The Basic Act on Cybersecurity

(Act No. 104 of November 12, 2014)

Table of Contents

Chapter I General Provisions (Articles 1 to 11)
Chapter II Cybersecurity Strategy (Article 12)
Chapter III Basic Policy (Articles 13 to 23)
Chapter IV Cybersecurity Strategic Headquarters (Articles 24 to 35)
Supplementary Provisions

Chapter I General Provisions

(Purpose)

Article 1 Facing domestic and foreign changes such as the intensification of threats against cybersecurity on a worldwide scale, and with the progression of the Internet and other advanced information and telecommunications networks, the use of information and telecommunications technologies, and the given situation of the urgent issue to ensure the free flow of information and the protection of cybersecurity simultaneously, the purpose of this Act is to comprehensively and effectively promote the cybersecurity policy by: stipulating basic principles of national the cybersecurity policy; clarifying the responsibilities of the national government, local governments, and other concerned public parties; stipulating essential matters for cybersecurity-related policies such as the cybersecurity strategy formulation; and establishing the Cybersecurity Strategic Headquarters and so forth, together with the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (Act. No. 144 of 2000), and as a result, attempting to enhance economic and social vitality, sustainable development and realizing social conditions where the people can live with a sense of safety and security, and contributing to the protection of international peace and security as well as national security.

(Definitions)

Article 2 For the purposes of this Act, the term "Cybersecurity" means the necessary measures that are needed to be taken to safely manage information, such as prevention against the leak, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive functions (hereinafter in this section referred to as "Electronic or Magnetic Means"); and to guarantee

the safety and reliability of information systems and information and telecommunications networks (including necessary preventive measures against malicious activities toward electronic computers through information network or storage media for information created by electronic or magnetic means (hereinafter referred to as "Electronic or Magnetic Storage Media")), and that those states are appropriately maintained.

(Basic Principles)

Article 3 (1) Given that ensuring the free flow of information through maintaining the Internet and other advanced information and telecommunications networks, the utilization of information and telecommunications technologies are critical to enjoying benefits through the freedom of expression, enabling the creation of innovation, improving economic and social vitality, and so forth, the promotion of the Cybersecurity policy must be carried out with the intent to produce active responses to threats against Cybersecurity through coordination among multiple stakeholders, including the national government, local governments, and critical information infrastructure CII Operators (referring to operators of businesses that provide infrastructure which is the foundation of the people's living conditions and economic activities and the functional failure or deterioration of which would risk enormous impacts to them; hereinafter, the same is to apply).

(2) The promotion of the Cybersecurity policy must be carried out with the intent to raise awareness to each member of the public about Cybersecurity and encourage each member of the public to take voluntary actions to prevent any damage caused by threats against Cybersecurity, and to positively promote actions to establish resilient systems which can quickly recover from damage or failure.

(3) The policy to promote Cybersecurity must proactively be carried out with the intent to implement on maintaining the Internet and other advanced information, telecommunications networks and actions toward the establishment of a vital economy and society through the utilization of information and telecommunications technologies.

(4) Given the fact that combatting threats against Cybersecurity is a common concern of the international community, and with recognition that Japan's economic and social activities are characterized by close international interdependence, the promotion of the Cybersecurity policy must be required to be carried out with intent to play a leading role in an internationally-coordinated effort for the creation and development of an international normative framework for Cybersecurity.

(5) The promotion of the Cybersecurity policy must be required to be carried out in consideration of the basic principles of the Basic Act on the Formation of an

Advanced Information and Telecommunications Network Society.

(6) The promotion of the Cybersecurity policy is required to be carried out with due consideration not to wrongfully impinge upon the peoples' rights.

(Responsibility of the Government)

Article 4 In accordance with the basic principles prescribed under the preceding article, (hereinafter referred to as the "Basic Principles"), the national government bears the responsibility to formulate and implement comprehensive Cybersecurity policies.

(Responsibility of Local Governments)

Article 5 In accordance with the Basic Principles, local governments bear the responsibility to formulate and implement independent Cybersecurity policies in consideration of the appropriate division of roles with the national government.

(Responsibility of CII Operators)

Article 6 In accordance with the Basic Principles and for the purpose of stable and appropriate provision of their services, CII Operators are to make an effort to: deepen their awareness and understanding of the critical value of Cybersecurity; ensure Cybersecurity voluntarily and proactively; and cooperate with the measures on Cybersecurity taken by the national government or local governments.

(Responsibility of Cyberspace-Related Business Entities and Other Business Entities)

Article 7 In accordance with the Basic Principles, Cyberspace-Related Business Entities (referring to those engaged in business regarding the maintenance of the Internet and other advanced information and telecommunications networks, the utilization of information and telecommunications technologies, or involved in business related to Cybersecurity; hereinafter, the same is to apply) and other business entities are to make an effort to ensure Cybersecurity voluntarily and proactively in their businesses and to cooperate with the measures on Cybersecurity taken by the national government or local governments.

(Responsibility of Educational and Research Organizations)

Article 8 In accordance with the basic principles, universities and other educational and research organizations are to make an effort to ensure Cybersecurity voluntarily and proactively, develop human resources specialized for Cybersecurity, disseminate research and the results of research

on Cybersecurity, and cooperate with measures taken by the national government or local governments.

(The Efforts of the People)

Article 9 In accordance with the Basic Principles, the people are to make an effort to deepen their awareness and understanding of the critical value of Cybersecurity and pay necessary attention to ensuring Cybersecurity.

(Legislative and Other Measures)

Article 10 The national government must take necessary measures for the implementation of Cybersecurity policies including legislative, financial, or taxation measures.

(Development of Administrative Organizations)

Article 11 In providing Cybersecurity policies, the national government is to make an effort to develop administrative organizations and to improve administrative management.

Chapter II The Cybersecurity Strategy

Article 12 (1) The national government must establish a basic plan for Cybersecurity (hereinafter referred to as the "Cybersecurity Strategy") with the aim of the comprehensive and effective promotion of the Cybersecurity policy.

(2) The Cybersecurity Strategy addresses the following:

(i) basic objectives of Cybersecurity policies;

(ii) matters regarding the ensuring of Cybersecurity within national administrative organs and other related organs;

(iii) matters regarding the promotion of the ensuring of Cybersecurity CII Operators, their professional associations, and local governments (hereinafter referred to as "CII Operators and Other Related Entities"); and

(iv) beyond the matters listed in the preceding three items, other matters required for the comprehensive and effective promotion of Cybersecurity policies.

(3) The Prime Minister must request a cabinet decision on the proposed Cybersecurity Strategy.

(4) When establishing the Cybersecurity Strategy, the national government must report it to the Diet without delay and to announce it publicly through the use of the Internet and other appropriate means.

(5) The provisions prescribed under the preceding two paragraphs apply in the case of amendments to the Cybersecurity Strategy.

(6) With the aim of ensuring necessary funds regarding the expenses to enable the implementation of the Cybersecurity Strategy, the national government must make an effort to provide necessary measures for the smooth implementation of the Cybersecurity Strategy, such as appropriating the necessary funds in its budget every fiscal year, to the extent permitted within national fiscal limitations.

Chapter III Basic Policy

(Ensuring of Cybersecurity at National Administrative Organs and Related Organs)

Article 13 With regard to Cybersecurity at national administrative organs, Incorporated Administrative Agencies (referring to Incorporated Administrative Agencies prescribed under Article 2, paragraph (1) of the Act on General Rules for Incorporated Administrative Agencies (Act No. 103 of 1999); hereinafter, the same is to apply), Quasi-governmental Agencies; (referring to a corporation directly incorporated by acts or a corporation incorporated by a special act pursuant to a special incorporation procedure and subject to the provision of Article 4 (xv) of the Act for Establishment of the Ministry of Internal Affairs and Communications (Act No. 91 of 1999); hereinafter, the same is to apply), and so forth, the national government is to provide necessary measures including: the formulation of common standards of Cybersecurity measures for national administrative organs and Incorporated Administrative Agencies; the collaborative use of interoperable information systems among national administrative organs; monitoring and analysis of malicious activities against information systems of national administrative organs through information and communications networks or Electronic or Magnetic Storage Media; Cybersecurity exercises and training at national administrative organs; 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, and so forth.

(Ensuring of Cybersecurity at CII Operators and Other Related Entities)

Article 14 With regard to Cybersecurity at CII Operators and Other Related Entities, the national government is to provide necessary measures, including the formulation of standards, exercises and training, the promotion of information sharing, and other voluntary activities.

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

Article 15 (1) Given the fact that information on intellectual property owned by private enterprises such as small and medium-sized enterprises, educational and research organizations such as universities are critical for the enhancement of Japan's international competitiveness, and in order to promote their voluntary activities for Cybersecurity, the national government is to provide necessary measures, including increasing awareness and understanding about the critical value of Cybersecurity, offering consultation on Cybersecurity, and providing necessary information and advice.

(2) Given the fact that it is important for each member of public to make an effort to voluntarily 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 about products and services in the daily use of electronic computers or the Internet and other advanced information and telecommunications networks.

(Coordination with Multiple Stakeholders)

Article 16 The national government is to aim at the enhancement of coordination among relevant ministries and is to provide necessary measures to enable multiple stakeholders, such as the national government, local governments, CII Operators, and Cyberspace-related Business Entities, to work on Cybersecurity policies in mutual coordination.

(Crackdown on Cybercrime and Prevention of Damage)

Article 17 The national government is to provide necessary measures to crackdown on cybercrime and prevent the spread of damage.

(Action for Matters Which May Critically Affect the Country's Safety)

Article 18 The national government is to provide necessary measures with the intention to: improve and strengthen systems to respond to Cybersecurity concerns at relevant bodies; strengthen the mutual coordination among relevant bodies; and clarify the division of roles among relevant bodies, as actions to address threats which may critically affect the country's safety with respect to Cybersecurity-related incidents.

(Enhancement of Industrial Development and International Competitiveness)

Article 19 Given that it is critical for Japan to have self-reliant capabilities to ensure Cybersecurity, and in order to create new business opportunities, develop sound businesses ', and improve international competitiveness, and so as to make the Cybersecurity sector a "growth industry" which is able to create employment opportunities, the national government is to provide 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, and the internationalization of technological safety and reliability standards and the participation in such frameworks on the basis of mutual recognition.

(Promotion of Research and Development)

Article 20 Given that it is critical for Japan to maintain self-reliant technological Cybersecurity capabilities, in order to promote research and development for Cybersecurity as well as the technological and other relevant demonstrations of Cybersecurity, and to expand the distribution of relevant Cybersecurity outcomes, the national government is to provide necessary measures related to Cybersecurity for: the improvement of the environment of Cybersecurity research; the promotion of basic research on technological safety and reliability as well as 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.

(Development of Human Resources)

Article 21 (1) In close coordination and cooperation with universities, colleges of technology, technical schools, private enterprises, and other relevant entities, the national government is to provide necessary measures to ensure appropriate assignments and employment conditions or treatment of the workforce in the field of Cybersecurity, thereby enabling their functions and work environments to become attractive enough to meet their professional values.

(2) In close coordination and cooperation with universities, technical schools, 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 provide 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) For the purpose of extensive public awareness raising and understanding about Cybersecurity among the people, the national government is to provide necessary measures including the promotion of education and learning, public awareness activities, and the dissemination of knowledge in

the field of Cybersecurity.

(2) In order to promote the measures prescribed under the preceding paragraph, the national government is to provide necessary measures, including the implementation of events for public awareness and the dissemination of information on Cybersecurity and the designation of a specific, focused campaign period to effectively promote Cybersecurity activities.

(Promotion of International Cooperation)

Article 23 In the field of Cybersecurity, to actively carry out Japan's role in the international community and to promote Japan's interests in the community, the national government is to promote: active participation in an international norm setting; confidence building and the promotion of information sharing with foreign countries; international technical cooperation such as active support for Cybersecurity capacity building in developing countries; international cooperation such as crackdowns on cybercrime; and is to provide necessary measures to deepen other countries' understanding of Japan's Cybersecurity.

Chapter IV Cybersecurity Strategic Headquarters

(Establishment)

Article 24 For the purpose of effectively and comprehensively promoting Cybersecurity policies, the Cybersecurity Strategic Headquarters (hereinafter referred to as the "Headquarters") are to be established under the Cabinet.

(Functions under Jurisdiction of the Headquarters)

Article 25 (1) The Headquarters will carry out the following functions:

(i) Preparing the Cybersecurity Strategy and promoting its implementation.

(ii) Establishing the standards of Cybersecurity measures for national administrative organs and Incorporated Administrative Agencies, and promoting the implementation of the evaluation (including audit) of measures based on the standards and other measures taken pursuant to the standards.

(iii) Evaluating the countermeasures against critical Cybersecurity-related incidents involving national administrative organs (including fact-finding activities to determine the cause or causes of the incident).

(iv) beyond the functions listed in the preceding three items, with respect to major Cybersecurity policies: engaging in research and deliberation on program proposals; establishing cross-governmental plans, budget plans and guidelines of relevant administrative organs, the basic principles of program implementation as well as promoting the implementation of policy evaluation

and other relevant policies; and carrying out overall coordination.

(2) In preparing the draft of the Cybersecurity Strategy, the Headquarters must be required to hear the opinions of the Strategic Headquarters for the Promotion of an Advanced Information Telecommunications Network Society, and the National Security Council in advance.

(3) The Headquarters are to work in close coordination with the Strategic Headquarters for the Promotion of an Advanced Information Telecommunications Network Society with regard to critical issues concerning Cybersecurity.

(4) The Headquarters are to work in close coordination with the National Security Council with regard to critical issues concerning Cybersecurity in the context of national security.

(Organization)

Article 26 The Headquarters are to consist of the Chief of Cybersecurity Strategy, the Deputy Chief of Cybersecurity Strategy, and the members of the Headquarters of Cybersecurity Strategy.

(The Chief of the Cybersecurity Strategic Headquarters)

Article 27 (1) The Chief Cabinet Secretary is to serve as the Chief of the Headquarters (hereinafter referred to as the "Chief")

(2) The Chief is to engage in the overall management of the Headquarters' functions and the oversight of personnel at the Headquarters.

(3) The Chief, where necessary, can make recommendations to the heads of relevant administrative organs, based on the evaluations prescribed under Article 25, paragraph (1), item (ii) to (iv), or the documents, information or other materials provided pursuant to the provisions under Articles 30 or 31.

(4) After making the recommendations as prescribed under 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.

(5) The Chief may, where particularly necessary in relation to the recommendations made in accordance with paragraph (3) of this article, present opinions for the Prime Minister to take an action for the matter, as prescribed under Article 6 of the Cabinet Law (Act No. 5 of 1947).

(The Deputy Chief of the Cybersecurity Strategic Headquarters)

Article 28 (1) A Minister of State is to be designated as the Deputy Chief of the Cybersecurity Strategic Headquarters (hereinafter referred to as the "Deputy Chief")

(2) The Deputy Chief is to assist the Chief's missions.

(Members of the Cybersecurity Strategic Headquarters)

Article 29 (1) The Headquarters are to establish the members of the Cybersecurity Strategic Headquarters (referred to in the succeeding paragraph as the "members").

(2) Those listed below are to be designated as the members (except in a case where someone listed in item (i) to (v) is designated as the Deputy Chief).

(i) The Chairperson of the National Public Safety Commission;

(ii) The Minister for Internal Affairs and Communications;

(iii) The Minister for Foreign Affairs;

(iv) The Minister of Economy, Trade and Industry;

(v) The Minister of Defense;

(vi) Beyond those listed above, any Minister of State, except the Chief and the Deputy Chief, who is designated by the Prime Minister as indispensable for the functions of the Headquarters; and

(vii) Among experts with exceptional knowledge and experiences on Cybersecurity, those designated by the Prime Minister.

(Submission of Materials)

Article 30 (1) As set by the Headquarters, the heads of the relevant administrative organs must have a duty to furnish the Headquarters timely with materials or information regarding Cybersecurity that are beneficial in fulfilling its functions.

(2) Beyond the provision under the preceding paragraph, when requested by the Chief, the heads of the relevant administrative organs have a duty to cooperate with the Headquarters for the fulfillment of its functions, by providing materials or information regarding Cybersecurity, explanation and other necessary cooperation.

(Submission of Materials and Other Cooperation)

Article 31 (1) The Headquarters may, where necessary for the fulfillment of its functions, request the submission of materials, the presentation of opinion, explanation and any other necessary cooperation from: the heads of local governments and Incorporated Administrative Agencies; the deans of national university corporations (referring to national university corporations prescribed under Article 2, paragraph (1) of the National University Corporation Act (Act No.112 of 2003)); the heads of inter-university research institute corporations (referring to inter-university research institute corporations prescribed under Article 2, paragraph (3) of the Act); the President of the Japan Legal Support Center (referring to the Japan Legal Support Center prescribed under Article 13 of the Comprehensive Legal

Support Act (Act No. 74 of 2004)); the representatives of Special Corporations and authorized corporations (referring to juridical persons incorporated by a special act and where the approval of a governmental entity is required for their incorporation and associated matters) designated by the Headquarters; and the representative of the relevant entity facilitating Cybersecurity-related communication and coordination with domestic and foreign parties concerned.

(2) In addition, the Headquarters may, where particularly necessary for the fulfillment of its functions, request necessary cooperation from a party other than the parties prescribed in the preceding paragraph.

(Cooperation for Local Governments)

Article 32 (1) Local governments may, request the provision of information and other cooperation from the Headquarters where necessary, for the establishment and implementation of the policies prescribed under Article 5.

(2) When cooperation is requested pursuant to the preceding paragraph, the Headquarters are to make an effort to meet the request.

(Functions)

Article 33 The functions of the Headquarters are to be performed by the Cabinet Secretariat and managed by a designated Assistant Chief Cabinet Secretary.

(Chief Minister)

Article 34 For matters pertaining to the Headquarters, the Prime Minister is to be the chief minister as prescribed in the Cabinet Act.

(Delegation to Cabinet Orders)

Article 35 Beyond the provisions of this Act, necessary matters pertaining to the Headquarters are to be prescribed by Cabinet Order.

Supplementary Provisions

(Effective Date)

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

(Updating of the Legal System Necessary to Enable the Cabinet Secretariat to Appropriately Perform the Headquarters-Related Functions)

Article 2 (1) The national government is to take necessary measures, such as making updates to the legal system (including the legislation of the National

Information Security Center, which is part of the Cabinet Secretariat, as determined by the Prime Minister) in order to enable the Cabinet Secretariat to appropriately fulfill Headquarters-related functions.

(2) In taking the measures prescribed under the preceding paragraph, the national government is to examine legislative and financial measures necessary for: the fixed-term appointments of specialists as staff members or researchers in the Cabinet Secretariat; the monitoring and analysis of malicious activities against the information systems of national governmental organs through information and telecommunications networks or Electronic or Magnetic Storage media; and the development of equipment and personnel systems required for Communication and coordination with relevant domestic and foreign organizations on Cybersecurity issues, and so forth, and is to take necessary measures based on the result of these examinations.

(Examination)

Article 3 Regarding Cybersecurity incidents equating to emergencies prescribed under Article 24, paragraph 1 of the Act on the Peace and Independence of Japan and Ensuring of Security of the Nation and the People in Armed Attack Situations etc. (Law No.79 of 2003), and other malicious activities against electronic computers through information and communications networks or Electronic or Magnetic Storage Media, the national government is to examine, from a broad point of view, measures aimed at further strengthening the capability of the defense of infrastructure, which is the foundation of citizens the peoples' living conditions and economic activities and the functional failure or deterioration of which would risk enormous impacts to them.

(Partial Revision of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society)

Article 4 The Basic Act on the Formation of an Advanced Information and Telecommunications Network Society is to be partially revised by inserting the following after the "work" in Article 26, paragraph 1: "(excluding those functions related to the promotion of the implementation of important Cybersecurity-related measures for the functions listed in Article 25, paragraph 1 of the Basic Act on Cybersecurity (Act No.104 of 2014))"