HITACHI
Inspire the Next

Information Security Report 2018

Hitachi Group

Greetings

The Hitachi Group is engaged in the social innovation business, where we use digital technologies to create new value through collaborative creation with our customers and partners. The foundation of the social innovation business is the IoT platform Lumada, which facilitates the use of artificial intelligence and big data analysis techniques. The Hitachi Group is expanding its social innovation business, with Lumada at its core, to contribute to the achievement of the goals of Society 5.0, a project being implemented by the Japanese government for the purpose of creating a safe, secure, comfortable, and sustainable next-generation digital society.

It is widely recognized that the biggest challenge related to Society 5.0 is information security. As the advancement of digital technologies accelerates day by day, the severity of threats to information security increases at a similarly accelerated pace. Sophisticated and diversified cyberattacks and security threats, such as information exploitation, targeted emails, fake news, manipulation of Internet opinions, and damage to critical infrastructure facilities, pose a grave threat that fundamentally undermines our trust in a digital society.

In May 2017, the Hitachi Group suffered a cyberattack involving a worm-type ransomware program, and some of our internal systems, including the email system, were damaged. Based on this experience, we further enhanced our information security framework. We created the position of CISO (Chief Information Security Officer), and an organizational system for global information-security governance, led by the CISO, began operation in October 2017.

In March 2018, the Japanese Business Federation published its “Declaration of Cyber Security Management” . This declaration states that efforts related to cybersecurity measures are an important management issue, both from the perspective of value creation and from the perspective of risk management. The Hitachi Group shares this vision, and is engaged in efforts to improve information security. Based on our “Information Security Policy” , which was created from a management perspective, we globally apply an information-security PDCA cycle by improving our rules and organizational systems, educating general employees and security experts, monitoring security through audits, and implementing security measures by using IT technologies.

Collaboration among industrial, academic, and government sectors is essential to information security. Hitachi Group has made efforts to provide the details of the ransomware incident that occurred in May 2017, as well as the lessons we learned from that incident, to external parties. As the Hitachi Incident Response Team continues to lead our efforts to accumulate case studies of countermeasures taken within the Hitachi Group, we will also continue to share our expertise through various collaborative efforts between the private sector and the government. The spirit of collaborative innovation is the core of our social innovation business, and by displaying this spirit in our information security efforts, as well, we can contribute to ensuring trust in Society 5.0.

I would be delighted if this report could help with the understanding of our information security activities and be of use to society.

Keiji Kojima
Executive Vice President and Executive Officer, CISO Hitachi, Ltd.

Information Security Report

INDEX

〈Overview of this report〉

- Scope of this report: This report covers information security initiatives taken by the Hitachi Group in FY 2017 and earlier.
- Publication of this report: This report was published in September 2018.

Lessons learned from the cyberattack incident and our efforts to improve the robustness of our internal systems

In May 2017, the Hitachi Group suffered a cyberattack involving a worm-type ransomware program called WannaCry. This attack resulted in the stoppage of our internal systems, and had an impact both on the Hitachi Group and on external parties. The advent of the IoT era is upon us, and in order to deal with the increasing threats to cybersecurity, we have decided to handle information security governance as the most important issue facing our business. In October 2017, we established a special organization for security control. This organization is led by the CISO, and is intended to improve the robustness of our systems in terms of management and technology.

1. Introduction

The Hitachi Group considers information security measures against new threats such as rapid cyberattacks to be one of our most important business issues. As such, we are promoting both governance-related and technological efforts to improve the robustness of our systems against cyberattacks.

2. Looking back on the cyberattack incident

2.1 Overview of the cyberattack

On May 12, 2017, a worm type ransomware program called WannaCry spread from Europe to infect systems all over the world. This virus exploits a vulnerability in Windows to spread to other vulnerable Windows systems via a network. In an infected system, files are encrypted and a threatening message appears saying that money must be paid in exchange for the decryption key. Within the Hitachi Group, the virus spread from a test device at a subsidiary in Europe to other devices, including servers for the internal network. The virus caused damage on a global scale.

2.2 Scope of impact

This incident impacted various devices that were connected to the internal network. Affected devices included everything from business system servers and PCs for office use that were managed by the information systems division, to systems such as manufacturing and production systems for factories, control devices and warehouse systems, and access control systems for facilities. Figure 1 shows the number of packets intended to spread WannaCry to other devices that were discarded from our outgoing firewall during the period beginning on May 12.

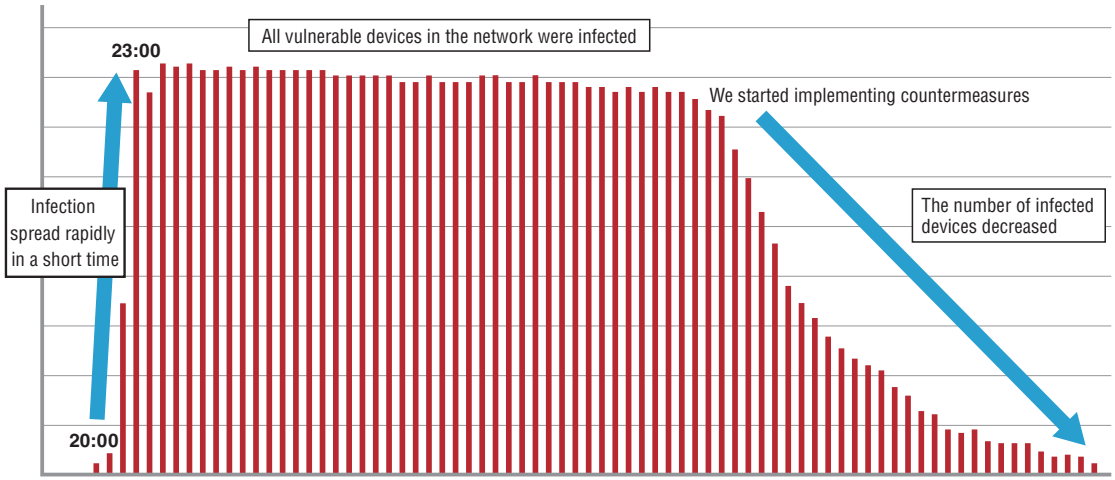
The infection started at about 8:00 p.m., and two hours later, at 11:00 p.m., it reached its saturation point, spreading to all devices for which vulnerability countermeasures were not in place. After that, the number of infected devices and the number of packets decreased, as a result of using antivirus software to quarantine infected devices, and of applying patches.

3. Lessons learned from the cyberattack incident

We learned four lessons from the cyberattack incident. The first lesson relates to the structure of the network. To eliminate segmentation, we had adopted wide-area Ethernet for our internal network, with the assumption that antivirus measures would be implemented at endpoints. As a result, the worm-type virus was able to spread quickly once an endpoint had been infected. Another cause of the infection was the fact that the endpoint in question was connected to the network while its security status was unknown. To improve upon these issues, it is important for our network to have monitoring functions that include security and recovery as prerequisites.

The second lesson we learned is that security measures were insufficient for server systems that operate 24 hours a day as a result of globalization. Because some important servers could not be stopped, patches could not be applied quickly to those systems, even if vulnerabilities were present. These servers were particularly susceptible to damage. It is important to change our awareness from a baseless mindset where we feel that patches do not need to be applied, to a mindset that considers patch application to be essential, and to promote the application of patches as part of our company-wide system operations.

Figure 1. Infection speed of WannaCry >>



The third lesson we learned involves the difficulty of implementing security measures for IoT devices. Like the test device that was the source of the ransomware infection, there are many devices for which patch application is not considered a requirement, although they use Windows, and many devices for which user companies do not think that system updates are necessary. This lesson made us realize how difficult it will be to take measures for these devices in the future. Unlike ordinary devices for office use, different countermeasures such as network-based countermeasures must be taken, under the assumption that these devices might be infected with a virus because they have no antivirus software and patch application might not be possible.

The fourth lesson that we learned is that the business continuity plan for IT (the IT-BCP) that we use for natural disasters is totally different from the IT-BCP that is needed for a cyberattack. In case of a natural disaster, such as an earthquake, we store data in a remote location and always synchronize it with the primary data as a backup for resuming business operations quickly. In the case of the ransomware infection, however, the files that were encrypted by the ransomware were also synchronized and backup data was destroyed. As a result, recovery took a great deal of time. When we consider the fact that malware such as ransomware can destroy data, it becomes clear that we must reexamine our way of thinking about the kind of backup data that is needed for recovery. In business continuity plans (BCPs) for both natural disasters and cyberattacks, measures must be implemented by assigning top priority to preserving human life and to recovering business operations.

When handling an incident, the worst possible scenario must be considered and the possibility of enormous damage must be kept in mind. To handle these possibilities, it is important that we create manuals and training programs and improve on-site capabilities based on anticipated attack scenarios.

Based on these lessons, we decided to focus on six elements of governance, as shown in Figure 2, to improve the robustness of the Hitachi Group against cyberattacks. A dedicated Group-wide information security division was established to improve our organizational system to promote security governance.

4. Enhancing the organizational system for security governance

Because of the increasing threat of new cyberattacks and the expansion of our business into fields such as the IoT and cloud domains, we regard information security governance as one of our most important management issues. In October 2017, the responsibilities related to information security that were formerly assumed by the CIO were divided, and the new position of Chief Information Security Officer (CISO) was created. A dedicated organization for managing the security of the entire Hitachi Group was formed under the CISO to collectively promote the information security governance of the whole Hitachi Group.

The security control function, which was formerly a part of the IT control function, was thereby clearly separated, and an organizational system was established to enforce governance for the entire Group.

The control organization reports to the executive committee its analysis of the impact of information and cybersecurity risks on business and the status of relevant countermeasures. It also provides instructions regarding these measures, thereby ensuring continuous improvement. When an incident occurs that affects the entire Hitachi Group, the control organization determines whether to stop systems and provides suggestions. This dedicated organization includes the SOC (Security Operation Center), which monitors cyberattacks 24 hours

Figure 2. Efforts related to governance >>

i **Design of a BCP for handling cyberattacks**
Design a BCP that takes into account the perspectives of cybersecurity and globalization, in addition to the BCP for handling a natural disaster.

ii **IT measures based on business risk analysis**
Implement IT measures that take into account the comparative importance of information assets.

iii **Mandatory security patch application as a part of patch management**
Establishing an organizational structure that can manage not only IoT devices and physical security but also on-site devices.

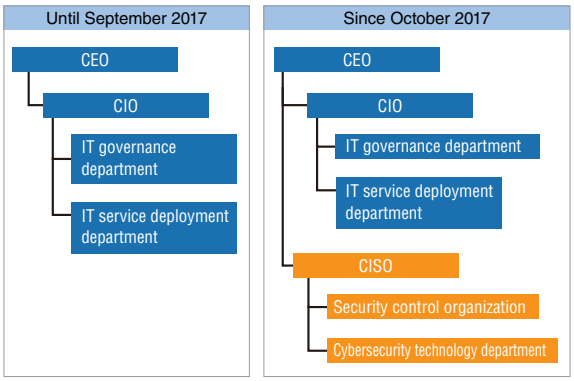
iv **Establishment of an organizational system for centralized management, by revising the management scope and authority of IT managers**

v **Global governance of security management**
Examine our system of governance, including country-based regions.

vi **Creation of IoT security guidelines**

→ **Establish a dedicated, Group-wide information security division.**

Figure 3. Organizational system and roles surrounding the CISO >>



Roles of the CISO and the security control organization:

a) Continuously implement cybersecurity management and information security management.

b) When an incident occurs that affects the entire Hitachi Group, determine whether to stop systems, and provide suggestions.

c) Periodically report to the Hitachi executive committee regarding the impact of residual risks on management and countermeasures against such risks, and implement the relevant countermeasures.

a day, 365 days a year, and the HIRT (Hitachi Incident Response Team), which enhances incident response.

As shown in Figure 4, we have organized the PDCA activities to be conducted under normal conditions, as well as an organizational structure for emergencies. When a cyberattack occurs that affects business activities, an emergency response headquarters straddling all Corporate divisions is established to handle the attack in cooperation with the cybersecurity section of each company. As part of the emergency response headquarters, each Corporate division works with the control organization to implement specific measures (such as issuing instructions, assessing the situation, or engaging in external relations with entities such as the police, the media, or government offices).

5. Technical enhancements

As we enhance our organizational system for governance, we are also making technical enhancements to monitoring and incident handling, in order to detect attacks at an early stage and respond to such incidents quickly. Since the WannaCry attack, we know that we must also prepare for possible attacks by its variants. We plan to introduce enhancements gradually in multiple phases, and steadily carry out our plans.

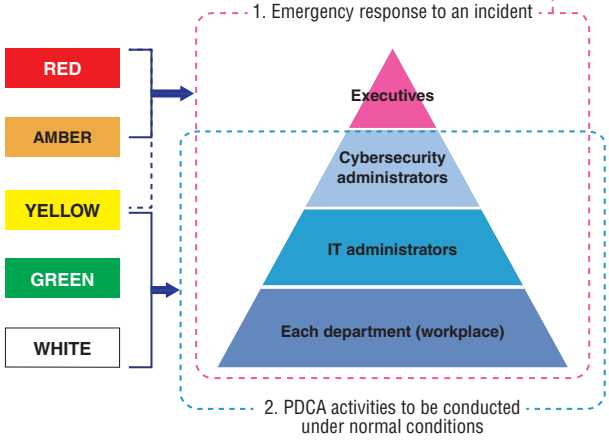
5.1 Measures to improve robustness, Phase I

In Phase I of our measures to improve robustness, we prioritized quick-acting measures, and made efforts based on our current operations to detect attacks at an earlier stage, and to make decisions and implement responses more quickly. Because each of our internal networks and business systems was independently operated and managed by the department in charge of the specific network or system, the monitoring department did not sufficiently understand the structure or details, and did not monitor the logs acquired for operational purposes. In an internal network with a flat structure, the increase of even a single monitoring point can lead to early detection. For this reason, we took inventory of the devices and systems managed by each section to gain an understanding of what was located where. We also checked which logs could be acquired and started to monitor the logs that were useful for detection, thus making early detection possible.

Because threats have been changing rapidly in recent years, we need to implement flexible monitoring measures to handle those changes. The operational procedures that were provided by the monitoring department were incomplete, and described only the common checks and measures. They assumed that the reader had expert-level knowledge, and were abstract. Therefore, if an emergency like the WannaCry incident were to occur when no such expert is present, it was likely to take time before a response could be implemented, and damage was likely to spread in that time. By revising the procedures to be followed in an emergency, we created manuals that enable even persons with a basic level of prerequisite knowledge to quickly and confidently make

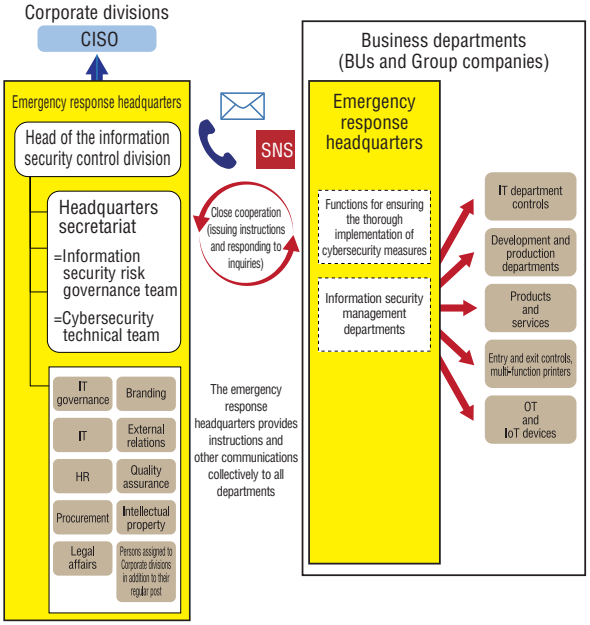
Figure 4. Cyberattack warnings and contact system of the emergency response headquarters >>

1. Relationship between cyberattack warning levels and the responders at each BU or Group company



	Action category	Action description
1	Emergency measures	• Establish the emergency response headquarters • Start the cyber-BCP plan (system protection activities) • Provide instructions to employees
2	Security PDCA activities to be conducted under normal circumstances	• Implement PDCA for the security management cycles for products and services, for development and production, and for OT and IoT devices • Implement vulnerability countermeasures • Carry out the plan for improving robustness (promote measures for improving robustness, assess residual risks, and understand and report to executives the impact of such risks on business) • Conduct security-enhancement and awareness-building activities for employees

2. System of cooperation with the emergency response headquarters in the event of an emergency



When an emergency occurs for which the cyber-BCP must be launched, establish the corporate-wide emergency response headquarters and implement measures through collaboration with each BU's and Group company's functions for ensuring the thorough implementation of cybersecurity countermeasures.
Each corporate section implements the relevant measures set forth by the emergency response headquarters.

decisions and implement a response.

Because previous manuals put an emphasis on targeted attacks occurring in Japan, we distinguished measures to be used in Japan from those to be used outside Japan. The WannaCry incident proved that an incident occurring outside Japan could cause major damage to our assets in Japan. Therefore, under the assumption that the measures that were already implemented for Japan would also be implemented in other countries, we set up an organizational structure that could receive incident reports and respond to incidents on a global scale 24 hours a day, 365 days a year. This enables us to quickly handle incidents representing a high level of risk.

5.2. Measures to improve robustness, Phase II

In Phase I of our measures to improve robustness, we enhanced security monitoring. First, we investigated the possibility of expanding the monitoring infrastructure to further enhance monitoring. We examined the idea of expanding the existing monitoring infrastructure of each company, and determined that we needed to quickly enhance monitoring both inside and outside Japan, while also keeping costs in mind. We decided to carry out this expansion based on the managed security service (MSS) of each company, and decided to adopt the Hitachi Group' s MSS because it can provide a wide range of services, from security monitoring to incident response when an incident occurs.

Next, to enhance monitoring on a global scale, we determined the target systems and network monitoring points, and made arrangements for the linkage and monitoring of the logs from each system and network device throughout our global network. Sites subject to monitoring include those in Japan, as well as sites belonging to Hitachi Europe, Hitachi America, Hitachi Asia, and Hitachi China.

For the monitoring mechanism, the logs from the systems and network devices at each target site were aggregated to the MSS monitoring infrastructure, and correlation analysis was conducted. If a site was subject to rules and laws, such as the General Data Protection Regulation (GDPR) in Europe, which prevents data containing personal information from being transferred outside Europe, correlation analysis was limited to on-site analysis, and logs were aggregated to and analyzed and monitored by the MSS monitoring infrastructure. This enables earlier detection of cyberattacks targeting the Hitachi Group, as well as faster implementation of countermeasures and faster recovery via incident response.

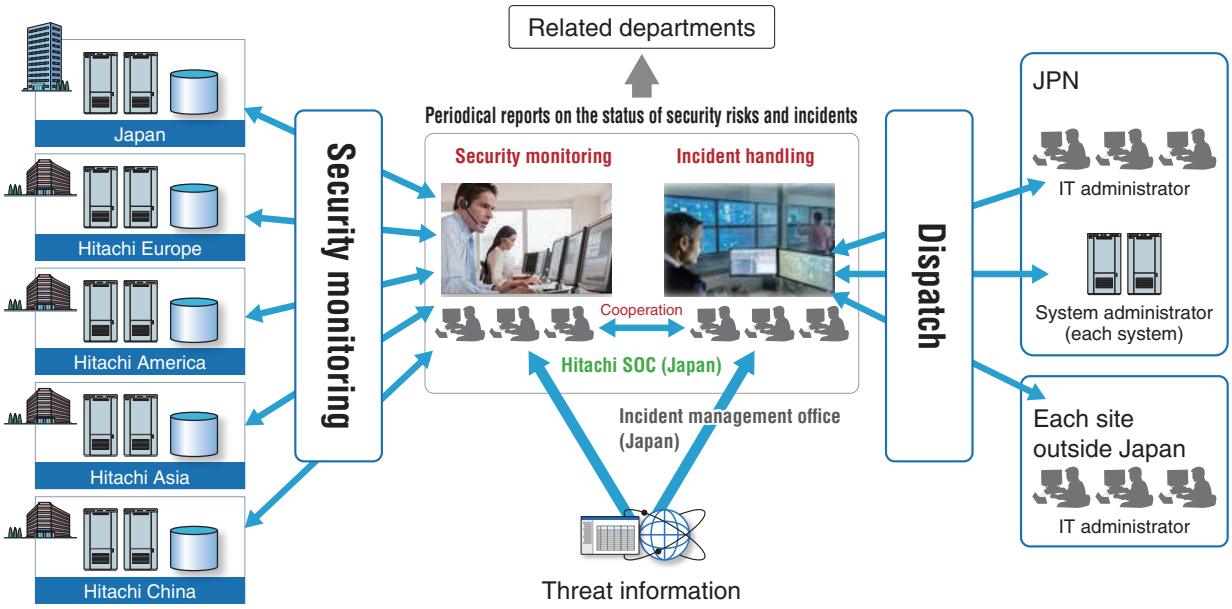
Currently, the SOC performs monitoring 24 hours a day, 365 days a year. However, IT managers and IT administrators at different sites conduct different operations, and some sites cannot provide 24-hour-a-day, 365-day-a-year support. In the future, efforts will be needed to address this issue.

Time differences may also cause delays and gaps in global measures. We will continue our efforts to minimize the damage caused by cyberattacks by accelerating the steps to be taken, from initial response to countermeasures, when an incident occurs.

6. Conclusion

We began our efforts to improve the robustness of our internal systems, based on the lessons learned from the recent cyberattack incident, by improving the robustness of IT systems used for general devices for office use. Measures are easy to implement for these systems, but we also need to expand our measures to manage all security risks facing the Hitachi Group inside and outside Japan, including risks facing our product and service businesses and our in-house development and production facilities. Target devices and systems also include IoT and control systems and all devices that are connected directly or indirectly to in-house networks or cloud environments.

Figure 5. Enhancement of global security monitoring >>



Basic approach to information security governance

Policy on information security governance initiatives

Hitachi regards initiatives for information security as vital for the safe management of information assets stored for customers in business operations that provide safe and secure social infrastructure systems. We have established information security initiatives policies shared by the Group, and are promoting enhanced information security activities.

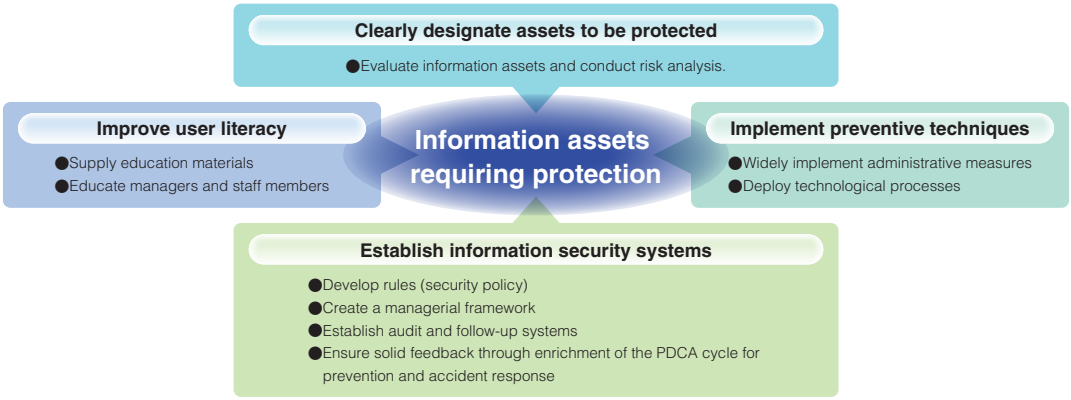
Approach to information security initiatives

Our approach to initiatives in information security encompasses four perspectives: ① Establishment of information security systems; ② Clearly designate of assets to be protected; ③ Improving user literacy, and; ④ Establishment of different types of security measures. We are making steady progress on action items for each of these perspectives.

Of these items we are paying particular attention to precautionary measures and prompt accident response, as well as improving staff ethical and security consciousness.

Furthermore, information security management PDCA (continuous improvement of activities) is moving forwards through the leadership of Hitachi, and we are working hard to improve security levels of the Group overall.

Basic approach to information asset protection >>



(1) Precautionary measures and prompt security response

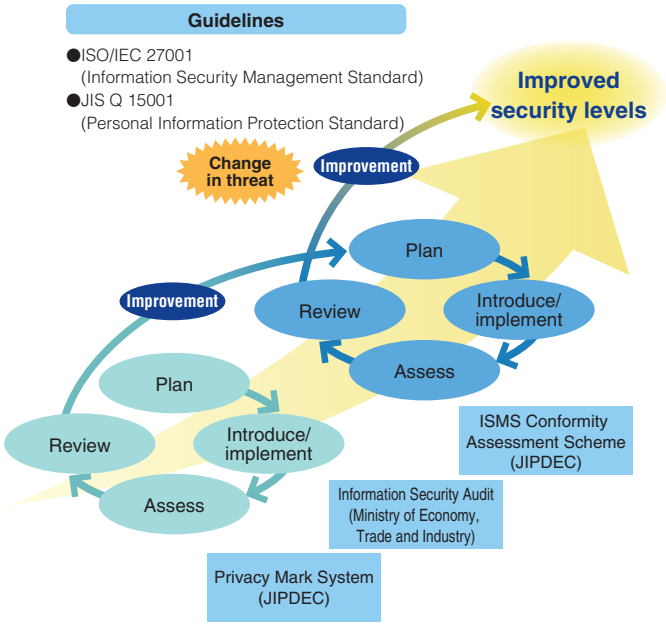
We clarify assets to be secured and have implemented safeguarding measures based on vulnerability and risk analyses.

We also have an emergency manual which we use for security breaches, based on the assumption that accidents do happen.

(2) Improving ethical and security awareness among staff members

We have prepared a program tailored to Hitachi' s various personnel levels including management and supervisors, and are working to improve ethics and security awareness through Group-wide e-learning. We are also conducting audits to identify and address problems at an early stage.

The PDCA cycle for security level improvement >>



Information Security Management System

Information security promotion and management cycles

Introducing Hitachi policies regarding information security, structures for promoting information security, regulations regarding information security, and information security management cycle.

Information security policies

As a global company representing Japan, Hitachi recognizes cyber security risks as one type of management risk. In order for us to announce (to those inside and outside the organization) a policy for the entire organization, we are making our utmost efforts to ensure information security by establishing information security policies and related guidelines, such that they take into account cyber security risk management and are in accordance with the enterprise management policy.

Based on this policy, we are expanding information security measures that support every aspect of business activities: such as enhancing cyber security, preventing information leakage caused by human errors, and protecting personal information such as social security and national ID numbers.

Information security policies >>

1. Formulation and continuous improvement to information security management regulations
We recognize information security initiatives as a major issue in management as well as business activities, and establish information security management regulations that comply and adapt to laws and other standards.
Furthermore, we establish information security management systems for the whole company that center on our executive officers, which we implement faithfully.
In addition, we maintain and continuously improve information security in terms of organization, human resources, physical systems, and technology.

2. Protection and continuous management of information assets
We plan safe management systems in order to appropriately protect information assets we handle from threats to confidentiality, integrity, and availability.
We also take appropriate control measures for business continuity.

3. Strict observance of laws and standards
We strictly observe laws and other standards regarding information security.
We also make our information security regulations conform with such laws and other standards.
If these are found to be violated, we check staff working regulations and take the appropriate action.

4. Education and training
We conduct education and training in order to increase executive officer and staff member awareness of information security.

5. Incident prevention and management
We strive to prevent information security accidents from occurring, and in the case that an accident occurs, promptly take the appropriate measures, including measures to ensure the accident does not happen again.

6. Assurance of fair business practices within the corporate group
We will construct a system to ensure fair business practices in the corporate group made up of Hitachi, Ltd. and Hitachi, Ltd., Group Companies, according to policies 1 to 5 listed above.

Information security promotion

The President will appoint the Chief Information Security Officer with rights and responsibilities towards information security, and the Information Security Chief Auditor with rights and responsibilities towards information security auditing.

The Chief Information Security Officer will set up the Information Security Committee, and determine policies, educational programs, and different measures regarding information security.

Decisions made by the Information Security Committee will be implemented at each business site through the Information Security Promotion Council attended by working-level employees from all business sites.

The person who responsible for each business site will be appointed to the Information Security Officer.

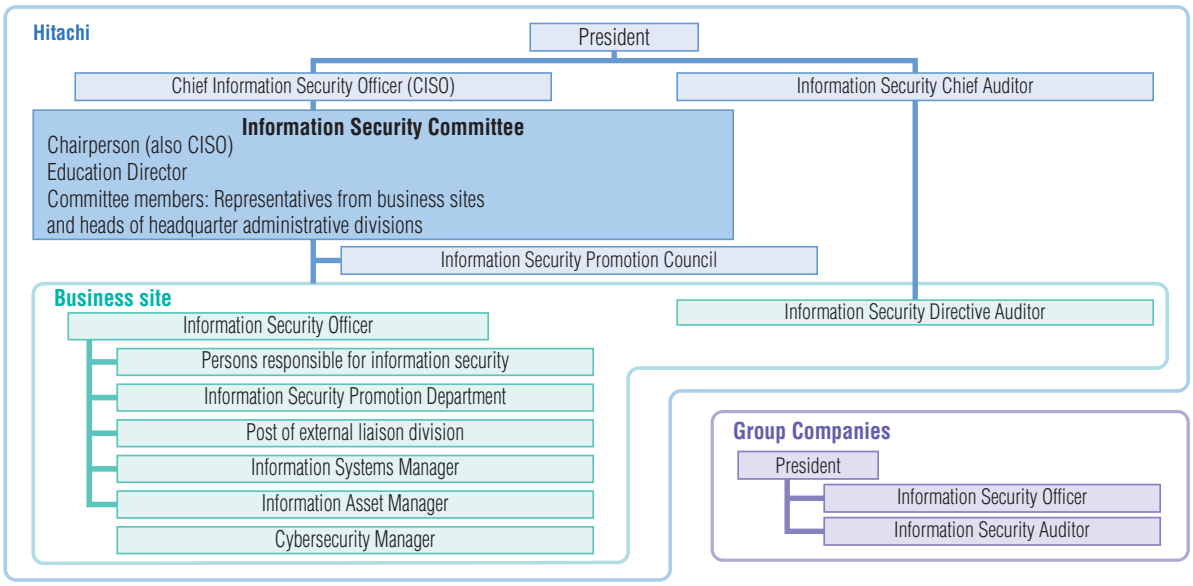
An Information Security Promotion Division will also be established, which will deal with personal information protection, information security, management of confidential information, entrance/exit management, and vendor management across all business sites in an integrated manner, as well as implement educational activities to promote a thorough awareness of information management amongst staff members at business sites.

An Information Asset Manager will be placed in all divisions, and responsibilities will be allocated regarding handling of information assets.

A similar organization will be established in Group Companies, and there will be mutual cooperation to promote information security across divisions.

Information Security Management System

Information security promotion >>



CISO : Chief Information Security Officer

Information Security Management System

Information security regulations

As displayed in the table below, we have established regulations based on information security policies.
Group companies have also established equivalent levels of regulations, and are promoting information security.

Information security regulations >>

Category	Regulation name	Details
Basic regulations	General Rules for Information Security Management Systems	We have established basic conditions relating to the formulation, implementation, maintenance, and continuous improvement of the Information Security Management System, based on the "HITACHI Company Conduct Standards", and aim to ensure the confidentiality, integrity, and availability of Hitachi's information assets including personal information, protecting this information.
	Information and Information Equipment Handling General Provisions	We have established basic conditions relating to handling and management of information and information equipment, and aim to promote the safe use of information, as well as prevent leaks of information overall by mediums such as paper and in information or other systems, and accidents caused by the misappropriation of information, by strict observance of regulations.
	Management Regulations for Confidential Information	We have established provisions necessary for the handling of confidential information based on the "HITACHI Company Conduct Standards", and aim to maintain confidentiality.
Individual regulations	Rules on Website Creation and Information Disclosure	We have established provisions requiring strict adherence so that information is disclosed and used correctly, and aim to provide an environment in which customers and staff members can use information effectively and with ease of mind.
	Systems Management Regulations for Information Security	We have established basic management provisions regarding information systems based on the "General Rules for Information Security Management Systems", aiming to ensure information security.
	Management Regulations for Entrance/Exit and Access Restriction Zones	We have established necessary provisions regarding the principals of entrance/exit management and premises access restrictions, as well as the designation of prohibited areas and their management and operation, and aim to protect confidential information.
Management of personal information	Management Regulations for Personal Information	We have established provisions to be strictly adhered to regarding the appropriate protection of personal information in accordance with laws and guidelines stipulated by the national government regarding the handling of personal information, and aim to protect the rights and interests of the individual, as well as prevent business losses and loss of social credibility. We have established the provisions, procedures etc. necessary to fulfil our responsibilities regarding operation/management systems creation, management regulation implementation and strict adherence, and personal information protection.
	Consignment Criteria for Business Handling Personal Information	We have established specific procedures for situations in which personal information stipulated in the Management Regulations for Personal Information is consigned to external vendors, and aim to manage and protect personal information in an appropriate manner by preventing external leakage, manipulation, destruction, or loss of personal information we possess.

●Three Principles for Preventing Leakage of Confidential Information

Hitachi has formulated Three Principles for Preventing Leakage of Confidential Information, and always pays sufficient caution to the handling of its own and its customers' information, working to prevent information leaks.

Principle 1: In principle, no confidential information shall be taken outside of the company's premises.
Principle 2: Any person taking confidential information out of the company's premises when necessary for conducting business shall obtain prior approval from the Information Asset Manager.
Principle 3: Any person taking confidential information out of the company's premises when necessary for conducting business shall carry out the necessary and appropriate measures to prevent information leakage.

●Basic regulations

The "General Rules for Information Security Management Systems" stipulates basic provisions that must be adhered to in a strict manner regarding the formulation, implementation, maintenance, and continuous improvement of information security management systems.

The "general provisions for information and information equipment handling" establishes basic conditions regarding handling and management of information and information equipment with the objective of preventing accidents caused by leakage of overall information, or the misappropriation of information.

The "Management Regulations for Confidential Information" stipulates how to handle protection of confidential information.

●Individual regulations

The "Rules on Website Creation and Information Disclosure" stipulate provisions for strict observance in order that information is disclosed and used correctly on the website.

The "Systems Management Regulations for Information Security" stipulates procedures to ensure the security of information systems.

The "Management Regulations for Entrance/Exit and Access Restriction Zones" includes stipulations about physical security assurance, for example regulations regarding how to manage entering and exiting buildings.

●Handling of personal information

We have established personal information regulations equivalent to JIS Q 15001: "Personal information protection management systems — Requirements" in order to carry out management activities at a level higher than the Personal Information Protection Law.

●Information security audits

An information security audit is conducted once a year under the command of the information security audit controller appointed by the president.

The information security audit assesses the following:

- Whether information asset management and information security measures comply with the information security regulations
- Whether organizational structures for managing personal information comply with the Act on the Protection of Personal Information and with JIS Q 15001
- Whether personal information management systems comply with JIS Q 15001

Group companies are also asked to conduct an information security audit once a year.

Information Security Management System

Information Security Management Cycle

By building a framework that implements cyber security measures in PDCA (Plan-Do-Check-Action) cycles, information security management thoroughly implements and improves plans.

Plan: We formulate information security policies and measures, and plan information security education and audits.

Do: We expand the security measures internally, putting them into practice.

We educate staff members about information security, ensuring there is a thorough understanding of the measures.

We hold promotion conferences for information security, where each business site is provided with information about security, and feedback on implementation status of measures.

Check: We inspect the operational status of security systems periodically, and implement audits based on audit plans as well as management reviews carried out by a manager.

We also review management systems through a representative depending on changes in the management environment or internal or external opinion.

Action: We review audits and management systems, and take corrective measures based on internal and external opinions.

Information security audits

Information security audits are carried out once a year under the direction of the Information Security Chief Auditor appointed by the President.

The following criteria will be checked in an information security audit.

- Correspondence of management systems for information assets and information security measures to information security regulations.
- Correspondence of personal information management systems to the Personal Information Protection Law and JIS Q 15001: 2006.
- Correspondence of personal information protection management systems and JIS Q 15001: 2006 .

Group Companies are also requested to perform an information security audit once a year.

Emerging security risks in business activities

The Hitachi Group is expanding its business on a global scale, and therefore has many sites located in a variety of countries and regions. These sites operate under a variety of business conditions, fulfilling functions such as those of headquarters, sales offices, and service and manufacturing sites. In such an environment, our organization has a wide variety of network environments, facilities, and locations and usage environments of IT devices. Because external communications are carried out via external network connections and removable media (USB flash drives), it is important that we are prepared for security risks, such as targeted attacks and malware infections, that might occur in the course of our business activities. The Hitachi Group has created common security rules and standards for all companies, has established organizational security policies, and has put the relevant operations into practice at each site. However, as the security threats that surround our business environment change over time, residual security risks are emerging that had not been previously anticipated or recognized by our organization. To maintain and improve the security of our organization, the following tasks must be conducted.

(i) Checking the effectiveness of security measures at workplaces
(ii) Clarifying the division of responsibilities according to changes in the environment

Information Security Management System

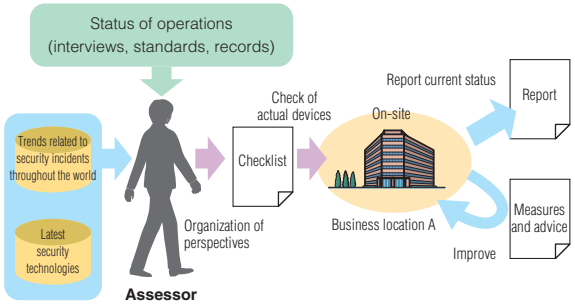
Enhancing risk-based measures through on-site security risk assessments

The Hitachi Group has been conducting high-level security measures and management activities related to confidential information and personal information. To handle the risks that accompany the environmental changes surrounding our business environment, we are enhancing the organizational structure for assessment by our team of security experts. This team, which operates independently of the IT control department in charge of internal IT measures, visits each business unit and each related company site in the Hitachi Group to actively implement enhancement measures from the following perspectives.

(i) Based on the latest trends, the team of security experts assesses all products and in-house facilities that are connected to the Hitachi Group's network.

(ii) The assessment team identifies issues that pose security risks, and proposes effective solutions to the workplace.

Figure 1. On-site risk assessment >>



Information Security Management System

Information Security Education

●Information Security Education

Continuously maintaining information security requires all parties to continually develop their knowledge of information handling and to remain strongly aware of the issues.

Therefore, we carry out education programs for all staff members, based on their hierarchical level and in accordance with the roles displayed in the table below.

Page 22 lists educational programs to develop more specialized security personnel.

Information security education list >>

	Target audience	Mode	Details
Education program by hierarchical level (all staff members)	Education for all staff	e-learning	Basic education regarding personal information protection, prevention of information leaks, and management of confidential information.
	Management education	Self-study, partial classroom style	Necessary information for managers about personal information protection, information security, and management of confidential information.
	New staff member education	Classroom style	Necessary information for new staff members about personal information protection, information security, and management of confidential information.
	Information security staff	Classroom style, partial practical exercise	Detailed knowledge about information security and management of confidential information. Practical education based in real examples.
	Personal information protection staff	Classroom style, partial practical exercise	Knowledge regarding protection of personal information (PrivacyMark). Practical education based in real examples.
	Information Asset Manager	Self-study, partial classroom style	Knowledge necessary as a person in charge of managing information assets for a division.
Education for relevant persons	Information systems staff	Classroom style, partial practical exercise	Education for information systems supervisors regarding network security, security incident response, web application security, and outsourcing server security

●Training for targeted cyber attack e-mails

The threat of cyber attacks via targeted e-mail is getting stronger, and it is vital that all staff members develop a resistance so that they can respond in the appropriate manner in the case that they are targeted.

Hitachi has been conducting targeted cyber attack e-mail training for all staff members at Hitachi as well as in Group Companies since 2012.

We actually send a mock e-mail disguised as a targeted cyber attack e-mail to all training staff members in order to increase their ability to judge what a suspicious e-mail is, and how you deal with it when you receive one, through actual experience.

●Other support

We distribute an abridged pamphlet version of the “Proper management and handling of Confidential Information” to all staff members to make sure that regulations regarding confidential information management are well known throughout the staff.

Cyber security vulnerability handling and incident response initiatives

Hitachi Group CSIRT activities initiatives

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.

What is an incident response team?

A security incident ("incident") is an artificial event related to cyber security, and refers to actions (events) such as unauthorized access, service disruption, or data destruction.

An incident response team is a group that leads "incident operations" in order to cooperate inter-organizationally and internationally to solve problems, through preventing (readiness: pre-handling) and resolving (response: post-handling) incidents, and has basic capabilities for "predicting and adjusting to threats from a technical perspective," "conducting technical collaboration activities," and "liaising with external communities on technical aspects."

HIRT activities model

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:

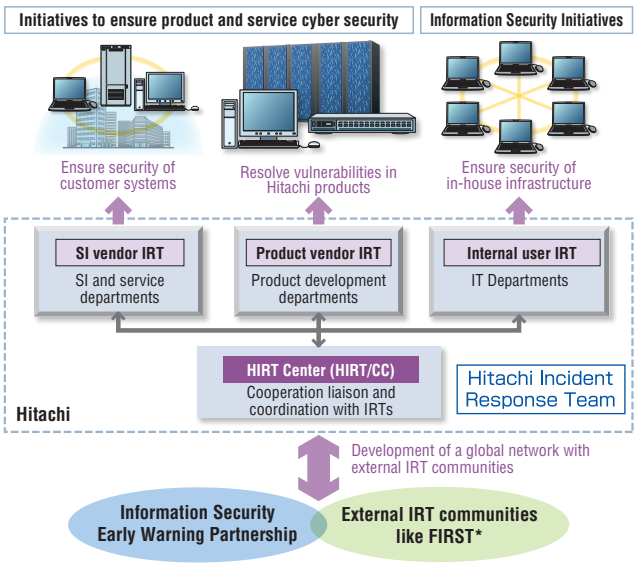
(1) The team that develops information and control system related products (Product Vendor IRT).

(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).

(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.

Four IRTs supporting vulnerability handling and incident response >>



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

Cyber security vulnerability handling and incident response initiatives

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

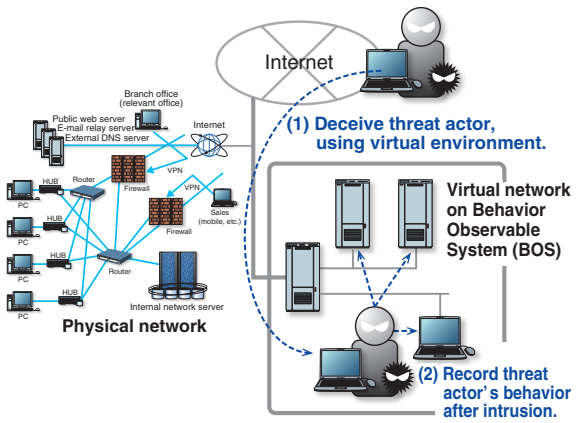
The HIRT Center disseminates information and business knowledge relating to vulnerability handling and incident response to the other teams through promotion of the Information Security Early Warning Partnership

(2) Developing a framework for research activities

The HIRT Center is engaged in “Observation of Threat Actors Activitie” 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.

BOS (Behavior Observable System) for Observable Threat Actors Activities >>



(3) Improving product and service security technology

The HIRT Center develops security measures for products that are related to information systems and control systems, and promotes the passing on of technologies to experts to improve our organizational IRT capabilities.

The HIRT Center also works on the development of simulation exercises for cyberattacks, such as targeted attacks and ransomware, as part of our practical in-house security education.

(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 responses informed by the context and trends in each domain.

As an advanced initiative in the financial field, HIRT-FIS (Financial Industry Information Systems HIRT) was established in October 1, 2012.

●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 that can contribute to the mutual improvement of IRT activities.

(1) Reinforcing domestic cooperation of IRT activities

The HIRT center reports vulnerability and incident information that is acquired during information collection to the PoCs (points of contact) of other member organizations of the Nippon CSIRT Association, in order to establish a collaborative network. They also support the establishment of an information-utilization infrastructure that uses JVN, which is operated by the JPCERT Coordination Center and Information-technology Promotion Agency (IPA).

(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 organization of a foundation for information use and application that utilize STIX and AIS by United States Department of Homeland Security and the like.

(3) Developing a framework for research activities

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.

Reference information >>

■Hitachi Incident Response Team
http://www.hitachi.co.jp/hirt/
http://www.hitachi.com/hirt/

Information security technical initiatives

IT based information security measures

At Hitachi we are working on a comprehensive plan to prevent problems like multiple cyber attacks, malware infection, unauthorized access, and information leaks, and are always looking for cutting edge IT security measures to counter new threats.

Safe and secure Hitachi IT security

At Hitachi Group, we have developed a secure Group-wide IT infrastructure environment, which allows Group staff members to share information between over 900 domestic companies.

Uniform security measures which are able to be implemented promptly in an emergency situation have been realized with the standardization and sharing of the IT infrastructure environment.

Hitachi Group products are incorporated proactively into this process, and feedback about their performance results are provided to product design departments, contributing to the further growth of Hitachi Group products.

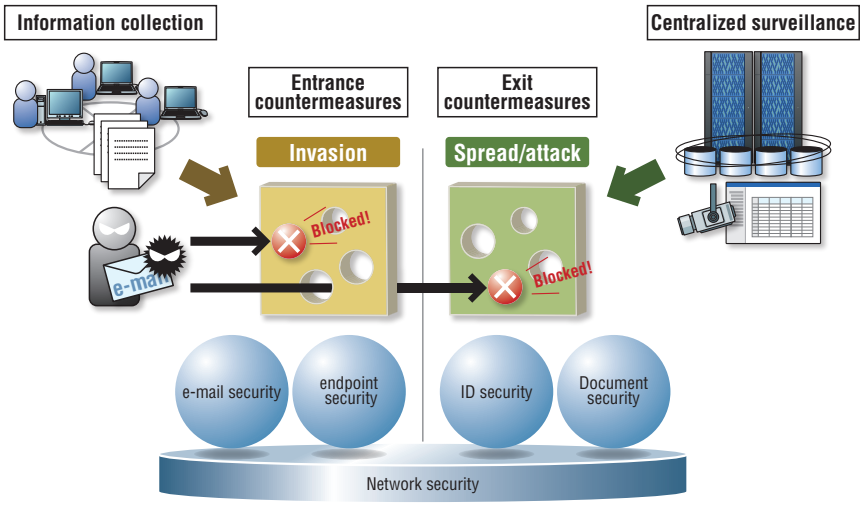
Hitachi IT security systems and multi-layered defenses against cyber attacks

Hitachi' s IT security framework, including network security (external connections such as internet connections, proxy servers, and remote access), email security, and ID security, provides various solutions and implements robust measures.

We understand it is important that countermeasures taken against cyber attacks, in particular targeted cyber attacks, need to be addressed without delay, and to be carried out on a continuous basis.

We are taking the following measures using the approach shown in the diagram below in order to achieve these outcomes.

- Collecting and utilizing incident information by the CSIRT.
- Adding more layers to our leak prevention systems (entrance and exit countermeasures) and defending important information.
- Understanding and analyzing attacks through centralized surveillance in order to minimize damage.
- Implementing prompt incident operations.
- Conducting cutting edge research about cyber attacks and educating and fostering personnel who deal with security issues.



Information security technical initiatives

Network security

1. External connections

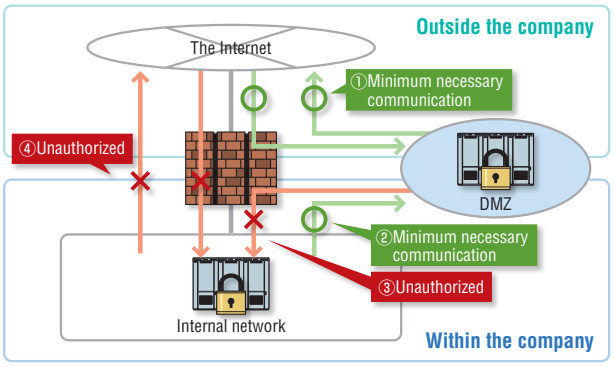
A firewall is in place at the point of connection when an external and internal network connect in order to disclose information to outside the company or to share information, creating a DMZ*1.

With a firewall in place there can be no direct internal and external communication. We use an indirect method to send information.

The IPS*2 monitors and blocks unauthorized access at the point of connection to the Internet.

Periodic security audits are also carried out on all servers and network equipment that releases information to outside the company, checking whether there are any security problems.

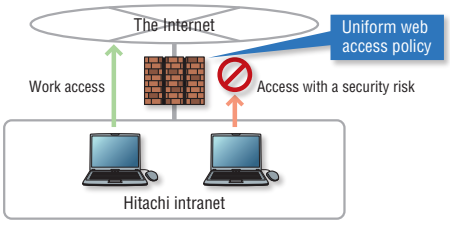
*1: DeMilitarized Zone *2: Intrusion Prevention System



2. Proxy

We are implementing the following countermeasures with a gateway in order to lower risk when accessing the Internet for work.

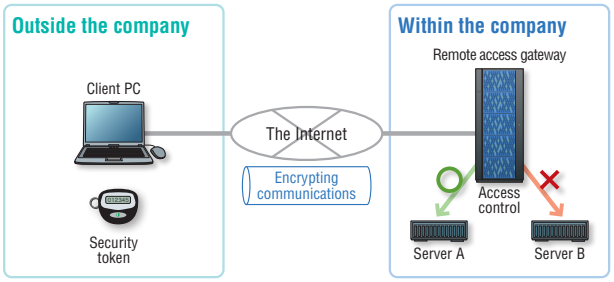
- Using ID and password authentication to regulate users, and storing and monitoring logs.
- Using image authentication to prevent machine communication by a virus.
- Filtering URLs via a standardized policy.
- Checking for web virus'.



3. Remote access

We prevent information leaks with a gateway using the following strategies.

- Implementing two-factor authentication (Authentication by authentication media or other method in addition to ID or password.)
- Encrypting communication in certain sections like the Internet.
- Controlling server access

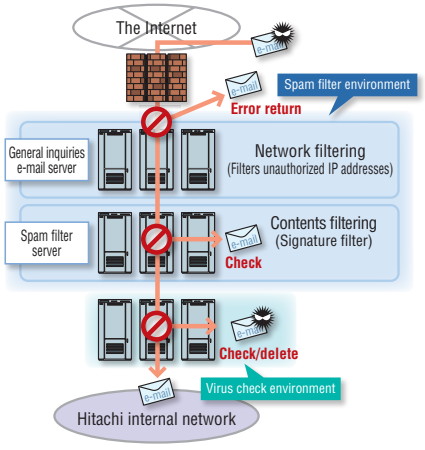


E-mail security

Hitachi has taken measures against external threats as well as threats that are generated internally.

1. Countermeasures against external threats

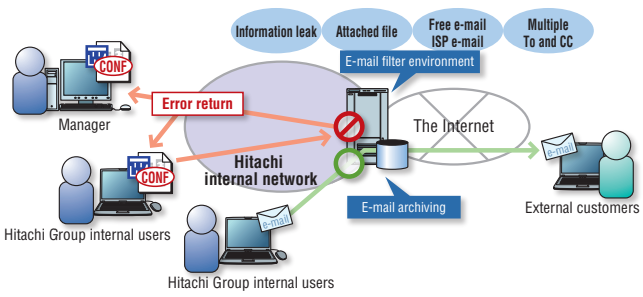
< Spam filters and virus checks >



Hitachi's e-mail delivery structure is especially responsive towards ① the threat of computer virus invasion, and ② the threat of spam e-mails, when protecting PCs from external threats.

2. Countermeasures against internal threats

There is an e-mail filter server in place for dealing with internal threats which is especially responsive to ① the threat of the spread of computer virus, and ② the threat of information leaks, and permits transmission of only e-mails without any issues.



Information security technical initiatives

Cybersecurity measures

To address cyberattacks and security incidents, Hitachi has established an internal security operation center (SOC) to enhance and promote security monitoring and incident handling.

Enhancing security monitoring and incident handling

In recent years, more complicated and sophisticated cyberattacks, such as advanced targeted email attacks and DDoS (distributed denial of service) attacks, pose an increased security risks for businesses and organizations. To confront these cyberattacks, it is important to detect threats quickly to prevent damage from spreading.

In October 2017, Hitachi established a security operation center (SOC) that operates 24 hours a day, 365 days a year to detect threats, such as malware infection and unauthorized access, at an early stage. This enables us to provide initial responses and measures quickly when an incident occurs, and to minimize the damage caused by a cyberattack. In this way, we are working to enhance security monitoring and incident handling.

(1) Security monitoring

Because even a single additional monitoring point can contribute to early detection in the internal network, we have taken inventory of the devices and systems managed by each department to gain an understanding of what is located where. We have also checked what logs can be acquired, and have started to monitor the logs that are useful for achieving earlier detection of threats. To improve monitoring on a global scale, we are working to identify the monitoring points in target systems and networks and to establish an integrated infrastructure for log monitoring and analysis, to enable linkage and monitoring of the logs from each system and network device in our global network.

(2) Incident response

We have developed response procedures and a contact network to be used in the event of an incident. When an incident occurs, we quickly investigate the cause, identify the extent of the impact, and control the situation. We also report the expertise we acquire through incident handling to the company as feedback regarding security measures, and implement measures to prevent similar incidents from recurring.

Collaboration with HIRT to collect threat information and discover potential threats

Recent cyberattacks use custom malware and sophisticated methods that are difficult or impossible to detect by using traditional security solutions. The security operation center works with HIRT, Hitachi Group's CSIRT, to collect information about the locations to which malware performs unauthorized access and to acquire threat indicators, such as the attack patterns of unauthorized accesses. Then it checks logs for threat indicators to discover potential threats and reduce the risk of information leakage.

Information security technical initiatives

Collecting, analyzing, and distributing alert information

Hitachi collects, analyzes, and distributes alert information to ensure the security of the information systems used internally and the products and services provided to our customers. We conduct these activities in cooperation with Group companies.

(1) Collecting cyber security information

When collecting cyber security information, we collect vulnerability information and threat information that are published online, as shown below.

We also use SHIELD global intelligence service provided by Hitachi Systems, to collect security information from Japan and other countries.

- Public institution websites, such as IPA and JPCERT/CC
- Security-released news websites
- Security reports and white papers published by security vendors.

(2) Analyzing information

For the security information we collect, we select the information to be distributed and we classify it with alert levels.

We classify the information one of five levels by considering the severity of the threat, CVSS base score published by vendor,state of usage of internal systems and the possibility of a successful attack.

(3) Distributing alert information

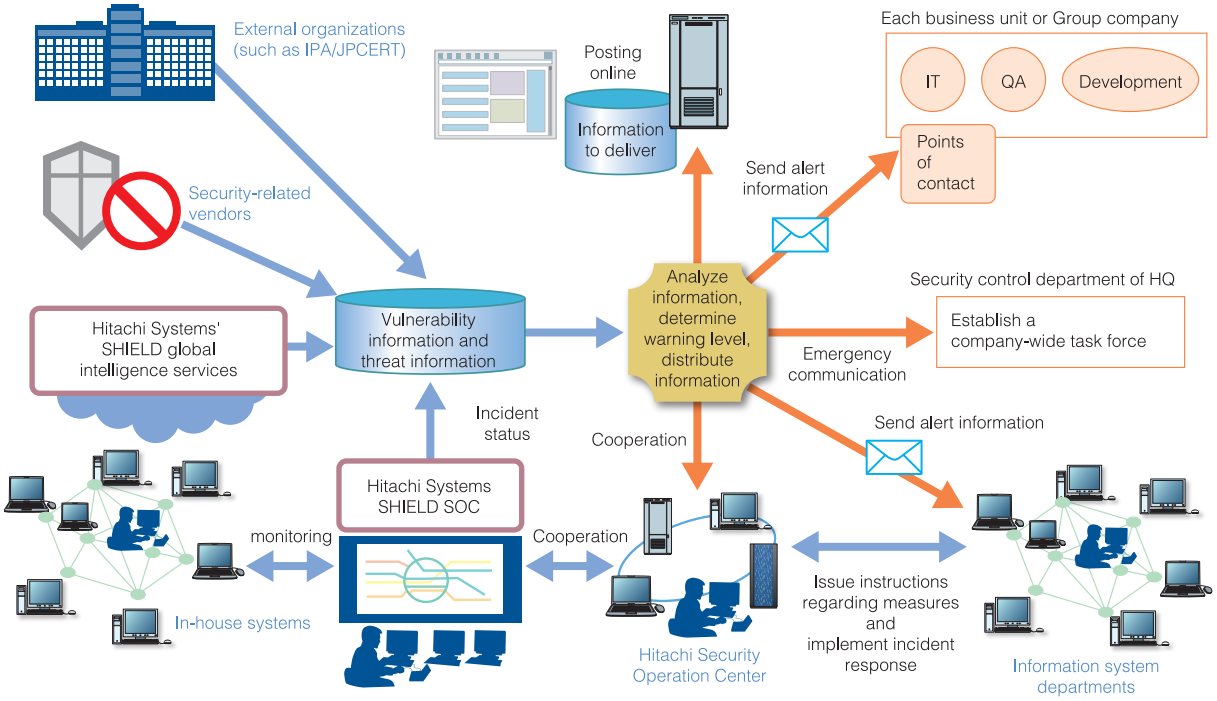
The information is distributed to the cybersecurity managers and information system divisions selected from each business unit and Group company.

Information is delivered immediately or up to weekly basis depending on the alert level, via communication channels such as email or internal website.

(4) Emergency measures

If an incident has a serious impact on the business of many sites within the company, or if the entire company is unable to continue business operations, a company-wide task force is established to provide centralized instructions about security measures.

*CVSS base score: A standard for assessing the characteristics of vulnerabilities. The impact of a vulnerability is evaluated and calculated based on the three security characteristics required for an information system (confidentiality, integrity, and availability), and on whether a network-based attack is possible.
(https://www.ipa.go.jp/security/vuln/CVSS.html)



Cloud computing security initiatives

Achieving safe use of the public cloud

In recent years, the public cloud has gained a lot of attention as a tool for implementing information systems. While the public cloud has the advantages of speeding up the building of information systems and reducing operating costs, there is a risk of information leakage. At Hitachi, we have implemented guidelines for controlling risks when using the public cloud, lowering such risks.

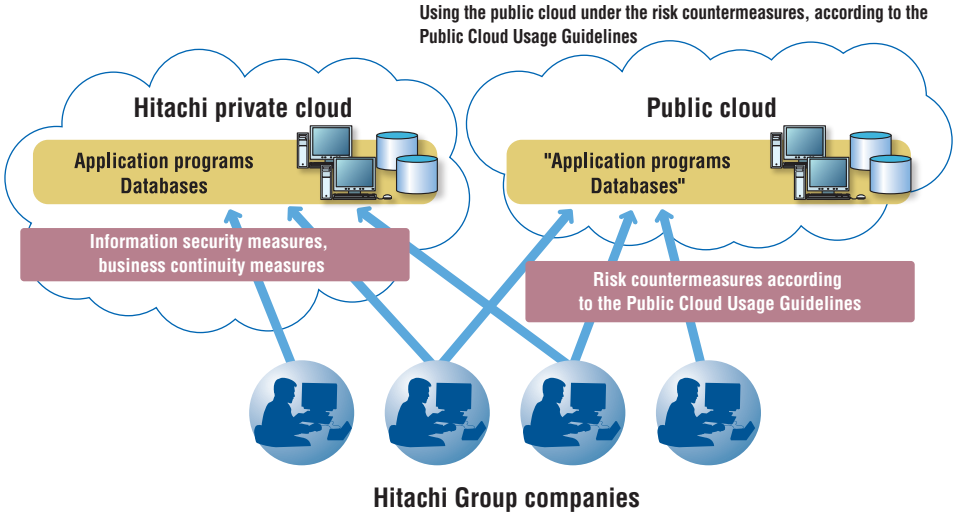
Cloud computing security initiatives

Cloud computing (“the cloud”) has been gaining a lot of attention in recent years. Generally speaking the cloud refers to “a method of using software or data etc. that is conventionally monitored and used on your desktop computer through networks like the Internet on an as-need basis, in the form of a service” *. There are two types of clouds, “private clouds” , which are created in the IT environment of a particular company or other entity, and “public clouds” , which are created by a service provider, and offered through the Internet.

At Hitachi, we are working towards consolidating a private cloud that can be shared by all companies in the Group, thereby implementing the security measures and service continuity during disaster situations stated in the “Information Security Technical Initiatives” section of this document. On the other hand, as displayed in Diagram 1, the public cloud is an area to which these initiatives do not extend, so Hitachi has reduced the risk of data leakage when the public cloud is used by establishing the “Guidelines for Using Public Clouds” .

*IT Term Dictionary e-Words, http://e-words.jp/, 1997-2013

Security for cloud use >>



Establishing the Public Cloud Usage Guidelines

As shown in Diagram 1, there is a risk of information leakage when using the public cloud through unauthorized access to the public cloud, as data and applications exist on the public cloud. In particular, there is already an increased risk of cyber attacks like unauthorized access by user identity fraud in IT services offered on the Internet, and there is concern that there is also a risk of information leakage with the public cloud. There is also the risk to business continuity, in that if the public cloud vendor goes bankrupt, user business might be interrupted, or data might be lost.

In order to decrease these risks, Hitachi Corporate indicates what sort of risk countermeasures are necessary when using the public cloud through the Public Cloud Usage Guidelines (the “Guidelines”), thus lowering risk.

The Guidelines include risk reduction measures relating to the risk of information leakage, for example processes for authentication and information protection necessary when using the public cloud, and requirements for public cloud vendors operations. Hitachi is also working on validating the degree of conformity to the Guidelines necessary for instances of public cloud use, in order to promote risk reduction through application of the Guidelines.

Physical security initiatives

Physical security initiatives

To prevent information leaks and crimes, it is necessary to install physical security measures, such as office entrance/exit management system and installation of security cameras, are indispensable for strengthening measures against information leaks and against crime. The Hitachi Group is promoting standardized Group-wide physical security measures. The following section outlines the physical security measures.

Standardization of physical security measures in Hitachi Group

In Hitachi Group, physical security measures such as entrance/exit management system used to be conducted at each business site individually. However, a basic policy for infrastructure has been established in order to reinforce measures, which are being implemented in a standardized manner across all Hitachi Group companies.

[Basic policy for infrastructure]

①Establish physical security standards to unify "Physical Security Measures and Operations".

②Introduce Hitachi Group products and services to Implement physical security management systems.

Outline of Physical Security Infrastructure

(1)Zoning and security level

The Standards for Physical Security Measures classify management zones into five security levels, and the entrance/exit management methods and the criteria for placing security cameras and intrusion sensors are defined according to the security level. By following these standards, Hitachi has standardized facilities and equipment.

(2) Introduction of Hitachi Group products and technology

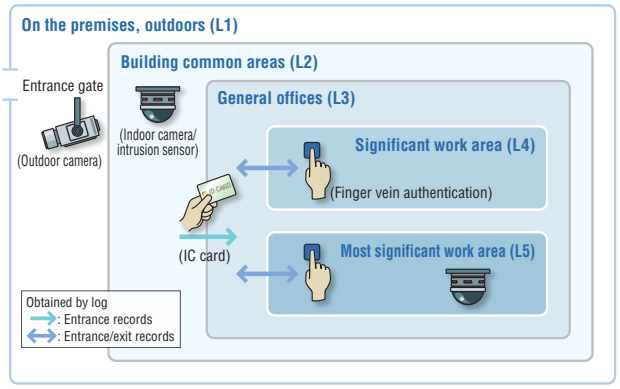
Hitachi Group products are being used in the entrance/exit management equipment, security cameras, and intrusion sensors to be prepared.

Hitachi Group's leading technology "finger vein authentication" has been introduced, in particular as a method for personal identity verification when entering significant zones.

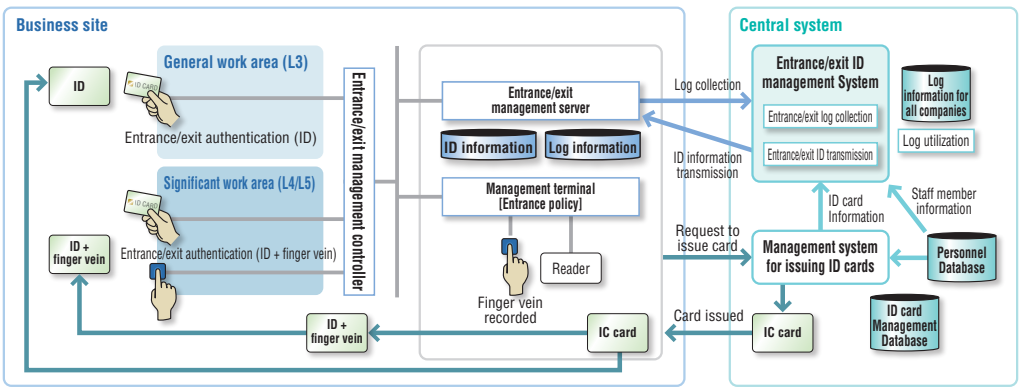
(3) Optimization of business with central control systems

Hitachi has developed an ID card issuance system and ID distribution system connecting to Hitachi Human Resource databases and that enables to optimize and standardize entrance/exit management operation in each business site. Also, forensic data like entrance/exit logs are centralized and used for analysis effectively.

Zone security levels and countermeasures >>



Entrance/exit management system schematic diagram >>



Initiatives in cooperation with procurement partners

Information security assurance initiatives in cooperation with procurement partners

As a corporate group that provides products and services that support social innovation business, Hitachi is working on information security measures in cooperation with its procurement partners. An agreement relating to the prevention of information leakages must be signed in advance when consigning work that deals with confidential or personal information. Our procurement partners also implement information management equivalent levels of security to Hitachi, and are making every effort to prevent accidents occurring or recurring.

Information Security Assurance with Procurement Partners

As corporate groups that support social innovation business, Hitachi' s procurement partners are implement the same level of management as Hitachi, and are making every effort to prevent accidents occurring or recurring.

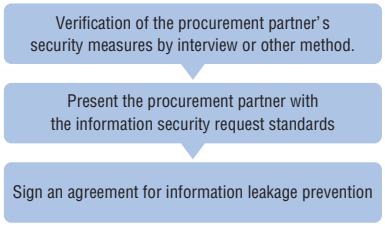
(1) Selection of procurement partners

When consigning work that involves the handling of confidential or personal information to a procurement partner, we perform a status review of their information security measures based on Hitachi' s own standards before allowing access to confidential information.

A business relationship only commences once an agreement regarding the prevention of information leakage that fulfils the security levels demanded by Hitachi has been entered into with the procurement partner.

Furthermore, Hitachi will perform a separate verification specifically for the handling of personal information on the occasion of consigning work that handles personal information.

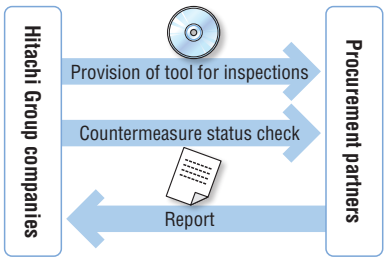
Work will only be consigned to procurement partners that have fulfilled the conditions of the review as an outcome of verification.



(2) Information security accident prevention measures

In order to prevent information leaving the company via the Internet by file exchange software, Hitachi provides information security tools, and carries out inspections to delete work information from individual' s PCs and other devices.

We also check whether information security measures are being implemented as specified in agreements with procurement partners, and suggest appropriate improvements based on the results of those checks.



(3) Strategies for information security accidents and recurrence prevention measures

If an information security accident occurs, an impact survey will be carried out together with related departments including the procurement partner, and as well as working on implementing measures to make sure any problems are solved expediently, Hitachi will also investigate the cause of the accident and make sure there are no recurrences in cooperation with the procurement partner.

In the case that a serious accident has occurred, or there is complete lack of improvement seen in the procurement partner, the continuation of a business relationship will be re-evaluated.

(4) Future initiatives

Hitachi will constantly check measures procurement partners have in place regarding information security with the aim of preventing accidents, and in addition to this, will work towards strengthening collaboration, and continue to carry out reliable preventative measures.

Global information security initiatives

Promoting global information security

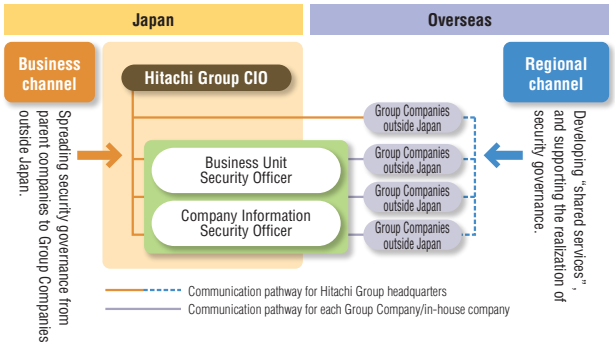
It is necessary for all Hitachi Group Companies worldwide to address strengthening of information security upon ensuring corporate public credibility. Hitachi has designated global information security management standards based on the international standards ISO/IEC 27001, and is promoting and working on the PDCA cycle.

Global information security structures

Hitachi employs two governance channels, a business channel and a regional channel, as its communication channels, the most significant prerequisite for the promotion of global information security.

These two channels constitute a system by which, through their effective utilization, issues particular to different regions or countries can be solved efficiently.

Furthermore, utilization of secure shared services has been proactively developed, with the aim of unification of security measures infrastructure and streamlining of IT investment.



Establishing global information security management regulations that conform with international standards

Effective utilization of IT as a foundation of business in order to expand Hitachi Group global business into the future is a vital strategy, and "Universal IT Policies" are being established to this end.

"Global Information Security Management Regulations" have been established in compliance with "Universal IT Policies" and the international standard for Information Security Management Systems (ISO/IEC 27001), in order to promote security governance.

The Management Regulations and related documents contain security risk measures that can be implemented with certainty, which were established upon consideration of the perspectives of developing countries experiencing significant growth, and the growth of Group Companies outside Japan, that also continue to support competition which opens up global business.

The PDCA cycle for improving levels of global information security

Hitachi promotes the PDCA cycle (continuous improvement) for the continuous operation, maintenance, and improvement of information security in order to improve security levels as stated in the "Global Information Security Management Regulations".

Group Companies outside Japan conduct self-checks to determine their security status.

The results of these checks are being visualized and analyzed in order to understand situations in different regions and different Group Companies outside Japan, and in the future, will be utilized during the formulation of the direction for Global Security Policies, which must be addressed by the entire company.

Information security human resources development initiatives

Information security human resources development initiatives

Hitachi Group has trained highly-skilled security human resources and human resources who can bridge security technologies to customers, by evaluating security related skills and careers, by conducting technical training and management education so that customers can securely use products and services.

Overview of information security human resources development activities

Due to intensifying cyber attacks on social infrastructure, Hitachi Group ① scouts and evaluates, ② develops and utilizes, ③ shares and links the security human resources who can handle these cyberattacks, and promotes activities for developing information security human resources, thereby contributing to ensuring the security of the social infrastructure.

These activities apply to all information security personnel, including not only high-level information security experts but also the engineers who develop and operate on-site systems and the users of in-house infrastructures. For the purposes of these activities, people who implement organizational measures against cyberattacks are divided into the following three groups below based on the IT skill standards (ITSS) defined by the Ministry of Economy, Trade, and Industry, which clarify and organize IT-related capabilities for each job type and specialty. As the education and training sessions required for each category, we provide education for highly skilled security personnel, e-learning courses for acquiring basic knowledge about responding to cyberattacks, and communication exercises.

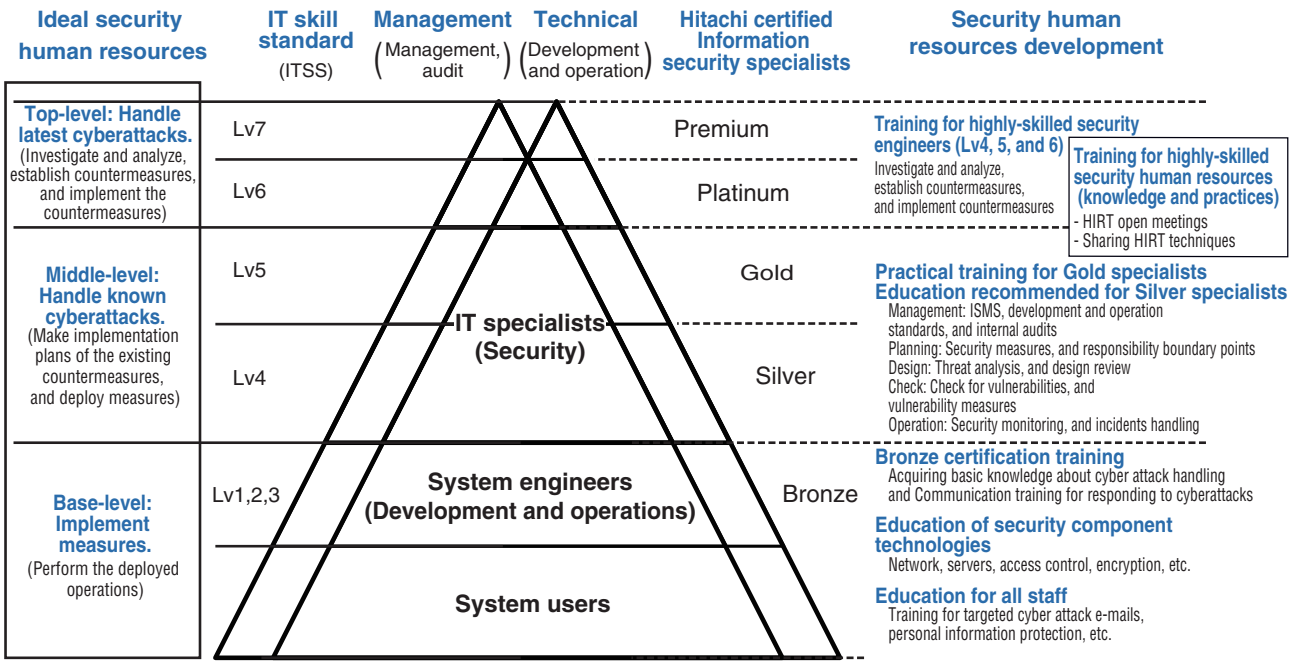
① Highly-skilled security human resources
Top-level human resources who can investigate and analyze latest cyberattacks and establish and implement countermeasures against them and guide the middle-level or base level human resources.

② Security human resources who organize system development and operation:
Middle-level human resources who can make plans to implement existing countermeasures against known cyberattacks, and who can deploy measures in the development and operation of information systems.

③ Human resources who implement deployed security measures:
Base-level human resources who investigate the systems they are responsible for, and who implement measures based on alerts issued by the top-level human resources and on instructions from the middle-level human resources.

In August 2014, the Hitachi Group established the Hitachi Certified IT Professional program, which complies with the standards for company certification in the Certified IT Professional program of the Information Processing Society of Japan. This program finds, nurtures, and evaluates information security human resources who have skills (gained, for example, through participation in training sessions) and careers (gained, for example, through job experience) and certifies them as information security specialists (ranked in levels from Bronze to Premium).

Figure 1. Information security human resources development activities >>



HIRT: Hitachi Incident Response Team

Information security human resources development initiatives

Expanding the training of information security human resources to the entire Hitachi Group

To respond quickly to cyberattacks, security experts, specialized security organizations, and the users and operators of on-site IT infrastructures and systems must respond to cyberattacks together.

If a user notices something unusual at their work, they must promptly report to, contact, or consult with a security expert, and take the appropriate initial response according to the expert's instructions. The persons in charge of responding to cyberattacks must share information smoothly and quickly determine the measures to implement as an organization.

To develop the fundamental human resources who serve as the foundation of this organizational structure for responding to cyberattacks, we began providing e-learning courses for acquiring basic knowledge about handling cyberattacks and communication exercises for responding to cyberattacks in the second half of the 2016 fiscal year. Persons who complete both courses are certified as bronze-class information security specialists, and work to promote this training and certification.

Initially, these courses were offered to the staff of the IT business divisions in the Tokyo area, and they are now available to workers in other areas and in other departments. Each year, over 2,000 people take these courses and are certified as bronze. Education continues to be expanded across the Hitachi Group, and we are promoting the development of security personnel who can support cyberattack responses.

Figure 2. Base personnel who support the organizational structure for responding to cyberattacks >>

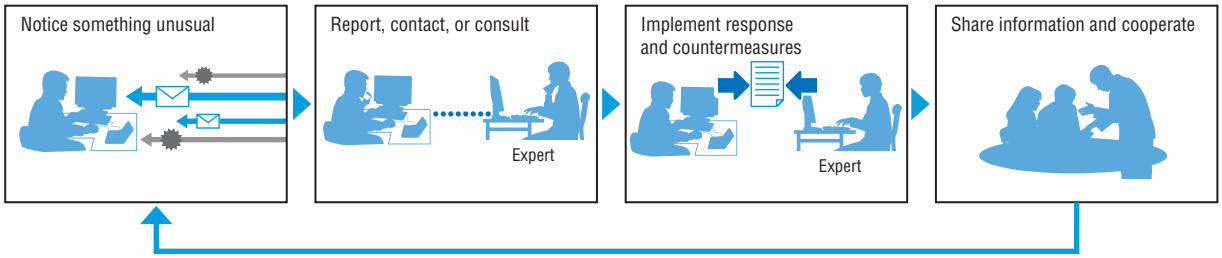


Figure 3. Training for cyberattack response >>

E-learning course for acquiring basic knowledge about responding to cyberattacks

Training course for learning about the impact of cyberattacks and the actions to be taken when a cyberattack occurs

[Basic knowledge]
(i) Points to be aware of during daily business activities, (ii) Response to a cyberattack, (iii) Points to be aware of during development, (iv) Collection of vulnerability information and investigation of countermeasures, (v) Preparation for an incident

[Virtual experiences of cyberattacks]
(i) Information leakage caused by a targeted attack, (ii) Interruption of business resulting from a ransomware infection, (iii) Damage caused by a vulnerability in a web-based application, (iv) Damage caused by malware

Communication training for responding to a cyberattack

Exercises to practice gaining an understanding of the situation determining the necessary response in the event of an incident

[OODA]
Acquire, through experience, the quickness and accuracy required for OODA:
(i) Observe, (ii) Orient, (iii) Decide, and (iv) Act

[Reporting, contacting, and consulting with experts]
Learn the importance of dividing responsibilities and describing incidents accurately (by explaining who, when, what, where, why, and how) when (1) reporting, (2) contacting, and (3) consulting with experts.

Personal information protection initiatives

Personal information protection guaranteeing security and trust

Hitachi was granted the Privacy Mark certification in March 2007, for implementing safe personal information management and protective measures. Hitachi operates the “personal information protection management system” , which is a framework for the protection of personal information, and is working continuously on personal information protection and appropriate handling for staff members as well as all other stakeholders.

Personal information protection

Hitachi has implemented management regulations for personal information that correspond to Japan Industrial Standards “Personal information protection management systems - Requirements (JISQ 15001: 2006)” , which stipulate management standards to a stricter level than the Personal Information Protection Law. These regulations are based on the “Hitachi personal information protection policies” , which stipulate principals and policies relating to personal information protection for the purpose of protecting personal information important to the owner of that information.

In March 2007, Hitachi acquired the third party PrivacyMark certification (granted by JIPDEC). This certificate is granted to companies recognized by JIPDEC to have implemented the appropriate safety control and protection measures for personal information. Hitachi is making efforts to ensure that we are able to acquire this certification for the seventh time in May 2019.

Hitachi strives to protect personal information with a sense of self awareness and responsibility as a vendor with Privacy Mark certification, maintained so that all stakeholders are able to provide Hitachi with personal information with peace of mind.

Hitachi Privacy Mark >>

System for promoting personal information protection

In April 2009, Hitachi merged the “Personal Information Protection Promotion System” and the “Information Security Promotion System” , and commenced the new “Information Security Promotions System” . Our aim is to realize a highly practical management system through the unification of management systems related to significant information including personal information, and systems related to information security.

Through this unification, we have carried out the four safety management measures required by the “Personal Information Protection Law” and other regulations, and have unified the “Information Security Technical Initiatives” , “Physical Security Initiatives” and others, promoting the protection of personal information.

The specific management structure is as stated in the “Information Security Promotion System” clause of the “Information Security Management System” .

Hitachi also strives to safeguard personal information globally at Group companies outside Japan based on the “Personal Information Protection Policy” and by adhering to all applicable laws and regulations, including social requirements.

〈Four measures for safety management〉

(1) Organizational Safety Management Measures:
Structuring and operating regulations and systems, verification of their implementation, etc.
(2) Human Resources Safety Management Measures:
Entering into non-disclosure and other agreements, education and training, etc.
(3) Physical Safety Management Measures:
Management of entrances/exiting buildings (rooms), theft prevention measures, etc.
(4) Technical Safety Management Measures:
Access control of information systems, unauthorized software countermeasures, etc.

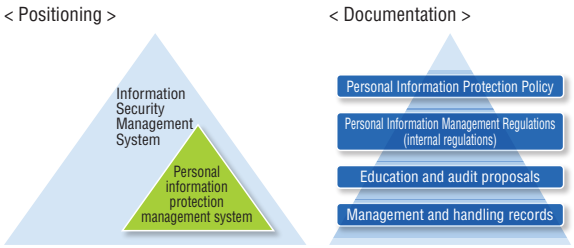
Personal information protection initiatives

Personal Information Protection Management System

The “Personal Information Protection Management System” (PMS) has also been positioned as part of the “Information Security Management System” (ISMS) in addition to the unification of management systems, with the exclusion of the operation of a section which is specific to personal information protection.

The “PMS Documentation” , which is a document containing the basic elements of the PMS, is made up of the “Personal Information Protection Policy” , “Personal Information Management Regulations (internal regulations)” , “proposals” for audits, education and similar, and a “record” of PMS implementation.

Hitachi personal information protection management system >>



Management and appropriate handling of personal information

Hitachi strives for strict management and appropriate handling of personal information entrusted with us, according to internal regulations “Personal Information Management Regulations”.

A person in charge of protecting personal information (an Information Asset Manager) is located at each workplace, and identifies all personal information entrusted to Hitachi, managing logs and carrying out appropriate measures according to the seriousness of that personal information.

This person also carries out periodic education on personal information protection, personal information protection audits, and checks status of operations in workplaces, in order to make personal information protection management systems an established practice.

In addition, they will also distribute the “Personal Information Protection/Information Security Card” to all staff members, and make sure that all staff members have been duly informed of the rules requiring strict adherence with regard to principles, as well as management and handling, relating to Hitachi’ s personal information protection.

Initiatives in the workplace >>

〈All personal information〉

- Identification and classification of personal information
- Risk recognition, analysis, and countermeasures
- Record of personal information on log
- Periodic revision of personal information
- Appropriate handling
- Personal information protection education
- Personal information protection audits
- Confirmation of operational status in the workplace

Compliance with the “My Number” system

Hitachi strives for strict management and appropriate handling of personal information according to internal regulations related to Japan's “My Number” IDs (used for social security and tax purposes).

We have established a system to manage “My Number” IDs. By assessing risks of business operations associated with “My Number” IDs, we are taking appropriate measures against risks.

Compliance with the legal systems for the protection of personal information outside Japan

In recent years, many countries and regions have created and modified legal systems for the protection of personal information, because privacy-related risks have increased due to the advancement of IT and the internationalization of socioeconomic activities. In particular, although the General Data Protection Regulation (GDPR) is a regulation stipulated by the EU, its obligations regarding the handling of personal information and harsh penalties for violations also impact countries outside Europe. To comply with the GDPR, the entire Hitachi Group, including local control companies and offices in Europe, is working together to identify those business activities that are subject to the GDPR (for example, business activities that involve receiving personal information from customers in Europe or storing employee information in the global human capital database), assess the risks, implement the appropriate safety control measures for the risks, and provide training to all employees. We are continuously monitoring the enforcement of the GDPR by European authorities and status of compliance within Hitachi, and are implementing appropriate measures.

Personal information protection initiatives

Enhancing subcontractor management

There have been a number of information leakage accidents from subcontractors handling personal information in the past few years, which has become a social problem.

Hitachi enhanced its management of subcontractors handling personal information from an early stage, and has established internal regulations relating to the consignment of the handling of personal information, and subcontractors are supervised in accordance with these regulations.

An assessment and selection process is carried out based on subcontractor selection standards stipulated by Hitachi Group so that Hitachi selects subcontractors with personal information protection standards equivalent to or surpassing Hitachi's own standards.

Furthermore, consignment only occurs after an agreement has been signed which includes strict personal information management conditions such as the establishment of a system of management, and a basic prohibition of re-entrustment.

Supervision of the subcontractor will also be carried out, with a self-awareness of Hitachi as responsible as the prime contractor, in the form of periodic reassessments of the subcontractor, and the implementation of audits.

Hitachi Group overall initiatives (promotion to be certified as Privacy Mark entity)

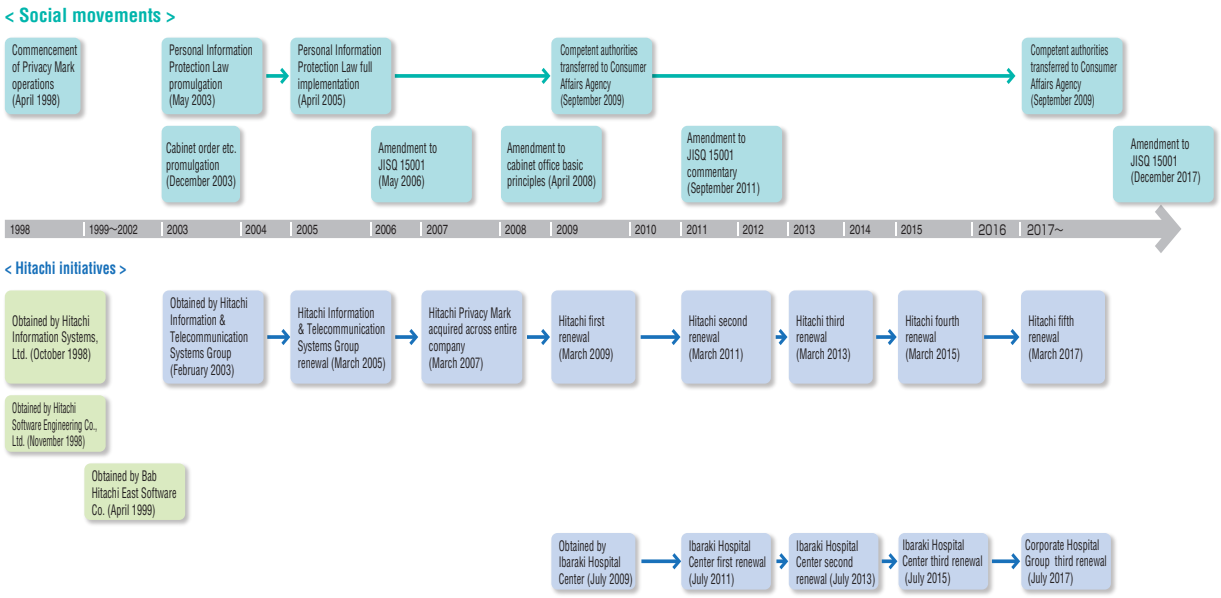
The Hitachi Group is engaged in the protection of personal information as a unified entity. As of May 31, 2018, the PrivacyMark certification has been obtained by 44 of our vendors who are protecting and handling personal information at a management level higher than the level required by law.

Hitachi has also established the "Hitachi Group Privacy Mark Liaison Committee" which consists of mainly companies that have obtained the Privacy Mark, and implements periodic information exchange sessions, study sessions, and seminars to which external specialists are invited. Information sharing and research about personal information protection is also building up across the Group.

Medical facilities like hospitals are also engaged in the protection of personal information as independent vendors.

In July 2009, the Corporate Hospital Group in Japan also gained Privacy Mark certification. Hitachi is working hard to protect and carefully handle the personal information of its patients and others.

Hitachi Privacy Mark initiatives >>



Initiatives to provide information security to our clients

Hitachi security supports social infrastructure in the IoT era

In the changing IoT era, Hitachi has adopted “Evolving Security for a Changing IoT World” as our security vision and is evolving security to protect our clients’ systems and services.

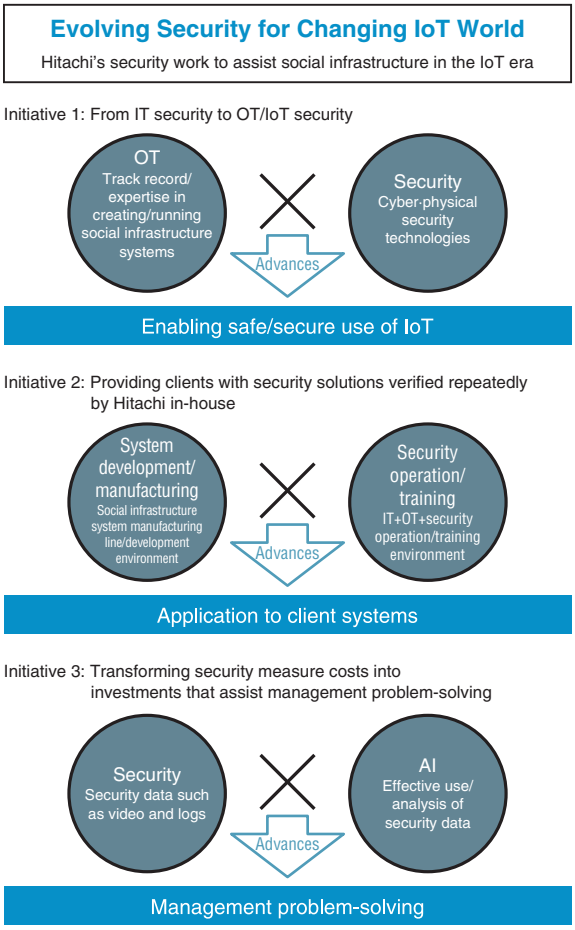
Hitachi’s Security Vision

Hitachi is accelerating the evolution in clients business and security in three directions.

- **Initiative 1: From IT security to OT/IoT security**
  Hitachi has expertise in protecting OT/IoT based on extensive experience in building and operating social infrastructure systems.
- **Initiative 2: Providing clients with security solutions verified repeatedly by Hitachi in-house**
  Hitachi has environments used to develop and manufacture social infrastructure systems and to perform security operations and training exercises.
- **Initiative 3: Transforming security measure costs into inverstments that assist management problem-solving**
  By using an AI to analyze security data, we can make use of the results in solutions that resolve business challenges.

OT : Operational Technology
IoT : Internet of Things
AI : Artificial Intelligence

Hitachi’s Security Vision >>



Hitachi’s approaches to security

To protect businesses from threats and risks, system-related measures alone are insufficient. In addition to such measures, you need comprehensive security that takes into account organizations and operations.

To achieve our clients’s safety and security, Hitachi takes three approaches for providing security: protect by organizations, protect by systems, and protect by operations.

In addition to building systems to ensure security, we also provide organizational management systems to continuously maintain the effectiveness of security measures, and provide operational policies for monitoring for and detecting unusual behavior.

Hitachi’s approaches to security>>

Initiatives to provide information security to our clients

Evolving security

Next we will describe some of Hitachi' s efforts as an innovation partner helping our clients tackle their challenges. We will introduce topics about evolving security: such as new services and solutions that support creation of new value, and verification tests in Hitachi OT/IoT for turning research into practical solutions.

Integrated Cyber Security training for providers of critical infrastructure

In Hitachi' s Omika Works, Hitachi established comprehensive training and verification facilities for handling cyberattacks, and has started providing a Integrated Cyber Security training for providers of critical infrastructure. The training combines the technologies and expertise in control systems and information systems that Hitachi has cultivated over the years.

First, at our own facilities, we built simulators modeled after the actual systems of our customers (power companies). By switching between the various simulators (such as those for thermal power, nuclear power, and power systems), we are able to respond to our customers' diverse needs. We started a program for organizational training for departments that monitor systems and provide instructions. We also started a service that can verify operation procedures and evaluate security products in preparation for cyberattacks.

Inside the facilities >>

(Please see p. 46.)

Solutions for security monitoring for control systems

The solutions enable early detection of security incidents in control system, and can analyze and make visible information that was formerly difficult to identify: including the source, propagation route, and the extent of impact. The solutions also accelerate the decisions and responses in an emergency, and support initial responses to prevent damage from spreading.

USB control solutions that prevent security incidents caused by unauthorized use of USB storage devices

In recent years, unauthorized use of USB storage devices is causing an increasing number of security incidents in control systems. We have started providing a USB control solution that can control USB connections to devices or computers, just by attaching a device that connects to the USB ports of control devices or computers in the control system.

Commercializing the Hitachi Anomaly Detector, a newly developed algorithm that detects the threats of cyberattacks at an early stage

We succeeded in developing an algorithm that can be installed in a control system to detect the threats of cyberattacks an early stage. After defining the normal system status, the software learns automatically while comparing the current state and normal state, and detects abnormalities. This will be provided as a new product called Hitachi Anomaly Detector.

The Hitachi Anomaly Detector is a software product developed by Hitachi based on R&D findings. This work was supported by the Cabinet Office (CAO), Cross-miniseterial Strategic Innovation Promotion Program (SIP), “Cybersecurity for Critical Infrastructure” (funding agency: NEDO).

Developing a cyber-risk analysis method that quantifies key security-incident information (the rate of occurrence and the amount of damage)

To support appropriate security investment decisions in industry and critical infrastructure fields, Hitachi worked with Sompo Japan Nipponkoa Insurance and Sompo Risk Management & Health Care to quantify key security-incident information: the rate of occurrence and the amount of damage. We developed a security diagnosis system and damage occurrence model simulator, and performed technical verification.

Initiatives to provide information security to our clients

Hitachi and Trend Micro start a new joint venture related to the development of security personnel

There is a shortage of security personnel in Japan. To accelerate the development of skilled personnel, Hitachi and Trend Micro will start to provide cyberattack response training sessions in October. The training will combine Hitachi' s expertise in training and in developing and operating systems, with Trend Micro' s information about the threat trends in Japan and foreign countries and the latest attack scenarios. In the future, this joint project will develop new training services that contribute to quicker development of security personnel.

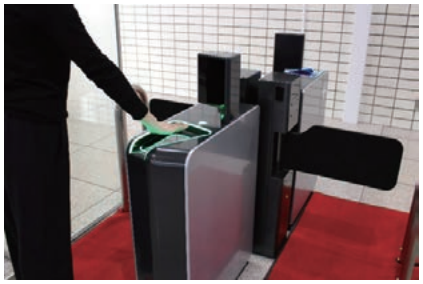
Verification test of a walk-through finger vein authentication gate

As a step towards making practical use of a physical security access control gate, we conducted verification tests at Hitachi' s Omori office located in Shinagawa-ku, Tokyo. For the evaluation, we used real data from about 1,000 company employees, which is equivalent to actual operation (March 2017 to February 2018).

The walk-through finger vein authentication gate used in the verification tests achieved high-speed and stable imaging of finger veins from moving hands. The gate is a noncontact type that can authenticate persons without their hands touching it. The demonstration showed the gate' s convenience, with high throughput similar to ticket gates and high authentication performance. As a result , we are now discussing its future application in fields requiring identification of people, such as in large-scale events.

(Please see p. 51.)

Walk-through finger vein authentication gate >>



Publishing of the white paper about our initiatives in privacy protection

For business operators that are considering the use of personal data, we made and published the white paper about Hitachi' s initiatives in privacy protection in use of personal data (October 2017).

The white paper describes basic concept about privacy protection and specific initiatives, such as establishing organizations and systems to protect privacy, evaluating privacy, risks implementing privacy protection measures in developing work, and continuously conducting privacy-related opinion surveys of citizens. The white paper also describes sample cases in which privacy protection measures have been applied.

(Please see p. 40 and 41.)

Masatoshi Terada in the Hitachi Incident Response Team (HIRT) received a Minister for Internal Affairs and Communications Encouragement Award

Hitachi' s Masato Terada won a Minister for Internal Affairs and Communications Encouragement Award for Cybersecurity. In 1998, he established an in-company CSIRT, the Hitachi Incident Response team (HIRT). Also, in 2007, he founded the Nippon CSIRT Association in cooperation with six CSIRT teams. As of 2018, he is promoting the proliferation of CSIRT activities as the steering committee chairperson of the Nippon CSIRT Association. From 2002, he has continued to promote vulnerability reduction measures in Japan, such as the building of the JVN (Japan Vulnerability Notes) website (https://jvn.jp/).

Certificate >>

"Minister for Internal Affairs and Communications Encouragement Award for Cybersecurity"
The award has been presented since fiscal year 2017 to individuals or organizations (teams) who have made remarkable contributions to local governments, private companies, and organizations from the viewpoint of improving cybersecurity, such as in network environments. The award indicates that such individuals or organizations are expected to play an active role in the cybersecurity field in the future.

Initiatives to provide information security to our clients

Hitachi's security solution Secureplaza

The integrated power of the entire Hitachi Group provides solutions that contribute to improving security and resolving business problems.

Comprehensive security that takes organizations and operations into account, and not just system-related measures

●Protect by organizations

First of all, responding as an organization is essential to prepare against various security risks. Security governance needs to be established in the organization via personnel training and risk assessment, and the security level needs to be continuously improved in steps.

●Protect by systems

A single solution, such as the introduction of security software, cannot protect businesses from ever-evolving threats. Multilayer protection measures that combine various methods are required.

●Protect by operations

More diversified and sophisticated cyberattacks are damaging business continuity. In addition to preparing for an emergency by creating a cyber BCP, it is important to establish a SOC/CSIRT that can move quickly (for example, to quickly detect incidents, conduct temporary measures at the site, collect and analyze relevant information, and plan and implement appropriate measures), and to perform security operations in an organizational structure that includes management.

Cyber BCP:Business continuity plan in the event of a cyberattack
BCP:Business Continuity Plan
SOC:Security Operation Center
CSIRT:Computer Security Incident Response Team

Hitachi's security solution Secureplaza >>

1 Establish security governance and develop human resources

- Establish security governance
- Develop security personnel and improve the security awareness of employees

2 Enhance cybersecurity measures

- Protect IT systems from known and unknown threats
- Develop and implement security measures specific to control systems

3 Enhance physical security and resolve business challenges

- Control access and monitor according to the importance of the area
- Implement more advanced security by image monitoring and analytical technologies
- Use physical security to resolve business challenges

4 Prevent information leakage and protect privacy

- Avoid the risk of information leakage from the viewpoint of 5W1H
- Prevent information leakage by prohibiting data from being taken out of the company
- Protect privacy when using personal data

5 Improve ID management and convenience

- Manage IDs efficiently in organizations
- Enhance access control for privileged IDs
- Use finger vein authentication to improve security and convenience

6 Understand incidents properly and respond to them quickly

- Perform integrated operation monitoring that enables appropriate decision and prompt handling
- Support the building and operation of a CSIRT
- Support security monitoring, and investigation and analysis

Information security products and services initiatives

Initiatives to provide information security for IT-related products and services

To ensure the security of information products and services provided to our customers, Hitachi has established an organizational structure for considering and planning security measures. Hitachi promotes activities to operate and improve security based on security management processes. These activities are promoted mainly by the operating divisions that provide information system products and services, under an in-house security-governance organizational structure.

Initiatives to ensure security

The following shows initiatives promoted to ensure the security of information products and services provided to our customers.

●Planning and promoting security measures for information products and services

To ensure the security of information products and services, Hitachi has established an organization structure for considering and planning security measures, targeting the operating divisions that provide information system products and services. (Please see Figure 1.) This organizational structure promotes the planning and operation of the measures that are specific to the operating divisions providing information system products and services, including security measures related to developing and operating products and services. Related companies in the Hitachi Group also participate in these activities, working together to devise measures. The devised measures are deployed to related operating divisions and implemented in each of them.

●Developing and operating products and services based on security management processes

For each phase in the development and operation of a product or service, a security management process is defined as rules to ensure its implementation in the organization. The rules first describe an overview of the management process and, under that, provide detailed regulations and standards to define more specific activities. Support tools and examples are provided as concrete expertise to promote activities reliably, appropriately, and effectively. (Please see Figure 2.)

The core of management processes are management standards for secure system development and operation. These standards, which are applied to the development and operation of information products and services provided by Hitachi, use the concept of security ranks and define ranking indices. The standards show the security management processes required to ensure security in development and operation for each security rank. (Please see Figure 3.) The adoption of security ranks encourages employees to consider a balance between risks and costs, as well as to recognize the level of a risk and to implement appropriate measures. The processes described in these standards align with the information-system development processes that have been standardized in Hitachi. The aforementioned security organizational structure revises the contents of the defined security management process as required, on a regular basis or from time to time. These reviews are based on feedback from incidents that occurred, the risks that have surfaced, and the result of continuous-improvement operations, so that the management processes become more appropriate.

Figure 1. Organizational structure for considering and planning security measures for information products and services >>

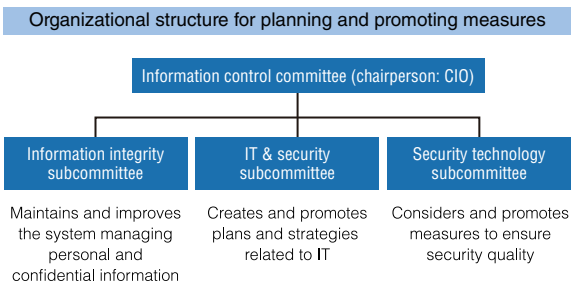
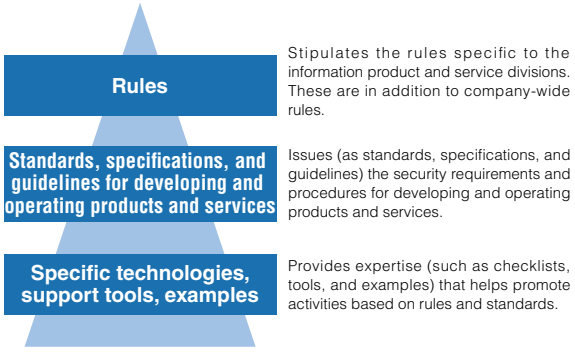


Figure 2. System of security rules for information products and services >>



Information security products and services initiatives

Figure 3. Security processes in the management standards for secure system development and operation (excerpts) >>

Plan	Basic design	Detailed design/ production	Testing	Operation preparation/ migration	Operation
• Specify a security rank • Create the security policy for the development environment • Clarify security requirements and measures Etc.	• Design a security system • Design review of the basic design Etc.	• Apply security-related content into the ordinary operation procedures • Create procedures for handling security incidents Etc.	• Create a test plan for the design of the security system • Check for vulnerabilities • Evaluate the test results Etc.	• Review before operation • Periodically analyze vulnerabilities Etc.	

●Checking for vulnerabilities

We periodically check for vulnerabilities to prevent damage by attacks exploiting such vulnerabilities. Checking is conducted during new development, when the environment changes, and periodically. Qualitative checking is performed using a checklist, and checking uses a vulnerability check tool. Based on the system characteristics and operation status, appropriate checks can be conducted by using one or both of them. Because internet connections are usually high risk, an authorization system for internet connections is provided, so that connecting to and publishing on the Internet are not possible without approval.

●Handling incidents

To reduce the likelihood of security incidents that exploit vulnerabilities, a guide was created to describe the process of handling vulnerability-related information in the departments that provide information products and services. Hitachi promotes activities based on this guide. (For an overview of Hitachi' s incident handling, see *Handling security incidents* (pp. 34 and 35).) By establishing an organizational structure for responses to large-scale incidents, preparing manuals, and providing training sessions, Hitachi is capable of responding quickly and appropriately.

Information security products and services initiatives

Initiatives to provide information security for software products

In recent years, the influence of software-product vulnerabilities on infrastructure has continued to increase. Ensuring the security of products is essential. To enable our customers to use our software products with peace of mind, we strive to ensure security in each phase (from design and development to operation), from a global viewpoint.

Security assurance initiatives

Ensuring such security is critical, because many of the software products provided by Hitachi play a central role in social infrastructure.

It is the obligation of the vendor to provide products that the customer can trust, and from design and development to operation, it is important to build a framework which takes security into consideration across the entire life cycle of the software.

We have incorporated security assurance measures for conventional development processes when developing Open Middleware Products.

We have defined this as the “Secure Development Life Cycle of products” and are working to ensure a global standard of security while incorporating the approach of information security international evaluation criteria ISO/IEC 15408 (Common Criteria) and other standards.

Software development based on Secure Development Life Cycle of products

The following criteria have been established as important development processes in the “Secure Development Life Cycle of products”.

(1) Definition of requirements
Determination of overall policies regarding product security, and development policies for ensuring security.

(2) Design
Determination of security requirements based on threat analysis and the fleshing out of functional design that takes security into consideration.

(3) Implementation (Secure programming)
Identification of vulnerabilities by applying secure programming checklists and static analysis tools to source codes.

(4) Testing
Vulnerability detection with security testing tools (security scanners) and validation based on security checklists.

(5) Support
Prompt response to vulnerability issues in our products that are discovered after commencement of operations. Support by creation of patches and information disclosure to minimize customers' risk of exposure.

Hitachi is developing products with assured security by educating and sharing information with security developers and inspection supervisors on a continuous basis about trends in technology and vulnerability issues.

Approach for incident response to software product vulnerabilities

The basic approach is to eliminate software vulnerability issues in the design, implementation, and test phases. However, it is possible that there will be new vulnerabilities discovered, and new attack methods appearing.

These efforts also conform with the Ministry of Economy, Trade and Industry (METI) Public Notice No.19, 2017, “Standards for Handling Software Vulnerability Information and Others” and the “Guidelines for Information Security Early Warning Partnerships” . These stipulate the procedures from reporting a vulnerability issue to providing solutions to our customers.

This framework is also coordinated with incident response activities (CSIRT) by “HIRT” *. Response to product vulnerability issues are done so in cooperation with affiliated institutions.

* HIRT：Hitachi Incident Response Team
CSIRT：Computer Security Incident Response Team

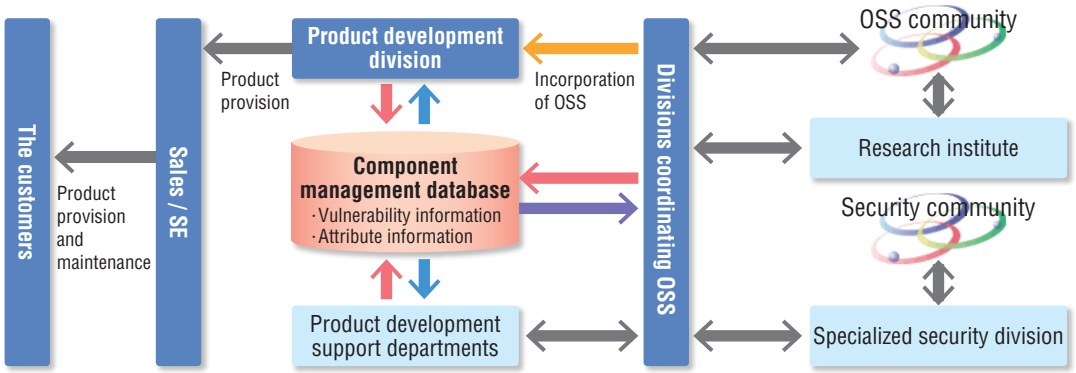
Information security products and services initiatives

Strategies for Open Source Software (OSS)

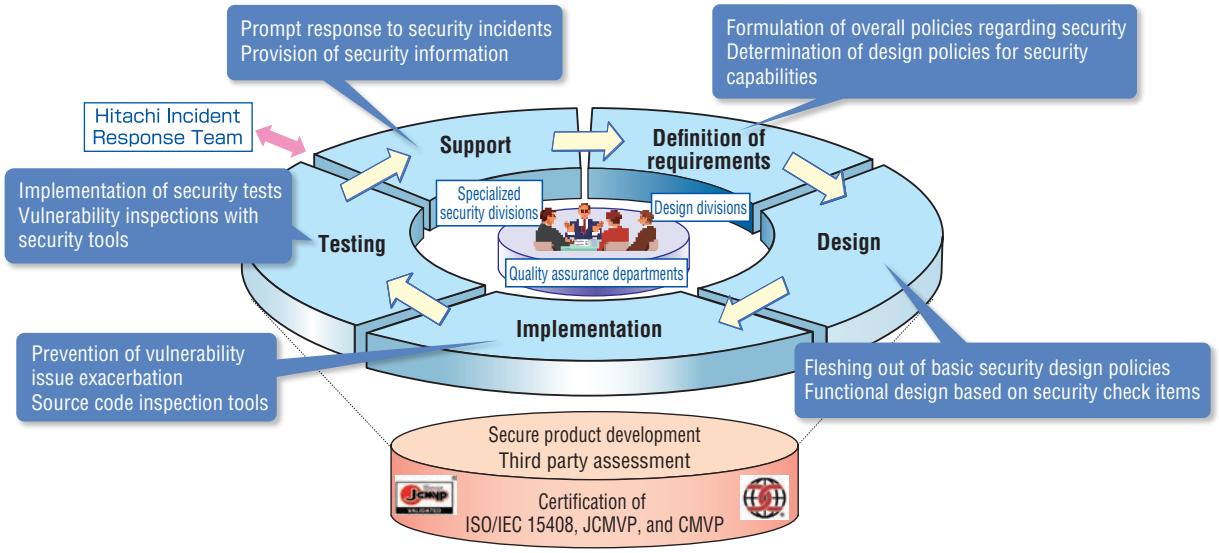
Examples of disclosure of vulnerability information in prominent OSS have become more prominent in recent years.

In order to deal with this, OSS information used in products is centrally managed, and initiatives have been put in place so that problem analysis, impact assessment, and selection of countermeasure policies can be carried out in a prompt manner.

OSS activity structure utilizing a component management database >>



Secure Development Life Cycle of Products Diagram >>



Application of third party assessment and certification systems

Initiatives in the “Secure Development Life Cycle of products” , namely, third party assessment and certification according to international security evaluation standard ISO/IEC 15408 are also incorporated as indicators objectively highlighting initiatives that ensure security, and the major Open Middleware Products HiRDB and Hitachi Command Suite have obtained these certifications.

This standard is also utilized in the “Standards for Information Security Measures for the Central Government Computer Systems” and other documents, as they are able to objectively highlight initiatives that “assure security” in product development.

By developing software based on the “Secure Development Life Cycle of Products” , it is possible to develop products that are on the same level as international standards like ISO/IEC 15408 (please refer to the “IT Security Certification” section in the “Third Party Assessment and Certification” for certified products.)

Reference information >>

■Japan Information Technology Security Evaluation and Certification Scheme (JISEC)
https://www.ipa.go.jp/security/jisec/index.html

■Japan Cryptographic Module Validation Program (JCMVP)
https://www.ipa.go.jp/security/jcmvp/index.html

■Cryptographic Module Validation Program (CMVP)
https://csrc.nist.gov/projects/cryptographic-module-validation-program

Information security products and services initiatives

Information security initiatives in cloud computing

Hitachi Cloud (Platform Resource Provisioning Services/Enterprise Cloud Services)
Hitachi is conducting various security initiatives relating to the cloud, a new form of IT provision and a part of social infrastructure, realizing a “safe and secure cloud” that is applicable to corporate information systems.

Cloud computing and security

IT, like electricity and water, is becoming common as “cloud computing” (“the cloud”) in which technology is used as a service, and does not require the user to possess any facilities or equipment.

In the cloud, not only are hardware and software maintained , but security measures are also carried out by service providers (cloud vendors), meaning the IT departments in user corporations can be freed from this task, and concentrate on constructing IT that will realize the core competencies of their own companies.

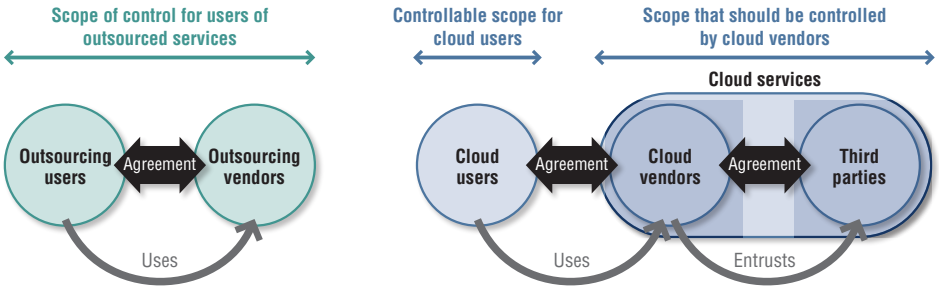
On the other hand, there are more than a few people who are concerned about problems like information leakage, as many different users share the same service provider environment.

Additionally, there is also the chance that the user will be put in danger of no longer knowing what content can be supervised or audited in the case of internal systems, for example compliance related to IT.

In this way, with the cloud, there is the necessity for information security corresponding to cloud-particular characteristics “sharing (resources with other users)” , and “using (vendor environments)” .

Furthermore, in the case that the cloud is used for only a portion of operational systems, assurance of information security to the same level as existing systems across all IT systems will be required.

Control scope differences between conventional consignment and the cloud>>



(a) Regular subcontracting (b) Using the cloud

Movements related to cloud computing information security

In response to this situation, guidelines and regulations for information security have been formulated regarding different sorts of industry groups and public bodies.

In addition to these, the proposal for international standards based on the guidelines of the Ministry of Economy, Trade and Industry, which was submitted by Japan's representatives to ISO/IEC SC 27, was standardized as ISO/IEC 27017.

The leading ones are listed below.

The purpose for the promotion and spread of these, Hitachi is also an active member of the “Cloud Information Security Promotion Alliance” which was established with cloud vendors and auditors from the “Japan Information Security Audit Association” .

Title	Security Guidance for Critical Areas of Focus in Cloud Computing	Cloud Computing Risk Assessment	Information security management guidelines for use of cloud services	Guidelines for information security measures for ASP/SaaS	Handbook for safe use of cloud services for small to medium sized enterprises
Publisher	CSA (Cloud Security Alliance), a not for profit group from the USA, with participating members from IT vendors, cloud service vendors, etc.	ENISA (European Network and Information Security Agency), a European network information security bureau (An EU institution)	Ministry of Economy, Trade and Industry, Commerce and Information Policy Bureau, Office for IT Security Policy	Ministry of Internal Affairs and Communications “ASP/SaaS Information Security Countermeasure Research Society”	Information-technology Promotion Agency, Japan (IPA) Security Center
Intended reader	Cloud vendors, Cloud users	Cloud vendors	Cloud vendors, Cloud users	Cloud vendors	Cloud users (Particularly small and medium-size enterprises)
Outline	Main issues and advice about domains	Cloud risk and control	Checklist for when using the cloud, functions for preparation when providing	Organizational, operational, physical, and technological countermeasures	A checklist designed for small to medium sized enterprises

Information security products and services initiatives

Information security initiatives to achieve a “safe and secure cloud”

Hitachi Group has made “Hitachi Cloud” , a global unified brand in the cloud, and is working to address the realization of a “safe and secure cloud” for the services belonging to this brand, based on these sorts of trends.

Using one of Hitachi Cloud services, the “Platform Resource Provisioning Services” (IaaS), as an example, the previously stated CSA, ENISA, and Ministry of Economy, Trade and Industry guidelines are used in a cross-sectoral manner, and checklists from the point of the service user and provider have been created relating to the IaaS/PaaS/SaaS service layer.

Necessary measures and procedures are being created and promoted based on the characteristics of each guideline, covering a variety of information security perspectives, through the implementation of systematic self-checks.

In particular, guidelines relating to each of the 13 domains indicated in CSA Ver. 3.0[*1] have had clarified for equivalent services, and different measures are being carried out in order to achieve those guidelines.

To give one example, in the “compliance and auditing” domain, it is necessary to implement services and audits with strict adherence to customer compliance stipulations even for cloud services.

The “Platform Resource Provisioning Services” provides guidance to be able to carry out thorough compliance for processing in the cloud in the, equivalent to customer internal compliances.

Measures to achieve these guidelines like compliance-related reporting and auditing methods are stipulated in an agreement with the customer, so that the customer can verify whether compliance is being followed.

Because standards relating to information security differ depending on the industry, organization of measures as they relate to the key criteria for each industry are also being promoted.

To give one example from the public sector which includes public authorities and local governments, the National center of Incident readiness and Strategy for Cybersecurity (the NISC) has published the “Unified Standards for Government Agency Information Security Countermeasures (2016 edition)” [*2], establishing criteria for administrative bodies.

Requirements relating to the application of cloud services to the public sector have been isolated, and information security enhancement reflecting services has been planned.

The vast business knowledge about information security that Hitachi has accumulated in product and SI business is being utilized in Hitachi Cloud. Hitachi will also continuously address initiatives to achieve a cloud that customers can use with peace of mind, based on trends in industry groups and standardization.

*1 Cloud security alliance: Security guidance for critical areas of focus in cloud computing V3.0
https://cloudsecurityalliance.org/ (November 2011)

*2 National center of Incident readiness and Strategy for Cybersecurity (the NISC):
Unified Standards for Government Agency Information Security Countermeasures (2016 edition)
http://www.nisc.go.jp/active/general/kijun28.html

Information security products and services initiatives

Efforts to protect privacy when using personal data

Advanced technologies such as IoT, AI and robotics have aroused our expectations that using large amounts of data, of various types, will achieve a super smart society. On the other hand, public awareness regarding privacy protection has been growing. Hitachi is striving to protect privacy, so that value can be created while client's and individual's safety and security are ensured.

Personal data utilization and protecting privacy

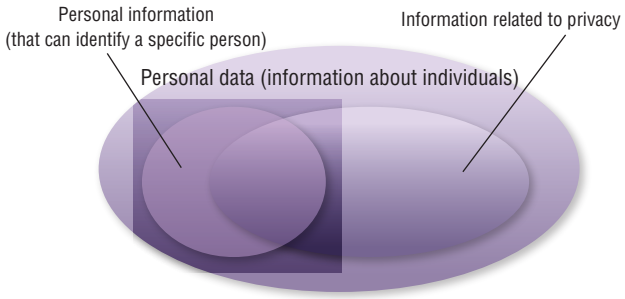
In Japan, the 5th Science and Technology Basic Plan, which was decided in 2016, focuses on the realization of a super smart society*1 (Society 5.0). People anticipate a society where a variety of things are connected via networks and large amounts of data, of various types, is analyzed by using AI and other technologies, to create new value. In particular, we expect to utilize personal data about individuals.

To protect the citizens' and consumers' privacy, legal systems are being improved and reviewed. In Japan, the Amended Act on the Protection of Personal Information went fully into effect in May 2017 to protect personal information appropriately while promoting the use of personal data. In the EU, the General Data Protection Regulation (GDPR) went into effect in May 2018.

As Diagram 1 shows, in the while of personal data overlaps with data related to one's privacy such as "location information" and "purchase history". To enable use of personal data, both personal information and privacy must be protected. Using this data to help citizens achieve affluent lives greatly contributes to the development of our societies.

*1: A society in which the things and services are provided to people who need them, when they need them, and in the amounts they need. In such a society, various social needs are handled in a fine-grained manner, and all people can derive from high quality services and live a comfortable life in which differences, such as age, sex, region, and language, are accepted.

Figure 1. Venn diagram "Types of personal data and their relationships"



Hitachi's privacy protection initiatives

Hitachi tries positively and proactively to solve new challenges in achieving a sustainable society where people can live easily, and implements initiatives to privacy protection to contribute the safety and security of individuals and our customers.

●Managing and operating a privacy protection advisory committee

Hitachi has been tackling privacy protection in big data businesses since 2012. In 2014, we expanded our initiatives to all departments related to information and telecommunications systems. We have assigned personal data manager, who manages privacy protection, and established the privacy protection advisory committee, which collects information about privacy protection and supports the risk assessments and countermeasures. These days, such support is expanding into IoT (Internet of Things) businesses because the whole Hitachi Group is putting considerable effort into IoT. Every employee strives to work with our customers to implement appropriate measures and to reduce privacy risks.

●Implementing privacy impact assessments

In businesses that handle personal data, Hitachi's original checklist is used to assess privacy impacts.

Furthermore, in cases which risks are identified as high, or assessments are difficult for operational departments to make, specialists from the privacy protection advisory committee support identify risk countermeasures.

More than 300 assessments have been conducted so far. Checklists are constantly being evaluated and improved based on the results of actual cases.

●Privacy protection education

To achieve appropriate privacy protection and use personal data appropriately, staff members must have a correct understanding about privacy, must protect privacy.

For these purposes, in addition to periodically conducting training and sharing information about privacy protection, we are also examining privacy best practices.

Information security products and services initiatives

Example of privacy protection at Hitachi

●Verification test using a humanoid robot

A camera and a microphone were installed in a robot, personal data such as the voices and images of the persons who talked to it was collected. We thought that it would be difficult for ordinary people to envision that a robot collects voices and images. Therefore, to protect the privacy of the persons talking to the robot, we posted an explanatory notice that indicated who was conducting the verification test, what data was collected, and how long the data would be stored. This notice was posted in a location where people could see it before they talked to the robot. We also provided a contact point and allocated personnel to answer inquiries quickly.

Privacy notice

Robot is taking Video and Audio in the following purpose.

The information is used only for

(1) Feasibility study of Robot as Service Staffs, and

(2) Improvement of Robot and its supporting system.

We DO NOT identify the individuals based on the information acquired.

Responsibility	Hitachi, Ltd.
Type of information	Robot has camera and microphone. We are collecting video and audio around Robot from these devices.
Term	We are planning to continue the feasibility study for 2 years. Information collected by Robot will be stored and used for improvement of Robot and its supporting system for 2 years. The information stored will be deleted immediately after 2 years.
Provision to the Third Party	We NEVER provide the information collected or stored to third parties.
Contact	Staffs around here, or Hitachi, Ltd. XXX Business Unit XXX XXX TEL：xx-xxxx-xxxx

Around Robot, Video and Audio are collected within 3meters.
Please be careful not to go near Robot if you would not like to be recorded.

Aiming to provide services that our customers can use safely

Privacy protection is important in making use of personal data made possible by technological advances. Since it published its privacy-protection initiatives in a white paper in 2013*2, Hitachi has applied this initiatives to many businesses. To use our expertise based on our experience on business with customers and to create a social consensus about safety and security on use of data, Hitachi revised and released the white paper based on our latest privacy-protection initiatives.*3 We hope that the white paper is read and referenced widely. We want to improve these initiatives while receiving feedback from a variety of readers.

Hitachi will contribute to the realization of a super smart society by ensuring the safety of individuals and providing services that our customers can use safely. We will achieve this through conducting opinion surveys, understanding trends in legal systems and technologies, and applying our expertise to actual businesses.

*2: Hitachi' s initiatives in privacy protection in big data businesses (released in May 2013)
http://www.hitachi.co.jp/products/it/bigdata/field/statica/wp_privacy.pdf

*3: Hitachi' s initiatives in privacy protection in use of personal data (released in October 2017)
http://www.hitachi.co.jp/products/it/bigdata/bigdata_ai/personaldata_privacy/index.html

Physical security products and services initiatives

Initiatives for improving solutions by using physical security products and services

Hitachi provides (i) video surveillance systems, (ii) video analysis systems, (iii) access control systems, and (iv) remote monitoring and support. These solutions are available for a range of facilities: from individual office buildings to multiple locations over a wide area. Hitachi strives to improve physical security solutions that help monitor and control people, things, and information, and that solve our customers' business issues and challenges.

Background to enhancing physical security

(1) Information security and physical security

The proliferation of IT and advances in IoT technologies are accelerating the digitization of customer and business information, and the networking of business systems. These changes, however, are accompanied by increasing risks of information leakage. To reduce such risks, we must improve information security. As part of these efforts, there is an increasing need for physical security, including restricting access to rooms where information is stored, monitoring images of scenes in important facilities, and controlling access to lockers and safes.

In introducing physical security, it is important to clarify which locations and what information are to be protected, to set an appropriate security level, and to build a system appropriate for that level. Many of the devices composing a physical security system can be regarded as IoT devices. Therefore, if attackers take over an IoT device that has no strong security measures, the subsequent intrusion into important systems might result in the theft and falsification of a variety of data (such as image data, personal information, and company information) stored on the physical security system, and attacks on critical systems. Thus, active use of IoT data is connected to increased risks of more serious threats.

Information security measures are also required for the physical security system itself.

(2) Physical security requirements for an office building

The physical security of an office building includes systems such as an access control system, which manages and controls the entrances and exits from the building and rooms, and an video surveillance system, which uses cameras to monitor the flow of people who enter and exit the building and to monitor the status of each area.

It is important to use an access control system in combination with an personal authentication technology (such as IC cards or finger vein authentication) that is appropriate for the security level required for each area in an office building. Other effective requirements include access control for PCs and business systems, cooperation with an information management system for authentication when printing documents, and cooperation with an equipment control system that uses authentication results to restrict which elevator floors can be accessed.

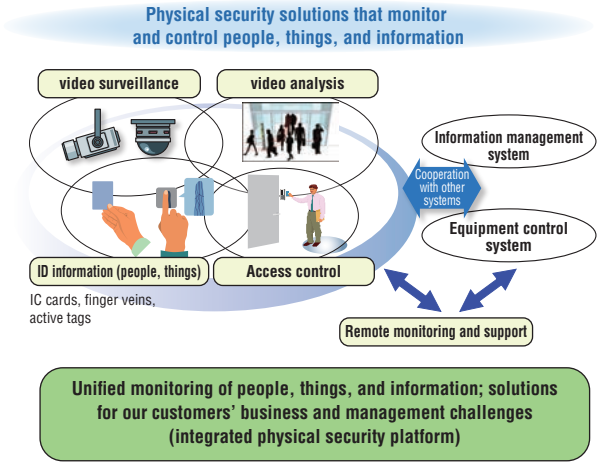
In addition to achieving the goals of physical security, in recent years linkage among systems has become important for energy savings. For example, to control air conditioning and lighting, a video analysis system and an access control system can be linked with an equipment control system.

A company with sites at multiple locations needs to unify the security level at each site and to provide unified management by a central department.

(3) Physical security requirements for multiple sites over a wide area

For physical security requirements for multiple sites over a wide area, such as at a power station, airport, factory, or railroad, it is important to have integrated monitoring of the dynamic state (flow and status) of people and things. To do this, you need many monitoring cameras, access control devices, and IoT sensors placed around the perimeters, in the area sites, in vehicles, and in the buildings.

Multiple sites over a wide area generate a large amount of dynamic state information, so it is important to reduce the labor required for monitoring. To achieve this, the information collected from many devices and multiple locations can be monitored automatically. For example, camera image analysis can automatically detect suspicious persons and things, while reducing the loads on network bandwidth and image storage space.



Physical security products and services initiatives

Security enhancement- concept and products/services

In order to assure physical security, it is necessary to construct systems to monitor and control the flow of movement of people and information, and to help resolve customers' operation and management issues. To do this, we need to appropriately combine video surveillance systems, video analysis systems, and access control systems with individual verification and ID information management technology. Where necessary, we plan coordinated operation with information and facility management systems. Based on these ideas, we provide solutions utilizing the products and services with the features below, and utilizing an integrated physical security platform.

(1) Video surveillance

In recent years, networked cameras that utilize IP networks have become increasingly common. We provide video surveillance systems with low installation cost and high performance. High-resolution technology developed by Hitachi is used for the network cameras installed at each location. This technology allows high-quality images to be compressed to 1/3 to 2/3 their original size, and reduces the loads on the storage devices for recorders and video servers, as well as on network bandwidth. Furthermore, we offer integrated video-management systems that can centrally manage live footage and can play back video from multiple locations.

(2) Video analysis

The flow of movement of people can be made visible by analyzing camera images. We are progressing with the automation of surveillance operations: for example, to count the number of people in camera images, and to detect a person entering a specified area and classify the situation as an intrusion. Different video analysis processing can be assigned to different cameras installed in different locations, which is useful for analyzing situations, detecting suspicious persons and objects, and detecting abnormal behavior.

(3) Access control

To offer an access control system appropriate to the operating environment, it is necessary to combine different technologies: such as various types of non-contact IC cards, finger vein technology to assure robust security, and active tags that enable wireless verification of individuals. For those companies that manage multiple locations, a unified security policy can bring flexibility to permission settings: for example, a single card having access to all locations but restricting entrance and exit to rooms according to the location or department. Designated persons can easily operate these settings from an internet browser, which makes it easier to implement and operate the systems. Furthermore, because these services can be provided via a cloud without setting up a server at each location, small and medium sized locations benefit from the simple implementation. Linkages with information management systems and facility management systems can enable both enhanced security and controls for energy savings.

(4) Remote surveillance/support structures

Customer service centers and call centers are connected to the service networks at sites across the country. With an organizational structure that enables constant (24 hours a day, 365 days a year) monitoring, the structure supports customers' security-related systems by ensuring safe operation and providing emergency responses.

(5) Integrated physical security platform

Hitachi provides solutions utilizing a integrated physical security platform to centrally monitor movement of people information and resolve customers' operational and managerial issues.

This platform enables central monitoring of on-site data collected and accumulated by means of various physical security systems, such as by surveillance cameras in access control systems, and by IoT sensors. In addition, however, the platform can also analyze and utilize such data to develop solutions that provide and control information to improve operational and managerial issues of customers.

For example, in factories and distribution sites, the platform can increase productivity by detecting deviations from normal operations from camera images of line operations, and by issuing instructions to correct such deviations. In commercial facilities, the platform contributes to sales increases by suggesting changes in products types and layouts through the analysis of gender, age, and buying behavior of people in camera images. Furthermore, Hitachi can provide even advanced solutions by using business intelligence tools and artificial intelligence to analyze big data collected from various physical security systems, IoT sensors, and camera images.

With these types of features, our physical security products and services enhance total solutions that resolve customers' operational and management issues and that protect assets, safety, and security. The solutions can scale from an office or building, to multiple locations and broad areas.

Control products and systems initiatives

Initiatives to ensure information security in control products and systems

Connection and coordination of control systems that support important infrastructure with information communications systems has moved forwards recent years, and information security risks starting with cyber attacks are heightened. Systems even more secure than present systems and rigorous management of customer confidential information is necessary for the uninterrupted and safe system management. The Control System Platform Division of Hitachi, Ltd. is working on solutions for these types of problems.

Background and goals

Information control systems, which form the center of control systems that make up the base of social infrastructure, must operate on a 24-hour basis as prerequisite, with a high level of reliability.

Information security is related to safety, and the uninterrupted and safe operation of information control systems is possible through the appropriate management, maintenance, and operation of information assets. In particular, the confidentiality of customer-related information must be maintained completely.

In order to fulfil these demands, information control systems maintain information security against threats from the outside, in principal by physically blocking other systems.

At the same time, under the national IT strategy of “a society in which anybody can freely access information” , measures such as “information cooperation infrastructure development” have been implemented.

Security threats relating to information control systems are diversifying in this environment of change, and the role of information security technology will become increasingly bigger in from now.

There are many instances in which important customer information is incorporated for system development, and these sorts of information leaks are a direct threat to social infrastructure.

The initiatives of the Control System Platform Division concerning these issues are stated below.

Management of customer confidential information and organization of development processes

●Establishment of Information Security Management System (ISMS)

The Control System Platform Division provides information control system solutions that support social infrastructure and the foundation of industry (such as electricity, traffic, steel, water, industry, and power electronics), and these require organizational information security management.

Maintenance of confidentiality for customer information and results configured from that information are of particular importance.

To respond to these demands, the Control System Platform Division constructed an ISMS based on the International Standards Information Security Management System (ISMS) (ISO/IEC 27001: 2005) under the direction of top management. In January 2010, the division completed acquisition of certification.

From now, ISMS certification will continue to be maintained while the fields to which it can be applied are expanded.

Currently, the Control System Platform Division is in the process of amending its ISMS according to the ISMS International Standards amendment (ISO/IEC 27001: 2013).

●Formation of security aware product development processes

The following development processes were formulated in 2005, and have been applied to system development.

(1) Evaluate security risk at the beginning of the development process.
(2) Verify security risk settings in the design review stage (protection settings, countermeasure policies).
(3) Confirm security requirements with a security verification tool or similar before shipping from plants and before handing over to customer.

However, security risk for control systems is increasing, and with corresponding trends like “acceleration of international standards and certification” and “customer demand for control vendors to acquire security verification” , the environment surrounding control systems is constantly changing.

The Control System Platform Division has responded to this situation by cooperating with domestic and international organizations like the Control System Security Center which commenced in 2012.

Regarding strategies for international standards, requirements for standards for different domains like the IEC 62443, NERC CIP (North American electric standards), and WIB (European industrial standards) have been investigated, and conditions requiring strict adherence have been formulated as security standards, and turned into guidelines.

Control products and systems initiatives

Control systems security

●Control-system security risks and government initiatives

Control systems are evolving each day and are being used more efficiently because control systems are operating over broad areas, business suppliers are collaborating in the use of control systems, and the application of IoT technologies to control systems has started.

On the other hand, cyber attacks, such as targeted attacks, have become more sophisticated and diversified. Control systems have came under cyber attacks, and security risks have appeared.

The Japanese government takes initiatives centering on NISC (National center of Incident readiness and Strategy for Cybersecurity), in cooperation with the Cabinet Office and each governmental ministry and agency.

For example, the Basic Act on Cybersecurity came into force in November 2015. Also, the Cybersecurity Management Guidelines were formulated by Japan' s Ministry of Economy, Trade and Industry in December 2015 to advance the handling of security threats caused by cyber attacks.

●Hitachi' s approach to security

It is important to apply countermeasures to protect control systems against security risks, but that alone is insufficient. Cyber attack methods advance every day, so systems need to be continuously improved even after security measures are applied. Furthermore, it is also vital to establish organizational structures so that, if a security incident occurs, the organization can promptly identify the problem, take countermeasures, and recover from the problem.

Hitachi, Ltd. has established the approach of "Protect by systems. Protect by organizations. Protect by operations." and has been working to implement this approach under the idea of H-ARC®. H-ARC® is an approach to protect control systems based on security platform products (H: Hardening). For "Protect by systems" , H-ARC® takes an adaptive (A: Adaptive) approach to implement countermeasures in advance and to prevent unknown threats. For "Protect by operations" , H-ARC® emphasizes responsiveness (R: Response) and strives to minimizes damage after an attack and shorten recovery time. For "Protect by organizations" , H-ARC® supports cooperation (C: Cooperative) among different organizations and business suppliers through security operation management services.

●Security platform products

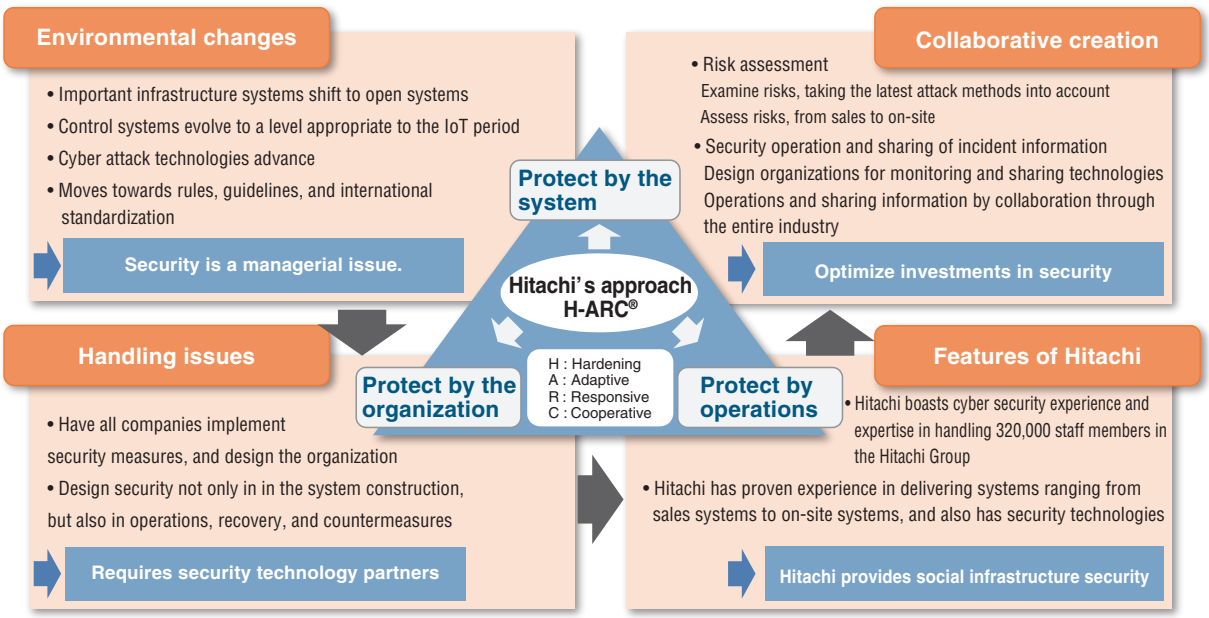
As security platform products, we provide products related both to the cyber and physical aspects. For cyber security, for example, we provide one-way relay systems that can protect control systems by physically shutting out unauthorized access from outside to prevent unauthorized intrusions in cyber space.

For physical security, we provide entrance/exit management systems that utilize finger vein verification. We also provide an integrated explosives detection system within gates.

●Security operation management service

Even after security measures are implemented to protect them, control systems must be continuously monitored. It must be possible to design appropriate security operations, to detect security threats at an early stage, to respond quickly. To enable these, it is essential to collect information from control systems in a timely manner, to effectively analyze the information, and to quickly develop and implement proper countermeasures.

Hitachi, Ltd. has established a Security Operation Center (SOC) that performs these tasks, provides services such as support for actual operation, provides analysis support from specialists who have SOC operation expertise in their companies, and provides training related to development of human resources who handle security threats.



Initiatives for strengthening organizations

Integrated Cyber Security training

For measures against cyberattacks, Strengthening the ability the human resources and organizations are as important as strengthening systems. Hitachi provides training services with the goal of enabling practical responses when a cyber incident occurs. Such training contributes to strengthening the security of important infrastructure systems.

Characteristics of Integrated Cyber Security training

Our Integrated Cyber Security training provide training sessions for handling cyberattacks. The training services focus on strengthening both people and organizations. The services provide support for verifying and improving our customers' cyber BCPs, and contribute to the building of organizations that can respond to cyberattacks quickly.

To simulate actual cyber incidents, we created training facilities (Nx Security Training Arena) that are equipped with information and control systems similar to those used in actual company infrastructures. In these facilities, we provide a training curriculum based on the technologies and expertise cultivated at Hitachi. The information and control system environment and the curriculum can be customized to best suit individual customers.

Aims of the Integrated Cyber Security training

(1) To provide cyber-BCP simulation training sessions in an environment where the information and control systems work together

By using an environment containing both information systems and control systems, we are able to support the verification of cyber BCPs based on cyberattacks on different systems.

(2) To provide SOC/CSIRT operation training sessions focusing on cooperation among organizations

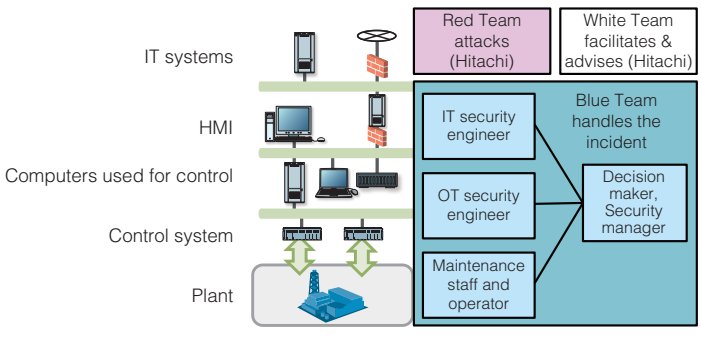
Trainees receive training after being assigned various roles (operator of an information or control system, SOC, CSIRT, manager, executive-level person, etc.). To practice communications among different locations, the trainees are located in separate rooms based on their assigned roles. Trainees are trained to handle incidents as a CSIRT or manager, in situations with limited means of communication.

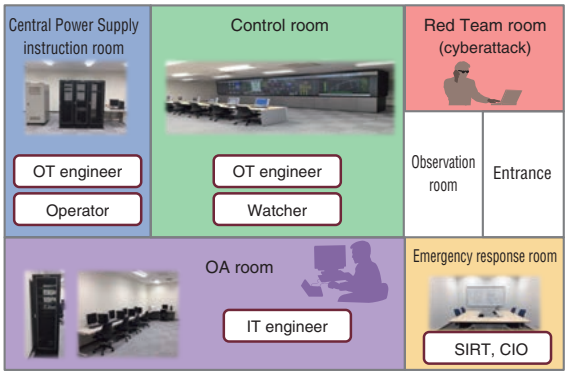
When trainees are at a loss over what to do during a training session, instructors advise them as necessary on what measures they need to implement. After the training finishes, feedback is provided about trainee responses during the training.

(3) To handle the latest variety of incident patterns

Training scenarios can provide various events from the failure of a device to a security incident. To determine whether an incident was caused by a cyberattack, trainees can practice complex responses such as checking information from multiple systems.

The latest security trends are provided in cooperation with the HIRT and research centers in Hitachi. For issues that have surfaced through cyber defense training services and potential issues about security, Hitachi continuously contributes to the building of stronger customer organizations from multiple perspectives, using the Nx Security Training Arena as a base point.





Research and development

Research and development for achieving and further evolving Hitachi's security vision

Hitachi conducts research and development (R&D) in security technologies to further evolve three approaches (*protect by organizations, protect by systems*, and *protect by operations*) that provide security against increasingly dangerous cyberattacks.

Introduction

In recent years, cyberattack threats have become increasingly dangerous, with attacks impacting not only conventional IT systems but also the entire social infrastructure including control systems. In response to this situation, Hitachi has adopted three approaches for providing security: protect by organizations, protect by systems, and protect by operations.

Hitachi's R&D team combines the security technologies cultivated by Hitachi with Hitachi's expertise in various social infrastructure systems, such as electricity, railroad, gas, water, manufacturing, information and communications, finance, and the public sector. The team is conducting R&D in security technologies so that these three approaches can evolve further.

Evolving the approach protect by organizations

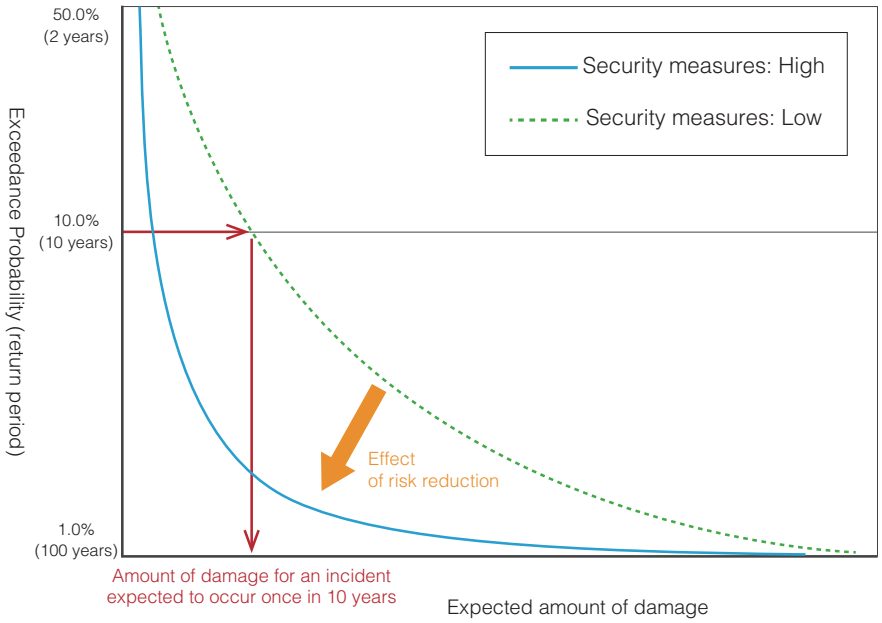
In recent years, security measures have become indispensable because the threats of cyberattacks are becoming increasingly dangerous. However, it is difficult to calculate the probability of a security incident, and to quantitatively measure the ROSI (Return On Security Investment). Therefore, it has been difficult to determine whether the cost of implementing countermeasures is a good investment.

●Technology to analyze security risks

Sompo Japan Nipponkoa Insurance, Sompo Risk Management & Health Care, and Hitachi conducted joint research to promote cybersecurity responses in industrial and critical infrastructures in Japan. This joint research combines (i) the risk assessment technologies cultivated by Sompo Japan Nipponkoa Insurance and Sompo Risk Management & Health Care in their nonlife insurance businesses, with (ii) the security handling technologies and vulnerability-risk evaluation techniques cultivated by Hitachi when building systems in the industrial and critical infrastructure fields. This combinatory research is developing comprehensive quantitative analysis methods for cyber risks.

As a result of developing and verifying technology that uses simulations to quantify the damage that would occur if a cyberattack occurred at a large manufacturing factory, we demonstrated that the cyber risk corresponding to the system structure and status of security measures can be calculated as the following information about a security incident: the rate of occurrence and the amount of damage.

Figure. Curve that shows the relationship between the expected amount of damage and the probability that the expected amount of damage will be exceeded in one year >>



Research and development

Evolving the approach protect by systems

As the targets of cyberattacks expand from IT systems to the entire social infrastructure including control systems, traditional security measures (which mainly aim to protect information and data) alone are insufficient.

Hitachi is developing security monitoring technologies for control systems that cannot be handled by traditional information security technologies, and physical security technologies that analyze image data to detect suspicious persons.

●Security monitoring for control systems

Because control systems cannot be stopped easily, it is difficult to frequently implement security measures that require system modifications. These days, however, it is necessary to continuously monitor systems and quickly respond to ever-evolving cyberattacks.

Hitachi developed security-monitoring devices and by using them in combination with Hitachi's incident-detection devices such as NX NetMonitor, Hitachi has developed a security monitoring solution available for existing control systems. The impact of the solution on systems is small, even in a control system where frequent system modifications are difficult. Therefore, the introduced solution minimizes verification costs and operation risks, and enables maintenance personnel to quickly detect and respond to incidents. The solution can accelerate the identification of the source of an incident and the extent of the impact on a control system, and can perform an initial response that isolates the problem area from the network. This prevents the spread of damage in an incident.

● Technology for tracking persons over a wide area

In large facilities, such as an airport or train station, and in public spaces, such as a town square, monitoring by security cameras is provided to ensure safety. However, it is difficult for the limited number of staff to check all images. As a result, existing technology was developed that uses cloth colors and facial images (from photographs taken beforehand at the entrance) as clues to discover or track a person.

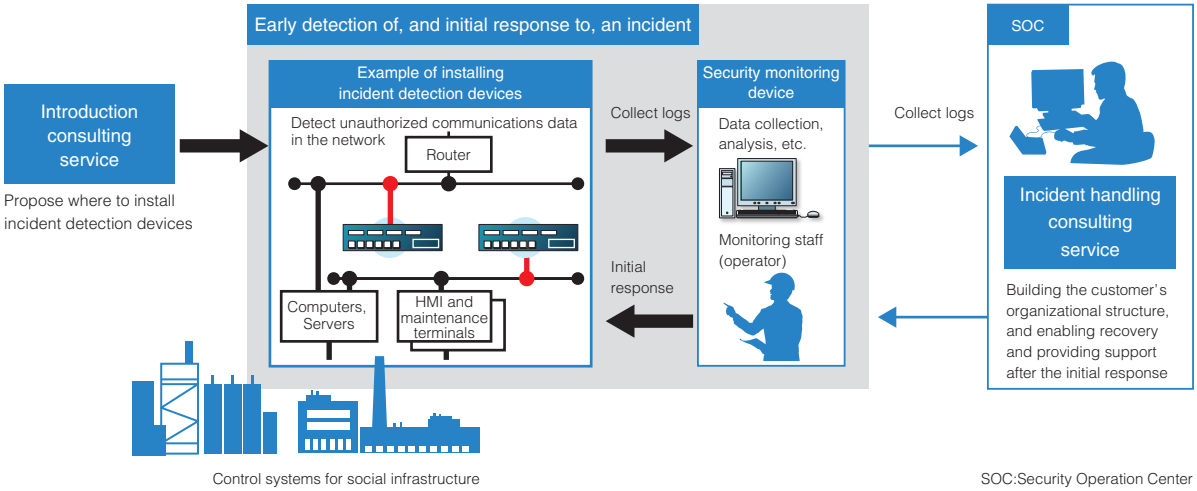
Hitachi is developing technologies that use an AI to distinguish features (such as the sex, age group, and clothes) to discover a relevant person and to trace the movement of that person from the images from security cameras over a wide area. The AI carries out these activities in real time. Features of these technologies are as follows:

(1) Technology that discovers persons at high speed, by distinguishing and searching for the characteristics of a person's appearance and movements

(2) Technology that tracks persons at high speed, by analyzing a person' s whole-body image in detail and extracting images of the same person

Figure. Wide-area human tracking system that uses these technologies >>

Figure. Security monitoring for control systems >>

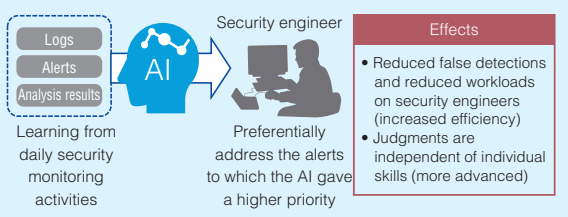


Research and development

Evolving the approach protect by operations

The number of cyberattacks is increasing year by year, and the risk of multiple locations being attacked in a short time is also increasing. To achieve security operations that can handle the increasing number of more sophisticated cyberattacks, Hitachi is developing a technology that uses an AI to provide more efficient and advanced security monitoring activities, and a technology that enables multiple organizations to respond to incidents by working together.

Figure. Using an AI in security monitoring activities >>



●Using an AI to provide more efficient and advanced security monitoring activities

In security monitoring activities, analysts analyze alerts from security devices, such as SIEM, and determine whether the alerts are caused by real incidents. Handling a large number of alerts places a big burden on analysts.

As a replacement for such analysis activities, Hitachi developed a technology that uses AI to automatically judge alerts. In this technology, the AI learns the relationships between past alerts and the corresponding human judgments. Based on these learned relationships, the AI automatically determines the priority of responses to an alert. Because the AI makes its determinations based on the facts, such as the results of analyzing past alerts, the system can avoid the problem of different analysts making different judgments. Verification tests show that the technology removed up to 95% of alerts while avoiding overlooked alerts, and resulted in a large increase in efficiency.

SIEM:Security Information and Event Management

●Decentralized security operations

In traditional incident responses, a specific security response team acts as a hub and collects incident information and analysis data, manually asks multiple security response teams to perform the analysis, and sends them the analysis data. Hitachi is developing *decentralized security operation technology* in which a specific security response team is not involved in all incident responses. Instead, the security response team in each organization addresses an incident autonomously in a decentralized manner and works with other teams as required. This technology formalizes and standardizes the functions (such as information collection and analysis) required to respond to an incident. The technology mutually checks the functions assigned to each security response team in real time, and automatically assigns processing to a dedicated team.

To verify the effects of this technology, incident-analysis data monitored by the Keio University Information Technology Center was sent to Hitachi's Open Lab Yokohama, where we built and have started evaluating a demonstration environment where analysis can be requested.

Figure. Distributed security operations >>

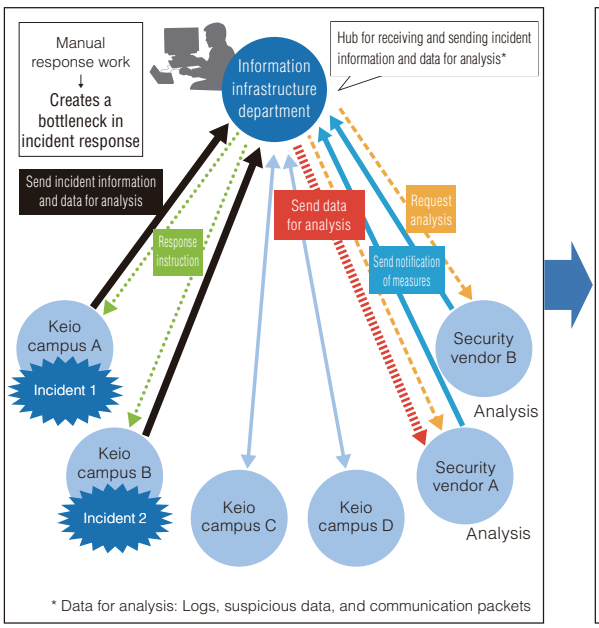


Figure (a): Traditional security operations

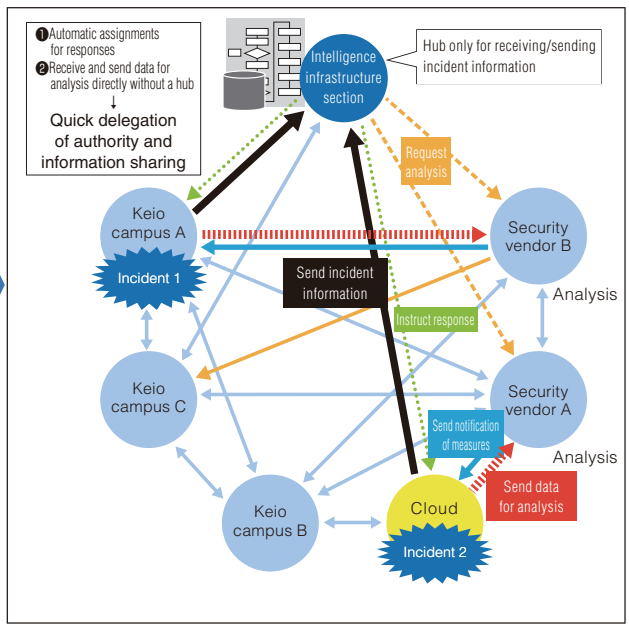


Figure (b): Distributed security operations using dynamic authentication and approval technologies

Research and development

Evolving personal authentication technologies

Personal authentication that checks whether a person has legitimate authority is indispensable for ensuring security. Hitachi has developed finger vein authentication technology and deployed it in access control systems and financial services. As digitization advances, personal authentication is becoming necessary in more services. It is also required in evolving the approaches protect by organizations, protect by systems, and protect by operations. Hitachi is developing technology that evolves personal authentication technology which uses our own finger vein authentication technology at the core.

●Walk-through finger vein authentication technology

With many of the personal authentication methods in current use, a person must stop for authentication. This results in congestion when many persons need to be authenticated. However, it is difficult to achieve high authentication accuracy in authentication methods that authenticate moving persons.

Hitachi has evolved its finger vein authentication technology further by developing the following: (i) technology that instantly detects the positions and directions of multiple fingers held over the sensor, and (ii) technology that photographs the vein pattern based on the positions and directions of the fingers. These technologies instantly detect the veins of fingers held in various positions and directions. Even in large facilities visited by many people, the technologies can smoothly and accurately identify persons holding their fingers over the sensor while walking.

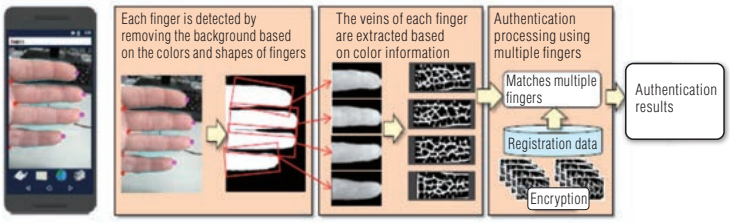
●Finger vein authentication technology for smartphones

In recent years, more and more people are using smart phones for online shopping and to manage personal information. While the personal authentication methods used in smartphones usually use a method such as a password or fingerprint, a safer and more accurate method is becoming more and more necessary.

Hitachi developed a technology that can accurately perform finger vein authentication by using a camera installed in a smartphone.

This technology detects each finger from a color image taken with the smartphone camera and extracts the vein pattern. By combining the vein patterns of multiple fingers, high authentication accuracy is achieved. This provides smartphones with finger vein authentication that prevents forgery and spoofing.

Figure. Basic principle of finger vein authentication with a camera in a smartphone >>



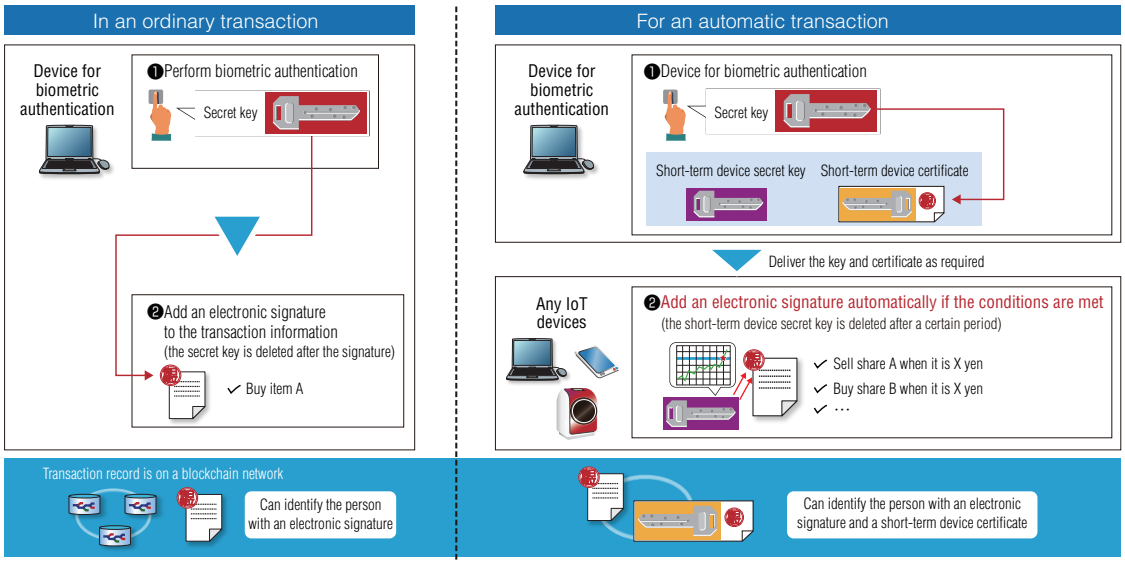
● PBI-blockchain technology

Blockchains provides a transaction infrastructure that enables transactions without the intervention of third-party organizations. As such, blockchains are expected to be used in many areas, such as for virtual currency trading, for buying and selling of goods, and for managing consultation histories in hospitals. The reliability of blockchain transactions is ensured, because the user adds an electronic signature to transaction information so that everyone can verify its validity. However, if the key for generating an electronic signature is lost or disclosed, the blockchain asset might be lost or unauthorized dealings by spoofing might occur.

PBI is a proprietary technology of Hitachi that can generate an electronic signature from biometric information. Hitachi developed a PBI-blockchain collaborative technology that makes PBI available on a blockchain. Because biometric information can be used as a key, external management of the key is not necessary. Hitachi also developed a technology that generates short-term device certificates for automatic transactions. The technology can automatically generate an electronic signature based on specified conditions, which eliminates the inconvenience of requiring authentication for each transaction.

PBI:Public Biometrics Infrastructure

Figure. Overview of PBI-blockchain collaborative technology >>



Company-external information security related activities

Hitachi leverages the skills and experiences of each of its staff members to achieve a more secure information technology based society through participating in different types of security related company-external activities.

International standardization activities

Hitachi participates in the following activities relating to international standardization.

●ISO/IEC JTC1/SC27

Subcommittee SC27 of the joint technical committee ISO/IEC JTC1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), formed to internationalize standards, is investigating the standardization of information security management systems (WG 1), cryptography and security mechanisms (WG 2), security assessment technology (WG 3), security controls and services (WG 4), and identity management and privacy technologies (WG 5).

●ISO TC292

The International Organization for Standardization (ISO) technical committee (TC) 292 is investigating the standardization of the security field including general security management, business continuity management, resilience and emergency management, fraud prevention countermeasures and management, security services, and homeland security.

●ISO TC262

Under the theme of risk management, the International Organization for Standardization (ISO) technical committee (TC) 262 is investigating the standardization of items such as terms, principles, policies, and risk assessment techniques, for all risks.

●ITU-T SG17

SG17, one of the study groups (SGs) of the International Telecommunication Union-Telecommunication Standardization Sector of the International Telecommunication Union, is investigating the standardization of cyber security, security management for communications vendors, telebiometrics, of security capabilities for communications and applications services, spam countermeasures, and identity management.

●IEC TC65/WG10, WG20

Technical committee TC 65 of the International Electrotechnical Commission (IEC) is promoting the standardization of industrial automation, monitoring, and control.TC 65/WG 10 is investigating the formulation of standards regarding the security of networks and control devices in control systems. In addition, TC 65/WG 20 is investigating the formulation of standards regarding both security and safety of functions in control systems.

●OASIS CTI

Cyber Threat Intelligence (CTI) of the Organization for the Advancement of Structured Information Standards (OASIS) is investigating the formulation of standards regarding Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), which will enable relevant personnel to describe cyber-attack activities and to exchange such information.

CSIRT activities

Besides the CSIRT activities in Hitachi Group, Hitachi is participating in external CSIRT activities with HIRT (Hitachi Incident Response Team) as the point of contact (PoC). Hitachi also works with external CSIRT organizations to promote the sharing and exchange of information, such as information about vulnerabilities.

●FIRST

FIRST (Forum of Incident Response and Security Teams) is an international community of incident response teams in universities, research institutions, companies, and government organizations based on a relationship of mutual trust. As of the end of June 2018, 431 teams in 89 countries have joined FIRST.

●Nippon CSIRT Association (NCA)

The NCA organization was established to resolve challenges in CSIRT activities by sharing information and cooperating among the CSIRT organizations that operate in Japan. It promotes and supports the establishment of a CSIRT and builds an organizational structure for cooperation between CSIRTs when an incident occurs. Thus, it provides an environment where organizations can autonomously improve basic incident handling capabilities so that the CSIRT community in Japan can cooperate in the event of an emergency. Hitachi is a foundation member of NCA and has chaired the steering committee since 2015. In this role, Hitachi promotes the proliferation of CSIRT activities in Japan.

Other activities

In addition to the above activities, Hitachi is participating in the following external activities that promote security-related research, examinations and discussions, deployments, and education. We also deliver lectures in various seminars and academic conferences.

- 10 Major Security Threats Committee etc. in the Information-technology Promotion Agency, Japan (IPA)
- ISMS committee, control system SMS committee etc. in JIPDEC
- Japan Cybercrime Control Center (JC3)
- Japan Information Security Audit Association (JASA)
- Japan Network Security Association (JNSA)
- Japan Information Security Management Systems User Group (J-ISMS UG)
- Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) Process automation and factory automation measurement control committee security survey and research WG
- Control System Security Center (CSSC)
- Information security investigation committee etc. in Japan Electronics and Information Technology Industries Association (JEITA)
- IC-Information Sharing and Analysis Center Japan (ICT-SAC Japan)
- Council of Anti-Phishing Japan
- Assessment organization certification technical committee etc. in the National Institute of Technology and Evaluation (NITE)
- Industrial security action group etc. in the Robot Revolution & Industrial IoT Initiative

Third party assessment and certification

Hitachi promotes the acquisition of third party assessments and certifications relating to personal information protection, information security management, and products.

Privacy Mark entities

The following companies have permission to use the Privacy Mark, acquired by Hitachi from JIPDEC (As of the end of May 2018).

Hitachi, Ltd.
Hitachi, Ltd. Corporate Hospital Group
Hitachi Building Systems Co., Ltd.
Hitachi Consulting Co., Ltd.
Hitachi Document Printing Co., Ltd.
Hitachi Document Solutions Co., Ltd.
Hitachi Foods & Logistics Systems Inc.
Hitachi Healthcare Systems, Inc.
Hitachi High-Tech Solutions Corporation
Hitachi Hi-System21 Co., Ltd.
Hitachi ICT Business Services, Ltd.
Hitachi Industry & Control Solutions, Ltd.
Hitachi Information Academy Co., Ltd.
Hitachi Information & Telecommunication Engineering, Ltd.
Hitachi Information Engineering, Ltd.
Hitachi Inspharma, Ltd.
Hitachi Insurance Services, Ltd.
Hitachi-kenpo
Hitachi KE Systems, Ltd.
Hitachi Management Partner Corp.
Hitachi-Omron Terminal Solutions, Corp
Hitachi Power Solutions Co., Ltd.
Hitachi Research Institute
Hitachi Social Information Services, Ltd.
Hitachi Softec Co.,Ltd.
Hitachi Solutions, Ltd.
Hitachi Solutions Create, Ltd.
Hitachi Solutions East Japan, Ltd.
Hitachi Solutions West Japan, Ltd.
Hitachi Systems, Ltd.
Hitachi Systems Engineering Services, Ltd.
Hitachi Systems Field Services, Ltd.
Hitachi Systems Networks, Ltd.
Hitachi Systems Power Services, Ltd.
Hitachi Technical Communications Co., Ltd.
Hitachi SC, Ltd.
Hitachi Techno-Information Services, Ltd.
Hitachi Urban Investment, Ltd.
Hitachi Urban Support, Ltd.
Hokkaido Hitachi Systems, Ltd.
Kyushu Hitachi Systems, Ltd.
Okinawa Hitachi Network Systems, Ltd.
SecureBrain Corporation
Shikoku Hitachi Systems, Ltd.

ISMS Certification

The following shows Hitachi' s organizations that have acquired the ISMS certification from the ISMS Accreditation Center (ISMS-AC) based on the international standard for information security management systems (ISO/IEC 27001) (as of the end of May 2018).

Hitachi, Ltd. (Financial Information Systems 2nd Division, Government & Public Corporation Information Systems Division)
Hitachi, Ltd. (Healthcare Business Unit, Healthcare Solutions Division, First Section)
Hitachi, Ltd. (Social Infrastructure Information Systems Division)
Hitachi, Ltd. (Services & Platforms Business Unit)
Hitachi, Ltd. (Services & Platforms Business Unit, Control System Platform Division)
Hitachi, Ltd. (Social Infrastructure Systems Business Unit, Government & Public Corporation Information Systems Division)
Hitachi, Ltd. Defense Systems Bisiness Unit (Yokohama Branch Office/Ikebukuro Branch Office) and Hitachi Advanced Systems Corporation (Headquarters)
Hitachi High-Tech Solutions Corporation (Solution Center)
Hitachi ICT Business Services, Ltd. (Media Solution Department Media Service Group)
Hitachi Information Engineering, Ltd.
Hitachi KE Systems, Ltd. (Tokyo Development Center)
Hitachi Kokusai Electric Inc. (Tokyo Works)
Hitachi Management Partner Corp.
Hitachi-Omron Terminal Solutions, Corp
Hitachi Pharma Evolutions, Ltd.
Hitachi Power Solutions Co., Ltd. (Customer Service Department, SRC Group and Remote Monitor Group)
Hitachi SC, Ltd. (Headquarters)
Hitachi Social Information Services, Ltd.
Hitachi Solutions Create, Ltd. (Developing and building systems for government offices, and maintaining services)
Hitachi Solutions West Japan, Ltd. (Environment building and operation management of a SaaS salary support system)
Hitachi Solutions, Ltd. (Security Diagnosis Division)
Hitachi Systems Power Services, Ltd. (Managed Services Division, Data Center Systems Support Department, Third System Support Group)
Hitachi Systems, Ltd. (Contact Center & Business Services Division)
Hitachi Systems, Ltd. (Financial Platform Division Service Office Cloud Computing Service Department)
Hitachi Systems, Ltd. (Public Platform Division)
Hitachi Systems, Ltd. (Public & Social Business Group)
Hitachi Systems, Ltd. (SHIELD Security Center)
Hitachi Systems, Ltd. (Smartsourcing and Services Division)
Kyushu Hitachi Systems, Ltd. (Application Division)
Japan Space Imaging Corporation
Hokkaido Hitachi Systems, Ltd. (Public & Social Systems Management Division/Private Sector Systems Management Division)
HYS Engineering Service Inc. (Service Management Division)
Shikoku Hitachi Systems, Ltd.
Okinawa Hitachi Network Systems, Ltd.

IT Security Certification

The following main products have been certified by the "IT Security Evaluation and Certification Scheme" , which is based on the ISO/IEC 15408 (Common Criteria). This scheme is operated by the Information-technology Promotion Agency, Japan (IPA). (As of the end of June 2018. This includes listing the product on the certified product archive list.)

Product	TOE Category*1	Certification number	Evaluation Assurance Level*2
HiRDB/Parallel Server Version 8 08-04	Database Management System	C0225	EAL4+ALC_FLR.1
HiRDB/Single Server Version 8 08-04	Database Management System	C0216	EAL4+ALC_FLR.1
HiRDB Server Version 9 (Linux edition) 09-01	Database Management System	C0351	EAL2+ALC_FLR.2
Smart Folder PKI MULTOS application 03-06	Smart card application software	C0014	EAL4
Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software 8.0.1-02	Access Control Device and Systems	C0536	EAL2+ALC_FLR.1
Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program 80-01-25-00/00(R8-01A-06_Z)	Control Program for storage system	C0514	EAL2+ALC_FLR.1
Hitachi Unified Storage VM Control Program 73-03-09-00/00(H7-03-10_Z)	Control Program for storage system	C0513	EAL2+ALC_FLR.1
Hitachi Unified Storage 110 Microprogram 0917/A	Storage device control software	C0421	EAL2
Hitachi Unified Storage 130 Microprogram 0917/A	Storage device control software	C0420	EAL2
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	Biometric equipment	C0332	EAL2
Certificate validation server 03-00	PKI	C0135	EAL2
CBT Engine 01-00	Major application for CBT assessment system	C0288	EAL1+ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
Security Threat Exclusion System SHIELD/ExLink-IA 1.0	Security management software	C0090	EAL1

Encryption module testing and certification

The following shows the main products certified by the Japan Cryptographic Module Validation Program (JCMVP), which is based on ISO/IEC 19790 and is operated by IPA, or certified by the Cryptographic Module Validation Program (CMVP), which is based on FIPS140-2 and is operated by NIST in the US and CSE in Canada (as of the end of June 2018).

Cryptographic Module	Certification number	Level
Hitachi Virtual Storage Platform (VSP) Encryption Adapter	CMVP #2727	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board	CMVP #2694	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	CMVP #2462	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Engine	CMVP #2386	Level 1
Hitachi Unified Storage Encryption Module	CMVP #2232	Level 1
HIBUN Cryptographic Module for User-Mode 1.0 Rev.2	JCMVP #J0015, CMVP #1696	Level 1
HIBUN Cryptographic Module for Kernel-Mode 1.0 Rev.2	JCMVP #J0016, CMVP #1697	Level 1
HIBUN Cryptographic Module for Pre-boot 1.0 Rev.2	JCMVP #J0017, CMVP #1698	Level 1
Keymate/Crypto JCMVP Library (Solaris and Windows versions)	JCMVP #J0007	Level 1
Keymate/Crypto JCMVP Library	JCMVP #J0005	Level 1

*1 TOE (Target of Evaluation):
A software or hardware product to be evaluated is called a TOE (Target of Evaluation). These may include related administrator and user guides (user manuals, guidance, and installation procedure documents).

*2 EAL (Evaluation Assurance Level):
ISO/IEC 15408 defines seven evaluation assurance levels (from EAL1 to 7) for the specified evaluation items (assurance requirements). As the level goes up, evaluation becomes stricter.
- EAL1 objectively evaluates the validity and testing of security functions and also the guidance for maintaining security.
- EAL2 adds vulnerability analysis assuming general attack capabilities and evaluation from manufacturing to the start of operations, from the viewpoint of product integrity. EAL2 adds a security-related viewpoint to the typical development life cycle.
- In addition to the assurance obtained in EAL2, EAL3 also evaluates the comprehensibility of testing and the development environment in order to prevent tampering of a product during development.
- EAL4 is the highest level for ordinary commercial products. It evaluates the whole development life cycle, including the integrity of the development assets in the development environment and the reliability of source code and staff.
- ALC_FLR.1 objectively evaluates the basic procedure for providing a required patch when a security defect is discovered in a product. The standard allows the addition of assurance requirements that are not included in a specified EAL. In such a case, the level is indicated in a form like EAL2+ALC_FLR.1.
ALC_FLR.2 requires that vulnerability information can be received from users and requires a procedure for notifying users.

Hitachi Group Overview

Company Profile (As of March 31, 2018)

Corporate name: Hitachi, Ltd.
Incorporated: February 1, 1920 (founded in 1910)
Head office: 1-6-6 Marunouchi, Chiyoda-ku, Tokyo 100-8280, Japan
Representative: Toshiaki Higashihara
Representative Executive Officer, President, and CEO

Capital: 458.79 billion yen
Number of employees: 34,925 (unconsolidated basis)
307,275 (consolidated basis)
Number of consolidated subsidiaries: 879
(Japan: 202, outside of Japan: 677)
(Including variable interest entities)
Number of equity-method affiliates: 407

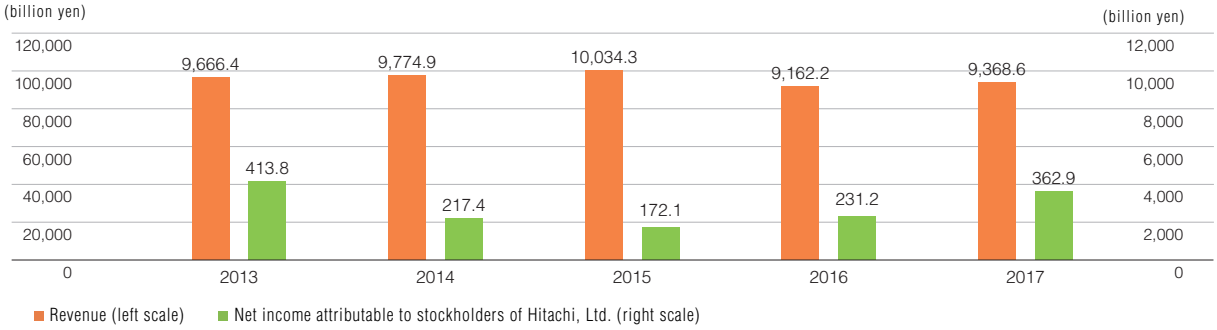
Consolidated Financial Highlights for Fiscal 2017, Based on the International Financial Reporting Standards (IFRS) (Consolidated for fiscal 2018, based on IFRS)

Revenues: 9,368.6 billion yen (up 2%, year on year)
EBIT*1: 644.2 billion yen (up 36%)
Income from continuing operations, before income taxes: 638.6 billion yen (up 36%)

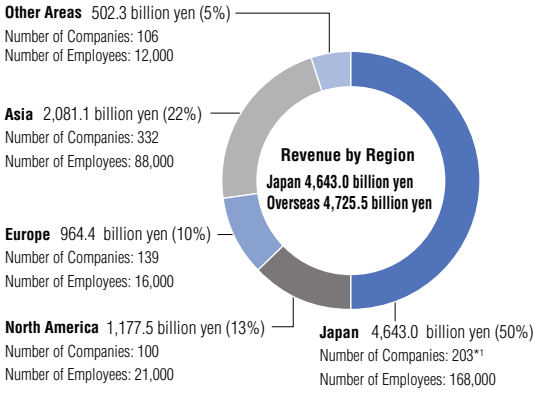
Capital expenditure*2: 374.9 billion yen (down 1%)
R&D expenditure: 332.9 billion yen (up 3%)
Total assets: 10,106.6 billion yen

*1 EBIT: Income from continuing operations before income tax, less interest income, plus interest charges.
*2 Since fiscal 2015, the amount of investment in leased assets that fall under the heading of finance and leases included in conventional capital expenditure are deducted from capital expenditure for disclosure.
Note: Hitachi's consolidated financial statement is prepared based on the International Financial Reporting Standards (IFRS).

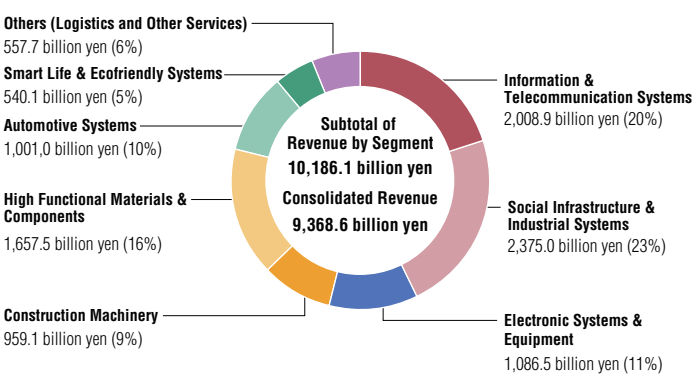
●Revenue and net income attributable to stockholders of Hitachi, Ltd.



●Revenues and ratio by region
(Consolidated for fiscal 2018, based on IFRS)



●Revenue and Ratio by Segment
(Consolidated for fiscal 2018, based on IFRS)



*1 203 companies, including Hitachi, Ltd., and 202 consolidated subsidiaries in Japan

Hitachi, Ltd.
Information Security Risk Management Division
1-6-6 Marunouchi, Chiyoda-ku, Tokyo 100-8280
Tel: 03-3258-1111

Printed in Japan (H) (2019.02)