

Information Security

We have established 30 Information Security Committees in various countries, areas, worksites and companies. These Information Security Committees take action to strengthen information security in order to protect information assets that include cybersecurity measures, trade secrets, and personal information as well as IT hardware, software and many kinds of data records.

Social issues

The “Information Security White Paper 2023,” issued by the Information-technology Promotion Agency, Japan (IPA) provides the following examples:

“An increasing number of companies and organizations are falling victim to ransomware attacks. Observed methods of attack involve double extortion, where stolen data is disclosed, along with DDoS attacks targeting victim organizations, and extortion tactics such as blackmailing victims by suggesting that the attack would be revealed to their customers and stakeholders.”

“A ransomware attack targeting an automobile parts company in February 2022 resulted in shutting down an automobile factory that purchased parts from the affected company for one day. In another ransomware attack targeting a medical center in Osaka City in October of the same year, the attacker gained access through a VPN-connected food service provider, damaging the electronic health record system in the medical center via the server.”

Although these are examples from Japan, the situation is similar overseas. Cyberattacks targeting companies and organizations have resulted in a significant number of incidents, including the leakage of trade secrets and personal information and the halting of production activities and business activities due to ransomware. Consequently, security measures to prevent cyberattacks are recognized as social issues.

Also, protection of personal information has been reinforced in recent years under 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.

Policies

We seek 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 such attacks.

At Kao, the ISC in Japan plays a central role in establishing incident response structures and preparing for incidents in collaboration with the Risk & Crisis Management Committee. For technical measures, Enterprise Information Solutions takes the initiative in assessing risk, creating a roadmap for security measures, and implementing measures in line with it.

In Japan,

- Information Security Policy
- Guidelines on Handling Trade Secret Information
- Guidelines on Handling Personal Information
- IT Security Guidelines (for Administrators)
- IT Security Guidelines (for Users)
- Website Application Security Guidelines

Overseas,

- Information security policy
- Global Trade Secret Regulation
- IT security guidelines (currently being formulated)

We have formulated policies and guidelines including those above to carefully manage cybersecurity measures, trade secrets (TS), and personal information in accordance with them. Such efforts are not only carried out in accordance with laws and regulations and the guidelines set forth by government agencies and committees, but are also designed to clarify our policies for the management framework and management methods.

The definition of personal information and the obligations of companies to handle personal information

vary from country to country, depending on their laws. We ascertain the details of these laws that are enacted and amended, implement the measures that the Kao Group should take, and comply with the laws of each country.

Regarding our personal information handling policy and contact information, we have released the “Kao Group Privacy Policy” on the websites of our domestic and overseas companies.



Kao Group Company Privacy Policy
 Japanese version
<https://www.kao.com/jp/privacy/>
 English version
<https://www.kao.com/global/en/privacy/>
 For EMEA (Europe, the Middle East and Africa) (GDPR compliant)
<https://www.kao.com/emea/en/privacy/>

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

Strategy

Risks and opportunities

Risks

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 leaks of information including TS and personal information, is a major risk.

Information Security GRI 2-28

Opportunities

By strengthening cybersecurity measures and the management of information assets including TS and personal information, such data can be utilized in new ways, new business can be created, and new work-styles will become possible through the use of the ICT.

Strategy

We have implemented cybersecurity measures in line with the security strategy roadmap, considering their urgency and budget. In 2023, we rendered email attachments and links harmless, prevented email spoofing, implemented measures to prevent account hacking, and introduced Endpoint Detection and Response, which is security software that detects suspicious behaviors on PCs and servers and provides prompt responses to them.

We are also globally expanding a Security Operation Center (SOC) that monitors the networks, servers, and PCs 24 hours a day, 365 days a year, detects suspicious behaviors including cyberattacks and viruses, and responds to them immediately. In August 2023, we started blocking the transmission of email with password-protected zip files attached to prohibit PPAP. In addition to these efforts, we provide a security education program to our employees.

Social impact

Kao helps improve security measures in the industry and of all companies in Japan by sharing information on the cyberattacks Kao Corporation experienced through the information-sharing network.

For this purpose, we participate in the following initiatives:

- the Initiative for Cyber Security Information Sharing Partnership of Japan (J-CSIP) of the Information-technology Promotion Agency, Japan (IPA)
- Cyber Intelligence Information Sharing Network of the National Police Agency and
- the Japan Computer Emergency Response Team Coordination Center's (JPCERT/CC) Information Security Early Warning Partnership scheme.

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.

Carrying out cybersecurity measures for the entire supply chain also plays a part in improving cybersecurity for the entire industry and for Japanese companies overall.

Contributions to the SDGs



Business impact

By using cybersecurity measures to fend off business interruptions and the leakage and exposure of TS and personal information due to cyberattacks, we can prevent the loss of trust on our company. At the same time, we can avoid compensation payments and costs

associated with cause location, measure implementation and the like in the event that damage does occur. Also, damage can be minimized if measures are in place to respond to cyberattack incidents and the leakage of TS and personal information.

The Kao Group can enhance trust in security measures and facilitate new ways to use data, new businesses, and diverse styles of working using the ICT by putting strong security measures against cyberattacks in place.

Governance

Framework

Information security management framework

The Information Security Policy, which is the primary provision regarding information security, stipulates that the President & CEO shall appoint a Chief Information Security Officer (CISO) to take command of, and be responsible for, supervising the formulation and maintenance of information security measures. The CISO is an Executive Officer and takes on the position of chairperson of the ISC. The ISC supports the protection of information assets (including hardware, software and various types of data files) such as trade secrets and personal information, in order to achieve management goals, takes measures against cyberattacks on the Kao Group as a whole, and responds 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,

Information Security

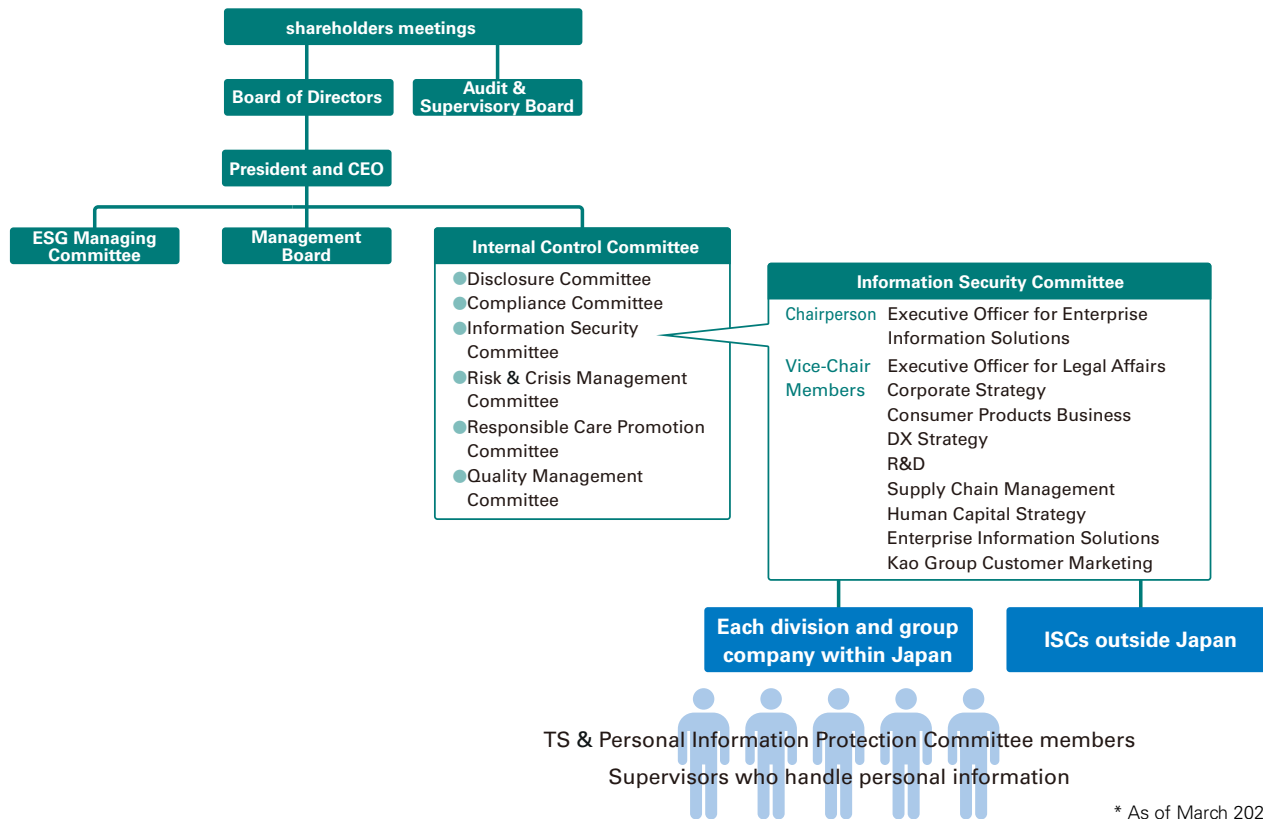
including Human Capital Development, Enterprise Information Solutions, Marketing, Research and Development, Intellectual Property Management, Supply Chain Management, and Legal. This enables us to benefit from a wide range of perspectives when determining policies, formulating internal rules, putting management systems in place, and implementing awareness-raising activities.

The ISC provides a report to the Board of Directors through the Internal Control Committee every quarter. 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 are also reported. In the event of an incident that requires an emergency response, the ISC works in collaboration with the Risk

& Crisis Management Committee and reports to management immediately.

Overseas ISCs comprise members of the Management Boards of each company, and the ISCs are positioned under Japan's ISC. As is the case with 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 framework



P25 Our ESG Vision and Strategy > Governance

Report format for submission to the ISC in Japan

No.	Item	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 does the respondent belong to? <ul style="list-style-type: none"> • 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 trade secrets, 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.

* As of March 2024

Information Security

Establishment status of Information Security Committee

Division	Number	Company / Region
Headquarters	1	Kao Corporation
Consumer Products	2	Kao (Taiwan)
	3	KPSS Taiwan Ltd.
	4	Kao (Hong Kong) Limited
	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
	9	Kao (Malaysia) Sdn. Bhd.
	10	Kao Vietnam Co., Ltd.
	11	Kao Consumer Products (EMEA)
	12	Kao Consumer Products (EMEA) U.S.
	Chemical	13
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, Sociedad Limitada
20		Kao Specialties Americas LLC
21		Kao Collins Inc.
China	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

Kao's incident response members and their roles

Name	Members	Roles, tasks, etc.
Top management	<ul style="list-style-type: none"> Representative Director Audit & Supervisory Board Members 	<ul style="list-style-type: none"> Identifying major incidents Determination and approval of response measures, disclosures and measures to prevent recurrence
Risk & Crisis Management Committee	<ul style="list-style-type: none"> Chairperson Secretariat 	<ul style="list-style-type: none"> Escalation by the cyberattack / personal information protection response team
Emergency Countermeasure Meeting CSIRT Computer Security Incident Response Team	<ul style="list-style-type: none"> ISC Chairperson ISC Members ISC Secretariat Risk Management & RC Strategic Public Relations Employee Services & General Affairs MK Platform Consumer CC Responsible divisions 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Enterprise Information Solutions: Networks, servers and security services Strategic Public Relations: Responses to mass media, preparation of news releases Risk Management & 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 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Suppliers Employees Consumers Mass media Supervisory authorities Police IPA JPCERT/CC Information-sharing networks 	<ul style="list-style-type: none"> 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

Note: Risk Management & 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		<p style="text-align: center;">Day of initial report</p>	<ul style="list-style-type: none"> Report Response measures, announcement, approval of measures to prevent recurrence <p style="text-align: center;">Next day and later</p>
ISC (CSIRT)	<p style="text-align: center;">Immediately</p>	<ul style="list-style-type: none"> Understanding the facts Decision on urgency Emergency Countermeasure Meeting Preparation of management report Requests for external support <p style="text-align: center;">Day of incident</p>	<ul style="list-style-type: none"> Response measures, warnings, announcement, recurrence prevention measures, examination of responses to inquiries, etc., preparations
SOC	<ul style="list-style-type: none"> Monitoring Reports from employees Reports from outside Social media posts 	<ul style="list-style-type: none"> Continuous analysis Investigation of causes 	<ul style="list-style-type: none"> Response measures, warnings, announcement, recurrence prevention measures, responses to inquiries
Stakeholders Stakeholders (Relevant external organizations, security companies)		<ul style="list-style-type: none"> Request for support to police, IPA and JPCERT/CC Coordination with contract counterparties 	<ul style="list-style-type: none"> Warnings, announcements, incident reports, information sharing

Information Security

Incident response system

An incident response system has been 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.

Education and promotion

Internal education is conducted by each division to ensure that employees throughout the group fundamentally understand the issues of protecting TS and personal information, in principle. To this end, a general meeting is held in Japan each November with Trade Secret & Personal Information Protection Committee members and Personal Information Controllers from each division to:

- (1) provide lectures and training on TS, personal information and information security;
- (2) analyze the number of incidents and trends related to Kao's TS and personal information and provide feedback;
- (3) set improvement targets; and
- (4) discuss topics on promoting TS and personal information protection and information security.

The 2023 meeting took place both offline and online with 266 TS & Personal Information Protection Committee members and Personal Information Controllers participating. (134 people viewed the meeting video.) 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 with stakeholders

Cybersecurity measures

Kao has conducted the security evaluations listed below in collaboration with contractors and suppliers as security measures for the entire supply chain.

- Security evaluation of third-party logistics (17 sites in Asia and 20 sites in the Americas/EMEA) in 2020
- Security evaluation of 107 packaging suppliers and 86 raw-material suppliers in 2022 (Procurement has consultations on effective measures for suppliers that are considered high-risk.)
- Security check evaluation of nine contract manufacturers in 2023

Paper audits of outsourcing partners handling personal information in Japan

We conducted paper audits of 200 service provider companies, confirmed the status of personal information management systems, rules and security management measures, and supervised service providers.

Website Application Security Guidelines

To present Kao's security requirements to system development contractors and ensure they meet the requirements when carrying out design and development, we have formulated and implemented the Website Application Security Guidelines.

These guidelines contain internal procedures and points of consideration related to the security of system personnel, development personnel, and operations personnel.

Risk management

Activities to promote TS and personal information protection conducted in Japan using the PDCA cycle were as follows.

Plan: Plan formulation and review

- Review of the promotion system and updating of information access authorizations
- Review of trade secrets lists
- Sharing of implementation plans for awareness raising and self-checks
- Report from the Information Security Committee outside Japan (previous year's results and this year's plan)

Do: Awareness-raising activities

- Re-inspection of the confidentiality level of trade secrets
- Secure written pledges from supervisors who handle personal information
- Awareness-raising activities for employees

Check: Self-checks and auditing of outsourcing partners

- TS and personal information
- Auditing of outsourcing partners that handle personal information

Information Security

Act: Improvement activities

- Summarizing incidents related to TS and personal information
- Feedback of TS and personal information self-checks
- Setting improvement targets

Risk identification

- Kao identifies whether trade secrets, personal information, and security are managed and operated according to rules through self-checks.
- Kao plans to identify risks associated with operations that handle personal information with risk scores in

the new personal information management system that began operating in July 2023.

Risk reduction

- Kao reduces risks identified through self-checks by providing feedback and setting improvement targets in plenary meetings.

P40 Our ESG Vision and Strategy > Risk management

Metrics and targets

Mid- to long-term targets and 2023 results

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, implementation of an emergency response, and formulation and implementation of measures to prevent recurrence

2023 results

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. Overseas, we received and promptly addressed 25 requests for deletion of personal information in the EU.

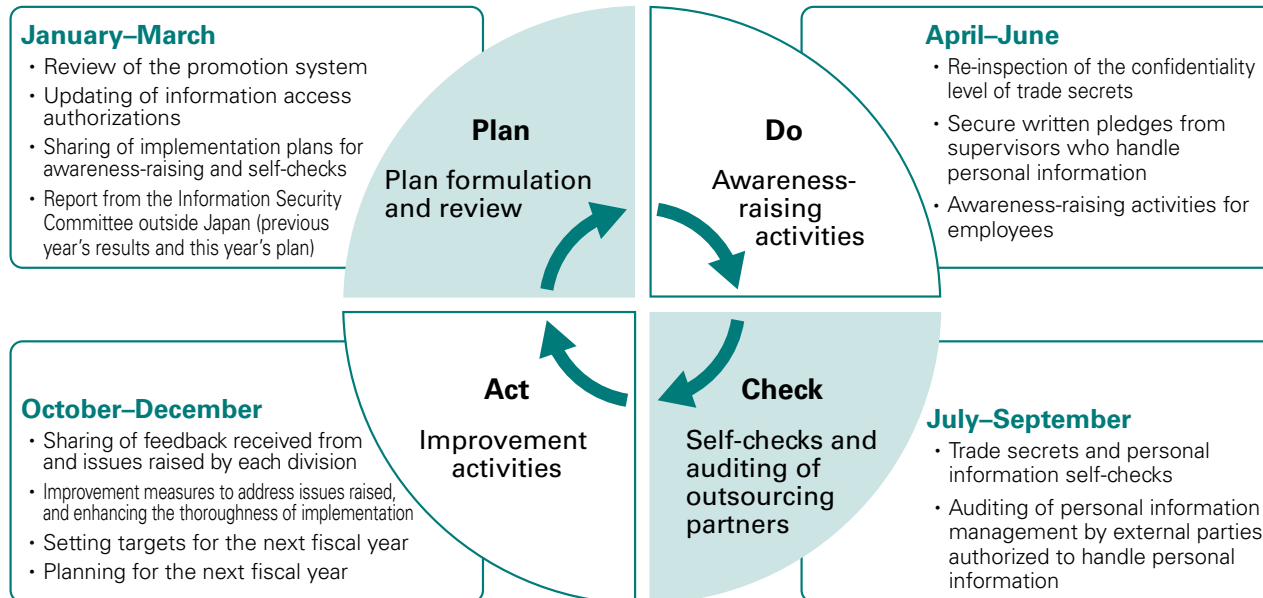
Plan: Plan formulation and adjustment

- Reviews of 316 TS Promotion Committee Members and 296 Personal Information Controllers
- Review of trade secrets lists by 125 divisions, departments and affiliated companies in Japan
- Reports received from 28 ISCs outside Japan (Kanebo Cosmetics Rus LLC is currently inactive.)

Do: Awareness-raising activities

- Submission of pledges on personal information from 2,391 people
- Conducted awareness-raising activities in 139 divisions, departments, and affiliated companies in Japan

PDCA cycle for information security activities



Information Security

Check: Self-checks and auditing of outsourcing partners

- Self-checks on TS in 146 divisions, departments and affiliated companies in Japan
- Self-checks on personal information in 116 divisions, departments and affiliated companies in Japan
- Audits of 200 outsourcing partners that handle personal information

Act: Improvement activities

At Kao, there were no serious incidents related to information security, including TS and personal information protection.

- On November 22, 2023, a plenary meeting was held both offline and online with 266 TS & Personal Information Protection Committee members and

Personal Information Controllers participating. (134 people viewed the meeting video.)

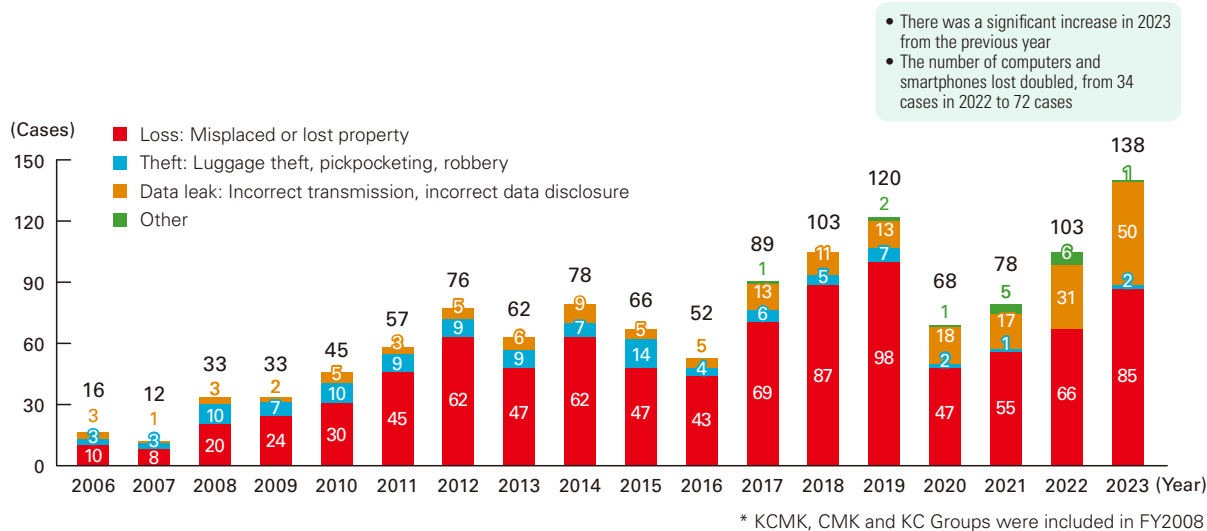
- The number of incidents related to TS and personal information in 2023 was 104 by the end of October. Out of these incidents, 67 were losses, with the majority involving the loss of company cell phones. Since company cell phones and company PCs are encrypted, the loss of these devices does not result in information leakage.

Reviews of 2023 results

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

In addition, 29 ISCs have been established overseas in overseas regions, corporate groups, and individual companies to promote the protection of TS and personal information throughout the Kao Group. We check the contents of the activities of ISCs outside Japan with activity reports they submit every March.

Change in the number of incidents in the Kao Group in Japan



Information Security

Main initiatives

Activity targets for the Information Security Committees (ISC)

The following ISC activity targets for 2023 were set and measures were taken to achieve them.

(1) Reinforcement of cybersecurity measures

- To enhance security, we strengthened security measures in accordance with the security strategy roadmap.
- We enhanced email security, website security, account security and endpoint security.
- Prohibition of PPAP

Because password-protected zip files attached to email cannot be checked for viruses, Kao has been blocking such email since August.

(2) Renewal of cyber insurance

- Coverage of cyber insurance
 - Crisis management costs
 - Third-party liabilities
 - Costs related to authorities in countries outside Japan
 - Economic damage to the Company (including data damage)
 - Costs related to business interruptions

(3) Interviews with suppliers about security measures

In July 2023, we considered conducting security checks at nine contract manufacturers but confirmed that they had already undergone checks during the supplier security check in 2022.

(4) Identification of main activities of the 29 Information Security Committees overseas

- Kanebo Cosmetics Rus: Inactive
- Conducting awareness-raising activities: 28

- Conducting self-checks: 26
- Setting targets: 26
- Incidents occurred: 22 cases from 6 companies
- Request for deletion of personal information: 25 (already addressed)
- Request for deletion of EU cookies: 84
- Complaints about personal information: 0

(5) Strengthening of domestic personal information management

The new personal information management system started in July. This system identifies the contents and amount of personal information, systems that processes the information, how the information is applied, and the locations of risks associated with the handling of personal information.

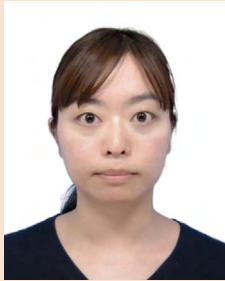
(6) PDCA (Plan, Do, Check, and Act) cycle for information security

1. Trade secrets lists, awareness-raising materials and TS and personal information self-check questions reviewed
2. Awareness-raising activities implemented (by individual divisions)
3. TS and personal information self-checks and audits of personal information outsourcing partners conducted
4. The Trade Secret and Personal Information Protection Promotion Meeting was held in November
 - Video presentations of awareness-raising activities and explanation of measures implemented by Kao
 - Report on incidents related to TS and personal information in Japan
 - Summary of self-checks
 - Setting of improvement targets
 - Explanation of changes to the scope of pledges on the handling of personal information

Information Security

Employees' opinions

Establishing a global secure infrastructure environment that supports DX



Shiho Amamiya

Enterprise Service Management,
Enterprise Information Solutions,
Kao Corporation

As a member of the Enterprise Information Solutions security team, I am in charge of planning security strategy, introducing solutions, monitoring, responding to incidents, and other activities across the entire Kao Group including overseas sites. In 2023, we completed global deployment of the authentication infrastructure that serves as the foundation of our security, establishing an environment where employees can securely use the IT anywhere, including overseas and work-at-home environments.

As cyberattacks become increasingly sophisticated and diversified each day, we will collaborate with IT staff not only in Japan but also overseas to establish a system that protects our company and employees.

Employees' opinions

Promoting global security enhancement



Tateki Nakaji

Legal,
Legal,
Kao Corporation

I am in charge of operations of the Information Security Committee's secretariat and of promoting personal information protection measures.

The Information Security Committee discusses new measures and other topics from various viewpoints, determines policies, formulates rules, maintains an internal management system, supervises periodic audits targeting external outsourcing partners, and promotes the implementation of awareness-raising activities every month except for August. In particular, regarding awareness-raising activities, the committee runs awareness-raising and educational activities for all employees in the Kao Group, and has observed that the awareness of every employee has increased through interactions such as question-and-answer sessions. The committee also closely liaises with the Information Security Committees outside Japan to globally promote security enhancement. Although measures to address increase every year as time marches forward, all employees will address them as a team.