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

We have established 30 business- or region-specific (or country- or territory-specific) Information Security Committees (ISCs). These ISCs formulate common policies, rules and guidelines and take action to strengthen information security in order to protect information assets that include confidential information (trade secrets [TS]) and personal information as well as IT hardware, software and many kinds of data records.

Kao's creating value to address social issues

Social issues we are aware of

The rapid development and spread of information technology (IT) has resulted in IT spreading to every aspect of our lives, and it has become an indispensable part of social infrastructure. If the IT infrastructure of society is disruptive, this could have a major impact on economic activities due to the interruption of electricity, gas and water lifelines as well as transportation infrastructure. Moreover, cyberattacks have resulted in leaks of information assets including confidential information and personal information from companies, and ensuring cybersecurity has become a social issue. With the enactment of the Basic Act on Cybersecurity in November 2014, the entire country has been working on cybersecurity issues.

At Kao, the ISC in Japan plays a central role in establishing incident response structures and preparing for incidents in collaboration with the Risk and Crisis Management Committee. For technical measures, Enterprise Information Solutions takes the initiative in conducting risk assessments and implementing measures in line with the roadmap for security measures. What we seek is to implement security measures that will prevent cyberattacks and to build and maintain mechanisms and systems that can minimize damage even if we are subjected to cyberattacks.

Also, the protection of personal information has been reinforced in recent years pursuant to the EU General Data Protection Regulation (GDPR) and the laws of individual countries. We are aware that responding to the increasingly rigorous protection of personal information in each country is a social issue. The definitions of personal information and the duties of business operators relating to the handling of personal information vary under the laws of each country. We ascertain the details of personal information protection laws that are enacted and amended, implement the measures that Kao Group companies should take, and comply with the personal information protection laws of each country.

Risks related to realization of What Kao Aims to Be by 2030

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

Opportunities related to realization of What Kao Aims to Be by 2030

By strengthening cybersecurity measures and the management of information assets including confidential information (TS) and personal information, such data can be utilized in new ways, new business can be created, and new styles of working will be enabled through the use of networks.

Kao's creating value

We hope to contribute to improving the security measures of the entire industry by sharing information with other companies in the industry about the cyberattacks that we have experienced through our participation in information-sharing networks: the Initiative for Cyber Security Information Sharing Partnership of Japan, 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). We also participate in the Security Information Management Subcommittee established by the Japan Chemical Industry Association, an industry organization, and are working to exchange information with other companies.

Contributions to the SDGs

8 DECENT WORK AND ECONOMIC GROWTH
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS

Information security 102-43, 404-2

Policies

We have formulated our Information Security Policy, Guidelines on Handling Trade Secrets, Guidelines on Handling Personal Information and IT Security Guidelines (for Administrators) (for Users). We also carefully manage cybersecurity measures, TS and personal information in accordance with the policy and guidelines. Such efforts are not only carried out in accordance with laws and regulations and the guidelines set forth by government agencies and committees, but also designed to clarify our management framework and management methods.

The way how to handle personal information is disclosed in the Kao Group Company's Privacy Policy. Kao Group Company Inquiries and Complaint Reception Desk Regarding Personal Information is set up for inquiries or complaints. No claims relating to personal information were made in 2021.

Web
Kao Group Company Privacy Policy
Japanese version
www.kao.com/jp/corporate/privacy/
English version
www.kao.com/global/en/privacy/
For EMEA (GDPR compliant)
www.kao.com/emea/en/privacy/

Web
Kao Group Company Inquiries and Complaint Reception Desk Regarding Personal Information
Japanese version
www.kao.com/jp/corporate/privacy/privacy-contact
For the EU (GDPR compliant)
www.kao.com/global/en/EU-Data-Subject-Request/

Education and promotion

To ensure that employees throughout the group fundamentally understand the issues of protecting TS and personal information, in principle, internal education is conducted by each division. To do this, a general meeting is held every November for the members of the TS & Personal Information Protection Committee and for Personal Information Controllers from each division to (i) give lectures on and raise awareness about TS, personal information and information security (ii) analyze the number of incidents and trends relating to TS and personal information and provide feedback and (iii) provide educational materials for training in each division. The November 2021 meeting was held in conference rooms and through web conferencing with 321 TS & Personal Information Protection Committee members and Personal Information Controllers participating.

Company-wide educational materials are posted and timely warnings for all staff are provided via the company intranet portal site. Also, to evaluate the effectiveness of the internal 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.

Overseas, each ISC prepares an education and self-inspection plan, carries it out, and submits a report to Japan in March.

Collaboration and engagement with stakeholders

Cybersecurity measures

To undertake security measures for the supply chain as a whole, in 2021 we sent security questionnaires to logistics service providers (five companies in Asia and six in Europe and the Americas) and based on the results received, requested improvements where necessary.

Personal information protection in Japan

We conducted paper audits of 179 service provider companies, confirmed the status of personal information management systems, rules and security management measures, and supervised service providers.

Website vulnerability diagnosis

We performed vulnerability diagnoses of websites managed by Kao Group companies within and outside Japan and made sure there are no unaddressed vulnerabilities that may be exploited in cyberattacks. In cases where vulnerabilities were identified, software updates were implemented. We made improvements, particularly with regard to websites of salon brands in Europe and the Americas.

Information security 102-20

Framework

Information security management system

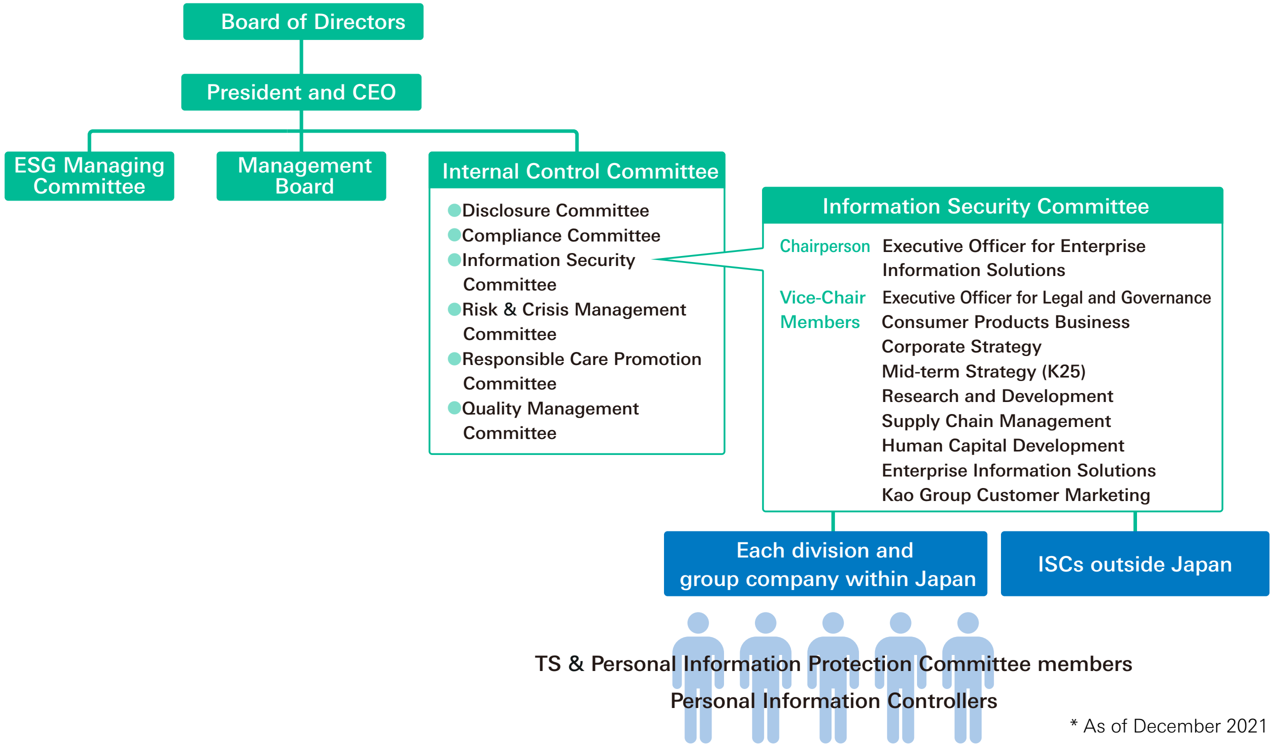
As a committee under the Internal Control Committee, the ISC in Japan supports the protection of information assets (including hardware, software and various types of data files) such as confidential information and personal information in order to achieve management goals, takes measures against cyberattacks on the Kao Group as a whole, and respond to the personal information protection laws of each country.

In Japan, we have appointed executive officers to serve as Chair and Vice-Chair of the ISC, and both the committee members and the staff of the committee's secretariat are appointed from different divisions, including Human Capital Development, Enterprise Information Solutions, Marketing, Research and Development, Intellectual Property Management, Supply Chain Management, and Legal and Governance. This allows us to benefit from a wide range of perspectives when determining policies, formulating internal rules, putting management systems in place and implementing awareness-raising activities.

The ISC reports on its activities to the Internal Control Committee, and each quarter 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, progress status and performance evaluations, and in the fourth quarter, the activity targets for the coming fiscal year is also reported. In the event of an incident that requires an emergency response, the ISC works in collaboration with the Risk and Crisis Management Committee and reports to management immediately.

Overseas ISCs are made up of members of the Management Boards of each company, and the ISCs are positioned under the ISC in Japan. As in the case in Japan, the activities of the ISCs include quarterly activities based on the PDCA cycle, and ISCs are required to submit reports to the ISC in Japan in March of each year.

Information security management system


Board of Directors
President and CEO
ESG Managing Committee
Management Board
Internal Control Committee
Disclosure Committee
Compliance Committee
Information Security Committee
Risk & Crisis Management Committee
Responsible Care Promotion Committee
Quality Management Committee
Information Security Committee
Chairperson
Executive Officer for Enterprise Information Solutions
Vice-Chair
Executive Officer for Legal and Governance
Members
Consumer Products Business
Corporate Strategy
Mid-term Strategy (K25)
Research and Development
Supply Chain Management
Human Capital Development
Enterprise Information Solutions
Kao Group Customer Marketing
Each division and group company within Japan
ISCs outside Japan
TS & Personal Information Protection Committee members
Personal Information Controllers

* As of December 2021

Information security 102-20

Status of establishing ISCs

Division	Number	Company / Region
Headquarters	1	Kao Corporation
Consumer Products	2	Kao (Taiwan) Corporation
	3	KPSS Taiwan Ltd.
	4	Kao (Hong Kong) Ltd.
	5	KPSS Hong Kong Ltd.
	6	Kao Industrial (Thailand) Co., Ltd. / Kao Consumer Products (Southeast Asia) Co., Ltd.
	7	PT. Kao Indonesia
	8	Kao Singapore Pte. Ltd.
	9	Kao (Malaysia) Sdn. Bhd.
	10	Kao Vietnam Co., Ltd.
	11	Kao Consumer Products (EMEA)
	12	Kao Consumer Products (Americas)
Chemical	13	Kao Group companies in Penang, Malaysia
	14	Pilipinas Kao, Incorporated
	15	PT. Kao Indonesia Chemicals
	16	Kao Corporation, S.A. (Spain)
	17	Kao Chemicals GmbH
	18	Quimi-Kao, S.A. de C.V.
	19	Kao Chimigraf, S.L.
	20	Kao Specialties Americas LLC
	21	Kao Collins Inc.
Kao Group	22	Kao Group companies in China
Kanebo Cosmetics Inc.	23	Kanebo Cosmetics (Europe) Ltd.
	24	Kanebo Cosmetics Deutschland GmbH
	25	Kanebo Cosmetics Italy S.p.A
	26	Taiwan Kanebo Cosmetics, Co., Ltd.
	27	Kanebo Cosmetics (Thailand) Co., Ltd.
	28	Kanebo Cosmetics Malaysia Sdn. Bhd.
	29	Kanebo Cosmetics Korea Co., Ltd.
	30	Kanebo Cosmetics Rus LLC

Report format for submission to the ISC in Japan

No.	Items	Content
1	Self-awareness-raising activities	Conducted for all employees. Describe the details of awareness-raising and the targets.
2	Self-checks	Describe the details of self-checks and the respondents. How have the respondents prepared the details? • Respondents are selected through sampling of employees in each division • Managers ascertain conditions in their divisions and respond • Other
3	Setting improvement targets and taking action	Based on the results of self-checks, set improvement targets for those items with poor results and describe an improvement plan.
4	Number of incidents	State the number of cases of theft, loss, erroneous transmission of confidential information, and theft or loss of information equipment for each type. Describe the details in an incident report.
5	Information relating to personal information	State the amount of personal information that is held, the number of complaints regarding personal information and the number of requests to delete personal information.
6	Other	Describe reports relating to TS, personal information and cyberattacks, if any.

Information security 102-20

Incident response system

Incident response systems are established and measures are taken to minimize damage in preparation for potential cyberattacks, leaks of information and other such incidents. To prepare for actual incidents, tabletop exercises are conducted multiple times each year.

Kao's incident response members and their roles

Name	Members	Roles, tasks, etc.
Top management	• Representative Director • Audit & Supervisory Board Members	• Identifying major incidents • Determination and approval of response measures, disclosures and measures to prevent recurrence
Risk & Crisis Management Committee	• Chairperson • Secretariat	• Escalation by the cyberattack / personal information protection response team
Emergency Countermeasure Meeting CSIRT (Computer Security Incident Response Team)	• ISC Chairperson • ISC Members • ISC Secretariat • Risk Management and RC • Strategic Public Relations • Employee Service • MK Platform • Consumer CC • Responsible divisions	• Identifying and responding to incidents • Immediate response: determination of network isolation, suspension of server operation, suspension of accounts and other related issues • Report to top management: Preparation, reporting and implementation of immediate response measures and measures to prevent recurrence, decisions on disclosure to stakeholders and relevant external organizations
SOC (Security Operation Center)	• Enterprise Information Solutions: Networks, servers and security services • Strategic Public Relations: Responses to mass media, preparation of news releases • Risk Management and RC: Social media monitoring • Customer Success: Management of memberships and campaign-related website • Consumer CC: Management of external reports • ISC Secretariat: Management of reports from the National Police Agency, IPA and JPCERT / CC	• Implementation of various types of monitoring and detection of outliers. If an outlier is detected, report to CSIRT, investigate the cause and implement technical responses • Receive external reports, confirm facts and report to CSIRT
Stakeholders / Relevant external organizations	• Suppliers • Employees • Consumers • Mass media • Supervisory authorities • Police • IPA • JPCERT / CC • Information sharing networks	• Disclosure of information to stakeholders, reporting to supervisory authorities • Request for support to police, IPA and JPCERT / CC • Provision of information to information sharing networks

* Risk Management and RC: Risk Management & Responsible Care, Consumer CC: Consumer Communication Center, MK Platform: Marketing Platform

Kao's incident response flow

	Detection	Identification	Response
Top management and Audit & Supervisory Board Members Risk & Crisis Management Committee		Day of initial report	• Report • Response measures, announcement, approval of measures to prevent recurrence Next day and later
ISC (CSIRT)	Immediately	• Understanding the facts • Decision on urgency • Emergency Countermeasure Meeting • Preparation of management report • Requests for external support Day of incident	• Response measures, warnings, announcement, recurrence prevention measures, examination of responses to inquiries, etc., preparations
SOC	• Monitoring • Reports from employees • Reports from outside • Social media posts	• Analysis • Investigation of causes	• Response measures, warnings, announcement, recurrence prevention measures, responses to inquiries
Stakeholders (Relevant external organizations, security companies)		• Request for support to police, IPA and JPCERT / CC • Coordination with contract counterparties	• Warnings, announcements, incident reports, information sharing

Information security

Mid- to long-term targets and performance

Mid- to long-term targets

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

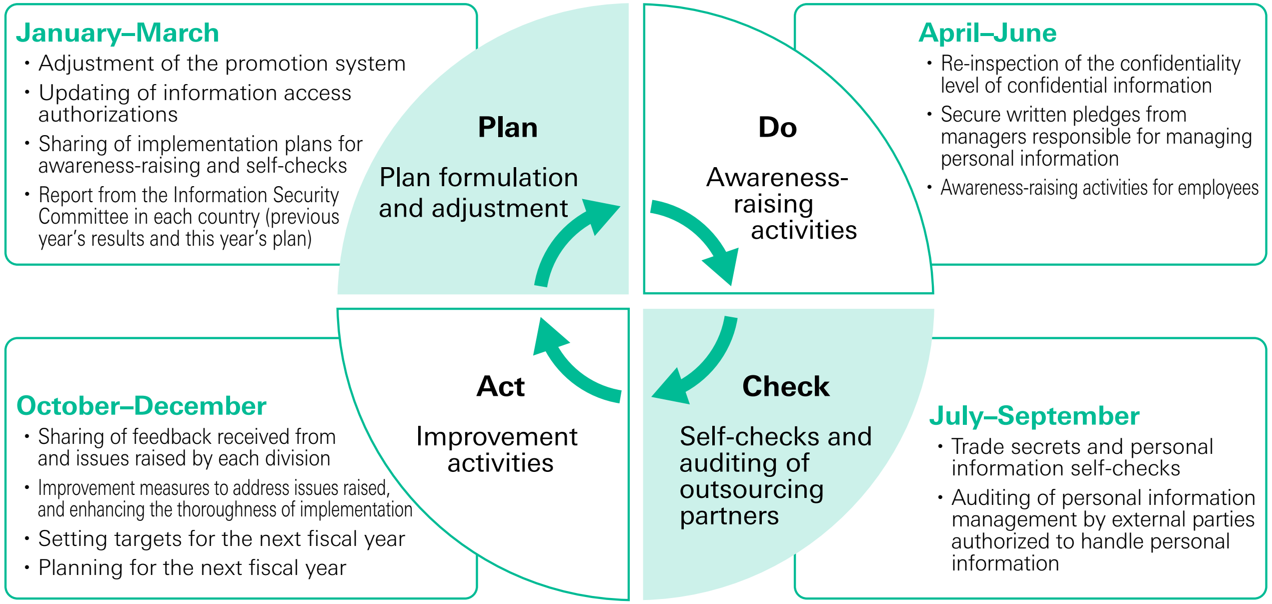
Business impacts

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

Social impacts

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



January–March

- Adjustment of the promotion system
- Updating of information access authorizations
- Sharing of implementation plans for awareness-raising and self-checks
- Report from the Information Security Committee in each country (previous year's results and this year's plan)

Plan

Plan formulation and adjustment

Do

Awareness-raising activities

April–June

- Re-inspection of the confidentiality level of confidential information
- Secure written pledges from managers responsible for managing personal information
- Awareness-raising activities for employees

Act

Improvement activities

Check

Self-checks and auditing of outsourcing partners

October–December

- Sharing of feedback received from and issues raised by each division
- Improvement measures to address issues raised, and enhancing the thoroughness of implementation
- Setting targets for the next fiscal year
- Planning for the next fiscal year

July–September

- Trade secrets and personal information self-checks
- Auditing of personal information management by external parties authorized to handle personal information

Information security

Performance in 2021

Performance

TS and personal information protection promotion activities conducted in Japan using the PDCA cycle were as follows.

Plan: Plan formulation and adjustment

- Adjustment of the promotion system and updating of information access authorizations
  —Reviews of 208 TS Promotion Committee Members and 192 Personal Information Controllers
- Review of confidential information lists
  —Reviews by 109 divisions, departments and affiliated companies in Japan
- Sharing of implementation plans for awareness-raising and self-checks
- Reports from overseas ISCs (previous year's results and this year's plan)

Do: Awareness-raising activities

- Re-inspection of the confidentiality level of confidential information
- Submission of a pledge by each Personal Information Controller
- Awareness-raising activities for employees
  —Awareness-raising activities in 108 divisions, departments and affiliated companies in Japan

Check: Self-checks and auditing of outsourcing partners

- TS and personal information self-checks
  —Working from home has become prolonged since March 2020, so the following questions were again reviewed before the TS self-checks were carried out.
  —Storage of confidential information when working from home
  —Necessity of printing confidential information when working from home
  —Self-checks on TS in 123 divisions, departments and affiliated companies in Japan
  —Self-checks on personal information in 97 divisions, departments and affiliated companies in Japan
- Auditing of outsourcing partners that handle personal information
  —Paper audits of 179 outsourcing partners that handle personal information

Act: Improvement activities

- Feedback to and issue sharing with individual divisions
- Improvement measures to address the issues raised, enhancing the thoroughness of their implementation and setting targets for the next fiscal year

At Kao, there were no serious incidents related to information security, including TS and personal information protection. No claims relating to personal information were directed to inquiry desks.

Reviews of performance

It is necessary to carry out promotion activities to protect TS and personal information on a continuous basis every year. Since even those who fully understood TS and personal information protection lose clarity in their knowledge over the years, the risk of an incident occurring increases. It is important that all employees, including new hires and mid-career hires, understand and follow our TS and personal information protection rules.

In order to expand our TS and personal information protection promotion activities globally, we established systems and created 29 overseas ISCs, which vary in size among regions, company groups and individual companies. Overseas ISCs submit activity reports in March of each year.

Information security

Our initiatives

First quarter: Plan formulation and adjustment

Formulation of Japan ISC activity targets

The following ISC activity targets for 2021 were set and measures were taken to achieve them.

1. ISC activities at overseas companies

- Submission of reports to Japan in March (PDCA cycle activities, etc.)
- Security assessment of third-party logistics

2. Cyber insurance coverage

- Coverage obtained on April 1, 2021. The scope of coverage is the entire Kao Group.
- Insurance coverage: Crisis management response costs, third-party liability costs, costs for responding to the authorities in foreign countries, financial damage to the company, business interruption expenses

3. Confirmation of compliance with personal information protection laws (GDPR / CCPA, etc.) in each country

- GDPR: 2018 cookie response method modified
- Personal information controls reinforced in response to the revised Act on the Protection of Personal Information coming into effect

4. Reinforcement of cybersecurity measures

- Security strategy roadmap formulated
- Measures implemented in line with the security strategy roadmap

5. Measures based on the PDCA cycle

- Awareness-raising materials and TS and personal information self-checks questions reviewed
- Awareness-raising activities implemented (by individual divisions)
- TS and personal information self-checks and audits of personal information outsourcing partners conducted
- The TS & Personal Information Protection Promotion Meeting held on November 15, 2021

Second quarter: Awareness-raising activities

Awareness-raising activities implemented by individual divisions and affiliated companies

In Japan, rules and general security awareness-raising materials are posted on the internal portal site. In addition, we undertake awareness-raising activities in each division using the educational videos used in the TS & Personal Information Protection Promotion Meeting held in November of the previous year as well as materials regarding TS and personal information incidents and self-checks feedback.

Third quarter: Self-checks and auditing of outsourcing partners

Self-checks of TS and personal information protection

TS self-checks are conducted every year as part of the thorough implementation of confidential information management including implementation of awareness-raising activities, maintenance of division manuals and implementation of TS marking. In 2021, self-checks took place from August 2 to September 10.

Personal information self-checks were similarly conducted at the same time regarding management of personal information, including implementation of awareness-raising activities, retention of personal information and outsourced tasks where personal information is handled.

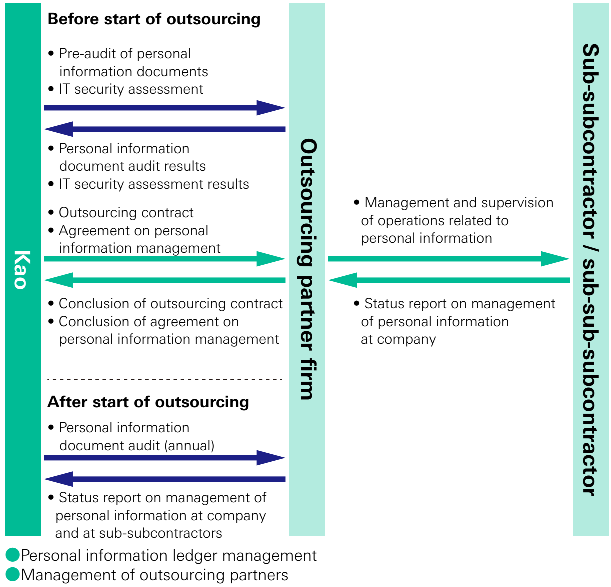
Auditing of outsourcing partners handling personal information

When outsourced business tasks involve handling personal information, we conduct a pre-audit to ensure that the outsourcing partner properly manages personal information. We also conduct an IT security assessment if the partner provides a service such as a web campaign. The conclusion of service contracts is conditioned on the outsourcing partner passing the personal information pre-audit and IT security assessment.

In addition, we manage and monitor partners handling personal information by conducting annual audits of such partners. In 2021, we conducted such audits at 179 companies and confirmed the status of personal information management and the systems for protecting personal information. If personal information is stored by a partner, we confirm the number of records and check for consistency with the number of data records registered in our personal information handling ledger system.

Information security 404-2

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


Kao
Outsourcing partner firm
Sub-subcontractor / sub-sub-subcontractor
Before start of outsourcing
• Pre-audit of personal information documents
• IT security assessment
• Personal information document audit results
• IT security assessment results
• Outsourcing contract
• Agreement on personal information management
• Conclusion of outsourcing contract
• Conclusion of agreement on personal information management
• Management and supervision of operations related to personal information
• Status report on management of personal information at company
After start of outsourcing
• Personal information document audit (annual)
• Status report on management of personal information at company and at sub-subcontractors
●Personal information ledger management
●Management of outsourcing partners

Fourth quarter: Improvement activities

Holding of the 28th TS & Personal Information Protection Promotion Meeting

The 28th TS & Personal Information Protection Promotion Meeting was held on November 15, 2021. The meeting was held in person and online with 321 persons participating. Continuing from the previous years, we conducted awareness-raising in the form of an explanation of Kao's current status after watching an awareness-raising video created by the IPA.

After that, a report was given on incidents related to TS and personal information in 2021. Feedback was then provided on TS and personal information self-checks, and improvement targets were set.

We set as improvement targets steady implementation of awareness-raising activities, prohibition of bringing out confidential information in paper form (documents) from the office in principle, and annual resubmission of the pledge when using the personal information dedicated server. The annual resubmission of the pledge also has the significance of calling attention to the handling of personal information, and we are considering using Microsoft Forms to ensure comprehensive implementation.