HITACHI

Information Security Report 2025

Hitachi Group

INDEX

Summary of this report:

- Scope and time period covered by this report: Hitachi Group information security initiatives up to and including FY 2024
- Report publication date: December 2025

CD&SO Message

Vice President and Executive Officer,
Chief Digital and Security Officer (CD & SO)
Michael Goodman

Building a Safer Future: Hitachi Strengthens Focus on Cybersecurity for a Harmonized Society

At Hitachi, we recognize our profound responsibility in supporting the critical infrastructure that powers and protects society every day. As a trusted partner to governments, industries, and communities around the world, our technologies are deeply integrated into systems essential to people's lives – from transportation and energy to healthcare and finance. This critical role compels us to always place the utmost importance on safety and resilience.

In April 2025, Hitachi announced a new management plan, "Inspire 2027", which aims to contribute to a "harmonized society" – where the environment, well-being, and economic growth coexist in harmony. Importantly, this vision places digital at the core of our efforts, recognizing the growing importance of innovation and connectivity in building a better future.

In today's increasingly digital world, cybersecurity is at the heart of these commitments. It is no longer simply a technical challenge, but a core pillar of safety and resilience. The landscape of digital threats continues to evolve, and with it, the potential impacts on organizations and individuals have grown in both complexity and scale. We acknowledge that safeguarding our systems and those of our partners and customers is not only a business imperative but a fundamental societal responsibility.

Hitachi views cybersecurity as a top enterprise risk and a critical management issue. We are resolutely committed to protecting our operations, solutions, and the communities we serve – now and into the future. To strengthen this commitment, as the newly appointed Chief Digital and Security Officer, I am leading efforts to advance our cybersecurity capabilities – integrating cutting-edge technologies and global expertise so our defenses are robust, adaptive, and responsive to emerging risks across all regions and industries we serve.

Our holistic cybersecurity strategy builds upon our longstanding culture of safety and innovation. We have adopted an increasingly ambitious management direction, reinforcing robust governance and accelerating the integration of advanced cybersecurity measures across all levels of the organization. These efforts do not mark a departure from our strong foundation, but rather an ongoing evolution – ensuring we stay ahead of emerging risks and ever-changing requirements.

As we move forward, Hitachi will continue to invest in technologies, talent, and partnerships that fortify the resilience of the world's most vital systems. Together with our stakeholders, we aim to foster a society that is not only more connected but also more secure and harmonious.

We thank our stakeholders for their trust, and reaffirm our unwavering dedication to building a safer, more prosperous future for all.

Hitachi's Approach to Information Security

While the rapid progress of digitalization is generating new value, the business environment is changing daily due to the complex global political and economic situation. Meanwhile, cyberattacks are becoming more advanced and sophisticated day by day, increasing the risk of information leaks and system stoppages that could disrupt the continuity of the business itself. Minimizing that risk through risk management around information security* is one of a company's important management tasks.

Given that background, Hitachi is working on various information security measures, including cybersecurity and data protection, to address both value creation and risk management aspects.

* The term "information security" as used in this report includes personal information protection unless otherwise indicated.

Information Security as a Management Strategy

Hitachi understands and analyzes the ever changing business environment, and based on social issues, our competitive advantages, and management resources, we implement risk management from the perspective of responding to risks that we should prepare for as well as opportunities for further growth. This approach creates earning opportunities while controlling risks.

Cyberattacks, which are becoming more sophisticated and intricate every day, are not limited to traditional internal IT*1 systems. They have expanded to target OT*2 areas, such as production and manufacturing environments, development environments, products and services provided to customers, and supply chains.

As a result, the probability of attacks in any part of the world is increasing, and the impact of such attacks on business continuity, through incidents such as information leaks and system stoppages, is immeasurable.

In addition, countries and regions are strengthening laws and regulations related to security and data protection, and Cyberattacks are increasing the risks in terms of corporate compliance in the event of an information breach.

"Inspire 2027," Hitachi's new management plan formulated in 2025, sets a goal for information security of "maintaining and improving the Hitachi Group's information security," taking into account global trends and legislative moves concerning security. To achieve this goal, we monitor our "Cybersecurity Score," based on the guidelines provided by Japan's Ministry of Economy, Trade and Industry for managing cybersecurity. We also conduct self-assessments that track the progress of Hitachi, Ltd.'s Information Security Risk Management Division (ISRD) which is responsible for information security across the entire Hitachi Group and is implementing appropriate security measures. We will take action based on the assessment results.

*1 Information Technology *2 Operational Technology

Hitachi's Information Security Vision

Hitachi is now promoting various efforts to improve cyber resilience, based on the three approaches of internal controls as "Governance", collaborative creation as "Co-creating Security," and ownership as "Jibungoto." (Figure 1-①)

Figure 1-① Hitachi's Information Security Vision

Governance	Continue and steadily implement security measures that have positioned cyber security as a management issues. There is no such an absolute security, thus we must build resilience to enable capability of recovery quickly in the case of emergency-state. (for securing business continuity)
Co-Creating Security	To protect us against the evolving and increasing cyberattacks, expanding internal communication and building security ecosystem together across the entire society.
Jibungoto	Each employee acquire correct understanding of security and empathize the importance, and foster the mindset, Jibungoto, to take an action as own matter.

Improve the security resilience → **Acquire adaptability / flexibility and cyber resistance**

■ Governance: Zero Trust Security Initiatives

Learning from the damage caused by the WannaCry ransomware in 2017, Hitachi has expanded the scope of its countermeasures beyond internal IT to the OT area, and is continuously and steadily strengthening operational, technical, and organizational countermeasures, focusing on strengthening security and cyber BCP* in products, services, and the supply chain.

In addition, we are working on zero-trust security measures based on cloud-based IT architecture, aiming to provide optimal security in light of the shift to cloud-based business systems and changes in working styles due to remote working. For implementation, we consider "authentication," "endpoint," and "cyber-integrated monitoring" to be key elements in achieving zero-trust security, and we are working to enhance our attack-detection capabilities.

* Business Continuity Plan

■ Co-creating Security: Initiatives for Building a Security Ecosystem

Responses to security incidents require the cooperation of all departments, including public relations, human resources and labor affairs, and legal affairs, not just the IT department. As the range of matters addressed by security measures broadens, the Monozukuri Group, Quality Assurance Department, Procurement Department, and other departments must also collaborate well to ensure full functionality. Hitachi sees this kind of security ecosystem as vitally important and is working to build it.

Our approach is that the elements of this ecosystem structure: "things," "people and organizations," and "society" must be connected.

DX*1 requires an environment in which things like devices and systems, exemplified by IoT*2, are connected. To maintain security in a world where "connections are being made between things that until now were unconnected," we are building "a system of connected people and organizations to promote countermeasures in which different organizations" work together to promote security measures.

Furthermore, connections should not be limited to within Hitachi; it is becoming essential to form a community that transcends boundaries, such as sharing threat information and issues that arise when implementing countermeasures with companies, government agencies, and educational institutions that are working on cybersecurity measures. Hitachi invites each enterprise and organization to feed back the knowledge it gains from the community into its own security measures, creating further "connections in society." (Figure 1-②)

*1 Digital Transformation　*2 Internet of Things

■ Jibungoto: Security Awareness-raising Initiatives

We presume that vulnerabilities in security awareness will be targeted, as it has become commonplace for employees to work from home over the past few years. When working outside the office with nobody around to act as a voice of reason, risk is ever present.

This means that improving each employee's security awareness will be the last defense. In addition to our existing strict governance, we have started activities to raise security awareness by encouraging employees to take the initiative and act independently. This does not mean making security feel like an obligation. Rather, our goal is to get employees interested in the issues, have them share our commitment from the heart, and take ownership of security. (Figure 1-③)

Figure 1-② Illustration of the security ecosystem

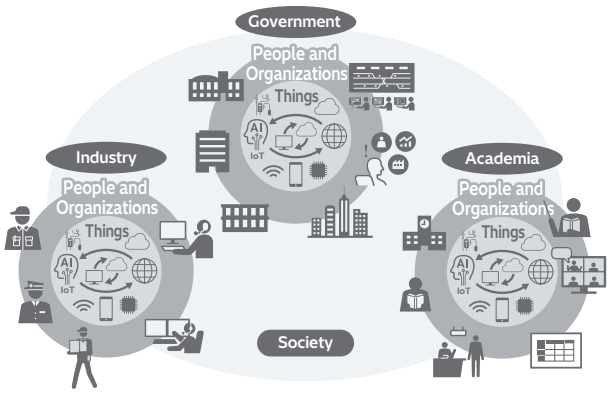
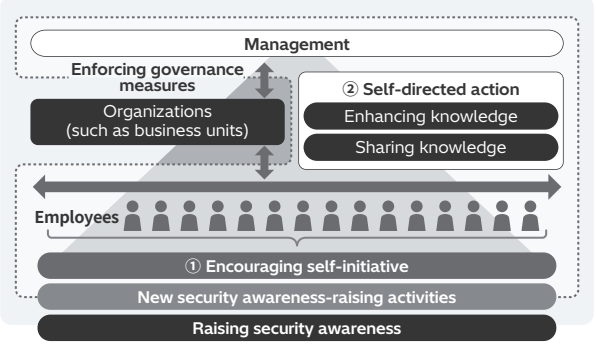


Figure 1-③ The ideal future form of security awareness

The important thing is to elevate the security awareness of each and every person

Key concepts: "Jibungoto (Ownership)" and empathy



Hitachi's Approach to Information Security

Information Security Scope

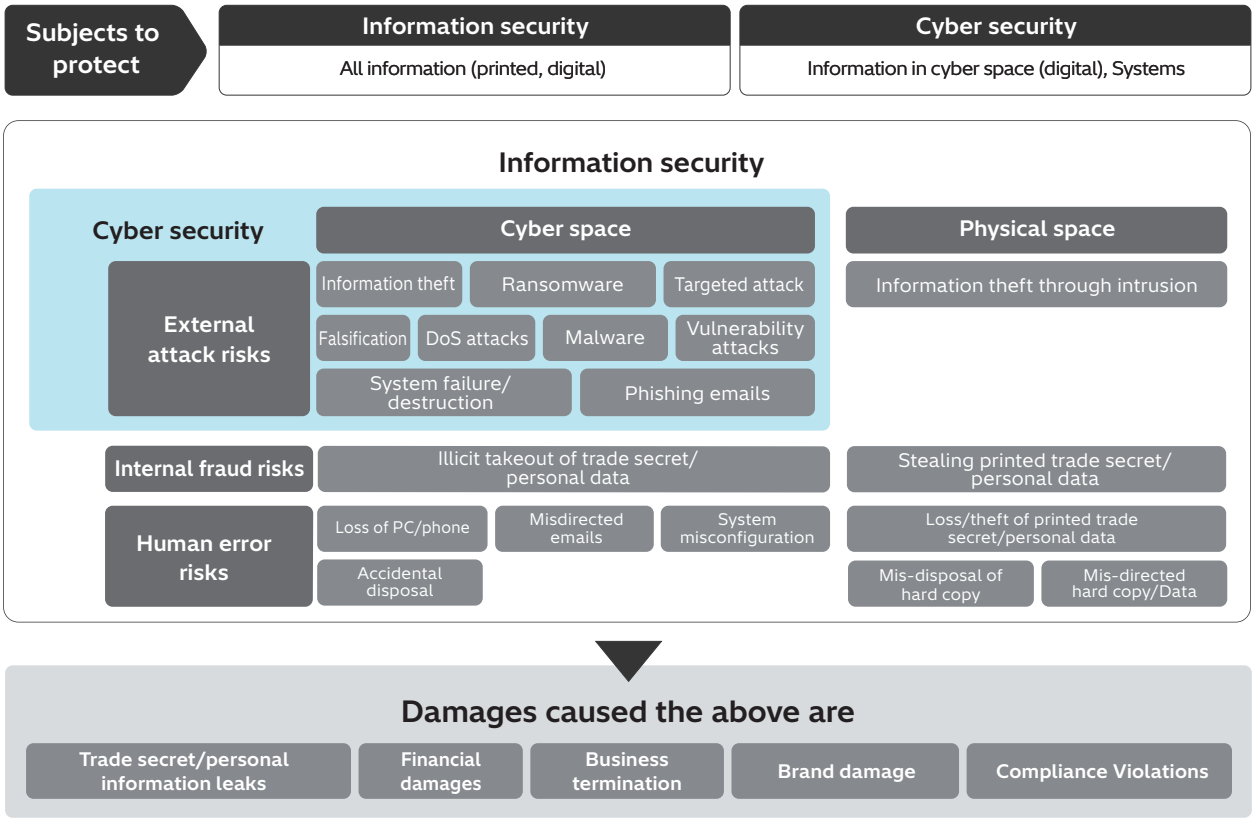
As shown in Figure 1-④, the targets to be protected to maintain information security are known as information assets. Hitachi believes that these targets must maintain their "CIA": confidentiality, integrity, and availability.

The Scope of Information Security

The term "Information" includes not only data in cyberspace, but also paper and physical media in physical space, which should also be protected as information security.

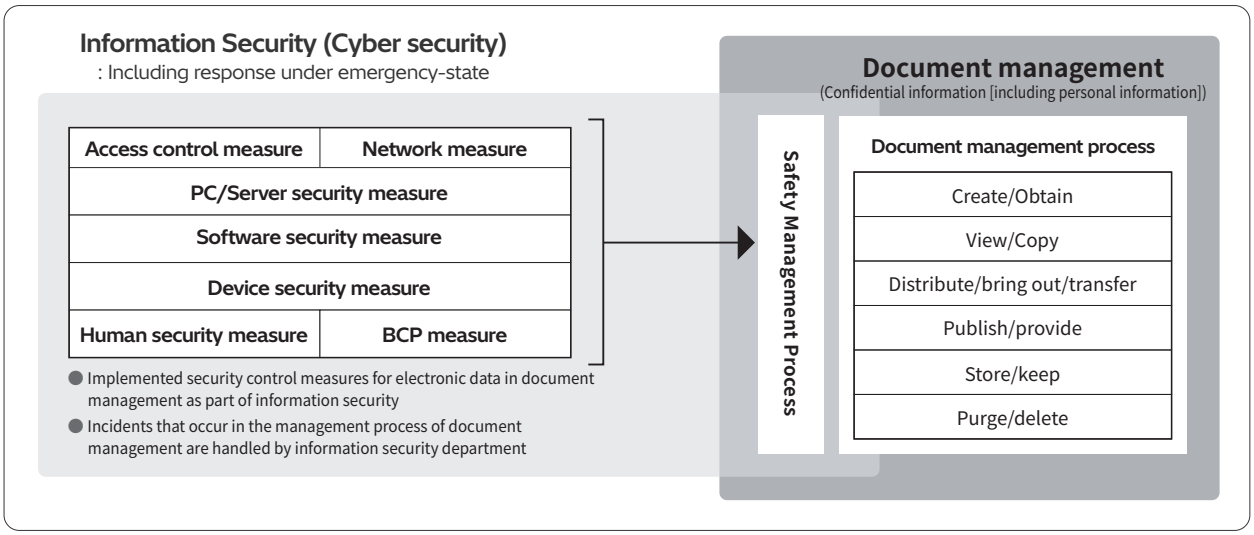
Hitachi formulates information security measures and strategies from a risk management perspective, anticipating the damage that could occur when risks materialize such as information leaks, economic losses, difficulties in business continuity, brand damage, and compliance violations and identifying the root causes of these risks, including external attacks, internal misconduct, and human error.

Figure 1-④ Scope to be protected as information security



In planning information security strategies and measures, we recognize the document management process, from creation and acquisition to disposal and deletion of information, as a target for information security maintenance measures, as shown in Figure 1-⑤. This approach is based on the perspectives of confidential information management as well as cybersecurity.

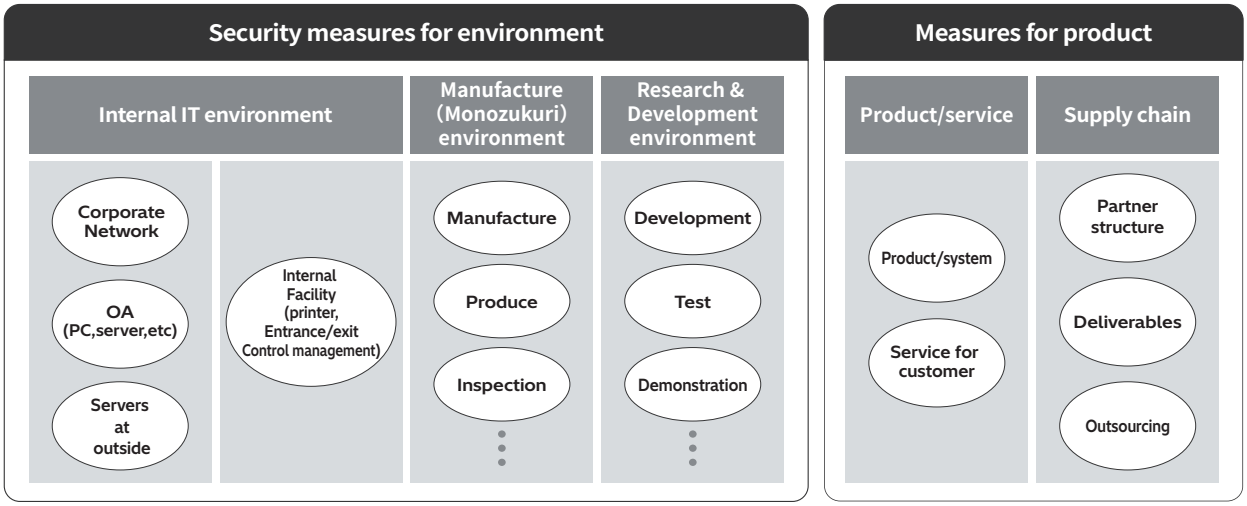
Figure 1-⑤ Current management scope of information security department



Scope of Governance

The scope of governance required to maintain information security was redefined in 2018 in response to the damage caused by the WannaCry ransomware attack in 2017. As shown in Figure 1-⑥, the scope of information security governance covers not only the internal IT environment but also all internal environments, including production and manufacturing environments and development environments, as well as products, services, and supply chains.

Figure 1-⑥ Scope of governance



Hitachi's Approach to Information Security

Information Security Strategy and Key Themes

Hitachi formulates information security strategies and implements measures from the perspectives of both value creation and risk management, based on the status of security incidents and on trends in security and data protection laws and regulations.

The Environment Surrounding Information Security

Recent security incidents are characterized by the diversification of attack methods and the continued expansion of attack surfaces*1. The attackers' method of attacking vulnerabilities in Internet-exposed devices and inadequate management of those devices to steal information or infect them with ransomware and demand a ransom has not changed. We believe that it remains necessary to recognize that inadequate countermeasures and inadequate management, if left unchecked, will always lead to the occurrence of damage.

As for trends in security laws and regulations, in addition to the ongoing movement since FY2023*2 to regulate product services when doing business in the EU, there has been an active movement in Japan to strengthen regulations related to security.

In Japan, in particular, there have been rapid developments since the beginning of FY2024 regarding the Economic Security Promotion Act, active cyber defense, and security clearances. As new bills will be debated and various laws will come into effect in FY2025, we believe it will be necessary to closely monitor the implementation of various laws and regulations.

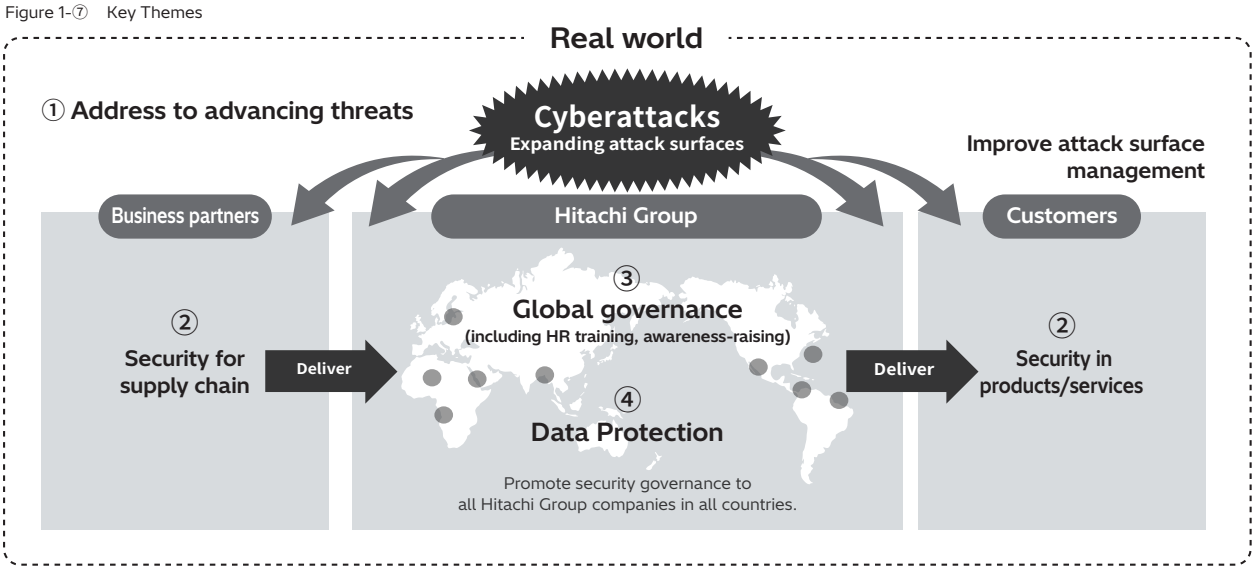
*1 Information assets that may be subject to external attack, such as from the Internet.

*2 The fiscal year or "FY" that Hitachi adopts starts in April and ends in March of the following year.

Key Themes and Activities

In light of the environment surrounding information security, Hitachi has been promoting the following four security strategies as shown in Figure 1-⑦: ① response to increasingly sophisticated threats, ② product service and supply chain security, ③ global governance, and ④ data protection.

Figure 1-⑦ Key Themes



1. Response to Increasingly Sophisticated Threats

In order to achieve a rapid global response, we have been advancing the global use of intelligence information, and enhancing our ability to detect and counter Cyberattacks. We are also making efforts to strengthen information asset management in order to quickly identify the target in the event of an attack. Along with strengthening Attack Surface Management*, we are making progress in rechecking high-risk environments, such as cloud services and Internet-exposed devices, which are increasingly becoming targets of attacks.

* A series of continuous activities that identify, monitor, analyze, and repair information assets that may be subject to external attacks, such as those from the internet.

2. Supply Chain Security for Products and Services

We are building a system to maintain security measures, including the reliable implementation of procedures and rules, based on the concept of three lines of defense*.

In addition, with regard to product and service security, liaison meetings have been held regularly with members of The Product Security Incident Response Team (PSIRT) established in each business unit ("BU") and Group company to share information and resolve respective issues, and to strengthen the functions of each PSIRT.

In the supply chain, we have strengthened communication with procurement partners through briefing sessions and other means, with the aim of raising security awareness.

* For details of the three lines of defense, please refer to "Concept of Cyber Security Enhancement Measures" on page 17.

3. Global Governance Enhancement

Region Branches established as information security divisions under the direct control of the headquarters in five countries and regions outside of Japan, including the Americas, Europe, Asia, India, and China. They have taken the lead in holding information-sharing meetings and seminars for Group companies in each country and region. These meetings and seminars aim to strengthen security management and incident response functions.In addition, we have been providing support for cybersecurity legislation that each BU and Group company will need to comply with, such as the Cyber Resilience Act (CRA), which will be fully in effect in the EU region from December 2027.

4. Data Protection Enhancement

In the field of data protection, we have strengthened the existing Data Protection Unit and promoted integrated management headed by the ISRD. In addition, we have created a playbook that defines data protection processes, and have been developing response processes, including training, knowledge, and thorough practice of these processes. Furthermore, in addition to China's three cybersecurity and data laws, we have been working on various responses to the personal data protection laws of India and Vietnam.

Future Key Initiatives

Hitachi will promote the following measures to further improve the effectiveness of information security risk management and the steady implementation of Cyberattack countermeasures. These efforts, based on global trends and the effective statuses of Hitachi's measures, are intended to reduce the information security risks of the entire Hitachi Group.

1. Improve the Efficacy of Information Security Risk Management

We believe that continuously and steadily managing global information and data security protection is crucial.

The ISRD will monitor the governance status of the Hitachi Group as a whole, and the state of effectiveness of measures at each BU and Group company, while working to improve the management system.

2. Respond to Increasingly Advanced and Sophisticated Cyberattacks

Cyberattacks are steadily increasing, and the nature of the attacks is becoming more advanced and sophisticated. The mixture of indiscriminate and pinpoint attacks is making it more difficult to determine the purpose of attacks. In order to cope with any type of attack, we will continue to sharpen existing measures and respond to new challenges, as well as promoting more sophisticated monitoring and faster incident response.

3. Respond Steadily to Tighter Global Laws and Regulations

In order to cope with the accelerated tightening of laws and regulations in many countries and regions in response to increasingly sophisticated threats, the ISRD will promote the development of a system to collect and disseminate information to the Hitachi Group and to implement specific measures.

Information Security Management

As one of Japan's leading global companies, Hitachi has established an information security management system to protect a variety of information assets, including information entrusted to us by our customers and the systems that store that information, and is working on stronger information security management.

Information Security Management Systems

Hitachi has established policies for information security and personal information protection and has built a system for promoting these policies in Japan and globally. We are working to develop various rules, while training employees, and monitoring and auditing to ensure that various measures are properly implemented.

Information Security Policy

Hitachi makes every effort to ensure information security by defining a security policy incorporating the wider management policy of the enterprise.

(1) Formulation and continuous improvement of information security control rules

Out of its recognition that the effort to maintain information security is one of the key tasks in its scheme of management and operations, the Hitachi Group shall formulate information security management regulations compliant with and adhering relevant laws and regulations and other codes of conduct. Further, it shall put in place a Company-wide information security management system having the executives at its center, and steadily implement such system. In addition, it shall maintain and continuously improve the security of organizational, human, physical and technological information.

(2) Protection of information assets and their continuous control

The Hitachi Group shall devise secure control measures to protect in appropriate ways the information assets that it handles from threats to the confidentiality, integrity and availability of the information assets. It shall also devise appropriate controlling measures to continue its businesses.

(3) Adherence to laws, regulations and other norms

The Hitachi Group shall adhere to laws, regulations and other norms relating to information security. Further, the Hitachi Group's information security control rules shall be formulated to conform to such laws, regulations, and other norms. The Hitachi Group shall also impose appropriate punishment in accordance with the Employee Work Provisions in the case of any offense to them.

(4) Education and training

The Hitachi Group shall raise the awareness of executives and employees for information security, and carry out education and training in information security.

(5) Prevention of accidents and action in the case of their occurrence

The Hitachi Group shall work to prevent information security breaches, and shall promptly take appropriate action, including recurrence prevention measures, in the event that such accidents occur.

(6) Securing proper operation in corporate group

The Hitachi Group shall work to create a system to secure proper operation in corporate groups consisting of the Hitachi Group's companies in accordance with Article 1 through 5 in this article.

Personal Information Protection Policy

Hitachi has established personal information protection policies and is committed to protecting personal information. For details of the personal information protection policies, please refer to "Personal Information Protection Policy" on page 29.

Promotion Framework for Information Security and Personal Information Protection

■ Information security promotion framework

At Hitachi, the ISRD provides governance for the entire group. Governance is instituted by a way of instructions passed down through lines of control to each Hitachi, Ltd. BU and business site and to each Group company. Governance of the Hitachi Group as a whole is achieved by each BU and Group company applying the same controls to their own group companies (subsidiaries) as they do to themselves. This framework applies not only within Japan but also overseas locations.

The company president of Hitachi, Ltd. (President & CEO) appoints the Chief information Security Officer (CISO) who has authority and responsibility to decide on information security policies and implement measures for the entire Hitachi Group in relation to information security, and the Information Security Audit Manager who has authority and responsibility in relation to Personal Information Protection and Information Security Audits.

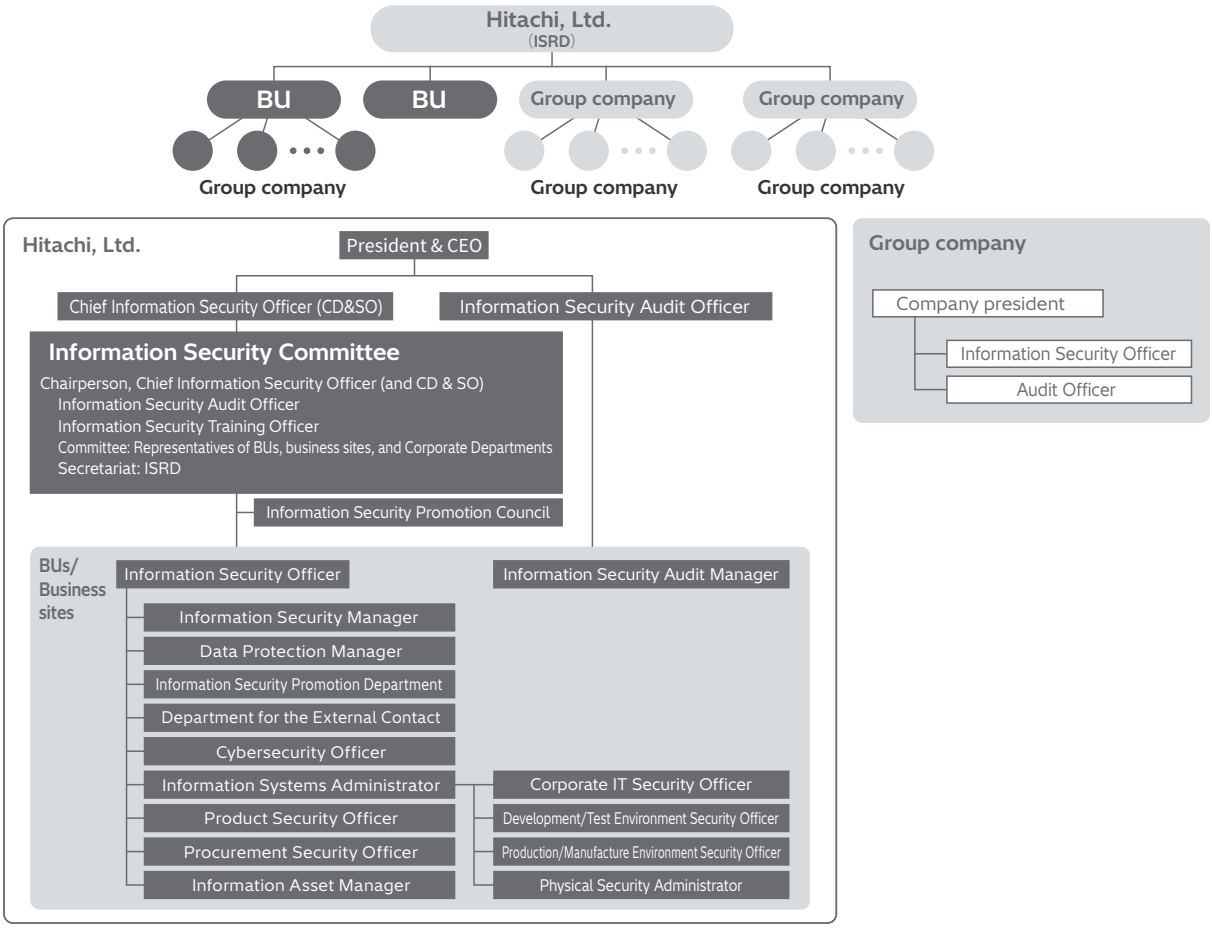
The CISO establishes the Information Security Committee which guides policy regarding information security, personal information protection policies, training plans, and various measures.

The matters decided by the Information Security Committee are disseminated to each organization through the Information Security Promotion Council attended by representatives of all BUs and business sites.

In principle, the head of the BU and business sites manager serves as the Information Security Officer of the BU and business sites. The Officer appoints an Information Security Manager and a Data Protection Manager. With the support and supervision of the Officer, they manage and control information security and personal information protection. In addition, as the scope of cyberattacks is expanding, we have appointed a person responsible for each physical security environment, including the internal IT environment, development and testing environment, production and manufacturing environment, and office access, under the supervision of the Information System Administrator. In addition, to strengthen the security of the supply chain, including products and services provided to customers and suppliers, we have also established the Product Security Officer and a Procurement Security Officer. We will establish a department to promote information security. This department will protect personal information, manage information security, and oversee confidential information, access control, and outsourced vendors for each organization. It will also provide training for employees. The Information Asset Manager is placed in all divisions, who has responsibilities regarding the handling of information assets including personal information.

Similar organizations are established in Group companies to promote information security through cooperation. (Figure 2-①)

Figure 2-① Information security promotion framework



Information Security Management

Information Security and Global Promotion Framework

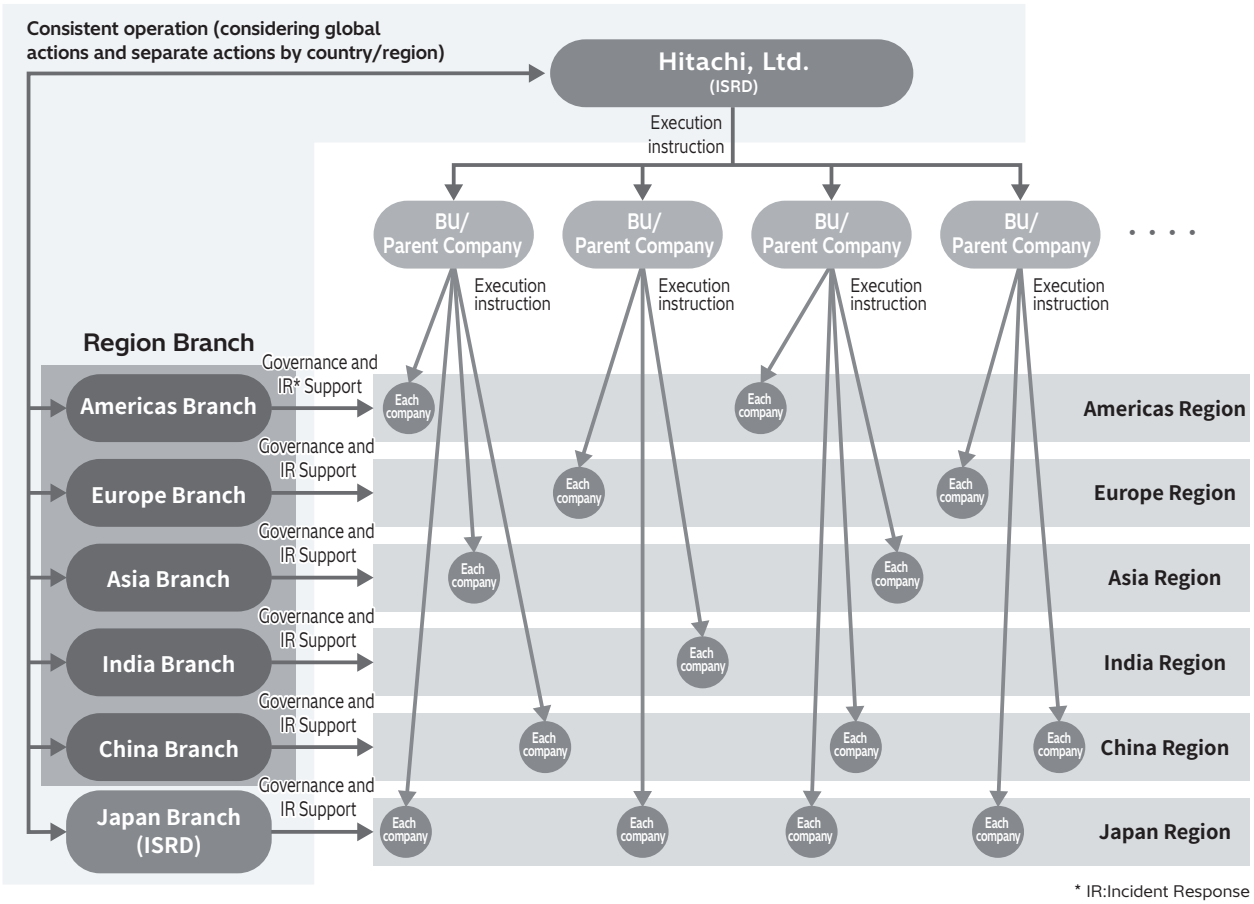
As global business expands, Hitachi is working to strengthen global governance by newly establishing information security departments (Region Branches) in each region to ensure the reliable implementation of security measures.

According to Hitachi's governance lines for information security, the ISRD provides policies, measures, and instructions to BUs and Group companies. These companies then direct their overseas subsidiaries under their respective jurisdictions to implement the policies.

Under the concept of “Security One Team,” we have established Region Branches that cover the Americas, Europe, Asia, India, and China. These branches allow us to respond promptly to incidents and comply with changing regional laws. Our goal is to further embed governance globally. In addition to the vertical governance line from BUs and parent companies to each subsidiaries, we have a horizontal line of support from the Region Branches to their regional subsidiaries to strengthen security measures on a global basis. In Japan, the ISRD plays the same role for the Japan branch.

A Head of Cybersecurity has been appointed at the Region Branch of each region and country to strengthen communication, incident management, and management oversight, in order to ensure a consistent global response to incidents. (Figure 2-②)

Figure 2-② System for strengthening governance of Region Branches



* IR:Incident Response

Data Protection Promotion System

For data protection, a Data Protection Manager has been appointed at each company in order to promote appropriate legal compliance with the Private Information Protection Law at each regional Group company. In addition, advisor positions for data protection have been established at the regional headquarters in the Americas, Europe, Asia, India, and China to support local Group companies in complying with their local laws and regulations.

Through our information security promotion framework, headed by the CEO, we thoroughly apply our policies on the protection of personal information, and manage personal information appropriately. All Hitachi, Ltd. BUs and business sites appoint an Information Asset Manager under the Information Security Officer for each department. These managers are responsible for handling and protecting personal information. Similar organizations are established in Group companies within Japan, to foster thorough personal information protection and management throughout Hitachi Group.

System of Rules for Information Security and Personal Information Protection

Hitachi has established the rules in the following table based on the Hitachi Group Information Security Policy. (Figure 2-③) Group companies have established similar rules to promote information security.

Basic Rules

"Information Security Management Rules" define the basic matters that must be complied with in relation to the formulation, implementation, maintenance, and ongoing improvement of information security management systems. We promote our cybersecurity measures worldwide according to our "Information Security Standards," which comply with the U.S. government SP 800 standard series.

The "Hitachi Group Privacy Principles," a Code of Conduct for the whole Hitachi Group, was established with reference to the OECD Privacy Guidelines*, which have been adopted as the basic principles for personal information protection legislation in various countries and regions. Furthermore, in our "Personal Information Protection Policy" and "Regulations for Personal Information Management" we have set rules equivalent to the JIS standard (JIS Q 15001) in order to manage personal information at a higher level than the Personal Information Protection Law.

For confidential information management, the handling of confidential information preservation is stipulated in the "Management Regulations for Confidential Information."

* Guidelines adopted by the Organization for Economic Cooperation and Development (OECD) in 1980 that set forth a set of principles for the international distribution of personal data.

Individual Rules

The "Rules on Website Creation and Information Disclosure" define the matters that must be complied with in order to disclose and use information correctly on websites.

The "Rules for the Management of Entry/Exit and Restricted Areas" define measures to maintain physical security, such as rules governing building access.

Figure 2-③ Information Security and Rules related to personal information protection

Category	Name of rules, etc
Basic rules	Information Security Management Rules
	Hitachi Group Information Security Policy
	Information Security Standards
	Hitachi Group Privacy Principles
	Personal Information Protection Policy
	Regulations for Personal Information Management
	Regulations for Confidential Information Management
Individual rules	Rules on website creation and information disclosure
	Rules for the Management of Entry / Exit and Restricted Areas
	Criteria for Consignment of Personal Information Handling

Information Security Management

Management Cycles for Information Security and Personal Information Protection

At Hitachi, we have built a framework to run PDCA (Plan-Do-Check-Action) cycles in our information security management as a whole, including personal information management. This framework defines information security management cycles which run through the stages of "Plan" to establish rules and measures, "Do" to implement measures, "Check" to monitor and assess risks, and "Action" to continue improvements.

For more information on the Personal Information Protection Management Cycle, see page 31.

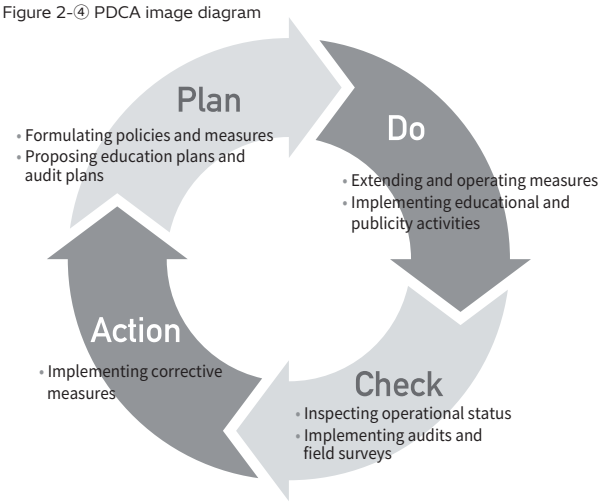
In the "Plan" stage, we set information security policies and measures, plan information security education, and formulate audit plans for personal information protection and information security.

In the "Do" stage, we deploy security measures within the company and operate them. We are working to ensure that all employees fully understand security measures and raise their awareness through information security education and awareness activities.

The "Check" stage includes periodic inspections of security operations, audits in accordance with audit plans, and on-site inspections by security experts.

The "Action" stage takes corrective action based on the results of audits, on-site investigations, etc. (Figure 2-④)

Figure 2-④ PDCA image diagram



Education on Information Security and the Protection of Personal Information

Education on Information Security and the Protection of Personal Information

An organization's ability to maintain information security and protect personal and confidential information depends on its employees understanding the importance of information security and making it part of their personal ethos as they go about their daily tasks.

Hitachi conducts annual training by e-learning of all executives, full-time employees, and temporary employees on the subjects of information security and personal information protection. The training participation rate for Hitachi, Ltd. in the previous fiscal year reached 100% (excluding those on leave or otherwise unable to attend). Hitachi, Ltd. also formulates an annual information security training plan and implements it using a diverse range of education programs tailored to specific subjects and purposes. For example, one program might target a specific group of people like newly hired employees and another those in new managerial positions, while another might offer specialized education to people in roles such as personal information protection manager. (Figure 2-⑤)

Hitachi, Ltd., makes its educational content available to Group companies within and outside Japan, and works towards a deeper understanding of information security and personal information protection of the Hitachi Group as a whole.

Drill-based Training for Spear Phishing Email Attacks

Cyberattacks based on spear phishing emails are a daily occurrence. Every employee must be trained in how to respond appropriately to such an attack.

We are globally implementing training on targeted attack emails for all employees including group companies. These drills involve sending emails that mimic those sent by actual spear phishing attackers, giving employees insight into the nature of such emails and how to respond if they receive one. This practical approach to education enhances the ability of Hitachi employees to respond appropriately in the event of a real attack. At the end of the training, employees are given instructions on how to recognize suspicious emails, which increases the effectiveness of the training.

Figure 2-⑤ Information security training target personnel and content

Category	Target audience	Description
All staff education	• All employees • Temporary employees • Employees on secondment	The importance of personal information protection and confidential information management, and the latest trends in information security.
Tiered education	Newly appointed section managers or equivalent	Knowledge that a manager needs to know about personal information protection, confidential information management, and information security, and Hitachi's initiatives for personal information protection.
	Newly appointed assistant managers or equivalent	Knowledge that an assistant manager needs to know about personal information protection, confidential information management, and information security, and Hitachi's initiatives for personal information protection.
	New employees	Basic knowledge of personal information protection, confidential information management, and information security.
Specialized education	Persons responsible for protecting personal information	Specialized knowledge and practical skills that can be learned from the exercise for a person responsible for protecting personal information, including internal rules, management systems, and procedures for actual operations.
	Information asset managers	Knowledge required for an Information Asset Manager to perform his or her role as a manager of information assets, including personal information, in his or her team.

Management Assessment and Monitoring

We conduct regular audits and on-site assessments to evaluate and monitor whether measures for information security are being implemented appropriately.

Hitachi, Ltd., and all Group companies within Japan conduct an annual audit of their personal information protection and information security status. The audit at Hitachi, Ltd., is carried out by independent auditors appointed by the CEO. To ensure fairness and independence, the audit process is mutual audit.

Personal information protection and information security audits verify compliance with the following items:

- Information security regulations, management of information assets, and conformity of information security measures
- Personal information protection and conformity between JIS Q 15001 and the personal information management system
- Conformity status of personal information protection management system and JIS Q 15001

All Group companies in Japan undergo the same audits as Hitachi, Ltd. and Hitachi, Ltd. confirms the results.

Information Security Management

Information Security Enhancement Initiatives

Hitachi's efforts to strengthen information security management include information asset management during normal times and emergencies, ensuring security during mergers and acquisitions, security personnel training, and activities to strengthen governance at overseas Group companies.

Our Approach and Initiatives for Information Asset Management

We provide appropriate protection and management to ensure that information assets targeted by various threats are not leaked or rendered unusable.

■ Handling in Normal Times

Hitachi believes that in order to protect and manage information assets, it is essential to be aware of what information exists in which systems. Therefore, we manage information assets in accordance with various information security-related rules, such as the procedures for managing confidential information. The Information System Administrator of each BU or business sites compiles a list of information systems. By integrating Attack Surface Management, we oversee all information systems intended for internet publication. The list of information systems is for managing information such as Internet connections and Cloud utilization, in addition to the administrator information of the relevant information system, and is used for operational management. Additionally, each information asset manager regularly inspects the information assets stored in each information system. This allows them to understand what information is stored, including whether customer or personal information is held in the system.

■ Response to Emergencies

In the course of managing and operating information systems, these systems may be compromised by unauthorized access or other means. In such cases, it is important to quickly identify information assets and confirm the scope of the breach and the impact of the incident. Hitachi's thorough daily management of information assets enables us to identify particular information assets, resulting in a prompt response to incidents.

Initiatives to Ensure Security During Mergers and Acquisitions

Hitachi is working to strengthen information security governance in companies that newly joined the Hitachi Group, to minimize the security risks that arise as we actively pursue mergers and acquisitions (M&A).

M&A creates new value by integrating companies with different corporate cultures. On the other hand, we must minimize the information security risks that occur as we integrate policies and systems. Early in the M&A process, we ask the target company to understand and comply with Hitachi's rules. This enables us to uphold controls and governance based on Hitachi policies.

Our security risk assessment during the M&A process is divided into two phases: one before the contract is signed and one after. (Figure 2-⑥)

① Before signing a contract (Day 0): "Information Security Risk Assessment"

We analyze the information security status of companies undergoing M&As based on published information and information provided to us in advance. This analysis covers the following aspects of their information security status: internal organization, systems, and rules; business characteristics; compliance with local legal systems; history of cybersecurity incidents; and responses to those incidents.

② After signing a contract (Day 0): Security Assessment

We select the sites to be assessed, with consideration of the situation and business characteristics of the country or region in which the acquired company operates, and then ask the company to conduct a self-assessment using the risk assessment items of the Hitachi Rules. Based on the results, an ISRD member will visit the target company to confirm its on-site status. Lastly, if any noncompliance issues remain, we will create a corrective action plan to help the target company resolve all issues.

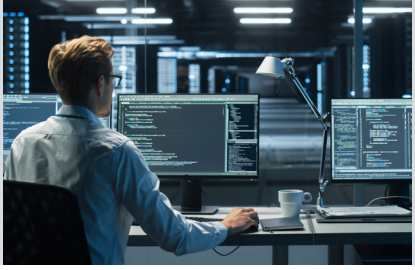
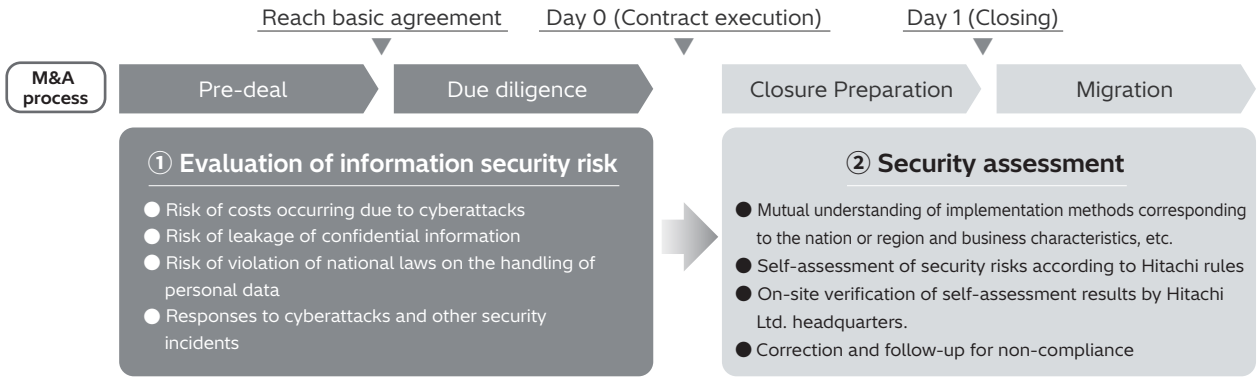


Figure 2-⑥ Information security risk assessment and security assessment



Approach and Initiatives for Security Human Resource Development

In response to the recent intensification of cyberattacks, Hitachi is promoting the development of security personnel throughout the Group in order to strengthen internal security and ensure appropriate security measures for products and services provided to customers.

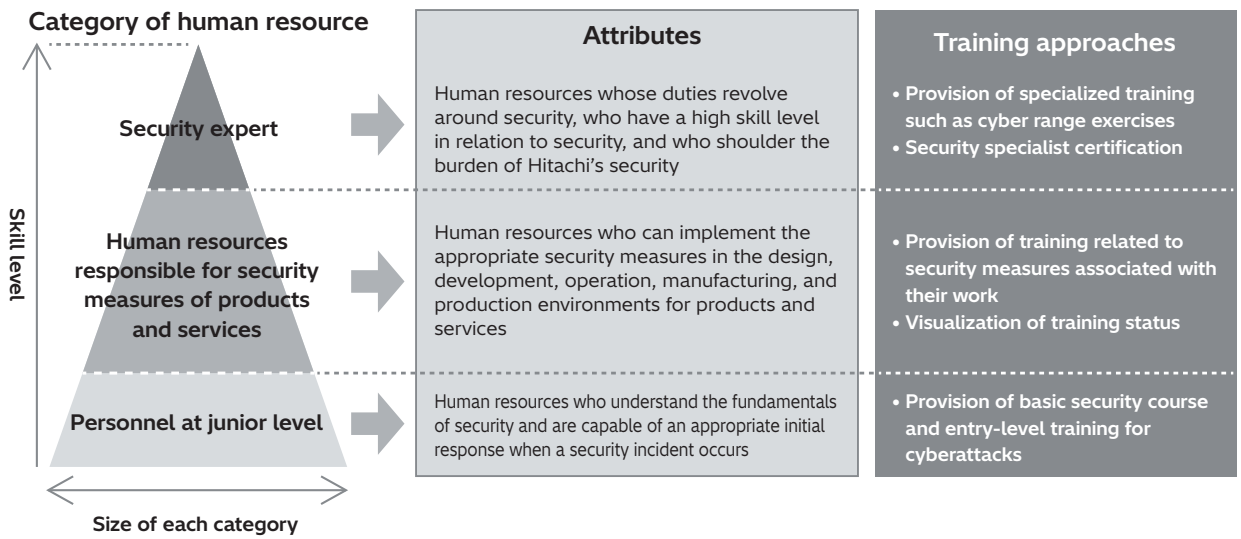
Our Approach to Security Human-Resources Education

As shown in Figure 2-⑦, Hitachi classifies security personnel development into three categories: security expert, personnel responsible for security measures for products and services, and basic personnel. We have developed training programs tailored to these personnel categories and are effectively promoting human resource development in accordance with their respective objectives.

Security Expert

The approach for security experts includes training in advanced techniques, such as cyber range exercises, as well as providing community websites that support information sharing and collaboration. We have the Hitachi Certified IT Professional certification, which conforms to the Certified IT Professional certification framework of the Information Processing Society of Japan. This certification framework identifies, trains, and evaluates candidates with the necessary security skills and backgrounds to earn certification as a Hitachi Certified Information Security Specialist (HISSP) Security Expert.

Figure 2-⑦ Three security HR categories and training measures



Information Security Management

Human Resources Responsible for Security Measures of products and Services

Human resources responsible for security measures in products and services are those who promote the necessary security measures as part of their work in providing the products or services. What's needed first is for these individuals to be responsible for carrying out appropriate security measures in the design, development, operation, and maintenance of products and services, as well as in the preparation of the environment in which these activities take place.

Also important is the development of security human resources focused on production and manufacturing. These human resources are provided with training to promote an understanding of security measures in accordance with company rules. We must establish and maintain environments for the design and development of products and services, as well as for production and manufacturing so that they are secure and do not interfere with each other. To this end, Hitachi is working to increase its employees' knowledge of IT and OT security measures. We also train PSIRT members, security risk assessors, and security system architects, all of whom are responsible for enhancing the security of our products and services.

Personnel With Basic Security Knowledge

We provide entry-level security training to employees to raise security awareness throughout the company and strengthen our security measures. The curriculum includes the basic knowledge of security and the necessary skills for an initial response to security incidents resulting from cyberattacks.

We provide the "Basic Knowledge e-learning Program for Cybersecurity Countermeasures" and the "Communication Training for Cybersecurity Response" are available. For the trainees who require further introductory training, e-Learning programs on basic security knowledge are available.

Global Governance Enhancement Activities

Region Branches hold security conferences and workshops for security managers and personnel from Hitachi Group companies in their region, to raise their understanding of Hitachi's overall strategy and initiatives, and to support the implementation of specific security measures. Through these activities, we aim to build local communities and activate communication across regions. We widely distribute security newsletters to raise awareness and promote security consciousness.

To strengthen incident management, we regularly share intelligence and incident information to enhance resilience in emergencies. We also promote emergency response support to minimize risks by coordinating with relevant parties.

Through these activities, the Region Branches promote the steady implementation of basic measures on a global basis. (Figure 2-⑧)

Figure 2-⑧ Main activities of Region Branches

Main Activities of Regional Branches
Support for a deeper understanding of Hitachi's overall strategy and initiatives by holding security conferences
Support for the implementation of specific security measures through workshops on individual themes.
Establish regional security communities and activate cross-regional communications
Foster security awareness through security newsletters, etc.
Promote security awareness activities conscious of taking ownership ("Jibungotoka")
Attend external conferences to gain insight into the latest trends
Share intelligence and incident information to strengthen resilience in emergencies
Promote support for incident response (IR) in cooperation with related departments during emergencies

Cybersecurity Initiatives

With the diversification of cyberattack techniques, the sources and impacts of incidents are expanding. To address these risks, Hitachi is engaged in environment-specific cybersecurity management, cybersecurity measures against cyberattacks and various incidents, and CSIRT (Cyber Security Incident Readiness /Response Team) activities to support countermeasure activities. Hitachi works on activities called the Cyber Security Incident Readiness /Response Team (CSIRT). Through this initiative, we implement environment-specific cybersecurity management and countermeasures against cyberattacks and other incidents. We also support Hitachi Group members in their related efforts.

Cybersecurity Management

Hitachi's scope of security risk management focused on internal IT environments in an OA context. We are expanding our scope to include the development, verification, production, manufacturing, supply chains, and development processes of products and services. This will ultimately reduce business risk.

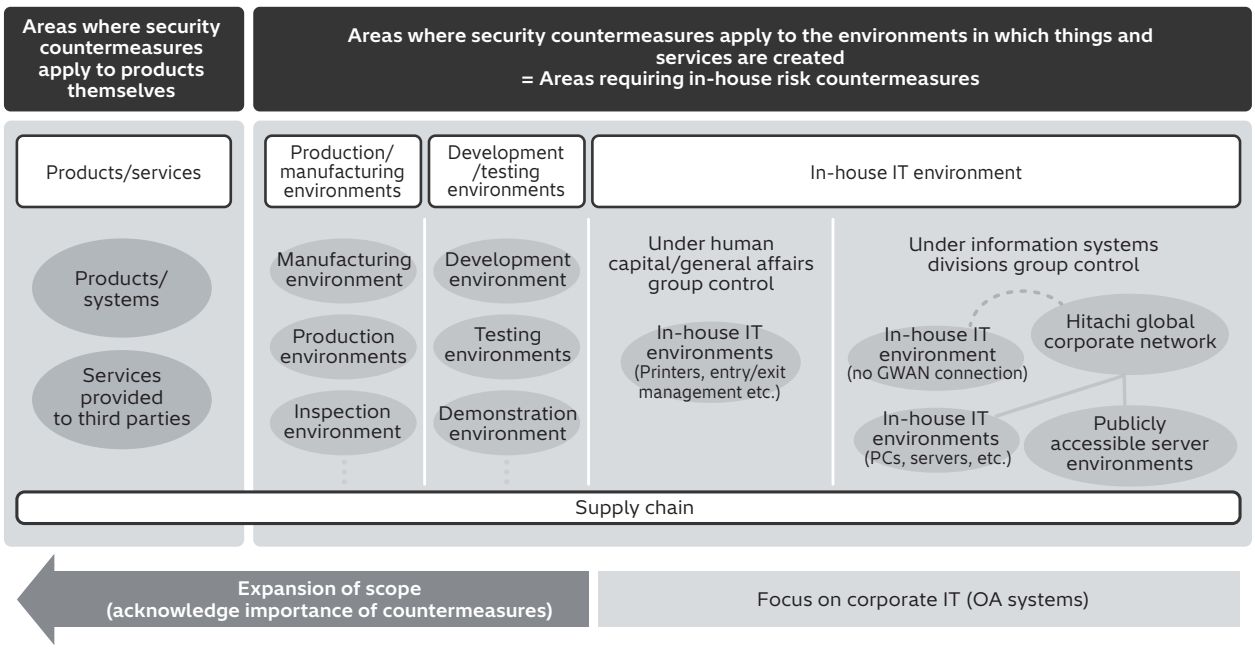
Approach to Initiatives to Enhance Cybersecurity Countermeasures

IT is becoming increasingly integrated into business operations, including Production and Manufacturing and Development and Testing. In addition to countering cyberattacks targeting these operations outside of traditional IT infrastructure, cybersecurity measures are now required for products, services, and supply chains. (Figure 2-⑨)

In this context, Hitachi is promoting various initiatives to strengthen cybersecurity measures in each area. More precisely, we are strengthening cybersecurity measures for internal IT, operations, and processes in Products and Services, as well as supply chains. (Figure 2-⑩)

In addition, since 2023, We have been developing a system based on the concept of the Three Defense Lines. This is a framework to maintain security measures for the Production and Manufacturing environment, the Development and testing environment, and products and services. In the 1st Defense Line, each BU/group company conducts self-inspections to ensure compliance with the guidelines and management principles. Then, the ISRD monitors the status of the 1st Defense line as the 2nd Defense Line. Lastly, the headquarters' audit department verifies the IRSD's monitoring results as the 3rd Defense Line.

Figure 2-⑨ Expanding the scope of cybersecurity countermeasures



Cybersecurity Initiatives

Security Enhancement in Internal IT Environments

Security enhancement in in-house IT environment means setting standards for vulnerability countermeasures and network security, etc. to protect the networks, IT devices, and information systems used in internal office work from security risks, and requiring all BUs and Group companies to periodically check and correct the state of countermeasures. As a common measure for all companies, we have started monitoring the status of vulnerability measures for each device and following up with users and administrators, and we are expanding the range of applications for this action.

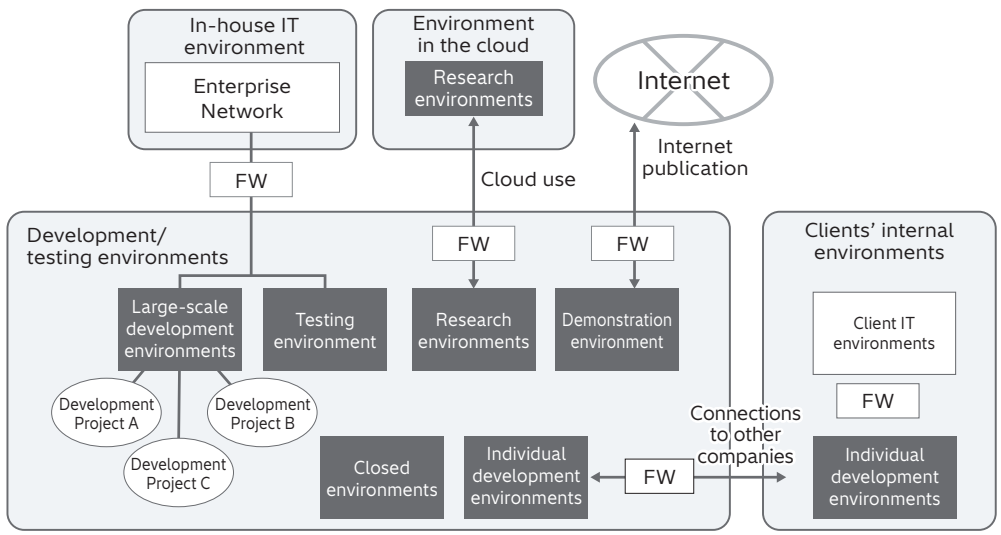
Security Enhancement in Development and Testing Environments

Development/testing environments include various environments for purposes such as development, testing, research, and demonstrations. We also use connections to customers' environments, the internet, and cloud environments. Security requirements vary between environments, but we have prepared guidelines for securely configuring and connecting each environment, and we work to apply the guidelines throughout the Hitachi Group. Development forms will go on changing due to factors such as use of the cloud and working from home, so we review our guidelines on a regular basis, and work to maintain and enhance security. (Figure 2-⑪)

Figure 2-⑩ Summary of actions to enhance cybersecurity countermeasures in various areas

Area		Target divisions	overview
In-house IT	Environment	IT	• Formulating and disseminating requirements for connection to and isolation from the in-house IT environments
Development and testing		Design and development	• Formulating and disseminating guidelines for building and securely connecting to in-house IT environments
Manufacturing and production		Manufacturing and production	• Formulating and disseminating guidelines for creating manufacturing and production environments based on IEC 62443 which is a series of standards regarding protecting control systems from cyberattacks
Products and services	Processes	Quality assurance for design and development	• Formulating quality management policies for the security of products and services • Formulating and disseminating requirements for product design, development, and maintenance processes
Supply chain		Procurement	•Formulate business partner cybersecurity countermeasure requirements and evaluate their implementation.

Figure 2-⑪ Development/testing environment security network



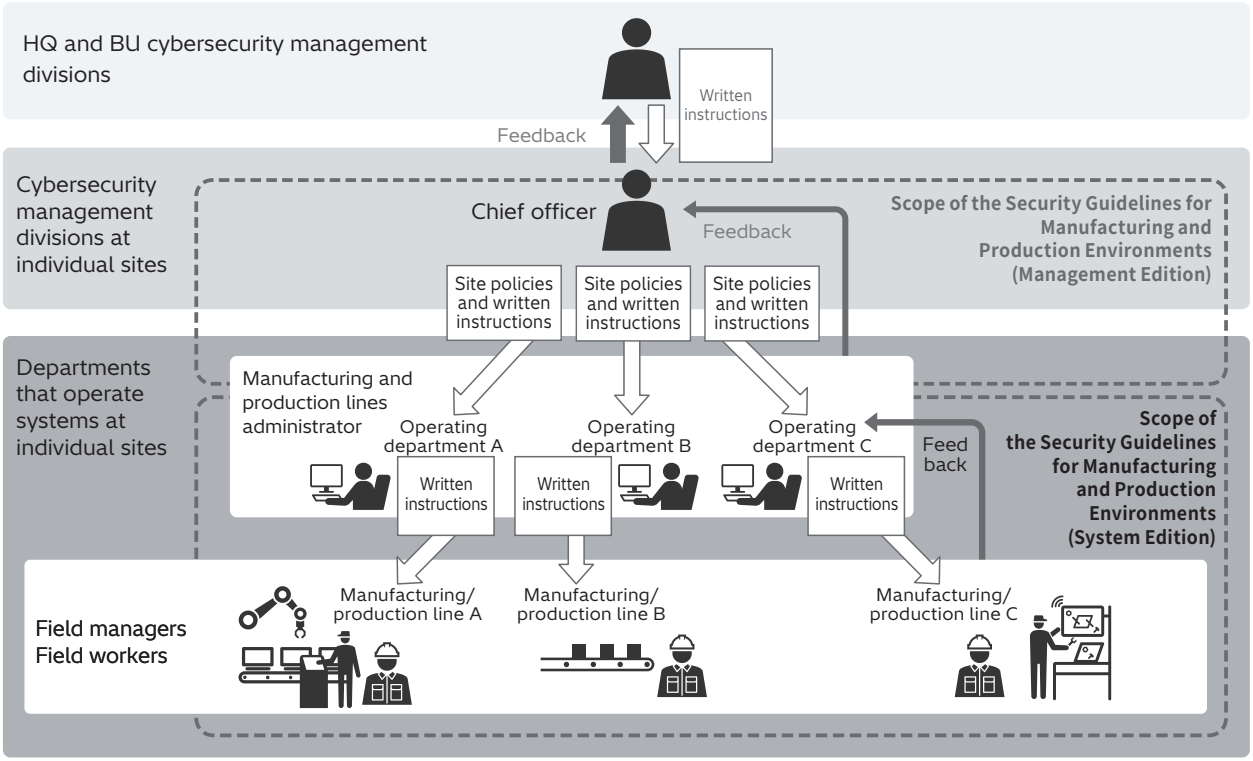
Security Enhancement in Production/Manufacturing Environments

Our Manufacturing and Production environments must not affect other environments, such as internal IT and development environments, and vice versa. This principle governs the creation and operations management of secure connections between environments within the Hitachi Group. (Figure 2-⑫)

At our Manufacturing and Production sites, posters and brochures outlining information security policies remind employees of their responsibility for compliance in their day-to-day work, resulting in greater security awareness. (Figure 2-⑬)

Figure 2-⑬ Posters/rule collections for production and manufacturing workplaces

Figure 2-⑫ Content of guidelines for production/manufacturing environments and an illustration of their use



Guideline structure	Description	Target audience
Management edition	From a managerial perspective (as initiatives for organizational and human resource management), this document describes the process of formulating and revising rules related to security operation and management for an entire site and specific divisions.	Person responsible for cybersecurity management
System edition	Describes the system configuration and approach to countermeasures in terms of ascertaining the current status and assessing countermeasures based on IEC 62443-3-3 with model used by the Hitachi Group. The contents of this document are reference to a typical customized by each division and department.	Manufacturing/production line manager
		Field manager
		Field worker

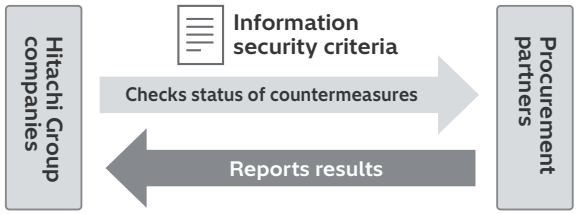
Cybersecurity Initiatives

Enhancing Supply Chain Security

We provide "Information Security Guidelines" to our procurement partners when outsourcing operations to a procurement partner. These guidelines include additional security measures for the supply chain to help our supply chain partners protect Hitachi's information assets. Our procurement partners are asked to maintain the same security level as ours by clarifying their requirements. We also regularly verify and audit their information security status. (Figure 2-⑭)

In addition, to encourage procurement partners to promote information security measures, we brief their management levels to explain the importance of supply chain security measures and our requirements for implementation using case studies of cyberattacks.

Figure 2-⑭ Security strengthening system in the supply chain

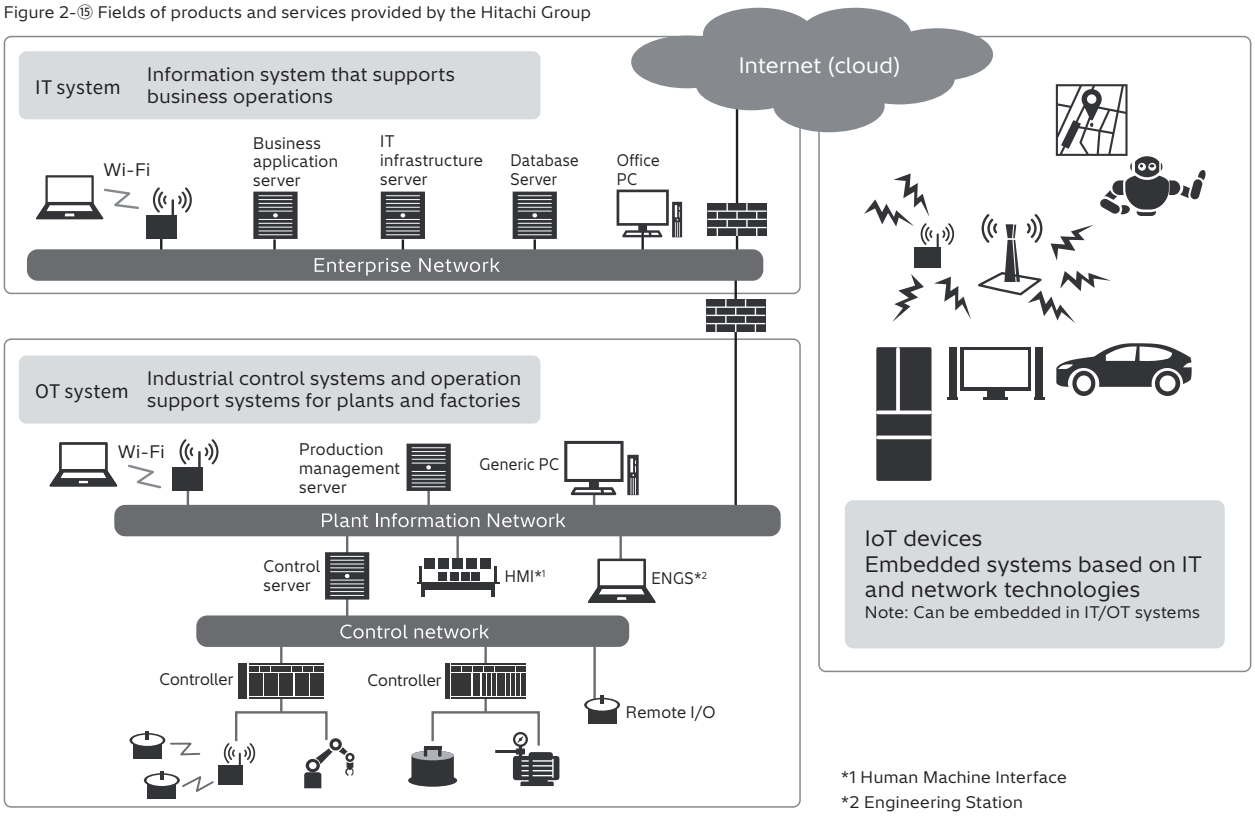


Security Initiatives Related to Products and Services

Hitachi's digital solution business advances digitalization technologies, network connection technologies, and system openness, bringing new value to our customers. Meanwhile, cybersecurity risks and responses become more important.

With the Hitachi Group's IT systems, OT systems, IoT devices, and various other products and services, we continue to drive initiatives to protect customer assets and social infrastructure from cyberattacks. (Figure 2-⑮)

Figure 2-⑮ Fields of products and services provided by the Hitachi Group



*1 Human Machine Interface
*2 Engineering Station

Security Management Policy for Products and Services

To unify the concept of security management for the many and varied products and services of the Hitachi Group, we have created the “Security Management Policy for Products and Services” and related materials as the guidelines for quality assurance. (Figure 2-⑯)

Each department incorporates this policy into its own security management policy to implement secure processes throughout the lifecycle of products and services in development, manufacturing, maintenance, and operations. (Figure 2-⑰)

Dissemination of Guidelines and Supporting Activities

We disseminate various guidebooks and other resources, such as the “Secure Process Implementation Guide,” to help business sites develop their own security management policies. These materials present case studies of design, production, and maintenance processes from the teams that have advanced initiatives against cybersecurity incidents. This initiative aims to accumulate and share knowledge throughout the Hitachi Group.

In addition to making these materials available on the intranet, we help all business units develop their own secure development processes.

PSIRT and Security Management System for Products and Services

In order to provide safe and secure products and services in accordance with the aforementioned “Security Management Policy for Products and Services,” a Product Security Officer is appointed at each BU and Group company to oversee the security system. Within this system, the ISRD and BUs and Group companies form teams called PSIRTs to address technical matters as part of the emergency response process. Each PSIRT collaborates with the others to handle product and service vulnerabilities and respond to incidents.

The Hitachi Group’s PSIRTs have guidelines for their own activities to follow. The PSIRTs meet in regular liaison meetings to present plans and technical information from the IRSD to the BUs and Group companies and to share activities at the sites.

To encourage autonomous RSIRT activities in the BUs and Group companies, the IRSD provides incident response exercises and other initiatives to the PRISRT members at each site.

Figure 2-⑯ Security management policy for products and services

Security management regulations etc.	Overview
Security Management Policy for Products and Services	A policy intended to unify the approach to security management for the products and services (hereinafter products) of the Hitachi Group.
Requirements for product development and maintenance processes	Requirements for product development and maintenance processes. Items in the requirements are interpreted into tasks according to the product characteristics, and a Product security inspection checklist is created as needed.
Product security inspection checklist	A checklist used to self-check the conformity of product development and maintenance processes at the site.

Figure 2-⑰ Overview of development and maintenance processes to ensure security

1. Design/manufacturing process	2. Operation/maintenance process	3. Security incident response process
1-1. Risk analysis and requirements definition/basic design	2-1. Change management	3-1. When detected internally
1-2. Configuration management	2-2. Collecting vulnerability information	3-2. When detected externally
1-3. Design/manufacturing	2-3. Predictive maintenance	3-3. Regular drills
1-4. Procurement (including OSS)	2-4. Routine vulnerability inspections	
1-5. Testing/evaluation	2-5. Reporting of vulnerabilities and countermeasure information to the customer	
1-6. Inspection		

Cybersecurity Initiatives

Cybersecurity Countermeasures

To stay on top of the handling of cyberattacks and incidents, Hitachi has a unit called the Hitachi Security Operation Center (SOC) to enhance security monitoring and incident response. We also take proactive measures, such as collecting and analyzing threat information, as well as disseminating vigilant information.

Enhancing Security Monitoring and Incident Response

All parties in our supply chain, regardless of size, are at an increasing risk of complex and sophisticated cyberattacks such as targeted attacks, ransomware attacks, and attacks that exploit system vulnerabilities. To confront such cyberattacks, it is crucial to detect threats and prevent the expansion of damage at the earliest stage. To this end, Hitachi launched the Hitachi Security Operation Center (Hitachi SOC) to enhance its security monitoring and incident response capabilities. The Hitachi SOC operates 24 hours a day, 365 days a year to minimize the damage of cyberattacks through early detection of malware infections and unauthorized access. We are also improving our global response capabilities through cooperation with the members in Europe and the Americas.

Cybersecurity Monitoring

Hitachi has established systems and network monitoring points that cover all core bases globally for integration, analysis, and monitoring of logs. In addition, we have introduced Endpoint Detection and Response (EDR) to enhance monitoring of terminal operations, for early detection of attacks on terminals and speedy response.

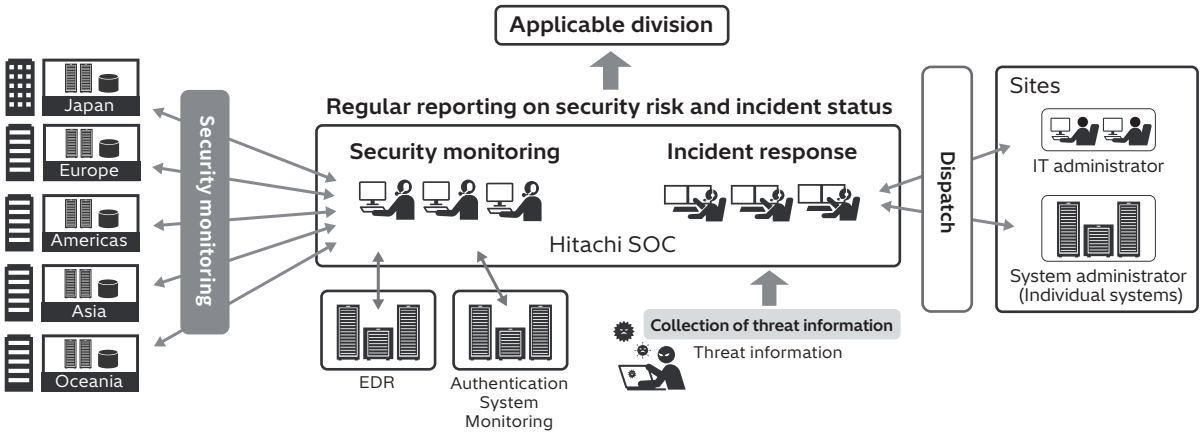
Also, by strengthening the monitoring of authentication systems, we are working to detect account compromise by third parties and attacks on authentication systems at an early stage, and to speed up response processes. These measures address increasingly complex and sophisticated cyberattacks and new threats arising from changes in work styles, such as working from home.

Incident Response

Hitachi has established an incident response procedure and communication structure. These allow us to quickly identify the cause of an incident, its scope, and its impact, and to take the appropriate countermeasures. Additionally, we can capture the details of any incident more quickly by combining log monitoring of core locations, EDR surveys, and authentication system monitoring. These mechanism allows us to reduce the time it takes to determine the priority and need for a response, making incident response more efficient.

We are also working to promote the automation of incident response by using new technologies to speed up and improve the accuracy of our response. The know-how we gather during incident response is then fed back to security monitoring and various internal security measures, making it less likely that the same kind of incident could occur again. (Figure 2-⑱)

Figure 2-⑱ Global security monitoring and incident response



Collecting and Analyzing Threat Information, and Disseminating Vigilance Information

Hitachi, Ltd. collects and analyzes threat information and disseminates vigilant information to ensure the security of the information systems used internally and the products and services it provides to its customers. We share the knowledge gained from these activities with the CISO for deliberation at the management level about security strategy for the Hitachi Group.

■ Collecting, Analyzing, and Verifying Threat Information

In addition to publicly available information on vulnerabilities and threats, we use various Cyber Threat Intelligence (CTI) services to collect threat information in Japan and abroad.

We classify and organize the collected threat information based on the metrics published by information providers, such as severity levels and CVSS scores, exploitation status, likelihood of attack success, and usage within our internal systems. For some threats, we use a simulated environment for verification to study the impact and damage that can be used in countermeasures.

We also collect and study information on the rapidly changing security related legal systems of various countries and regions to improve the Hitachi Group's risk response.

■ Disseminating Vigilance Information and Thorough Implementation of Countermeasures

The information collected is disseminated to selected people responsible for cybersecurity of BUs and Group companies through weekly digest emails, immediate email alerts, and intranet postings. For major threats that affect the entire Hitachi Group, we consider activating a Cyber BCP and issue a Cyber Alert with actionable instructions to ensure that countermeasures are thoroughly implemented.

We also utilize this information for threat hunting, incident response, and enhanced monitoring in collaboration with Hitachi SOC and the IT System Departments.

■ Escalation to Strategic Intelligence

Using the knowledge gained from collecting and analyzing threat information, as well as feedback from disseminating alert information, we analyze the current status of the Hitachi Group and areas for improvement. The results are shared with the ISRD, the CISO, and the Region Branches to help formulate the Hitachi Group's security strategy. This is intended to accelerate the execution cycle of security measures in the Hitachi Group.

■ Handling External Attacks

Systems exposed to the Internet are always at risk of external attack. We receive numerous vulnerability reports daily, as attackers steal confidential information through unauthorized access or infect targets with malware such as ransomware. There has also been an increase in attacks that take advantage of zero-day vulnerabilities (N-day vulnerabilities), which have already been exploited by the time the information is disclosed.

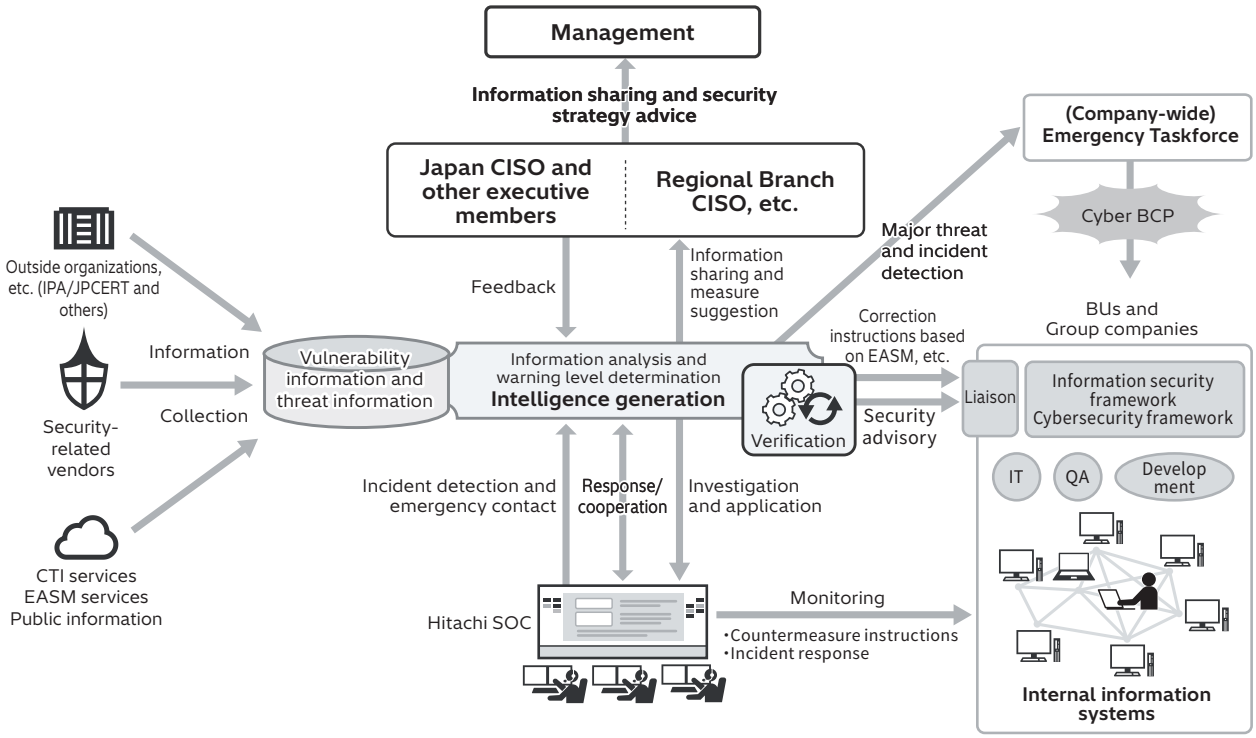
To respond quickly to these vulnerabilities, we use External Attack Surface Management (EASM) tools to manage the latest status of externally exposed devices. For equipment that has or may have manifested a risk, a Cyber Alert is issued to the relevant department, requesting immediate confirmation and correction. This action reduces the risk of external attacks and speeds up the response process.

■ Taking Action in Emergency Situations

If a threat might severely impact business operations at numerous sites within Hitachi, or would make company-wide business operations impossible, Hitachi establish a task force that directs the response at the company level, with measures such as issuing a cyber BCP. (Figure 2-⑲)

Cybersecurity Initiatives

Figure 2-⑲ Application of threat information in ordinary times and extension to emergency measures



CSIRT Activities

Hitachi established the Hitachi Incident Response Team (HIRT) as a CSIRT (Cyber Security Incident Readiness/Response Team) to support our cybersecurity countermeasures. By preventing any security incidents and promptly responding to them if they do occur, the HIRT contributes to the realization of a safe and secure network environment for our customers and society.

What is an Incident Response Team?

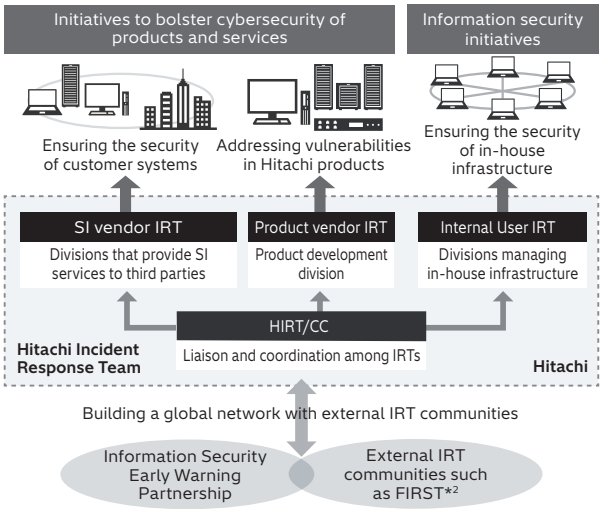
An incident response team is a group of people who lead “incident operations” to resolve issues through inter-organizational and international cooperation. The team members must have a basic skill set that includes “understanding and communicating threats from a technical perspective,” “coordinating technical activity,” and “liaising with external parties on technical matters.” This skill set enables the members to prevent (through readiness) and resolve (through responsiveness) various issues that might arise.

Model of HIRT Activities

The HIRT “eliminate vulnerabilities that may pose a cybersecurity threat” and “responds to incidents to prevent and resolve cyberattacks” in order to support Hitachi’s cybersecurity countermeasures. To accomplish these objectives, the HIRT has the perspectives of “Internal Activities” and “Collaborative Activities.” The former focuses on "information security initiatives for our own information systems," while the latter focuses on "cybersecurity measures for products and services for our customers." Furthermore, by implementing countermeasures early in the process of “catching up with the next threat,” the HIRT aims to contribute to the realization of a safe and secure internet society.

The HIRT has adopted a model that consists of four Incident Response Teams (IRTs) to improve vulnerability handling and incident response. The four IRTs are: (1) Product vendor IRT, responsible for developing products related to information systems and control systems; (2) System Integration (SI) vendor IRT, responsible for building systems and providing services using these products; (3) Internal user IRT, responsible for managing the operation of Hitachi’s information systems as an internet user; and (4) The HIRT/CC (HIRT) which coordinates among these IRTs. The A Model of HIRT activities promotes efficient and effective security countermeasure activities by clarifying the roles of each IRT while fostering collaboration among them. (Figure 2-⑳)

Figure 2-⑳ Four IRTs that support vulnerability countermeasures and incident response activities



Category	Role
HIRT/CC*1	Applicable division: SIRT Coordination Center Promotes vulnerability countermeasures and incident response activity through coordination with external IRT groups such as FIRST*2, JPCERT/CC*3 and CERT/CC4, and cooperation with SI vendor IRTs, product vendor IRTs, and in-house user IRTs.
SI vendor IRT	Applicable division: SI/service division Supports vulnerability handling and incident response for customer systems by ensuring their security in the same way as in-house systems in relation to known vulnerabilities.
Product vendor IRT	Applicable division: Product development division Supports vulnerability countermeasures for Hitachi products by investigating from an early stage whether any products are affected by known vulnerabilities, and taking action to resolve any issues found by patches or other means.
In-house user IRT	Applicable division: Divisions that provide internal infrastructure Supports promotion of vulnerability countermeasures and incident response so that Hitachi-related websites do not become the point of origin of a security breach.

*1 HIRT/CC: HIRT Coordination Center *2 FIRST: Forum of Incident Response and Security Teams
*3 JPCERT/CC: Japan Computer Emergency Response Team/Coordination Center
*4 CERT/CC: CERT Coordination Center

Cybersecurity Initiatives

Activity Promoted by the HIRT

HIRT's internal activities include promoting cybersecurity measures on institutional and technical fronts. These activities are carried out through cooperation between the ISRD and quality assurance departments to establish systems. The HIRT also supports vulnerability countermeasures and incident response for each BU and group company. On behalf of the IRTs, the HIRT serves as a liaison with external parties to promote cybersecurity measures.

■ Internal IRT Activity

Internal IRT activities include alerting and advising based on collected security information and analysis results and providing feedback on service/product development in the form of guidance and support tools.

(1) Collecting, analyzing, and disseminating security information

The HIRT disseminates information and expertise related to vulnerability mitigation and incident response gained through participation in the Information Security Early Warning Partnership*1 and other initiatives.

*1 A public-private partnership framework that facilitates the free flow of information about vulnerabilities in software products and websites, and the dissemination of mitigations.

(2) Developing the research infrastructure

The HIRT uses "behavior observation technology" to detect the early signs of invisible threats to take preventive action at the earliest possible stage. This technology observes and records behaviors of cyberattacks, such as spear phishing, in simulated internal network environments in order to investigate their activities. (Figure 2-㉑)

(3) Improving security technology for products and services

To improve overall IRT capabilities, HIRT implements security measures for information and control systems and related products and passes accumulated knowledge and skills on to expert personnel. As part of an approach to increasing hands-on internal security awareness, the HIRT develops simulated cyberattack drills that help employees learn about attacks such as targeted attacks and ransomware attacks.

To use the Common Vulnerabilities and Exposures (CVE) system for Hitachi products, the HIRT registered with the CVE Numbering Authority (CNA) program in June 2022. This program allows us to assign unique CVE IDs to Hitachi product vulnerabilities and publish our CVE records of the vulnerabilities, allowing us to offer products that our customers can use with confidence.

(4) Implementing IRT activities by sector

To take concrete and tailored action based on the background and trends in each sector, we have established sector-specific IRTs, such as the HIRT-FIS*2 for the financial sector.

*2 HIRT-FIS: Financial Industry Information Systems

Inter-Organizational IRT Activities

In interorganizational IRT activities, multiple IRTs build relationships with each other to collaborate against emerging threats and improve their own operations.

(1) Improving IRT collaboration within Japan

Through activities in the Nippon CSIRT Association (NCA), the HIRT Center shares information about vulnerabilities and incidents discovered in our intelligence activities with the Point of Contacts (PoCs) of other NCA members to build a collaborative network. The HIRT also supports the creation of an information-sharing platform based on the JVN*3 service jointly operated by the Japan Computer Emergency Response Team Coordination Center (JPCERT) and the Information-technology Promotion Agency (IPA).

*3 JVN: Japan Vulnerability Notes (a portal site that provides information about vulnerability countermeasures)

(2) Strengthening international IRT collaboration

Through the FIRST activities, we are promoting VRDX*4 activities to strengthen a collaborative framework with overseas IRTs and product vendor IRTs, as well as develop a format for exchanging information on vulnerability countermeasures.

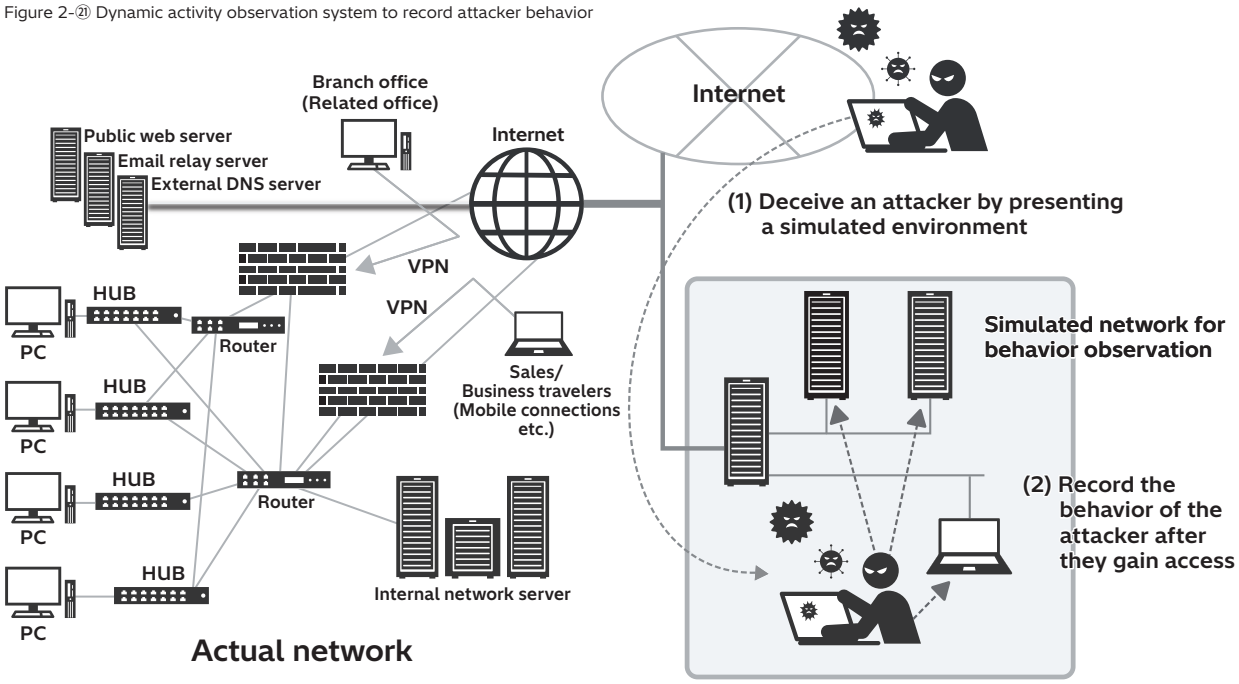
*4 Vulnerability Reporting and Data eXchange

(3) Creating opportunities for talent development

Hitachi actively participates in academic research and the anti-Malware and anti-cyberattacks engineering WorkShop (MWS), among others. Through these initiatives, we foster collaboration between industry and academia, developing talent and nurturing researchers and practitioners who are experts in their fields.

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

Figure 2-㉑ Dynamic activity observation system to record attacker behavior



Initiatives for Data Protection

Initiatives for Personal Information Protection

With the advancement of digital technology causing rapid growth in data usage, the protection of personal information and its transfer across borders are growing concerns. Against this background, as a provider of safe and secure social infrastructure systems, Hitachi places a high priority on personal information protection initiatives to reliably manage the personal information and trade secrets entrusted to us by our customers. “Providing safety and trustworthiness” and “recognizing the importance of individual rights” are our vision for personal information protection. As a member of the global community, we are committed to protecting personal information.

Visions for Personal Information Protection Governance

Hitachi’s vision for personal information protection is “providing safety and trustworthiness and recognizing the importance of individual rights.” Hitachi has positioned personal information protection as a key issue in its business and is making steady progress towards achieving its vision. (Figure 2-㉒)

Personal Information Protection Framework

To ensure adequate handling of personal information at the organizational level, Hitachi's top management established a personal information protection policy. By adhering to this policy, we have developed in-house rules and guidelines for managing personal information. Hitachi has a framework in place to check and evaluate whether its internal regulations conform to applicable laws and to Japanese Industrial Standards (JIS) Q 15001 which is the standard serving as the basis for PrivacyMark certification. In addition to this framework, when handling personal information, we implement concrete security management measures from four perspectives: organizational, personal, physical, and technical. (Figure 2-㉓)

Figure 2-㉒ Vision for personal information protection governance

VISION

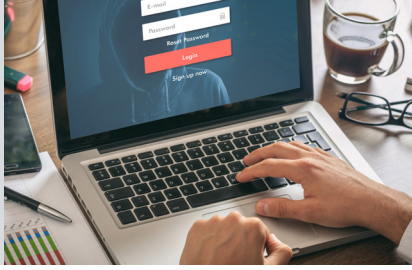
Protect personal information as a member of global society

1 Provide safety and trustworthiness

- We will conduct our business by adhering to a personal information protection and confidential information management program (process regulations) that complies with laws and regulations, thereby providing peace of mind and trust.

2 Recognize the importance of individual rights

- Keen to global trends, Hitachi respects individual rights in good faith.
- Hitachi considers the protection of personal information to be a fundamental human right and addresses it as a key business management issue.



■ Personal Information Protection Policy

As a global supplier of total solutions, Hitachi manages various types of information, including internal technical data and information entrusted to us by our customers. Therefore, Hitachi has strived to establish and rigorously implement an information management framework to respect the value of information. With that in mind, Hitachi, Ltd. has established a personal information protection policy and makes it widely available to stakeholders, on its website and by other means.

(https://www.hitachi.com/privacy-e/)

Hitachi Personal Information Protection Policy

(1) Establishment of personal information management rules and continuous improvement of the Personal information protection Management Systems

Hitachi will make sure that the Corporate Executive and employees recognize the importance of personal information protection, establish rules for personal information management to use and protect personal information appropriately, and ensure that the management system is put in execution. These rules will be maintained and improved continually.

(2) Collection, use and provision of personal information, and prohibition against using such information for purposes other than the original intent

While carefully considering the personal information is entrusted to us in our company activities, Hitachi will handle such information appropriately by establishing a management system for personal information protection for each type of business, and also by following our rules for collecting, using or providing personal information. In addition, Hitachi will not use such information for purposes other than the original intent and will implement appropriate measures for it.

(3) Implementation and correction of safety measures

To ensure the correctness and safety of personal information, in accordance with the rules for information security, Hitachi will implement various measures such as managing access to personal information, restricting the means for transporting personal information outside the company and preventing incorrect access from outside the company, and strive to prevent the leakage, loss or destruction of personal information. In addition, when any problems due to inappropriate safety measures are found, Hitachi will identify the cause to take corrective actions.

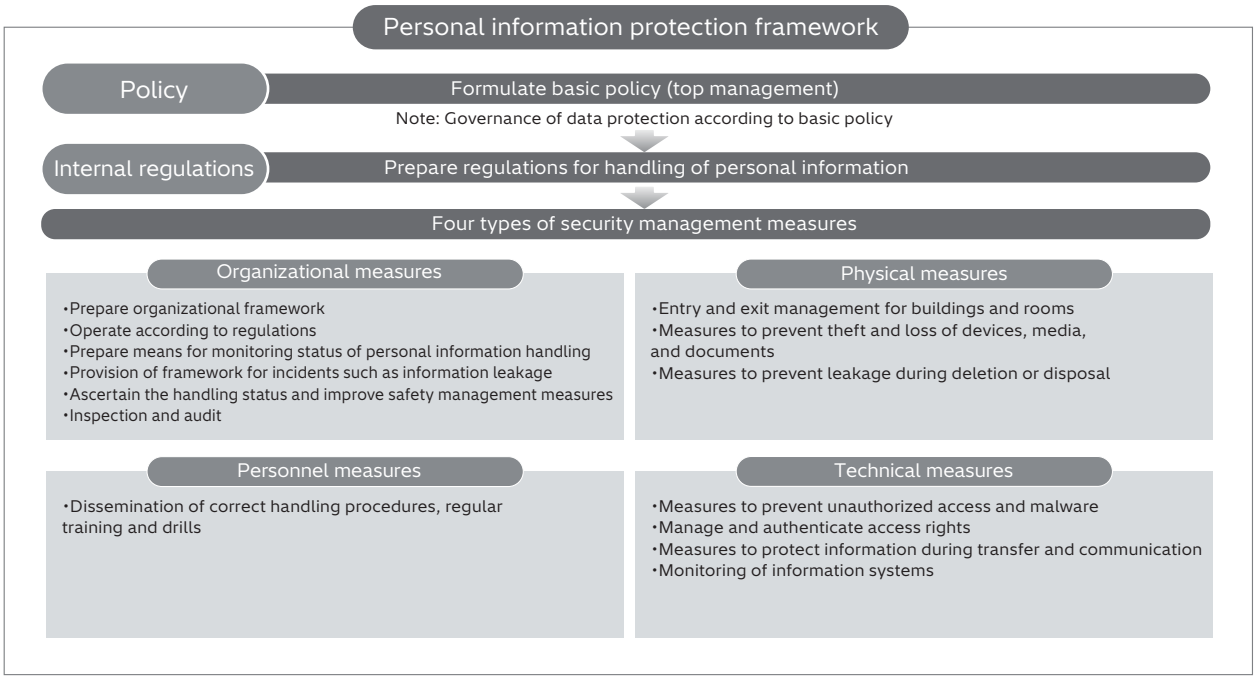
(4) Compliance with laws and norms

Hitachi will comply with the Japanese laws, guidelines and other norms for the handling of personal information. Also, Hitachi will conform our personal information management rules to these laws, guidelines and other norms.

(5) Respect for a person's rights regarding their personal information

When a person makes a request to disclose, correct or delete their own personal information, seeks to prevent the use or provision of such information, or gives any complaints or requires consultation, Hitachi will respond with sincerity, respecting the person's rights related to their personal information.

Figure 2-㉓ Personal information protection framework



Initiatives for Data Protection

■ System of Rules for Personal Information

Hitachi appropriately manages the personal information it obtains and holds according to a set of rules governing personal information protection. (Figure 2-㉔)

■ Security Management Measures

As part of its organizational security management measures, Hitachi designates people responsible for personal information protection and establishes a personal information protection system.

Hitachi defines rules related to the roles and responsibilities of workers in relation to security management and handling of personal information and operates according to those rules. Hitachi has also put in place a response framework to follow when an incident such as information leakage occurs, and defined rules related to inspection and audit, and carries out its operations accordingly.

As personnel security management measures, Hitachi conducts education and training in how to handle personal information appropriately based on the education plan for personal information protection. This includes stratified education, specialized education, and universal e-learning.

As physical security management measures, Hitachi has put security measures in place including managing entry and exit to various buildings and rooms, physically protecting devices and documents, anti-theft measures, and measures to prevent information leakage when disposing of devices and documents.

As technical security management measures, Hitachi prevents unauthorized access to information systems and takes measures against malware. Hitachi also manages and authenticates access rights, implements measures during transfer and communication, and monitors information systems according to the importance of the personal information being handled.

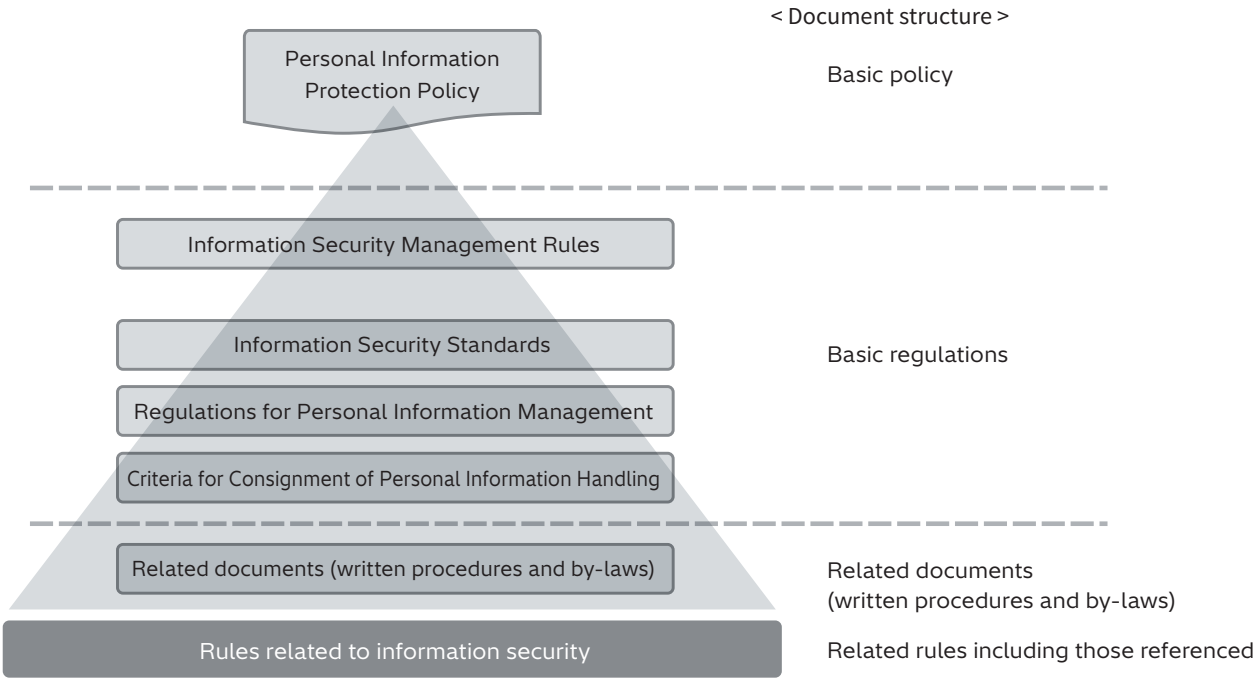
Personal Information Protection Management System

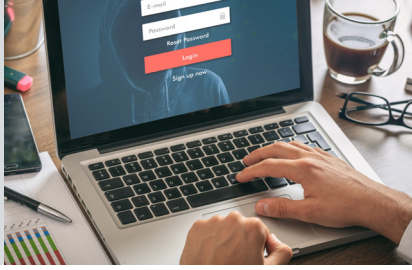
Hitachi's personal information protection management system was established based on JIS Q15001. Hitachi's "Personal Information Protection Policy" defines its policy regarding the protection of personal information.

The Article 52 of the "Information Security Management Rules" define the rules for personal information protection management.

The handling of personal information is stipulated in the Article 73 of "Regulations for Personal Information Management," the Article 12 of "Criteria for Consignment of Personal Information Handling." and related documents.

Figure 2-㉔ : System of personal information protection rules





Personal Information Protection Management Cycle

Hitachi's framework for personal information protection management is subject to the PDCA (Plan-Do-Check-Action) cycle, undergoing continuous improvement through decisive implementation of a plan.

The "Plan" stage entails formulating the personal information protection policy and personal information protection measures and establishing a personal information protection training plan and personal information protection audit plan. These are then approved by the President & CEO on behalf of Hitachi.

During the "Do" stage, the personal information protection measures are disseminated and used within Hitachi.

We conduct personal information protection training to ensure that all Hitachi members fully understand the measures and management approach. Hitachi also holds meetings to promote personal information protection matters to share information the status of implemented measures.

During the "check" stage, each department regularly assesses its own operations, which will be audited according to a company-wide audit plan. The Audit Manager creates the audit plan and reports, which are then approved by the President & CEO. We remain vigilant until any issues raised by these audits are resolved.

During the "Action" stage, Hitachi updates its management system based on various factors. These include amendments to rules and regulations regarding the handling of personal information, changes in the social landscape, opinions gathered from inside and outside the company, changes in the business environment, and the results of internal operations. (Figure 2-㉕)

Management and Appropriate Handling of Personal Information

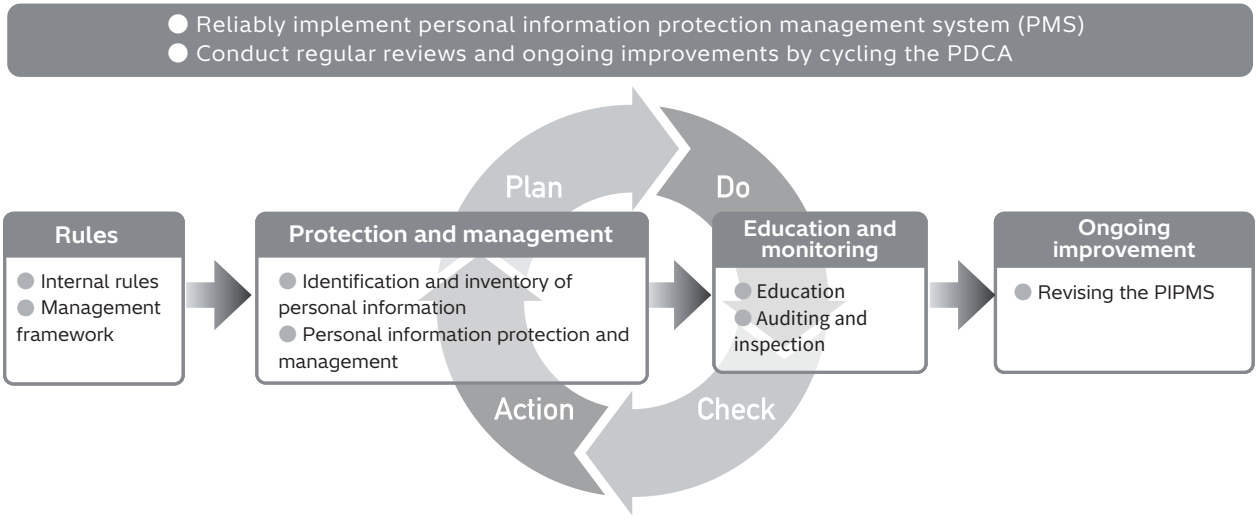
To ensure protection of personal information at a level exceeding that specified by Japan's Personal Information Protection Act, Hitachi has established internal regulations equivalent to the provisions of Japan Industrial Standard (JIS) Q 15001: "Personal information protection management systems requirements." These law and standard are the basis for Hitachi's efforts to strictly manage and appropriately handle personal information. An Information Asset Manager is appointed at each workplace to identify and manage all personal information handled in business, as well as to take appropriate measures according to the importance level and risks of the information.

We define "personal information handling" as the process of identifying and analyzing risks specific to business operations that pose a threat to personal information. Based on these risks, we establish operational rules for handling information and regularly review them.

All members who handle personal information fully understand these rules. They confirm their understanding before starting work and maintain a record of the verification.

Hitachi's internal rules comply with Japan's My Number system, which identifies all residents and manages social insurance services, tax payments, and more. We have assessed the risks associated with handling My Numbers and have established a management system that adheres to these rules. This system allows us to address those risks appropriately.

Figure 2-㉕: The framework of personal information protection management though the PDCA (Plan-Do-Check-Action) cycle



Initiatives for Data Protection

Auditing and Inspecting Personal Information Protection

Hitachi, Ltd. and all Group companies within Japan conduct an annual audit of their personal information protection and information security status. In the "Personal Information Protection and Information Security Audits," we verify compliance with internal personal information protection and management rules and audit compliance with legal requirements.

Group companies outside Japan conduct unified, global self-assessments by monitoring compliance status in order to implement Hitachi-wide inspections. As part of on-site self-assessments, all Hitachi, Ltd. workplaces perform “Personal Information Protection and Information Security Operation Checks” every year. Additionally, monthly "Personal Information Protection Operation Checks" are performed in sections where important personal information is handled to regularly confirm the implementation of security measures.

Employee Training for Promoting Personal Information Protection Awareness

To ensure the reliable protection of personal information, Hitachi provides annual e-learning training to all executives, full-time employees, and temporary staff. Hitachi, Ltd. distributes an Information Protection Card to each of them with the Personal Information Protection Policy and the basis of information security on it to ensure they fully understand the content.

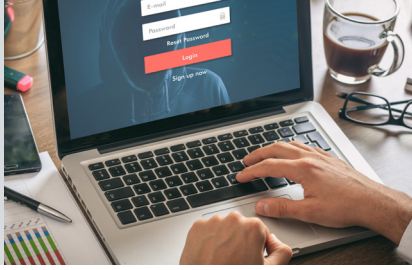
Improving Outsourced Vender Management

Hitachi has a long history of improving its management of outsourced venders performing our outsourced operations involving personal information. Through these initiatives, we developed internal outsourcing rules for handling personal information and oversee the venders to ensure compliance. When outsourcing business operations, Hitachi screens candidate companies and selects only those that protect personal information at a level equal to or higher than Hitachi's own standards. We only outsource our business operations to vendors who agree to a contract that strictly requires the establishment of a management structure and prohibits subcontracting. Furthermore, we regularly inspect their site to encourage the vendors to proactively manage and control the personal information that we entrust to them.

Global Approach for Information Protection

We define the Hitachi Group Privacy Principles as a common code of conduct for personal information protection throughout the Hitachi Group, and appoint Data Protection Managers. Additionally, to ensure the protection of personal information across all group companies, we share information on regulatory trends and send advisors to assist with personal data protection. To ascertain risk status in relation to personal information protection within the Hitachi Group and take action, Hitachi conducts ongoing monitoring of the compliance status of Group companies and implements appropriate measures.

The entire Hitachi Group will continue to strictly enforce compliance with personal information protection.



PrivacyMark*-Related Initiatives Across the Hitachi Group

Hitachi engages in personal information protection as a single entity.

Since our first PrivacyMark certification in 1998, as of the end of July 2025, 37 Hitachi group companies now hold this certification and handle and protect personal information at a level higher than required by law. After the tenth renewal of its certification in March 2025 and Hitachi, Ltd. is working toward the next renewal in March 2027.

The “Hitachi Group P Mark Liaison Committee” is a group of certified companies and stakeholders that regularly meet to share information, participate in study sessions, and receive lectures by external experts. Beyond this initiative, we exchange information on protecting personal information and learn about it throughout the Hitachi Group.

* The PrivacyMark is a third-party certification program that certifies businesses recognized to be implementing security measures and protection measures appropriate for personal information. (Issuing organization: Japan Institute for Promotion of Digital Economy and Community)

Hitachi’s Privacy Mark

Protecting your PRIVACY
10300031(10)

The URL of PrivacyMark System of Japan Institute for Promotion of Digital Economy and Community (https://privacymark.org/)

Holders of PrivacyMark Certification Within the Hitachi Group

As of the end of July 2025, the following Hitachi Group companies hold PrivacyMark certification:

Hitachi, Ltd.
Hitachi, Ltd., Corporate Hospital Group
Hitachi Health Insurance Society
Okinawa Hitachi Network Systems, Ltd.
Kyushu Hitachi Systems, Ltd.
Nichiwa Service, Ltd.
Hitachi ICT Business Services, Ltd.
Hitachi Academy Co., Ltd.
Hitachi Pharma Information Solutions, Ltd.
Hitachi Global Life Solutions, Inc.
Hitachi KE Systems, Ltd.
Hitachi Transportation Technologies, Ltd.
Hitachi Consulting Co., Ltd.
Hitachi Industry & Control Solutions, Ltd.
Hitachi Systems, Ltd.
Hitachi Systems Engineering Services, Ltd.
Hitachi Systems Power Services, Ltd.
Hitachi Systems Field Services, Ltd.
Hitachi Social Information Services, Ltd.
Hitachi Information & Telecommunication Engineering, Ltd.
Hitachi Research Institute
Hitachi Solutions, Ltd.
Hitachi Solutions Create, Ltd.
Hitachi Solutions West Japan, Ltd.
Hitachi Solutions East Japan, Ltd.
Hitachi Channel Solutions, Corp.
Hitachi Document Solutions Co., Ltd.
Hitachi Hi-System21 Co., Ltd.
Hitachi Power Solutions Co., Ltd.
Hitachi Building Systems Co., Ltd.
Hitachi Foods & Logistics Systems Inc.
Hitachi Property and Service, Ltd.
Hitachi Insurance Services, Ltd.
Hitachi Management Partner Corp.
Hitachi Real Estate Partners, Ltd.
Hokkaido Hitachi Systems, Ltd.
Hitachi Vantara, Ltd.

Initiatives for Data Protection

Privacy Protection Initiatives

As digital technologies such as artificial intelligence (AI) and the Internet of Things (IoT) advance, we expect to see more social innovations that utilize large amounts of varied data. However, this trend raises privacy concerns for ordinary people. Hitachi engages in privacy protection to create value, ensuring that people can enjoy safety and security.

Hitachi's Approach to Privacy Protection

Recently, there has been a growing expectation for value creation through the use of personal data, regardless of whether it constitutes personal information. This situation requires us to handle personal data carefully. In the DX era, more personal data is collected, and a wider variety of privacy risks arise. As shown in Figure 2-㉖, there is a partial overlap between personal data and information about individuals. This includes location data and purchase histories, for example, which have privacy implications. To create value using personal data, a business must protect personal information while also protecting privacy.

Through various business interactions with customers, Hitachi has accumulated privacy protection know-how. We use this knowledge to incorporate privacy considerations into our services and technology. This is how we contribute to making safe and secure social innovation a reality.

Hitachi's Privacy Protection Initiatives

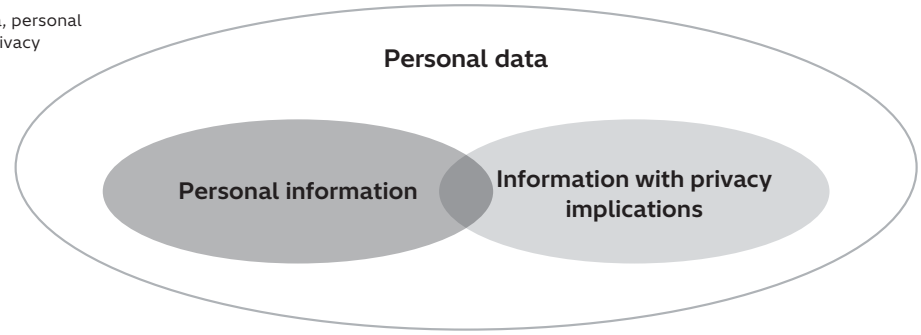
Hitachi, Ltd. seeks to create value through the safe and secure use of personal data. To this end, Hitachi works on privacy protection initiatives for data use in the Digital Systems & Services Sector.

In response to requests from society to protect our privacy, Hitachi introduces the Hitachi Privacy Impact Assessment (PIA) System and evaluates the impact of handling personal data. This initiative aims to balance privacy protection with the use of personal data to improve the quality and suitability of products and services, and to build trust with consumers and other stakeholders.

To promote the PIA system, we created procedure manuals and checklist forms for employees. By explaining the specific procedures for privacy impact assessments and the considerations for using the checklists, we ensure that all employees can implement our privacy protection measures. We will provide individual assistance if any questions arise about filling out the checklists. In addition, we offer regular training programs. These support systems raise awareness of privacy protection.

The Digital Systems & Services Sector has a unique business nature that must be addressed because it drives our digital business. Therefore, we appointed a "Personal Data Officer" to oversee the handling of personal data and established a "Privacy Protection Advisory Committee" to gather knowledge on privacy protection, assess risks, and support the consideration of countermeasures. This promotes our privacy protection initiative even more proactively.

Figure 2-㉖
Relationship between personal data, personal information, and information with privacy implications



Internal and External Activity Related to Information Security

Recent cyberattacks are gaining in level and sophistication, so the scope of their impact is widening, to include supply chains. To counter the threat of such cyberattacks, it is vitally important to build a security ecosystem that goes beyond internal departmental boundaries and also collaborates with external organizations. To that end, we are building a framework for inter-divisional collaboration, between divisions other than security, through various internal activities. We also participate actively in external activities, to enable collaborative creation with others in industry, government, and academia.

Internal Activity Related to Information Security

Now that we are in an environment where devices, systems, and other things “interconnect” in the IoT, even divisions which previously had few occasions to think about security must do so.

Therefore we organize seminars, workshops, and other events to build communities beyond barriers of position or organization, in addition to thorough implementation of measures by using IT systems and tools, and controls such as rules, regulations, and guidelines. These opportunities strengthen security by helping participants to reaffirm their individual roles and deepen connections with those around them.

We are holding workshops in the various countries and regions of the Americas, Europe, China, India, and other areas of Asia as activities to deepen understanding of measures we are promoting as internal controls. In Japan, we regularly hold seminars and workshops to provide opportunities to learn specialized knowledge about information security. We invite people from diverse fields as lecturers and strive to provide not only knowledge but also awareness to improve security consciousness.

External Activity Related to Information Security

Through communication with a community that bridges the barriers between government agencies, universities, research institutes, and other companies that are working to promote cyber security, we can share and agree on threat information, issues, and know-how when implementing countermeasures. That approach not only leads to more effective countermeasures for our own companies, but also contributes to strengthening the security of society as a whole.

Based on that perspective, we also use the knowledge and experience of our employees to participate in various external activities related to information security, such as the global international standardization activities noted below, and CSIRT work.

■ International standardization activity

Hitachi participates in the following international standardization activities.

■ ISO/IEC JTC1/SC27

SC27 is a subcommittee of the ISO/IEC joint technical committee JTC1 instituted by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) for the purpose of international standardization.

SC27 assesses the standardization of information security management systems (WG1), encryption and security mechanisms (WG2), security evaluation technology (WG3), security control and services (WG4), and identity management and privacy technology (WG5).

■ ISO TC292

ISO’s Technical Committee (TC) 292 assesses various security-related standardization including general security management, business continuity management, resilience and emergency management, prevention and management of unauthorized activity, security services, homeland security, and assurance of supply chain reliability.

■ ISO TC262

ISO's TC262 is focused on risk management, and assesses standardization of terminology, principles, policies, risk assessment methodology, and other aspects for all types of risk.

■ ITU-T SG17

SG17 is a Study Group (SG) under the ITU Telecommunication Standardization Sector (ITU-T) of the International Telecommunication Union (ITU). SG17 looks at standardization in such matters as

Internal and External Activity Related to Information Security

cybersecurity, security management for communications providers, telebiometrics, security functions for communication and application services, anti-spam measures, and ID management.

■ IEC TC65/WG10, WG20, and ISA-99 WG

IEC's TC65 promotes the standardization of industrial automation, measurement, and control. Within it, WG10 is working with the ISA-99 WG of the International Society of Automation (ISA) to standardize the technical, operational, and administrative security measures required for control systems. Also, IEC TC65/WG20 is working on standardization of development processes that achieve both security and functional safety in control systems.

■ CSIRT Activity

In addition to the CSIRT activity of the Hitachi Group, Hitachi participates in external CSIRT activity with the HIRT (Hitachi Incident Response Team) as its PoC (Point of Contact). Hitachi also promotes the sharing and exchange of information about vulnerabilities and other matters through cooperation with external CSIRT organizations.

■ FIRST

FIRST (Forum of Incident Response and Security Teams) is an international community of incident response teams bound by mutual trust. FIRST includes universities, research institutions, corporations, and government agencies among its members. As of the end of October 2024, membership consists of 753 teams from 111 countries.

■ Nippon CSIRT Association (NCA)

The NCA was established to help resolve issues faced during CSIRT activity by facilitating information sharing and cooperation among Japanese CSIRT organizations. Its mission includes helping organizations establish CSIRTs and creating collaborative frameworks among CSIRTs when an issue occurs, providing a venue through which Japan's CSIRT community can independently improve its basic incident response capability and find partners for collaboration in times of need. Hitachi is a founding member of the association, and from 2015 through 2020, a Hitachi representative held the position of chairperson and advanced it toward becoming a general incorporated association. As an executive committee member from 2021, and as deputy director since 2022, Hitachi has helped to promote CSIRT activities within Japan.

■ Other Activity

As part of our global external activities, we endorse the Cybersecurity Tech Accord joint declaration, which the IT and technology industries called for as a way to ensure safety in cyberspace. We aim to work within this global collaborative framework to protect user companies from cyberattacks. We have also joined the Information Security Forum (ISF), an organization engaged in world-leading investigation and research into subjects such as information security standardization and best practices for cybersecurity and digital risks.

Within Japan, Hitachi participates in various outside activity to promote research, discussion, proliferation, public awareness, and matters related to security. Hitachi also holds various seminars and conferences across the country.

- Information-technology Promotion Agency (IPA): Ten Major Security Threats Authors' Committee, etc.
- Japan Institute for Promotion of Digital Economy and Community (JIPDEC) ISMS Expert Committee, etc.
- Japan Cybercrime Control Center (JC3)
- Japan Information Security Audit Association (JASA)
- NPO Japan Network Security Association (JNSA)
- Information Security Operation providers Group Japan (ISOG-J)
- Japan Digital Trust Foundation (JDTF)
- Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) PA/FA Committee on Instrumentation and Control, Security Research WG
- Control System Security Center (CSSC)

- Japan Electronics and Information Technology Industries Association (JEITA), Information Security Expert Committee, Personal Information Protection Expert Committee, etc.
- Council of Anti-Phishing Japan
- National Institute of Technology and Evaluation (NITE) Evaluation Body Certification Technical Committee
- Robot Revolution & Industrial IoT Initiative
- CRIC Cross-Sector Cybersecurity Committee, CRIC Security Quality Committee, etc.
- Japan Society of Security Management (JSSM)
- The Society of Instrument and Control Engineers (SICE), Industrial Application Division, Technical Committee on Industrial Networks System
- Japan Automatic Identification Systems Association (JAISA)
- ICT-ISAC
- J-Auto-ISAC
- Transportation ISAC JAPAN
- JE-ISAC

Topics

Hitachi Systems, an IT company of the Hitachi Group, aim to realize safety and security across society, including the cyber domain, by providing safe and reliable digital infrastructure.

The security risk management department at Hitachi Systems gains technical experience through supporting customers in responding to security incidents, feeds this expertise back into human rewource development and research and development, and futher disseminates technology and knowledge externally to contribute to society. This cycle supports the sustainable growth of society's overall security level.

As one of the important elements of external collaboration, Hitachi work with police organizations, NPO's, and other industry-government-academia institutions, engage in joint research and development with academic institutions, facilitate personnel exchanges and participate in external conferences.

■ Activities as a Prefectural Police Technical Advisor

Each prefectural police department has established an advisor system to improve the police's ability to deal with cyber crimes and cyberattacks by appointing technicians from private-sector business operators as advisors. Hitachi Systems has had its own employees appointed as "Shimane Prefectural Police Cybercrime Countermeasures Technical Advisors" for Shimane Prefectural Police Headquarters in 2019, Hiroshima Prefectural Police Cybercrime Countermeasures Technical Advisor for Hiroshima Prefectural Police Headquarters in 2022, and Kinki Regional Police Bureau Cybersecurity Technical Advisor for the Kinki Regional Police Bureau.

Employees serving as advisors are security experts who assist in training investigators by providing advice and training on cybercrime investigations and countermeasures, as well as the latest trends and knowledge on security technology. They also take the stage at seminars held jointly by prefectural governments, industry, government, and academia, and give accessible lectures to local businesses and residents on security measures that each individual can take, thereby contributing to the improvement of the police's ability to respond to cybercrime.

Technical Advisor Appointment Ceremony

■ Activities with the Japan Network Security Association

Hitachi Systems is a member of the Japan Network Security Association (JNSA), a non-profit organization that contributes to the promotion and awareness of cyber security. As part of these activities, Hitachi Systems employees chaired the creative committee and worked with member companies to promote the "Everyone's Cyber Security Comic" sponsored event. Everyone's Cyber Security Comic is an activity aimed at spreading security knowledge, raising Internet literacy, increasing interest in and improving the image of hackers who protect the Internet, and promoting the development of security personnel. Everyone's Cyber Security Comic was produced between FY2020 and FY2023, and published on Twitter.

This activity received the Excellence Award in the Web and Content category at the "Cybersecurity Award 2023," hosted by the Digital Policy Forum and sponsored by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry.

In FY2024, Hitachi Systems also created and released an English-language version of the comic so that more people can view it.

Cyber Security Comic (English version)

*Source: From the official website of the Japan Network Security Association

Working to Raise Information Security Awareness

We see each employee's individual security awareness as security's last line of defense. Therefore, in addition to our existing strict governance, we have started activities to foster independence in our employees and raise their security awareness by encouraging them to take the initiative and act independently.

"Jibungoto (ownership)" in information security

Diverse ways of working such as working from home have rapidly become the norm, but with growth in cyberattack threats showing no signs of abating, it is more essential than ever for each and every employee to take adequate security measures. Until now, attacks have primarily targeted vulnerabilities in organizations' IT infrastructure, but with work styles increasingly based on working from places other than the office, attackers are beginning to target employees' lapses in security awareness.

Security measures have always required a balance between the three elements of IT, processes, and people.

We have begun expanding and enhancing education and awareness-building for employees and moving forward with more balanced security measures to reduce future security risks against attacks targeting "vulnerabilities in security awareness". We see improving security awareness as the last line of defense, so in addition to our existing strict governance, we are working to raise security awareness by encouraging employees to take the initiative and act independently. With the keywords "Jibungoto (ownership)" and "employees genuinely empathizing," we aim for employees to take an active interest in security and engage with it as their own responsibility, rather than being passive.

Encourraging self-initiative: Harry's Security

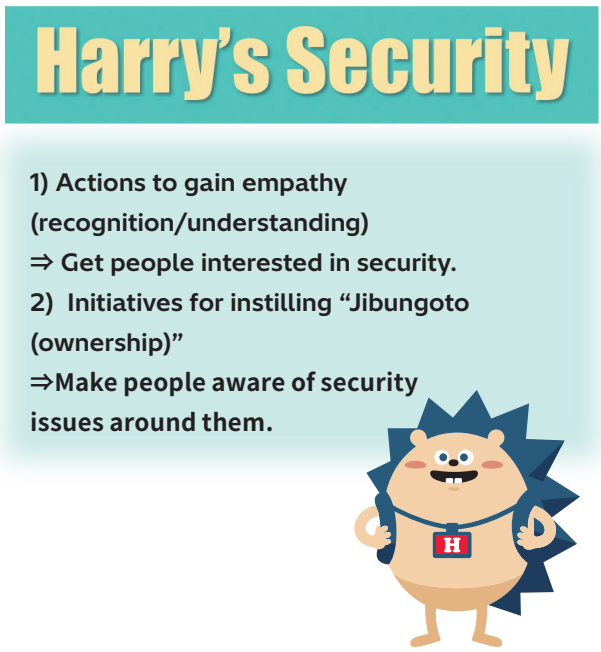
We are promoting "Harry's Security" for internal communications as a "mindset reform" to help employees see that security is an issue that directly impacts them, and to encourage them to get involved independently. (Figure 3-①)

Security work tends to have a negative impression of being difficult and tiresome, but this activity is intended to raise people's awareness of security around them by making them interested in it.

We use the newly developed mascot character "Harry" with the intranet and internal chats using Microsoft Teams* and other means to get closer to employees by making information dissemination more fun and accessible. The intranet provides information on information security through animations featuring "Harry" and content such as KYT (risk prediction training), so that users can easily learn about information security.

*Microsoft Teams is a registered trademark or trademark of Microsoft Corporation in the United States and other countries.

Figure 3-① Harry's Security Activities



Self-directed action: Green Aegis

We are promoting “Green Aegis” internal community activities as “behavior reform” to support employees in their own independent actions on security measures. (Figure 3-②)

The aim of this activity is to get employees interested in security issues, so that they independently acquire knowledge and research the issues, and share this knowledge with their colleagues.

Intranets and dedicated Microsoft Teams* are positioned as “communities for enjoyable involvement with security, which spread with open sharing and harmony”. We use them to provide places for introducing actions that we have taken, distributing videos that employees have planned for themselves, and encouraging employees to freely exchange opinions and take the initiative to get involved with security in ways which suit them.

In addition, every year we hold seminars and workshops for members who have been active in GREEN AEGIS to strengthen networking among members and expand community activities.

Figure 3-② Green Aegis Activities

Behavioral reform

GREEN AEGIS

Actions to make each employee see security as a personal matter and take the initiative in their behavior.
⇒ Get people to learn, investigate, and share knowledge.

GREEN AEGIS

Topics

Stimulate GREEN AEGIS community activities through events

GREEN AEGIS presents a GREEN AEGIS Award each fiscal year to employees who have actively participated or cooperated in its activities, including the dissemination of information within the community and the provision of information. In addition, an event called GA Summit is held for each year's award winners to stimulate communication among members and strengthen networking.

GA Summit 2024 was held in March 2025 with approximately 40 participants from 16 Hitachi Group divisions. The program consisted of workshops, the GREEN AEGIS Award 2024 award ceremony, and a reception.

At the award ceremony, the Chief Information Security Officer presented each recipient with a certificate and a commemorative plaque.

Through workshops in small groups and social gatherings, participants were able to gain operational hints from good practices in each department and share issues and ideas of those in charge, providing an opportunity for horizontal cooperation. With these members at the core, we will promote further expansion and revitalization of this community.

At the GA Summit 2024

Editorial

Security measures to respond to more advanced attacks, and generative AI-based systems

Damage caused by ransomware attacks and information leaks from organizations remains a major security challenge, as evidenced by its selection as one of the top 10 information security threats 2025 by the Information-technology Promotion Agency (IPA). To counter these threats, we must keep abreast of attack trends and keep countermeasures up-to-date. Hitachi is analyzing malware attack techniques and conducting research and development on information leakage countermeasure technologies that utilize large-scale language models.

TOPIC 1 Potential application of information obtainable from malware dynamic analysis screens to security measures

In recent years, as the number of cyberattacks has increased, the types and number of malware used in attacks has also been growing rapidly. Under these circumstances, it is increasingly important to examine malware developments in detail and consider appropriate countermeasures.

There are several different ways to examine malware. For example, surface analysis examines superficial information such as file names and malware types. Dynamic analysis activates the malware and records its behavior. There is also static analysis, which examines the code and assembly language inside the malware. Among these, dynamic analysis is used by many specialists because it reveals actual behavior.

One method of dynamic analysis is to record screenshots of the screen being analyzed. This screen shows a lot of information, including the apps launched by the malware and the messages displayed. These are used, for example, to detect ransomware and for research to improve the accuracy of Android malware detection.

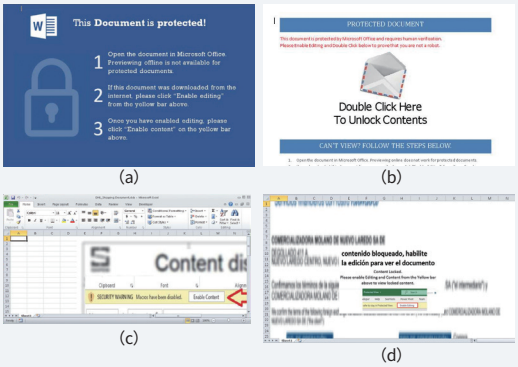
In addition, these screens may be used to understand attack techniques and educate users, as they also show what techniques attackers may be using to trick users. The information contained in the screen is not just technical data, but also hints about human behavior, such as how they are trying to guide the user visually.

So far, however, few studies have systematically examined the information obtained from these analysis screens. Therefore, in this study, we actually collected many analysis screens, organized the information obtained from them, and summarized what kinds of uses they can be put to.

Specifically, we examined 211 analysis reports for 93 types of malware families, for a total of 3,590 screens. In addition, we compared the information with that obtained from the logs to reveal information that can only be found from the screens. We were also able to confirm the ingenuity with which malware deceives (Figure 4-①) and threatens (Figure 4-②) users, and the difficulties faced by analysts, so we made suggestions to help improve education and tools.

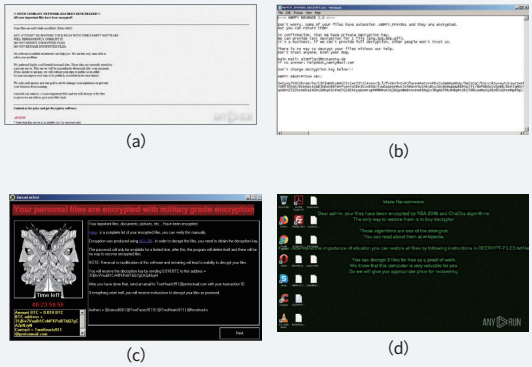
Thus, better use of the information on analysis screens is expected to lead to a deeper understanding of malware and better preparedness for cyberattacks. This is an important clue for the future development of security measures.

Figure 4-① Example of a malware screen that induces users to click



It prompts users to click by mimicking well-known software icons, etc.

Figure 4-② Example Ransomware Threat Screen



They encourage users to pay the ransom with threats such as, "If you don't finish the payment in time, we won't restore your data."

TOPIC 2 Automated identification of company confidential information using large-scale language models

In order for an organization to maintain its competitive advantage, it must properly manage company confidential information, which is to say, information that is both useful for the company's business activities and is kept secret. That requires the promotion of data security measures, but the reality is that these measures depend on education, and the risk of mismanagement of information assets arises due to the lack of progress in the operation of confidentiality classification in accordance with regulations.

Technology to detect sensitive data in text has been developed to assist in the prevention of information leaks. Techniques for detecting short phrases such as customer or product names have been studied as unique expression extraction and applied to privacy information detection. On the other hand, since the identification of company confidential information requires an understanding of the meaning of the text, it has been difficult to build a powerful automated technology.

For that reason, company confidential information is currently managed on a per-file basis which is easy for manual management. Strict control requires management in semantic units (per sentence), but that has not been implemented due to the enormous work quantities involved (Figure 4-③). This blurs the distinction between confidential and non-confidential information in files, a factor that hinders the sharing of knowledge of non-confidential information.

In recent years, Large Language Models (hereafter abbreviated as “LLM”) have been developing day by day, and their ability to understand the meaning of a sentence is also improving. Based on the hypothesis that this could be used to automatically identify company confidential information, we examined the possibility of automating the identification process. Specifically, in order to automate the task of identifying trade secret information in semantic units with an LLM, we gave them the name of the company confidential information, the entire document, and a sentence, and had them determine whether the sentence contained the relevant company confidential information (Figure 4-④). As a result, sentences with company confidential information could be detected with high accuracy, demonstrating the system’s feasibility.

This automated identification technology significantly reduces the work quantities required to manage information in semantic units, enabling both the protection of confidential information and the utilization of non-confidential information. This is also expected to improve RAG* search performance by utilizing the non-confidential portions of confidential files.

In addition, this technology can support thorough data management/operation in accordance with information management rules. Referring the identification results of this technology to the administrator is expected to reduce data management and operation costs and improve security literacy.

* RAG: Retrieval Augmented Generation.

Figure 4-③ Current (As Is) and Ideal (To Be) Forms of Management of Company Confidential Information

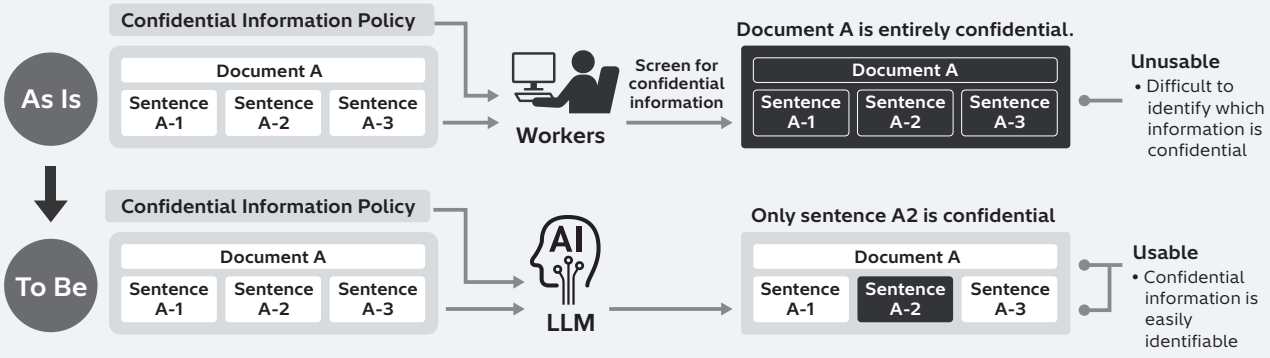
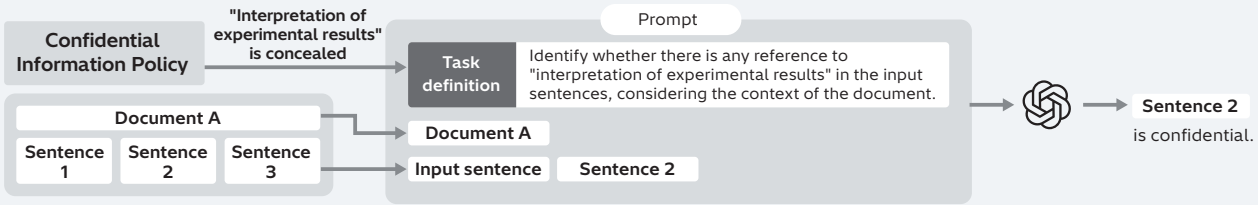


Figure 4-④ Overview Chart of Identification of Company Confidential Information by LLM



Third-Party Evaluation and Certification

Hitachi promotes third-party evaluation and certification in relation to information security management.

Status of ISMS certification

The following organizations of Hitachi, Ltd. and Hitachi Group companies within Japan have gained 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 July 2025). The names of the organizations are listed with reference to how they appear in the list of ISMS-accredited organizations maintained by the ISMS-AC and other sources.

- Hitachi, Ltd. (Financial Information Systems 2nd Division, Governmental & Public Financial Systems Division)
- Hitachi, Ltd. (AI & Software Services Business Unit, Managed & Platform Services Business Division, Digital Business Development Division, Business Development Data & Design, Application Services Division, Technology Transformation Division, Delivery Transformation Division)
- Hitachi, Ltd. (Social Infrastructure Information Systems Division, Strategy Planning Division, Energy Systems Division 1, Energy Systems Division 2, Energy Solutions Division and Mobility Solution & Innovation Division)
- Hitachi, Ltd. (Social Infrastructure Systems Business Unit, Government & Public Corporation Information Systems Division)
- Hitachi, Ltd. (Industrial AI Business Unit, Water & Environment Business Division, Value Chain Business Development Division, TSS Green & Digital Solutions Department, Environment Solutions Division, Information System Engineering Department, Industrial Digital and Water & Environment Business Management Division, Digital & IT Innovation Division, Secure IT Innovation Center, Secure Information Group)
- Hitachi, Ltd., Social Infrastructure Systems Business Unit, Defense Systems Division (Yokohama Office), Corporate Sales & Marketing Group, Digital Systems & Services Business Sales Management Division, Defense Systems Sales Management, and Hitachi Advanced Systems Corporation (HQ)
- Hitachi, Ltd. (Industrial AI Business Unit, Industrial Digital Business Division, Enterprise Solutions Division, Life Industry & Platform Solutions Division, Platform Solutions Dept.)
- Hitachi Channel Solutions, Corp.
- Hitachi Social Information Services, Ltd. (System Service Division)
- Japan Space Imaging Corporation
- Hitachi Information & Telecommunication Engineering, Ltd. (Managed Services Department)
- Hitachi ICT Business Services, Ltd. (Solution Business Support Department 1, Media Service Group)
- Kyushu Hitachi Systems, Ltd.
- Hitachi Systems, Ltd. (Public & Social Business Group)
- Hitachi Systems, Ltd. (Public & Social Platform Services Division)
- Hitachi Systems, Ltd. (Contact Center & BPO Services Division)
- Hitachi Systems, Ltd. (Solution Business Administration Group, Maintenance Business Promotion Division, Platform Support Department)
- Hitachi Systems, Ltd. (Industrial & Distribution Business Group, Industrial & Distribution Solution Services Division 1, Digital Life Science Services Office, Health Support Services Department)
- Hitachi Systems, Ltd. (Managed Services Division, Security Services Division)
- Hitachi Systems Power Services, Ltd. (Information and Communication Technology Services Division, Platform Systems Services Office)
- Hitachi Systems Engineering Services, Ltd. (Managed Services Business Group)
- Hitachi Systems Engineering Services, Ltd. (Corporate Systems Division, Corporate Systems Office 2, Systems Department 3)
- Hokkaido Hitachi Systems, Ltd.
- Hitachi Solutions Create, Ltd.
- Hitachi Solutions West Japan, Ltd. (Cloud Platform Operating Support Department)
- Hitachi Solutions East Japan, Ltd. (Social Infrastructure Solution Div.3)
- Hitachi Solutions East Japan, Ltd.(Service Delivery Group I)
- Hitachi Solutions, Ltd. (Subscription platform service operation and maintenance)
- Hitachi Solutions, Ltd. (Security assessment services)
- Hitachi Pharma Information Solutions, Ltd.
- Hitachi KE Systems, Ltd. (Tokyo Development Center)
- Hitachi High-Tech Corporation(Solution Center)
- Hitachi Management Partner Corp. (Corporate Planning Division, Human Resources Solution Division)

Status of IT security evaluation and certification

The following table lists the key products certified under the Japan Information Technology Security Evaluation and Certification Scheme run by the Information-technology Promotion Agency (IPA) based on ISO/IEC 15408. (This includes listing in the "archived list of certified products" as of the end of August 2025) (Figure 5-①)

Figure 5-① Main products certified under the Japan Information Technology Security Evaluation and Certification Scheme

Product	TOE type*1	Certification No.	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)	Storage device control software	C0514	EAL2+ALC_FLR.1
Hitachi Unified Storage VM Control Program 73-03-09-00/00(H7-03-10_Z)	Storage device control software	C0513	EAL2+ALC_FLR.1
Microprogram 0917/A for Hitachi Unified Storage 110	Storage device control software	C0421	EAL2
Microprogram 0917/A for Hitachi Unified Storage 130	Storage device control software	C0420	EAL2
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	Biometric device	C0332	EAL2
Certificate Validation Server 03-00	PKI	C0135	EAL2
CBT Engine 01-00	Major application of CBT examination 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

*1 TOE (Target Of Evaluation)
A TOE is defined as a product such as software or hardware that is the subject of evaluation. This can include written guidance for managers and users (user manuals, guidance,installation procedures etc.).

*2 EAL (Evaluation Assurance Level)
ISO/IEC 15408 stipulates the degree of assurance of evaluation items (assurance requirements) in a range from EAL1 to EAL7. A higher level means more stringent evaluation.
- EAL1 involves the validation and testing of security functions and the objective evaluation of guidance used to maintain security.
- EAL2 adds vulnerability analysis with respect to typical attack vectors and evaluation from the perspective of product integrity from manufacturing to commencement of operation. This adds a security perspective to the standard development lifecycle.
- EAL3 adds to the assurance of EAL2 by evaluating the development environment to assure the comprehensiveness of testing and prevent tampering of the product during development.
- EAL4 is considered a high level of assurance for general consumer products, and evaluates the entire development lifecycle including the integrity of development assets in the development environment, the source code of the product, and the trustworthiness of personnel.
- ALC_FLR.1 objectively evaluates the basic procedures for providing the necessary patches when a security defect is found in the product. You can use this assurance level to add assurance requirements not included in the EAL of the standard. The level is expressed as EAL2+ALC_FLR.1, for example.
- ALC_FLR.2 requires that procedures are in place to accept reports about vulnerability information and to notify users.

Third-Party Evaluation and Certification

Status of testing and certification of cryptographic modules

The following table lists the main products certified by the Japan Cryptographic Module Validation Program (JCMVP) based on ISO/IEC 19790 operated by the IPA or the Cryptographic Module Validation Program (CMVP) based on FIPS 140-2 and FIPS140-3 operated by NIST in the United States and CSE in Canada. (This includes listing in the “historical list” by CMVP as of the end of August 2025) (Figure 5-②)

Figure 5-② Main products certified by the Cryptographic Module Validation Program (CMVP)

Product	Certification No.	Level
Hitachi Storage Hybrid Firmware Encryption Module	5013	Level 1
Hitachi Vantara Cryptographic Library	4239	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Board for NVMe	4194	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	4183	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board for NVMe	4076	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module for NVMe	3803	Level 2
Hitachi Flash Module Drive HDE	3314	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board	3279	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	3278	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Adapter	2727	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board	2694	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	2462	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Engine	2386	Level 1
Hitachi Unified Storage Encryption Module	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*1and Windows*2editions)	JCMVP #J0007	Level 1
Keymate/Crypto JCMVP Library	JCMVP #J0005	Level 1

*1 Solaris is a trademark or registered trademark of Oracle Corporation, its subsidiaries, and affiliated companies in the USA and other countries.
*2 Windows is a trademark or registered trademark of Microsoft Corporation in the USA and other countries.

Overview of the Hitachi Group

Company Profile (As of March 31, 2025)

Corporate name
Hitachi, Ltd.

Incorporated
February 1, 1920 (founded in1910)

Head office
1-6-6 Marunouchi,Chiyoda-ku, Tokyo,Japan

Representative
Toshiaki Tokunaga, President & CEO

Capital
464.384 billion yen

Number of employees
282,743 (Japan:112,749, outside Japan:169,994)

Business Performance Highlights for FY 2024, Based on the International Financial Reporting Standards(IFRS)

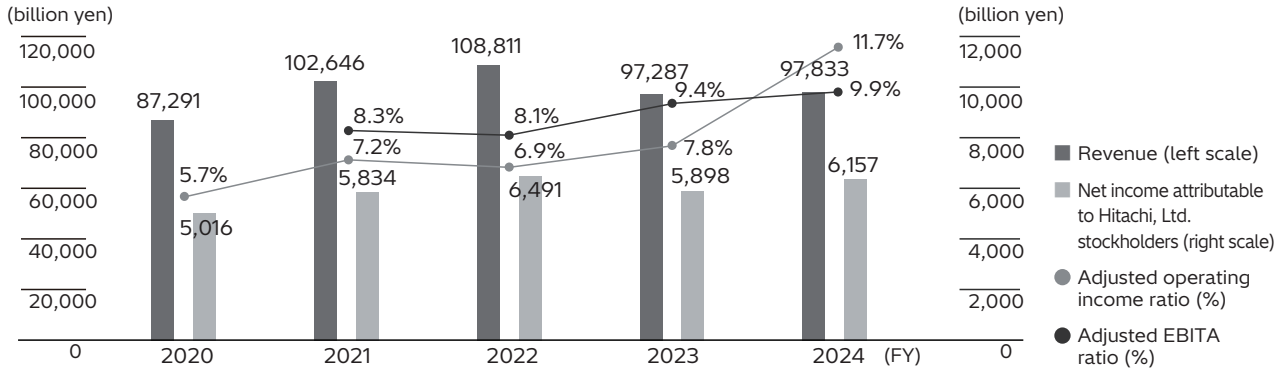
Revenue
9,783.3 billion yen (up 1%, year on year)

Net income attributable to Hitachi, Ltd. stockholders
615.7 billion yen (up 4% year on year)

Adjusted EBITA*1
1,141.8 billion yen (up 4% year on year)

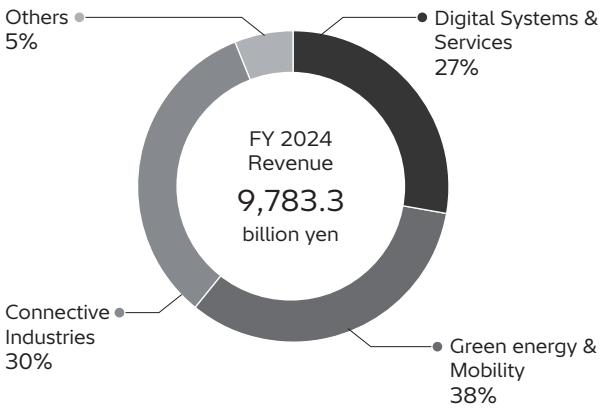
Adjusted operating income ratio
9.9% (up 2.1 percentage points, year on year)

Adjusted EBITA ratio
11.7% (up 2.3 percentage points, year on year)

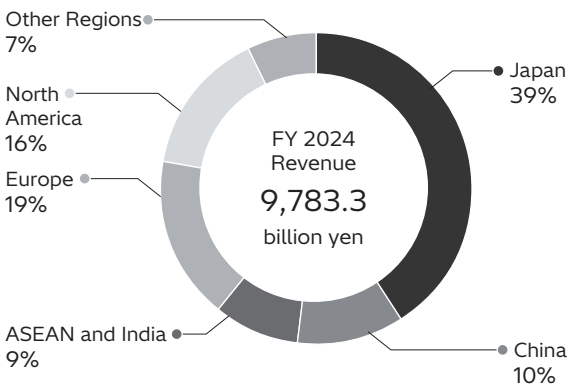


*1 Adjusted EBITA (Adjusted Earnings Before Interest, Taxes and Amortization): Adjusted operating income + Acquisition-related amortization + Share of profits (losses) of investments accounted for using the equity method

Business Composition*2



Revenue by Region*2



*2 Revenues from each division as a percentage of total revenues. Revenues of each division include interdivisional internal revenues.

Hitachi, Ltd.

Information Security Risk Management Division

1-6-6 Marunouchi, Chiyoda-ku, Tokyo 100-8280

TEL.03-3258-1111

Printed in Japan (H) (2025.12)