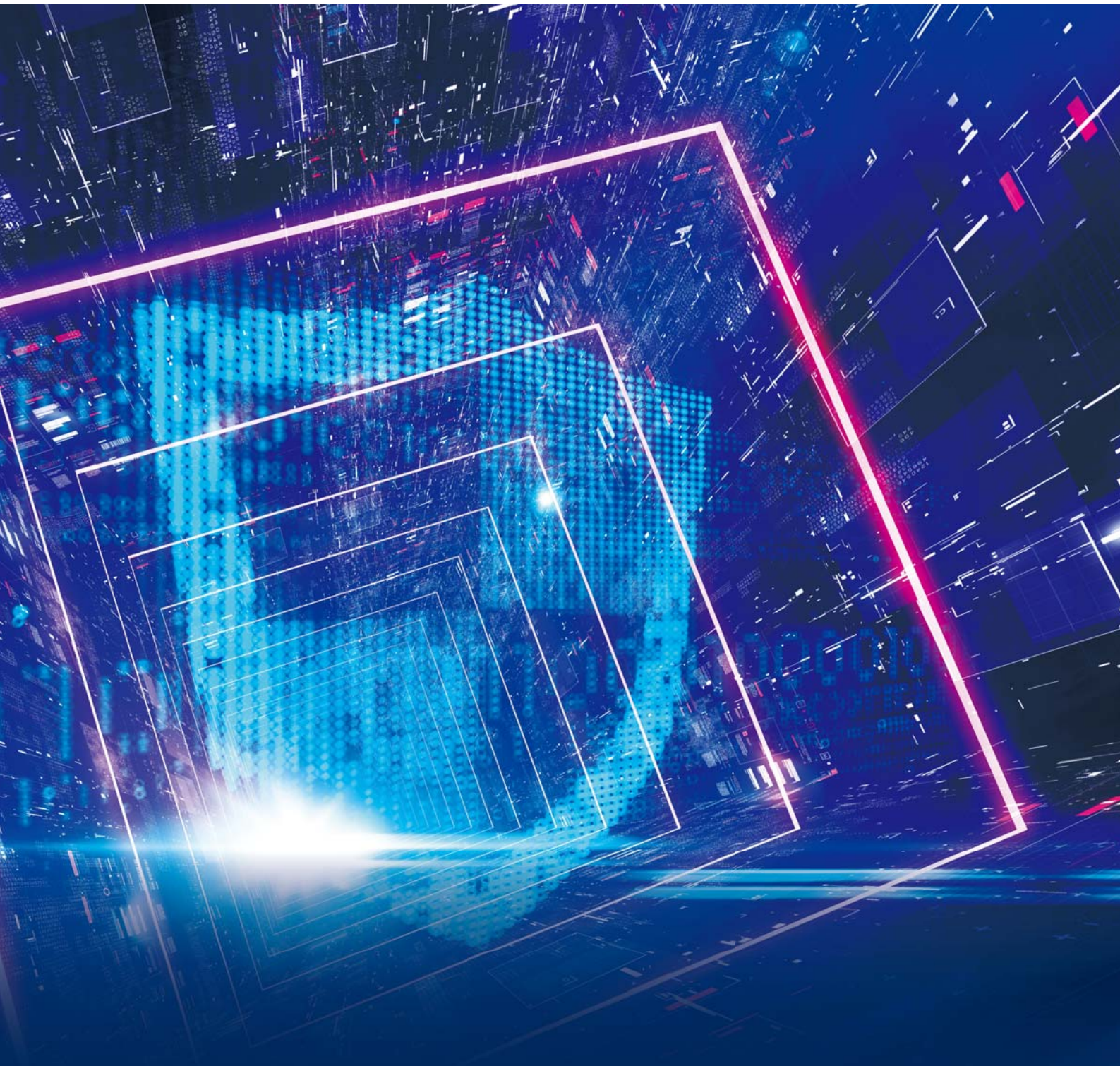


## Information Security Report 2021



# INDEX

CISO Interview	1
Topics	4
Information Security Governance	7
Information Security Management	8
CSIRT Activity in the Hitachi Group	13
Cybersecurity Countermeasures	16
Global Information Security Initiatives	18
Initiatives for Security Human Resource Development	20
Cybersecurity Management Initiatives	22
Initiatives Related to Personal Information Protection	28
<b>Editorial</b> PrivacyMark-Related Initiatives of the Hitachi Group	35
Privacy Protection Initiatives	36
Research and Development for Achieving Information Security	38
External Activity Related to Information Security	40
Third-Party Evaluation and Certification	42
Overview of the Hitachi Group	45

---

## Summary of this report:

- Scope and time period covered by this report: Hitachi Group information security initiatives up to and including FY 2020
- Report publication date: December 2021

---

## Registered Trademark

Windows® is a trademark or registered trademarks of Microsoft Corporation in U.S.A. and in other countries.  
Other company and product names may be trademarks of the respective companies with which they are associated.



## As the "New Normal," Co-creation, and Global Expansion are Progressing, Information Security's Mission is to Underpin the Required Infrastructure

— Looking back over the year, the COVID-19 pandemic has changed the way we work. How do you see the impact on companies' security?

Contactless technology and remote meetings have progressed in various company departments and business scenarios, and the "New Normal" workstyle has taken hold. Online systems are very useful, and it's easy to see the benefits, but we must also be aware of the risks that come with this convenience.

It was assumed that employees would go to the office to do business before the COVID-19 pandemic, but this is no longer the case. As long as the task is accomplished, you can be anywhere in the world. Hitachi also promotes working from home as standard for a wide range of functions, except for work that must be done at the office, such as work to maintain social functions, manufacturing work, and interacting directly with customers. IT systems and tools need to be put in place to allow physically-distanced work. Companies are responsible for building that infrastructure, and information security to support that infrastructure reliably is very important.

— As workstyles change, IT systems are increasingly moving to the cloud, but how do you see the risks involved in these changes?

Cloud-based systems send data over the Internet, so they have higher security risks such as information leaks and unauthorized access. Companies must implement different types of risk countermeasures compared with conventional systems centered on internal networks. Monitoring tools are required, but in parallel to this, it is also important for companies to set certain rules that assume risks, since the actions of each employee are important.

— What form would such rules take? What kind of security awareness should employees that are subject to constant security risks have?

Working styles have changed due to the COVID-19 pandemic, and Hitachi is pushing ahead with creating environments that support remote work. It is essential that employees follow the rules and work in accordance with the systems built by the company. Excuses such as having been in a hurry at the time, being inexperienced, or being unfamiliar with digital technology will not be accepted. Just as we live by the basic rules in society, it is also necessary to approach information security with a strict attitude that takes appropriate measures when rules are broken.



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.

## As the "New Normal," Co-creation, and Global Expansion are Progressing, Information Security's Mission is to Underpin the Required Infrastructure

Also, if your personal laptop or smartphone becomes infected with a virus, you will consider it to be a major issue, so why would you think it is any different for company property? I would like employees to consider all equipment lent by the company to have the same value and meaning as their own personal belongings.

### – How do you position information security within collaborative business based on the use of data?

The Hitachi Group is expanding the "Lumada business" to focus on customer data and bring new insights to light, contributing to solving customer management problems and business growth. Companies use data for Co-creation, but I believe that Co-creation is also about sharing risks in addition to value.

Even if you think your information security is adequate, cyberattacks can enter through the tiniest hole. To avoid this, you need speed and transparency. When you are serving matcha ice cream to your Co-creation partners, you mustn't allow spicy wasabi to get mixed in.

### – Wasabi in the matcha ice cream! What does this mean in terms of security?

There are aspects of business that you must never hide. We must not hide from each other in matters of information security, and we must bring transparency. It is important to be open even if it's inconvenient. When I was younger, I worked in the Procurement Department and was also posted overseas, so I interacted with a wide variety of business people. I realized that the driving force of business is trust between people. I believe that trust is also what is needed to deliver reliable information security for Co-creation.

### – The Hitachi Group is accelerating large-scale M&A at a global scale. What points should be kept in mind from the perspective of information security?

System integration following M&A may create unanticipated security risks, so maintaining a high level of information security is a critical management risk. It is too late to start taking measures after the system integration. We need to be thoroughly familiar with the other company's situation before the merger.

The risk may appear to be small at first, but if something happens, it will affect not only the partner company, but the Hitachi Group as a whole, its customers, and even society. This means that, when a company becomes a new member of the Hitachi Group, we need to conduct interviews in advance, ask them to take countermeasures, and in some cases, go to the site to confirm the situation. Similarly, for our supply chain, we must build our security in a monolithic manner so that confidential information will not be leaked due to unauthorized access by external contractor companies.

### – What types of measures are required to defend against ever-more-intense cyberattacks?

In FY 2021, there have been frequent cases of companies being threatened using ransomware. And the attacks are becoming more sophisticated and ingenious. It's important to remind ourselves that these attackers have different values from us, and that such attacks are constantly being directed at society and companies. We must acknowledge these facts, become more broad-minded, and take appropriate measures in advance. And we must be aware that no matter how strong we make our security systems, they will not prevent 100% of



sophisticated and ingenious cyberattacks. "Perfect" information security measures no longer exist. I believe that we should consider security incidents to be a constant occurrence. Therefore, I believe that we should make efforts every day to develop resistance and cyber resilience, so that we can recover from attacks in the shortest possible time, while implementing thorough monitoring and a diverse range of measures.

**– What do you see as the key success factor in digital environments where gaps and vulnerabilities in human awareness are targeted?**

I believe that the key success factor is the initiative of each employee. Employee security awareness has increased over the long period of remote working during the COVID-19 pandemic. In addition, more and more people are taking the lead by launching activities to improve awareness in the workplace covering a wide range of situations. This includes those involved in manufacturing, those involved in local construction, and those who work regularly together with customers. Ideally, leaders will emerge not only among information security staff, but also in each workplace. In the past, workplace fire brigades were established at Hitachi Factories to ensure that a major fire never occurred again. Today, we continue this spirit, and volunteer fire brigades are stationed at all Hitachi bases. Similarly, if each workplace were to have a "workplace security fire brigade," and if a culture of taking the initiative to monitor the safety of information and report incidents as soon as they occur was established, the Hitachi Group's information security would take a major leap forward.

**– What future course of action and decisions do you see the Hitachi Group taking?**

In recent years, cyberattacks have become increasingly sophisticated and complex, and I feel that there is a limit to what just one company can do to counteract them. Even when I talk to information security staff at other companies, they all have the same challenges. It may now be the time to push for an information security community that crosses the boundaries between companies. We have been doing this on a small scale, but we need more dynamic connections to develop such a community on a broader scale.

Regardless of the industry, cyberattacks enter through vulnerabilities. I believe that the Hitachi Group should take leadership in creating a community that is based not on self-interest but right and wrong.



# Towards Improved Cyber Resilience that Responds to Changes in Society

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. Security threats have become more targeted, 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 initiatives to improve cyber resilience, based on the three approaches of "Governance," "Co-creating security," and "Jibungoto (taking ownership)" for a "new normal" society.

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

**Improve the security resilience**  
**→ Acquire adaptability / flexibility**  
**Cyber resistance**

## ● Governance: zero trust security initiative

In addition to its past initiatives, the Hitachi Group is taking zero-trust security measures as we move our IT platforms to the cloud as a response to global trends and increasingly sophisticated and complex cyberattacks.

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 in the future—as the foundation, and our conventional perimeter-type systems. In creating this zero-trust security built on these cloud-based IT architectures, "Authentication," "Endpoints," and "Cyber-integrated monitoring" are the key elements.

### Authentication

In recent cloud usage, cloud systems that do not use multifactor authentication have a very high risk of unauthorized access. Therefore, we are considering the to-be model of cloud-based authentication, and strengthening privilege management and authentication of individual users.

### Endpoints

We are aiming to strengthen endpoints across the entire system, including not just computers, servers, and smartphones, but also cloud systems and applications. In FY 2020, we deployed EDR to all PC terminals in the Hitachi Group. We are also looking into the security of the network gateway and data itself.

### Cyber-integrated monitoring

Up to now, we have focused on analyzing and responding to our perimeter-type network logs. Going forward, we will need to collect and perform correlation analysis on the cloud, endpoint, and other logs, and respond to any incidents. We have therefore started looking into monitoring systems and structures that are more advanced than our previous cybersecurity monitoring.

## ● Co-creating Security: Work on building a security ecosystem

In general, when people think of security they tend to think of the IT department. But the support of various departments such as PR, HR/Labor, and Legal is also required to respond to incidents. And with the broader scope of security measures, the response is ineffective unless departments such as manufacturing, QA, and procurement also cooperate closely. Since WannaCry, the whole company believes that creating this type of security ecosystem to respond to cyber threats is important, and is taking action. Our approach is that the elements of this ecosystem structure: "things," "organizations or individuals" and "society," must be connected.

### Connections between "things"

With DX, in order to create new added value and solve social issues, things such as equipment and systems require a connected environment, as exemplified by IoT. In response to this, Hitachi is taking comprehensive cybersecurity measures for all types of environments.

### Connections between organizations or individuals

Maintaining security in a world where connections are made between things that until now were unconnected requires that different organizations work together to promote security measures. As well as enforcing measures through internal controls, Hitachi engages in community-building across positions and organizations, reaffirms individual responsibility, and deepens connections with others. This activity forms connections between organizations or individuals.

### Connections within society

Connections are not just needed within Hitachi. It is now essential to share threat information and issues encountered when implementing countermeasures with governments, schools, enterprises, 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 management cycle, creating further connections in society.

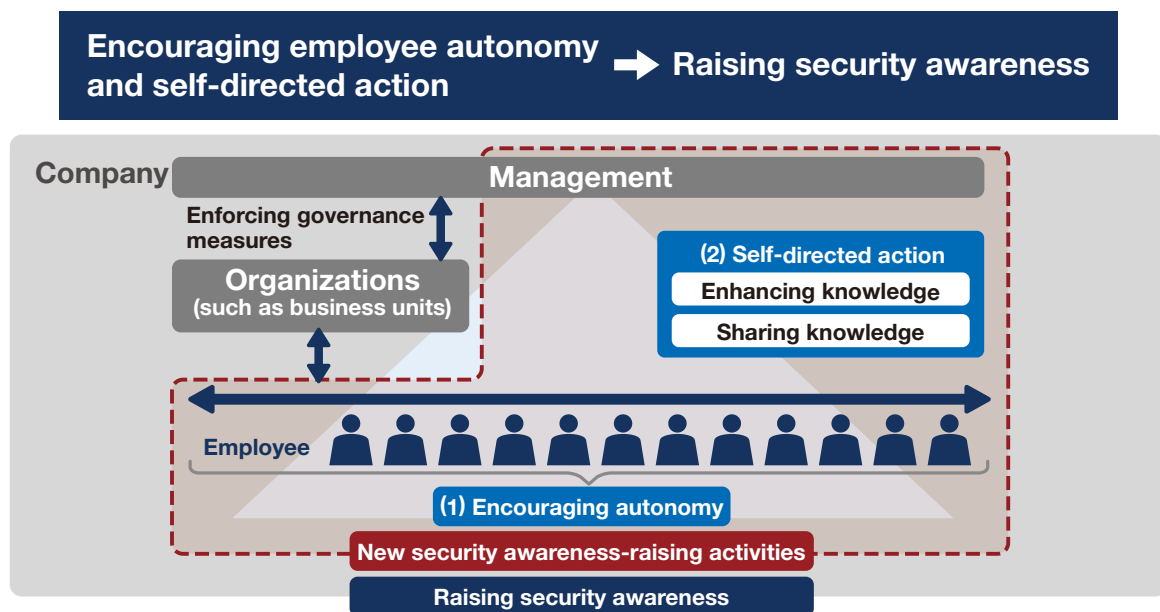
## Towards Improved Cyber Resilience that Responds to Changes in Society

### ● Jibungoto: security awareness-raising work

It is assumed that vulnerabilities in security awareness will be targeted as employees recently work from home due to the COVID-19 pandemic. Working outside the office in an unfamiliar environment can lower your 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 ownership of security. Since December 2020, we have been promoting internal communications to help employees see that security is an issue that directly impacts them and to encourage them to get involved independently. And since May 2021, we have started internal community activities to provide opportunities for employees to independently acquire knowledge and research the issues, and to share this knowledge with their colleagues.



At Hitachi, in addition to implementing strict internal control within the company, through our external activities, we are building a security ecosystem with Co-creation between industry, government, and academia for the whole of society. To build a line of defense strong enough to protect the organization, we are promoting "Jibungoto" and aim to foster a correct understanding of security among all workers and build an awareness that encourages ideal ways of working. Hitachi is taking steps to improve cyber resilience by making "Governance" "Co-creating security" and "Jibungoto" a reality so that people can feel safer, more secure, and comfortable in the "new normal," and to avoid the risks of this new era.



# Information Security Governance

## Basic philosophy of information security governance

The advancement of IoT has created new value through the interconnection of all manner of "things". However, cyberattacks growing more sophisticated every day and their range of targets has expanded from traditional IT to the Internet of Things (IoT) and to OT which encompasses control and operational technology. To minimize risks such as information leakage and business shutdowns that impact the continuation of business itself, risk management as it pertains to information security is one of the most important issues a business faces.

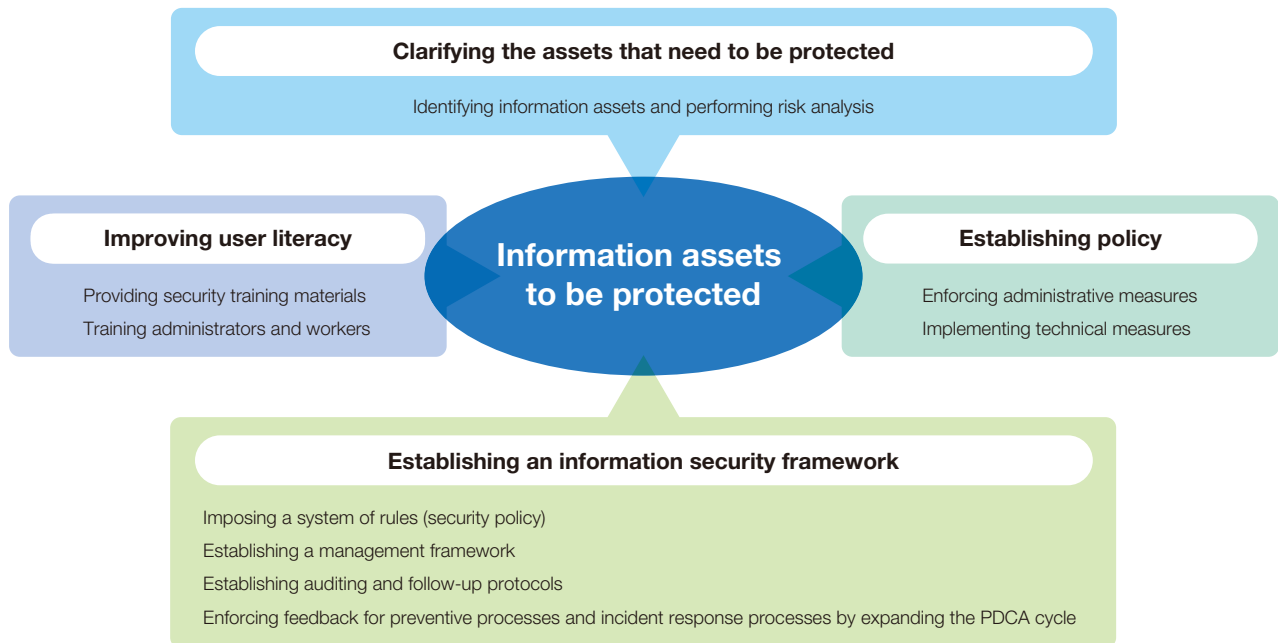
Hitachi endeavors to be a global leader in social innovation

business. In this role, Hitachi deems cybersecurity one of its key business challenges from dual perspectives of value creation and risk management, and is honing its expertise in information security governance.

## Information security initiatives

Hitachi is duty-bound to protect its diverse information assets including information kept on customers' behalf, the systems that hold this information, and the information systems that underpin social infrastructure services. To this end, Hitachi engages in information security from four perspectives grounded on the assumption that incidents will inevitably occur. By maintaining the PDCA cycle for the information security management systems of

the Hitachi Group under the guidance of Hitachi, Ltd., we are improving the security level of Hitachi Group companies around the world.



# Information Security Management

The following gives an overview of Hitachi's policy, promotion frameworks, rules, management cycle, and other matters in relation to information security.

## 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. Group management is achieved through similar controls implemented by BUs and Group companies with respect to its subsidiaries. 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.

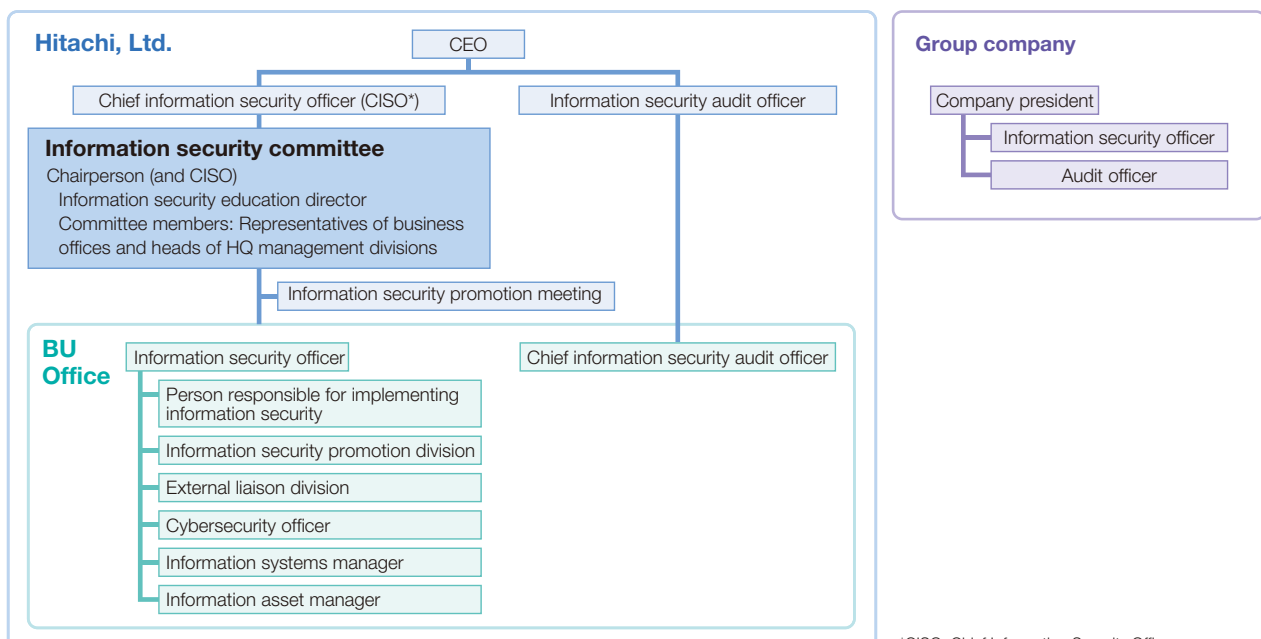
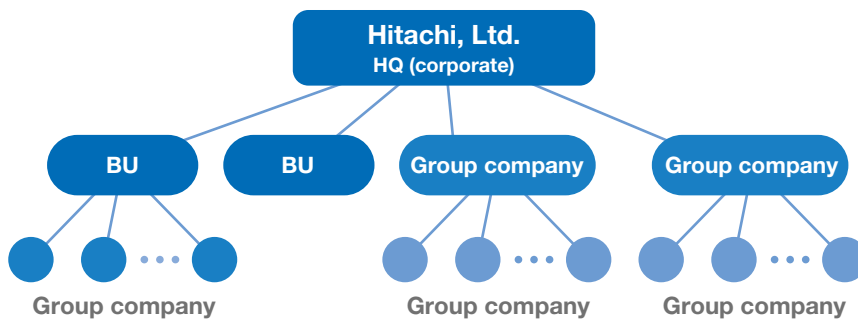
The chief information security officer establishes an information security committee which guides policy regarding information security, personal information protection policies, training plans, and various measures.

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.

An information security promotion division is also established to handle its personal information protection, information security, confidential information management, entry and exit management, and order management processes, and to educate workers. 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.



\*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. Group companies have established similar regulations to promote information security.

Category	Name of regulation
Basic regulations	Information Security Management Rules
	Hitachi Group Information Security Policy
	Information Security Standards
	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

### Basic regulations

The "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 have completely revised our "Information Security Standards" compared to the previous revisions, based on NIST SP800, to strengthen our cybersecurity measures.

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 Act on the Protection of Personal Information.

The "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 Areas" define measures to maintain physical security, such as rules governing building access.

## Information security management cycle

Hitachi has established a framework that subjects information security management including personal information management to the PDCA (Plan-Do-Check-Action) cycle. In the **Plan** stage of the PDCA cycle, Hitachi formulates information security management rules and measures. In the **Do** stage, Hitachi implements those rules and measures. The **Check** stage entails raising awareness of and monitoring of the activity in the Do stage, which leads to the **Action** stage in which ongoing improvements are made. This cycle takes six months from start to finish.





## Educating workers on information security

### Information security education

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 40,000 employees and other workers of Hitachi, Ltd., receive this education 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 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.

Category	Target audience	Description
All staff education	<ul style="list-style-type: none"> <li>• All employees</li> <li>• Temporary employees</li> <li>• Employees on secondment</li> </ul>	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
	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.
	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.

The specialized education related to information systems and information security is described in *Initiatives for Security Human Resource Development*.

### Drill-based education 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.

# Information Security Management

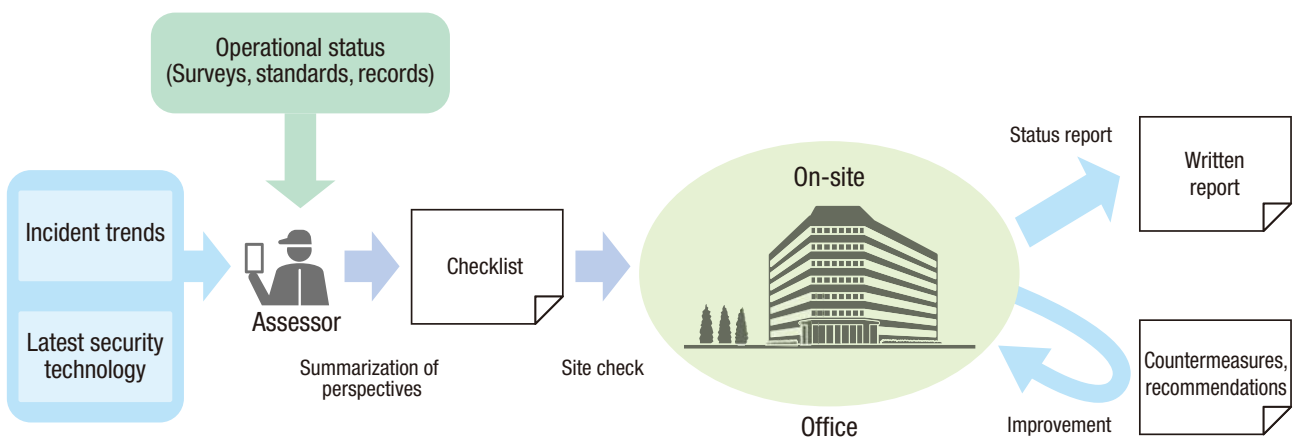
## On-site security risk assessment

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. There is also communication with outside parties via internet connections, removable 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 developments.
- (2) Identify issues that might present a security risk and propose effective countermeasures on site.



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.

With COVID-19 preventing us from performing onsite checks again in FY 2021, we are implementing various alternative means of assessment such as remote checks.

# CSIRT Activity in the Hitachi Group

The Hitachi Incident Response Team (HIRT) is a CSIRT (Cyber Security Incident Readiness/Response Team) that supports Hitachi's activity in relation to 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

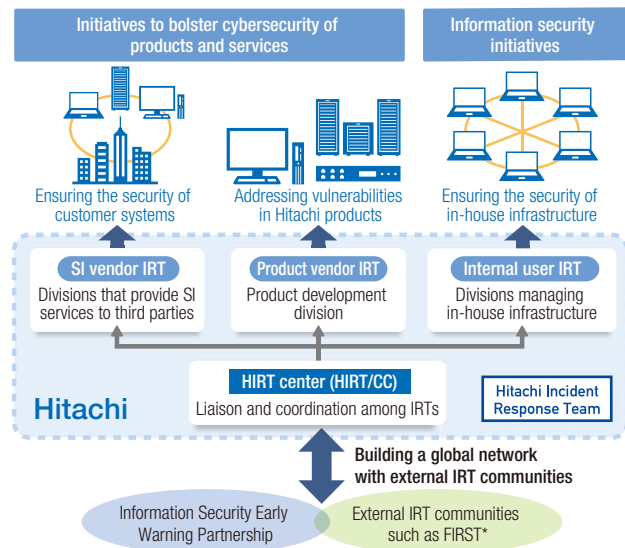
The role of the HIRT is to provide ongoing support for Hitachi's cybersecurity countermeasures through *vulnerability handling*, which eliminates vulnerabilities that threats might exploit, and *incident response* which involves evading and resolving cyberattacks. The team approaches these tasks from 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.



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

# CSIRT Activity in the Hitachi Group

## 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\*<sup>1</sup> 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.

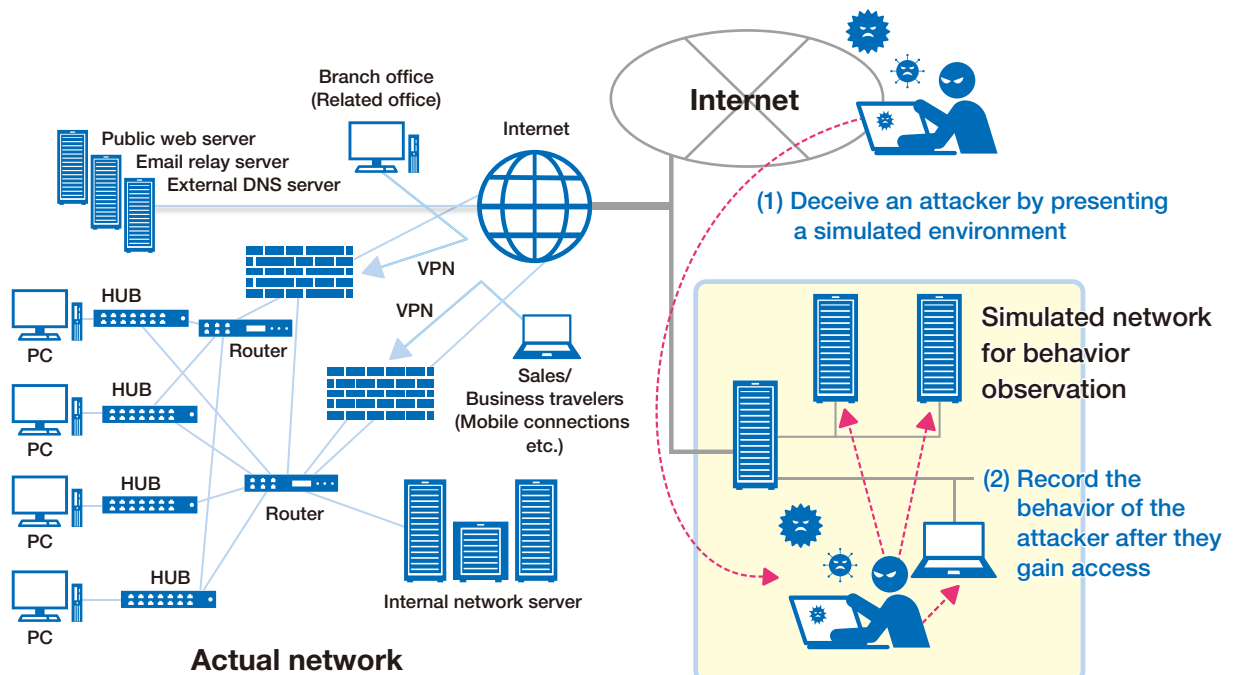
#### (3) Improving security technology for products and services

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.

#### (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 preminent example of such an initiative is HIRT-FIS\*<sup>2</sup> 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\*<sup>3</sup> 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\*<sup>4</sup> and United States Department of Homeland Security's AIS\*<sup>5</sup> 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/>

# 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.

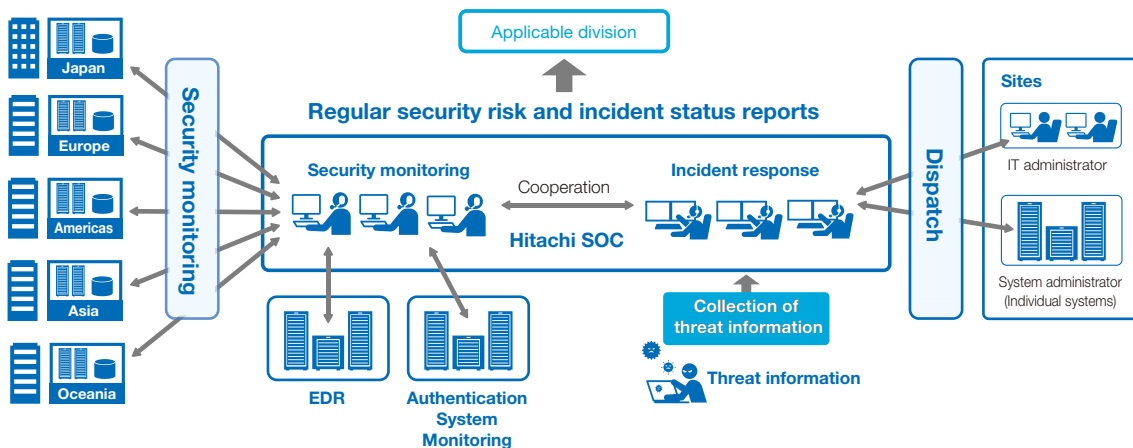
### ● Security monitoring

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.



## 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.

This activity take place in cooperation with Group companies.

### ● 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.

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

Hitachi uses the collected information to assess the likelihood of a successful attack based on the metrics published by the information provider (such as severity and CVSS base score), the prevalence of the vector in in-house systems, and CTI services. Based on the results, Hitachi determines who needs to be notified and assigns one of three vigilance levels. For some threats, we use a simulated environment to perform verifications. This allows us to compile information to assist with our surveys of the impact on in-house systems, countermeasures, and damage, which we use in our countermeasure activities.

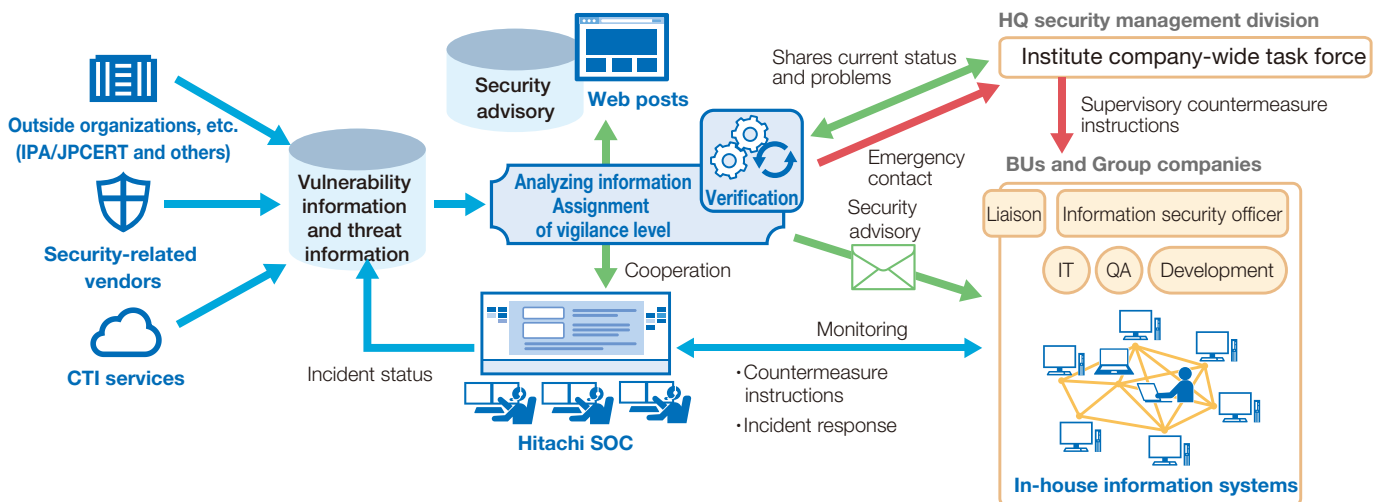
### ● Disseminating vigilance information

The collected information is disseminated according to the vigilance level 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, a security advisory is circulated to urge caution. If the situation requires, a cyber warning is also issued. We also survey public systems, 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 confirm countermeasures and enhance monitoring.

Based on the accumulated results of these activities, we determine the current status of the Hitachi Group and countermeasures that require improvement. We then share this with the HQ (corporate) security management division 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 can institute a task force that controls the response at the company level.



# Global Information Security Initiatives

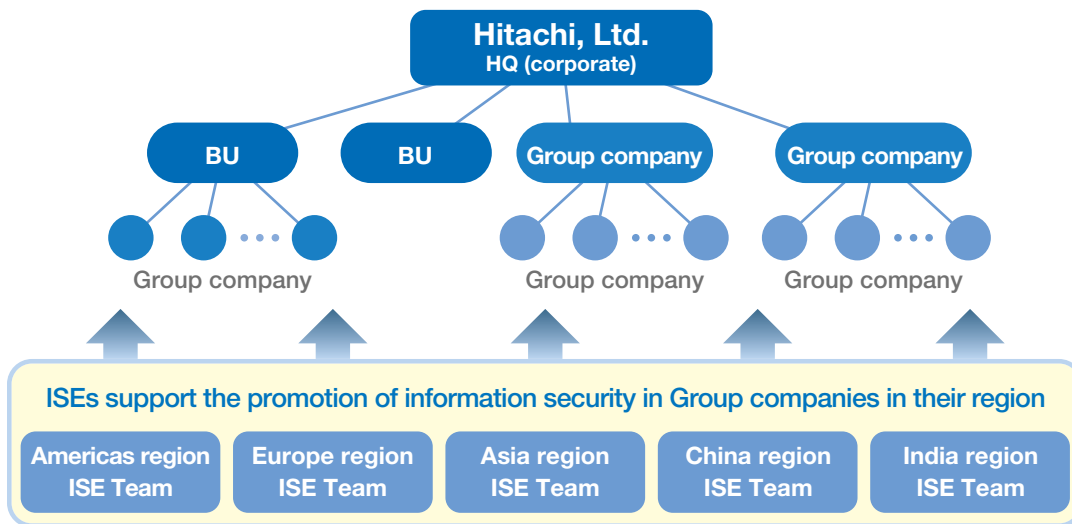
Information security initiatives are essential to the Hitachi Group's presence on the global stage. To ensure reliable implementation of security countermeasures, Hitachi is strengthening its global governance by posting information security experts in various regions to entrench global security governance.

## Global security governance

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.



## Enhancing governance through information security experts

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

To establish regional communities and open lines of communication, ISEs hold cybersecurity workshops and online seminars as an adjunct to traditional lines of governance via parent companies, supporting better governance of local subsidiaries.

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



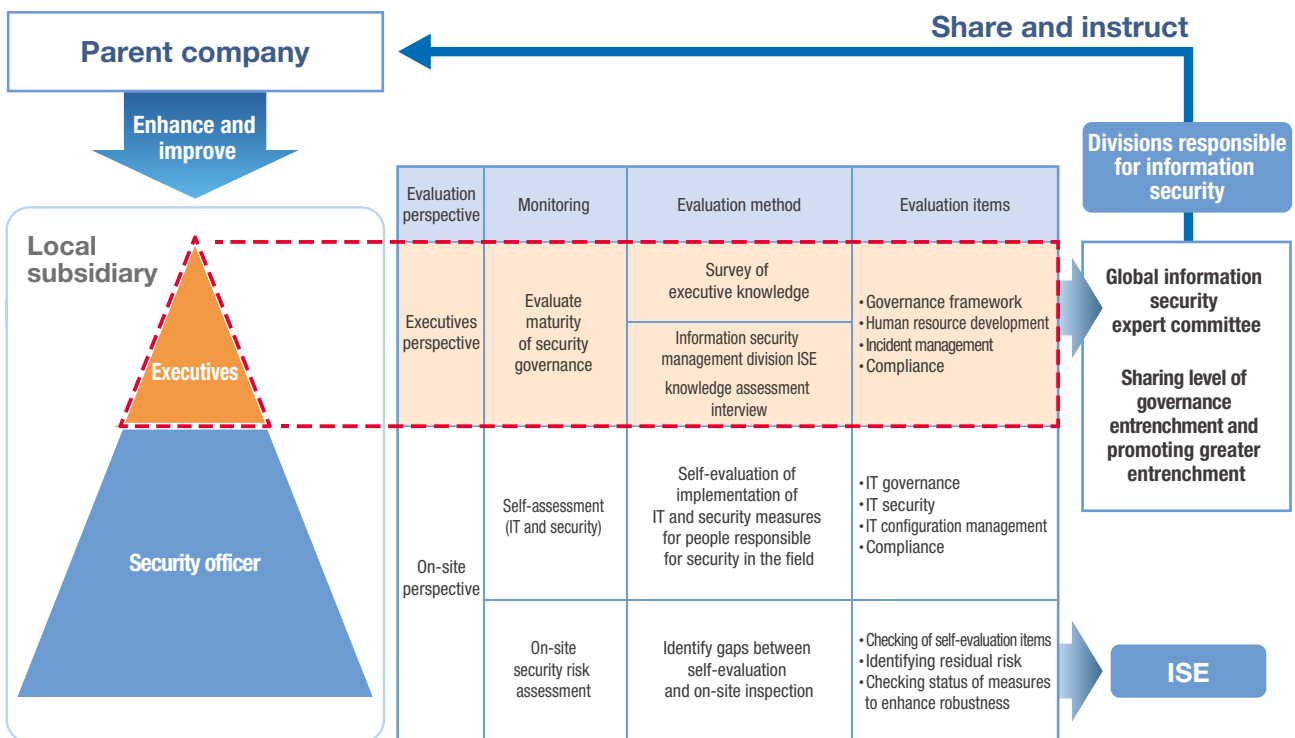
## Assessing management knowledge

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.



## Visualizing survey results and incorporating them into PDCA activity

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

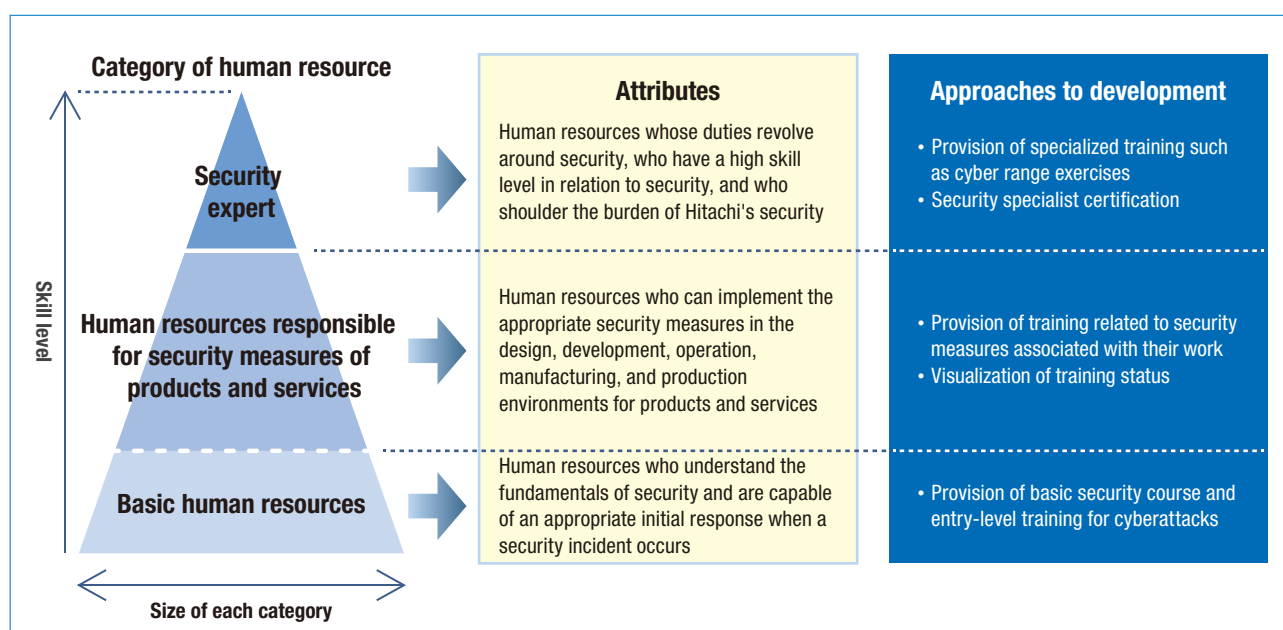
who manage and control security for BUs and Group companies. Here, it finds effective use as context for security activity in the Plan, Do, Check, and Act stages of the PDCA cycle.

# 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.

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.

- 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



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.

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.

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

## Initiatives for Security Human Resource Development

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.

### 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

# Cybersecurity Management Initiatives

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.

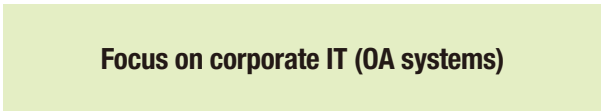
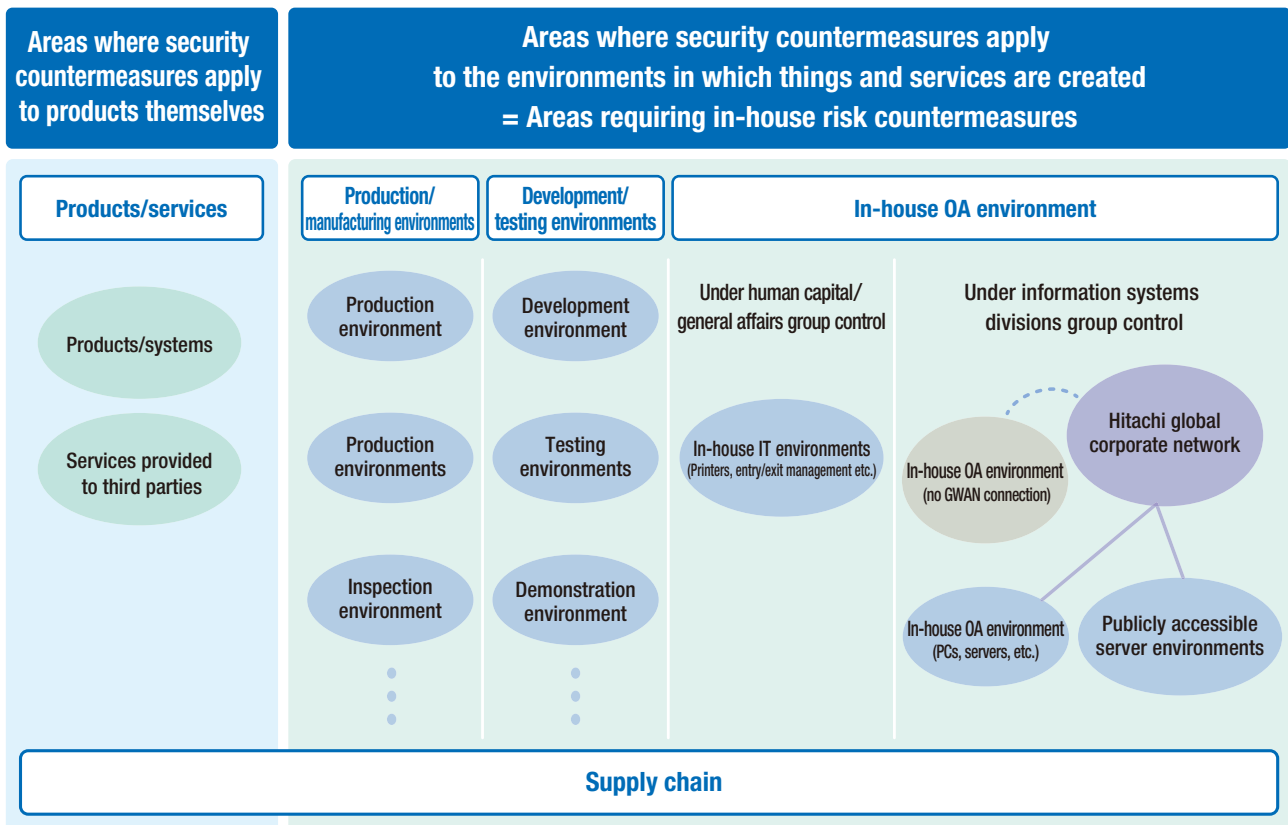
## Context and objectives

In May of 2017, testing equipment at a manufacturing site became infected with the WannaCry ransomware, spreading damage to the entire Hitachi Group.

IT's growing presence in every aspect of business including production, manufacturing, development, and testing means cybersecurity measures must broaden their scope beyond

traditional OA environments to products, services, and procurement.

In this context, since 2018, Hitachi is strengthening cybersecurity measures in the in-house OA, development and testing, and production and manufacturing environments, and in relation to products, services, and supply chain processes.



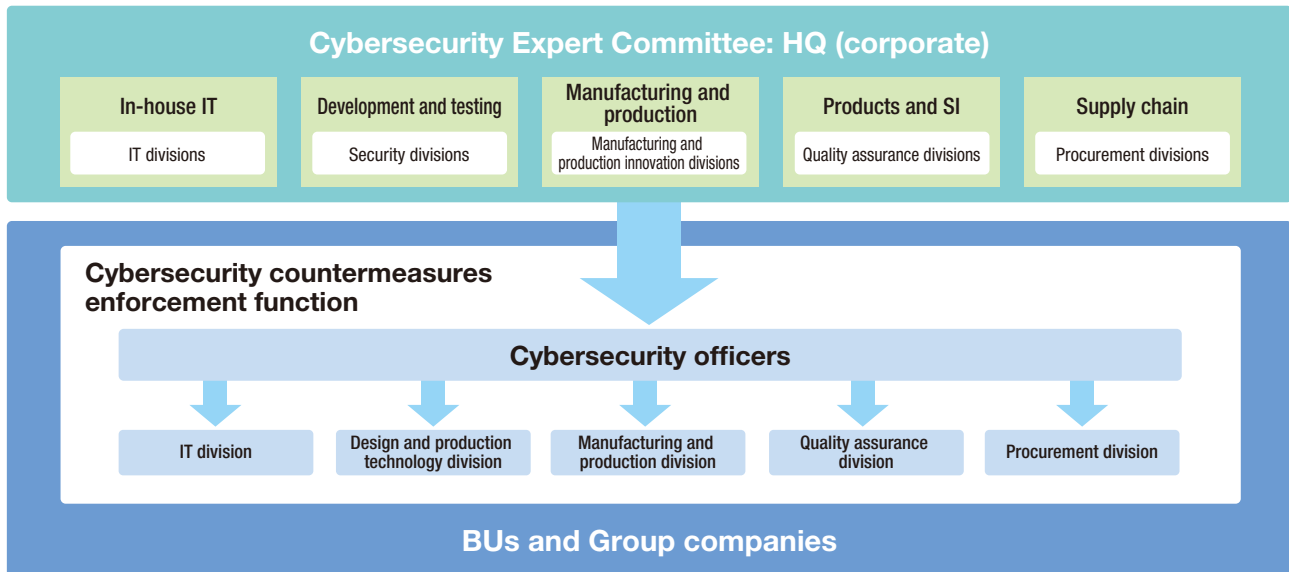
## Promotion framework

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.



## Initiatives to enhance cybersecurity countermeasures

Hitachi promotes the initiatives in the following table to enhance cybersecurity countermeasures in various areas.

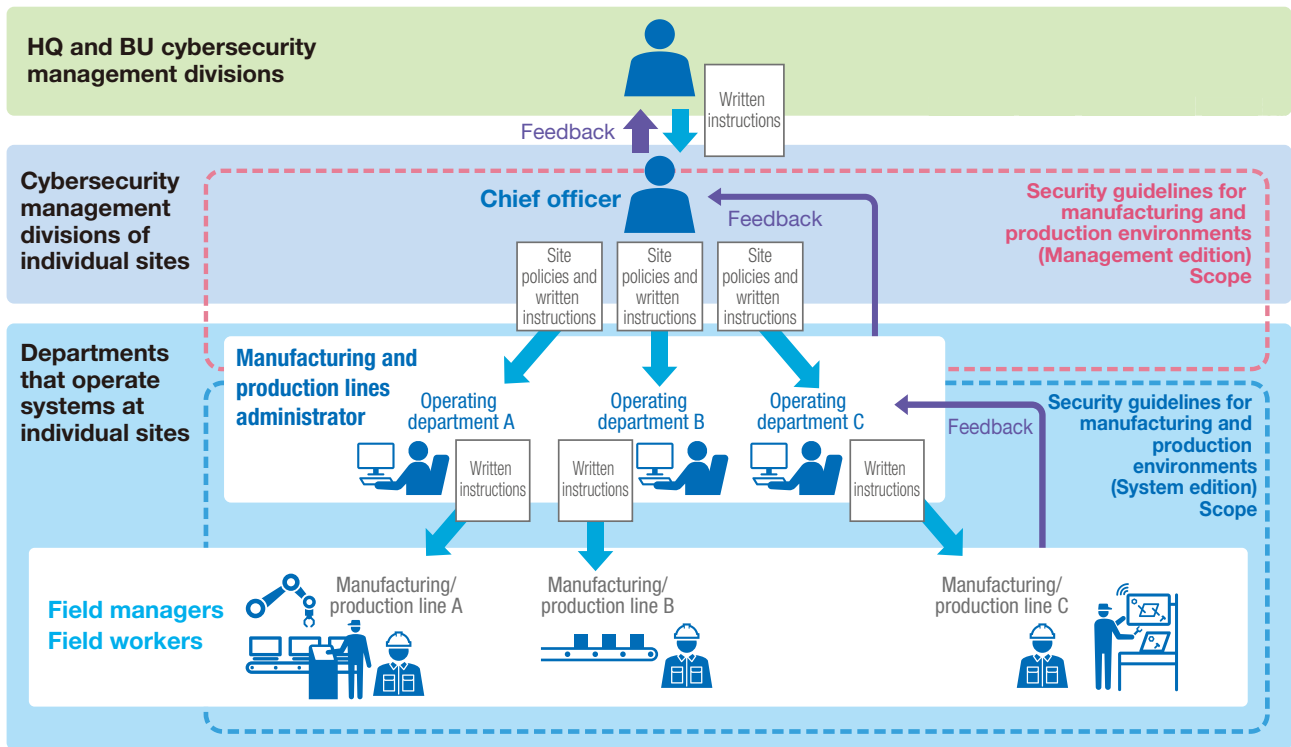
Area		Target divisions	Overview
In-house OA	Environment	IT	•Formulating and disseminating requirements for connection to and isolation from the in-house OA environment
Development and testing		Design and development	•Formulating and disseminating guidelines for creating in-house OA environments and environments 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



# Cybersecurity Management Initiatives

## Initiatives to enhance manufacturing and production security in the field

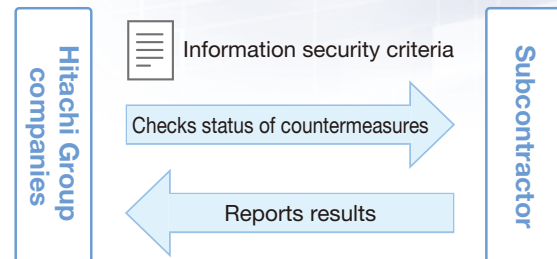
It is important that manufacturing and production environments do not affect other environments, such as in-house OA and development environments, and vice-versa. Hitachi has established guidelines governing the creation and operations management of mutually secure connection environments, and acts according to those guidelines within the Hitachi Group. At actual manufacturing and production sites, posters are displayed and rulebooks and other resources made available to remind field workers of their obligations during their day-to-day work. This leads to greater security awareness in the manufacturing and production sites.



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 reference to a typical model used by the Hitachi Group. The contents of this document are customized by each division and department.	Manufacturing/production line manager
		Field manager
		Field worker

## ● Initiatives to enhance supply chain security

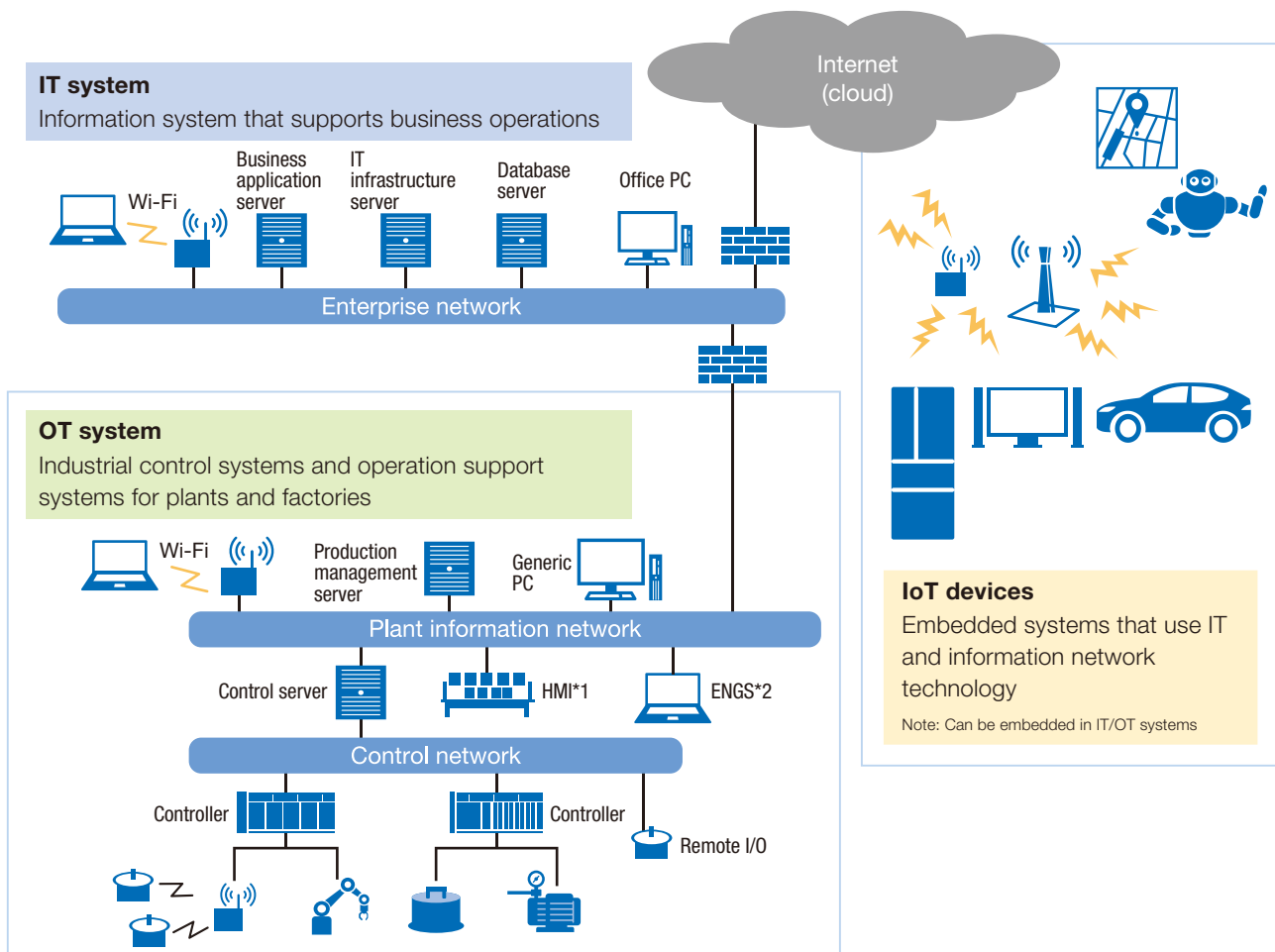
When subcontracting business operations to another party, Hitachi checks and audits the status of the security countermeasures implemented by the subcontractor based on Hitachi's information security criteria. To these information security criteria, Hitachi has added Information Security Guidelines which incorporate security countermeasures against current supply chain attacks. These guidelines make clear Hitachi's requirements regarding information security and form the basis of the checks Hitachi performs.



## 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, Hitachi continues to promote initiatives intended to protect customer assets and social infrastructure from cyberattacks.



\*1 Human Machine Interface \*2 Engineering Station

## Cybersecurity Management Initiatives

### ● 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.

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.

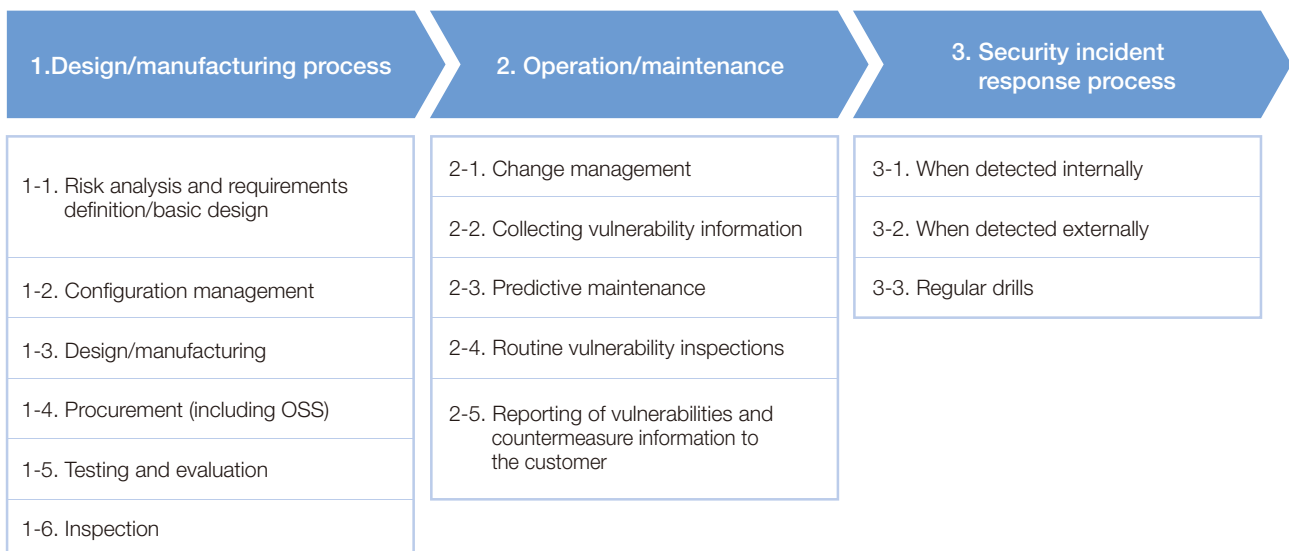
Security management regulations etc.	Overview
Security Management Policy for Products and Services	A policy intended to unify the approach to security management for the products and services (hereinafter <i>products</i> ) of the Hitachi Group.
Requirements for product development and maintenance processes	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.

### ● 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.



### ● 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) Systematic Implementation of Reviews by Security Personnel

We have systematically implemented professional reviews by security personnel at each step of the development and operation process to confirm that products and services can withstand security risks and to ensure security quality. For products and services connected to the Internet, we train each business division, and the security personnel appointed by the head of the business division conducts a review as the representative of the business division. This enables us to develop and deliver secure products and services to our 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.

# Initiatives Related to Personal Information Protection

With the advancement of digital technology causing rapid growth in data usage, personal information protection is a growing concern. More than 130 countries and regions including the EU have enacted laws to protect rights related to personal information.

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

### 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.

Hitachi's vision regarding personal information protection is **1** Providing a safe and trustworthy environment and **2** 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.

## Personal information protection policy

Hitachi, Ltd., has established a personal information protection policy which it makes widely available to stakeholders on its website and by other means.

(<http://www.hitachi.com/privacy-e/index.html>)

### ● Hitachi's approach to personal information protection

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. To reflect how highly it values this information, Hitachi has established an information management framework and endeavored to enforce it.



## Initiatives Related to Personal Information Protection

### ● Personal information protection policy

#### (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

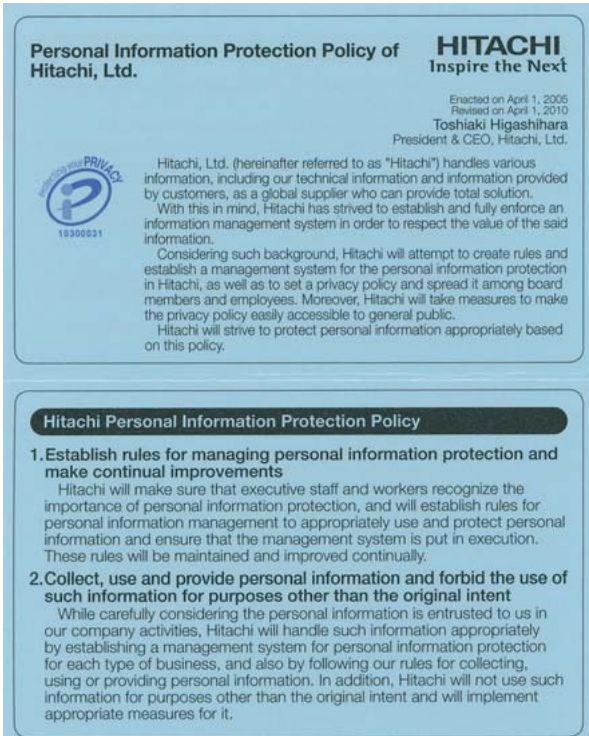
Hitachi complies with applicable laws, national guidelines, and other standards relating to the handling of personal information. Hitachi's own personal information management rules confirm to these laws, guidelines, and standards.

#### (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.

### Personal information protection card


Hitachi, Ltd., gives to each of its employees a personal information protection card that outlines Hitachi's personal information protection policy and basic matters regarding information security.



**Personal Information Protection Policy of Hitachi, Ltd.**

**HITACHI**  
Inspire the Next

Enacted on April 1, 2005  
Revised on April 1, 2010  
Toshiaki Higashihara  
President & CEO, Hitachi, Ltd.

 Hitachi, Ltd. (hereinafter referred to as "Hitachi") handles various information, including our technical information and information provided by customers, as a global supplier who can provide total solution. With this in mind, Hitachi has strived to establish and fully enforce an information management system in order to respect the value of the said information. Considering such background, Hitachi will attempt to create rules and establish a management system for the personal information protection in Hitachi, as well as to set a privacy policy and spread it among board members and employees. Moreover, Hitachi will take measures to make the privacy policy easily accessible to general public. Hitachi will strive to protect personal information appropriately based on this policy.

**Hitachi Personal Information Protection Policy**

**1. Establish rules for managing personal information protection and make continual improvements**  
Hitachi will make sure that executive staff and workers recognize the importance of personal information protection, and will establish rules for personal information management to appropriately use and protect personal information and ensure that the management system is put in execution. These rules will be maintained and improved continually.

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

## Initiatives Related to Personal Information Protection

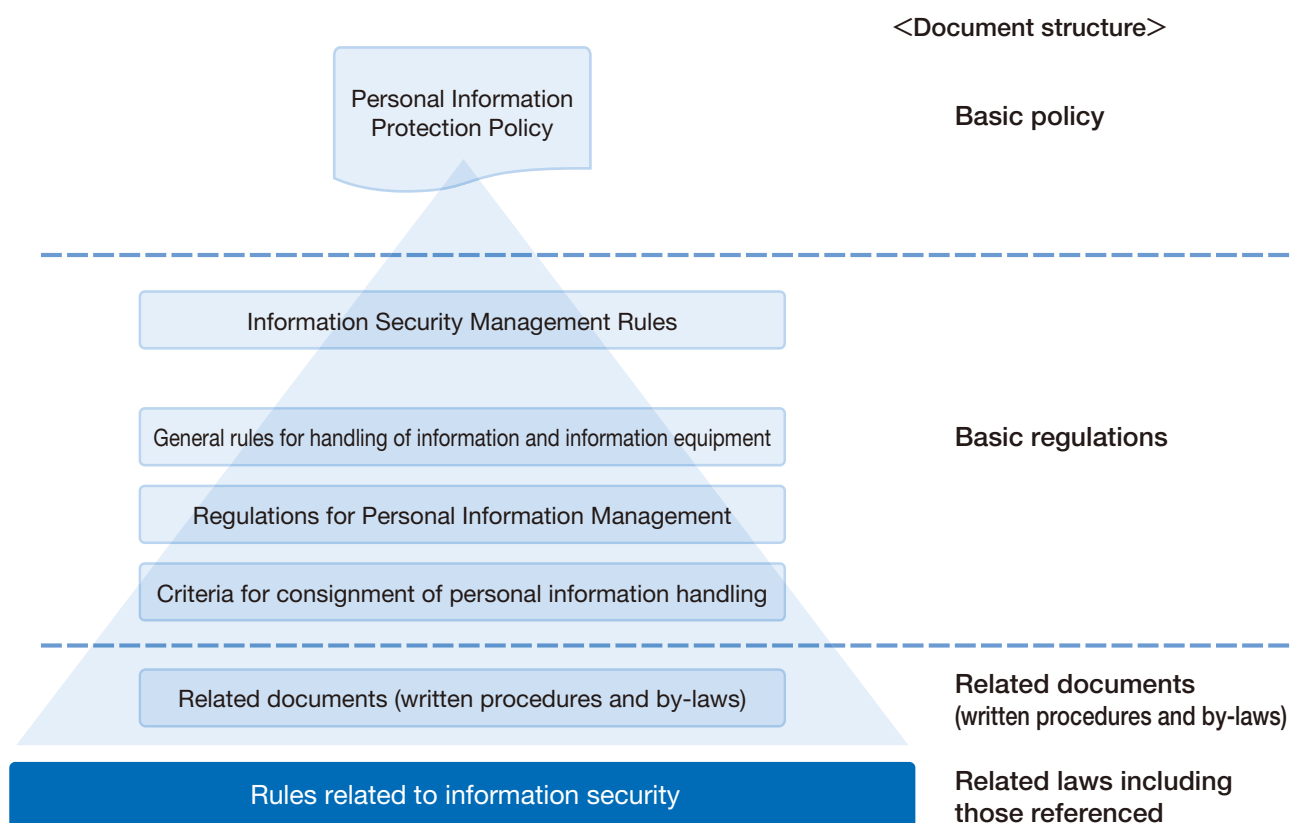
### Personal information protection system

To realize its vision in relation to personal information protection, Hitachi is establishing a company-wide information security framework.

For details, see *Information security promotion framework*.

### System of rules for personal information

Hitachi appropriately manages the personal information it holds according to a set of rules that regulate personal information protection.



### 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 (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.

- Reliably implement personal information protection management system (PMS)
- Conduct regular reviews and ongoing improvements by cycling the PDCA



# Initiatives Related to Personal Information Protection

## 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.

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

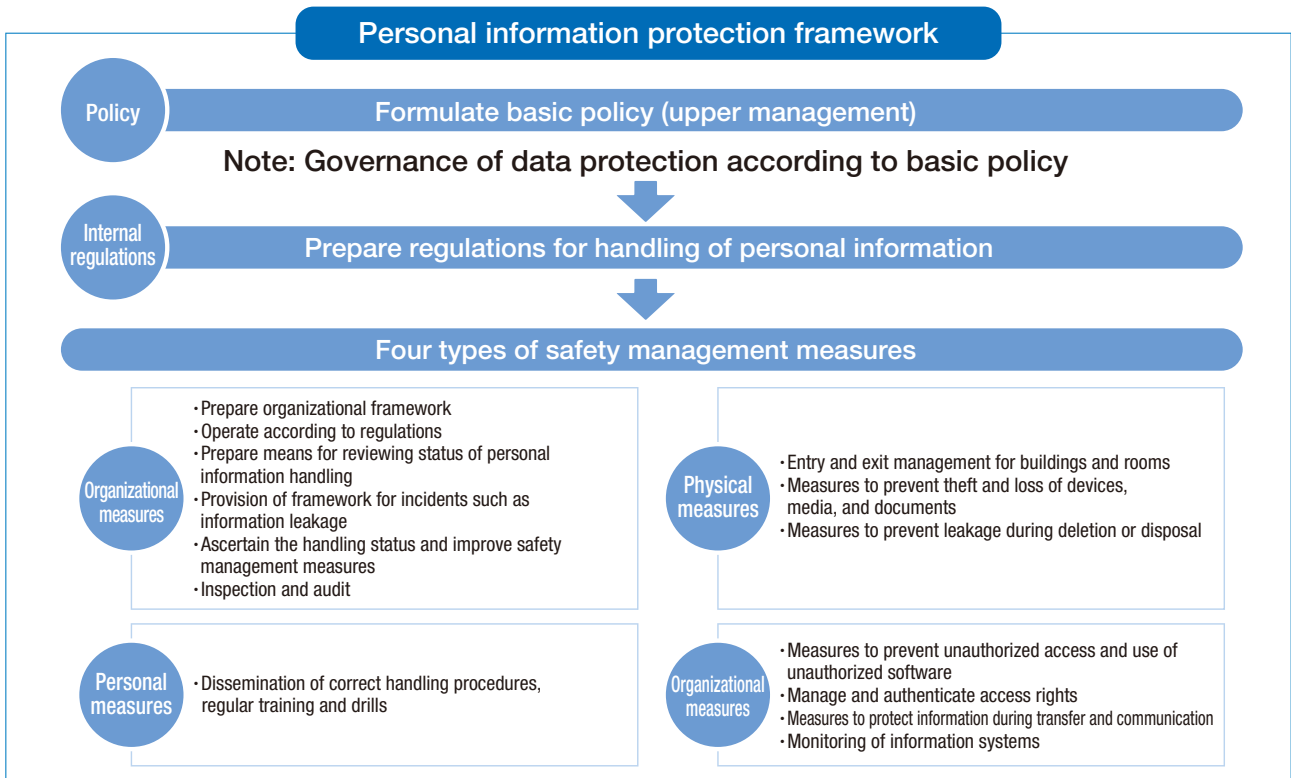
Hitachi defines rules related to the roles and responsibilities of workers in relation to safety management and handling of personal information, and operates according to those rules. Hitachi has also put in place a response framework to follow when an incident such as information leakage occurs, and 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.



### 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.

### Compliance with Japan's My Number system

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 personal information protection

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.

All 153 Japanese Group companies conduct a similar audit to Hitachi, Ltd., and Hitachi, Ltd., reviews the results.

An information security audit reviews compliance with personal information protection and management and assesses conformance to legal requirements.

### Education regarding personal information protection

To ensure that personal information is reliably protected, Hitachi conducts annual training by e-learning of all executives, workers, and temporary employees.

For details, see *Educating workers on information security under Information Security Management*.



## Initiatives Related to Personal Information Protection

### 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.

Hitachi has taken the initiative by promoting compliance with the EU's General Data Protection Regulation (GDPR). Through cooperation among Hitachi Group companies including its European regional headquarters and offices, Hitachi identifies business processes that are subject to the GDPR and evaluates the associated risk. Based on this evaluation, Hitachi takes action such as implementing safety management measures commensurate with the level of risk and offering training to all employees.

Hitachi is also promoting compliance with other data protection laws through cooperation with regional headquarters and other affected entities. To ascertain the risk status in relation to personal information protection within the Hitachi Group and ensure appropriate compliance, Hitachi conducts ongoing monitoring of the compliance status of Group companies and implements the appropriate measures.

To support overseas Group companies in their compliance with personal information protection requirements, Hitachi 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 October 2021, 37 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. Hitachi, Ltd., has also established a *Hitachi Group PrivacyMark Liaison Committee* whose membership is primarily drawn from PrivacyMark holders within the Hitachi Group. This committee regularly convenes information exchange meetings, study sessions, and seminars with visiting experts. There is a growing foundation of information sharing and research on personal information protection building across the Hitachi Group as a whole.



Website for PrivacyMark System of Japan Institute for Promotion of Digital Economy and Community  
(<https://privacymark.org/>)

\* 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)

## Holders of PrivacyMark certification within the Hitachi Group

As of the end of October 2021, the following Hitachi Group companies hold PrivacyMark certification:

Hitachi, Ltd.	Hitachi Information & Telecommunication Engineering, Ltd.
Hitachi, Ltd., Corporate Hospital Group	Hitachi Research Institute
Hitachi Kenpo	Hitachi Solutions, Ltd.
Okinawa Hitachi Network Systems, Ltd.	Hitachi Solutions Create, Ltd.
Kyushu Hitachi Systems, Ltd.	Hitachi Solutions West Japan, Ltd.
Shikoku Hitachi Systems, Ltd.	Hitachi Solutions East Japan, Ltd.
SecureBrain Corporation	Hitachi Document Solutions Co., Ltd.
Hitachi ICT Business Services, Ltd.	Hitachi Hi-System21 Co., Ltd.
Hitachi Urban Support, Ltd.	Hitachi High-Tech Solutions Corporation
Hitachi Academy Co., Ltd.	Hitachi Power Solutions Co., Ltd.
Hitachi Information Engineering, Ltd.	Hitachi Channel Solutions, Corp.
Hitachi SC, Ltd.	Hitachi Building Systems Co., Ltd.
Hitachi KE Systems, Ltd.	Hitachi Foods & Logistics Systems Inc.
Hitachi Consulting Co., Ltd.	Hitachi Insurance Services, Ltd.
Hitachi Industry & Control Solutions, Ltd.	Hitachi Management Partner, Corp.
Hitachi Systems, Ltd.	Hitachi Real Estate Partners, Ltd.
Hitachi Systems Engineering Services, Ltd.	Hokkaido Hitachi Systems, Ltd.
Hitachi Systems Power Services, Ltd.	
Hitachi Systems Field Services, Ltd.	
Hitachi Social Information Services, Ltd.	

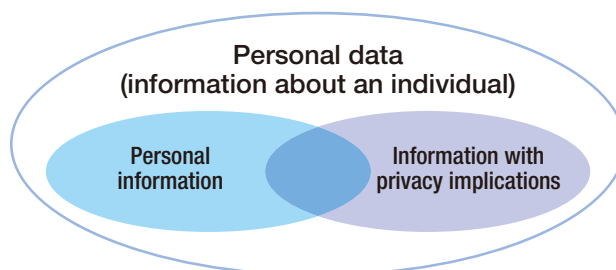
# Privacy Protection Initiatives

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 information that pertains to an individual is collectively called *personal data* regardless of whether it meets the definition of personal information. While businesses are expected to use this data to create value, doing so comes with concerns around 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. The figure to the right illustrates the partial overlap between personal data and information about an individual. For example, information like location data and purchase histories has privacy

implications. To create value using personal data, a business must protect personal information while also protecting privacy.



## 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.

### ● 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 evaluations to many business processes—approx. 220 in FY 2020 alone. In addition, in FY 2020, more businesses started handling personal data for

the purpose of COVID-19 countermeasures, such as detecting body temperature in offices and commercial facilities. We are also taking privacy protection measures for these new types of work.

### ● 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"<sup>\*1</sup>. In the FY 2020 survey, when comparing expectations and anxieties about the utilization of personal data, there was a decrease in the number of people who responded that their concerns were high, and an increase in the percentage of people in the middle group who responded that their levels of expectations and anxieties were "about the same." In addition, the survey revealed trends that are assumed to be caused by recent events in society, such as consumers expectations surrounding measures using personal data to prevent the spread of COVID-19. The diverse range of opinions has brought into sharp relief the need for fine-grained privacy measures, and Hitachi endeavors to account for changes in consumer attitudes

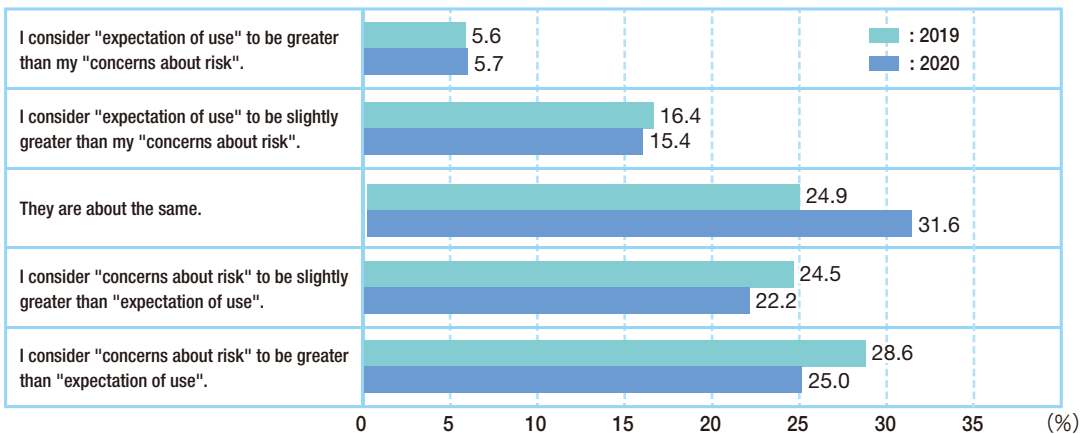
in its approach to privacy protection. The "Corporate Privacy Governance in the DX Era Guidebook ver1.1"<sup>\*2</sup> published by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry also notes the importance of regularly surveying public opinion in these types of surveys to facilitate the evaluation and improvement of measures. Hitachi's efforts were also noted as a case study in the guidebook.

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.

<sup>\*1</sup> "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>

<sup>\*2</sup> "Corporate Privacy Governance in the DX Era Guidebook ver1.1" (published July 2021)  
[https://www.meti.go.jp/policy/it\\_policy/privacy/guidebook1.1.pdf](https://www.meti.go.jp/policy/it_policy/privacy/guidebook1.1.pdf)

**Q** How do you feel about the use of personal data by corporations and public institutions? Do you consider "expectation of use" or "concerns about risk" to be greater?



**Q** What are your expectations regarding use of personal data to help prevent the spread of COVID-19? What are your expectations regarding the following anticipated measures?

■ : Total of "Expect good results" and "Expect somewhat good results"



# Research and Development for Achieving Information Security

The environment surrounding society and companies is undergoing major changes, including the recent emergence of sophisticated and ingenious cyberattacks, and the spread of cloud-based IT systems. At Hitachi, we are working on a variety of technological developments that will contribute to the new form of security which these changes are bringing about. In particular, we are actively promoting the development of contactless and secure biometric technologies that are attracting attention as we switch to and become accustomed to "new normal" workstyles and lifestyles in the wake of the COVID-19 pandemic that began in FY 2020.

## Promoting the development of information security technology to help deal with the COVID-19 pandemic

The COVID-19 pandemic is forcing us to switch to and become accustomed to "new normal" workstyles and lifestyles. Contactless and secure biometric technologies are attracting attention as society shifts to cashless payments, cardless building entry/exit systems, remote working, and business without personal seals. However, concern about the leakage or misuse of the biological information used in such systems was hampering market penetration.

In response, Hitachi has advanced the research, development, and commercialization of Public Biometric Infrastructure (PBI) that provides a secure and convenient common authentication

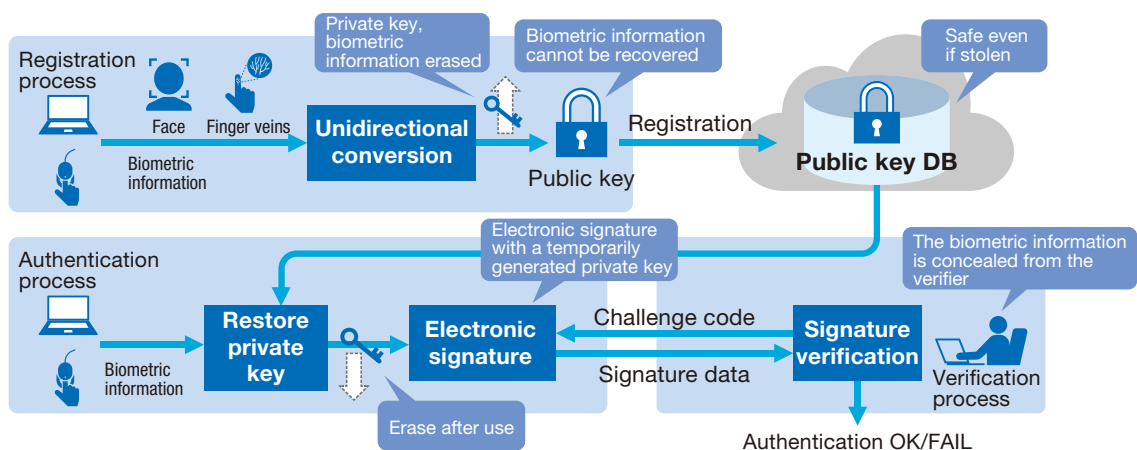
platform on an open network, and in October 2020, Hitachi began providing "integrated biometric infrastructure services." The R&D Group is developing biometric technology that meets the needs of various fields such as finance, healthcare, offices, and retail in the COVID-19 era, including contactless finger vein authentication equipment, general-purpose camera finger vein PBI authentication technology, and face PBI authentication technology that provides secure and convenient access to internal and external systems through biometrics using a PC's internal camera.

### Public Biometric Infrastructure (PBI) Technology

Public Biometric Infrastructure (PBI) is a system that converts and registers biological information such as veins and faces used for biometric authentication into a public key that cannot be restored to the original data. It can be used to authenticate individuals with an electronic signature based on the biometric information. Electronic signatures are based on Public Key Infrastructure (PKI\*), which is a system to guarantee that the public key matches its owner. PKI authenticates individuals by

verifying the electronic signature stored in the private key held by the client against the corresponding public key.

PBI minimizes the risk of information leakage by replacing this private key with biometric information for temporary use by the client at the time of authentication. With this technology, the biometric information used by various devices can be safely utilized in open networks, allowing a wide variety of authentication services to be deployed.



Public Biometric Infrastructure (PBI) Overview

\*Abbreviation for Public Key Infrastructure. A technology for secure operation of public key cryptography and digital signatures using Internet communications.



## Research and Development for Achieving Information Security

### ● Contactless Finger Vein Authentication Technology

We have developed the authentication device C-1 that allows users to be authenticated with just their finger, eliminating the need to carry a physical card or other authentication key. Conventional finger vein authentication devices required the user to place their finger on the device and keep it still to obtain a stable vein pattern. In response to this problem, we have developed a new two-wavelength simultaneous irradiation system that uses infrared and visible reflected light. The system improves authentication accuracy by reliably detecting the user's fingers without the need for contact and using the biological

features of the user's three fingers that are simultaneously photographed. Furthermore, since the system rapidly searches for candidate users using compressed biometric characteristics at the time of authentication, it can perform PBI authentication on millions of users without the need for physical cards or other authentication keys. This makes it possible to handle contactless authentication of a large number of users, and the system can be applied to many B-to-B-to-C situations such as card-free cashless payments.

### ● General-purpose Camera PBI Authentication Technology

We have developed a general-purpose camera PBI authentication technology that uses the built-in camera on a PC as a contactless, low-cost biometric method. It can be used with peace-of-mind since the finger vein or face information used for authentication is converted to an unrecoverable form.

#### (1) General-purpose camera finger vein PBI

We have developed a finger vein PBI authentication technology that allows you to authenticate yourself by simply holding your finger up to your PC's internal camera or an external camera. The challenge in performing finger vein authentication using a general-purpose camera is to reliably extract only the vein pattern from the image of visible light, and to accurately detect and authenticate the position of multiple fingers. For the former, we developed a technique for extracting the vein pattern using color information, and for the latter, we developed a technique for detecting finger regions against any background using deep learning. To perfect the system, we also developed a technology to speed up PBI verification while maintaining finger vein protection safety. This makes it possible to securely authenticate a user in an environment suitable for PCs and business systems. The technology can be applied in a wide range of situations, from Windows sign-ins to single sign-ons on business systems, to electronic signatures.

#### (2) General-purpose camera face PBI

We have developed a face PBI authentication technology that allows you to authenticate yourself by simply positioning your face in front of your PC's internal camera or an external camera. We developed this facial authentication PBI authentication technology by fusing the biometric security knowledge we accumulated by developing finger vein PBI with the latest facial authentication technology based on deep learning. In addition, we identified and improved issues such as compatibility with various races, registration image judgment, and high-speed calculation, and launched the product in September 2020. In July 2021, we launched "Biometric Signature Sign-in Software," which provides secure and easy access to internal and external systems using a PC. Even when you're working away from the office, such as at home, at a satellite office, or at a coworking space, this system delivers high security using biometrics at low cost.



Hitachi finger vein authentication device C-1



Hitachi Camera Biometrics SDK for Windows Front Camera



Contactless finger vein authentication device and biometrics software development kit for PC cameras to support "new normal" living and workstyles

# External Activity Related to Information Security

Hitachi is helping to achieve a more secure IT society by using the experience and knowledge of its employees and participating in various external activities related to information security.

## 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 a global community of incident response teams bound by mutual trust. FIRST counts universities, research institutions, corporations, and government agencies among its members. As of the end of October 2021, membership consists of 598 teams from 98 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.

# 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

September 2021). 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. (Services & Platforms Business Unit, Control System Platform Division)
- Hitachi, Ltd. (Service & Platform Business Unit Service Platform Division, Lumada CoE, Software CoE)
- 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, Solutions Business Development Department, Digital Solutions Development Group, Water & Environment Business Unit, Environment Solutions Division, Information System Engineering Department, Industry Business Division, Information Technology & Business Process Innovation Division, Secure IT Innovation Center, IT Prevention 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)
- Kyushu Hitachi Systems, Ltd.
- Shikoku Hitachi Systems, Ltd.
- Japan Space Imaging Corporation
- Hitachi ICT Business Services, Ltd. (Product Support Department Media Service Group)
- Hitachi Pharma Information Solutions
- Hitachi Information Engineering, Ltd.
- Hitachi SC, Ltd. (HQ)
- Hitachi KE Systems, Ltd. (Tokyo Development Center)
- 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. (Managed Services Division, Cloud Services Division, Business Services Division)
- Hitachi Systems Power Services, Ltd. (Managed Services Division, Platform Services Office)
- Hitachi Systems Field Services, Ltd. (Branch HQ, Tokyo Branch, Tokyo Office)
- Hitachi Social Information Services, Ltd. and Okinawa Hitachi Network Systems, Ltd.
- Hitachi Information & Telecommunication Engineering, Ltd. (Customer Support Center)
- Hitachi Solutions, Ltd.
- Hitachi Solutions Create, Ltd.
- Hitachi Solutions West Japan, Ltd. (Cloud Platform Operating Support Department)
- Hitachi Solutions East Japan, Ltd.
- Hitachi Channel Solutions, Corp.
- Hitachi High-Tech Solutions Corporation (Solution Center)
- Hitachi Power Solutions Co., Ltd.
- Hitachi Foods & Logistics Systems Inc.
- Hokkaido Hitachi Systems, Ltd. (Public and Social Services Division, Corporate Services Division, Business Planning Department, System Division, System Part 1, The first group, Second group, System Part 2, Platform Business 1st Division, Facility Business Promotion Department, Facility Service Group, Platform Business Second Division, Corporate Sales & Marketing Group, Power Sales Planning Division, Public and social Sales division, Business First part, Sales First Group, Sales Section 2, Corporate Sales Division, Business First part, Sales First Group, Sales Section 2, Production Technology Management Division, Corporate Quality Assurance Division)
- Hitachi Management Partner Corp.

### 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

November 2021 [Includes products in the certified products archive list])

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 November 2021 [Includes products in the CMVP "historical list"])

Product	Certification No.	Level
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 and Windows editions)	JCMVP #J0007	Level 1
Keymate/Crypto JCMVP Library	JCMVP #J0005	Level 1



# Overview of the Hitachi Group

## Company Profile (As of March 31, 2021)

Corporate name	Hitachi, Ltd.
Incorporated	February 1, 1920 (founded in 1910)
Head office	1-6-6 Marunouchi, Chiyoda-ku, Tokyo, Japan
Representative	Keiji Kojima, President and COO
Capital	460.79 billion yen

Number of employees	350,864 (Japan: 158,194, outside Japan: 192,670)
Number of consolidated subsidiaries (including variable interest entities)	871 (Japan: 159, outside Japan: 712)
Number of equity-method associates and joint ventures	345

\*1 As of June 23, 2021

## Consolidated Financial Highlights for Fiscal 2020, Based on the International Financial Reporting Standards (IFRS)

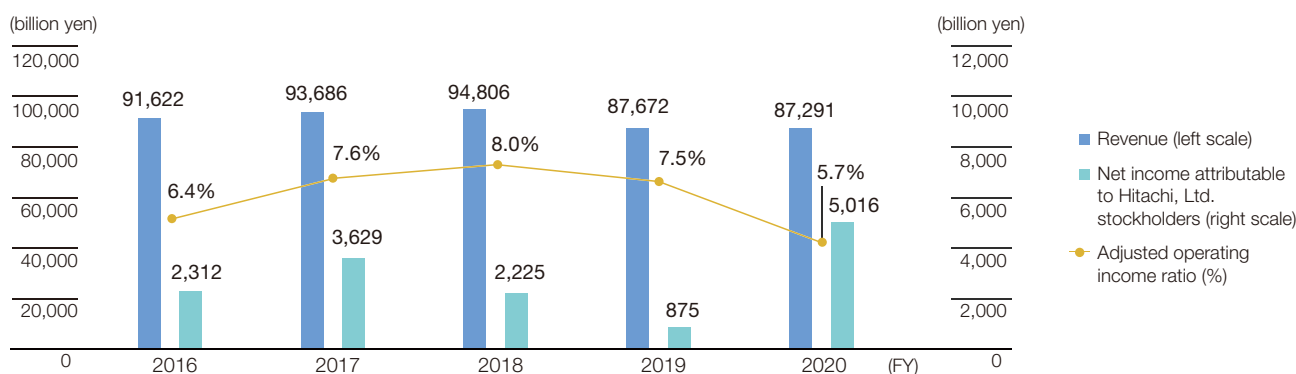
Revenue	8,729.1 billion yen (100% year on year)	Net income attributable to Hitachi, Ltd. stockholders	501.6 billion yen (up 414.0 billion yen, year on year)
Adjusted operating income	5.7% (down 1.8 percentage points, year on year)	ROIC* <sup>3</sup>	6.4% (up 3.0 percentage points year on year)
EBIT* <sup>2</sup>	850.2 billion yen (up 666.6 billion yen, 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.

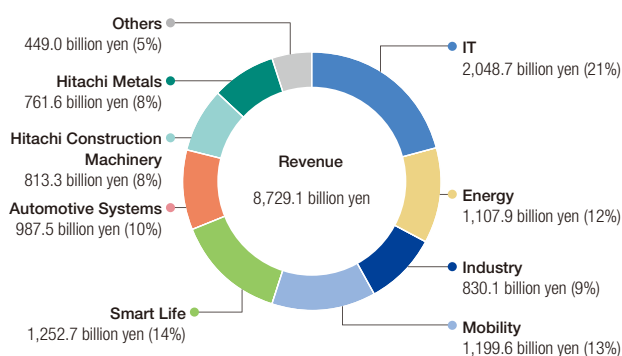
Note: Hitachi's consolidated financial statement is prepared based on the International Financial Reporting Standards (IFRS).

## Revenue, Adjusted Operating Income Ratio, and Net Income



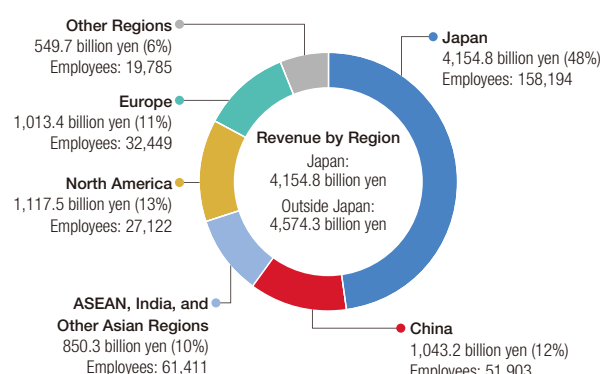
## Revenue and Share by Segment

(Consolidated for FY 2020, based on IFRS)



## Revenue and Share by Region

(Consolidated for FY 2020, based on IFRS)



Note: Revenue by segment includes intersegment transactions.



**Information Security Risk Management Division**

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

Tel: 03-3258-1111