Hitachi Security Solution for Supporting Establishment and Operation of PSIRTs

In response to the recent increase in cyberattacks on IoT devices, companies that develop and manufacture devices are required to establish PSIRTs that are responsible for security measures throughout the entire product lifecycle, but in many cases, it is difficult to implement and operate such systems on their own due to a lack of human capital with the required security expertise. By utilizing its experience in providing a wide range of solutions as an IT vendor and its proven results and knowledge from building security organizations and improving governance as a manufacturer, Hitachi provides a PSIRT solution that supports customers from implementation to operation of the PSIRT. This article describes Hitachi's initiatives for ensuring product security and the available solutions.

Atsushi Suzuki
Yusuke Matsui

1. Introduction

With the proliferation of Internet-connected home appliances and connected cars, the risk of cyberattacks targeting Internet of Things (IoT) devices that incorporate open source and other technologies is increasing.

A number of vulnerabilities have been found that have a significant impact on manufacturers. For example, a US automaker found a vulnerability that could allow remote control of brakes, engine, and door unlocking and locking, while a medical pacemaker manufacturer identified a vulnerability that could cause heartbeat malfunction.

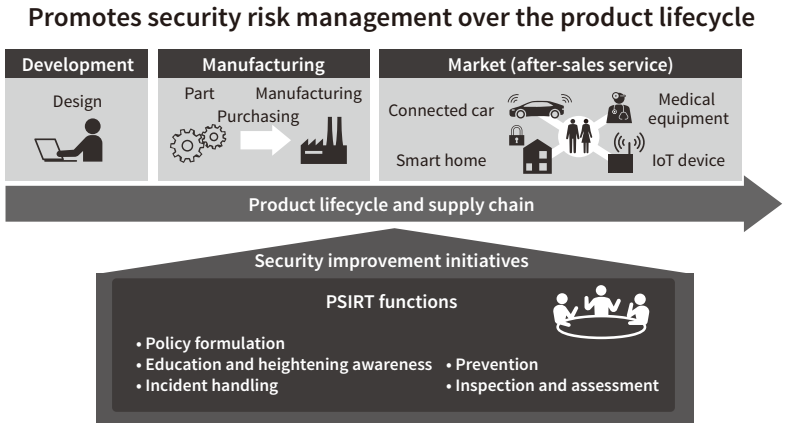
With this as a backdrop, companies are also required to comply with global security laws and regulations to ensure the security of their products and services, and they are strongly required to establish a system to promptly identify the causes of vulnerabilities and security incidents in their products and services, take action, and disclose information.

This is where the product security incident response team (PSIRT) comes into play. While the computer security incident response team (CSIRT) is an internal system and organization that responds to cyberattacks, the PSIRT is an internal system and organization that responds to security incidents related to the company's own products.

The role of PSIRTs is to conduct security risk management over the entire product lifecycle and supply chain, including development, manufacturing, and market (after-sales service), and to minimize the damage and impact when incidents occur in shipped products (see **Figure 1**).

2. Hitachi's Approach

Since 1998, Hitachi has established a system for PSIRT activities and has been implementing initiatives to deal with vulnerabilities in its products and services and to manage and improve the security quality of its products and services.



IoT: Internet of Things PSIRT: product security incident response team

Figure 1 — PSIRT and Product Lifecycle

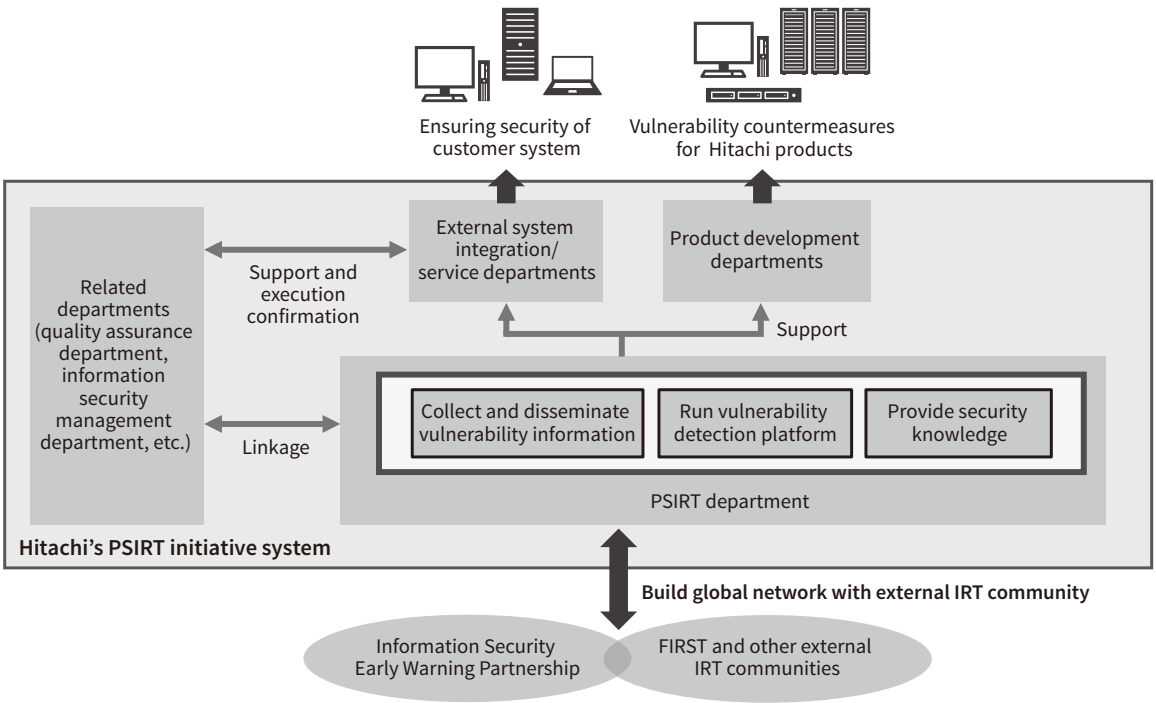
Security risk management is implemented for the entire product lifecycle, including development, manufacturing, and market (after-sales service).

2. 1 System for PSIRT Activities

PSIRT activities are implemented through coordination and cooperation with the product development departments that provide the products and services, system integration/service departments for customers, the PSIRT department that supports these initiatives, quality assurance departments, information security management departments, and other related departments. The product development departments and system integration/service departments should build security into the product or service, take action on disclosed vulnerabilities, and respond to incidents. The PSIRT department mainly coordinates the technical aspects in PSIRT activities, provides knowledge, and develops security enhancement measures in coordination and cooperation with related departments (see **Figure 2**).

Figure 2 — Overview of PSIRT Initiative System

PSIRT activities are implemented through coordination and cooperation with external system integration/service departments, product development departments, PSIRT departments, and related departments.



FIRST: Forum of Incident Response and Security Teams IRT: incident response team

2. 2
Overview of PSIRT Activities

In support of product development departments and system integration/service departments, the PSIRT department promotes two activities: (1) Pre-emptive measures against cyber threats, and (2) Enhanced resilience to cyberattack. An overview of each initiative is presented below.

(1) Pre-emptive measures against cyber threats

This activity is primarily focused on the collection, research analysis, and dissemination of vulnerability information. The collection of vulnerability information involves not only the collection of information released by product vendors, but also the collection of a wide range of vulnerability information on the company's products and services through implementation of the Information Security Early Warning Partnership* and cooperation with external incident response team (IRT) communities. This information is then disseminated within the organization. The PSIRT also operates a system for early detection of vulnerabilities in its products and services (vulnerability detection platform) and deploys it within the company. Many open-source software (OSS) and software components are used in each product and service. It takes considerable time and effort to manage the vulnerability information for each OSS/software component and to determine whether the product or service is impacted by the vulnerability. Consequently, a vulnerability detection platform is used for centralized management of vulnerability information and OSS/software configuration information of products and services. The vulnerability information and OSS/software configuration information are linked and managed, and if a software component of a product or service is affected by a vulnerability, the person in charge of the product or service is notified and urged to take action.

* A public-private partnership system based on public rules to facilitate the smooth distribution of vulnerability-related information on software products and web applications and to promote the use of vulnerability countermeasures.

(2) Enhanced resilience to cyberattack

This initiative is used to maintain security knowledge in order to build security into products and services. In the midst of a changing business environment, including the spread of cloud-native technologies, artificial intelligence (AI), and increasingly sophisticated cyberattacks, the PSIRT compiles information obtained from international standards, knowledge from outside the company, and internal case studies into guides and checklists that can be easily used by development staff, with the aim of strengthening resistance to attacks, and this information is disseminated within the company.

3. PSIRT Solution

This chapter describes the Hitachi PSIRT solution, which utilizes Hitachi's experience in providing solutions as an IT vendor and its expertise in building security organizations and maintaining governance as a manufacturer.

Figure 3 shows an overview of the Hitachi PSIRT solution. The Hitachi PSIRT solution is divided into consulting solutions and platform and operation solutions, and this section provides an overview of each solution type. Examples of customer applications of each solution will also be presented.

3. 1
Consulting Solution

(1) Solution overview

Hitachi provides a one-stop consulting service to support PSIRT management to strengthen governance in customer companies.

First of all, PSIRT establishment and planning supports the following four steps for rapid establishment of the PSIRT: Analysis of the current situation, implementation of a system, process development, and documentation. Using

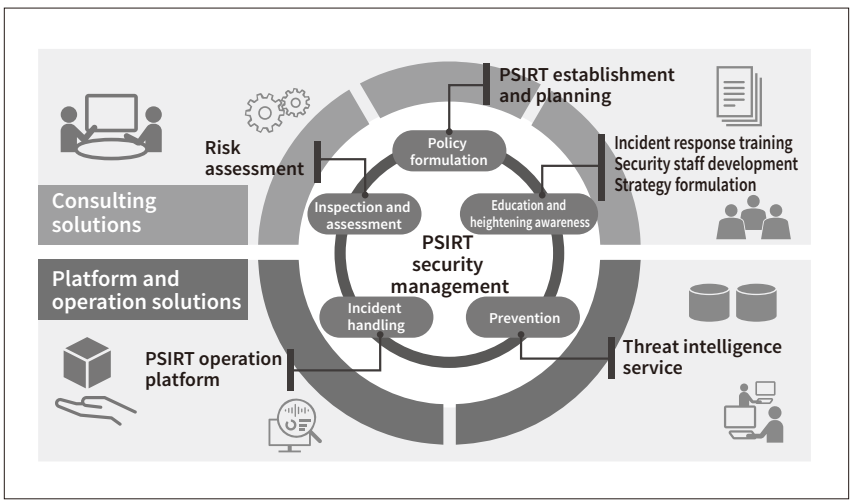


Figure 3 — Overview of Hitachi's PSIRT Solution

Hitachi provides consulting solutions aimed at strengthening the governance of customer companies, and platform and operation solutions aimed at reducing the operational burden on customers, speeding up incident response, and eliminating dependence on individual skills.

templates based on Hitachi's extensive experience in establishing CSIRTs and PSIRTs in the fields of IT and product control systems, as well as Hitachi's experience in initiatives such as collaboration by its own PSIRTs with internal and external stakeholders, Hitachi will build an effective PSIRT organization and support event analysis using the Common Vulnerability Scoring System (CVSS), a quantitative evaluation index based on international standards.

In incident response training, training scenarios are developed based on the customer's organization and products, and desktop incident response training is conducted. To raise the awareness of the people in charge in the relevant departments, bottlenecks are identified in the existing workflow and procedure manuals used by the departments undergoing training, and support is provided to discover any issues and provide improvement proposals and reviews.

The risk assessment service is a comprehensive threat identification and quantitative risk assessment service that uses the what, where, when, who, why (5W) method and spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege (STRIDE) method for the products and services of the customer company. Effective security measures and schedules are determined for the identified threats.

(2) Application example

Figure 4 shows an application example of PSIRT establishment and planning. In this case, Hitachi assisted in establishing a PSIRT using the PSIRT framework provided by Forum of Incident Response and Security Teams (FIRST) to help the customer comply with international laws and regulations. After assessing the current situation of the customer organization, the company defined the purpose and role of the PSIRT and clarified the mission to be performed as a PSIRT within the customer. It also defined the workflow, organized the stakeholders, established the necessary systems for execution, and prepared various procedure manuals.

3. 2
Platform and Operation Solutions

(1) Solution Overview

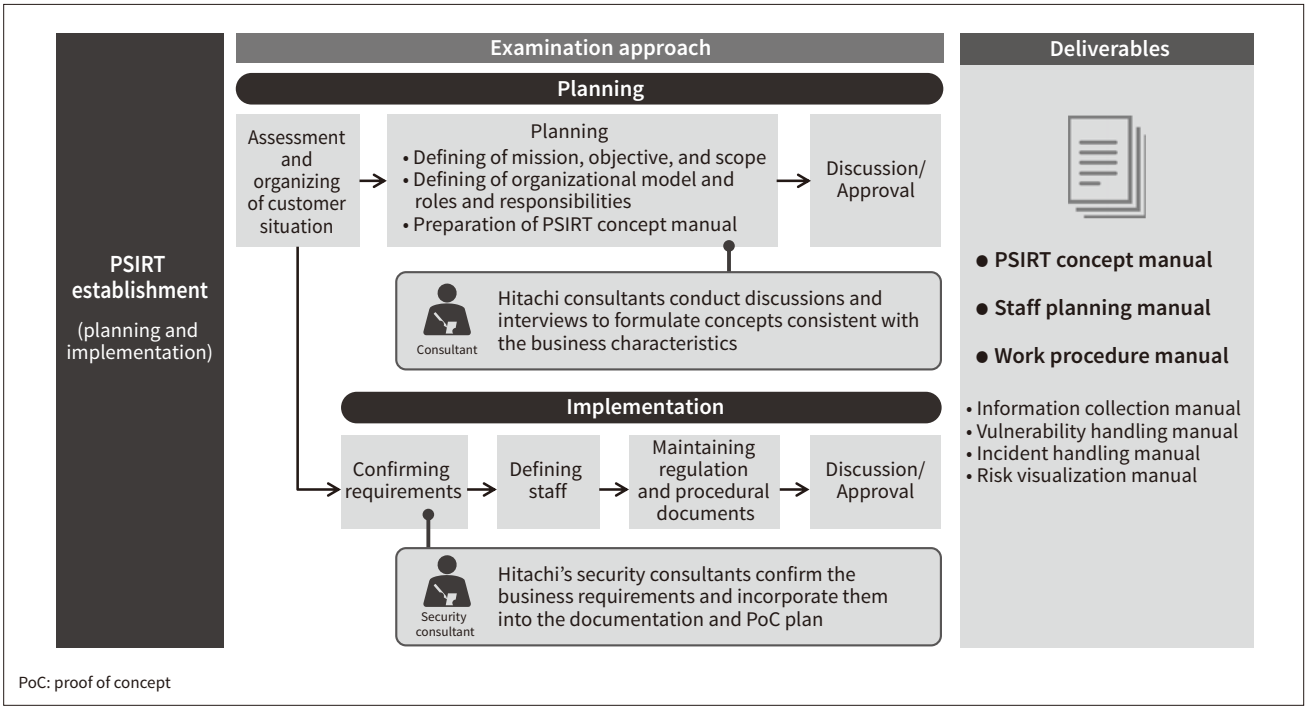
The operational area of the PSIRT includes a mechanism for analyzing and centrally managing threat and vulnerability information. This reduces the operational burden on customers, speeds up incident response, and eliminates dependence on individual skills.

In the threat intelligence service, Hitachi conducts highly specialized PSIRT operations, such as information collection, sorting, and impact analysis as an outsourcing service, and selects threat and vulnerability information related to the customer's industry, products, and services, and evaluates their impact on products.

The incident response service provides a platform for centralized management of threat and vulnerability information and product configuration information for enabling automation of some operations. In addition to reducing the operational load, the system supports faster and more reliable incident response.

Figure 4 — Application Example of PSIRT Planning

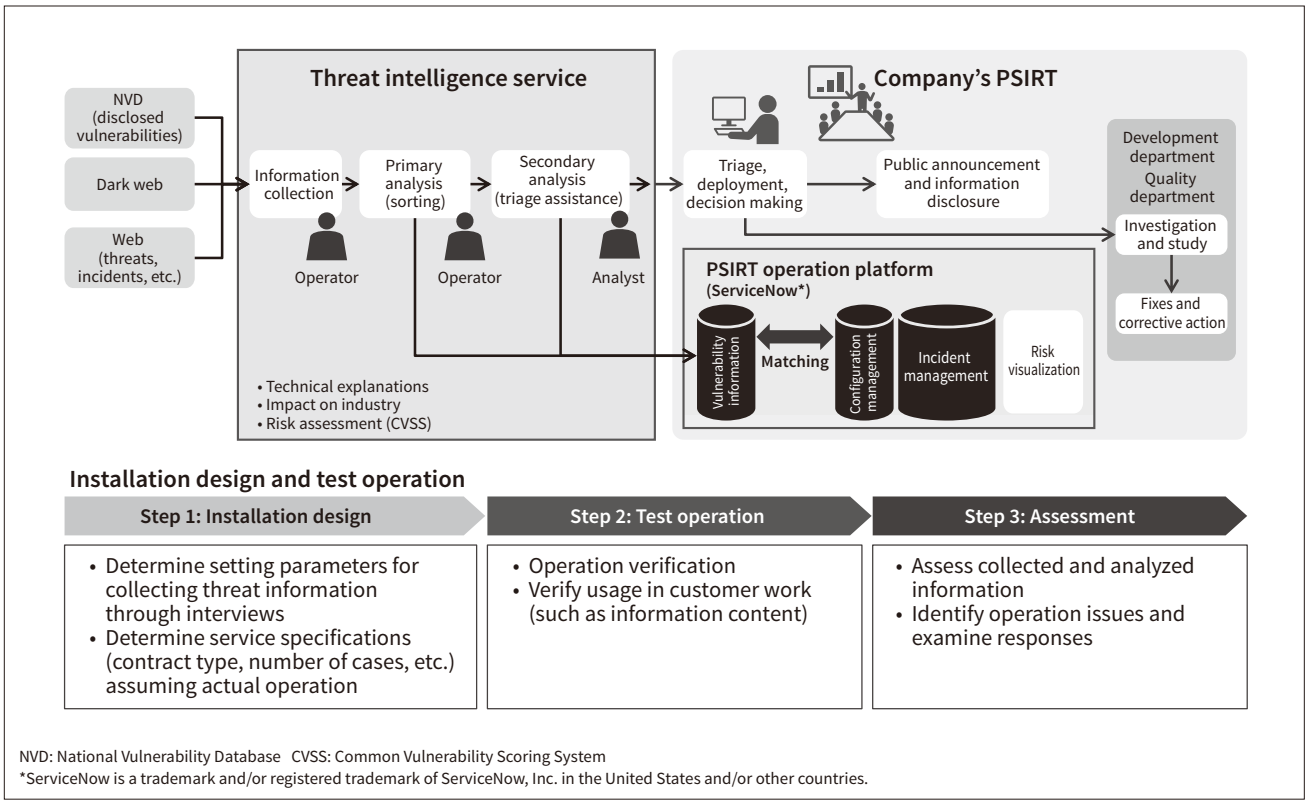
To help customers set up their PSIRT, Hitachi examines how things should be after an assessment of the current situation, and supports the preparation of organizational concepts and various work procedure manuals.



PoC: proof of concept

Figure 5 — Application Example of Threat Intelligence Service and Operation Platform

The work of collecting and sorting information for customers' PSIRTs is outsourced to Hitachi for providing technical explanations of the collected information in the form of reports.



NVD: National Vulnerability Database CVSS: Common Vulnerability Scoring System

*ServiceNow is a trademark and/or registered trademark of ServiceNow, Inc. in the United States and/or other countries.

(2) Application example

Figure 5 shows an example where a platform and operation solution is provided.

In this case, Hitachi is providing threat intelligence services to a PSIRT owned by a customer in the manufacturing industry. Using the information collection tools of this service, Hitachi collects information on publicly-disclosed vulnerabilities and information on undisclosed threats and vulnerabilities on the dark web, and provides information that is closely related to the customer company and its products. Hitachi analysts prepare analysis reports on the target information and provide them on a weekly basis.

4. Conclusions

This article described Hitachi's own efforts and the solutions it offers to its customers for security measures against threats that are increasing as products become more IoT-compatible and connected.

In the future, Hitachi will expand its solutions by focusing on upgrading and automating PSIRT operation to include a product security operation center (PSOC), which monitors and responds to attacks on products in real time, and security orchestration, automation, and response (SOAR), which monitors security incidents and makes decisions efficiently on a common platform.

Authors

Atsushi Suzuki
Integration and Service 3 Department, Engineering Services Operation 1, IoT & Cloud Services Business Division, Service Platform Business Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Security consulting for industry.

Yusuke Matsui
Hitachi Security Technical Center, Cyber Security Technology Operations, IoT & Cloud Services Business Division, Service Platform Business Division, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research:* Planning measures to ensure the security of products and services.