

Risk Management

Canon's Approach to Risk Management

Canon Inc. recognizes that the improvement and implementation of a risk management system to deal with serious risks that Canon Group may face in the course of business is extremely important to ensure the proper operation of the Group and to continually improve corporate value.

Risk Management System

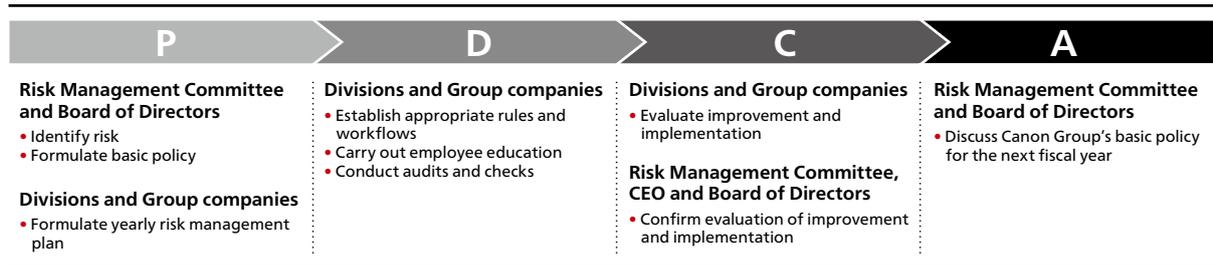
Canon Inc. has established a risk management committee based on a resolution of the Board of Directors. Chaired by the Executive Vice President, the committee has established three subcommittees: the Financial Risk Management Subcommittee, Compliance Subcommittee, and Business Risk Management Subcommittee.

The Risk Management Committee develops

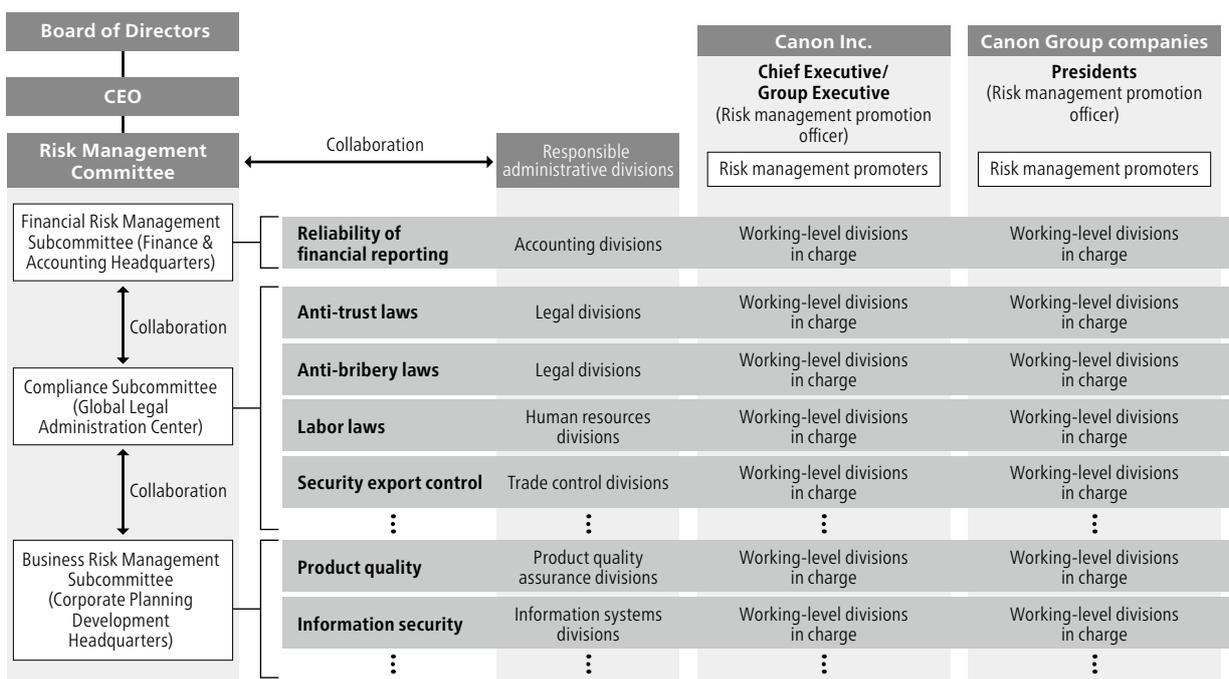
various measures to promote the Canon Group's risk management activities, including identifying any significant risks (violations of laws and regulations, inappropriate financial reporting, quality issues or information leaks, etc.) that the Canon Group may face in the course of business.

The committee creates an annual basic policy for risk management activities and, after obtaining the approval of the Board of Directors, carries out risk management activities at Canon Inc. divisions and Group companies. The committee evaluates the improvement and implementation of the risk management system for each division and Group company, and reports the result of such evaluation to the CEO and Board of Directors. In 2016, the result of the evaluation did not discover any major flaws in the system.

Processes for Improvement and Implementation of Risk Management System



Risk Management Promotion System



Based on the above basic policy, the heads of Canon Inc. divisions and presidents of Canon Group companies, as a risk management promotion officer, formulate a yearly risk management plan for their own division or Group company, and assume the responsibility of promoting their own risk management activities. Risk management promoters appointed for each division and Group company coordinate risk management practices.

Additionally, Canon Inc. administrative divisions with jurisdiction over miscellaneous risks associated with business activities, including the legal division, human resources division, security trade control division, and quality assurance division, control and support the risk management activities of each division and Canon Group company.

Groupwide Risk Management Communication

During training for newly appointed Canon Group executives conducted by the human resources division, Canon Inc. educates them on the importance of autonomously improving and implementing a risk management system at each company and the role of executives in improving and implementing such system.

Similarly, when the human resources division conducts training for newly appointed general managers and managers, it educates them on the importance of the system to manage legal risk and the role of management in constructing such system.

In addition, an intranet website provides employees of Canon Inc. and Group companies with timely information on the Canon Group's approach regarding risk management and updates on activities.

Financial Risk Management

The Financial Risk Management Subcommittee carries out activities to strengthen internal controls pertaining to financial risks for the entire Canon Group, including compliance with Japan's Companies Act and Financial Instruments and Exchange Act as well as the United States' Sarbanes-Oxley Act.

We endeavor to make qualitative improvements in ensuring the reliability of the Group's financial reporting. We support independent initiatives and self-driven educational activities at Group companies as they implement the PDCA cycle (review business procedures for financial risk).

As a result of these initiatives, Canon's accounting auditor determined that the company's internal

controls related to financial reporting were effective in fiscal 2016.

Compliance

The Compliance Subcommittee works to promote corporate ethics in accordance with the Canon Group Code of Conduct, and to improve the Group's legal risk management system.

Sections of the Canon Group Code of Conduct (Extract)

Management Stance

1. Contribution to Society

- Provision of Excellent Products • Protection of Consumers
- Preservation of the Global Environment
- Social and Cultural Contributions • Communication

2. Fair Business Activities

- Practice of Fair competition • Observance of Corporate Ethics
- Appropriate Disclosure of Information

Code of Conduct for Executives and Employees

1. Compliance with Corporate Ethics and Laws

- Fairness and Sincerity • Legal Compliance in Performance of Duties
- Appropriate Interpretation of Applicable Laws, Regulations and Company Rules

2. Management of Corporate Assets and Property

- Strict Management of Assets and Property • Prohibition Against Improper Use of Company Assets and Property • Protection of the Company's Intellectual Property Rights

3. Management of Information

- Management in Compliance with Rules • Prohibition Against Personal Use of Confidential and Proprietary Information • Prohibition Against Insider Trading • Prohibition Against the Unlawful Acquisition of Confidential or Proprietary Information Pertaining to Other Companies • Appropriate Use of Confidential and Proprietary Information Pertaining to Other Companies

4. Conflicts of Interests/Separation of Personal and Company Matters

- Avoidance of Conflicts of Interests • Prohibition Against Seeking, Accepting or Offering Improper Gifts, Entertainment, or Other Benefits
- Prohibition Against Acquisition of Pre-IPO shares

5. Maintenance and Improvement of Working Environment

- Respect for the Individual and Prohibition Against Discrimination
- Prohibition Against Sexual Harassment • Prohibition Against Bringing Weapons or Drugs to the Company Workplace

Promoting Corporate Ethics

Canon Group Code of Conduct and Compliance Card

Canon established the Canon Code of Conduct in 1992, and later updated it as the Canon Group Code of Conduct in 2001. This set of principles clarifies the Canon Group's management stance and standards that Canon Group executives and employees must comply with in their duties. In addition to Japanese, the Code of Conduct has been translated into 14 languages, including English, French and Chinese, and adopted by resolution of the Board of Directors of each Canon Group company, which also strives to ensure that it is known and practiced by all.

In addition, a portable Compliance Card has been created in Japanese as well as 16 other languages,



including English, French and Chinese, and given out to Group executives and employees inside and outside Japan. Written on one side of the card is the *San-ji* (Three Selves) Spirit, which has been the guiding principle of the company since its founding, and on the other side is a compliance test that enables employees to carry out self-questioning of their actions on a daily basis.



Compliance Card

Corporate Ethics and Compliance Training

Canon Inc. carries out corporate ethics and compliance training for employees suited to the circumstances and conditions of the region where they operate.

For example, Canon Inc. conducts rank-based training designed to foster compliance awareness for newly appointed general managers and managers as well as new employees.

Additionally, Canon Inc. and its subsidiaries in Japan have since 2004 designated a Compliance Week twice a year—once in the first half of the year and the other in the second half—in order to foster discussions in the workplace about compliance issues. Through these efforts, we strive to develop and improve operational processes to ensure that employees are aware of compliance and abide by the law.

Whistleblower System

Canon Inc. has established a hotline to receive information related to compliance issues. The confidentiality of callers is strictly maintained, and they are guaranteed not to suffer any unfair treatment for using the hotline. We continually work to encourage use of the system by raising awareness of the hotline services, using such means as an intranet compliance website and compliance training.

Hotlines have been established at nearly all Group companies inside and outside Japan. Canon Inc. and Group company divisions in charge of the hotlines are in close coordination to continuously respond to incoming reports and increase system reliability.

Legal Risk Management System

At Canon, we have identified significant legal risks that the Canon Group may face in the course of business (e.g. violations of anti-trust laws, anti-bribery laws and export control regulations) by considering the potential likelihood and impacts on Canon’s business. To minimize these risks, we are working to improve a system to ensure legal compliance by improving operational workflows and rules, providing training on laws for related employees, and conducting audits and checks.

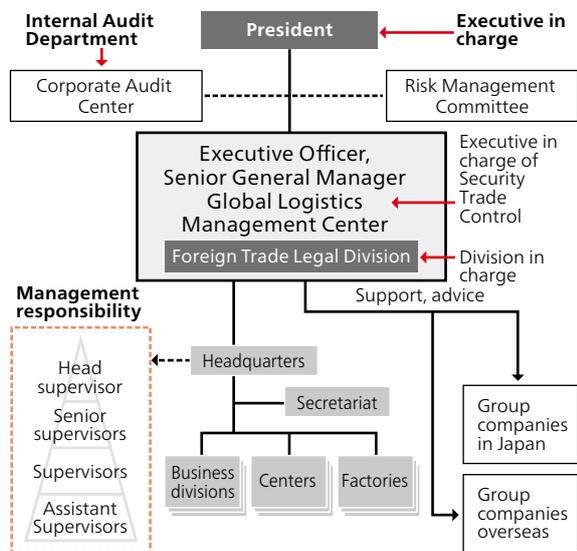
Strict Compliance with Export Control Regulations

Canon Inc. has established a security trade control framework headed by the president and overseen by the Foreign Trade Legal Division within the Global Logistics Management Center. This ensures that we can implement proper security trade controls in compliance with strict regulations on the export of goods and technologies for civil use that could be diverted for use in weapons of mass destruction or conventional weaponry.

The Foreign Trade Legal Division works with divisions involved with individual goods and technologies to double-check such issues as whether export goods and technologies are controlled by regulations, or whether counterparties are engaged in the development of weapons of mass destruction. We have also established and revised Security Trade Control Guidelines, and hold regular briefings and training sessions for persons in charge of Canon Inc. business divisions and Group companies in Japan to further educate employees about the importance of security trade control. We also provide Group companies with templates for company rules, training materials for employees, and support via the help desk to help these companies establish control frameworks and rules.

Such thorough internal controls have ensured that the Canon Group has never violated security trade control laws. Canon Inc. has also maintained a bulk export license from Japan’s Ministry of Economy, Trade and Industry continuously since 1990. This license is granted only to exporters who exercise strict controls.

Canon Inc.'s Security Trade Control System



Training on Security Trade Control in 2016

Category	Subject	Number of sessions
Rank-based	New employee training	1
	New manager training	3
	New general manager training	2
Expatriates	International staff training	7
Canon Group	Expert training for security trade control employees	9
	Global e-learning (Japanese, English, Chinese and Thai languages)	Ongoing

Compliance with Anti-Trust Laws

Anti-trust laws apply to all of Canon's business activities, from product development to production, sales and after-sales service, and therefore, Canon recognizes that compliance with these laws is absolutely vital.

Based on this awareness, business divisions of Canon Inc. and sales and service companies of the Canon Group inside and outside Japan conduct regular training for employees of divisions exposed to the risk of anti-trust law violations to educate them about the laws, provide examples of legal violations, and inform them of what to be aware of in carrying out their duties. We also make our anti-trust law hotline known to all employees and thoroughly encourage employees to use this hotline if they are unsure of how to interpret or apply anti-trust laws.

Prevention of Bribery

The Canon Group Code of Conduct clearly stipulates that Canon will not receive benefits in the form of

gifts or entertainment that exceed the social norm, or provide similar benefits to other parties.

Canon carries out regular training for employees of divisions involved with negotiations between public officials and business partners to inform them about the latest regulatory trends (including provisions to prevent bribery of public officials outside Japan) in major countries and details of the Code of Conduct.

Promoting Business Risk Management

The Business Risk Management Subcommittee is responsible for operational risks excluding legal violations and errors in financial reporting.

Individual risks are assigned to the responsible administrative divisions for the entire Canon Group. The Business Risk Management Subcommittee works with working-level divisions in charge from each Canon Inc. organization and Canon Group company to implement risk mitigation activities and further develop the risk management system.

Ensuring Thorough Information Security

Recognizing that information security is a vital management task, Canon has established an appropriate management system for the entire Group, in accordance with the fundamental principles of information security regulations. Under this system, we implement training to raise employee's awareness and to prevent external threats and leaks of confidential internal information.

Since 2005, Canon has had external certification, ISO27001, for its information security management systems.

Information Security Management System Operations

Canon has established an Information Security Committee as the decision-making body for information security measures. This committee is made up of experts from information security departments and is responsible for information security management for the entire Group.

Committee members have also drawn up Canon Group Information Security Rules in order to maintain the same level of and approach to information security across the entire company. These rules apply to all Group companies worldwide. Each Group company creates regulations and guidelines based on these rules in line with its needs, and conducts training and awareness activities.

Based on these rules, regional administration companies conduct regular inspections to confirm how information security is being implemented at

Message from Management	Canon Group Business Operations	CSR Management	Growth Strategy and Sustainability	Activity Highlights
Relationship with SDGs	CSR Reporting	Management Structure	GRI Guideline Implementation	Third-Party Opinion / Assurance

each Group company, using the data to review and improve information security controls.

If an information security incident occurs, the matter must be reported to the Information Security Committee via the respective regional administration company. In turn, the committee issues appropriate instructions.

CSIRT*, a dedicated team for dealing with growing information network threats, was established within Canon Inc. in 2015. At that time, Canon officially joined the Nippon CSIRT Association as Canon-CSIRT in order to address the increasingly sophisticated nature of cyber attacks by strengthening collaboration with external CSIRTs. Additionally, in 2016, Canon Inc.'s Information & Communication Systems Headquarters implement information security checks on 29 Group companies in Japan and 18 Group companies overseas. These inspections found that each company's system was sound and in good working order.

Canon will maintain an expedient and smooth communication channel with its Group companies and make every effort to ensure that its mechanisms can identify and remedy issues based on regular information security checks. Moreover, we are also working to further reinforce our information security system by establishing a structure to discover information security incidents at an early stage and measures to eliminate security leaks and risks connected to these incidents.

* CSIRT: stands for Computer Security Incident Response Team. This is a dedicated organization that deals with incidents involving computer security.

Preventing Information Leaks

Canon implements measures to safeguard the three elements of information security: confidentiality*,

integrity*, and availability*.

The most important information is stored using a dedicated system with reinforced security. By controlling access and recording usage, we guard against external attacks and prevent information leaks from within.

In addition, we have established an environment in which employees can safely access the company's information assets while away on a business trip, and we have also placed restrictions on email attachments and taking company computers and storage media offsite.

To safeguard against the threat of external attacks, we implement training and other measures to prevent tampering with Canon's official websites and to deal with targeted email attacks.

In 2016, we continued with these initiatives and also worked on responses to cyber attacks, upgraded email security, and improved security regarding internet access to further enhance security and protect against the threat of information leaks. Going forward, we will continue to work on improving our countermeasures to maintain the three elements of information security.

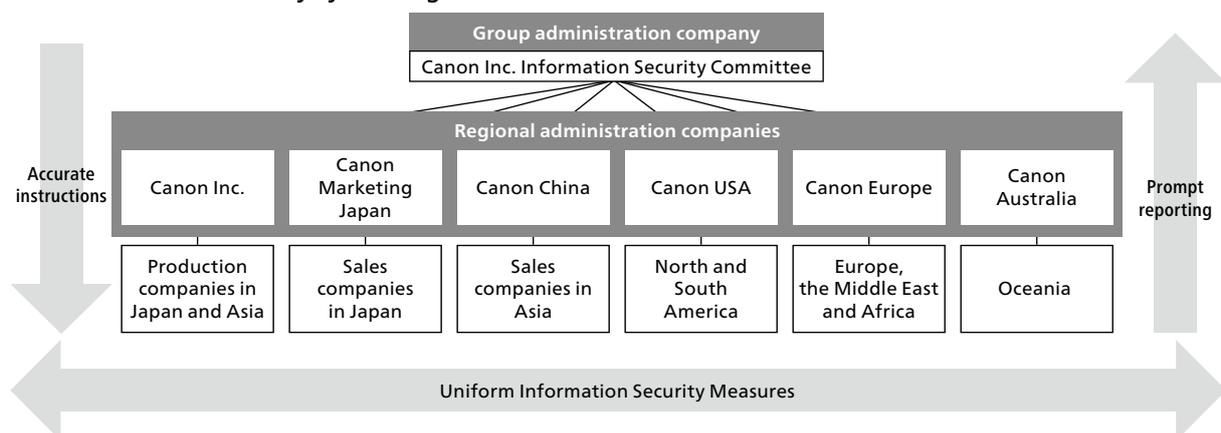
- *1 Confidentiality
Enable only authorized personnel to access information.
- *2 Integrity
Ensure data and processing methods are accurate and cannot be modified without authorization.
- *3 Availability
Make data accessible to authorized personnel when needed.

Protecting Personal Information

Canon recognizes that personal information is an important asset, and that protecting this asset is one of its social responsibilities.

At Canon Inc., we have created rules to

Global Information Security System Organization



safeguard personal information, including a Personal Information Protection Policy and Personal Information Protection Rules, and conduct training and audits regularly as part of our system to prevent leaks of information.

Starting in 2015, we expanded the scope of these activities to include all Group companies, creating a centralized management system covering the entire Canon Group. As a result, there were no incidents involving the loss or leakage of personal information at Canon Inc. or any of its Group companies in 2016.

Canon Inc. and Group companies in Japan have also implemented measures to deal with Japan's new Social Security and Tax Number System (referred to as the "My Number" system), which was introduced in Japan last year, in an appropriate manner. To this end, the entire Group in Japan formulated My Number Handling Rules, My Number Regulations as well as a detailed handling procedure manual. In particular, our measures regarding physical and technological security are more stringent than those mandated by law, and we continue to collaborate with the IT department on this matter.

Going forward, Canon will regularly monitor its management of "My Number" and other personal information while reviewing operations as needed to make appropriate improvements.

I Information Security Training to Raise Employee Awareness

In order to maintain and improve information security, Canon is focusing on raising awareness among the employees who use information systems.

New employees are thoroughly trained on Canon's information security measures and rules through group training for both regular and mid-career hires. In addition, all employees undergo annual training using our e-learning system.

In 2016, roughly 27,000 employees—equivalent to Canon Inc.'s total workforce—received information security training. The training curriculum focused on reaffirming essential measures, focusing on cyber security in particular. This included how to respond to targeted email attacks, what to look out for when sending emails and the risk of information leaks from posting on external translation websites, among other protocols for using information infrastructure.

Canon is committed to improving the content of its training programs in order to raise employee understanding and awareness of information security matters.

Bolstering Physical Security

Aiming to strengthen physical security, Canon has been working to establish physical-security systems at each of its operational sites based on the following three policies:

- Establish and put into practice at operational sites an overall design from the viewpoint of crime prevention, disaster prevention, and safety to optimize entry and exit routes for all persons.
- Fully implement strict internal and external security measures to comprehensively prevent company assets (physical objects, information, etc.) from being removed, suspicious objects from being brought in, and suspicious individuals from entering.
- Limit entry to certain areas to people who have been authorized by area managers, and integrate management of room entry and exit logs.

I Physical Security Promotion System

Canon has established Canon Security Guidelines that outline policies and rules regarding room entry and exit management and other aspects of physical security. We have also been proactively implementing security measures according to these guidelines, and revising the guidelines as needed. Each Canon site is now responsible for drafting a self-checklist that complies with the guidelines and also takes into account the unique security risks of each region in order to check the adequacy of its security protocols. In this way, each site implements security measures tailored to changes in its own environment.

In addition, the Group has adopted an Integrated Entry and Exit Management System and a control system that comprehensively manage surveillance cameras and sensors as part of Canon's efforts to strengthen physical security across the entire Group.

Due to the serious risk to society posed by toxic materials, we have developed a particularly thorough audit system, covering all Canon Group sites in Japan. Improvements and revisions to physical security measures are implemented based on audit results.

Learning from the terrorist incidents in Paris and Belgium, Canon has stepped up its security efforts in order to quickly detect suspicious persons and suspicious objects with the aim of preventing indiscriminate terrorist attacks against companies considered to be soft targets. We are also working more closely with the police, fire departments and other government agencies to heighten vigilance against possible attacks.

Message from Management	Canon Group Business Operations	CSR Management	Growth Strategy and Sustainability	Activity Highlights
Relationship with SDGs	CSR Reporting	Management Structure	GRI Guideline Implementation	Third-Party Opinion / Assurance

Post-Disaster Business Continuity Plan Responding to the Risk of Damage to Infrastructure

Canon believes that establishing a system to ensure that business operations can continue after a natural disaster or emergency represents one of the most important social responsibilities of any company. Based on this recognition, we have formulated a business continuity plan (BCP) *1 and Canon Group Disaster Preparedness Guidelines, and are working hard on advancing business continuity measures for disasters, including upgrading buildings constructed according to old aseismic design standards, concluding disaster agreements with local communities, and developing systems for collecting information and reporting.

Due to the critical importance of our Shimomaruko headquarters in Tokyo, Japan, as the home base for all Group operations, we have rebuilt all on-site buildings, established a crisis control center, installed backup generators, stockpiled fuel, equipment, and supplies, and established a multiplex communication system. Moreover, we set up a Disaster Recovery Center*2 to back up information systems to ensure that the core IT system will operate securely in the event of a disaster.

We have also updated all Group company facilities, setting up emergency communications equipment and support structures, and inculcated a sense of readiness in our employees through practical disaster-preparedness training. We also have systems that use data from canon surveillance cameras installed at each Group location to enable swift understanding of damage incurred at other locations and factories in the event of a disaster. Furthermore, we have prepared a manual for persons in charge in order to safeguard human life immediately following a natural disaster or fire, prevent secondary disasters, and protect company assets. Using this manual as a model, Group companies are also creating localized manuals based on the unique risks in the areas where they operate to facilitate the smooth restoration of services in the event of a disaster. Last year, 35 operational sites conducted 36 emergency drills based on these manuals.

*1 business continuity plan (BCP): A business continuity plan is an action plan that includes measures to provide for the continuation of a minimal level of business in the event of fire, accident, or other such event, and to restore operations promptly.

*2 Disaster Recovery Center: A facility prepared for data backup in the event of a system breakdown due to a disaster.

System to Promote Responses to Infrastructure Disaster Risk and Goals

Organization in charge	Facility Management Headquarters (Facility Management Division)
Policy	Conduct drills to verify that manuals prepared by individual sites are effective. Revise manual where there are shortcomings to improve ability to respond in an emergency.
Goals	Each operational site to conduct a drill once a year

Canon Group Response to Risk of Infrastructure Damage

2014	<ul style="list-style-type: none"> Established monthly communications drills at headquarters and individual business locations /Group companies using satellite phones Disaster Provision Standards created following enactment of Tokyo Metropolitan Ordinance on Measures for Stranded Persons
2015	<ul style="list-style-type: none"> Continued communications drills mentioned above Conducted training exercise to set up disaster recovery headquarters in event of major natural disaster at Shimomaruko headquarters Stocked nonfood provisions (emergency blankets and portable toilets) based on Disaster Provision Standards
2016	<ul style="list-style-type: none"> Increased frequency of central disaster recovery headquarters training exercises (focused on earthquake and flood in 2016) to twice yearly

Disaster Agreement with Ota Ward, Tokyo

Canon Inc. has concluded a disaster agreement with Ota Ward, Tokyo, where its Shimomaruko headquarters is located. In line with the request of the Disaster Prevention Section of Ota Ward, under the agreement our newest facilities, including a lecture hall, gymnasium and heliport, can be offered in the case of an emergency situation.

Going forward, we will continue to work closely with local governments to fulfill the role of a disaster-response base in the local community.

Disaster Agreement with Susono City, Shizuoka Prefecture

In July 2016, Canon Inc.'s Fuji-Susono Research Park concluded a disaster agreement with Susono City, Shizuoka Prefecture, regarding support in the event of a major disaster. Susono City is working to create an urban environment resilient against disaster. Under the agreement, if there is a major earthquake in Susono City, the two parties will offer mutual support and cooperate in relief and recovery activities, such as providing food aid and permission to travel along designated disaster roads.