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

We are working to strengthen information security in order to protect information assets that include confidential information and personal information as well as IT hardware, software and many kinds of data records, in accordance with our Information Security Policy. We promote information security through the use of a PDCA cycle created to set internal rules and ensure that those rules are observed and that internal controls are implemented thoroughly.

Kao's creating value to address social issues

Social issues we are aware of

Every company uses IT to promote efficiency in its business and operations, and data to develop innovations and initiate reforms. Information technology has spawned new cross-industry growth areas and the engagement of diverse human resources. The rising use of IT has also recently increased the threat of cyberattacks, which can temporarily interrupt business activities and cause information leakage. Cyberattacks adversely affect business performance and have turned cybersecurity into a social issue.

Kao's creating value

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

Risks related to realization of our vision by 2030

A major risk is the occurrence of cyberattacks that can cause the 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 our vision by 2030

By strengthening cybersecurity measures and the management of data, trade secrets 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, trade secrets 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.

➜ Kao Group Company Privacy Policy
www.kao.com/jp/corporate/privacy/privacy-en/

➜ Kao Group Company Inquiries and Complaint Reception Desk Regarding Personal Information (Japanese)
www.kao.com/jp/corporate/privacy/privacy-contact

Education and promotion

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

Also, to evaluate the effectiveness of the 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.

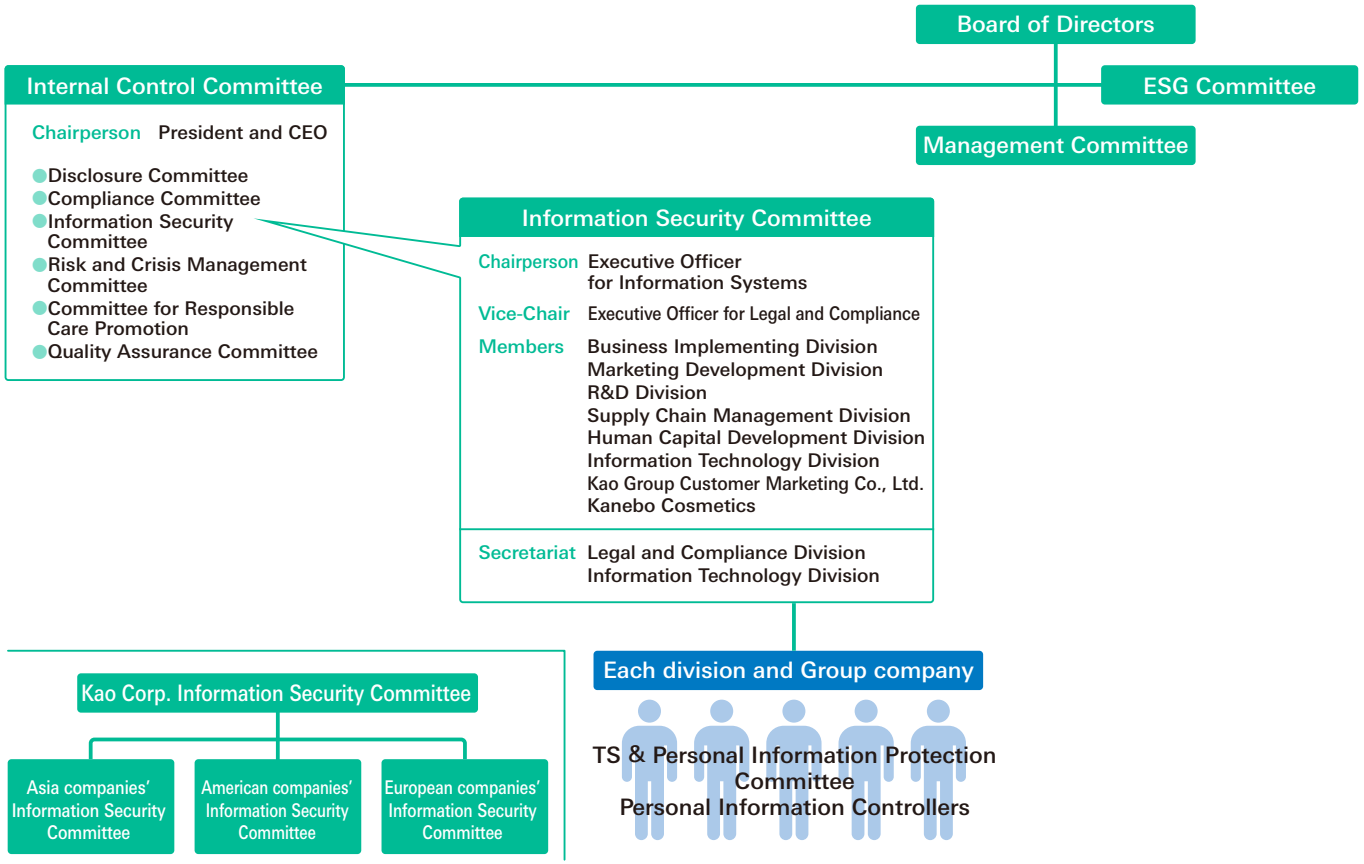
Information security 102-20, 103-2

Framework

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

The Information Security Committee reports on its activities to the Internal Control Committee on a quarterly basis, and the Internal Control Committee reports to the Board of Directors on the activities of all subordinate committees. The report contains the activity targets of the current fiscal year, progress status and performance evaluations, and in the fourth quarter, the activity targets for the coming fiscal year is also reported. Kao promoted development of a global system establishing information security committees in each country under the umbrella of the Information Security Committee.

Information Security Management System



* As of December 2019.

Information security 103-2, 103-3

Mid- to long-term targets and performance

Mid- to long-term targets

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

Anticipated benefits from achieving mid- to long-term targets

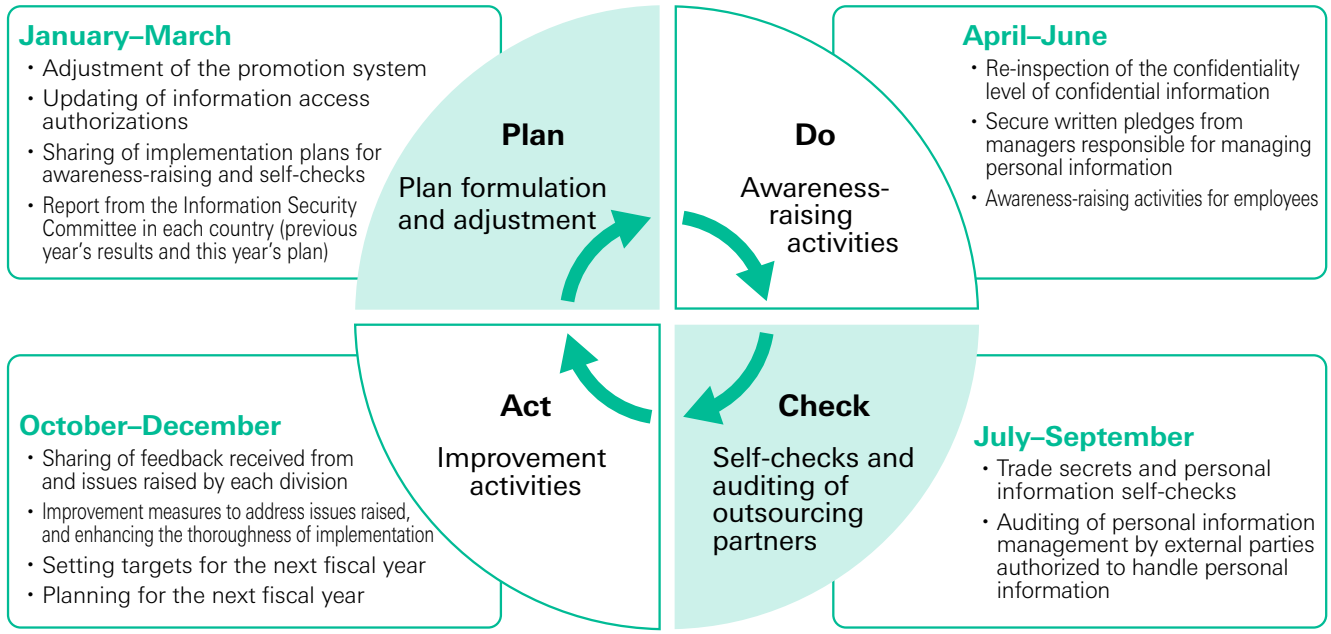
Business impacts

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

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 2019

Performance

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

First Quarter: Plan formulation and adjustment

- Adjustment of TS and personal information protection promotion system.
- Plan formulation and implementation.
- Revision of educational materials ("IT Security Guidelines [for Users]" compliance).

Second Quarter: Awareness-raising activities

- TS awareness-raising activities in 120 divisions, departments, and affiliated companies in Japan.
- Personal information awareness-raising activities in 93 divisions, departments and affiliated companies in Japan.
- Global promotion system approved by the Management Committee.
- Confirmation of status of compliance with China's Cybersecurity Law.
- Continued compliance of the Ministry of Economy, Trade and Industry (METI) "Cybersecurity Management Guidelines V2.0."

Third Quarter: Self-checks and auditing of outsourcing partners

- Self-checks on trade secrets in 130 divisions, departments and affiliated companies in Japan.
- Self-checks on personal information in 101 divisions, departments and affiliated companies in Japan.
- Paper audits of 195 subcontractors that handle personal information.

Fourth Quarter: Improvement activities

- The 26th TS & Personal Information Protection Promotion Meeting was held at the Plenary Meeting (relayed to remote locations via web teleconference) on November 14, 2019. In the Meeting employee awareness and behavior improvement were promoted based on recent incidents related to information security, reminders about the last year's improvement goals and a 2019 incident report on trade secrets and personal information were presented, feedback was given on self-checks, and improvement targets were set.
- Confirmation of compliance with the California Consumer Protection Act.
- Confirmation of GDPR operational status.

At the Japan Kao Group, there were no serious incidents related to information security, including trade secret and personal information protection. Furthermore, with regards to personal information protection, to date the company has never been fined nor given any advisories or recommendations based on applicable laws.

In 2019, concerning issues sent to the Inquiries and Complaint Reception Desk Regarding Personal Information, there were three cases related to changing member registration information.

Reviews of performance

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

Information security 103-2

Our initiatives

First Quarter: Plan formulation and adjustment

Adjustment of TS and personal information protection promotion system

In line with the changes in roles due to organizational restructuring and personnel changes, adjustments were made for 56 members of the TS & Personal Information Protection Committee, 50 supervisors who handle personal information, and 2 Information Security Committee members, and 1 secretariat member. To ensure that trade secret and personal information protection promotion activities are not interrupted even if organizational changes or personnel changes are made, the adjustments assure that a handover to the next people in charge will take place.

Second Quarter: Awareness-raising activities

Redevelopment of internal policies

In order to strengthen our response to cyberattacks, in June 2019 the company's internal rules, the IT Security Guidelines, were revised to IT Security Guidelines (for Administrators) and IT Security Guidelines (for Users) was newly established. Regarding IT Security Guidelines (for Administrators), revisions were made from the position of IT system management for administrators, and limited the position related to user's usage to its policies. On the other hand, the user operational level and the Guide for Using Information Equipment are integrated into IT Security Guidelines (for Users), and we are working to raise user awareness of cyberattacks by revising our awareness materials.

List of guidelines and an example

Information security 103-2

Alerts about business e-mail compromise and targeted e-mail attacks

Since March 2019, there have been multiple confirmations of business e-mail compromise and targeted e-mail attacks against Kao. As part of our technical measures to prevent damages, the company has enhanced filtering of incoming mail and implemented a safe web browsing tool. Moreover, concerning business e-mail compromise and targeted e-mail attacks, since most were sent in the name of Kao's actual people, the company has taken measures to prevent spoofing from malicious outsiders by adding [External] at the beginning of e-mail subjects on e-mails sent from outside of Kao.

On the other hand, as part of personal measures, regarding business e-mail compromise, Kao also alerts domestic and overseas employees on the Japanese and English intranet bulletin board. Furthermore, with regards to targeted attack e-mails, we also warn employees who may be potentially attacked.

E-mail alerts

E-mail alerts are sent to each company president, as well as alerts to our English portal site.

METI "Cybersecurity Management Guidelines V2.0" compliance

The Japanese government's Cybersecurity Management Guidelines V2.0, revised in November 2017, define three principles that executives need to recognize and ten important items concerning which they should instruct the chief information security officer (CISO). The latter refers to the National Institute of Standards and Technology (NIST) security framework. Kao uses NIST's security framework to ascertain the group's current status and identify issues as well as to continue to make improvements as to the remaining issues that could not be addressed in 2018.

Third Quarter: Self-checks and auditing of outsourcing partners

Self-checks of TS and personal information protection

Trade secret self-checks are conducted every year as part of the thorough implementation of awareness-raising activities and efforts to develop division manuals, implement TS labeling, and manage confidential information. In 2019, the self-checks took place from July 22 to August 23.

Personal information self-checks were similarly conducted at the same time to raise awareness, and also to manage the retention of personal information and determine which outsourced tasks involve the handling of personal information. Feedback on the self-checks was given at the TS & Personal Information Protection Promotion Meeting held on November 14, 2019, and improvement targets were set.

The improvement target for trade secrets was set in this way: "Confidential information on paper should not be taken out of the office," use of the company's cloud system on a company computer requiring access with a login ID and password, or a company smartphone locked with a PIN code, is promoted so that the theft or loss of the computer or smartphone will not lead immediately to an information leak.

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

Information security 103-2, 404-2

Kao TS自主パトロール INTERNAL USE ONLY Information security Committee

設問	選択肢	%	N
Q7.	TS表示の実施		
1).	TS表示を実施していますか？（マル秘の場合、責任部署と期限を含む）（社内用の場合、責任部署を含む）	129	
	①実施している	98%	126
	②実施していない	1%	1
	③部署として機密情報を作成する機会が無い	2%	2
Q8.	TS表示について		
1).	部門マニュアル（機密情報リスト）の機密情報のグレードと整合性が取れていますか？	128	
	①整合性が取れている（機密情報リストを参考にしている）	95%	122
	②整合性が取れていない（機密情報リストを参考にしていない）	5%	6
2).	海外に機密情報を送るときに英語でTS表示を行っていますか？（マル秘の場合、責任部署と期限を含む）（社内用の場合、責任部署を含む）	128	
	①英語でTS表示を行っている	63%	81
	②英語でTS表示を行っていない	0%	0
	③海外に機密情報を送っていない	37%	47
3).	取引先から受取った機密情報へのTS表示は適切に表示されていますか？	128	
	①TS表示を行っている	59%	76
	②TS表示を行っていない	3%	4
	③取引先から機密情報を受取っていない	38%	48

設問	選択肢	%	N
Q9.	機密情報の開示		
1).	自部門で作成したマル秘情報を開示する場合、開示範囲について機密情報管理責任者（部門長）の承認を得ていますか？	129	
	①承認を得ている	70%	90
	②承認を得ていない	4%	5
	③該当する開示無し	26%	34
2).	他部門で作成したマル秘情報を受取り、さらに他の部門に開示する場合、マル秘情報の責任部門の承認を得ていますか？	129	
	①承認を得ている	60%	77
	②承認を得ていない	4%	5
	③該当する開示無し	36%	47
3).	社外にマル秘情報を開示する場合、秘密保持契約等の契約や覚書を締結していますか？	129	
	①締結している	70%	90
	②締結していない	1%	1
	③社外にマル秘情報を開示していない	29%	38
4).	社外に情報開示される場合は、開示先を明示していますか？	129	
	①明示をしている	64%	83
	②明示をしていない	5%	6
	③社外に情報を開示していない	32%	40

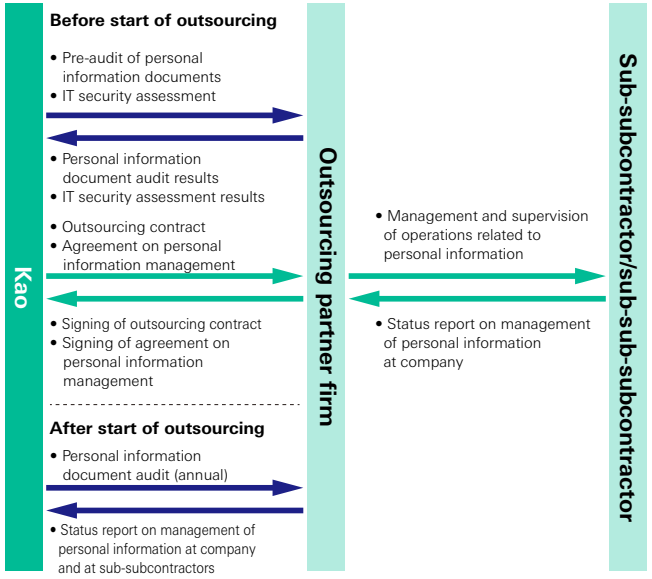
Trade secret self-assessment checklist

Auditing of external parties authorized to handle personal information

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

In addition, we manage and oversee outsourced personal information by conducting annual audits of subcontractors that handle personal information. In 2019, we conducted such audits at 195 companies and confirmed the status of personal information management and the systems used by subcontractors for protecting personal information. If personal information is stored by a subcontractor, we confirm the number of records and check for consistency with the number of data records registered in their personal information handling ledger system.

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



●Personal information ledger management
●Management of subcontractor

Fourth Quarter: Improvement activities

Holding of the 26th TS & Personal Information Protection Promotion Meeting

The 26th TS & Personal Information Protection Promotion Meeting was held on November 14, 2019. The theme of our in-house lecturer seminar was: “Cyber Security Seminar: Everyone is a key-person of preventing targeted e-mail attacks!,” where in addition to introducing how targeted attack e-mails are the one cause of confidential information leaks, along with business e-mail compromise and ransomware, we also introduced common tricks used by malicious individuals targeting individual employees and worked to ensure that appropriate actions are to be taken in response. After the seminar, a report was given on incidents related to TS and personal information in 2019. Feedback was then provided on TS and personal information self-checks, and improvement targets were set.

TS and Personal Information Protection Promotion Meeting
110 participants at head office venue; 169 participants via relay at other business sites.

Information security 103-2, 102-43

Confirmation of GDPR operational status after implementation

The European Union's General Data Protection Regulation (GDPR) came into force on May 25, 2018. The GDPR regulates the handling and transfer of personal data and is characterized by strict rules and penalties. Confirmation with the European Kao Group of operational status was done after the enforcement of GDPR.

Protection measures when handing personal information, such as organization and rule maintenance in addition to conclusion of necessary contracts, correspond with rules in relation to the required content. In addition, it has been properly implemented for responding to personal information requests by individuals as well as for reporting accidents to supervisory authorities both of which are newly defined in GDPR.

As far as challenges go, we recognize the regular periodic checks of the hundreds of records created for personal information processing (Record of Processing Activity) and are making improvements to this implementation process at our EU companies, in addition to considering the introduction of management tools for this purpose.

Expanding Information Security Committee for overseas companies

To respond to cyber attacks and strengthen information asset protection at overseas group companies, we expand the Information Security Committee overseas. In doing so, it has allowed us to expand information security activities, including promoting the protection of trade secrets and personal information, to the employee level at our overseas companies, and a reporting line to Kao Corporation for important information security incidents was established.

Required internal rule revisions at Kao were approved in May 2019, and overseas Kao Group companies are in the process of establishing internal rules and systems with the goal of beginning activity from 2020.

Official website security confirmation

If websites published on the internet do not have proper security measures in place, these websites can be hijacked by malicious individuals, and can be abused as a starting point for cyber attacks.

Regarding newly created websites, group companies in Japan confirm that there are no vulnerabilities and other security issues. In addition, to prevent damage to websites already published on the internet by our domestic group companies, we monitor the current situation, confirm each security status, and if any issues are found, take necessary action.

Collaboration with stakeholders

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

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

In preparation for cyberattacks that are expected to surge, Kao participated in the Industrial Cyber Security Measures Briefing Session held by the Ministry of Economy, Trade, and Industry. We will continue to work on these measures in accordance with Japanese government policy.