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

We have established 24 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.

ESG Keyword | Cybersecurity measures | Confidential information protection | Personal information protection | Information assets protection | GDPR responses | Incident response system | Website vulnerability diagnosis | Security measures for working from home

Kao's creating value to address social issues

Social issues we are aware of

Every company uses information technology (IT) to promote efficiency in its business and operations, and data to develop innovations and initiate reforms. IT 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 lead to information leaks. Cyberattacks adversely affect business performance and have turned cybersecurity into a social issue.

With the increase in working from home during the COVID-19 pandemic, information management and ensuring security including when employees work from home have become key issues.

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 (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 What Kao Aims to Be by 2030

A major risk is 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.

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

By strengthening cybersecurity measures and the management of data, TS and personal information, such data can be utilized in new ways and new styles of working will be 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 (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 Kao's 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 2020.

➡ 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/
➡ 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/

Information security 102-20, 102-43, 103-2, 404-2

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. We arrange lectures covering information security related to the protection of TS and personal information for the members of the TS & Personal Information Protection Committee and for Personal Information Controllers, conduct awareness-raising activities to familiarize staff with the latest trends, and provide educational materials to each division.

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 and carries it out.

Collaboration and engagement 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: J-CSIP, which is directed by the Information-technology Promotion Agency, Japan (IPA), and the National Police Agency's Cyber Intelligence Information Sharing Network. Since 2017, we have also participated in the JPCERT/CC's Early Warning Information program.

In addition to obtaining information on software vulnerabilities and cyberattacks from these information sharing networks, by disclosing and sharing information about Kao's cyberattacks, we contribute to Japan's cyber security measures.

Framework

Information security management system

In Japan, we have appointed executive officers to serve as Chair and Vice-Chair of the Information Security Committee (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, R&D, Intellectual Property Management, Production and Engineering, and Legal and Compliance. 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 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.

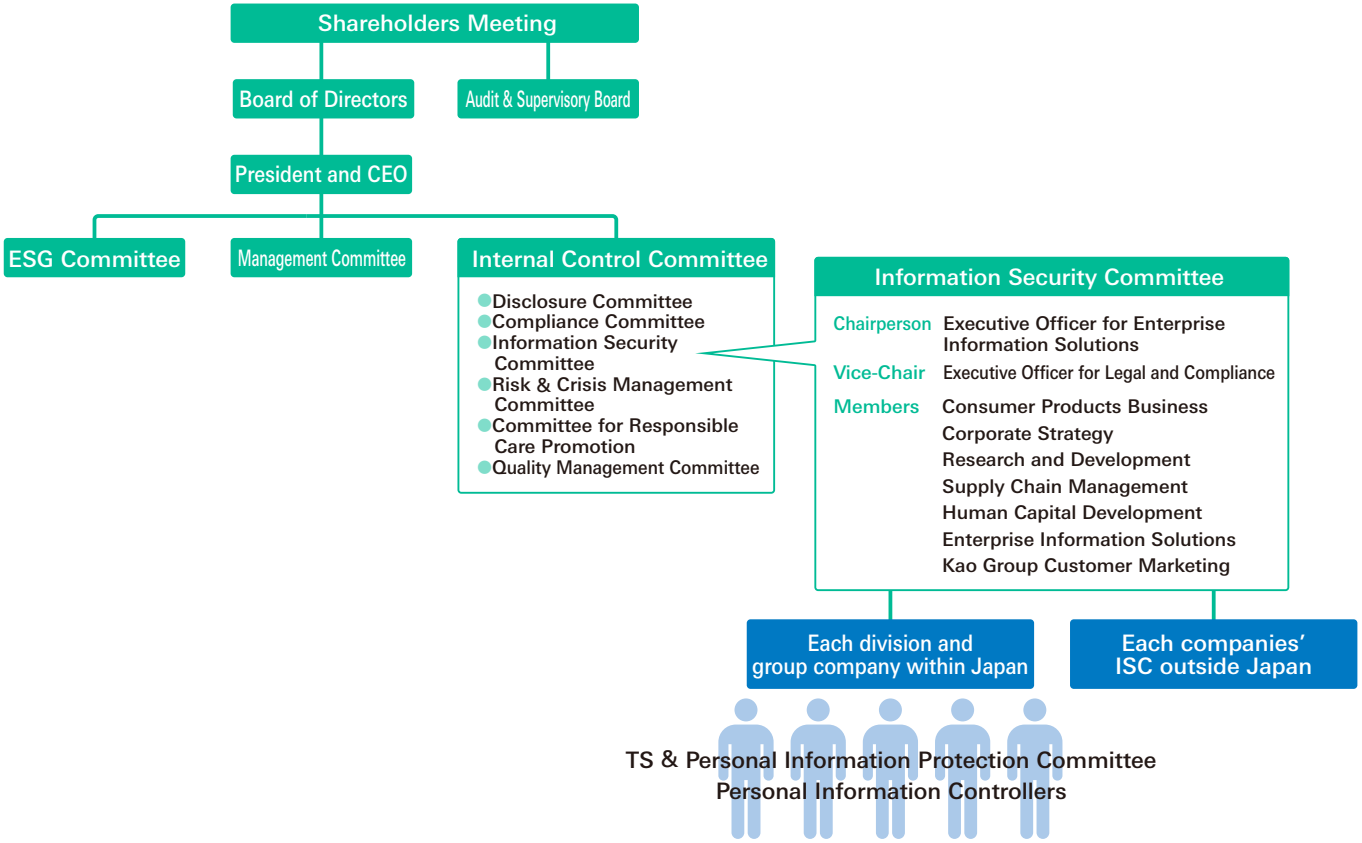
Overseas ISCs are made up of members of the Management Committees of each company, and individual ISCs are positioned under the ISC in Japan. As in the case in Japan, the activities of overseas ISCs include quarterly activities based on the PDCA cycle, and ISCs are required to submit reports to the ISC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

Status of ISC

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

Information security 102-20, 103-2

Information security management system



* As of December 2020

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. Which of the following patterns to the respondents fall under? • 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	Amount of personal information held	State the amount of personal information that is held.
6	Number of claims relating to personal information	State the number of claims that were made relating to personal information.
7	Other	Describe reports relating to TS, personal information and cyberattacks, if any.

Information security 102-20, 103-2

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 • Crisis Management and RC Promotion • Employee Service • Corporate Communications • Consumer CC • MK Platform • 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 • Corporate Communications: Response to mass media, preparation of news releases • Crisis Management and RC Promotion: 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 Tokyo Metropolitan Police Department, 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

* Crisis Management and RC Promotion: 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 • Announcement of response measures • Approval of measures to prevent recurrence Next day and later
Information Security Committee (ISC) Emergency Countermeasure Meeting	Immediately	• Understanding the facts • Decision on urgency • Emergency Countermeasure Meeting • Preparation of management report • Requests for external support Day of incident	• Announcement of response measures • Announcement of warnings • Announcement of recurrence prevention measures • Preparations for responses to inquiries, etc.
Security Operation Center (SOC)	• Monitoring • Reports from employees • Reports from outside • Social media posts	• Analysis • Investigation of causes	• Announcement of response measures • Announcement of warnings • Announcement of 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	• Announcement of warnings • Filing reports on incidents to authorities • Information sharing

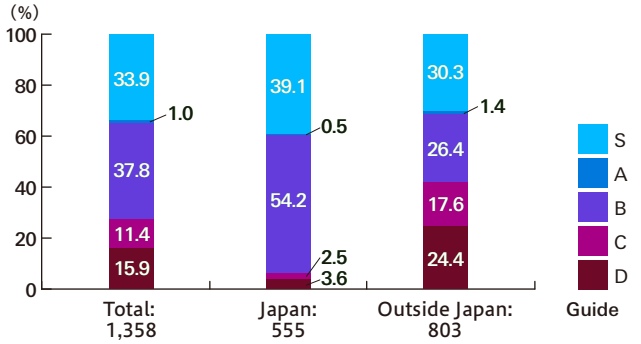
Information security 103-3

Website vulnerability diagnosis

We perform vulnerability diagnoses of Kao websites, check for any unaddressed vulnerabilities that may be used in cyberattacks, and if any exist, resolve the problems as soon as possible. For example, we resolve issues through responses such as updating software for which support has terminated.

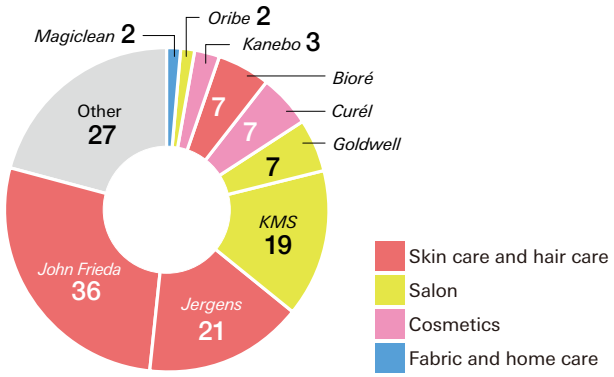
An improvement trend has been observed, particularly in European and U.S. salon brands' websites.

Website vulnerability diagnosis (2020)



Level	Priority	Example of vulnerability	Anticipated risks
S	N/A	No problems detected	
A	Reference	Deficiency in server certificate settings	Distrust in websites by users Decreasing website reputation
B	Low	Unneeded ports opened	Risk of being used in attacks
		Exposure of product version information	Used as valuable information in attacks
		Deficient SSL encryption settings	Interception of user communications
C	Medium	Opening of maintenance ports	Increase in likelihood of attack
D	High	Use of products with reported high-risk vulnerabilities	Exploitation of product vulnerabilities
		Use of products for which support has terminated	

Corresponding brands



Corresponding domains

Domains	Number of rank C / D	Countries and regions
ca	6	Canada
nl	4	Netherlands
us	4	U.S.
org	3	—
kr	3	Korea
cm	3	Cameroon
eu	3	EU
br	2	Brazil
mobi	2	—
be	2	Belgium
ch	2	Switzerland
nz	2	New Zealand
dk	2	Denmark
fi	2	Finland
no	2	Norway
se	2	Sweden
ie	1	Ireland

Information security 103-2, 103-3

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

Anticipated benefits from achieving mid- to long-term targets

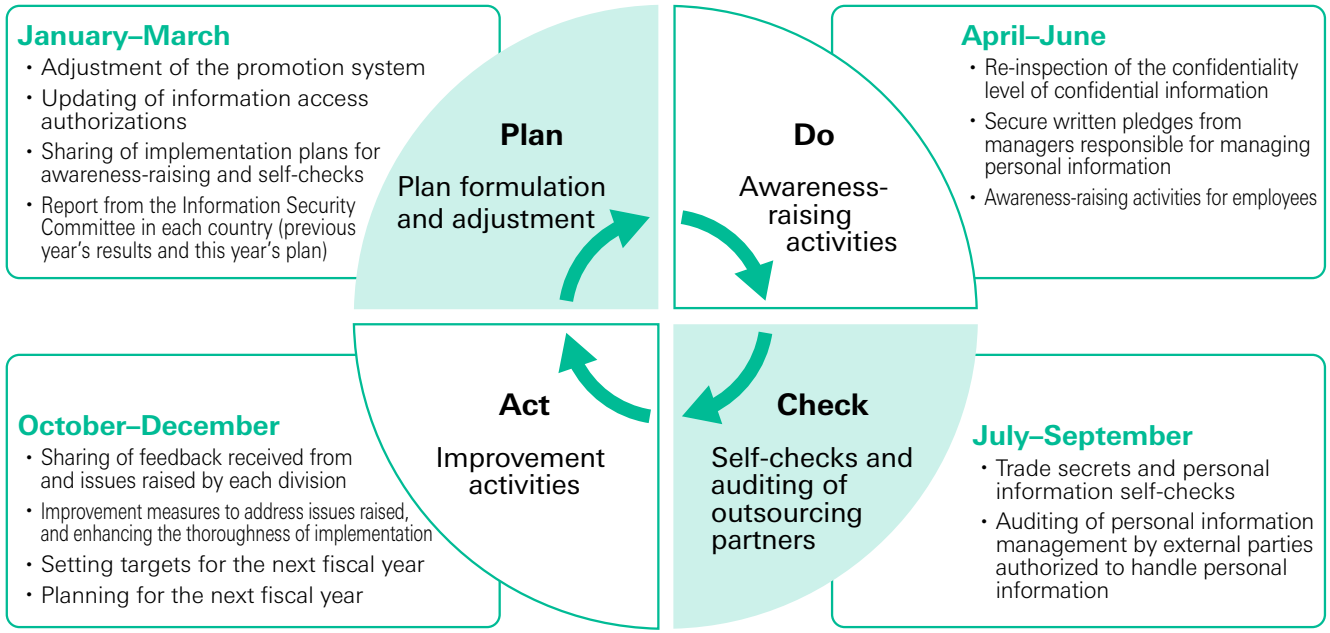
Business impacts

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



Information security 103-2, 103-3

Performance in 2020

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 59 TS Promotion Committee Members and 71 Personal Information Controllers
- Review of confidential information lists
  —Reviews by 105 divisions, departments and affiliated companies in Japan
- Sharing of implementation plans for awareness-raising and self-checks
- Report from the ISC in each country (previous year's results and this year's plan)

Do: Awareness-raising activities

- Submission of a pledge by each Personal Information Controller
- Submission of a pledge by each Personal Information Controller
- Awareness-raising activities for employees
  —Awareness-raising activities in 113 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, 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 124 divisions, departments and affiliated companies in Japan
  —Self-checks on personal information in 109 divisions, departments and affiliated companies in Japan
- Auditing of outsourcing partners that handle personal information
  —Paper audits of 190 outsourcing partners that handle personal information

Act: Improvement activities

- Feedback to and issue sharing with individual divisions
  —As a result of people working from home, refraining from going out and self-imposed restrictions on restaurant operations and the like, incidents involving TS and personal information were halved.
  —Incidents resulting from misdirected e-mail and postal mail increased while people worked from home
- Improvement measures to address the issues raised, enhancing the thoroughness of their implementation and setting targets for the next fiscal year
  —Thorough management of confidential information when working from home
  —Prevention of misdirected e-mail and postal mail

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 including submission of activity reports by affiliated companies outside Japan in March of each year. Going forward, we will gather overseas information for disclosure.

Information security 103-2

Our initiatives

First quarter: Plan formulation and adjustment

Formulation of Japan ISC activity targets

The following ISC activity targets for 2020 were set and measures were taken to achieve them.

1. Expanding ISC for overseas companies
- Submission of reports to Japan (PDCA cycle activities, etc.) (March)
  → Reports submitted by 23 ISCs
- Timely issuance of warnings
  → Warnings were issued regarding an online conferencing tool (April)

2. Enhanced control of personal information
- Introduction of personal information management tools at overseas companies
  → Full-scale operations in the EU starting in August

3. Confirmation of compliance with personal information protection laws (CCPA, etc.) in each country and region
  → New activities started in response to the laws of foreign countries

4. Preparation of recovery plans for when incidents occur
  → Recovery completed when an incident occurred in April

5. Implementation of TS and personal information protection promotion activities using the PDCA cycle
  → Improvement targets were set at the TS & Personal Information Protection Promotion Meeting in November.

Second quarter: Awareness-raising activities

Warnings regarding an online conferencing tool

Many Kao employees have switched to working from home as a measure to prevent the spread of COVID-19. As a result, the use of online conferencing tools has increased; however, security issues with an online conferencing tool were identified. Because of the risk of information leaks and the possibility of unauthorized PC access, warnings were issued to employees prohibiting the use of the tool. The prohibition was later lifted when the security risks were resolved through software updates.

In this way, we exercise caution with regard to external circumstances that arise and take measures to protect our security.

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 2020, self-checks took place from July 21 to August 21.

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. Feedback on the self-checks was given at the TS & Personal Information Protection Promotion Meeting held on November 16, 2020, and improvement targets were set.

We set “thorough confidential information management when working from home” and “prevention of misdirected e-mail and postal mail” as improvement targets. To address handling of confidential information, in Japan we adopted the Kao Guidelines on Handling Trade Secrets, and overseas, we established the Global Trade Secret Regulations, and we manage confidential information accordingly.

We require employees to comply with the guidelines or regulations when they are working outside the office such as when working from home. When working in the office, checks by multiple staff members are possible, but when working from home, checks done by a single person increase. In these instances in particular, prevention measures such as requiring reconfirmation are necessary to prevent simple errors.

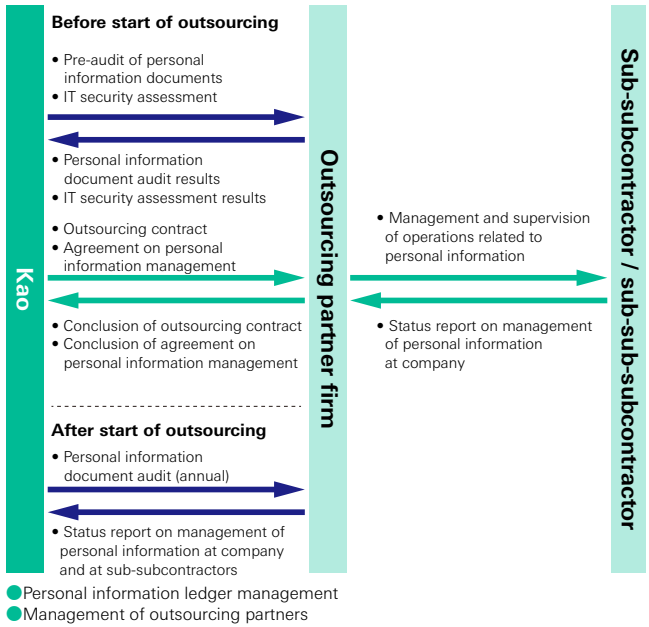
Information security 103-2, 404-2

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. A contract is not concluded unless the personal information pre-audit and IT security assessment show no problems.

In addition, we manage and monitor partners handling personal information by conducting annual audits of such partners. In 2020, we conducted such audits at 190 companies and confirmed the status of personal information management and the systems used by the partners 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 their personal information handling ledger system.

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



Third quarter: Announcement

Rules on printing when working from home established

We prepared rules on printing when working from home in March 2020, but internal announcement of the rules was suspended when it became possible to return to the office after the state of emergency declaration was lifted in May. In mid-July, however, we again shifted to working from home in response to a resurgence of COVID-19, and in August we announced that we would allow printing during working from home at the discretion of each department. This avoided a situation where employees would have to go to the office simply to print documents and reduced the risk of employee infection.

Fourth quarter: Improvement activities

Holding of the 27th TS & Personal Information Protection Promotion Meeting

The 27th TS & Personal Information Protection Promotion Meeting was held on November 16, 2020. Since the meeting was held during the COVID-19 pandemic, it was conducted fully online for the first time. In other years, outside instructors have been invited to give lectures on confidential information, personal information and security, and these issues were used as topics for educational activities in individual divisions. This year, we adopted a format where each participant watched instructional videos prepared by organizations involved in security such as the Tokyo Metropolitan Police Department and IPA, and then confirmed their key points. After the videos, a report was given on incidents related to TS and personal information in 2020. Feedback was then provided on TS and personal information self-checks, and improvement targets were set.