrusion that uses a hashed Windows password, called a "pass-the-hash" attack; and remote control of an infected PC by means of Poison Ivy or some other RAT[*a] tool.

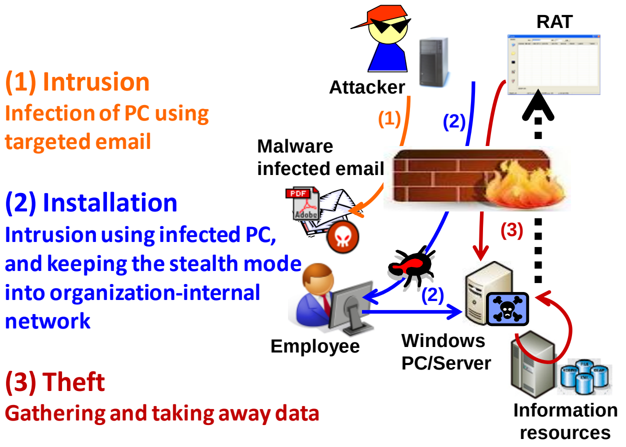
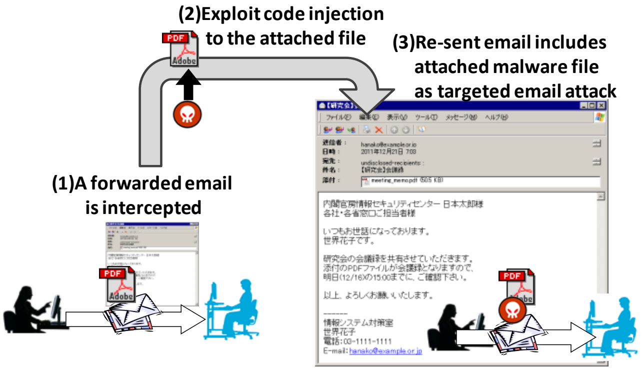

(1) Intrusion
Infection of PC using targeted email
(2) Installation
Intrusion using infected PC, and keeping the stealth mode into organization-internal network
(3) Theft
Gathering and taking away data
Attacker
RAT
(1)
(2)
Malware infected email
(3)
(2)
Employee
Windows PC/Server
Information resources
PDF
Adobe

Figure 2: Example of targeted attack scenario.

A particularly sophisticated method has been reported - besides the simple one of disguised icon and file name - for targeted email that uses social engineering. Namely, a forwarded email is stolen and then sent on again with exploit code injected in its attached file (Figure 3).


(2)Exploit code injection to the attached file
(3)Re-sent email includes attached malware file as targeted email attack
(1)A forwarded email is intercepted
PDF
Adobe
【研究会】
ファイル(F) 編集(E) 表示(V) ツール(T) メッセージ(M) ヘルプ(H)

送信者： hanako@example.or.jp
日時： 2011年12月21日 7:03
宛先： undisclosed-recipients：
件名： 【研究会】会議録
添付： meeting_memo.pdf (50.5 KB)

内閣官房情報セキュリティセンター 日本太郎様
各社・各省窓口ご担当者様

いつもお世話になっております。
世界花子です。

研究会の会議録を共有させていただきます。
添付のPDFファイルが会議録となりますので、
明日(12/16)の15:00までに、ご確認下さい。

以上、よろしくお願いいたします。

情報システム対策室
世界花子
電話：03-1111-1111
E-mail: hanako@example.or.jp

Figure 3: Social engineering attack - using a genuine item -.

- **Collateral issue observed in website invasive incidents**

A feature of the website invasive incidents reported in 2011 was that the information acquired was made public on the website by the attacker (Table 2). A collateral issue of such incidents is that the information so published may be utilized in targeted attacks or the like described earlier.

Table 2: Cases of leaked information being made public on websites.

Time	Outline
July 2011	Booz Allen Hamilton On the order of 90,000 email addresses and passwords
November 2011	OhMedia On the order of 60,000 email addresses and passwords
December 2011	China Software Developer Network (CSDN) On the order of 6 million email addresses and passwords
	Strategic Forecasting Inc. (Stratfor) On the order of 860,000 items of customer information and 75,000 of credit card information

- **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 4) [1]. However, according to the report of the Conficker Work Group, the number of computers infected with Conficker is about 3 million on the IP address base (Figure 5) [2].

[*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.

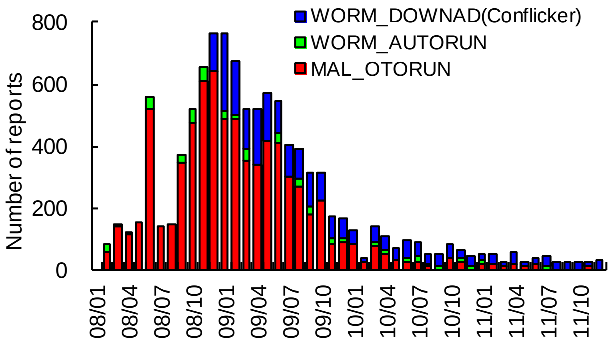


Figure 4: Number of Infection of USB Malware (per month).

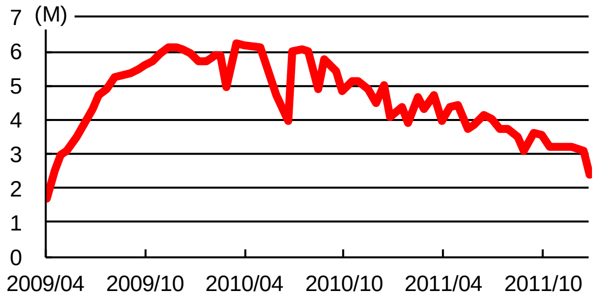


Figure 5: Number of Infection of ConfickerA+B (per day).

(2) Overview of Vulnerabilities

● Overall Trend

The total number of vulnerabilities entered in the NIST NVD (National Vulnerability Database) was 4,151 in 2012 [3]. About 20% (902) of the vulnerabilities were in web software application products (Figure 6). Breaking these down, cross-site scripting (XSS) and SQL injection account for about 80%, which is a continuing trend (Figure 7). Likewise, some 60% of the vulnerabilities in operational websites that were reported to the IPA (Information Promotion Agency, Japan) 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 8) [4].

● Control System Products

The ICS-CERT (Industrial Control System-CERT) has issued 37 alerts and 64 advisories concerning vulnerabilities (Figure 9). 12 of the advisories (accounting for 19%) pointed out vulnerabilities in the ActiveX control that is present in control system products.

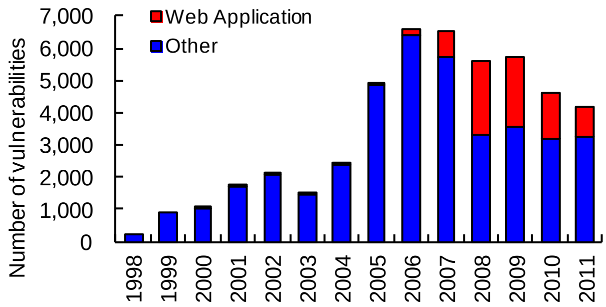


Figure 6: Number of Vulnerabilities Reported (Source: NIST NVD).

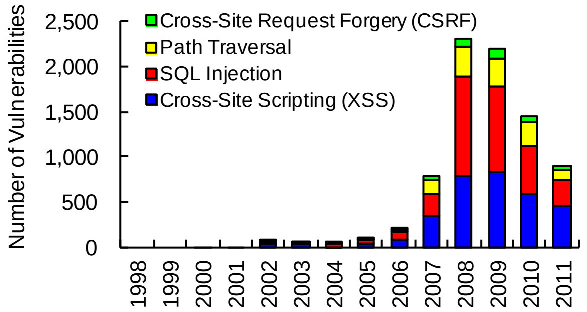


Figure 7: Changes in the number of vulnerabilities reported for software products of web application (Source: NIST NVD).

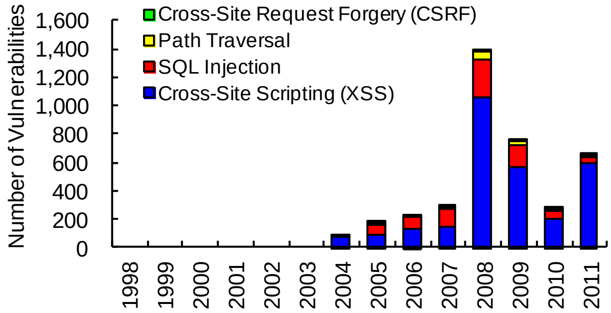


Figure 8: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC).

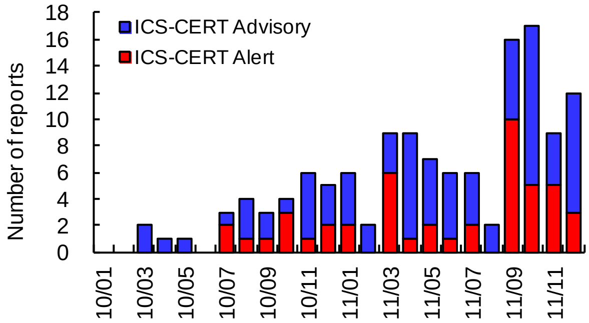


Figure 9: Change in the number of control system vulnerabilities reported (Source: ICS-CERT).

2.2 HIRT Activities

This subsection describes the HIRT activities in 2011.

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

In 2010, we started improvements of Hitachi Group CSIRT activities with the goal of "instilling incident operation into the whole Hitachi Group" (Figure 11).

2011 was the second and concluding year of Phase 1, and in it we concentrated our efforts on entrenching a support activity cycle (issue identification, analysis, countermeasure deliberation and dissemination) that links with the business divisions and the Group company IRTs (Figure 10).

- **Drawing-up of Must-reconfirm Check Points for FY 2010**

In entrenching the cycle, we narrowed down to a few typical Check Points the issues that had been brought to light through the security reviews and incident response support, and utilized them for countermeasure dissemination.

- **Expansion of technology-themed HIRT OPEN Meetings**

As a part of countermeasure dissemination, we effected an enhancement of the "technical meetings", mainly through workshops providing a Guide to Drawing Up Basic Security Specifications that is intended to encourage utilization of existing documents, and lectures by external instructors with a view to objectively rethinking efforts regarding security measures (Table 3) [*b].

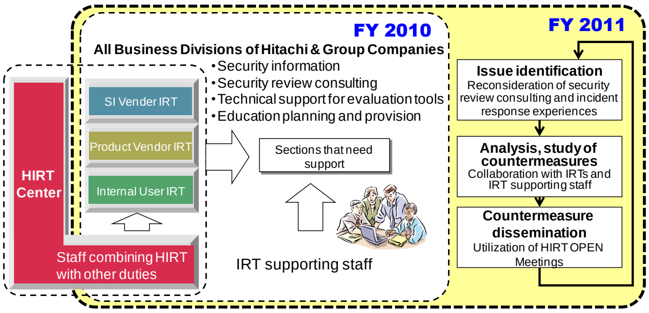
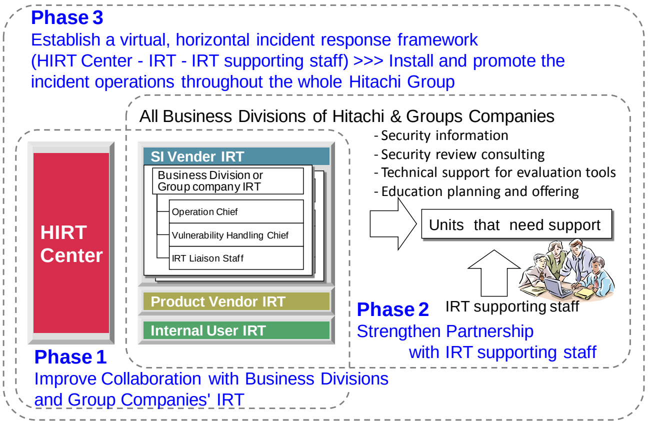

FY 2010
FY 2011
All Business Divisions of Hitachi & Group Companies
•Security information
•Security review consulting
•Technical support for evaluation tools
•Education planning and provision
HIRT Center
SI Vender IRT
Product Vendor IRT
Internal User IRT
Staff combining HIRT with other duties
Sections that need support
IRT supporting staff
Issue identification
Reconsideration of security review consulting and incident response experiences
Analysis, study of countermeasures
Collaboration with IRTs and IRT supporting staff
Countermeasure dissemination
Utilization of HIRT OPEN Meetings

Figure 10: Phase 1 activities.


Phase 3
Establish a virtual, horizontal incident response framework
(HIRT Center - IRT - IRT supporting staff) >>> Install and promote the incident operations throughout the whole Hitachi Group
All Business Divisions of Hitachi & Groups Companies
- Security information
- Security review consulting
- Technical support for evaluation tools
- Education planning and offering
HIRT Center
SI Vender IRT
Business Division or Group company IRT
Operation Chief
Vulnerability Handling Chief
IRT Liaison Staff
Product Vendor IRT
Internal User IRT
Units that need support
IRT supporting staff
Phase 2
Strengthen Partnership with IRT supporting staff
Phase 1
Improve Collaboration with Business Divisions and Group Companies' IRT

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 11: Scenario on a Virtual, Horizontal Incident Response System.

(2) Publishing of Information on Vulnerability in Control System Products

The ICS-CERT's alert and advisory issuance activities are now in their second year, and reports of vulnerabilities in control system products have increased. Accordingly, in order to keep regular track of the trends in the vulnerabilities reported, in September 2011 we began dealing with control system product vulnerabilities on a monthly basis in our company-internal information transmission activities. This has resulted in a slight increase in the number of HIRT security information items issued (Figure 14).

[*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 3: HIRT OPEN Meeting (Technical meeting) in 2011.

Month	Outline
April	Hands-on: Forensics of USB virus infection
June	Guide to Drawing Up Basic Security Specifications - introductory session - Overview of the guidelines and how to use them
July	Guide to Drawing Up Basic Security Specifications - hands-on session - Group discussion using Worksheet 1
	Guide to Drawing Up Basic Security Specifications - application session [External instructor] Mr. Hiroshi Tokumaru (HASH Consulting Corporation) *Defining Security Requirements for Web Application Development*
September	[External instructor] Mr. Toshifumi Tokuda (IBM Japan) *Difficulties and Actual Practice in the Information Leakage Countermeasure Field - Tracking Down Malicious Data Diffusion Crimes*
November	How to Interpret and Effectively Utilize Vulnerability Information
December	[External instructor] Mr. Norihiko Maeda (Kaspersky Labs Japan) *Circumstances Surrounding Android (Trends in the Android Malware)*

(3) Strengthening of Partnership with the CSIRT Community

A specific instance of the strengthening of this partnership is the periodic gatherings with NTT-CERT [5] that we have held continuously since 2006 to exchange information for improving the CSIRT activities themselves. Also, we carried out information transmission in cooperation with the Nippon CSIRT Association's Incident Information Utilization Framework Working Group [6].

- Regarding attack mstmp via websites using web service linkage

(4) Cooperation with the Standardization Activities for ITU-T's Cybersecurity Information Exchange Framework ("CYBEX")

ITU-T, which is the Standardization Sector of the International Telecommunication Union (ITU), is proceeding with the CYBEX series of standardizations of technical specifications for telecommunications - formats, numbering schemes and so forth pertaining to vulnerability countermeasure information and incident responses. The spread of these technical specifications will promote mechanical processing of vulnerability countermeasures and incident responses. Meanwhile in Japan, efforts have been underway since 2008 to put in place, by means of MyJVN [7], a mechanical processing infrastructure for vulnerability countermeasures that use SCAP (Security Content Automation Protocol), a component of the CYBEX series. To assist with putting the mechanical processing infrastructure for vulnerability countermeasures in place, we have moved ahead with publishing the U.S. FDCC (Federal Desktop Core Configuration) efforts and the JVN and MyJVN efforts in Japan, as use cases in the Appendix to X.cybex (X.1500) [8].

(5) Other Activities

- Sponsored (as part of the recommending team) the membership of MBSD-SIRT (Mitsui Bussan Secure Directions) and of UFG-CERT (Mitsubishi UFJ Financial Group) in FIRST.
- Contributed an article on vulnerability countermeasures titled "*Vulnerability Information to Keep in Mind*", to the ITpro CSIRT Forum held by Nikkei Business Publications, Inc.[9].
- Posted a report on HIRT's activities on our security information portal (Table 4).

Table 4: Reports Published on the Security Information Portal.

Number	Title
HIRT-PUB10008 (English version)	Hitachi Vulnerability Disclosure Process
HIRT-PUB11003	Malware Circulating in P2P File-Sharing Environment (2011)
HIRT-PUB11002	HIRT Annual Report 2010
HIRT-PUB11001	Zero-Day Response (2011)

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 12 and Table 5). 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 6) 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 [10] 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.

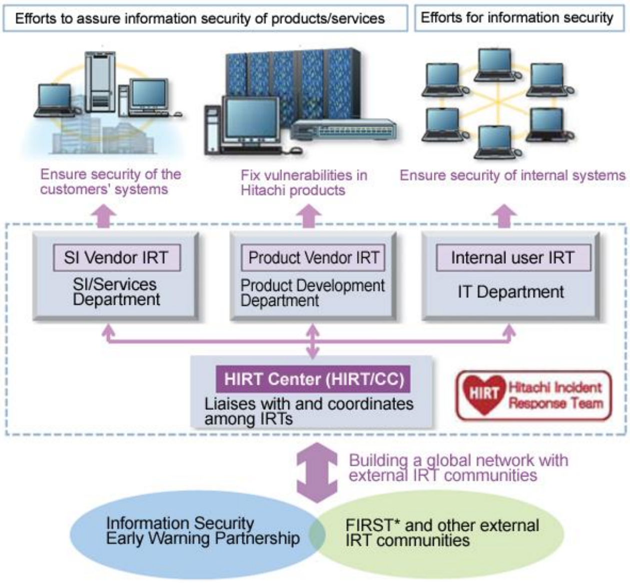

Efforts to assure information security of products/services
Efforts for information security
Ensure security of the customers' systems
Fix vulnerabilities in Hitachi products
Ensure security of internal systems
SI Vendor IRT
SI/Services Department
Product Vendor IRT
Product Development Department
Internal user IRT
IT Department
HIRT Center (HIRT/CC)
Liaises with and coordinates among IRTs
HIRT Hitachi Incident Response Team
Building a global network with external IRT communities
Information Security Early Warning Partnership
FIRST* and other external IRT communities

Figure 12: Four IRTs as an organizational model.

Table 5: 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 6: 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.

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.

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 13).

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 7) and those for external organizations (Table 8). 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 9 and Figure 14). 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.

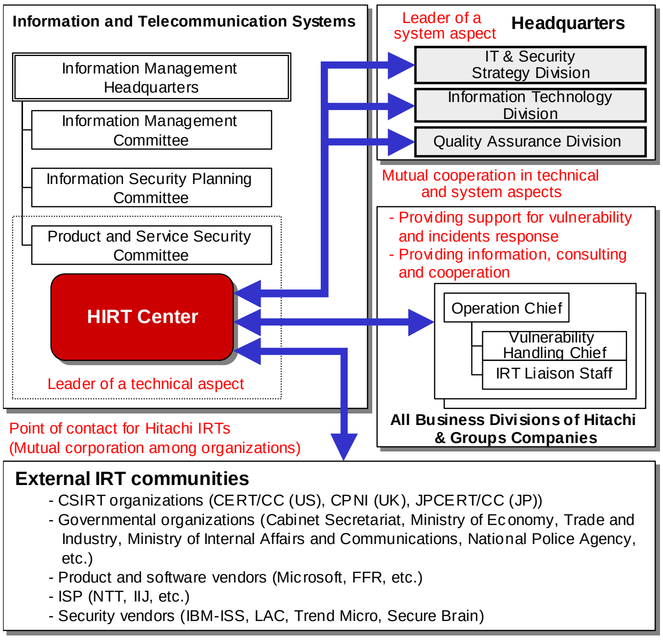

Information and Telecommunication Systems
Information Management Headquarters
Information Management Committee
Information Security Planning Committee
Product and Service Security Committee
HIRT Center
Leader of a technical aspect
Point of contact for Hitachi IRTs
(Mutual corporation among organizations)
Leader of a system aspect
Headquarters
IT & Security Strategy Division
Information Technology Division
Quality Assurance Division
Mutual cooperation in technical and system aspects
- Providing support for vulnerability and incidents response
- Providing information, consulting and cooperation
Operation Chief
Vulnerability Handling Chief
IRT Liaison Staff
All Business Divisions of Hitachi & Groups Companies
External IRT communities
- CSIRT organizations (CERT/CC (US), CPNI (UK), JPCERT/CC (JP))
- Governmental organizations (Cabinet Secretariat, Ministry of Economy, Trade and Industry, Ministry of Internal Affairs and Communications, National Police Agency, etc.)
- Product and software vendors (Microsoft, FFR, etc.)
- ISP (NTT, IIJ, etc.)
- Security vendors (IBM-ISS, LAC, Trend Micro, Secure Brain)

Figure 13: Position of HIRT Center.

Table 7: (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 8: (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) [11]

[*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)".

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 15).

Table 9: 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.

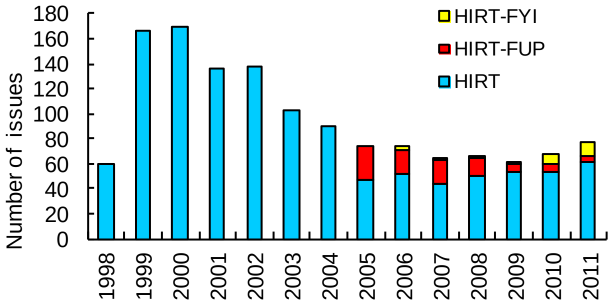


Figure 14: Number of issues of security information by ID number.

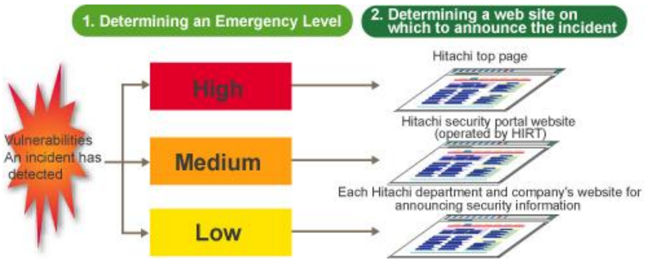

1. Determining an Emergency Level
2. Determining a web site on which to announce the incident
Vulnerabilities
An incident has detected
High
Medium
Low
Hitachi top page
Hitachi security portal website (operated by HIRT)
Each Hitachi department and company's website for announcing security information

Figure 15: Conceptual view of issuing information based on "Emergency Level" x "Website Level".

4 Activity Summary from 1998 to 2010

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

4.1 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 [6]:

- 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 [12].
- "Survey on Malware Circulating Within the P2P File Exchange Environment" [13]
- 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 16).

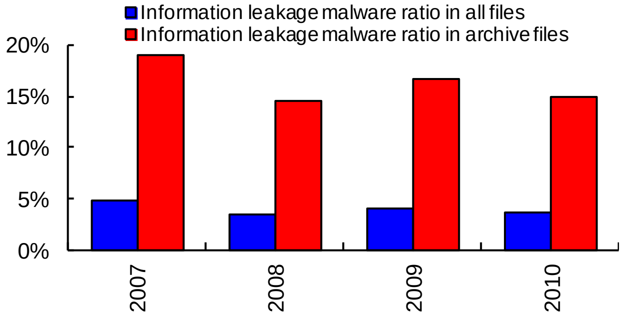


Figure 16: Change in Malware Circulating in Winny That Causes Information Leakage.

4.2 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 17).

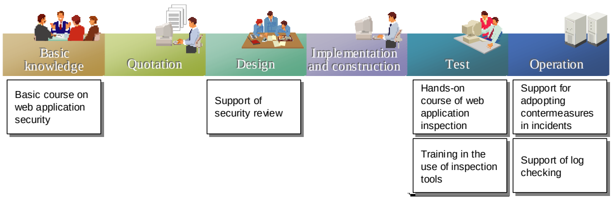

Basic knowledge
Quotation
Design
Implementation and construction
Test
Operation
Basic course on web application security
Support of security review
Hands-on course of web application inspection
Training in the use of inspection tools
Support for adpopting contermeasures in incidents
Support of log checking

Figure 17: 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" [14]
- 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) [15] which tries to visualize the observational data.

4.3 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" [16] 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 [17].

(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)" [18].

(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.

4.4 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 [19]. As of December 2012, 31 teams have been joined (Figure 18).

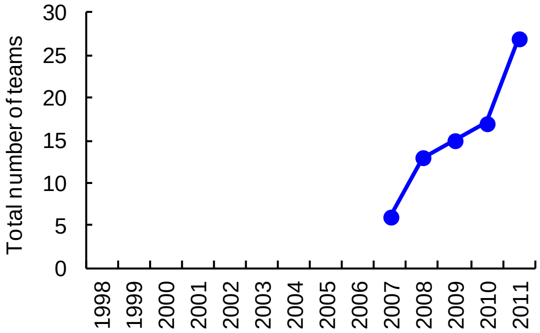


Figure 18: Change in Number of Nippon CSIRT Association Members.

(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 [20].

(4) Lectures

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

4.5 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 [21]

4.6 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 [22]. 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 2013, a total of 289 teams have joined this community, including 23 Japanese teams (Figure 19) [*d].

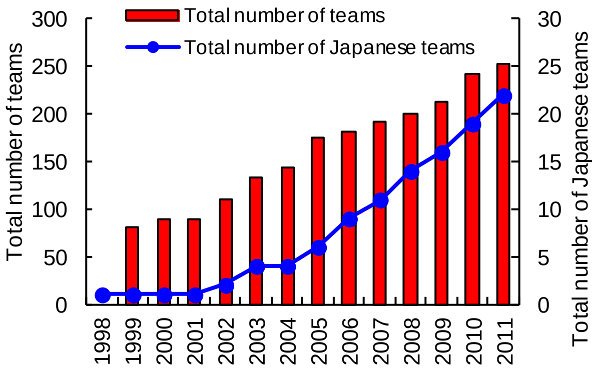


Figure 19: Changes in the number of members of FIRST.

(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 20). 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/

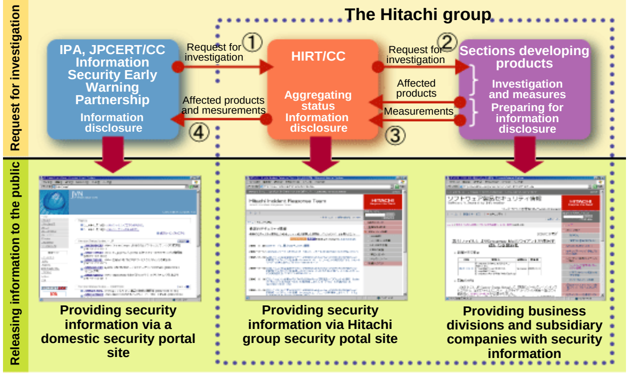

Request for investigation
Releasing information to the public
The Hitachi group
IPA, JPCERT/CC Information Security Early Warning Partnership
Information disclosure
Request for investigation
①
HIRT/CC
Aggregating status
Information disclosure
Request for investigation
②
Sections developing products
Investigation and measures
Preparing for information disclosure
Affected products and mesurements
④
Affected products
Measurements
③
Providing security information via a domestic security portal site
Providing security information via Hitachi group security potal site
Providing business divisions and subsidiary companies with security information

Figure 20: 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.

4.7 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 [23][24].

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) [25].

(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)

4.8 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 [26].

[*d] 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).

(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 [27], we provided a point of contact, as shown in Table 10, that initiates actions when vulnerabilities or malicious actions in Hitachi products and Hitachi-related websites are pointed out.

Table 10: 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

4.9 The Year 2002

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

SNMP vulnerability [10] 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 [28]. 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 [29].

(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 21) [30][31].

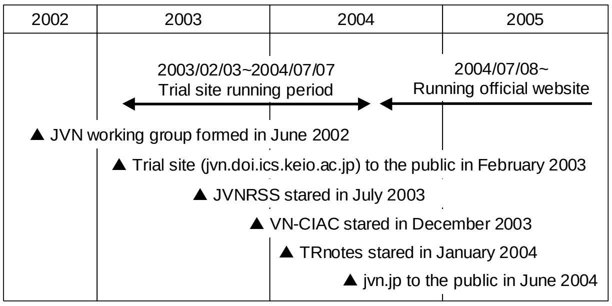

2002
2003
2004
2005
2003/02/03~2004/07/07
Trial site running period
2004/07/08~
Running official website
▲ JVN working group formed in June 2002
▲ Trial site (jvn.doi.ics.keio.ac.jp) to the public in February 2003
▲ JVNRSS stared in July 2003
▲ VN-CIAC stared in December 2003
▲ TRnotes stared in January 2004
▲ jvn.jp to the public in June 2004

Figure 21: 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/).

4.10 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 22), 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.

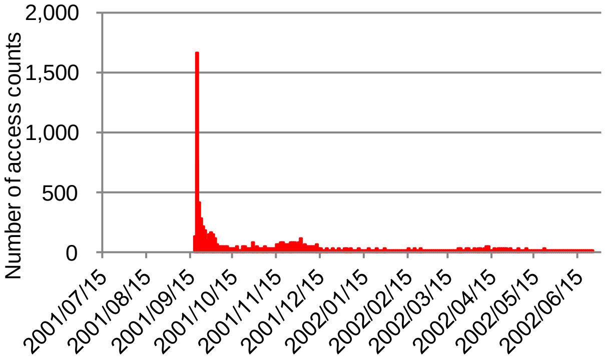


Figure 22: Changes in the number of Nimda log counts found during the observation period (for Nimda).

4.11 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" [32] for vulnerability. It provides the Severity Metric indicating the severity of vulnerability [33] Common Vulnerabilities and Exposures (CVE) classified information security vulnerabilities into "Vulnerabilities" and "Exposures" and focuses on the former [34]. 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 [35], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [36] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

4.12 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 23).

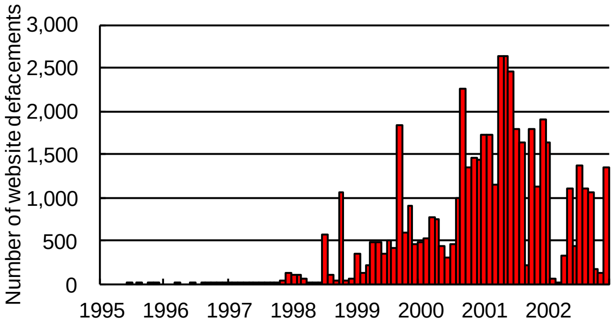


Figure 23: Changes in the number of websites defacements.

4.13 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 [37] as a speaker as an instructor.

5 Conclusion

Rigorously implementing all information security measures lowers degrees of freedom and makes it impossible to respond to business speed. And taking information security measures individually on one's own responsibility can lead to a single failure causing multiple knock-on security incidents. We believe that CSIRTs can be used as a balanced means of implementing cyber attack countermeasures.

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 also plan, via leadership activities in the CSIRT community, to progressively develop into a real practice the utilization of CSIRTs for cyber attack countermeasures.

(April 30, 2013)

References

1) Trend Micro Incorporated: Report on Internet Threat, http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html
2) Conficker Work Group - ANY - Infection Tracking, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking
3) NIST NVD (National Vulnerability Database), http://nvd.nist.gov/
4) Information-Technology Promotion Agency, Japan: Quarterly Reports, http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html
5) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/
6) Nippon CSIRT Association: incident response, http://www.nca.gr.jp/2010/incidentresponse.html
7) Information-technology Promotion Agency, Japan: Security Content Automation Framework, http://jvndb.jvn.jp/en/apis/myjvn/index.html
8) ITU-T X.1500 : Overview of cybersecurity information exchange, http://www.itu.int/rec/T-REC-X.1500-201104-I
9) ITpro Security, http://itpro.nikkeibp.co.jp/security/
10) 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
11) anti Malware engineering workshop, http://www.iwsec.org/mws/2012/
12) SGU MIT Workshop Academy CERT Meeting(2010/7), http://academy-cert-indonesia.blogspot.jp/2010/06/academy-cert-meeting.html
13) Malware Circulating in P2P File Exchange Software Environment (2011) (2011/9), http://www.hitachi.co.jp/hirt/publications/hirt-pub11003/index.html
14) 2009 Survey on information leakage via P2P File Exchange Software Environment (2009/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html
15) cNotes: Current Status Notes, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi
16) Information-Technology Promotion Agency, Japan: Countermeasures against DNS Cache Poisoning (2009/2), http://www.ipa.go.jp/security/vuln/DNS_security.html
17) Recording Site for Joint Workshop on Security 2008, Tokyo (2008/3), http://www.nca.gr.jp/jws2008/index.html
18) 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
19) CSIRT - Nippon CSIRT Association, http://www.nca.gr.jp/
20) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
21) GlobalSign Adobe Certified Document Services, http://jp.globalsign.com/solution/example/hitachi.html
22) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
23) 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
24) Information-technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline (2004/7), http://www.ipa.go.jp/security/ciadr/partnership_guide.html
25) JVN (Japan Vulnerability Notes), http://jvn.jp/
26) 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
27) 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 (not available)
28) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
29) 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
30) Considerations on JPCERT/CC Vendor Status Notes DB: JVN, CSS2002 (2002/10), http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf
31) Development of JVN to Support Dissemination of Security Information (2005/5), http://www.hitachi.co.jp/hirt/csirt/jvn/index.html
32) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
33) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp
34) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/
35) ICAT, http://icat.nist.gov/(not available)
36) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
37) 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.