

The Basic Act on Cybersecurity (Partially unenforced)

(Act No. 104 of November 12, 2014)

Table of Contents

- Chapter I General Provisions (Articles 1 through 11)
- Chapter II Cybersecurity Strategy (Article 12)
- Chapter III Basic Policies (Articles 13 through 23)
- Chapter IV Cybersecurity Strategic Headquarters (Articles 24 through 37)
- Chapter V Penal Provisions (Article 38)
- Supplementary Provisions

Chapter I General Provisions

(Purpose)

Article 1 In consideration of the fact that ensuring cybersecurity while securing the free flow of information is an urgent issue, due to the increasing severity of threats to cybersecurity and other changes in internal and external circumstances that are arising on a global scale, as the internet and other advanced information and telecommunications networks develop, and the use of information and communications technologies (referred to below as "information and communications technologies") prescribed in Article 2 of the Basic Act on Forming a Digital Society (Act No. 35 of 2021) expands, the purpose of this Act is to set basic principles for Japan's cybersecurity policies, clarify the responsibilities and other aspects of the national government and local governments, and provide for the formulation of a cybersecurity strategy and other matters that will become the foundation of cybersecurity policies, and also in conjunction with the same Act, comprehensively and effectively advance cybersecurity policies in ways such as establishing a Cybersecurity Strategic Headquarters, and by doing so, enhance economic and social vitality and achieve sustainable development and bring about a society which enables its people to live safely and free of anxiety, and also contribute to ensuring peace and safety in the international community and contribute to Japan's national security.

(Definitions)

Article 2 The term "cybersecurity" as used in this Act means that the necessary measures have been taken to prevent the leakage, loss, or damage of information that is recorded, sent, transmitted, or received in electronic form,

magnetic form, or any other form that cannot be perceived by the human senses (referred to below as "electronic or magnetic form" in this Article) and to securely manage that information in other ways, and that the necessary measures have been taken to ensure the security and reliability of information systems and of information and communications networks (including the necessary measures to prevent damage from unauthorized activities directed at a computer through an information and communications network or through a storage medium associated with a record that has been created in electronic or magnetic form (referred to below as "electronic or magnetic recording medium"), and that these systems and networks are being properly maintained and managed.

(Basic Principles)

- Article 3 (1) In view of the importance of ensuring the free flow of information through the development of the internet and other advanced information and telecommunications networks and through the use of information and communications technologies for activities including the enjoyment of freedom of expression, the creation of innovations, and the enhancement of economic and social vitality through the use of these networks and technologies, cybersecurity policy must be advanced based on the principle of proactively responding to cybersecurity threats, through coordination among a variety of entities, such as the national government and local governments and critical social infrastructure providers (meaning those engaged in business that provides infrastructure which is the foundation of the lives of the people and economic activities, and whose functional failure or deterioration would cause an enormous impact to them; the same applies below).
- (2) The cybersecurity policy must be advanced based on the principle of raising the awareness of each individual member of the public regarding cybersecurity and encouraging each individual member of the public to take voluntary actions, and positively promoting actions to establish resilient systems which can prevent any damage caused by threats against cybersecurity and quickly recover from damage or failure.
- (3) The cybersecurity policy must be advanced based on the principle of developing the internet and other advanced information and telecommunications networks, and positively promoting actions to establish a vital economy and society through the utilization of information and communications technologies.
- (4) The cybersecurity policy must be advanced through international cooperation based on the principle of Japan assuming a leading role in formulating and developing an international cybersecurity framework, in consideration of the fact that responding to cybersecurity threats is a common issue throughout the

international community, and that Japan's economy and society operate within the context of internationally close and interdependent relationships.

(5) The cybersecurity policy must be advanced taking into consideration the basic principles of the Basic Act on Forming a Digital Society.

(6) The cybersecurity policy must be advanced with due consideration to not unjustly infringing on the rights of the people.

(Responsibilities of the National Government)

Article 4 The national government is responsible for formulating and implementing comprehensive cybersecurity policies in line with the basic principles prescribed in the preceding Article (referred to below as "basic principles").

(Responsibilities of Local Governments)

Article 5 Local governments are responsible for formulating and implementing independent cybersecurity policies in line with the basic principles, taking into consideration of the appropriate division of roles with the national government.

(Responsibilities of Critical Social Infrastructure Providers)

Article 6 In line with the basic principles, a critical social infrastructure provider is to deepen their interest in and understanding of the importance of cybersecurity and to endeavor independently and actively to ensure cybersecurity, while also endeavoring to cooperate in the implementation of the cybersecurity policy that the national government or local governments implements, to provide their services in a stable and appropriate manner.

(Responsibilities of Business Entities Related to Cyberspace and Other Business Entities)

Article 7 (1) In line with the basic principles, business entities related to cyberspace (meaning those engaged in business regarding the maintenance of the internet and other advanced information and telecommunications networks, the utilization of information and communications technologies, or business relating to cybersecurity; the same applies below) and other business entities are to endeavor independently and actively to ensure cybersecurity, while also endeavoring to cooperate with the cybersecurity policy that the national government or local governments implement, in the course of their business activities.

(2) Suppliers of the information systems, or computers or programs that constitute a part of those systems, information and communications networks, or electronic or magnetic recording medium (referred to below as "information systems, etc." in this paragraph) are to endeavor, in order to prevent damage to

the information systems, etc. that they have supplied due to threats to cybersecurity, to support the measures taken by the users of information systems, etc. to ensure cybersecurity, including designing and developing information systems, etc. that take into consideration the measures taken by the users to ensure their security and reliability, and continuously providing the necessary information for their proper maintenance and management.

(Responsibilities of Educational and Research Organizations)

Article 8 In line with the basic principles, universities and other educational and research organizations are to independently and actively endeavor to ensure cybersecurity, foster human resources related to cybersecurity, carry out research on cybersecurity, and disseminate the results, while endeavoring to cooperate with the cybersecurity policy that the national government or local governments implement.

(Efforts of the People)

Article 9 In line with the basic principles, the people are to endeavor to deepen their interest in and understanding of the importance of cybersecurity and pay necessary attention to ensuring cybersecurity.

(Legislative Measures)

Article 10 The national government must take legislative, financial, or tax measures or any other measures that are necessary to implement the cybersecurity policy.

(Development of Administrative Organizations)

Article 11 In implementing the cybersecurity policy, the national government is to endeavor to develop administrative organizations and to improve administrative management.

Chapter II Cybersecurity Strategy

Article 12 (1) The national government must establish a basic plan for cybersecurity (referred to below as the "cybersecurity strategy") to comprehensively and effectively promote the cybersecurity policy.

(2) The cybersecurity strategy is to provide for the following matters:

- (i) basic guidelines for the cybersecurity policy;
- (ii) information concerning the ensuring of cybersecurity within national administrative organs and other related organs;
- (iii) information concerning the promotion of ensuring cybersecurity in critical social infrastructure providers, the associations that they form, and local

- governments (referred to below as "critical social infrastructure providers and other related entities"); and
- (iv) beyond what is stated in the preceding three items, matters necessary to comprehensively and effectively promote cybersecurity policies.
- (3) The Prime Minister must request a cabinet decision on the proposed cybersecurity strategy.
- (4) When the cybersecurity strategy is established, the national government must report it to the Diet without delay and make it public through the use of the internet and other appropriate means.
- (5) The provisions of the preceding two paragraphs apply *mutatis mutandis* in the case of amendments to the cybersecurity strategy.
- (6) The national government must endeavor to take necessary measures for implementing the cybersecurity strategy smoothly, such as appropriating the necessary funding in the budget each fiscal year, to the extent that national finances allow, to ensure necessary funding for the costs needed to implement the cybersecurity strategy.

Chapter III Basic Policies

(Ensuring Cybersecurity at National Administrative Organs and Related Organs)

Article 13 Regarding cybersecurity at national administrative organs, incorporated administrative agencies (meaning incorporated administrative agencies prescribed in Article 2, paragraph (1) of the Act on General Rules for Incorporated Administrative Agencies (Act No. 103 of 1999); the same applies below), special corporations (meaning a corporation directly incorporated by law or incorporated by a special law through a special incorporation procedure which is subject to Article 4, paragraph (1), item (viii) of the Act for Establishment of the Ministry of Internal Affairs and Communications (Act No. 91 of 1999); the same applies below), etc., the national government is to provide necessary measures including: formulating common standards regarding cybersecurity measures for national administrative organs, incorporated administrative agencies and designated corporations (special corporations and authorized corporations (meaning a corporation incorporated by a special law which needs the approval of a governmental entity for their incorporation and associated matters; the same applies in Article 33, paragraph (1)) which are designated by the Cybersecurity Strategic Headquarters as ones for which the national government needs to further enhance measures which it is providing to ensure cybersecurity, in consideration of the impact on the people's living conditions and economic activities accrued in the case in which cybersecurity in the corporations is not

ensured; the same applies below); the collaborative use of information systems among national administrative organs; monitoring and analysis of malicious activities against information systems of national administrative organs, incorporated administrative agencies or designated corporations through information and communications networks or electronic or magnetic recording media; cybersecurity exercises and training at national administrative organs, incorporated administrative agencies and designated corporations; responses to cybersecurity threats in cooperation, communication and coordination with relevant domestic and foreign parties; the sharing of information regarding cybersecurity among national administrative organs, incorporated administrative agencies, special corporations, etc.

(Ensuring Cybersecurity at Critical Social Infrastructure Providers and Other Related Entities)

Article 14 Regarding cybersecurity at critical social infrastructure providers and other related entities, the national government is to organize and analyze information to prevent damage to computers associated with their important facilities, and is to take necessary measures including the formulation of standards, exercises and training, the promotion of information sharing and other voluntary efforts.

(Facilitation of Voluntary Activities of Private Enterprises, Educational and Research Organizations, and Other Organizations)

Article 15 (1) In view of the fact that the information related to the intellectual property of private enterprises such as small and medium-sized enterprises or of educational and research organizations such as universities is critical for enhancing Japan's international competitiveness, the national government is to provide necessary measures, including promoting their voluntary activities for cybersecurity by increasing interest in and understanding of the importance of cybersecurity, offering consultation on cybersecurity, and providing necessary information and advice.

(2) Considering that it is important for each member of the public to voluntarily endeavor to ensure cybersecurity, the national government is to provide necessary measures, including offering consultation on cybersecurity and providing necessary information and advice on actions such as appropriate choices concerning products and services in the daily use of computers, the internet or other advanced information and telecommunications networks.

(Coordination with Diverse Entities)

Article 16 The national government is to enhance coordination among relevant administrative organs, and is to take necessary measures to enable diverse

entities, such as the national government, local governments, critical social infrastructure providers, and business entities related to cyberspace, to work on cybersecurity policies in mutual coordination.

(Cybercrime Control and Prevention of Spread of Damage)

Article 17 The national government is to take necessary measures to control crimes related to cybersecurity and prevent the spread of damage caused by these crimes.

(Response to Incidents Which May Critically Impact Japan's Safety)

Article 18 The national government is to take necessary measures to improve and strengthen systems at the relevant bodies, and to strengthen mutual coordination and clarify the division of roles among the relevant bodies for responding to incidents related to cybersecurity that might critically affect Japan's safety.

(Enhancement of Industrial Development and International Competitiveness)

Article 19 In consideration of the fact that it is critical for Japan to have self-reliant capabilities to ensure cybersecurity, the national government is to take necessary measures related to cybersecurity, including the promotion of advanced research and development, technological advancements, the development and recruitment of human resources, the strengthening of the market environment and the development of new businesses through the improvement of competitive conditions, the internationalization of technological safety and reliability standards and the participation in frameworks for mutual recognition of those standards, to create new business opportunities, develop sound businesses, and enhance international competitiveness, so that the cybersecurity sector can become a "growth industry" which creates employment opportunities.

(Promotion of Research and Development)

Article 20 In consideration of the fact that it is critical for Japan to maintain self-reliant technological cybersecurity capabilities, the national government is to take necessary measures related to cybersecurity, including the improvement of the cybersecurity research environment, the promotion of basic research on technological safety and reliability, the promotion of research and development for core technologies, the development of skilled researchers and engineers, the strengthening of coordination among national research institutes, universities, the private sector, and other relevant parties, and international coordination for research and development, to promote research and development for cybersecurity and its technological and other relevant

demonstrations, and to have the relevant cybersecurity results publicized.

(Development of Human Resources)

Article 21 (1) In close coordination and cooperation with universities, colleges of technology, specialized training colleges, private enterprises, and other relevant entities, the national government is to take necessary measures to ensure appropriate employment conditions and treatment of the workforce in the field of cybersecurity, and by doing so, enabling their duties and work environments to become attractive enough to match their importance.

(2) In close coordination and cooperation with universities, colleges of technology, specialized training colleges, private enterprises, and other relevant entities, for the purposes of recruitment, development, and quality improvement of cybersecurity-related human resources, the national government is to take necessary measures, including the utilization of a qualification scheme and training of young technical experts.

(Promotion of Education and Learning, Public Awareness Raising)

Article 22 (1) The national government is to take necessary measures, including the promotion of education and learning, public awareness activities, and the dissemination of knowledge in the field of cybersecurity, to deepen interest and understanding regarding cybersecurity among the people on a broad scale.

(2) The national government is to take necessary measures, including the implementation of events for public awareness and the dissemination of information on cybersecurity, and the designation of the period to promote cybersecurity activities in a focused and effective manner, to contribute to the promotion of the measures referred to in the preceding paragraph.

(Promotion of International Cooperation)

Article 23 In order for Japan to play an active role in the international community in the field of cybersecurity and promote Japan's international interests, the national government is to advance international cooperation relating to cybersecurity, including through independent participation in the formulation of international rules, by building relationships of trust and promoting information-sharing on an international level, by providing active support for capacity building in developing regions' cybersecurity response and other such international technological cooperation, and through crime control; and is also to take the necessary measures for deepening other countries' understanding of cybersecurity in Japan.

Chapter IV Cybersecurity Strategic Headquarters

(Establishment)

Article 24 The Cybersecurity Strategic Headquarters (referred to below as the "Headquarters") is established under the Cabinet to effectively and comprehensively advance cybersecurity policies.

(Affairs under Jurisdiction of the Headquarters)

Article 25 (1) The Headquarters is responsible for the following affairs:

- (i) preparing a draft of the cybersecurity strategy and promoting its implementation;
 - (ii) establishing the standards of cybersecurity measures for national administrative organs, incorporated administrative agencies and designated corporations, and promoting the implementation of the evaluation (including audit) of measures based on the standards and other measures taken
 - (iii) establishing the standards for policies implemented by national administrative organs to ensure cybersecurity at critical social infrastructure providers and other related entities (including surveys on the state of cybersecurity assurance at critical social infrastructure providers and other related entities for establishing the standards), evaluating policies based on the standards, and promoting the implementation of other policies based on the standards;
 - (iv) evaluating the state of cybersecurity assurance at national administrative organs, incorporated administrative agencies, and designated corporations (including monitoring and analyzing unauthorized activities against information systems that are conducted through an information and telecommunications network or electronic or magnetic recording medium, and evaluating measures against critical cybersecurity-related incidents (including investigations into the causes of those incidents));
 - (v) beyond the affairs stated in the preceding items, engaging in research and deliberation on proposals for major cybersecurity policies; establishing cross-departmental plans; making guidelines for estimates of relevant administrative organs' expenditures and establishing the basic principles for implementing their policies; promoting the implementation of those policies, through measures such as evaluating them; and carrying out overall coordination.
- (2) In preparing a draft of the cybersecurity strategy, the Headquarters must hear the opinions of the National Security Council in advance.
- (3) In the following cases, the Headquarters must hear the opinions of the Cybersecurity Promotion Expert Council in advance:
- (i) when it intends to prepare a draft of the cybersecurity strategy;
 - (ii) when it intends to establish the standards referred to in paragraph (1), item (ii) or (iii);

- (iii) when it intends to compile the results of the evaluation referred to in paragraph (1), item (ii) or (iii).
- (4) The Headquarters is to work in close coordination with the National Security Council on critical issues concerning cybersecurity in the context of national security.

(Organization)

Article 26 The Headquarters consists of the Chief of the Cybersecurity Strategic Headquarters, the Deputy Chief of the Cybersecurity Strategic Headquarters, and the members of the Cybersecurity Strategic Headquarters.

(Chief of the Cybersecurity Strategic Headquarters)

- Article 27 (1) The person in charge of the Headquarters is referred to as the Chief of the Cybersecurity Strategic Headquarters (referred to below as the "Chief"), and the Prime Minister serves in that capacity.
- (2) The Chief engages in the overall management of the Headquarters' affairs and directs and supervises personnel at the Headquarters.
- (3) If the Chief finds it necessary based on the evaluation provided for in Article 25, paragraph (1), items (ii) through (v), or the materials, data, etc. provided pursuant to the provisions of Article 32 or 33, the Chief may make recommendations to the head of the relevant administrative organ.
- (4) After making the recommendations pursuant to the provisions of the preceding paragraph, the Chief may request a report from the heads of the relevant administrative organs regarding the measures taken based on the recommendations.

(Deputy Chief of the Cybersecurity Strategic Headquarters)

- Article 28 (1) The Deputy Chief of the Cybersecurity Strategic Headquarters (referred to below as the "Deputy Chief") is assigned to the Headquarters, and a Minister of State serves in that capacity.
- (2) The Deputy Chief assists the Chief's duties.

(Members of the Cybersecurity Strategic Headquarters)

- Article 29 (1) The members of the Cybersecurity Strategic Headquarters are assigned to the Headquarters (referred to as "members" in the following paragraph).
- (2) All Ministers of State other than the Chief and the Deputy Chief serve as members.

(Cybersecurity Promotion Expert Council)

- Article 30 (1) The Cybersecurity Promotion Expert Council (referred to below as

the "Expert Council" in this Article) is established in the Headquarters.

(2) The Expert Council takes charge of the following affairs:

- (i) stating its opinions to the Chief pursuant to the provisions of Article 25, paragraph (3);
- (ii) beyond what is stated in the preceding item, studying and deliberating important cybersecurity policies, and, when it finds necessary, stating its opinions to the Chief.

(3) The members of the Expert Council are appointed by the Prime Minister from among persons with relevant expertise in cybersecurity.

(Entrustment of Affairs)

Article 31 (1) The Headquarters may entrust a part of its affairs to the persons specified in each of the items according to the category of affairs stated in the following items:

- (i) affairs stated in Article 25, paragraph (1), item (ii) (limited to those relating to audits prescribed in the same item (limited to those related to incorporated administrative agencies and designated corporations)), affairs stated in item (iii) of that paragraph (limited to those related to investigations prescribed in that item), or affairs stated in item (iv) of that paragraph (limited to those related to investigations prescribed in that item (limited to those related to incorporated administrative agencies and designated corporations)): the Information-Technology Promotion Agency or other corporations specified by Cabinet Order as having sufficient technical capability and expert knowledge and experience concerning cybersecurity-related measures and being capable of reliably implementing the relevant affairs;
- (ii) affairs stated in Article 25, paragraph (1), item (iv) (limited to those related to the monitoring and analysis of activities prescribed in that item): the National Institute of Information and Communications Technology, the Information-Technology Promotion Agency, or other corporations specified by Cabinet Order as having sufficient technical capability and expert knowledge and experience concerning the monitoring and analysis of the activities and being capable of carrying out the affairs reliably.

(2) An officer or employee of a corporation that has been entrusted with affairs pursuant to the provisions of the preceding paragraph or a person who had been in that position, must not divulge or misappropriate any secrets learned in connection with those affairs under that entrustment, without justifiable grounds.

(3) An officer or employee of a corporation entrusted with affairs pursuant to the provisions of paragraph (1) who engages in the affairs under the entrustment, is deemed to be an official engaged in public services pursuant to laws and

regulations, regarding the application of the Penal Code (Act No. 45 of 1907) or other penal provisions.

(Submission of Materials)

- Article 32 (1) The heads of relevant administrative organs must provide the Headquarters with materials or information related to cybersecurity that is beneficial to the performance of the affairs under its jurisdiction in a timely manner, as prescribed by Headquarters.
- (2) Beyond what is provided for in the preceding paragraph, as requested by the Chief, the heads of the relevant administrative organs must cooperate with the Headquarters, by activities such as providing materials or information related to cybersecurity that is necessary for the performance of the affairs under its jurisdiction, or by explaining those materials or information.

(Submission of Materials and Other Cooperation)

- Article 33 (1) If the Headquarters finds it necessary for carrying out the functions under its jurisdiction, in relation to the measures which the Headquarters takes in coordination with the national government, or other cybersecurity measures for preventing the spread of damage caused by threats against cybersecurity and promoting a quick recovery from any damage, it may request the submission of the necessary materials, presentation of the necessary opinions, provision of the necessary explanations or any other cooperation from the following persons: the heads of local governments or incorporated administrative agencies; the deans or the presidents of national university corporations (meaning national university corporations prescribed in Article 2, paragraph (1) of the National University Corporation Act (Act No.112 of 2003)); the heads of inter-university research institute corporations (meaning inter-university research institute corporations provided for in Article 2, paragraph (3) of that Act); the president of the Japan Legal Support Center (meaning the Japan Legal Support Center provided for in Article 13 of the Comprehensive Legal Support Act (Act No. 74 of 2004)); the representatives of special corporations or authorized corporations designated by the Headquarters; and the representatives of the relevant entity facilitating cybersecurity-related communication and coordination with related domestic and foreign parties. In this case, the relevant person must respond to the request, unless there is a justifiable reason for not doing so.
- (2) If the Headquarters finds it necessary for carrying out the functions under its jurisdiction, the Headquarters may ask for the cooperation referred to in the preceding paragraph from the representatives of the critical social infrastructure providers and the associations that they have organized. In this case, the persons that have been requested to do so are to endeavor to meet

that request.

- (3) If the Headquarters finds it particularly necessary for carrying out the functions under its jurisdiction, it may request the cooperation referred to in paragraph (1) from persons other than those prescribed in the preceding two paragraphs.

(Cooperation for Local Governments)

Article 34 (1) If a local government finds it necessary for formulating or implementing the policy prescribed in Article 5, it may request the Headquarters to provide information and other cooperation.

- (2) If the Headquarters is requested to provide cooperation under the preceding paragraph, it is to endeavor to meet the request.

(Administrative Affairs)

Article 35 Administrative affairs concerning the Headquarters are processed by the Cabinet Secretariat and administered by the Cabinet Cyber Officer.

(Competent Minister)

Article 36 The competent minister under the Cabinet Act (Act No. 5 of 1947) for matters related to the Headquarters is the Prime Minister.

(Delegation to Cabinet Orders)

Article 37 Beyond what is provided for in this Act, Cabinet Order prescribes the necessary matters relating to the Headquarters.

Chapter V Penal Provisions

Article 38 A person who has violated the provisions of Article 31, paragraph (2) is punished by imprisonment for not more than one year or a fine of not more than 500,000 yen.

Supplementary Provisions

(Effective Date)

Article 1 This Act comes into effect on the date of promulgation; provided, however, that the provisions of Chapters II and IV as well as Article 4 of the Supplementary Provisions come into effect on the day specified by Cabinet Order within a period not exceeding one year from the date of promulgation.

(Review)

Article 2 For cybersecurity incidents classed as emergencies specified in Article

21, paragraph (1) of the Act on the Peace and Independence of Japan and Maintenance of the Security of the Nation and the People in Armed Attack Situations, etc., and Survival-Threatening Situations (Act No.79 of 2003), and other malicious activities against computers through information and communications networks or electronic or magnetic recording media, the national government is to review, from a broad point of view, measures aimed at further strengthening the capability of the defense of infrastructure which is the foundation of the peoples' living conditions and economic activities, and for which the functional failure or deterioration of the infrastructure would risk enormous impacts on the people.

Supplementary Provisions [Act No. 66 of September 11, 2015] [Extract]

(Effective Date)

Article 1 This Act comes into effect on April 1, 2016.

Supplementary Provisions [Act No. 76 of September 30, 2015] [Extract]

(Effective Date)

Article 1 This Act comes into effect on the day specified by Cabinet Order within a period not exceeding six months from the date of promulgation.

Supplementary Provisions [Act No. 31 of April 22, 2016] [Extract]

(Effective Date)

Article 1 This Act comes into effect on the day specified by Cabinet Order within a period not exceeding six months from the date of promulgation; provided, however, that the provisions of the following Article and Article 3, Article 5 and Article 6 of the Supplementary Provisions come into effect on the date of promulgation.

(Delegation to Cabinet Order)

Article 6 Beyond what is provided for in Articles 2 through the preceding Article of the Supplementary Provisions, Cabinet Order prescribes the necessary transitional measures for the enforcement of this Act (including transitional measures for penal provisions).

Supplementary Provisions [Act No. 91 of December 12, 2018] [Extract]

(Effective Date)

(1) This Act comes into effect on the day specified by Cabinet Order within a

period not exceeding one year from the date of promulgation.

Supplementary Provisions [Act No. 11 of May 24, 2019] [Extract]

(Effective Date)

Article 1 This Act comes into effect on April 1, 2020.

Supplementary Provisions [Act No. 35 of May 19, 2021] [Extract]

(Effective Date)

Article 1 This Act comes into effect on September 1, 2021.

Supplementary Provisions [Act No. 36 of May 19, 2021] [Extract]

(Effective Date)

Article 1 This Act comes into effect on September 1, 2021; provided, however, that the provisions of Article 60 of the Supplementary Provisions come into effect on the date of promulgation.

(Transitional Measures Concerning Dispositions)

Article 57 (1) After this Act comes into effect, beyond what is otherwise provided for in laws and regulations, any dispositions such as authorizations or other acts which a former national government organ granted or made before this Act comes into effect pursuant to the provisions of one of the relevant laws before amendment by this Act (including orders based on them; referred to below as "former laws and regulations" in this Article and the following Article) are deemed to be dispositions such as authorizations or other acts which a corresponding national government organ granted or made pursuant to the corresponding provisions of the relevant Act after its amendment by this Act (including orders based on them; referred to below as "new laws and regulations" in this Article and the following Article).

(2) Beyond what is otherwise provided for in laws and regulations, an application, notification or any other act that has been filed with or made to the former national government organs pursuant to the provisions of the former laws and regulations at the time of the enforcement of this Act is deemed to be an application, notification or any other act that has been filed with or made to the corresponding national government organs pursuant to the corresponding provisions of new laws and regulations after this Act comes into effect.

(3) Beyond what is otherwise provided for in laws and regulations, if procedures such as applications or notifications are required to be made with the former national government organs pursuant to the provisions of the former laws and

regulations before this Act comes into effect, but those procedures have not been made with the former national government organs before the effective date of this Act, the provisions of the new laws and regulations apply after this Act comes into effect, deeming that the procedures have not been made to the corresponding national government organs pursuant to the corresponding provisions of new laws and regulations.

(Transitional Measures Concerning Effect of Order)

Article 58 After this Act comes into effect, the Cabinet Office Order referred to in Article 7, paragraph (3) of the Act for Establishment of the Cabinet Office, or the Ministerial Order stated in Article 12, paragraph (1) of the National Government Organization Act that has been issued pursuant to the provisions of the former laws and regulations is to remain in force as the corresponding Order of the Digital Agency stated in Article 7, paragraph (3), or the Ministerial Order stated in Article 12, paragraph (1) of the National Government Organization Act that has been issued based on the corresponding provisions of the new laws and regulations, unless otherwise provided for in laws and regulations.

(Transitional Measures for Application of Penal Provisions)

Article 59 Prior laws and regulations continue to govern the applicability of penal provisions to conduct that a person engages in before this Act comes into effect.

(Delegation to Cabinet Orders)

Article 60 Beyond what is provided for in Article 15, Article 16, Article 51 and the preceding three Articles of the Supplementary Provisions, transitional measures necessary for the enforcement of this Act (including transitional measures concerning penal provisions) are to be provided for by Cabinet Order.

Supplementary Provisions [Act No. 68 of June 17, 2022] [Extract]

(Effective Date)

- (1) This Act comes into effect on the date on which the Act Partially Amending the Penal Code and Related Acts comes into effect; provided, however, that the provisions stated in the following items come into effect on the date prescribed in the items:
- (i) the provisions of Article 509: the date of promulgation

Supplementary Provisions [Act No. 43 of May 23, 2025] [Extract]

(Effective Date)

Article 1 This Act comes into effect on the date on which the Act on Prevention of Damage Caused by Wrongful Acts against Important Computers (Act No. 42 of 2025) comes into effect; provided, however, that the provisions stated in the following items come into effect on the dates specified respectively in those items:

- (i) the provisions of Article 4 of the Supplementary Provisions: the date of promulgation;
- (ii) the provisions of Article 1, the provisions in Article 3 to amend Article 1, item (viii) of the Act on Remuneration of Officials with Special Capacity and Appended Table 1 of the same Act (limited to the part amending "and the Director of Cabinet Intelligence" to ", the Director of Cabinet Intelligence, and the Cabinet Cyber Officer"), the provisions of Article 5, Article 7, Article 12, and Article 15, and the provisions in Article 17 to add one item to Article 4, paragraph (1) of the Act for Establishment of the Cabinet Office and to add one item after paragraph (3), item (xxvii) - 6 of that Article: the effective date of the provisions stated in Article 1, item (ii) of the Supplementary Provisions of the Act on Prevention of Damage Caused by Wrongful Acts against Important Computers.

(Transitional Measures Associated with Partial Amendment in The Basic Act on Cybersecurity)

Article 2 Even after the effective date of this Act (referred to below as "the effective date" in this Article and the following Article), prior laws and regulations continue to govern the duty not to divulge or misappropriate any secret learned in connection with the administrative affairs of the Cybersecurity Council referred to in Article 17, paragraph (1) of The Basic Act on Cybersecurity before amendment by the provisions of Article 13, related to a person who was engaged in those administrative affairs before the effective date, and the duty not to divulge or misappropriate any secret learned in connection with the entrusted administrative affairs related to a person who was an officer or employee of a corporation entrusted with the administrative affairs stated in Article 31, paragraph (1), item (iii) of that Act before the effective date.

(Transitional Measures for Application of Penal Provisions)

Article 3 Prior laws and regulations continue to govern the applicability of penal provisions to conduct that a person engages in before the effective date, and to conduct that a person engages in after the effective date but which, pursuant to the preceding Article, is to continue to be governed by prior laws and regulations.

(Delegation to Cabinet Orders)

Article 4 Beyond what is provided for in the preceding two Articles, transitional measures necessary for the enforcement of this Act (including transitional measures concerning penal provisions) are specified by Cabinet Order.