Information Security

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

Social issues

The rapid development and expansion 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. Disruption to the social IT infrastructure 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 trade secrets and personal information from companies, so ensuring cybersecurity has become a social issue. With the Basic Act on Cybersecurity's enactment 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 & 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 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 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.

Policies

We have formulated our Information Security Policy, Guidelines on Handling Trade Secret Information, Guidelines on Handling Personal Information, IT Security Guidelines (for Administrators) (for Users) and Website Application Security Guidelines. We also carefully manage cybersecurity measures, trade secrets (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 are also designed to clarify our management framework and management methods.

The way to handle personal information is disclosed in the Kao Group Company's Privacy Policy. The Kao Group Company Inquiries and Complaints Reception Desk Regarding Personal Information has been established for inquiries or complaints.

Web

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 trade secrets (TS) and personal information, is a major risk.

Opportunities

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

Information Security GRI 3-3

Strategy

With regard to cybersecurity measures, we have secured a budget in accordance with the security strategy roadmap and implemented measures (determined by the degree of urgency of the security measures and the budget that can be allocated).

In 2022, we introduced various cybersecurity measures such as email security functionality (that renders email attachments and links harmless and prevents email spoofing), account monitoring functionality (a measure to prevent account hacking), and Endpoint Detection and Response (EDR: software that detects suspicious behaviors on PCs and servers and provides prompt responses to them) in AEMEA (the Americas, Europe, the Middle East and Africa) and Japan. We will complete the introduction of EDR in Asia in the first quarter of FY2023. We are also planning a global expansion of 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. At the same time, we will provide a security education program to our employees.

Social impact

Kao intends to help improve security measures in the industry and of all companies in Japan by sharing information about the cyberattacks Kao Corporation experienced with the industry and companies in Japan through the information-sharing network. For this reason, we participate in 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 Information Security Early Warning Partnership scheme of 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.

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

Contributions to the SDGs

Business impact

Cybersecurity measures can reduce costs incurred to respond to leaks of trade secrets (TS) and personal information by preventing such leaks. Also, damage can be minimized if measures are in place to respond to leaks of trade secrets (TS) and personal information.

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, the supervision of the formulation and maintenance of information security measures. The Chief Information Security Officer (CISO) is an Executive Officer and takes on the position of chairperson of the Information Security Committee (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, 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 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

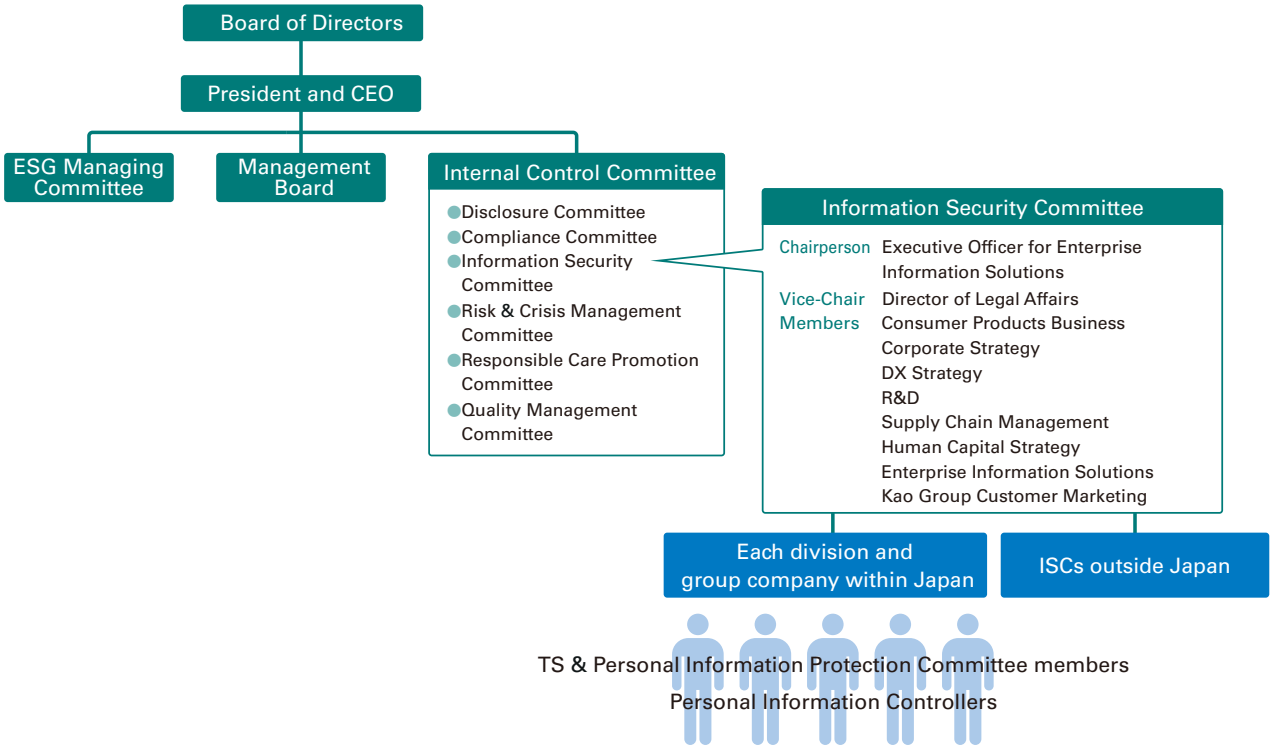
Information Security GRI 3-3

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 Managing Boards of each company, and the ISCs are positioned under Japan's ISC. As in 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.

P18 Our ESG Vision and Strategy > Governance

Information security management system



* As of January 2023

Information Security GRI 3-3

Establishment status of Information Security Committee (ISC)

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	Kao Penang Group
	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.
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.	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? • 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.

Information Security GRI 3-3

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.

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 & RC • Strategic Public Relations • Employee Services & General Affairs • 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 & 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

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		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	• Continuous analysis • Investigation of causes	• Response measures, warnings, announcement, recurrence prevention measures, responses to inquiries
Stakeholders 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 GRI 3-3, 404-2

Education and promotion

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

(1) provide lectures and training on trade secrets (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, and
(3) provide awareness materials for training in each division.

The November 2022 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 with stakeholders

Cybersecurity measures

In 2022, for security measures throughout the entire supply chain, we interviewed 107 packaging suppliers and 86 raw material suppliers and assessed their security measures. Procurement has consultations on effective measures for suppliers that are considered high-risk.

Paper audits of outsourcing partners handling personal information in Japan

We conducted paper audits of 206 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 trade secrets (TS) and personal information protection conducted in Japan using the PDCA cycle were as follows.

Plan: Plan formulation and adjustment

- 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 in each country (previous year's results and this year's plan)

Do: Awareness-raising activities

- Re-inspection of the confidentiality level of trade secrets
- Submission of a pledge by each Personal Information Controller
- Awareness-raising activities for employees

Check: Self-checks and auditing of outsourcing partners

- Conducting self-audits on trade secrets (TS) and personal information
- Auditing of outsourcing partners that handle personal information

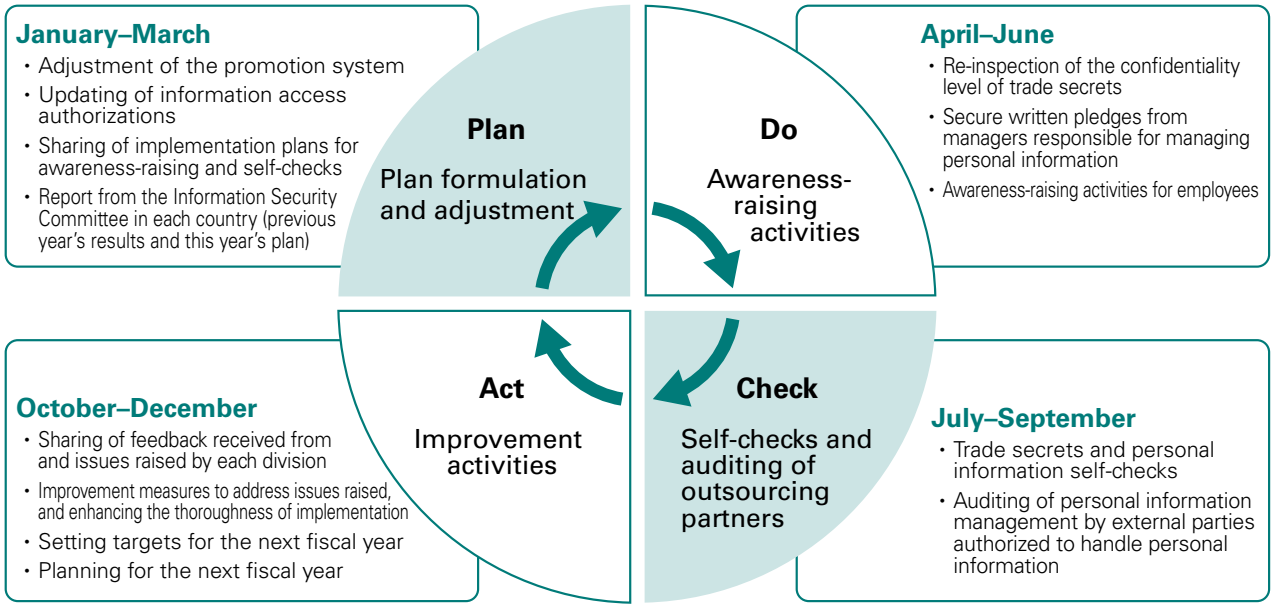
Act: Improvement activities

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

P33 Our ESG Vision and Strategy > Risk Management

Information Security

PDCA cycle for information security activities



Targets and metrics

Mid- to long-term targets and 2022 results

Mid- to long-term targets

- Protection of information assets such as trade secrets (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

2022 results

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

Plan: Plan formulation and adjustment

- Reviews of 303 TS Promotion Committee Members and 247 Personal Information Controllers
- Review of trade secrets lists by 144 divisions, departments and affiliated companies in Japan
- Reports received from 29 ISCs outside Japan

Do: Awareness-raising activities

- Pledge submissions from 2,090 personal data controllers
- Conducted awareness-raising activities in 160 divisions, departments, and affiliated companies in Japan

Information Security

Check: Self-checks and auditing of outsourcing partners

- Self-checks on TS in 166 divisions, departments and affiliated companies in Japan
  - Self-checks on personal information in 124 divisions, departments and affiliated companies in Japan
- Audits of 179 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. No claims relating to personal information were directed to inquiry desks.

- 305 members participated in the plenary meeting held on November 15, 2022.
- The number of incidents related to trade secrets (TS) and personal information in 2022 was 78 by the end of October.

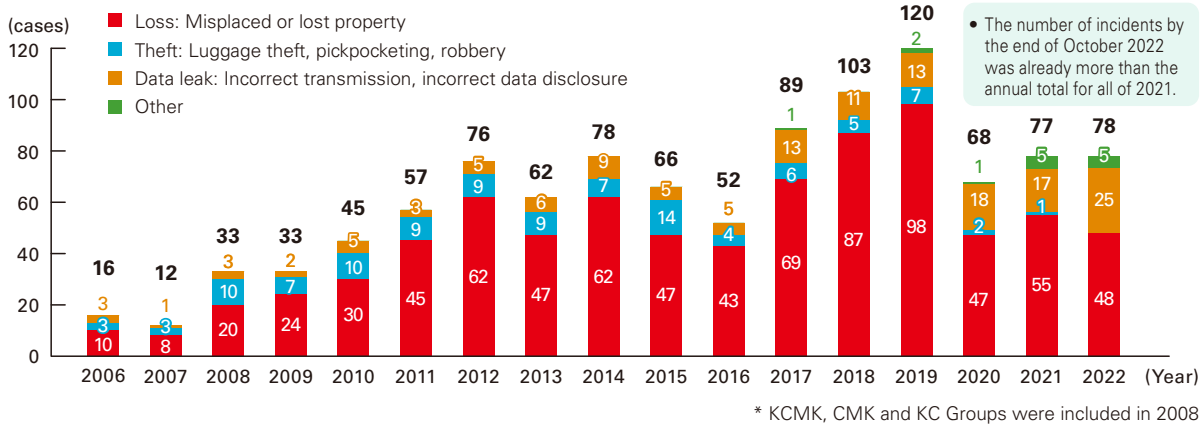
The results of trade secrets (TS) self-checks and improvement targets in 2022 are as follows:

- Review the division manual (trade secrets lists) periodically and clearly write the storage period.
- Carry out thorough management of trade secrets at home and always lock the PC screen when leaving your desk.

As a result of self-checks on personal information in 2022, we established improvement targets as follows:

- Periodically check whether personal information is included in the information handled in your division. If the division obtains and stores personal information, register the personal information in the personal information register system.

Change in the number of incidents in the Kao Group in Japan (at the end of October 2022)



* KCMK, CMK and KC Groups were included in 2008

Reviews of 2022 results

It is necessary to carry out activities to protect trade secrets (TS) and personal information on a continual basis every year. Since even those who fully understood trade secrets (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 trade secrets (TS) and personal information protection rules.

In addition, 29 Information Security Committees (ISCs) have been established overseas in overseas regions, corporate groups, and individual companies to promote the protection of trade secrets (TS) and personal information throughout the Kao Group. We check the contents of the activities of each ISC with activity reports which are sent once a year in March from ISCs outside Japan.

Information Security

Main initiatives

Formulation of activity targets for the Information Security Committees (ISC) in Japan

The following ISC activity targets for 2022 were set and measures were taken to achieve them.

(1) Main activities of the 29 Information Security Committees overseas

- KC Russia: 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

(2) Renewal of cyber insurance

(3) Responding to the enforcement of the revised Personal Information Protection Act in Japan

- A briefing about revised rules was held in January.
- Obtaining consent regarding website cookies began in Japan in April.

(4) Interviews with suppliers about security measures

- We interviewed 107 packaging suppliers and 86 raw material suppliers in June, grasping what risks they were facing and what measures we should take to mitigate those risks.

Reinforcement of cybersecurity measures

(5) Strengthening security measures in accordance with the security strategy roadmap to enhance the security strategy

- We enhanced email security, website security, account security and endpoint security.

(6) Consideration of the abolition of PPAP

- Because when a zip file with a password is attached to an email, it is not possible to check it for viruses, we discussed the provision of alternative means and the revision of internal rules so that Kao would not send and receive emails with zip files attached that require a password. We will start implementing the provisions in June 2023.

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)

- We pledged to manage electronic data through MS Forms for the use of the personal information dedicated server.

(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
- Explanations regarding the abolition of PPAP
- Report on incidents related to TS and personal information in Japan
- Summary of self-checks
- Setting of improvement targets