HITACHI
Inspire the Next

Information Security Report 2022

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 2021
- Report publication date: October 2022

CISO Interview

“One Hitachi” Initiatives for Swift and Flexible Information Security Response

— Recently we've seen many news reports of ransomware attacks on companies, municipal systems, and hospitals. What's your view of this situation? And what is most important for people involved in security as they develop countermeasures?

Ransomware attacks have been getting increasingly sophisticated and diverse in the last year. Everyone is at risk of attack from anywhere in the world, and companies' overstretched supply chains are the starting points for attacks in growing numbers of cases. What's more, the current tense international situation appears to be accelerating the frequency of attacks.

When developing countermeasures, it's important to have an overview of information security within its context of international conditions and historical background. Why is Japan under cyber attack, and why is Hitachi a target? I think that finding the facts of an attack and countering it require recognition that Hitachi, as a company, bears an important social role that goes beyond the business of a single enterprise.

There was a case a few days ago in which a cyber attack on a supplier to one of Japan's leading manufacturers caused a system failure that forced all the company's factories in Japan to suspend operations. What was the causal factor that invited such a severe situation, despite the implementation of advanced countermeasures on a daily basis? When we consider the current state of security, we need to be aware that the same could happen to us.

— What impact do attacks targeting vulnerabilities in products or services have on the progress of the Lumada business?

We expect the kind of attacks targeting products and services which are happening now to occur in more diverse cases, as we greatly expand and advance our data usage and collaborative creation business through our Lumada business. For any client, there's one-time business, but there are also services that can continue to provide solutions. Hitachi must build solid frameworks for extent of our responsibility for the characteristics of each business. What we already do is that if we find some level of vulnerability, we contact the client concerned and have them tackle the problem, or tackle it for them. For the solutions and software we provide to our clients, we are aware that the question of the right

Hitachi, Ltd.
Vice President and Executive Officer, CTrO/CISO
Masashi Murayama

Mr. Murayama joined Hitachi in 1985. Drawing on his experience as the leader of the Project Management Promotion Office Smart Transformation Project Initiatives Division, beginning in 2016, Murayama drove strategic and structural reform as CPO and general manager of Value Chain Integration. Appointed to role of Managing Executive Officer in 2019 and CISO in 2020.

form in which to maintain information security is a major issue for Hitachi as a company, from the perspective of social responsibility.

— Information leaks can occur as a result of human-factor risks, rather than cyber attacks, so what kind of response is required?

The two types of human risks are due to malice or inadvertent errors. Malicious risks can only be countered by thorough ethical education to raise each person's awareness. As for inadvertent errors, I believe it is the responsibility of the company to provide systems which absolutely minimize the potential for errors, because human beings do make mistakes. The role of the company is to provide secure PCs, build safe network environments, and otherwise develop places where employees can work with safety and peace of mind.

The culture of shame is deeply rooted in Japanese companies, but there is no place for shame about security. Building an open corporate culture—so that if your own PC causes a problem, you can report it immediately—limits the spread of damage.

— While many diverse factors are raising risks of information leaks, what is your view of the European GDPR*1 and the global movement to reinforce data protection regulations?

The perspective of compliance is indispensable when we consider the impact of cyber attacks on companies and society. When we consider the fact that data is interlinked beyond nations and regions, the Hitachi Group as a whole must think about how to respond globally. For example, there are Hitachi Group companies in countries and regions around the world, but if each company has its own different interpretation of the GDPR, it becomes meaningless. Therefore, if the Hitachi Group clarifies its unified interpretation and holds common policies for handling it, and then places specialist teams in each region, we can get checked by native staff with regional specializations. In short, we must consider how to handle the laws of each country and region in three broad layers: things to observe at the global level, things to observe in regional ranges, and things to observe in national ranges.

— What is most important as the core of security management, in the context of increasingly wide-ranging and complex cyber attacks and the trends in data protection regulation?

It's important to start from the premise that risks will always emerge and security will inevitably be broken down. So rather than just pursue robustness, we need to decide in advance how to respond when we get attacked, and establish security that's able to respond flexibly to diverse risks.

In Sumo, wrestlers of small stature employ an array of techniques to take on the biggest opponents, and sometimes they win. I think the same is true of security management. If they run headlong into huge risks, they will just get knocked away. We have to respond with the idea of flexibility to overcome rigidity, thinking carefully about how to avoid getting knocked away, and having scenarios for attacks from the side, or from above, or from below. Security with flexibility can use that sinuous strength to take down powerful risks. If we prepare and refine various response methods for risks, and then practice every day, as if they were fire drills, we will be able to gauge the situation swiftly and respond. Firefighters envisage all kinds of situations that could happen at the site of a fire, and they practice for them repeatedly, so they can make quicker decisions in an emergency. Alongside flexibility, that swift action is a key point to minimize the damage caused by a risk.

— What does an organization need to do to act faster?

Under a global system, in particular, the key point is how quickly information is shared in the first stage after an incident occurs. Just as initial response is vital when a fire breaks out, when the Hitachi Group is hit with an incident somewhere in the world, contacts must go out immediately, to share the situation and put a stop to the risk quickly. But in a conventional pyramidal organization, information sharing is like a bucket relay in a sense, so it's hard for water to move up, and the volume dwindles as it does, with speed dropping as well. We need information to move swiftly, straight

through from the site of the incident up to top management, within an organizational structure that's as flat as possible. Another thing we need is to strengthen lateral connections for information sharing within regional units. That means, for example, if an incident occurs in a country in Europe, information can be shared rapidly among Group companies in Europe. We have placed ISEs*2 in our sites in the Americas, Europe, China, India, and elsewhere in Asia, and I want to expand them on the basis of their functions. We've still got a long way to go, but I want to accelerate information sharing in the two directions of a “vertical axis” that starts from headquarters, and a “horizontal axis” that starts in regional sites.

— What is the position of information security within the Hitachi Group's 2024 Mid-term Management Plan?

The 2024 Mid-term Management Plan newly adds our stance of “supporting people and society with data and technology to achieve a sustainable society”. We must consider security management based on the current situation of fading barriers between inside and outside the company. There's a mountain of challenges, such as how to strengthen security for products and services and how to enhance the security of entire supply chains, and we'll go on tackling them head on.

Cyber attacks and other information leakage risks, due to malice or error, could happen anywhere in the world. That's why we must basically prepare ourselves to respond to whatever happens, detect the problem as quickly as possible, and then apply analysis and measures every time to prevent recurrence. Also, measures in a single company won't be sufficient, so it's important to extend them laterally to other companies.

The places we can't see are the most dangerous for this kind of information security risk. There are some aspects, including supply chains, where it's difficult to apply security at exactly the same level, but we as Hitachi must carry on asking our external partners to do things like properly applying patches, using multifactor authentication, changing passwords regularly, and incorporating biometric authentication.

— What future course of action and decisions do you see for Hitachi Group's security strategy?

The Hitachi Group is a corporate group consisting of numerous companies, but going forward we'll be doing business as a single company, under “One Hitachi”. In line with that business policy, I think the most important thing is for us to tackle information security as “One Hitachi”. I want to accelerate the construction of ideal security by setting policies for Hitachi as a whole, with thorough validation of sharing and speed based on common measures, rather than each company acting on its own.

※1 GDPR：General Data Protection Regulation
※2 ISE：Information Security Expert

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

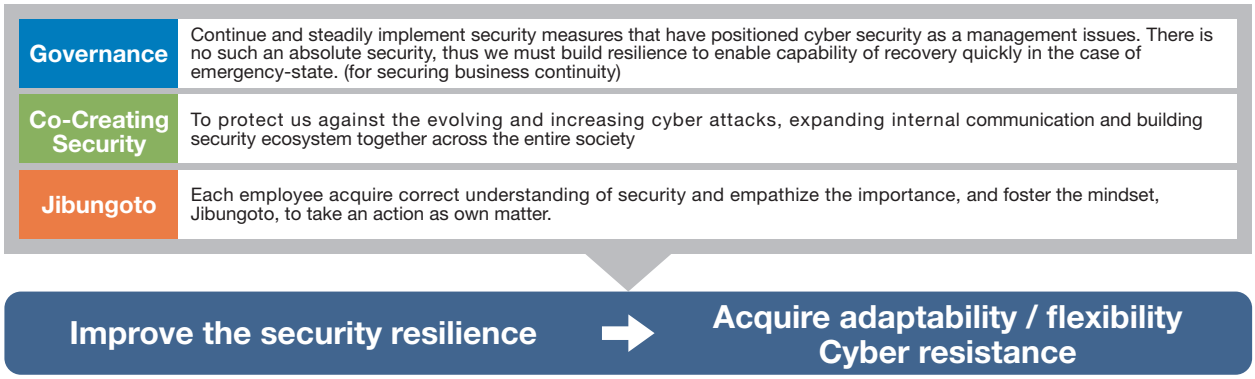
The rapid advance of digitalization and the complex global changes in political and economic conditions are changing the business environment on a daily basis. Hitachi monitors and analyzes this business environment and practices risk management to address the aspects of the risks Hitachi should be ready 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, with the recent COVID-19 pandemic, 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 “Governance,” “Co-Creating Security,” and “Jibungoto(Ownership),” for a “next normal” society. (Figure 1-❶)

Figure 1-❶ Hitachi's Information Security Vision



Governance: zero trust security initiative

Hitachi Group will implement security measures steadily and continuously to counter the tide of increasingly advanced and complex cyber attacks. As part of that effort, we have started applying zero-trust security measures as we move our IT platforms to the cloud, as an IT infrastructure countermeasure. Given the trend toward cloud-based work systems and workstyle reform, we are aiming for optimal security that uses a hybrid of cloud—which will be the mainstream architecture going forward—as the foundation, and our conventional perimeter-type systems. In realizing zero-trust security, with these cloud-based IT architectures as the standard, we are promoting authentication, endpoints, and cyber integrated monitoring as key components.

Co-creating Security: work on building a security ecosystem

Responses to security incidents require cooperation between 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.

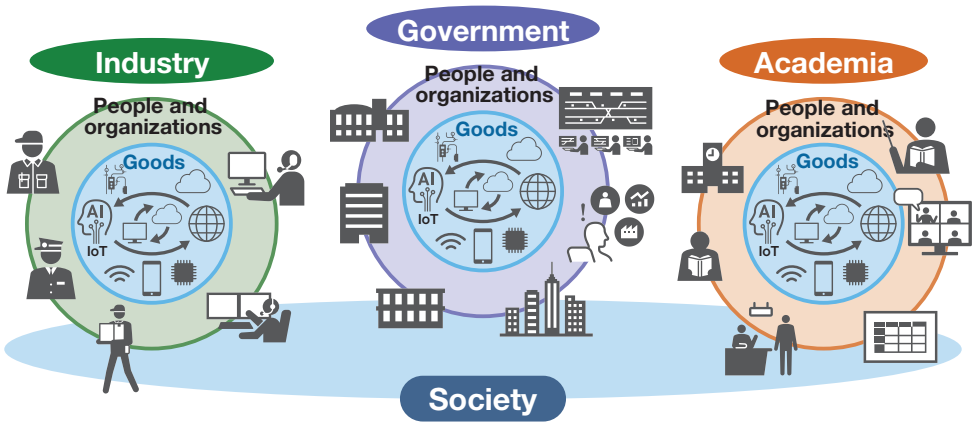
Connections are not just needed within Hitachi. It is now essential to share threat information and issues encountered when implementing countermeasures with enterprises, governments, academia, and other entities engaged in cybersecurity initiatives to create a community not bound by traditional constraints. Hitachi encourages 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 1-❷)

Jibungoto: security awareness-raising initiatives

We estimate that vulnerabilities in security awareness will be targeted, as employees have been working from home due to the recent COVID-19 pandemic. Working outside the office in an unfamiliar environment can lower their defenses, and 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 “Jibungoto (ownership)” of security.

Figure 1-❷ Illustration of the security ecosystem



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. Those assets include information entrusted to us by customers, the systems which store such information, and the information systems that run social infrastructure services.

Information security policy

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

(1) Formulating administrative rules for information security and ensuring their continual improvement

Hitachi acknowledges that information security initiatives are a key issue for management and business operations, and will formulate administrative rules for information security that comply with the law and other regulations. Hitachi will also establish a company-wide information security management framework with Hitachi, Ltd. executives at its core, and ensure its enforcement. Hitachi will maintain information security from organizational, personal, physical, and technical perspectives, and ensure its continuous improvement.

(2) Protection and ongoing management of information assets

Hitachi implements safe management measures that appropriately protect information assets from threats to their confidentiality, integrity, and availability. Hitachi also implements appropriate control measures to ensure business continuation.

(3) Legal and regulatory compliance

Hitachi complies with laws and other regulations related to information security, and ensures its administrative rules for information security conform to these laws and regulations. In the event of a legal or regulatory violation, Hitachi takes the appropriate punitive action as defined in the employee work rules and other relevant policies.

(4) Education and training

Hitachi aims to improve information security awareness among its executives and workers and conduct education and training in relation to information security.

(5) Preventing incidents and taking action when they occur

Hitachi endeavors to prevent information security incidents, and if such an incident were to occur, to take appropriate action without delay including preventing its recurrence.

(6) Ensuring business processes are optimized within the corporate group

According to (1) to (5), Hitachi will endeavor to build frameworks that ensure proper business processes within the corporate group consisting of Hitachi and Hitachi Group companies.

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 office 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.

The company president nominates a chief information security officer who has authority and responsibility in relation to information security, and an information security audit officer who has authority and responsibility in relation to information security audits.

The chief information security officer establishes an 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

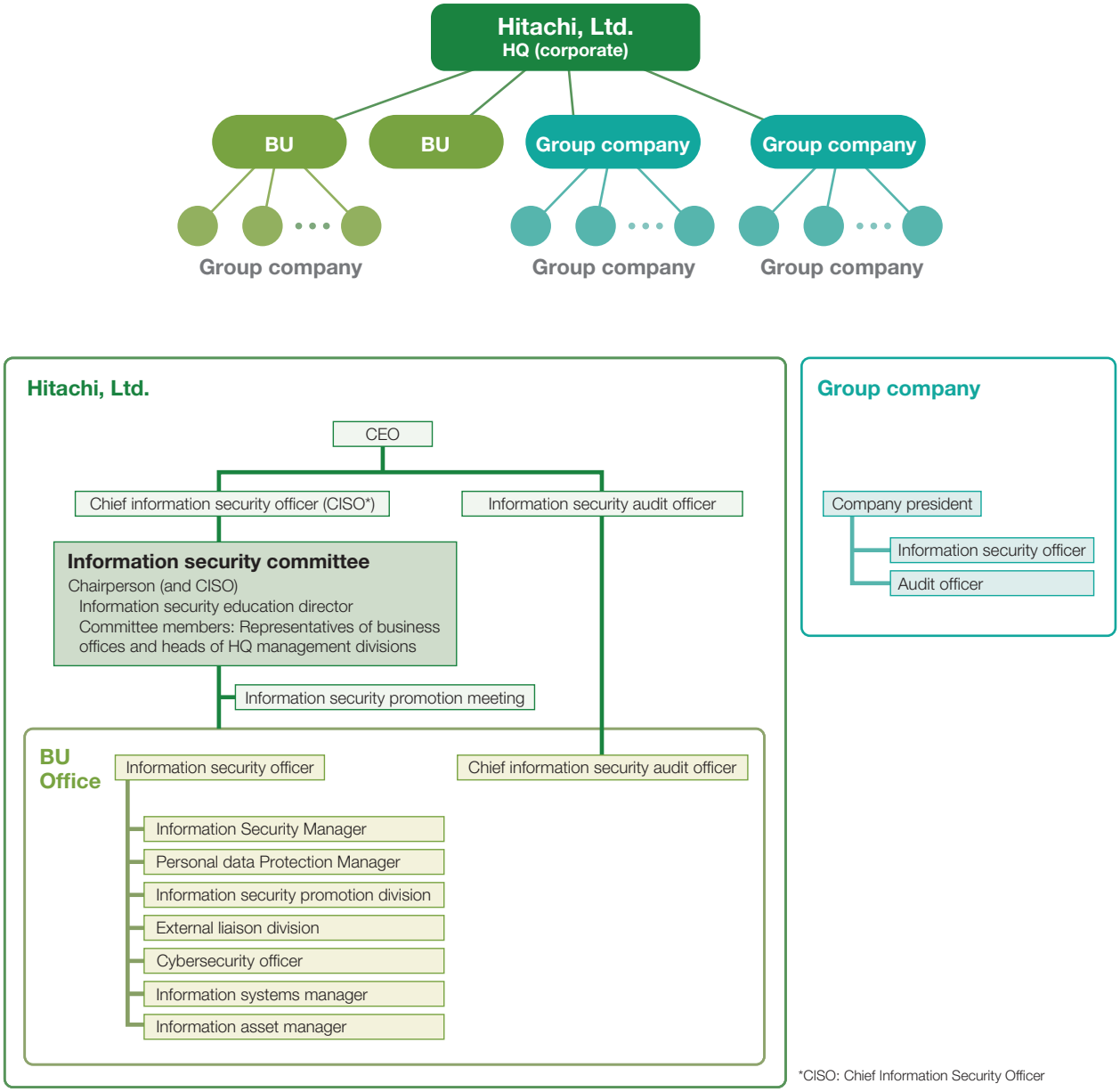
through information security promotion meetings attended by representatives of all BUs and offices.

In principle, the head of the BU and the office manager serve as the information security officer of the BU and office. Information security officers appoint Information Security Execution Officer and Personal data Protection Manager to support implementation, in order to manage and control personal information protection and information security.

An 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 which act to promote information security through cooperation. (Figure 2-❶)

Figure 2-❶ Information security promotion framework



*CISO: Chief Information Security Officer

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 regulations to promote information security.

Basic regulations

"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 countermeasure standards, which comply with US government standard SP800.

In 2021, we enacted the Hitachi Group Privacy Principles as a common code of conduct for personal information protection throughout the Hitachi Group.

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 regulations

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 reas" 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", setting rules and measures, "Do", which implements measures, "Check", which monitors and assesses, and "Action", which makes ongoing 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・Regulations related to personal information protection

Category	Name of regulation
Basic regulations	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 regulations	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)

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 workers 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, workers, and temporary employees on the subjects of information security and personal information protection. Approximately 35,000 employees and other workers of Hitachi, Ltd., receive this training each year, and attendance has reached 100%. Hitachi 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 specific group of people like newly hired employees and another those in new managerial. (Figure 2-❹)

positions, while another might offer specialized education to people in roles such as personal information protection manager.

Hitachi, Ltd., makes its educational content available to Group companies inside and outside Japan, and works towards deepening the 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 when targeted by such an attack.

We have implemented training on targeted attack emails for all employees including group companies, and from FY 2020 we have expanded these efforts globally and have started training our local subsidiaries. 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.

Figure 2-❹ 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	Executives and managers	Trends in personal information protection and the latest Hitachi initiatives
	Newly-appointed section manager or equivalent	Knowledge someone in a management position must possess in relation to personal information protection, confidential information management, and information security, and Hitachi's initiatives in relation to personal information protection.
	Newly-appointed assistant manager or equivalent	Personal information protection, confidential information management, information security knowledge necessary as a manager or equivalent, and Hitachi's efforts to protect personal information
	New employees	The fundamentals of personal information protection, confidential information management, and information security.
Specialized education	People responsible for protecting personal information	Practical exercises and the specialized knowledge a person responsible for protecting personal information must possess, such as internal and management rules and real-world operating procedures.
	Information asset manager	Knowledge required for an information asset manager to carry out their role as a manager of information assets including personal information in their division.

Information Security Management

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 of Hitachi, Ltd., is carried out by independent auditors appointed by the CEO. To ensure fairness and objectivity, the audit process is mutual audit.

Personal information protection and information security audits confirm 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, and Hitachi confirms the results.

On-site risk assessment

With an ever-expanding global presence, the Hitachi Group makes its home in many countries and regions, counting headquarters, sales offices, service centers, and manufacturing sites among its business entities. This environment inevitably gives rise to diverse in-Group network environments and facilities and varied installation and usage environments for IT equipment and cloud environments, etc. There is also communication with outside parties via internet connections, information storage media (USB storage), and other means. Preparing for security risks such as spear phishing and malware infection is very important.

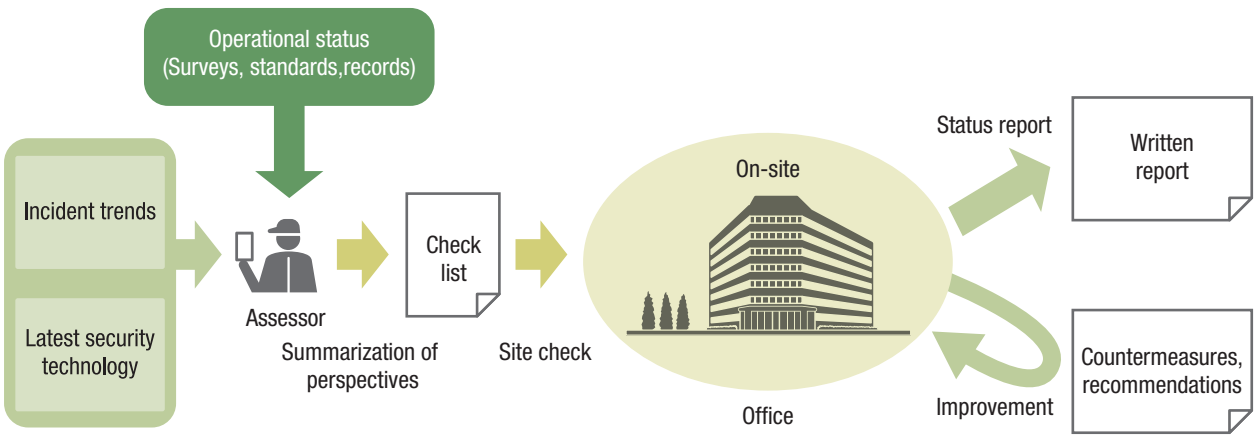
To address the risk that comes with changes to the business environment, Hitachi has strengthened its assessment framework that uses expert security teams. Specifically, a security team will visit the workplace of a BU or Group company and implement enhancements from the following perspectives:

(1) Carry out assessments of all products and internal facilities that connect to the network of the Hitachi Group based on the latest security trends.

(2) Identify issues that might present a security risk and propose effective countermeasures on site. (Figure 2-5)

Since FY 2017, we have assessed a total of around 120 sites, identified a large number of security risks, and given advice on necessary measures. We also take feedback from the problems that we encounter across the company and incorporate it into the measures.

Figure 2-5 On-site risk assessment flow



The outlook is for the impact of COVID-19 to fade in FY 2022, so we started to visits and on-site assessments of overseas Group companies, which are thought to have relatively high security risks, and make assessments.

From FY 2022 we also started assessment of companies acquired through M&A. We will grasp security risks and make suggestions to enable countermeasures earliest possible.

Vulnerability check on public servers

Cyber attacks in recent years have found vulnerable servers which are open to the internet and exploited them as entry points to access internal networks, leading to ransomware and other malware infections, and to thefts of personal and confidential information.

We regularly perform vulnerability checks on the servers that exposed to public using vulnerability search sites such as Shodan.

We're working to reduce security risks by checking for any gaps compared to self checks run by the server administrator.

Information Security Management

Initiatives for Security Human Resource Development

To ensure the effective implementation of 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 ensure the security of the products and services it provides to its customers. You can see the three categories of human resource development on the right. This initiative targets not only high-level security experts, but also the technicians involved in the development and operation of products and services and the users of in-house IT services. (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, and that of production and manufacturing sites
- Basic human resources who understand the fundamentals of security and can respond appropriately when a security incident occurs

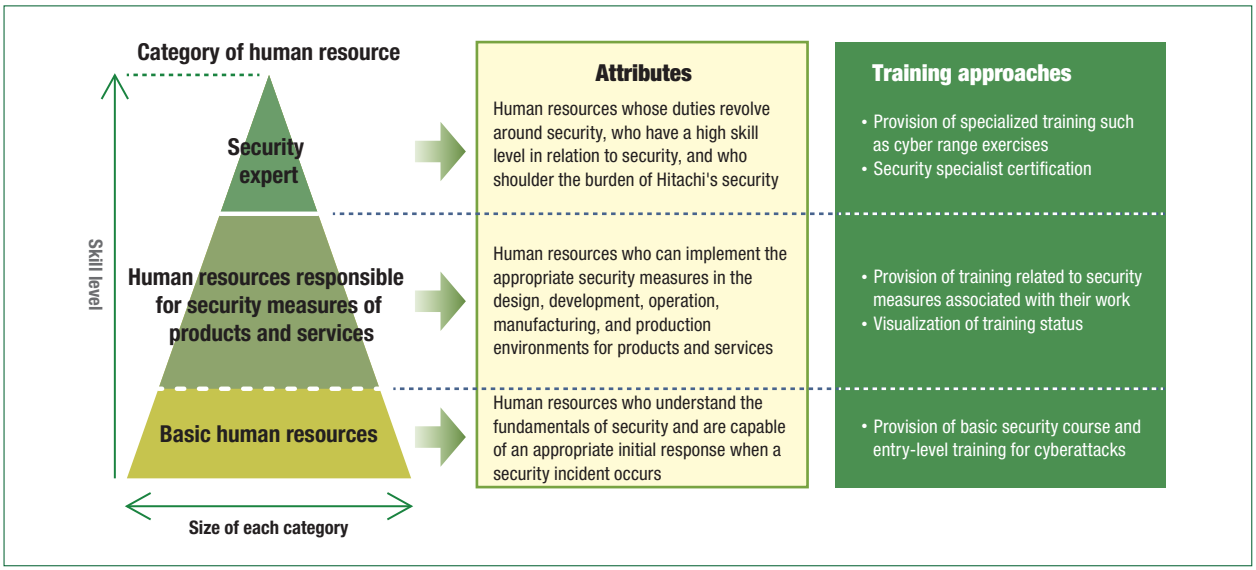
Educational programs for each category of human resources

We are developing educational programs tailored to three categories of human resources, and effectively promoting human resource education according to the objectives of each category.

Security expert

The approach to human resource development for security experts includes high-level training techniques such as cyber range exercises, and the provision of community sites that support information sharing and cooperation. 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, information security specialists (HISSP: Hitachi Certified Information Security Specialist) who have the necessary security skills and are on the appropriate career path are discovered, trained, and evaluated. Hitachi has now certified more than 1,300 such experts.

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 of products and services are those who promote the necessary security measures as part of their work providing the product or service. These people are responsible for carrying out the appropriate security measures during the design, development, operation, and maintenance of products and services, and when preparing the environments in which this work takes place. Also important is the development of security human resources focused on production and manufacturing. These human resources are provided with education to promote an understanding of security measures according to company regulations. Environments must be created and operated in a way that maintains the safety in the design and development of products and services and at production and manufacturing sites, while allowing neither of these environments to adversely affect the other. To this end, Hitachi is engaged in improving the skill of its workers in relation to security measures for IT and OT.

We have also started measures such as developing key PSIRT personnel to handle actions to strengthen security systems for products and services.

Basic human resources

The development of basic human resources targets many people with the objective of raising the security awareness of the company as a whole and enhancing its security countermeasures. In addition to imparting fundamental security knowledge, this initiative ingrains the appropriate initial response when a cyberattack or other security incident occurs. Training for basic human resources includes the Basic Knowledge e-learning Program for Cybersecurity Countermeasures and the Communication Training for Cybersecurity Response provided since FY 2016 and taken by more than 6,000 people. Hitachi also provides e-Learning programs on security fundamentals for people who require introductory training. The societal changes brought about by COVID-19 mean that group training is now carried out online. The Communication Training for Cybersecurity Response offered to basic human resources in a workshop format has also moved online since FY 2020. (Figure 2-❼)

Figure 2-❼ Education for Basic human resources

Basic Knowledge e-Learning Program for Cybersecurity Countermeasures

✓ **Training for learning behavior and impact when a cyberattack occurs**

【Basic knowledge】
(1) Matters to note in your daily work,(2) Responding to cyberattacks, (3) Matters to note during development, (4) Collecting vulnerability information and assessing countermeasures, (5) Preparing for a security incident

【Hands-on learning】
(1) Information leakage from a spear phishing attack, (2) Damage to business from ransomware infection, (3) Damage caused by a vulnerability in a web application, (4) Damage due to malware

Communication Training for Cybersecurity Response (workshop)

✓ **Training in understanding the situation when an incident occurs and determining a course of action**

【Response process】
Experience the speed and accuracy required in the (1) Observe, (2) Orient, (3) Decide, and (4) Act stages

【Communication skills】
Understand the importance of knowing your role and responsibilities when (1) reporting, (2) notifying, and (3) discussing, and the importance of accurately describing an event using the 5W1H method

Information Security Management

Action to Strengthen Global Information Security

Information security initiatives are essential to the Hitachi Group's presence on the global stage. To ensure reliable implementation of security countermeasures, Hitachi is strengthening its global governance by posting information security experts in various regions to entrench global security governance.

Enhancing governance through information security experts

Hitachi's lines of governance for information security entails the security management divisions of the Hitachi Group sharing policies with and giving countermeasure instructions to BUs and Group companies, who in turn direct their overseas subsidiaries to implement them.

To support the advancement of information security at a global level, Hitachi has in 2019 posted ISEs (Information Security Experts) in various regions and begun activity intended to entrench governance. As of 2020, Hitachi has posted ISEs in the Americas, Europe, Asia, China, and India who are supporting local subsidiaries in their region.

ISEs (Information Security Experts) work together with organizations responsible for security to enhance governance in their region. (Figure 2-8)

To establish regional communities, open lines of communication, and foster security awareness, ISEs hold cybersecurity workshops and online seminars, and publish a security newsletter, as an adjunct to traditional lines of governance via parent companies, supporting better governance of local subsidiaries. (Figure 2-9)

Figure 2-8 Governance strengthening system of Information Security Experts (ISE)

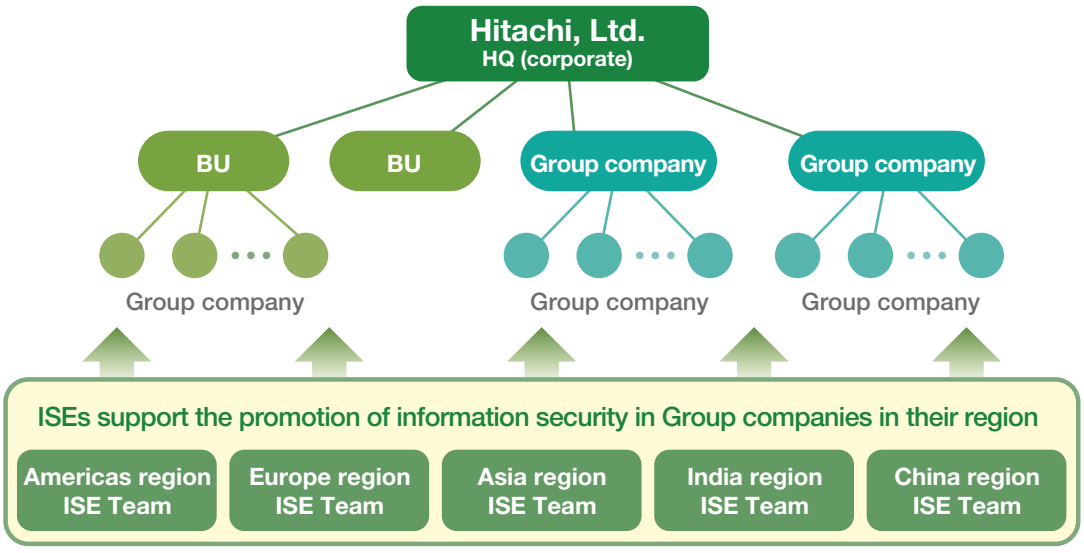


Figure 2-9 Main activities of information security experts (ISEs)

Key ISE activity	
1. Formulating and implementing security plans in cooperation with organizations responsible for security	5. Support for security awareness activities with an awareness of "Jibungoto(Ownership)"
2. Ascertaining the level of cybersecurity maturity and the reach of governance and supporting companies in their efforts to improve	6. Working together with impacted divisions in relation to local laws and regulations
3. Establishing security communities in various regions	7. Participating in outside conferences to gain insight into the latest trends
4. Holding workshops for people responsible for security of overseas subsidiaries	

Security status visualization and PDCA activity

The Hitachi Group promotes better IT governance by conducting self-assessment and third-party assessment of IT and security countermeasures from a field perspective.

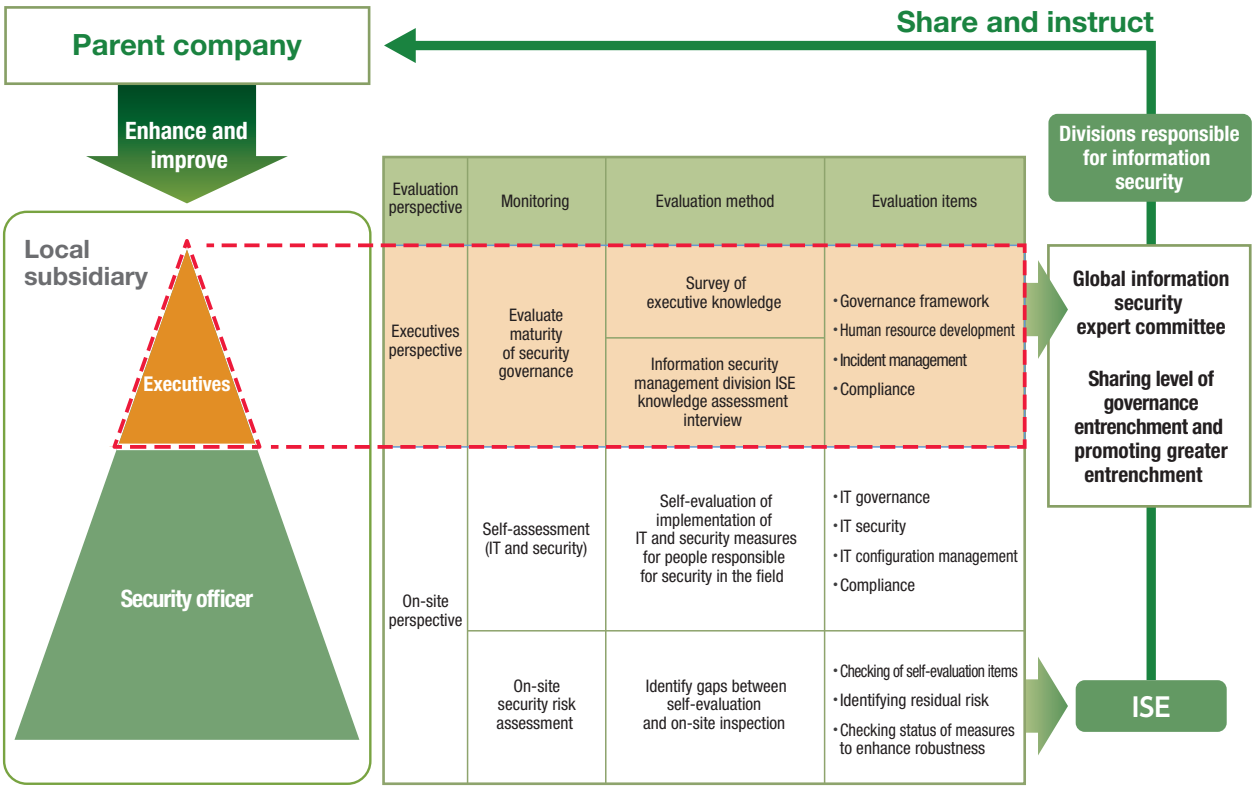
Hitachi surveys the executives of overseas subsidiaries to assess their knowledge of security governance initiatives. This offers insight into the maturity level of security governance from a management perspective that goes beyond a conventional field perspective.

This survey covers a range of themes including governance frameworks, human resource development, in-house IT security, security for production and manufacturing, product security, third-party vendors, and compliance.

Hitachi visualizes and analyzes the results of the survey of executives of overseas subsidiaries, and uses the results of this process to develop concrete plans to improve the entrenchment of governance. It also shares the visualized data with the people who manage and control security for BUs and Group companies. Here, it finds effective use as context for security activity in the Plan, Do, Check, and Act stages of the PDCA cycle. (Figure 2-⑩)

We promote PDCA implementation from the two perspectives of management and the workplace.

Figure 2-⑩ The process of global security status monitoring and assessment feedback



Information Security Management

Action to Strengthen Information Security in M&A

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

Policy on reinforcing information security governance in M&A

The Hitachi Group actively pursues M&A as a way to expand our business. M&A generates new value by integrating companies with differing corporate cultures. On the other hand, we must minimize the information security risks that occur as we integrate policies and systems.

If we discover an information security incident after acquisition, there is the risk of major impact that could extend beyond the acquired company to the entire Hitachi Group (affecting corporate value, sales activities, and more). Therefore, it is essential for us to identify any information risks as soon as possible and control them appropriately. Starting at an early stage of the M&A process, it is important to enforce in the company to be acquired an understanding of, and compliance with, Hitachi rules, and to apply controls and management based on Hitachi policies.

Information security risk assessment during M&A

Our risk assessment during M&A is divided into two phases: before and after the contract is signed.

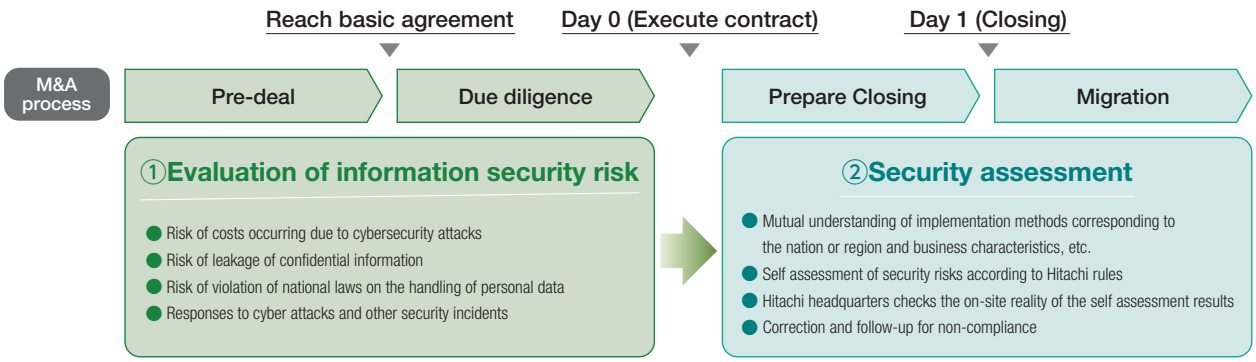
① Information security risk assessment performed before contract signing (Day 0).

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, policies, and standards, 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 Security assessment performed after contract signing (Day 0).

We select the sites to assess on the basis of the situation, characteristics, etc. of the countries and regions where the acquired company does business. Next, we have the company perform a self assessment of the selected site, addressing risk assessment items which we have prepared for each subject field on the basis of Hitachi rules. After that, Hitachi headquarters makes a direct visit to the assessed site and checks the local situation, to get a more detailed grasp of the results of the self assessment. Finally, if there are any matters which do not comply with Hitachi rules, we have the company prepare a corrective plan, and follow up until the correction is complete. (Figure 2-⓫)

Figure 2-⓫ Information security risk assessment and security assessment



Hitachi's Approach to Security Risk Assessment

Regardless of the size of the company when it is acquired, it is important to correctly grasp the existence of information security risks at an early stage in the negotiation. We must assess what kind of risks are present according to the business activities and service content, but if there are clearly risks such as information leakage, we must consider passing on the acquisition cost and the IT system migration costs.

If a severe information security risk is discovered that requires correction, we must deliberate with the acquired company about specific measures to reduce that risk in the future, and move forward with planned improvement measures.

Hitachi practices information sharing with the whole group, alongside feedback, while also building controls and systems for appropriate control of each company's risk situations, and maintaining a comprehensive overview.

Target fields and assessment items for security assessment

Hitachi sees all devices and systems used in product development and manufacturing, the environments which deliver products and services to customers, and other areas as subject to cybersecurity risks, not just the PCs and servers (internal IT environments) employees use in regular office work. We also check the management methods and the leak countermeasures related to personal information protection and confidential information management. (Figure 2-⓬)

The assessment items for security assessment consist of 10 categories, based on internal security standards (Hitachi rules) that were formulated with reference to ISMS and the NIST SP-800 Series, and taking information security incidents in recent years into account. (Figure 2-⓭)

Figure 2-⓬ Cybersecurity risks and information security risks

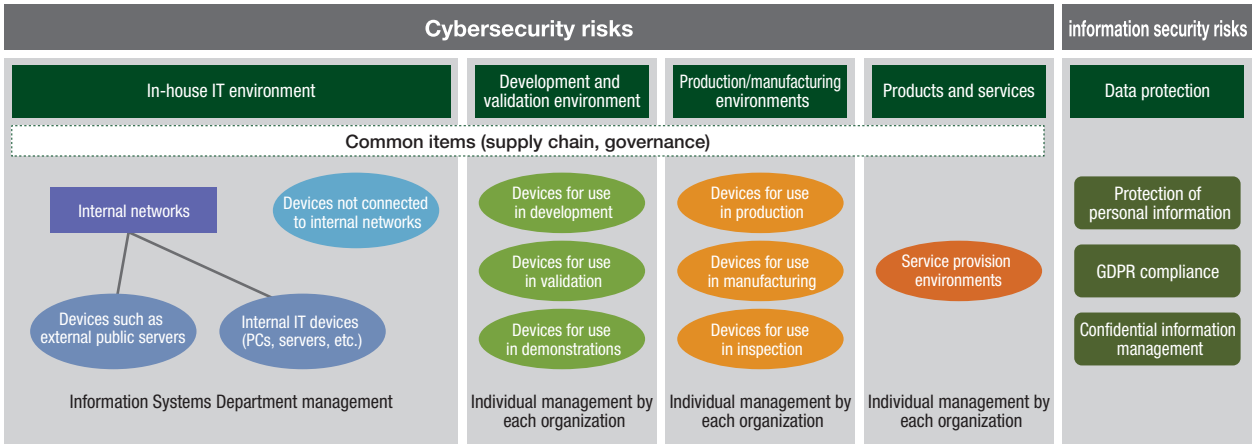
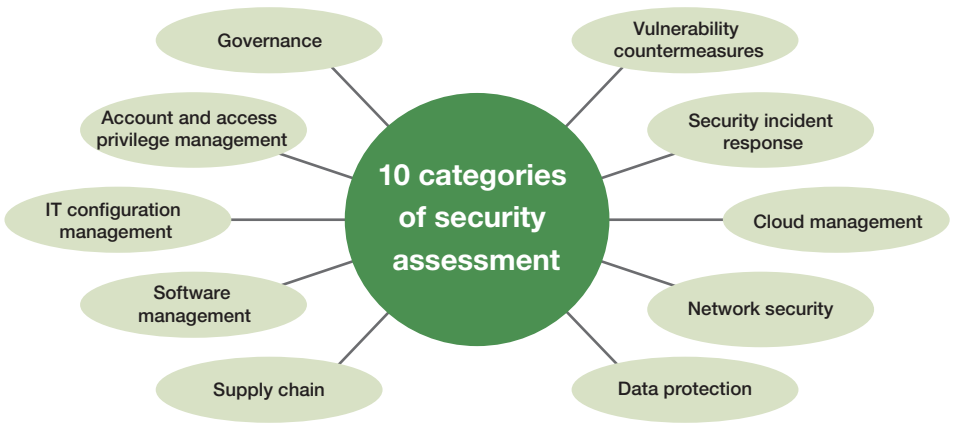


Figure 2-⓭ 10 categories of security assessment items



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 in-house 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 2-14)

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 2-15)

Figure 2-14 Expanding the scope of cybersecurity countermeasures

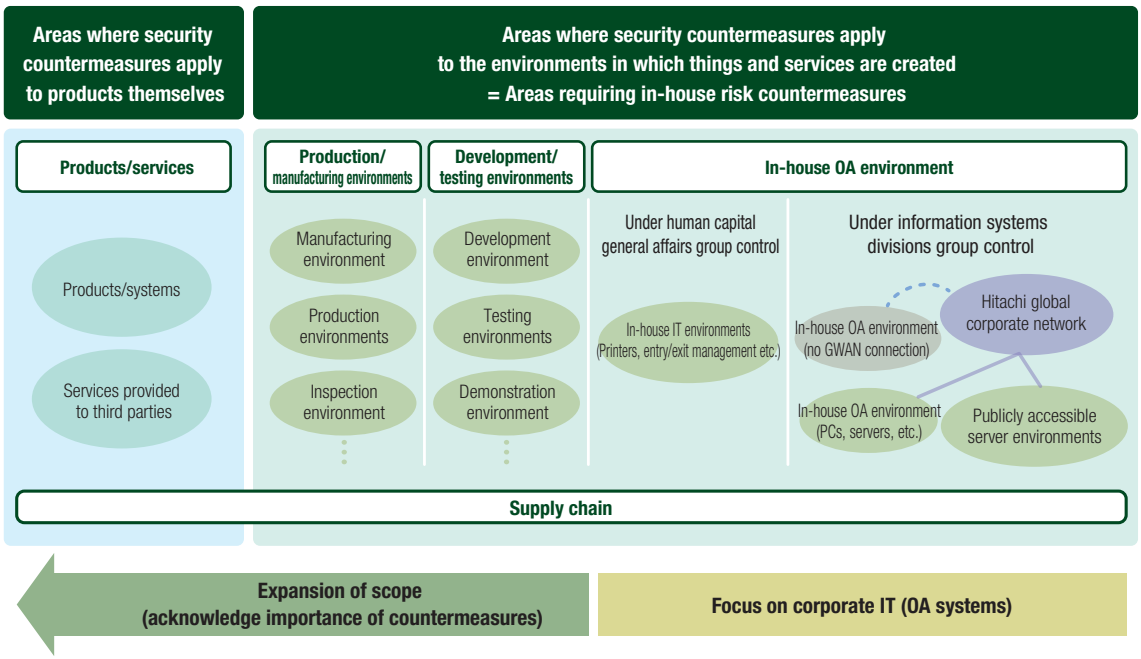


Figure 2-15 Summary of actions to enhance cybersecurity countermeasures in various areas

Area		Target divisions	Overview
In-house OA	Environment	IT	・Formulating and disseminating requirements for connection to and isolation from the in-house OA environment
Development and testing		Design and development	・Formulating and disseminating guidelines for creating in-house OA environments and environments for securely connecting to them
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 related to 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	・Formulating requirements for cybersecurity countermeasures for business partners and evaluating them based on evaluation processes

Promotion framework

HQ (corporate) is planning measures to enhance cybersecurity by establishing subcommittees for each area under the auspices of the cybersecurity expert committee.

The policies of each subcommittee are rolled out via the cybersecurity officers whose role is to enforce cybersecurity countermeasures in BUs and Group companies.

Each division disseminates and enforces its cybersecurity countermeasures under the direction of the cybersecurity officer. (Figure 2-16)

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 each BU and Group company 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/validation environments

Development/testing environments include various environments for purposes such as development, testing, research, and demonstrations. We also use connections with customers' environments and to the internet, as well as cloud environments. Security requirements vary between environments, but we have prepared guidelines for configuring and connecting each environment safely, and we are working on applying the guidelines across 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 2-17)

Figure 2-16
Cybersecurity promotion framework

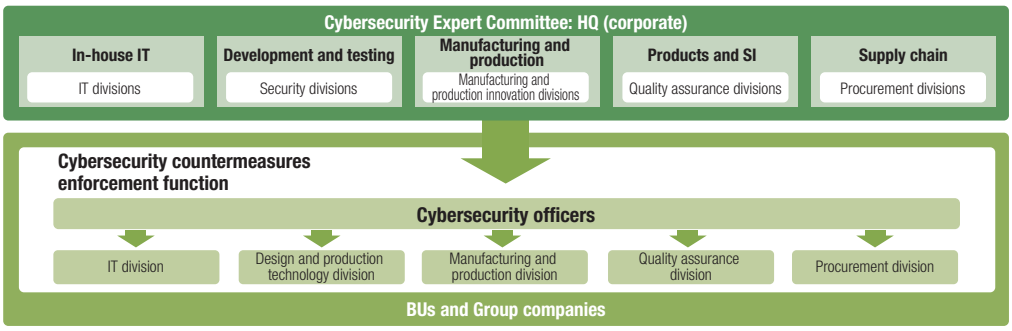
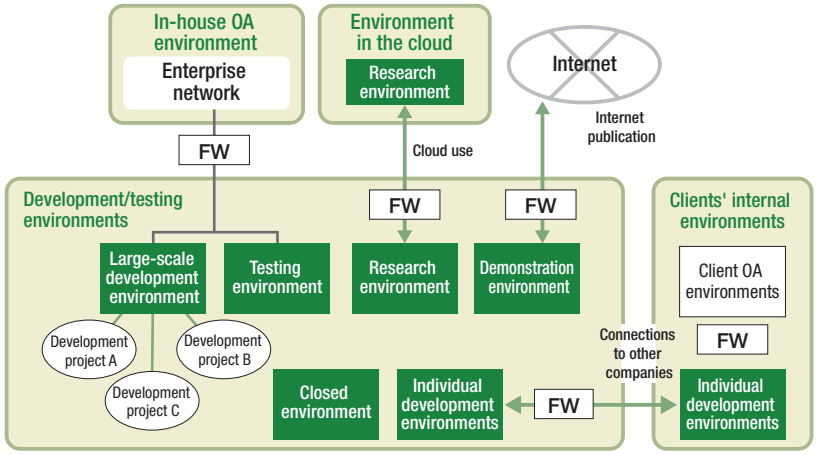


Figure 2-17
Development/validation environment security network



Cybersecurity Initiatives

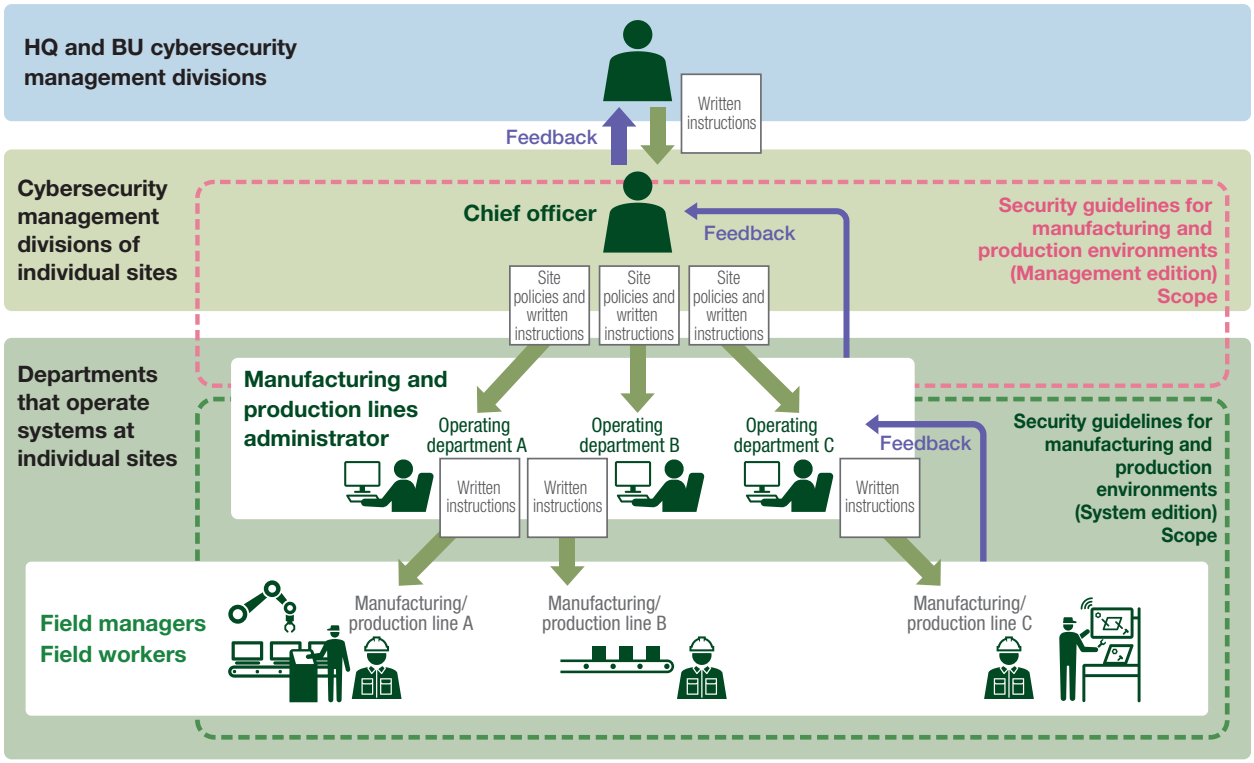
Security enhancement in production/manufacturing environments

It is important that manufacturing and production environments do not affect other environments, such as in-house 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 2-⑱)

At actual manufacturing and production sites, posters are displayed workers of their obligations during their day-to-day work. This leads to greater security awareness in the manufacturing and production sites. (Figure 2-⑲)

Figure 2-⑲ Posters/rule collections for production and manufacturing workplaces

Figure 2-⑱ 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

When security operations to take care of Hitachi's information assets are consigned to a procurement partner, Hitachi checks and screens the procurement partner's information security in advance, based on Information security criteria set by Hitachi.

These nformation security criteria have supplementary information security guidelines which have added security measures against recent cyber attacks on supply chains.

Hitachi also specifically stipulates requirements concerning information security, so procurement partners can perform checks. (Figure 2-20)

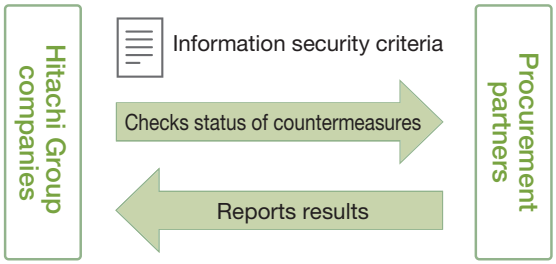
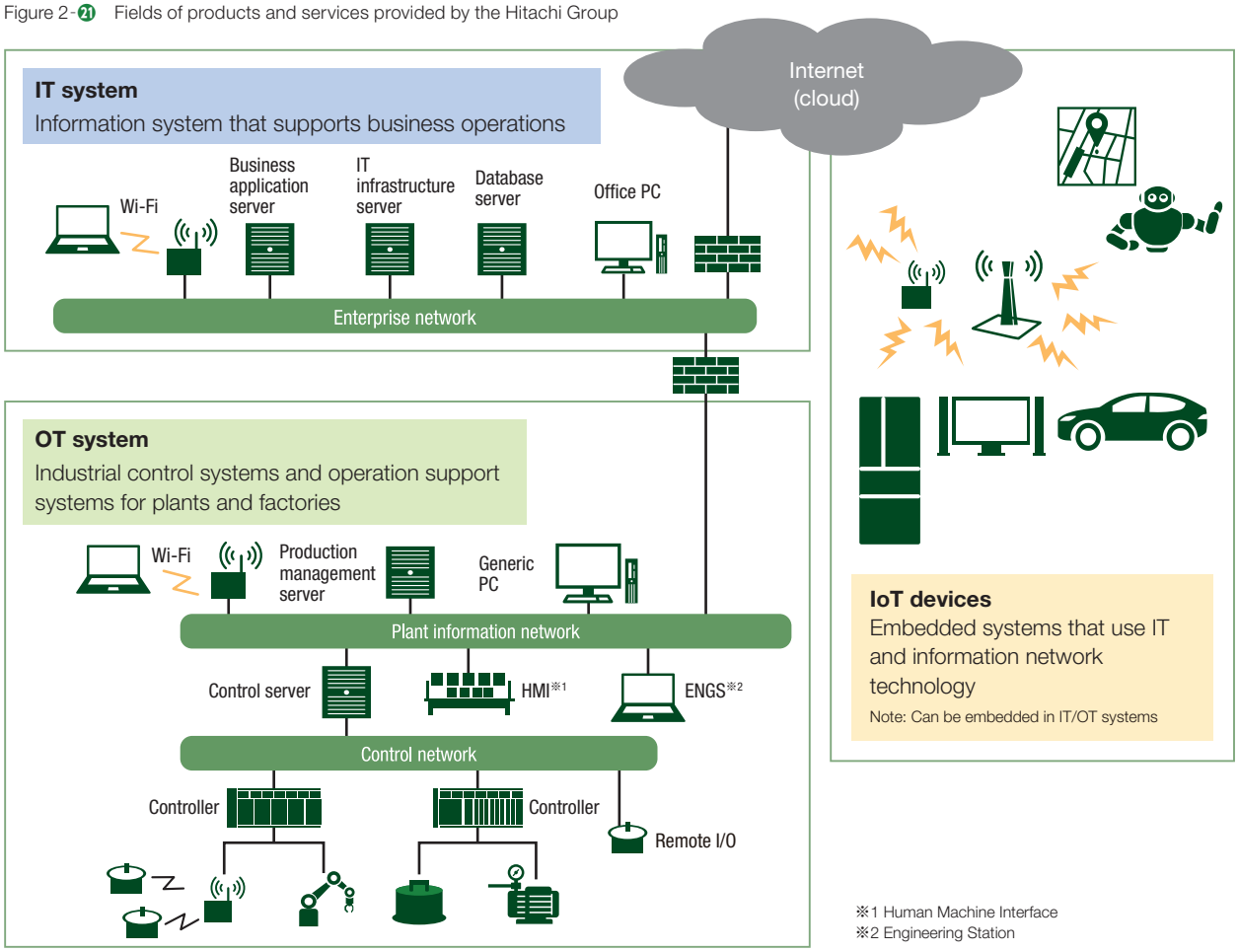


Figure 2-20 Security strengthening system in the supply chain

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. In relation to the IT systems, OT systems, IoT devices, and other assorted products and services provided by the Hitachi Group,

Figure 2-21 Fields of products and services provided by the Hitachi Group



※1 Human Machine Interface
※2 Engineering Station

Cybersecurity Initiatives

Hitachi continues to promote initiatives intended to protect customer assets and social infrastructure from cyberattacks. (Figure 2-㉑)

Since FY 2022, new product security officers have been placed in each BU and Group company, and we are building a security management organization under their control, to enhance product and service security. We have also developed PSIRTs to handle technological responses at headquarters (Corporate) and at each BU and Group company. They work together to take appropriate action in response to vulnerabilities and incidents involving products and services.

Security management policy for products and services

To unify the approach to security management for the many and varied products and services of the Hitachi Group, Hitachi has prepared guidelines for quality assurance in the form of a Security Management Policy for Products and Services and related documentation. (Figure 2-㉒)

By applying the contents of this policy to its own security management regulations, each division can advance the implementation of secure processes across all stages of the lifecycle of its products and services including development, manufacturing, maintenance, and operation. (Figure 2-㉓)

Dissemination of guide material and support activity

Hitachi disseminates various guidebooks and other resources that divisions can use to prepare their own security management regulations. One example is the Secure Process Implementation Guide. These resources accumulate and share the know-how of the Hitachi Group by presenting case studies of the initiatives of divisions that have taken the lead in terms of security measures. The case studies cover implementation procedures and the like for each design and manufacturing, operation and maintenance, and security incident response process.

Hitachi shares this guide material on the intranet, and otherwise supports each division in the creation of its secure development processes.

Figure 2-㉒ 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 that apply to processes associated with product development and maintenance. These requirements form the basis for specific tasks appropriate to the nature of the product and can be enforced through checklists or other means as needed.
Product security inspection checklist	An inspection checklist used to confirm that the product development and maintenance processes of the division conform to the policies and criteria.

Figure 2-㉓ 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		

Pioneering initiatives related to ensuring security for products and services

To ensure the security of information-related products and services provided to its customers, Hitachi, Ltd., has established frameworks to assess and formulate security measures. Hitachi implements and improves security measures according to the security management process. The pioneering initiatives over the long term are as follows:

(1) Formulating and implementing security countermeasures

Hitachi promotes the formulation and implementation of security countermeasures. For example, because internet connections are typically high risk, Hitachi requires approval for internet connections. A framework is in place that prohibits internet connections or sharing without the appropriate permission. This approach has also been adopted by related Group companies, and measures formulated through collaboration have been deployed to and used by related business divisions.

(2) Product and service development and operation that conforms to security management processes

Hitachi defines security management processes for each phase of product and service development and operation. Formalizing rules based on these processes has allowed security countermeasures to be implemented reliably within organizations. Using the concept of a security ranking which defines the magnitude of risk, these rules define security management processes required to ensure security during development and operation for each security ranking. The use of a security ranking encourages people to take the appropriate measures commensurate with the seriousness of the risk, but also promotes a way of thinking that considers the balance between risk and cost. These processes link with Hitachi's standardized development process for information systems. The contents of the formalized security management processes are revised routinely or as needed. This process takes place based on feedback from incidents that occur, risks that manifest, and the results of prior use, and aims to ensure ongoing improvement of management processes.

(3) Promoting measures concerning the placement of security personnel

In order to ensure security quality to counter security risks in products and services, we have defined three types of personnel with appropriate qualifications, experience, and knowledge (① security risk assessors, ② security systems architects, and ③ security operations administrators), and we are advancing measures to allocate them to each review, design and testing, and operation process. Security risk assessors are appointed by the head of each business department. They conduct security reviews from their expert perspectives, and give advice and guidance. The security systems architect and security operations administrator use their expert knowledge to design, test, and operate security for each project. This allows us to develop and operate products and services with assured security and deliver them to customers.

(4) Implementing vulnerability inspections

Hitachi conducts regular vulnerability assessments with the aim of minimizing damage from attacks that exploit vulnerabilities. These inspections occur routinely or when starting a new development or changing an environment. Methods of inspection include a qualitative approach that uses a checklist and an approach that uses a vulnerability inspection tool. These methods can be used independently or together to conduct an inspection appropriate to the characteristics and operation status of the system.

(5) Handling vulnerability-related information and establishing an incident response framework

To reduce the likelihood of an exploited vulnerability causing a security incident, Hitachi has created a guide that summarizes handling process for vulnerability-related information in divisions that provide information-related products and services, and encourages activity based on this guide. Hitachi also provides a response framework and response manual accompanied by drills to ensure a rapid and appropriate response when a large-scale incident occurs.

Cybersecurity Initiatives

Cybersecurity Countermeasures

To stay on top of its handling of cyberattacks and incidents, Hitachi enhances security monitoring and incident response at the Hitachi Security Operation Center (SOC). We also take proactive measures by collecting and analyzing threat information, and disseminating vigilance information.

Enhancing security monitoring and incident response

Security risks are increasing not only for individual companies and organizations, but across the supply chain, with complex and ingenious cyberattacks such as targeted attacks, ransomware, and double extortion. To establish an effective line of defense against such cyberattacks, it is crucial to discover them early and limit the damage. To enhance its security monitoring and incident response capabilities, Hitachi, Ltd. established a Hitachi Security Operation Center (Hitachi SOC) in October of 2017. The Hitachi SOC operates 24 hours a day, 365 days a year, detecting threats such as malware infection or unauthorized access at an early stage. This condenses the timeline from initial response to resolution and minimizes the extent of damage.

Security monitoring

The Hitachi Group has established systems and network monitoring points that cover the entire globe for integration, analysis, and monitoring of logs. We have expanded our monitoring scope since 2017, and our systems now cover all core global bases. With the introduction of EDR (Endpoint Detection and Response), we can now also monitor the operation of devices, carry out surveys, and address issues. This means that we can analyze logs from EDR and core bases in combination, and implement high accuracy, efficient monitoring.

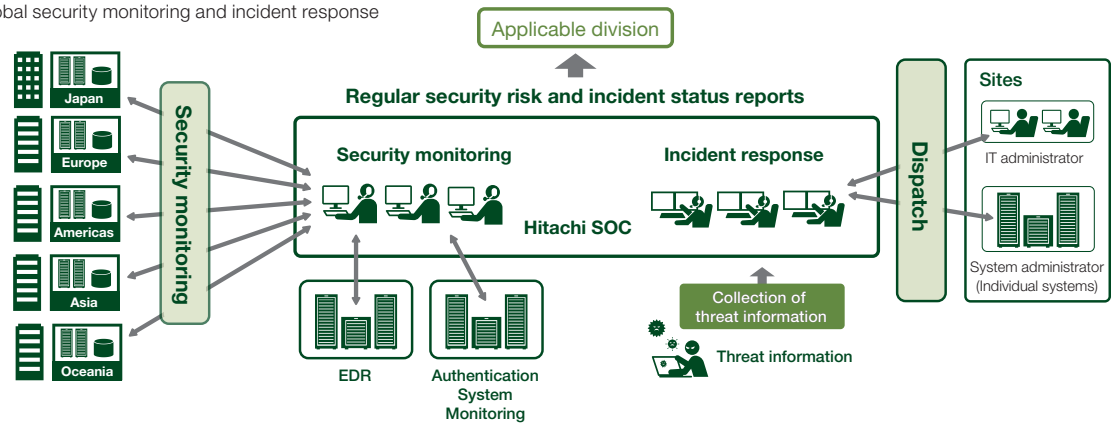
Recently, there have been more attacks where genuine authentication information is acquired fraudulently and used maliciously. These attacks are difficult to detect since genuine authentic authentication information is used. So, we have enhanced our monitoring of the authentication system to allow early detection of fraudulent account use by third parties.

Incident response

The Hitachi Group has established a handling procedure and contact system 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 bases and EDR surveys. This means that we can judge the response priority and whether a response is required, allowing us to handle incidents more efficiently.

Moreover, we can handle the new threats associated with work-from-home environments by monitoring the authentication system. The know-how we gather during incident response is then fed back to various internal security measures, making it less likely that the same kind of incident could occur again. (Figure 2-24)

Figure 2-24 Global security monitoring and incident response



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 its in-house information systems 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

When collecting information, in addition to the following vulnerability and threat information published on the web, we also make use of a range of CTI (Cyber Threat Intelligence) services to collect information on threats in Japan and internationally.

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

We use metrics published by the information provider (such as severity and CVSS base score) to classify threats into five vigilance levels, based on factors such as their likelihood of success and the prevalence of the vector in in-house systems.

For some threats, we use a simulated environment to perform verifications. This allows us to compile information to assist with our investigations of impact, countermeasures, and damage, which we use in our countermeasure activities.

Disseminating security advisory information

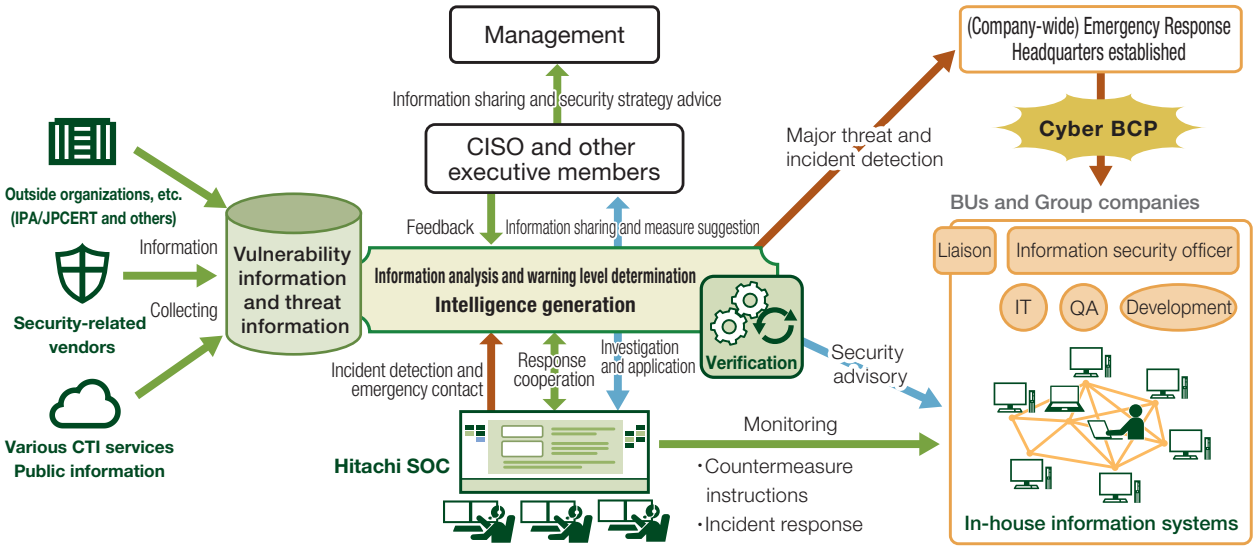
Collected information is disseminated to selected people responsible for cybersecurity of BUs and Group companies. This might take place by email (immediate or weekly digest) or posting to an internal website. Additionally, to enhance countermeasures, when a threat has the potential to widely impact the whole Hitachi Group's operations, we issue a cyber alert to urge thorough implementation of countermeasures, and we consider issuing a cyber BCP. We also survey public systems outside of the company, and if there is a risk of damage, we contact the relevant departments individually and recommend countermeasures. We share the collected and analyzed information with Hitachi SOC and IT system departments, and use it to enhance incident responses and monitoring.

Based on the knowledge gained through these activities, we examine the current status of the Hitachi Group and countermeasures that require improvement. We then share this with the HQ security management division and link it with deliberations at the management level about security strategy for the Hitachi Group, to accelerate the security response execution cycle.

Taking action in emergency situations

If a threat might severely impact business operations at numerous sites within Hitachi, or would render continuation of business impossible on a company-wide scale, Hitachi establish a task force that directs the response at the company level, with measures such a issuing a cyber BCP. (Figure 2-㉕)

Figure 2-㉕ 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 an artificial cybersecurity-related occurrence, 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 skill set of an incident response team 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 role of the HIRT is to provide ongoing support for Hitachi's cybersecurity countermeasures through vulnerability handling, which eliminates vulnerabilities that threats might exploit, and incident response which involves evading and resolving cyberattacks. The team approaches these tasks from the perspective of intra-organizational activity and collaborative activity. Intra-organizational activity covers information security initiatives targeting Hitachi's corporate information systems, and collaborative activity covers initiatives intended to ensure the cybersecurity of products and services targeting our customers' information systems and control systems. HIRT's mission also includes helping to realize a safe and secure internet society by catching the early signs of nascent threats and taking preventive measures at the earliest possible stage.

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

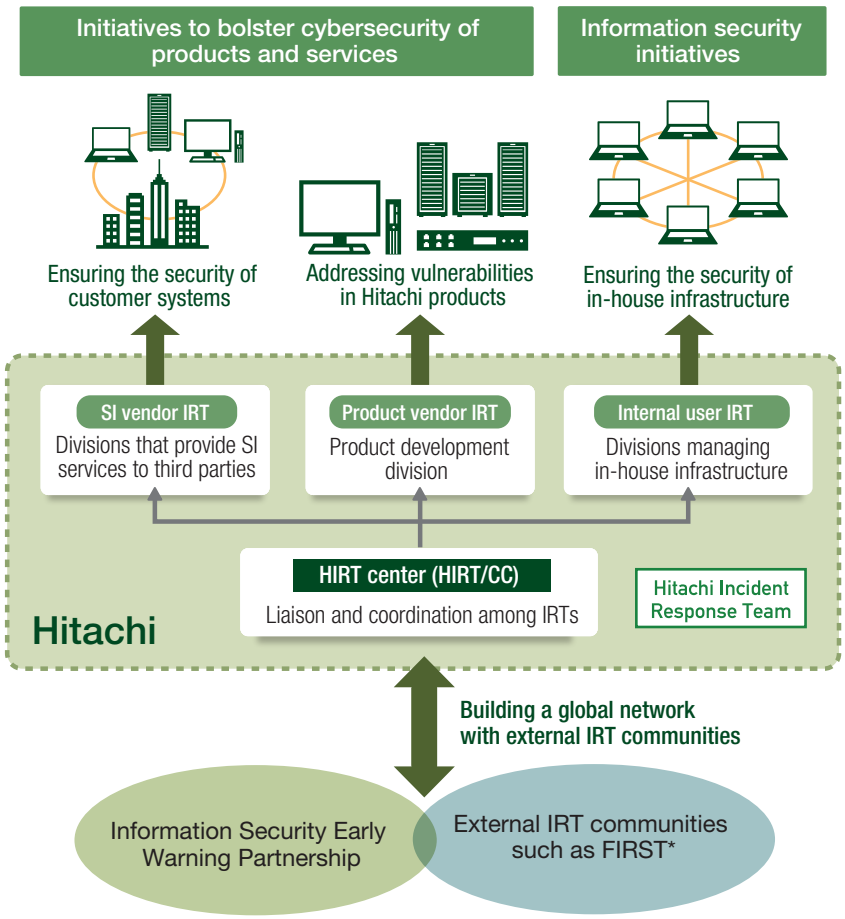
(1) Product vendor IRT, responsible for developing products related to information systems and control systems

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

(3) In-house user IRT, responsible for managing the operation of Hitachi's information systems as an internet user Plus the fourth:

(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 2-26)

Figure 2-㉖ 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*, 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.

* HIRT/CC: HIRT Coordination Center
FIRST: Forum of Incident Response and Security Teams
JPCERT/CC: Japan Computer Emergency Response Team/Coordination Center
CERT/CC: CERT Coordination Center
SI: System Integration

Cybersecurity Initiatives

Activity promoted by the HIRT center

The activity of the HIRT center in relation to in-house IRTs includes promoting cybersecurity measures on a systemic and technical level through cooperation with information security supervisory divisions, which leads the institutional side of IRT activities, and quality assurance divisions, and supporting vulnerability countermeasures and incident response in business divisions and Group companies. The HIRT center also serves as liaison with external IRTs to promote inter-organizational cybersecurity measures.

In-house IRT activity

In-house IRT activity includes issuing alerts and advisories derived from know-how obtained through the gathering and analysis of security-related information, and feeding this know-how back into product and service development processes in the form of guidelines and support tools.

(1) Collecting, analyzing, and disseminating security-related information

The HIRT center disseminates information and know-how related to vulnerability countermeasures and incident response fostered through involvement in the Information Security Early Warning Partnership*1 and other initiatives.

*1 A public-private partnership based on official rules that facilitates the unimpeded dissemination of information related to vulnerabilities in software products and websites and the proliferation of countermeasures.

(2) Developing frameworks for research activity

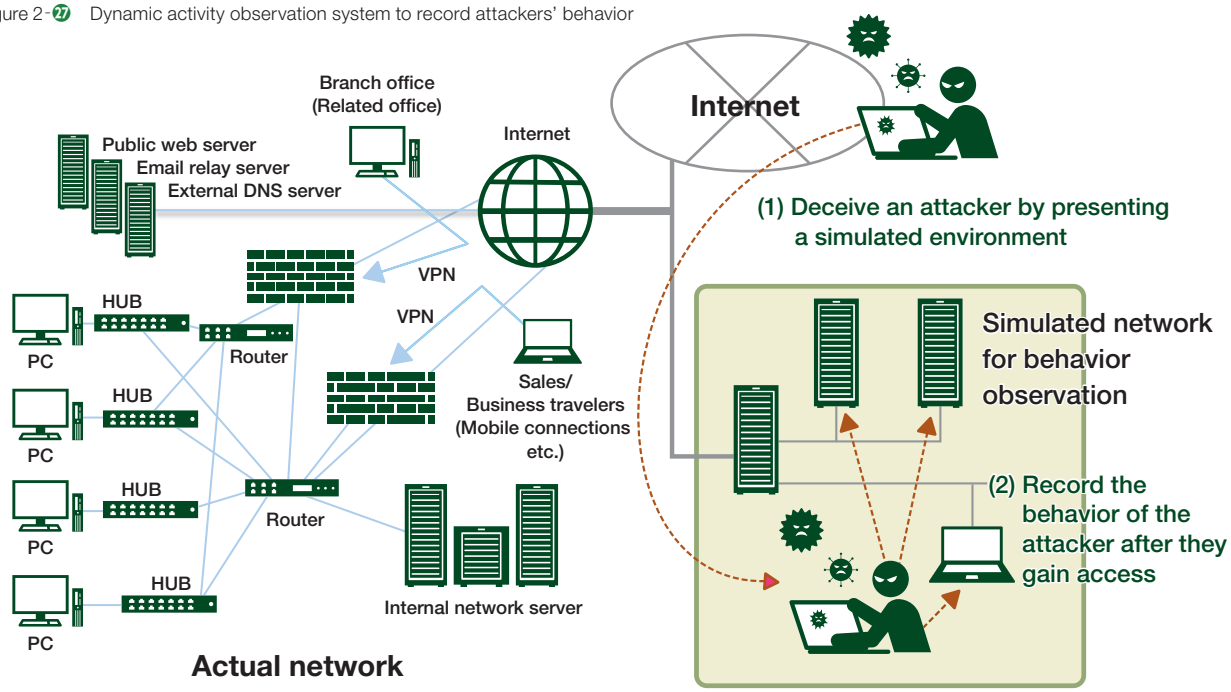
The HIRT center uses behavior observation technology to identify nascent threats and implement countermeasures as early as possible. Behavior observation is an observational technique that uses a simulated version of an organization's internal network to investigate cyberattacks such as spear phishing. This technique is used to record and analyze the behavior of an attacker who has managed to infiltrate the system. (Figure 2-27)

(3) Improving security technology for products and services

To improve the IRT capability at an 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 dissemination of practical in-house security know-how, the HIRT center is also involved in the development of simulated cyberattack drills that teach workers how to handle spear phishing and ransomware.

In June 2022, HIRT was registered with the CVE Numbering Authority (CNA), to be able to assign CVE ID numbers to vulnerabilities in Hitachi products, and to create and publish CVE records.As a CNA, HIRT

Figure 2-27 Dynamic activity observation system to record attackers' behavior



assigns a CVE ID when a vulnerability is reported in a Hitachi product and publishes suitable vulnerability information, as it works to enable customers to use our products with peace of mind.

(4) Implementing IRT activity for individual sectors

The HIRT center assesses and organizes IRT activity for specific sectors that accounts for the context and trends of that sector. A preeminent example of such an initiative is HIRT-FIS*2 established in October of 2012 for the financial sector.

*2 HIRT-FIS: Financial Industry Information Systems

Inter-organizational IRT activity

As inter-organizational IRT activity, multiple IRTs promote inter-organizational cooperation to present a united front against developing threats and build partnerships that can help improve each other's IRT activity.

(1) Enhancing domestic cooperation for IRT activity

The HIRT center endeavors to create networks for cooperation, including passing on information about vulnerabilities and incidents that came to be known through information gathering to the PoC of other member organizations as part of CSIRT activity. The HIRT center also supports the creation of an information-sharing platform based on the JVN*3 service jointly operated by the JPCERT coordination center and the Information-technology Promotion Agency (IPA).

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

(2) Enhancing international cooperation for IRT activity

The HIRT center promotes the organization of a framework for collaboration among international IRT organizations and overseas product vendor IRTs that make use of FIRST initiatives, and a platform for information sharing that uses STIX*4 and United States Department of Homeland Security's AIS*5 program.

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

(3) Organizing research activity

The HIRT center fosters opportunities for human resource development and the development of researchers and workers with specialized knowledge through participation in academic research including anti-Malware engineering WorkShops (MWS).

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 a safe and trustworthy environment and Valuing 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 2-㉘)

Personal information protection framework

To fulfill its mandate as an organization committed to the appropriate handling of personal information, Hitachi's upper 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 JIS Q 15001 which is the basis for PrivacyMark certification. In addition to creating these rules, Hitachi implements concrete safety management measures that come into effect when handling personal information. There are four aspects to these measures: organizational, personal, physical, and technical. (Figure 2-㉙)

Figure 2-㉘ 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. (hereinafter "Hitachi") is a global supplier of total solutions. In this role, Hitachi handles all manner 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.co.jp/utility/privacy/).

(1) Formulation of personal information management rules and ongoing improvement of personal information protection management systems

Hitachi has formulated personal information management rules that ingrain the importance of personal information protection in its managers and workers, and ensure that personal information is used appropriately and protected. Hitachi thereby reliably operates personal information protection management systems. Hitachi also maintains these systems and subjects them to ongoing improvement.

(2) Collecting, using, and providing Personal information and prohibiting use for unintended purposes

Knowing the respect owed to the personal information it possesses, Hitachi establishes management frameworks for personal information protection that reflect its use in day-to-day business. Hitachi also collects, uses, and provides personal information appropriately according to predetermined rules. Hitachi does not use personal information other than for its intended purpose, and has measures in place to prevent such misuse.

(3) Implementing and revising safety measures

To ensure the accuracy and safety of personal information, Hitachi complies with rules and regulations related to information security. This includes controlling access to personal information, limiting means by which it can be removed from business premises, preventing unauthorized access from external sources, and other measures to prevent leakage, loss, or damage. Upon discovering an issue with its safety measures, Hitachi identifies the cause and takes remedial action.

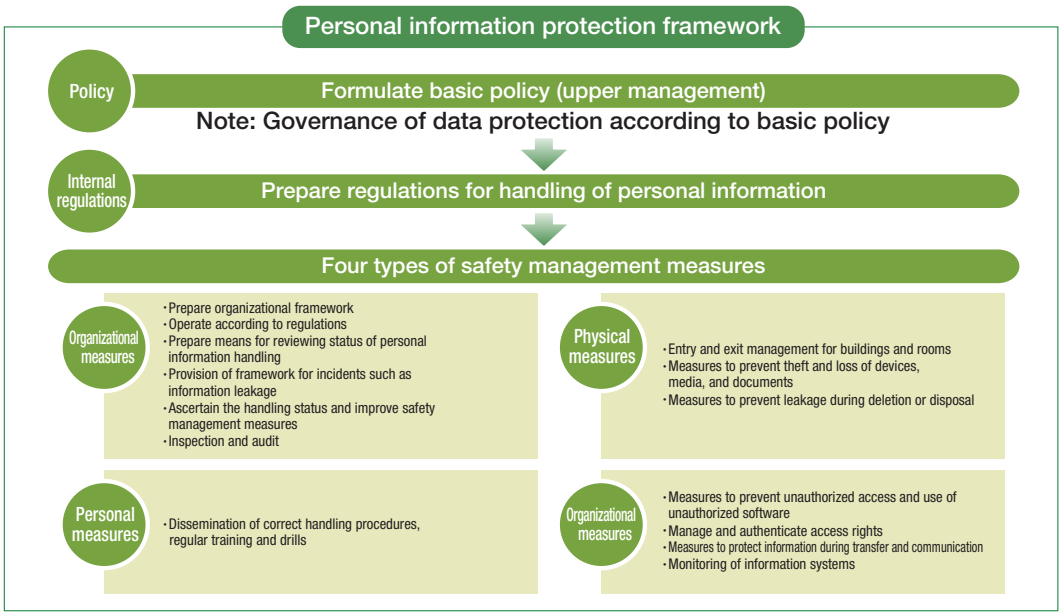
(4) Complying with laws and regulations

Hitachi complies with applicable laws, national guidelines, and other standards relating to the handling of personal information. Hitachi's own personal information management rules confirm to these laws, guidelines, and standards.

(5) Respecting the rights of the subject in relation to personal information

Hitachi will comply with requests from the subject of personal information to disclose, modify, delete, cease use of, or cease provision of that information, and respond in good faith to complaints and inquiries concerning the handling of personal information.

Figure 2-㉙ 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 offices appoint information asset managers in all divisions, 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 2-㉚)

■Safety management measures

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

Hitachi defines rules related to the roles and responsibilities of workers in relation to safety 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 personal safety 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. (See Education regarding personal information protection).

As physical safety management measures, Hitachi has put safety 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 safety management measures, Hitachi prevents unauthorized access to information systems and eliminates unauthorized software. 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.

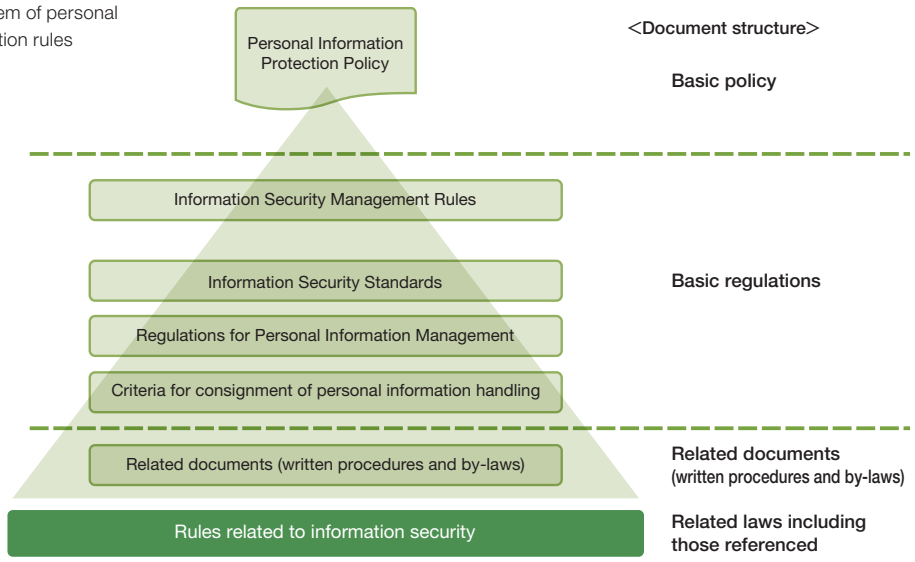
The 47 articles of the general rules for information security management define the rules for personal information protection management.

The handling of personal information is based on the 63 articles of the personal information protection rules, the 12 articles of the criteria for consignment of personal information handling, and related documents.

■Personal information protection management cycle

Hitachi's framework for personal information protection management is subject to the PDCA

Figure 2-㉚ System of personal information protection rules



(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. (See Management and appropriate handling of personal information)

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. (See Auditing personal information protection)

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.

In FY 2021, we formulated a plan for compliance with the Amended Act on the Protection of Personal Information and amended related rules, as the “Plan” stage. The “Do” stage is now in progress at all sites, to be followed by the “Check” stage of testing and auditing within FY 2022 to confirm progress, and the “Action” stage to assess results and make revisions. (Figure 2-31)

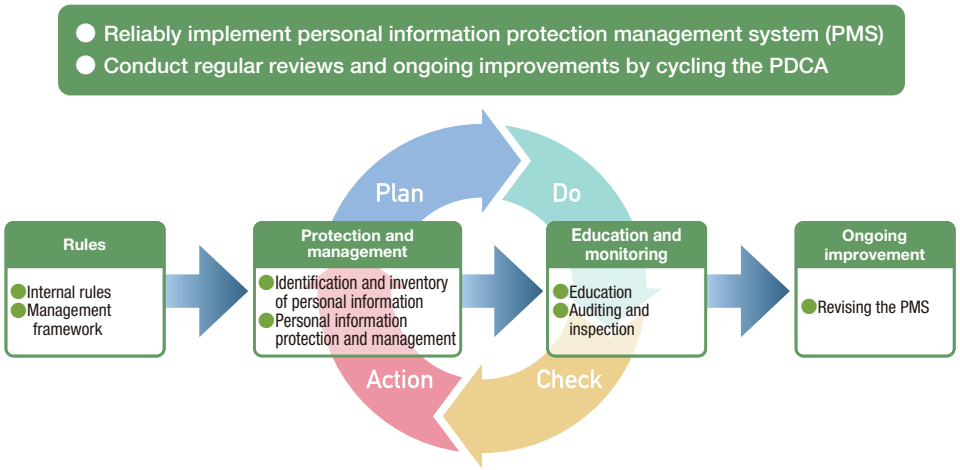
Management and appropriate handling of personal information

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 workspace nominates a person to be responsible for personal information management (an information asset manager). This person identifies all personal information handled during business, manages it in a ledger, and takes the appropriate measures according to the importance and risk of 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 sign a document attesting as such before starting their work. During operations, each workplace conducts a monthly self-check to assess the status of safety management measures and operations.

Figure 2-31 The framework of personal information protection management though the PDCA (Plan-Do-Check-Action) cycle



Initiatives for Data Protection

Hitachi's internal regulations comply with the standards required by the My Number system. 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 testing 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 in a Hitachi-wide auditing and inspection process. All Hitachi, Ltd. departments perform “Personal Information Protection and Information Security Operation Checks” annually, as self-checks in the workplace. In addition, departments involved in operations that handle important personal information (740 operations*) perform “Personal Information Protection Operation Checks” every month. With these measures, we regularly check safety management measures and their operational status.

*As of March 2022

Education regarding personal information protection, and fostering understanding among employees

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.

Stricter management of subcontractors

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.

Global personal information protection initiatives

Advancements in data use driven by the significant progress being made in digitalization will inevitably result in increased privacy risk and impose greater demands on personal information protection. Under these circumstances, countries all over the world are formulating and revising legal frameworks related to personal information protection.

With data use sometimes crossing international borders, the personal information protected by a country's legal framework will not always belong to its domestic subjects, and restrictions might apply to cross-border transfer. For this reason, compliance for personal information protection must be based on a thorough understanding of current trends in various countries' legal systems.

As a pioneer in global compliance with personal information protection legislation, Hitachi has been promoting compliance with the European General Data Protection Regulation (GDPR).

We are also promoting compliance with data protection laws and regulations in other countries and regions in cooperation with local regional management companies.

In 2021, we enacted the “Hitachi Group Privacy Principles” as a common code of conduct for personal information protection throughout the Hitachi Group, 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.

To promote compliance with personal information protection requirements by all Hitachi Group companies, we will continue to bolster and develop the ability of these companies to comply with applicable 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 eighth certification in March 2021 and is continuously working towards the next renewal in March 2023.

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 2022, 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
Hitachi ICT Business Services, Ltd.
Hitachi Urban Support, Ltd.
Hitachi Academy Co., Ltd.
Hitachi Information Engineering, Ltd.
Hitachi SC, Ltd.
Hitachi Global Life Solutions, Inc.
Hitachi KE Systems, 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 High-Tech Solutions Corporation
Hitachi Power Solutions Co., Ltd.
Hitachi Building Systems Co., Ltd.
Hitachi Foods & Logistics Systems Inc.
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.

Using personal data and protecting privacy

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-xDBCA__xDD28_ illustrates, 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 2-32)

Hitachi's privacy protection initiatives

Hitachi 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 since 2014 led by the IT sector.

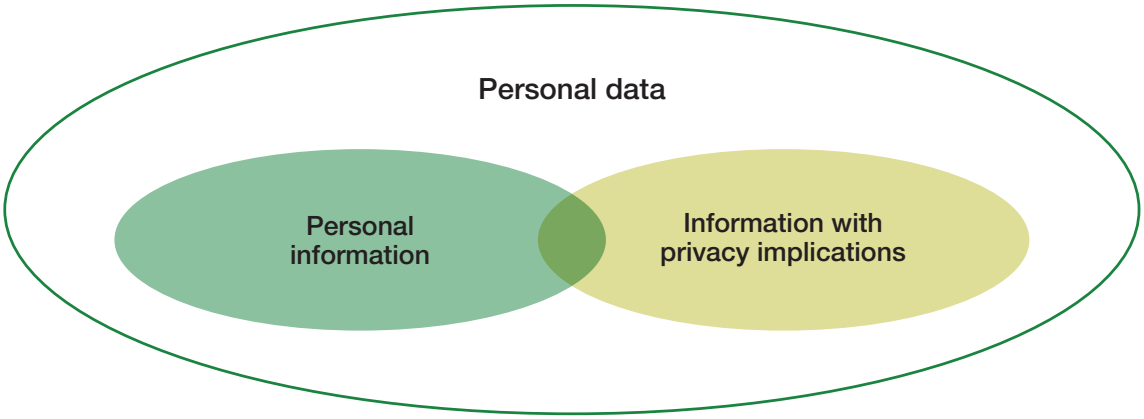
■Operation of the privacy protection advisory committee

In the IT sector that is at the forefront of digital business, Hitachi has nominated personal data managers who oversee the handling of personal data, and established a privacy protection advisory committee which supports risk evaluation and countermeasure assessment by aggregating knowledge related to privacy protection.

■Preparing rules and manuals related to privacy protection

Hitachi has defined a privacy protection policy with reference to this framework, defined rules for handling personal data based on its policies, and created manuals for workers. These manuals set out specific processes to be followed and matters to consider to protect privacy, allowing each employee to implement privacy protection measures.

Figure 2-32 Relationship between personal data, personal information, and information with privacy implications



Assessing privacy impact

Using these rules and manuals, workers involved in business processes that handle personal data can conduct a privacy impact assessment and take measures to prevent privacy issues from arising. To carry out this assessment, the worker uses a checklist in a format created by Hitachi based on legal systems, technological trends, case studies, and knowledge gleaned from opinion surveys (described later). If the employee's judgment will not suffice or risk is determined to be high, the privacy protection advisory committee can reduce risk by providing support.

Hitachi has applied privacy impact assessments to many of its operations, with approximately 230 in fiscal 2021 alone. The business fields covered are also diverse, including finance, public, social infrastructure, and industry/distribution.

Privacy protection education

Using personal data while also protecting privacy requires that individual employees understand the importance of privacy protection and implement privacy measures accordingly. To this end, Hitachi conducts regular education and information sharing related to privacy protection and keeps a keen eye on attitudes regarding privacy protection in wider society.

Ensuring the safety and security of consumers and customers

With the goal of meeting consumer expectations regarding privacy protection, Hitachi worked with Hakuhodo Inc. in 2020 to conduct its “5th Opinion Poll Regarding Consumer Information Handled as Big Data”*1.

Hitachi reflects changes in consumer attitudes, learned through such investigations, in our privacy protection measures.

The “Corporate Privacy Governance in the DX Era Guidebook ver1.2”*2 published by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry also notes the importance of regularly surveying public opinion in these types of surveys to facilitate the evaluation and improvement of measures. Hitachi's efforts were also noted as a case study in the guidebook.

In March 2022, we presented our actions on privacy protection under the title of “Personal Data Usage and Privacy Protection” at the Symposium on the Proper Use of Personal Data, which was organized by the Japan Business Federation (Keidanren).

At a panel discussion after the presentation, the panelists rated Hitachi's privacy protection initiatives as advanced and valuable.

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.

*1 “5th Opinion Poll Regarding Consumer Information Handled as Big Data” (published December 2020)
https://www.hitachi.co.jp/New/cnews/month/2020/12/1222a.html
*2 “Corporate Privacy Governance in the DX Era Guidebook ver1.2” (Published in February 2022)
https://www.meti.go.jp/policy/it_policy/privacy/guidebook11.pdf

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.

Global security workshops held with counterparts in Europe and the Americas deepen understanding of measures that are promoted as internal controls. Workshops in Japan hold panel discussions under the heading of security ecosystems with a perspective completely different from 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 activity:

- 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, and homeland security.

• 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
IEC's TC 65 promotes the standardization of industrial automation, measurement, and control. In TC 65, WG10 assesses the standardization of security of the networks and control device in control systems. WG20 assesses frameworks to bridge the requirements for safety and security.
• 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 September 2022, membership consists of 652 teams from 101 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, and between 2015 and 2020, a Hitachi representative held the position of chairperson of the association. In 2021, FIRST became a general incorporated association, and Hitachi has helped to promote domestic CSIRT activities as an executive committee member.

■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, Control Systems SMS 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
• ICT-ISAC
• Council of Anti-Phishing Japan
• National Institute of Technology and Evaluation (NITE) Evaluation Body Certification Technical Committee
• Robot Revolution & Industrial IoT Initiative and Industrial Security Action Group
• Japan Society of Security Management (JSSM)
• CRIC Cross-Sector Cybersecurity Committee, CRIC Security Quality Committee, etc.

Working to Raise Information Security Awareness

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

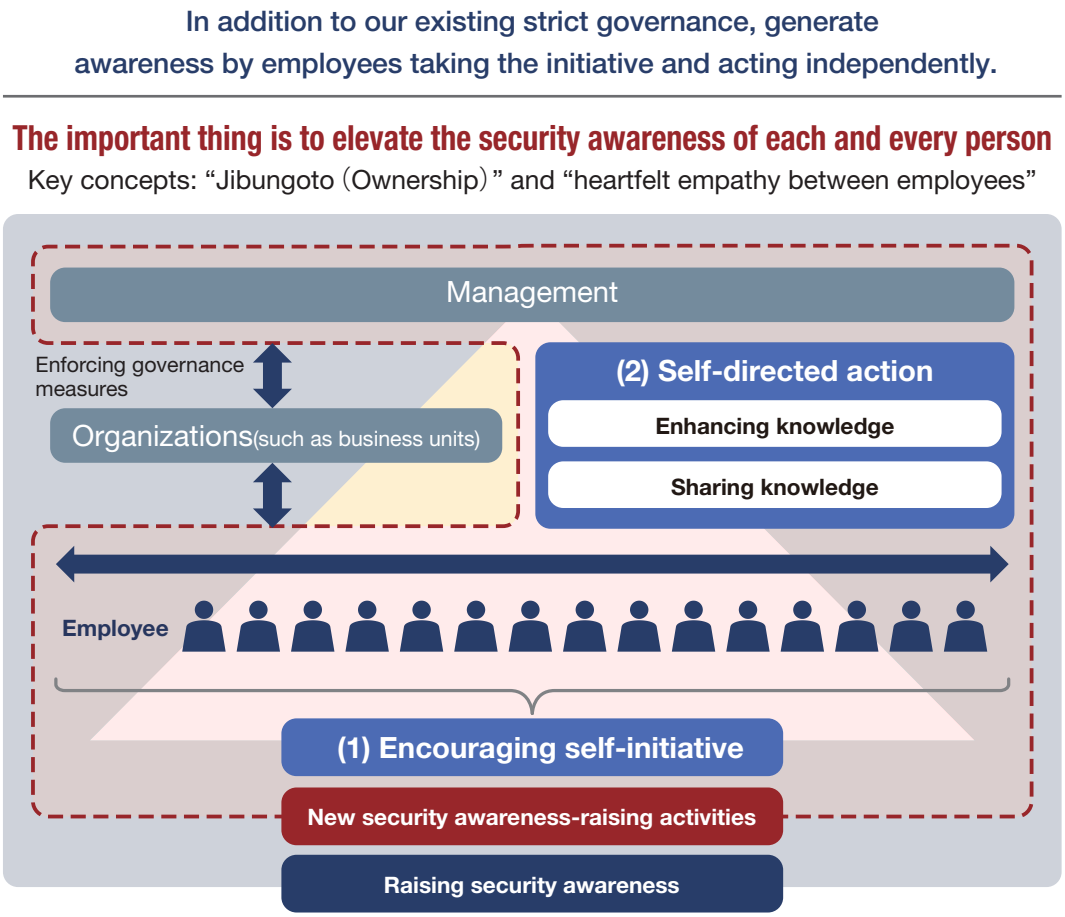
"Jibungoto(ownership)" in information security

The ongoing COVID-19 pandemic has accelerated and normalized working from home, but with growth in cyber attack threats showing no signs of abating, adequate security measures are essential to unlock the potential of working from home. Until now, attacks have primarily targeted vulnerabilities in organizations' IT infrastructure, but with work styles increasingly based on working from home, attackers are beginning to target 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 promoting more balanced security measures, in order to adapt to the current dramatically-changing environment 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 "heartfelt empathy between employees". (Figure 3-❶)

Figure 3-❶ The ideal future form of security awareness



Encourraging self-initiative: Harry's Security

Since December 2020, we have been 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 3-❷)

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.

Self-directed action: Green Aegis

In May 2021 we started Green Aegis internal community activities as “behavior reform” to support employees in their own independent actions on security measures. (Figure 3-❸)

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 which we have taken, distributing videos that employees have planned for themselves, and allowing 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 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.

Figure 3-❸ 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.

COLUMN

Product Security Technologies to Protect Clients' Businesses

Recent cyber attacks have targeted products and OT systems that are increasingly connected, and the resulting damage is increasingly severe. Legal regulation and standardization of product security is advancing rapidly in every industry, and response is becoming indispensable for Clients' businesses.
Hitachi is working to develop various security technologies to protect Clients' businesses.

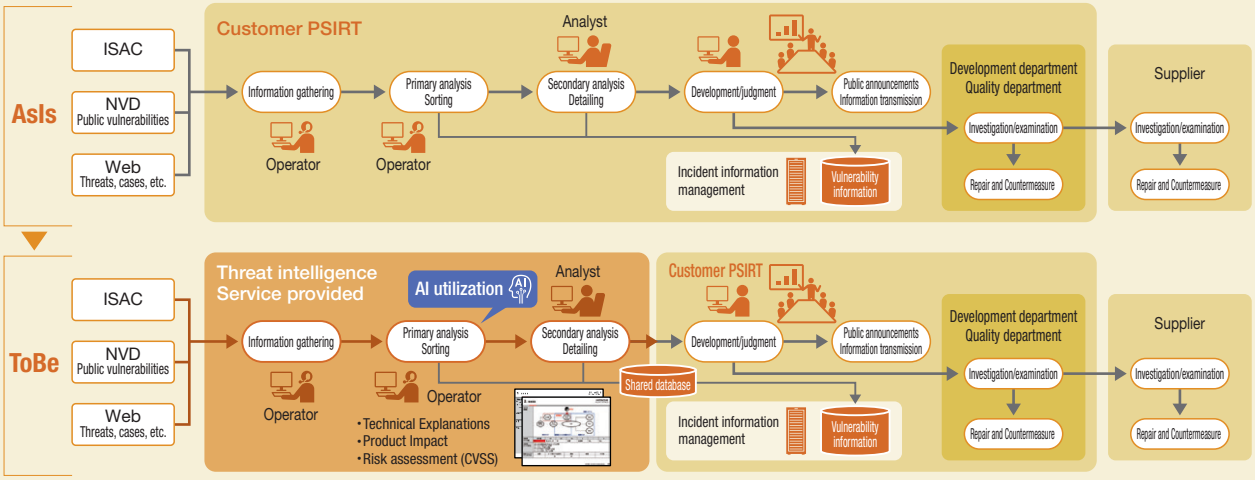
Promoting the development of product security technologies to protect Clients' businesses

Cyber attacks used to target IT systems. More recently, products from vehicles to home appliances and OT systems such as factories and social infrastructure have been connected to the internet and other networks, exposing them to unprecedented cyber attack threats. Many of these “Internet of Things” (IoT) systems are directly linked to people's lives and safety, making it extremely important for customer companies, which bear responsibility for sales and operations, to protect the security of their own products. The enactment and mandatory enforcement of legal regulation and guidelines about product security is advancing rapidly in every industry and around the world, and compliance is becoming indispensable for Clients' businesses. Security must be considered in all parts of the product life cycle, through design, development, and operation. In recent years, products which have been in operation for long periods are getting connected, and the software they run is becoming increasingly complicated, so security needs in the operation phase are rising. Hitachi is developing product security technologies for the operation phase, such as intelligent threat analysis for PSIRT and security operation technology for vehicles.

Intelligent threat analysis technology for PSIRTs

Customer companies are calling for the establishment of a PSIRT (Product Security Incident Response Team) organization to protect product security in the operation phase. A PSIRT monitors product-related vulnerability information, judges the impact of such information on products, and makes decisions about responses. A PSIRT gathers large amounts of information about product security every day, from the internet, external organizations, and other sources. This information must be sorted appropriately and its impact determined. Expert personnel well versed in security and our products are essential for that work. The extension of the IoT into products is accelerating and the volume of security information grows day by day, but it was difficult to train

Figure 1 Summary of intelligent threat analysis for PSIRTs



and maintain the expert personnel needed for the work. That made scalability a challenge.

Hitachi is addressing that challenge by developing AI-based intelligent threat analysis for PSIRT. This technology uses AI to automatically judge whether collected security information is related to the relevant field and the client company. Using AI with judgment models trained on IT-related and industry-specific security information can eliminate 80% of the information that PSIRT experts would have had to see. The intelligent threat analysis delivery service that Hitachi provides uses this technology, helping to provide client companies and industries with timely analysis reports tailored to their needs. (Figure 1)

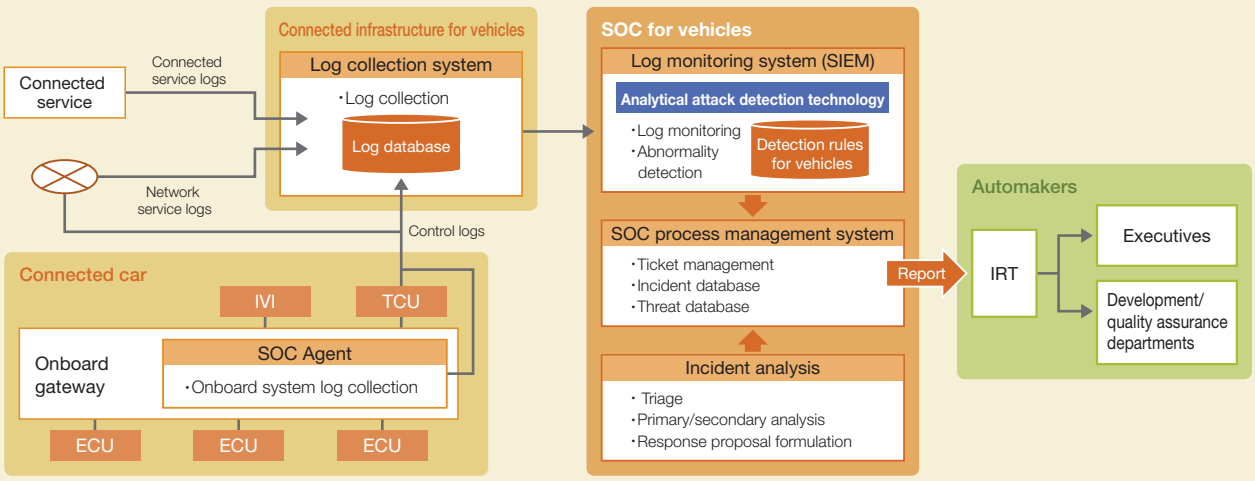
Security operation technology for vehicles

The risks of cyber attacks on connected cars and other vehicles are growing. Regulations on vehicular cybersecurity are enacted by UNECE WP29. They call for the maintenance of security at the operation stage, in addition to measures applied during manufacturing. In response, automakers are working to set up vehicle security operation centers to monitor vehicles and detect and handle attacks. We apply our experience with SOCs (Security Operation Centers) for IT and our knowledge of developing vehicular devices to develop technologies and provide solutions for vehicle-related SOCs.

Hitachi's vehicular SOCs monitor logs for vehicles, centers, mobile connections, etc. in real time, detect attacks quickly, and limit the damage. We provide systems that extend from onboard systems to the cloud and support fast and accurate incident responses. On the vehicle side, in particular, we ascertain the features that are unique to onboard systems, design and place monitoring logs, and provide software to efficiently collect logs from vehicles into monitoring systems. We use comprehensive analysis of logs collected at onboard gateways to estimate attack scenarios, and detect the signs of an attack from the moment an attacker enters from outside the vehicle.

The creation of appropriate attack-detection rules is essential for the effective analysis of logs in monitoring systems. The creation of attack detection rules in conventional IT-oriented SOCs required the accumulation of attack cases, but the small body of cases of attacks on cars was a problem, and it would have been difficult to apply the system as it was. In the absence of cases, it's necessary to comprehensively imagine all kinds of attacks, but to keep up with the release timing of vehicle models, detection rules had to be designed efficiently. We responded the situation by developing analytical cyber attack detection technology for vehicular SOCs as a way to create detection rules even when there were few attack cases. By that method, we used our security design technology to analytically identify threats to vehicles, and then assigned the attacker's behavior to categories which we could infer from attack examples accumulated in the IT field. We could then convert attacker behaviors to apply to the vehicular field on the basis of differences between the IT and vehicular fields. That approach enabled us to efficiently create detection rules without omissions. We use that technology in our solutions for vehicular SOCs. (Figure 2)

Figure 2 Summary of security operations for vehicles



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 August 2022). 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. (Social Infrastructure Systems Business Unit, Control System Platform Division)
- Hitachi, Ltd. (Service & Platform Business Unit Service Platform Division, Lumada CoE, Software CoE, Application Services Division Lumada Solutions Operation)
- Hitachi, Ltd. (Social Infrastructure Information Systems Division, Strategy Planning Division, Energy Systems Division 1, Energy Systems Division 2, Energy Solutions Division and Transportation Information Systems Division)
- Hitachi, Ltd. (Social Infrastructure Systems Business Unit, Government & Public Corporation Information Systems Division)
- Hitachi, Ltd. (Water & Environment Business Unit, Water Solutions Division, Digital Solutions Business Development Department, Water & Environment Business Unit, 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, Systems & Services Business Sales Management Division, Defense Systems Sales Management, and Hitachi Advanced Systems Corporation (HQ)
- Hitachi Channel Solutions, Corp.
- Hitachi Social Information Services, Ltd. and Okinawa Hitachi Network Systems, Ltd.
- Japan Space Imaging Corporation
- Hitachi Information & Telecommunication Engineering, Ltd. (Customer Support Center)
- Hitachi Information Engineering, Ltd.
- Hitachi ICT Business Services, Ltd. (Product Support Department Media Service Group)
- Kyushu Hitachi Systems, Ltd.
- Shikoku Hitachi Systems, Ltd.
- Hitachi Systems, Ltd. (Financial Platform Division Service 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 Advanced Support Platform Design Department)
- Hitachi Systems, Ltd. (Managed Services Division, Cloud Services Division, Business Services Division, Security Services Division)
- Hitachi Systems Power Services, Ltd. (Managed Services Division, Platform Services Office)
- Hitachi Systems Field Services, Ltd. (Branch HQ, Tokyo Branch, Tokyo Office)
- Hokkaido Hitachi Systems, Ltd. (Management Planning Group, Administration Division, Public & Social Systems Management Division, Corporation Services Business Division, Business Planning Department, Systems Division, Systems Section 1, Group 1, Group 2, Systems Section 2, Platforms Division Section 1, Facilities Division Promotion Department, Facilities Service Group, Platforms Division Section 2 Sales Management Division, Sales Planning Division, Public & Social Sales Division, Sales Section 1, Sales Group 1, Sales Section 2, Corporate Sales Division, Sales Section 1, Sales Group 1, Sales Section 2 Production Technology Management Division, Quality Assurance Division)
- Hitachi Solutions Create, Ltd.
- Hitachi Solutions West Japan, Ltd. (Cloud Platform Operating Support Department, Financial Solution Division 1 Department 3)
- Hitachi Solutions East Japan, Ltd.
- Hitachi Solutions, Ltd.
- Hitachi Power Solutions Co., Ltd.
- Hitachi SC, Ltd. (HQ)
- Hitachi Foods & Logistics Systems Inc.
- Hitachi Pharma Information Solutions
- Hitachi KE Systems, Ltd. (Tokyo Development Center)
- Hitachi High-Tech Solutions 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. (As of August 2022 [Includes products in the certified products archive list]) (Figure 4-❶)

Figure 4-❶ 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. (As of August 2022 [Includes products in the CMVP "historical list"]) (Figure 4-❷)

Figure 4-❷ 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, 2022)

Corporate name	Hitachi, Ltd.
Incorporated	February 1, 1920 (founded in1910)
Head office	1-6-6 Marunouchi,Chiyoda-ku, Tokyo,Japan
Representative*1	Keiji Kojima, President and COO
Capital	461.731 billion yen
Number of employees	368,247 (Japan: 156,768, outside Japan: 211,479)
Number of consolidated subsidiaries	853(Japan: 157, outside Japan: 696)
Numberof equity-method associates andjoint ventures	287

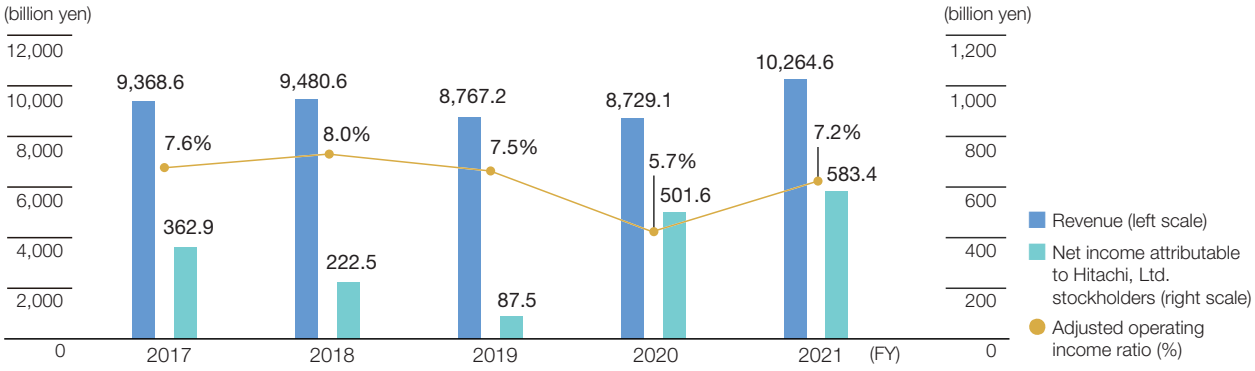
*1 As of June 23, 2021

Consolidated Financial Highlights for Fiscal 2021, Based on the International Financial Reporting Standards (IFRS)

Revenue	10,264.6 billion yen (118% year on year)
Adjusted operating income	7.2% (up 1.5 percentage points, year on year)
EBIT*2	850.9 billion yen (up 6 billion yen, year on year)
Net income attributable to Hitachi, Ltd. stockholders	583.4 billion yen (up 818 billion yen, year on year)
ROIC*3	7.7% (up 1.3 percentage points, year on year)

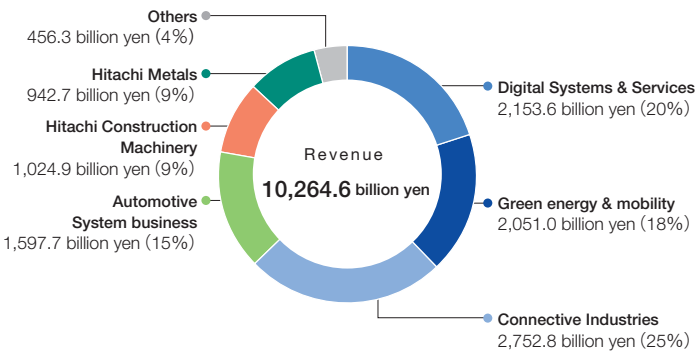
*2 EBIT: Income from continuing operations before income tax, less interest income, plus interest charges.
*3 ROIC: Return on invested capital. Calculated as follows: ROIC = (NOPAT + Equity method gain/loss) ÷ Invested capital × 100. NOPAT (Netoperating profit after tax) = Adjusted operating income × (1 – Tax burden). Invested capital = Interest-bearing debts + Capital.
Note: Hitachi's consolidated financial statement is prepared based on the International Financial Reporting Standards (IFRS).

Revenue, Adjusted Operating Income Ratio, and Net Income



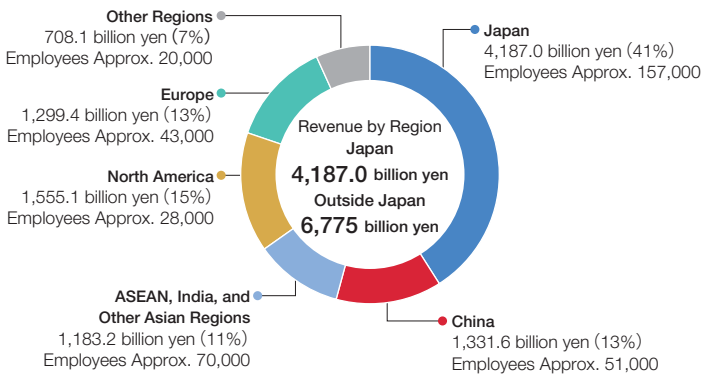
Revenue and Share by Segment

(Consolidated for FY 2021, based on IFRS)



Revenue and Share by Region

(Consolidated for FY 2021, based on IFRS)



Note: Revenue by segment includes intersegment transactions.

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