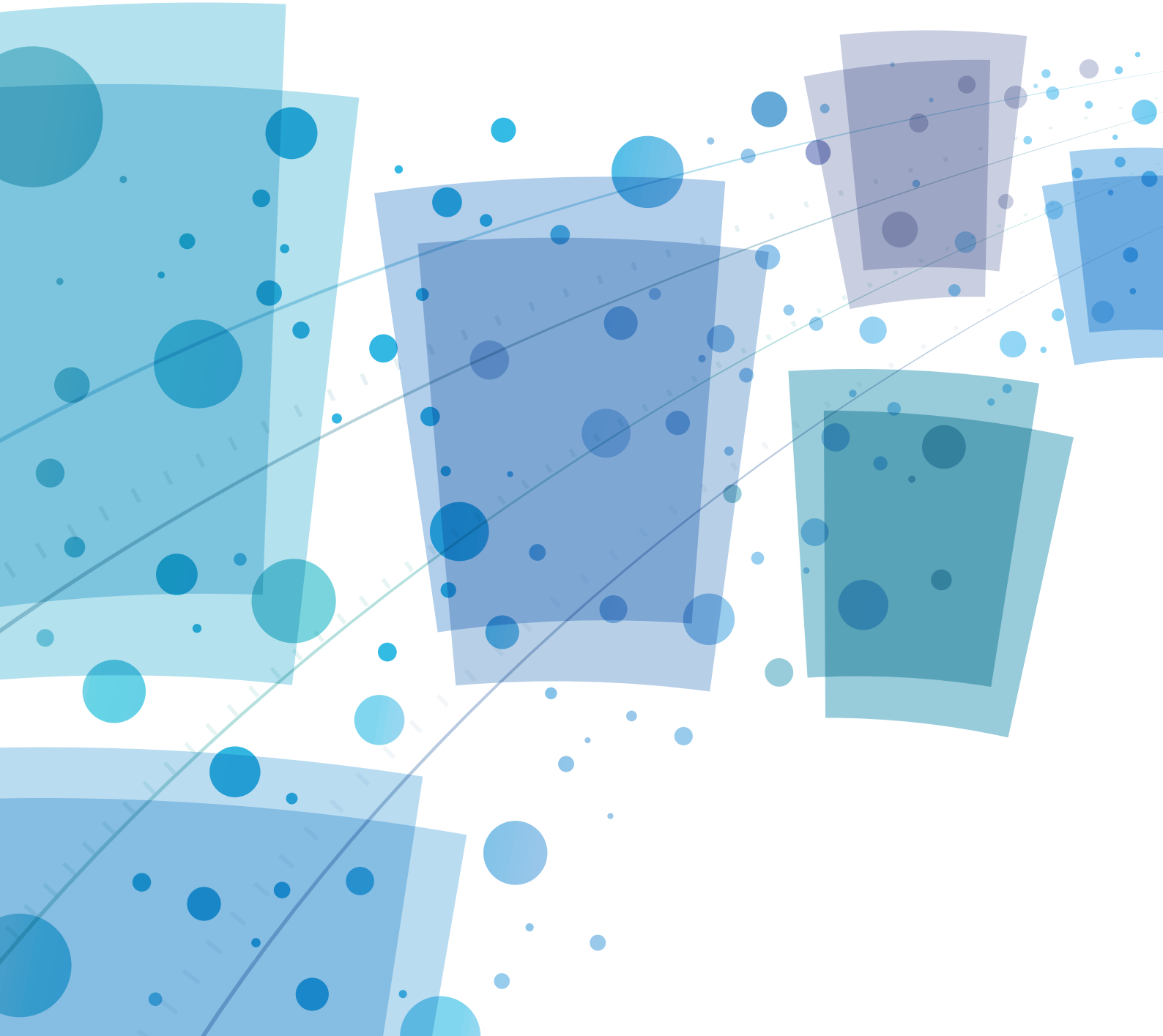
MITSUBISHI ELECTRIC
Changes for the Better

for a greener tomorrow eco Changes

Mitsubishi Electric Group Information Security Report 2019



Contents

Editorial Policy

The purpose of this report is to apprise 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

Fiscal 2019 (April 1, 2018 – March 31, 2019)

Scope of the Report

Information security initiatives
at the Mitsubishi Electric Group

Publication Date of the Report

July 2019

Our Approach to Information Security

Message from the Corporate Manager

We view, and address, information security as an important management issue.

The Mitsubishi Electric Group acts upon its Corporate Mission, which states that, "The Mitsubishi Electric Group will continually improve its technologies and services by applying creativity to all aspects of its business. By doing so, we enhance the quality of life in our society." Our aims are to realize a sustainable society and to provide safety, security, and comfort. We take information security seriously as one means to provide safety and security.

The Mitsubishi Electric Group established the Mitsubishi Electric Corporation Declaration of Confidential Corporate Information Security Management in order to express our information security policy in the world in 2005. Before that, we had established a Personal Information Protection Policy in 2004 to handle personal information appropriately.

Proper handling of confidential corporate information and personal information is extremely important from the viewpoint of administrative risk management. To put the above declaration and policy into practice, the Mitsubishi Electric Group carries out a variety of activities including establishment of regulations and a framework, provision of regular training to all employees, implementation of comprehensive IT-driven measures, and establishment of a Plan, Do, Check, Act (PDCA) cycle including inspections.

Additionally, in line with the 2018 Declaration of Cyber Security Management from the Japan Business Federation (Keidanren), we also regard cyber security as an important management issue as we seek to fully respond to today's increasingly sophisticated and diverse cyber-attacks. At the same time, we provide information security solutions in fields such as IT, room entry access control, and network cameras. Our products and services therefore contribute to a safe and secure society.

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

Shinji Harada

Corporate Manager for Confidential Corporate Information Management

Executive Officer

Mitsubishi Electric Corporation

Information Security Governance: Human and Organizational Security Measures

Basic Policy

The Mitsubishi Electric Group handles confidential corporate and personal information appropriately as part of its corporate social responsibility to make certain that such sensitive information does not leak out and cause concern for our customers and society, as can be caused by cyber-attacks or the loss of storage media.

The Mitsubishi Electric Group manages confidential corporate information, which includes information on Mitsubishi Electric's sales, engineering matters and intellectual property, based on the "Declaration of Confidential Corporate Information Security Management" that was established in February 2005. Information that is entrusted to us by our corporate customers is managed and protected in compliance with a non-disclosure agreement, as well as by the same level of security measures that are applied to our own confidential corporate information.

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-Action) 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.

April 1, 2018
Takeshi Sugiyama, President & CEO
Mitsubishi Electric Corporation

Personal information collected from customers through questionnaires, registration of purchased products, repair services, and other such means is managed based on the "Personal Information Protection Policy" that was established in April 2004. On the basis of this system, in January 2008 Mitsubishi Electric was granted the right to use the "PrivacyMark" under Japan's system for certifying personal information protection systems, in recognition of its ongoing efforts to ensure proper handling of personal information.

Personal Information Protection Policy

Mitsubishi Electric Corporation fully complies with Japan's laws and regulations, national policies and other rules concerning the protection of personal information.

Personal information can be defined as any information that may be used to identify an individual, including, but not limited to, a first and last name, a home or other physical address, an e-mail address or other contact information.

Mitsubishi Electric Corporation sometimes collects personal information from its customers while conducting business activities. On the Global Website, personal information is collected predominantly through the various contact/inquiry forms.

When we directly solicit personal information from you in writing, we will specify how we intend to use the information, and ask for your consent. When we collect personal information by other means, we will announce on our website how we intend to use it.

When you provide us with personal information, we use the information to respond to and confirm your inquiry, and may keep a record of the inquiry for the same purposes. In addition, to support our customer relationship, we may store and process personal information and share it with our worldwide subsidiaries and affiliates to better understand your needs and how we can improve our products and services.

At times Mitsubishi Electric Corporation may conduct online surveys to better understand the needs and profile of our visitors. When we conduct a survey, we will do our utmost to let you know how we will use the information collected from you. Our site may provide contests, sweepstakes or other promotions that may ask you to enter your personal information. We will use the information you provide for the purpose of conducting the promotion, like providing customer support or contacting you if you're a winner.

Mitsubishi Electric Corporation does not use or disclose information gathered from individual visits to the Site or information that you may give us to any third parties for intention to sell, rent or otherwise market your personal information. We may at times employ a third party service providers to perform or assist us on the on-line surveys, contests, sweepstakes or other promotions. For example, administering the survey or promotion, compiling the data or providing customer support. These parties will have signed a Non-Disclosure Agreement prior to any services we initiate with them. They will not disclose any personal information they receive from you and will only use it in order to initiate and or continue the services they are providing for us.

You have the option not to provide personal information to Mitsubishi Electric Corporation. If you choose not to provide the personal information we request, you can still visit most of the Site, but you may be unable to access certain options, offers and services that involve our interaction with you.

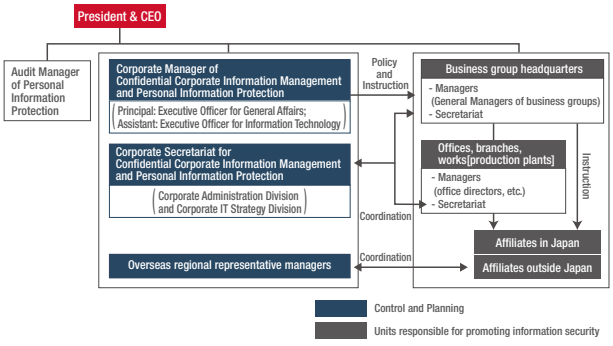
"PrivacyMark"

Framework and Guidelines

The President & CEO assigns a Corporate Manager for Confidential Corporate Information Management and Personal Information Protection (hereafter Corporate Manager), who assumes overall responsibility for confidential corporate information management, and an Audit Manager for Personal Information Protection, who is responsible for implementing and reporting the results of personal information audits. The Corporate Manager assumes overall responsibility for information security, and the Corporate Secretariat for Confidential Corporate Information Management and Personal Information Protection (hereafter Corporate Secretariat) under the Corporate Manager is in charge of planning and promoting information security measures. Responsibility for the actual utilization and management of confidential corporate information and personal information lies with the General Manager of each business group (the Confidential Corporate Information Management and Personal Information Protection Manager) and the manager of each business site (office directors, etc.). The Business Group Secretariats and Business Office Secretariats under the General Manager of each business group and manager of each business site strive to ensure information security by maintaining close coordination and regularly holding meetings with the Corporate Secretariat. In the event an incident were to occur, reports and instructions would be given in keeping with this framework and appropriate responses would be taken to prevent secondary damage.

Business groups and offices (offices, branches, works [production plants]) issue instructions and guidance on information security to affiliates in and outside Japan. Paying special attention to the circumstances and special characteristics of overseas affiliates, the Corporate Secretariat places overseas regional representative managers at sites in the Americas, Europe, China, and other Asian countries and coordinates with them to ensure information security.

Framework (Mitsubishi Electric Group)



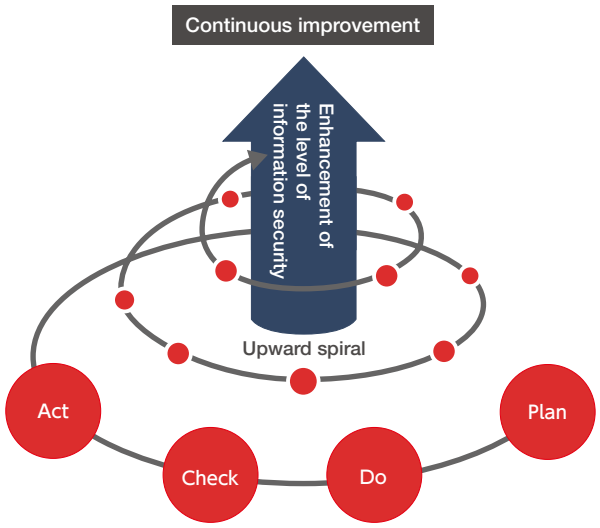
Management Principles

The Mitsubishi Electric Group practices confidential corporate information management and personal information protection utilizing a continuous improvement approach implemented using the Plan, Do, Check, Act (PDCA) cycle, and employs four security measures to ensure proper management and protection of confidential corporate information and personal information from the organizational, human, physical, and technological perspectives.

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

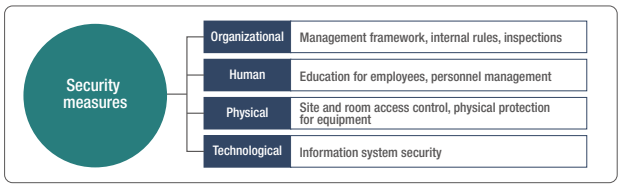
Organizational security measures consist of systems such as a management framework, internal rules, and internal audits to safeguard confidential corporate information and personal information. They are revised as needed to ensure no loss of effectiveness due to changes in the operating environment.

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

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

Technological security measures consist of information system security efforts such as cyber-attack countermeasures.

Four security measures



Global activities

To maintain and improve the information security level of the Mitsubishi Electric Group as a whole, including overseas affiliates, various inspections are conducted as appropriate for each information security system, as prescribed in the Guidelines to Information Security Management Rules for Affiliated Companies.

Information Security Regulations and Guidelines

Committed to living up to its Declaration of Confidential Corporate Information Security Management and Personal Information Protection Policy, Mitsubishi Electric Corporation has established information security regulations and guidelines alongside the four security measures, and reviews them as necessary to stay in compliance with current laws. In addition, we have similar rules for personal information protection and affiliates.

Item	Basic regulations
Security measures	**Organizational security measures:** Regulations on confidential corporate information security management
	Human security measures: Regulations on the work of employees
	Physical security measures: Physical security guidelines
	Technological security measures: Regulations on information security management

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 operating 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 affiliates. 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 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 affiliates in and outside Japan.

Inspections related to information security

	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 affiliated companies.
	Personal information protection audits (Personal information protection management system audits)	In Mitsubishi Electric, the status of personal information protection is internally audited under the supervision of the Audit Manager for Personal Information Protection. In affiliated companies in Japan that have been granted the right to use the "PrivacyMark," the same internal audit is conducted by the audit manager in each company.

Information Security Education

Mitsubishi Electric provides the following education programs to foster a corporate culture that enforces the proper handling of confidential corporate information and personal information.

Education for all employees

An e-learning program on information security is offered once a year to all of the Company's roughly 50,000 employees, to disseminate thorough knowledge of various issues on information security, including Mitsubishi Electric's policies, the status of information leakage incidents, laws and regulations on the protection of personal information, the Unfair Competition Prevention Act, and security measures (human, physical, technological, and organizational) to be taken by all employees.

Education corresponding to each career stage

Education on confidential corporate information management and personal information protection is provided to new employees, employees in their twenties and thirties, and newly appointed section managers, so that they may fulfill the roles that are expected of them at each career stage.

Exercises to practice handling spoofed e-mails

As a measure against cyber-attacks, Mitsubishi Electric regularly conduct exercises that allow all employees, including officers, to verify that they know how to handle spoofed e-mails. Employees of affiliates in Japan can participate in this exercise. At overseas affiliates in the Americas, Europe, and China, 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 information leakage incidents that have occurred overseas.

Activities for Personal Information Protection

Personal information protection

In efforts to protect personal information, Mitsubishi Electric first created company rules on personal information protection in October 2001, and since then it has required all employees and affiliated persons to obey those rules strictly. Mitsubishi Electric issued a personal information protection policy in 2004, complying with 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 maintained our "PrivacyMark" certification until the present.

We have also conducted a review of our internal regulations to ensure a proper response to Japan's amended Act on the Protection of Personal Information, which went into force in May 2017.

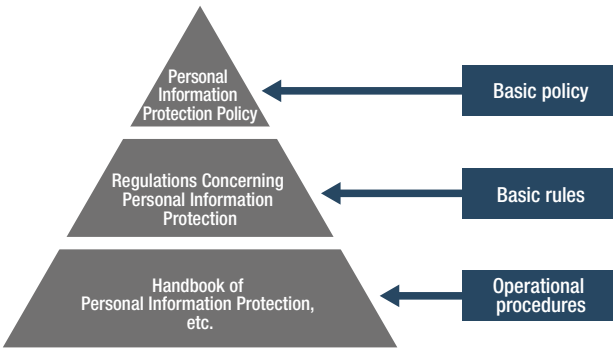
Proper handling of personal information

Mitsubishi Electric handles personal information appropriately; we acquire it by specifying purpose of use, use it only within the intended scope, and provide it to a third party only with prior consent from users.

PrivacyMark

Mitsubishi Electric and some affiliates in Japan have been granted the right to use the "PrivacyMark."

System of rules for personal information protection



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.

Response to the EU General Data Protection Regulation (GDPR)

The Mitsubishi Electric Group handles personal data from the EU in an appropriate manner with due consideration to the General Data Protection Regulation (GDPR) that was put into force in the EU in May 2018 as a framework to protect privacy.

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 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. Moreover, the agreement includes a special clause that provides for the protection of the personal information that we have submitted.

Information Security Initiatives: Technological and Physical Security Measures

Cyber-Attack Countermeasures

Cyber-attacks have become a major threat for businesses. As they are growing increasingly sophisticated and diverse year-by-year, it is becoming difficult to prevent them. The Mitsubishi Electric Group deploys cyber-attack countermeasures through a multilayered defense consisting of a number of different defense measures stacked on top of each other. Furthermore, there are cyber-attacks that cannot be prevented entirely with a multilayered defense alone. Accordingly, we monitor cyber-attacks and have put in place a system to respond immediately should a case occur, in an effort to prevent or minimize damage.

Internet websites are constantly exposed to many external threats, and so we only launch websites that are approved in order to maintain high security level.

Multilayered defense

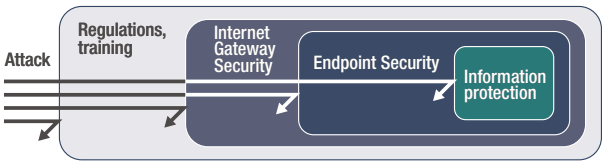
The Mitsubishi Electric Group has implemented three levels of technological measures as a multilayered defense: Internet Gateway Security, Endpoint Security, and information protection. Internet Gateway Security block unauthorized access and malware from entering the company and prevent information from leaking out of the company through the installation of various security devices at points of contact between the Internet and internal networks to monitor and control communications including email and web traffic.

Attacks that slip through Internet Gateway Security are handled by Endpoint Security. Endpoint Security include the prevention of malware infections through the detection and elimination of malware using anti-malware software and the application of security patches that fix software vulnerabilities as well as the attempt to contain attacks and localize damage by defining and applying a security policy for Endpoints. That is why we centrally control Endpoints and implement thorough measures.

We have also implemented information protection in case a Endpoints happens to become infected with malware. Information protection involves storing information, according to its degree of importance, in secured locations and limiting its use to people who are given prior approval. In preparation for cyber-attacks, we take measures such as storing information in document management systems that cannot be accessed from outside and automatically encrypting information retrieved. The aim is to prevent access to information and to prevent information leaks even if document management systems were to be accessed. We also take information operation logs and regularly check for suspicious operations.

Although we have taken various measures such as those mentioned above, technological measures alone are not sufficient against sophisticated cyber-attacks. Accordingly, we also develop and enforce security regulations and provide training to employees.

Multilayered defense

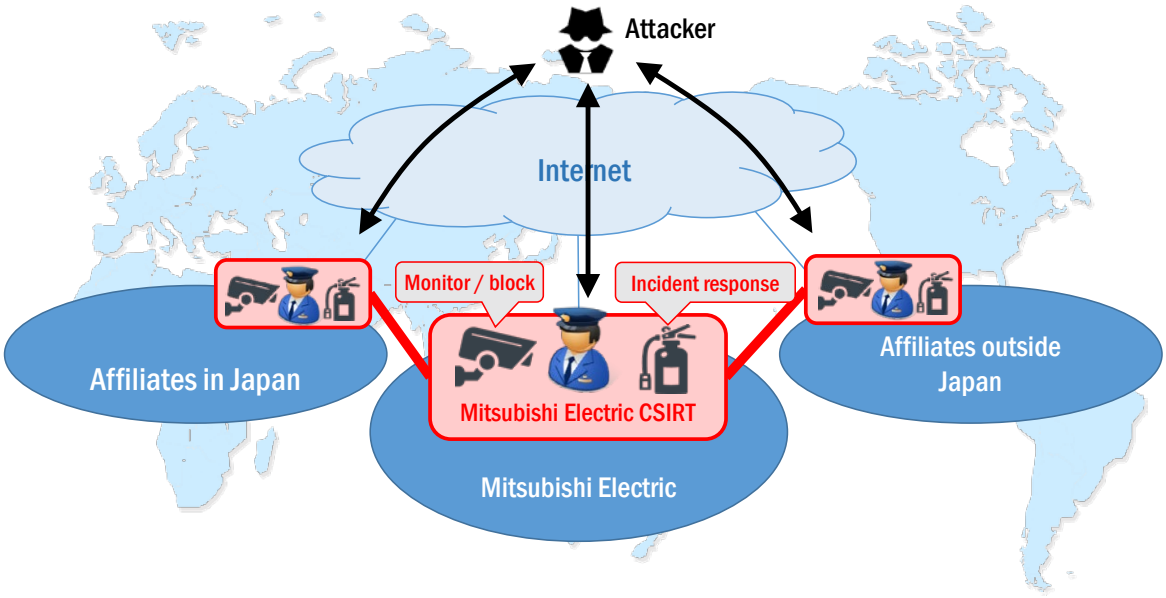


Computer Security Incident Response Team

The Mitsubishi Electric Group has established the Mitsubishi Electric Computer Security Incident Response Team (CSIRT) to monitor cyber-attacks and respond immediately to any incidents that occur. We have also put in place a monitoring system for affiliates in and outside Japan, as their handling had tended to be inadequate before. Suspicious behavior can be detected and safety confirmed by monitoring communications through the above-mentioned Internet Gateway Security, thereby quickly detecting and blocking cyber-attacks.

Through the Endpoint Security, we can collect and assess malware detection information and the status of Endpoint Security. Were an incident detected, the above arrangement would immediately be used to assess the damage situation, take appropriate emergency responses, perform restoration, and limit damage as much as possible. Later, we would analyze the incident in detail and support the implementation of permanent measures by the department where the incident occurred.

Mitsubishi Electric CSIRT



Management of Internet websites

Learning from an incident caused by unauthorized access in the past, the Mitsubishi Electric Group only launch websites that are approved in order to maintain high security level. It does not permit websites to go live unless a security probe has been conducted and problems resolved in advance.

We also regularly inspect our Internet websites and assess their management status in an effort to remove unneeded websites and strengthen the security measures of websites with inadequate security. Additionally, if we find an unauthorized website, a pentetration test is carried out immediately.

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's 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.

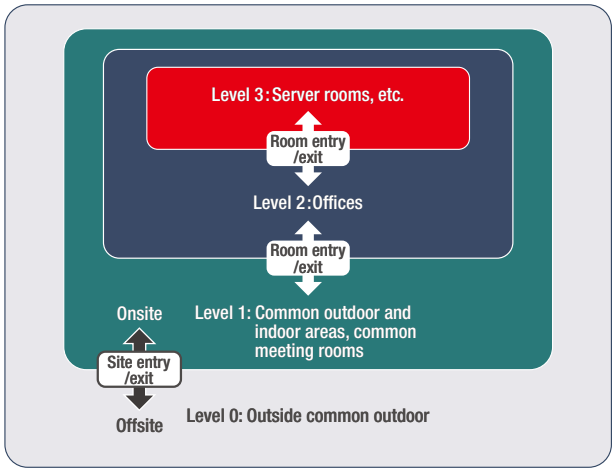
Designation of area levels

	Level	Evaluation criteria	Example	
High ↑	Area level 3	Onsite; areas that can be accessed and used only by specific Mitsubishi Electric employees	Server rooms, data rooms, development rooms	Onsite
	Area level 2	Onsite; in principle, areas that can be accessed and used only by Mitsubishi Electric employees	Offices	
	Area level 1	Onsite; areas that can be used by Mitsubishi Electric employees, employees of affiliates (including sales representatives), and customers that have gone through an entry procedure	Common outdoor and indoor areas, common meeting rooms, corridors	
Low ↓	Area level 0	Offsite	Outside common outdoor areas	Offsite

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



Note: We use the MELSAFETY series of security systems for entry/exit access control, as described on page 16.

Initiatives Regarding Security Quality of Products and Services

Initiatives Regarding Security Quality of Products and Services

In April 2019, Mitsubishi Electric reinforced its initiatives with the establishment of the Mitsubishi Electric Product Security Incident Response Team (PSIRT) as an internal framework to handle the security quality of products and services.

Roles of Mitsubishi Electric PSIRT

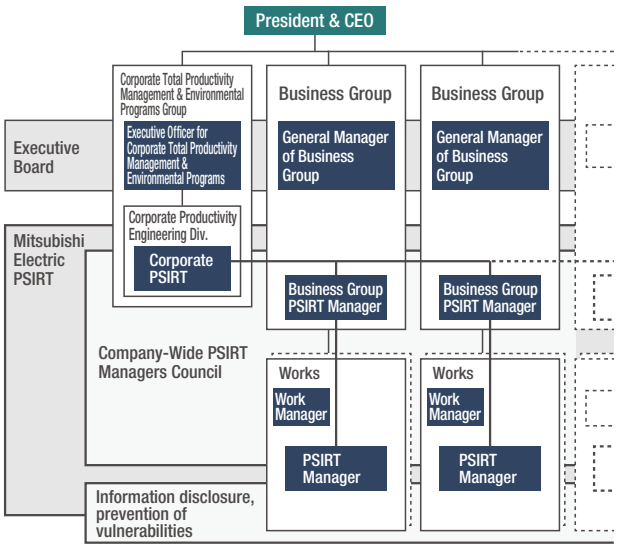
The following are Mitsubishi Electric PSIRT's roles:

- 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

Mitsubishi Electric PSIRT framework

Mitsubishi Electric has appointed PSIRT managers to every business group headquarter and works to handle any problems and drive risk reduction as persons responsible for product and service security. We have also established a corporate PSIRT in the Corporate Total Productivity Management & Environmental Programs Group to provide overall supervision and work to increase the security quality of products and services.

Mitsubishi Electric PSIRT framework



Information Security Solutions

IT

Information security solutions for IT systems

Cyber-attacks have been become increasingly advanced and sophisticated in recent years. In response, we establish information security systems for customers' IT systems and provide solutions 24/7 monitoring and management plus incident response.

1. Importance of information security

In recent years, Internet-connected IT systems have become important tools that support corporate activities. In exchange for convenience, however, the Internet poses the dangers of unauthorized access and cyber-attacks. To reduce these risks, it is essential to implement appropriate information security measures. Were personal information or a business partner's confidential information leaked, not only would damages be sought, but the incident could also have grave repercussions for management of the business itself, including a drop in social credibility. Moreover, if a system were shut down to prevent damage from spreading, work would also come to a halt during that time, and if that were to last for a long time, business survival could even be endangered.

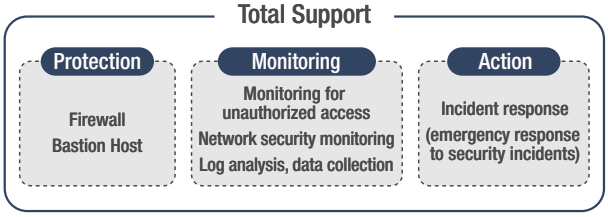
The purpose of information security measures goes beyond the protection of corporate and customer information and the prevention of financial damage; they are tools to maintain a company's image and brand and to protect its very business activities.

2. Basic information security measures

In IT system information security it is important to have a combination of measures in place, including protection, monitoring, and action. Daily monitoring and management is essential to ensure that security holes (shortcoming of a computer program) do not appear and unauthorized access does not occur without being detected.

It is also important to regularly review information security measures, including measures against new threats such as the latest viruses.

Basic information security measures offered by MIND*



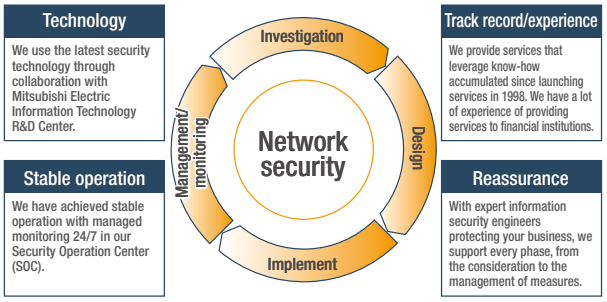
* Mitsubishi Electric Information Network Corporation: A Mitsubishi Electric group company which mainly provides information communication services.

3. Mitsubishi Electric Group's solutions

Companies need to take measures against unauthorized access from the outside and cyber-attacks. However, since there are a wide variety of security measures, which require engineers with a high level of expertise and know-how, there is a limit to what companies can do on their own.

The Mitsubishi Electric Group offers CyberMinder, a comprehensive information security solution named as CyberMinder which performs a PDCA cycle of adoption, management/monitoring, investigation/analysis, and consideration/design.

PDCA cycle in information network security

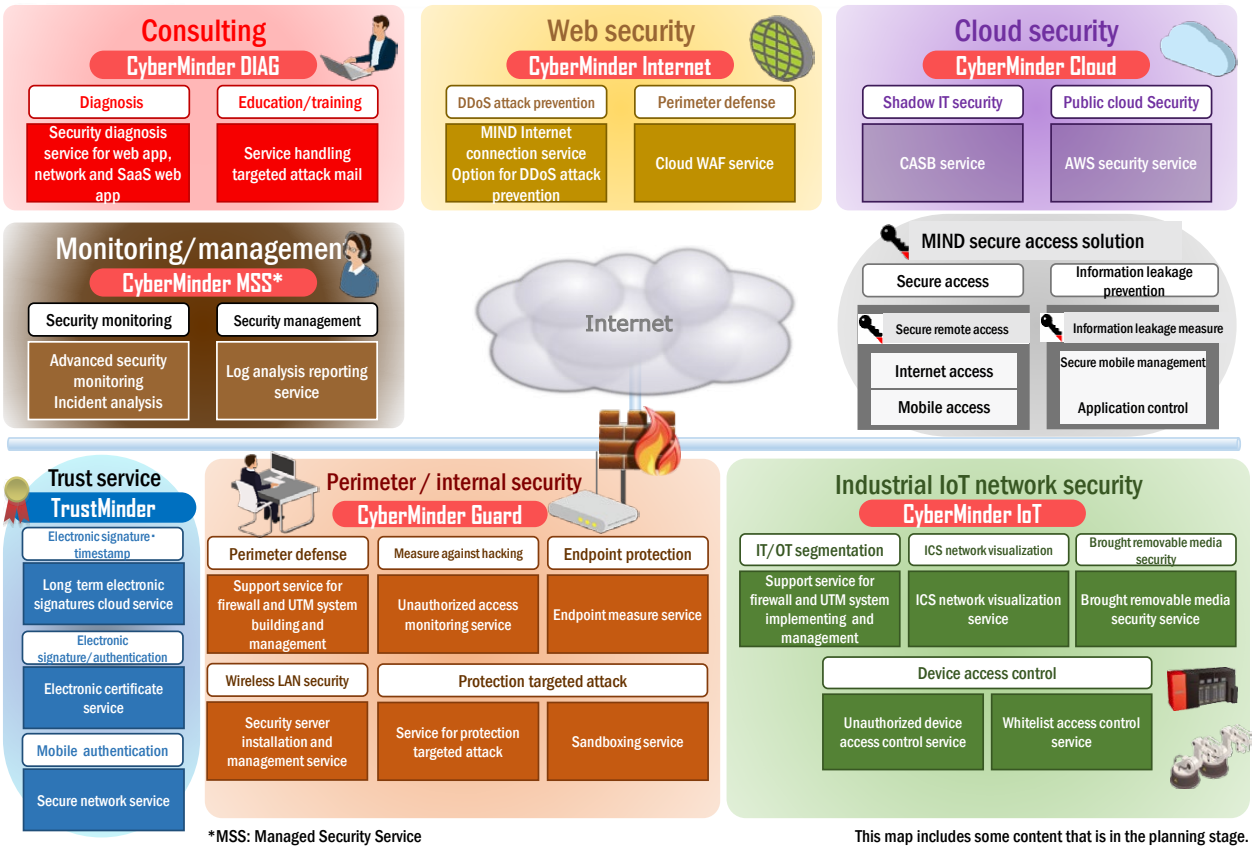


(1) CyberMinder

Information Security measures are wide-ranging including, in addition to those mentioned above, proactive measures and defense measures to prevent unauthorized access and cyber-attacks as well as after-the-fact measures in case of situations such as a malware infection. Furthermore, recently there has been a need for information security measures for IT systems based on cloud infrastructure trends and increase of IoT devices.

CyberMinder offers comprehensive information solutions that cover today's evolving IT systems, including a proactive measure (CyberMinder DIAG), a defense measure (CyberMinder Guard), a security measure for industrial IoT (CyberMinder IoT), a cloud security measure (CyberMinder Cloud), web security (CyberMinder Internet), and 24/7 monitoring and management of these measures (CyberMinder MSS [Managed Security Service]).

CyberMinder solution map



*MSS: Managed Security Service

This map includes some content that is in the planning stage.

(2) 24/7 monitoring center serves as the backbone of monitoring and management

We monitor and manage customers' systems continually 24/7. When security alerts are detected, we notify the customer depending on the degree of urgency, allowing us to reduce the customer's management burden while still responding swiftly to security incidents.

Using Security Information and Event Management (SIEM) infrastructure equipped with analysis rules independently developed by the Mitsubishi Electric Group, we gather and automatically analyze logs from servers, network devices, and security devices. The detection requirements, threshold to detect abnormal access (e.g., access frequency within a certain period of time), and black list data are updated daily, and we can make customizations suited to a customer's environment.

Depending on the seriousness of an incident, it will escalate up to an analyst, who will quickly assess the incident from a higher point of view and provide the appropriate result. Artificial intelligence (AI) is used in the investigation and analysis, reducing the time it takes to get the result. An investigation drawing on a high level of expertise and widespread coordination are used to protect the customer from cyber-attacks.

(3) Initiatives to keep pace with changes in IT systems

a. CyberMinder IoT: Cyber Security for IoT

With falling IT costs, the increase of IoT that connects all kinds of devices to networks, and advances in big data analysis techniques, the move to make use of information and communication technology (ICT) in manufacturing is progressing rapidly. With that, manufacturing site networks become connected to external networks, increasing the risk that they will become the target of cyber-attacks.

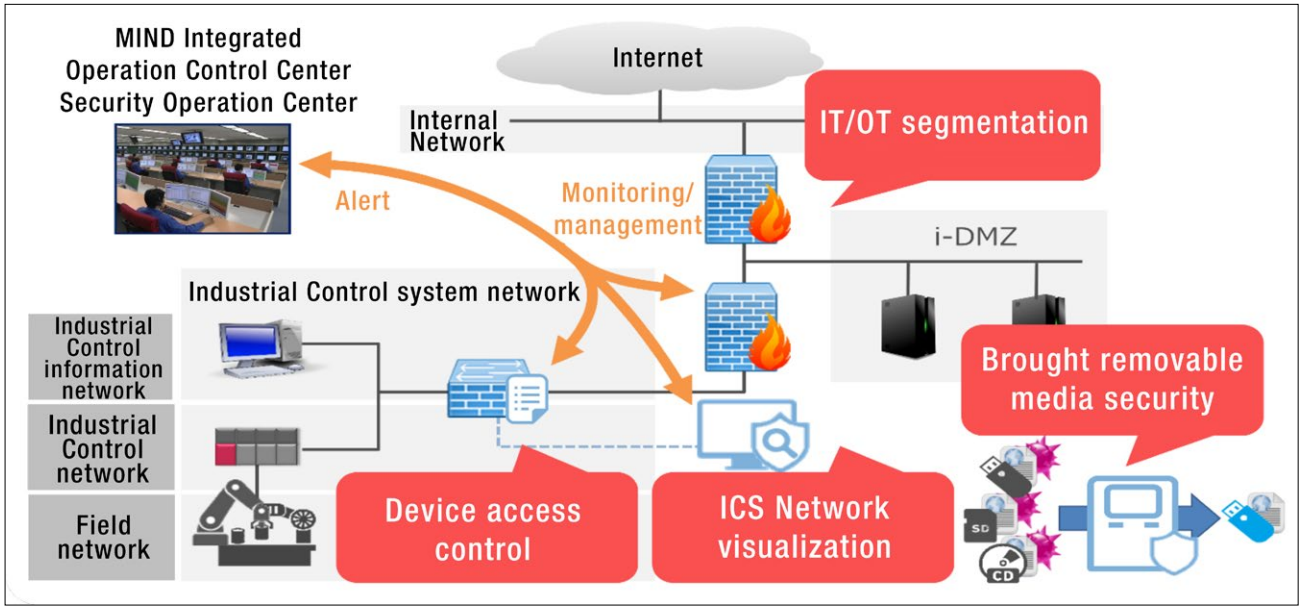
The Mitsubishi Electric Group combines IoT technology that it has worked on as a manufacturer with information security know-how for IT to provide IT/OT segmentation between the manufacturing site network and IT system, ICS network visualization, Device access control, and measures against removable media brought into a manufacturing site.

b. CyberMinder Cloud: Cyber Security for the cloud

The cloud creates an environment in which to use IT systems by combining various Internet-based services. It has a number of conveniences such as flexible scalability that differs from the on-premises in which a company purchases its own machines and manages them in a datacenter or machine room, as well as a overhead management burden from not possessing those assets.

In regards to information security, however, from the user's perspective, the internal workings of the cloud are a black box, which has been noted to appear the different type of risks. The Mitsubishi Electric Group offers appropriate information security measures even for the cloud, the use of which is being increasingly promoted. We provide total support services in every phase from investigation to design, implement, and management.

CyberMinder IoT



Access Control (MELSAFETY series)

Mitsubishi Electric's MELSAFETY series of integrated building security systems

The MELSAFETY series of integrated building security systems is Mitsubishi Electric's answer to the advanced security needs of all kinds of buildings in an era that demands stronger compliance and management of confidential information. Positioned at the core of security solutions, the MELSAFETY series enables an efficient access control system and promotes energy savings by linking with information systems and building facilities such as elevators, air conditioning, and lighting as well as integrated control of access logs and video footage. The system has been installed in numerous buildings over the 20-plus years since it was first launched.

1. Contributing to society through the security delivered by the MELSAFETY series

- Stopping trespassing, stopping inside crime, and establishing a safe, secure, and comfortable society
- Providing building managers with more efficient and higher quality building operation and management
- Providing end users with a comfortable environment
- Providing building owners with greater added value

2. Features of solutions provided by the MELSAFETY series

The MELSAFETY series of access control system offers a wide lineup of authentication terminals which enable contactless card authentication, hands-free authentication with wireless tags, and biometric authentication including penetrated light fingerprint authentication and face recognition. Another feature is the system's high flexibility, which makes it compatible with customers' diverse environments and requirements. Furthermore, Mitsubishi Electric's engineers ascertain each customer's security level and operational challenges and design each system individually to provide optimal access control solutions. We also have a full after-sales service system to respond flexibly to customers' operational changes.

Additionally, by using individuals' identification information (IDs) in the access control system to control building facilities such as elevators, air conditioning, lighting, and surveillance cameras, the system can contribute various solutions to customers, including greater convenience, energy savings, operational efficiency improvement, and asset value enhancement.

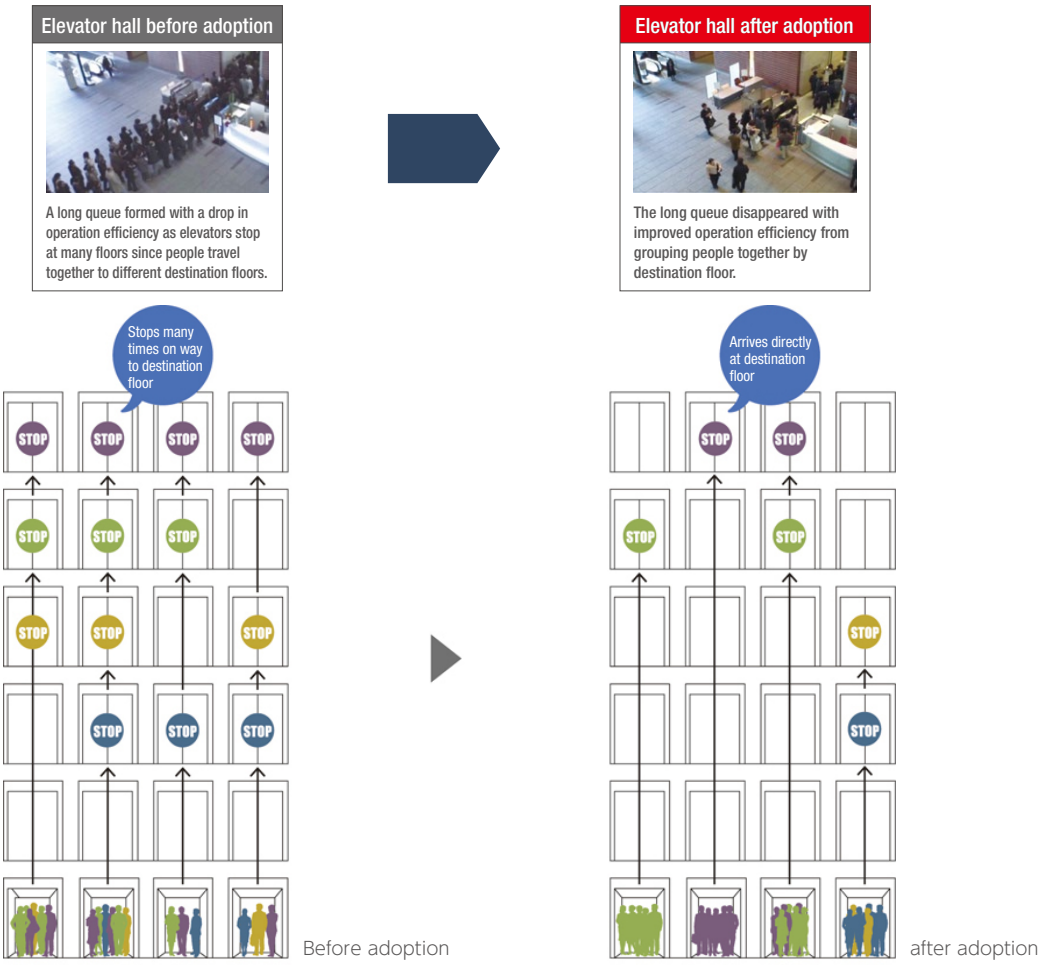
3. Examples of specific solutions

In building operation and management, the status of doors' locking and unlocking can be centrally controlled through monitors in the control room where MELSAFETY is set up. The on-site situation can be checked efficiently during an emergency by linking to surveillance cameras, and several buildings and sites can be managed centrally. By connecting with a personnel management system, the management workload can be reduced, for instance by automatically changing access privileges when personnel transfer.

By using the MELSAFETY series' presence control features to control things such as air conditioning and lighting, end users can expect greater comfort and convenience in the office environment. Individuals can be spared the trouble of making work requests by linking access logs to an attendance management system.

The MELSAFETY series also helps increase a building's added value using interlocking control with elevators. In high-rise office buildings, people waiting for elevators can cause major congestion at times such as the start of working hours in the morning. In addition, it can be difficult to make progress even after getting into an elevator, if it stops at every floor. This morning bottleneck is stressful for workers and lowers the building's image. The MELSAFETY access control system reduces the number of floors an elevator stops by using identification information (IDs) to determine a user's destination floor and assign an elevator for a group of people who are going to the same floor. This improves operation efficiency, resolving the above problems.

Before/after comparison of adoption of interlocked elevator access control system (Mitsubishi Electric example)



MELOOK 3 Series of Network Cameras

Network cameras nowadays require greater features and performance than the mere image recording and surveillance of the past, with growing needs for more sophisticated uses through video footage analysis.

Mitsubishi Electric is striving to help create a safer, more secure society by providing network cameras that meet rapidly advancing and expanding video surveillance needs through its latest lineup—the MELOOK 3 series.

1. The MELOOK 3 Series

We offer a rich lineup to meet diversifying surveillance needs, from a basic type equipped with basic functionality, to a multi type suited to multipoint surveillance and large-scale system establishment via LAN connections, to a coaxial type that enables digital and full HD utilizing existing coaxial cables.

<Basic Type>

The optimal type for simple setups with 16 cameras connected to one recorder. Up to 32 cameras can be connected through a HUB, doubling the surveillance coverage and reducing past blind spots. Comes with a wide variety of standard features including a face thumbnail function that allows simple searching from recorded footage.

<Multi Type>

The optimal type for setting up large-scale systems, enabling up to 64 cameras to be connected to one recorder. This type achieves high-precision video surveillance, scalability, and low power consumption, which are required by large supermarkets and medium-size to large buildings. Also, up to 512 cameras can be centrally managed together on a single computer. With video and sound recording, it ensures evidence and improves the crime deterrence effect.

<Coaxial Type>

Achieve full HD high functionality surveillance simply by changing cameras and recorders while making effective use of coaxial cables for existing analog cameras. Set up the system at low cost in a short time by making use of existing wiring.

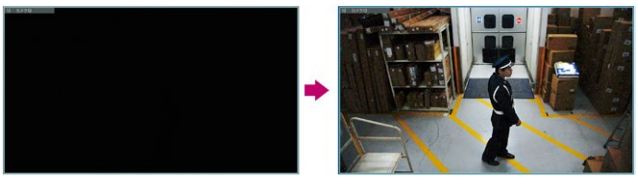
Video technology of the MELOOK 3 series

We have improved the video technology to enable smooth display at 30 frames per second (30 fps) even when displaying the images of 16 cameras on a split screen with full HD compatibility, New Digital Sensitization, and Super Fine View Ⅲ.

<Full HD compatibility>

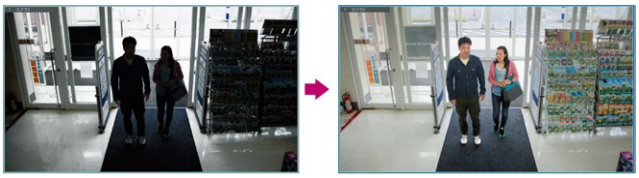
●Full HD video (1920×1080)　●Analog camera video　●Megapixel camera video　●Full HD camera video

<New Digital Sensitization>



●Shooting in the dark　●New Digital Sensitization

<Super Fine View Ⅲ>



●When backlit　●Super Fine View Ⅲ

<30-fps display with screen split 16 ways>

Up to 16-way split/30 fps display

*1 16-way split/30 fps display applies to either live viewing or recorded playback.

*2 16-way split/30 fps display is possible when there are 16 MELOOK 3 cameras connected.

2. Examples of security delivered by the MELOOK 3 series

Achieve a high security effect everywhere, indoors and outdoors, by eliminating blind spots and enabling clear discrimination of bank notes and product names through full HD display and clear display even in poor conditions such as backlit entrances and parking lots/warehouses at night. Also ensures evidence and improves the crime deterrence effect and enables long-period recording as well as video and sound recording.





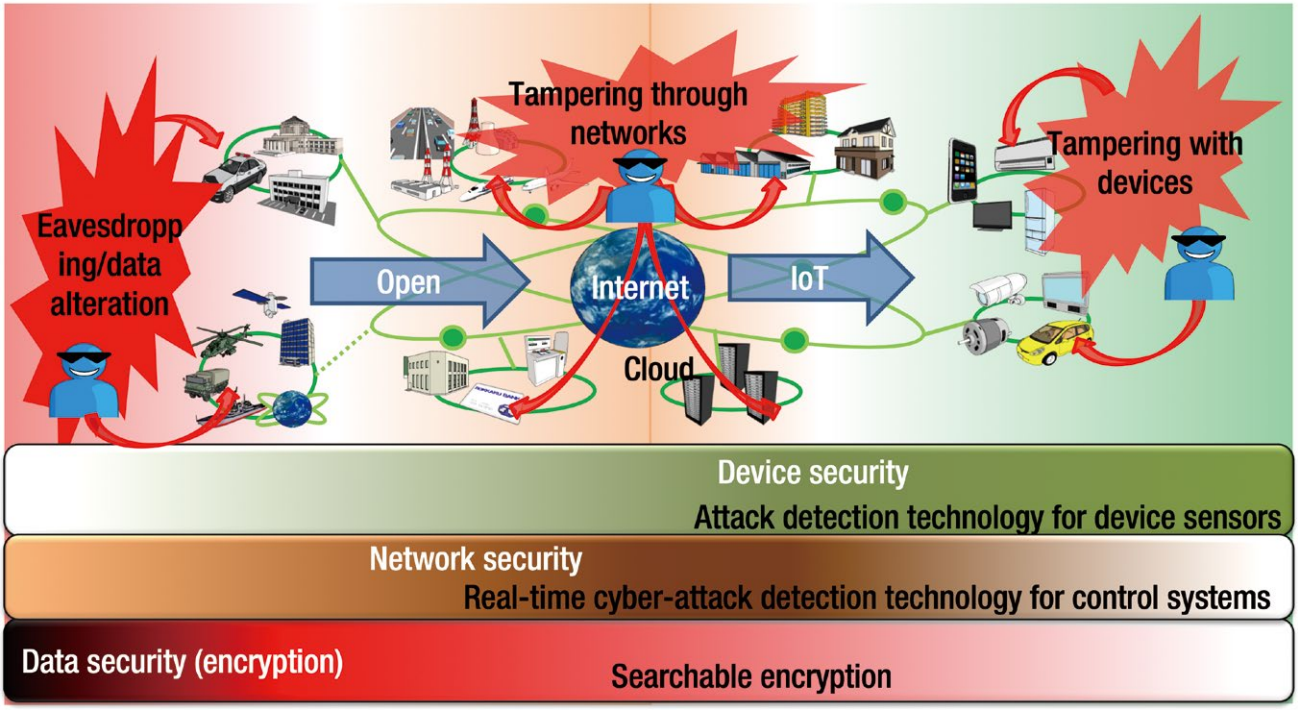
Security-Related R&D

Security-Related R&D

Background

In recent years, progress in IoT has increased the risks of confidential information leakage and malfunction of critical infrastructure due to network-based cyber-attacks. In May 2017, the WannaCry virus, which exploited vulnerabilities in PCs, spread to 150 countries, causing a succession of damage that brought services and operations to a halt in a wide range of fields including finance, railways, and manufacturing. Since the Japanese government put the Basic Act on Cybersecurity into force in January 2015, it has established the Cybersecurity Strategy Headquarters in the Cabinet and the National center of Incident readiness and Strategy for Cybersecurity (NISC) in the Cabinet Secretariat and has promoted the formulation of policies for cybersecurity measures. Also, in 2019, Japan's Ministry of Economy, Trade and Industry formulated cybersecurity measures needed in "Society 5.0," a national policy achieved by integrating cyberspace and physical space in a sophisticated manner, as the Cyber/Physical Security Framework (CPSF), and it is expected to strengthen cross-industrial security, including in defense, electricity, homes, buildings, and manufacturing.

Cybersecurity measures must provide comprehensive security for data, networks, and devices. Encryption, which has long been used to prevent eavesdropping and data alteration, is representative of data security. With the spread of the Internet, on the other hand, tampering with information systems through networks has become serious, and so there is also a need for network security to protect and detect against such tampering. And, in the era of IoT, in addition to data and network security, device security is also important to prevent tampering with devices that are connected to networks.

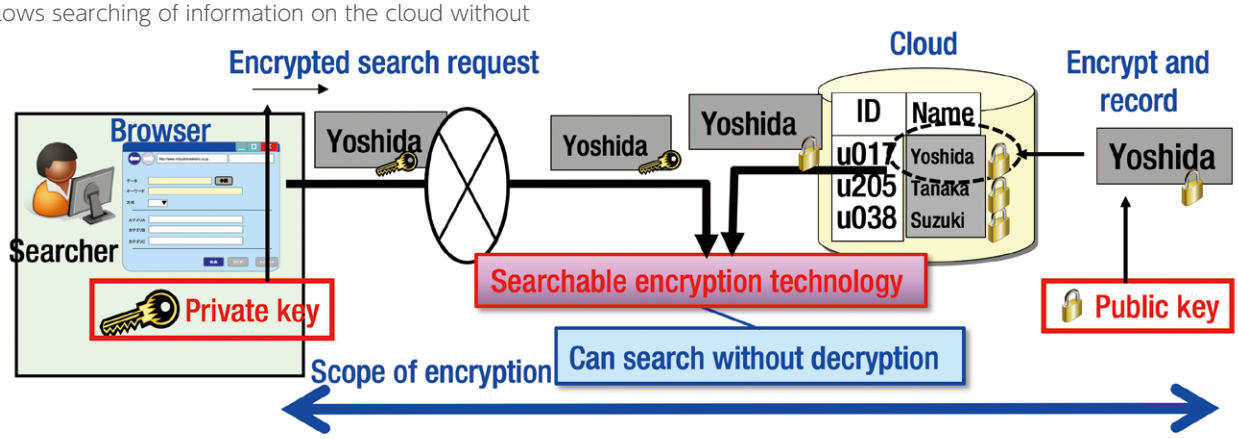


Mitsubishi Electric Group's R&D initiatives

In addition to general R&D into security, we are also engaged in R&D that anticipates the needs of the IoT era by developing differentiated technologies in the fields of data security, network security, and device security.

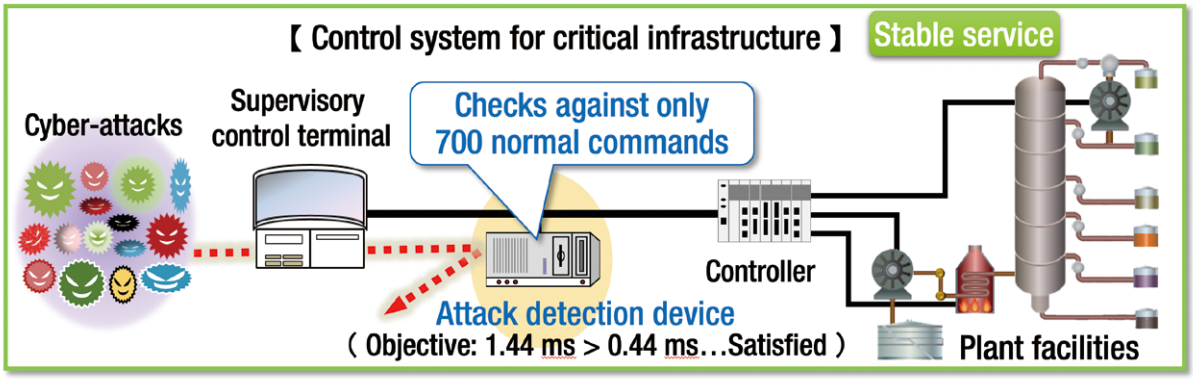
Data security: Searchable encryption

In the IoT era, it is expected that added value will be created through the processing of Big Data by gathering and analyzing information on people and devices in the cloud. However, since information on people and devices is highly confidential, it should be encrypted when stored in the cloud. When searching encrypted information, on the other hand, it has conventionally been necessary to first decrypt it in the cloud, which posed the concern of confidential information leakage (see the figure below). In response, we developed searchable encryption that allows searching of information on the cloud without decrypting it. This technology enables information to be kept private while still being usable. At present, we are working to develop the technology so that it can be applied to cases where device information and privacy information such as customer information and device operation information are processed in a public cloud. We are also working on development of homomorphic encryption, which expands the processing that can be performed on encrypted data from search to calculations such as statistical processing.



Network security: Attack detection technology

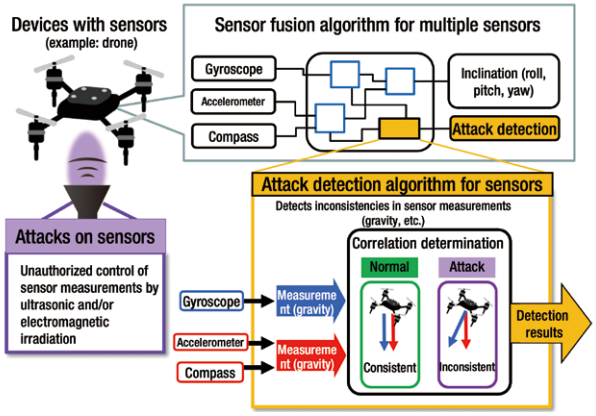
As IoT pervades infrastructure fields, the strengthening of network security for critical infrastructure that underpins the foundation of social life has become an important issue. Until now, the safety of critical infrastructure for electricity, gas, water, chemicals and petroleum has been protected through rigorous operational management in addition to traffic control such as physical isolation and firewalls. In recent years, however, there has been a rise, especially overseas, in sophisticated cyber-attacks that penetrate control systems for critical infrastructure and cause damage such as power blackouts and equipment destruction by sending fake control commands disguised as control commands from a supervisory control terminal. In response, calls are increasing for new technical responses. In answer, in May 2017, the Mitsubishi Electric Group announced technology to detect cyber-attacks without reducing real-time control capability.[*1] A feature of the system is that it defines the detection rules based on the normal commands for each operational state of the control system and interprets deviations from the normal commands as an attack. At present, we are working at applying the technology to various control systems.



Note 1) The development results were partially supported by a project called "Cyber-Security for Critical Infrastructure" undertaken by the Control System Security Center (CSSC) as part of the cross-ministerial Strategic Innovation Promotion Program (SIP) promoted by the Council for Science, Technology and Innovation and managed by the New Energy and Industrial Technology Development Organization (NEDO).

Device security: Technology to detect direct attacks on sensors

Optimal automatic control based on data measured by sensors is becoming increasingly common in devices such as in-vehicle equipment, production facilities, drones and more. At the same time, there is a need for measures to counter cyber-attacks, in order to create a secure, safe, and comfortable society. In response, the Mitsubishi Electric Group focused in on internal computation of sensor fusion algorithms that combine measurement data from multiple sensors, which play a key role in automatic control of devices such as drones. We assessed and tested the safety of sensor fusion algorithms, which had been unproven. Then, by embedding a proprietary "attack detection algorithm for sensors" into sensor fusion algorithms, we became the first in the world to develop sensor security technology that detects attacks based on measurement data that is generated in a malicious attack. This development was announced in February 2019.[*2]



Note 2) The development was partially supported by business commissioned by the New Energy and Industrial Technology Development Organization (NEDO) under Japan's National Research and Development Agency.

Conclusion

The companies that provide devices and systems need to embed security measures appropriately in order to improve the security of IoT systems. In order to encourage companies to embed security measures, it is important for each industry to establish consensus about how far measures should go to address what kinds of threats. In addition to R&D into differentiated technologies like those introduced above, Mitsubishi Electric also participates actively in consensus building for security measures in different industries and will continue contributing to the creation of a secure, safe, and comfortable society in the IoT era.

MITSUBISHI ELECTRIC CORPORATION

www.MitsubishiElectric.com

eco Changes

for a greener tomorrow

Eco Changes is the Mitsubishi Electric Group's environmental statement, and expresses the Group's stance on environmental management. Through a wide range of businesses, we are helping contribute to the realization of a sustainable society.

Inquiry: Information Security Center, Corporate Administration Division, Mitsubishi Electric Corporation
Tokyo Building, 2-7-3, Marunouchi, Chiyoda-ku, Tokyo 100-8310, Japan
Phone: 81-3-3218-2210