Japan: Cybersecurity

Yoshifumi Onodera, Hiroyuki Tanaka, Daisuke Tsuta and Naoto Shimamura

Mori Hamada & Matsumoto

Key cybersecurity statutes, regulations and adopted international standards

The Basic Act on Cybersecurity

The Basic Act on Cybersecurity (the BAC) comprehensively and effectively promotes cybersecurity measures, defines the basic principles, and establishes the cybersecurity strategy headquarters (CSHQ). Article 2 of the BAC defines cybersecurity as the measures that are necessary for the safe management of information, such as:

- the prevention of leakage, loss of, or damage to information that is stored, sent, transmitted or received by electronic or magnetic means;
- guaranteeing the safety and reliability of information systems and information and telecommunications networks; and
- ensuring that those states are appropriately maintained.

This includes not only countermeasures against cyberattack but also countermeasures against internal fraud and system failures. No specific obligations with respect to cybersecurity are imposed on private companies under the BAC. Rather, a number of disparate laws prescribe the statutory and regulatory requirements applicable to cybersecurity as defined in the BAC. We outline key statutes and regulations in the section below (note that this is not an exhaustive list of all statutory and regulatory requirements).

The Act on the Protection of Personal Information

The Act on the Protection of Personal Information (the APPI) mainly aims at protecting personal information. A business operator that processes personal data must take necessary and appropriate actions to ensure the security of that data, including preventing the leakage, loss of or damage to any personal data (article 23).

Anyone who uses or discloses personal information contained in a database that they use in relation to their business for the purpose of seeking their own or a third party's illegal profits is subject to imprisonment for up to one year or a fine of up to ¥500,000; a corporate body whose employee commits the crime in the course of performing his or her duties as an employee is also subject to a fine of up to ¥100 million.

The bills to amend the APPI were approved in 2020 and 2021, respectively. The 2020 amendment took effect from 1 April 2022. The effective date of the 2021 amendment is two-staged – the first stage was 1 April 2022 and the second will be 1 April 2023. The 2021 amendment is called the Basic Bill on the Formation of a Digital Society, and mainly aims at unifying data protection laws that are currently diversified across the private and public sectors and therefore, the 2021 Amendment has little impact on practice in the private sector.

Right of privacy

The APPI is an administrative regulation, so it does not provide for a data subject's statutory right to receive compensation for a breach of the APPI. However, the right of privacy has been acknowledged under case law and a data subject may bring a tort claim based on the violation of his or her right of privacy. If a tort claim is granted, in addition to actual damages, compensation may be awarded for emotional distress to the extent deemed reasonable. Under Japanese law, no punitive damages are awarded.

The Telecommunication Business Act

Under the Telecommunication Business Act (the TBA), the secrecy of communications handled by a telecommunications carrier may not be violated (article 4). There is a prohibition against obtaining, using and providing information that is protected under this principle unless the communicating parties give consent or the action meets certain requirements to establish the absence of illegality. The secrecy of communications includes:

- the contents of individual communications; and
- all of the following information in connection with individual communications, the knowledge of which enables inference of the contents:
- the date and time of communication;
- the location of communication;
- the name, address and location of the communicating parties;
- codes for identifying the parties, such as telephone numbers; and

- the frequency of communication (Tokyo District Court judgment on 30 April 2002).

The Unfair Competition Prevention Act

The Unfair Competition Prevention Act (the UCPA) protects 'trade secrets' (defined below) and 'data for limited provision' (article 2). A trade secret is a production method, sales method, or any other technical or operational information useful for business activities that is controlled as a secret and is not publicly known. Data for limited provision means technical or business data that is handled as data to be provided to specific persons and is accumulated in substantial quantities by electronic, magnetic or other methods that cannot be recognised by human perception. The UCPA stipulates civil measures, including compensation and injunctive relief for:

- the acquisition of trade secrets or data for limited provision by theft, fraud, duress, or other wrongful means;
- using or disclosing trade secrets or data for limited provision acquired by such wrongful means; and
- other unfair competition regarding trade secrets or data for limited provision.

The UCPA also imposes criminal sanctions on unfair competition regarding Trade Secrets.

Other criminal law

There are criminal sanctions for those who create, provide, acquire or store 'improper command records', namely electronic records that send improper commands to computers, such as computer viruses or malware. These are imposed under articles 168-2 and 168-3 of the Penal Code. The penalties for creating or providing improper command records are imprisonment of up to three years or a fine of up to ¥500,000 (article 168-2); the penalties for acquiring or storing improper command records are imprisonment of up to two years or a fine of up to ¥300,000 (article 168-3).

The Act on the Prohibition on Unauthorised Computer Access (the APUCA) imposes criminal sanctions on anyone who remotely accesses a computer without authorisation. The penalties are imprisonment for up to three years or a fine of up to ¥1 million (article 3 and article 11).

International standards

There is no comprehensive obligation to comply with international standards. However, some companies are certified under Information Security Management System (ISMS) certified under ISO/IEC 27001:2013. It is also becoming more common for companies to refer to the SP800 series guidelines, published by the National Institute of Standards and Technology (NIST).

Under the Instalment Sales Act, business operators handling credit card numbers must take measures to protect those numbers; some operators have therefore adopted the Payment Card Industry Data Security Standard (PCI-DSS).

Regulatory bodies responsible for enforcing cybersecurity rules

The CSHQ and the NISC

The Cybersecurity Strategy Headquarters (CSHQ) established under article 25 of the BAC and its secretariat, the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC), are responsible for the promotion of cybersecurity policy. However, while the NISC has the authority to oversee government agencies, the authority is not exercisable against private companies.

The Personal Information Protection Commission

By contrast, the Personal Information Protection Commission (PPC), in principle, has enforcement powers, by issuing guidance and advice, mandatory reporting obligations, recommendations and orders.

The PPC may issue the following administrative sanctions when a business operator fails to comply with its obligations under the APPI, including article 23, which stipulates the necessary and appropriate actions to ensure the security of that personal data:

- the PPC may render issue guidance or advice to the business operator (article 144);
- the PPC may recommend that the business operator cease the violation and take other necessary measures to correct it (article 145.1); or
- the PPC may order the business operator to take certain necessary measures (articles 145.2 and 145.3).

The Ministry of Internal Affairs and Communications

The Ministry of Internal Affairs and Communications (MIC) has administrative jurisdiction over information and communication-related laws, including the TBA. The MIC promotes cybersecurity measures mainly focused on cloud services and the security of information and communication networks, including 5G and IoT devices.

When a telecommunications carrier breaches the secrecy of communications with respect to its telecommunications activities, it must without delay report the incident to the MIC, including the reasons or causes of the breach, and must submit a detailed report to the MIC within 30 days of becoming aware of such violation the breach (article 28 of the TBA).

The Ministry of Economy, Trade and Industry

The Ministry of Economy, Trade and Industry (METI) is an administrative authority in charge of the UCPA. It publishes guidelines on the UCPA, such as the Management Guidelines for Trade Secrets and the Handbook for Protecting Confidential Information. However, the METI has no powers to enforce the UCPA. The METI promotes cybersecurity measures with the aim of influencing Japanese industry, including the information processing industry.

Law enforcement agencies

The Prosecutors' Office, police, and the National Police Agency have powers to enforce cybercrime laws by conducting investigations and arrests. Criminal penalties are usually imposed only on individuals (eg, directors, officers and employees), but some provisions impose criminal penalties on companies.

Obligations on companies to protect IT systems and data from cyberthreats

Obligations to ensure the security of personal data

As described above, a business operator that processes personal data must take necessary and appropriate actions to ensure the security of personal data (article 23 of the APPI). The PPC publishes guidelines for the handling of personal data. The guidelines provide examples of the approved handling measures, such as establishing a basic policy and internal rules; implementing organisational, personal, physical and technical security measures; and understanding the external environment.

In addition to the APPI, various other laws have provisions aimed at protecting certain personal data from cyberthreats. For example:

- credit card information (the Instalment Sales Act);
- information on the physical and mental condition of workers (the Industrial Safety and Health Act);
- customer information of financial institutions (eg, the Banking Act); and
- 'My Number', the individual number assigned to each person in Japan (the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure).

Cybersecurity Management Guidelines

Cybersecurity Management Guidelines (most recent version as of November 2017) have been jointly issued by the METI and the Independent Administrative Agency Information-technology Promotion Agency (IPA). While the guidelines are not legally binding, they are observed on a voluntary basis by many companies in implementing cybersecurity measures. The guidelines set out three principles that should be observed by companies that have a dedicated IT department and are using IT to protect against cyberattacks. The guidelines also set out 10 key recommendations for those in charge of IT security, for example, a chief information security officer (CISO):

- recognise cybersecurity risks and develop company-wide measures;
- build a structure or process for cybersecurity risk management;
- secure resources (eg, budget and employees) to execute cybersecurity measures;
- understand possible cybersecurity risks and develop plans to deal with those risks;
- build a structure to deal with cybersecurity risks;
- publish a cybersecurity measures framework (PDCA) and action plan;
- develop an emergency response system (emergency contacts, initial action manual and Computer Security Incident Response Team (CSIRT)) and execute regular hands-on drills;
- develop a system to recover from the damages caused by an incident;
- ensure that entities in the company's entire supply chain, including business partners and outsourcing companies for system operations, implement security measures; and
- collect information on cyberattacks by participating in information-sharing activities and develop an environment to use that information.

The IPA issues a Cybersecurity Management Guideline Practice Edition that contains ideas, implementation procedures and practical examples to help implement the 10 recommendations.

Common standards on information security measures of government entities

The CSHQ and the NISC jointly issued the Common Standards on Cybersecurity Measures of Governmental Entities under article 26(1) of the BAC. The standards are a unified framework for improving the level of information security of governmental entities and define the baseline for information security measures to ensure a higher level of information security. Although these standards do not apply to private companies, some entities refer to these standards for their information security measures.

Effect of local laws on foreign businesses

Cybercrime

As a general matter, criminal penalties will apply if a crime causes an effect in Japan, even where the active elements of the crime are committed overseas. Similarly, where a crime is governed by a treaty, the Penal Code and the APUCA apply to the perpetrator, even where the active elements of the crime are committed overseas (article 4-2 of the Penal Code and article 14 of the APUCA). Accordingly, the Penal Code and the APUCA are applicable when a server or a person in Japan suffers damage from cyberattacks launched from overseas. Further, the UCPA (articles 21(6), (7) and (8)) and the APPI (article 166) have extraterritorial reach.

Additionally, Japan is a signatory of the Convention on Cybercrime (2001 Budapest Convention). Japan established domestic substantive and procedural laws under the convention in 2011 and ratified the convention in 2012. Additionally, mutual legal assistance treaties (MLAT) to collect and obtain evidence within each country have been signed by Japan with the United States, South Korea, China, Hong Kong, Vietnam, the European Union and Russia.

Responsibilities of directors

Directors of large companies must, under the Companies Act, determine matters relevant to the establishment of an internal control system (ie, a risk management system reflecting the size and features of the company), including cybersecurity measures. Company directors may be deemed to be in breach of

this obligation if no determination has been made with respect to the required matters – for example, if internal policies related to cybersecurity have not been implemented.

Further, if company directors, including directors of small or medium-sized companies, fail to implement adequate cybersecurity measures, they may be in breach of their statutory duties of due care and loyalty. In such a case, directors can be liable to their companies if the companies suffer damage. Moreover, shareholder representative lawsuits can seek compensation for damages caused to a company due to the negligent actions of directors.

Directors will also be personally liable for injury if their failure to determine the necessary matters causes damage to data subjects.

Best practices for responding to breaches

Responding to cyber incidents in relation to critical infrastructure

The term 'critical information infrastructure operators' is defined under article 3.1 of the BAC as operators of businesses that provide infrastructure foundational to life and economic activity, which could be dramatically impacted by the failure or deterioration of that infrastructure. Fourteen critical infrastructure areas are specified under the CSHQ: information and communication (eg, internet service providers, cable TV operators and broadcasters), financial services, aviation, airports, railways, electric power, gas supply, government and administration, medical services, water, logistics, chemicals, credit cards and petroleum.

Notification in the event of a cyber incident is not mandatory. However, the CSHQ's Cybersecurity Policy for Critical Infrastructure Protection encourages critical infrastructure operators to report, on a voluntary basis to the NISC through competent ministries and agencies, information system failures – including symptoms of these failures – as well as cyber incidents that threaten the confidentiality, integrity or availability of information.

Additionally, financial companies are required to report data breaches according to the financial regulation laws. In the telecommunications industry, significant incidents – including cyber incidents – must be reported without delay to the MIC as described above.

Personal data breaches

The 2020 Amendment introduced obligations to report a data breach to the authorities or notify affected individuals from 1 April 2022 (article 26 of the APPI). According to this rule, the business operator is obligated to report a data breach to the PPC in the following cases:

1. the occurrence or likelihood of a data breach involving special care-required personal information (defined in the APPI);

2. the occurrence or likelihood of a data breach involving personal data (defined in the APPI) that poses a risk of financial damage to data subjects;
3. the occurrence or the likelihood of a data breach caused by wrongful intent; or
4. the occurrence or the likelihood of a data breach involving more than 1,000 data subjects.

The reporting obligation is two-staged. When a business operator recognises that one of the above cases has occurred, it must promptly submit a preliminary report on the matters known at the time of reporting and a second report within 30 days (60 days in the case of item 3 above). The report must include:

- an overview of the data breach;
- items of the compromised personal data;
- the number of data subjects affected as a result of the data breach;
- the cause of the data breach;
- the presence or absence of secondary damage and the details thereof (if any);
- the status of the response to the data subjects;
- the status of public announcement;
- measures to prevent recurrence; and
- other information that is helpful to data subjects.

In addition, in the case of a data breach subject to the mandatory reporting, the 2020 Amendment requires that a handling operator notify data subjects whose personal data is compromised. However, this notification obligation does not apply when it is difficult to inform data subjects – necessary alternative actions, such as a public announcement, can be taken to protect data subjects' rights and interests.

There is a rule for exemption from these obligations: if the breached data was subject to advanced encryption or other measures that are necessary to protect the rights and interests of data subjects, incidents will be excluded from the reporting and notification obligations.

Private redress options for unauthorised cyberactivity

A data subject can file a claim for damages under tort or contract law against a company if personal data is breached as a result of a cyberattack against the company where the company is at fault.

Security of cloud services

An outline of the Information System Security Management and Assessment Programme (ISMAP) was released in June 2020. ISMAP's objective is to ensure security in the procurement of governmental cloud services and thereby promote the smooth use of cloud services through the registration and evaluation of cloud services that meet the government's security requirements. The system is based on the US Federal Risk and Authorization Management Program (FedRAMP).

Thirty-eight services are now published as satisfying the registration requirements of ISMAP. Government agencies are expected to select from the list when procuring cloud services. While this system is intended to be used principally by government agencies, it is likely that it will also be useful for the private sector.

Information-sharing about cybersecurity

The Cybersecurity Management Guidelines described above recommend that organisations collect information on cyberattacks by participating in information-sharing activities.

In December 2018, the BAC was amended to establish the Cybersecurity Council, which aims to be a forum where national and local governmental authorities and businesses can share information on cybersecurity measures. The Cybersecurity Council was established in April 2019.

Yoshifumi Onodera

Mori Hamada & Matsumoto

Yoshifumi Onodera is a partner at Mori Hamada & Matsumoto. Highly experienced in all kinds of data-related matters, he is particularly articulate in the delivery of advice to both foreign and domestic clients on complex business structures in

vast industries including internet-related services, social networking services, games, music, movies and telecommunications. Most of his work relates to communication, media, competition, consumer and information laws. His expertise also extends to IP-related transactions, concerning licensing and dispute resolution aspects of a case in the subsidiary fields of infringement litigations, invalidity trials, appellate litigation and arbitration, and licensing in relation to intellectual property including patents, trademarks, and copyright. Yoshifumi is a member of the Intellectual Property Centre Committee, the Japan Federation of Bar Associations and the International Bar Association (IBA), and is an officer of the Intellectual Property and Entertainment Law Committee.

Hiroyuki Tanaka

Mori Hamada & Matsumoto

Hiroyuki Tanaka is a partner at Mori Hamada & Matsumoto, admitted in Japan and New York. His practice areas are data protection, IT and IP. He has extensive experience advising foreign clients on Japanese data protection law and cybersecurity law. He has a long list of publications relating to his area of expertise, including 'Japan updates enforcement rules for amended APPI' (IAPP, 2021), 'Q&A on Revised Act on the Protection of Personal Information of 2020 [2nd ed.]' (Chuokeizai-sha, Inc, 2022), and 'EU Data Compliance for Practitioners (GDPR and e-Privacy Regulations)' (Shojihoumu, Co, Ltd, 2019). He was selected as one of the National Leaders in the Data area by *Who's Who Legal: Japan 2021*. He was also selected as one of the top five best performing lawyers in 2019 (as selected by companies) in the data-related area by the 15th *Corporate Legal Affairs and Lawyer Survey* published by Nikkei Inc (Japan). He was listed as one of the best lawyers in Japan by the 13rd edition of *The Best Lawyers* in Japan published by Best Lawyers in the Technology Law area. He has LLB and JD degrees from Keio University and an LLM in Competition, Innovation, and Information Law from New York University School of Law.

Daisuke Tsuta

Mori Hamada & Matsumoto

Daisuke Tsuta is a senior associate at Mori Hamada & Matsumoto, which he joined in 2020. Daisuke specialises in cybersecurity and privacy law. He was admitted to the bar in Japan in 2010. Daisuke worked at the Kinki Local Finance Bureau of the Ministry of Finance from 2014 to 2015, at the Ministry of Internal Affairs and Communications (MIC) from 2015 to 2017, and at the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) from 2017 to 2020. Daisuke was in charge of amending the Act on the Protection of Personal Information Held by Administrative Organs in the MIC, and of amending the Basic Act on Cybersecurity and drafting the Q&A handbook for cybersecurity law and regulations in the NISC. He has written various books and articles including *Criminal Law for Information Security I – Crimes Related to Cybersecurity* (2022, Koubundou) and *Digital Forensics and Cybersecurity for Legal Practice* (2021, Shojihoumu).

Naoto Shimamura

Mori Hamada & Matsumoto

Naoto Shimamura is a senior associate, licensed in Japan, New York and California. He has a deep and extensive knowledge and experience in technology, the internet, privacy, data, IP laws and related litigation, as well as the qualifications of CIPP/E and CIPP/US and Registered Information Security Specialist in Japan. His professional experience includes secondment to SoftBank Corp, one of the leading Japanese companies, and employment at a reputable US business law firm. He has an LLB with honours from Waseda University and an LLM from UC Berkeley School of Law. He authored various books and articles, including the Japan chapter of *Chambers Global Practice Guides Data Protection & Privacy/Cybersecurity 2022* (2022, Chambers), *Q&A:Digital Health and Law [2nd ed.]* (2022, Shojihomu) and *Legal Practice Concerning Use of Information Content* (2020, Seirin Shoin).

Mori Hamada & Matsumoto

Mori Hamada & Matsumoto is a full-service law firm that has served clients with distinction since its establishment, in December 2002, by the merger of Mori Sogo and Hamada & Matsumoto. Even as business conditions have rapidly shifted both within Japan and internationally, the firm's goal has been to grow with our clients through tireless effort and constant innovation.

Led by top-rated lawyers across a wide array of practice areas, our large team of legal professionals and support staff offer the firm their experience, expertise and hard work to bring our clients the best results in every matter we handle. Our team strives to build new frameworks to tackle cutting-edge problems, to break down barriers on tough cases, and to find a common resolution in matters with many conflicting interests.

Based on this solid foundation of experience, Mori Hamada & Matsumoto also contributes significantly to the constant evolution and improvement of the Japanese legal system, and to the creation of a legal infrastructure that will enable our clients to excel.

16th Floor, Marunouchi Park Building
2-6-1 Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan
Tel: +81 3 5220 1800

www.mhmjapan.com

Yoshifumi Onodera
yoshifumi.onodera@mhm-global.com

Hiroyuki Tanaka
hiroyuki.tanaka@mhm-global.com

Daisuke Tsuta
daisuke.tsuta@mhm-global.com

Naoto Shimamura
naoto.shimamura@mhm-global.com