HIRT: Annual Report 2009

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

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

1 Introduction

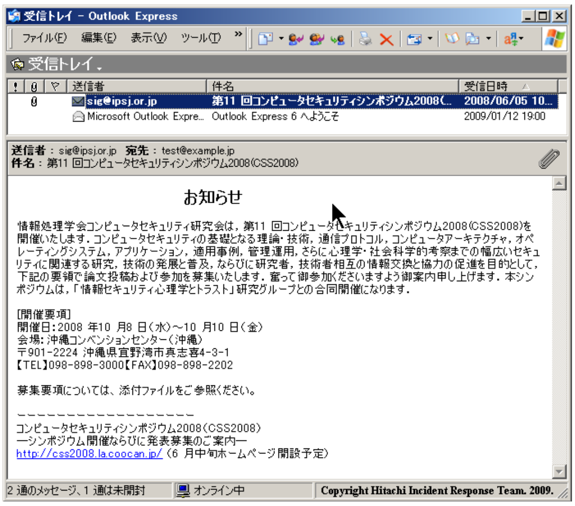
While information assurance measures have been taken since 2005 to reduce damage from information leakage, there has also been a significant transition in cyber attack technologies, which has been rendered invisible by such measures. From the perspective of the technical transition over the last decade, new attack technologies have been created in a short time cycle, and once established, will be continued to use in activities indefinitely. The technical inheritance and thorough customization through attack activities have hampered efforts to gain a clear overview of attack activities.

In particular, since 2008, cyber attack activities no longer arouse suspicion, but look apparently normal. Figure 1 shows a targeted attack using e-mail with attached malware. The malware sent to Hitachi disguised itself as Call For Papers for a 2008 (CSS2008) computer security symposium. The received e-mail messages were cut and pasted from original Call For Papers and look perfectly normal. Figure 2 shows a method used by Gumblar, web-based malware, to redirect a user to an attacker's site. A landing website, once hacked with redirection-code, will also encourage such infection cycle. Despite the intention of the user to access the landing website, the injected redirection-code will forcibly involve him/her in a series of attacks, such as access to harmful websites, downloading malware, and infection with the same by exploiting vulnerabilities.

Changes in incidents caused by such cyber attacks are also reflected in the attitude taken to address them. The emergence of Internet worms in 1988 provided an opportunity to recognize the importance of sharing information concerning the causes of incidents and countermeasures to establish a concept of "Incident response" to respond reactively in accordance with a predetermined plan. From 2001 to 2003, network worms appeared and countermeasures to them spawned the "Incident operations" model. Incident operations represent a series of security activities implemented to predict and prevent damage caused by incidents and adopt countermeasures to reduce the expansion of the damage once such incidents have occurred. From 2006 onwards, a new reaction scenario called inter-organization collaborative operations has been under consideration. Here, organizations coordinate, cooperate and collaborate with each other to predict and prevent damage caused by such incidents.

Such changes in incidents also require CSIRT (Computer Security Incident Response Teams) not only to be capable of "predicting and alerting from a technical point of view", "making technical adjustments" and "collaborating with external communities on the technical aspects" but also to play the following roles based on our experience, including the following technical transitions in cyber attacks.

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



!	0	▽	送信者	件名	受信日時
	0		sig@ipsj.or.jp	第11 回コンピュータセキュリティシンポジウム2008(…	2008/06/05 10…
			Microsoft Outlook Expre…	Outlook Express 6 へようこそ	2009/01/12 19:00

送信者：sig@ipsj.or.jp **宛先**：test@example.jp
件名：第11 回コンピュータセキュリティシンポジウム2008(CSS2008)

お知らせ

情報処理学会コンピュータセキュリティ研究会は，第11 回コンピュータセキュリティシンポジウム2008(CSS2008)を開催いたします．コンピュータセキュリティの基礎となる理論・技術，通信プロトコル，コンピュータアーキテクチャ，オペレーティングシステム，アプリケーション，適用事例，管理運用，さらに心理学・社会科学的考察までの幅広いセキュリティに関連する研究，技術の発展と普及，ならびに研究者，技術者相互の情報交換と協力の促進を目的として，下記の要領で論文投稿および参加を募集いたします．奮って御参加くださいますよう御案内申し上げます．本シンポジウムは，「情報セキュリティ心理学とトラスト」研究グループとの合同開催になります．

[開催要項]
開催日：2008 年10 月8 日（水）～10 月10 日（金）
会場：沖縄コンベンションセンター（沖縄）
〒901-2224 沖縄県宜野湾市真志喜4-3-1
【TEL】098-898-3000【FAX】098-898-2202

募集要項については、添付ファイルをご参照ください。

－－－－－－－－－－－－－－－－－－－－
コンピュータセキュリティシンポジウム2008（CSS2008）
―シンポジウム開催ならびに発表募集のご案内―
http://css2008.la.coocan.jp/（6 月中旬ホームページ開設予定）

2 通のメッセージ、1 通は未開封　オンライン中　Copyright Hitachi Incident Response Team. 2009.

Figure 1: Example of a targeted attack using non-suspicious E-mail.

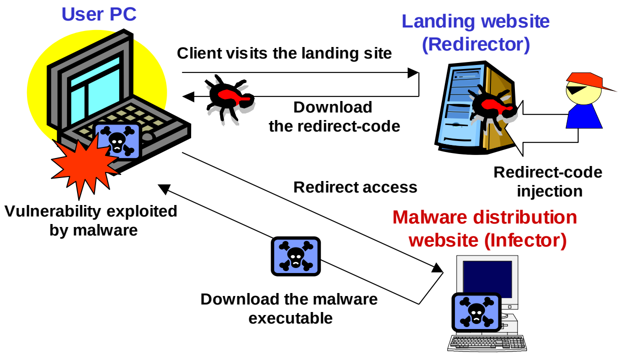


Figure 2: Example of web-based malware infection activities.

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

This document gives you an overview of the threats and vulnerabilities in 2009, as well as HIRT activities, as the HIRT annual report for 2009.

2 Overview of activities in 2009

This section focuses on HIRT activities in 2009.

2.1 Overview of threats and vulnerabilities

(1) Overview of threats

In 2009, passive (redirection) type attacks, which use websites as the basis for attacks, have become more general, as shown by the proliferation of Conficker, USB memory type malware and Gumblar, web-based malware. Along with the generalization, websites serve not only as download sites through which the web-based malware obtains new programs with other functions but also as a base from which the infection spreads. In particular, with regard to malware infection activities using website redirection, websites are now being established as an attack base that incorporates a cycle to spread infection using account capturing.

- **Conficker**

Conficker emerged in around November 2008 as a worm that exploits vulnerability (MS08-067) in Windows Server services. In December 2008, as Conficker obtained an additional function to spread infection via USB memory, infection also spread to isolated networks via physical USB memory media. The proliferation of USB memory type malware started in 2008, but the reported damage has decreased since early 2009 (Figure 3) [1]. While the number of infections detected with Conficker, a kind of USB memory type malware, is decreasing (Figure 4) [2], the Conficker Work Group reported that about 6 million PCs had been infected worldwide in term of IP addresses (Figure 5) [3].

- **Gumblar**

Gumblar is a colloquial term for web-based malware that cause damage via malware infections by redirecting users from websites with which they are familiar to the malware distribution website. This malware is named after the malware distribution website "gumblar.cn", which was used in May 2009. The following paragraphs give an overview of Gumblar's infection activities (Figure 6).

As for Gumblar damage, there have been many incidents of redirection-code injection to domestic websites from April to June in 2009. During the period October to November, PCs infected with a subspecies of Gumblar failed to start, even after powering on, and only displayed black screens. In December, there were many incidents of redirection-code injection to websites of large domestic enterprise companies (Figure 7) [4].

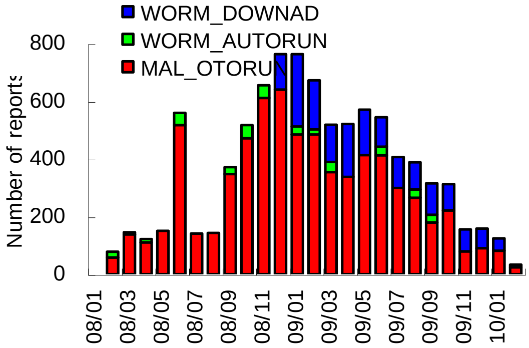


Figure 3: Number of infections with USB memory type malware (/Month) (Source: Trend Micro).

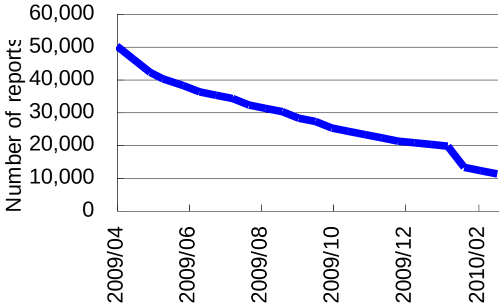


Figure 4: Number of detections with Conficker (/day) (Source: IBM Tokyo SOC).

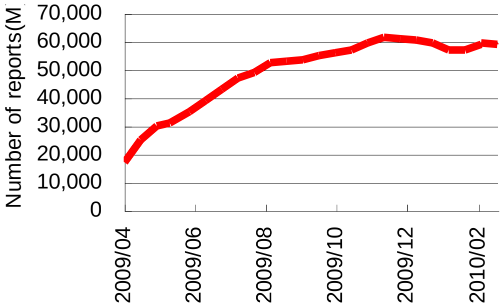
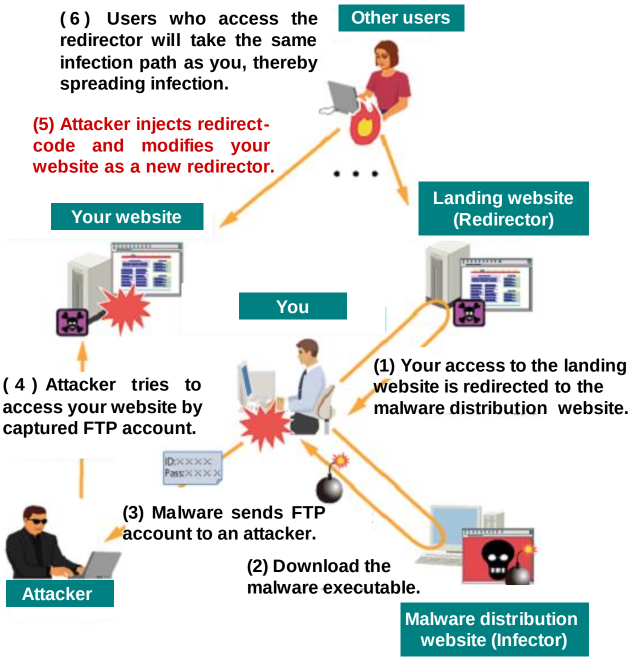


Figure 5: Number of PCs infected with Conficker A+B (/day) (Source: Conficker Work Group).


(6) Users who access the redirector will take the same infection path as you, thereby spreading infection.
Other users
(5) Attacker injects redirect-code and modifies your website as a new redirector.
Landing website (Redirector)
Your website
You
(4) Attacker tries to access your website by captured FTP account.
(1) Your access to the landing website is redirected to the malware distribution website.
ID:××××
Pass:××××
(3) Malware sends FTP account to an attacker.
(2) Download the malware executable.
Attacker
Malware distribution website (Infector)

(1) Landing website (Redirector): Guides you, who have accessed the malware distribution website that spreads malware infection.

(2) Malware distribution website (Infector): Exploit vulnerability in a program to infect your PC with Gumblar.

(3) Gumblar: Sends your FTP account information to the attacker.

(4) Attacker: Intrude into your website by your FTP account.

(5) Injects the redirect-code in your website as a new landing website (redirector).

(6) Other user: General users who access the your website will be exposed to the same attack as you, thus causing the infection to proliferate.

Figure 6: Flow of the web-based malware infection activities.

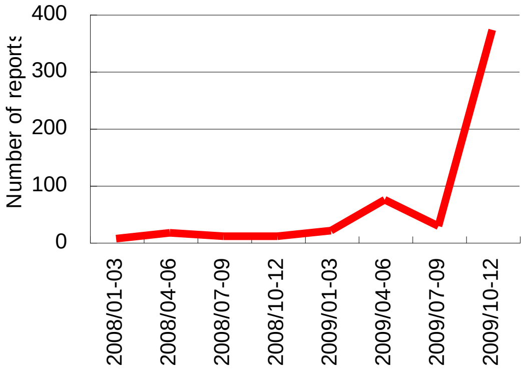


Figure 7: Changes in the number of redirect-code injection reported for websites (Source: IPA and JPCERT/CC).

(2) Overview of vulnerabilities

As for vulnerabilities, the total number entered in 2009 in the US NIST NVD (National Vulnerability Database) remains on the same level at 5,733, as shown in Figure 8. Of those specified vulnerabilities in web application software products, such as Cross Site Scripting (XSS), SQL Injection, Directory Traversal and Cross Site Request Forgeries (CSRF) accounted for 2,202 or about 38% of the total (Figure 9) [5]. In addition, of the vulnerabilities in active websites that were reported to the IPA, Cross Site Scripting (XSS) and SQL Injection accounted for approximately 50%, with the number of such reported vulnerabilities increasing (Figure 10) [6].

As the passive (redirection) type attacks, which use websites as an attack base, have become more generalized, countermeasures against vulnerabilities need to be promoted in terms of developing secure web application software products and active secure websites to avoid web-based malware intrusion activities.

In addition, the number of vulnerabilities in embedded devices that are reported to IPA tends to increase gradually, which necessitates further promotion of countermeasures against vulnerabilities lest they be included as early as the product development stage (Figure 11).

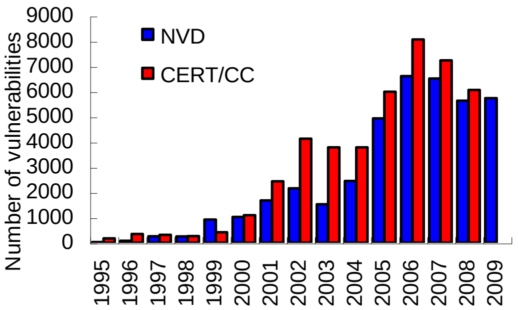


Figure 8: Changes in the number of vulnerabilities reported (Source: NIST NVD).

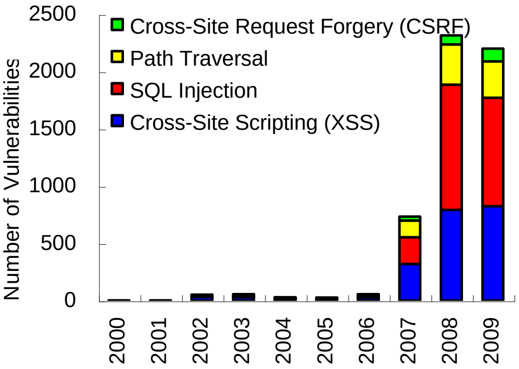


Figure 9: Changes in the number of vulnerabilities reported for software products of web application (Source: NIST NVD).

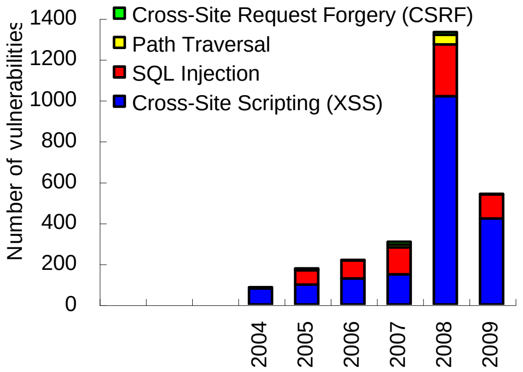


Figure 10: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC).

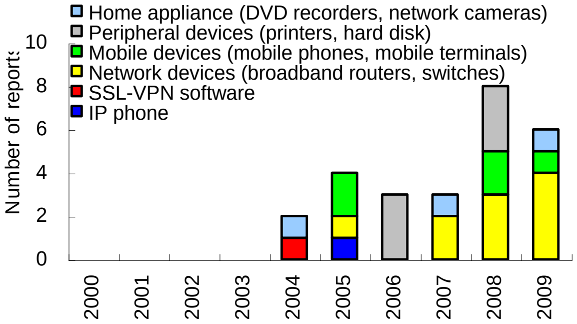


Figure 11: Changes in the number of vulnerabilities reported for embedded software products (Source: IPA, JPCERT/CC).

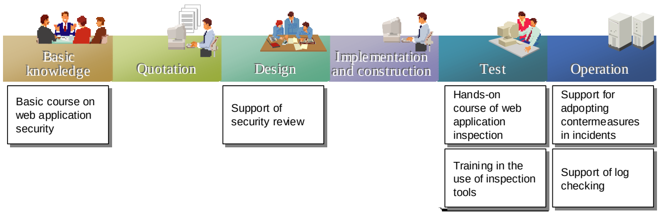

Basic knowledge
Quotation
Design
Implementation and construction
Test
Operation
Basic course on web application security
Support of security review
Hands-on course of web application inspection
Training in the use of inspection tools
Support for adpopting contermeasures in incidents
Support of log checking

Figure 12: Systematizing HIRT support activities (Web application security).

Table 1: Released publications on HIRT website.

Number	Title
HIRT-PUB09008	A survey on information leakage via P2P file exchange software environment (2009)
HIRT-PUB09007	A survey on malware circulating in a P2P file exchange software environment (2009)
HIRT-PUB09005	Estimating the number of circulation files on P2P file exchange software environment
HIRT-PUB09003	USB memory Autorun infection - Virtual experience demonstration (2)
HIRT-PUB09002	Virus attached mail of old style and new style - Virtual experience demonstration (1) -
HIRT-PUB09001	Information Security Day for 2009

2.2 HIRT activities

This subsection describes the HIRT activities in 2009.

(1) Starting product/service security support activities

In order to provide the product development processes with feedback on knowledge obtained through countermeasures against vulnerabilities and incident response activities, we have started HIRT support activities for each process. For web application security, with preceding support activities, we provided hands-on classes in the HIRT OPEN Meeting (Total 11 times, Number of participants: About 170) and security review support (Figure 12). At present, whereas it seems common sense to take security measures before releasing a website, a whole series of incidents or accidents targeting vulnerabilities in websites still occur. To cope with this situation, we invited Dr. Hiromitsu Takagi of the National Institute of Advanced Industrial Science and Technology as an instructor in July 2009 to give a lecture on viewpoints to be considered in order to ensure the security of websites and web applications.

(2) Implementing a security engineer training program

As a part of security engineer training that leverages our CSIRT activities, we received trainees from group affiliates for 6 months of training focusing on security measures of web system. Subsequently, we had the trainees cooperate with us in planning and implementing educational training on secure design for web systems for their software development engineers and system engineers.

(3) Survey on malware circulating within the P2P file exchange environment

As for the ongoing information leakage via P2P file exchange software, we need to collaborate with external organizations. Therefore we conducted a survey on this issue with Systems Development Laboratory, Hitachi, Ltd, as was performed in 2008, involving cooperation from the Secure Trusted Network Forum (P2P Research group), which participates in the “Development of Technology to Detect Information Leaks through Networks and Block the Automatic Circulation of Leaked Information”, a project commissioned by the Ministry of Internal Affairs and Communications (Table 1) [7][8]. We need to monitor the P2P file exchange environment (Winny network), where there are considerable instances of known malware causing Antinny type information leakage, and in which many fake themselves as icons resembling so-called safe content in order to tactically execute the malware.

- 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.

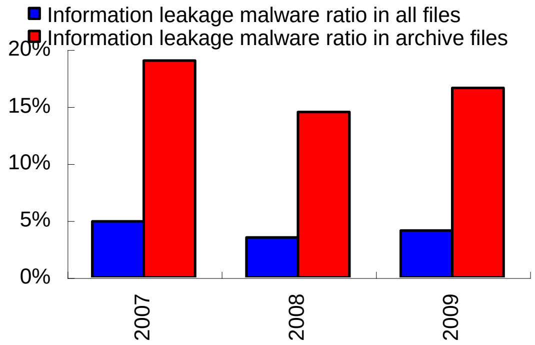
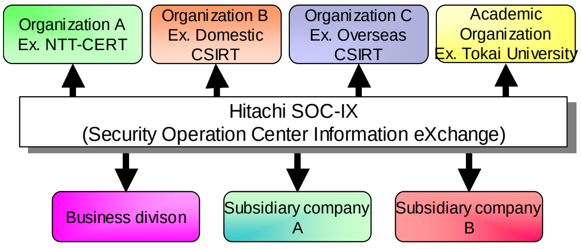
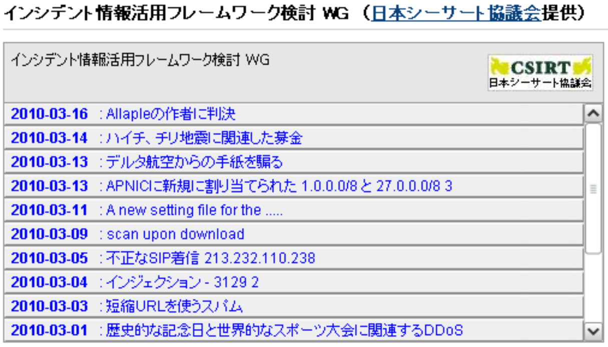


Figure 13: Changes for malware circulating in Winny that causes information leakage.



Creating a framework or mechainism 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 14: Schematic view of the Hitachi SOC-IX.



インシデント情報活用フレームワーク検討 WG （日本シーサート協議会提供）

インシデント情報活用フレームワーク検討 WG

CSIRT 日本シーサート協議会

2010-03-16 : Allapleの作者に判決
2010-03-14 : ハイチ、チリ地震に関連した募金
2010-03-13 : デルタ航空からの手紙を騙る
2010-03-13 : APNICに新規に割り当てられた 1.0.0.0/8 と 27.0.0.0/8 3
2010-03-11 : A new setting file for the .....
2010-03-09 : scan upon download
2010-03-05 : 不正なSIP着信 213.232.110.238
2010-03-04 : インジェクション - 3129 2
2010-03-03 : 短縮URLを使うスパム
2010-03-01 : 歴史的な記念日と世界的なスポーツ大会に関連するDDoS

Figure 15: Providing security information using cNotes on the Hitachi security information portal.

(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. In 2009, with a view to improving the educational menus implemented in hands-on classes in the HIRT OPEN Meeting, we have provided a drill of web application development for the NTT group in the workshop held by NTT-CERT in February.

As for the "Hitachi Security Operation Center Information eXchange (SOC-IX)" (Figure 14), a framework that allows organizations to share and jointly use the information, including observation data, required to analyze threats. We have started sending such information using cNotes (Current Status Notes) [10] for which we collaborate with a WG in the Nippon CSIRT Association that considers an incident information utilization framework to try to visually represent information based on observation data (Figure 15).

(5) Others

- We contributed an article "Vulnerability Information Needing to Be Checked" to the ITpro Computer Security Incident Response Team (CSIRT) Forum of Nikkei Business Publications.
- At the 2009 First Symposium, Riga, we identified a potential risk that may be caused by externally controlling P2P file location information (key information) and communications used by the P2P file exchange software. Therefore we reported the possibility for a third party to control an overlay network by leveraging and taking advantage of the function of the overlay network to circulate the key information [11].
- During the fifth Annual WARP Forum 2009, we reported on WARP activities in Japan using slides and video letters [12].

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

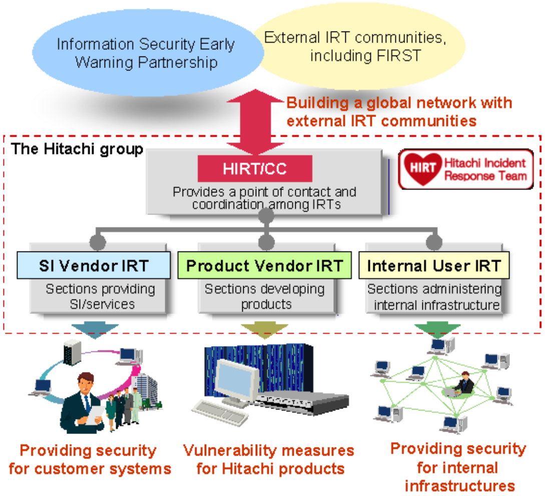

Information Security Early Warning Partnership
External IRT communities, including FIRST
Building a global network with external IRT communities
The Hitachi group
HIRT/CC
Provides a point of contact and coordination among IRTs
HIRT Hitachi Incident Response Team
SI Vendor IRT
Sections providing SI/services
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 - 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 3: Phases until the organization was formed.

Phase	Overview
April 1998	We started CSIRT activities as a project to establish a Hitachi CSIRT framework.
1st phase Establishing the Internal User IRT (1998 - 2002)	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.

As shown in Table 3, we experienced four phases before four IRTs had been established. After the roles and functions of the three IRTs had been roughly decided, the HIRT/CC was formed as a coordinator for the internal and external IRTs. In addition, each phase has a trigger that causes a corresponding IRT to be formed. For example, Multiple Vulnerabilities in Many Implementations of SNMP [13], as reported by CERT/CC, worked as a trigger to form the Product Vendor IRT in the second phase, while in the third, the start of an "Information Security Early Warning Partnership" worked as a trigger to establish the SI Vendor IRT.

3.2 Positioning of the HIRT/CC

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

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) ➢ 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 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) ➢ 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 Systems Development Laboratory (for P2P observation, etc)

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.

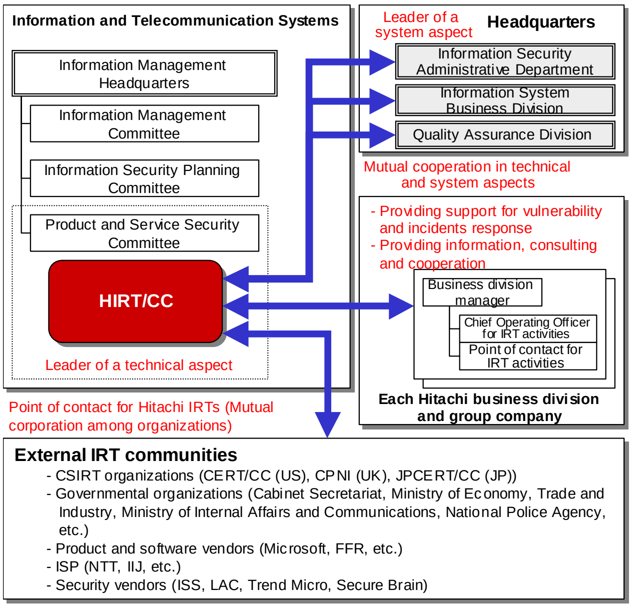

Information and Telecommunication Systems
Information Management Headquarters
Information Management Committee
Information Security Planning Committee
Product and Service Security Committee
HIRT/CC
Leader of a technical aspect
Leader of a system aspect
Headquarters
Information Security Administrative Department
Information System Business Division
Quality Assurance Division
Mutual cooperation in technical and system aspects
- Providing support for vulnerability and incidents response
- Providing information, consulting and cooperation
Business division manager
Chief Operating Officer for IRT activities
Point of contact for IRT activities
Each Hitachi business division and group company
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 (ISS, LAC, Trend Micro, Secure Brain)

Figure 17: Positioning of the HIRT/CC.

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 ➢ 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) [*]
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

*) 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 Information Security Administrative Department and Quality Assurance Division.

Table 6: Classification of security information issued by HIRT.

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

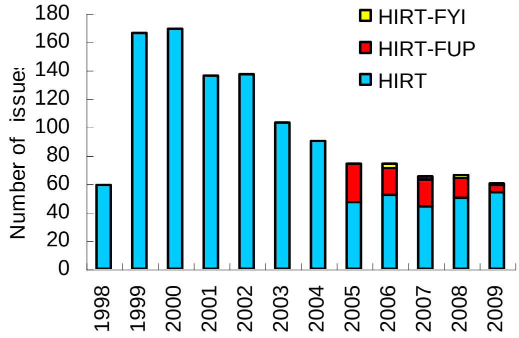


Figure 18: Number of issues of security information by ID number.

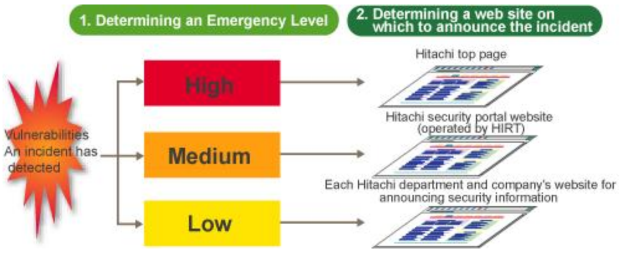

1. Determining an Emergency Level
2. Determining a web site on which to announce the incident
Vulnerabilities An incident has detected
High
Medium
Low
Hitachi top page
Hitachi security portal website (operated by HIRT)
Each Hitachi department and company's website for announcing security information

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

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).

4 Activity summary from 1998 to 2008

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

4.1 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” [14], 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. [15]

(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) [16].

(5) Lecture meeting
April 2008: "Management of High Reliability Organizations" [17] by Prof. Aki Nakanishi, the Faculty of Business Administration, Meiji University.

(6) Others
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.

4.2 Year 2007

(1) Starting Hands-on security training in HIRT OPEN Meetings
We held HIRT OPEN Meetings focusing on Hands-on security training twice in March and June 2007 in order for web application developers to implement the guideline "Web Application Security Guide" more practically.

(2) Founding the Nippon CSIRT Association
In order to develop a system based on a strong trusting relationship among CSIRTs that can successfully and promptly react to events that single CSIRTs find it difficult to solve, we founded the Nippon CSIRT Association with IIJ-SECT (IIJ), JPCERT/CC, JSOC (LAC), NTT-CERT (NTT) and SBCSIRT (Softbank) in April 2007 [18].

(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 [19].

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

(5) Lecture meetings

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

4.3 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) Lecture meetings

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

(7) Other activities

- Starting to sign a digital signature to technical documents (PDF files) issued from HIRT [20].

4.4 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 [21]. 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 February 2010, sixteen teams from Japan had 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), KKCSIRT (Kakaku.com), MIXIRT (Mixi), NCSIRT (NRI Secure Technologies), NISC (National Information Security Center), NTT-CERT (NTT), Rakuten-CERT (Rakuten), RicohPSIRT (Ricoh), SBCSIRT (Softbank) and YIRD (Yahoo) (See Figure 20).

(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 21). We also created "Guidance for Providing Security Information from Websites to External Users, V1.0".

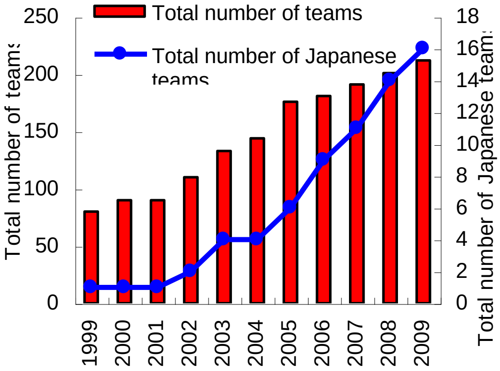
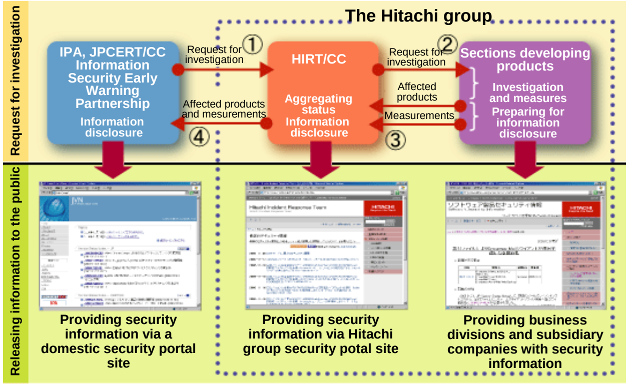


Figure 20: Changes in the number of members of FIRST.



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

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

(3) Strengthening the domestic partnership for CSIRT activities

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.

4.5 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 [22][23].

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) [24].

(2) Enhancing web application security

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

(3) Lecture meetings

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

4.6 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 [25].

(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 ([26], [27] and [28]), 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.

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 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

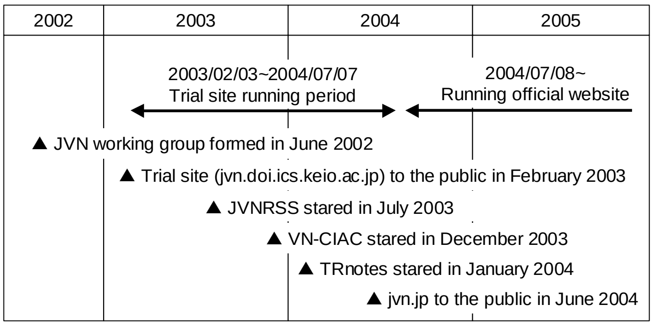

2002
2003
2004
2005
2003/02/03~2004/07/07
Trial site running period
2004/07/08~
Running official website
▲ JVN working group formed in June 2002
▲ Trial site (jvn.doi.ics.keio.ac.jp) to the public in February 2003
▲ JVNRSS stared in July 2003
▲ VN-CIAC stared in December 2003
▲ TRnotes stared in January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

Figure 22: Building and running a JVN trial site.

4.7 Year 2002

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

SNMP vulnerability [13] 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 [29]. 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 [30].

(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 22)[31][32]. With the implementation of the "Standard for Handling Information Related to Vulnerabilities in Software, etc." in July 2004, the roles of the trial site were transferred to Japan Vulnerability Notes (JVN), a site releasing information on reported vulnerabilities (http://jvn.jp/en/index.html).

4.8 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 23), 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.

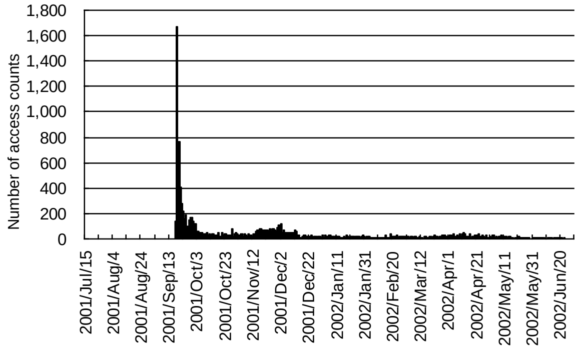


Figure 23: Changes in the number of Nimda log counts found during the observation period (for Nimda).

4.9 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” [33] for vulnerability. It provides the Severity Metric indicating the severity of vulnerability [34]. Common Vulnerabilities and Exposures (CVE) classifies information security vulnerabilities into “Vulnerabilities” and “Exposures” and focuses on the former [35]. 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 [36], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [37] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

4.10 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 24).

4.11 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.).

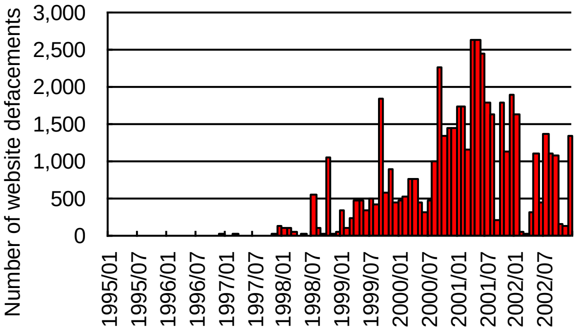


Figure 24: Changes in the number of websites defacements

(2) Lecture meetings
On June 25 - 26, 1998, we provided “Network security” training for Hitachi. We invited an US security expert who had also participated in the US Security Conference DEFCON [38] as a speaker as an instructor.

5 Conclusion

The cyber attack activities have become increasingly systematic, and the incidents that derive from such activities are gaining in complexity. Such new threats can be successfully addressed only by combining the abilities of each organization to observe, analyze and address the situation.

With changes in the incident situation in mind, HIRT will promote activities to deploy measures early in the process to catch subsequent threats. We will continue to establish a cooperative relationship that can contribute to international measures against vulnerabilities and incident response activities, including inter-organizational collaboration; allowing several CSIRT members to address new threats in close collaboration, and visual representation based on observation data.

(March 23, 2010)

References

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

2) IBM Tokyo SOC Report: Detection status of Conficker worms (April 2009 - February 2010), https://www.ibm.com/blogs/tokyo-soc/entry/conficker-201002

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

4) JPCERT/CC Alert 2010-01-07: Web sites compromise and Gumblar attacks growth continue, http://www.jpcert.or.jp/at/2010/at100001.txt

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

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

7) 2009 Survey on information leakage via P2P File Exchange Software Environment (2009/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html

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

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

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

11) Feasibility Study of DoS attack with P2P System (2009/1), http://www.first.org/events/symposium/riga-2009/program/

12) Annual WARP Forum Report September 2009 (2009/9), http://www.warp.gov.uk/Index/Forum/5th Annual WARP Forum v1.0.pdf

13) 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

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

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

16) 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

17) Information-Technology Promotion Agency, Japan: High Reliability Organization Requirements for Critical Infrastructures (2008/2), http://www.ipa.go.jp/security/event/2007/infra-sem/pdf/20080220MEIJI-Nakanishi_sama.pdf

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

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

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

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

22) 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

23) Information-Technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline (2008/7), http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html#Partnership

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

25) 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

26 Organization for Internet Safety: Guidelines for Security Vulnerability Reporting and Response V2.0 (2004/9), http://www.symantec.com/security/OIS_Guidelines%20for%20responsible%20disclosure.pdf

27 Information-Technology Promotion Agency, Japan: Research Reports on Policy for Security Vulnerability Information Disclosure, http://www.ipa.go.jp/security/awareness/vendor/vulnerability200309012.pdf

28 LAC Corporation: Policy for Vulnerability Reporting and Disclosure (2003/8), http://www.lac.co.jp/info/advisory/pdf/vulnerability_reporting_and_disclosure.pdf

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

30) 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

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

32) Deploying JP Vendor Status Notes (JVN) for Dissemination of Security Information Throughout Japan (2005/5), http://www.hitachi.com/rd/sdl/people/jvn/

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

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

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

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

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

38 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, and vice chief of the steering committee for the Nippon CSIRT Association.