# HIRT: Annual Report 2010

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

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

## 1 Introduction

The last ten years of the CSIRT's efforts to fight cyber attacks in Japan can be divided into two phases (Figure 1). The first phase is the acknowledge phase. During this phase, looking at the CSIRT activities developed in the U.S., we introduced the idea of "incident response", where people would handle an incident based on a predefined plan. The second phase is the predawn phase, where Japanese CSIRT got in gear with the feedback from the experience of dealing with network worms that ran riot between 2001 and 2003. During this phase, the basis of the CSIRT's activities in Japan that reflected our regionality has started to develop, such as the launch of the Information Security Early Warning Partnership, release of the Vulnerability Information Database JVN (Japan Vulnerability Notes) and establishment of Nippon CSIRT Association.

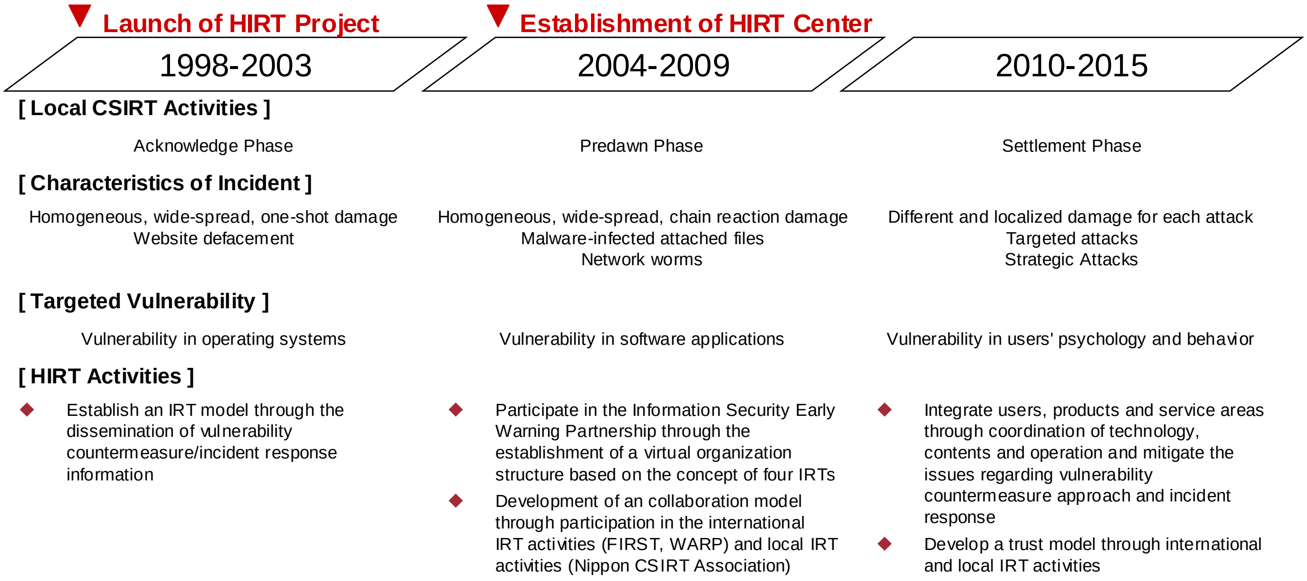
On the other hand, cyber attacks continued to develop and their targets began to shift from the operating systems to software applications, especially to web applications. Malicious programs have evolved into more advanced forms, such as malware-infected attachment files, network worms and bots, improving technology for good or bad. In addition, like web malware and USB malware, attacks that exploit vulnerability in the Internet users' psychology and behavior and use it for advantage have become common since around 2008.

Considering the change in the nature of incidents, the next five years should be used to penetrate the CSIRT activities into Japan, understanding our regionality. We should also go forward to develop a new trust model between the local CSIRTs and international counterparts.

The requirements we think a CSIRT must satisfy to promote vulnerability countermeasure approach and incident response are that it can "predicting and alerting from a technical point of view", "making technical coordination" and "collaborating with external communities on the technical aspects". Here, we do not assume some special occasions. The role of a CSIRT is to "catch the emerging threats and take actions as early as possible" using the experience of incident response operations, where predicting and preventing the damage from possible incidents and implementing the security measures to mitigate the damage should it happen.

As an entity that has the necessary skills and the part and as the Hitachi Group's single point of contact for the CSIRT activities, HIRT (Hitachi Incident Response Team) is responsible to lead the fight against vulnerability in products and services and incident response for malware infection and information leakage, and to advance Hitachi's brand image in the security field.

This report will introduce a summary of the vulnerabilities and threats and the activities of HIRT in 2010.



| | ▼ Launch of HIRT Project | ▼ Establishment of HIRT Center | |
|---|---|---|---|
| | 1998-2003 | 2004-2009 | 2010-2015 |
| [ Local CSIRT Activities ] | Acknowledge Phase | Predawn Phase | Settlement Phase |
| [ Characteristics of Incident ] | Homogeneous, wide-spread, one-shot damage<br>Website defacement | Homogeneous, wide-spread, chain reaction damage<br>Malware-infected attached files<br>Network worms | Different and localized damage for each attack<br>Targeted attacks<br>Strategic Attacks |
| [ Targeted Vulnerability ] | Vulnerability in operating systems | Vulnerability in software applications | Vulnerability in users' psychology and behavior |
| [ HIRT Activities ] | ◆ Establish an IRT model through the dissemination of vulnerability countermeasure/incident response information | ◆ Participate in the Information Security Early Warning Partnership through the establishment of a virtual organization structure based on the concept of four IRTs<br>◆ Development of an collaboration model through participation in the international IRT activities (FIRST, WARP) and local IRT activities (Nippon CSIRT Association) | ◆ Integrate users, products and service areas through coordination of technology, contents and operation and mitigate the issues regarding vulnerability countermeasure approach and incident response<br>◆ Develop a trust model through international and local IRT activities |

Figure 1: Change in Incidents and HIRT Activities.

# 2 Overview of activities in 2010

This section focuses on HIRT activities in 2010.

## 2.1 Overview of Threats and Vulnerabilities

### (1) Overview of Threats

In 2010, the attacks that targeted a specific organization (targeted attack) and used an organization's internal network as an attack base (stealth attack) gathered attention, such as the attack that exploited the vulnerabilities in Internet Explore in January (so-called Operation Aurora) and the emergence of Stuxnet in July that targeted control systems. The known threats like web malware (e.g. Gumblar) and USB malware (e.g. Conficker) have continued to cause damage.

Especially, in September 2010, a large-scale malware infection occurred caused by the contents generated by web service combination (mash-up). The incident showed that we needed to consider security measures from the unique viewpoint of the web services.

- **APT: Advanced Persistent Threats (advanced, stealth attacks that target specific organization)**

APT is a collective term for "attacks that target a specific organization (targeted attack) and use an organization's internal network as an attack base (stealth attack)". After the "attacks that exploited the vulnerabilities in Internet Explore in January (so-called Operation Aurora)", the term has become well known [1].

The term APT was used earlier in around April 2008, in the article "An Evolving Crisis" in the Bloomberg Businessweek magazine. The term is used to explain a new attack method seen in the Byzantine Foothold operations [2] that have started around 2006 and targeted the U.S. government and defense industries. The characteristics of a new attack method are that it uses whatever resource available for attack, that it is advanced and sophisticated, that the target is clear and that it never gives up. The name APT reflects those characteristics [3].

In Japan, in an IPA report "Report on APT" released in December 2010, it is defined as "attacks that are persisting, viciously exploit vulnerability, combine multiple attack methods tactfully, target a particular business or person through social engineering, and are therefore very difficult to deal with" [4].

In many cases, APT is an attack method that combines the 'common attacks' that are composed of common attack techniques to breach the target system and the 'customized attacks' that are composed of specialized attack techniques to attack the target system (Figure 2).

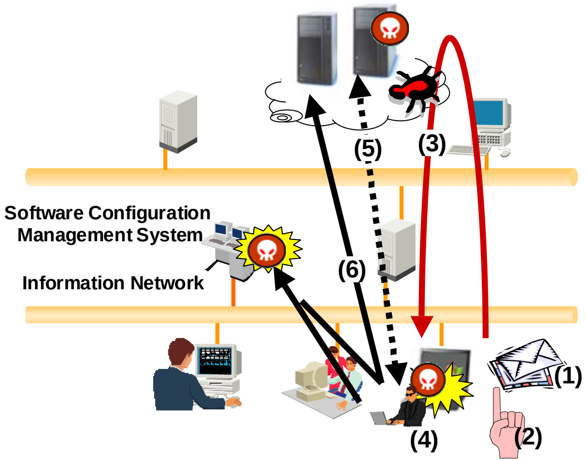
As shown in Figure 3, the attack against more than 30 corporations including Google, Adobe, Symantec and Yahoo, aimed to steal intellectual property in January 2010, was composed of the common attacks (1) to (2) that exploited vulnerability in Internet Explorer (MS10-035) and the customized attack (6) that attacked a software configuration management system.

Likewise, in the case of Stuxnet that targeted a control system in July 2010, after the attacker breached the information network via a USB malware attack exploiting Windows vulnerability, the attack was composed of the common attack (1) and (2) to breach the control information network and the customized attack (3) and (4) to breach the control network and disrupt the operation of the control system as shown in Figure 4.

The common attacks use various attack techniques and they are designed to bypass the traditional countermeasures. On top of this, since an APT attack is versatile and can change the customized attack part accordingly to its target, it will continue to be a big threat.

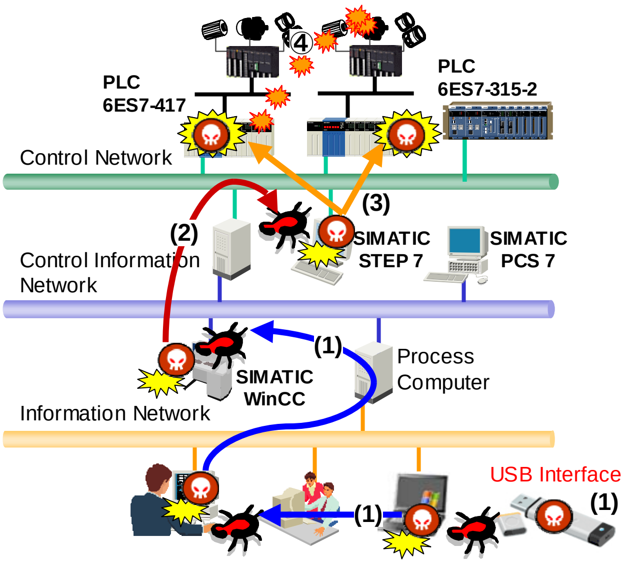
| | | |
|---|---|---|
| A | **It starts as a targeted attack using social engineering.**<br>■ Send an email or instant message from a trusted source that includes a link and lure the target to a malicious website. (>>Gumblar)<br>■ Use a USB malware and exploits the Windows vulnerabilities. (>>Conficker) | Common Attacks |
| P | **While being stealthy, the malware keeps a communication environment it can communicate with external computers.**<br>■ Communicates with a command and control server.<br>■ Downloads new features or files to update itself. | |
| T | **The final goal (final threat) differs depending on the target.**<br>■ Attack the software configuration management system (>> Operation Aurora)<br>■ Disrupt the control system's operation (>> Stuxnet)<br>■ Steal classified information (>> Night Dragon, RSA SecureID incident) | Customized Attacks |

Figure 2: APT = Common Attacks and Customized Attacks.



| | | |
|---|---|---|
| Common Attacks | (1) | Sends an email or instant message from a trusted source that includes a link |
| | (2) | Redirect the target to a website embedded with malicious JavaScript code upon clicking the link |
| | (3) | Malicious JavaScript code that exploits vulnerability in Internet Explorer (MS10-035) is executed |
| | (4) | Download a new binary and execute it |
| | (5) | Setup a backdoor and communicate with the command and control server |
| Customized Attacks | (6) | Attack the software configuration management system (such as Perforce) accessible from the breached system |

Figure 3: Operation Aurora Scenario.



| | | |
|---|---|---|
| Common Attacks | (1) | **Breach the information network**<br>Spread infection exploiting vulnerabilities in Windows (MS08-067, MS10-046, MS10-061, MS10-073, MS10-092) |
| | (2) | **Breach the control information network**<br>Win Infect SIMANTIC WinCC, PCS7 and STEP7 exploiting vulnerabilities in Windows and Siemens software (CVE-2010-2772) |
| Customized Attacks | (3) | **Infect the control network**<br>Exploit a Siemens software (SIMANTIC Step7), insert a malicious code into PLC (programmable Logic Controller) |
| | (4) | **Disrupt the control system's operation**<br>Change the output frequencies for short periods of time over the months >>> disrupt the operation of the control system |

Figure 4: Control System Attack Scenario (Stuxnet).

- **Web Malware exploiting Mash-up**

An attack exploiting mash-up is a technique that guides users who have visited a website to a malicious website and infects their PC with malware without their knowledge by altering a component file stored on the other website. For example, if an advisement file that the website displays is altered (embedded with a malicious code to guide to the malicious website), the users' browser will load the malicious website by executing the malicious code (Figure 5). If the advertisement file is linked by many websites, a single alteration can achieve the same result with the alteration of nth number of websites, and impact will be broad. Also, since the advertisement file is stored on the other website and it would be difficult for the website administrator to find the cause, a countermeasure from a unique viewpoint of the web services, in this case, mash-up, is necessary.

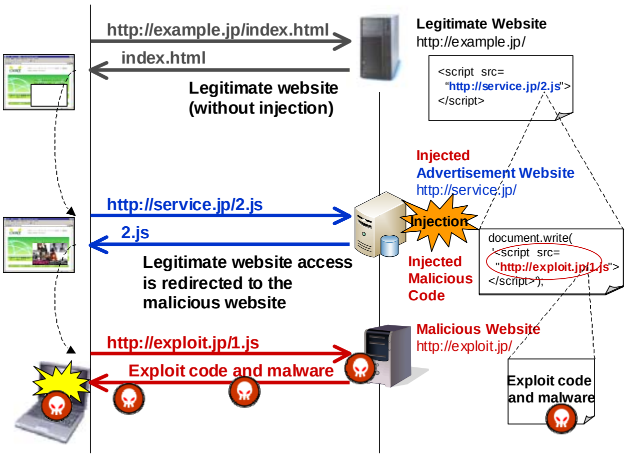


Figure 5: Web Malware Exploiting Mash-up

- **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 6) [5]. However, according to the report of the Conficker Work Group, the number of computers infected with Conficker is about 5 million on the IP address base (Figure 7) [6].

Considering such situation, in addition to the deployment of security guards (implementation of antivirus software) and training of security guards (application of security patch), we need to educate people to lock the door (disable the Autorun feature for the external media[a*].

### (2) Overview of Vulnerabilities

The total number of the vulnerabilities added to the U.S. NIST NVD (National Vulnerability Database) [7] in 2010 is 4,639. Among them, a web software application products account for about 30 percent (1,458) and has shown an increasing tendency since 2008 (Figure 8). Looking at the breakdown, the situation where cross-site scripting (XSS) and SQL injection account for about 80 percent does not change (Figure 9). Likewise, among the reports to IPA on the in-service websites, cross-site scripting and SQL injection account for about 70 percent and the number of reports on these two vulnerabilities is more than 200 in a year (Figure 10) [8].

[a*] Microsoft reported that as the result of sending out an update program 971029 that would disable the Autorun feature through the auto update channel, the infection rate of malware that exploit the Autorun feature was dramatically decreased (as of May 2011, 62 percent decrease for Windows XP 3SP and 74 percent decrease for Windows Vista overall).

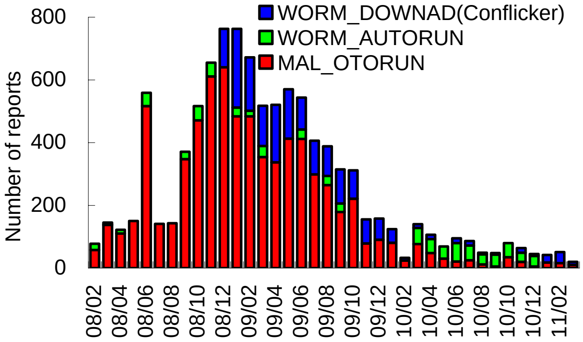


Figure 6: Number of Infection of USB Malware (per month).

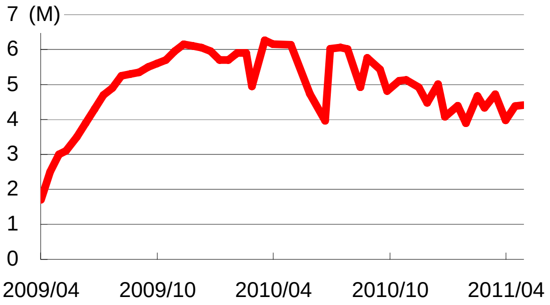


Figure 7: Number of Infection of ConfickerA+B (per day).

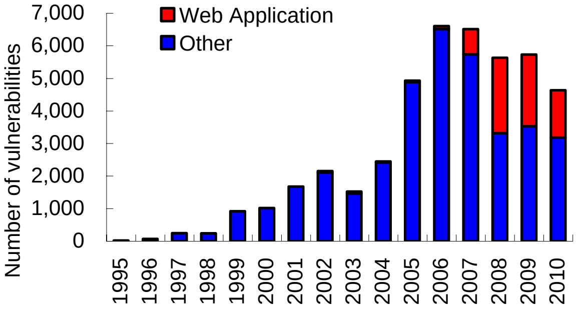


Figure 8: Number of Vulnerabilities Reported (Source: NIST NVD).

Meanwhile, the number of reports on the applications often used on the client computers, so-called standard software, is on the increase. Especially, the number for Adobe Acrobat, Adobe Reader and Adobe Flash Player tripled (20 to 57 for Adobe Flash Player) or quadrupled (17 to 68 for Adobe Acrobat and Adobe Reader) from 2008 to 2010 (Figure 11).

Since the web-based passive attack (web malware attack) has been becoming common, in addition to vulnerability countermeasure approach for standard software, promotion of that for web application development and operation is needed to prevent the websites from being used as an attack base.

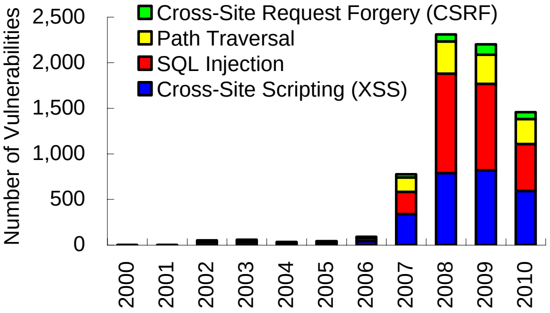


Figure 9: Changes in the number of vulnerabilities reported for software products of web application (Source: NIST NVD).

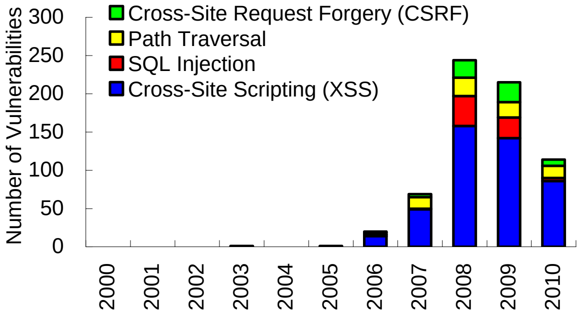


Figure 10: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC).

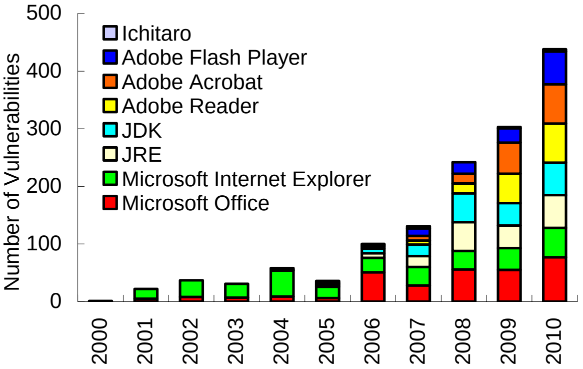


Figure 11: Number of Vulnerability in Standard Software.

## 2.2 HIRT Activities

This subsection describes the HIRT activities in 2010.

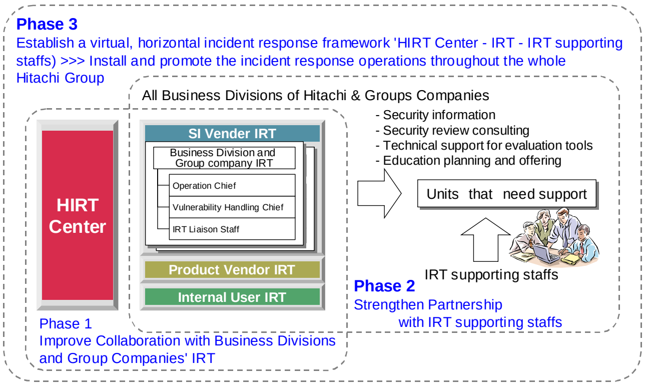
### (1) Improve Hitachi Group's CSIRT Activities (Phase 1)

Each business division and group company that belongs to the Information and Communication Systems Company have an IRT that consists of an operating officer for IRT activities, a vulnerability-related information handling officer and an IRT liaison staff. To install incident response operations into the whole Hitachi Group, however, not only the collaboration among the existing IRTs is necessary but also it is absolutely imperative to take a new effort, for instance, expanding the IRTs or establishing a close partnership with a person who belongs to a business division or group company and working with the HIRT Center to actively promote the HIRT activities (hereinafter referred to as an "IRT supporting staffs").

In 2010, to improve the Hitachi Group's CSIRT activities, with a goal of installing incident response operations into the whole Hitachi Group, we launched the efforts divided into three phases (Figure 12).

### (2) Disseminate Countermeasure Information through HIRT Open Meetings

A HIRT Open Meeting is an activity to popularize the HIRT community based on the trust relationship. A meeting is held reflecting the policy that "it offers an opportunity for the HIRT Center members to share information about the HIRT activities", that "it offers an open event for people of the Hitachi Group to learn about the HIRT Center's activities and for the HIRT Center members to share information with and get opinions from non HIRT Center members, and that "it provides a opportunity to call for participation to the HIRT community based on the trust".


Phase 3
Establish a virtual, horizontal incident response framework 'HIRT Center - IRT - IRT supporting staffs) >>> Install and promote the incident response operations throughout the whole Hitachi Group
All Business Divisions of Hitachi & Groups Companies
HIRT Center
SI Vender IRT
Business Division and Group company IRT
Operation Chief
Vulnerability Handling Chief
IRT Liaison Staff
Product Vendor IRT
Internal User IRT
- Security information
- Security review consulting
- Technical support for evaluation tools
- Education planning and offering
Units that need support
IRT supporting staffs
Phase 2
Strengthen Partnership with IRT supporting staffs
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<br>➢ Promote support activities with the collaboration between the IRT of Business Divisions and Group Companies<br>➢ Establish an IRT coalition framework and mechanism to share technological know-how using the HIRT open meetings<br>➢ Disseminate information about solutions/countermeasures for the problems discussed in the security review consultation. |
| Phase 2 | Strengthen Partnership with IRT supporting staffs<br>➢ Trial collaboration with IRT supporting staffs (of business divisions and group companies)<br>➢ Bottom up the IRT activities with the IRT supporting staffs as a starting point |
| Phase 3 | Establish Virtual, Horizontal Incident Response System<br>➢ Promote various support activities by the HIRT Center, IRTs and IRT collision support members<br>➢ Develop a HIRT in a broad sense (virtual organization model) by combining the user collaboration model (Phase 1,2) and entity collaboration model (Phase 3). |

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

In 2010, to start with the Phase 1 to improve the Hitachi Group's CSIRT activities, we established an operation system for IRT collaboration and a mechanism for disseminating technical know-how using HIRT Open Meetings. To be specific, based on the policies of the HIRT Open Meeting, we set up two types of regular liaison meetings (operational and technical meeting) for the vulnerability related information handling officers and IRT liaison staff.

- Operational Meeting (once per half year): A meeting for the vulnerability related information handling officers and IRT liaison staff to share and learn know-how on the operation of an IRT.
- Technical Meeting (2 - 4 times per half year): A meeting for the designers, system engineers and those who are willing to share their technical know-how to share and learn the technical know-how necessary to implement security into products and services.

Especially for the technical meetings, since we wanted to pick up a timely topic, we have held three meetings in December 2010.

- Control System Security Seminar
  Trends in Control System Security and Stuxnet Case Studies
- Mobile Website Security
  Discussed and shared the experiences on the development and operation of mobile websites with a focus on easy login.
- Year 2010 issues on cryptographic algorithms
  Transition of cryptographic algorithms

### (3) Survey on Malware Circulating within the P2P File Exchange Environment

As for information leakage via file-sharing software, we thought that it was necessary to work with the external entity. HIRT, with the System Development Laboratory, gained the cooperation of the P2P Study Group of the Secure Trusted Network Forum and conducted a research. In particular, since 2007, many Antinny-type, known malware that could cause information leakage have been swarming on a P2P file-sharing environment "Winny". Most of them disguised themselves as safe contents (disguise with folder/file icon) to tactfully lure users into executing the malware. The users must be careful about them.

- Malware is found in one in every 20-30 files (Figure 13)
- As for archive files, such as .zip, .lzh and .rar, which circulate widely in significant quantities, malware is found in one in every 5-7 files.
- Antinny and its subspecies, which cause information leakage, account for 70% of the known malware.
- About 90% of malware fakes itself as an icon, such as a folder, which resembles safe content. About 30% use faked file names.

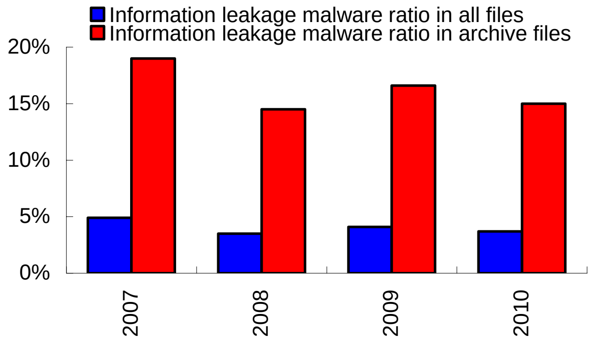


Figure 13: Change in Malware Circulating in Winny That Causes Information Leakage.

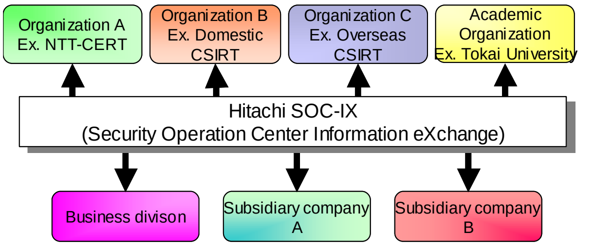
### (4) Strengthening Partnership with the CSIRT Community

As part of activities to strengthen partnerships among organizations, we have had meeting with NTT-CERT [9] on a regular basis since 2006 to exchange information to help improve CSIRT activities. Also, as part of the activity to strengthen the inter-organizational collaboration, we supported the Nippon CSIRT Association in organizing an international partnership workshop in December [10]. At the workshop, the experts on malware and Botnet were invited and they gave a lecture and hands-on exercise (Figure 14).

Figure 14: International Partnership Workshop (Source: Nippon CSIRT Association).

- "Honeywell and virtual honeypots" by David Watson from Honeynet Project
- "Becoming Criminal-A Botnet Exercise" by Richard e. of Shadowserver

As for the Hitachi SOX-IX (Security Operation Center Information eXchange) (Figure 15), which was a framework for organizations to mutually utilize the information such as observational data for threat analysis, we collaborated with the Incident Information Utilization Framework Working Group and disseminated the following information [11].



Creating a framework or mechanism for exchange information, such as observation data, has the following advantages:
- It allows analysis using a large amount of various observation data.
- It allows you to use observation data you do not have
- It allows you to use technology and know-how in fields in which each CSIRT excels.

Figure 15: Schematic view of the Hitachi SOC-IX.

- A website with the information about Gumblar countermeasure
- Information on the SSL attack by the Botnet PushDo A DDoS incident where a large volume of ill-formed SSL requests had been sent against the port 443/tcp (https) from a number of sources since February 3, 2010. About 40 .jp domains had been targeted.
- Information about Stuxnet

### (5) Other Activity

- Reported on an industry-university joint event "Anti-Malware Engineering Workshop (MWS2009)" held at the 2010 FIRST Symposium, Hamburg [12]
- Supported an organization of "Academy CERT Meeting" in July 2010 with JPCERT/CC to help Indonesian academic CSIRT activities [13]
- Contributed an article "Must-Read Vulnerability Information" to ITPro CSIRT (Computer Security Incident Response Team) Forum, Nikkei Business Publications Inc. [14]
- Published a report on the HIRT activities on the security information portal (Table 1)

Table 1: Reports Published on the Security Information Portal.

| Number | Title |
|---|---|
| HIRT-PUB10008 | Hitachi Vulnerability Disclosure Process |
| HIRT-PUB10004 | Zero-Day Response (2010) |
| HIRT-PUB10003 | Malware Circulating in P2P File-Sharing Environment (2010) |
| HIRT-PUB10002 | HIRT: Annual Report 2009 |

## 3 HIRT

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

### 3.1 Organizational Model

We have adopted an organizational model consisting of four IRTs (See Figure 16 and Table 2). In the case of the Hitachi Group, it has three faces: the face of a developer of information system products (Product IRT), the face of a system integrator (SI) and service provider using those products (SI Vendor IRT), and the face of the Internet user to operate and maintain its information systems (Internal User IRT). By adding the HIRT/CC (HIRT Coordination Center) to coordinate these IRTs, we thought that the 4- IRT model could promote a more efficient and effective security countermeasure approach that would prompt the collaboration between IRTs at the same time clarifying the role of each IRT. The name HIRT means the incident response operation promoted by the whole Hitachi Group in a broad sense and means the HIRT/CC (HIRT Center) in a limited sense.

In fact, by the time 4 IRTs were established, we went through about four steps shown in Table 3. At each step, there was a "trigger" that encouraged the establishment of the organization. For example, when the Product IRT was launched at the second step, the fact that the vulnerability in SNMP [15] reported by CER/CC had affected a number of Hitachi products gave a push. Also, when the SI Vendor IRT was launched, it was the start of the "Information Security Early Warning Partnership" that gave a boost. The HIRT Center was later set up as a coordinator within and with the entities outside Hitachi after other three IRTs had been mostly formed.

## 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.

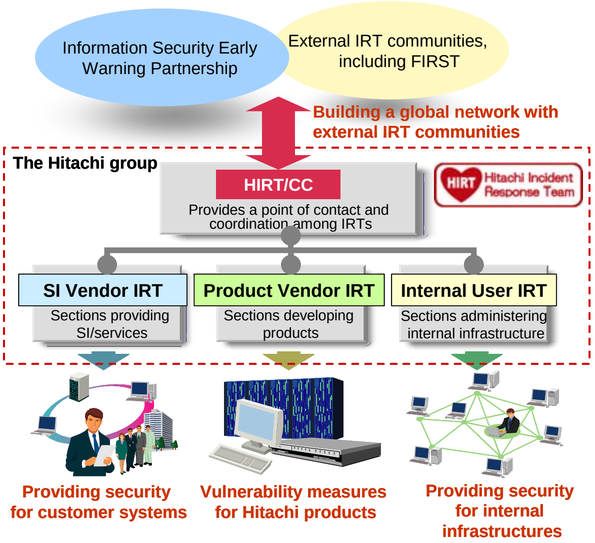

Information Security Early Warning Partnership
External IRT communities, including FIRST
Building a global network with external IRT communities
The Hitachi group
HIRT/CC
Provides a point of contact and coordination among IRTs
Hitachi Incident Response Team
SI Vendor IRT
Sections providing SI/services
Product Vendor IRT
Sections developing products
Internal User IRT
Sections administering internal infrastructure
Providing security for customer systems
Vulnerability measures for Hitachi products
Providing security for internal infrastructures

Figure 16: Four IRTs as an organizational model.

Table 2: Role of each IRT.

| Category | Role |
|---|---|
| HIRT/CC | Corresponding sections: HIRT/CC<br>- Provides a point of contact to external CSIRT organizations, such as FIRST, JPCERT/CC and CERT/CC.<br>- Provides coordination among the SI Vendor, Product Vendor and Internal User IRTs. |
| SI Vendor IRT | Corresponding sections: Sections providing SI/services<br>- Promotes CSIRT activities for customer systems.<br>- Provides customer systems with equivalent security against reported vulnerabilities to that for internal systems. |
| Product Vendor IRT | Corresponding sections: Sections developing products<br>- Provides support to promote vulnerability measures for Hitachi products and the release of information concerning such countermeasures<br>- 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<br>- Provide support to promote security measures for internal networks lest Hitachi websites should be used as a base for making unauthorized access. |

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<br>Establishing the Internal User IRT<br>(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<br>Establishing the Product Vendor IRT<br>(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<br>Establishing the SI Vendor IRT<br>(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. |

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.

## 3.3 Main Activities of HIRT Center

The main activities of the HIRT center currently being promoted include CSIRT activities for internal organizations (See Table 4) and those for external organizations (See Table 5).

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

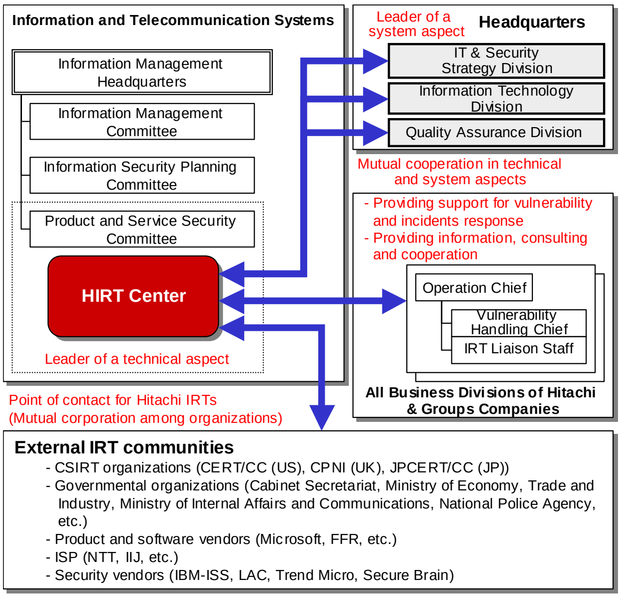

Information and Telecommunication Systems
Information Management Headquarters
Information Management Committee
Information Security Planning Committee
Product and Service Security Committee
HIRT Center
Leader of a technical aspect
Leader of a system aspect
Headquarters
IT & Security Strategy Division
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
Point of contact for Hitachi IRTs
(Mutual corporation among organizations)
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 17: Position of HIRT Center.

Table 4: (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)<br>➢ 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<br>➢ Accumulating and deploying technical know-how for countermeasures against vulnerabilities and incident response<br>➢ Promoting the transmission 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)<br>➢ Enhancing and expanding support and processes though internal support activities<br>➢ Enhancing web application security |
| Developing a framework for research activities | ➢ Developing a framework for joint research with the Systems Development Laboratory (for P2P observation, etc) |

Table 5: (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<br>➢ 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<br>➢ Promoting UK WARP related activities.<br>➢ 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 Tokai University (Professor Hiroaki Kikuchi) and HIRT.<br>➢ Participating in academic research activities, such as a workshop to develop human resources for research on malware countermeasures |

[b*] 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)".

As for the internal issue of security alerts and advisories, we have broken down HIRT security information into two types since June 2005. HIRT security information that aims to distribute security alerts and hot topics widely and HIRT-FUP information used to request relevant sections to take reactive measures, to take its priority and the needs into account (See Table 6 and Figure 18). To convey information efficiently, we reduce the number of issues of information by aggregating the same, and release the information in collaboration with the IT and Security Strategy Division and Quality Assurance Division.

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

In particular, for issuing security information 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 (See Figure 19).

Table 6: Classification of security information issued by HIRT.

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

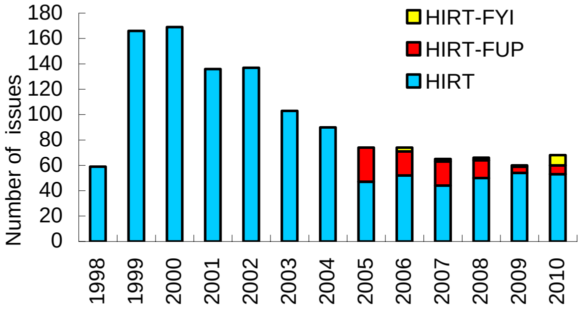


Figure 18: Number of issues of security information by ID number.

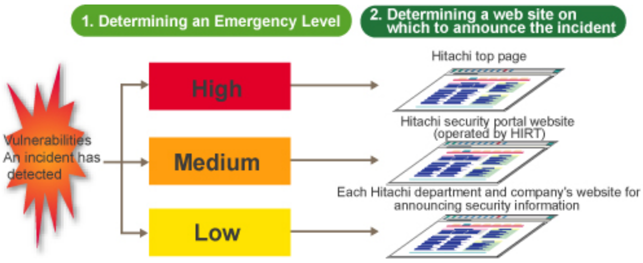

1. Determining an Emergency Level
2. Determining a web site on which to announce the incident
Vulnerabilities An incident has detected
High
Medium
Low
Hitachi top page
Hitachi security portal website (operated by HIRT)
Each Hitachi department and company's website for announcing security information

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

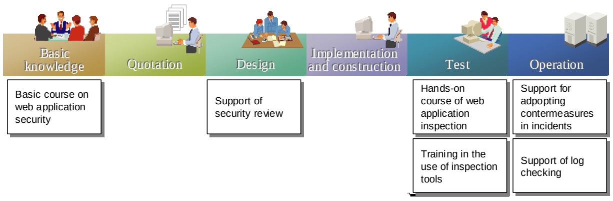

Basic knowledge
Quotation
Design
Implementation and construction
Test
Operation
Basic course on web application security
Support of security review
Hands-on course of web application inspection
Training in the use of inspection tools
Support for adpopting contermeasures in incidents
Support of log checking

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

## 4 Activity Summary from 1998 to 2009

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

### 4.1 The Year 2009

**(1) The Start of Product/Service Security Feedback**

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

**(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" [17][18]
- 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) [19] which tries to visualize the observational data.

## 4.2 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" [20] 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 [21].

### (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)" [22].

### (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 attacks 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.

## 4.3 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 [23]. As of April 2011, 20 teams have been joined (Figure 21).

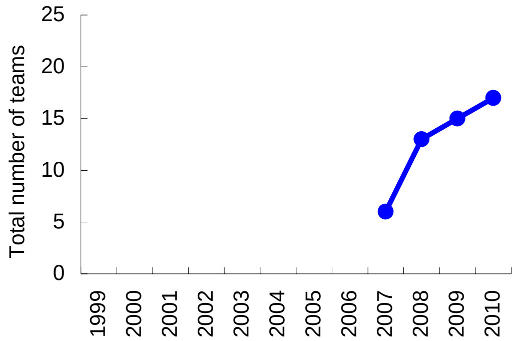


Figure 21: Change in Number of Nippon CSIRT Association Members.

### (3) Joining UK WARP

In order to strengthen the overseas partnership on CSIRT activities, we joined the Warning, Advice and Reporting Point (WARP), promoted by the Centre for the Protection of National Infrastructure (CPNI), a British government security organization, in May 2007 [24].

### (4) Lectures

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

## 4.4 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 [25]

## 4.5 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 [26]. 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 April 2011, 19 Japanese teams have joined the community. They include the CDI-CERT (Cyber Defense Institute), CFC (Info-Communications Bureau, the National Police Agency), HIRT (Hitachi), IIJ-SECT (IIJ), IPA-CERT (Information-technology Promotion Agency), JPCERT/CC, JSOC (LAC), KDDI-SOC (KDDI), KKCSIRT (Kakaku.com), MIXIRT (Mixi), NCSIRT (NRI Secure Technologies), NISC (National Information Security Center), NTT-CERT (NTT), NTT-DATA-CERT (NTT Data), Panasonic PSIRT (Panasonic), Rakuten-CERT (Rakuten), RicohPSIRT (Ricoh), SBCSIRT (Softbank) and YIRD (Yahoo) (See Figure 22).

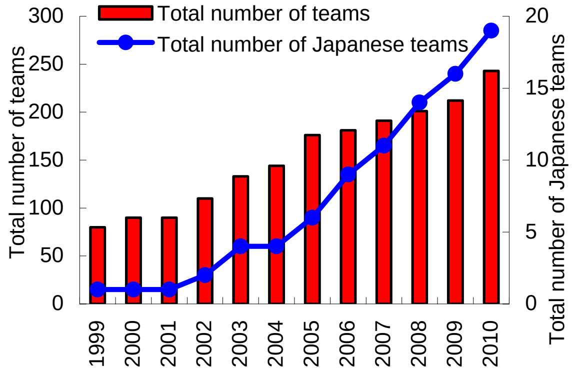


Figure 22: Changes in the number of members of FIRST.

### (2) Setting Up a Security Information Portal Site

In September 2005, in order to provide Internet users with comprehensive information on security problems applicable to the products and service of the Hitachi group, we set up a security information portal site within which the security information provided through the websites of Hitachi business divisions and group companies is integrated (See Figure 23). We also created "Guidance for Providing Security Information from Websites to External Users, V1.0".

**Security information portal site:**
**Japanese: http://www.hitachi.co.jp/hirt/**
**English: http://www.hitachi.com/hirt/**

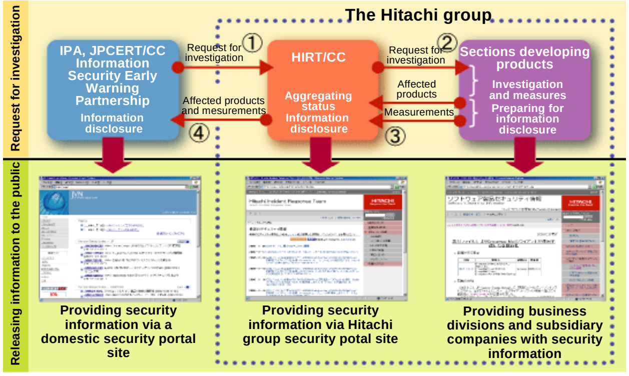

Request for investigation
Releasing information to the public
The Hitachi group
IPA, JPCERT/CC Information Security Early Warning Partnership
Information disclosure
Request for investigation ①
HIRT/CC
Aggregating status
Information disclosure
Request for investigation ②
Sections developing products
Investigation and measures
Preparing for information disclosure
Affected products
Measurements ③
Affected products and mesurements ④
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 23: Providing security information on the Hitachi security information portal.

### (3) Strengthening the Domestic Partnership for CSIRT Activities

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

## 4.6 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 [27][28].

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) [29].

### (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)

## 4.7 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 [30].

### (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 [31], we provided a point of contact, as shown in Table 7, that initiates actions when vulnerabilities or malicious actions in Hitachi products and Hitachi-related websites are pointed out.

## 4.8 The Year 2002

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

SNMP vulnerability [15] 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 [32]. 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 [33].

### (2) Assisting JPCERT/CC in Building Vendor Status Notes

We provided support to build and operate a trial website, JPCERT/CC Vendor Status Notes (JVN) (http://jvn.doi.ics.keio.ac.jp/), in February 2003, as an attempt to improve the domestic circulation of security information (See Figure 24) [34][35]. With the implementation of the "Standard for Handling Information Related to Vulnerabilities in Software, etc." in July 2004, the roles of the trial site were transferred to Japan Vulnerability Notes (JVN), a site releasing information on reported vulnerabilities (http://jvn.jp/en/index.html).

Table 7: Information on point of contact.

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

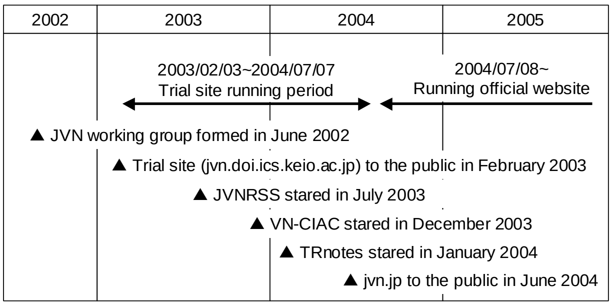

2002
2003
2004
2005
2003/02/03~2004/07/07
Trial site running period
2004/07/08~
Running official website
▲ JVN working group formed in June 2002
▲ Trial site (jvn.doi.ics.keio.ac.jp) to the public in February 2003
▲ JVNRSS stared in July 2003
▲ VN-CIAC stared in December 2003
▲ TRnotes stared in January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

Figure 24: Building and running a JVN trial site.

## 4.9 The Year 2001

### (1) Investigating the Activities of Worms Attacking Web Services

We investigated the activities of worms attacking web services in 2001, CodeRed I, CodeRed II and Nimda, from June 15, 2001 to June 30, 2002, based on the log data from the websites on the Internet. For CodeRed II and Nimda (Figure 25), which caused significant damage in Japan, the log reveals that the time span between the time at which the attack was first logged and the date on which attacks occurred most frequently was only approximately two days, indicating that damage caused by the worms had spread rapidly and widely.

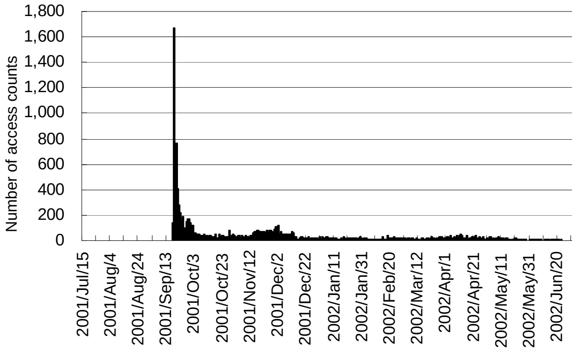


Figure 25: Changes in the number of Nimda log counts found during the observation period (for Nimda).

## 4.10 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" [36] for vulnerability. It provides the Severity Metric indicating the severity of vulnerability [37] Common Vulnerabilities and Exposures (CVE) classified information security vulnerabilities into "Vulnerabilities" and "Exposures" and focuses on the former [38]. 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 [39], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [40] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

## 4.11 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 (See Figure 26).

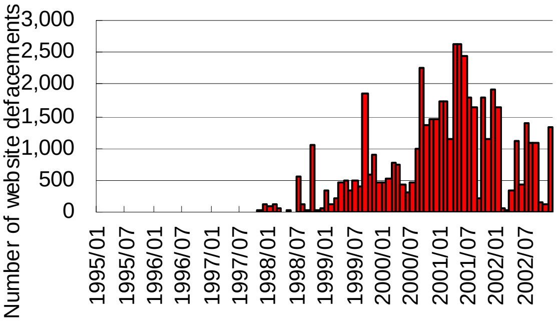


Figure 26: Changes in the number of websites defacements.

## 4.12 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 [41] as a speaker as an instructor.

# 5 Conclusion

Attack techniques in cyber attacks have become advanced and sophisticated, and there seems to be a change in the attackers' mind as well and they do not give up easily. It is necessary to respond to an incident not only with the technical consideration but also the physiological consideration as well. Under the circumstances, it is now that we must penetrate the CSIRT activities into Japan understanding our regionality. We should also go forward to develop a new trust model between the local CSIRTs and international counterparts.

With the changes surrounding the incident response in mind, HIRT will "catch the emerging threats and take actions as early as possible". Through the improvement of Hitachi Group's CSIRT activities and consolidation of inter-organizational collaboration, we will continue to contribute actively to promote vulnerability countermeasure approach and incident response in Japan.

(July 1, 2011)

## References

1) Protecting Your Critical Assets (2010), http://www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf

2) The New E-spionage Threat (2009), http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm

3) Under Cyberthreat: Defense Contractors (2009), http://www.businessweek.com/technology/content/jul2009/tc2009076_873512.htm

4) Information-technology Promotion Agency, IPA Technical Watch "Report on APT" (2010), http://www.ipa.go.jp/about/technicalwatch/20101217.html

5) Trend Micro Incorporated: Report on Internet Threat, http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html

6) Conficker Work Group - ANY - Infection Tracking, http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking

7) NIST NVD (National Vulnerability Database), http://nvd.nist.gov/

8) Information-Technology Promotion Agency, Japan: Quarterly Reports, http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html

9) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/

10) Nippon CSIRT Association: Report on International Collaboration Workshop (2010) http://www.nca.gr.jp/2010/event/index.html

11) Nippon CSIRT Association: incident respond http://www.nca.gr.jp/2010/incidentresponse.html

12) MS2009, FIRST Symposium (2010/1), http://www.first.org/events/symposium/hamburg-2010/program/

13) SGU MIT Workshop Academy CERT Meeting (2010/7), http://idsirtii.or.id/academy-cert-meeting/

14) ITpro Security, http://itpro.nikkeibp.co.jp/security/

15) 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

16) Anti-Malware Engineering Workshop (MWS2009) http://www.iwsec.org/mws/2011/

17) 2009 Survey on information leakage via P2P File Exchange Software Environment (2009/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html

18) Malware Circulating in P2P File Exchange Software Environment (2009) (2010/3), http://www.hitachi.co.jp/hirt/publications/hirt-pub09007/index.html

19) cNotes: Current Status Notes, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi

20) Information-Technology Promotion Agency, Japan: Countermeasures against DNS Cache Poisoning (2009/2), http://www.ipa.go.jp/security/vuln/DNS_security.html

21) Recording Site for Joint Workshop on Security 2008, Tokyo (2008/3), http://www.nca.gr.jp/jws2008/index.html

22) 2008 Information Technology Period Promotion - Awarding companies that have contributed to the promotion of information technology in 2008 (2008/10), http://www.jipdec.or.jp/gekkan/ceremony/prize02.html

23) CSIRT - Nippon CSIRT Association, http://www.nca.gr.jp/

24) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/

25) GlobalSign Adobe Certified Document Services, http://www.globalsign.com/adobe-cds/index.htm

26) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/

27) 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

28) Information-technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline (2004/7), http://www.ipa.go.jp/security/ciadr/partnership_guide.html

29) JVN (Japan Vulnerability Notes), http://jvn.jp/

30) 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

31) 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

32) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html

33) 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

34) Considerations on JPCERT/CC Vendor Status Notes DB: JVN, CSS2002 (2002/10), http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf

35) Development of JVN to Support Dissemination of Security Information (2005/5), http://www.hitachi.co.jp/rd/yrl/people/jvn/index.html

36) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls

37) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp

38) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/

39) ICAT, http://icat.nist.gov/

40) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/

41) 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.