

HITACHI

Information Security Report 2026



Hitachi Group

INDEX

CD&SO Message	1
The Philosophy Behind Hitachi's Information Security.....	2
Information Security Management	8
Information Security Management Systems	8
Information Security Enhancement Initiatives	14
Cybersecurity Initiatives	17
Cybersecurity Management	17
Cybersecurity Countermeasures.....	22
SIRT Activities	25
Initiatives for Data Protection	28
Initiatives for Personal Information Protection.....	28
Privacy Protection Initiatives	34
Internal and External Activity Related to Information Security	35
Working to Raise Information Security Awareness.....	38
Editorial AI-Based Security Verification Technology to	40
Protect OT Systems and Equipment	
Third-Party Evaluation and Certification	42
Overview of the Hitachi Group	45

Summary of this report:

- Scope and time period covered by this report: Hitachi Group information security initiatives up to and including FY 2025
- Report publication date: September 2026

CD&SO Message

Hitachi, Ltd.
Vice President and Executive Officer,
Chief Digital and Security Officer (CD & SO)
Satoko Fujimori



Achieving both speed and reliability in digitalization, and delivering peace of mind to our customers and to society

The landscapes surrounding cybersecurity, IT and AI are changing minute by minute. Malicious use of AI in particular is making cyberattacks more sophisticated and intricate at an alarming rate. Even under these circumstances, we at Hitachi remain committed to our mission: through our social innovation initiatives, we deliver secure and trustworthy environments to society and our customers.

To accomplish this mission, Hitachi's IT and security units are working together more closely than ever before, as they design and promote protective measures against cyberattacks, develop robust digital infrastructure, and improve IT and security governance across the entire Hitachi Group.

Furthermore, by fully leveraging AI to review our operations and processes, we are enhancing our digital infrastructure and strengthening our cyber resilience. This enables us at Hitachi to make decisions more quickly and flexibly to achieve our

management plan, "Inspire 2027."

In the field of information security, Hitachi analyzes risks from an attacker's perspective, and quickly and continually implements high-priority measures. We have developed a group-wide framework to adapt quickly to changes and improve our governance. We are also developing more advanced AI-powered defense technologies. With the "Customer Zero" philosophy, we implement and validate the effectiveness of cybersecurity measures before providing them to our customers, to deliver cybersecurity technologies backed by real-world experience.

The Hitachi Group incorporates IT and security into its strategy planning and governance to promote digitalization and minimize security risks. With a flexible structure for change and robust, secure digital environments, we achieve both speed and reliability for strengthening the foundation for our future business growth.

The Philosophy Behind Hitachi's Information Security

Hitachi identifies and manages risks by considering social issues, competitive advantages, and management resources, based on observations and analyses of ever-changing business environments. This approach allows us to identify potential risks and generate growth opportunities, thereby increasing revenue while maintaining control over risks.

In particular, the change in the landscape surrounding information security is drastic. Increasing cyberattacks around the world target not only individual businesses, but also their entire value chains, causing societal problems.

Misuse of AI can make cyberattacks more widespread and sophisticated, posing a greater risk to businesses. To minimize these risks, Hitachi positions information security risk management as one of the most important business management issues. In this context, Hitachi implements various information security measures, such as cybersecurity and data protection, to create value and manage risks.

Information Security as a Management Strategy

Our goal of maintaining and improving the Hitachi Group's information security is part of our management plan, Inspire 2027, formulated in 2025 to promote information security. To achieve this, Hitachi, Ltd.'s Digital & Security Strategy Division (D&SD) conducts annual self-assessments of security measures and takes necessary follow-up actions. The assessments are based on our "Cybersecurity Scoring," which we created using the

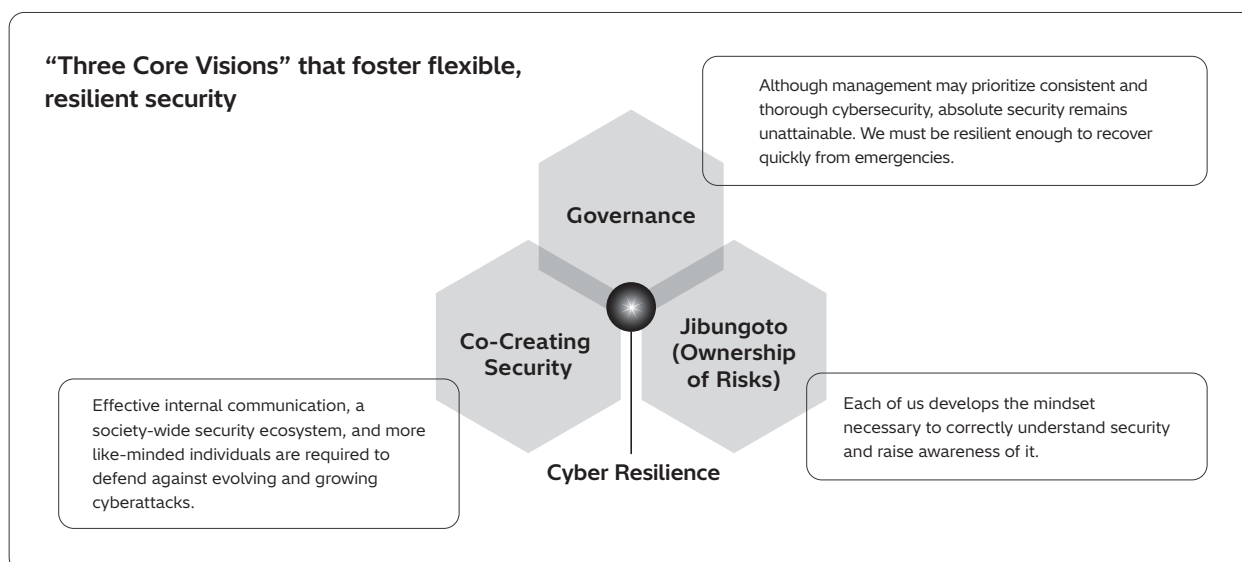
cybersecurity management guidelines from Japan's Ministry of Economy, Trade and Industry and other materials.

The risk mitigation is verified, and its effectiveness is regularly monitored from a management perspective. Corrective actions, such as additional measures, will be gradually taken as needed.

Hitachi's Information Security Vision

Hitachi promotes various initiatives to enhance cyber resilience through three approaches: "Governance," "Co-creating Security," and "Jibungoto" (ownership of risks). (Figure 1-①)

Figure 1-① Hitachi's information security vision





■ Governance: Zero Trust Security Initiatives

From the WannaCry ransomware attack in 2017, we learned valuable lessons. The scope of protection has expanded beyond internal IT systems to include OT systems. We consistently and thoroughly develop robust measures in terms of operations, technologies, and organization. We focus on robust security and business continuity planning (BCP) for products, services, and supply chains.

We are developing zero-trust security measures based on a cloud-based IT architecture. The goal is to optimize the security of cloud-based business systems and remote work. To implement zero-trust security, we have defined "authentication," "endpoint," and "cyber-integrated monitoring" as key elements. Based on these elements, we are raising the level of attack-detection capabilities even higher.

■ Co-Creating: Initiatives for Building a Security Ecosystem

In a security emergency, the IT department requires the cooperation of many teams, including public relations, human resources, labor affairs, and legal affairs. As the scope of security expands, the MONOZUKURI (creation), quality assurance, and procurement departments, among others, must collaborate closely to maintain security functions. Hitachi sees a security ecosystem like this as vitally important and is working to build it.

Our belief that "things," "people in an organization," and "society" must be connected is the key to building this ecosystem.

Digital Transformation (DX) requires an environment in which "things," such as devices and

systems exemplified by the Internet of Things (IoT), are "connected." We must ensure security when "things" that were once isolated become connected to each other. To do this, we establish a framework that "connects people and organizations," enabling collaboration between different organizations. We must not only connect internally, but also with businesses, government agencies, and educational institutions. Together, we must form a community that transcends organizational boundaries to share threat intelligence and the challenges we encounter when implementing countermeasures. We proactively engage in "connected society" activities. In these activities, individual companies and organizations use the knowledge gained in this community to inform their own security measures and build upon them.

(Figure 1-②)

■ Jibungoto: Security Awareness-raising Initiatives

As remote work becomes more widespread, weaknesses in security awareness become an easy target. When working outside the office, we don't have anyone to ask for advice. As a result, we are all constantly facing risks.

Therefore, we must be security-conscious: each of us is the last line of defense. Based on this belief, we are fostering employee autonomy, encouraging proactive behavior, and fully implementing existing governance measures. Our goal is to encourage our colleagues to understand the importance of security and to view it as their own responsibility rather than an obligation. (Figure 1-③)

Figure 1-②: Illustration of the security ecosystem

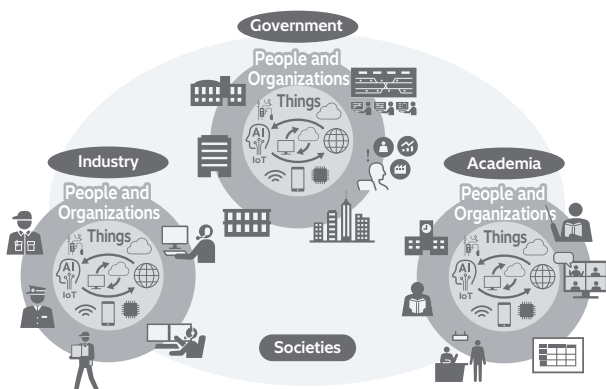
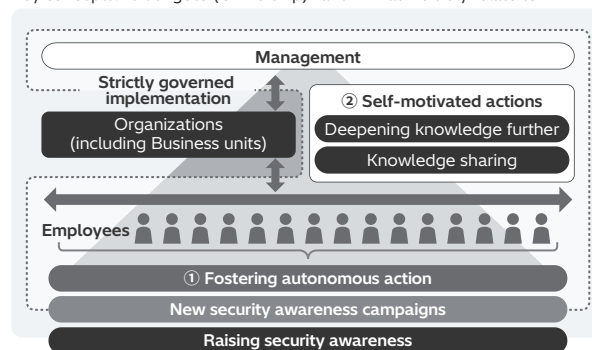


Figure 1-③ Our Goal for Security Awareness

We must be highly aware of security.

Key concepts: "Jibungoto (Ownership)" and "What we truly relate to"



The Philosophy Behind Hitachi's Information Security

Scope of Information Security

As shown in Figure 1-④, Hitachi defines the scope of protection for maintaining information security as information assets “information” and “systems” and their “CIA” attributes: “confidentiality,” “integrity,” and “availability.”

■ Scope of Protection in Terms of Information Security

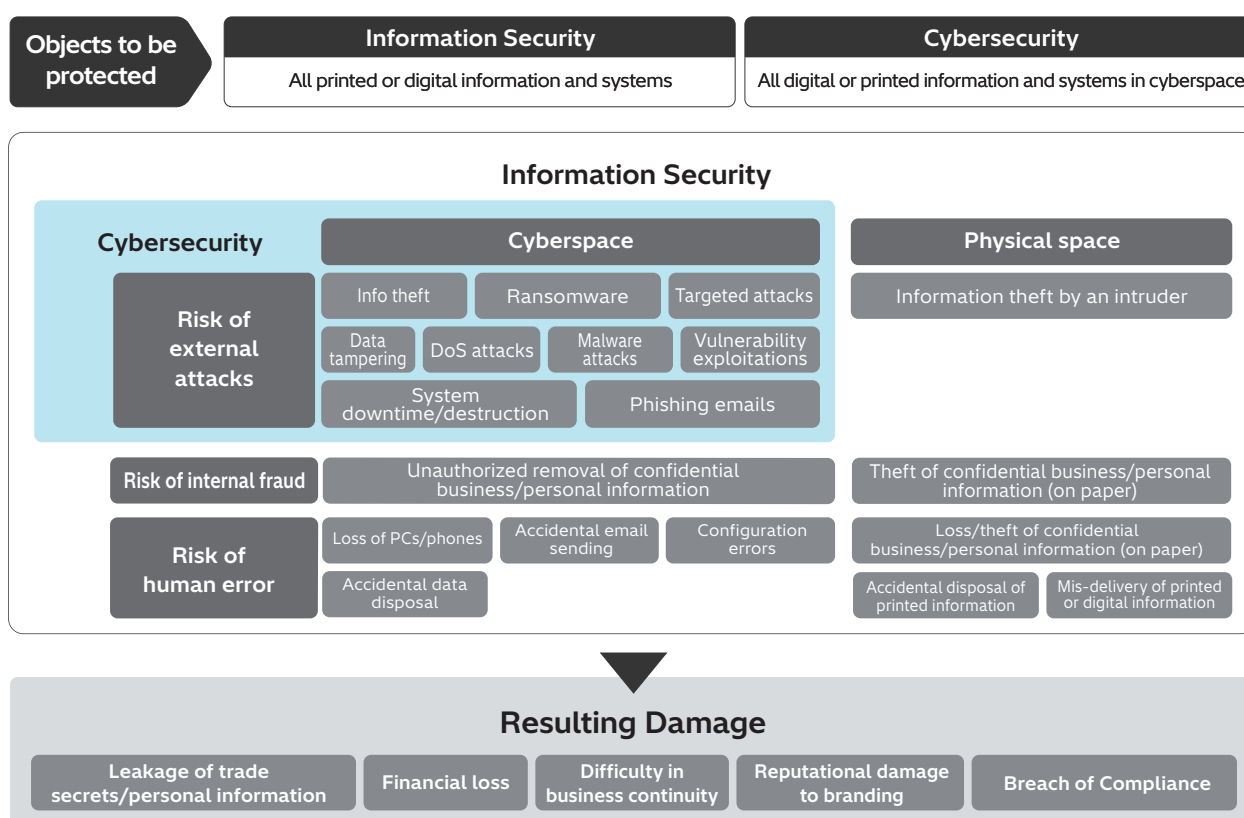
We define “information” as data in both cyberspace and physical space. This includes data printed on paper or stored in other physical media, which is protected by information security.

Risk events include risk drivers such as external attacks, internal fraud, human error and compliance

violations. These events can result in financial losses, brand damage and business continuity disruption.

At Hitachi, we develop information security strategies and design measures from a risk management perspective and based on a preemptive assessment of potential damage resulting from risk events.

Figure 1-④ Targets to be protected in Information Security

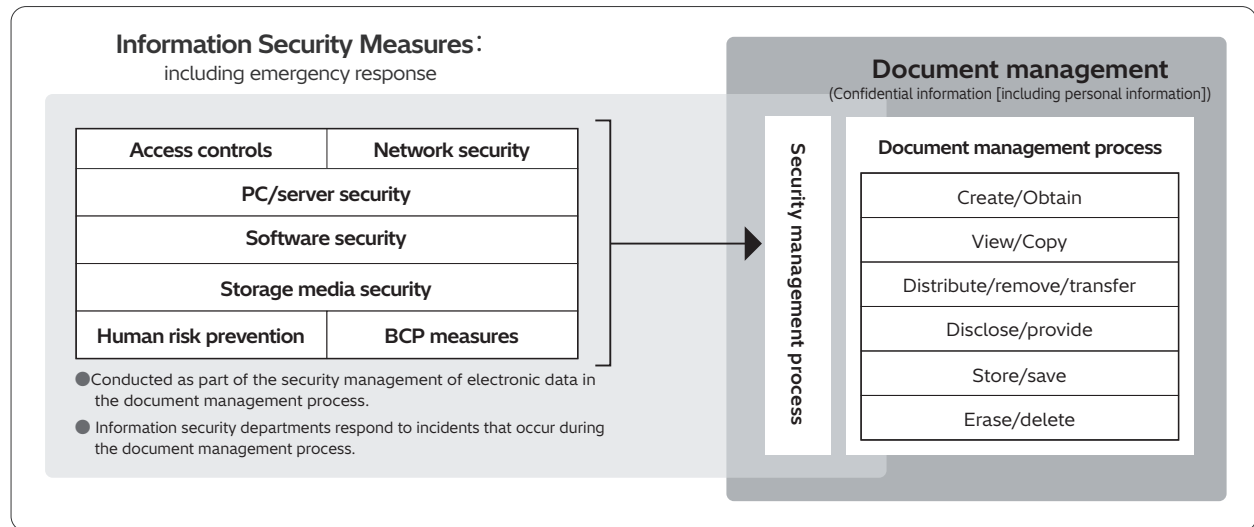




Our information security strategies and measures are based on the management of confidential information and cybersecurity. As illustrated in Figure 1-⑤, we also consider the document

management process from creation and acquisition to disposal and deletion of information as a scope for information security maintenance measures.

Figure 1-⑤ Scope of current management by information security departments

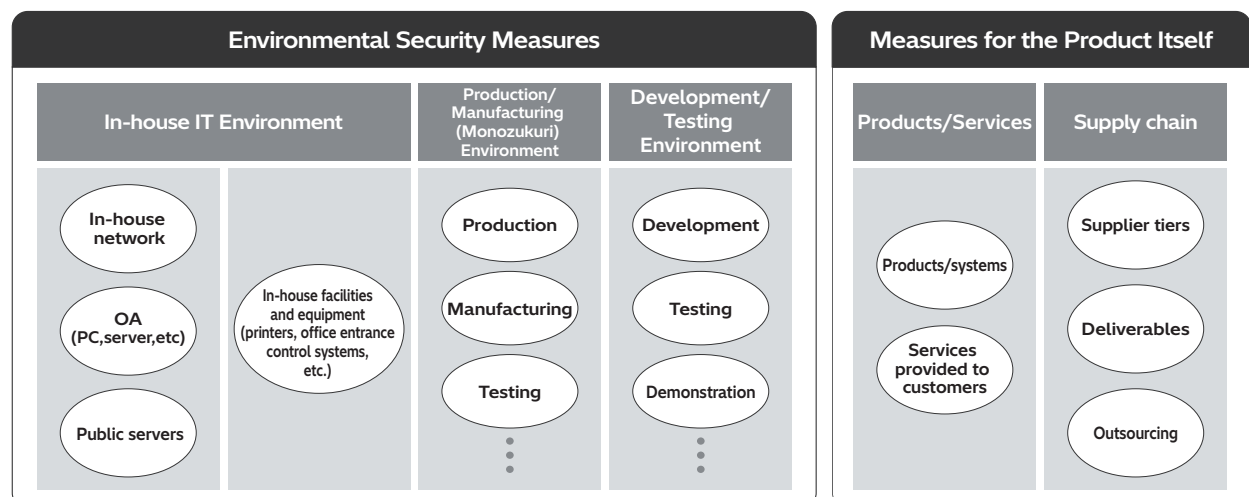


Scope of Governance

After the damage caused by the WannaCry ransomware attack in 2017, we redefined the scope of governance for information security in 2018. As illustrated in Figure 1-⑥, our information security governance covers not only internal IT environments,

but also production, manufacturing, and development environments, as well as products, services, and supply chains.

Figure 1-⑥ Scope of governance



The Philosophy Behind Hitachi's Information Security

Information Security Strategy and Key Themes

As shown in Figure 1-⑦, Hitachi's D&SD formulates its security strategy based on three main components.

The first is governance and management. As part of our governance functions, we establish and disseminate rules, as well as plan for the monitoring and auditing of compliance with those rules. We also develop guidelines, processes, and educational and training programs to help our colleagues comply with these rules.

The second component involves tracking trends in information security expertise, monitoring technological developments, and implementing technical measures. Information on attack trends, technological developments, and regulatory changes are collected and shared with the Hitachi Group's business units. These units use the information to plan their own measures. Furthermore, as cyber security experts, we develop the necessary measures for the Hitachi Group's monitoring and incident response.

The third component is improving awareness and literacy. We design awareness campaigns to improve the security literacy of all Hitachi Group employees, using both a bottom-up and a top-down approach.

The Environment Surrounding Information Security

Key trends in security incidents for fiscal year 2025 include the growing prevalence of attacks exploiting AI and the prolonged impact of ransomware. The growing misuse of AI is eliminating language barriers and making phishing attacks more sophisticated and widespread. The limitations of human-powered responses necessitate a reevaluation of the traditional concept of incident response. For example, we should use AI to immediately isolate devices when signs of an attack are detected.

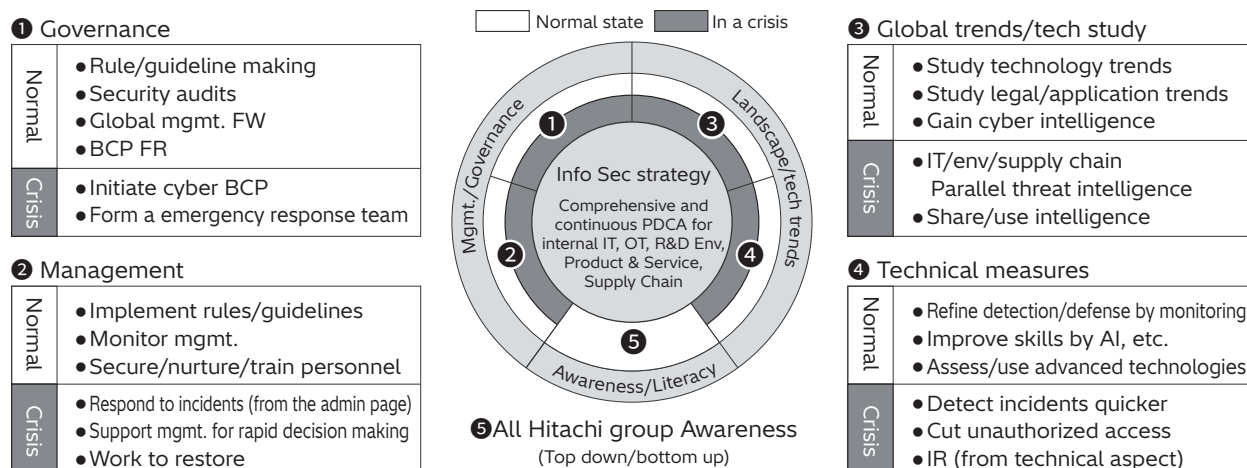
As seen in incidents involving major Japanese companies, their business impact of ransomware attacks tends to be prolonged. Now more than ever, we must take a business continuity approach that considers the time required to ensure security after an incident occurs. The prevailing trend in attacks is to cause widespread disruption to business operations for financial gain and to extort ransom payments. In addition, the misuse of AI has automated the entire

process—from preparation to execution—resulting in attacks that are constant, rapid, and increasingly frequent. We must recognize that sophisticated attacks have become a very real threat capable of disabling our traditional defenses.

Global policy trends are seeing a strengthening of security regulations, such as the Cyber Resilience Act (CRA), which EU member states are fully implementing by December 2027. Japan is rapidly tightening its security regulations, including the Economic Security Promotion Act and the Act on the Prevention of Damage to Critical Computers Caused by Unauthorized Acts. A security evaluation system that strengthens security clearances and supply chain security is also becoming important.

The Hitachi Group handles many critical infrastructure projects and must therefore closely monitor this development and respond appropriately. Many nations are quickly implementing regulations regarding the privacy and use of data by AI. This

Figure 1-⑦ Security governance elements





*1 Digital Transformation *2 Internet of Things

requires us to continue making systematic preparations and taking the right measures.

■ Key Themes and Activities

In fiscal year 2025, we promoted various measures focusing on three key themes in light of trends in security incidents and policy developments: ① improving the effectiveness of information security risk management, ② responding to increasingly sophisticated and capable cyberattacks, and ③ addressing the tightening of global laws and regulations.

1. Improving Information Security Risk Management

To manage information security risks more effectively, we have implemented 3DL* monitoring since the previous fiscal year. The scope initiative includes internal IT and each environment for development and testing, production and manufacturing, and products and services at business units and group companies. This initiative clarifies their Information Security Risk Management status and enables us to identify and eliminate areas of improvement.

In response to the growing number of cyberattacks on the supply chain, we have implemented thorough measures to prevent incidents and drive improvements, with a focus on key suppliers. Our data protection program monitors our group companies in Japan and overseas to identify those that require corrective action and pinpoint areas for improvement. This allows us to track progress and achieve better practices.

* "3DL" refers to Three Defense Lines. For details, refer to "Approaches to Enhancing Cybersecurity Measures" on page 17.

2. Responding to More Sophisticated and Capable Cyberattacks

In response to more sophisticated and capable cyberattacks, we focus on enhancing cloud environment security, data security and internal fraud monitoring.

To ensure security when using cloud environments, we have created guidelines and started monitoring. These guidelines address the risks associated with mutual authentication in Hitachi Group cloud services. To enhance data security, we redesigned the classifications of confidential information to make them more recognizable to users and ensure consistency with the rules. This new data security measure will take effect in fiscal year 2026. Internal fraud monitoring is also under review. We are verifying its functions to identify issues in actual operations and exploring its implementation in fiscal year 2026.

3. Consistently Complying with Tightening Global Laws and Regulations

According to the CRA, reporting on vulnerabilities and incidents will be mandated in September 2026, for which we are preparing. To comply with the EU Data Act, we have made templates of contracts and notifications, as well as a practical guide, available. All business divisions are working on design-level compliance efforts for the Act's implementation in September 2026.

The Act on the Protection and Utilization of Important Economic Security Information went into effect in Japan in May 2025. We are creating various templates to help internal applicants prepare documents for "eligible contractor" certifications under the Act.

Key Initiatives Going Forward

The misuse of AI makes cyberattacks quicker and more sophisticated. AI agents increase the number of potential accounts being victimized. Data protection laws are being strengthened worldwide. Therefore, we must implement consistent and fundamental measures in the medium to long term.

Moving forward, we will adopt the strategy of "prioritizing potential targets from the attacker's perspective to improve cyber resilience in an agile and constant manner" under our "Customer Zero" approach, in which we fully utilize AI before its rollout to market. The following initiatives will be our focus.

- Improve tactics by setting priorities from the attacker's perspective.
- Promote constant, agile management measures by using AI-powered technologies.
- Improve business environments by applying AI-powered frontline measures.

Information Security Management

Information Security Management Systems

Hitachi has established policies on information security and the protection of personal information and has built a framework to implement these policies both in Japan and globally. Through this monitoring and auditing framework, the D&SD ensures that various regulations are properly in place established across the group and that employee training and other measures are being implemented appropriately.

Information Security Policy

Hitachi makes every effort to ensure information security by incorporating security policies into the enterprise's broader management policies.

Information Security Policy

(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 a Personal Information Protection Policy to protect personal information. For

more information, see the "Personal Information Protection Policy" on page 29.

Promotion Framework for Information Security and Personal Information Protection

Promotion Framework for Information Security

At Hitachi, the D&SD is responsible for the entire group's information security governance. Hitachi, Ltd. conducts this governance through the respective lines of control of its business units (BUs), business sites, and group companies. Then, the BUs and group companies implement similar controls over their respective group companies

(subsidiaries), thereby ensuring governance across the entire Hitachi Group. This framework applies to Japan and other locations overseas.

At Hitachi, the Representative Executive Officer, President & CEO of Hitachi, Ltd. (hereinafter, "President & CEO") shall appoint a Chief Information Security Officer (CISO) and an Information Security Audit Officer. The CISO will have the



responsibility and authority to determine policies and implement measures related to information security across the entire Hitachi Group, while the Information Security Audit Officer will have the responsibility and authority for personal information protection and information security audits.

As the CISO, the Chief Digital and Security Officer (CD&SO) chairs the Information Security Committee and determines policies related to information security, the protection of personal information, training plans, and other measures. The Committee communicates its decisions to all organizations through the Information Security Promotion Council which brings together operational staff from all BUs and offices.

The Committee deliberates and decides on rules and initiatives, regularly reporting them to members of the Audit Committee, who are also members of the Management Committee and the Board of Directors.

In BUs and business sites, the Chief of BU or Site Manager serves concurrently as the Information Security Officer. The Officer sets up an information security

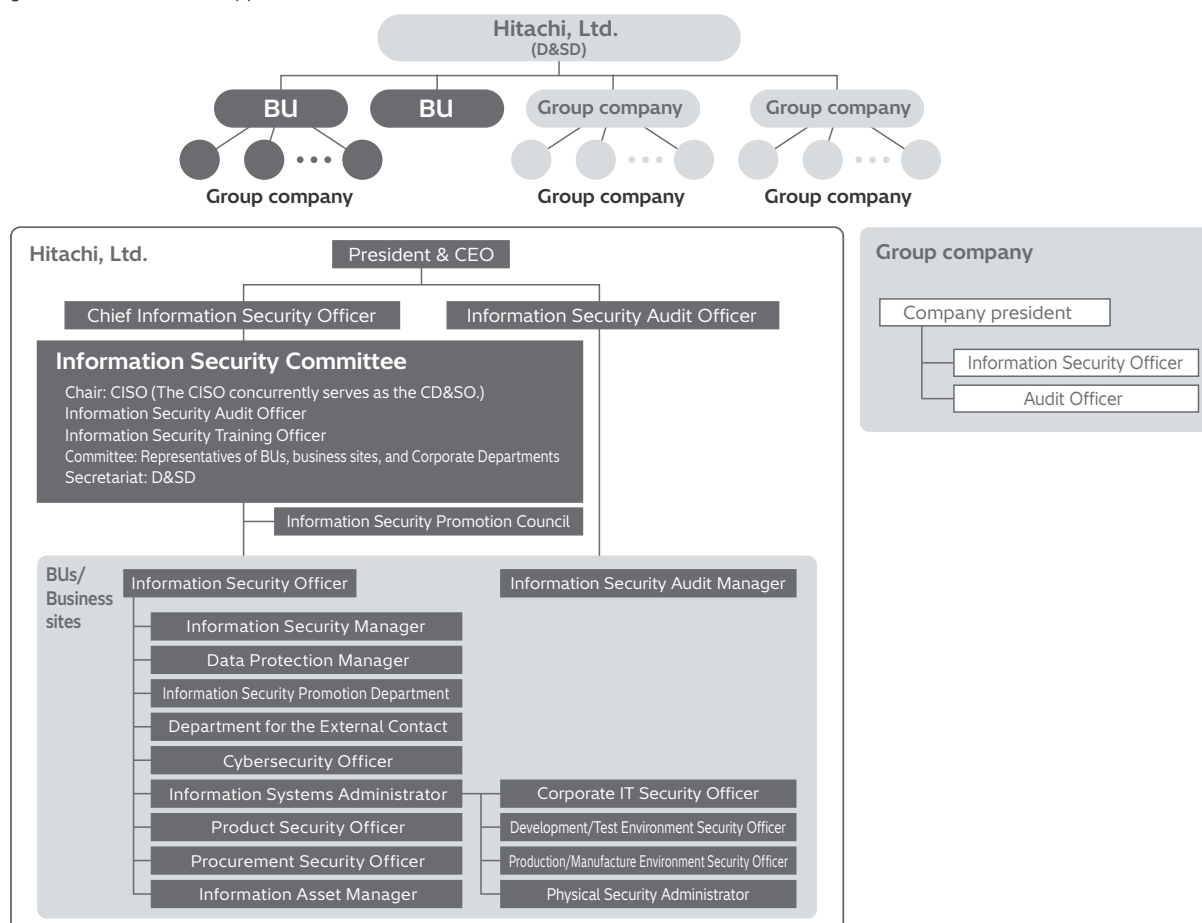
promotion department and appoints an Information Security Manager. The Manager promotes various security initiatives and employee training within the departments and group companies in charge. To address the consistently expanding number of cyberattack targets, the Manager assigns members to oversee physical security measures, such as office access control. They are responsible for the internal IT environment, as well as the development, testing, production, and manufacturing environments. We also appoint Product Security Officer and Procurement Security Officer. They will improve the security of the products and services that we provide for our customers and that of business partners in our supply chain.

To protect personal information, Data Protection Managers are appointed to thoroughly implement various measures related to their areas of responsibility and provide training to employees.

Our group companies organize similar frameworks and work with peer entities to promote cross-functional information security.

(Figure 2-①)

Figure 2-① Information security promotion framework



Information Security Management

Global Framework for Information Security Promotion

As the global business landscape continues to grow, Hitachi is strengthening its global governance by establishing Region Branches as new regional information security units which fully implement security measures. Through the "Information Security Governance Line," a chain of command, we deliver policies, measures, and orders from the D&SD to BUs and group companies. These entities then disseminate the policies, measures, and orders to their overseas subsidiaries.

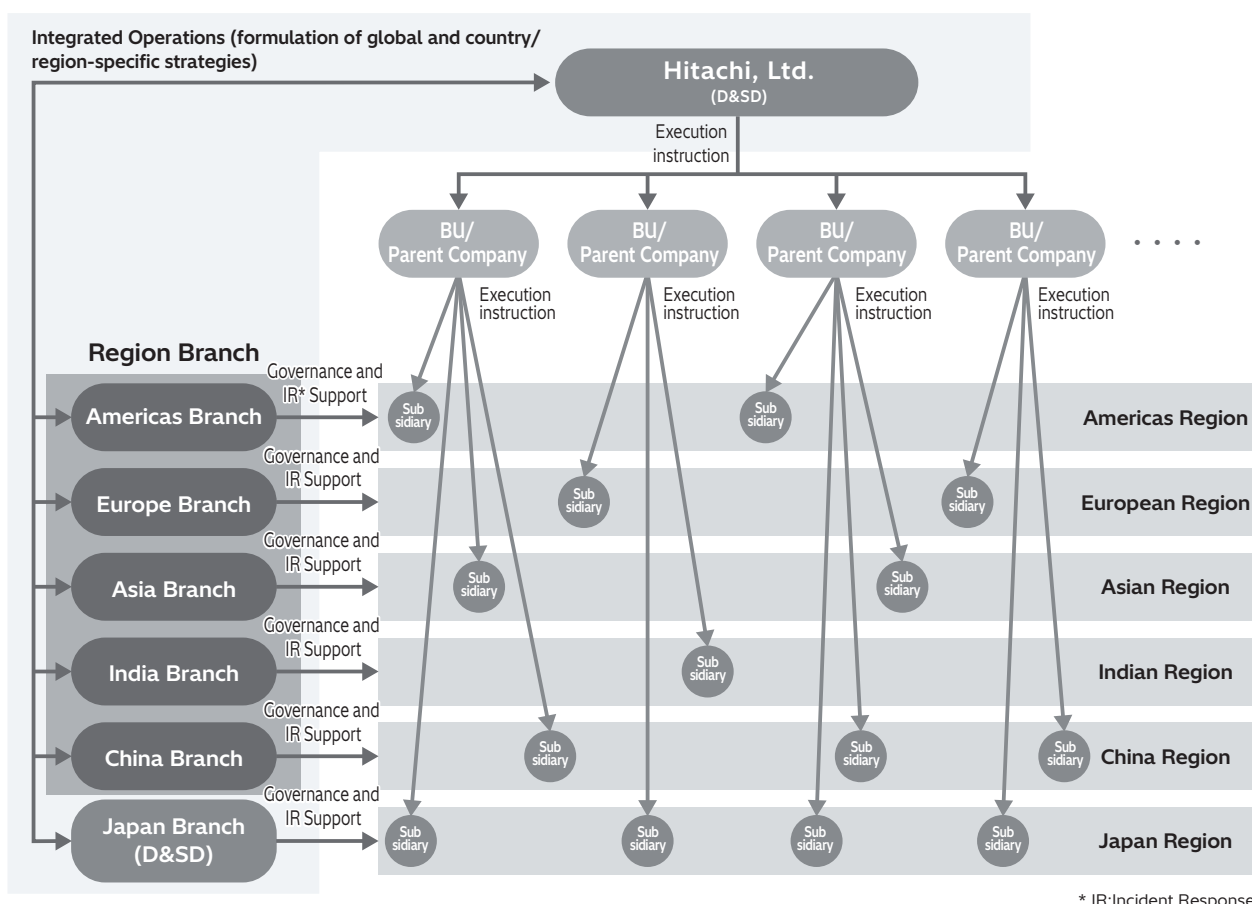
Under the slogan "One Security Team," our goal is to respond promptly to incidents and comply with changing regional laws. As part of this initiative, we have opened Region Branches that cover the

Americas, Europe, Asia, India, and China. These branches enable us to achieve our goals and further embed governance globally.

In addition to this vertical governance line from BUs and parent companies to their group companies, the Region Branches support regional entities horizontally to improve security globally within Hitachi. In Japan, the D&SD serves as the Japan Branch and fulfills a similar role.

Each Region Branch appoints a Head of Cybersecurity to improve communication, incident management, and monitoring management on a day-to-day basis. The goal is to ensure a global response in coordination with other regions in the event of an emergency. (Figure 2-②)

Figure 2-② Framework for Strengthening Governance Through Region Branches



Promotion Framework for Data Protection

To fully comply with applicable personal data protection laws and regulations, a Data Protection Manager has been appointed to each group company in each region. Data

Protection Advisors have been appointed at regional headquarters in the Americas, Europe, Asia, India, and China to support local group companies and promote compliance with laws and regulations in each country and



region.

The President & CEO oversees our information security promotion framework, through which, we manage personal information by implementing all necessary measures. At Hitachi, Ltd.'s BUs and business sites, under the supervision of the Information Security Officer, each

department has an Information Asset Manager, establishing a clear chain of responsibility for the handling of personal information. Similar organizations exist within group companies in Japan, and as a Hitachi Group member, they work to protect and manage personal information.

Systematic Rules for Information Security and Personal Information Protection

As shown in Figure 2-③, Hitachi has established various security rules. Group companies do the same to promote information security.

Fundamental rules

"Information Security Management Rules" stipulate the fundamental requirements for the development, implementation, maintenance, and continuous improvement of an information security management system.

The "Hitachi Group Information Security Policy" is a set of rules that define the information security guidelines described above.

The "Information Security Standards" are globally applicable cybersecurity strategy regulations in accordance with U.S. National Institute of Standards and Technology Special Publications 800 (NIST*1 SP 800 series).

The "Hitachi Group Privacy Principles" establish a common code of conduct for data protection across the Hitachi Group, based on the OECD*2 Privacy Guidelines, which have been adopted as the basis for personal information protection laws and regulations in numerous countries and regions.

The "Personal Information Protection Policy" and "Personal Information Management Rules" set standards

equivalent to the Japanese Industrial Standard "Personal Information Protection Management Systems - Requirements" (JIS Q 15001).

These standards maintain our management level, which exceeds Japan's Personal Information Protection Act requirements.

The "Confidential Information Management Rules" establish procedures for the protection of confidential information.

*1 National Institute of Standards and Technology

*2 The OECD (Organisation for Economic Co-operation and Development) Privacy Guidelines, officially titled Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and first adopted in 1980, establish principles for the international transfer of personal data.

Individual Rules

The "Rules on Website Creation and Information Disclosure" outline the requirements for properly disclosing and using information on websites.

The "Rules for the Management of Entry/Exit and Restricted Areas" establish provisions for ensuring physical security, including rules regarding access to buildings.

Figure 2-③ Rules for Information Security and the Protection of Personal Information

Category	Name of rules, etc
Fundamental rules	Information Security Management Rules
	Hitachi Group Information Security Policy
	Information Security Standards
	Hitachi Group Privacy Principles
	Personal Information Protection Policy
	Personal Information Management Rules
	Confidential Information Management Rules
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

We have developed a framework for running PDCA (Plan-Do-Check-Act) cycles in our information security management as well as personal information management. The information security management cycle consists of four stages. The "plan" stage involves establishing rules and measures. The "do" stage involves implementing these measures. The "check" stage involves monitoring and assessing risks. The "action" stage involves making continuous improvements.

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

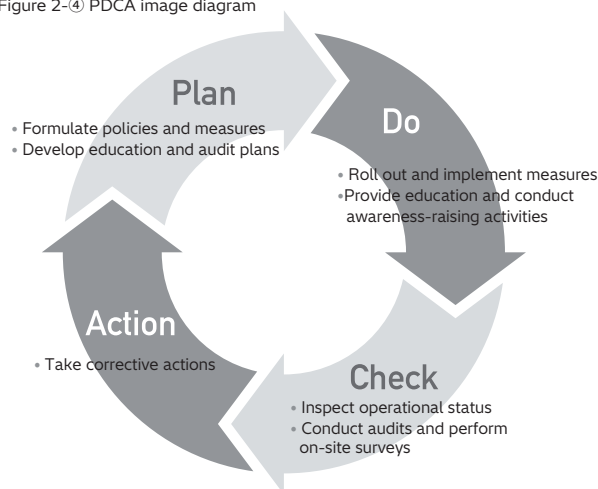
During the [Plan] stage, we establish information security policies and measures, plan information security education, and develop audit plans for safeguarding personal information and ensuring information security.

The measures from the [Plan] stage are rolled out and implemented in the [Do] stage. All employees participate in information security education and awareness activities to understand security measures and raise awareness.

The [Check] stage includes periodic inspections of security operations, audits according to audit plans, and on-site inspections by security experts.

The [Action] stage involves taking corrective action based on the results of audits and on-site investigations. (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

To maintain information security and protect personal and confidential information, all employees must understand the importance of information security and act consciously in their daily business operations.

All Hitachi members, including executives, employees, and temporary staff, receive annual e-learning training on this topic.

In the previous fiscal year, the training participation rate for Hitachi, Ltd. reached 100% (excluding those on leave or otherwise unable to attend). Additionally, the company plans annual training programs on information security and privacy protection. These programs are classroom-based and tailored to specific target groups, including new employees, newly appointed managers, and information security officers. (Figure 2-⑤)

These materials of the company are made available to group companies in Japan and overseas for proactive

training on information security and the protection of personal information throughout the Hitachi Group.

Drill-based Training for Targeted Attack Emails

To respond correctly to the daily occurrence of phishing email cyberattacks, we must all be trained.

All Hitachi employees, including those from its group companies around the world, undergo training on how to respond to targeted attack emails. Trainees receive simulated emails disguised as targeted attacks and learn what suspicious emails look like and how to respond to them. Our goal is to strengthen their adaptability through real-life experience. This is how we transform real-life experience into greater adaptability. The training concludes with an explanation of how to distinguish a suspicious email from others, making the training more effective.



Figure 2-⑤ Information Security Courses, Their Descriptions and Targets

Category	Target	Description
Training for all employees	• All employees • Temporary employees • Employees on inbound secondment	The importance of personal information protection and confidential information management, as well as the latest developments in information security.
Training by level of responsibility	Newly appointed section managers or their equivalents	The essential knowledge that managers need to know about personal information protection, confidential information management, and information security, as well as Hitachi, Ltd.'s initiatives for protecting personal information.
	Newly appointed assistant managers or their equivalents	The essential knowledge that assistant managers need to know about personal information protection, confidential information management, and information security, as well as Hitachi, Ltd.'s initiatives for protecting personal information.
	New employees	Basic knowledge of personal information protection, confidential information management, and information security.
Specialized training	Employees in charge of protecting personal information	The specialized knowledge and practical skills that employees in charge of personal information protection need to know, including internal rules, management systems, and operational procedures.
	Information asset managers	The knowledge necessary to act as the person responsible for managing information assets, including personal information, in each department.

Management Assessment and Monitoring

At Hitachi, we implement our information security and personal information protection management systems based on the PDCA cycle outlined in the Information Security Management Regulations. We regularly audit, assess, and monitor each BU, business site, and group company to verify that they have correctly implemented the management system.

The audit department of Hitachi, Ltd. conducts regular audits of BUs, business sites, and group companies regarding all business operations, including information security.

The specialized team of security experts from the D&SD, BUs, and business sites regularly conducts assessments focusing on information security. The D&SD also assesses external vulnerabilities, such as those in publicly accessible servers, on a quarterly basis for Hitachi, Ltd. and its group companies in Japan.

Regarding personal information protection, the D&SD audits domestic and overseas group companies annually to verify that each Hitachi Group company has established internal rules according to the “Hitachi Group Privacy Principles” and is implementing them. The audits also confirm each company’s compliance status. Hitachi, Ltd. and all its domestic group companies conduct

annual internal audits of personal information protection and information security. The company’s internal audits are conducted independently by the Information Security Audit Officer who is appointed by the President & CEO. To ensure audits are fair and independent, our policy prohibits auditors from auditing their own department. The D&SD verifies the audit results.

During personal information protection and information security audits, we verify the following:

- Compliance with information security rules regarding our management of information assets and information security measures.
- Compliance of the personal information protection management and its operations with the Personal Information Protection Rules.

In addition, all departments at Hitachi, Ltd. conduct self-inspections of their personal information protection practices once a year. Business departments that handle sensitive personal information also verify their operations on a per-task basis monthly, thereby regularly monitoring their operational status.

Information Security Management

Information Security Enhancement

Hitachi is working to improve its information security management. These efforts include managing information assets in normal and emergency situations and ensuring security during company mergers and acquisitions. We also cultivate security talent and strengthen governance of our overseas group companies.

Approach to Information Asset Management

Because information assets are vulnerable to various threats, we protect and manage them appropriately to prevent leakage and unavailability.

■ Operations in Normal Situations

To protect and manage information assets, Hitachi must know which systems contain which information. This belief is reflected in our information asset management under predefined security rules, such as the Procedures for the Management of Confidential Information.

First, system administrators from each BU/business site compile lists of information systems and integrate them with their attack surface management to manage every internet-connected system. The lists include the administrators in charge of each system, as well as the status of internet connections and cloud usage for operational and management purposes. The

administrators periodically take an inventory of the systems' assets to determine whether any customer or personal information is stored.

■ Operations in Emergency Situations

Our information systems may be compromised through unauthorized access or other means. Then, it is crucial to swiftly identify the affected information assets and determine the scope of the breach and its impact. Hitachi thoroughly manages information assets daily, helping to identify affected assets and respond to incidents quickly.

Security Assurance During Mergers and Acquisition

As Hitachi actively pursues mergers and acquisitions (M&As), it strengthens information security governance within newly acquired Hitachi Group companies to minimize security risks.

M&As create new value by integrating companies with different corporate cultures. Conversely, we must minimize the information security risks posed by integrated policies and systems. Early in the M&A process, we ask the target company to familiarize themselves with Hitachi's rules, and importantly, to conduct controls and governance based on Hitachi policies.

We assess security risks from an M&A before and after signing a contract. (Figure 2-⑥)

① Before the contract is signed (Day 0): "Information Security Risk Assessment"

Study publicly available information or that which is

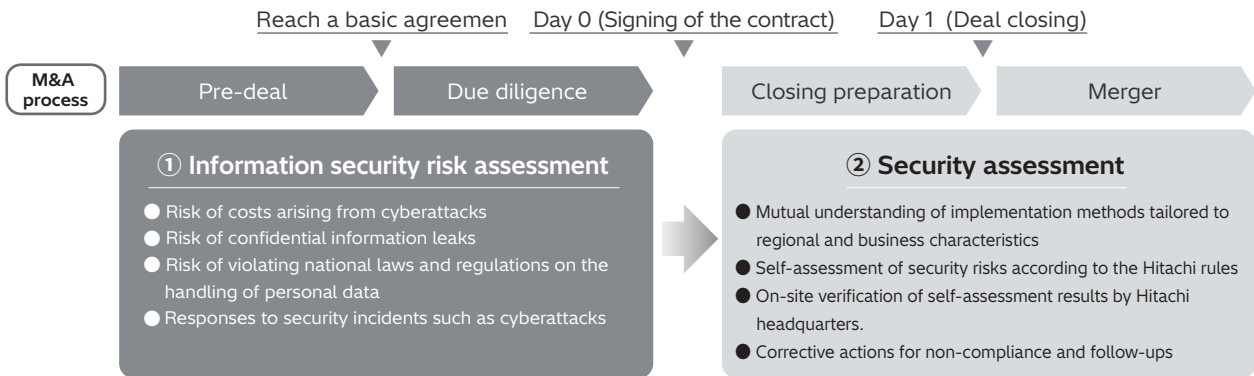
provided by the target company in advance to find information security risks. This covers their ongoing organization, framework, and rules for information security; their business characteristics; their compliance status with local legal systems; and their history of cybersecurity incidents and how they were handled.

② Post-Day 0: "Security Assessment"

Select the locations to be assessed based on the conditions in which the acquired company operates and its business characteristics. Ask the target company to conduct a self-assessment using Hitachi's risk assessment standard. Against the assessment results, the D&SD conducts an on-site inspection. If any issues are found, the D&SD will plan corrections and provide follow-up support until they are completed.



Figure 2-⑥ Information security risk assessment and security assessment



Approaches for Security Talent Development

In recent years, cyberattacks have intensified. While enhancing its internal security, the entire Hitachi Group is committed to developing security personnel to provide our customers with secure products and services.

Approaches to Security Talent Training

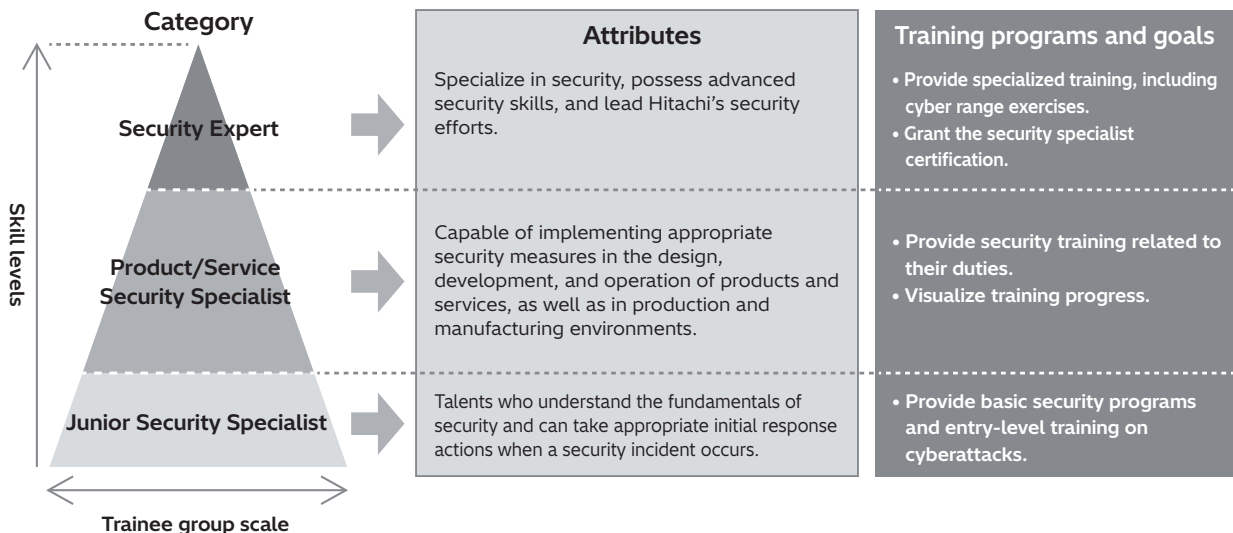
As shown in Figure 2-⑦, Hitachi's cybersecurity personnel fall into one of three categories: Security Experts, Product and Service Security Specialists, and Junior Security Specialists. We have developed specialized programs for each group and effectively train them to achieve their respective goals.

Security Experts

For security experts, we provide high-level training, including cyber range exercises and a community site for

information sharing and collaboration. These experts are recognized as Hitachi Certified Information Security Specialist (HISSP) within the Hitachi Certified IT Professional Certification that conforms to the Certified IT Professional certification framework of the Information Processing Society of Japan. We search for candidates with the necessary security skills and professional backgrounds. Then, we educate and evaluate them for this certification.

Figure 2-⑦ Three categories of cybersecurity personnel with their own training objectives



Information Security Management



■ Product/Service Security Specialists

Product/Service Security Specialists are responsible for ensuring the security of the products and services they provide. They are trained to ensure the security of the environment for the design, development, operation, and maintenance of products and services. It is also important to train security specialists who have an in-depth understanding of the security measures outlined in company rules for specific production and manufacturing workplaces. Both the design/development and production/manufacturing worksites of products and services must ensure safety and prevent adverse effects on one another. To this end, Hitachi is working to develop the IT and OT skills of its personnel. We also foster PSIRT* members, as well as security risk assessors and security system architects, who are responsible for enhancing the

security of products and services.

*PSIRT (Product Security Incident Readiness/Response Team)

■ Junior Security Specialist

Junior Security Specialists are trained to promote security awareness and improve security measures at Hitachi. Many on-site colleagues are eligible for this certification. Trainees will learn the fundamentals of security and how to initially respond to security incidents, such as cyberattacks. We provide the “Basic Knowledge e-learning Program for Cybersecurity Countermeasures” and the “Communication Training for Cybersecurity Response.” For those who require further introductory training, e-learning programs on basic security knowledge are available.

Global Activities to Enhance Governance

Region Branches hold security conferences and workshops for security managers and staff from Hitachi Group companies worldwide. Participants will have a better understanding of Hitachi’s overall strategy and receive practical support for their security measures. Through these activities, we build local communities and promote communication across regions. The widely distributed security newsletters help raise awareness and consciousness.

The Branches are also committed to incident management by regularly sharing intelligence and incident information with each other. This increases resilience and helps work with relevant units to minimize risks during emergencies. Through these activities, Region Branches ensure to promote basic measures globally. (Figure 2-⑧)

Figure 2-⑧ Main activities at Region Branches

Main activities at Region Branches
Hold security conferences to deepen understanding of Hitachi’s overall strategies and initiatives.
Organize workshops tailored to specific security measures.
Build regional security communities and encourage cross-regional communication.
Raise security awareness through security newsletters, etc.
Make security awareness activities “Jibungoto-ka” (view them as your own responsibility)
Participate in external conferences to stay up to date on the latest movements.
Share intelligence and incident information to build resilience in emergencies.
Support incident response by coordinating with related teams during emergencies.

Cybersecurity Initiatives



Diverse cyberattack methods increase entry points and the severity of incidents. To address these situations, Hitachi established the Cyber Security Incident Readiness/Response Teams (CSIRTs) to manage cybersecurity in specific environments against cyberattacks and various incidents while supporting others.

Cybersecurity Management

Our security risk management focused on the internal IT systems for OA usage. To minimize operational risks, we have expanded the scope to include the development, testing, production, and manufacturing environments. We also cover supply chain and development processes for products and services.

Approaches to Enhancing Cybersecurity Measures

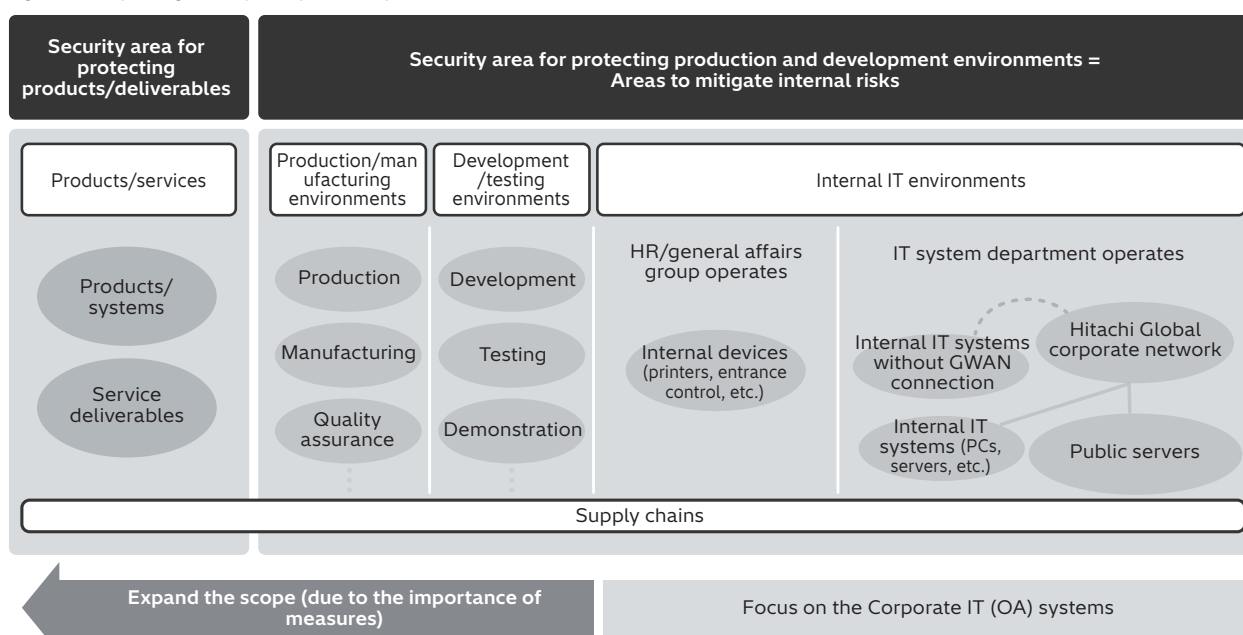
IT is essential for production, manufacturing, development, and testing at work sites. In addition to cybersecurity measures for conventional internal IT systems, we need them for attacks on products, services, and supply chains. (Figure 2-⑨)

Given this, Hitachi is reinforcing its cybersecurity measures, including environments for internal IT, production, manufacturing, development, and testing, as well as process controls for products, services, and the supply chain. This involves various initiatives. (Figure 2-⑩)

Based on the Three Defense Lines (3DL) concept adopted in 2023, we are developing security measures for production, manufacturing, development, and testing environments, as well as for product and service processes.

The 1st Defense Line involves self-assessment by BUs and group companies of the guidelines and management policies. In the 2nd Defense Line that follows, the D&SD monitors their progress of the 1st Defense Line. Lastly, the audit department at headquarters verifies the D&SD's monitoring results as the 3rd Defense Line.

Figure 2-⑨ Expanding the scope of cybersecurity measures



Cybersecurity Initiatives

Security Enhancement in Internal IT Environments

We establish standards for vulnerability measures and network security to safeguard the IT systems used in offices, including networks, IT devices, and information systems. BUs/group companies are asked to regularly verify their status against the standards

and correct any issues. As part of a company-wide initiative, we have begun monitoring the status of vulnerability measures for each device and following up with users and administrators in broader areas.

Security Enhancement in Development and Testing Environments

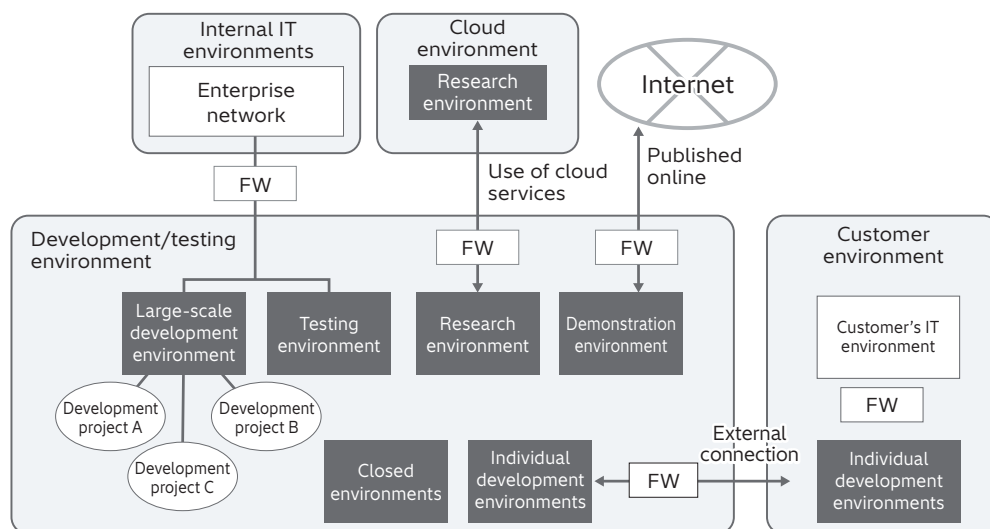
Development and testing environments are divided by purpose, such as development, testing, research, and demonstration, as well as by usage, such as customer sites, internet connectivity, and cloud services. In the Hitachi Group, we develop security guidelines for each environment, even those with

diverse requirements, to build and connect them securely. Due to the use of the cloud and remote working, our development style is changing. Therefore, we regularly update the guidelines and improve security levels. (Figure 2-⑪)

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

Area	Target unit	overview
Internal IT	IT	• Develop and implement requirements for connecting to or disconnecting from Internal IT environments.
Development/testing	Design/development	• Develop and implement guidelines for creating secure environments connected to Internal IT systems.
Production/manufacturing	Production/manufacturing	• Develop and implement guidelines for production and manufacturing environments based on the IEC 62443 standard for protecting control systems from cyberattacks.
Products/services	Quality assurance for design and development	• Develop management policies to maintain the security level of products and services. • Develop and implement process requirements for product design, development, and maintenance.
Supply chains	Procurement	• Develop security requirements for business partners and evaluate their status using an evaluation process.

Figure 2-⑪ Security network in development/testing environments



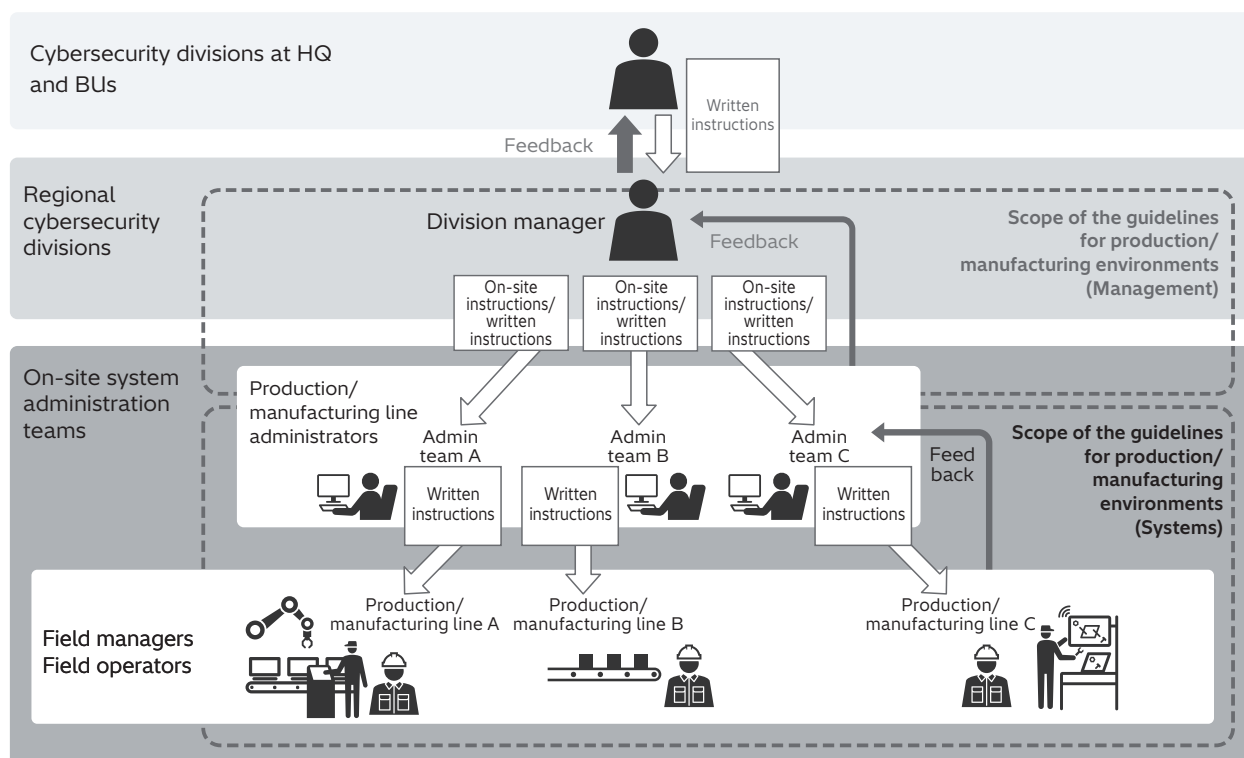
Security Enhancement in Production/Manufacturing Environments

The manufacturing and production environments must not affect the internal IT and development environments, and vice versa. We build and operate our environments according to Hitachi Group guidelines to ensure this. (Figure 2-12) At our production and manufacturing sites, we raise security awareness through educational materials such as posters on the walls and rulebooks available to all personnel. (Figure 2-13)

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



Figure 2-12 Guidelines for production/manufacturing environments and their implementation



Guideline structure	Description	Intended audience
Management part	Serves to formulate and revise security operation and management rules for an entire site and specific departments from a managerial perspective involving organizational and human resource management.	Cybersecurity chief officer
System part	Serves as a representative model for the Hitachi Group, outlining the system configuration and mitigation measures based on "IEC 62443-3-3" to assess the status and consider countermeasures. Intended to be customized and used by each department and division.	Production/manufacturing line administrators Field managers Field operators

Cybersecurity Initiatives

Security Enhancement in Supply Chains

We expect our outsourced procurement partners to take security precautions regarding Hitachi's information assets. Thus, we present them with our "Information Security Guidelines," which clearly outline the supply chain security requirements. We expect our partners to implement the same level of security measures as Hitachi and to uphold them through regular monitoring and verification. (Figure 2-14)

Furthermore, to encourage partners to implement information security measures, we present case studies of cyberattacks to their management teams,

emphasizing the importance of supply chain security and explaining our security requirements.

Figure 2-14 Framework for enhancing supply chain security

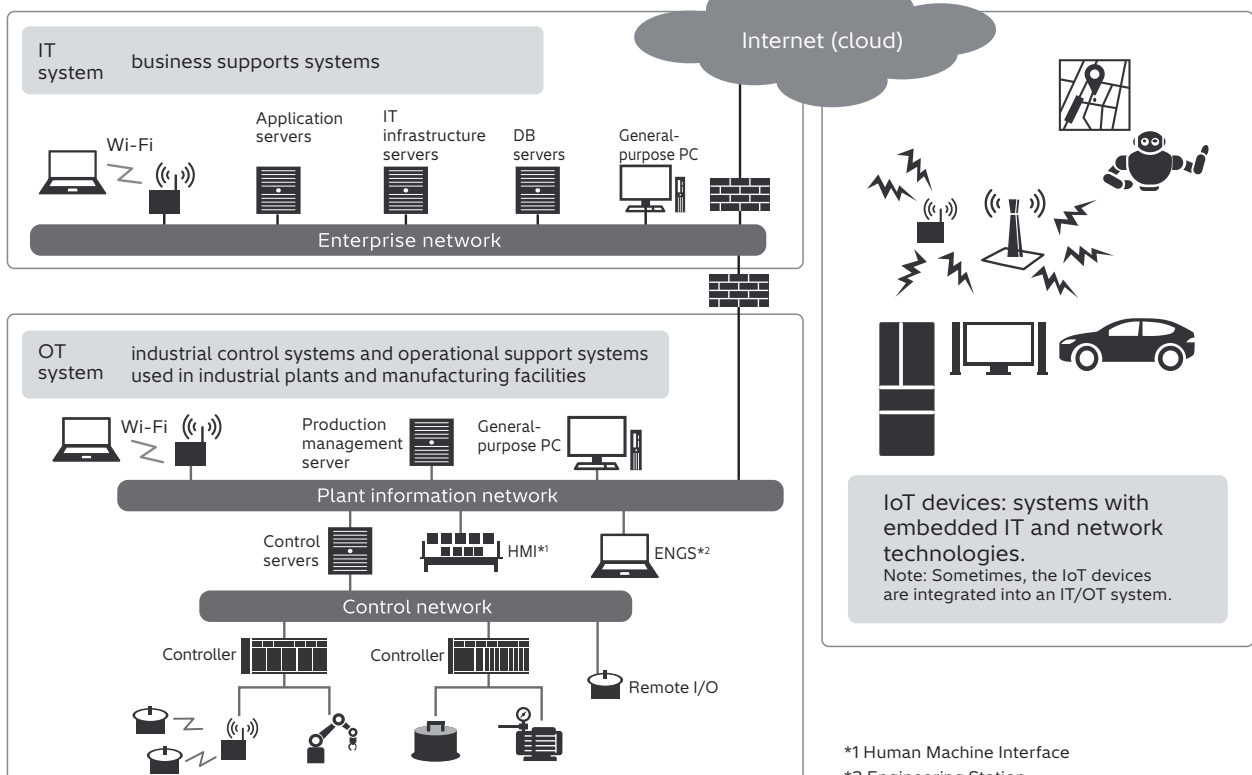


Security Enhancement in Products and Services

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 are becoming more important

than ever. The Hitachi Group protects our customers' assets and critical infrastructure from cyberattacks by offering IT, OT, and IoT products and services. (Figure 2-15)

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



■ Security Management Policy for Products and Services

To unify our security management policies for Hitachi Group's wide variety of products and services, we have established the "Security Management Policy for Products and Services" and related materials as quality assurance guidelines. (Figure 2-16)

This policy is incorporated into the security management policies of all departments, which carry out secure processes throughout the lifecycle of products and services in development, manufacturing, maintenance, and operations. (Figure 2-17)

■ Provision of the Guidelines and Supports

We have various reference materials, including the "Secure Process Implementation Guide," to help each department formulate its own security management rules. These materials present case studies of proactive security measures, allowing us to accumulate and share knowledge on implementing processes during the design, manufacturing, operation, maintenance, and security incident handling phases across the entire Hitachi Group.

While sharing these materials on the Internet, we help each department develop its own secure

development process.

■ Security Management Framework and PSIRT for Products and Services

To provide safe and secure products and services that meet the Security Management Policy, a Product Security Officer is appointed at each BU and group company to oversee the security management framework. Within the company-wide security framework, the D&SD, BUs, and group companies collaborate to establish PSIRTs for emergency response preparation. Together with the relevant parties, the PSIRTs address the technical aspects of security issues, vulnerabilities, and incidents affecting products and services.

The PSIRTs hold regular liaison meetings where the D&SD presents measures and technical information to the BUs/group companies. Participants also share case studies of their activities with each other. The D&SD supports PSIRT members in promoting their activities within their respective BUs and group companies through incident response training and other initiatives.

Figure 2-16 Security management guidelines for products and services

Documents for standards, etc.	Overview
Security Management Policy for Products and Services	Guidelines aimed at standardizing the approach to security management for products and services (hereinafter, "Products") within the Hitachi Group.
Requirements for each process in product development and maintenance	Requirements for product development and maintenance processes. These are translated into practical tasks and necessary checklists based on the nature of the products.
Product security inspection checklist	An inspection checklist to verify that the product development and maintenance processes within one's own department comply with the guidelines and requirements.

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/requirements definition/basic design	2-1. Change management	3-1. Incidents detected internally
1-2. Configuration management	2-2. Vulnerability information gathering	3-2. Incidents discovered externally
1-3. Design/production	2-3. Preventive maintenance	3-3. Regular drills
1-4. Procurement (including OSS)	2-4. Regular vulnerability inspections	
1-5. Testing/evaluation	2-5. Notifying customers of vulnerabilities and mitigation measures	
1-6. Inspection		

Cybersecurity Initiatives

Cybersecurity Countermeasures

To address cyberattacks and other security incidents, Hitachi has a unit called the Security Operations Center (SOC). It proactively improves security monitoring and incident response, as well as collects, analyzes, and distributes threat information to increase vigilance.

Improve Security Monitoring and Incident Response

Regardless of size, all participants in supply chains are at an increasing risk of complex and sophisticated cyberattacks, including targeted attacks, ransomware attacks, and system vulnerability attacks. Additionally, the misuse of AI is making cyberattacks more sophisticated and widespread than ever before. To confront these attacks, it is essential to detect threats and prevent further damage as early as possible. The Hitachi Security Operations Center (SOC) plays a key internal role at Hitachi in monitoring security threats and responding to incidents. Operating 24/7, the SOC swiftly handles incidents from initial response to mitigation, thereby minimizing the damage caused by cyberattacks. We are also improving our global response capabilities through cooperation with the members in Europe and the Americas.

■ Cybersecurity Monitoring

Hitachi establishes monitoring points for systems and networks. These points cover all core locations worldwide where logs are collected and analyzed. Endpoint Detection and Response (EDR) closely monitors endpoints and authentication systems. This allows us to detect and respond to attacks targeting

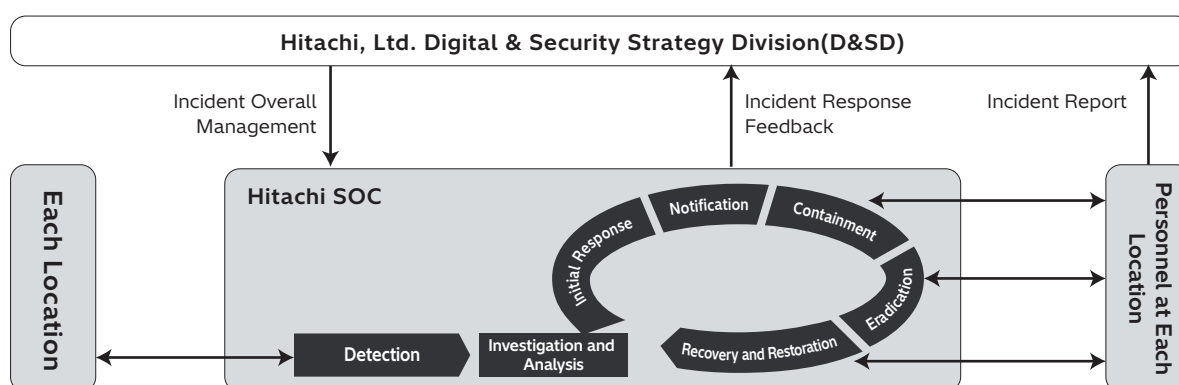
them early and promptly. This is how we are transitioning from traditional, perimeter-based security monitoring to zero-trust security monitoring.

■ Incident Response

Hitachi's response procedures and communication system allow us to quickly identify the cause and scope of an incident's impact and act from containment to eradication and recovery. At Hitachi SOC, we combine threat intelligence with investigations based on log monitoring at core sites, EDR, and authentication system monitoring to quickly capture the details of any incident. This also reduces the time needed for triage and determining response priorities. Furthermore, AI-powered Security Orchestration, Automation, and Response (SOAR) technology automates incident response processes, including triage, investigation, and containment. This leads to quick and accurate action.

Furthermore, we apply the insights gained from incident response to security monitoring and various internal measures to prevent similar incidents. (Figure 2-18)

Figure 2-18 Security monitoring and incident response





Collect and Analyze Threat Information for Alert Distribution

To ensure the security of its internal information systems, products, and services, Hitachi, Ltd. collects and analyzes threat information and issues alerts. These activities provide insights that are shared with the CISO and discussed by senior management as part of formulating the Hitachi Group's security strategy.

■ Collect, Analyze, and Verify Threat Information

In addition to publicly available vulnerability and threat information, we collect threat information in Japan and abroad using various Cyber Threat Intelligence (CTI) sources.

The collected information is classified and organized based on metrics such as severity levels, Common Vulnerability Scoring System (CVSS) scores, and exploitation status, as well as the probability of a successful attack and its potential impact on our internal systems. We also study the potential impact and damage of certain threats in simulated environments to improve measures.

Furthermore, legal systems related to security rapidly change in various countries and regions. The Hitachi Group collects and classifies this type of information to better manage risks.

■ Issue Alerts and Execute All Measures

We deliver collected information to cybersecurity officers of BUs and group companies through immediate alerts, weekly digest emails, and intranet postings. For major threats affecting the entire Hitachi Group, we issue a Cyber BCP directive or a Cyber Alert, which has the power to enforce the execution of the measure.

This information is also used for joint initiatives with Hitachi's SOC and IT system departments. These initiatives involve threat hunting, incident response, and monitoring enhancement.

■ Transform Information into Strategic Intelligence

We analyze the current situation and areas for improvement within the Hitachi Group based on

threat information gathered and studied, as well as alerts issued. The findings, shared with the CISO, the D&SD, and the regional branches, are reflected in the security strategy of the Hitachi Group. This is how we execute security measures quickly within the Hitachi Group.

■ Respond to External Attacks

Public systems connected to the internet are constantly at risk of external attacks. Every day, we learn about new vulnerabilities that attackers exploit to gain unauthorized access, steal confidential information, and infect targets with malware. Attacks on zero-day vulnerabilities are also on the rise. These attacks occur before a mitigation strategy is available.

To respond quickly to these vulnerabilities, we use Attack Surface Management (ASM) tools to manage the latest status of externally exposed devices. When a device is found to pose a risk, we immediately send a Cyber Alert to the relevant departments, asking them to confirm and mitigate the risk immediately. This is how we minimize the risk of external attacks and speed up the response process.

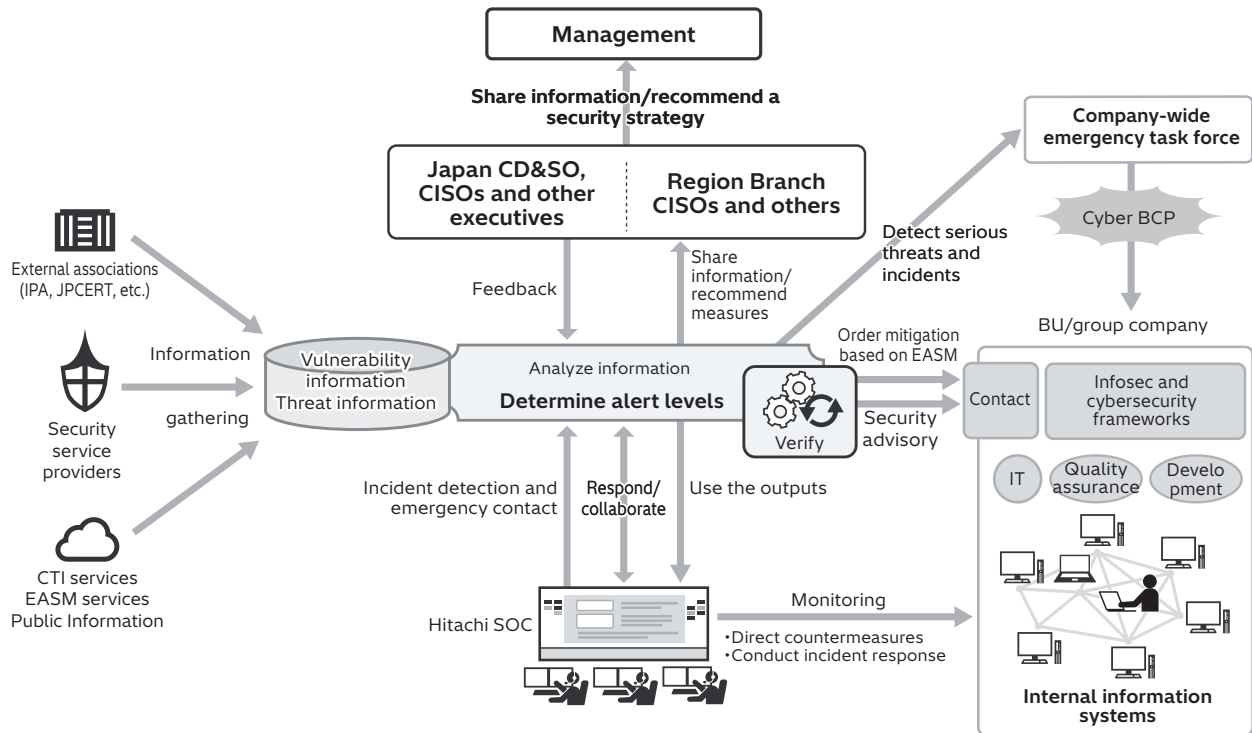
We use insights from ASM to monitor for signs of leaks of confidential information and account credentials from the Hitachi Group. If any signs are detected, our joint action with the relevant departments enables us to respond promptly to threats and prevent damage before it occurs.

■ Handle Emergency Situations

In the case of a threat that could severely impact business operations at numerous Hitachi sites or compromise business operations company-wide, we will launch a task force and implement security countermeasures across the company, including activating the cyber BCP. (Figure 2-¹⁹)

Cybersecurity Initiatives

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





SIRT Activities

Hitachi has established the Hitachi Incident Response Team (HIRT) as a “Cyber Security Incident Readiness/Response Team (CSIRT)” as well as a “Product Security Incident Readiness/Response Team (PSIRT).” The aim is to promote cybersecurity measures. The HIRT prevents security incidents involving Hitachi's products, services, and internal infrastructure, and responds swiftly if an incident occurs. These efforts help create a safe and secure network environment for our customers and society.

HIRT's Concept and Definition

The HIRT is not a single organization, but rather a “collection of functions” that drives cybersecurity initiatives across the Hitachi Group. By addressing issues through cross-organizational and international collaboration, the HIRT contributes to the realization of a safe and secure network environment for the Hitachi Group, its customers and society at large. HIRT drives “incident operations” through the following three approaches:

- Readiness (prevention): We routinely collect and organize vulnerability information, as well as

strengthen development and testing environments to proactively prevent incidents.

- Response (technical response): When an incident occurs, we promptly investigate and analyze it, making technical adjustments to prevent and resolve damage caused by cyberattacks.
- Resilience (greater flexibility and resilience): Based on threat intelligence analysis, we consistently make improvements to enhance our ability to recover and continue operations in the event of an attack. This strengthens our resilience.

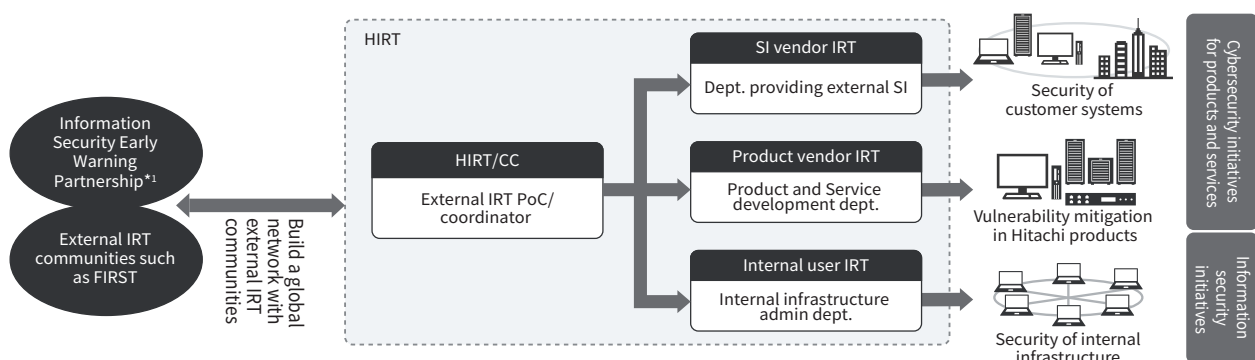
Promotion Framework for HIRT Activities

The Four IRT(Incident Readiness/Response Team) Models

In the HIRT, the HIRT Coordination Center(HIRT/CC) Hub serves as the coordinator and point of contact (PoC) for each IRT to promote vulnerability

management and incident response. Adopting a collaboration model among the internal IRTs ensures the security of our products, services, and internal infrastructure. (Figure 2-²⁰)

Figure 2-²⁰ Four IRTs supporting vulnerability management and incident response activities



*1 An officially regulated public-private partnership framework that aims to smoothly distribute vulnerability information for software products and websites and to promote the countermeasures.

Category	Roles and areas of responsibility
1. Coordination Center (HIRT/CC)	[Overall coordination and PoC functions] Oversees vulnerability measures and incident response activities across the entire Hitachi Group by serving as the PoC for external IRTs, including the Forum of Incident Response and Security Teams (FIRST) and the Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC), as well as coordinating and consolidating efforts among the various internal IRTs.
2. SI vendor IRT	[Protection of customers' systems] The SI services departments are in charge. They use public vulnerability information to provide support for security measures and incident response to ensure the security of their customers' systems.
3. Product vendor IRT	[Product security] The Product and Service Development Departments are in charge. This IRT provides support for vulnerability mitigation, such as investigating the impact of vulnerabilities on Hitachi products. It also provides information on mitigation and requests for and management of Common Vulnerabilities and Exposures (CVE) identifiers.
4. Internal User IRT	[Protection of internal infrastructure] The internal infrastructure administration teams are in charge. This IRT addresses vulnerabilities in the internal infrastructure and responds to incidents to prevent the internal IT environment from being used as a base for cyberattacks.

Cybersecurity Initiatives

Decentralized, Autonomous Governance Structure

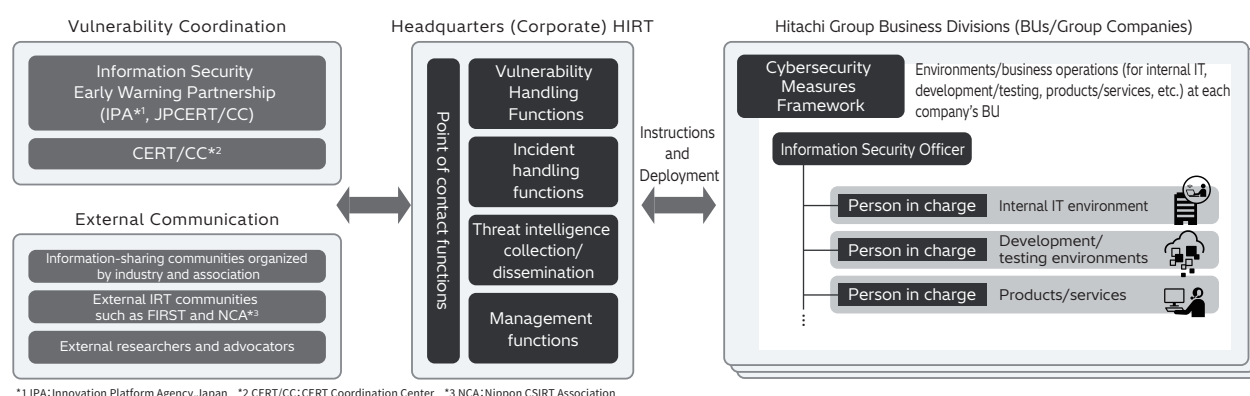
The HIRT's governance involves the entire Hitachi Group and has a hierarchical IRT structure. In this decentralized, autonomous governance framework, the headquarters' D&SD does not oversee everything. Instead, the heads of each business unit and group company are responsible for developing and implementing their own cybersecurity measures. (Figure 2-②)

- **Headquarters (Corporate):** Coordinates with external CSIRT organizations and other entities (as

the PoC). Its management roles include handling vulnerabilities and incidents, as well as collecting and disseminating threat intelligence.

- **Cybersecurity measures by BUs and group companies:** Cybersecurity officers are appointed as the PoC for each BU and group company. They are responsible for planning, maintaining, and implementing security measures in both normal and emergency situations. This includes internal IT environments, development and testing environments, and products and services.

Figure 2-② Governance framework for HIRT activities



Activities by the HIRT

The HIRT serves as an internal IRT and the PoC for external IRTs. Its internal activities include developing policies and technical measures in collaboration with the D&SD, which leads policy development, and the quality assurance division. The HIRT also assists each BU and group company with their vulnerability mitigation and incident response. On the other hand, the HIRT is responsible for PoC functions related to cybersecurity measures with external IRTs.

Internal IRT Activities

Hitachi has acquired insight through the collection and analysis of security information. This knowledge is shared internally in the form of security alerts and advisories. It is also incorporated into various guidelines and support tools for the development of Hitachi's products and services.

(1) Collecting, analyzing, and disseminating security information

The HIRT disseminates information and expertise related to vulnerability mitigation and incident response, which was gained through "the Information Security Early Warning Partnership" and other activities.

(2) Improving security technology for products and services

To improve overall IRT capabilities, the HIRT implements security measures for information and products related to control systems. In June 2022, HIRT registered with the CVE*1 Numbering Authority (CNA) program. In this program, HIRT assigns CVE identifiers to vulnerabilities in Hitachi products and publishes them as CVE records. This allows us to deliver our products with confidence through these activities to our customers.

*1 CVE: Common Vulnerabilities and Exposures.

(3) Performing sectoral IRT activities

To translate background and sectoral trends into concrete measures, we form IRT teams specific to



each area. For example, the HIRT-FIS*² is specific to the financial sector.

*2 HIRT-FIS: Financial Industry Information Systems HIRT

■ IRT Activities among Teams

Multiple IRTs work together to build cooperative relationships that facilitate addressing new threats and improving each other's activities.

(1) Closer Collaboration in IRT Activities in Japan

We are building a collaborative network by leveraging the Nippon CSIRT Association's (NCA) activities. This includes notifying the PoCs of other NCA members of the vulnerabilities and incident information that we have collected. We also support the information-sharing infrastructure based on the Japan Vulnerability Notes (JVN), a vulnerability

information portal site, operated jointly by the Japan Computer Emergency Response Team/Coordination Center (JPCERT/CC) and the Innovation Platform Agency, Japan (IPA).

(2) Closer Collaboration in IRT Activities in the World

Our FIRST initiatives promote Vulnerability Reporting and Data eXchange (VRDX) activities. These initiatives include establishing a framework for global collaboration with IRTs, including those of product vendors, and standardizing the format for exchanging vulnerability response information.

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

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

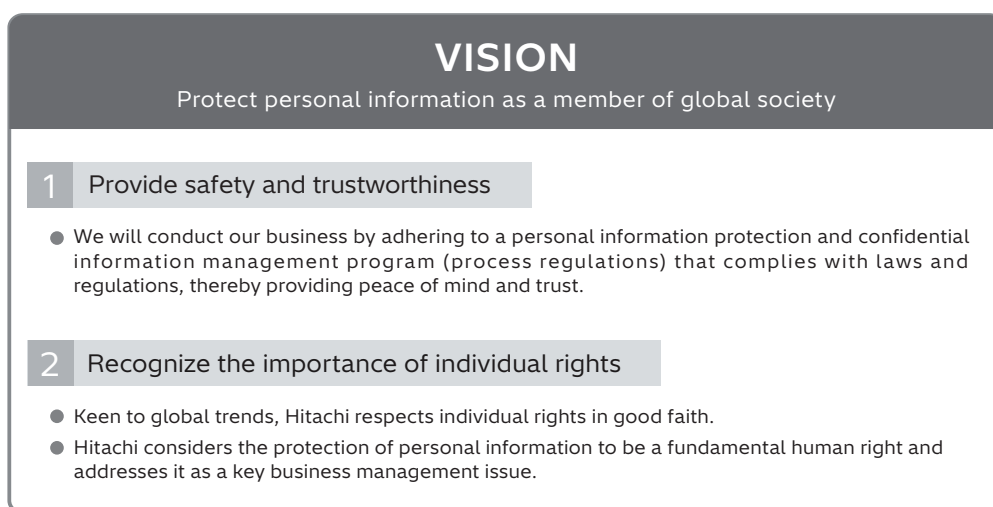
positioned personal information protection as a key issue in its business and is making steady progress towards achieving its vision. (Figure 2-22)

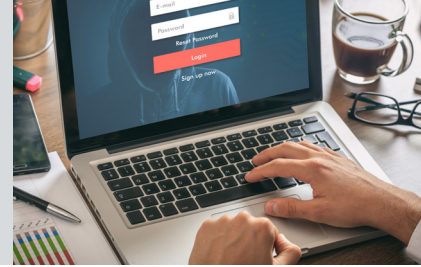
Personal Information Protection Framework

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





■ 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/>)

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.

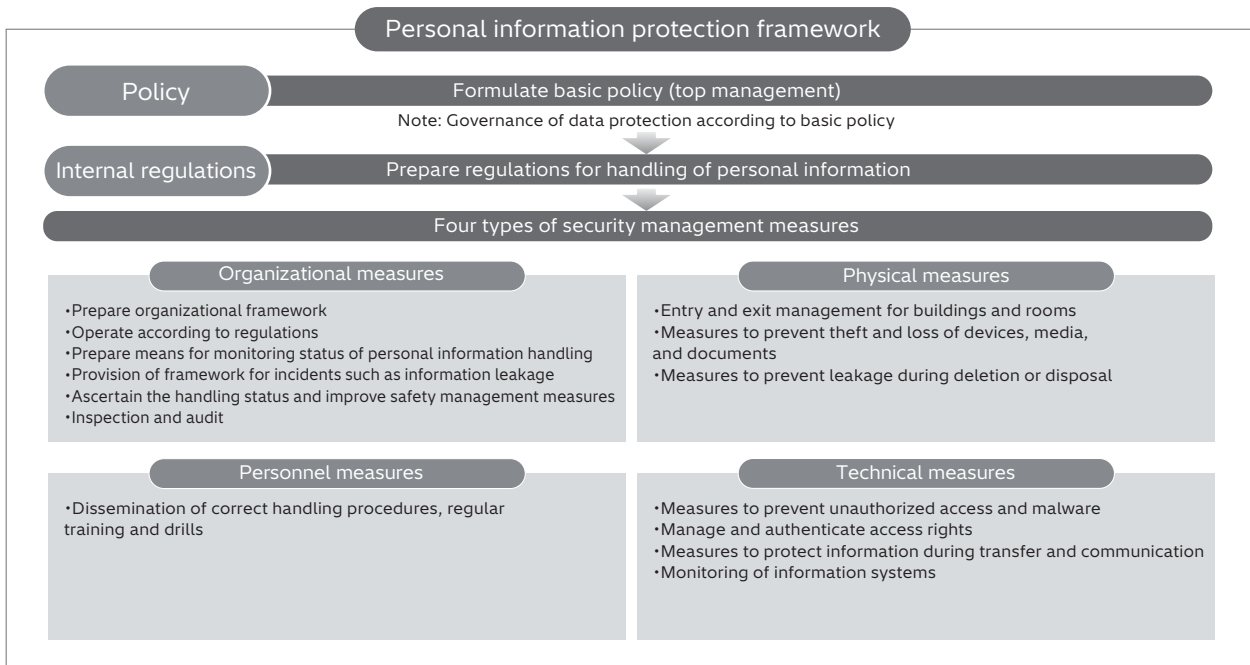
(4) Compliance with laws and norms

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.

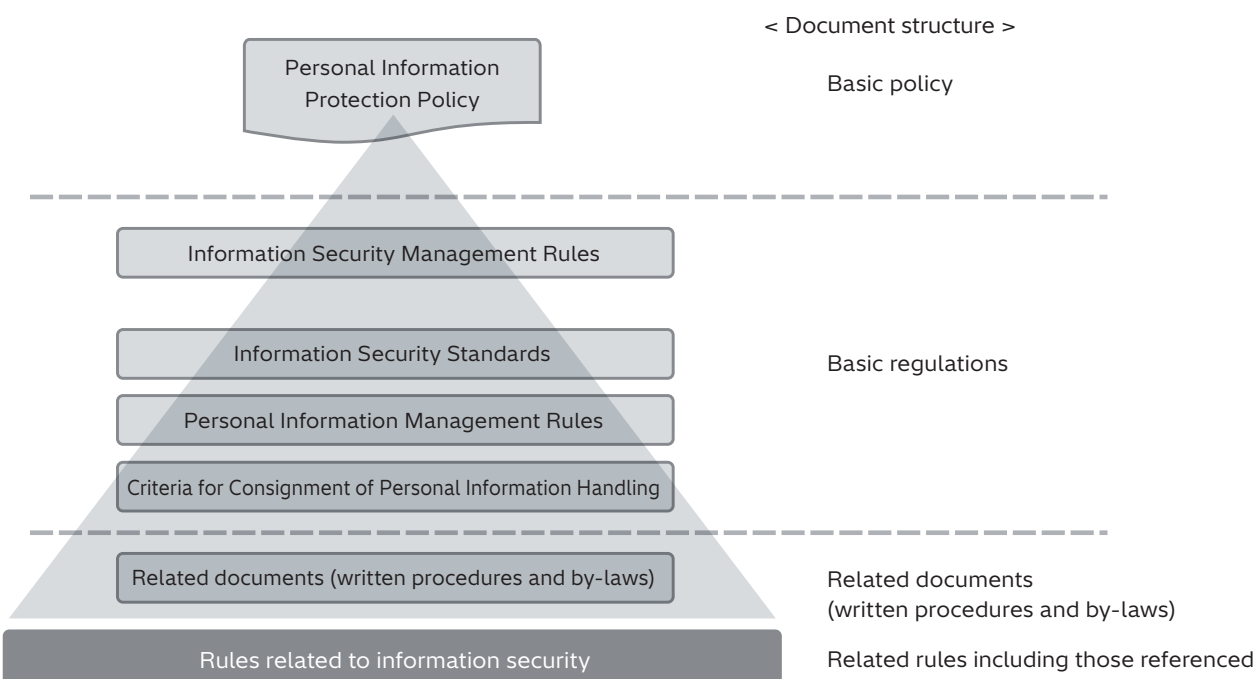
Personal Information Protection Management System

Hitachi's personal information protection management system was established based on JIS Q 15001. Hitachi's "Personal Information Protection Policy" defines its policy regarding the protection of personal information.

Rules for personal information protection management are set forth in the "Information Security Management

Rules," which consist of 52 articles. The handling of personal information is set forth in the 73-article "Personal Information Management Rules," the 12-article "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 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.

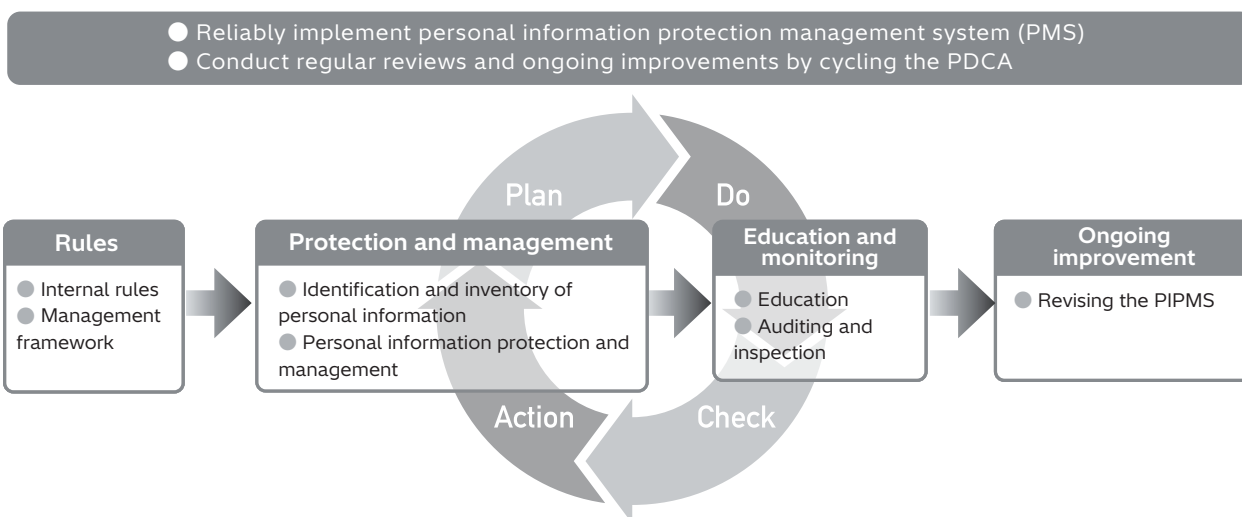
We define "personal information handling" as the process of identifying and analyzing risks specific to business

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 through 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 Contractor Management

Hitachi was quick to take steps to improve its management of contractors performing its outsourced operations involving personal information. Through these initiatives, we developed internal rules for contractors handling personal information to ensure compliance. When outsourcing business operations, Hitachi screens contractor candidates and selects only those that protect personal information to a level equal to or higher than its own standards. All contractors are bound by strict contracts that require them to establish a management structure and prohibit subcontracting. Furthermore, we regularly inspect the contractors' sites to encourage them 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 2026, 38 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 (as of September 2026)



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 2026, 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.
Hitachi High-Tech Corporation

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.

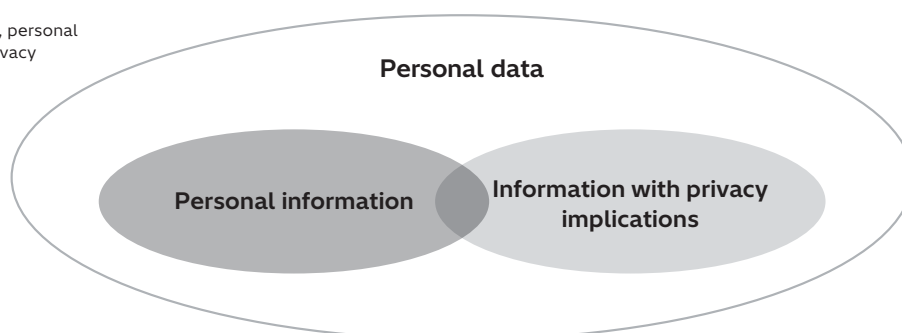
In response to requests from society to protect our privacy, Hitachi introduces the Hitachi Privacy Impact Assessment (PIA) System and evaluates the impact of handling personal data. This initiative aims to balance privacy protection with the use of personal data to improve the quality and suitability 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 cyber attacks, Hitachi is working to establish a system that enables collaboration between our internal security department and other departments. We also participate actively in external activities, to enable collaborative creation with others in industry, government, and academia.

Internal Activity Related to Information Security

Because cyber attacks target a wide range of business activities, collaboration with various departments within the company is essential even during normal times. To that end, we have established subcommittees organized by theme, such as product security, supply chain security, confidential information management, security technology information, and web security, in collaboration with the respective departments responsible for quality assurance, procurement, intellectual property management, research and development, and Web management.

Through these activities, we are building a system for the timely exchange of information among us, to ensure effective security measures. Furthermore, in the unlikely event that an incident occurs, we must respond appropriately to each stakeholder, and work in collaboration with the Sales, PR, Legal, Procurement, and Human Resources Departments to move forward. To ensure a swift response in the event of an emergency, we have established contact points in each relevant department and provide information on security measures.

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) Industrial-process Measurement and Control Committee
- 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

■ Activities with the Japan Network Security Association The Contribution of Games to Information Security Education

Hitachi, Ltd. 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 those efforts, we participate in and contribute to the Game Education Working Group of the JNSA Education Committee. This working group conducts surveys, research, and planning related to the use of games to promote information security awareness and practical security education.

In FY2025, as part of this working group's activities, we planned and produced a new educational resource called "CoRepo" in collaboration with members from each member company. CoRepo is a board game that allows players to take on the role of a member of an organization

where an incident has occurred, to learn about the importance of responding to and reporting data breaches. While the theme of "reporting, sharing, and disclosure" is important, appropriate decisions tend to vary depending on the situation, so it often comes down to a "case-by-case" basis. This training material aims to help participants improve their ability to make practical, operational decisions, and to effectively communicate those decisions by simulating real-world scenarios and practicing how to provide the best possible explanations in various situations.

Going forward, we will promote the use of this program in schools (universities, graduate schools, technical colleges, vocational schools, high schools, etc.), as well as in NPOs, incorporated associations, and community study groups.



Cards used in CoRepo

*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

The threat of cyber attacks targeting employees, such as suspicious emails and phone calls purporting to be from management executives or familiar departments, as well as support scams that prey on people's anxieties, is growing increasingly severe. That makes it more essential than ever for every single employee to maintain a high level of security awareness. 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". In our awareness-raising activities, 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.

Encouraging 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.

Utilizing the uniquely developed character "Harry," we provide fun and friendly information from a perspective that is close to each employee through the intranet and internal chats using Microsoft Teams*. The intranet provides information on information security through animations featuring "Harry" and content such as 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

Mindset Reform

Harry's Security

- 1) Actions to gain empathy (recognition/understanding)
⇒ Get people interested in security.
- 2) Initiatives for instilling "Jibungoto (ownership)"
⇒ Make people aware of security issues around them.





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

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.



Topics

Developing measures to assess risks from an attacker's perspective

There has been an increase in attacks that use more sophisticated methods, such as impersonating company executives or departments within the organization, to steal information via channels such as email or phone calls. Under such circumstances, it is important to consider what risks exist from the attacker's perspective, in order to prevent attacks before they occur. Therefore, in FY2025, we implemented measures designed to raise awareness of how attackers think.

As part of the “Harry's Security” initiative, featuring “Warumono-kun” as the main character who represents an attacker, we created a three-part series and published it on the intranet (Figure 3-③). In each case, employees who view the content are asked to put themselves in the attacker's shoes and consider: what methods are most likely to deceive people, depending on their job role; what strategies can be

used in phishing emails to make people more susceptible to deception; and in what places attacks might be possible within the office or on a train. These materials are incorporated into our information security e-learning programs so that they can be widely used.

At a seminar for Hitachi Group employees, we invited an outside expert to give a presentation on the theme “Thinking About Security from the Bad Guy's Perspective: Change Our Perspective and Take Action.” In addition, to coincide with the Japanese government's Cybersecurity Month, which began on February 1, 2026, we distributed posters (Figure 3-④) and displayed pop-up messages on PCs throughout the Hitachi Group, to encourage employees to think from an attacker's perspective.

Figure 3-③ Intranet Content for Thinking from an Attacker's Perspective



Figure 3-④: Poster for the Hitachi Group Released During Cybersecurity Month



Hitachi is developing AI-powered automated penetration testing technology and pre-shipment security inspection technology to strengthen the security of the OT systems and devices that support critical infrastructure. These enable efficient inspections even in low-bandwidth environments, without disclosing confidential information. By utilizing digital twin environments and technologies to reduce data traffic, we will streamline and standardize inspections while minimizing the impact on actual systems, thereby contributing to the resilience of social infrastructure.

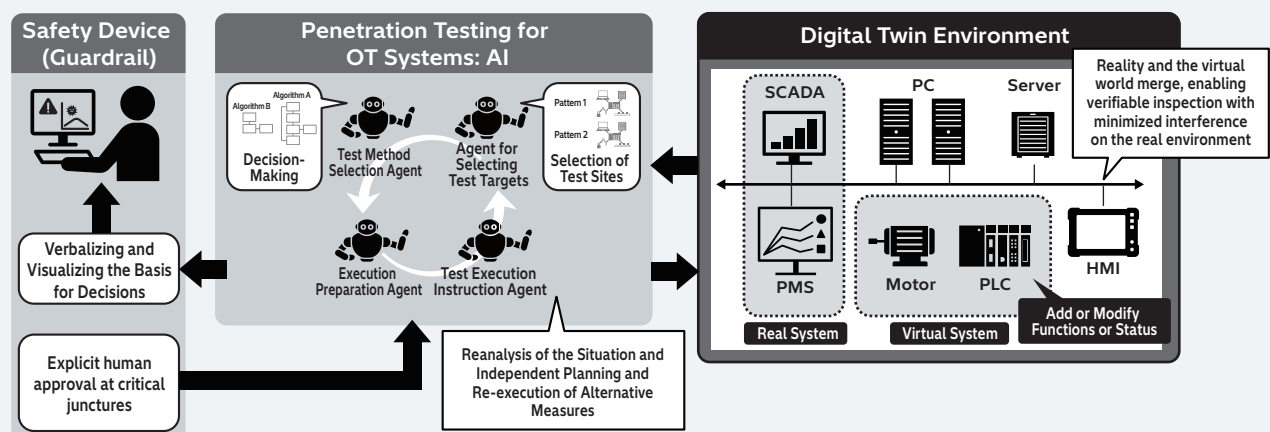
TOPIC

To ensure the stable operation of OT (Operational Technology) systems, such as those in the power, transportation, and manufacturing sectors, which underpin society, it is essential to continuously implement high-quality security measures, to protect these systems and their constituent devices from cyber attacks. In recent years, as cyber attacks targeting OT have become increasingly sophisticated and diverse, and amid growing concerns that the misuse of Frontier AI could lead to automated and accelerated attacks, it has become crucial to pursue both efforts to assess the vulnerabilities of all operational OT systems and initiatives, and to identify and solve vulnerabilities in OT devices before they are shipped. Hitachi is working to advance security validation technologies for both OT systems and OT devices, with the goal of enhancing the resilience of critical infrastructure.

As cyber attacks targeting OT systems become increasingly sophisticated and diverse, the importance of “penetration testing,” which thoroughly examines system weaknesses (vulnerabilities) from the perspective of real attackers, is rising. However, because OT systems feature diverse protocols and architectures and are large in scale, conducting penetration tests relies on a limited number of

experts with advanced expertise in both IT and OT, and the global shortage of such personnel has become a major challenge. Furthermore, because it is difficult to shut down infrastructure systems that operate continuously 24 hours a day to conduct tests, there was a risk that comprehensive verification would not be carried out sufficiently, due to concerns about the impact on real operations. In response, Hitachi is conducting research and development on “AI for Penetration Testing of OT Systems” (Figure 4-①), based on the hypothesis that automating verification through the use of AI technologies, such as large language models, can reduce the workload on experts and minimize reliance on individual expertise. In this technology, for OT systems consisting of multiple devices and networks, specialized “agents” share the responsibility for each phase. These phases include selecting test subjects at the level of system components such as devices and networks, selecting test methods such as information gathering and obtaining administrator-level permissions, and preparing for and issuing instructions for the actual execution of tests. As a result, we aim to go beyond simply automating routine tasks and achieve a collaborative and flexible testing process, much like that of a team of skilled experts. Thus, the system reanalyzes the

Figure 4-①: Overview of AI Technology for Penetration Testing of OT Systems



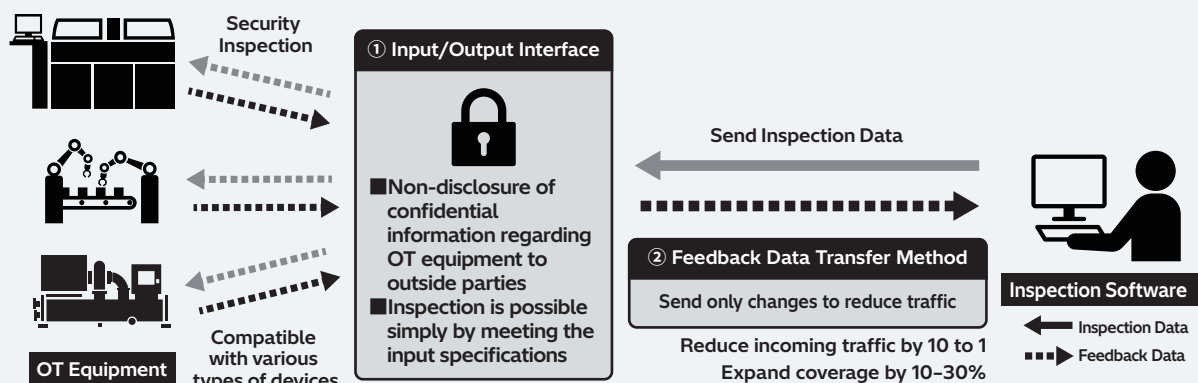
situation when a test pattern hits a dead end, and autonomously devises and re-executes alternative approaches. Furthermore, one of the notable strengths of this technology is that it conducts testing in a “digital twin environment,” where real systems, such as the software and hardware that make up actual systems, are integrated with virtual systems with functions and states virtually added or modified based on those real systems. That makes it possible to conduct testing that closely resembles the actual systems, while minimizing impacts on live systems. At the same time, as a safety measure (guardrail) to prevent inappropriate AI decisions and testing, we are developing a system that not only verbalizes and visualizes the rationale behind the AI’s choice of testing methods in a way that humans can understand, but also requires explicit human approval in situations that could have a significant impact on the system, such as device operation or the external transfer of data.

At the same time, it is important to identify and fix vulnerabilities in OT devices, such as in the factories and power facilities that make up OT systems, before products are shipped, in order to minimize the occurrence of damage once they are put into operation. Tests that involve repeatedly simulating attacks to identify vulnerabilities (such as fuzzing) are effective in verifying the security of OT devices. However, since testing requires specialized equipment and expertise, companies sometimes outsource it to external organizations. A major challenge in such cases has been the difficulty of disclosing confidential information, such as source code. Furthermore, in environments with limited communication bandwidth, the transmission and reception of coverage bitmaps, which indicate the progress of the inspection, became a bottleneck in communication, making it difficult to

increase the number of inspections. To address that, Hitachi has developed a technology (Figure 4-②) that streamlines pre-shipment security inspections of OT devices even in environments with limited communication bandwidth, without disclosing confidential information. This technology uses innovative inspection software to standardize the connection methods between inspection tools and equipment, which vary by product, and defines input/output interfaces that exchange only the information necessary for inspection. This allows us to conduct tests such as fuzzing without disclosing confidential information, such as source code, to external testing organizations. Furthermore, regarding coverage bitmaps, which indicate the progress of the inspection, only the changed portions are transmitted. If there are no changes, only the IDs of similar past data are sent, to reduce data traffic. In an environment with a bandwidth limit of 10 Mbps to 100 Mbps, we evaluated a web server used for OT and confirmed that, compared to conventional methods, this approach reduces incoming traffic to the inspection tool by a factor of 10, while maintaining inspection accuracy and increasing coverage by 10 to 30 percent. That makes it possible to increase the number of inspections per hour, thereby promoting the standardization and streamlining of pre-shipment security inspections. Through these security verification technologies for OT systems and OT devices, we at Hitachi will continue to enhance the resilience of our customers’ valuable assets and social infrastructure, thereby contributing to the achievement of a safe and secure society.

This work is based on results obtained from a project, JPNP24003, commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

Figure 4-②: Overview of Fuzzing Technology for OT Devices



Third-Party Evaluation and Certification

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 2026).

Hitachi is also expanding its ISMS certification efforts outside Japan.

For example, Hitachi Energy has obtained ISMS certification for the entire organization under a global multi-site certification scheme based on ISO/IEC 27001.

- 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 OT Solutions Business Division, Environment Solutions Division, TSS Green&Digital Solutions Department, Industrial OT Solutions Business Division, Environment Solutions Division, Smart Utility Division, Information System Engineering Department, Industrial OT Solutions Business Division, Water Solutions Division, Social Infrastructure Systems Division, Service Department SIDXGroup, Connective Industries Sector, 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. (Digital Systems & Services Sector, Digital Services Business Unit, Enterprise Solutions Division, Life Industry & Platform Solutions Division, Platform Solutions Department)
- Hitachi, Ltd. (Service Business Promotion Center Financial Information Systems Business Unit 5 Financial Information System 1st Division Digital Services Business Unit)
- Hitachi Channel Solutions, Corp.
- Hitachi Social Information Services, Ltd.
- Japan Space Imaging Corporation
- Hitachi Information & Telecommunication Engineering, Ltd. (Managed Services Department)
- 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, Frontline Collaborative Creation Promotion Division, Field Service Platform Promotion Department)
- Hitachi Systems, Ltd. (Industrial & Distribution Solution Services Division 1, Life Science & SAP Infrastructure Services Office, Welfare and Health Support Services Department)
- Hitachi Systems, Ltd. (Managed Services Division, Security Services Division)
- Hitachi Systems, Ltd. (Alliance & Services Development Division, Technical Services Office 1, Technical Services Office 2)
- 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. (Public & Social Systems Division, 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. (The operation and maintenance of subscription platform service)
- Hitachi Solutions, Ltd. (Security assessment services)
- Hitachi Solutions, Ltd. (Asset and Distribution Management Solution Department)
- Hitachi Pharma Information Solutions, Ltd.
- Hitachi KE Systems, Ltd.
- Hitachi High-Tech Corporation(Solution Center)
- Hitachi High-Tech Corporation(Particle Therapy Engineering and Product Division, Operation Service Department, Operations & Services Group)
- 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 Innovation Platform Agency, Japan (IPA) based on

ISO/IEC 15408. (This includes listing in the “archived list of certified products” as of the end of July 2026) (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
Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box HA-DKC-04A-03X	Network-attached Disk Storage Device	C0870	PP Compliance (collaborative Protection Profile for Network Devices Version 3.0e, Certification ID: CCEVS-VR-PP-0099)

*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 FIPS 140-3 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 July 2026) (Figure 5-②)

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

Product	Certification No.	Level
Hitachi Storage Hardware Encryption Module	5389	Level 2
Hitachi Embedded Storage Manager Kernel Crypto API Cryptographic Module	5086	Level 1
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.

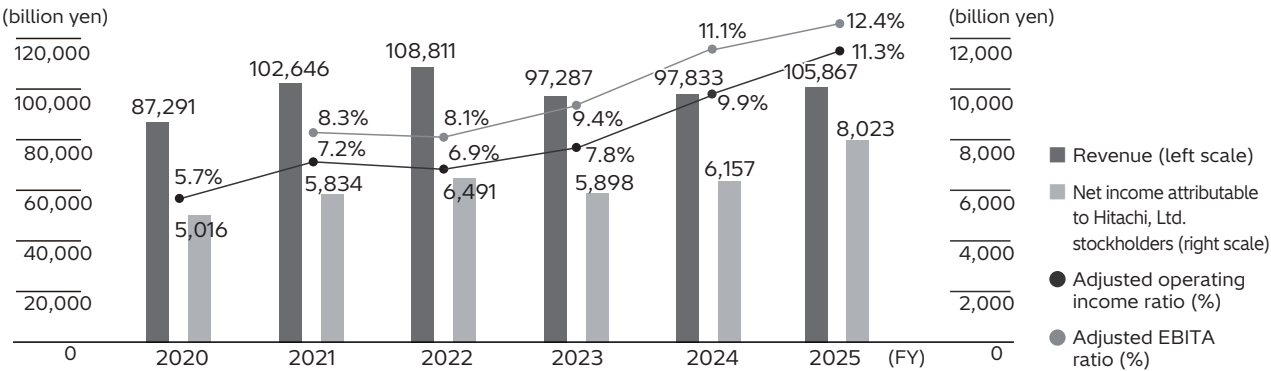
Overview of the Hitachi Group

Company Profile (As of March 31, 2026)

Corporate name Hitachi, Ltd.	Representative Toshiaki Tokunaga, President & CEO
Incorporated February 1, 1920 (founded in 1910)	Capital 466.666 billion yen
Head office 1-6-6 Marunouchi, Chiyoda-ku, Tokyo, Japan	Number of employees 287,901 (Japan:115,544, outside Japan:172,357)

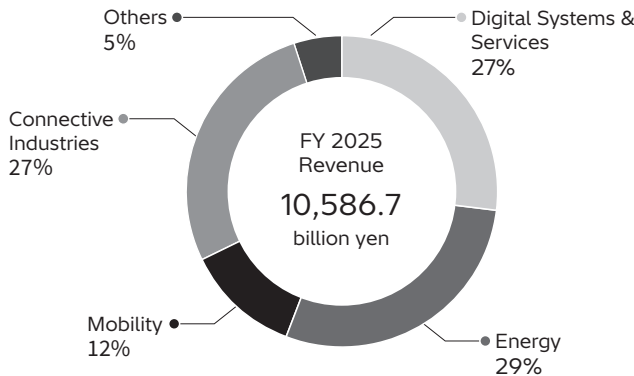
Business Performance Highlights for FY 2026 Based on the International Financial Reporting Standards (IFRS)

Revenue 10,586.7 billion yen (up 8%, year on year)	Adjusted operating income ratio 11.3% (up 1.4 percentage points, year on year)
Net income attributable to Hitachi, Ltd. stockholders 802.3 billion yen (up 30.3% year on year)	Adjusted EBITA ratio 12.4% (up 1.3 percentage points, year on year)
Adjusted EBITA*1 1,311.4 billion yen (up 21.0% year on year)	

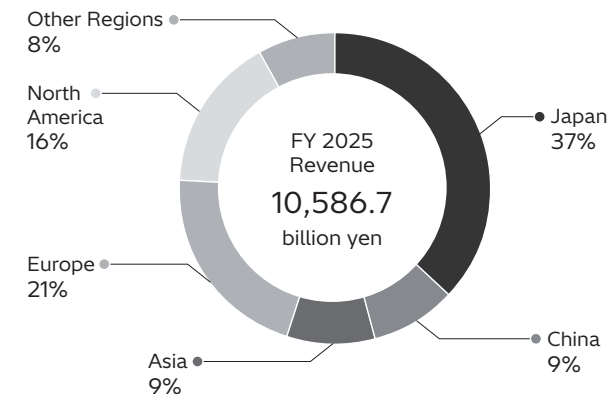


*1 Adjusted EBITA (Adjusted Earnings Before Interest, Taxes and Amortization): Adjusted operating income + Acquisition-related amortization + Share of profits (losses) of investments accounted for using the equity method

Business Composition*2



Revenue by Region*2



*2 Revenues from each segment as a percentage of total revenues. Revenue for each segment includes inter-segment internal revenue.

Hitachi, Ltd.

Digital & Security Strategy Division

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

TEL.03-3258-1111