HITACHI
Inspire the Next

【Abbreviation and Terms】

- **CERT/CC (Computer Emergency Response Team/Coordination Center)**
  An institute that collects information on security incidents and vulnerabilities in the U.S.
- **CPNI (Center for the Protection of National Infrastructure)**
  A government agency that collects information on security incidents and vulnerabilities in the U.K.
- **CSIRT (Computer Security Incident Response Team)**
  An organization that aims to detect security incidents, collaborate with relevant people/organizations and investigate the cause and fix the problem to minimize the damage and prevent the recurrence.
- **FIRST (Forum of Incident Response and Security Teams)**
  A global community of CSIRTs built on the trust. Currently it has more than 200 members from 43 nations.
- **IPA (Information-technology Promotion Agency)**
  A governmental organization that promotes development and spread of general-purpose programs, R&D on advanced information technology, computer virus prevention, and establishment and operation of the center for information infrastructure.
- **JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center)**
  An institute that collects information on security incidents and vulnerabilities in Japan.
- **JVN (JP Vendor Status Notes)**
  A website that provides information on the domestic vendors' response to the publicly released vulnerabilities, established under the "Standard for Handling of Vulnerability Information on Software and Others" by METI.
- **NCA (Nippon CSIRT Association)**
  A community that was established in March 2007 to promote the collaboration among domestic CSIRTs to solve common issues.
- **NISC (National Information Security Center)**
  A national center dedicated to information security issues established in the Cabinet Secretariat.
- **WARP (Warning, Advice and Reporting Point)**
  A collection of mutual-support communities that aim to share security and incident information and exchange advice to help each other improve security.
- **Incident (Computer Security Incident)**
  A man-made event related to computer security that can be malicious/intentional or accidental.
- **Information Security Early Warning Partnership**
  A framework where that IPA collects reports on security issues found in software products and websites and encourages the product vendors and website operators to disclose the information and fix the problems.
- **Vulnerability**
  A weakness in software and other products that could be exploited by attacks, such as computer virus and unauthorized access, and impair their functions and/or capabilities. As for web applications, it could mean a situation that lacks safety considerations, for example, where anyone can access the information that should have been protected by the website operators with access control.
- **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 promote safe circulation of security information.

HIRT Hitachi Incident Response Team

For More Information

HIRT (Hitachi Incident Response Team)
Cloud Services Division, Hitachi Ltd.

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

- URL : http://www.hitachi.com/hirt/
- Contact : http://www.hitachi.com/hirt/ask.html

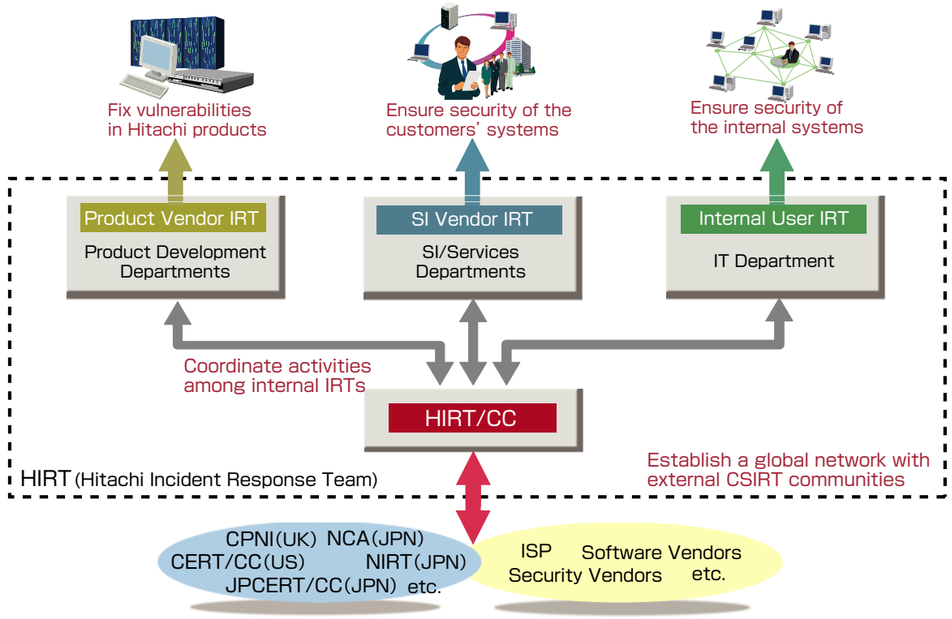
2015.11

About the HIRT

Hitachi Group assembled HIRT(Hitachi Incident Response Team) in April, 1998 as a project to consolidate IRT(Incident Response Team) framework within Hitachi.

HIRT disseminates information on vulnerability countermeasures and incident response to those relevant in the Hitachi Group to support their efforts to protect the Hitachi Group's and its customers' information systems from security incidents, such as unauthorized access. As Hitachi Group's unified effort, by preventing security incidents and quickly responding to the incidents, should they happen, HIRT aims to contribute to the establishment of a safe and secure network environment where our customers and society can rely on. As the Hitachi Group's single point of contact for the outside world, HIRT proactively participates in the CSIRT communities, such as FIRST and NCA, and keeps working on improving information security for the global society.

Four IRTs Underpinning HIRT's Vulnerability and Incident Response Activities



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

HIRT Center acts as the Point of Contact for the external CSIRTs, such as FIRST, NCA, JPCERT/CC and CERT/CC. It also coordinates 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】

SI Vendor IRT promotes IRT efforts for the customer systems. It works to make sure that the customers' systems are well protected against known vulnerabilities and security incidents.

Product Vendor IRT【= departments involved in developing products】

Product Vendor IRT publishes information on vulnerabilities found in Hitachi products and how to fix them. It also investigates publicly released vulnerabilities for their applicability to Hitachi products and if they have the vulnerabilities, notifies the customers and provides 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】

Internal User IRT enforces adequate security measures to prevent the Hitachi networks and websites from being exploited and becoming a threat to the Internet community.

Mission of HIRT

As the Internet rapidly grows into a critical social infrastructure, the number of security incidents increases and the potential impact of the incidents becomes more and more serious. Various systems are connected through the network of networks and that allows people to enjoy easy communication and convenient services. At the same time, however, unauthorized access and information leak that exploit vulnerabilities of software and web applications are becoming serious social problems. Today, problems concerning the Internet should be considered as not only an organizational issue but also a social one. Interorganizational and international collaboration and response across CSIRTs are getting critically important.

With this situation in mind, HIRT will support information security efforts of the Hitachi Group as well as establishment, maintenance and development of a safe and secure Internet through its two missions: "Vulnerability Handling: efforts to eliminate security vulnerabilities to prevent incidents " and "Incident Response: efforts 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 collaborate in information sharing and analysis, and incident response.
HIRT joined the FIRST, an international CSIRT forum, in 2005, NCA, a domestic CSIRT community, in March 2007, and WARP, a security community in UK, in May 2007 to strengthen its global collaboration. Through the partnership with other Internet communities, HIRT will make continuous efforts to make a safe and secure Internet a reality.

Promote Dissemination of Security Information

As the Hitachi Group's Point of Contact, HIRT acts as a coordinator within the Hitachi Group and between the Hitachi Group and external organizations to share information and prevent incidents, pursuant to the Guideline for the Information Security Early Warning Partnership program.
Through proper dissemination of vulnerability countermeasure and incident information, HIRT strives to prevent incidents, such as unauthorized access and virus infection, as well as to minimize the damage should incidents do occur.

Effort to Improve HIRT (Hitachi Group's CSIRT)

Each division/company within Hitachi Group has set up each IRT in order to strengthen cooperation with HIRT Center.

IRT activities within Hitachi group

Information Sharing
HIRT facilitates sharing of security information (for example, vulnerability countermeasure information, security alerts to respond to incidents) via mailing lists and websites to solve information security problems in the Hitachi Group.

Coordination and Consulting
HIRT coordinates vulnerability handling and incident response within the Hitachi Group and between Hitachi and the outside world in case vulnerability is found in Hitachi products and Hitachi-related websites.

Education
HIRT supports security education and security training using know-hows learned in IRT experiences.

HIRT's community activities

HIRT Open Meeting
A place to share information for HIRT Center and the IRTs in order to collaborate and promote vulnerability handling and incident response. It also allows HIRT community that is based on bonds of people to develop in the Hitachi group.

Advanced HIRT Open meeting
A place to share information among HIRT Centers and leaders CSIRT activities (Collaboration Support Members).More technical and advanced information has been exchanged.