Hitachi Incident Response Team
2016.11.21 11:42:41 +09'00'

# HIRT: Annual Report 2015

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

OMORI BELLPORT Tower D, 6-26-3 Minamioi, Shinagawa, Tokyo, Japan 140-0013

## 1 Introduction

When a large-impact incident occurs, great change in the counterapproach is also seen. In 2006 when information leaks occurred in file-sharing software, thin client terminals were adopted. In 2011 when defense industry and other enterprise companies were hit by targeted attacks, egress countermeasures were introduced. Then in 2015 when a rash of similar cyber attacks occurred, there was renewed emphasis on the risk decremental approach of access blocking until safety can be confirmed (Figure 1). Here, the intent of the approach of access blocking until safety is confirmed is to shorten the potential threat period and service interruption time (Figure 2). In other words, the attacker's cyber attack speed is tracked.

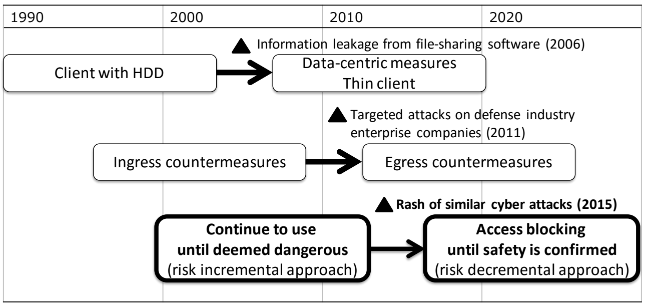

1990
2000
2010
2020
Information leakage from file-sharing software (2006)
Client with HDD
Data-centric measures
Thin client
Targeted attacks on defense industry enterprise companies (2011)
Ingress countermeasures
Egress countermeasures
Rash of similar cyber attacks (2015)
Continue to use until deemed dangerous (risk incremental approach)
Access blocking until safety is confirmed (risk decremental approach)

Figure 1: Change in counterapproach.

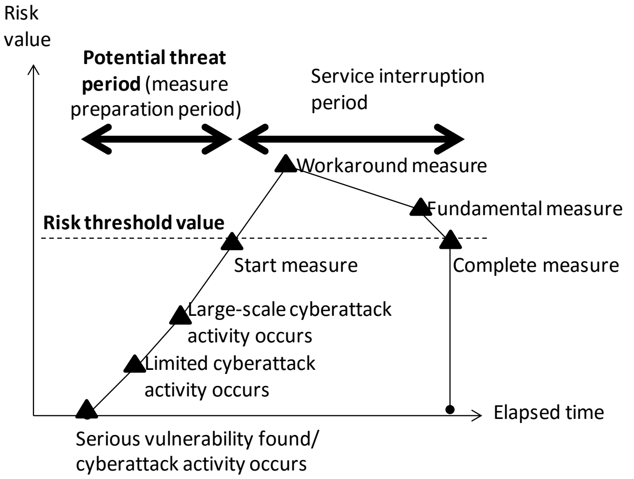

Risk value
Potential threat period (measure preparation period)
Service interruption period
Workaround measure
Fundamental measure
Risk threshold value
Start measure
Complete measure
Large-scale cyberattack activity occurs
Limited cyberattack activity occurs
Serious vulnerability found/ cyberattack activity occurs
Elapsed time

Figure 2: Potential threat period.

Furthermore, with a targeted attack such as an APT (Advanced Persistent Threat: advanced hidden attack aimed at a specific target), which has drawn attention since 2010, the successful result of an invasive activity will act as a platform for use in the next targeted attack and/or be tied to an invasion of a specific organization, which is the ultimate target. In short, security measures and incident responses are composed in no small part to affect other organizations/be affected by other organizations; therefore, a speed-up in professional, practical collaboration between CSIRTs will be sought as well.

The specific role of HIRT (Hitachi Incident Response Team) as a CSIRT (Computer/Cyber Security Incident Response/Readiness Team) remains, as before, to lead the cyber security measure activities of the Hitachi Group, through vulnerability countermeasures - activities to eliminate vulnerabilities that could pose a threat for cyber security, and incident responses - activities to avert and resolve cyber attacks when they occur. Further, we consider that the requirements for CSIRTs in carrying out vulnerability countermeasures and incident responses are to possess the capabilities for "predicting and altering from a technical point of view", "making technical collaboration" and "collaborating with external communities on the technical aspects".

We are not envisioning special requirements here. It is a matter of making use of experience in incident operations (the series of security measure activities implemented in order to predict and prevent damage from incidents and to lessen the expansion of damage after incidents occur) so as to "catch any signs of future threats and take actions as early as possible". As an organization that possesses these roles, HIRT leads the way in vulnerability countermeasures for products and services and in incident responses for malware infection damage and information leakage, besides shouldering duties as the Hitachi Group's integrated CSIRT liaison organization.

This report will introduce a summary of the threats and vulnerabilities, and the activities of HIRT, in 2015.

## 2 Overview of activities in 2015

This section focuses on the threats and vulnerabilities, and HIRT's activities, in 2015.

### 2.1 Overview of Threats and Vulnerabilities

**(1) Overview of Threats**

The known threats like targeted attack and website compromised actions have continued to cause damage.

The feature of 2015 in terms of incidents was that damage by malicious programs that target online banking become serious. Meanwhile, the following methods became steady occurrences: ransomware attacks, which hold the files in a PC to ransom, and amplification attacks, which use amplification of request/response messages (also known as reflection attacks).

- **Internet Banking**

According to a National Policy Agency report, there were a total of 1,495 cases of fraudulent money transfer damage occurred in Japan in 2015 (0.8 times more than in 2014), amounting to some 3.073 billion yen in total damage (1.05 times the 2014 level; Figure 3) [1]. Characteristics of these cases were a rapid rise in damage to credit union corporate accounts, and record amounts of damage related to accounts in the name of corporations.

- **Website Cyberattack Activities**

Incidents of website alteration in Japan with the intention of infecting the sites with redirecting malware have been continuing since March 2013. Looking at the number of reported cases, one sees that these alterations are continuing to occur in larger quantities than the Gumblar incidents that took place in 2009 (Figure 4).

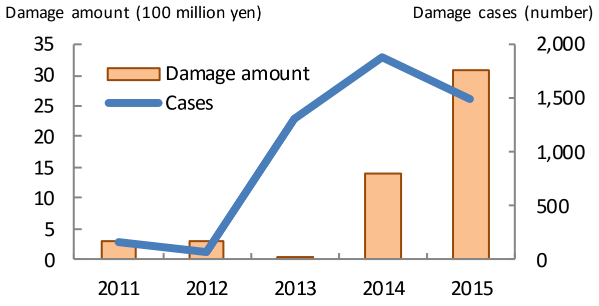


Figure 3: Fraudulent money transfers by year and damage. (Source: National Police Agency)

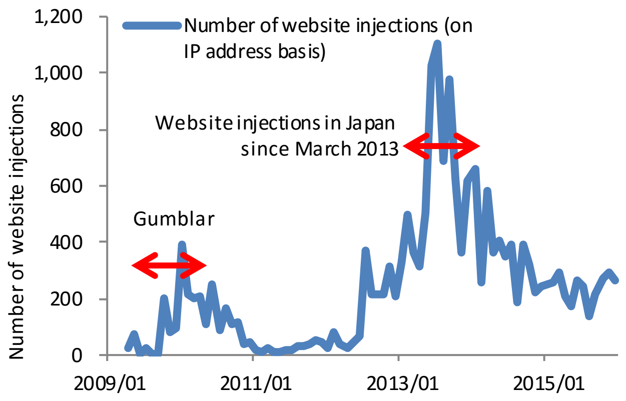


Figure 4: Number of reported cases of website injections. (Source: JPCERT/CC).

- **Ransomware**

"Ransomware" is a generic term for malicious programs that hold the files in a PC to ransom. Since 2015 in particular, ransomware that encrypts the files in a PC and demands money in return for decrypting them has increased sharply (Table 1). According to a report by Symantec [2], 64% of the ransomware was the crypto type, which encrypts a PC's files, while 36% was the locker type, which restricts access to a PC. Japan is number two in number of crypto ransomware cases detected. Also, according to a report by McAfee [3], ransomware cases increased 127% from 2014, with approximately 1.2 million new samples discovered in the second quarter of 2015 alone.

If important files are encrypted by ransomware, business continuity can be directly impacted; therefore, it is necessary not only to acquire backup but to direct attention to recovery from backup.

- **Reflection Attacks**

DDoS attack peak traffic is on an increasing trend (Figure 5), and the threat from DDoS attacks is ongoing. According to a report by Arbor Networks [4], over 20% of the attacks exceed 1 Gbps, and attack traffic from DrDoS (Distributed Reflective Denial of Service) attacks is increasing. Attacks that use the SSDP (Simple Service Discovery Protocol) of equipment that supports UPnP (Universal Plug and Play) are particularly prominent.

Table 1: Notable Ransomware since 2013.

| Year/Month | | Ransomware |
|---|---|---|
| 2013 | September | CryptoLocker |
| | December | CryptoLocker 2.0 |
| 2014 | Feburay | CryptoDefense |
| | March | CryptoWall 1.0 |
| | May | ANDROIDOS_LOCKER.HBT (Android Env.) |
| | July | CTB-Locker |
| | August | TorrentLocker |
| | October | CryptoWall 2.0 |
| | November | Coinvault |
| 2015 | January | CryptoWall 3.0 |
| | Feburay | TeslaCrypt |
| | March | CRYPVAULT |
| | July | TeslaCrypt 2.0 |
| | September | Chimera, TeslaCrypt 2.1 |
| | November | CryptoWall 4.0, Linux.Encoder (Linux Env.) |
| | December | TeslaCrypt 2.2 |

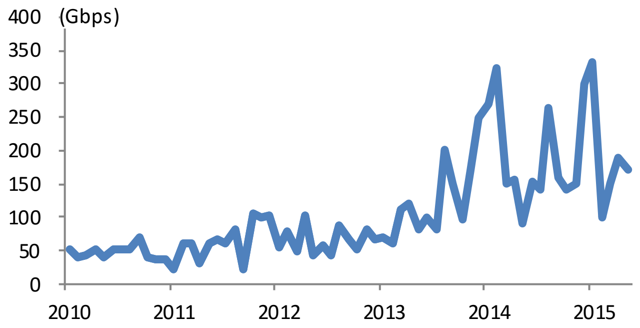


Figure 5: Trend in DrDoS attack peak traffic. (Source: Arbor Networks) [4]

Also, SSDP and NTP reflection attacks and Wordpress XML-RPC reflection attacks have been utilized even in attacks called DD4BC (DDos for Bitcoin), which demand Bitcoins as ransom to stop DDoS attacks that are intended to cause service interruptions [5]. Damage from DD4BC attacks in other countries became noticeable starting in mid-2014, and damage was reported in Japan, too, in 2015.

### (2) Overview of Vulnerabilities

- **Overall Trend**

The total number of vulnerabilities entered in the NIST NVD (National Vulnerability Database) [6] was 6,488 in 2015. About 20% (1,319) of the vulnerabilities were in web software application products (Figure 6). Breaking these down, cross-site scripting (XSS) and SQL injection account for about 70%, which is a continuing trend (Figure 7). Likewise, some 60% of the vulnerabilities in operational websites that were reported to the IPA are accounted for by cross-site scripting (XSS) and SQL injection, though this percentage is lower than most years (Figure 8) [7].

- **Industrial Control System Products**

The ICS-CERT (Industrial Control System-CERT) issued 10 alerts and 126 advisories (Figure 9).

Vulnerabilities arising from stack buffer overflow (CWE-121), cross-site scripting (CWE-79), and inadequate verification of input data (CWE-20) were the most commonly reported types, followed by problems associated with hard-coded passwords (CWE-798). There were 10 reports of vulnerabilities in Device Type Manager (DTM) products that utilize the Highway Addressable Remote Transducer (HART) Protocol, which superimposes and transmits digital signals over analog transmission signals. Also, in the healthcare domain, there were 6 reports of vulnerabilities in infusion systems.

## 2.2 HIRT Activities

This subsection describes the HIRT activities in 2015.

### (1) Improvement of Hitachi Group CSIRT activities (Phase 3)

In 2010, we started improvements of Hitachi Group CSIRT activities with the goal of "instilling incident operations into the whole Hitachi Group" (Figure 11). In 2015, the sixth and final year of the activities, we took regulation-strengthening steps to make our virtual, horizontal incident response framework (HIRT Center - IRT - IRT supporting staff) a reality. Specifically, in the relevant regulations for security incident countermeasures, we stipulated that the role of the Division IRT is "the construction and maintenance of the security response system," based on future operations.

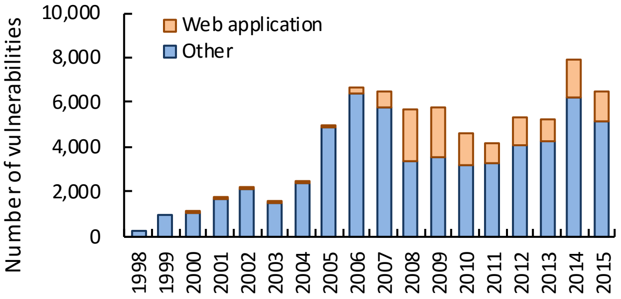


Figure 6: Number of vulnerabilities reported (Source: NIST NVD).

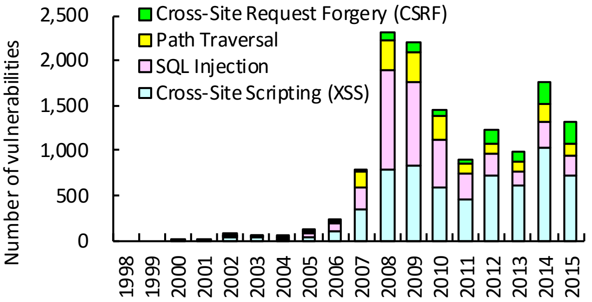


Figure 7: Changes in the number of vulnerabilities reported for software products of web-based application (Source: NIST NVD).

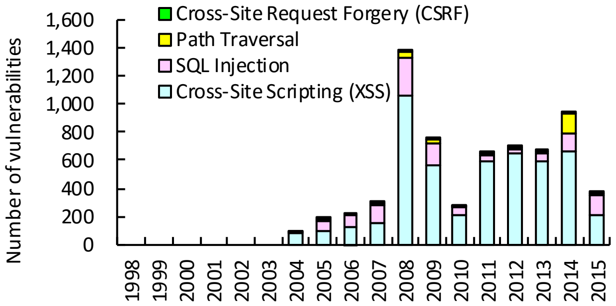


Figure 8: Changes in the number of vulnerabilities reported for websites (Source: IPA and JPCERT/CC).

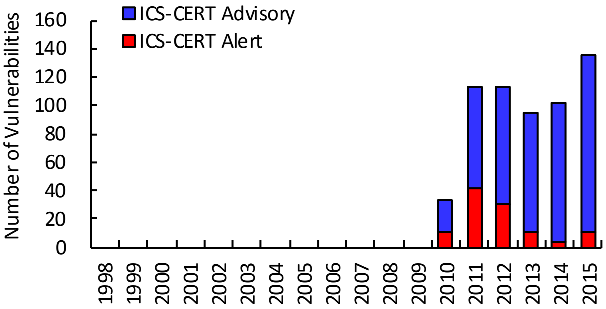


Figure 9: Changes in the number of control system vulnerabilities reported (Source: ICS-CERT).

Also, to pass on technical skills, we held HIRT OPEN Meetings (Technical Meetings) (Table 2) [*a], and held Advanced HIRT OPEN Meetings in the Omika district with IRT supporting staff. In addition, utilizing the HIRT Laboratory Project Room, which opened in 2014 inside the Yokohama Research Laboratory, we constructed a virtual environment of the organization's internal networks to investigate targeted attacks and other cyber attacks. There, we have begun to engage in "Observation of Threat Actors Activities" (Figure 10), recording and analyzing the behavior of a threat actor following intrusion, and in the practical use of cyber security information between organizations utilizing STIX/TAXII [*b] [8].

### (2) Trial IRT activities for individual domains

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

In order to put into practice the three-tiered cycle for incident response and readiness (Figure 12) that incorporates the perspectives of individual business domains, HIRT-FIS (Financial Industry Information Systems HIRT) engaged as main actor in internal/external readiness activities for the financial domain.

Table 2: HIRT OPEN Meeting (Technical meeting) in 2015.

| Month | Outline |
|---|---|
| January | Advanced HIRT OPEN Meeting |
| | Hands-on forensic investigation |
| Feburary | [External instructor]<br>Yukata Kokubu, Takeshi Terada (Mitsui Bussan Secure Directions)<br>*"From the Standpoint of Vulnerability Finder"* |
| March | Advanced HIRT OPEN Meeting @Omika |
| April | Seminar on Technical Countermeasures for External Server Vulnerability Surveys |
| May | [External instructor]<br>Jack YS Lin (JPCERT Coordination Center (General Foundation))<br>*"China: Emerging Cyber Power?"* |
| Auguest | Advanced HIRT OPEN Meeting |
| September | Hands-on Windows event log investigation |

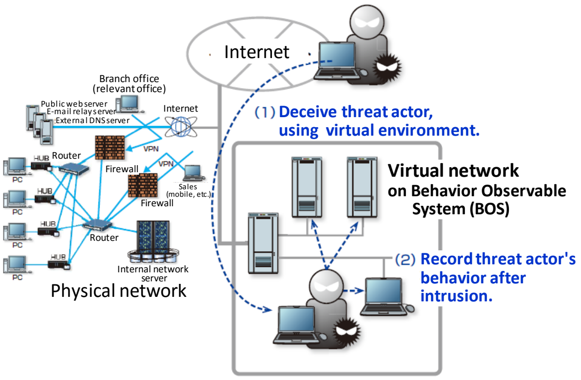
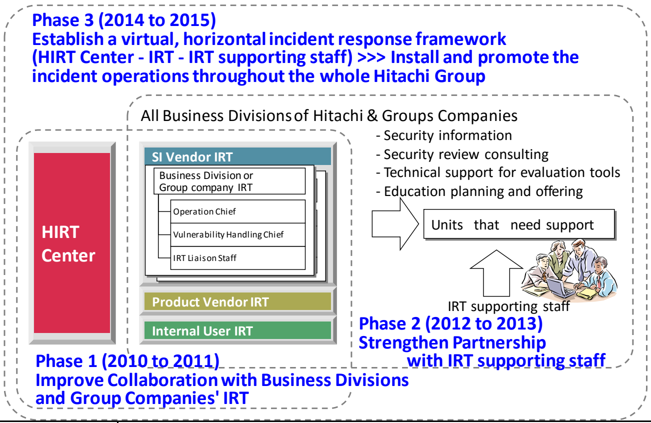


Figure 10: BOS (Behavior Observable System) for Observable Threat Actors Activities.


Phase 3 (2014 to 2015)
Establish a virtual, horizontal incident response framework
(HIRT Center - IRT - IRT supporting staff) >>> Install and promote the
incident operations throughout the whole Hitachi Group
All Business Divisions of Hitachi & Groups Companies
HIRT
Center
SI Vendor IRT
Business Division or
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 staff
Phase 2 (2012 to 2013)
Strengthen Partnership
with IRT supporting staff
Phase 1 (2010 to 2011)
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 and 2) and entity collaboration model (Phase 3). |

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

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

[*b] STIX (Structured Threat Information eXpression) is an XML specification that describes cyber attack activities. TAXII (Trusted Automated eXchange of Indicator Information) is a procedure for exchanging threat information. They are attracting attention as specifications for information infrastructure.

In the HIRT-FIS internal activities, they proceeded with gathering and analyzing financial-related security information and issuing HIRT-FIS reports. In the external activities, they held view-exchange meetings with financial-related CSIRTs, and tried out weekly dissemination of HIRT-FIS Security Notes in order to put out feelers for collaboration with financial-related CSIRTs (Table 3, Figure 13). The HIRT-FIS Security Notes are simple reports that cover subjects such as financial-related security incidents that have arisen in Japan or overseas, relevant regulations and so forth.

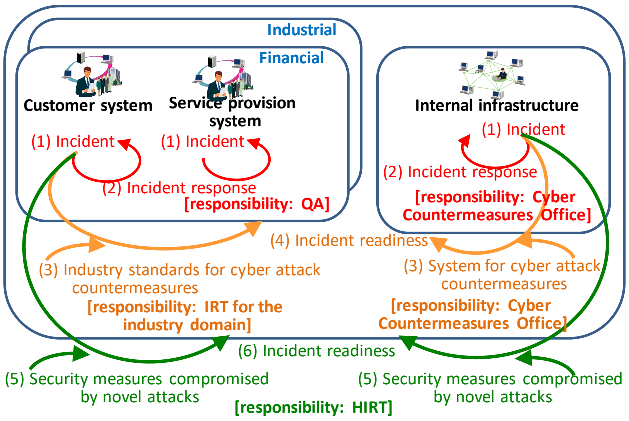
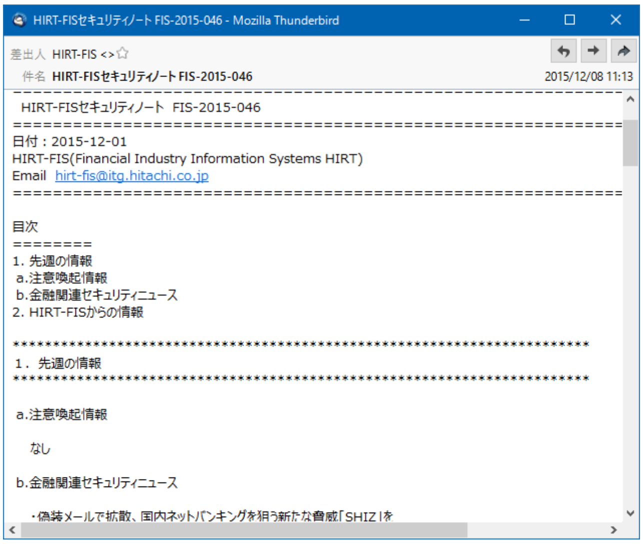

Industrial
Financial
Customer system
Service provision system
(1) Incident
(1) Incident
(2) Incident response
[responsibility: QA]
Internal infrastructure
(1) Incident
(2) Incident response
[responsibility: Cyber Countermeasures Office]
(4) Incident readiness
(3) Industry standards for cyber attack countermeasures
[responsibility: IRT for the industry domain]
(3) System for cyber attack countermeasures
[responsibility: Cyber Countermeasures Office]
(6) Incident readiness
(5) Security measures compromised by novel attacks
(5) Security measures compromised by novel attacks
[responsibility: HIRT]

Figure 12: System view of "Three-tiered cycle for Incident Response and Readiness" approach.

Table 3: HIRT-FIS Security Notes.

| Item | 2013 | 2014 | 2015 |
|---|---|---|---|
| Number issued | 10 Notes | 48 | 48 |
| Number of recipients | 4 persons | 9 | 35 |
| Number of receiving organizations | 2 organizations | 5 | 22 |


HIRT-FISセキュリティノート FIS-2015-046 - Mozilla Thunderbird
差出人 HIRT-FIS <>
件名 HIRT-FISセキュリティノート FIS-2015-046
2015/12/08 11:13

```
 HIRT-FISセキュリティノート  FIS-2015-046
==================================================================
日付：2015-12-01
HIRT-FIS(Financial Industry Information Systems HIRT)
Email  hirt-fis@itg.hitachi.co.jp
==================================================================

目次
========
1. 先週の情報
 a.注意喚起情報
 b.金融関連セキュリティニュース
2. HIRT-FISからの情報

**********************************************************************
 1． 先週の情報
**********************************************************************

 a.注意喚起情報

   なし

 b.金融関連セキュリティニュース

   ・偽装メールで拡散、国内ネットバンキングを狙う新たな脅威「SHIZ」を
```

Figure 13: Example of the HIRT-FIS Security Notes that are disseminated weekly to financial-domain CSIRTs.

### (3) Strengthening of Partnership with the CSIRT Community

We support membership in the Nippon CSIRT Association (Table 4) and, in cooperation with the SSH Server Secure Configuration Working Group, issued "SSH Server Secure Configuration Guide V1.0" [9].

Table 4: Support for membership in Nippon CSIRT Association.

| Approval | Team Name |
|---|---|
| March 2015 | MY-SIRT (Meiji Yasuda Life Insurance Company) |
| October 2015 | AHIRU (Aflac) |
| November 2015 | MELCO-CSIRT (Mitsubishi Electric Corporation) |

### (4) Eleventh "IISEC Information Security Culture Award"

After receiving recognition for a number of constructive activities, such as launching an in-house CSIRT ahead of other companies and being the first Japanese manufacturer to join the international forum FIRST in the same field, we received the Institute of Information Security's "IISEC Information Security Culture Award" [10].

### (5) Other activities

- Participation in MWS (anti Malware engineering workshop) 2015.
  We took part in this workshop with the aim of supporting research activities for malware countermeasures and contributing, through such support, to the formation of the next-generation CSIRT community.
- Contributed an article on vulnerability countermeasures titled "*Vulnerability Information to Keep in Mind*", to the ITpro CSIRT Forum held by Nikkei Business Publications, Inc. [11].

## 3 HIRT

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

### 3.1 Organizational Model

We have adopted an organizational model that consists of four IRTs (Figure 14 and Table 5). From the perspective of incident response, there are three IRTs for the Hitachi Group's corporate activities; Product Vendor IRT; SI Vendor IRT, and Internal User IRT; each corresponding to one of the IRT's aspects: the Product Vendor IRT corresponds to the aspect of developer of products such as information systems and control systems, the SI Vendor IRT to that of a system integrator/service provider that uses those products, and the Internal User IRT to that of an internet user that operates and manages its own enterprise. By adding to these a fourth IRT - the HIRT/CC (HIRT

Coordination Center), which carries out coordination work among the others - a model is obtained which we considered would be able to implement efficient and effective security measure activities that achieve collaboration among the IRTs, while making clear their individual functions. The name "HIRT" signifies the incident operation activities promoted by the Hitachi Group as a whole, in the broad sense, and signifies the HIRT/CC (HIRT Center) in the narrow sense.

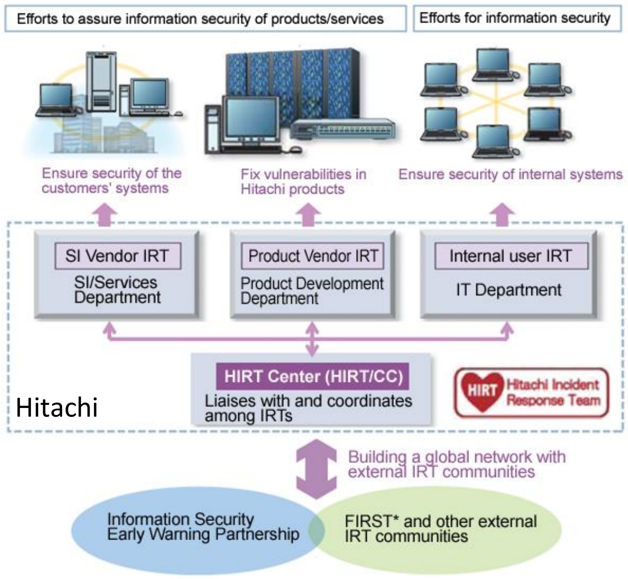

Efforts to assure information security of products/services
Efforts for information security
Ensure security of the customers' systems
Fix vulnerabilities in Hitachi products
Ensure security of internal systems
SI Vendor IRT
SI/Services Department
Product Vendor IRT
Product Development Department
Internal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

Figure 14: Four IRTs as an organizational model.

Table 5: 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. |

In fact, four phases (set forth in Table 6) had to be gone through in order to put the four IRTs in place. For each phase, there was an "impetus" that encouraged organizational formation. For instance, the impetus for the second phase - establishing of the Product Vendor IRT - was the fact that the vulnerability in SNMP [12] reported by CERT/CC had affected large numbers of Hitachi products. The impetus for the third phase - establishing of the SI Vendor IRT - was the commencement of the Information Security Early Warning Partnership. The HIRT Center was set up to play the role of coordinator inside Hitachi and with external entities, after the other three IRTs had largely taken shape.

Table 6: Phases until the organization was formed.

| Phase | Overview |
|---|---|
| April 1998 | We started CSIRT activities as a project to establish a Hitachi CSIRT framework. |
| 1st phase<br>Establishing the Internal User IRT<br>(1998 - 2002)<br><Establishment> | In order to run a Hitachi CSIRT on a trial basis, we formed a cross-sectional virtual team within the Hitachi group to start mailing list based activities. Most of the members comprised internal security experts and those from sections administering internal infrastructures. |
| 2nd phase<br>Establishing the Product Vendor IRT<br>(From 2002 -)<br><Establishment> | In order to start conducting activities seriously as a Hitachi CSIRT, the sections developing products played a central role in establishing an organizational structure of the Product Vendor IRT with related business sites through cooperation from internal security experts, the sections administering internal infrastructures, the sections developing products and the Quality Assurance Department. |
| 3rd phase<br>Establishing the SI Vendor IRT<br>(From 2004 -)<br><Establishment> | We started to form an SI Vendor IRT with the sections providing SI/services. In order to swiftly implement proactive measures against vulnerabilities, as well as reactive measures against incidents, via partnership with Internet communities, we started to form HIRT/CC, which provides a point of contact for external organizations and enhances coordination among Internal IRTs. |
| 4th phase<br>(October 2004)<br><Establishment> | We established the HIRT/CC. |
| 1st phase<br>(2010-2011)<br><Improvement> | Improvements of Hitachi group CSIRT activities<br>**Goal: instilling incident operation into the whole Hitachi Group** |
| 2nd phase<br>(2012-2013)<br><Improvement> | |
| 3rd phase<br>(2014-2015)<br><Improvement> | |

## 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 technical and institutional aspect in cooperation with the IT & Security Strategy Division, Information Technology Division and Quality Assurance Division. Moreover, it also includes helping each business division and group company implement proactive security measures against vulnerabilities, as well as reactive measures against incidents, and promoting security measures through partnerships among organizations as a point of contact for CSIRT activities in the Hitachi group (Figure 15).

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.

Table 7: (Internally) promoting projects.

| Category | Overview |
|---|---|
| Collecting, analyzing and providing security information | - Promoting Information Security Early Warning Partnership (Information concerning proactive measures against vulnerabilities, as well as reactive measures against incidents/horizontal deployment of know-how)<br>- Building a wide-area observation network based on the concepts of the Hitachi Security Operation Center Information eXchange (SOCIX) |
| Promoting proactive measures against vulnerabilities, as well as reactive measures against incidents for products/services | - Strengthening of collaboration with IRT contact points of business divisions and group companies (Phases 1 and 2<br>- Passing on of techniques for the incident operation<br>- Promoting the publication of security information from external websites using the Security Information Integration Site |
| Enhancing security technology for products/services | -- Establishment of processes for building-in of security (approach from the three perspectives of specifications, codes and configurations, and in addition move ahead with creating precedents in control devices and systems) |
| Developing a framework for research activities | - Developing a framework for joint research with the Yokohama Research Laboratory |

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 diversity of equipment in the information and control systems.

## 3.3 Main Activities of HIRT Center

The main activities of the HIRT center currently being promoted include CSIRT activities for internal organizations (Table 7) and those for external organizations (Table 8). The internally-oriented CSIRT activities comprise issuing alerts and advisories that embody the know-how obtained through gathering and analyzing security information. Besides those, we are currently engaged in activities to feed such knowledge back into product development processes in the form of various guidelines and support tools.

HIRT security information in internally-oriented alerts and advisories has been broken down into two types since June 2005. One is HIRT security information that aims to distribute alerts and hot topics widely, and the other is HIRT-FUP information, which is used to request individual sections to take counter-action. This distinction is for the sake of information propagation and priority ranking. (Table 9 and Figure 16). To communicate information efficiently, we condense it to reduce the number of information items and release it in tandem with the IT & Security Strategy Division and the Quality Assurance Division.

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

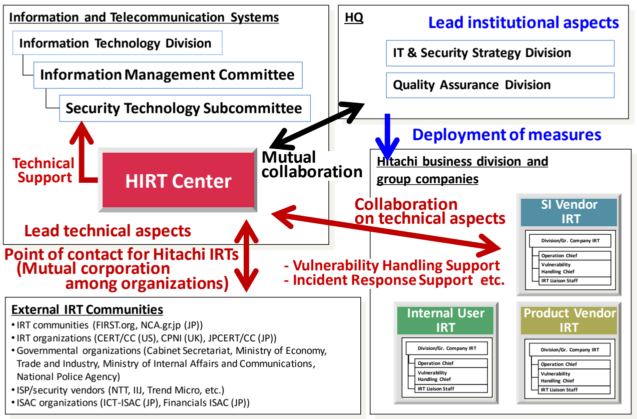

Information and Telecommunication Systems
Information Technology Division
Information Management Committee
Security Technology Subcommittee
HQ
Lead institutional aspects
IT & Security Strategy Division
Quality Assurance Division
Deployment of measures
Technical Support
HIRT Center
Mutual collaboration
Lead technical aspects
Hitachi business division and group companies
Collaboration on technical aspects
SI Vendor IRT
Division/Gr. Company IRT
Operation Chief
Vulnerability Handling Chief
IRT Liaison Staff
Point of contact for Hitachi IRTs (Mutual corporation among organizations)
- Vulnerability Handling Support
- Incident Response Support etc.
External IRT Communities
• IRT communities (FIRST.org, NCA.gr.jp (JP))
• IRT 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)
• ISP/security vendors (NTT, IIJ, Trend Micro, etc.)
• ISAC organizations (ICT-ISAC (JP), Financials ISAC (JP))
Internal User IRT
Division/Gr. Company IRT
Operation Chief
Vulnerability Handling Chief
IRT Liaison Staff
Product Vendor IRT
Division/Gr. Company IRT
Operation Chief
Vulnerability Handling Chief
IRT Liaison Staff

Figure 15: Position of HIRT Center.

In particular, for issuing security information for vulnerabilities and incidents, to external entities, we also adopt an approach in which an "Emergency Level" of information is determined and a "Website Level" at which the information is to be published is selected, in addition to just routinely publishing security information via our security portal website (Figure 17).

Table 8: (Externally) promoting projects.

| Category | Overview |
|---|---|
| Strengthening the domestic partnership for CSIRT activities | - Deploying proactive measures against vulnerabilities based on the Information Security Early Warning Partnership<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) [*c] [13] |
| Developing a framework for research activities | - Establish a joint research between Meiji 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 (MWS) [14] |

Table 9: 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 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. |

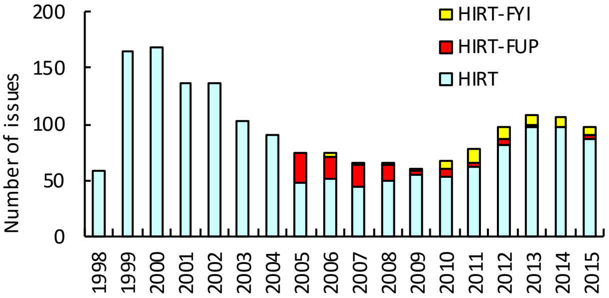


Figure 16: Number of issues of security information by ID number.

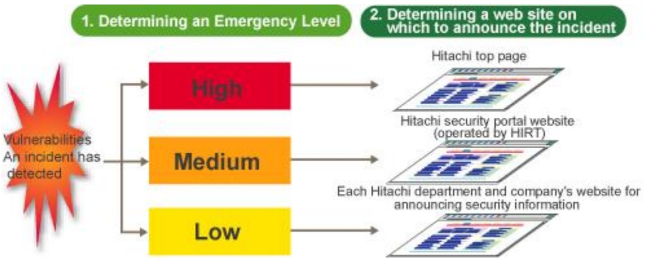

1. Determining an Emergency Level
2. Determining a web site on which to announce the incident
Vulnerabilities An incident has detected
High
Medium
Low
Hitachi top page
Hitachi security portal website (operated by HIRT)
Each Hitachi department and company's website for announcing security information

Figure 17: Conceptual view of issuing information based on "Emergency Level" x "Website Level".

# 4 Activity Summary from 1998 to 2014

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

## 4.1 The Year 2014

### (1) Improvement of Hitachi Group CSIRT activities (Phase 3)

In 2014, the fifth year of the activities, we opened a HIRT Laboratory Project Room inside the Yokohama Research Laboratory's facilities to mark the start year of Phase 3. The purposes of this Project Room are to be a locus for passing on technical skills and to serve as a hub for support activities and for collaboration with the Research Laboratory.

### (2) Trial IRT activities for Individual Domains

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

For external readiness activities for the financial domain, we expanded weekly distribution of the HIRT-FIS Security Notes and held view-exchange meetings with financial-related CSIRTs in order to put out feelers for collaboration with financial-related CSIRTs.

- **Vulnerability countermeasures for industrial control systems**

We moved ahead with approaching vulnerability countermeasures for industrial control systems, starting from three perspectives: specification designs, codes, and configurations.

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

### (3) Strengthening of Partnership with the CSIRT Community

As concrete activities for strengthening our partnership with the CISIRT community, we continued with the gatherings with NTT-CERT [15] that we have been holding periodically since 2006, at which we exchanged information for improving CSIRT activities. Also, we supported membership in the Nippon CSIRT Association (Table 10), launched the SSH Server Secure Configuration Working Group, and carried out information dissemination in cooperation with its Incident Information Utilization Framework Working Group [20].

- Regarding vulnerability of GNU bash - shellshock
- Struts: Regarding vulnerabilities that allow operation of ClassLoader (CVE-2014-0094, CVE-2014-0112, CVE-2014-0113)
- Regarding vulnerability that allows OpenSSL information leakage - Heartbleed

Table 10: Support for membership in Nippon CSIRT Association.

| Approval | Team Name |
|---|---|
| May 2014 | YMC-CSIRT (Yamaha Motor Co., Ltd.) |
| October 2014 | NISSAY IT CSIRT (Nissay Information Technology Corporation) |
| November 2014 | MS&AD-CSIRT (MS&AD Insurance Group Holdings, Inc.) |

### (4) Lectures

- February 2014: "A Security Incident in China: DarKnight" by Jack YS Lin, JPCERT Coordination Center
- March 2014: "The Surveilled Internet" by Masafumi Negishi, Internet Initiative Japan Inc.
- August 2014: "General Coping Flow for Targeted Attacks, and Proactive Countering and Profiling Using Big Data: What are They?" by Nobuaki Hirahara, Trend Micro Incorporated.

## 4.2 The Year 2013

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

In 2013 - the fourth year of the improvements and the final year of Phase 2 - we moved ahead with entrenching loci for passing on techniques for cyber security countermeasures, in concert with the HIRT supporting staff (staff who work with the HIRT Center to actively promote IRT activities).

For the passing on of the techniques, we divided them into three: (a) **analysis (reverse engineering)** of the behavior of the malware and so forth used in cyber attacks, (b) **investigation (forensics)** to extract information and data from computers to serve as digital evidence, and (c) **assessment (penetration)** to looks for the vulnerabilities, then possibly attempting to exploit them if access may be gained.

### (2) Trial IRT activities for individual domains

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

For external readiness in the financial domain, we began trial weekly distribution of the HIRT-FIS Security Notes.

- **Vulnerability countermeasures for industrial control systems**

We established a framework for vulnerability handling and incident handling with HIRT as basic point of contact for external organizations (Figure 18) [16].

### (3) Strengthening of Partnership with the CSIRT Community

We carried out information dissemination in cooperation with the Nippon CSIRT Association’s Incident Information Utilization Framework Working Group [20].

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

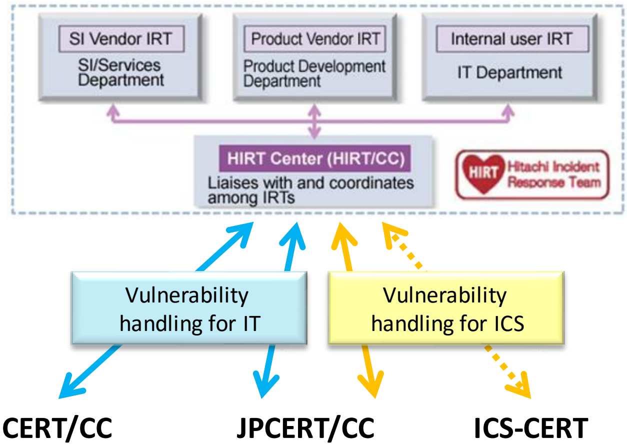

SI Vendor IRT
SI/Services Department
Product Vendor IRT
Product Development Department
Internal user IRT
IT Department
HIRT Center (HIRT/CC)
Liaises with and coordinates among IRTs
HIRT Hitachi Incident Response Team
Vulnerability handling for IT
Vulnerability handling for ICS
CERT/CC
JPCERT/CC
ICS-CERT

Figure 18: Framework for vulnerability handling.

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

We won the 2013 Senior Information Security Professional Award for ISLA (Information Security Leadership Achievements) from (ISC)$^2$, which runs the CISSP information security certification and is highly appraised for its contributions to the vulnerability countermeasure activities pertaining to the JVN (Japan Vulnerability Notes), in which HIRT is involved [17].

### (5) Lectures

- June 2013: "Security for Android Apps and Security Activities for Software Development Worksites" by Masaru Matsunami, Sony Digital Network Applications, Inc.

- September 2013: "Control System Security: Suggestions for Proactive Approaches Toward the Generation When Information and Control Systems Fusion" by Lauri Korts-Pärn, Cyber Defense Institute.

## 4.3 The Year 2012

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

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

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

### (2) Trial IRT activities for individual domains

We started trial IRT activities for individual domains, in order to take the approach of the three-tiered cycle for incident response and readiness that incorporates the perspectives of individual business domains (Figure 12).

Also, as an advanced endeavor in the financial domain, we set up HIRT-FIS inside our financial section on October 1, 2012 (Figure 19).

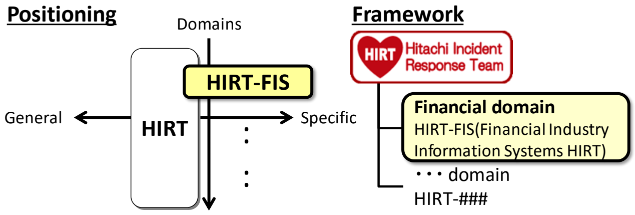


Figure 19: Positioning and framework of IRT activities for individual industry domains

### (3) Strengthening of Partnership with the CSIRT community

- On Febuary 29, 2012 we held the CSIRT Workshop 2012 as an opportunity for exchange of opinions on corporate CSIRT, targeting corporate staff interested in CSIRT activities [18].
- Together with the FIRST member teams in Japan, we held the FIRST Technical Colloquium 2012 Kyoto at the Kyoto International Community House from November 13 to 15, 2012 [19].
- In order to continue with study of "Future of Global Vulnerability Reporting", which was raised at the FIRST Technical Colloquium 2012 Kyoto, we launched a Vulnerability Reporting and Data eXchange SIG (Special Interest Group) inside FIRST.

### (4) Lectures

- March 2012: "Framework for Promoting Security Measures in Organizations" by Nobuo Miwa, S&J Consulting
- August 2012: "Elements and Implementation of Database Security" by Haruto Kitano, Oracle Corporation Japan
- September 2012: "Trends in Cyber Attacks and the Cutting Edge of Cyber Security Research" by Daisuke Inoue, National Institute of Information and Communications Technology
- November 2012: "A Look Back Over Remote Control Incidents, the Firstserver Problem and the Leap-Second Problem" by Tetsutaro Uehara, The Research Institute of Information Security (NPO)

## 4.4 The Year 2011

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

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

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

### (2) Disseminating Information on Vulnerability in Control System Products

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

### (3) Strengthening of Partnership with the CSIRT Community

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

- Web Malware "mstmp" exploiting Mash-up

### (4) Lectures

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

### (5) Other activities

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

## 4.5 The Year 2010

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

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

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

### (2) Strengthening of Partnership with the CSIRT Community

In December 2012, we provided support for the holding of the Nippon CSIRT Association's International Partnership Workshop Also, in cooperation with the Nippon CSIRT Association's Incident Information Utilization Framework Working Group, we carried out information disseminated [20]:

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

### (3) Other activities

- In July 2010, we provided backing for the organizing of an "Academy CERT Meeting" in collaboration with JPCERT/CC, to help Indonesia's academic CSIRT activities [21].
- "Survey on Malware Circulating Within the P2P File Exchange Environment" [22]
- Since 2007, many Antinny-type known malwares that are liable to cause information leakage have been swarming on the "Winny" P2P file-sharing environment (Figure 20).

## 4.6 The Year 2009

### (1) Start of Product/Service Security Feedback

To give feedback to the product development processes about the know-how we learned from the experience of vulnerability fighting and incident response, we started to provide support for each process (Figure 21).

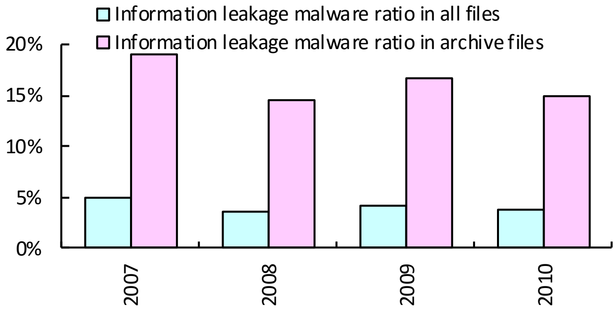
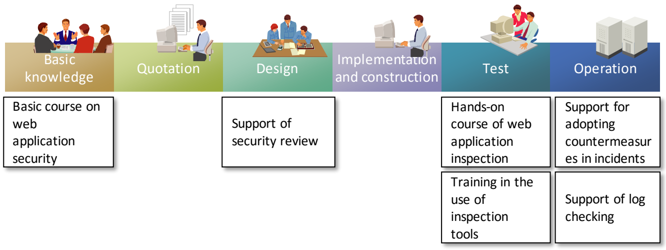


Figure 20: Changes in malware circulating in Winny that causes information leakage.



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 adopting countermeasures in incidents
Support of log checking

Figure 21: Systematizing HIRT support activities (Web application security).

### (2) Providing Security Engineer Training

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

### (3) Lectures

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

### (4) Other Activities

- "Survey on Malware Circulating within the P2P File Exchange Environment" [23]
- 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) [24] which tries to visualize the observational data.

## 4.7 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" [25] 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 [26].

### (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)" [27].

### (5) Lectures

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

### (6) Other Activity

In order to partially reveal the actual circumstances of targeted attack as a part of efforts to develop a new inter-organization collaboration, we provided related organizations with a malware-attached e-mail, which faked itself as Call for Papers (CFP) for the symposium held by the Computer Security Symposium 2008 of Information Processing Societies Japan as a sample [28].

## 4.8 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 SoftBank CSIRT (Softbank) in April 2007 [29]. As of December 2015, 106 teams have been joined (Figure 22).

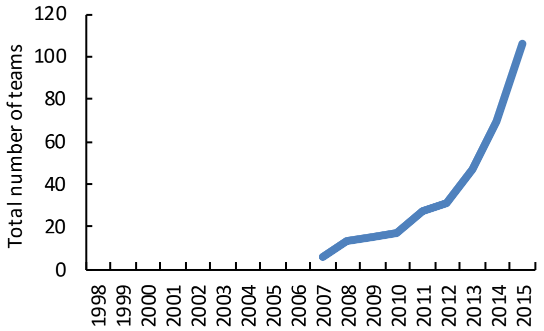


Figure 22: Change in Number of Nippon CSIRT Association Members.

### (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 [30].

### (4) Lectures

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

## 4.9 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 Activity

- Starting to sign a digital signature to technical documents (PDF files) issued from HIRT [31]

## 4.10 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 [ 32 ]. The preparation period extended for about one year, since any team wishing to join the community must obtain recommendations from two member teams before doing so.

As of December 2015, a total of 345 teams have joined this community, including 25 Japanese teams (Figure 23) [*d].

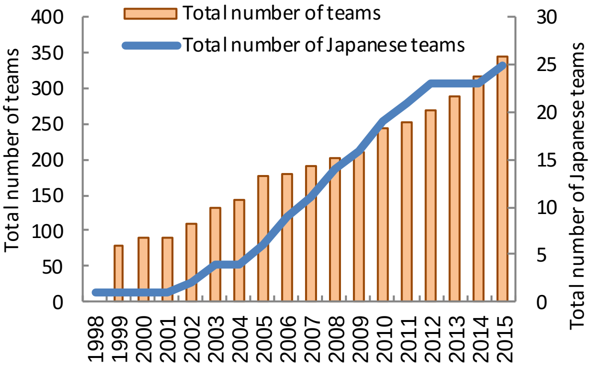


Figure 23: Changes in the number of members of FIRST.

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

In September 2005, in order to provide Internet users with comprehensive information on security problems applicable to the products and service of the Hitachi group, we set up a security information portal site within which the security information provided through the websites of Hitachi business divisions and group companies is integrated (Figure 24). We also created "Guidance for Providing Security Information from Websites to External Users, V1.0".

### (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.

[*d] CDI-CIRT (Cyber Defense Institute, Inc.), CFC (National Police Agency, Japan), DeNA CERT (DeNA Co., Ltd.), DT-CIRT (Deloitte Touche Tohmatsu LLC), FJC-CERT (Fujitsu Limited), Fuji Xerox-CERT (Fuji Xerox Co., Ltd.), HIRT (Hitachi Ltd.), IIJ-SECT (Internet Initiative Japan, Inc.), IPA-CERT (Information-technology Promotion Agency, Japan), JPCERT/CC, JSOC (LAC Co., Ltd.), KDDI-CSIRT (KDDI Corporation), KKCSIRT (Kakaku.com, Inc.), LINE-CSIRT (LINE Corporation), MBSD-SIRT (Mitsui Bussan Secure Directions, Inc.), MIXIRT (Mixi), MUFG-CERT (Bank of Tokyo-Mitsubishi UFJ, Ltd.), NCSIRT (NRI SecureTechnologies, Ltd.), NISC (Cabinet Secretariat, Japan), NTT-CERT (Nippon Telegraph and Telephone Corporation), NTTDATA-CERT (NTT DATA Corporation), Panasonic PSIRT (Panasonic Corporation), Rakuten-CERT (Rakuten, Inc.), RicohPSIRT (Ricoh Company, Ltd.), SoftBank CSIRT (SoftBank Corp.) and YIRD (Yahoo! JAPAN Corporation).

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

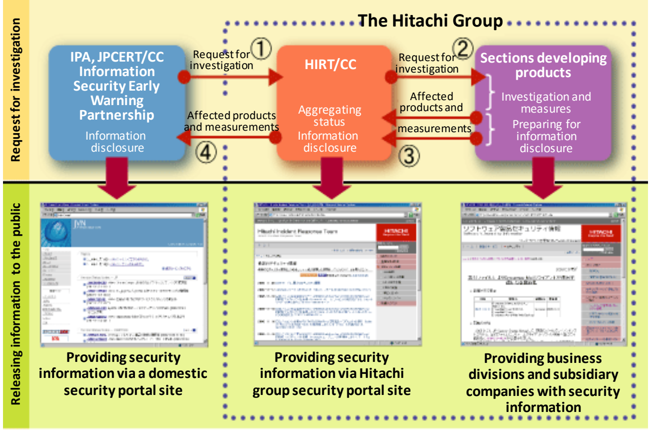

Request for investigation
Releasing information to the public
The Hitachi Group
IPA, JPCERT/CC Information Security Early Warning Partnership
Information disclosure
① Request for investigation
HIRT/CC
Aggregating status
Information disclosure
② Request for investigation
Sections developing products
Investigation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

Figure 24: Providing security information on the Hitachi security information portal.

## 4.11 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 [33][34].

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) [35].

### (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)

## 4.12 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 [36].

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

Table 11: Information on point of contact.

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

## 4.13 The Year 2002

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

SNMP vulnerability [12] reported from CERT/CC in 2002 affected a wide range of software and devices. This provided an opportunity to start the Product Vendor IRT and obtaining/publishing information based on the CERT/CC Vulnerability Disclosure Policy [ 37 ]. 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 [38].

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

We provided support to build and operate a trial website, JPCERT/CC Vendor Status Notes (JVN) (http://jvn.doi.ics.keio.ac.jp/), in February 2003, as an attempt to improve the domestic circulation of security information (Figure 25) [39][40].

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/).

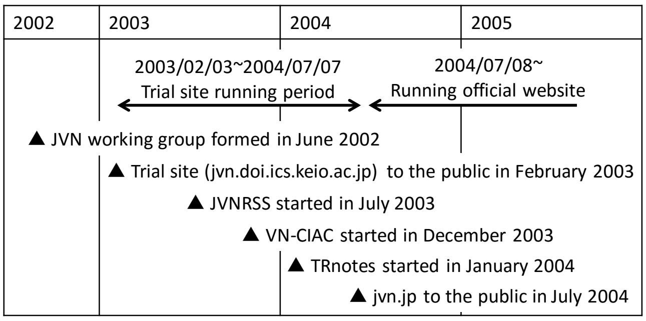

2002
2003
2004
2005
2003/02/03~2004/07/07
Trial site running period
2004/07/08~
Running official website
▲ JVN working group formed in June 2002
▲ Trial site (jvn.doi.ics.keio.ac.jp) to the public in February 2003
▲ JVNRSS started in July 2003
▲ VN-CIAC started in December 2003
▲ TRnotes started in January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

Figure 25: Building and running a JVN trial site.

## 4.14 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 26), 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.

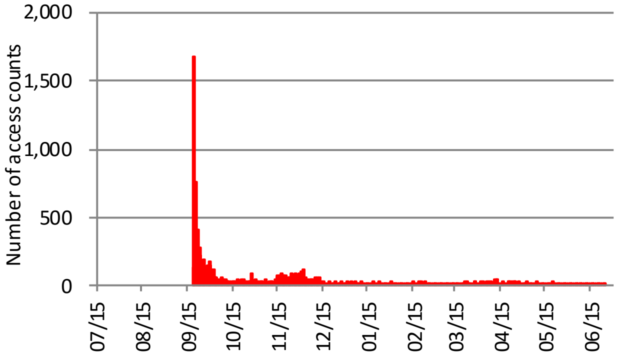


Figure 26: Changes in the number of Nimda log counts found during the observation period (for Nimda).

## 4.15 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" [41] for vulnerability. It provides the Severity Metric indicating the severity of vulnerability [42] Common Vulnerabilities and Exposures (CVE) classified information security vulnerabilities into "Vulnerabilities" and "Exposures" and focuses on the former [43]. 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 [44], a predecessor of NVD.

Note that as severity metrics for vulnerabilities vary, depending on organizations, the Common Vulnerability Scoring System (CVSS) [45] was proposed as a common language with which to evaluate the severity of vulnerability in a comprehensive and general way in 2004.

## 4.16 The Year 1999

### (1) Launch of the hirt.hitachi.co.jp domain

To improve the provision of security information to the Hitachi group, we created an internal domain for HIRT projects to set up a website (hirt.hitachi.co.jp) in December 1999.

### (2) Investigation of website defacement

Website defacement was a major type of incidents since it occurred for the first time in the US in 1996 until the network worm era started (2001 - 2004). We conducted a research on webpage defacing from 1999 to 2002 to find out how malicious activities were performed (Figure 27).

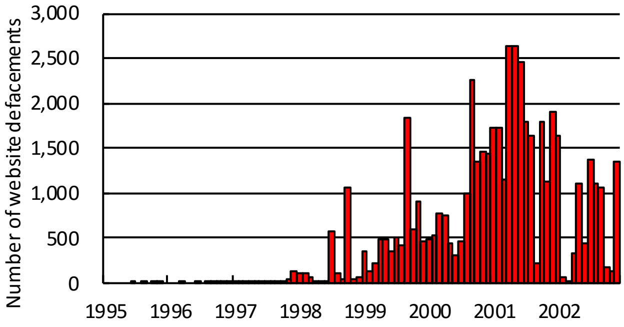


Figure 27: Changes in the number of websites defacements.

## 4.17 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 [46] as a speaker as an instructor.

## 5 Conclusion

Security measures and incident responses are composed in no small part to affect/be affected by other organizations; therefore, not only will a speed-up in professional, practical collaboration between CSIRTs be sought but damage associated with physical effects has also started to emerge. The next challenges to overcome will likely be the tracking of attackers' cyber attack speed, and the establishment of a system of incident response from both cyber and physical aspects. At HIRT, we plan to start a "Six-Year Plan for Promoting CSIRT Activities for Individual Domains" following the "Six-Year Plan for Improving Hitachi Group CSIRT Activities" in order to deal with these new threat situations. At the same time, we will be moving progressively forward with activities that "catch any signs of future threats and take actions as early as possible", so as to deal with new threats.

(August 14, 2016)

## References

1) National Police Agency: Occurrence of Fraudulent Money Transfer Crimes Relating to Internet Banking in 2015, http://www.npa.go.jp/cyber/pdf/H280303_banking.pdf

2) Symantec, The evolution of ransomware (Aug. 2015), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

3) McAfee, Threat Report (Aug. 2015), http://www.mcafee.com/jp/resources/reports/rp-quarterly-threat-q2-2015.pdf

4) Arbor Networks, ATLAS Q2 2015 Global DDoS Attack Trends, http://www.slideshare.net/Arbor_Networks/atlas-q2-2015final

5) Arbor Networks, ASERT Threat Intelligence Report 2015-04; "DD4BC DDoS Extortion Threat Activity", http://pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf

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

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

8) Hitachi Begins Trial for Sharing Cyber Threat Data with HP, http://www.hitachi.com/New/cnews/month/2015/10/151006a.html

9) Nippon CSIRT Association, SSH Server Secure Configuration Working Group, http://www.nca.gr.jp/activity/sshconfig-wg.html

10) Institute of Information Security, Eleventh "IISEC Information Security Culture Award", https://www.iisec.ac.jp/news/20150210culsec_11th.html

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

12) CERT Advisory CA-2002-03, "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol(SNMP)" (2002/2), http://www.cert.org/advisories/CA-2002-03.html

13) HIRT-PUB14008: Cybersecurity information exchange framework CYBEX, http://www.hitachi.co.jp/hirt/publications/hirt-pub14008/index.html

14) anti Malware engineering workshop, http://www.iwsec.org/mws/2015/

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

16) HIRT-PUB10008： Hitachi Vulnerability Disclosure Process (2011/9), http://www.hitachi.com/hirt/publications/hirt-pub10008/index.html

17) (ISC)$^2$: Information Security Leadership Achievements (ISLA)プログラム, https://www.isc2.org/japan/isla.html

18) CSIRT Workshop 2012, http://www.hitachi.co.jp/hirt/topics/20120229.html

19) Kyoto 2012 FIRST Technical Colloquium, http://www.first.org/events/colloquia/kyoto2012

20) Nippon CSIRT Association: incident response, http://www.nca.gr.jp/2010/incidentresponse.html

21) SGU MIT Workshop Academy CERT Meeting(2010/7), http://academy-cert-indonesia.blogspot.jp/2010/06/academy-cert-meeting.html

22) Malware Circulating in P2P File Exchange Software Environment (2011) (2011/9), http://www.hitachi.co.jp/hirt/publications/hirt-pub11003/index.html
23) 2009 Survey on information leakage via P2P File Exchange Software Environment (2009/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub09008/index.html
24) cNotes: Current Status Notes, http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi
25) Information-Technology Promotion Agency, Japan: Countermeasures against DNS Cache Poisoning (2009/2), http://www.ipa.go.jp/security/vuln/DNS_security.html
26) Recording Site for Joint Workshop on Security 2008, Tokyo (2008/3), http://www.nca.gr.jp/jws2008/index.html
27) 2008 Information Technology Period Promotion - Awarding companies that have contributed to the promotion of information technology in 2008 (2008/10), http://www.jipdec.or.jp/archives/project/gekkan/2008/ceremony/prize02.html
28) IPSJ, Information Processing: Malware: 5. column: Targeted Email Attack for CSS2008 CFP (2010/3), https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=69232&file_id=1
29) CSIRT - Nippon CSIRT Association, http://www.nca.gr.jp/
30) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
31) GlobalSign Adobe Certified Document Services, http://jp.globalsign.com/solution/example/hitachi.html
32) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
33) 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
34) Information-technology Promotion Agency, Japan: Information Security Early Warning Partnership Guideline (2004/7), http://www.ipa.go.jp/security/ciadr/partnership_guide.html
35) JVN (Japan Vulnerability Notes), http://jvn.jp/
36) 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
37) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
38) 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
39) Considerations on JPCERT/CC Vendor Status Notes DB: JVN, CSS2002 (2002/10), http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf
40) Development of JVN to Support Dissemination of Security Information (2005/5), http://www.hitachi.co.jp/hirt/csirt/jvn/index.html
41) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
42) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp
43) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/
44) ICAT, http://icat.nist.gov/(not available)
45) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
46) 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. Also, 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 a chief of the steering committee for the Nippon CSIRT Association.