HITACHI
Inspire the Next

【Words and Terms】

■**CERT/CC** (Computer Emergency Response Team/Coordination Center)
CERT/CC is an institute that collects information on security incidents and vulnerabilities in the United States.

■**CPNI** (Center for the Protection of National Infrastructure)
CPNI is a government agency that collects information on security incidents and vulnerabilities in the United Kingdom.

■**CSIRT** (Computer Security Incident Response Team)
CSIRT is a unit that detects a security incident, cooperates with relevant people/entities, minimize the damage, investigate the cause and solve the problem to prevent recurrence of the same sort of incident.

■**FIRST** (Forum of Incident Response and Security Teams)
FIRST is a global community of CSIRTs formed on the trust network. Formed in 1990 to establish communications among CSIRTs across the world. Currently it has more than 200 members.

■**IPA** (Information-technology Promotion Agency)
IPA is a governmental organization established in October 1970 pursuant to "Act on Facilitation of Information Processing". It promotes development and spread of general-purpose programs, R&D on advanced information technology, financing support for information technology service companies, computer virus prevention, operation of the multimedia research center, promotion and operation of the center for information infrastructure, and development of regional capability of software provisioning.

■**JPCERT/CC** (Japan Computer Emergency Response Team/Coordination Center)
JPCERT/CC is an institute that collects information on security incidents and vulnerabilities in Japan. Also promotes public awareness of security issues.

■**JVN** (JP Vendor Status Notes)
JVN was established pursuant to "the Standard for Handling of Vulnerability Information on Software and Others" set by METI. JVN provides information on vulnerability countermeasure information mainly on domestic products on its web site. JPCERT/CC and the IPA together operate JVN.

■**NCA** (Nippon CSIRT Association)
NCA was established in March 2007 to promote the collaboration among domestic CSIRTs to solve common issues. HIRT is one of the founding and board members.

■**NISC** (National Information Security Center)
A national center dedicated to information security issues established in the Cabinet Secretariat.

■**WARP** (Warning, Advice and Reporting Point)
WARP, developed by the UK government, is a community of interest-oriented, mutual-support communities that aim to share security information, advice and lesson-learned through incidents among its members to help each other within the a WARP community and with other WARP communities.

■**Incident** (Computer Security Incident)
An incident means a man-made event related to computer security that can be malicious or accidental including not factual but a suspicious situation. For example, unauthorized use of resources, denial of services, data destruction, unintended information disclosure and actions/events led to these activities.

■**Vulnerability**
A vulnerability is a problem/weakness in software and other products that could be exploited by attacks, such as computer virus and unauthorized access, and cause loss of functions and features. As for web applications, it could mean a situation where anyone can access the information that should have been protected by the administrator with some means of access control, lacking safety considerations.

■**the Standard for Handling of Vulnerability Information on Software and Others**
A framework that defines how to handle and process vulnerability information within Japan, to whom to report and how the information should be treated. By leveraging this framework, product vendors can take care of the vulnerability (if there are any) before it is made public.

HIRT Hitachi Incident Response Team

For More Information

HIRT (Hitachi Incident Response Team)

Security & Smart ID Solutions Division, Hitachi Ltd.
Hitachi Systemplaza Shinkawasaki
890 Kashimada, Saiwai, Kawasaki, Kanagawa, 212-8567 JAPAN

- URL : http://www.hitachi.com/hirt/
- Contact : https://www3.hitachi.co.jp/inquiry/hirt/en/form.jsp
- Tel: +81-44-555-0894
- Fax: +81-44-549-1382

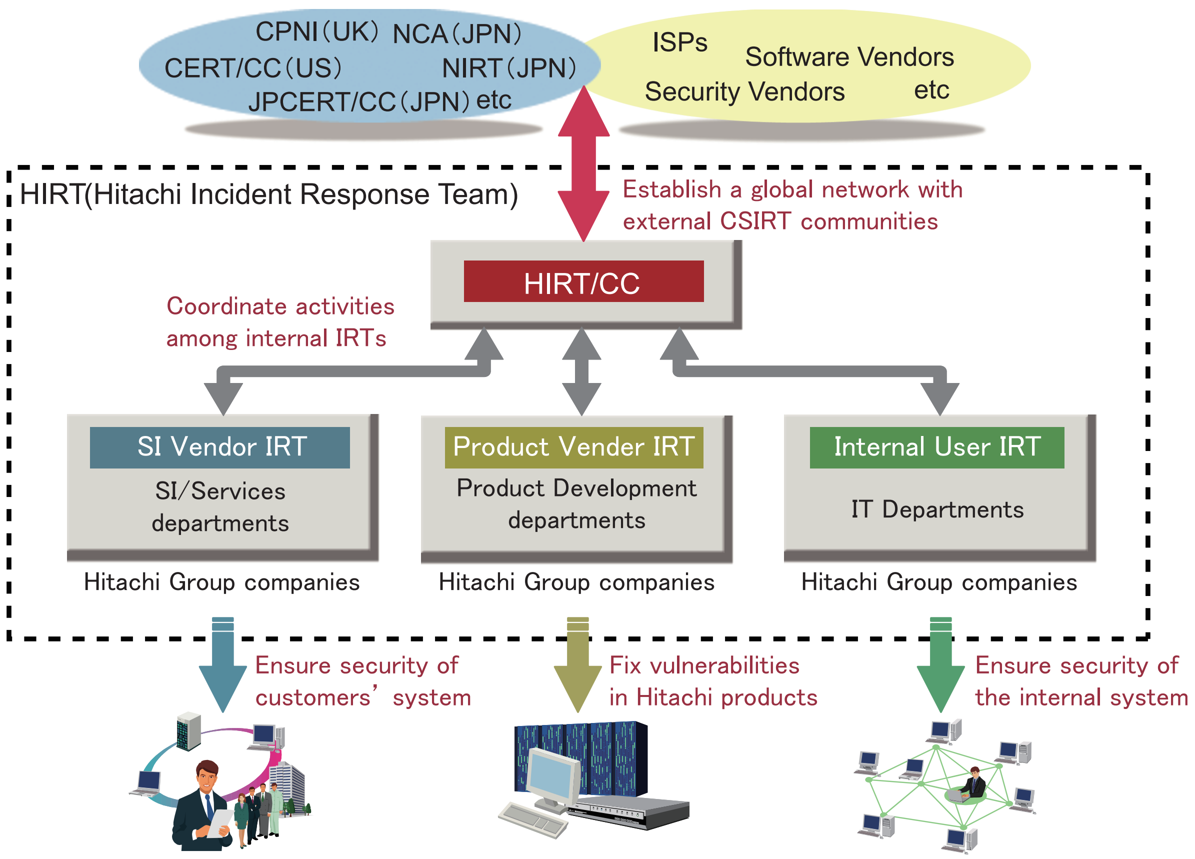
2009.03

uVALUE

About the HIRT

The Hitachi Incident Response Team (HIRT) was formed in October 2004 to be a CSIRT (Computer Security Incident Response Team) of the Hitachi Group. It disseminates security information to the Hitachi Group companies to support their efforts to protect Hitachi's and customers' systems from vulnerabilities and incidents. HIRT aims to contribute to development of a safe network environment the society can rely on through prevention of security incidents and enhancement of incident response capability, making them a unified effort by the entire Hitachi Group. As the Hitachi's single point of contact for other CSIRTs, HIRT has joined the CSIRT communities, such as FIRST and NCA, and keeps working on improving information security for the global society.

Four IRTs Underpinning HIRT Activities


CPNI(UK) NCA(JPN)
CERT/CC(US) NIRT(JPN)
JPCERT/CC(JPN) etc
ISPs
Software Vendors
Security Vendors
etc
HIRT(Hitachi Incident Response Team)
Establish a global network with external CSIRT communities
HIRT/CC
Coordinate activities among internal IRTs
SI Vendor IRT
SI/Services departments
Hitachi Group companies
Product Vender IRT
Product Development departments
Hitachi Group companies
Internal User IRT
IT Departments
Hitachi Group companies
Ensure security of customers' system
Fix vulnerabilities in Hitachi products
Ensure security of the internal system

■HIRT/CC(HIRT/Coordination Center) 【= HIRT Center】

Act as the Point of Contact for the external CSIRTs, such as FIRST, NCA, JPCERT/CC and CERT/CC as well as coordinate efforts and activities among the SI Vendor IRT, the Product Vendor IRT and the Internal User IRT.

■SI Vendor IRT 【= departments involved in offering SI/Services】

Promote IRT activities for the customer systems. Work on to make sure all known vulnerabilities in the customer systems and security incidents have been taken care of.

■Product Vendor IRT 【= departments involved in developing products】

Publish information on vulnerabilities found in Hitachi products and how to fix them. Investigate vulnerabilities for their applicability to Hitachi products and if they have them, provide a security patch to prevent incidents which could be caused by viruses and/or unauthorized access that exploit those vulnerabilities via the Internet.

■Internal User IRT 【= IT Department】

Enforce adequate security measures to prevent Hitachi networks and web sites from being exploited and becoming a threat to the Internet community.

Mission of the HIRT

As the Internet rapidly grows into a social infrastructure, the number of security incidents increases and the magnitude of the potential damage becomes more significant. Various devices are connected through the network of networks and allow people to enjoy easy communication and useful services. At the same time, however, unauthorized access and information leak exploiting vulnerabilities of software and web applications are becoming a serious social problem. Today, problems concerning the Internet should be considered as not only an organizational issue but also a social one. Interorganizational and international coordination and response through CSIRTs are getting more and more important. With this situation in mind, HIRT will support security efforts of the Hitachi Group as well as making the Internet safe through its two missions: "Vulnerability Handling: effort to counter security vulnerabilities to prevent incidents " and "Incident Response: effort to stop ongoing security incidents".

Strengthen Domestic & International Partnership on the CSIRT Activity

Since the emergence of the Blaster worm in 2003, attacking methods have been rapidly evolving into more stealthy, sophisticated and target-oriented ones. To counter them, it is necessary for CSIRTs to cooperate in information sharing and incident response. In 2005, HIRT joined the FIRST, an international CSIRT forum, NCA, a domestic CSIRT community, in March 2007, and WARP, a security community in UK, in May 2007 to strengthen global collaboration. Through the partnership with other Internet communities, HIRT will make a continuous effort to make a safe and secure Internet a reality.

Promote Dissemination of Security Information

HIRT acts as a coordinator within the Hitachi Group and between the Hitachi Group and external organizations as the Hitachi's Point of Contact, pursuant to the Guideline for the Information Security Early Warning Partnership program, for information sharing and incident prevention. Through proper dissemination of vulnerability countermeasure information, HIRT strives to deter incidents, such as unauthorized access and virus infection, as well as to minimize the damage in case an incident does strike.

- Publish information on vulnerabilities found in Hitachi products and how to fix them on the JVN web site
- Report vulnerability-related information on software

About the Guideline for the Information Security Early Warning Partnership
http://www.ipa.go.jp/security/english/vuln/200807_announce_manual_en.html
The Ministry of Economy, Trade and Industry developed an official vulnerability-reporting procedure called "The Standard for Handling of Vulnerability Information on Software and Others" in July 2004 and launched "the Information Security Early Warning Partnership" as its operational framework. In this framework, IPA receives reports on vulnerability found in software products and/or websites and encourages software vendors and web site operators to fix them. It also sets down recommended actions toward product vendors and expects them to make a preventive efforts and ensure safety of the advanced information and telecommunications networks we find ourselves in.

About JVN（JP Vendor Status Notes ）
http://jvn.jp/en/
Pursuant to "the Standard for Handling of Vulnerability Information on Software and Others" set by the METI, JVN provides information on vulnerability countermeasure information mainly on domestic products. JPCERT/CC and the IPA together run JVN.

Improve Security in the Hitachi Group ～ Information Sharing, Response Coordination and Education ～

■Information Sharing

To solve information security issues, promote information sharing of security alerts and vulnerability countermeasures among the Hitachi Group companies, through mailing lists and HIRT web site.

■Coordination of Security-Related Issues

When a vulnerability is found in Hitachi products or Hitachi-related web sites, HIRT coordinates response within the Hitachi Group and between Hitachi and external organizations.

■Support for Information Security Education

Support information security education and training with know-hows gathered through HIRT's CSIRT experience.

HIRT supports security efforts by the Hitachi Group, and in doing so, contributes to security of out networked society.