Information security 102-11, 102-12, 102-15, 103-1, 103-2, 103-3, 404-2

Kao's approach

The Kao Group is working to strengthen information security in order to protect information assets that include confidential information (trade secrets) and personal information, as well as IT hardware, software and many kinds of data records, in accordance with Kao's Information Security Policy. Kao promotes information security through the use of a PDCA cycle created to set internal rules and ensure that those rules are observed and that internal controls are implemented thoroughly.

Kao's creating value to address social issues

Social issues we are aware of

Every company uses IT to promote efficiency in its business and operations, and uses data to develop innovations and initiate reforms. Information technology has spawned new cross-industry growth areas and the engagement of diverse human resources.

The rising use of IT has also recently increased the threat of cyberattacks, which can temporarily interrupt business activities and cause information leakage. Cyberattacks adversely affect business performance and have turned cybersecurity into a social issue.

Kao's creating value

Kao hopes to contribute to improving the security measures of the entire industry by sharing information with other companies in the industry about the cyberattacks that Kao has experienced through our participation in information-sharing networks: the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP), which is directed by the Information technology Promotion Agency, Japan (IPA), the National Police Agency's Cyber Intelligence Information Sharing Network, and the early warning information system of the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC).

Risks related to realization of our vision by 2030

A major risk is the occurrence of cyberattacks that can cause the extended suspension of production, sales, marketing, and R&D activities, along with the loss of corporate trust due to information leaks.

Opportunities related to realization of our vision by 2030

By strengthening cybersecurity measures and the management of data—trade secrets and personal information—can be utilized in new ways and new styles of working enabled through the use of networks.

Contributions to the SDGs

Policies

We have formulated our Information Security Policy, Guidelines on Handling Trade Secrets, Guidelines on Handling Personal Information and IT Security Guidelines. We also carefully manage cybersecurity measures, trade secrets, and personal information. Such efforts are carried out in accordance with laws and regulations and the guidelines set forth by government agencies and committees, and are also designed to clarify Kao's management framework and management methods.

Education and promotion

To ensure that employees throughout the group fundamentally understand the issues of protecting trade secrets and personal information, internal education is provided at times of the year when new hires are assigned positions or personnel transfers are made. We arrange lectures by external instructors for the members of the TS & Personal Information Protection Committee and for Personal Information Controllers, and awareness-raising activities are held to familiarize our staff with the latest trends. Awareness-raising materials for education at the level of the individual divisions are provided to the members of the TS & Personal Information Protection Committee and Personal Information Controllers. Company-wide warnings and awareness-raising messages for all staff are sent via the company intranet portal site.

Also, to evaluate the effectiveness of the in-house education, self-checks are performed. On the basis of the results obtained, any problems that may exist are identified, improvement targets are set, and improvement activities are implemented.

Information security 103-2, 103-3

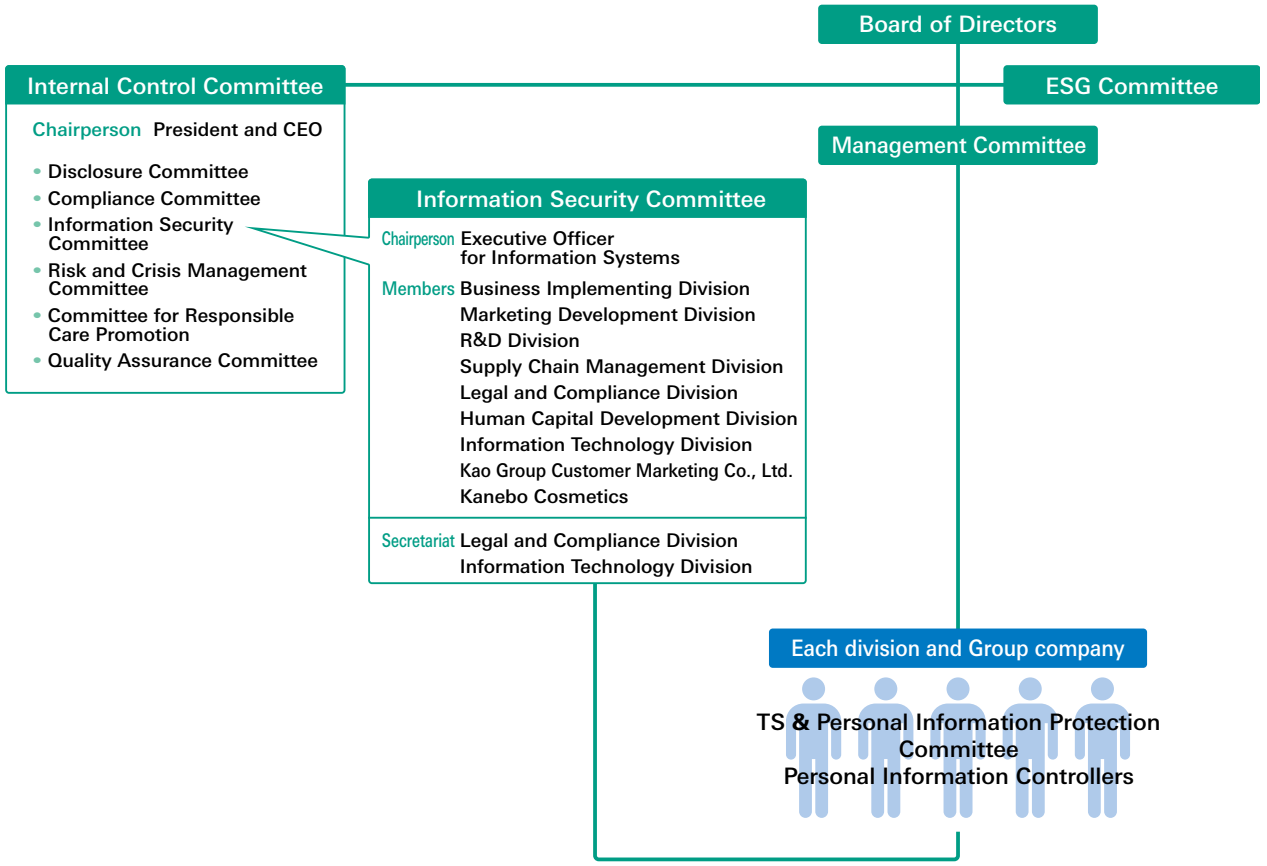
Kao's approach

Framework

We have appointed executive officers to serve as Chair and Vice-Chair of the Information Security Committee, and both the committee members and the staff of the committee's secretariat are drawn from different divisions, including Human Capital Development, Information Technology, Marketing, Intellectual Property Management, Production and Engineering, and Legal and Compliance. In this way, we benefit from a wide range of perspectives when determining policies, formulating internal rules, putting management systems in place, and implementing awareness-raising activities.

The Information Security Committee reports on its activities to the Internal Control Committee on a quarterly basis, and the Internal Control Committee reports to the Board of Directors on the activities of all subordinate committees. The report contains the activity targets of the current fiscal year, plus progress status and performance evaluations, and is reported in the fourth quarter, together with the activity targets for the coming fiscal year. The global system places the information security committees of each country under the umbrella of Japan's Information Security Committee. Primarily for Europe and the Americas, which have taken measures to be GDPR compliant, and China, which already has a corresponding information security body, we will develop the system in fiscal 2019.

Information Security Management System



* As of December 2018.

Information security 103-1, 103-2, 103-3

Kao's approach

Mid- to long-term targets and performance

Mid- to long-term targets

- Protection of information assets such as trade secrets, personal information, hardware, software, and many kinds of data records, including cybersecurity measures.
- In the event of an information leak or other emergency, the quick confirmation of facts, decision on a response, and the formulation and implementation of measures to prevent recurrence.

Anticipated benefits from achieving Mid- to long-term targets

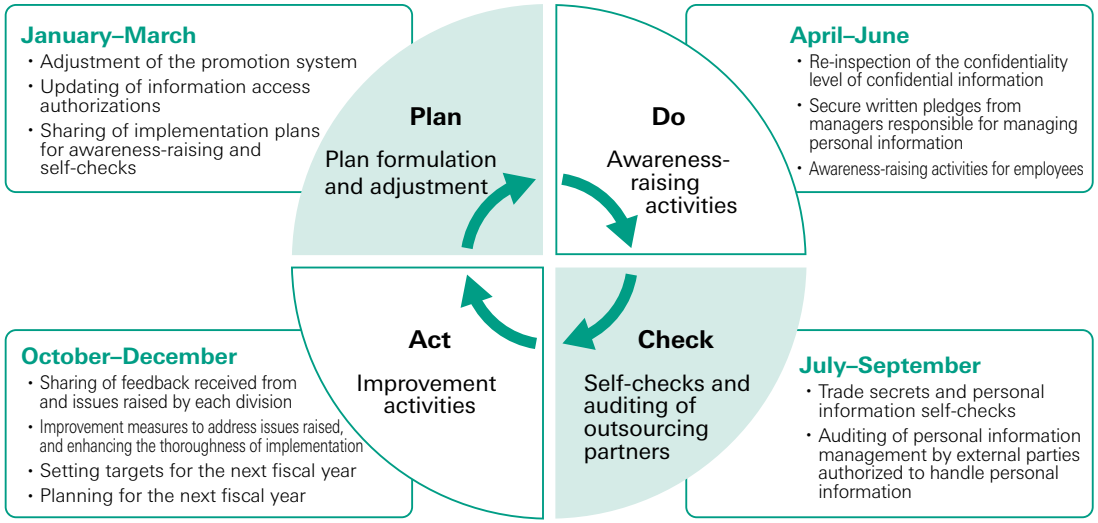
Cost reduction or profit expansion

Cybersecurity measures can reduce costs incurred to respond to leaks of trade secrets or personal information by preventing such leaks. Also, damage can be minimized if measures are in place to respond to the leak of trade secrets or personal information.

Impacts on society

Implementing cybersecurity measures for the entire supply chain will play a part in improving cybersecurity for the entire industry and for Japanese companies overall.

PDCA cycle for information security activities



Information security 103-1, 103-2, 103-3

Kao's approach

Performance in 2018

Performance

The PDCA cycle was implemented in TS and personal information protection promotion activities.

First Quarter: Plan formulation and adjustment

- Adjustment of TS and personal information protection promotion system.
- Targeted e-mail training.
- Report on GDPR response to the Supervisory Board.

Second Quarter: Awareness-raising activities

- TS awareness-raising activities in 99 divisions, departments, and affiliated companies in Japan.
- Personal information awareness-raising activities in 77 divisions, departments and affiliated companies in Japan.
- Personal information leak response training.
- Website GDPR compliance implementation for the EU.
- Report on GDPR compliance at the Board of Directors meeting.
- Confirmation of status of compliance with China's Cybersecurity Law.
- Ministry of Economy, Trade and Industry (METI) "Cybersecurity Management Guidelines V2.0" compliance.

Third Quarter: Self-checks and auditing of outsourcing partners

- Self-checks on trade secrets in 109 divisions, departments and affiliated companies in Japan.
- Self-checks on personal information in 88 divisions, departments and affiliated companies in Japan.
- Paper audits of 182 subcontractors that handle personal information.

Fourth Quarter: Improvement activities

- The 25th TS & Personal Information Protection Promotion Meeting was held at the Plenary Meeting (relayed to remote locations via Web teleconference) on November 15, 2018 at which a 2018 incident report on trade secrets and personal information was presented, feedback was given on self-checks, and improvement targets were set.
- Implementation of overseas security assessment: 10 companies in Asia, 3 in the Americas, 3 in Europe.

Reviews of performance

It is necessary to carry out promotion activities to protect trade secrets and personal information on a continuous basis every year. Even those who fully understand TS and personal information protection lose clarity in their knowledge over a number of years, increasing the risk of an incident. It is important that all employees, including new hires and mid-career hires, understand and follow the Kao Group's TS and personal information protection rules. We have also begun to consider TS and personal information protection promotion activities as necessary to expand globally.

Collaboration with stakeholders

We contribute to the enhancement of information security in Japan's chemical industry through our participation in the Security Information Management Subcommittee established by the Japan Chemical Industry Association (JCIA), an industry body whose members include chemical product manufacturers.

We also participate in two information-sharing networks that work to combat cyberattacks: the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP), which is directed by the Information technology Promotion Agency, Japan (IPA), and the National Police Agency's Cyber Intelligence Information Sharing Network. Starting in 2017, we are also participating in the JPCERT Coordination Center's Early Warning Information program.

Through our participation in these information-sharing networks, besides obtaining information about software vulnerabilities and cyberattacks, we are also able to disclose and share information about cyberattacks that we have experienced, thereby contributing to the enhancement of cyberattack prevention measures in Japan.

In June 2018, an incident occurred in which a false Kao marketing campaign was created, aimed at stealing the personal information of consumers. To address this attack, we issued a warning on the Kao website and on Kao's official Twitter and Facebook accounts, and worked with consumers to prevent damage.

Information security 103-1, 103-2, 103-3

Our initiatives

Our initiatives

First Quarter: Plan formulation and adjustment

Adjustment of TS and personal information protection promotion system

In line with the changes in roles due to organizational restructuring and personnel changes, adjustments were made for 46 members of the TS & Personal Information Protection Committee, 35 supervisors who handle personal information, and one Information Security Committee member. To ensure that the Kao Group's trade secret and personal information protection promotion activities are not interrupted even if organizational changes or personnel changes are made, the adjustments assure that a handover to the next people in charge will take place.

Targeted e-mail training

The fourth targeted e-mail training was conducted in February 2018 for 19,746 people in the Kao Group in Japan, and the attachment open rate was 13.7%, an improvement over last year. It is still necessary to ensure that every employee is able to identify suspicious e-mails with an awareness of cybersecurity so as not to inadvertently open attachments.

Open rate in targeted e-mail training

	2015	2016	2017	2018
Open rate	21.3%	31.5%	18.5%	13.7%

Second Quarter: Awareness-raising activities

Personal information leak response training

A personal information leak response drill was conducted in April 2018 in two parts: Part one—Incident response training; and Part two—Press conference training.

In the incident response training, Kao's servers were infected with malware by a cyberattack, resulting in an assumed leak of personal information. Several crisis response meetings were held at which discovered facts were shared and countermeasures studied and implemented. In the press conference training, two executive officers took the podium and were peppered with tough questions by consultants playing the role of the press. An issue identified through these training sessions was the need for call center outsourcing and capacity planning. Before announcing a leak of personal information, a number for consumers to call needs to be set up. Assuming that the answering of phone calls cannot be adequately handled with internal resources, a call center would have to be set up on short notice and the call center's personnel increased to the maximum. The training made clear that it would be necessary to choose a contractor in advance who would be able to do both.

From press conference for personal information leak response training

METI "Cybersecurity Management Guidelines V2.0" compliance

The Japanese government's Cybersecurity Management Guidelines V2.0, revised in November 2017, define three principles that executives need to recognize and ten important items concerning which they should instruct the chief information security officer (CISO). The latter refers to the National Institute of Standards and Technology (NIST) security framework. Kao uses NIST's security framework to ascertain the group's current status, identify issues, and make improvements.

Information security 103-1, 103-2, 103-3

Our initiatives

Third Quarter: Self-checks and auditing of outsourcing partners

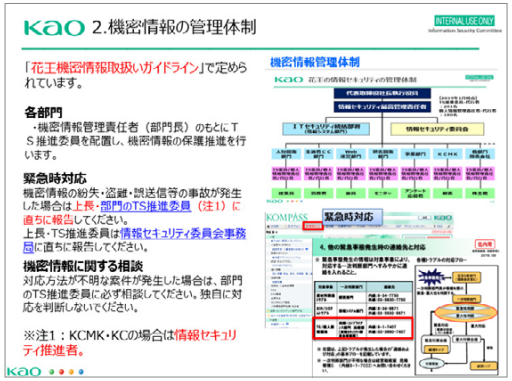
Self-checks of TS and personal information protection

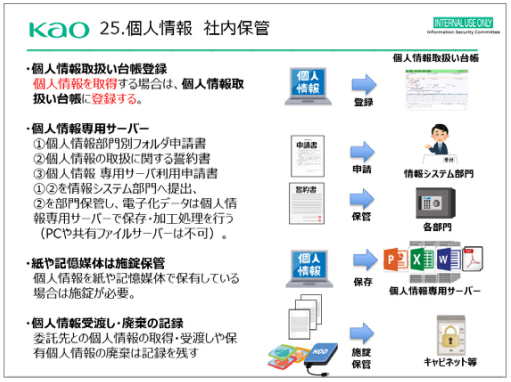
Trade secret self-checks are conducted every year as part of the thorough implementation of awareness-raising activities and efforts to develop division manuals, implement TS labeling, and manage confidential information. In 2018, the self-checks took place from July 9 to August 10.

Personal information self-checks were conducted at the same time to similarly raise awareness, and also to manage the retention of personal information and determine which outsourced tasks involve the handling of personal information. Feedback on the self-checks was given at the TS & Personal Information Protection Promotion Meeting held on November 15, 2018, and improvement targets were set.

The improvement target for trade secrets was set in this way: "When taking confidential information out of the office is unavoidable, it should not be on paper but on a company PC or company smartphone." If it is a company PC locked with an ID or password, or a company smartphone locked with a PIN code, a theft or loss will not lead immediately to an information leak.

The improvement target for personal information was set in this way: "Personal information is to be kept on a server dedicated to personal information protected by a security function." When personal information is stored on a dedicated server, access can be controlled on a file-by-file basis, so even if a file is leaked, it can only be opened by the person who has the access permissions to open it, so the information is protected.





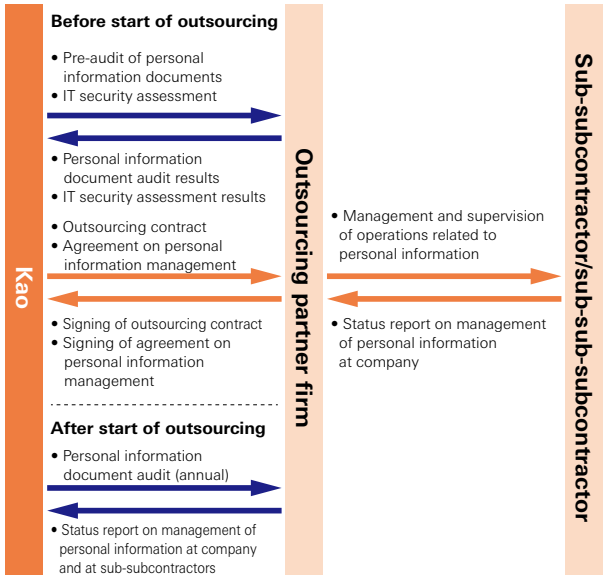
From information security awareness-raising materials.

Auditing of external parties authorized to handle personal information

When the outsourcing of business tasks involves personal information, Kao conducts a preliminary audit to see if the subcontractor can manage personal information safely. We also conduct an IT security assessment if the subcontractor provides a service such as a Web campaign. A contract will not be signed unless the personal information pre-audit and IT security assessment show no problems.

In addition, Kao manages and oversees outsourced personal information by conducting annual audits of subcontractors that handle personal information. In 2018, we conducted such audits at 182 companies and confirmed the status of personal information management and the systems used by subcontractors for protecting personal information. If personal information is stored by a subcontractor, we confirm the number of records and check for consistency with the number of data records registered in their personal information handling ledger system.

Outsourcing of business tasks that involve personal information and auditing of outsourcing partners



Information security 102-12, 103-1, 103-2, 103-3

Our initiatives

Fourth Quarter: Improvement activities

Holding of the 25th TS & Personal Information Protection Promotion Meeting

The 25th TS & Personal Information Protection Promotion Meeting was held on November 15, 2018. An external lecturer gave a talk on the topic of cybersecurity as a business continuity issue in which he gave many examples of cyberattacks in the last few years. Cyberattacks have become a major threat for causing leaks of confidential information and personal information. After the talk, a report was given on incidents related to TS and personal information in 2018. Feedback was then provided on TS and personal information self-checks, and improvement targets were set.

TS and Personal Information Protection Promotion Meeting
113 participants at head office venue; 174 participants via relay at other business sites.

GDPR compliance

The European Union's General Data Protection Regulation (GDPR) came into force on May 25, 2018. The GDPR regulates the handling and transfer of personal data, and is characterized by strict rules and penalties.

Main Compliance Measures

- Transfers of personal data outside the EU based on adequacy: the use of standard contractual clauses (SCCs).
- Respect for an individual's exercise of rights: Privacy Policy update and Agreement to use of cookies.
- Establishment of data protection officer (DPO).
- Preparation of data protection impact assessments (DPIAs) and records of processing activities (RoPA).
- Security management measures (conclusion of Data Processing Agreement (DPA)).
- Obligatory disclosure upon infringement of rights.

Response to China's Cyber Security Law (CSL)

The Cybersecurity Law of China, which came into force in June 2017, requires that important data collected in China be stored in China. Personal information is classified as important data. If personal information is to be transferred across borders, it is necessary to indicate to the personal information provider "the purpose, scope and type of data being transferred and the recipient country or overseas region," and obtain consent.

In addition, when transferring personal information across borders, it is necessary to undergo a security review by a government agency. The Kao Group processes personal information on a Japanese server as part of its information system for cosmetics customers. In order to meet China's legal requirements, the cosmetics customer system that deals with customers in China must be separated out and the data stored in China.

Security assessments outside Japan

Security assessments outside Japan are conducted by the Kao Group's overseas companies to check the following 158 items in order to identify areas where security measures are weak and to make improvements.

Main items to check

- Security policies and standards
- User authentication
- System operation & control
- IT asset management
- Control of the physical environment
- Protection from malware
- Incident management
- Compliance
- Handling of disaster recovery

In 2018, overseas security assessments were conducted at 10 companies in Asia, three companies in the Americas, and three companies in Europe to improve cybersecurity.