HITACHI
Inspire the Next

[Abbreviation and Terms]

- **CERT/CC (CERT Coordination Center)**
  An institute that studies and solves problems with cybersecurity implications in the U.S.
- **CSIRT (Computer Security Incident Response Team)**
  An organization that leads to detect security incidents, collaborate with relevant persons/organizations and investigate causes and solve problems to minimize impacts and prevent recurrences.
- **FIRST (Forum of Incident Response and Security Teams**)
  A community of global CSIRTs built on the trust.
- **IPA (Information-technology Promotion Agency)**
  A public organization that promotes on mitigating the weaknesses of IT/ICS systems and preventing cyber attacks.
- **JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center)**
  An institute that studies and solves problems with cybersecurity implications in Japan.
- **JVN (Japan Vulnerability Notes)**
  A website that provides countermeasure information for reported vulnerabilities by "Information Security Early Warning Partnership".
- **NCA (Nippon CSIRT Association)**
  A community of Japanese CSIRTs built on the trust. Established in March 2007.
- **Incident (Cyber Security Incident)**
  A threat artifact event related to cyber security that can be malicious/intentional or accidental.
- **Information Security Early Warning Partnership**
  A public-private partnership framework to promote software product and web site security and prevent the damage to spread to the vast range of computers due to cyber attacks.
- **Vulnerability**
  A weakness in software and other products that could be exploited by cyber attacks, and impair their functions and/or capabilities.
- **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.

HIRT Hitachi Incident Response Team

For More Information

HIRT (Hitachi Incident Response Team)
Service Platform Business Division Group Information and Communication Technology Business Division, Hitachi Ltd.

Hitachi Omori 2nd Bldg., 6-27-18
Minamioi, Shinagawa, Tokyo, Japan 140-8572

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

2016.12

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.

The Hitachi Incident Response Team (HIRT) is an organization that supports Hitachi' s cyber security countermeasure activities. They contribute to the realization of a safe and secure network environment for customers and companies by preventing security incidents, and by providing a prompt response if an incident does happen.As the Hitachi Group's single point of contact for the outside world, HIRT proactively participates in the CSIRT communities, such as FIRST and Nippon CSIRT Association, and keeps working on improving information security for the global society.

The role of the HIRT is to provide ongoing assistance for Hitachi' s cyber security countermeasure activities through vulnerability handling (eliminating vulnerability that threatens cyber security), and incident response (evading and resolving cyber attacks), from the perspective of organization solo activities (information security initiatives targeted at Hitachi corporate information systems), and organization collaborative activities (initiatives to ensure product and service cyber security targeted at customer information systems or control systems). Furthermore, HIRT' s mission is also to contribute to a safe and secure Internet society by catching any signs of future threats and taking actions as early as possible. The HIRT has adopted an activities model consisting of four IRTs as listed below, in order to expedite both vulnerability handling and incident response.

The four IRTs are:

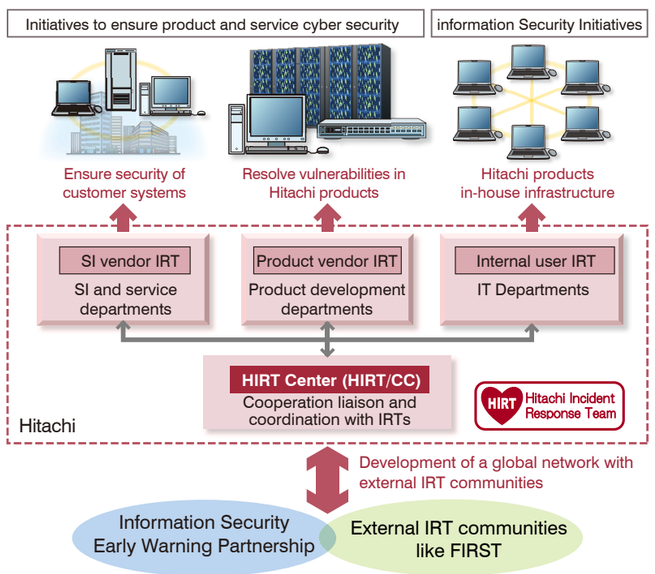
(1)The team that develops information and control system related products (Product Vendor IRT).

(2)The team that uses those products to develop systems and provide services to customers (SI (System Integration) Vendor IRT).

(3)The team that operates and manages Hitachi information systems as an Internet user (Internal User IRT).

As well as these three teams, there is also:

(4)A HIRT/CC (HIRT Center) will be put in place to adjust the work load between each IRT, and while making the role of each IRT clear, is a model that promotes efficient and effective security that promote inter-IRT cooperation.



Category	Role
HIRT/CC*	Corresponding sections: HIRT Center Promote vulnerability handling and incident response through collaboration with external IRT organizations like FIRST, JPCERT/CC*, and CERT/CC*, and SI vendors, product vendors, and between internal user IRT.
SI vendor IRT	Corresponding sections: SI/Service provision Support vulnerability handling and incident response for customer systems by ensuring the security of customer systems in the same manner as internal systems for vulnerabilities that have been exposed.
Product vendor IRT	Corresponding sections: Product development Promptly investigate whether any disclosed vulnerabilities have impacted products, and if there are problems, support measures to counter vulnerabilities in Hitachi products by providing a patch or other solution.
Internal user IRT	Corresponding sections: Internal infrastructure provision Support the advancement of vulnerability handling and incident response in order that the Hitachi related sites do not become a base point for invasion.

*HIRT/CC: HIRT Coordination Center
FIRST: Forum of Incident Response and Security Teams
JPCERT/CC: Japan Computer Emergency Response Team/Coordination Center
CERT/CC: CERT/Coordination Center
SI: System Integration

Four IRTs supporting vulnerability handling and incident response

Activities actioned by the HIRT Center

HIRT Center activities, in the capacity of internally-oriented IRT activities, include moving cyber security measures forwards on both a systematic and technical level by cooperating with information security supervisory divisions in charge of systems as well as quality assurance divisions, and assisting different divisions and Group Companies with vulnerability handling and incident response. Hitachi is also promoting cyber security measures formulated by collaboration between IRTs as a point of contact for external IRTs.

Internally-oriented IRT activities

Internally-oriented IRT activities include issuing alerts and advisories containing business knowledge obtained by collecting and analyzing security information to internal organizations, as well as providing feedback about products or service development processes in the form of guidelines or support tools.

(1) Collecting, analyzing, and disseminating security information

The HIRT Center disseminates information and business knowledge relating to vulnerability handling and incident response to the other teams through promotion of the Information Security Early Warning Partnership.

(2) Developing a framework for research activities

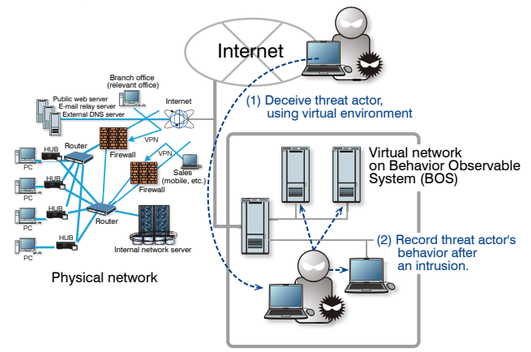
The HIRT Center is engaged in "Observation of Threat Actors Activities" as a technology to "catch any signs of future threats and take actions as early as possible". "Observation of Threat Actors Activities" is an observation method that uses a virtual environment of the organization's internal networks to investigate targeted attacks and other cyber attacks, and records and analyzes the behavior of a threat actor following an intrusion.

(3) Improving product and service security technology

The HIRT Center fleshes out security measures for products related to information and control systems, develops and administering those processes, and promotes the handing down of technology to expert personnel.

(4) Implementing IRT activities for individual domains

The HIRT Center promotes the investigation and organization of IRT activities specific to individual business domains in order to flesh out a response informed by the context and trends in each domain.



BOS (Behavior Observable System) for Observable Threat Actors Activities

Externally-oriented IRT activities

Externally-oriented IRT activities involve the cooperation of multiple IRTs in promoting the development of inter-organizational alliances with the objective of tackling new threats, and the development of cooperative relationships which can contribute to the mutual improvement of IRT activities.

(1) Reinforcing domestic cooperation of IRT activities

Organization of a foundation for information use and application based on JVN jointly operated by the JPCERT Coordination Center and the Information-technology Promotion Agency, Japan; the promotion of vulnerability handling based on the Information Security Early Warning Partnership; and the promotion of strengthening of partnership with the CSIRTs through the Nippon CSIRT Association.

(2) Reinforcing overseas cooperation of IRT activities

Organization of a system of collaboration between overseas IRTs that make use of FIRST activities and overseas product vendor IRTs, and the promotion of incident operations that utilize STIX and the like.

(3) Developing a framework for research activities

Joint research with academic organizations, fostering opportunities for personnel development through participation in academic research activities such as the Anti Malware Engineering Workshop, and promoting the education of researchers and engineers with specialist knowledge.