| Message from Management | Canon Operations and Sustainability | CSR Management | Activity Highlights | CSR Reporting | Management Structure | Third-Party Opinion / Assurance |

Risk Management

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 the 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.
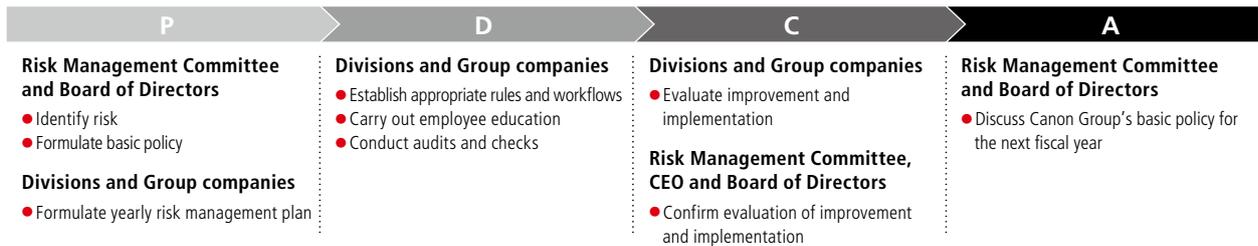
Risk Management System

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 also creates an annual basic policy for risk management activities and, after obtaining the approval of the Board of Directors, carries out risk management activities within 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 results of such evaluations to the CEO and Board of Directors. Results of evaluations conducted in 2017 showed no major flaws in the system.

Processes for Improvement and Implementation of Risk Management System

P	D	C	A
Risk Management Committee and Board of Directors ● Identify risk ● Formulate basic policy **Divisions and Group companies** ● Formulate yearly risk management plan	**Divisions and Group companies** ● Establish appropriate rules and workflows ● Carry out employee education ● Conduct audits and checks	**Divisions and Group companies** ● Evaluate improvement and implementation **Risk Management Committee, CEO and Board of Directors** ● Confirm evaluation of improvement and implementation	**Risk Management Committee and Board of Directors** ● Discuss Canon Group's basic policy for the next fiscal year

Risk Management Promotion System
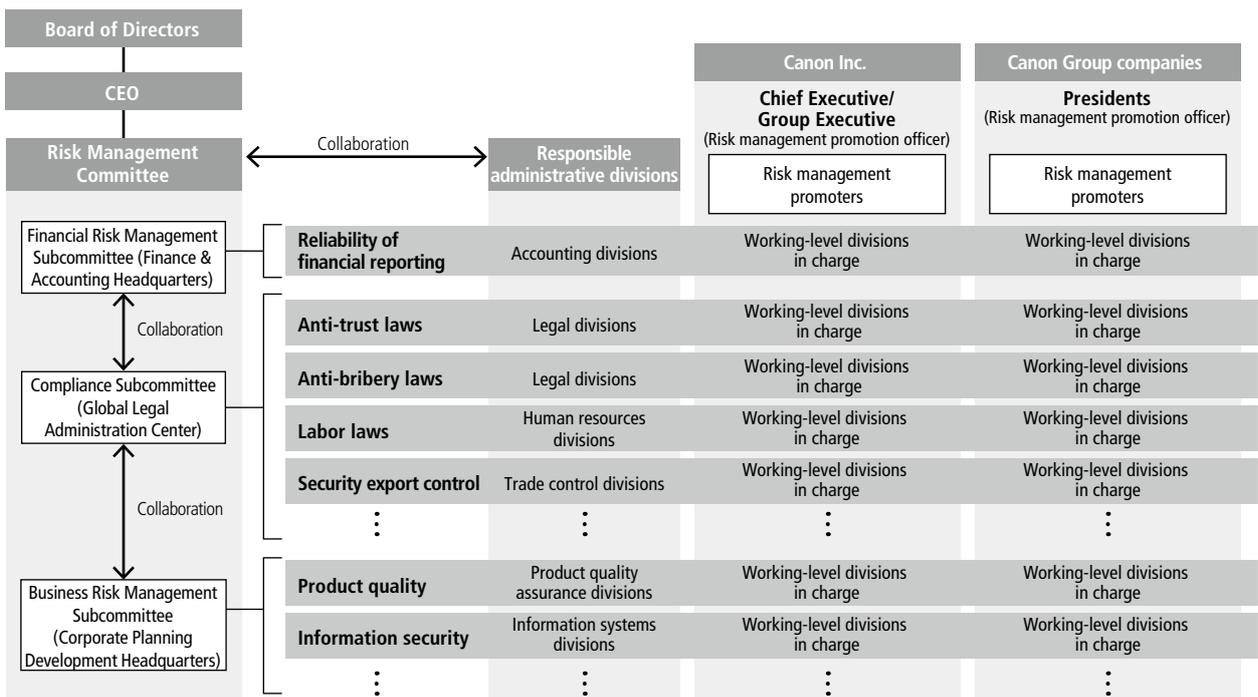
In line with the basic policy prepared by the committee, in their capacity as risk management promotion officer, the heads of Canon Inc. divisions and presidents of Canon Group companies each formulate an annual risk management plan for their own division or Group company, and assume responsibility for promoting related risk management activities. Risk management promoters appointed within each division and Group company assist risk management promotion officers in coordinating 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 Group company.

Group-Wide 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, including 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 2017.

Compliance

The Compliance Subcommittee works to promote corporate ethics across the Group 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. It 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 many languages, including English, French and Chinese, and adopted by a 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 and many 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 Selfs) 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 corporate ethics and compliance training as part of rank-based training 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. receives regular reports from Group companies on the operational status of their whistleblower system.

Legal Risk Management System

At Canon, we have identified significant legal risks that the Canon Group may face in the course of business (for example, 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.
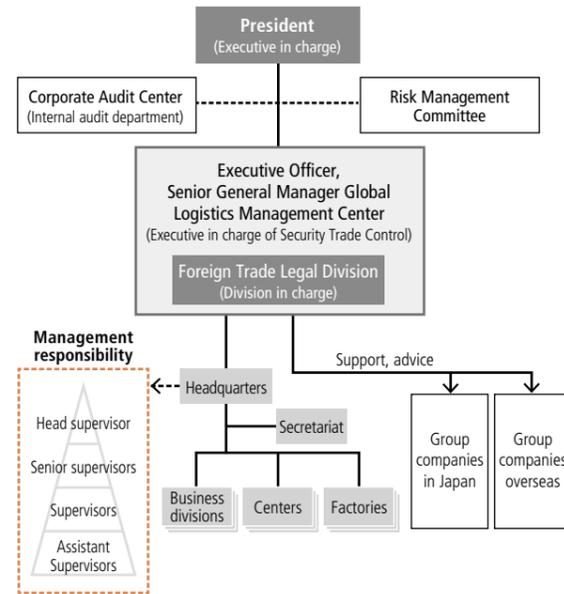
■ Strict Compliance with Export Control Regulations

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 relevant persons at Canon Inc. 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 at each Group company ensure that the Canon Group doesn't violate 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.

Message from Management | Canon Operations and Sustainability | CSR Management | Activity Highlights | CSR Reporting | Management Structure | Third-Party Opinion / Assurance

Risk Management

| Message from Management | Canon Operations and Sustainability | CSR Management | Activity Highlights | CSR Reporting | Management Structure | Third-Party Opinion / Assurance |

Risk Management

Canon Inc.'s Security Trade Control System

President
(Executive in charge)

Corporate Audit Center
(Internal audit department)

Risk Management Committee

Executive Officer,
Senior General Manager Global
Logistics Management Center
(Executive in charge of Security Trade Control)

Foreign Trade Legal Division
(Division in charge)

Management responsibility

Support, advice

Headquarters

Secretariat

Head supervisor
Senior supervisors
Supervisors
Assistant Supervisors

Business divisions | Centers | Factories

Group companies in Japan | Group companies overseas

Training on Security Trade Control in 2017

Category	Subject	Number of sessions
Rank-based	New employee training	1
	New general manager training	2
	New manager training	2
	New staff manager training	2
	Employee seminars on trade controls	4
Expatriates	International staff training	7
Canon Group	Expert training for security trade control employees	3
	Global e-learning (Japanese, English, Chinese and Thai languages)	Ongoing

■ Compliance with Anti-Trust Laws

Canon recognizes that compliance with anti-trust laws, which apply to all of its business activities, from product development to production, sales and after-sales service, is absolutely vital.

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 violations to educate them about anti-trust laws, give examples of legal violations, and provide everyday operational compliance guidance. Employees are encouraged to make use of Canon's anti-trust law hotline (connected to the Legal Division) when 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 mitigating serious operational risks.

Action policies and plans for each serious risk are decided in cooperation with the responsible administrative divisions for the entire Canon group and implemented throughout Canon Inc. business divisions and Group companies, along with the promotion of risk mitigation activities.

Ensuring Complete 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. The steps that we take under this system include measures to prevent leaks of confidential information, handle external cyberattacks, bolster information security at production facilities, and provide information security training to raise employee awareness.

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

■ Information Security Management System Operations

The Information Security Committee is the decision-making body for information security measures at Canon. It is chaired by the senior executive with responsibility for information security, namely the Group Executive in charge of the Information & Communication Systems Headquarters. The latter is responsible for implementing measures determined by the Information Security Committee to manage this issue across the Canon Group.

If an information security incident occurs, the matter must be reported to the Information & Communication Systems Headquarters. It may also be reported to the Risk Management Committee, depending on circumstances (→P124).

The Information & Communication Systems Headquarters formulated the Canon Group Information Security Rules to ensure the same level of measures and a consistent approach to information security are applied across the Canon Group globally. Each Group company creates regulations and guidelines based on these rules in line with its needs, and conducts related training and awareness activities. Periodic inspections are also carried out to assess the status of each Group company's information security measures and enable improvements or revisions as needed.

In 2017, information security checks were carried out at 21 Group companies in Japan and 19 Group companies overseas. These inspections found that each company's system was sound and in good working order.
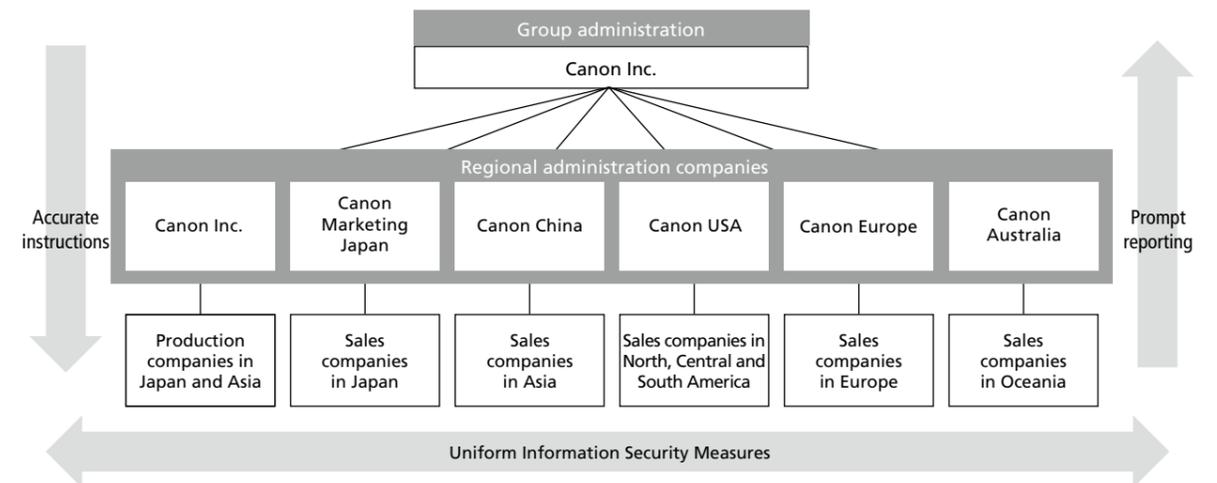
Canon will maintain an expedient and smooth communication channel with its Group companies and make every effort to ensure that its mechanisms can identify and remedy issues based on regular information security checks.

CSIRT*, a dedicated team for dealing with information security incidents, was created within Canon Inc.'s Information & Communication Systems Headquarters in 2015. At that time, Canon joined the Nippon CSIRT Association (NCA) to strengthen collaboration with CSIRTs in other companies.

Canon plans to reinforce its information security systems further by strengthening countermeasures in response to information security incidents, while also seeking to prevent more widespread damage by developing early-detection capabilities and promoting collaboration with outside organizations.

* CSIRT: Computer Security Incident Response Team. This is a dedicated, organized group that deals with incidents involving computer security.

Global Information Security System Organization

Group administration
Canon Inc.

Regional administration companies

Canon Inc. | Canon Marketing Japan | Canon China | Canon USA | Canon Europe | Canon Australia

Accurate instructions

Prompt reporting

Production companies in Japan and Asia | Sales companies in Japan | Sales companies in Asia | Sales companies in North, Central and South America | Sales companies in Europe | Sales companies in Oceania

Uniform Information Security Measures

| Message from Management | Canon Operations and Sustainability | CSR Management | Activity Highlights | CSR Reporting | Management Structure | Third-Party Opinion / Assurance |

Risk Management

■ Information System Security Measures

Canon implements measures to safeguard the three elements of information security: confidentiality, integrity, and availability*[1].

As part of measures to prevent the leakage of confidential data, we ensure the most important information is stored using a dedicated, access-controlled system with reinforced security and auto-recorded user activity. 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.

As part of measures against cyberattacks, we use monitoring systems to identify any suspicious emails with possible malware*[2] attachments. We also attempt to monitor unauthorized online communications from internal sources as part of stopping attacks from causing more widespread damage.

In 2018, we also plan to initiate further risk mitigation measures in anticipation of a heightened risk of cyberattacks ahead of Rugby World Cup 2019™, Japan and the Olympic and Paralympic Games Tokyo 2020.

*1 Confidentiality: Enable only authorized personnel to access information.
　Integrity: Ensure data and processing methods are accurate and cannot be modified without authorization.
　Availability: Make data accessible to authorized personnel when needed.
*2 Malware: malicious software (including computer viruses and ransomware) created with the deliberate intention of performing unauthorized or harmful operations

■ Security Measures for Production Facilities

Canon implements security measures for its production facilities to ensure malware, cyberattacks or other information security issues do not reduce productive capacity or otherwise disrupt production plans.

In the past, corporate mainframes or online information systems were the major targets for cyberattacks. Today, the growing use of off-the-shelf OS software and networks means that production facilities attract the same level of information security risk. A separate approach is needed for production systems because production lead-times are longer than the customer support periods for off-the-shelf OS software. In 2017, we began undertaking critical information security audits for Canon Inc. and Canon Group production companies in Japan. We also began monitoring the networks linked to important facilities and production lines for any unauthorized activity.

We plan to extend these measures to Group production companies based overseas to ensure Canon Group production facilities worldwide can operate safely without disruption.

■ 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.

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

In 2017, roughly 26,000 employees—equivalent to Canon Inc.'s total workforce—received information security training. This included training to develop information security literacy*, including how to deal with suspicious emails, measures to prevent email misdirection, and other IT protocols. In addition, special training sessions based on a targeted email attack were conducted involving roughly 71,000 Canon Inc. and Group company employees to provide practical instruction in responding appropriately to suspicious emails so widespread damage is avoided.

* Information security literacy: knowledge and skills needed to implement proper information security measures

■ 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 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 2017. Canon did not receive any privacy infringement complaints from customers in 2017.

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 in 2016, in an appropriate manner. To this end, the entire Group in Japan formulated My Number Handling Rules, My Number Regulations, and 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 division 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.

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.

■ 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 toxic materials 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 in detecting risks.

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 updated all Group company facilities in Japan, 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 site so any damage caused by natural disasters or other emergencies can be evaluated swiftly. Furthermore, we have prepared a leader's manual 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): 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	• 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	• 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	• Increased frequency of central disaster recovery headquarters training exercises (focused on earthquakes and floods in 2016) to twice yearly
2017	• Created and distributed a disaster-prevention video detailing how to prevent fire after an earthquake • Carried out semiannual tests of disaster preparedness at home with participation of 18,000 Canon Group employees in Japan • Conducted natural disaster hazard checks at each operational site

■ 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. 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, offering support in the event of a major disaster. Susono City is working to create an urban environment resilient to 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.

Proper Payment of Taxes

Canon believes that, as a multinational corporation with operations spanning the globe, the proper payment of taxes in the countries and regions where it operates is one of its most fundamental and important social responsibilities. Accordingly, Canon abides by the following principles on tax matters. In 2017, Canon was not subject to any material meaningful fines or negative tax-related judgments or assessments.

1. Pay taxes properly in accordance with tax-related laws and ordinances.
2. Ensure that tax accounting and other related processes are carried out unfailingly, according to law.
3. Develop tax-related governance systems and work to raise awareness about tax compliance.
4. Adhere to common international rules on international taxation (guidelines set by the Organization for Economic Co-operation and Development and the United Nations), and ensure that actions are in compliance with the tax laws of each country.

Corporate Income Taxes

	2013	2014	2015	2016	2017
Taxes on income before income taxes (hundred million yen)	1,081	1,180	1,161	827	980
Effective tax rate on income before income taxes (%)	31.1	30.8	33.4	33.8	27.7