

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2025

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Japan: Trends and Developments

Yasushi Kudo, Yukiko Konno
and Takayuki Inukai
Nagashima Ohno & Tsunematsu



Trends and Developments

Contributed by:

Yasushi Kudo, Yukiko Konno and Takayuki Inukai
Nagashima Ohno & Tsunematsu

Nagashima Ohno & Tsunematsu is one of the foremost providers of international and commercial legal services, based in Tokyo. The firm has approximately 600 lawyers, including nearly 50 experienced foreign lawyers from various jurisdictions. Its overseas network includes offices in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi and Shanghai, Jakarta and collaborative relationships with prominent local law firms throughout Asia, Europe, North and South America, and other regions. The firm provides comprehensive assistance in the devel-

opment of cybersecurity systems, including the establishment of internal governance systems and vendor management. It also has extensive experience in crisis management in the event of a security incident. In collaboration with IT system experts, the firm also provides one-stop support for the entire process, from the initial response, including fact-finding and evidence preservation, to dealing with the authorities, information disclosure and the mass media, liaising with victims, root cause analysis and recurrence prevention measures.

Authors



Yasushi Kudo is a partner at Nagashima Ohno & Tsunematsu. He mainly focuses his practice on crisis management, including dealings with domestic and international authorities,

regulatory compliance, cybersecurity/data privacy, and advice on compliance systems and corporate governance, leveraging his expertise and experience gained from secondment to the Financial Services Agency and the Securities and Exchange Surveillance Commission. Recently, his focus has been on legal issues raised by cybersecurity incidents such as ransomware attacks, data compromise and business e-mail compromise, as well as the development of internal control systems so as to mitigate cybersecurity risks such as supply chain risk.



Yukiko Konno is a counsel at Nagashima Ohno & Tsunematsu. Her practice primarily focuses on domestic and global data governance and other emerging areas, including cybersecurity,

data privacy/data protection, AI and IoT issues, as well as cross-border general corporate matters across a range of industry sectors. She is a graduate of Keio University (2005), Chuo Law School (JD, 2008) and Columbia Law School (LLM, 2015). She was seconded to a private trading company (2015–17) and the Trade Policy Bureau of Ministry of Economy, Trade and Industry of Japan (METI) (2019-22).

JAPAN TRENDS AND DEVELOPMENTS

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu



Takayuki Inukai is an associate at Nagashima Ohno & Tsunematsu. His practice primarily focuses on technology, media and telecommunications (TMT) including data privacy, cybersecurity, telecommunications regulation and intellectual property. He provides advice in various situations, utilising his technical expertise. He is a graduate of the Department of Computer Science and Engineering, Waseda University in 2018 (Bachelor of Engineering). He was seconded to the Telecommunications Bureau and Information and Communications Bureau of the Ministry of Internal Affairs and Communications (MIC) (2022-24).

Nagashima Ohno & Tsunematsu

JP Tower, 2-7-2 Marunouchi
Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 368 897 396
Fax: +81 368 898 396
Email: yasushi_kudo@noandt.com
Web: www.noandt.com/en/lawyers/yasushi_kudo/



Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

Introduction

In 2024, as in previous years, numerous incidents involving the leakage of personal data occurred in Japan due to cyber-attacks such as ransomware and internal misconduct by outsourced contractors. In response, the Personal Information Protection Commission (PPC), the Japanese data protection authority, has decided to publish quarterly summaries of its supervision activities, detailing the content of its administrative guidance and advice. In this context, the PPC has focused on issues related to the “handling of large volumes of personal information”, identifying problems with security measures and the need for necessary and appropriate oversight of data processors. Taking into consideration past judicial precedents in Japan regarding data breaches, these insights provide valuable references in order for businesses managing significant volumes of personal information to assess the required security standards. This article highlights these developments and introduces trends in legal reforms surrounding cybersecurity in Japan.

Recent Enforcement and Administrative Guidance by the PPC

Since August 2024, the PPC has published quarterly reports summarising its “Overview of the Exercise of Monitoring and Supervisory Authority” and the “Handling Status of Breach Notifications” (as of the end of December 2024, the latest being the second quarter of FY2024). While the PPC has previously disclosed cases of administrative guidance or advice based on the severity of incidents, these announcements were limited in scope. The quarterly reports thus serve as valuable reference materials for businesses to understand the PPC’s enforcement policies on data breach incidents.

Handling status of breach notifications

In the second quarter of FY2024, there were 3,599 reports of breaches from businesses handling personal information. Of these, 1,087 cases (30.2%) stemmed from unauthorised access, including breaches caused by external cyber-attacks.

Overview of the exercise of monitoring and supervisory authority

During the second quarter of FY2024, it was reported that there were 87 cases in which the PPC gave administrative guidance and/or gave advice to private businesses. Of these, 70 cases related to security measures (Article 23 of the Japanese Act on Protection of Personal Information (APPI)) and supervision of contractors (Article 25 of the APPI), and 33 cases concerned delays in breach notification submissions. (Note: a single case may fall under multiple categories.)

Among the said 87 cases, 48 involved breaches due to unauthorised access. Excluding formal violations such as delayed reporting, administrative guidance on unauthorised access breaches was most frequent course of action. The PPC gave the following reasons to explain this trend.

- Unlike cases such as the leakage of sensitive personal information, which require reporting even for a single incident, unauthorised access incidents often involve a large number of individuals (most unauthorised access cases involved breaches affecting over 1,000 individuals).
- These incidents were often linked to businesses failing to implement the necessary security measures that should have been in place as a matter of course.

JAPAN TRENDS AND DEVELOPMENTS

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

Causes of unauthorised access and content of administrative guidance

For unauthorised access incidents in the second quarter of FY2024, the causes and the types of attack were analysed as follows.

- By cause:
 - (a) software vulnerabilities: 27 cases (including VPN: six, e-commerce sites: five);
 - (b) weak ID/password protection: 22 cases; and
 - (c) misconfigured access controls: 16 cases.
- By type of attack:
 - (a) brute-force attacks: 12 cases;
 - (b) cross-site scripting: six cases;
 - (c) SQL injection: four cases; and
 - (d) ransomware: 21 cases.

Most of the identified inadequacies in security measures for FY2024 concerned technical safeguards. In the second quarter, the most common administrative guidance related to the requirement of “preventing unauthorised external access” (42 cases), followed by “identification and authentication of users” (eight cases).

Primary causes of breaches included:

- known vulnerabilities in VPN devices or applications used to build e-commerce sites left unaddressed by businesses;
- easily guessable IDs and passwords; and
- misconfigured system settings allowing improper database access control.

Such inadequacies in security measures often led to the PPC’s enforcement actions.

Implications for businesses

The PPC’s reports provide detailed case studies, including the specifics of incidents and deficiencies addressed in their administrative

guidance, offering valuable insights for practical countermeasures. Businesses in Japan, especially those handling substantial volumes of personal information, should regularly review these reports. They should also continuously update their technical security measures and implement robust oversight frameworks for contractors.

Practical Measures to be Taken by Companies in the Event of a Data Breach Procedures for reporting leakages and the like

In Japan, upon the occurrence of a leakage, or the like, in respect of personal data it is in principle necessary to report the incident to the authorities. In this regard: (i) for personal data, under the APPI the occurrence must be reported to the PPC (however, in relation to certain industries, the leakage, or the like, must be reported to the competent ministries such as the Ministry of Internal Affairs and Communications (MIC)); and (ii) for information to which the secrecy of telecommunications applies and/or which is specified user information, under the Telecommunications Business Act (TBA) the occurrence must be reported to the MIC. In addition: (iii) in the case of listed companies, timely disclosure under the relevant rules established by each security exchange in Japan and/or disclosure through extraordinary reports under the Financial Instruments and Exchange Act may be required in the event of a major incident. In such cases, careful consideration should be given to the scope of information to be disclosed, in order that the perpetrators of the incident or other persons do not use the information to cause further damage.

As regards (i) and (ii) above, these entail different scopes, procedures and institutional purposes. In the event of a leakage, or the like, it is important to be aware of the difference between (i) and

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

(ii), and to handle both at the same time and in a timely manner.

- (i) The situations that require reporting under the APPI (Article 26, paragraph 1 of the APPI) are when personal data has been leaked, etc (ie, leakage, loss, damage or other circumstances pertaining to the security of personal data) and there is a significant risk of harm to the rights and interests of individuals. Under the APPI, there are two types of reports: a preliminary report (promptly after learning of the situation); and a definitive report (within 30 days (60 days in certain cases) from the date of learning of the situation).
- (ii) The situations that require reporting under the TBA (Article 28 of the TBA) are: (a) when there is a leakage in respect of secrecy of telecommunications (eg, content of chats); (b) when there is a leakage of specified user information (eg, telecommunications account information) – in which case, only designated businesses are required to report; and (c) when a “threat” of such a situation arises. There are two types of reports under the TBA: a first report (promptly after becoming aware of the situation); and a detailed report (within 30 days).

In addition, as is common for both procedures, it is necessary to comply with the deadlines for submitting each of the above reports, and therefore it would be advisable to establish a response process in advance – ie, in normal times prior to any such incident. In addition, when submitting a report, it is necessary to (i) describe the status of implementation in respect of security control measures and supervision of contractors, and (ii) investigate the technical causes of the leak. With the increase in the number of cases of leakage, there is an inevitable increase in the number of cases necessitating the use of the reporting

procedures, and thus the day when a report is required may come at any time. Therefore, it is important, regarding (i), to establish and conduct the appropriate security control measures and supervisory procedures in advance, and, regarding (ii), to establish relationships with security vendors who have the necessary capabilities to conduct required investigations so that they can be immediately engaged when needed.

Risks in respect of disclosure of administrative guidance and recommendations

In addition, there has been an increase in the number of cases of public disclosure of administrative guidance, order and the like, and therefore de facto risks such as reputational risks, that are not purely legal in nature in recent years.

- In 2023, NTT West discovered that an employee of a re-outsourcer had accessed the server where customer data was stored and had illegally appropriated customer data for about ten years. In response, in 2024, the PPC issued recommendations and administrative guidance to the outsourcer and the re-outsourcer, directing them to improve the inadequate organisational security control measures. In addition, the MIC issued administrative guidance to NTT West, directing it to review its supervision of its outsourced companies and strengthen its measures. The content of said guidance, including the name of the company, has been made public.
- In 2023, an incident occurred involving NTT DOCOMO and NTT NEXIA, whereby temporary employees of NTT NEXIA, NTT DOCOMO's outsourcer for customer information management, appropriated personal data of a total of approximately 5.96 million people. In response, in 2024, the PPC issued administrative guidance to NTT DOCOMO and NTT

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

NEXIA, directing them to implement measures to prevent a recurrence and to report on the implementation status. The content of this guidance, including the names of the companies, was made public.

In both cases, the incidents occurred at the outsourcee, and the authorities identified issues related to the maintenance of organisational security control measures. It is becoming increasingly difficult for large companies that outsource parts of their business handling personal information to third parties to manage the personal information on their own, and thus it is important to ensure that security control measures are implemented, including at outsourcees.

As mentioned above, in recent years there have been an increasing number of cases of administrative guidance and public announcements in response to leaks. Businesses that handle large volumes of personal data are likely to be more vulnerable to attacks and to risks of leakage and therefore must employ caution because of the increased risk of administrative guidance, administrative order and public disclosure.

Civil risks

In 2014, a very well-known Japanese company (the “Company”) in educational and publishing industry suffered a massive leak (the “Case”), in which an insider (a former employee of the outsourcee) appropriated the personal information of tens of millions of people and sold the information to a directory company. Over the past few years, a series of court judgments have been issued to determine civil liability in the Case.

Corporate responsibility

In the Case, numerous victims filed lawsuits for damages. The court stated that “regarding information security, necessary measures must

be taken in consideration of each company’s business, environment, risks, and suchlike” and noted that “a large amount of personal information from customers forms the subject of business activities, and in light of the general public perception of information management, close attention is to be paid to information security measures.” As a result, the court concluded that “the Company is in a position to pay close attention to information security measures, in light of the fact that it handles a large amount of personal information from its customers in its business activities and in light of the general public perception of information management”, and partially granted the plaintiffs’ (victims’) damages claims against the Company (Tokyo High Court, 17 March 2021, (Ne) No 102).

From this, it can be concluded that businesses handling large volumes of personal data have a heightened duty of care in terms of the security measures required to prevent information leaks of personal data. Therefore, such businesses are susceptible to the risk that a finding of either default (contract liability) based on a breach of the obligation to implement security controls or negligence based on foreseeability (tort liability) may be easily made. In particular, since foreseeability is more likely to be established in relation to known security risks, it is of paramount importance for companies to constantly collect the latest information and take technical countermeasures.

Liability of company officers

If the company were to post an extraordinary loss due to payment of a large amount of compensation for damages or loss in respect of operating profit, the officers could be accused by shareholders and others of violating their duty of care (Article 330 of the Companies Act and Article 644 of the Civil Code) due to the inad-

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

equacy of their establishment and operation of a cybersecurity system.

In the Case, a shareholder derivative suit was filed against the officers (more precisely, the officers of the Company group's holding company) to hold them liable. In its judgment, the court held that it was necessary to establish an internal control system based on the nature and scale of the business, management conditions, and other related circumstances (Hiroshima High Court, Okayama Branch, 18 October 2019 (2018 (Ne) No 201)). Therefore, in the case of a large corporation, it is necessary to establish an appropriate internal control system from the perspective of cybersecurity, taking into account the trends in practice. In the Case, the responsibility of the officers of the holding company was in question, not the Company itself, since it was the holding company that had established the relevant internal control system. In conclusion, the court dismissed the claim against the officers of the holding company.

Additionally, in a case where the issue was whether or not there were deficiencies in the risk management system of a listed company due to the false statements made in the securities report required under the Financial Instruments and Exchange Act, as a result of fictitious sales being recorded by employees, the Japanese Supreme Court made its judgment based on (i) whether the company had a management system sufficient to prevent the type of misconduct that could normally be expected, and (ii) whether there were special circumstances that should have led the company to anticipate the misconduct that occurred (Supreme Court, 9 July 2009 (2008 (Ju) No 1602)).

If the responsibility of company officers for the inadequacy of risk management systems for

cyber-attacks is contested in court, this Supreme Court judgment may be cited as a precedent. In such cases, security incidents and tactics employed by attackers, as introduced in public alerts by relevant authorities like the PPC, such as the PPC's quarterly report and in publicised cases by other companies, would be taken into account. As a result, it should be noted that the court may assess whether a degree of control was exercised that could have prevented security incidents that occurred, assuming that the incidents were caused by normal, expected cyber-attacks.

Necessity of ensuring adequate security levels

As discussed above, the legal risks associated with cybersecurity are increasing, and so is the need to ensure an adequate level of cybersecurity. For example, the following are beneficial in ensuring adequate standards.

- Considering, from the viewpoint of system maintenance, the necessary cybersecurity measures from the perspective of maintenance of internal controls, with reference to the technical management described in the "Guidelines for Internal Fraud Prevention in Organizations" of the Information-technology Promotion Agency, Japan (IPA) and the evaluation items set forth in "Evaluation of the effectiveness of maintenance and operation status of internal controls using IT" listed in the "Standards for evaluation and audit of internal controls over financial reports" of the Financial Services Agency.
- Conducting cyber due diligence, including penetration tests (actual simulated attacks) and systemic checks, with a view to reducing risks before they occur.
- Participating in the Cyber Security Council (a council legally established under Article 17 of

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

the Cyber Security Basic Act, in which both the public and private sector participate) to obtain non-public information on the latest attack trends, and such like, from the viewpoint of information gathering.

Trends in Legal Reforms and in Other Areas *Discussion on the review of the APPI*

When the APPI was amended in 2020, it was decided that the regulatory regime would thenceforth be reviewed every three years. Based on this, the PPC is currently reviewing the regime, including the introduction of a surcharge system and revision of the system for demanding injunctions; and on 25 December 2024, the report of the Expert Panel was published (albeit in the form of both sides of the argument).

The report examines, with respect to both (i) violations of various conduct regulations and (ii) violations of regulations pertaining to leaks, and the like, as well as security control measures, narrowing down the cases to which the surcharge system applies.

Specifically, with respect to the situation in which the surcharge system is to be applied, the report proposes the following.

With respect to (i) above:

- limiting the subject acts (situations) to violations of the following four types: restrictions on provision to third parties (Article 27, Paragraph 1); prohibition of inappropriate use (Article 19); restrictions based on the purpose of use (Article 18); and appropriate acquisition (Article 20);
- limiting the subject cases to those where the violator can be said to have failed to have been negligent in respect of taking reasonable care to prevent the violation;

- limiting the subject cases to those where individual rights and interests have been infringed or there is a concrete threat of infringement; and
- limiting the subject cases to those where a large-scale breach has occurred (specifically, where the number of data subjects involved in the breach is 1,000 or more), etc.

With respect to (ii), above:

- limiting the subject acts to cases where a large-scale leakage, or the like of personal data and the like occurs as a result of a breach of the obligation to take security control measures (specifically, cases where the number of data subjects involved in the breach is 1,000 or more);
- limiting the subject cases to those where the violator can be said to have been extremely negligent in respect of taking reasonable care to prevent violations of the obligation to take security control measures; and
- limiting the subject cases to those where individual rights and interests have been infringed or there is a concrete threat of infringement.

With respect to the method of calculation of the surcharge, the report proposes the following.

With respect to (i) above:

- the surcharge be the full amount of financial gain (or an amount exceeding the full amount of such financial gain) obtained by the violating business operator from the violation or from the use of personal information acquired through the violation.

With respect to (ii), above:

JAPAN TRENDS AND DEVELOPMENTS

Contributed by: Yasushi Kudo, Yukiko Konno and Takayuki Inukai,
Nagashima Ohno & Tsunematsu

- the surcharge be such amount as is obtained by multiplying (x) the amount of sales generated by the business activities of the business operator in violation of the obligation to take security control measures during the period of the relevant violation by (y) a certain “calculation rate” – this proposal is based on the viewpoint of speediness and efficiency of administrative penalties, and it is believed that the proposal considers the ease of calculation.

In addition, there are proposals to establish a provision for reducing penalties for violators who voluntarily report violations, and an additional provision to impose a surcharge of 1.5 times the normal surcharge on repeat violators.

From the viewpoint of civil law, with regard to the system for demanding an injunction, there is a proposal to grant qualified consumer organisations the right to demand an injunction under the APPI as their own right, targeting violations that are highly likely to infringe on the rights and interests of individuals.

Although the report of the expert panel is still in the process of being put forward for consideration, if these systems are introduced, both the administrative law and civil law risks from an enforcement perspective may increase in Japan in the future.

Trends in legal reforms in the national security sector

In 2024, the Act on the Protection and Use of Critical Economic Security Information came into effect. This Law stipulates:

- the designation of critical economic security information;

- the provision of critical economic security information; and
- restrictions on who can handle critical economic security information (so-called “security clearance”), among other matters.

It is important for businesses that handle critical infrastructure, such as information and communications, to comply with this Law.

In addition, recently the government has been preparing Active Cyber Defense legislation, and the bill was submitted to the Diet in February 2025. This bill aims to enhance Japan’s cybersecurity response capabilities to a level equal to or higher than that of major Western countries. Among other things, it stipulates provisions for:

- strengthening public-private sector co-operation, such as imposing reporting requirements on critical infrastructure operators when they notice certain types of cyber-attacks;
- the government’s use of communication information to understand the actual situation of cyber-attacks on Japan; and
- allowing the National Police Agency and the Self-Defense Forces to intrude into and neutralise servers possessed by attackers to prevent serious harm from cyber-attacks under certain conditions.

It will be necessary to keep a close eye on the deliberations on the bill in the Diet.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com