MITSUBISHI ELECTRIC

Changes for the Better

Mitsubishi Electric Group Information Security Report 2024

Contents

Editorial Policy

The purpose of this report is to apprise customers and stakeholders of the information security initiatives that the Mitsubishi Electric Group engages in on a daily basis in order to enhance the quality of life in our society.

Period Covered by the Report

April 1, 2023 to March 31, 2024

Scope of the Report

Information security initiatives at the Mitsubishi Electric Group

Publication Date of the Report

December 2024

Inquiries

Corporate Information Security Division
100-8310
Tokyo Building, 2-7-3, Marunouchi, Chiyoda-ku, Tokyo

Inquiries about the Information Security Report

Executive Message

We tackle information security as an important management issue.

The Mitsubishi Electric Group recognizes that cyber security is an important management issue. The Corporate Information Security Division, which oversees all information security management activities, is responsible for promoting confidential corporate information management, personal information protection, information system security, and product security. The Corporate Information Security Division also has a dedicated OT security unit to strengthen security measures.

Cyberattacks against businesses are becoming more sophisticated and diverse every year, posing a significant threat to us. In addition, equipment and system vulnerabilities are reported daily. This increases the threat. To respond to these cyberattacks, necessary security measures are being developed and implemented throughout the Mitsubishi Electric Group. Newly reported vulnerabilities are assessed and dealt with immediately.

Also, the Mitsubishi Electric Group has made a Declaration of Confidential Corporate Information Security Management and formulated the Personal Information Protection Policy to foster a corporate culture that ensures the appropriate handling of confidential corporate information and personal information. To put the above declaration and policy into practice, the Mitsubishi Electric Group is not only developing regulations and frameworks, providing education regularly to all employees, and implementing IT-based comprehensive measures, but also constantly making improvements through the PDCA cycle, including inspections.

In addition to the security measures to respond to the more sophisticated and diverse cyberattacks, we will accelerate risk assessment and response processes in overseas regions. This will be done both from a global perspective, such as the EU Cyber Resilience Act due to come into force this year, and from an economic security perspective. To protect personal information, the Mitsubishi Electric Group takes a global approach complying with the laws and regulations of Japan and applicable third countries and regions. Our common guidelines are also applied to associated companies. Mitsubishi Electric Group will continue to carry out information security actions that will meet your expectations.

This report provides information on the Mitsubishi Electric Group's information security efforts. We hope that it will be useful to you.

Eiichiro Mitani

Executive Officer,
CIO (In charge of Information Security),
Mitsubishi Electric Corporation

Basic Information Security Principles

Basic Policy

In order to respond to the threat of cyberattacks, which are rapidly becoming more sophisticated and diverse, the Mitsubishi Electric Group is continually working to strengthen its cyber security and governance of information management and operations. Our goal is to achieve Level 2 or higher on Cybersecurity Maturity Model Certification (CMMC)*1 Version 2.

We manage the information entrusted to us by customers and stakeholders of Mitsubishi Electric as well as confidential corporate information, including sales, engineering, and intellectual property information, based on the Declaration of Confidential Corporate Information Security Management.

*1 The Cybersecurity Maturity Model Certification framework by the U.S. Department of Defense. Certification Level 2 or higher means excellent security measures and management structure.

Declaration of Confidential Corporate Information Security Management

With respect to the information assets that constitute its core business activities, Mitsubishi Electric Corporation shall disclose information that should be released externally in a timely and appropriate manner, while ensuring strict and appropriate management of confidential corporate information.

In the unlikely event that valuable information or confidential corporate information entrusted to us by others were to leak, this would not only cost the trust and confidence invested in the Company; the improper use of this information could also threaten national, societal and individual security.

Recognizing that appropriate management of confidential corporate information is a key corporate social responsibility, the Company hereby declares that all employees shall comply with the following confidential corporate information management policies.

1) Appropriate Management of Confidential Corporate Information through Compliance with Laws, Ordinances and Regulations
   The Company shall manage all confidential corporate information concerning business activities appropriately in accordance with laws, ordinances and Company regulations. “Confidential corporate information” means valuable technical or business information held by the Company, and information (such as personal information, information obtained from outside the Company and insider information), which if disclosed or used in an unauthorized way, could be disadvantageous to the Company and/or its stakeholders. Physical objects that constitute confidential corporate information are also subject to control.
2) Enforcement of Security Management Measures
   The Company shall implement appropriate security management measures for the protection and proper control of confidential corporate information. “Security management measures” means organizational, human, technological and physical measures that are strictly enforced according to the confidentiality level of the applicable corporate information.
3) Enhancement of Information System Security Measures
   The Company shall enhance its information system security measures to prevent unauthorized access, intrusion and wrongful use of confidential corporate information, and implement comprehensive countermeasures with IT.
4) Education
   Recognizing that the awareness of individual employees who are involved in handling confidential corporate information is fundamental to management, the Company shall provide regular education for all employees concerning the importance of confidential corporate information management and the Company’s efforts to enhance it.
5) Continual Improvement of Management through the PDCA Cycle
   The Company shall establish a confidential corporate information management system and improve it proactively and continually through the PDCA (Plan-Do-Check-Act) cycle.
6) Timely and Appropriate Information Disclosure
   In addition to rigorously managing confidential corporate information in an appropriate manner in line with items 1 through 5 above, the Company shall disclose information that should be externally released in a timely and appropriate manner.

Date of formulation: February 16, 2005
Date of revision: July 28, 2021
Kei Uruma, President & CEO
Mitsubishi Electric Corporation

Information Security Organization Structure

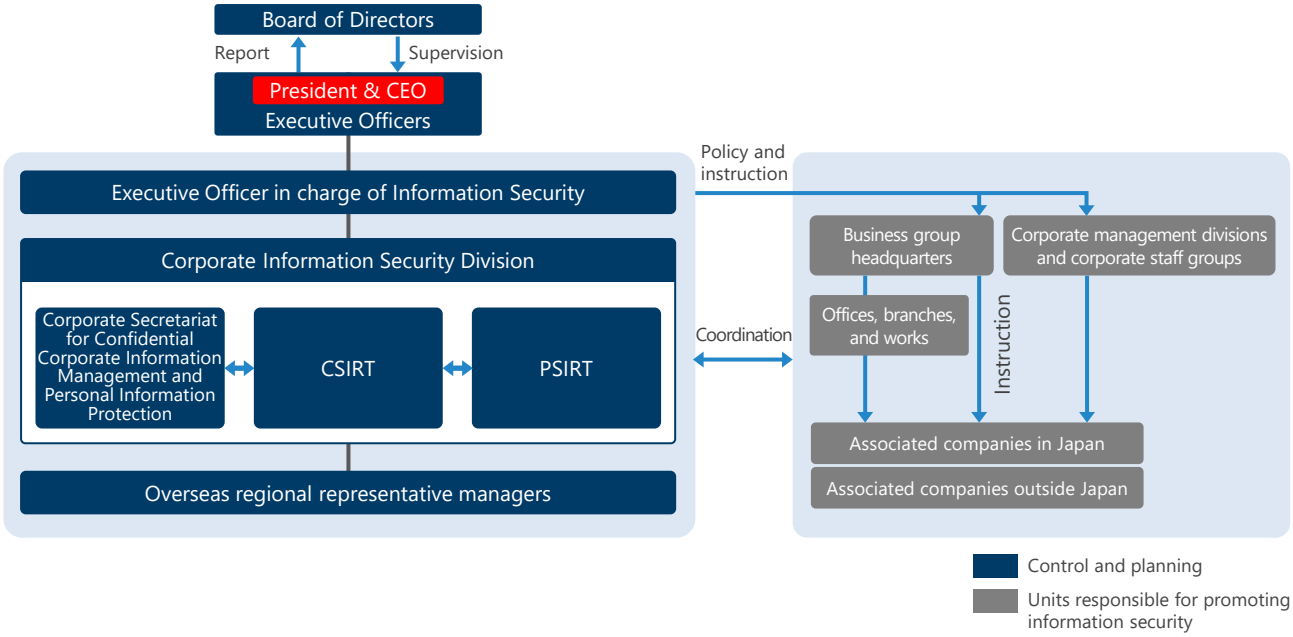
In April 2020, we established the Corporate Information Security Division directly under the president and integrated three functions—"confidential corporate information management and personal information protection", "information systems security", and "product security"—to oversee all information security management activities. We have been continually enhancing the functions of the division and increasing the number of staff. We will invest over 50 billion yen to strengthen cyber security measures and improve our information security management system to achieve Level 2 or higher on CMMC Version 2. The Executive Officer in charge of Information Security supervises information security management. Under the Executive Officer's instruction, the Corporate Information Security Division plans and implements countermeasures for the Mitsubishi Electric Group's information security management system and rules, cybersecurity, and compliance with the laws and regulations related to personal information protection. Meanwhile, Corporate CSIRT in the division cooperates with CSIRTs*2 in business groups and business sites to ensure information security.

In addition, in response to the cyberattack targeting a factory of a manufacturer, which caused production to shut down, Mitsubishi Electric has established a group in the division in charge of OT security.

The PSIRT*3 in the division, which is in charge of enhancing product security, was certified as a CNA*4 in November 2020. It has begun allocating CVE IDs*5 to vulnerabilities that affect Mitsubishi Electric products, and it announces these vulnerabilities to the public.
By doing so, the PSIRT strengthens vulnerability handling processes in cooperation with outside stakeholders. The PSIRT reports identified vulnerabilities according to the processes and issues instructions to respond properly and prevent secondary damage.

Business groups and business sites (offices, branches, and production plants [works]) provide instructions and guidance on information security to domestic and overseas associated companies. As for cybersecurity issues at overseas associated companies, the Corporate Information Security Division cooperates with overseas regional representative managers in America, Europe, and Asian countries, while considering each region's unique circumstances.

*2 CSIRT stands for Computer Security Incident Response Team.
*3 PSIRT stands for Product Security Incident Response Team. This team works on improving the security quality of products and services.
*4 CNA stands for CVE Numbering Authority, and CVE stands for Common Vulnerabilities and Exposures.
*5 Globally used vulnerability identifiers.



Information Security Organization Structure (Mitsubishi Electric Group)

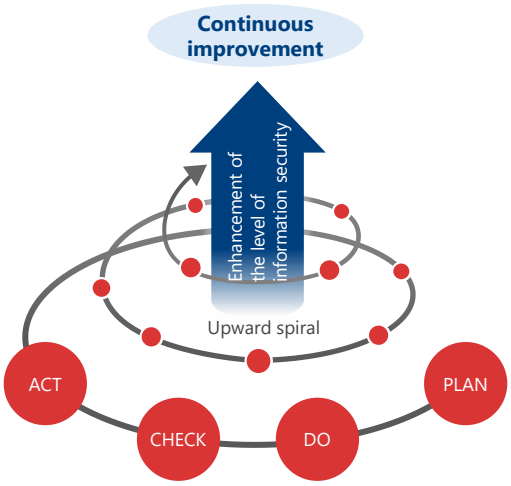
Information Security Management

Management Principles

The Mitsubishi Electric Group oversees confidential corporate information management and protects personal information as its continuous improvement activity using the Plan, Do, Check, Act (PDCA) cycle and implements four security measures, which are organizational, human, technological, and physical security measures, to safeguard confidential corporate information and personal information while taking into consideration external factors such as handling of personal data overseas.

PDCA cycle

We strive to continually raise the level of our information security in an upward spiral. First, plans are formulated at the beginning of the fiscal year based on an annual policy (Plan). Then, various information security measures are rolled out and employees are trained (Do). Afterward, the status of information security management is checked (Check). Finally, the measures are revised accordingly based on the results (Act).



PDCA cycle to ensure information security

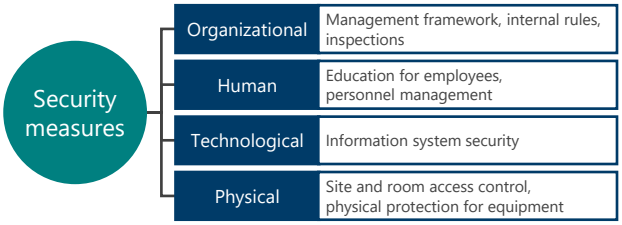
Four security measures

Organizational security measures consist of systems such as a management framework, internal rules, and internal audits to safeguard confidential corporate information and personal information. They are revised as needed to ensure no loss of effectiveness due to changes in the operating environment.

Human security measures consist of education for employees and personnel management to ensure employees carry out information security measures.

Technological security measures consist of information system security efforts such as cyberattack countermeasures.

Physical security measures consist of site and room access control as well as physical protection for equipment to prevent unauthorized third parties from entering a business site and potentially accessing confidential corporate information and personal information.



Four security measures

Global activities

To maintain and improve the information security level of the Mitsubishi Electric Group including overseas associated companies, various inspections are conducted according to information management system prescribed in the Guidelines to Information Security Management Rules for associated companies.

Information Security Regulations and Guidelines

In accordance with Declaration of Confidential Corporate Information Security Management and Personal Information Protection Policy, Mitsubishi Electric Corporation has established information security regulations and guidelines from the perspective of the four security measures, and reviews them as necessary to comply with current laws.

To protect personal information, the Mitsubishi Electric Group handles the personal information appropriately and takes a global approach complying with the laws and regulations of Japan and applicable third countries and regions. Our common guidelines are also applied to associated companies.

Item		Basic regulations
Security measures	Organizational security measures	Regulations on confidential corporate information security management / Personal data protection guidelines
	Human security measures	Regulations on the work of employees
	Technological security measures	Regulations on information security management
	Physical security guidelines	Physical security guidelines

Responding to changes in the operating environment

In addition to the basic regulations given above, we have established regulations concerning the release of information on public-facing websites, regulations concerning the use of smartphones, management standards to strengthen information security in the supply chain, and other regulations to address today's changing business operation environment.

Information Security Inspections

The Mitsubishi Electric Group performs the following inspections as part of the C (Check) stage of the PDCA cycle at head office management departments, business groups and offices, and associated companies. These inspections focus on checking whether confidential corporate information management and personal information protection activities are being implemented properly by the Mitsubishi Electric Group as a whole, and on confirming the status of those activities.

The group reviews measures based on the results, and this leads to the A (Act) stage of the PDCA cycle.

These inspections are set down in the Confidential Corporate Information Management Regulations, which cover Mitsubishi Electric Corporation, and in the Guidelines for Information Security Management Regulations, which cover domestic and overseas associated companies.

Name Content	Name	Content
Self-check	Self-check program for confidential corporate information management and personal information protection	Using a checklist, each Mitsubishi Electric Group company performs a self-inspection of its activities for information security.
Third-party check	Third-party check program for confidential corporate information management and personal information protection	Mitsubishi Electric's business sites mutually check each other's status of information security management. Mitsubishi Electric checks the status of information security at associated companies.
	Personal information protection audits (Personal information protection management system audits)	At Mitsubishi Electric, the status of personal information protection is audited company-wide under the instructions of the Audit Manager for Personal Information Protection appointed by the President & CEO of Mitsubishi Electric. At associated companies in Japan that have been granted the right to use the PrivacyMark, the same audit is carried out by the audit manager of each company.

Information Security Education

Mitsubishi Electric is working on fostering a corporate culture that ensures the appropriate handling of confidential corporate information and personal information. We provide the educational programs described below to train employees on how to fully implement concrete security measures, including storing files on servers or encrypting them in accordance with their confidentiality level.

Education for all employees

An e-learning program on information security is provided once a year to all employees and other staff members (about 50,000 in total) to ensure their full understanding of the Mitsubishi Electric policies, status of data breach incidents, laws and regulations related to the protection of personal information, Unfair Competition Prevention Act, and security measures (organizational, human, technological, and physical measures) that each employee must be aware of. In addition, due to the rapid increase in teleworking and the shift in business type and environment due to the use of cloud services, educational materials for employees are released as needed.

Education corresponding to each career stage

We teach confidential corporate information management and personal information protection through training programs for new employees, newly appointed section managers, the personal information asset manager, the Corporate Secretariat involved in operation and the like, so that our employees can fulfill the roles expected at each career stage in the duties for which they are responsible.

Exercises to practice handling spoofed e-mails

As a measure against cyberattacks, Mitsubishi Electric regularly conduct exercises that allow all employees, including officers, to verify that they know how to handle spoofed e-mails. Employees of associated companies in Japan can participate in this exercise. At overseas associated companies in America, Europe, and other Asian countries practice exercises are conducted according to local circumstances under the direction of regional representative managers.

Other individual training

Employees posted overseas are provided with a preliminary education program which covers risks in confidential corporate information management and personal information protection outside Japan and examples of data breach incidents that have occurred overseas.

Personal Information Protection Activities by Mitsubishi Electric Group

The Mitsubishi Electric Group's core philosophy regarding personal data protection

The Mitsubishi Electric Group has established a corporate purpose: "We, the Mitsubishi Electric Group, will contribute to the realization of a vibrant and sustainable society through continuous technological innovation and ceaseless creativity." We are engaged in a variety of businesses and receive a variety of information from all stakeholders—including customers, shareholders, investors, business partners and employees—through our business activities while recognizing that personal data is an important asset.
As such, it is our social responsibility to ensure accurate and safe processing of personal data.

We handle personal data in accordance with eight principles based on laws and regulations of various countries and regions, and strive to improve and maintain these principles by establishing systems and implementing appropriate measures.

The Mitsubishi Electric Group's principles for processing of personal data

The Mitsubishi Electric Group processes your important personal data in accordance with the following principles.

(1) Lawfulness: We acquire and process personal data appropriately in accordance with relevant laws and regulations.
(2) Fairness and transparency: When processing personal data, we provide you with clear and easily understandable information about our procedures for handling personal data, using simple and accessible methods, at the appropriate time and from your perspective.
(3) Purpose limitation: We process personal data only if it is sufficient, relevant and necessary in relation to the purpose.
(4) Data minimization: We limit our processing of personal data to what is necessary in relation to the purpose.
(5) Accuracy: We keep personal data accurate and up to date where necessary.
(6) Storage limitation: We determine the period for which storing personal data is necessary for its purpose. When the storage period ends, we delete personal data by an appropriate method.
(7) Integrity and confidentiality: We take appropriate technical and organizational measures to protect personal data from breaches, including unauthorized access, accidental loss, destruction, alteration, or leakage.
(8) Privacy by design: We consider protective measures necessary to comply with the above principles at the planning stage, or in other words, prior to conducting the processing of personal data.

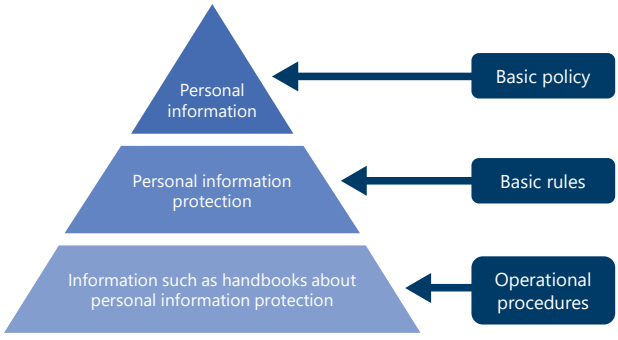
Personal Information Protection Activities at Mitsubishi Electric

Establishment of personal information protection management system

Mitsubishi Electric formulated company rules on personal information protection in October 2001. Since then, it has ensured that all employees and relevant individuals understand the rules and has worked on protecting personal information.

In 2004, the company formulated the Personal Information Protection Policy and improved it as a set of personal information protection activities that meet the requirements of JIS Q 15001: 2006 Personal Information Protection Management Systems. In January 2008, we were granted the right to use the PrivacyMark, which certifies the establishment of management systems that ensure proper measures for personal information protection. We have been renewing the PrivacyMark certification since then.

In January 2024, we completed the eighth PrivacyMark renewal process.



Structure of personal information protection rules

Personal information collected from customers through questionnaires, registration of purchased products, after-sales service, and so on is managed in accordance with the "Personal Information Protection Policy". Furthermore, Mitsubishi Electric has been granted the right to use the PrivacyMark and is making ongoing efforts to ensure the proper handling of personal information.

Personal Information Protection Policy

Mitsubishi Electric ("the Company") will continually improve its technologies and services by applying creativity to all aspects of its business, thus enhancing the quality of life in society. Through these activities, the Company collects various types of information from its customers and affiliated persons. Since personal information is an important asset of individuals, it is the company's social responsibility to protect the personal information appropriately and use it correctly and safely in compliance with laws. The Company has established the personal information protection management system as a part of corporate management. With this system, the Company will ensure that the Company's employees (including corporate officers, employees, short-term/long-term part-timers, and temporary staff) and affiliated persons fully understand personal information protection, implement the actions listed below, and improve and maintain personal information protection.

1. Objective of Personal Information Protection
   The objective of personal information protection is to appropriately and effectively use personal information and protect the rights and interests of individuals with due consideration given to the usefulness of personal information.
2. Purpose of Use of Personal Information
   The Company uses personal information within the extent of the purpose of use clearly described to the information owner and uses such information only when required for business reasons.
3. Acquisition of Personal Information
   The Company acquires personal information through legal and fair means. When acquiring information directly from the information owner, the Company will clearly explain the requirements, including the purpose of use, and obtain consent.
4. Disclosure and Submission of Personal Information
   The Company will obtain the consent of the information owner before disclosing or submitting his/her personal information to a third party for the purpose of outsourcing or collaboration.
5. Handling of Personal Information
   (1) Compliance with laws and regulations on the protection of personal information
   The Company fully complies with laws, regulations, national policies, and other rules concerning the protection of personal information.
   (2) Prevention of data breach, losses, and damage to personal information (e.g., security measures), and corrective measures
   The Company takes reasonable safety actions and necessary security measures to prevent unauthorized access, losses, corruption, falsification, or leakage of personal information. It also audits all departments to check the handling of personal information and implements corrective measures. Through this audit, all divisions review the latest data breach risks or issues and make improvements to avoid similar incidents in the future.
   (3) Creation and operation of the personal information protection management system
   The Company has created and is operating the personal information protection management system in line with the requirements of JIS Q 15001: 2006 Personal Information Protection Management Systems. It has also been reviewed by JIPDEC and as a result, obtained the right to use PrivacyMark, which is given to businesses that handle personal information properly. It will continue to protect personal information while continually improving the personal information protection management system.
6. Handling of Information Related to Individuals
   When the Company handles information related to an individual such as location data, IP address, and cookies on the Company website or in other places, it may notify the information owner of the purpose of use and obtain his/her consent.
7. Responses to Inquiries from Information Owners
   When the information owner requests the disclosure, correction, removal, or suspension of use of his/her personal information, or when the Company receives inquiries, including complaints or consultation, from the information owner, it will respond without delay. The Company also strives to keep personal information accurate and up to date.

PrivacyMark

Date of formulation: April 16, 2004
Date of revision: April 1, 2022
Kei Uruma, President & CEO
Mitsubishi Electric Corporation

Proper handling of personal information

We handle personal information appropriately; we acquire it by specifying the purpose of use, use it only within the intended scope, and provide it to a third party only with the consent of information owners. At the same time, we will further strengthen security measures, including storing data on servers and using data encryption, to address the risk of data breach caused by cyberattacks.

PrivacyMark

Mitsubishi Electric and some associated companies in Japan have been granted the right to use the PrivacyMark.

Response to Japan's "My Number" system

Personal identity numbers are managed strictly and handled appropriately in accordance with internal regulations adapted to Japan's "My Number" system. Employees who handle personal identity numbers are trained individually.

Compliance with the EU General Data Protection Regulation (GDPR) and China's Personal Information Protection Law

When Mitsubishi Electric transfers or handles personal information as defined by national and regional laws, such as the EU General Data Protection Regulation (GDPR*6: Effective May 2018) and China's Personal Information Protection Law (Effective November 1, 2021), Mitsubishi Electric shall appropriately protect personal information in accordance with the requirements of the relevant national and regional laws.

*6 GDPR stands for General Data Protection Regulation.

Other Measures

Contractor management

Confidential corporate information and personal information are entrusted to a contractor only after a proper non-disclosure agreement is concluded between Mitsubishi Electric and the contractor. The agreement stipulates all the security and personal information protection matters that we require.

To ensure that confidential corporate information and personal information entrusted to a contractor will be handled with appropriate control, before entrusting the information to the contractor, we confirm that the contractor will maintain the proper level of protection. After submitting the information, we supervise the contractor by regularly examining a status report on the use and management of the information that we have submitted.

Information Security Initiatives

(Technological and Physical Security Measures)

The information security initiatives of the Mitsubishi Electric Group include cyberattack countermeasures and physical security measures for the IT infrastructure.

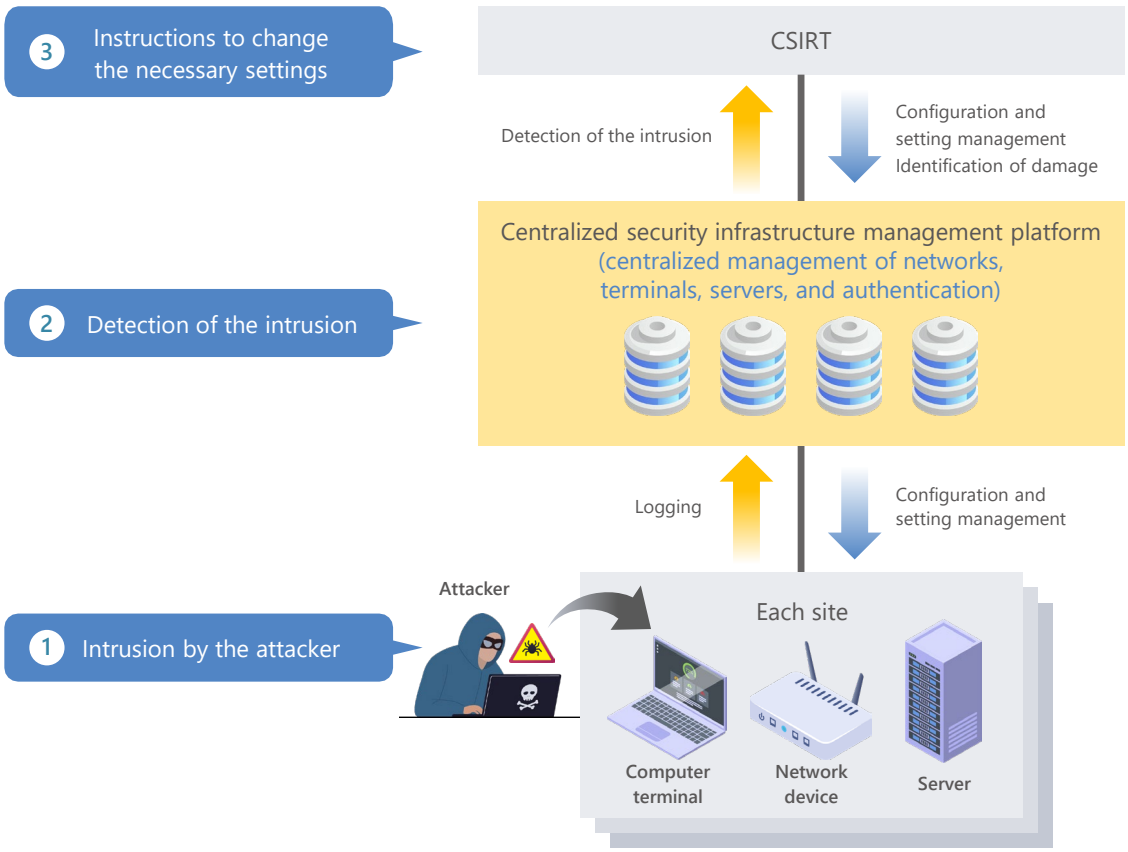
Cyberattack Countermeasures

Cyberattacks against companies are becoming more sophisticated and diversified every year, posing major threats to them.

To combat cyberattacks, the Mitsubishi Electric Group has introduced the centralized management of networks, computer terminals, and servers (cloud) and adopted defense in depth. The defense in depth provides protection against cyberattacks and enables the detection of suspicious activities and intrusions. The immediate response system we have established also helps to prevent and minimize damage.

Defense in depth provides protection against cyberattacks and enables the detection of suspicious activities and intrusions. Furthermore, developing incident response processes helps to prevent and minimize damage.

To support work at the office as well as work requiring access from home or on a business trip, strong multifactor authentication has been introduced and authentications are centrally managed. Internet websites are constantly exposed to many external threats, and so we only launch websites that are approved in order to maintain a high security level.



Centralized security management

Defense in depth

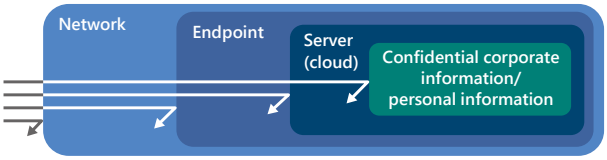
The Mitsubishi Electric Group has adopted defense in depth, consisting of three layers of technological security measures, which are network, computer terminal, and server (cloud) security measures.

In the network security measures, various security devices are installed at perimeter to control and monitor email and web communications, among others. This will block unauthorized access or malware from outside or prevent information from being leaked. The Mitsubishi Electric Group will improve this communication filtering function.

In the computer terminal security measures, anti-malware software detects and removes malware, and security patches for software vulnerabilities are applied. Doing so will lead to the prevention of computer terminal malware infections, suppression of attacks, and localization of damage. For this reason, computer terminals are centrally managed, and measures are sure to be applied to them. Anomaly behavior detection (EDR: Endpoint Detection and Response) tool*7 will be installed in all computer terminals to enhance computer terminal security. In addition, we have deployed multifactor authentication that combines two or more authentication factors to implement more powerful security measures.

Servers that are becoming cloud-based are periodically checked to find vulnerabilities, and communications and operations are monitored. This will make servers (cloud) robust, which have critical information.

To confidential corporate information and personal information stored in servers or in the cloud, access control and encryption is applied based on the principle of least privilege. For the management of these types of information, the Mitsubishi Electric Group also develops and fully implements rules, educates employees, and carries out inspections.



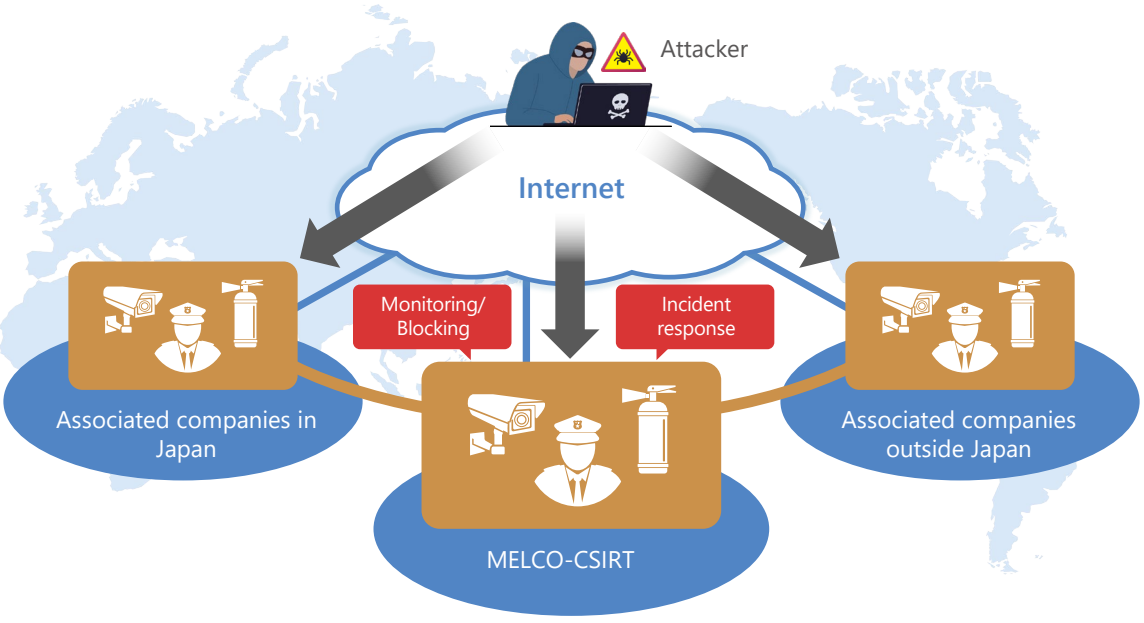
Multilayered defense

Computer Security Incident Response Team

The Mitsubishi Electric Group has established the Mitsubishi Electric Corporation Computer Security Incident Response Team (MELCO-CSIRT) to monitor cyberattacks and respond immediately to any incidents.

In order to prevent cyberattacks, we have also developed a process to monitor our associated companies inside and outside Japan, which has been insufficient in the past. The above-mentioned communication monitoring identifies suspicious behavior, allowing you to quickly detect and block cyberattacks. On the terminal side, information on malware infections and the current soundness of computer terminals are gathered and identified. In the event of an incident, the MELCO-CSIRT will utilize these security measures to immediately assess the damage, make prompt and appropriate responses, restore operations, and minimize damage as much as possible. After that, it will analyze the incident in detail and support the implementation of permanent measures by the department where the incident occurred.

*7 EDR stands for Endpoint Detection and Response.



MELCO-CSIRT

Security measures for teleworking

Teleworking is becoming more common as work styles diversify to include working from home or at a satellite office, in addition to mobile work during a business trip.

Meanwhile, the use of a network and the cloud contributes to the diversification of business operation, and traditional security measures at the perimeter becomes insufficient due to an increase in normal access from outside. For this reason, we are implementing more powerful security measures, including the encryption of communications using a virtual private network (VPN) for security and the use of multifactor authentication.

In order to support work at the office as well as work requiring access from home or on a business trip, strong multifactor authentication has been introduced and authentications are centrally managed.

Management of Internet websites

As a lesson learned from past incidents that occurred due to unauthorized access, the Mitsubishi Electric Group now ensures that only websites that have been approved by Mitsubishi Electric are launched in order to maintain the security level of websites.

Websites may go live only after they have passed a security test and problems have been resolved. We also regularly inspect our public websites on the Internet to assess their management status. By doing so, we remove unnecessary websites and strengthen security measures for websites where they are insufficient.

Physical Security

To prevent suspicious individuals from entering a business site and coming into contact with confidential corporate information, the Mitsubishi Electric Group sections physical spaces of human activity, such as a site' grounds, corridors, offices, meeting rooms, server areas, and data rooms, into areas and designates a security level (area level) for each area.

Area levels

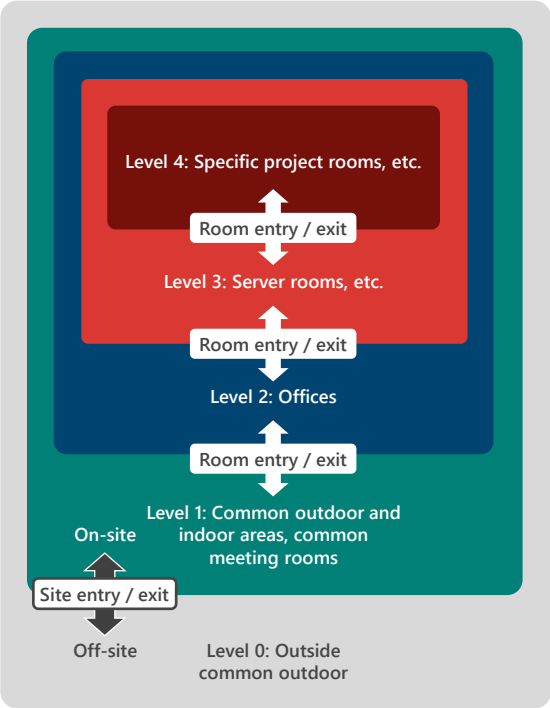
The designation of area levels is as given in the following table. We define security rules according to area level.

	Level	Evaluation criteria	Example	
High	Area level 4	On-site: Areas that can be accessed and used only by a limited number of Mitsubishi Electric employees, employees of associated companies, etc.	Special rooms, specially managed project rooms	On-site
	Area level 3	On-site: Areas that can be accessed and used only by specific Mitsubishi Electric employees, employees of associated companies, etc.	Server rooms, drawing/project rooms, development rooms, critical equipment rooms	
	Area level 2	On-site: In principle, areas that can be accessed and used by all Mitsubishi Electric employees, as well as specific persons (such as employees of associated companies).	Offices, common meeting rooms (for internal use)	
	Area level 1	On-site: In principle, areas that can be accessed and used by all Mitsubishi Electric employees and persons who completed entry procedures (such as employees of associated companies, business partners, and general visitors).	Common outdoor/indoor areas, common meeting rooms (including those for external use), corridors	
Low	Area level 0	Off-site	Outside common outdoor areas	Off-site

Designation of area levels

Entry/exit access control

We use entry/exit access control to ensure that only authorized persons enter rooms and sites when going between areas with different area levels. In particular, Mitsubishi Electric sites use ID card-based authentication systems to ensure security as well as more efficient entry and exiting.



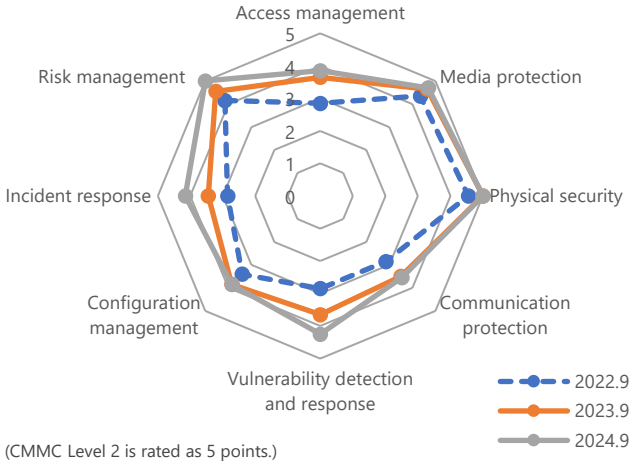
Entry/exit access control

Promotion of Information Security Measures

Mitsubishi Electric Corporation is continuously working to improve its information security management system as well as strengthen cyberattack countermeasures.

In order to evaluate these improvement activities, we set specific goals for information security measures and conduct self-assessments for Mitsubishi Electric Corporation and its domestic associated companies based on the major assessment axes and inspect the effectiveness of the measures we have formulated.

We will continue to improve our information security measures through the PDCA cycle, including these inspections, and going forward, we plan to expand this evaluation to the entire Mitsubishi Electric Group, including overseas associated companies.



(CMMC Level 2 is rated as 5 points.)

Self-assessments for information security measures and conduct

Initiatives Regarding the Security Quality of Products and Services

Roles of the Mitsubishi Electric PSIRT

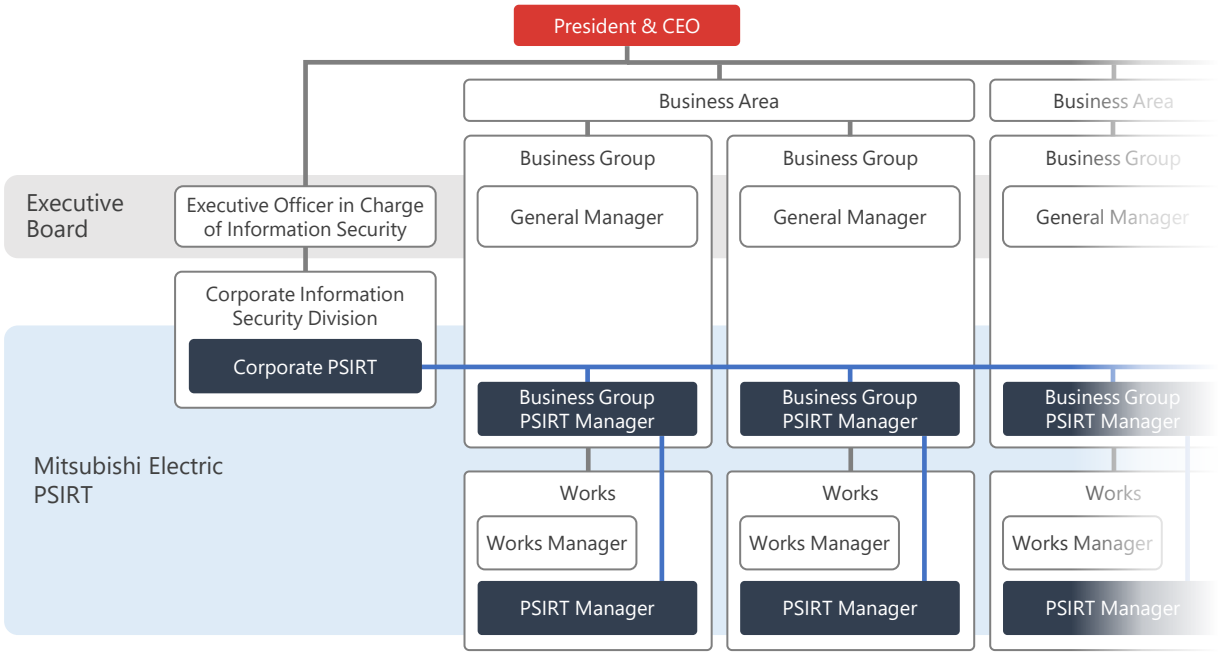
Mitsubishi Electric has formed the Mitsubishi Electric Product Security Incident Response Team (PSIRT), an internal unit for handling issues related to the security quality of products and services, and is making company-wide efforts to ensure the information security of our products and services.

The roles of the Mitsubishi Electric PSIRT are listed on the right:

- Gather information on vulnerabilities in products and services provided to customers
- Respond swiftly to vulnerabilities discovered in cooperation with product design and production departments and service management departments
- Strengthen and promote technical initiatives to preclude vulnerabilities from the stage of product and service development
- Provide necessary security training to all officers and employees concerned with product and service development
- Disclose vulnerability information and measures to Customers

The Mitsubishi Electric PSIRT Organization Structure

Mitsubishi Electric has appointed PSIRT managers to all business group headquarters and business sites to reduce risks by tackling security issues. A corporate PSIRT has been established within the Corporate Information Security Division to improve the security of product and service.



The Mitsubishi Electric PSIRT Organizational Structure

Compliance with Laws and Regulations Related to Product Security

With the advancement of digitalization in recent years, the impact of cyberattacks on society has been increasing. Countries around the world have strengthened their legal regulations on products by introducing cyber security acts such as the EU Cyber Resilience Act. In addition to measures that ensure the security quality of products and services, Mitsubishi Electric is constantly working with all our businesses to comply with the legal requirements of each country.

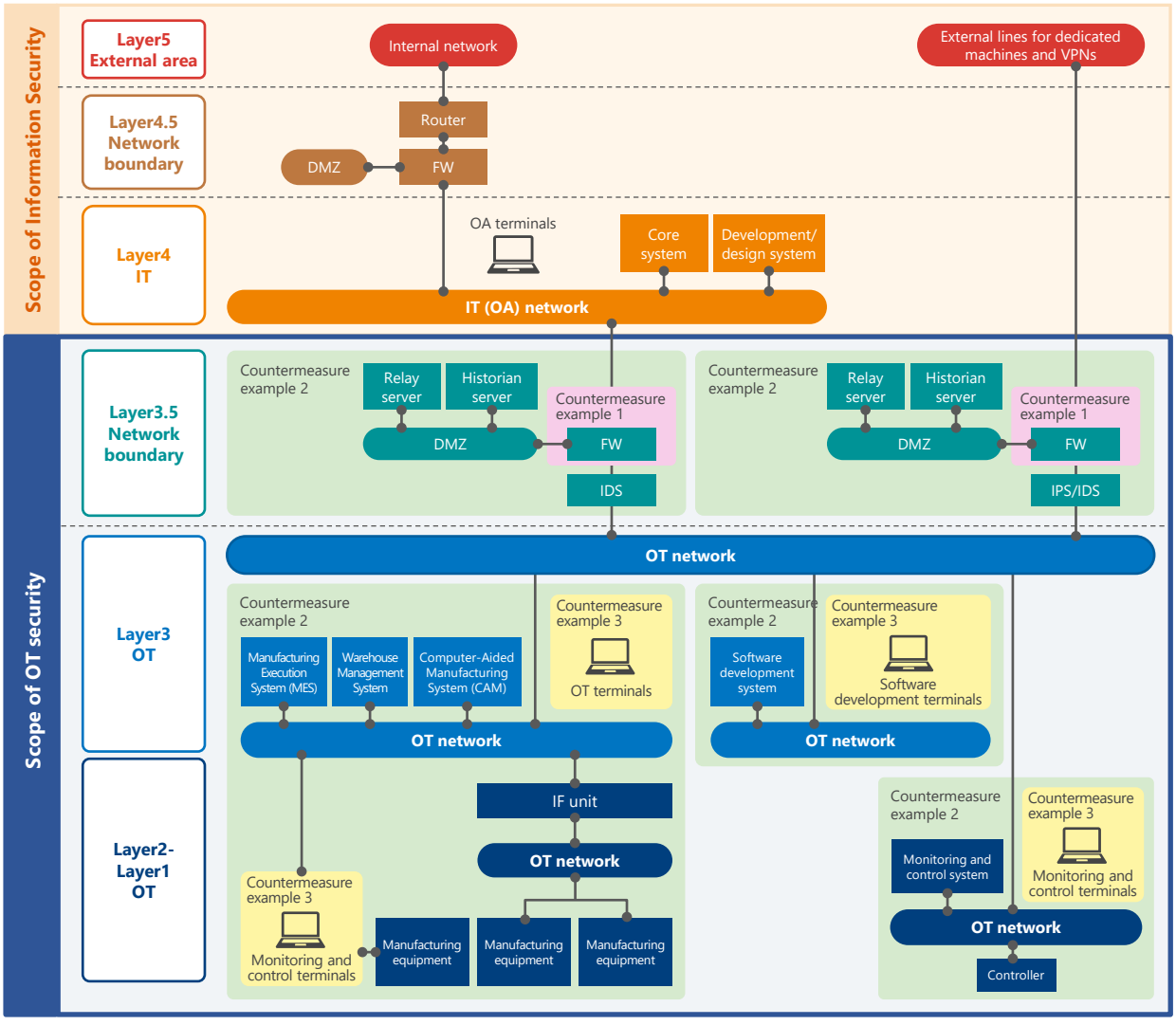
Factory (OT Security) Initiatives

Promotion of OT Security Measures

Various new technologies and environmental changes, such as IoT, DX (Digital Transformation), and teleworking, are flowing into factories that have been operating in closed environments with no external connections such as the Internet. As a result, factories are now starting to operate in more open environments.

Consequently, the threat of cyberattacks, which had previously been unheard of in the factory environment, has reached factories, leading to numerous incidents that cause significant damage, such as factory shutdowns, in recent years. At Mitsubishi Electric, as an internal framework to protect our factories from cyberattacks, we have organized a specialized group for OT (Operational Technology) security within the Corporate Information Security Division and are working to strengthen cybersecurity measures for our factories.

Specifically, based on the Purdue reference model*8, we are promoting security measures at each factory by logically stratifying installation positions of systems and equipment within the factory into layers and clarifying the security requirements for each layer in documentation. The security requirements are based on IEC 62443-2-1*9 and other standards.



Overview of the overall factory system based on the Purdue reference model

*8 Purdue reference model: A framework that logically categorizes industrial control systems into functional layers, enabling to present a map of IT/OT network zones that need to be secured.

*9 IEC 62443 is a set of standards issued by the International Electrotechnical Commission (IEC), which is widely used as security guidelines for control systems. Among them, the IEC 62443-2 series provides requirements specifically for factories.

MITSUBISHI ELECTRIC CORPORATION

https://www.mitsubishielectric.com