HITACHI
Inspire the Next

Information Security Report 2017

Hitachi Group

Greetings

Hitachi Group is engaged in the social innovation business which creates new value through collaborative creation with customers and partners by combining OT (Operational Technology, such as the control and operation technologies which we have been developing for many years) with advanced IT and product systems.

In the future, we want to contribute to the realization of a society in which people can live safely, securely, and comfortably. By further taking advantage of digital technologies to evolve solutions, we aim to become the innovation partner in the IoT (Internet of Things) era.

The environment surrounding information security has been changing drastically in recent years.

A society of internet users and the rapid development of information technology have brought new technologies and higher level of services: such as cloud computing, smart devices, social networking services, and artificial intelligence. This means there is increased risk and complexity associated with information security.

Especially, in addition to information being acquired by unauthorized access, cyber attacks (including targeted e-mail attacks, which have increased recently) are become increasingly sophisticated, causing problems such as damage to important facilities. This is leading to serious impacts on our society.

In May 2017, some internal systems within the Hitachi group, including email systems, were damaged by a worm-type ransomware, which inflicted damage in over 150 countries.

On the other hand, we recognize that, as a corporation that handles corporate customer information as well as personal information of members of the public through the IoT and Big Data, it has become necessary for us to operate with an awareness of human rights, including protection of privacy.

In these circumstances, we have been promoting our information security management cycle globally, and have been enhancing our information security, by methods such as implementing regulations and frameworks, implementing security measures that utilize information technology and other tools, educating general staff members and security specialists alike, and conducting inspections by auditors, under our “Information Security Policy”.

At Hitachi Group, in order to build more robust cyber security from lessons learned from the damage caused by the infection this time, as well as to participate proactively in initiatives conducted jointly by government and citizens, we continue to develop and construct countermeasures to deal with these sorts of threats. We have done this in cooperation primarily with the Hitachi Incident Response Team but also across all business divisions, drawing fully on Hitachi's business knowledge and the latest technology.

By sharing outcomes established here with customers, we aim to bring about an even safer and more secure society.

I would be delighted if our information security activities, introduced in this report, are able to be of use to society, and are able to further increase the trust felt towards the Hitachi Group.

Shinichiro Omori

Senior Vice President and Executive
Officer, CIO Hitachi, Ltd.

Information Security Report

INDEX

Hitachi Group information security initiatives

Product and service information security assurance initiatives

〈Overview of this report〉

●Report scope and period: Hitachi Group information security initiatives until the 2016 fiscal year.

●Date published: August 2017

Basic approach to information security governance

Policy on information security governance initiatives

Hitachi regards initiatives for information security as vital for the safe management of information assets stored for customers in business operations that provide safe and secure social infrastructure systems. We have established information security initiatives policies shared by the Group, and are promoting enhanced information security activities.

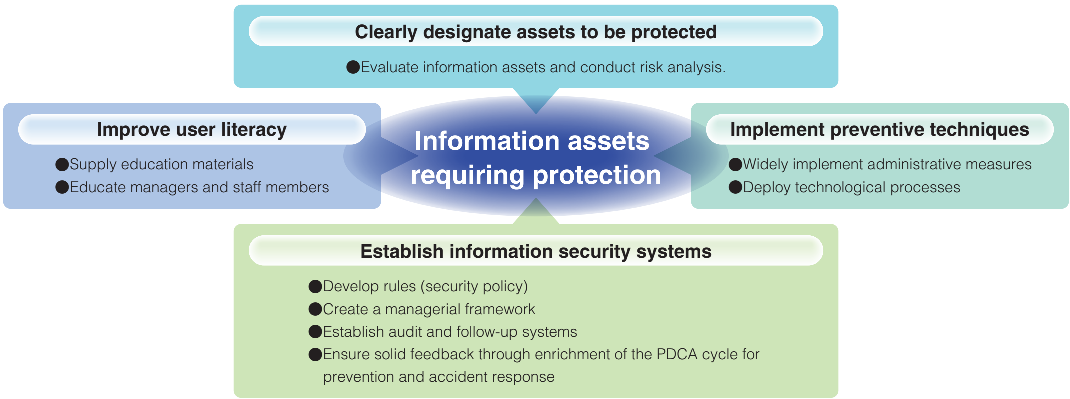
Approach to information security initiatives

Our approach to initiatives in information security encompasses four perspectives: ① Establishment of information security systems; ② Clearly designate of assets to be protected; ③ Improving user literacy, and; ④ Establishment of different types of security measures. We are making steady progress on action items for each of these perspectives.

Of these items we are paying particular attention to precautionary measures and prompt accident response, as well as improving staff ethical and security consciousness.

Furthermore, information security management PDCA (continuous improvement of activities) is moving forwards through the leadership of Hitachi, and we are working hard to improve security levels of the Group overall.

Basic approach to information asset protection >>



Clearly designate assets to be protected

●Evaluate information assets and conduct risk analysis.

Improve user literacy

●Supply education materials
●Educate managers and staff members

Information assets requiring protection

Implement preventive techniques

●Widely implement administrative measures
●Deploy technological processes

Establish information security systems

●Develop rules (security policy)
●Create a managerial framework
●Establish audit and follow-up systems
●Ensure solid feedback through enrichment of the PDCA cycle for prevention and accident response

(1) Precautionary measures and prompt security response

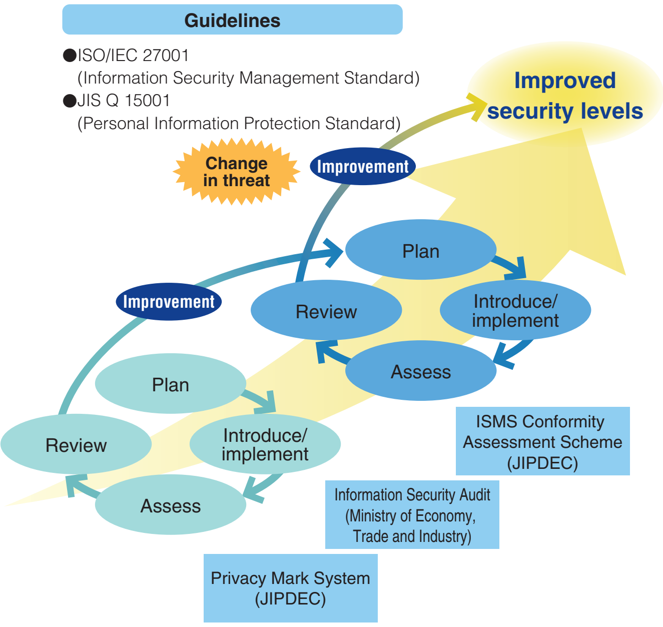
We clarify assets to be secured and have implemented safeguarding measures based on vulnerability and risk analyses.

We also have an emergency manual which we use for security breaches, based on the assumption that accidents do happen.

(2) Improving ethical and security awareness among staff members

We have prepared a program tailored to Hitachi' s various personnel levels including management and supervisors, and are working to improve ethics and security awareness through Group-wide e-learning. We are also conducting audits to identify and address problems at an early stage.

The PDCA cycle for security level improvement >>



Guidelines

●ISO/IEC 27001
(Information Security Management Standard)
●JIS Q 15001
(Personal Information Protection Standard)

Improved security levels
Change in threat
Improvement
Plan
Review
Introduce/ implement
Assess
Improvement
Plan
Review
Introduce/ implement
Assess
ISMS Conformity Assessment Scheme (JIPDEC)
Information Security Audit (Ministry of Economy, Trade and Industry)
Privacy Mark System (JIPDEC)

Information Security Management System

Information security promotion and management cycles

Introducing Hitachi policies regarding information security, structures for promoting information security, regulations regarding information security, and information security management cycle.

Information security policies

As a global company representing Japan, Hitachi recognizes cyber security risks as one type of management risk. In order for us to announce (to those inside and outside the organization) a policy for the entire organization, we are making our utmost efforts to ensure information security by establishing information security policies and related guidelines, such that they take into account cyber security risk management and are in accordance with the enterprise management policy.

Based on this policy, we are expanding information security measures that support every aspect of business activities: such as enhancing cyber security, preventing information leakage caused by human errors, and protecting personal information such as social security and national ID numbers.

Information security policies >>

1. Formulation and continuous improvement to information security management regulations
We recognize information security initiatives as a major issue in management as well as business activities, and establish information security management regulations that comply and adapt to laws and other standards.
Furthermore, we establish information security management systems for the whole company that center on our executive officers, which we implement faithfully.
In addition, we maintain and continuously improve information security in terms of organization, human resources, physical systems, and technology.

2. Protection and continuous management of information assets
We plan safe management systems in order to appropriately protect information assets we handle from threats to confidentiality, integrity, and availability.
We also take appropriate control measures for business continuity.

3. Strict observance of laws and standards
We strictly observe laws and other standards regarding information security.
We also make our information security regulations conform with such laws and other standards.
If these are found to be violated, we check staff working regulations and take the appropriate action.

4. Education and training
We conduct education and training in order to increase executive officer and staff member awareness of information security.

5. Incident prevention and management
We strive to prevent information security accidents from occurring, and in the case that an accident occurs, promptly take the appropriate measures, including measures to ensure the accident does not happen again.

6. Assurance of fair business practices within the corporate group
We will construct a system to ensure fair business practices in the corporate group made up of Hitachi, Ltd. and Hitachi, Ltd., Group Companies, according to policies 1 to 5 listed above.

Information security promotion

The President will appoint the Chief Information Security Officer with rights and responsibilities towards information security, and the Information Security Chief Auditor with rights and responsibilities towards information security auditing.

The Chief Information Security Officer will set up the Information Security Committee, and determine policies, educational programs, and different measures regarding information security.

Decisions made by the Information Security Committee will be implemented at each business site through the Information Security Promotion Council attended by working-level employees from all business sites.

The person who responsible for each business site will be appointed to the Information Security Officer.

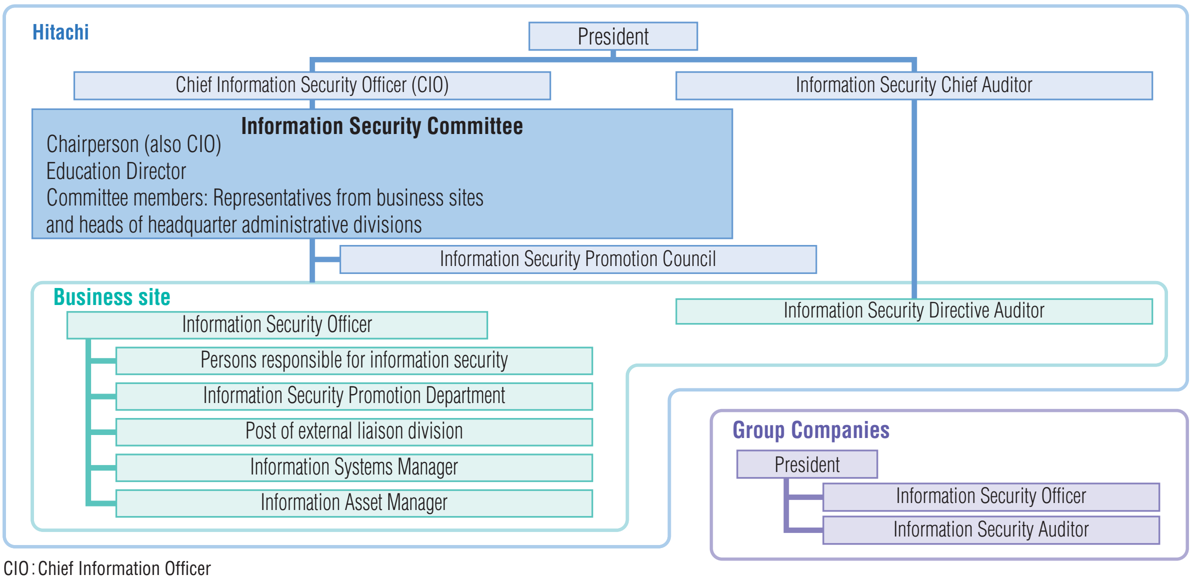
An Information Security Promotion Division will also be established, which will deal with personal information protection, information security, management of confidential information, entrance/exit management, and vendor management across all business sites in an integrated manner, as well as implement educational activities to promote a thorough awareness of information management amongst staff members at business sites.

An Information Asset Manager will be placed in all divisions, and responsibilities will be allocated regarding handling of information assets.

A similar organization will be established in Group Companies, and there will be mutual cooperation to promote information security across divisions.

Information Security Management System

Information security promotion >>


Hitachi

President

Chief Information Security Officer (CIO)

Information Security Chief Auditor

Information Security Committee

Chairperson (also CIO)
Education Director
Committee members: Representatives from business sites and heads of headquarter administrative divisions

Information Security Promotion Council

Business site

Information Security Officer

Persons responsible for information security

Information Security Promotion Department

Post of external liaison division

Information Systems Manager

Information Asset Manager

Information Security Directive Auditor

Group Companies

President

Information Security Officer

Information Security Auditor

CIO : Chief Information Officer

Information security regulations

As displayed in the table below, we have established regulations based on information security policies.

Group companies have also established equivalent levels of regulations, and are promoting information security.

Information security regulations >>

Category	Regulation name	Details
Basic regulations	General Rules for Information Security Management Systems	We have established basic conditions relating to the formulation, implementation, maintenance, and continuous improvement of the Information Security Management System, based on the “HITACHI Company Conduct Standards” , and aim to ensure the confidentiality, integrity, and availability of Hitachi’ s information assets including personal information, protecting this information.
	Information and Information Equipment Handling General Provisions	We have established basic conditions relating to handling and management of information and information equipment, and aim to promote the safe use of information, as well as prevent leaks of information overall by mediums such as paper and in information or other systems, and accidents caused by the misappropriation of information, by strict observance of regulations.
	Management Regulations for Confidential Information	We have established provisions necessary for the handling of confidential information based on the “HITACHI Company Conduct Standards” , and aim to maintain confidentiality.
Individual regulations	Rules on Website Creation and Information Disclosure	We have established provisions requiring strict adherence so that information is disclosed and used correctly, and aim to provide an environment in which customers and staff members can use information effectively and with ease of mind.
	Systems Management Regulations for Information Security	We have established basic management provisions regarding information systems based on the “General Rules for Information Security Management Systems” , aiming to ensure information security.
	Management Regulations for Entrance/Exit and Access Restriction Zones	We have established necessary provisions regarding the principals of entrance/exit management and premises access restrictions, as well as the designation of prohibited areas and their management and operation, and aim to protect confidential information.
Management of personal information	Management Regulations for Personal Information	We have established provisions to be strictly adhered to regarding the appropriate protection of personal information in accordance with laws and guidelines stipulated by the national government regarding the handling of personal information, and aim to protect the rights and interests of the individual, as well as prevent business losses and loss of social credibility. We have established the provisions, procedures etc. necessary to fulfil our responsibilities regarding operation/management systems creation, management regulation implementation and strict adherence, and personal information protection.
	Consignment Criteria for Business Handling Personal Information	We have established specific procedures for situations in which personal information stipulated in the Management Regulations for Personal Information is consigned to external vendors, and aim to manage and protect personal information in an appropriate manner by preventing external leakage, manipulation, destruction, or loss of personal information we possess.

●Three Principles for Preventing Leakage of Confidential Information

Hitachi has formulated Three Principles for Preventing Leakage of Confidential Information, and always pays sufficient caution to the handling of its own and its customers’ information, working to prevent information leaks.

Principal 1: In principal, no confidential information shall be taken outside of the company’ s premises.
Principal 2: Any person taking confidential information out of the company’ s premises when necessary for conducting business shall obtain prior approval from the Information Asset Manager.
Principal 3: Any person taking confidential information out of the company’ s premises when necessary for conducting business shall carry out the necessary and appropriate measures to prevent information leakage.

Information Security Management System

●Basic regulations

The "General Rules for Information Security Management Systems" stipulates basic provisions that must be adhered to in a strict manner regarding the formulation, implementation, maintenance, and continuous improvement of information security management systems.

The "general provisions for information and information equipment handling" establishes basic conditions regarding handling and management of information and information equipment with the objective of preventing accidents caused by leakage of overall information, or the misappropriation of information.

The "Management Regulations for Confidential Information" stipulates how to handle protection of confidential information.

●Individual regulations

The "Rules on Website Creation and Information Disclosure" stipulate provisions for strict observance in order that information is disclosed and used correctly on the website.

The "Systems Management Regulations for Information Security" stipulates procedures to ensure the security of information systems.

The "Management Regulations for Entrance/Exit and Access Restriction Zones" includes stipulations about physical security assurance, for example regulations regarding how to manage entering and exiting buildings.

●Handling of personal information

We have established personal information regulations equivalent to JIS Q 15001: 2006 "Personal information protection management systems — Requirements" in order to carry out management activities at a level higher than the Personal Information Protection Law.

Our "Management Regulations for Personal Information" stipulates provisions, procedures etc. necessary to fulfil responsibilities regarding operation/management systems creation, management regulation implementation and strict adherence, and personal information protection.

Our "Consignment Criteria for Business Handling Personal Information" stipulates specific procedures for consigning work that deals with personal information to outside vendors, stipulating appropriate management and protection of personal information.

Information Security Management Cycle

By building a framework that implements cyber security measures in PDCA (Plan-Do-Check-Action) cycles, information security management thoroughly implements and improves plans.

Plan: We formulate information security policies and measures, and plan information security education and audits.

Do: We expand the security measures internally, putting them into practice.

We educate staff members about information security, ensuring there is a thorough understanding of the measures.

We hold promotion conferences for information security, where each business site is provided with information about security, and feedback on implementation status of measures.

Check: We inspect the operational status of security systems periodically, and implement audits based on audit plans as well as management reviews carried out by a manager.

We also review management systems through a representative depending on changes in the management environment or internal or external opinion.

Action: We review audits and management systems, and take corrective measures based on internal and external opinions.

Information Security Management System

Information security audits

Information security audits are carried out once a year under the direction of the Information Security Chief Auditor appointed by the President.

The following criteria will be checked in an information security audit.

- Correspondence of management systems for information assets and information security measures to information security regulations.
- Correspondence of personal information management systems to the Personal Information Protection Law and JIS Q 15001: 2006.
- Correspondence of personal information protection management systems and JIS Q 15001: 2006 .

Group Companies are also requested to perform an information security audit once a year.

Information Security Education

●Information Security Education

Continuously maintaining information security requires all parties to continually develop their knowledge of information handling and to remain strongly aware of the issues.

Therefore, we carry out education programs for all staff members, based on their hierarchical level and in accordance with the roles displayed in the table below.

Page 30 lists educational programs to develop more specialized security personnel.

Information security education list >>

	Target audience	Mode	Details
Education program by hierarchical level (all staff members)	Education for all staff	e-learning	Basic education regarding personal information protection, prevention of information leaks, and management of confidential information.
	Management education	Self-study, partial classroom style	Necessary information for managers about personal information protection, information security, and management of confidential information.
	New staff member education	Classroom style	Necessary information for new staff members about personal information protection, information security, and management of confidential information.
	Information security staff	Classroom style, partial practical exercise	Detailed knowledge about information security and management of confidential information. Practical education based in real examples.
	Personal information protection staff	Classroom style, partial practical exercise	Knowledge regarding protection of personal information (PrivacyMark). Practical education based in real examples.
	Information Asset Manager	Self-study, partial classroom style	Knowledge necessary as a person in charge of managing information assets for a division.
Education for relevant persons	Information systems staff	Classroom style, partial practical exercise	Education for information systems supervisors regarding network security, security incident response, web application security, and outsourcing server security

●Training for targeted cyber attack e-mails

The threat of cyber attacks via targeted e-mail is getting stronger, and it is vital that all staff members develop a resistance so that they can respond in the appropriate manner in the case that they are targeted.

Hitachi has been conducting targeted cyber attack e-mail training for all staff members at Hitachi as well as in Group Companies since 2012.

We actually send a mock e-mail disguised as a targeted cyber attack e-mail to all training staff members in order to increase their ability to judge what a suspicious e-mail is, and how you deal with it when you receive one, through actual experience.

●Other support

We distribute an abridged pamphlet version of the “Proper management and handling of Confidential Information” to all staff members to make sure that regulations regarding confidential information management are well known throughout the staff.

Information security technical initiatives

IT based information security measures

At Hitachi we are working on a comprehensive plan to prevent problems like multiple cyber attacks, malware infection, unauthorized access, and information leaks, and are always looking for cutting edge IT security measures to counter new threats.

Safe and secure Hitachi IT security

At Hitachi Group, we have developed a secure Group-wide IT infrastructure environment, which allows Group staff members to share information between over 900 domestic companies.

Uniform security measures which are able to be implemented promptly in an emergency situation have been realized with the standardization and sharing of the IT infrastructure environment.

Hitachi Group products are incorporated proactively into this process, and feedback about their performance results are provided to product design departments, contributing to the further growth of Hitachi Group products.

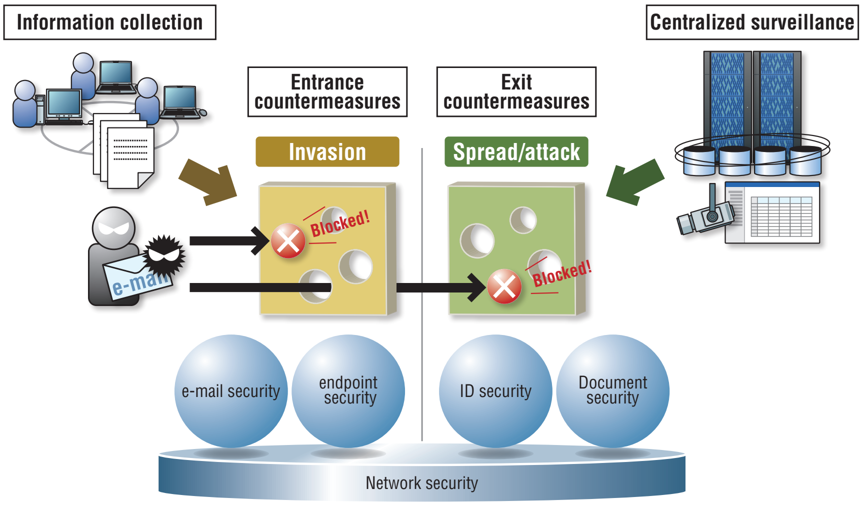
Hitachi IT security systems and multi-layered defenses against cyber attacks

Security systems based on Hitachi IT consist largely of network security (external connections to the Internet or other systems, proxies, and remote access), e-mail security, endpoint security document security, and ID security, and Hitachi has established measures for each of these types of systems, which we implement in a robust manner.

We understand it is important that countermeasures taken against cyber attacks, in particular targeted cyber attacks, need to be addressed without delay, and to be carried out on a continuous basis.

We are taking the following measures using the approach shown in the diagram below in order to achieve these outcomes.

- ･Collecting and utilizing incident information by the CSIRT.
- ･Adding more layers to our leak prevention systems (entrance and exit countermeasures) and defending important information.
- ･Understanding and analyzing attacks through centralized surveillance in order to minimize damage.
- ･Implementing prompt incident operations.
- ･Conducting cutting edge research about cyber attacks and educating and fostering personnel who deal with security issues.



Information security technical initiatives

Network security

1. External connections

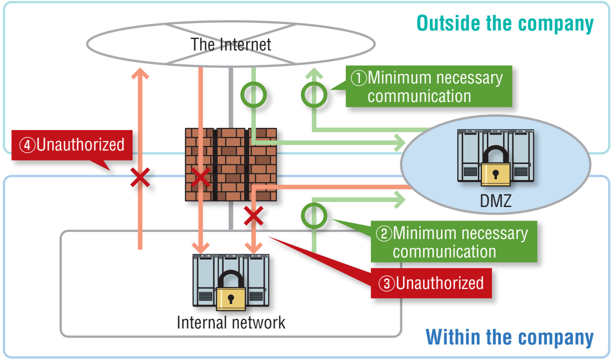
A firewall is in place at the point of connection when an external and internal network connect in order to disclose information to outside the company or to share information, creating a DMZ[*1].

With a firewall in place there can be no direct internal and external communication. We use an indirect method to send information.

The IPS[*2] monitors and blocks unauthorized access at the point of connection to the Internet.

Periodic security audits are also carried out on all servers and network equipment that releases information to outside the company, checking whether there are any security problems.

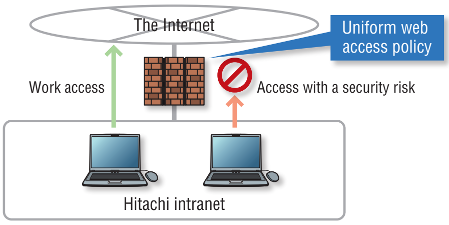
[*1] DeMilitarized Zone   [*2] Intrusion Prevention System



2. Proxy

We are implementing the following countermeasures with a gateway in order to lower risk when accessing the Internet for work.

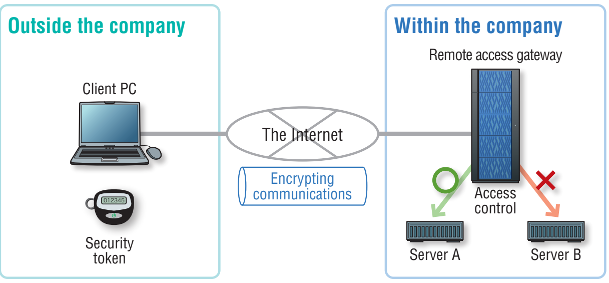
- Limiting users, and saving and auditing logs with the use of certification.
- Filtering URLs via a standardized policy.
- Checking for web virus'.



3. Remote access

We prevent information leaks with a gateway using the following strategies.

- Implementing two-factor authentication (Authentication by authentication media or other method in addition to ID or password.)
- Encrypting communication in certain sections like the Internet.
- Controlling server access

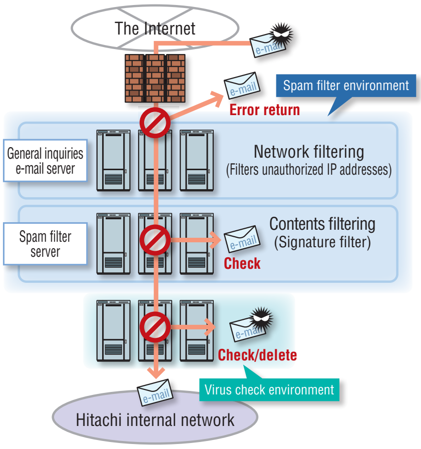


E-mail security

Hitachi has taken measures against external threats as well as threats that are generated internally.

1. Countermeasures against external threats

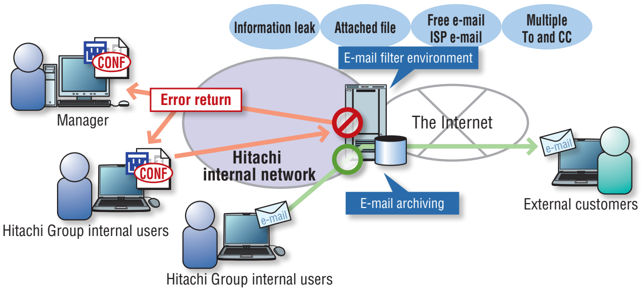
< Spam filters and virus checks >



Hitachi' s e-mail delivery structure is especially responsive towards ① the threat of computer virus invasion, and ② the threat of spam e-mails, when protecting PCs from external threats.

2. Countermeasures against internal threats

There is an e-mail filter server in place for dealing with internal threats which is especially responsive to ① the threat of the spread of computer virus, and ② the threat of information leaks, and permits transmission of only e-mails without any issues.



Information security technical initiatives

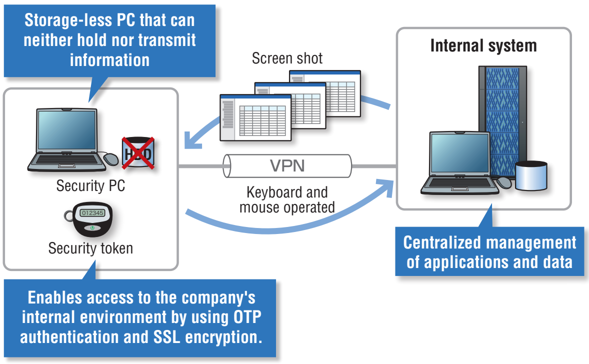
Endpoint security (PCs and smart phones)

Endpoint security protects terminals connected to the internet or to internal LANs, or data stored in such terminals.

As endpoint security, Hitachi applies the latest security patches to each OS and application as measures against exploitation of vulnerabilities and virus infections, and also implements other security measures based on the type of each terminal. The following describes security measures for PCs and smart phones.

1. Turning mobile PCs into thin client PCs

Use thin-client PCs. This is based on the idea that information leaks will not occur if information is not stored on terminals


Storage-less PC that can neither hold nor transmit information
Screen shot
Internal system
HDD
Security PC
VPN
Keyboard and mouse operated
Security token
Centralized management of applications and data
Enables access to the company's internal environment by using OTP authentication and SSL encryption.

2. Using mobile PCs when taking data outside the company

Thin client PCs cannot be used at certain locations: for example, where network connections are unstable. In such locations, workers can take data outside the company on Mobile PCs, which are provided with the functions below to reduce the risk of information leaks.

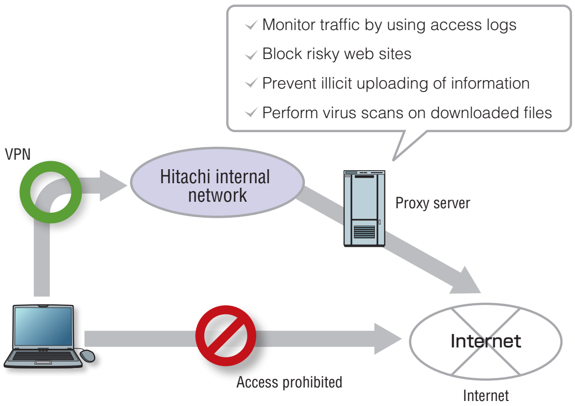
(1) Encryption of internal disks

Encrypting disks such as internal hard disks reduces the risk of information leaks.

(2) Control of network access

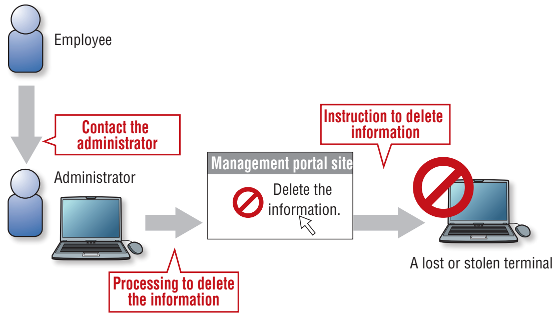
Prohibiting direct internet access reduces risks of events such as computer virus infections.

Access to the internet from an internal network via a proxy server


Monitor traffic by using access logs
Block risky web sites
Prevent illicit uploading of information
Perform virus scans on downloaded files
VPN
Hitachi internal network
Proxy server
Access prohibited
Internet
Internet

(3) Remote erasure of data (remote wiping)

Enabling remote wiping reduces the risk of information leaking if a terminal is lost or stolen.


Employee
Contact the administrator
Instruction to delete information
Administrator
Management portal site
Delete the information.
A lost or stolen terminal
Processing to delete the information

(4) Suppression of writing to external media

Prohibiting writing to external media reduces the risk of information leaks.

(For details, see the description of managing logs when suppressing writing to external media.)

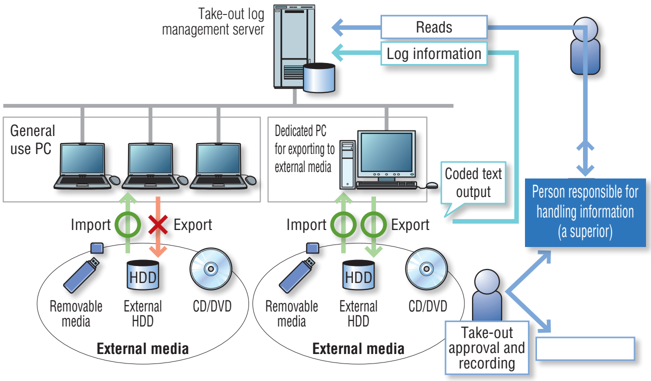
Information security technical initiatives

3. Managing logs when suppressing writing to external media

Workers cannot write data from their PCs to external media.

To physically take data out of the company, approval from a supervisor is necessary, and the writing must be done from a dedicated PC. The logs for data writes are regularly checked to make sure that data is not taken out in an unauthorized manner.

Depending on the vulnerability, risks will increase as time passes. So we have been periodically implementing countermeasures, and have constructed a system for inspecting, maintaining, and managing PC security.



4. Preventing information leaks from smart phones

The following functions are provided in order to reduce the risk of information leaks from theft or loss of smart phones.

(1) Safe management of information

Prohibiting information in smart phones taken out of the company reduces the risk of information leaks.

(2) Remote erasure of data (remote wipes)

Enabling remote wiping reduces the risk of information leaks.

ID Security

Certification and access control on an individual level is a vital part of information security infrastructure.

At Hitachi Group, we have developed a Group-wide authentication infrastructure, making security levels uniform across the entire group, raising standards across the board.

The four authentication infrastructure objectives are as follows.

1. Management of authentication/access control information

Information on IT users is managed in an integrated way with a common system, preventing information renewal failures, ensuring the information is always up to date, and improving accuracy.

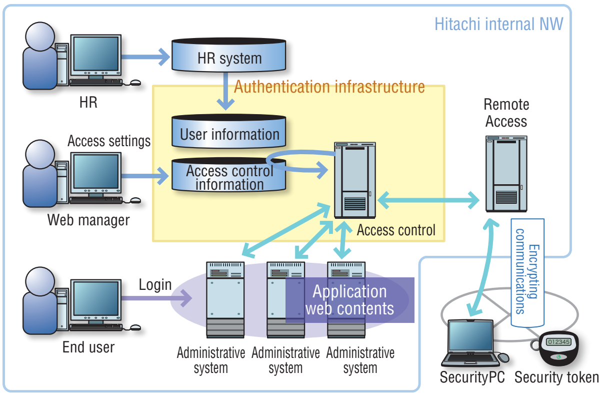
2. Authorization and access control on an individual level

We manage multiple access restrictions for each individual IT user, thus carrying out appropriate access management.

3. Promotion of a ubiquitous environment

Hitachi Group staff members are able to use the systems they need from anywhere with the same conditions, with a common access control system for each administrative system.

Furthermore, the information stored in the authentication infrastructure must be always up to date, and always be highly accurate.



4. Initiatives for the cloud

Risks when using clouds include illegal access by spoofing. Hitachi takes countermeasures against spoofing by linking with Hitachi's internal authentication system when a public cloud is used, and achieves a convenient authentication environment by adopting a single sign-on (SSO) configuration.

In order for this to happen, the following two steps are being taken.

1. ID registration

The HR department registers user information, and updates authentication infrastructure with new information in a prompt manner.

2. Freshness maintenance

Not only passwords, but also IDs have an expiration date, and the ID will become invalid after the period has passed.

Information security technical initiatives

Document security

As documents are being shared frequently with information sharing programs etc., there is an increased risk of information leaks.

In particular, it is very easy to duplicate electronic documents, meaning the damage caused when information is leaked is even bigger.

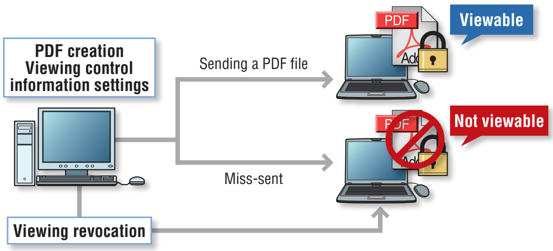
Because of this situation, the following preventative measures have been put in place.

1. Prevention of information leaks from electronic documents

(1) Prevention of information leaks by suspension of electronic document viewing

In general, if an electronic document has been leaked, there is no way of stopping it being viewed.

As a countermeasure, there are document settings for enabling or disabling viewing, duplication, and printing, and if information on a document does get leaked to outside the company, viewing of the document can be stopped by revocation of the owner.



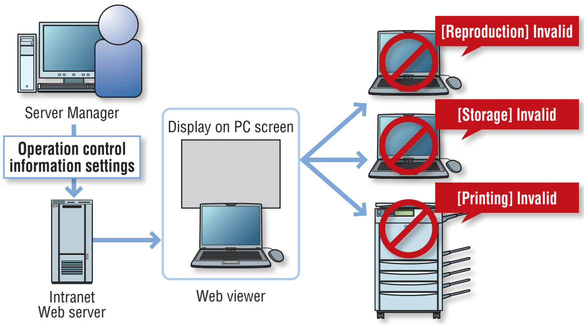
(2) Increased convenience by auto-encryption of electronic documents

We have prepared a storage location that automatically encrypts electronic documents, and have achieved highly convenient management of electronic documents.

2. Prevention of web server contents information leaks

The intranet web is used widely for sharing information internally. It is possible to download the information displayed on the browser to the PC, and it is also possible to print it on to paper, meaning there is a constantly inherent danger of information leaks.

Because of this, there are settings for enabling or disabling functions of contents uploaded onto the website, like duplication, saving, and printing, in order to decrease the risk of information leaks.



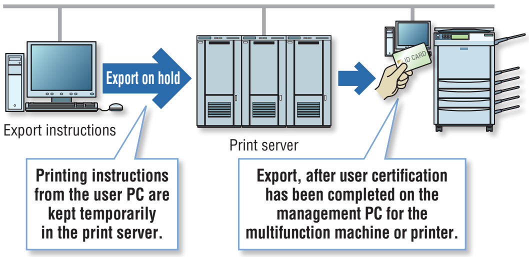
3. Preventing information leaks with paper output from the printer

Leaving printed paper lying around can be a source of information leaks.

This problem occurs because people forget to go and retrieve their paper after pressing the print button on the computer; therefor, the problem can be solved by making it necessary to perform operations at the printer as well as the PC.

At Hitachi, printing from a PC means only that the printing information is stored on the printer server. The user can only print onto paper by operating the management PC located next to the printer.

At this time, the person printing must undergo individual authorization, by inserting their ID card in the management PC in order to identify themselves.



Cloud computing security initiatives

Achieving safe use of the public cloud

In recent years, the public cloud has gained a lot of attention as a tool for implementing information systems. While the public cloud has the advantages of speeding up the building of information systems and reducing operating costs, there is a risk of information leakage. At Hitachi, we have implemented guidelines for controlling risks when using the public cloud, lowering such risks.

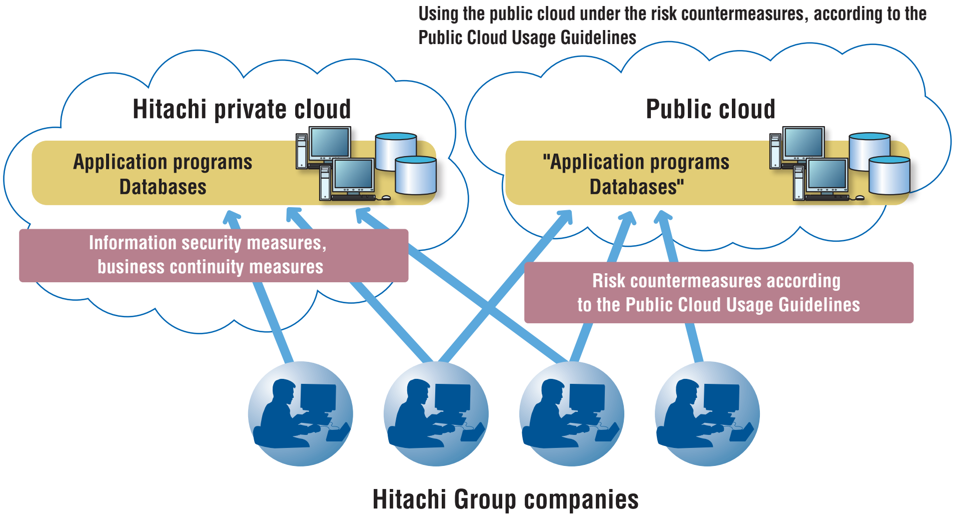
Cloud computing security initiatives

Cloud computing ("the cloud") has been gaining a lot of attention in recent years. Generally speaking the cloud refers to "a method of using software or data etc. that is conventionally monitored and used on your desktop computer through networks like the Internet on an as-need basis, in the form of a service" *. There are two types of clouds, "private clouds" , which are created in the IT environment of a particular company or other entity, and "public clouds" , which are created by a service provider, and offered through the Internet.

At Hitachi, we are working towards consolidating a private cloud that can be shared by all companies in the Group, thereby implementing the security measures and service continuity during disaster situations stated in the "Information Security Technical Initiatives" section of this document. On the other hand, as displayed in Diagram 1, the public cloud is an area to which these initiatives do not extend, so Hitachi has reduced the risk of data leakage when the public cloud is used by establishing the "Guidelines for Using Public Clouds" .

*IT Term Dictionary e-Words, http://e-words.jp/, 1997-2013

Security for cloud use >>


Using the public cloud under the risk countermeasures, according to the Public Cloud Usage Guidelines
Hitachi private cloud
Application programs
Databases
Information security measures,
business continuity measures
Public cloud
"Application programs
Databases"
Risk countermeasures according
to the Public Cloud Usage Guidelines
Hitachi Group companies

Establishing the Public Cloud Usage Guidelines

As shown in Diagram 1, there is a risk of information leakage when using the public cloud through unauthorized access to the public cloud, as data and applications exist on the public cloud. In particular, there is already an increased risk of cyber attacks like unauthorized access by user identity fraud in IT services offered on the Internet, and there is concern that there is also a risk of information leakage with the public cloud. There is also the risk to business continuity, in that if the public cloud vendor goes bankrupt, user business might be interrupted, or data might be lost.

In order to decrease these risks, Hitachi Corporate indicates what sort of risk countermeasures are necessary when using the public cloud through the Public Cloud Usage Guidelines (the "Guidelines"), thus lowering risk.

The Guidelines include risk reduction measures relating to the risk of information leakage, for example processes for authentication and information protection necessary when using the public cloud, and requirements for public cloud vendors operations. Hitachi is also working on validating the degree of conformity to the Guidelines necessary for instances of public cloud use, in order to promote risk reduction through application of the Guidelines.

Physical security initiatives

Physical security initiatives

To prevent information leaks and crimes, it is necessary to install physical security measures, such as office entrance/exit management system and installation of security cameras, are indispensable for strengthening measures against information leaks and against crime. The Hitachi Group is promoting standardized Group-wide physical security measures. The following section outlines the physical security measures.

Standardization of physical security measures in Hitachi Group

In Hitachi Group, physical security measures such as entrance/exit management system used to be conducted at each business site individually. However, a basic policy for infrastructure has been established in order to reinforce measures, which are being implemented in a standardized manner across all Hitachi Group companies.

[Basic policy for infrastructure]

①Establish physical security standards to unify "Physical Security Measures and Operations".

②Introduce Hitachi Group products and services to Implement physical security management systems.

Outline of Physical Security Infrastructure

(1)Zoning and security level

The Standards for Physical Security Measures classify management zones into five security levels, and the entrance/exit management methods and the criteria for placing security cameras and intrusion sensors are defined according to the security level. By following these standards, Hitachi has standardized facilities and equipment.

(2) Introduction of Hitachi Group products and technology

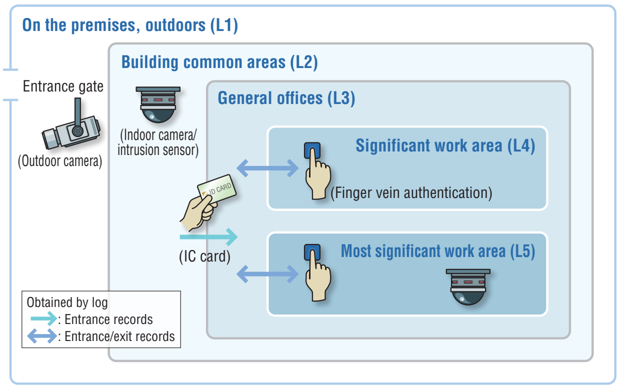
Hitachi Group products are being used in the entrance/exit management equipment, security cameras, and intrusion sensors to be prepared.

Hitachi Group's leading technology "finger vein authentication" has been introduced, in particular as a method for personal identity verification when entering significant zones.

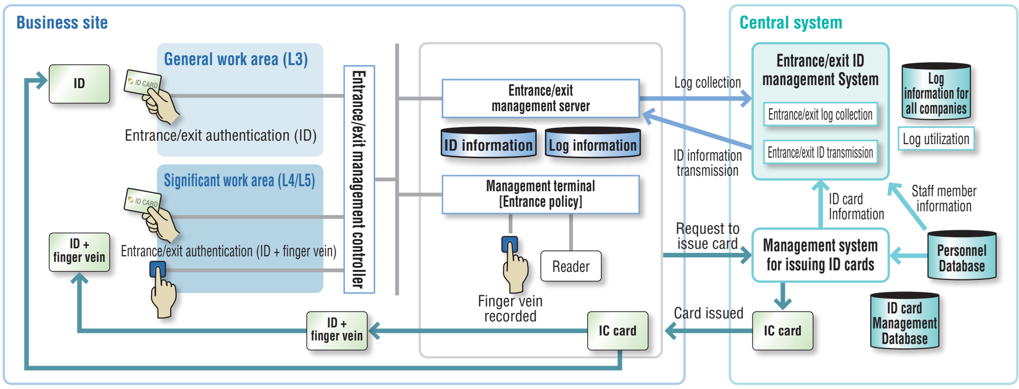
(3) Optimization of business with central control systems

Hitachi has developed an ID card issuance system and ID distribution system connecting to Hitachi Human Resource databases and that enables to optimize and standardize entrance/exit management operation in each business site. Also, forensic data like entrance/exit logs are centralized and used for analysis effectively.

Zone security levels and countermeasures >>


On the premises, outdoors (L1)
Building common areas (L2)
General offices (L3)
Significant work area (L4)
Most significant work area (L5)
Entrance gate
(Outdoor camera)
(Indoor camera/ intrusion sensor)
(Finger vein authentication)
ID CARD
(IC card)
Obtained by log
: Entrance records
: Entrance/exit records

Entrance/exit management system schematic diagram >>



Initiatives in cooperation with procurement partners

Information security assurance initiatives in cooperation with procurement partners

As a corporate group that provides products and services that support social innovation business, Hitachi is working on information security measures in cooperation with its procurement partners. An agreement relating to the prevention of information leakages must be signed in advance when consigning work that deals with confidential or personal information. Our procurement partners also implement information management equivalent levels of security to Hitachi, and are making every effort to prevent accidents occurring or recurring.

Information Security Assurance with Procurement Partners

As corporate groups that support social innovation business, Hitachi' s procurement partners are implement the same level of management as Hitachi, and are making every effort to prevent accidents occurring or recurring.

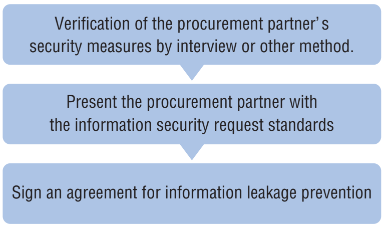
(1) Selection of procurement partners

When consigning work that involves the handling of confidential or personal information to a procurement partner, we perform a status review of their information security measures based on Hitachi' s own standards before allowing access to confidential information.

A business relationship only commences once an agreement regarding the prevention of information leakage that fulfils the security levels demanded by Hitachi has been entered into with the procurement partner.

Furthermore, Hitachi will perform a separate verification specifically for the handling of personal information on the occasion of consigning work that handles personal information.

Work will only be consigned to procurement partners that have fulfilled the conditions of the review as an outcome of verification.



Verification of the procurement partner' s security measures by interview or other method.

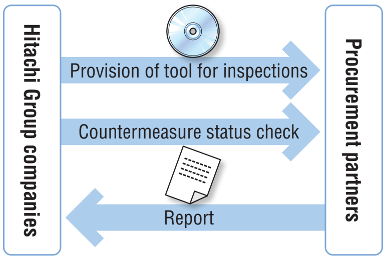
Present the procurement partner with the information security request standards

Sign an agreement for information leakage prevention

(2) Information security accident prevention measures

In order to prevent information leaving the company via the Internet by file exchange software, Hitachi provides information security tools, and carries out inspections to delete work information from individual' s PCs and other devices.

We also check whether information security measures are being implemented as specified in agreements with procurement partners, and suggest appropriate improvements based on the results of those checks.


Hitachi Group companies
Provision of tool for inspections
Countermeasure status check
Report
Procurement partners

(3) Strategies for information security accidents and recurrence prevention measures

If an information security accident occurs, an impact survey will be carried out together with related departments including the procurement partner, and as well as working on implementing measures to make sure any problems are solved expediently, Hitachi will also investigate the cause of the accident and make sure there are no recurrences in cooperation with the procurement partner.

In the case that a serious accident has occurred, or there is complete lack of improvement seen in the procurement partner, the continuation of a business relationship will be re-evaluated.

(4) Future initiatives

Hitachi will constantly check measures procurement partners have in place regarding information security with the aim of preventing accidents, and in addition to this, will work towards strengthening collaboration, and continue to carry out reliable preventative measures.

Cyber security vulnerability handling and incident response initiatives

Security incident initiatives

The Hitachi Incident Response Team (HIRT) is an organization that supports Hitachi' s cyber security countermeasure activities. They contribute to the realization of a safe and secure network environment for customers and companies by preventing security incidents, and by providing a prompt response if an incident does happen.

What is an incident response team?

A security incident ("incident") is an artificial event related to cyber security, and refers to actions (events) such as unauthorized access, service disruption, or data destruction.

An incident response team is a group that leads "incident operations" in order to cooperate inter-organizationally and internationally to solve problems, through preventing (readiness: pre-handling) and resolving (response: post-handling) incidents, and has basic capabilities for "predicting and adjusting to threats from a technical perspective," "conducting technical collaboration activities," and "liaising with external communities on technical aspects."

HIRT activities model

The role of the HIRT is to provide ongoing assistance for Hitachi' s cyber security countermeasure activities through vulnerability handling (eliminating vulnerability that threatens cyber security), and incident response (evading and resolving cyber attacks), from the perspective of organization solo activities (information security initiatives targeted at Hitachi corporate information systems), and organization collaborative activities (initiatives to ensure product and service cyber security targeted at customer information systems or control systems). Furthermore, HIRT' s mission is also to contribute to a safe and secure Internet society by catching any signs of future threats and taking actions as early as possible. The HIRT has adopted an activities model consisting of four IRTs as listed below, in order to expedite both vulnerability handling and incident response.

The four IRTs are:

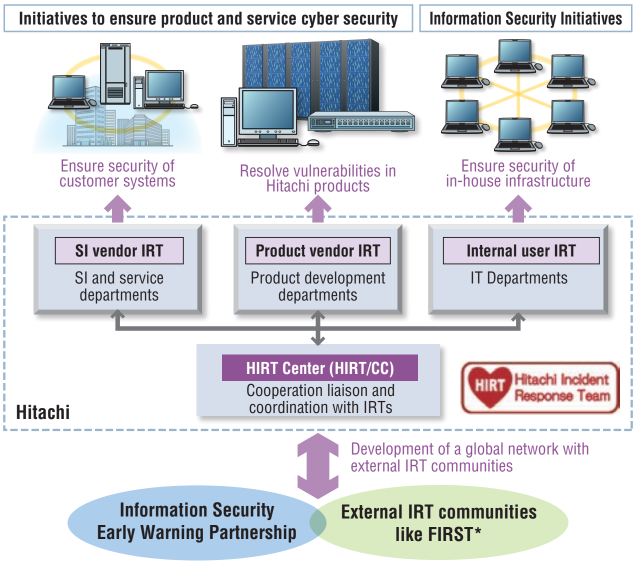
(1) The team that develops information and control system related products (Product Vendor IRT).

(2) The team that uses those products to develop systems and provide services to customers (SI (System Integration) Vendor IRT).

(3) The team that operates and manages Hitachi information systems as an Internet user (Internal User IRT).

(4) A HIRT/CC (HIRT Center) will be put in place to adjust the work load between each IRT, and while making the role of each IRT clear, is a model that promotes efficient and effective security that promote inter-IRT cooperation.

Four IRTs supporting vulnerability handling and incident response >>


Initiatives to ensure product and service cyber security
Information Security Initiatives
Ensure security of customer systems
Resolve vulnerabilities in Hitachi products
Ensure security of in-house infrastructure
SI vendor IRT
SI and service departments
Product vendor IRT
Product development departments
Internal user IRT
IT Departments
HIRT Center (HIRT/CC)
Cooperation liaison and coordination with IRTs
HIRT Hitachi Incident Response Team
Hitachi
Development of a global network with external IRT communities
Information Security Early Warning Partnership
External IRT communities like FIRST*

Category	Role
HIRT/CC*	Corresponding sections: HIRT Center Promote vulnerability handling and incident response through collaboration with external IRT organizations like FIRST, JPCERT/CC* and CERT/CC*, and SI vendors, product vendors, and between internal user IRT.
SI vendor IRT	Corresponding sections: SI/Service provision Support vulnerability handling and incident response for customer systems by ensuring the security of customer systems in the same manner as internal systems for vulnerabilities that have been exposed.
Product vendor IRT	Corresponding sections: Product development Promptly investigate whether any disclosed vulnerabilities have impacted products, and if there are problems, support measures to counter vulnerabilities in Hitachi products by providing a patch or other solution.
Internal user IRT	Corresponding sections: Internal infrastructure provision Support the advancement of vulnerability handling and incident response in order that the Hitachi related sites do not become a base point for invasion.

*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

Cyber security vulnerability handling and incident response initiatives

Activities actioned by the HIRT Center

HIRT Center activities, in the capacity of internally-oriented IRT activities, include moving cyber security measures forwards on both a systematic and technical level by cooperating with information security supervisory divisions in charge of systems as well as quality assurance divisions, and assisting different divisions and Group Companies with vulnerability handling and incident response.

Hitachi is also promoting cyber security measures formulated by collaboration between IRTs as a point of contact for external IRTs.

●Internally-oriented IRT activities

Internally-oriented IRT activities include issuing alerts and advisories containing business knowledge obtained by collecting and analyzing security information to internal organizations, as well as providing feedback about products or service development processes in the form of guidelines or support tools.

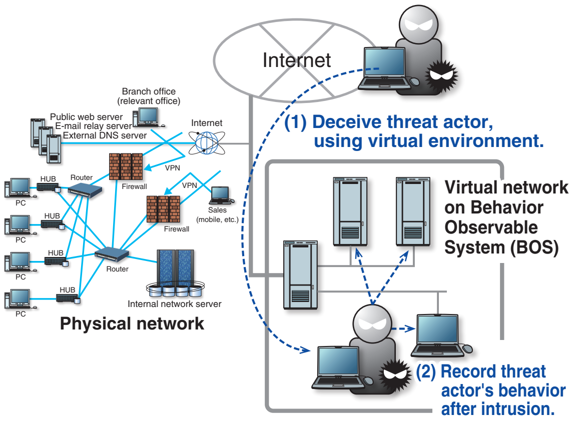
(1) Collecting, analyzing, and disseminating security information

The HIRT Center disseminates information and business knowledge relating to vulnerability handling and incident response to the other teams through promotion of the Information Security Early Warning Partnership

(2) Developing a framework for research activities

The HIRT Center is engaged in "Observation of Threat Actors Activitie" as a technology to "catch any signs of future threats and take actions as early as possible".

BOS (Behavior Observable System) for Observable Threat Actors Activities >>



"Observation of Threat Actors Activities" is an observation method that uses a virtual environment of the organization's internal networks to investigate targeted attacks and other cyber attacks, and records and analyzes the behavior of a threat actor following an intrusion.

(3) Improving product and service security technology

The HIRT Center fleshes out security measures for products related to information and control systems, develops and administering those processes, and promotes the handing down of technology to expert personnel.

(4) Implementing IRT activities for individual domains

The HIRT Center promotes the investigation and organization of IRT activities specific to individual business domains in order to flesh out responses informed by the context and trends in each domain.

As an advanced initiative in the financial field, HIRT-FIS (Financial Industry Information Systems HIRT) was established in October 1, 2012.

●Externally-oriented IRT activities

Externally-oriented IRT activities involve the cooperation of multiple IRTs in promoting the development of inter-organizational alliances with the objective of tackling new threats, and the development of cooperative relationships that can contribute to the mutual improvement of IRT activities.

(1) Reinforcing domestic cooperation of IRT activities

Activities that are strengthened are as follows: the organization of a foundation for information use and application based on JVN jointly operated by the JPCERT Coordination Center and the Information-technology Promotion Agency, Japan; initiatives for vulnerability countermeasures based on Information Security Early Warning Partnership; inter-organization IRT linkage through the Nippon CSIRT Association.

(2) Reinforcing overseas cooperation of IRT activities

Organization of a system of collaboration between overseas IRTs that make use of FIRST activities and overseas product vendor IRTs, and the organization of a foundation for information use and application that utilize STIX and AIS by United States Department of Homeland Security and the like.

(3) Developing a framework for research activities

Fostering opportunities for personnel development through participation in academic research activities, such as the Anti Malware Engineering Workshop, and promoting the education of researchers and engineers with specialist knowledge.

Reference information >>

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

Global information security initiatives

Promoting global information security

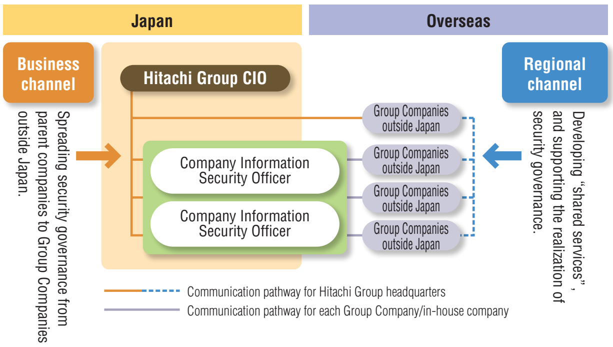
It is necessary for all Hitachi Group Companies worldwide to address strengthening of information security upon ensuring corporate public credibility. Hitachi has designated global information security management standards based on the international standards ISO/IEC 27001, and is promoting and working on the PDCA cycle.

Global information security structures

Hitachi employs two governance channels, a business channel and a regional channel, as its communication channels, the most significant prerequisite for the promotion of global information security.

These two channels constitute a system by which, through their effective utilization, issues particular to different regions or countries can be solved efficiently.

Furthermore, utilization of secure shared services has been proactively developed, with the aim of unification of security measures infrastructure and streamlining of IT investment.



Japan
Overseas
Business channel
Regional channel
Hitachi Group CIO
Company Information Security Officer
Company Information Security Officer
Group Companies outside Japan
Group Companies outside Japan
Group Companies outside Japan
Group Companies outside Japan
Spreading security governance from parent companies to Group Companies outside Japan.
Developing "shared services", and supporting the realization of security governance.
Communication pathway for Hitachi Group headquarters
Communication pathway for each Group Company/in-house company

Establishing global information security management regulations that conform with international standards

Effective utilization of IT as a foundation of business in order to expand Hitachi Group global business into the future is a vital strategy, and "Universal IT Policies" are being established to this end.

"Global Information Security Management Regulations" have been established in compliance with "Universal IT Policies" and the international standard for Information Security Management Systems (ISO/IEC 27001), in order to promote security governance.

The Management Regulations and related documents contain security risk measures that can be implemented with certainty, which were established upon consideration of the perspectives of developing countries experiencing significant growth, and the growth of Group Companies outside Japan, that also continue to support competition which opens up global business.

The PDCA cycle for improving levels of global information security

Hitachi promotes the PDCA cycle (continuous improvement) for the continuous operation, maintenance, and improvement of information security in order to improve security levels as stated in the "Global Information Security Management Regulations".

Group Companies outside Japan conduct self-checks to determine their security status.

The results of these checks are being visualized and analyzed in order to understand situations in different regions and different Group Companies outside Japan, and in the future, will be utilized during the formulation of the direction for Global Security Policies, which must be addressed by the entire company.

Personal information protection initiatives

Personal information protection guaranteeing security and trust

Hitachi was granted the Privacy Mark certification in March 2007, for implementing safe personal information management and protective measures. Hitachi operates the “personal information protection management system” , which is a framework for the protection of personal information, and is working continuously on personal information protection and appropriate handling for staff members as well as all other stakeholders.

Personal information protection

Hitachi has implemented management regulations for personal information that correspond to Japan Industrial Standards “Personal information protection management systems - Requirements (JISQ 15001: 2006)” , which stipulate management standards to a stricter level than the Personal Information Protection Law. These regulations are based on the “Hitachi personal information protection policies” , which stipulate principals and policies relating to personal information protection for the purpose of protecting personal information important to the owner of that information.

Hitachi obtained third-party certification, the “Privacy Mark” (granting institution: JIPDEC) in March 2007, granted to vendors that are recognized as taking appropriate security management and protection measures related to personal information. The certification was renewed for the fourth time in March 2015.

Hitachi strives to protect personal information with a sense of self awareness and responsibility as a vendor with Privacy Mark certification, maintained so that all stakeholders are able to provide Hitachi with personal information with peace of mind.

Hitachi Privacy Mark >>

System for promoting personal information protection

In April 2009, Hitachi merged the “Personal Information Protection Promotion System” and the “Information Security Promotion System” , and commenced the new “Information Security Promotions System” . Our aim is to realize a highly practical management system through the unification of management systems related to significant information including personal information, and systems related to information security.

Through this unification, we have carried out the four safety management measures required by the “Personal Information Protection Law” and other regulations, and have unified the “Information Security Technical Initiatives” , “Physical Security Initiatives” and others, promoting the protection of personal information.

The specific management structure is as stated in the “Information Security Promotion System” clause of the “Information Security Management System” .

Hitachi also strives to safeguard personal information globally at Group companies outside Japan based on the “Personal Information Protection Policy” and by adhering to all applicable laws and regulations, including social requirements.

〈Four measures for safety management〉

(1) Organizational Safety Management Measures:
Structuring and operating regulations and systems, verification of their implementation, etc.

(2) Human Resources Safety Management Measures:
Entering into non-disclosure and other agreements, education and training, etc.

(3) Physical Safety Management Measures:
Management of entrances/exiting buildings (rooms), theft prevention measures, etc.

(4) Technical Safety Management Measures:
Access control of information systems, unauthorized software countermeasures, etc.

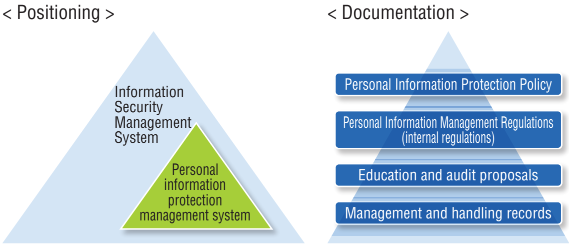
Personal information protection initiatives

Personal Information Protection Management System

The "Personal Information Protection Management System" (PMS) has also been positioned as part of the "Information Security Management System" (ISMS) in addition to the unification of management systems, with the exclusion of the operation of a section which is specific to personal information protection.

The "PMS Documentation" , which is a document containing the basic elements of the PMS, is made up of the "Personal Information Protection Policy" , "Personal Information Management Regulations (internal regulations)" , "proposals" for audits, education and similar, and a "record" of PMS implementation.

Hitachi personal information protection management system >>


< Positioning >
Information Security Management System
Personal information protection management system
< Documentation >
Personal Information Protection Policy
Personal Information Management Regulations (internal regulations)
Education and audit proposals
Management and handling records

Management and appropriate handling of personal information

Hitachi strives for strict management and appropriate handling of personal information entrusted with us, according to internal regulations "Personal Information Management Regulations" .

A person in charge of protecting personal information (an Information Asset Manager) is located at each workplace, and identifies all personal information entrusted to Hitachi, managing logs and carrying out appropriate measures according to the seriousness of that personal information.

This person also carries out periodic education on personal information protection, personal information protection audits, and checks status of operations in workplaces, in order to make personal information protection management systems an established practice.

In addition, they will also distribute the "Personal Information Protection/Information Security Card" to all staff members, and make sure that all staff members have been duly informed of the rules requiring strict adherence with regard to principles, as well as management and handling, relating to Hitachi' s personal information protection.

Initiatives in the workplace >>

〈All personal information〉
･Identification and classification of personal information
･Risk recognition, analysis, and countermeasures
･Record of personal information on log
･Periodic revision of personal information
･Appropriate handling
･Personal information protection education
･Personal information protection audits
･Confirmation of operational status in the workplace

Compliance with the "My Number" system

Hitachi strives for strict management and appropriate handling of personal information according to internal regulations related to Japan's "My Number" IDs (used for social security and tax purposes).

We have established a system to manage "My Number" IDs. By assessing risks of business operations associated with "My Number" IDs, we are taking appropriate measures against risks.

Personal information protection initiatives

Enhancing subcontractor management

There have been a number of information leakage accidents from subcontractors handling personal information in the past few years, which has become a social problem.

Hitachi enhanced its management of subcontractors handling personal information from an early stage, and has established internal regulations relating to the consignment of the handling of personal information, and subcontractors are supervised in accordance with these regulations.

An assessment and selection process is carried out based on subcontractor selection standards stipulated by Hitachi Group so that Hitachi selects subcontractors with personal information protection standards equivalent to or surpassing Hitachi's own standards.

Furthermore, consignment only occurs after an agreement has been signed which includes strict personal information management conditions such as the establishment of a system of management, and a basic prohibition of re-entrustment.

Supervision of the subcontractor will also be carried out, with a self-awareness of Hitachi as responsible as the prime contractor, in the form of periodic reassessments of the subcontractor, and the implementation of audits.

Hitachi Group overall initiatives (promotion to be certified as Privacy Mark entity)

Hitachi Group is engaged in the protection of personal information as a unified entity.

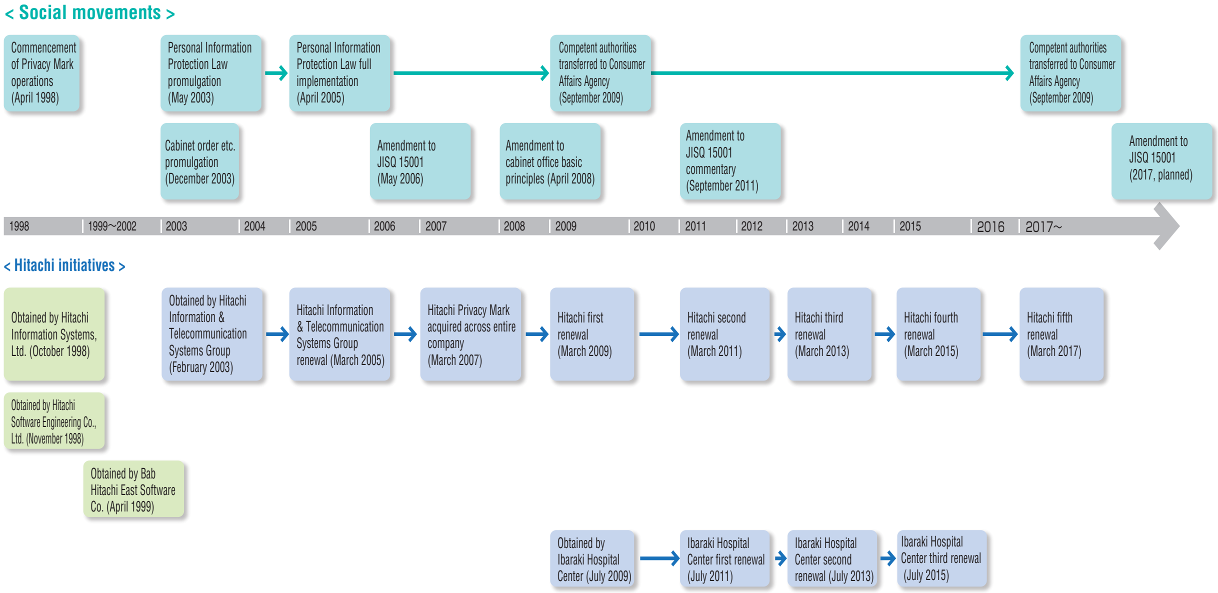
As of this date May 31, 2017, the Privacy Mark has been obtained by 47 vendors, which are protecting and handling personal information at a management level higher than the level required by the law.

Hitachi has also established the "Hitachi Group Privacy Mark Liaison Committee" which consists of mainly companies that have obtained the Privacy Mark, and implements periodic information exchange sessions, study sessions, and seminars to which external specialists are invited. Information sharing and research about personal information protection is also building up across the Group.

Medical facilities like hospitals are also engaged in the protection of personal information as independent vendors.

In July 2009, the Corporate Hospital Group in Japan also gained Privacy Mark certification. Hitachi is working hard to protect and carefully handle the personal information of its patients and others.

Hitachi Privacy Mark initiatives >>


< Social movements >
Commencement of Privacy Mark operations (April 1998)
Personal Information Protection Law promulgation (May 2003)
Personal Information Protection Law full implementation (April 2005)
Competent authorities transferred to Consumer Affairs Agency (September 2009)
Competent authorities transferred to Consumer Affairs Agency (September 2009)
Cabinet order etc. promulgation (December 2003)
Amendment to JISQ 15001 (May 2006)
Amendment to cabinet office basic principles (April 2008)
Amendment to JISQ 15001 commentary (September 2011)
Amendment to JISQ 15001 (2017, planned)
1998
1999~2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017~
< Hitachi initiatives >
Obtained by Hitachi Information Systems, Ltd. (October 1998)
Obtained by Hitachi Software Engineering Co., Ltd. (November 1998)
Obtained by Bab Hitachi East Software Co. (April 1999)
Obtained by Hitachi Information & Telecommunication Systems Group (February 2003)
Hitachi Information & Telecommunication Systems Group renewal (March 2005)
Hitachi Privacy Mark acquired across entire company (March 2007)
Hitachi first renewal (March 2009)
Hitachi second renewal (March 2011)
Hitachi third renewal (March 2013)
Hitachi fourth renewal (March 2015)
Hitachi fifth renewal (March 2017)
Obtained by Ibaraki Hospital Center (July 2009)
Ibaraki Hospital Center first renewal (July 2011)
Ibaraki Hospital Center second renewal (July 2013)
Ibaraki Hospital Center third renewal (July 2015)

Information security products and services initiatives

Information security products and services security assurance initiatives

Hitachi promotes activities that ensure the information security of products and services provided to customers. These activities are promoted in cooperation with Group Companies.

Information security initiatives

Hitachi has established the following security policies and three security clauses regarding products and services provided to customers, promoting intiatives to maintain information security. The Security Technology Commitee is at the center of these initiatives.

The committee formulates guidelines and plans security measures in order to maintain the quality of products and services from the aspect of information security, along with maintaining a grasp of information security technology trends.

●Security policies

The mission of a vendor who provides information security products and services is to provide a secure and reliable IT infrastructure, for a society that utilizes a wide variety of information at a high rate.

As a vendor of products and services as well as a user of Hitachi Group common IT platforms, its activities must properly maintain information security, and contribute to the security and value of every stakeholder, including customers.

●Three security clauses

(1) Establishment of security management systems

Establish the security management systems and improve them by undertaking regular reviews, in order to maintain the information security products and services and to ensure a quick, effective, and orderly response to information security incidents.

(2) Provision of secure products and services

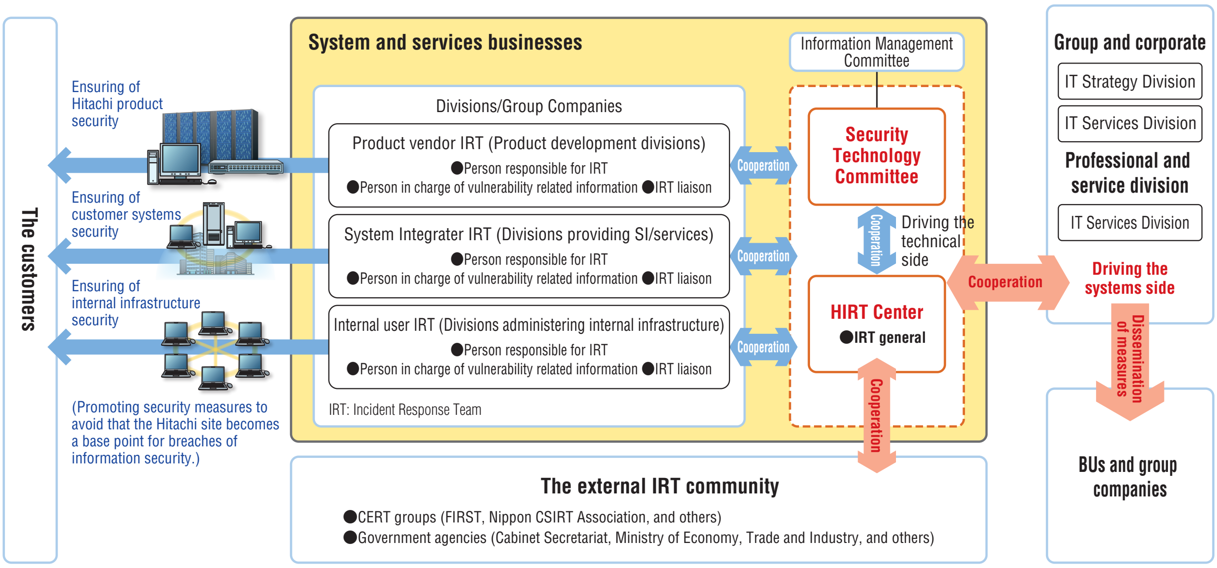
Design and implement the security functions and periodically undertake inspections of the products and services as well as their development and operation processes,s in order to provide secure information security products and services.

(3) Prompt response to security incidents

Monitor internal and external security incidents and properly respond to security incidents that have occurred and that are related to provided information security products and services

Provide the users with vulnerability-related information in order to prevent security incidents.

●Organizational structure for promotion


The customers
Ensuring of Hitachi product security
Ensuring of customer systems security
Ensuring of internal infrastructure security
(Promoting security measures to avoid that the Hitachi site becomes a base point for breaches of information security.)
System and services businesses
Divisions/Group Companies
Product vendor IRT (Product development divisions)
●Person responsible for IRT
●Person in charge of vulnerability related information ●IRT liaison
System Integrater IRT (Divisions providing SI/services)
●Person responsible for IRT
●Person in charge of vulnerability related information ●IRT liaison
Internal user IRT (Divisions administering internal infrastructure)
●Person responsible for IRT
●Person in charge of vulnerability related information ●IRT liaison
IRT: Incident Response Team
Cooperation
Cooperation
Cooperation
Information Management Committee
Security Technology Committee
Cooperation
Driving the technical side
HIRT Center
●IRT general
Cooperation
Cooperation
Group and corporate
IT Strategy Division
IT Services Division
Professional and service division
IT Services Division
Driving the systems side
Dissemination of measures
BUs and group companies
The external IRT community
●CERT groups (FIRST, Nippon CSIRT Association, and others)
●Government agencies (Cabinet Secretariat, Ministry of Economy, Trade and Industry, and others)

HIRT: Hitachi Incident Response Team (organization for security incident/vulnerability countermeasures and response. Composed of Hitachi specialists.)
FIRST: Forum of Incident Response and Security Team

Information security products and services initiatives

Group Company activities

Group Companies that provide information security products and services have established organizations to ensure the security of supplied products and services. The following activities are being promoted.

(1) Web security

A division devoted to ensuring security quality for internal and external websites and systems has been established, and a division devoted to ensuring security quality for internal and external websites and systems has been established.

This division provides periodical diagnosis of the websites, the processes to approve the websites (application, consultation and implementation), and the preventive actions to ensure web security, as well as responding promptly to any web security incidents.

(2) System development security

Guidelines have been established for secure system development. In addition, tools which support the secure development, such as a security design checklist, vulnerability detection tool and other measures, are being utilized.

(3) Security education for engineers

In order to improve skills for engineers related to secure system development, education courses are provided, such as web application vulnerability prevention countermeasure courses, security courses for each developer language, and threat analysis courses.

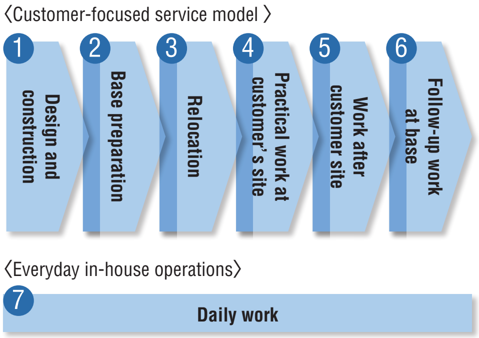
(4) System operation and maintenance services security

It is necessary to provide secure system operation and maintenance services in order to prevent the customer from breaches such as leakage of information assets, theft, destruction, manipulation, or unauthorized use.

For this reason, the process for providing systems operations and maintenance services has been clarified, and security standards that require actions necessary for each process have been provided and applied.

For example, for the process of design and construction, identification of information assets and their risks, and decision of security measures are required, and such requirements are fully disseminated in the organization. Traceability is also ensured for operations carried out at customer sites to replace faulty hard disk drives.

Business processes for provision of system operation and maintenance services >>



Information security products and services initiatives

Open Middleware Product security assurance initiatives

In recent years, the impact of software product vulnerability on social infrastructure has been growing steadily, and assurance of product security has become vital. From a global perspective, Hitachi Open Middleware Products, which play a central role in systems, have security assured at each phase from design and implementation to operation, so that the customer can use these products securely.

Security assurance initiatives

Many Open Middleware Products provided by Hitachi play a central role in social infrastructure, making security assurance vital.

It is the obligation of the vendor to provide products that the customer can trust, and from design and development to operation, it is important to build a framework which takes security into consideration across the entire life cycle of the software.

We have incorporated security assurance measures for conventional development processes when developing Open Middleware Products.

We have defined this as the “Secure Development Life Cycle of products” and are working to ensure a global standard of security while incorporating the approach of information security international evaluation criteria ISO/IEC 15408 (common criteria) and other standards.

Software development based on Secure Development Life Cycle of products

The following criteria have been established as important development processes in the “Secure Development Life Cycle of products”.

(1) Definition of requirements
Determination of overall policies regarding product security, and development policies for ensuring security.

(2) Design
Determination of security requirements based on threat analysis and the fleshing out of functional design that takes security into consideration.

(3) Implementation (Secure programming)
Identification of vulnerabilities by applying secure programming checklists and static analysis tools to source codes.

(4) Testing
Vulnerability detection with security testing tools (security scanners) and validation based on security checklists.

(5) Support
Prompt response to vulnerability issues in our products that are discovered after commencement of operations. Support by creation of patches and information disclosure to minimize customers' risk of exposure.

Hitachi is developing products with assured security by educating and sharing information with security developers and inspection supervisors on a continuous basis about trends in technology and vulnerability issues.

Approach for incident response to software product vulnerabilities

The basic approach is to eliminate software vulnerability issues in the design, implementation, and test phases. However, it is possible that there will be new vulnerabilities discovered, and new attack methods appearing.

Therefore, it is also necessary to consider a response for the operation phase of software products.

These initiatives also take into account the 2014 Ministry of Economy, Trade and Industry Public Notice Number 110 “Software Vulnerability Related Information Handling Measures” and the “Information Security Early Warning Partnership Guideline” , and stipulate the process from communication about a vulnerability issue to presenting a customer with a solution.

This framework is also coordinated with incident response activities (CSIRT) by “HIRT” *. Response to product vulnerability issues are done so in cooperation with affiliated institutions.

* HIRT：Hitachi Incident Response Team
CSIRT：Computer Security Incident Response Team

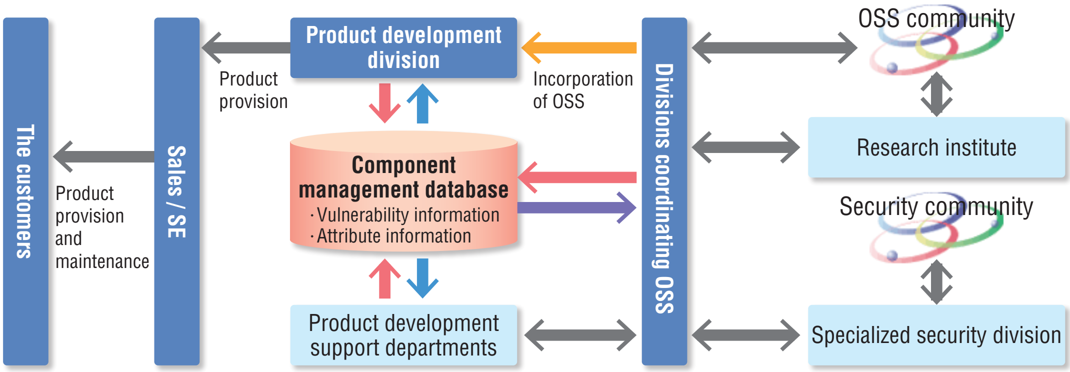
Information security products and services initiatives

Strategies for Open Source Software (OSS)

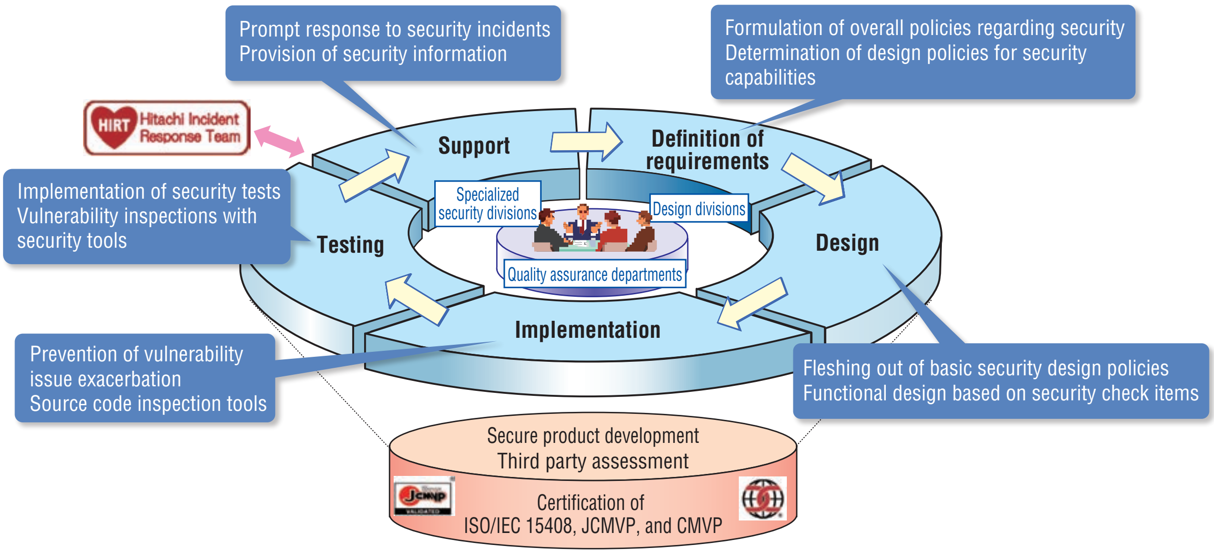
Examples of disclosure of vulnerability information in prominent OSS have become more prominent in recent years.

In order to deal with this, OSS information used in products is centrally managed, and initiatives have been put in place so that problem analysis, impact assessment, and selection of countermeasure policies can be carried out in a prompt manner.

OSS activity structure utilizing a component management database >>


The customers
Sales / SE
Product provision and maintenance
Product provision
Product development division
Incorporation of OSS
Component management database
· Vulnerability information
· Attribute information
Product development support departments
Divisions coordinating OSS
OSS community
Research institute
Security community
Specialized security division

Secure Development Life Cycle of Products Diagram >>


Prompt response to security incidents
Provision of security information
Formulation of overall policies regarding security
Determination of design policies for security capabilities
HIRT Hitachi Incident Response Team
Implementation of security tests
Vulnerability inspections with security tools
Support
Definition of requirements
Testing
Design
Implementation
Specialized security divisions
Design divisions
Quality assurance departments
Prevention of vulnerability issue exacerbation
Source code inspection tools
Fleshing out of basic security design policies
Functional design based on security check items
Secure product development
Third party assessment
Certification of ISO/IEC 15408, JCMVP, and CMVP

Application of third party assessment and certification systems

Initiatives in the "Secure Development Life Cycle of products" , namely, third party assessment and certification according to international security evaluation standard ISO/IEC 15408 are also incorporated as indicators objectively highlighting initiatives that ensure security, and the major Open Middleware Products HiRDB and Hitachi Command Suite have obtained these certifications.

This standard is also utilized in the "Standards for Information Security Measures for the Central Government Computer Systems" and other documents, as they are able to objectively highlight initiatives that "assure security" in product development.

By developing software based on the "Secure Development Life Cycle of Products" , it is possible to develop products that are on the same level as international standards like ISO/IEC 15408 (please refer to the "IT Security Certification" section in the "Third Party Assessment and Certification" for certified products.)

Reference information >>

■ISO/IEC 15408 information for Hitachi Open Middleware
http://www.hitachi.co.jp/Prod/comp/soft1/sec_cert/index.html

JCMVP (Japan Cryptographic Module Validation Program)
CMVP (Cryptographic Module Validation Program)

Information security products and services initiatives

Information security initiatives in cloud computing

Hitachi Cloud (Platform Resource Provisioning Services/Enterprise Cloud Services)

Hitachi is conducting various security initiatives relating to the cloud, a new form of IT provision and a part of social infrastructure, realizing a “safe and secure cloud” that is applicable to corporate information systems.

Cloud computing and security

IT, like electricity and water, is becoming common as “cloud computing” (“the cloud”) in which technology is used as a service, and does not require the user to possess any facilities or equipment.

In the cloud, not only are hardware and software maintained , but security measures are also carried out by service providers (cloud vendors), meaning the IT departments in user corporations can be freed from this task, and concentrate on constructing IT that will realize the core competencies of their own companies.

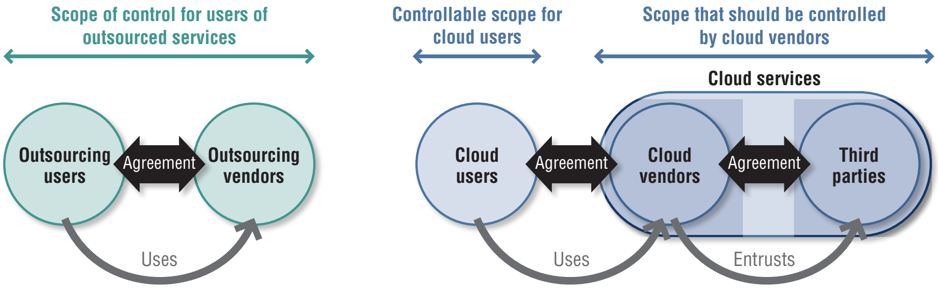
On the other hand, there are more than a few people who are concerned about problems like information leakage, as many different users share the same service provider environment.

Additionally, there is also the chance that the user will be put in danger of no longer knowing what content can be supervised or audited in the case of internal systems, for example compliance related to IT.

In this way, with the cloud, there is the necessity for information security corresponding to cloud-particular characteristics “sharing (resources with other users)” , and “using (vendor environments)” .

Furthermore, in the case that the cloud is used for only a portion of operational systems, assurance of information security to the same level as existing systems across all IT systems will be required.

Control scope differences between conventional consignment and the cloud>>


Scope of control for users of outsourced services
Controllable scope for cloud users
Scope that should be controlled by cloud vendors
Cloud services
Outsourcing users
Agreement
Outsourcing vendors
Uses
Cloud users
Agreement
Cloud vendors
Agreement
Third parties
Uses
Entrusts

(a) Regular subcontracting

(b) Using the cloud

Movements related to cloud computing information security

In response to this situation, guidelines and regulations for information security have been formulated regarding different sorts of industry groups and public bodies.

In addition to these, the proposal for international standards based on the guidelines of the Ministry of Economy, Trade and Industry, which was submitted by Japan's representatives to ISO/IEC SC 27, was standardized as ISO/IEC 27017.

The leading ones are listed below.

The purpose for the promotion and spread of these, Hitachi is also an active member of the “Cloud Information Security Promotion Alliance” which was established with cloud vendors and auditors from the “Japan Information Security Audit Association” .

Title	Security Guidance for Critical Areas of Focus in Cloud Computing	Cloud Computing Risk Assessment	Information security management guidelines for use of cloud services	Guidelines for information security measures for ASP/SaaS	Handbook for safe use of cloud services for small to medium sized enterprises
Publisher	CSA (Cloud Security Alliance), a not for profit group from the USA, with participating members from IT vendors, cloud service vendors, etc.	ENISA (European Network and Information Security Agency), a European network information security bureau (An EU institution)	Ministry of Economy, Trade and Industry, Commerce and Information Policy Bureau, Office for IT Security Policy	Ministry of Internal Affairs and Communications “ASP/SaaS Information Security Countermeasure Research Society”	Information-technology Promotion Agency, Japan (IPA) Security Center
Intended reader	Cloud vendors, Cloud users	Cloud vendors	Cloud vendors, Cloud users	Cloud vendors	Cloud users (Particularly small and medium-size enterprises)
Outline	Main issues and advice about domains	Cloud risk and control	Checklist for when using the cloud, functions for preparation when providing	Organizational, operational, physical, and technological countermeasures	A checklist designed for small to medium sized enterprises

Information security products and services initiatives

Information security initiatives to achieve a “safe and secure cloud”

Hitachi Group has made “Hitachi Cloud” , a global unified brand in the cloud, and is working to address the realization of a “safe and secure cloud” for the services belonging to this brand, based on these sorts of trends.

Using one of Hitachi Cloud services, the “Platform Resource Provisioning Services” (IaaS), as an example, the previously stated CSA, ENISA, and Ministry of Economy, Trade and Industry guidelines are used in a cross-sectoral manner, and checklists from the point of the service user and provider have been created relating to the IaaS/PaaS/SaaS service layer.

Necessary measures and procedures are being created and promoted based on the characteristics of each guideline, covering a variety of information security perspectives, through the implementation of systematic self-checks.

In particular, guidelines relating to each of the 13 domains indicated in CSA Ver. 3.0[*1] have had clarified for equivalent services, and different measures are being carried out in order to achieve those guidelines.

To give one example, in the “compliance and auditing” domain, it is necessary to implement services and audits with strict adherence to customer compliance stipulations even for cloud services.

The “Platform Resource Provisioning Services” provides guidance to be able to carry out thorough compliance for processing in the cloud in the, equivalent to customer internal compliances.

Measures to achieve these guidelines like compliance-related reporting and auditing methods are stipulated in an agreement with the customer, so that the customer can verify whether compliance is being followed.

Because standards relating to information security differ depending on the industry, organization of measures as they relate to the key criteria for each industry are also being promoted.

To give one example from the public sector which includes public authorities and local governments, the National center of Incident readiness and Strategy for Cybersecurity (the NISC) has published the “Unified Standards for Government Agency Information Security Countermeasures (2016 edition)” [*2], establishing criteria for administrative bodies.

Requirements relating to the application of cloud services to the public sector have been isolated, and information security enhancement reflecting services has been planned.

The vast business knowledge about information security that Hitachi has accumulated in product and SI business is being utilized in Hitachi Cloud. Hitachi will also continuously address initiatives to achieve a cloud that customers can use with peace of mind, based on trends in industry groups and standardization.

[*1] Cloud security alliance: Security guidance for critical areas of focus in cloud computing V3.0
https://cloudsecurityalliance.org/ (November 2011)

[*2] National center of Incident readiness and Strategy for Cybersecurity (the NISC):
Unified Standards for Government Agency Information Security Countermeasures (2016 edition)
http://www.nisc.go.jp/active/general/kijun28.html

Information security products and services initiatives

Initiatives to protect privacy when using personal data

Advanced technologies such as IoT, AI and robotics have aroused our expectations that using large amounts of data, of various types, will achieve a super smart society. On the other hand, public awareness regarding privacy protection has been growing. Hitachi is striving to protect privacy, so that value can be created while client's and individual's safety and security are ensured.

Personal data utilization and protecting privacy

Japan has been focusing on achieving a super smart society*[1] as the major theme in the 5th Science and Technology Basic Plan established in 2016. People anticipate a society where a variety of things are connected via networks and large amounts of data, of various types, is analyzed by using AI and other technologies, to create new value. In particular, we expect to utilize personal data about individuals.

The amended Act on the Protection of Personal Information took effect in its entirety in May 2017. The law requires that, among personal information, any data that can be used to identify a specific person must be used appropriately and efficiently, and, at the same time, the rights and benefits of individuals must be protected. As Diagram 1 shows, in the while of personal data overlaps with data related to one's privacy such as "location information" and "purchase history". Recent advancement of technologies has made it possible to collect an large amount of personal data related to an individuals' privacy. Using such data to enrich lives of citizens while protecting their privacy contributes to the social development.

Hitachi and Hakuhodo Inc. have continued research on individual awareness of the use of personal data. "The Third Attitude Survey regarding Lifestyle Information Handled as Big Data"*[2] (announced in December 2016) suggests that proactive measures taken by business suppliers can reduce concerns of individuals and increase tolerance towards the use of personal data (see Diagram 2). Based on this suggestion, Hitachi concludes that it is important to capture privacy risks associated with data to be handled, and to exercise appropriate measures in order to use personal data safely and securely.

*1: A society in which the things and services are provided to people who need them, when they need them, and in the amounts they need. In such a society, various social needs are handled in a fine-grained manner, and all people can derive from high quality services and live a comfortable life in which differences, such as age, sex, region, and language, are accepted.

*2: http://www.hitachi.co.jp/New/cnews/month/2016/12/1202a.html

Diagram 1 Venn diagram "Types of personal data and their relationships"

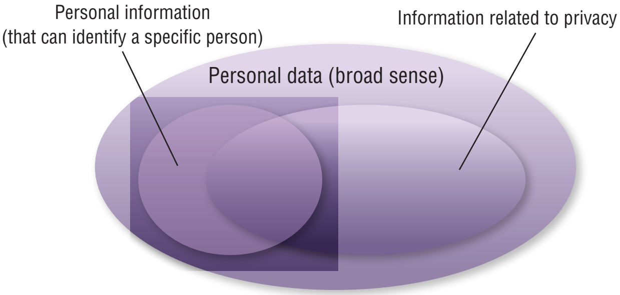
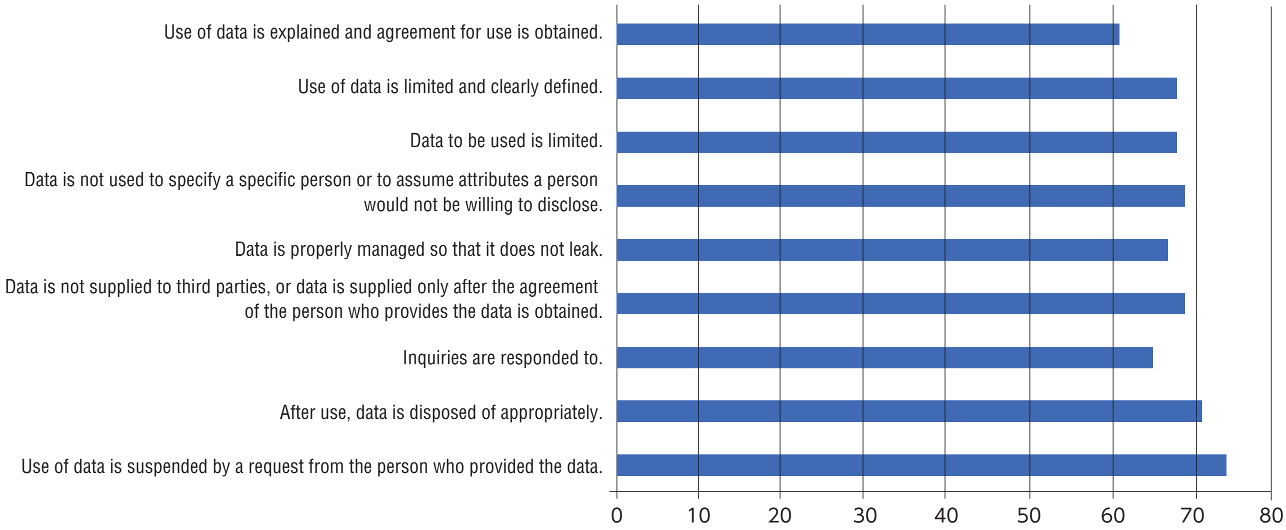

Personal information
(that can identify a specific person)
Information related to privacy
Personal data (broad sense)

Diagram 2 Survey of attitudes regarding personal information handled as big data

What sort of privacy measures should a company take to reduce your concerns regarding secondary uses of your personal data?

Note: The total percentage (%) of the people who selected "Reduces" or "Slightly reduces".



Information security products and services initiatives

Hitachi's privacy protection initiatives

Hitachi strives to proactively resolve new issues in order to achieve a sustainable society where people can lead a comfortable life. We promote privacy protection initiatives to contribute to the safety and security of individuals and customers, with the requirement that we strictly observe Act on the Protection of Personal Information when we use personal data.

●Managing and operating a privacy protection advisory committee

Hitachi has taken initiatives to protect privacy in big data businesses since 2013. In 2014, these initiatives were deployed to the departments related to Information & Telecommunication Systems. In addition, the following were established to aid this goal: a "personal data manager" who manages privacy protection, and the "privacy protection advisory committee" which integrates knowledge about privacy protection, and which supports privacy impact assessments and countermeasures. Through these initiatives, we have systematically developed and deployed privacy protection measures and have been striving to reduce privacy risks in business operations, so that each staff member deals with personal data by exercising appropriate measures in cooperation with customers.

● Implementing privacy impact assessments

Using Hitachi's own checklist, we conduct privacy impact assessments to check the likelihood of risks in operations that deal with personal data. Furthermore, in cases which risks are identified as high, or assessments are difficult for operational departments to make, specialists from the privacy protection advisory committee support identify risk countermeasures. The number of such cases has increased year by year since 2014 and the actual number reached 120 cases in 2016. Based on the outcomes from these actual cases, materials such as the checklist have been assessed and revised accordingly to reduce risks related to privacy,therefore we could appropriately handle personal data when we support customer business operations as well as when we provide our own services.

● Privacy protection education

To achieve appropriate privacy protection and use personal data appropriately, staff members must have a correct understanding about privacy, must protect privacy. To achieve these objectives, Hitachi regularly provides training and education for staff members regarding privacy protection, and holds regular study sessions at divisions and Group Companies that handle personal data. During such events, we share information about in business and legal systems trends, and examine the ideal state of privacy protection.

Aiming to provide services that customers can use with peace of mind

Privacy protection is important utilizing personal data made available by advanced technologies. Hitachi contributes to achieving a super smart society by providing services that customers can use safely. To do this, we use our expertise generated from knowledge gained through surveys, through understanding the trends in legal systems and technologies, and through handling of actual cases.

Information security products and services initiatives

Information security human resources development initiatives

Hitachi Group has trained highly-skilled security human resources and human resources who can bridge security technologies to customers, by evaluating security related skills and careers, by conducting technical training and management education so that customers can securely use products and services.

Overview of information security human resources development activities

Due to intensifying cyber attacks on social infrastructure, Hitachi Group ① scouts and evaluates, ② develops and utilizes, ③ shares and links the security human resources who can handle these attacks, and promotes activities for developing information security human resources, thereby contributing to ensuring the security of the social infrastructure.

Through these activities, we focus on the following persons as information security human resources: highly-skilled specialists in information security, and also IT engineers involved in the development and operation of systems on-site, and on internal IT users.

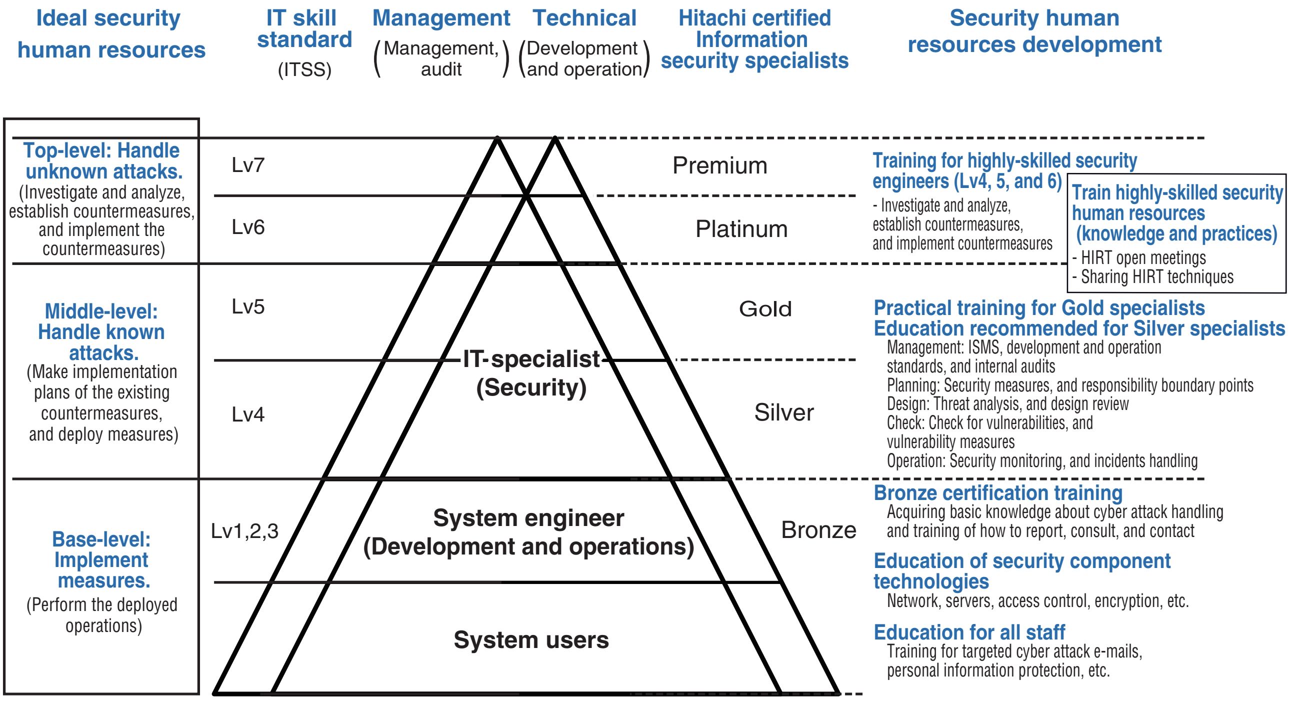
These activities are based on ITSS (Information Technology Skill Standard), which is defined by the Ministry of Economy, Trade and Industry and which clarifies and systematizes IT-related capabilities. We categorize the ideal human resources who systematically handle cyber attacks into the following three classes. In addition, we are providing education broadly from training highly-skilled security human resources to acquiring basic knowledge about cyber attack handling and reporting, discussing, and communicating.

① Highly-skilled security human resources
Top-level human resources who can investigate and analyze unknown attacks and establish and implement countermeasures against them and guide the middle-level or base level human resources.

② Security human resources who organize system development and operation:
Middle-level human resources who can make plans to implement existing countermeasures against known attacks, and who can deploy measures in the development and operation of information systems.

③ Human resources who implement deployed security measures:
Base-level human resources who investigate the systems they are responsible for, and who implement measures based on alerts issued by the top-level human resources and on instructions from the middle-level human resources.

Information security human resources development activities >>


Ideal security human resources
IT skill standard (ITSS)
Management (Management, audit)
Technical (Development and operation)
Hitachi certified Information security specialists
Security human resources development
Top-level: Handle unknown attacks.
(Investigate and analyze, establish countermeasures, and implement the countermeasures)
Middle-level: Handle known attacks.
(Make implementation plans of the existing countermeasures, and deploy measures)
Base-level: Implement measures.
(Perform the deployed operations)
Lv7
Lv6
Lv5
Lv4
Lv1,2,3
IT-specialist (Security)
System engineer (Development and operations)
System users
Premium
Platinum
Gold
Silver
Bronze
Training for highly-skilled security engineers (Lv4, 5, and 6)
- Investigate and analyze, establish countermeasures, and implement countermeasures
Train highly-skilled security human resources (knowledge and practices)
- HIRT open meetings
- Sharing HIRT techniques
Practical training for Gold specialists
Education recommended for Silver specialists
Management: ISMS, development and operation standards, and internal audits
Planning: Security measures, and responsibility boundary points
Design: Threat analysis, and design review
Check: Check for vulnerabilities, and vulnerability measures
Operation: Security monitoring, and incidents handling
Bronze certification training
Acquiring basic knowledge about cyber attack handling and training of how to report, consult, and contact
Education of security component technologies
Network, servers, access control, encryption, etc.
Education for all staff
Training for targeted cyber attack e-mails, personal information protection, etc.

HIRT: Hitachi Incident Response Team

Information security products and services initiatives

Scouting and evaluating of information security human resources

Hitachi Group has established the category of “Hitachi Certified IT Professional” , which conforms to the company certification system, which has been based on the system for Certified IT Professionals of the Information Processing Society of Japan since August, 2014. Hitachi Group started scouting and evaluating information security human resources.

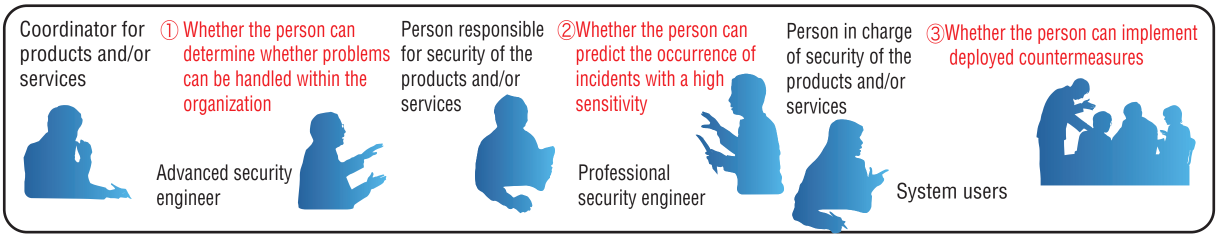
This certification system defines certification criteria that include whether public qualifications are held, actual experience in the Hitachi Group, and contribution to society (public relation activity), and evaluates the skills and careers by using four levels (Premium, Platinum, Gold, and Silver). Hitachi Group examines certifications with the goal of having 1,000 certified persons by 2020.

In addition, the new certification level "Bronze" has been been established in HISSP from May 2017. This promotes the certification and development of human resources who can implement deployed security countermeasures, and have undergone training to experience screen changes related to cyber attacks, and have undergone training in how to report, communicate, and discuss.

■Points focused on in the examination (requirements for information security specialist certification of the CIP system)

√ Whether the person has the identity, originality, and productivity as a professional.

√ Whether the person has the skills and career with which he or she can act voluntarily and efficiently with a sense of responsibility when developing security or handling incidents.



Coordinator for products and/or services

① Whether the person can determine whether problems can be handled within the organization

Advanced security engineer

Person responsible for security of the products and/or services

②Whether the person can predict the occurrence of incidents with a high sensitivity

Professional security engineer

Person in charge of security of the products and/or services

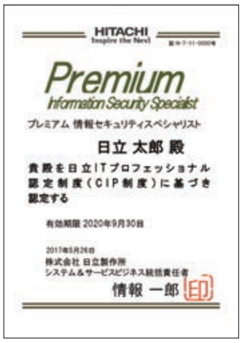
③Whether the person can implement deployed countermeasures

System users

■Certification levels (HISSP classes)

[Premium]

Information security engineer who Hitachi is proud of



HITACHI
Inspire the Next

Premium
Information Security Specialist
プレミアム 情報セキュリティスペシャリスト

日立 太郎 殿

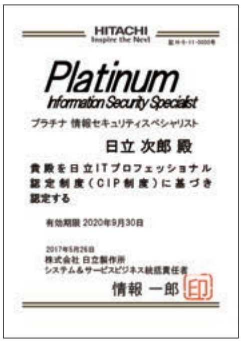
貴殿を日立ITプロフェッショナル
認定制度（CIP制度）に基づき
認定する

有効期限 2020年9月30日

2017年5月26日
株式会社 日立製作所
システム＆サービスビジネス統括責任者
情報 一郎 印

[Platinum]

Information security engineer who represents the information communication field



HITACHI
Inspire the Next

Platinum
Information Security Specialist
プラチナ 情報セキュリティスペシャリスト

日立 次郎 殿

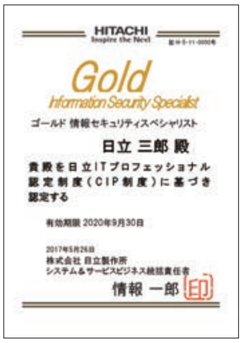
貴殿を日立ITプロフェッショナル
認定制度（CIP制度）に基づき
認定する

有効期限 2020年9月30日

2017年5月26日
株式会社 日立製作所
システム＆サービスビジネス統括責任者
情報 一郎 印

[Gold]

Information security engineer who represents the business or organization



HITACHI
Inspire the Next

Gold
Information Security Specialist
ゴールド 情報セキュリティスペシャリスト

日立 三郎 殿

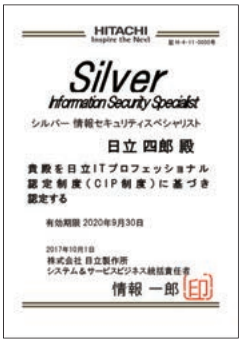
貴殿を日立ITプロフェッショナル
認定制度（CIP制度）に基づき
認定する

有効期限 2020年9月30日

2017年5月26日
株式会社 日立製作所
システム＆サービスビジネス統括責任者
情報 一郎 印

[Silver]

Information technology engineer who is responsible for the information security of each project



HITACHI
Inspire the Next

Silver
Information Security Specialist
シルバー 情報セキュリティスペシャリスト

日立 四郎 殿

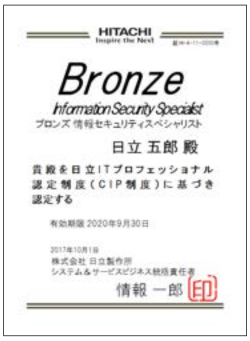
貴殿を日立ITプロフェッショナル
認定制度（CIP制度）に基づき
認定する

有効期限 2020年9月30日

2017年10月1日
株式会社 日立製作所
システム＆サービスビジネス統括責任者
情報 一郎 印

[Bronze]

Person who is in charge of implementing security countermeasures for the systems being used



HITACHI
Inspire the Next

Bronze
Information Security Specialist
ブロンズ 情報セキュリティスペシャリスト

日立 五郎 殿

貴殿を日立ITプロフェッショナル
認定制度（CIP制度）に基づき
認定する

有効期限 2020年9月30日

2017年10月1日
株式会社 日立製作所
システム＆サービスビジネス統括責任者
情報 一郎 印

Physical security products and services initiatives

Initiatives to enhance security for physical security products and services

Hitachi offers ① video surveillance systems, ② video analysis systems, ③ room access control systems, and ④ remote surveillance and support systems. The systems can scale from an office or building, to multiple locations and broad areas. To help resolve business and management issues of customers, Hitachi is also working to enhance physical security solutions for monitoring and controlling the flow of movement of people, and information.

Background of physical security enhancement

(1) Information security and physical security

The digitalization of corporate and customer information is moving forward with the spread of IT and the advancement of IoT technologies, and there is increased risk of information leaks associated with the networking of operational systems.

It is necessary to enhance information security in order to decrease these risks.

As part of this, there is also an increased necessity for physical security, such as entrance restrictions to rooms where information is being stored, surveillance of internal images of important facilities, and access management for lockers, safes and other locations.

It is important to designate the appropriate security level upon clarifying the place and items to be protected, and to construct a system that corresponds to that level, when implementing physical security.

(2) Requirements for physical security for offices and buildings

Physical security systems for offices and buildings consist of access control systems, which manage entrance/exit to buildings and rooms, and video surveillance systems, which monitor each area and the flow of people who enter and exit offices and buildings.

It is important to combine access control systems with individual verification technology like IC cards or finger vein verification corresponding to the security level necessary for each area in an office or building.

Coordination with information management systems, which use authentication results in the access management of PC and work systems and for authentication when printing documents, as well as the coordination with facilities management systems, like restricting the destination floor of an elevator based on authentication results, are also requirements.

In recent years, initiatives to use less energy have also become important in addition to physical security objectives: for example, controlling air condition and lighting by linking video monitoring systems and access control systems with facility management systems.

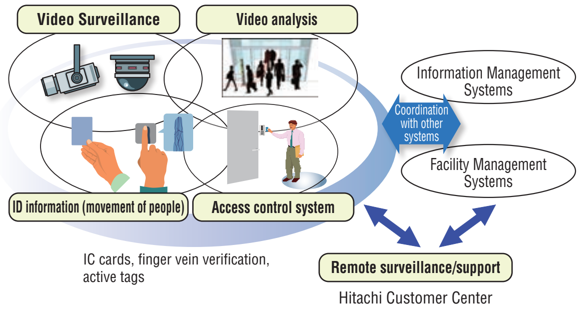
Furthermore, there is also a need for companies that have multiple operations bases to standardize security levels across each location, and provide central management from a supervisory department.

(3) Requirements for physical security in multiple sites and over wide areas

For the physical security of facilities that span multiple sites or a large area (such as power generation facilities, airports, factories, and railways), it is important to implement overall monitoring of dynamic states (flow and statuses) of both persons and things, by using multiple devices, such as surveillance cameras, devices to manage entry to or exit from facilities, and IoT sensors. Such devices must be installed in multiple locations, such as on the periphery of an area, within an area, in vehicles, and in buildings.

Also, massive amounts of information about dynamic states are obtained when monitoring multiple sites or large areas. Therefore, it is important to reduce monitoring tasks by summarizing the information from multiple devices and from multiple sites, and by automating such monitoring. These approaches will also reduce the amount of needed network bandwidth and the amount of needed image-storage capacity. This summarization and automation can be achieved by methods such as using camera image analysis to automatically detect suspicious persons and suspicious objects.

Physical security solutions for monitoring and controlling the flow of movement of people and information


Video Surveillance
Video analysis
Information Management Systems
Coordination with other systems
Facility Management Systems
ID information (movement of people)
Access control system
IC cards, finger vein verification, active tags
Remote surveillance/support
Hitachi Customer Center

Centrally monitoring the flow of movement of people, and information, and resolving management issues
(Integrated physical security platform)

Physical security products and services initiatives

Security enhancement- concept and products/services

In order to assure physical security, it is necessary to construct systems to monitor and control the flow of movement of people and information, and to help resolve customers' operation and management issues. To do this, we need to appropriately combine video surveillance systems, video analysis systems, and access control systems with individual verification and ID information management technology. Where necessary, we plan coordinated operation with information and facility management systems. Based on these ideas, we provide solutions utilizing the products and services with the features below, and utilizing an integrated physical security platform.

(1) Video surveillance

In recent years, networked cameras that utilize IP networks have become increasingly common. We provide video surveillance systems with low installation cost and high performance. High-resolution technology developed by Hitachi is used for the network cameras installed at each location. This technology allows high-quality images to be compressed to 1/3 to 2/3 their original size, and reduces the loads on the storage devices for recorders and video servers, as well as on network bandwidth. Furthermore, we offer integrated video-management systems that can centrally manage live footage and can play back video from multiple locations.

(2) Video analysis

The flow of movement of people can be made visible by analyzing camera images. We are progressing with the automation of surveillance operations: for example, to count the number of people in camera images, and to detect a person entering a specified area and classify the situation as an intrusion. Different video analysis processing can be assigned to different cameras installed in different locations, which is useful for analyzing situations, detecting suspicious persons and objects, and detecting abnormal behavior.

(3) Access control

To offer an access control system appropriate to the operating environment, it is necessary to combine different technologies: such as various types of non-contact IC cards, finger vein technology to assure robust security, and active tags that enable wireless verification of individuals. For those companies that manage multiple locations, a unified security policy can bring flexibility to permission settings: for example, a single card having access to all locations but restricting entrance and exit to rooms according to the location or department. Designated persons can easily operate these settings from an internet browser, which makes it easier to implement and operate the systems. Furthermore, because these services can be provided via a cloud without setting up a server at each location, small and medium sized locations benefit from the simple implementation. Linkages with information management systems and facility management systems can enable both enhanced security and controls for energy savings.

(4) Remote surveillance/support structures

Customer service centers and call centers are connected to the service networks at sites across the country. With an organizational structure that enables constant (24 hours a day, 365 days a year) monitoring, the structure supports customers' security-related systems by ensuring safe operation and providing emergency responses.

(5) Integrated physical security platform

Hitachi provides solutions utilizing a integrated physical security platform to centrally monitor movement of people information and resolve customers' operational and managerial issues.

This platform enables central monitoring of on-site data collected and accumulated by means of various physical security systems, such as by surveillance cameras in access control systems, and by IoT sensors. In addition, however, the platform can also analyze and utilize such data to develop solutions that provide and control information to improve operational and managerial issues of customers.

For example, in factories and distribution sites, the platform can increase productivity by detecting deviations from normal operations from camera images of line operations, and by issuing instructions to correct such deviations. In commercial facilities, the platform contributes to sales increases by suggesting changes in products types and layouts through the analysis of gender, age, and buying behavior of people in camera images. Furthermore, Hitachi can provide even advanced solutions by using business intelligence tools and artificial intelligence to analyze big data collected from various physical security systems, IoT sensors, and camera images.

With these types of features, our physical security products and services enhance total solutions that resolve customers' operational and management issues and that protect assets, safety, and security. The solutions can scale from an office or building, to multiple locations and broad areas.

Control products and systems initiatives

Initiatives to ensure information security in control products and systems

Connection and coordination of control systems that support important infrastructure with information communications systems has moved forwards recent years, and information security risks starting with cyber attacks are heightened. Systems even more secure than present systems and rigorous management of customer confidential information is necessary for the uninterrupted and safe system management. The Control System Platform Division of Hitachi, Ltd. is working on solutions for these types of problems.

Background and goals

Information control systems, which form the center of control systems that make up the base of social infrastructure, must operate on a 24-hour basis as prerequisite, with a high level of reliability.

Information security is related to safety, and the uninterrupted and safe operation of information control systems is possible through the appropriate management, maintenance, and operation of information assets. In particular, the confidentiality of customer-related information must be maintained completely.

In order to fulfil these demands, information control systems maintain information security against threats from the outside, in principal by physically blocking other systems.

At the same time, under the national IT strategy of “a society in which anybody can freely access information” , measures such as “information cooperation infrastructure development” have been implemented.

Security threats relating to information control systems are diversifying in this environment of change, and the role of information security technology will become increasingly bigger in from now.

There are many instances in which important customer information is incorporated for system development, and these sorts of information leaks are a direct threat to social infrastructure.

The initiatives of the Control System Platform Division concerning these issues are stated below.

Management of customer confidential information and organization of development processes

●Establishment of Information Security Management System (ISMS)

The Control System Platform Division provides information control system solutions that support social infrastructure and the foundation of industry (such as electricity, traffic, steel, water, industry, and power electronics), and these require organizational information security management.

Maintenance of confidentiality for customer information and results configured from that information are of particular importance.

To respond to these demands, the Control System Platform Division constructed an ISMS based on the International Standards Information Security Management System (ISMS) (ISO/IEC 27001: 2005) under the direction of top management. In January 2010, the division completed acquisition of certification.

From now, ISMS certification will continue to be maintained while the fields to which it can be applied are expanded.

Currently, the Control System Platform Division is in the process of amending its ISMS according to the ISMS International Standards amendment (ISO/IEC 27001: 2013).

●Formation of security aware product development processes

The following development processes were formulated in 2005, and have been applied to system development.

(1) Evaluate security risk at the beginning of the development process.

(2) Verify security risk settings in the design review stage (protection settings, countermeasure policies).

(3) Confirm security requirements with a security verification tool or similar before shipping from plants and before handing over to customer.

However, security risk for control systems is increasing, and with corresponding trends like “acceleration of international standards and certification” and “customer demand for control vendors to acquire security verification” , the environment surrounding control systems is constantly changing.

The Control System Platform Division has responded to this situation by cooperating with domestic and international organizations like the Control System Security Center which commenced in 2012.

Regarding strategies for international standards, requirements for standards for different domains like the IEC 62443, NERC CIP (North American electric standards), and WIB (European industrial standards) have been investigated, and conditions requiring strict adherence have been formulated as security standards, and turned into guidelines.

Control products and systems initiatives

Control systems security

●Control-system security risks and government initiatives

Control systems are evolving each day and are being used more efficiently because control systems are operating over broad areas, business suppliers are collaborating in the use of control systems, and the application of IoT technologies to control systems has started.

On the other hand, cyber attacks, such as targeted attacks, have become more sophisticated and diversified. Control systems have came under cyber attacks, and security risks have appeared.

The Japanese government takes initiatives centering on NISC (National center of Incident readiness and Strategy for Cybersecurity), in cooperation with the Cabinet Office and each governmental ministry and agency.

For example, the Basic Act on Cybersecurity came into force in November 2015. Also, the Cybersecurity Management Guidelines were formulated by Japan's Ministry of Economy, Trade and Industry in December 2015 to advance the handling of security threats caused by cyber attacks.

●Hitachi's approach to security

It is important to apply countermeasures to protect control systems against security risks, but that alone is insufficient. Cyber attack methods advance every day, so systems need to be continuously improved even after security measures are applied. Furthermore, it is also vital to establish organizational structures so that, if a security incident occurs, the organization can promptly identify the problem, take countermeasures, and recover from the problem.

Hitachi, Ltd. has established the approach of "Protect by systems. Protect by organizations. Protect by operations." and has been working to implement this approach under the idea of H-ARC®. H-ARC® is an approach to protect control systems based on security platform products (H: Hardening). For "Protect by systems", H-ARC® takes an adaptive (A: Adaptive) approach to implement countermeasures in advance and to prevent unknown threats. For "Protect by operations", H-ARC® emphasizes responsiveness (R: Response) and strives to minimizes damage after an attack and shorten recovery time. For "Protect by organizations", H-ARC® supports cooperation (C: Cooperative) among different organizations and business suppliers through security operation management services.

●Security platform products

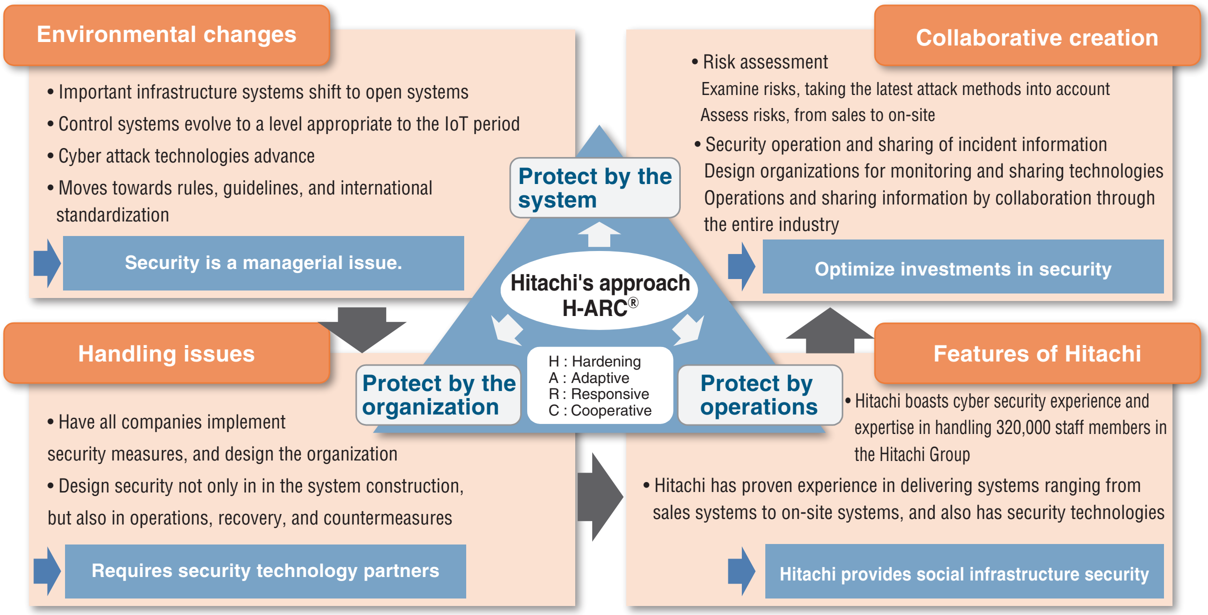
As security platform products, we provide products related both to the cyber and physical aspects. For cyber security, for example, we provide one-way relay systems that can protect control systems by physically shutting out unauthorized access from outside to prevent unauthorized intrusions in cyber space.

For physical security, we provide entrance/exit management systems that utilize finger vein verification. We also provide an integrated explosives detection system within gates.

●Security operation management service

Even after security measures are implemented to protect them, control systems must be continuously monitored. It must be possible to design appropriate security operations, to detect security threats at an early stage, to respond quickly. To enable these, it is essential to collect information from control systems in a timely manner, to effectively analyze the information, and to quickly develop and implement proper countermeasures.

Hitachi, Ltd. has established a Security Operation Center (SOC) that performs these tasks, provides services such as support for actual operation, provides analysis support from specialists who have SOC operation expertise in their companies, and provides training related to development of human resources who handle security threats.



Environmental changes

- Important infrastructure systems shift to open systems
- Control systems evolve to a level appropriate to the IoT period
- Cyber attack technologies advance
- Moves towards rules, guidelines, and international standardization

Security is a managerial issue.

Collaborative creation

- Risk assessment
  Examine risks, taking the latest attack methods into account
  Assess risks, from sales to on-site
- Security operation and sharing of incident information
  Design organizations for monitoring and sharing technologies
  Operations and sharing information by collaboration through the entire industry

Optimize investments in security

Handling issues

- Have all companies implement security measures, and design the organization
- Design security not only in in the system construction, but also in operations, recovery, and countermeasures

Requires security technology partners

Features of Hitachi

- Hitachi boasts cyber security experience and expertise in handling 320,000 staff members in the Hitachi Group
- Hitachi has proven experience in delivering systems ranging from sales systems to on-site systems, and also has security technologies

Hitachi provides social infrastructure security

Research and development supporting product and service security

Security research and development for a safe, secure and comfortable society

Security technology that can handle ever-changing risks is necessary for the realization of more advanced social infrastructure systems which utilize information and communication technology. We provide the world with products and services that are both reliable and secure, as well as convenient, and are also researching and developing cutting edge security technology in order to achieve a society in which people can live with peace of mind.

Security research and development initiatives

Along with the normalization, development and usage expansion of information and communications technology, security is being applied to various business domains as a standard technology.

Hitachi is aware that security technology is vital to social infrastructure systems and corporate information systems, and has been researching and developing approaches that protect systems with prior security designing since the 1980s, with the three pillars of “cryptography” , “authentication” , and “assessment” .

However, in recent years many problems have become a reality that cannot be addressed with security design alone.

Examples of these problems include more sophisticated cyber attacks represented by targeted cyber attacks, new software component vulnerabilities being discovered on a daily basis, the rapid increase in internet banking fraud victims, the issue of anonymizing information and protecting privacy when utilizing big data, and protecting IoT field devices.

A new approach is necessary to deal with these sorts of new issues in addition to conventional technology, achieve both effective and accurate responses after an attack, and to balance concealing and analyzing.

Hitachi is researching and developing the world’ s most advanced security technology which can respond to a variety of threats which are getting more sophisticated on a daily basis, aware that it is Hitachi’ s responsibility to be the leader in social infrastructure business, in order to achieve a safe society in which people can live with secure and comfortable lives.

Development of technology to process secret information

Cloud services have been gaining a considerable attention in recent years, yet there is a lot of user anxiety regarding cloud security, and users avoid business change to handle highly sensitive data on the cloud.

The risk of information being leaked to a third party including administrators on the cloud manager has become a problem, as even if the sensitive data is stored in the cloud as an encrypted state, information must be temporarily decrypted to search for or check information on the cloud.

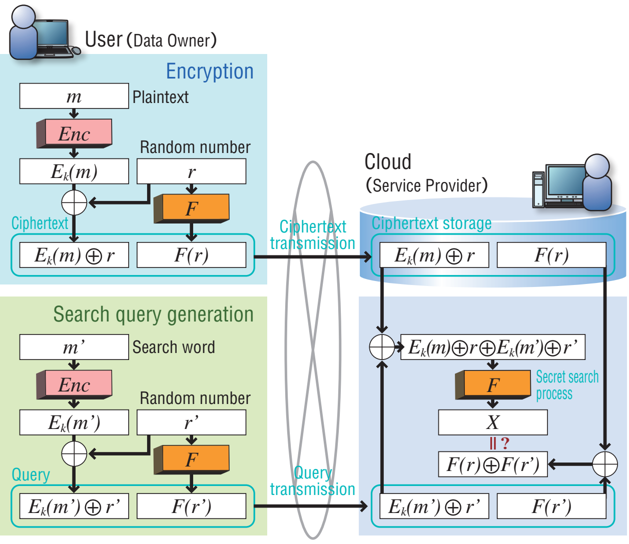
Hitachi has developed searchable encryption technology, which allows information to be searched while still encrypted in the cloud, and searching even large amounts of data while maintaining a high level of security is now possible.

Conventional encryption methods had safety concerns. If the same information was encrypted multiple times, there would be a one-to-one relationship with the encrypted text. With this new technology, random numbers that change every time are applied so even if the same data is searched for, it will be turned into completely different ciphertext, increasing randomization.

Additionally, by using symmetric key algorithms which make high speed processing possible, large amounts of data can be searched effectively by minimizing encryption processing overheads.

This technology was applied to the Remudy WEB patient information registration system, developed jointly by the National Center of Neurology and Psychiatry and Hitachi Solutions Ltd. in 2014, and became the world's first practically implemented technology for processing secret information. Furthermore, in 2015, this technology was also applied to the "My Number secure management system" and the "Credeon Secure Full-text Search" developed by Hitachi Solutions. We will promote the commercialization of this technology as a versatile solution to improving cloud security.

Searchable encryption data flow >>



Research and development supporting product and service security

Development of security risk assessment technology for handling of disclosed critical vulnerabilities

Disclosures of vulnerability information, records of security defects in software and other products, are increasing every year, with approximately 8,000 cases of vulnerability information disclosure in 2014 according to public authority for IT security (like NIST in the USA).

Of these, Heartbleed, a vulnerability in OpenSSL, attracted a high amount of interest, as directly after its disclosure there was a sharp rise in attacks targeted at that vulnerability, and it became necessary for System administration division in corporate to respond in a prompt manner.

In these sorts of situations, identification or urgency of vulnerabilities that require a response becomes necessary, demanding a high level of information security skills.

However, it is difficult for each organization to secure and develop these sorts of specialists.

This is why at Hitachi, we have developed technology that will analyze cyber threat penetration routes and order vulnerabilities that require a response on a priority basis, as well as identify system vulnerabilities in a prompt manner.

This technology can automatically identify the existence of vulnerabilities by comparing software information obtained from equipment and disclosed vulnerability information.

Furthermore, the level of each vulnerability risk in a system is dependent on the likelihood and ease of a cyber attack reaching equipment with a vulnerability, and the degree of impact.

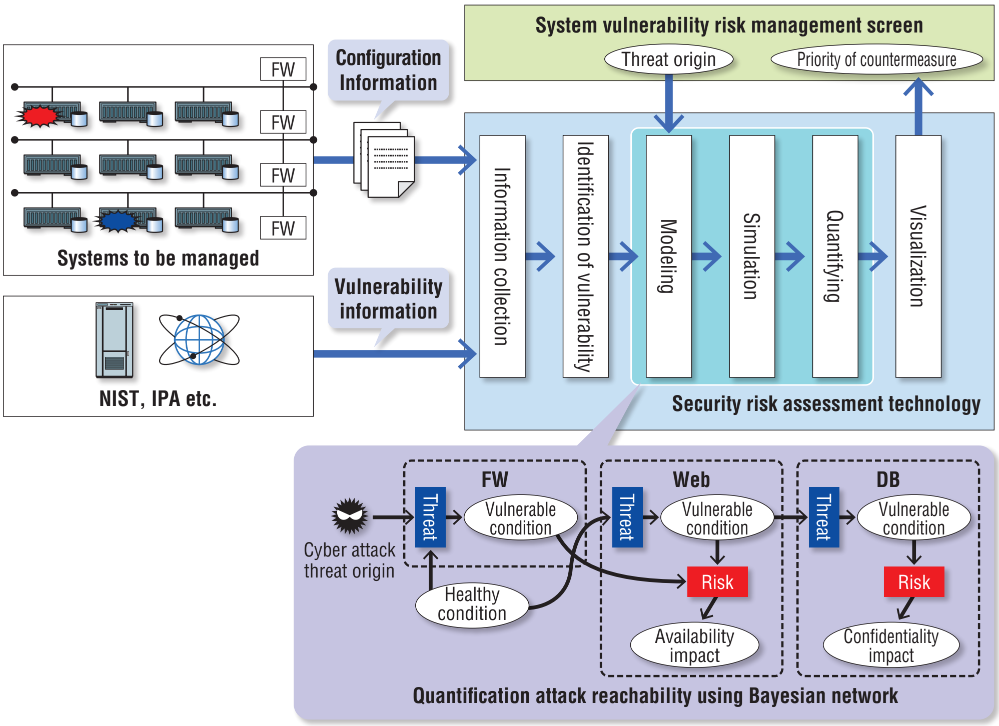
In order for this to happen, the technology automatically analyzes how likely it is that a cyber attack will reach its target from network configuration and other information, and extracts possible penetration routes for each system in a comprehensive manner.

Additionally, the penetration probability for each route and degree of impact for each vulnerability is calculated using Bayesian network technology.

With this technology, it is possible to automatically prioritize vulnerability countermeasures that require a high level of information security skills, meaning customers can expect uniform and prompt handling of vulnerabilities.

By introducing this technology to organization information system divisions and CSIRTs (computer security incident response teams) workloads associated with vulnerability measures can be significantly reduced, and organizations without a specialist will be able to easily prioritize countermeasures, meaning this technology will be useful for operating security efficiently.

Overview of security assessment technology based on attack route simulation >>



Research and development supporting product and service security

Development of self-evolving security operation technology

Recently, the importance of 24-hour security operation has been increasing due to intensified cyber attacks.

To perform security operations, operators with advanced specialist knowledge are required. However, the numbers of such human resources are insufficient.

So, Hitachi has been developing “self-evolving security operation technology” , which performs security operations efficiently.

One of the security operations is to detect and block unauthorized communications.

Until now, we have registered communications determined as dangerous in a blacklist and blocked communications that match the blacklist.

However, registering all doubtful communications in a blacklist might stop the carrying out of the originally intended work.

For this reason, in situations in which incidents such as unauthorized communications might occur, both of the following reduction actions are required: “risk reduction” in which you instantly handle the incident to suppress occurrence of risks, and “reduction of the impact on work” in which you minimize the negative impact on work.

The technology that solves these issues is “self-evolving security operation technology” .

This technology does not stop all doubtful communications but registers them in a graylist and temporarily keeps them on hold.

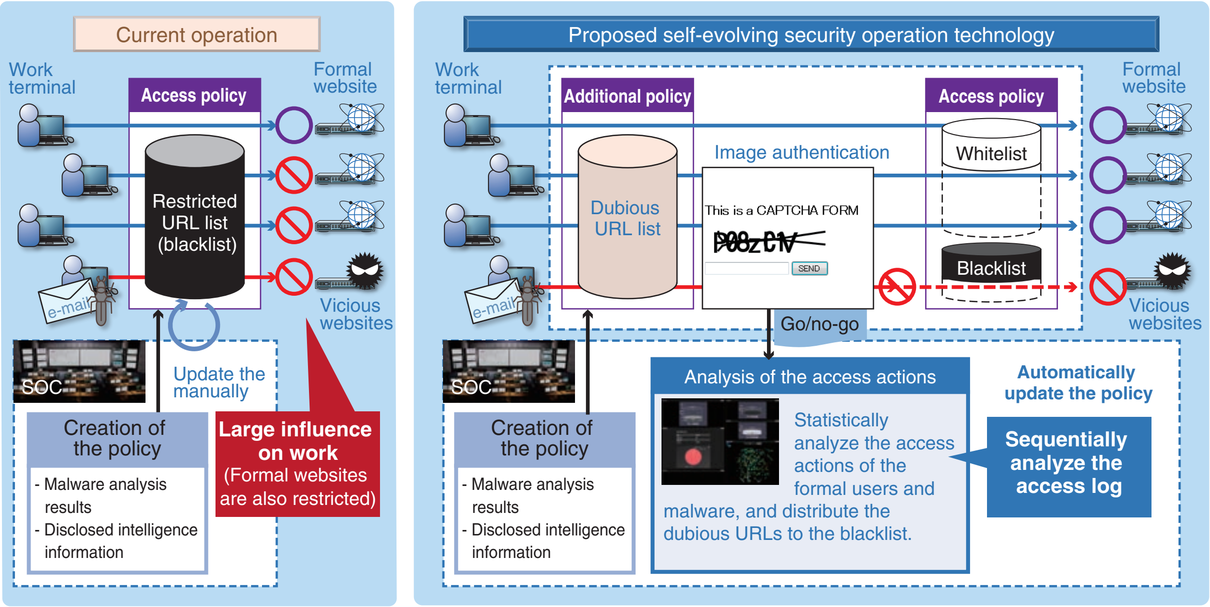
Then, when an employee or malware tries to access a website in the graylist, the technology performs a Turing Test to determine whether the access is from a human being or program.

If a certain number of employees succeed in the above test, the technology considers the website to be safe and automatically moves the website from the graylist to the whitelist.

In addition, if the above test fails a certain number times, the technology considers the website to be accessed from malware, and distributes the website to the blacklist.

As described above, due to the system that statistically analyzes the authentication results of employees to enable the access policy to self-evolve, we can expect a positive network effect in which the accuracy is improved as the number of users increases.

Overview of self-evolving security operation technology >>


Current operation
Work terminal
Access policy
Formal website
Restricted URL list (blacklist)
e-mail
Vicious websites
SOC
Update the manually
Creation of the policy
- Malware analysis results
- Disclosed intelligence information
Large influence on work
(Formal websites are also restricted)
Proposed self-evolving security operation technology
Work terminal
Additional policy
Dubious URL list
Image authentication
This is a CAPTCHA FORM
SEND
Access policy
Whitelist
Blacklist
Formal website
Vicious websites
e-mail
Go/no-go
SOC
Creation of the policy
- Malware analysis results
- Disclosed intelligence information
Analysis of the access actions
Statistically analyze the access actions of the formal users and malware, and distribute the dubious URLs to the blacklist.
Automatically update the policy
Sequentially analyze the access log

Research and development supporting product and service security

Development of PBI technology that achieves a safe, secure and convenient individual verification service

Damage from information leaks, unauthorized handling and other sources due to unauthorized access has increased sharply with the expansion of cloud services, electronic funds transfers, national ID and more, and reliable user verification is in demand.

Expectations about biometrics as a reliable and convenient verification method that can replace passwords are heightened, but use of this method is not widespread because of concerns about privacy.

As biometric information, for example fingerprints or veins, cannot be replaced, it was necessary to protect and manage biometric registration information (templates) in a robust manner, and common use between multiple services was not possible.

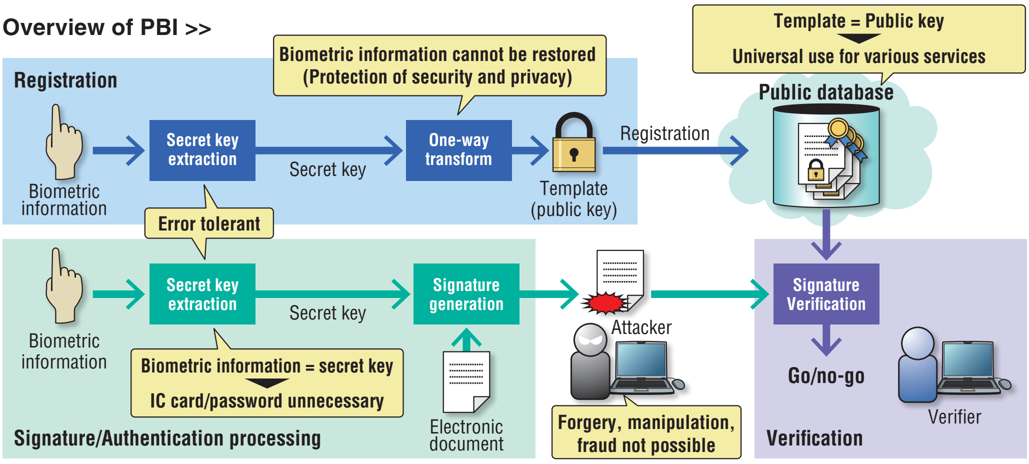
Against this background, Hitachi has developed PBI (Public Biometrics Infrastructure) technology that will safely achieve template sharing between multiple services while protecting privacy in a robust manner, by enabling the registration and verification of biometric information in its converted irreversible form.

With this technology, the user can access various services safely and securely, hands-free and without password, just by registering their biometric information one time

PBI technology can also achieve digital signatures and public key encryption, which is the "secret key" to biometric information.

Because of this, public-key infrastructure (PKI) that supports safety in electronic funds transfer and electronic government services will be able to be achieved with biometric information in a safe and convenient manner, without the need to rely on IC cards or passwords.

Overview of PBI >>



Company-external information security related activities

Hitachi leverages the skills and experiences of each of its staff members to achieve a more secure information technology based society through participating in different types of security related company-external activities.

International standardization activities

Hitachi participates in the following activities relating to international standardization.

●ISO/IEC JTC1/SC27

Subcommittee SC27 of the joint technical committee ISO/IEC JTC1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), formed to internationalize standards, is investigating the standardization of information security management systems (WG 1), cryptography and security mechanisms (WG 2), security assessment technology (WG 3), security controls and services (WG 4), and identity management and privacy technologies (WG 5).

●ISO TC292

The International Organization for Standardization (ISO) technical committee (TC) 292 is investigating the standardization of the security field including general security management, business continuity management, resilience and emergency management, fraud prevention countermeasures and management, security services, and homeland security.

●ISO TC262

Under the theme of risk management, the International Organization for Standardization (ISO) technical committee (TC) 262 is investigating the standardization of items such as terms, principles, policies, and risk assessment techniques, for all risks.

●ITU-T SG17

SG17, one of the study groups (SGs) of the International Telecommunication Union-Telecommunication Standardization Sector of the International Telecommunication Union, is investigating the standardization of cyber security, security management for communications vendors, telebiometrics, of security capabilities for communications and applications services, spam countermeasures, and identity management.

●IEC TC65/WG10, WG20

Technical committee TC 65 of the International Electrotechnical Commission (IEC) is promoting the standardization of industrial automation, monitoring, and control.TC 65/WG 10 is investigating the formulation of standards regarding the security of networks and control devices in control systems. In addition, TC 65/WG 20 is investigating the formulation of standards regarding both security and safety of functions in control systems.

●OASIS CTI

Cyber Threat Intelligence (CTI) of the Organization for the Advancement of Structured Information Standards (OASIS) is investigating the formulation of standards regarding Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII), which will enable relevant personnel to describe cyber-attack activities and to exchange such information.

Participation in FIRST (Forum of Incident Response and Security Teams)

FIRST is an international community of worldwide computer incident response teams bound together by a relationship of trust.

Presently more than 369 teams are participating, from more than 80 countries.

Hitachi' s HIRT (Hitachi Incident Response Team) is also a member.

Other activities

Hitachi is also participating in a variety of security related activities like the ones listed below, including research, investigation and promulgation, and enlightenment activities.

- Information-technology Promotion Agency, Japan (IPA)
  Contributing author to "10 Major Security Threats Committee", and more
- The JIPDEC Conformity Assessment Scheme
  ISMS(Information Security Management System) expert committee,
  CSMS (Cyber Security Management System) technical committee
- ICT-ISAC Japan
- Council of Anti-Phishing Japan
- Nippon CSIRT Association
- Japan Information Security Audit Association (JASA)
- Japan ISMS User Group
- Japan Electric Measuring Instruments Manufacturers' Association (JEMIMA) Process automation and factory automation measurement control committee security survey and research WG
- Control System Security Center (CSSC)
- Industrial Internet Consortium Security Working Group
- United States Department of Homeland Security (DHS) AIS (Automated Indicator Sharing)

Third party assessment and certification

Hitachi promotes the acquisition of third party assessments and certifications relating to personal information protection, information security management, and products.

Privacy Mark entities

The following companies have permission to use the Privacy Mark, acquired by Hitachi from JIPDEC (as of May 31, 2017).

Hitachi, Ltd.
Hitachi, Ltd. Corporate Hospital Group
Hitachi Business International, Ltd.
Hitachi Consulting Co., Ltd.
Hitachi Document Printing Co., Ltd.
Hitachi Document Solutions Co., Ltd.
Hitachi Foods & Logistics Systems Inc.
Hitachi Government & Public Sector Systems, Ltd.
Hitachi High-Tech Solutions Corporation
Hitachi Hi-System21 Co., Ltd.
Hitachi ICT Business Services, Ltd.
Hitachi Industry & Control Solutions, Ltd.
Hitachi Information Academy Co., Ltd.
Hitachi Information & Telecommunication Engineering, Ltd.
Hitachi Information Engineering, Ltd.
Hitachi INS Software, Ltd.1997,
Hitachi Inspharma, Ltd.
Hitachi Insurance Services, Ltd.
Hitachi-kenpo
Hitachi KE Systems, Ltd.
Hitachi Management Partner Corp.
Hitachi Medical Computer Systems, inc.
Hitachi-Omron Terminal Solutions, Corp
Hitachi Power Solutions Co., Ltd.
Hitachi Research Institute
Hitachi Softec Co.,Ltd.
Hitachi Solutions, Ltd.
Hitachi Solutions Create, Ltd.
Hitachi Solutions East Japan, Ltd.
Hitachi Solutions Service, Ltd.
Hitachi Solutions West Japan, Ltd.
Hitachi Systems, Ltd.
Hitachi Systems Engineering Services, Ltd.
Hitachi Systems Networks, Ltd.
Hitachi Systems Power Services, Ltd.
Hitachi Systems Techno Services, Ltd.
Hitachi Technical Communications Co., Ltd.
Hitachi SC, Ltd.
Hitachi Techno-Information Services, Ltd.
Hitachi Urban Support, Ltd.
Hokkaido Hitachi Systems, Ltd.
Kokusai Electric Techno Service Co., Ltd.
Kyushu Hitachi Systems, Ltd.
Okinawa Hitachi Network Systems, Ltd.
SecureBrain Corporation
Shikoku Hitachi Systems, Ltd.
Tokyo Eco Recycle Co., Ltd.

ISMS Certification

The following companies or organizations within companies at Hitachi have obtained ISMS certification from JIPDEC based on the international standard for information security management system ISO/IEC 27001 (as of April 30, 2017)

Hitachi, Ltd. (Financial Information Systems Division, Government & Public Corporation Information Systems Division)
Hitachi, Ltd. (Government, Public Corporation & Social Infrastructure Business Unit, Government & Public Corporation Information Systems Division)
Hitachi, Ltd. (Information & Communication Technology Business Division, Smart Information Systems Division, Healthcare, Insurer Business Solutions Department, Medical Information Solutions Department, and Healthcare IT Services Department)
Hitachi, Ltd. (Information & Communication Technology Business Division, Social Infrastructure Information Systems Division)
Hitachi, Ltd. (IoT & Cloud Service Business Division)
Hitachi, Ltd. (Services & Platforms Business Unit, Control System Platform Division)
Hitachi, Ltd. Defense Systems Bisiness Unit (Yokohama Branch Office/Ikebukuro Branch Office) and Hitachi Advanced Systems Corporation (Headquarters)
ALAXALA Networks Corporation
Hitachi Capital Services Co., Ltd.(CS Tokyo Product Center)
Hitachi Government & Public Sector Systems, Ltd.
Hitachi High-Tech Solutions Corporation (Solution Center)
Hitachi ICT Business Services, Ltd. (Media Solution Department Media Service Group)
Hitachi INS Software, Ltd.
Hitachi KE Systems, Ltd. (Tokyo Development Center)
Hitachi Kokusai Electric Inc. (Tokyo Works)
Hitachi Kokusai Yagi Solutions Inc.（Solution Division）
Hitachi Management Partner Corp.
Hitachi-Omron Terminal Solutions, Corp
Hitachi Pharma Evolutions, Ltd.
Hitachi Power Solutions Co., Ltd.
Hitachi SC, Ltd. (Headquarters)
Hitachi Solutions Create, Ltd. (Developing and building systems for government offices, and maintaining services)
Hitachi Solutions West Japan, Ltd. (Cloud Business Promotion Center)
Hitachi Solutions, Ltd. (Security Diagnosis Division)
Hitachi Systems Power Services, Ltd.(Managed Services Division Data Center Operation Office ePowerCloud Data Center Operation Department ePowerCloud Data Center Group)
Hitachi Systems, Ltd. (Akita/Sendai-Center)
Hitachi Systems, Ltd. (Contact Center Administration Division)
Hitachi Systems, Ltd. (Financial Platform Division Service Office ATM Cloud Computing Service Department)
Hitachi Systems, Ltd. (Outsourcing Data Center Division)
Hitachi Systems, Ltd. (Public Platform Division)
Hitachi Systems, Ltd. (SHIELD Security Center)
Hitachi Transport System, Ltd.
Hokkaido Hitachi Systems, Ltd. (Information Systems Division)
Okinawa Hitachi Network Systems, Ltd.

Third party assessment and certification

IT Security Certification

The following main products have been certified by the "IT Security Evaluation and Certification Scheme" based on the ISO/IEC 15408 (Common Criteria) which is operated by the Information-technology Promotion Agency, Japan (IPA) (as of the end of December, 2017; includes listings from the certified product archive list).

Product	TOE Category*1	Certification number	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
Enterprise Certificate Server Set 01-01-A	Certification authority function	C0013	EAL3
JP1/Base Certification server 08-10 (Windows edition)	System operation management	C0114	EAL2+ALC_FLR.1
uCosminexus Application Server 08-00	Application server	C0234	EAL2+ALC_FLR.1
EUR Form Client 05-07	Form data creation support software	C0068	EAL2+ALC_FLR.1
Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software 8.0.1-02	Access Control Device and Systems	C0536	EAL2+ALC_FLR.1
Hitachi Command Suite Common Component 7.0.1-00	Circuit board module	C0303	EAL2+ALC_FLR.1
Hitachi Storage Command Suite Common Component 6.0.0-01	Circuit board module	C0199	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)	Control Program for storage system	C0514	EAL2+ALC_FLR.1
Hitachi Unified Storage VM Control Program 73-03-09-00/00(H7-03-10_Z)	Control Program for storage system	C0513	EAL2+ALC_FLR.1
Hitachi Unified Storage 110 Microprogram 0917/A	Storage device control software	C0421	EAL2
Hitachi Unified Storage 130 Microprogram 0917/A	Storage device control software	C0420	EAL2
Hitachi Unified Storage 150 Microprogram 0917/A	Storage device control software	C0419	EAL2
Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 control program 70-02-05-00/00（R7-02-06A）	Storage device control software	C0315	EAL2
Hitachi Adaptable Modular Storage Microprogram 0862/A Hitachi Adaptable Modular Storage 2300 Microprogram 0862/ A-M	Display equipment control software	C0220	EAL2
Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000 Control Program 60-02-32-00/00（R6-02A-14）	Storage device control software	C0200	EAL2
SANRISE Universal Storage Platform CHA/DKA Program*3 TagmaStore Universal Storage Platform CHA/DKA Program*4 SANRISE Network Storage Controller CHA/DKA Program*3 TagmaStore Network Storage Controller CHA/DKA Program*4 SANRISE H12000 CHA/DKA Program*3 SANRISE H10000 CHA/DKA Program 50-04-34-00/00*3	Storage device control software	C0102	EAL2
Finger Vein Authentication Device UBReader2 Hardware: D, Software: 03-00	Biometric equipment	C0332	EAL2
Certificate validation server 03-00	PKI	C0135	EAL2
Appliporter Security Kit Version 01-00	Electronic application basic software	C0025	EAL2
DocumentBroker Server Version 3 03-11	Document management	C0158	EAL1+ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
CBT Engine 01-00	Major application for CBT assessment 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):
TOE refers to software, firmware or hardware that will be the target of evaluation.
In some instances this also includes related administrator and user manuals (user guidances, installation procedures manuals etc.)

*2 EAL (Evaluation Assurance Level):
In ISO/IEC 15408, the degree of assurance of evaluation criteria (assurance requirements) is divided into 7 levels, from EAL1 to EAL7, with assessment requirements getting stricter as the levels get higher.

- In EAL1, the suitability of security functions are tested, and guidance for maintaining security is evaluated objectively.
- In EAL2, assessment is augmented from a product integrity perspective, analyzing vulnerabilities imagining common attack capabilities from the manufacturing to the operation stages. The regular development cycle is adjusted to include a security perspective.
- In addition to the assurances of EAL2, EAL3 also evaluates test comprehensiveness, and the development environment for the purpose of preventing product manipulation during the development process.
- EAL4 is considered the highest level for commercial products. The integrity and source code of development assets in the development environment, and the development life cycle overall including the reliability of key personnel, are evaluated.
- ALC_FLR.1 is an objective evaluation of the basic procedures for providing the necessary patch when a security defect is discovered in the product. Assurance requirements not included in the EAL stipulated in the standards can be supplemented, which in this case would be displayed as EAL2+ALC_FLR.1. ALC_FLR.2 necessitates the acceptance of reports from users and the provision of notifications to users.

*3 Japan domestic

*4 outside of Japan

Third party assessment and certification

Encryption module testing and certification

The following products have been certified by the Japan Cryptographic Module Validation Program (JCMVP) based on ISO/IEC 19790 which is operated by the Information-technology Promotion Agency, Japan (IPA), or Cryptographic Module Validation Program (CMVP) based on FIPS140-2 which is operated by the USA's NIST and Canada's CSE (as of the end of December, 2017).

Cryptographic Module	Certification number	Level
Hitachi Virtual Storage Platform (VSP) Encryption Adapter	CMVP #2727	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Board	CMVP #2694	Level 1
Hitachi Virtual Storage Platform (VSP) Encryption Module	CMVP #2462	Level 2
Hitachi Virtual Storage Platform (VSP) Encryption Engine	CMVP #2386	Level 1
Hitachi Unified Storage Encryption Module	CMVP #2232	Level 1
HIBUN Cryptographic Module for User-Mode 1.0 Rev.2	JCMVP #J0015, CMVP #1696	Level 1 (*1)
HIBUN Cryptographic Module for Kernel-Mode 1.0 Rev.2	JCMVP #J0016, CMVP #1697	Level 1 (*1)
HIBUN Cryptographic Module for Pre-boot 1.0 Rev.2	JCMVP #J0017, CMVP #1698	Level 1 (*1)
Keymate/Crypto JCMVP Library 04-00 (Solaris edition, Windows edition)	JCMVP #J0007	Level 1
Keymate/Crypto JCMVP Library 04-00	JCMVP #J0005	Level 1

*1 This Cryptographic Module has been certified JCMVP and CMVP simultaneously (joint certification).
ISO/IEC 19790 as applied by JCMVP uses Federal Information Processing Standard (FIPS) 140-2 as applied by CMVP as a base, with equivalent standards.

Control device security certification

The ISCI*1 is an international security certification system for control devices run by the Control System Security Center (CSSC). Products certified by the ISCI's "ISASecure® EDSA certification" *2 are as follows. (As of May 31, 2017).

Product	Certification number	Certification acquisition level
Controller HISEC 04/R900E	CSSC-C00002	EDSA 2010.1 Level 1

*1 ISCI: ISA Security Compliance Institute *2 EDSA: Embedded Device Security Assurance

Hitachi Group Overview

Company Profile (as of March 31, 2017)

Corporate name: Hitachi, Ltd.
Incorporated: February 1, 1920 (founded in 1910)
Head office: 1-6-6 Marunouchi, Chiyoda-ku, Tokyo
100-8280, Japan
Representative: Toshiaki Higashihara
Representative Executive Officer,
President, and CEO

Capital: 458.79 billion yen
Number of employees: 35,631 (unconsolidated basis)
303,887 (consolidated basis)
Number of consolidated subsidiaries: 864
(Japan: 208, outside of Japan: 656)
(Including variable interest entities)
Number of equity-method affiliates: 388

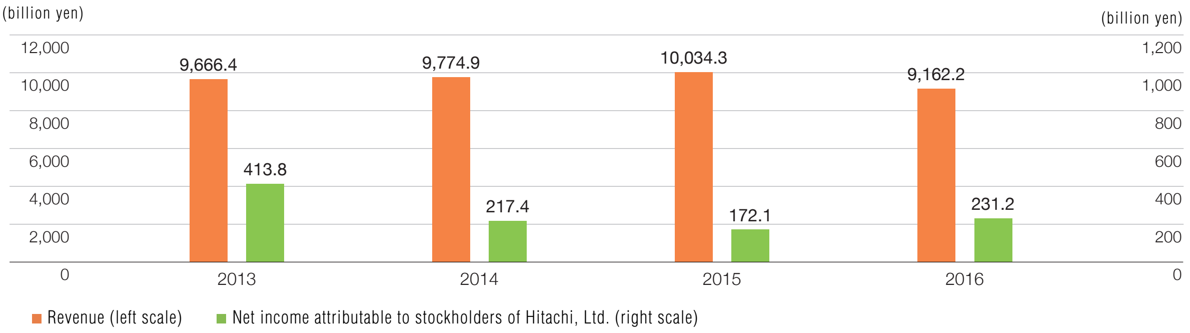
Consolidated Financial Highlights for Fiscal 2016, Based on the International Financial Reporting Standards (IFRS)

Revenues: 9,162.2 billion yen (down 9%, year on year)
EBIT[*1]: 475.1 billion yen (down 11%)
Income from continuing operations, before income taxes:
469.0 billion yen (down 9%)

Capital expenditure[*2]: 377.5 billion yen (down 29%)
R&D expenditure: 323.9 billion yen
Total assets: 9,663.9 billion yen billion yen

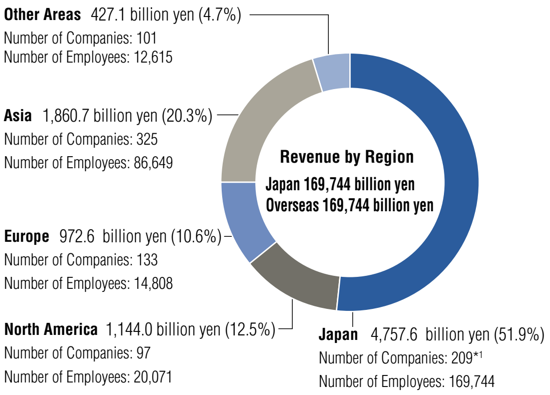
*1 EBIT: Income from continuing operations before income tax, less interest income, plus interest charges.
*2 Since fiscal 2015, the amount of investment in leased assets that fall under the heading of finance and leases included in conventional capital expenditure are deducted from capital expenditure for disclosure.
Note: Hitachi' s consolidated financial statement is prepared based on the International Financial Reporting Standards (IFRS).

●Revenue and net income attributable to stockholders of Hitachi, Ltd.



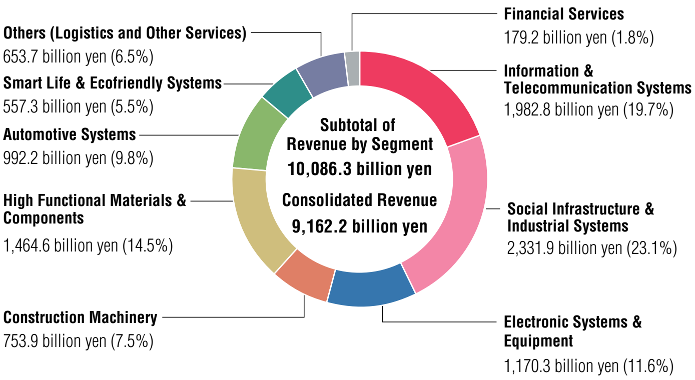
●Revenues and ratio by region

(Consolidated for fiscal 2016, based on IFRS)



●Revenue and Ratio by Segment

(Consolidated for fiscal 2016, based on IFRS)



*1 Including Hitachi, Ltd. and 208 consolidated subsidiaries in Japan.

Hitachi, Ltd.

IT Strategy Division, IT Security Management Department

1-6-6 Marunouchi, Chiyoda-ku, Tokyo 100-8280
Tel: 03-3258-1111