HITACHI
Inspire the Next

Information Security Report 2024

Hitachi Group

INDEX

Summary of this report:

- Scope and time period covered by this report: Hitachi Group information security initiatives up to and including FY 2023
- Report publication date: November 2024

Accelerating Information Security Globally and Swiftly with “One Hitachi”.

Cyber attacks are becoming increasingly advanced and sophisticated, crossing over national, regional, and corporate borders, and they pose a threat to society as a whole. Companies are constantly at risk of not only information leaks and system shutdowns, but also loss of corporate value, and security measures must be taken without delay.

As Hitachi continues to promote its global business centered on Lumada, it is becoming increasingly important to consider information security on a global scale and create mechanisms to prepare for cyber attacks that are unpredictable as to when and where they will occur. As we work towards the Hitachi Group’s vision of supporting people’s happiness through the use of data and technology to achieve a sustainable society, all divisions and employees involved in our business work on information security as One Hitachi, aiming for the same goal.

Hitachi, Ltd.
Vice President and Executive Officer, CISO

Yoshiaki Kagata

Kagata joined Hitachi in 1985. Drawing on his experience as the leader of the Project Management Promotion Office Smart Transformation Project Initiatives Division, beginning in 2020, Kagata drove strategic and structural reform as CPO and general manager of Value Integration. Appointed to role of Managing Executive Officer of CISO in 2024.

The Rising Importance of Information Security Initiatives

The frequency of cyber attacks has been accelerating in recent years, and the types and methods of attacks are diversifying, while the time it takes for damage to manifest itself is becoming shorter and shorter. There are countless incidents that threaten companies, such as the ransomware attacks and the disclosure of stolen information. There are also notable attacks on targets closer to the workplace, such as those targeting cloud services, which have become an important component of IT systems, and those targeting supply chains, which are part of business processes.

Meanwhile, data protection regulations and cybersecurity-related legislation for companies are being developed in many countries around the world.

The European General Data Protection Regulation (GDPR) and China's three cybersecurity and data laws, as well as the EU Data Act, are about to come into effect The Hitachi Group also needs to manage security risks while complying with the laws and regulations of each country as it develops its global business.

It is an important management issue for companies to keep abreast of the various risks surrounding them, such as rapidly changing global conditions and the increasingly severe impact of natural disasters, and to respond with a sense of urgency in the event of an emergency. Changes in the environment surrounding information systems have elevated cyber attacks and data leaks to become one of the major corporate risks, and corporate value is significantly influenced by the company's ability to respond appropriately to such risks.

Information Security Is Our Mission as a Company That Provides Social Innovation

In its 2024 Medium-term Management Plan, the Hitachi Group has set its vision on "supporting people's happiness through the use of data and technology to achieve a sustainable society," and we promote social innovation business based on IT*1, OT*2, and products. We are delivering our products and services globally, and revenues earned in countries and regions outside of Japan covers 60% of Hitachi's total sales. Our business is truly involved in the social infrastructure that supports business and daily life in various countries and regions around the world.

If a cyber attack were to cause information leaks or faults in the products and services we provide, impacts on society would be very serious concern. To ensure that our customers and consumers everywhere are not harmed in any way, we need to keep a firm grasp of the current situation and recognize information security as one of our most important management issues. We believe that information security is a mission of the Hitachi Group as a developer of business that supports society on a global scale, and we will continue to work on this issue.

Steadily Responding to Cyber Attacks of Expanding Scope

We are implementing security measures in a wide range of areas, including the supply chain. We believe that it is becoming more important than ever to be aware of security measures for normal situations and for contingencies, not only for internal IT areas, but also for manufacturing and development sites, products and services, and the supply chain.

To ensure the security of our products and services, we have established a department responsible for security in each business unit, and we have procedures in place to manage software vulnerabilities and take appropriate measures when problems occur. We recognize that our supply chain partners are in the same situation and aiming for the same goal, so we work together with them to implement information security initiatives, while assessing the feasibility of those measures and gaining our partners' understanding. If there is anything the Hitachi Group can do to support such initiatives as they move forward, we like to collaborate to resolve issues one by one.

Reliably Implementing Data Protection in Compliance with Global Regulations

The next step is to strengthen data protection in compliance with national and regional laws and regulations. The secure use of customer data is vitally important to our Lumada operations, which support the growth of our customers and contribute to the achievement of a sustainable society by sharing important customer data and reflecting it in our products and services. The Hitachi Group, delivering

*1 IT: Information Technology
*2 OT: Operational Technology

solutions to customers leveraging its digital technology named as “Lumada”, will ensure compliance with laws and regulations related to data protection, which are being strengthened globally.

It goes without saying that we manage data protection and privacy protection in accordance with the laws and regulations of each country and region. To make sure confidential information, which is our customers’ asset, is never lost or leaked, we not only establish solid internal operation and management methods, but also build security processes and control systems that extend their coverage as far as the point at which the information is provided to our customers.

Strengthening Our Global Implementation Structure for Immediate Response

We are also strengthening our global information security structure. In response to the growing concern over how quickly we can respond to cyber attacks, we are strengthening our global information security structure so that we can detect attacks and take countermeasures swiftly, and quickly implement thorough measures in normal state as well.

In developing global business, it is essential to have a solid understanding of the business concepts and laws and regulations of each country and region, and to be properly accepted in each region in a manner appropriate for that region. In the area of information security, we promote information security measures in a manner that is appropriate to each region as early as possible, by identifying the latest trends, centered on the security departments established in the Americas, Europe, Asia, India, and China. Those departments are under the direct authority of our headquarters, and operate in cooperation with the departments that monitor laws and regulations in each region.

Open Collaborative Creation with External Parties and Heightened Empathic Awareness Within the Company

In response to cyber attacks that are becoming more and more organized, it is important not only for individual companies to take action, but also for companies to join in efforts with each other. That collaboration must extend to stronger cooperation between industry, government, and academia. Raising the level of information security in society as a whole will also raise the level of Hitachi’s information security. Based on this open mindset, we promote active participation and discussion in various industry associations and academic societies.

It is also essential to foster a security culture within the Hitachi Group that enables employees to act properly with security awareness. Just as a fire alarm detects smoke, it is important for each of us to have the habit of sensing that something is wrong and responding to it. The concept of “right-and-wrong before profit-and-loss” is firmly ingrained in the Hitachi Group. In information security as well, based on this concept, we all share what we are doing now, and what we aspire to beyond that. We are working to raise the information security awareness of our employees so that they develop empathy and can each work on issues with a sense of conviction.

Promoting Information Security Globally With Swift Responsiveness

In my varied work experience, I have learned the importance of always working under the premise that we are a group of human beings. Regardless of nationality, age, or other aspects of our individual backgrounds, as long as we are human, we will, unfortunately, sometimes make mistakes. It is essential to be willing to proceed on the assumption that failures happen. In information security as well, we will always work with the understanding that no countermeasure is 100% effective.

The Hitachi Group is engaged in business that supports society. In the event of an incident, impacts on society on a global scale would be very serious concern. That is a fact that we must never forget. This year marks the 150th anniversary of the birth of Hitachi’s founder, Namihei Odaira. We will keep in mind the principles of harmony, sincerity, and pioneering spirit that Odaira set forth, in information security as in other fields, and will boldly confront ever-changing threats by imagining every possible case, and seriously considering and implementing countermeasures for them. As One Hitachi, we will continue to strongly promote information security for the benefit of our customers and society, with each and every member of the Hitachi Group globally and responsively working together.

Hitachi's Approach to Information Security

The advance of digitalization generates new value, but there is the growing risk that increasingly sophisticated cyber attacks could impede the continuation of business, through threats such as information leaks and shutdowns. Minimizing that risk through risk management around information security is one of a company's most important tasks.
Given that background, Hitachi, aiming to become a global leader with our social innovation business, positions cybersecurity measures to address the value creation and risk management aspects as a key management issue, as we work on information security.

Promoting information security as risk management

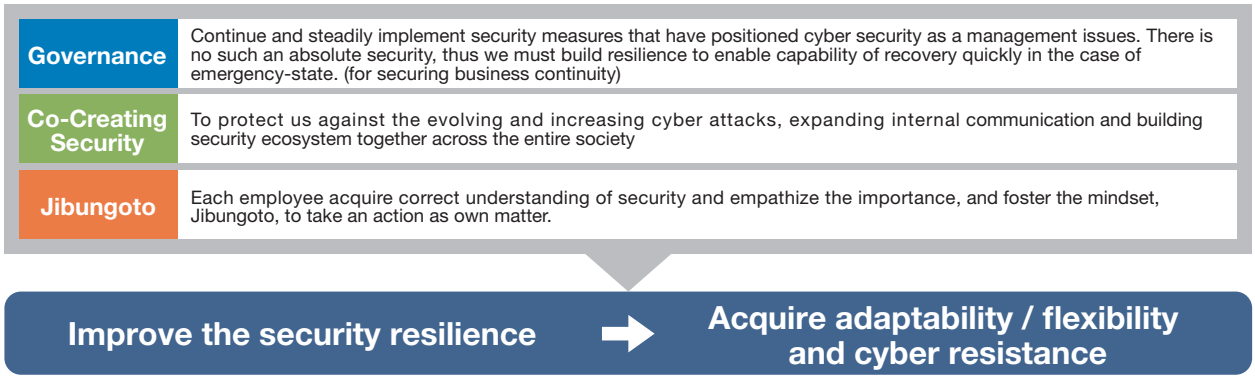
The rapid advance of digitalization and the complex global changes in political and economic conditions are changing the business environment on a daily basis. Hitachi monitors and analyzes this business environment and practices risk management to address the aspects of the risks Hitachi should be ready for and the opportunities we should seize, based on social issues, our competitive advantages, management resources, and other considerations. We aim to create profit opportunities while controlling risks.

Recent cyber attacks are gaining in level and sophistication, and their scope is widening, to cover production and manufacturing environments and development environments, which are OT fields, as well as the usual internal IT systems. There are also attacks targeting the products and services we provide to customers, and our supply chains. As a result, everywhere around the world is increasingly likely to be attacked, and many incidents have major repercussions on business continuity, including information leakage and factory shutdowns. Data protection laws, as exemplified by China's set of three cybersecurity and data laws, are being reinforced around the world, and data leaks due to cyber attacks are a rising risk from the perspective of a company's legal compliance. Given this background, Hitachi recognizes information security as a major risk, and handles countermeasures aggressively as a management issue.

Hitachi's Information Security Vision

In digital society, while the enormous amount of diverse data creates value, there are also major threats to safety and security. In addition, workstyles have changed dramatically, such as with the promotion of working from home, and the future form of security must also change dramatically. Targeted attacks are becoming more sophisticated and diverse than ever, and existing attack methods are now being used in combination, for example, using ransomware threats to steal information. In such a situation, Hitachi is now promoting various efforts to improve cyber resilience, based on the three approaches of internal controls as "Governance," collabrateive creation as "Co-creating Security," and ownership as "Jibungoto." (Figure 1-1)

Figure 1-1 Hitachi's Information Security Vision



Governance: zero trust security initiatives

The Hitachi Group, which began full-scale cyber-attack countermeasures in 2011, has learned from the WannaCry infection in 2017 to expand the scope of countermeasures not only to internal IT but also to OT areas. We are continuously and steadily strengthening operational, technical, and organizational measures, focusing on enhancing security and cyber BCP in products, services, and supply chains.

In addition, we have initiated zero-trust security measures on the standard of cloud-based IT architecture, aiming for optimal security in light of the recent shifting of business systems to the cloud, and work-style changes such as the establishment of working from home. For implementation, we consider "authentication," "endpoint," and "cyber-integrated monitoring" to be key elements in achieving zero-trust security, and we are working to enhance our attack-detection capabilities.

Co-creating Security: work on building a security ecosystem

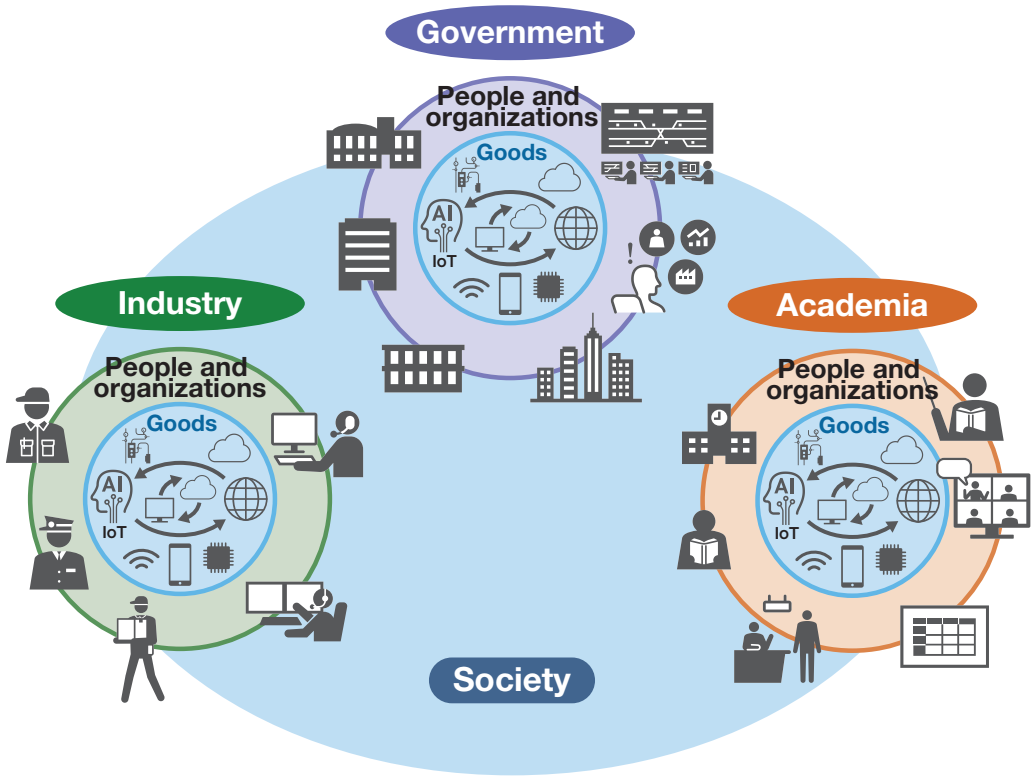
Responses to security incidents require cooperation among all departments, including PR, personnel, and legal affairs, not just the IT department. As the range of matters addressed by security measures broadens, the Monozukuri Group, Quality Assurance Department, Procurement Department, and other departments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

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

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

Connections are not just needed within Hitachi. It is now essential to share threat information and issues encountered when implementing countermeasures with enterprises, governments, academia, and other entities engaged in cybersecurity initiatives to create a community not bound by traditional constraints. Hitachi invites each enterprise and organization to feed back the knowledge it gains from the community into its own security measures, creating further connections in society. (Figure 1-2)

Figure 1-2 Illustration of the security ecosystem



Hitachi's Approach to Information Security

Jibungoto: security awareness-raising initiatives

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

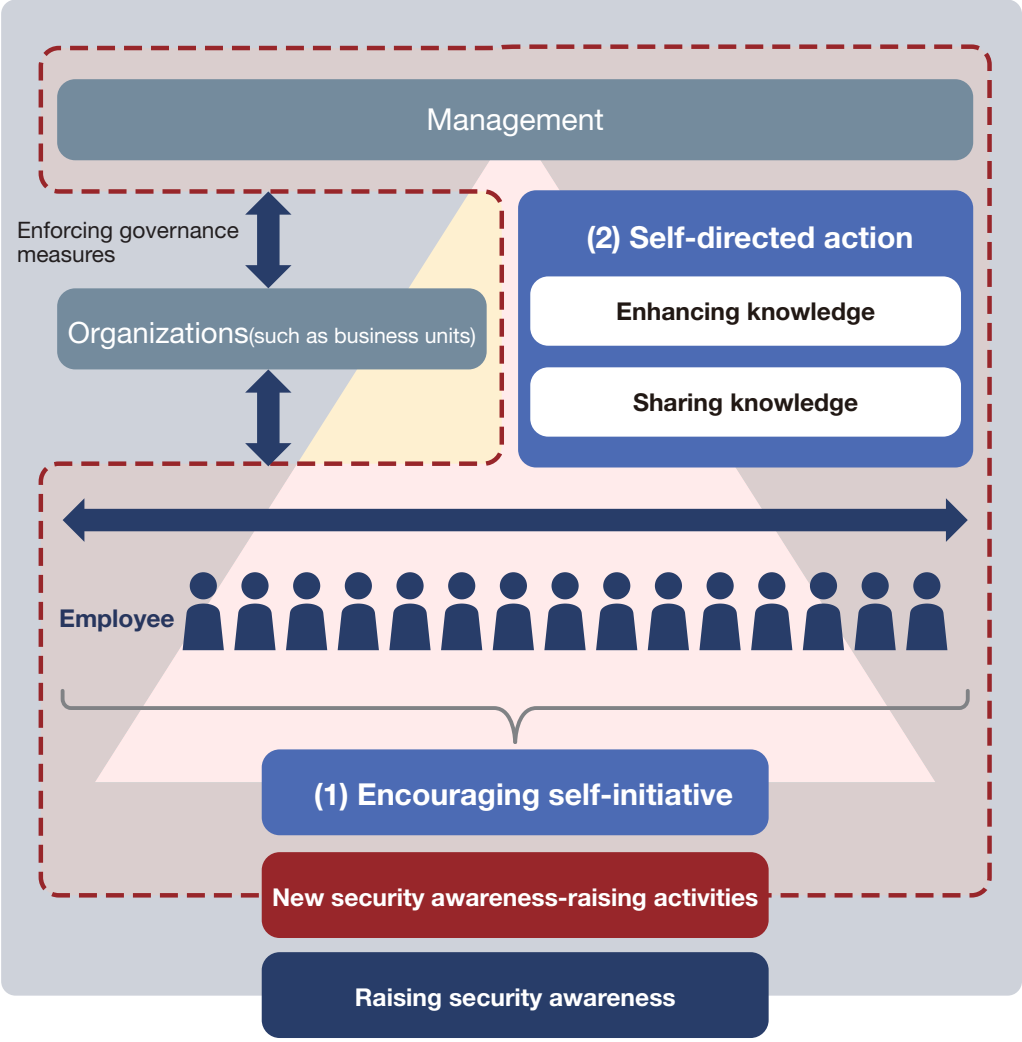
This means that improving each employee's security awareness will be the last defense. In addition to our existing strict governance, we have started activities to raise security awareness by encouraging employees to take the initiative and act independently. This does not mean making security feel like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

Figure 1-❸ The ideal future form of security awareness

In addition to our existing strict governance, generate awareness by employees taking the initiative and acting independently.

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

Key concepts: "Jibungoto (Ownership)" and empathy



Key themes for FY2023:

At Hitachi, we formulate security strategies and implement measures based on the current state of security incidents, and on trends in the laws and regulations for security and data protection.

Recent security incidents have been characterized by expansion of the attack surfaces and the intensifying of information theft, ransomware, and other money-oriented attacks, which are having an impact on the business of various companies. In particular, there have been cases of business shutdowns due to supply chain damage. As attack surfaces are expanding, the increase in attacks on cloud services stands out. In addition, vulnerabilities in Internet-exposed devices and mismanagement of those devices are often exploited to steal information or infect devices with ransomware in order to extort money.

Global trends in security and data protection laws and regulations show a noticeable shift toward stricter regulations in Europe. In security matters, there is the NIS2 Directive, which is an urgent security requirement for the provision of products and services related to critical infrastructure, the Cyber Resilience Act, which is still several years away but will further broaden the scope of regulation, and the EU Data Act, which will become applicable in the data protection field. In addition, about 70% of countries are progressing in the regulation and development of data protection laws, with Vietnam, India, and other parts of Asia particularly active in the development of such laws.

In light of these circumstances, Hitachi has worked on the following four priority themes.

1. Global governance enhancement

We have established five regional branches with security-management and incident-response functions outside Japan, in the Americas, Europe, Asia, India, and China, as information security departments under the direct authority of our headquarters, promoting rapid response to incidents worldwide through our “Security One Team” and compliance with changing local laws and regulations. In addition, we are strengthening our current data protection unit and are operating it unified globally, headed by our headquarters.

2. Response to increasingly sophisticated threats

In order to achieve a rapid global response, we are promoting the global use of intelligence information, and enhancing our ability to detect and counter cyber attacks. We are also promoting the strengthening of information asset management in order to quickly identify the target in the event of an attack.

Along with strengthening attack-surface management, we are proceeding with rechecking high-risk environments, such as cloud services and Internet-exposed devices, which are increasingly becoming targets of attacks.

3. Product/service/supply chain security acceleration

We are building a system to maintain security measures, including the reliable implementation of procedures and rules, based on the concept of three lines of defense. For product and service security, we hold regular liaison meetings for improving the functionality of the PSIRTs (Product Security Incident Response Teams) established in each BU and company, and for sharing information and resolving each of their issues. In the supply chain, we are strengthening communication with procurement partners through briefing sessions and other means, with the aim of raising security awareness.

4. Data protection enhancement

Along with strengthening global data governance, we have created a playbook that defines data protection processes, and have promoted thorough awareness of and training for these processes. In addition to China’s three cybersecurity and data laws, we are also taking various measures to comply with the Personal Data Protection Laws of India and Vietnam, and with the EU Data Act which is set to become applicable.

Information Security Management

Information Security Management Systems

Hitachi sets information security policies, establishes various rules and promotion frameworks based on these policies, and works on information security management in order to protect the information assets to be protected. These assets include information entrusted to us by customers, the systems that store such information, and the information systems that operate social infrastructure services.

Information security policy

As an organization that contributes to Japan's reputation on the global stage, Hitachi recognizes that security risks are business risks, and makes every effort to ensure information security by defining a security policy incorporating the wider management policy of the enterprise.

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

Out of its recognition that the effort to maintain information security is one of the key tasks in its scheme of management and operations, the Company 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 Company 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 Company shall adhere to laws, regulations and other norms relating to information security. Further, the Company's information security control rules shall be formulated to conform to such laws, regulations, and other norms. The Company 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 Company 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 Company 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 Company shall work to create a system to secure proper operation in corporate groups consisting of the Company and group companies in accordance with Article 1 through 5 in this article.

Information security promotion framework

Within the Hitachi Group, Hitachi, Ltd. HQ (corporate) is responsible for governance of the group as a whole. Governance is instituted by way of instructions passed down through lines of control to each Hitachi, Ltd. business unit (hereinafter BU) and business sites and to each Group company. Governance of the Hitachi Group as a whole is achieved by each BU and Group company applying the same controls to the Group companies (subsidiaries) that they manage.This framework applies not only within Japan but also overseas locations.

The company president appoints the Chief Information Security Officer who has authority and responsibility in relation to information security, and the Information Security Audit Manager who has authority and responsibility in relation to information security audits.

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

The matters decided by the Information Security Committee are disseminated to each organization through the Information Security Promotion Council

attended by representatives of all BUs and business sites.

In principle, the head of the BU and business sites manager serve as the Information Security Officer of the BU and business sites. the Information Security Officer appoint the Information Security Manager and the Date Protection Manager to support implementation, in order to manage and control personal information protection and information security.

In addition, as the scope of cyber attacks is expanding, we have appointed a person responsible for each physical security environment, including the internal IT environment, development and verification environment, production and manufacturing environment, and office access, under the supervision of the Information System Administrator. In addition, to strengthen the security of the supply chain, including products and services provided to customers and suppliers, we have also established the Product Security Officer and a Procurement Security Officer.

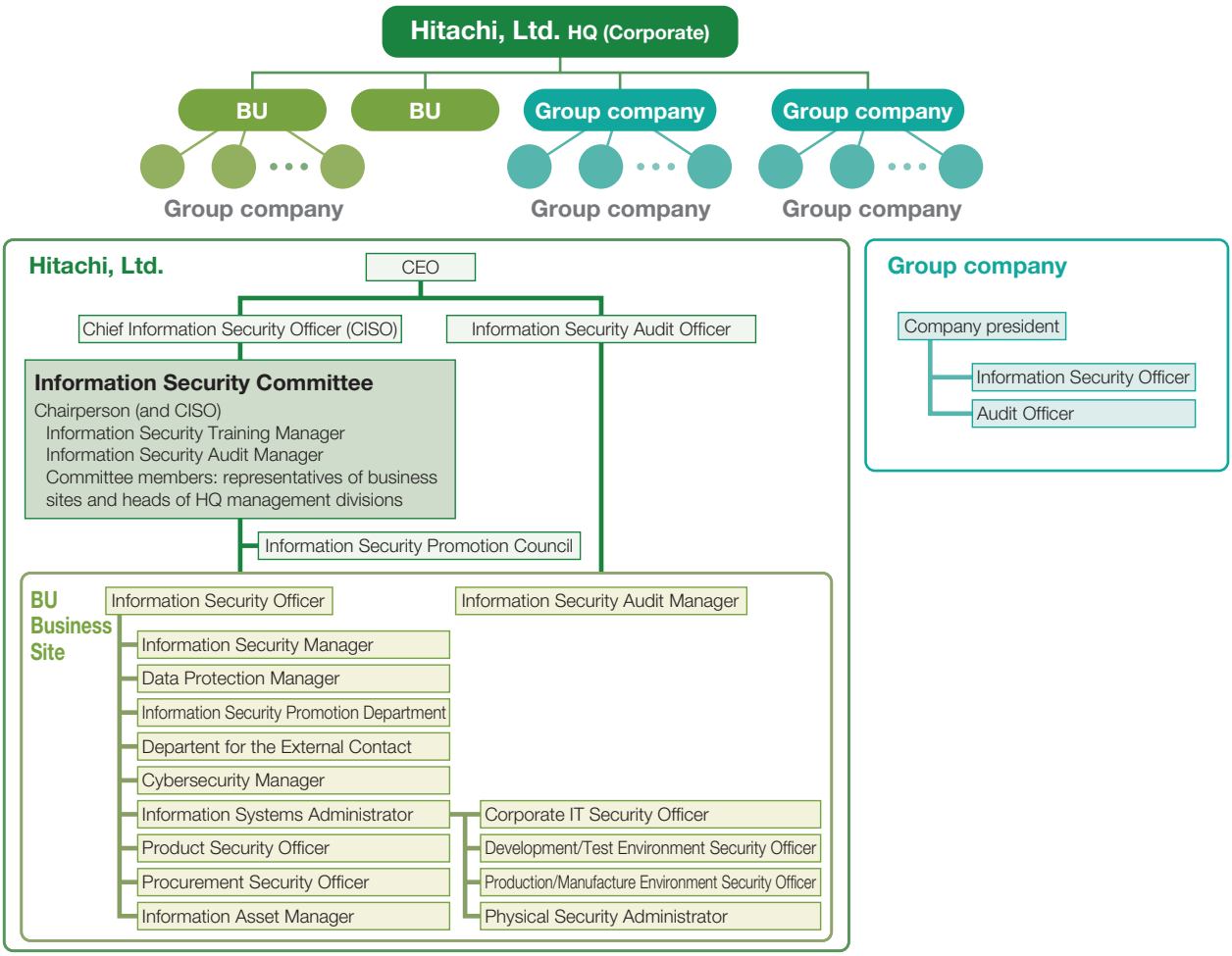
The Information Asset Manager is placed in all divisions, and allocates responsibilities in relation to the handling of information assets including personal information.

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

Since FY 2022, the regional headquarters in the Americas, Europe, Asia, India, and China have established local Group company support functions for personal data protection, to ensure personal data protection compliance.

In FY 2023, we also established new regional branches in the Americas, Europe, Asia, India, and China, which are departments in charge of information security under the direct authority of the headquarters, to provide support to Group companies in each region and strengthen management on a global basis.

Figure 2-❶ Information security promotion framework



Information Security Management

System of rules for information security

Hitachi has established the rules in the following table based on its information security policies. (Figure 2-❷)

Group companies have established similar rules to promote information security.

Basic rules

"Information Security Management Rules" define the basic matters that must be complied with in relation to the formulation, implementation, maintenance, and ongoing improvement of information security management systems.

We promote our cybersecurity measures worldwide according to our "Information Security Standards", which comply with the U.S. government SP800 standard series.

Addressing the personal information protection, we have established "Hitachi Group Privacy Principles", a code of conduct common to all Hitachi Group companies, with reference to the OECD Privacy Guidelines.

Furthermore, in our "Personal information protection policy" and "Regulations for personal information management," we have set rules equivalent to the JIS standard (JIS Q 15001) in order to manage personal information at a higher level than the Personal Information Protection Law.

"Regulations for Confidential Information Management" define the handling procedures used to protect confidential information.

Individual rules

The "Rules on website creation and information disclosure" define the matters that must be complied with in order to disclose and use information correctly on websites.

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

Information security management cycle

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

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

In the "Do" stage, we deploy security measures within the company and operate them. We are working to ensure thorough knowledge of security measures and raise each employee's awareness through information security education and awareness activities.

Figure 2-❷ Information Security・Rules related to personal information protection

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

Figure 2-❸ PDCA image diagram

In the “Check” stage, periodic security operation status inspections, audits according to the audit plan, and on-site inspections by security experts are conducted.

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

Each fiscal year, the maturity of information security measures is assessed based on the Cyber Security Management Guidelines Ver. 3.0 issued by the Ministry of Economy, Trade and Industry (METI), and the measures for the following fiscal year and beyond are formulated.

Information asset management initiatives

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

Handling in Normal Times

Hitachi believes that in order to protect and manage information assets, it is essential to be aware of what information exists in which systems. Therefore, we manage information assets in accordance with various information security-related rules, such as the Confidential Information Management Implementation Procedures.

The Information System Administrator of each BU or business sites compiles a list of information systems. In cooperation with Attack Surface Management, we manage information systems for Internet publication to ensure that there are no omissions. The list of information systems is for managing information such as Internet connections and Cloud utilization, in addition to the administrator information of the relevant information system, and is used for operational management. In addition, each Information Asset Manager regularly manages the information assets stored in each information system, so that they can understand what information is stored, including whether or not customer information, personal information, etc. is held in the system.

Response to Emergencies

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

Initiatives to ensure security during mergers and acquisitions

Hitachi is working to strengthen information security governance in companies that newly join the Hitachi Group, to minimize the security risks that arise as we actively pursue M&A.

M&A creates new value by integrating companies with different corporate cultures. On the other hand, we must minimize the information security risks that occur as we integrate policies and systems. At an early stage in the M&A process, it is important to ensure that the target company understands and complies with the Hitachi rules and to implement controls and governance based on the Hitachi policies.

Information Security Management

Our security risk assessment during the M&A process is divided into two phases: before and after the contract is signed.(Figure 2-4)

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

We analyze the information security of the acquired company on the basis of published information and information provided to us in advance. This analysis covers matters such as information security organizations and systems, the readiness of rules, etc., the characteristics of the business and its adaptation to the legal system of the country or region, and the occurrence of any cybersecurity incidents and responses to them.

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

We select the sites to be assessed, with consideration of the situation and business characteristics of the country or region in which the acquired company operates, and then ask the company to conduct a self-assessment using the risk assessment items of the Hitachi Rules. Acting on the results, Hitachi's headquarters staff directly visit the target sites to confirm the on-site situation. Lastly, if any noncompliance remains, we will create a corrective action plan and follow up on the plan until the action is completed.

Educating workers on information security

Information security training

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

Hitachi conducts annual training by e-learning of all executives, full-time employees, and temporary employees on the subjects of information security and personal information protection. The training participation rate for Hitachi, Ltd. in FY 2023 reached 100% (excluding those on leave or otherwise unable to attend). Hitachi, Ltd. also formulates an annual information security training plan, and implements it using a diverse range of education programs tailored to specific subjects and purposes. For example, one program might target a specific group of people like newly hired employees and another those in new managerial positions, while another might offer specialized education to people in roles such as personal information protection manager. (Figure 2-5)

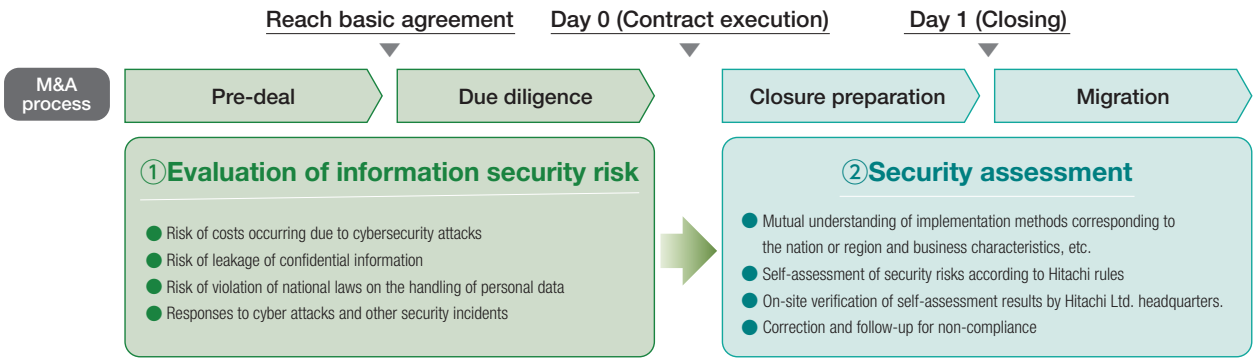
Hitachi, Ltd., makes its educational content available to Group companies within and outside Japan, and works towards a deeper understanding of information security and personal information protection of the Hitachi Group as a whole.

Drill-based training for spear phishing email attacks

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

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

Figure 2-4 Information security risk assessment and security assessment



Management assessment and monitoring

Hitachi conducts regular audits and on-site assessments to evaluate and monitor whether information security measures are being implemented appropriately.

Personal information protection and information security audit

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

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

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

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

Figure 2-❺ Information security training target personnel and content

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

Information Security Management

Initiatives for Security Human Resource Development

To ensure our own internal security and to effectively implement security measures in the products and services provided to customers, the Hitachi Group promotes company-wide human resource development from a security perspective.

Our Approach to Security Human-Resources Education

In response to the intensification of cyberattacks in recent years, the Hitachi Group has promoted human resource development from a security perspective, to strengthen its own internal security and to ensure the security of the products and services it provides to its customers. The scope of this development initiative includes not only high-level security experts, but also technical members involved in the development and operation of products and services, as well as users of internal IT services. There are three categories of our human resources: (Figure 2-6)

- Security experts who possess considerable security skill and shoulder the security burden of the Hitachi Group
- Human resources responsible for security measures in relation to the design, development, and operation of products and services provided to customers as well as those at production and manufacturing sites
- Personnel at junior level who understand the basics and can respond appropriately when a security incident occurs

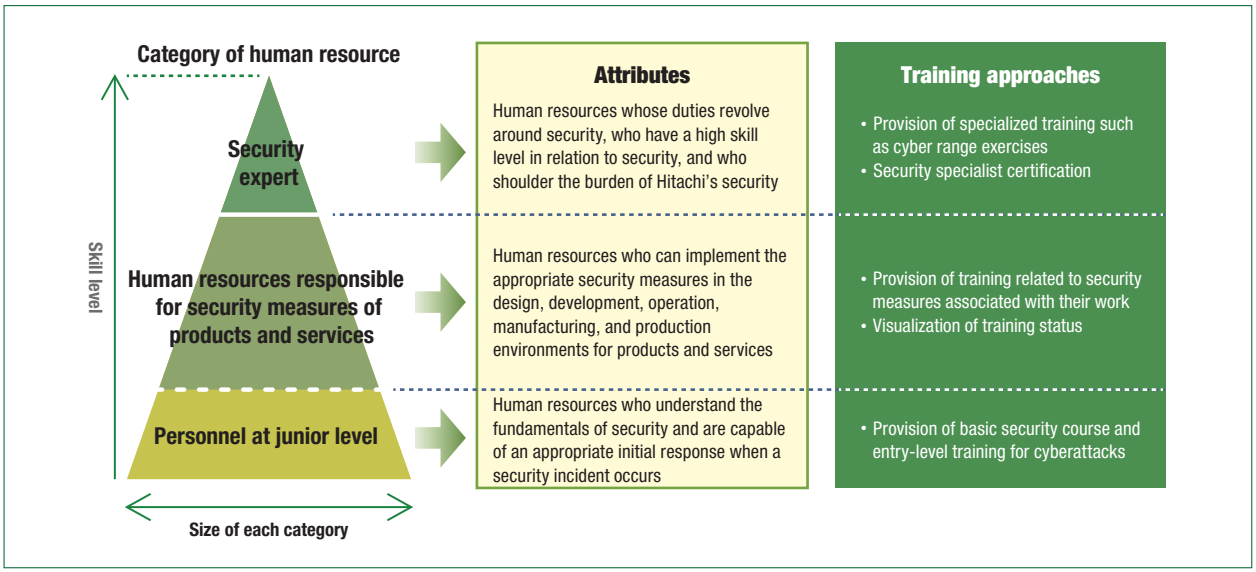
Educational programs for each category of human resources

We develop educational programs tailored to the three categories above and effectively promote human resource education according to the objectives of each category.

Security expert

The approach for security experts in this human resource development includes training in advanced techniques, such as cyber range exercises, and providing community sites that support information sharing and collaboration. Hitachi established its Hitachi Certified IT Professional framework for security experts in August of 2014. This certification framework for Hitachi IT professionals conforms to the IPSJ Model for IT Professional Certification. Under this certification model, candidates with the necessary security skills are identified, trained, and evaluated to pursue an appropriate career path as an information security specialist (Hitachi Certified Information Security Specialist: HISSP).

Figure 2-6 Three security HR categories and training measures



Human resources responsible for security measures of products and services

Human resources responsible for security measures in products and services are those who promote the necessary security measures as part of their work in providing the products or services. These individuals are responsible for carrying out appropriate security measures in the design, development, operation, and maintenance of products and services, as well as in the preparation of the environments in which these activities take place. Also important is the development of security human resources focused on production and manufacturing. These human resources are provided with training to promote an understanding of security measures in accordance with company rules. Environments for the design and development of products and services, as well as for production and manufacturing, must be established and maintained to ensure that each site for the design and development of products and services, as well as for the production and manufacturing of those products and services, is secure and does not interfere with each other. To this end, Hitachi is working to improve its employees' knowledge of IT and OT security measures. We also train PSIRT personnel, security risk assessors, and security system architects who are responsible for improving the security of products and services.

Employees with basic security knowledge

We train employees in basic security skills to raise security awareness throughout the company and strengthen our security measures. In addition to the basic training, we cover skills for appropriate first response to security incidents resulting from cyberattacks. The Basic Knowledge e-learning Program for Cybersecurity Countermeasures and the Communication Training for Cybersecurity Response, both offered since FY 2016, fall into this category. Hitachi also provides e-Learning programs on security fundamentals for people who require further introductory training

To accommodate remote work environments, the Communication Training for Cybersecurity Response, which was previously an introductory training in a workshop format, was converted to an online format beginning in FY2020.

Information Security Management

Action to Strengthen Global Information Security

As global business expands, information security initiatives are becoming even more important throughout the Hitachi Group worldwide. Hitachi is working to strengthen global governance by newly establishing information security departments (regional branches) in each region to ensure the reliable implementation of security measures and to improve governance penetration in global security.

Enhancing governance through regional branches

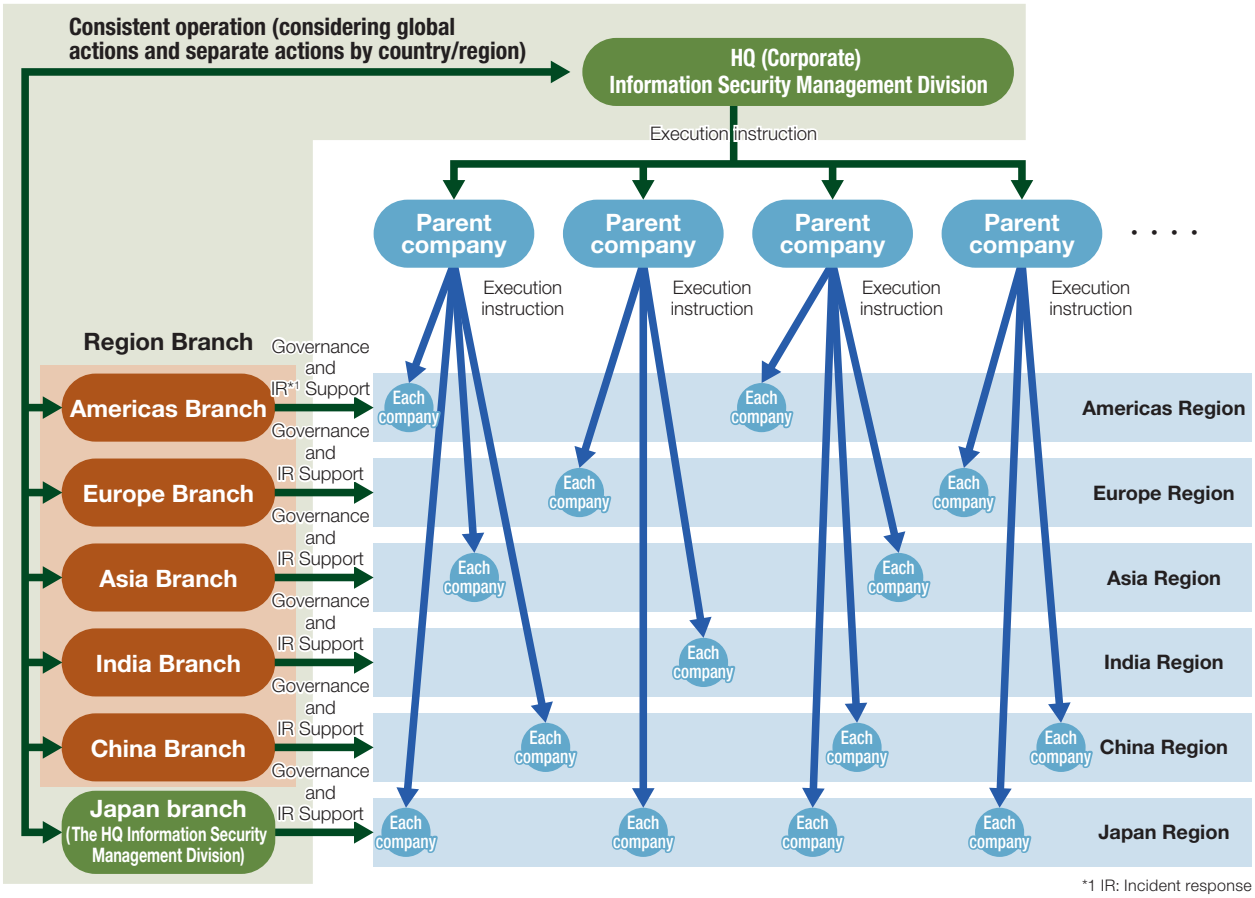
Hitachi's lines of governance for information security are that the security management divisions of the Hitachi Group provide policies/measures and instructions to the BUs and Group companies. The BUs and Group companies direct their overseas subsidiaries to implement the policies and measures.

For the purpose of prompt response to incidents by the Security One Team and compliance with changing regional legislation, regional branches have been established in the Americas, Europe, China, India, and other regions in Asia since FY 2023 to spread and embed globally. In addition to the vertical governance line from a parent BU/the company to subordinate group companies, we have a horizontal line of support from the branches to their regional subsidiaries to strengthen security measures on a global basis. In Japan, the Information Security Management Division at headquarters plays the same role for the Japan branch.

A Head of Cybersecurity has been appointed at each regional branch to strengthen communication, incident management, and management oversight, in order to ensure a consistent global response to incidents. (Figure 2-❼)

Regional branches hold security conferences and workshops for security managers and personnel from Hitachi Group companies in their region, to raise their understanding of Hitachi's overall strategy and initiatives, and to support the implementation of specific security measures. Through these activities, we are working to establish local communities and make

Figure 2-❼ System for strengthening governance of regional branches



*1 IR: Incident response

cross-regional communication more active. We also aim to build security awareness and consciousness through the widespread distribution of our security newsletter.

In strengthening incident management, intelligence and incident information are shared on a regular basis, to enhance resilience in emergencies and to promote support for responses that minimize risk, in cooperation with related departments in the event of an emergency.

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

Figure 2-8 Main activities of regional branches

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

Cybersecurity Initiatives

Cybersecurity Management

The diversification of cyberattack techniques means incidents come from many sources and their impact can be magnified. To deal with these risks, Hitachi has expanded the scope of security risk management. A traditional focus on internal IT environments in an OA context has been expanded to include the development, verification, production, and manufacturing environments, supply chains, and development processes for products and services, ultimately reducing business risk.

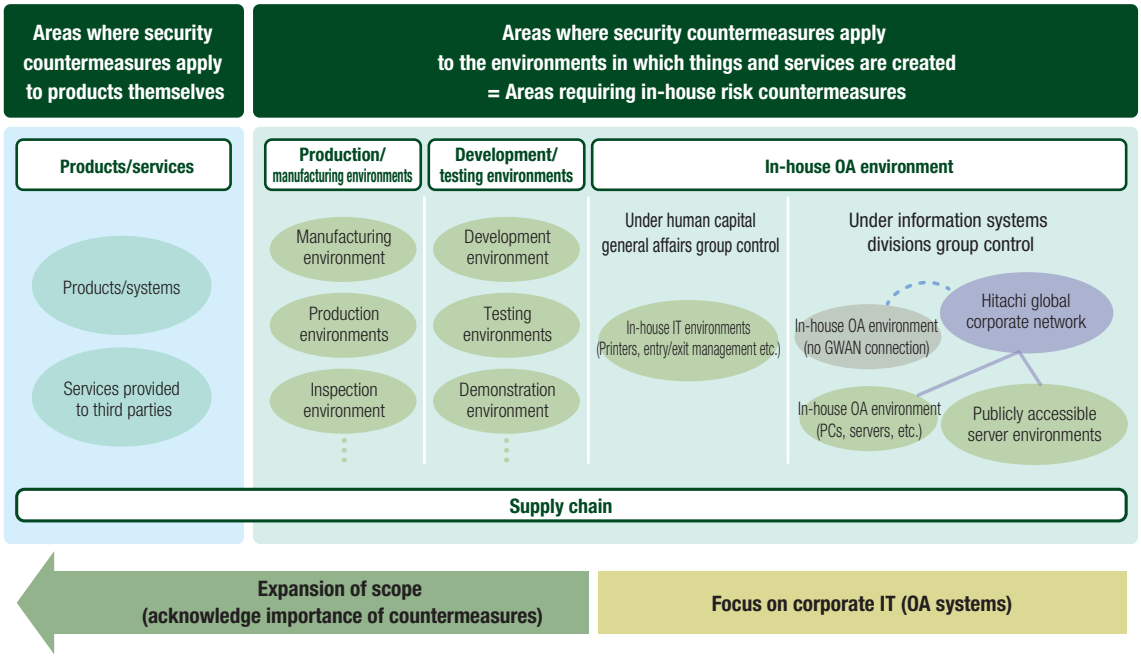
Initiatives to enhance cybersecurity countermeasures

As IT permeates production, manufacturing, development, testing, and other business operations, there is an increasing need to respond to attacks outside the traditional office automation environment, as well as cybersecurity measures for products, services, and procurement. (Figure 2-9)

For this reason, since 2018, we have been working to strengthen cybersecurity measures for internal OA, development and testing, environmental systems in production and manufacturing, and process systems in products, services and supply chains. Various initiatives are underway to strengthen cybersecurity measures in each area. (Figure 2-10)

In addition, since 2023, we have been building a system based on the concept of three lines of defense to maintain security measures for the development and testing environment, the production and manufacturing environment, and products and services. As the first line of defense, each of BUs/Group companies conducts a self-inspection to ensure compliance with the guidelines and management principles. As the second line of defense, the headquarters monitors the results of this self-inspection. As the third and final line of defense, the audit department checks the status of monitoring.

Figure 2-9 Expanding the scope of cybersecurity countermeasures



Initiatives to strengthen security for each environment

Security enhancement in in-house OA environments

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

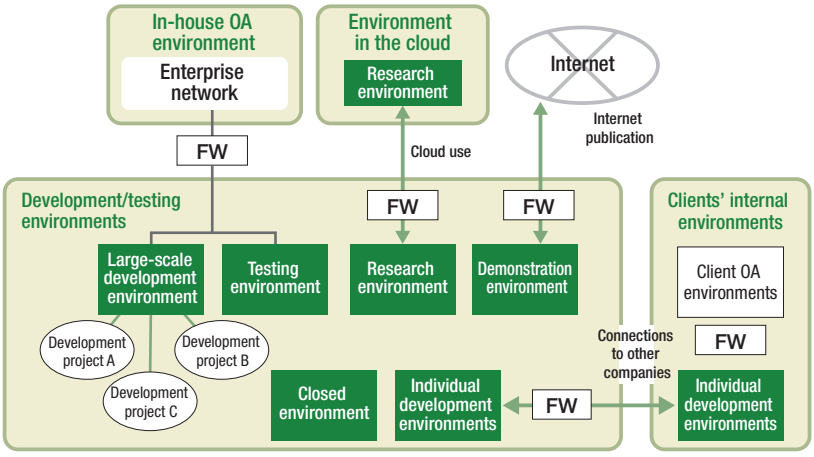
Security enhancement in development/testing environments

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

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

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

Figure 2-⓫ Development/testing environment security network



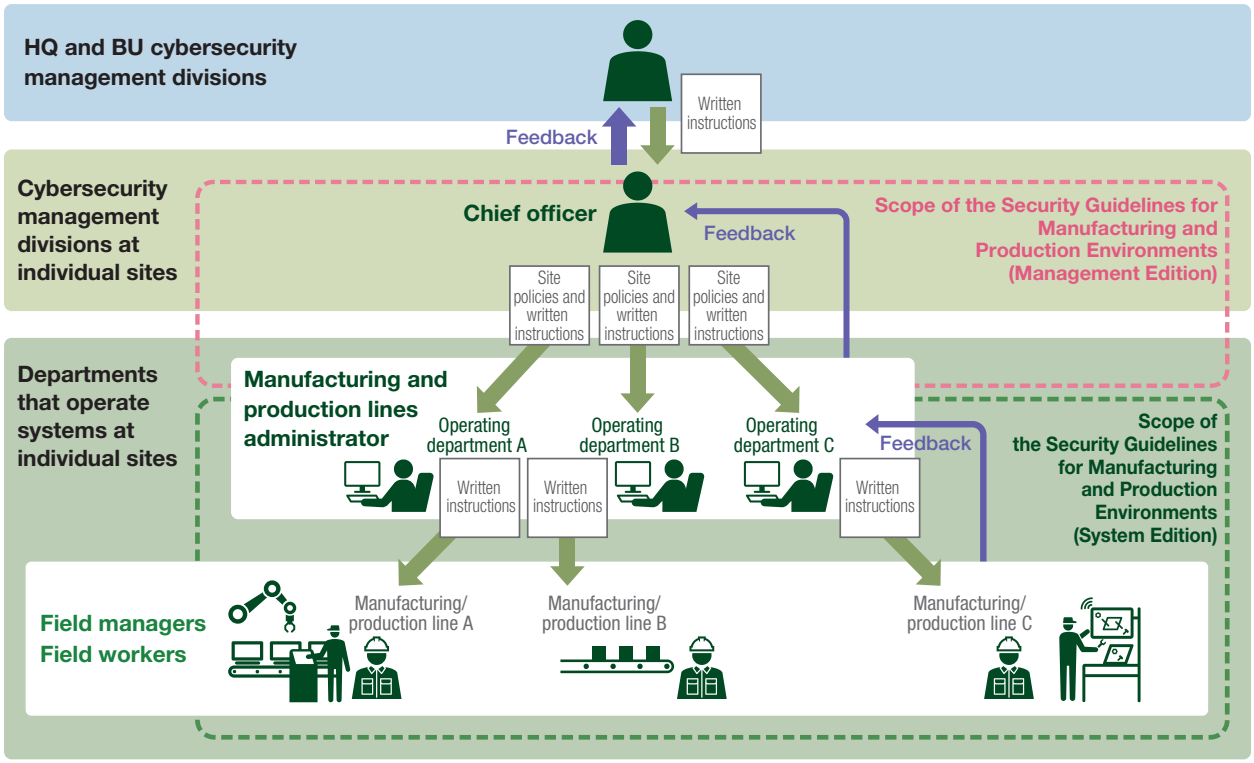
Cybersecurity Initiatives

Security enhancement in production/manufacturing environments

It is important that manufacturing and production environments do not affect other environments, such as internal OA and development environments, and vice versa. Hitachi has established guidelines governing the creation and operations management of mutually secure connection environments, and acts according to those guidelines within the Hitachi Group. (Figure 2-⑫) At our manufacturing and production sites, posters and brochures outlining information security policies remind employees of their responsibility for compliance in their day-to-day work, resulting in greater security awareness. (Figure 2-⑬)

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

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



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

Initiatives to enhance supply chain security

To have procurement partners handle Hitachi's information assets with security considerations, Hitachi verifies and screens the partner's information security levels in advance, based on Information security criteria set by Hitachi.

These criteria also include "information security guidelines," including security measures against recent cyberattacks on supply chains.

Specifying the information security requirements as Hitachi. allows procurement partners to perform checks against the requirements. (Figure 2-⓮)

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

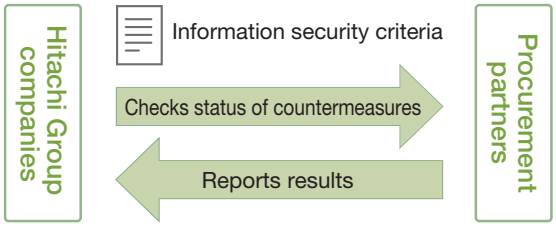
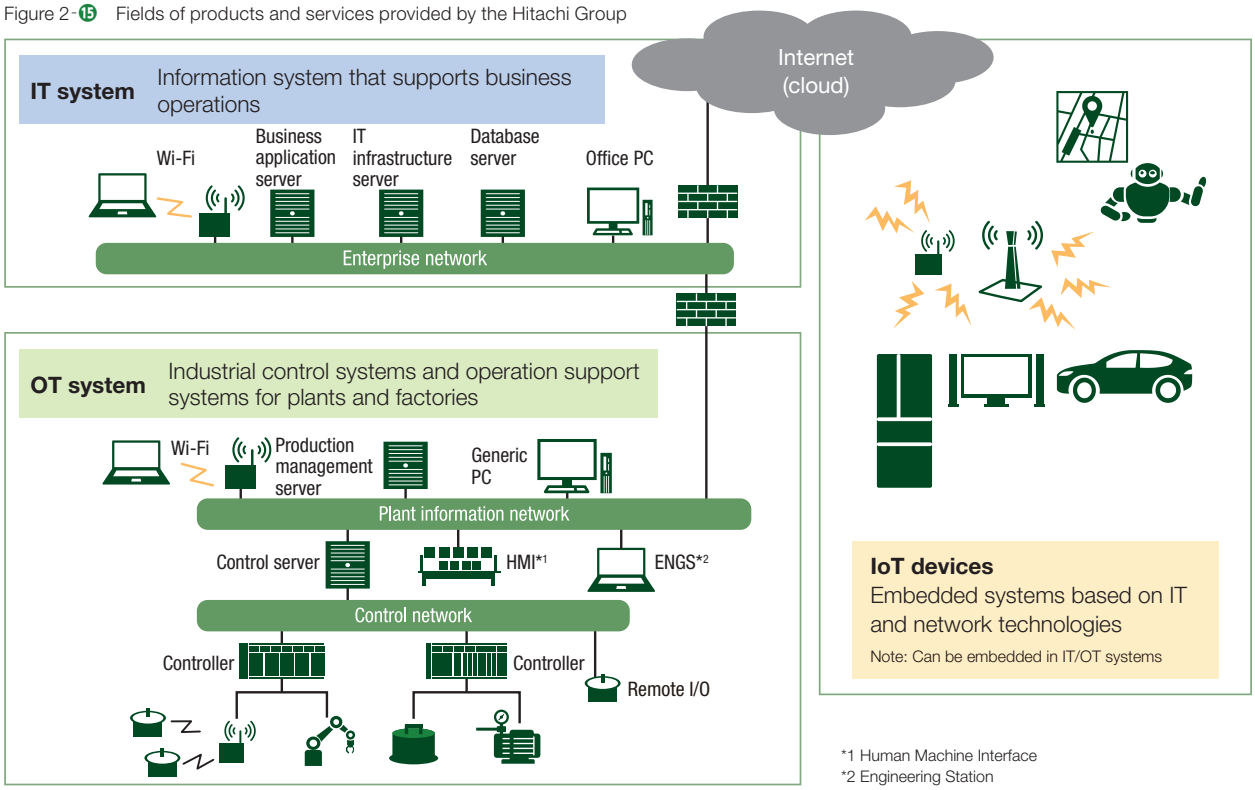


Figure 2-⓮ Security strengthening system in the supply chain

Security initiatives related to products and services

Hitachi's digital solutions business provides new customer value through increasingly sophisticated digitalization and networking technology and more open systems. However, this is accompanied by a growth in cybersecurity risks and the importance of countermeasures for those risks. With the Hitachi Group's IT systems, OT systems, IoT devices, and various other products and services, we continue to drive initiatives to protect customer assets and social infrastructure from cyberattacks. (Figure 2-⓯)

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



*1 Human Machine Interface
*2 Engineering Station

Cybersecurity Initiatives

Security management policy for products and services

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

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

Dissemination of guide material and support activity

Hitachi disseminates various guidebooks and other resources, such as the Secure Process Implementation Guide, to help business sites develop their own security management policies. These materials present case studies of design, production, and maintenance processes from sites that have advanced initiatives against cybersecurity incidents, so that this knowledge can be accumulated and shared across the Hitachi Group.

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

PSIRT and security management system for products and services

We have appointed a person in charge of product security at each BU and Group company and established a security management system under the control of that person. This is based on the Product Security Management System, PSIRD, and the aforementioned “Security Management Policy for Products and Services” and is aimed at continuously providing safe and secure products and services. In order to respond to any vulnerabilities or incidents under the security management system, the Product Security Incident Response Team (“PSIRT”) has been established at the headquarters (of corporate) and at BUs and group companies as an organization in charge of security technical response for products and services. The PSIRTs work together for appropriate response to vulnerabilities and incidents for products and services.

The Hitachi Group’s PSIRTs have established guidelines for their own activities to follow. The PSIRTs meet in regular liaison meetings to present plans and technical information from the headquarters (Corporate) to the BUs and Group companies and to share activities at the sites. To encourage autonomous RSIRT activities in the BUs and Group companies, we provide incident response exercises and other initiatives to the PRISRT members at each site.

Figure 2-⑯ Security management policy for products and services

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

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

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

Cybersecurity Initiatives

Cybersecurity Countermeasures

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

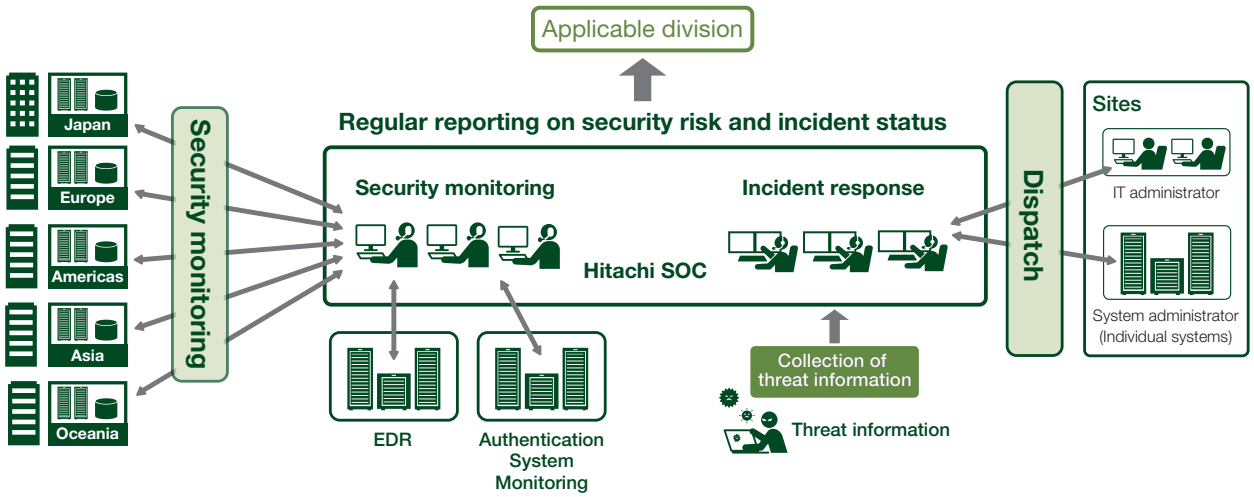
Enhancing security monitoring and incident response

All parties in our supply chain, regardless of size, are at an increasing risk of complex and sophisticated cyberattacks such as targeted attacks, ransomware, and double extortion. To confront such cyberattacks, it is crucial to detect threats and prevent the expansion of damage. To this end, the Hitachi group launched the Hitachi Security Operation Center (Hitachi SOC) in October of 2017 to enhance its security monitoring and incident response capabilities. The Hitachi SOC operates 24 hours a day, 365 days a year to minimize the damage of cyberattacks through early detection of malware infections and unauthorized access. We are also improving our global response capabilities by strengthening cooperation with Europe and the Americas.

Cybersecurity monitoring

The Hitachi Group has established system and network monitoring points with global coverage to integrate, analyze, and monitor logs. Since 2017, the scope has been expanded to reach all core global locations. With the introduction of Endpoint Detection and Response (EDR), we can now also monitor the operation of devices, carry out surveys, and address issues. Recently, there have also been attacks where genuine authentication information is acquired fraudulently and used maliciously. These attacks are difficult to detect because genuine authentic authentication information is used, so we have enhanced our monitoring of the authentication system to allow early detection of fraudulent account use by third parties and attacks on the authentication system. These measures address the new threats posed by new ways of working, such as working from home.

Figure 2-⓲ Global security monitoring and incident response



Incident response

The Hitachi Group has established a handling procedure and a communication structure that come into play when an incident occurs. This allows the cause and scope of impact of an incident to be quickly identified and the appropriate countermeasures to be taken. Since 2020, we have been able to capture the details of any incident more quickly by combining log monitoring of core locations and surveys by EDR and authentication system monitoring. This allows us to reduce the time it takes to determine the priority and need for a response, making incident response more efficient.

The know-how we gather during incident response is then fed back to security monitoring and various internal security measures, making it less likely that the same kind of incident could occur again. (Figure 2-⑱)

Collecting and Analyzing Threat Information, and Disseminating Vigilance Information

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

Collecting, analyzing, and verifying threat information

In addition to the following vulnerability and threat information published on the Internet, we collect threat information for Japan and abroad using various Cyber Threat Intelligence (CTI) services.

- Publication sites operated by public third parties such as IPA, JPCERT/CC*1, and CISA
- Security-related news sites
- Blogs and white papers published by various security vendors

We use the metrics published by the information provider, such as severity levels and CVSS base metrics, to classify threats into five levels of vigilance based on factors such as status of malicious use, likelihood of success, and use of internal systems. For some threats, we use a simulated environment for verification to study the impact and damage that can be used in countermeasures.

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

Disseminating vigilance information

The information collected is disseminated to selected people responsible for cybersecurity of BUs and Group companies through weekly digest emails, immediate email alerts, and intranet postings. Additionally, to enhance countermeasures, when a threat has the potential to widely impact the whole Hitachi Group's operations, we issue a cyber BCP order as well as a cyber warning to urge thorough implementation of countermeasures. We use this collected and analyzed information to enhance incident responses and monitoring, and to collaborate with Hitachi SOC and the IT System Department in hunting for threats.

From the knowledge gained through these activities, we study the facts of the Hitachi Group and countermeasures that need improvement and share the information with the HQ Security Management Division, CISO, and regional branch management divisions. This leads to management-level deliberations on the Group's security strategy to accelerate the execution cycle of security measures.

*1 JPCERT/CC: Japan Computer Emergency Response Team/Coordination Center

Cybersecurity Initiatives

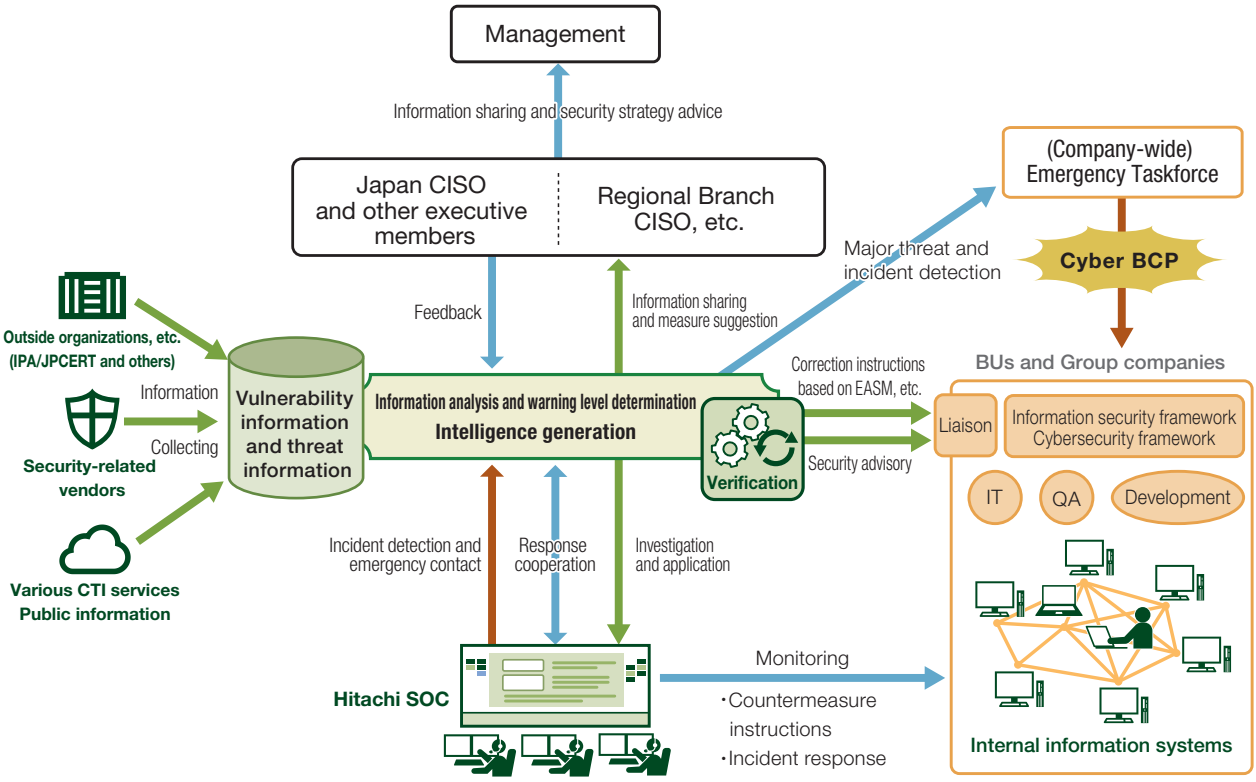
Handling External Attacks

Systems exposed to the Internet are always at risk of external attack. Vulnerabilities in their software and hardware components are discovered and made public nearly every day. Attackers attempt to exploit these vulnerabilities to gain unauthorized access, infect their targets with malware such as ransomware, and steal confidential information. To address these issues, we conduct External Attack Surface Management (EASM) and issue individual corrective instructions to the relevant departments when there is a possibility of damage, thereby reducing the risk of external attacks and speeding up our responses.

Taking action in emergency situations

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

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



Cybersecurity Initiatives

CSIRT Activity in the Hitachi Group

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

What is an incident response team?

A security incident (hereinafter incident) is a human-caused occurrence related to cybersecurity, examples of which include unauthorized access, denial of service, and destruction of data.

An incident response team is a group of people who lead incident operations to resolve issues through inter-organizational and international cooperation. The team's skill set includes understanding and communicating threats from a technical perspective, coordinating technical activity, and liaising with external parties on technical matters. A team with these skills can prevent (through readiness) and resolve (through responsiveness) various issues that might arise.

Model of HIRT activity

The HIRT is responsible for "eliminating vulnerabilities that may pose a cybersecurity threat" and "incident response to prevent and resolve cyberattacks" to support Hitachi's cybersecurity activities. For these purposes, the HIRT has the perspectives of "Internal Activities" and "Collaborative Activities." While the former is about "information security initiatives for our own information system", the latter is about "cybersecurity measures of products and services for our customers". Its mission also includes contributing to the realization of a safe and secure Internet society by detecting the early signs of invisible threats to take preventive action at the earliest possible stage.

The HIRT has adopted a model that consists of four Incident Response Teams (IRTs) to improve vulnerability handling and incident response. The four IRTs are:

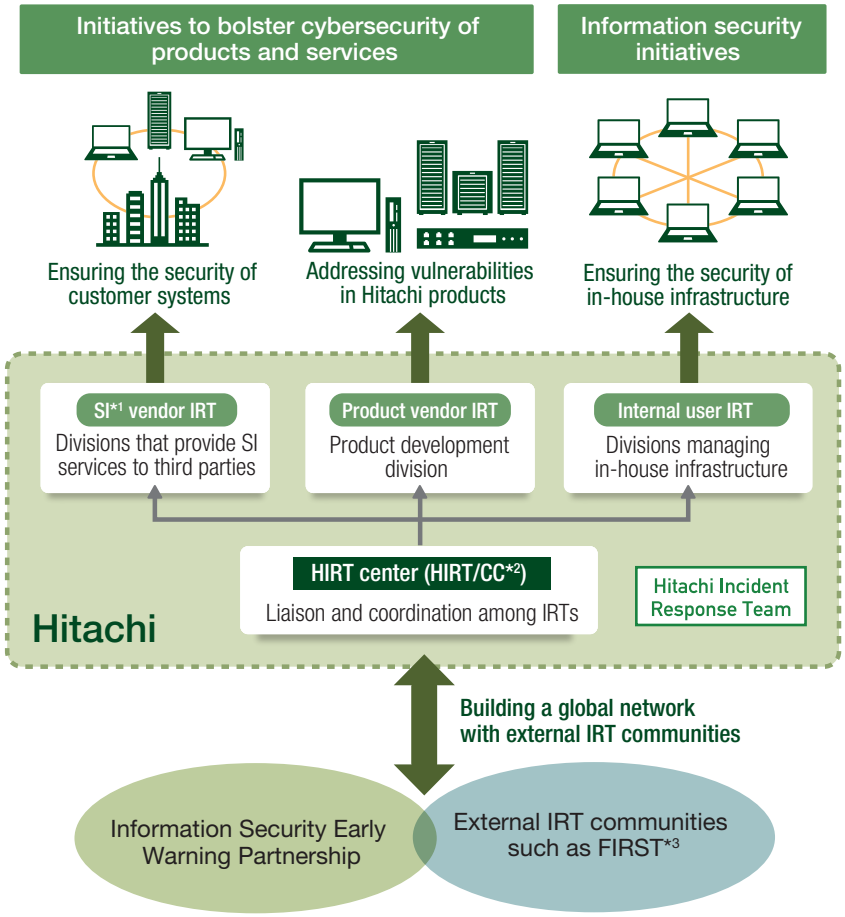
(1) Product vendor IRT, responsible for developing products related to information systems and control systems

(2) System Integration (SI) vendor IRT, responsible for building systems and providing services using these products

(3) Internal user IRT, responsible for managing the operation of Hitachi's information systems as an internet user

(4) The HIRT/CC (HIRT center) which coordinates among these IRTs, combining to create a model that makes the role of each IRT clear and promotes efficient and effective security countermeasures through inter-IRT cooperation. (Figure 2-20)

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



Category	Role
HIRT/CC	Applicable division: HIRT center Promotes vulnerability countermeasures and incident response activity through coordination with external IRT groups such as FIRST, JPCERT/CC and CERT/CC*4, and cooperation with SI vendor IRTs, product vendor IRTs, and in-house user IRTs.
SI vendor IRT	Applicable division: SI/service division Supports vulnerability handling and incident response for customer systems by ensuring their security in the same way as in-house systems in relation to known vulnerabilities.
Product vendor IRT	Applicable division: Product development division Supports vulnerability countermeasures for Hitachi products by investigating from an early stage whether any products are affected by known vulnerabilities, and taking action to resolve any issues found by patches or other means.
In-house user IRT	Applicable division: Divisions that provide internal infrastructure Supports promotion of vulnerability countermeasures and incident response so that Hitachi-related websites do not become the point of origin of a security breach.

*1 SI: System Integration
*2 HIRT/CC: HIRT Coordination Center
*3 FIRST: Forum of Incident Response and Security Teams
*4 CERT/CC: CERT Coordination Center

Cybersecurity Initiatives

Activity promoted by the HIRT center

As for internal activities, the HIRT Center works with the information security supervisory divisions in charge of rulemaking and the quality assurance divisions to promote cybersecurity measures from both a system and technical perspective. At the same time, the center also plays a role in supporting the business divisions and group companies with vulnerability countermeasures and incident response. The HIRT center also serves as a liaison with external IRTs to promote cybersecurity measures in collaboration with external IRT parties.

Internal IRT activity

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

(1) Collecting, analyzing, and disseminating security information

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

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

(2) Developing the research infrastructure

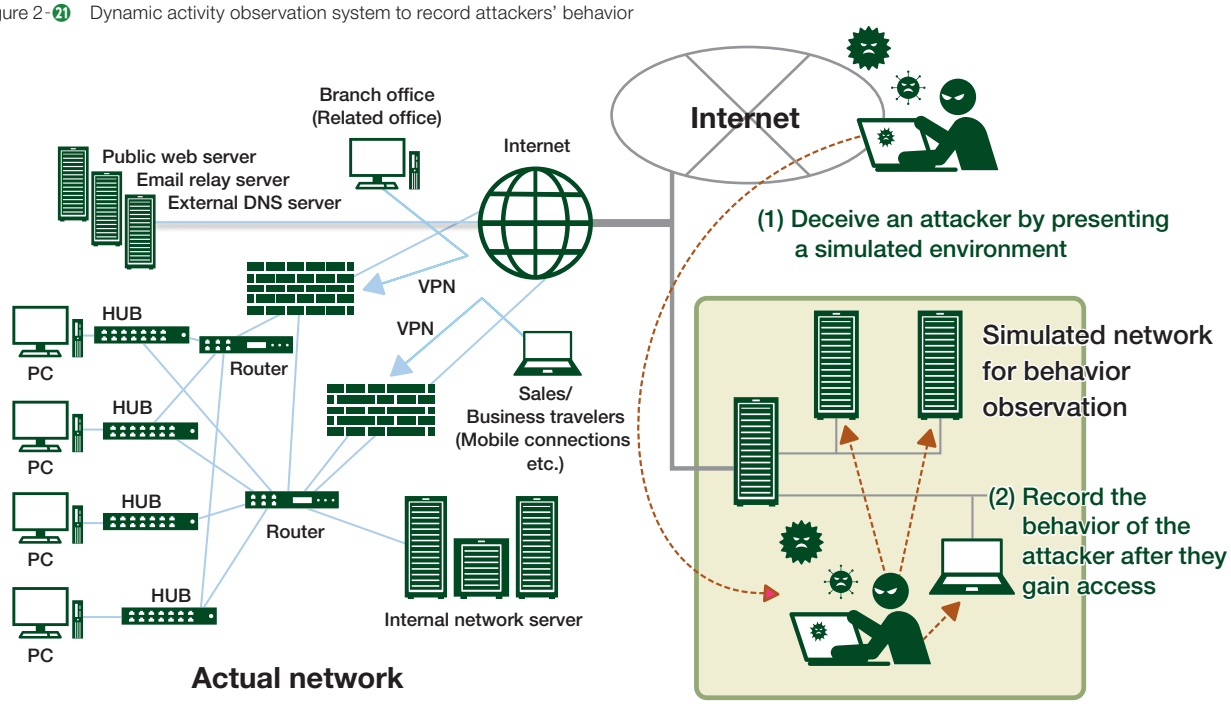
The HIRT center uses behavior observation technology to detect the early signs of invisible threats to take preventive action at the earliest possible stage. Behavior observation is an observational technique that uses a simulated version of an organization's internal network to investigate cyberattacks such as spear phishing. This technique is used to record and analyze the behavior of an attacker who has managed to infiltrate the system. (Figure 2-21)

(3) Improving security technology for products and services

To improve the IRT capability at the organizational level, the HIRT center establishes concrete security countermeasures for products related to information systems and control systems and ensures that skills learned are passed on to the relevant experts. As part of an approach to increasing hands-on internal security awareness, the center develops simulated cyberattack drills that help employees learn about attacks such as targeted attacks and ransomware attacks.

In June 2022, Hitachi became a partner of the CVE Numbering Authority (CNA). Through this partnership, HIRT has been authorized to assign CVE IDs to vulnerabilities in Hitachi products and to create and publish CVE records of the vulnerabilities, enabling us to

Figure 2-21 Dynamic activity observation system to record attackers' behavior



provide products that our customers can use with peace of mind.

(4) Implementing IRT activities byr sector

To take concrete action based on the background and trends in each sector, the HIRT designs and organizes industry-specific IRT activities. As a pioneering initiative in the financial sector, we launched the HIRT-FIS*2 in October 2012.

*2 HIRT-FIS: Financial Industry Information Systems

■ Inter-organizational IRT activities

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

(1) Improving IRT collaboration within Japan

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

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

(2) Improving international IRT collaboration

The HIRT center promotes the development of a collaborative framework with overseas IRT bodies and product vendor IRTs through FIRST activities, as well as the facilitation of an information sharing platform using STIX*4 and the United States Department of Homeland Security's AIS*5 program.

*4 STIX: Structured Threat Information eXpression
*5 AIS: Automated Indicator Sharing

(3) Supporting research activity

Through participation in academic research, including the anti-Malware and anti-cyberattacks engineering WorkShop (MWS), the HIRT Center provides opportunities for talent development and nurtures researchers and our human resources with expertise.

■ 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 considerable importance on personal information protection initiatives to reliably manage personal information kept on customers' behalf and personal information used during business. Hitachi has defined its vision for personal information protection, summarized as providing safety and trustworthiness and recognizing the importance of individual rights. This vision underpins Hitachi's role as a member of a global society.

Vision for personal information protection governance

Hitachi's vision regarding 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 fulfill its mandate as an organization committed to the appropriate handling of personal information, Hitachi's top management has formulated a personal information protection policy. Rules and guidelines for managing personal information are then formulated in-house that conform to this basic policy. Hitachi has a framework in place to check and evaluate whether its internal rules confirm 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 creating these rules, Hitachi implements concrete security management measures that come into effect when handling personal information. There are four aspects to these measures: organizational, personnel, physical, and technical. (Figure 2-㉓)

Figure 2-㉒ Vision for personal information protection governance

VISION

Doing its part to protect personal information as a member of global society

1 Providing safety and trustworthiness

- Hitachi provides a safe and trustworthy environment by observing personal information protection and confidential information management programs (process regulations) based on laws and other regulations.

2 Recognizing the importance of individual rights

- Hitachi faces the global trend of respecting the rights of the individual from a good faith position.
- Personal information protection equates to the protection of a fundamental human right, and Hitachi considers it a key issue in terms of business management.

Personal information protection policy

Hitachi, Ltd. is a global supplier of total solutions. In this role, Hitachi handles all types of information including its own technical information and information it holds on behalf of customers. Reflecting how highly it values this information, Hitachi has established an information management framework and endeavored to enforce it. 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/).

(1) Establish rules for managing personal information protection and make continual improvements

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

(2) Collect, use and provide personal information and forbid the use of 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) Implement safety measures and correct problems

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.

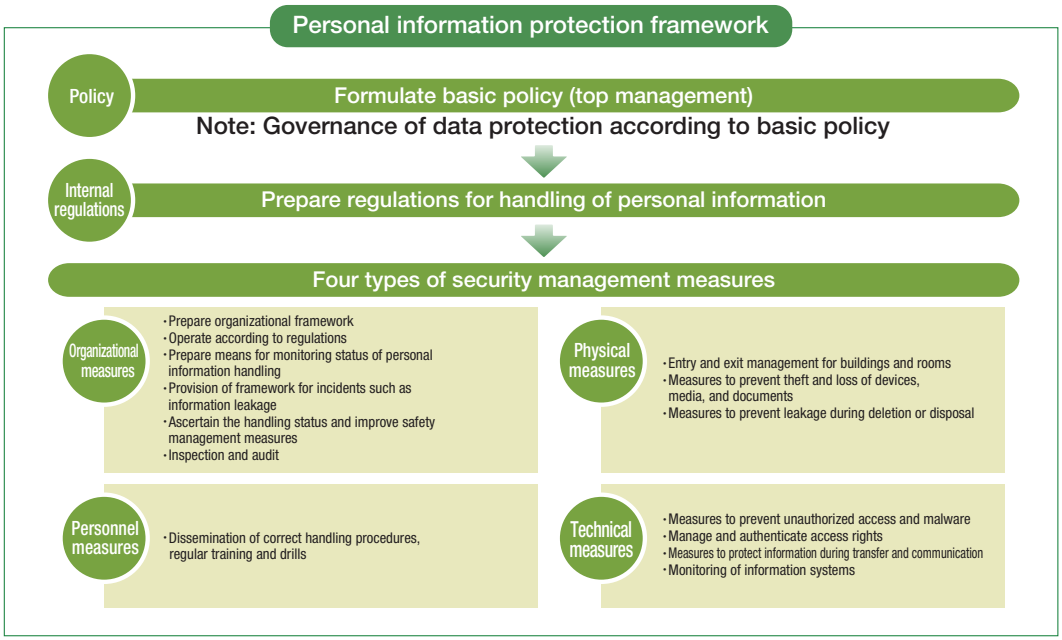
(4) Comply with laws and norms

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 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

■Personal information protection system

Through our information security promotion framework, headed by the CEO, we thoroughly apply our policies on the protection of personal information, and manage personal information appropriately. All Hitachi, Ltd. BUs and business sites appoint information asset managers in all departments, under the information security officer, and allocates responsibilities in relation to the handling and protection of personal information. Similar organizations are established in Group companies, to foster thorough personal information protection and management throughout Hitachi Group.

■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 person 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 take 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.

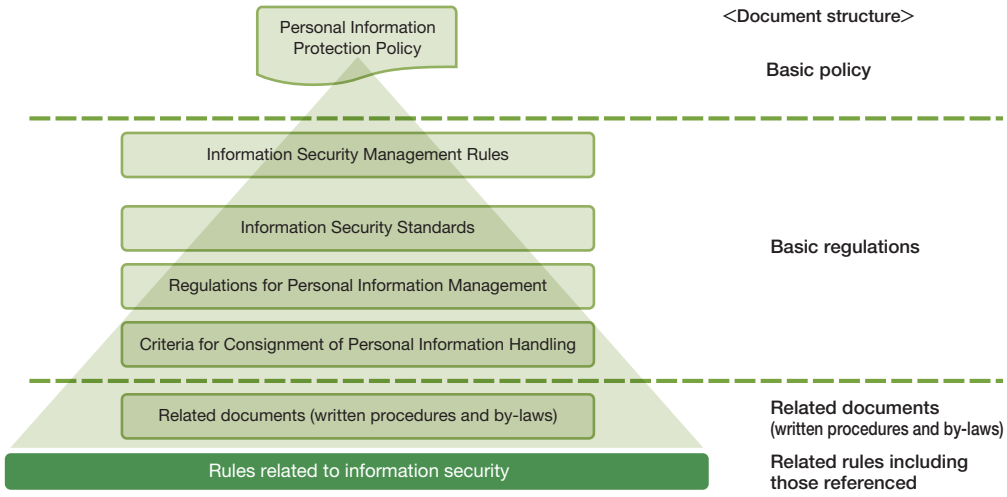
The 52 article of "Infomation Security Management Rules" define the rules for personal information protection management.

The handling of personal information is based on the 73 articles of "Regulations for Personal Information Management", on the 12 articles of "Criteria for Consignment of Personal Information Handling", and on related documents.

■Personal information protection management cycle

Hitachi's framework for personal information protection

Figure 2-㉔ System of personal information protection rules



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 company president.

In the “Do” stage, the personal information protection measures are disseminated and used in-house.

Personal information protection training is conducted to make the personal information protection measures and management approach well-known throughout Hitachi.

Hitachi also holds meetings to promote personal information protection matters, using these meetings to provide information and to report the status of implemented measures.

In the “Check” stage, Hitachi asks each department to conduct regular self-checks of its operations, and conducts audits based on the audit plan to check the status of other divisions. The person responsible for the audit formulates a written company audit plan and written report and has them approved by the company president. If there are any matters raised by these audits, Hitachi remains vigilant until the issues are remedied.

In the “Action” stage, Hitachi revises its management system based on various factors. These include changes to legal obligations 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

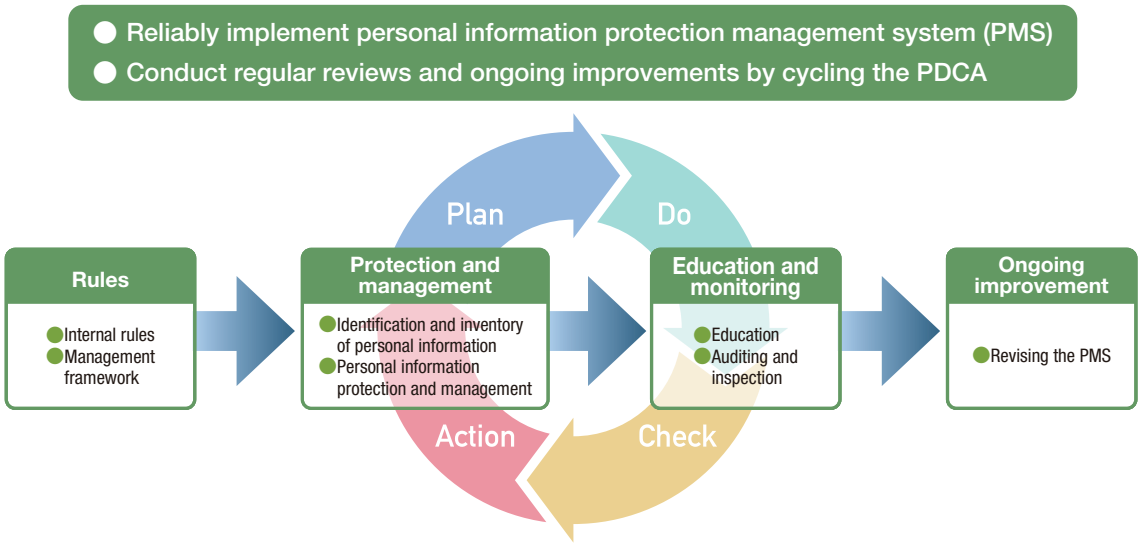
To ensure protection of personal information at a level exceeding that specified by the Personal Information Protection Act, Hitachi has established internal regulations equivalent to the stipulations of JIS Q 15001 (“Personal information protection management systems—Requirements”). These regulations are the basis for Hitachi’s efforts to strictly manage and appropriately handle personal information. Each department nominates a person to be responsible for personal information management (an information asset manager). This person identifies all personal information handled during business, and manages it while taking the appropriate measures according to the importance of and risk associated with the personal information.

For each business operation that handles personal information, Hitachi recognizes and analyzes the associated risks. Hitachi defines rules for business operations that handle personal information. These rules are centrally managed by the company and regularly reviewed.

People who handle personal information are informed of the rules for its handling, and leave a record of having confirmed them before starting their work. During operations, each workplace conducts a monthly self-check to assess the status of safety management measures and operations.

Hitachi’s internal regulation also comply with the standards required by the My Number system, Japan’s

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



Initiatives for Data Protection

system of social insurance, tax numbers and others. Based on these regulations, Hitachi makes every effort to manage and handle this information with the necessary discipline. Hitachi has established a framework for managing My Number information. It uses this framework to evaluate the risk of business operations that handle My Number information, and ensure the appropriate measures are taken.

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.

A "personal information protection and information security audit" reviews compliance with personal information protection and management, and audits compliance with legal requirements.

Group companies outside Japan perform common global self checks to monitor compliance status in a Hitachi-wide inspection process. All Hitachi, Ltd. departments perform "Personal Information Protection and Information Security Operation Checks" annually, as self-inspections in the workplace. In addition, departments involved in operations that handle important personal information perform "Personal Information Protection Operation Checks" every month. With these measures, we regularly check safety management measures and their operational status.

Educating employees about personal information protection and promoting their understanding

To ensure that personal information is reliably protected, Hitachi conducts annual training by e-learning of all executives, workers, and temporary employees. Hitachi, Ltd., gives each of its employees a personal information protection card that outlines Hitachi's personal information protection policy and basic matters regarding information security.

Strengthening subcontractor management

Hitachi has taken the early initiative to enhance its policies regarding subcontractors' handling of personal information. It has established internal regulations that apply when subcontracting the handling of personal information and implemented screening and supervision of subcontractors. When subcontracting business operations, Hitachi screens its subcontractors so that only those whose level of personal information protection equals or exceeds that of Hitachi are selected. The contracts Hitachi signs with its subcontractors incorporate strict provisions regarding personal information management. These provisions might include the need to establish a management framework and a ban in principle on further subcontracting. As part of its approach to managing and supervising subcontractors, Hitachi also conducts regular assessment of its subcontractors and reminds them of their obligations.

*As of March 2024

Global personal information protection initiatives

Advancements in data utilization driven by the remarkable progress being made in digitalization will inevitably result in increased privacy risks. Countries all over the world are formulating and revising legal frameworks related to personal information protection, strengthening such protection in response to rising demand.

With the widespread use of data across national borders, the legal systems of various countries may require the protection of personal information in the home country for businesses located abroad, or may regulate the cross-border transfer of personal information to other countries. For this reason, compliance for personal information protection must be based on a thorough understanding of current trends in various countries' legal systems.

Hitachi has taken the initiative by promoting compliance with the EU's General Data Protection Regulation (GDPR).

In order to promote appropriate compliance with personal information protection laws and regulations at Group companies in each region, functions to support local Group companies have been established at regional headquarters in the Americas, Europe, Asia, India, and China, and compliance with laws and regulations in each country is being promoted.

Hitachi is also promoting compliance with the Chinese Personal Information Protection Law and the data protection laws of other countries and regions through cooperation with regional headquarters.

We have enacted the Hitachi Group Privacy Principles as a common code of conduct for personal information protection throughout the Hitachi Group, and appointed Data Protection Managers to ensure thorough action on personal information protection in each Group company. 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.

All Hitachi Group companies will continue to bolster and develop their ability to comply with personal information protection regulations.

PrivacyMark*-Related Initiatives of the Hitachi Group

The Hitachi Group engages in personal information protection as a single entity.

The first instance of PrivacyMark certification by a Group company was in 1998. As of the end of July 2022, 38 business operators now hold this certification. These businesses protect and handle personal information at a higher level than that required by law.
Hitachi, Ltd. received its ninth certification in March 2023 and is continuously working towards the next renewal in March 2025.

In addition, the “Hitachi Group P Mark Liaison Committee” is organized mainly by companies that have acquired the Privacy Mark, and regularly holds information exchange meetings, study sessions, and lectures by invited outside experts, as well as sharing and studying information on personal information protection throughout the Group.

* 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

Website for 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 2024, the following Hitachi Group companies hold PrivacyMark certification:

- Hitachi, Ltd.
- Hitachi, Ltd., Corporate Hospital Group
- Hitachi Kenpo
- Okinawa Hitachi Network Systems, Ltd.
- Kyushu Hitachi Systems, Ltd.
- Shikoku Hitachi Systems, Ltd.
- SecureBrain Corporation
- Nichiwa Service, Ltd.
- Hitachi ICT Business Services, Ltd.
- Hitachi Academy Co., Ltd.
- Hitachi Pharma Information Solutions, Ltd.
- Hitachi Information Engineering, 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.

Initiatives for Data Protection

Privacy Protection Initiatives

Advancements in digital technologies such as AI and IoT have set high expectations for social innovation using the varied and vast data they produce. However, public awareness is also growing around privacy protection for consumers. Hitachi is taking the initiative regarding privacy protection to foster value creation in a way that protects people's safety and security.

Hitachi's Approach to Privacy Protection

Recently, all businesses are expected to use personal data to create value, regardless of whether it is deemed "personal information". This situation demands concern for personal privacy. In the DX era, the amount of personal data collected is increasing exponentially, which inevitably changes the privacy risk a business must manage. As Figure 2, there is a partial overlap between personal data and information about an individual. For example, they include information like location data and purchase histories which have privacy implications.

To create value using personal data, a business must protect personal information while also protecting privacy. (Figure 2-26)

Hitachi also applies its privacy protection know-how to its customers' businesses by offering better services and technology that consider privacy. In this way, Hitachi helps make progress towards safe and secure social innovation.

Hitachi's privacy protection initiatives

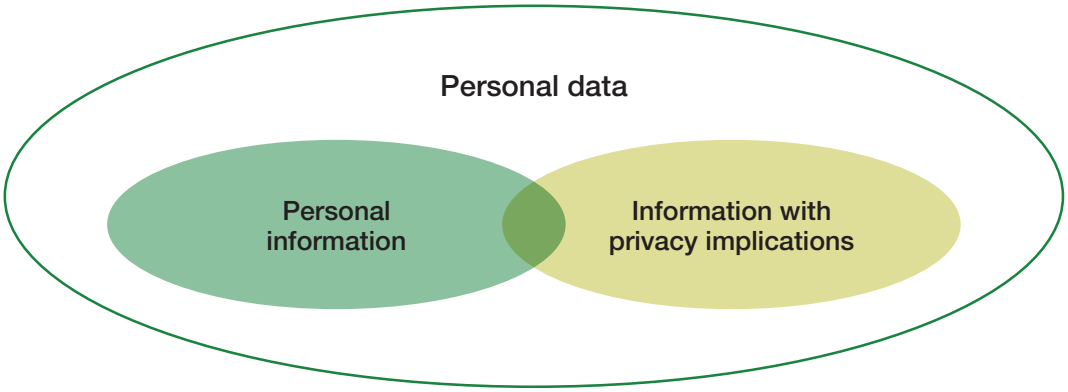
Hitachi, Ltd. seeks to create value through the safe and secure use of personal data. To this end, Hitachi has been working on privacy protection initiatives for data use in the Digital Systems & Services Sector since 2014.

Furthermore, in response to societal demand for privacy protection measures, Hitachi aims to provide more appropriate and high-quality services and products and build trust with consumers and other stakeholders by balancing privacy protection and its use of personal data. In order to do so, Hitachi introduced the Hitachi Privacy Protection System (hereinafter referred to as the "PIA System") in 2023 and is working on privacy protection measures by conducting Privacy Impact Assessments for operations that handle personal data.

In promoting the PIA System, we have developed guidelines and check-sheets for employees, and we explain the specific process of privacy-impact assessment and the points to keep in mind for the check-sheets, so that individual employees are able to implement privacy protection measures. If employees have difficulty making decisions when preparing the check-sheets, we provide support through individual consultation. At the same time, we provide periodic training to raise awareness of privacy protection.

Additionally, in the Digital Systems & Services Sector, which drives our digital business, in light of the nature of the business, we have established a "Personal Data Officer" to oversee the handling of personal data and a "Privacy Protection Advisory Committee" to gather knowledge on privacy protection, assess risks, and support the consideration of countermeasures, as part of our more proactive approach to privacy protection.

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



Internal and External Activity Related to Information Security

Recent cyber attacks 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, it is vitally important to build a security ecosystem that goes beyond internal departmental boundaries and also collaborates with external organizations. To that end, we are building a framework for inter-divisional collaboration, between divisions other than security, through various internal activities. We also participate actively in external activities, to enable collaborative creation with others in industry, government, and academia.

Internal Activity Related to Information Security

Now that we are in an environment where devices, systems, and other things “interconnect” in the IoT, even divisions which previously had few occasions to think about security must do so. Therefore we organize seminars, workshops, and other events to build communities beyond barriers of position or organization, in addition to thorough implementation of measures by using IT systems and tools, and controls such as rules, regulations, and guidelines. These opportunities strengthen security by helping participants to reaffirm their individual roles and deepen connections with those around them.

We are holding workshops in the Americas, Europe, China, India, and other regions of Asia as activities to deepen understanding of measures we are promoting as internal controls. In Japan, our panel discussions and workshops provide opportunities to learn specialized security knowledge and insights from a perspective completely different from those of security and IT experts. Points raised and lessons learned at these events are then shared.

External Activity Related to Information Security

We communicate with communities that transcend frameworks, to share matters such as threat information and issues arising when countermeasures are applied, with other nations, academia, and companies which are working to promote cybersecurity.

Hitachi participates in global communities to that end. 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 cyber attacks. 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.

We also use the knowledge and experience of our employees to participate in various external activities related to information security, such as the 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 TC 262 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 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-99WG
IEC's TC65 promotes the standardization of industrial automation, measurement, and control. Within it, WG10 is working with the ISA-99WG 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.
• OASIS CTI
The Organization for the Advancement of Structured Information Standards (OASIS) Cyber Threat Intelligence (CTI) committee assesses the standardization of the Structured Threat Information eXpression (STIX) format for exchanging cyber threat intelligence and procedures for automatically exchanging detection index information.

■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

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

• Information-technology Promotion Agency (IPA): Ten Major Security Threats Authors' Committee, etc.
• Japan Institute for Promotion of Digital Economy and Community (JIPDEC) ISMS Expert Committee, etc.
• Japan Cybercrime Control Center (JC3)
• Japan Information Security Audit Association (JASA)
• NPO Japan Network Security Association (JNSA)
• Information Security Operation providers Group Japan (ISOG-J)
• Japan Digital Trust Foundation (JDTF)
• Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) PA/FA Committee on Instrumentation and Control, Security Research WG
• Control System Security Center (CSSC)
• Japan Electronics and Information Technology Industries Association (JEITA), Information Security Expert Committee, Personal Information Protection Expert Committee, etc.
• Council of Anti-Phishing Japan
• National Institute of Technology and Evaluation (NITE) Evaluation Body Certification Technical Committee
• Robot Revolution & Industrial IoT Initiative
• CRIC Cross-Sector Cybersecurity Committee, CRIC Security Quality Committee, etc.
• Japan Society of Security Management (JSSM)
• The Society of Instrument and Control Engineers (SICE), Industrial Application Division, Technical Committee on Industrial Networks System
• Japan Automatic Identification Systems Association (JAISA)
• ICT-ISAC
• Japan Data Communications Association, Telecom-ISAC Japan
• J-Auto-ISAC
• Transportation ISAC JAPAN
• JE-ISAC

Working to Raise Information Security Awareness

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

"Jibungoto (ownership)" in information security

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

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

We have begun expanding and enhancing education and awareness-building for employees and moving forward with more balanced security measures, in order to adapt to the current dramatically-changing work-styles of employees and to reduce future security risks. We see improving security awareness as the last line of defense, so in addition to our existing strict governance, we are working to raise security awareness by encouraging employees to take the initiative and act independently. Our goal is to get employees interested in the issues and have them take ownership of security, rather than taking a passive role. Our mottos for this approach are "Jibungoto (ownership)" and "Sharing a common mindset".

Encourraging self-initiative: Harry's Security

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

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

We use the newly developed mascot character "Harry" with animations, chats, and other means to get closer to employees by making information dissemination more fun and accessible.

Figure 3-❶ 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 3-❷)

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.

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

Figure 3-❷ Green Aegis Activities

Behavior 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

Created Kiken(Risk) Yochi(Prediction) Training(Training) (“KYT”) materials with employee participation

In 2023 we began creating materials for hazard prediction training (known as “KYT”) featuring “Harry,” our security character. KYT is training to consider what hazards are present in a given situation. Our employees participated in the process of creating these materials. We gathered ideas from our employees on what kinds of dangers lurk in what kinds of situations. From the candidate themes created based on these ideas, the final themes of “Misdirected Emails” and “Conversation in Public Places” were defined based on votes from employees and used in creating the materials. The resulting educational materials are available on our intranet and incorporated into our information security e-learning programs so that they can be widely used. By having employees participate in the creation of these materials, we aim to provide an opportunity for them to think about security in their daily lives, and at the same time, to make the finished educational materials feel relatable to them.

COLUMN

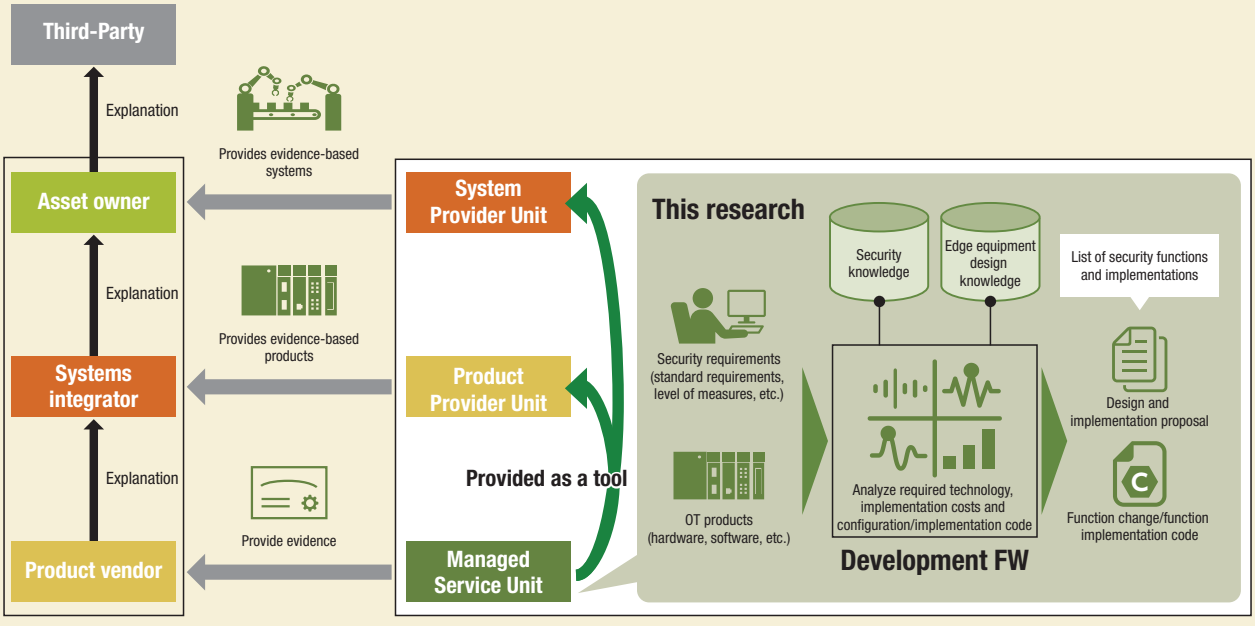
Technology development addressing imminent security laws and regulations

**In recent years, the European Cyber Resilience Act and other security legislation have increased the regulation of security responses on a global scale.
Businesses will be excluded from markets if they fail to comply with regulations. Therefore, it is vital to respond appropriately and efficiently. Hitachi is developing technologies to meet security legal and regulatory requirements in an accountable manner, as well as to streamline security responses in the operational phase and supply chains.**

Accountable Security Technology

The threat of cyber attacks on the Industrial Internet of Things (IIoT) is becoming increasingly apparent. Accordingly, companies that handle IoT products are required to implement reasonable measures that achieve both compliance with security regulations and performance of systems and devices, and to explain these measures to the outside world. In order for a measure to be accountable, the validity of the measures implemented in the devices that make up a system is important. As shown in the diagram below, the asset owner must be able to explain that the security of the system provided by the system integrator is assured, in order to explain to third parties that the security of their own assets is assured. The same is true for system integrators and equipment vendors. In other words, accountability for the security of the equipment provided by the equipment vendor is the starting point for being accountable, and it also ensures accountability for the system integrator and asset owner. Hitachi defines accountability as “the ability to explain the security functions and requirements necessary for OT systems and devices,” and aims to ensure accountability by presenting specific design and implementation proposals for devices. Specifically, by solving the requirements of security regulations as a “constraint satisfaction problem” in which the performance of the system or device is considered as a constraint, we derive secure countermeasures that satisfy all the conditions to be considered, are valid, and can be implemented in the device. To evaluate the work quantities required to derive countermeasures, we created a prototype using OSS (open source software) and confirmed that the work quantity required to explain the validity of the countermeasures to a third party could be reduced by more than 1/20.

Diagram ❶ Overview of Accountable Security Technology



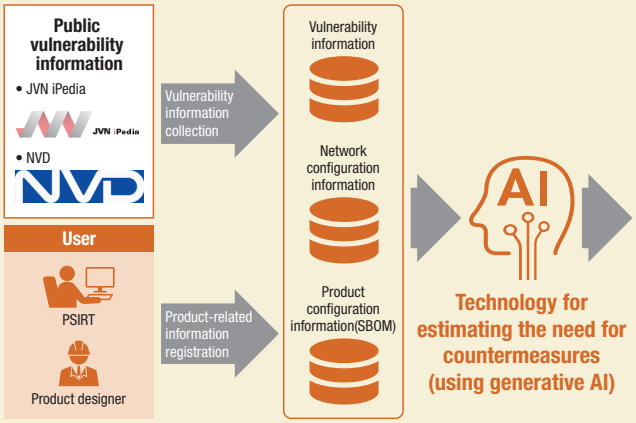
Vulnerability management and SBOM utilization in the operation phase

PSIRTs (Product Security Incident Response Teams) are being established in various companies to protect product security during the operation phase. Vulnerability handling by PSIRTs involves collecting vulnerability information on a daily basis, and selecting vulnerabilities that are likely to affect the company's products and services and are also expected to be highly dangerous. Selected vulnerabilities are analyzed in detail to determine whether or not they could be exploited to attack the company's products or services.

With the recent increase in the use of OSS and the greater number of vulnerabilities discovered, the work quantities required for vulnerability handling by PSIRTs are increasing, and the number of experts is limited so it is becoming difficult to carry out the work. While we have developed technologies to narrow down the vulnerabilities to be analyzed, detailed analysis of each vulnerability after doing so still requires large amounts of work.

In response, Hitachi has developed a technology that extracts the conditions necessary for exploitation from the description of the vulnerability, and presents the results of the condition applicability judgment and investigation viewpoints by comparing them with the product configuration information (SBOM, network configuration information, etc.). This proposed method is expected to reduce the work quantity required for vulnerability handling by up to 40% compared to the existing technology alone.

Figure ❷ Overview of Vulnerability Countermeasure Necessity Estimation Technology



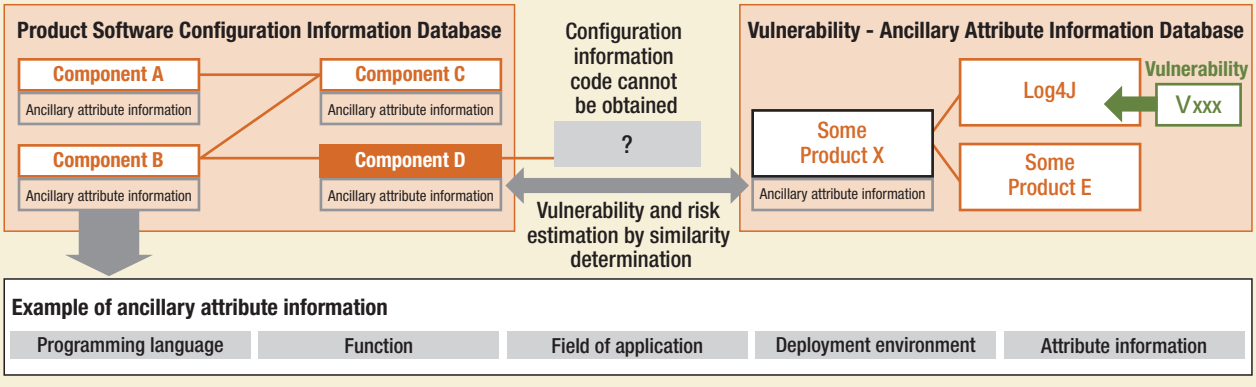
Priority ranking	Perspective	Conditions for attack success	Rationale/Suggestions	Applicability
1	Software	zlib	The software concerned is present in SBOM(xxx.spdx.json).	Applicable
2	Version	1.2.12	The software concerned is present in SBOM(xxx.spdx.json).	Applicable
3-1	Function	inflateGet Header	There is no function that calls the corresponding function.	Not applicable
3-2	Source file	inflate.c	The corresponding source file does not exist.	Not applicable
4	NW path existence	-	Network path from device A to target device C exists.	Applicable
…	…	…	…	Unconfirmed

- In judgments of the necessity of countermeasures, automatically and thoroughly extract points to be checked by the operators from vulnerability information.
- Assign priority to each extracted check item from each perspective, based on how low the checking work quantity is and on its level of persuasiveness to the customer, then present the work priorities.

Software Supply Chain Security

Recent software has many pieces of open source and commercial software built in, and includes components with restrictions on obfuscation and disclosed information. For components for which source code and software configuration information cannot be obtained, it is difficult to determine vulnerabilities and risk manifestations, which poses a challenge for security measures in the software supply chain. As a method to effectively validate malicious functions even when software configuration information is incomplete, we have developed a technology to estimate the vulnerabilities and risks of software components based on the similarity of their databased attributes, such as programming language, deployment environment, and software utilization domain information, to the ancillary data of other software for which risk information is already known. This technology helps reduce software security risks across the supply chain.

Diagram ❸ Overview of vulnerability risk estimation techniques based on software similarity



Third-Party Evaluation and Certification

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

Status of ISMS certification

The following Hitachi organizations 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 2024). The names of the organizations are as they appear in the list of ISMS-accredited organizations maintained by the ISMS-AC.

- Hitachi, Ltd. (Financial Information Systems 2nd Division, Governmental & Public Financial Systems Division)
- Hitachi, Ltd. (Cloud Services Platform Business Unit, Managed Services Business Division, Digital Platform Business Division, Digital Engineering Business Unit, Applications Services Division, Lumada Solutions Operation, Data & Design,Business Development)
- 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. (Water & Environment Business Unit, Value Chain Business Development Division, DX Solutions Development Department, Environment Solutions Division, Information System Engineering Department, Connective Industries Division, Information Technology & Business Process Innovation Division, Secure IT Innovation Center, Secure Information Group)
- Hitachi, Ltd., Social Infrastructure Systems Business Unit, Defense Systems Division (Yokohama Office), Corporate Sales & Marketing Group, Digital Systems & Services Business Sales Management Division, Defense Systems Sales Management, and Hitachi Advanced Systems Corporation (HQ)
- Hitachi, Ltd. (Industrial Digital Business Unit Enterprise Solutions Division, DX Cloud Solutions Department)
- Hitachi Channel Solutions, Corp.
- Hitachi Social Information Services, Ltd.
- Japan Space Imaging Corporation
- Hitachi Information & Telecommunication Engineering, Ltd. (Managed Services Department)
- Hitachi ICT Business Services, Ltd. (System Engineer Support Center, Media Service Group)
- Kyushu Hitachi Systems, Ltd.
- Hitachi Systems, Ltd. (Financial Digital Transformation Division, Office 2, ATM Services Department)
- Hitachi Systems, Ltd. (Public & Social Business Group)
- Hitachi Systems, Ltd. (Public & Social Platform Services Division)
- Hitachi Systems, Ltd. (Contact Center & BPO Services Division)
- Hitachi Systems, Ltd. (Solution Business Administration Group, Maintenance Business Promotion Division, Platform Support Department)
- Hitachi Systems, Ltd. (Industrial & Distribution Business Group, Industrial & Distribution Solution Services Division 1, Digital Life Science Services Office, Health Support Services Department)
- Hitachi Systems, Ltd. (Managed Services Division, Security Services Division)
- Hitachi Systems Power Services, Ltd. (Information and Communication Technology Services Division, Platform Systems Services Office)
- Hitachi Systems Engineering Services, Ltd. (Managed Services Business Group)
- Hokkaido Hitachi Systems, Ltd.
- Hitachi Solutions Create, Ltd.
- Hitachi Solutions West Japan, Ltd. (Cloud Platform Operating Support Department)
- Hitachi Solutions East Japan, Ltd.
- Hitachi Solutions, Ltd.
- Hitachi Power Solutions Co., Ltd.
- Hitachi Pharma Information Solutions
- Hitachi KE Systems, Ltd. (Tokyo Development Center)
- Hitachi High-Tech Corporation(Solution Center)
- Hitachi Management Partner Corp.(Business Planning Division, Human Resources Solution Division)

Status of IT security evaluation and certification

The following table lists the key products certified under the Japan Information Technology Security Evaluation and Certification Scheme run by the Information-technology Promotion Agency (IPA) based on ISO/IEC 15408. (This includes listing in the “archived list of certified products” as of the end of September 2024) (Figure 5-❶)

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

Product	TOE type*1	Certification No.	Evaluation assurance level*2
HiRDB/Parallel Server Version 8 08-04	Database management system	C0225	EAL4+ALC_FLR.1
HiRDB/Single Server Version 8 08-04	Database management system	C0216	EAL4+ALC_FLR.1
HiRDB Server Version 9 (Linux Edition) 09-01	Database management system	C0351	EAL2+ALC_FLR.2
Smart Folder PKI MULTOS application 03-06	Smart card application software	C0014	EAL4
Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software 8.0.1-02	Access Control Device and Systems	C0536	EAL2+ALC_FLR.1
Hitachi Virtual Storage Platform G1000, Hitachi Virtual Storage Platform VX7 Control Program 80-01-25-00/00 (R8-01A-06_Z)	Storage device control software	C0514	EAL2+ALC_FLR.1
Hitachi Unified Storage VM Control Program 73-03-09-00/00 (H7-03-10_Z)	Storage device control software	C0513	EAL2+ALC_FLR.1
Microprogram 0917/A for Hitachi Unified Storage 110	Storage device control software	C0421	EAL2
Microprogram 0917/A for Hitachi Unified Storage 130	Storage device control software	C0420	EAL2
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	Biometric device	C0332	EAL2
Certificate Validation Server 03-00	PKI	C0135	EAL2
CBT Engine 01-00	Major application of CBT examination system	C0288	EAL1+ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
Security Threat Exclusion System SHIELD/ExLink-IA 1.0	Security Management Software	C0090	EAL1

*1 TOE (Target Of Evaluation)

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

*2 EAL (Evaluation Assurance Level)

ISO/IEC 15408 stipulates the degree of assurance of evaluation items (assurance requirements) in a range from EAL1 to EAL7. A higher level means more stringent evaluation.

- EAL1 involves the validation and testing of security functions and the objective evaluation of guidance used to maintain security.
- EAL2 adds vulnerability analysis with respect to typical attack vectors and evaluation from the perspective of product integrity from manufacturing to commencement of operation. This adds a security perspective to the standard development lifecycle.
- EAL3 adds to the assurance of EAL2 by evaluating the development environment to assure the comprehensiveness of testing and prevent tampering of the product during development.
- EAL4 is considered a high level of assurance for general consumer products, and evaluates the entire development lifecycle including the integrity of development assets in the development environment, the source code of the product, and the trustworthiness of personnel.
- ALC_FLR.1 objectively evaluates the basic procedures for providing the necessary patches when a security defect is found in the product. You can use this assurance level to add assurance requirements not included in the EAL of the standard. The level is expressed as EAL2+ALC_FLR.1, for example.

  ALC_FLR.2 requires that procedures are in place to accept reports about vulnerability information and to notify users.

Third-Party Evaluation and Certification

Status of testing and certification of cryptographic modules

The following table lists the main products certified by the Japan Cryptographic Module Validation Program (JCMVP) based on ISO/IEC 19790 operated by the IPA or the Cryptographic Module Validation Program (CMVP) based on FIPS 140-2 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 September 2024) (Figure 5-❷)

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

Product	Certification No.	Level
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.

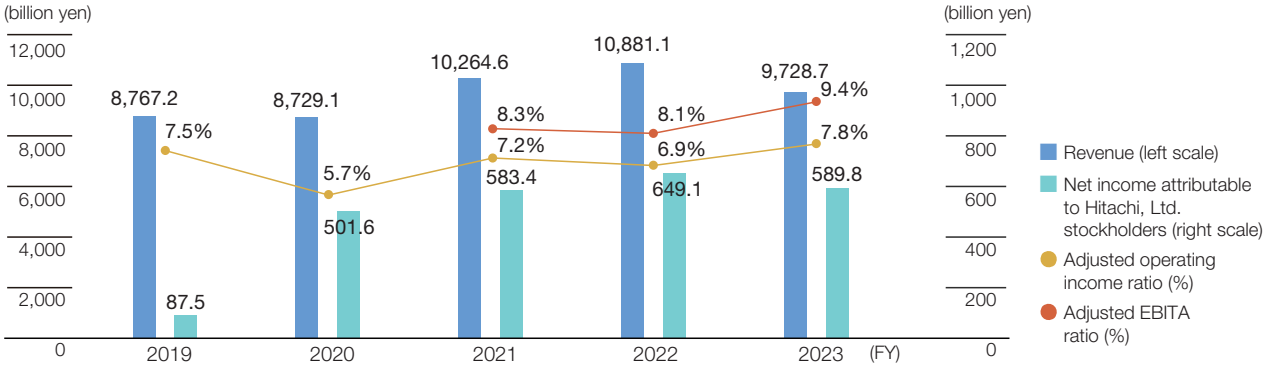
Overview of the Hitachi Group

Company Profile (As of March 31, 2024)

Corporate name	Hitachi, Ltd.	**Representative**	Keiji Kojima, President and CEO
Incorporated	February 1, 1920 (founded in1910)	**Capital**	463.417 billion yen
Head office	1-6-6 Marunouchi,Chiyoda-ku, Tokyo,Japan	**Number of employees**	268,655 (Japan: 113,737, outside Japan:154,918)

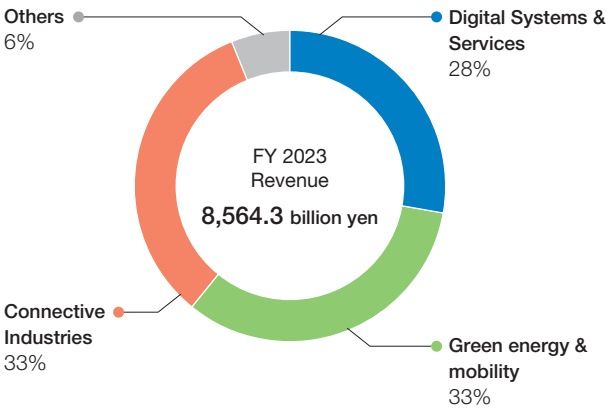
Business Performance Highlights for FY 2024, Based on the International Financial Reporting Standards(IFRS)

Revenue	9,728.7 billion yen (89% year on year)	**Adjusted EBITA**[*1]	918.1 billion yen (up 33.5 billion yen, year on year)
Net income attributable to Hitachi, Ltd. stockholders	589.8 billion yen (down 59.3 billion yen, year on year)	**Adjusted operating income ratio**	7.8% (up 0.9 percentage points, year on year)
		Adjusted EBITA ratio	9.4% (up 1.3 percentage points, year on year)

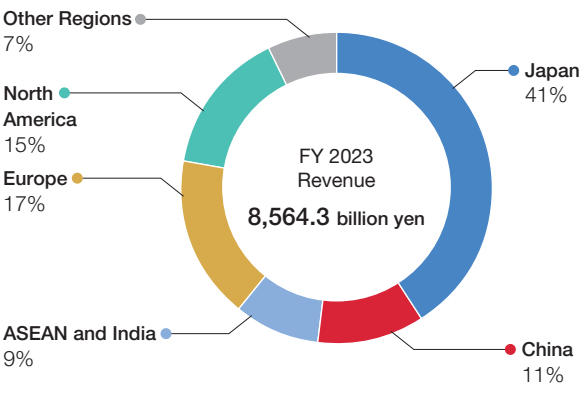


*1 Adjusted EBITA (Adjusted Earnings Before Interest, Taxes and Amortization): Adjusted operating income + Acquisition–related amortization + Share of profits (losses) of investments accounted for using the equity method

Business Composition*



Revenue by Region*



*Note: Figures are for the continuing consolidated business (three sectors), excluding Hitachi Metals and Hitachi Construction Machinery, which were deconsolidated in FY2022, and Hitachi Astemo, which is scheduled to be deconsolidated in FY2023. The figures on this page are FY2022 results

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