サイバーセキュリティ基本法（一部未施行）
The Basic Act on Cybersecurity (Partially unenforced)

（平成二十六年十一月十二日法律第百四号）
(Act No. 104 of November 12, 2014)

目次
Table of Contents

第一章　総則
Chapter I General Provisions

（目的）
(Purpose)

第一条　この法律は、インターネットその他の高度情報通信ネットワークの整備及びデジタル社会形成基本法（令和三年法律第三十五号）第二条に規定する情報通信技術（以下「情報通信技術」という。）の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定めるとともに、サイバーセキュリティ戦略本部を設置すること等により、同法と相まって、サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。

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.

（定義）
(Definitions)

第二条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

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.

（基本理念）
(Basic Principles)

第三条　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による情報の自由な流通の確保が、これを通じた表現の自由の享有、イノベーションの創出、経済社会の活力の向上等にとって重要であることに鑑み、サイバーセキュリティに対する脅威に対して、国、地方公共団体、重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者をいう。以下同じ。）等の多様な主体の連携により、積極的に対応することを旨として、行われなければならない。

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　サイバーセキュリティに関する施策の推進は、国民一人一人のサイバーセキュリティに関する認識を深め、自発的に対応することを促すとともに、サイバーセキュリティに対する脅威による被害を防ぎ、かつ、被害から迅速に復旧できる強靱（じん）な体制を構築するための取組を積極的に推進することを旨として、行われなければならない。

(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　サイバーセキュリティに関する施策の推進は、インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用による活力ある経済社会を構築するた

めの取組を積極的に推進することを旨として、行われなければならない。
(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　サイバーセキュリティに関する施策の推進は、サイバーセキュリティに対する脅威への対応が国際社会にとって共通の課題であり、かつ、我が国の経済社会が国際的な密接な相互依存関係の中で営まれていることに鑑み、サイバーセキュリティに関する国際的な秩序の形成及び発展のために先導的な役割を担うことを旨として、国際的協調の下に行われなければならない。
(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　サイバーセキュリティに関する施策の推進は、デジタル社会形成基本法の基本理念に配慮して行われなければならない。
(5) The cybersecurity policy must be advanced taking into consideration the basic principles of the Basic Act on Forming a Digital Society.
6　サイバーセキュリティに関する施策の推進に当たっては、国民の権利を不当に侵害しないように留意しなければならない。
(6) The cybersecurity policy must be advanced with due consideration to not unjustly infringing on the rights of the people.

（国の責務）
(Responsibilities of the National Government)
第四条　国は、前条の基本理念（以下「基本理念」という。）にのっとり、サイバーセキュリティに関する総合的な施策を策定し、及び実施する責務を有する。
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").

（地方公共団体の責務）
(Responsibilities of Local Governments)
第五条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。
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.

（重要社会基盤事業者の責務）
(Responsibilities of Critical Social Infrastructure Providers)

第六条　重要社会基盤事業者は、基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

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.

（サイバー関連事業者その他の事業者の責務）
(Responsibilities of Business Entities Related to Cyberspace and Other Business Entities)

第七条　サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

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　情報システム若しくはその一部を構成する電子計算機若しくはプログラム、情報通信ネットワーク又は電磁的記録媒体（以下この項において「情報システム等」という。）の供給者は、サイバーセキュリティに対する脅威により自らが供給した情報システム等に被害が生ずることを防ぐため、情報システム等の利用者がその安全性及び信頼性の確保のために講ずる措置に配慮した設計及び開発、適切な維持管理に必要な情報の継続的な提供その他の情報システム等の利用者がサイバーセキュリティの確保のために講ずる措置を支援する取組を行うよう努めるものとする。

(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.

（教育研究機関の責務）

(Responsibilities of Educational and Research Organizations)

第八条　大学その他の教育研究機関は、基本理念にのっとり、自主的かつ積極的にサイバーセキュリティの確保、サイバーセキュリティに係る人材の育成並びにサイバーセキュリティに関する研究及びその成果の普及に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。

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.

（国民の努力）

(Efforts of the People)

第九条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

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.

（法制上の措置等）

(Legislative Measures)

第十条　政府は、サイバーセキュリティに関する施策を実施するため必要な法制上、財政上又は税制上の措置その他の措置を講じなければならない。

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

（行政組織の整備等）

(Development of Administrative Organizations)

第十一条　国は、サイバーセキュリティに関する施策を講ずるにつき、行政組織の整備

及び行政運営の改善に努めるものとする。

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

第二章　サイバーセキュリティ戦略
Chapter II Cybersecurity Strategy

第十二条　政府は、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティに関する基本的な計画（以下「サイバーセキュリティ戦略」という。）を定めなければならない。

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　サイバーセキュリティ戦略は、次に掲げる事項について定めるものとする。

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

一　サイバーセキュリティに関する施策についての基本的な方針

(i) basic guidelines for the cybersecurity policy;

二　国の行政機関等におけるサイバーセキュリティの確保に関する事項

(ii) information concerning the ensuring of cybersecurity within national administrative organs and other related organs;

三　重要社会基盤事業者及びその組織する団体並びに地方公共団体（以下「重要社会基盤事業者等」という。）におけるサイバーセキュリティの確保に関する事項

(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

四　前三号に掲げるもののほか、サイバーセキュリティに関する施策を総合的かつ効果的に推進するために必要な事項

(iv) beyond what is stated in the preceding three items, matters necessary to comprehensively and effectively promote cybersecurity policies.

３　内閣総理大臣は、サイバーセキュリティ戦略の案につき閣議の決定を求めなければならない。

(3) The Prime Minister must request a cabinet decision on the proposed cybersecurity strategy.

４　政府は、サイバーセキュリティ戦略を策定したときは、遅滞なく、これを国会に報告するとともに、インターネットの利用その他適切な方法により公表しなければならない。

(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　前二項の規定は、サイバーセキュリティ戦略の変更について準用する。

(5) The provisions of the preceding two paragraphs apply mutatis mutandis in the case of amendments to the cybersecurity strategy.

６　政府は、サイバーセキュリティ戦略について、その実施に要する経費に関し必要な資金の確保を図るため、毎年度、国の財政の許す範囲内で、これを予算に計上する等その円滑な実施に必要な措置を講ずるよう努めなければならない。

(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.

第三章　基本的施策
Chapter III Basic Policies

（国の行政機関等におけるサイバーセキュリティの確保）

(Ensuring Cybersecurity at National Administrative Organs and Related Organs)

第十三条　国は、国の行政機関、独立行政法人（独立行政法人通則法（平成十一年法律第百三号）第二条第一項に規定する独立行政法人をいう。以下同じ。）及び特殊法人（法律により直接に設立された法人又は特別の法律により特別の設立行為をもって設立された法人であって、総務省設置法（平成十一年法律第九十一号）第四条第一項第八号の規定の適用を受けるものをいう。以下同じ。）等におけるサイバーセキュリティに関し、国の行政機関、独立行政法人及び指定法人（特殊法人及び認可法人（特別の法律により設立され、かつ、その設立等に関し行政官庁の認可を要する法人をいう。第三十三条第一項において同じ。）のうち、当該法人におけるサイバーセキュリティが確保されない場合に生ずる国民生活又は経済活動への影響を勘案して、国が当該法人におけるサイバーセキュリティの確保のために講ずる施策の一層の充実を図る必要があるものとしてサイバーセキュリティ戦略本部が指定するものをいう。以下同じ。）におけるサイバーセキュリティに関する統一的な基準の策定、国の行政機関における情報システムの共同化、情報通信ネットワーク又は電磁的記録媒体を通じた国の行政機関、独立行政法人又は指定法人の情報システムに対する不正な活動の監視及び分析、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する演習及び訓練並びに国内外の関係機関との連携及び連絡調整によるサイバーセキュリティに対する脅威への対応、国の行政機関、独立行政法人及び特殊法人等の間におけるサイバーセキュリティに関する情報の共有その他の必要な施策を講ずるものとする。

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.

（重要社会基盤事業者等におけるサイバーセキュリティの確保）

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

第十四条　国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、重要な設備に係る電子計算機の被害の防止のための情報の整理及び分析を行うとともに、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。

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.

（民間事業者及び教育研究機関等の自発的な取組の促進）

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

第十五条　国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する知的財産に関する情報が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリティの重要性に関する関心と理解の増進、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

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　国は、国民一人一人が自発的にサイバーセキュリティの確保に努めることが重要であることに鑑み、日常生活における電子計算機又はインターネットその他の高度情報通信ネットワークの利用に際して適切な製品又はサービスを選択することその他の取組について、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

(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.

（多様な主体の連携等）

(Coordination with Diverse Entities)

第十六条　国は、関係行政機関相互間の連携の強化を図るとともに、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体が相互に連携してサイバーセキュリティに関する施策に取り組むことができるよう必要な施策を講ずるものとする。

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.

（犯罪の取締り及び被害の拡大の防止）

(Cybercrime Control and Prevention of Spread of Damage)

第十七条　国は、サイバーセキュリティに関する犯罪の取締り及びその被害の拡大の防止のために必要な施策を講ずるものとする。

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.

（我が国の安全に重大な影響を及ぼすおそれのある事象への対応）

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

第十八条　国は、サイバーセキュリティに関する事象のうち我が国の安全に重大な影響を及ぼすおそれがあるものへの対応について、関係機関における体制の充実強化並びに関係機関相互の連携強化及び役割分担の明確化を図るために必要な施策を講ずるものとする。

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.

（産業の振興及び国際競争力の強化）

(Enhancement of Industrial Development and International Competitiveness)

第十九条　国は、サイバーセキュリティの確保を自立的に行う能力を我が国が有することの重要性に鑑み、サイバーセキュリティに関連する産業が雇用機会を創出することができる成長産業となるよう、新たな事業の創出並びに産業の健全な発展及び国際競争力の強化を図るため、サイバーセキュリティに関し、先端的な研究開発の推進、技術の高度化、人材の育成及び確保、競争条件の整備等による経営基盤の強化及び新たな事業の開拓、技術の安全性及び信頼性に係る規格等の国際標準化及びその相互承認の枠組みへの参画その他の必要な施策を講ずるものとする。

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.

（研究開発の推進等）

(Promotion of Research and Development)

第二十条　国は、我が国においてサイバーセキュリティに関する技術力を自立的に保持することの重要性に鑑み、サイバーセキュリティに関する研究開発及び技術等の実証の推進並びにその成果の普及を図るため、サイバーセキュリティに関し、研究体制の整備、技術の安全性及び信頼性に関する基礎研究及び基盤的技術の研究開発の推進、研究者及び技術者の育成、国の試験研究機関、大学、民間等の連携の強化、研究開発のための国際的な連携その他の必要な施策を講ずるものとする。

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.

（人材の確保等）

(Development of Human Resources)

第二十一条　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る事務に従事する者の職務及び職場環境がその重要性にふさわしい魅力あるものとなるよう、当該者の適切な処遇の確保に必要な施策を講ずるものとする。

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　国は、大学、高等専門学校、専修学校、民間事業者等と緊密な連携協力を図りながら、サイバーセキュリティに係る人材の確保、養成及び資質の向上のため、資格制度の活用、若年技術者の養成その他の必要な施策を講ずるものとする。

(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.

（教育及び学習の振興、普及啓発等）

(Promotion of Education and Learning, Public Awareness Raising)

第二十二条　国は、国民が広くサイバーセキュリティに関する関心と理解を深めるよう、サイバーセキュリティに関する教育及び学習の振興、啓発及び知識の普及その他の必要な施策を講ずるものとする。

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　国は、前項の施策の推進に資するよう、サイバーセキュリティに関する啓発及び知識の普及を図るための行事の実施、重点的かつ効果的にサイバーセキュリティに対する取組を推進するための期間の指定その他の必要な施策を講ずるものとする。

(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.

（国際協力の推進等）

(Promotion of International Cooperation)

第二十三条　国は、サイバーセキュリティに関する分野において、我が国の国際社会における役割を積極的に果たすとともに、国際社会における我が国の利益を増進するため、サイバーセキュリティに関し、国際的な規範の策定への主体的な参画、国際間における信頼関係の構築及び情報の共有の推進、開発途上地域のサイバーセキュリティに関する対応能力の構築の積極的な支援その他の国際的な技術協力、犯罪の取締りその他の国際協力を推進するとともに、我が国のサイバーセキュリティに対する諸外国の理解を深めるために必要な施策を講ずるものとする。

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.

第四章　サイバーセキュリティ戦略本部
Chapter IV Cybersecurity Strategic Headquarters

（設置）
(Establishment)

第二十四条　サイバーセキュリティに関する施策を総合的かつ効果的に推進するため、内閣に、サイバーセキュリティ戦略本部（以下「本部」という。）を置く。

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

（所掌事務等）
(Affairs under Jurisdiction of the Headquarters)

第二十五条　本部は、次に掲げる事務をつかさどる。

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

一　サイバーセキュリティ戦略の案の作成及び実施の推進に関すること。

(i) preparing a draft of the cybersecurity strategy and promoting its implementation;

二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

(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

三　重要社会基盤事業者等におけるサイバーセキュリティの確保に関して国の行政機関が実施する施策の基準の作成（当該基準の作成のための重要社会基盤事業者等におけるサイバーセキュリティの確保の状況の調査を含む。）及び当該基準に基づく施策の評価その他の当該基準に基づく施策の実施の推進に関すること。

(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;

四　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティの確保の状況の評価（情報システムに対する不正な活動であって情報通信ネットワーク又は電磁的記録媒体を通じて行われるものの監視及び分析並びにサイバーセキュリティに関する重大な事象に対する施策の評価（原因究明のための調査を含む。）を含む。）に関すること。

(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));

五　前各号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

(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　本部は、サイバーセキュリティ戦略の案を作成しようとするときは、あらかじめ、国家安全保障会議の意見を聴かなければならない。

(2) In preparing a draft of the cybersecurity strategy, the Headquarters must hear the opinions of the National Security Council in advance.

３　本部は、次に掲げる場合には、あらかじめ、サイバーセキュリティ推進専門家会議の意見を聴かなければならない。

(3) In the following cases, the Headquarters must hear the opinions of the Cybersecurity Promotion Expert Council:

一　サイバーセキュリティ戦略の案を作成しようとするとき。

(i) when it intends to prepare a draft of the cybersecurity strategy;

二　第一項第二号又は第三号の基準を作成しようとするとき。

(ii) when it intends to establish the standards referred to in paragraph (1), item (ii) or (iii);

三　第一項第二号又は第三号の評価について、その結果の取りまとめを行おうとするとき。

(iii) when it intends to compile the results of the evaluation referred to in paragraph (1), item (ii) or (iii).

４　本部は、我が国の安全保障に係るサイバーセキュリティに関する重要事項について、国家安全保障会議との緊密な連携を図るものとする。

(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.

（組織）

(Organization)

第二十六条　本部は、サイバーセキュリティ戦略本部長、サイバーセキュリティ戦略副本部長及びサイバーセキュリティ戦略本部員をもって組織する。

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.

（サイバーセキュリティ戦略本部長）

(Chief of the Cybersecurity Strategic Headquarters)

第二十七条　本部の長は、サイバーセキュリティ戦略本部長（以下「本部長」という。）とし、内閣総理大臣をもって充てる。

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　本部長は、本部の事務を総括し、所部の職員を指揮監督する。

(2) The Chief engages in the overall management of the Headquarters' affairs and directs and supervises personnel at the Headquarters.

３　本部長は、第二十五条第一項第二号から第五号までに規定する評価又は第三十二条若しくは第三十三条の規定により提供された資料、情報等に基づき、必要があると認めるときは、関係行政機関の長に対し、勧告することができる。

(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　本部長は、前項の規定により関係行政機関の長に対し勧告したときは、当該関係行政機関の長に対し、その勧告に基づいてとった措置について報告を求めることができる。

(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.

（サイバーセキュリティ戦略副本部長）

(Deputy Chief of the Cybersecurity Strategic Headquarters)

第二十八条　本部に、サイバーセキュリティ戦略副本部長（以下「副本部長」という。）を置き、国務大臣をもって充てる。

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　副本部長は、本部長の職務を助ける。

(2) The Deputy Chief assists the Chief's duties.

（サイバーセキュリティ戦略本部員）

(Members of the Cybersecurity Strategic Headquarters)

第二十九条　本部に、サイバーセキュリティ戦略本部員（次項において「本部員」という。）を置く。

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

２　本部員は、本部長及び副本部長以外の全ての国務大臣をもって充てる。

(2) All Ministers of State other than the Chief and the Deputy Chief serve as members.

（サイバーセキュリティ推進専門家会議）

(Cybersecurity Promotion Expert Council)

第三十条　本部に、サイバーセキュリティ推進専門家会議（以下この条において「専門家会議」という。）を置く。

Article 30 (1) The Cybersecurity Promotion Expert Council (referred to below as the "Expert Council" in this Article) is established in the Headquarters.

２　専門家会議は、次に掲げる事務をつかさどる。

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

一　第二十五条第三項の規定により本部長に意見を述べること。

(i) stating its opinions to the Chief pursuant to the provisions of Article 25, paragraph (3);

二　前号に掲げるもののほか、サイバーセキュリティに関する施策で重要なものについて調査審議し、必要があると認めるときは、本部長に意見を述べること。

(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　専門家会議の委員は、サイバーセキュリティに関し優れた識見を有する者のうちから、内閣総理大臣が任命する。

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

（事務の委託）

(Entrustment of Affairs)

第三十一条　本部は、次の各号に掲げる事務の区分に応じて、当該事務の一部を当該各号に定める者に委託することができる。

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:

一　第二十五条第一項第二号に掲げる事務（同号に規定する監査（独立行政法人及び指定法人に係るものに限る。）に係るものに限る。）、同項第三号に掲げる事務（同号に規定する調査に係るものに限る。）又は同項第四号に掲げる事務（同号に規定する調査（独立行政法人及び指定法人に係るものに限る。）に係るものに限る。）　独立行政法人情報処理推進機構その他サイバーセキュリティに関する対策について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人

(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;

二　第二十五条第一項第四号に掲げる事務（同号に規定する活動の監視及び分析に係るものに限る。）　国立研究開発法人情報通信研究機構、独立行政法人情報処理推進機構その他当該活動の監視及び分析について十分な技術的能力及び専門的な知識経験を有するとともに、当該事務を確実に実施することができるものとして政令で定める法人

(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　前項の規定により事務の委託を受けた法人の役員若しくは職員又はこれらの職にあった者は、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用してはならない。

(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　第一項の規定により事務の委託を受けた法人の役員又は職員であって当該委託に係る事務に従事するものは、刑法（明治四十年法律第四十五号）その他の罰則の適用に

ついては、法令により公務に従事する職員とみなす。
(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.

（資料提供等）
(Submission of Materials)
第三十二条　関係行政機関の長は、本部の定めるところにより、本部に対し、サイバーセキュリティに関する資料又は情報であって、本部の所掌事務の遂行に資するものを、適時に提供しなければならない。
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　前項に定めるもののほか、関係行政機関の長は、本部長の求めに応じて、本部に対し、本部の所掌事務の遂行に必要なサイバーセキュリティに関する資料又は情報の提供及び説明その他必要な協力を行わなければならない。
(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.

（資料の提出その他の協力）
(Submission of Materials and Other Cooperation)
第三十三条　本部は、その所掌事務を遂行するため必要があると認めるときは、地方公共団体及び独立行政法人の長、国立大学法人（国立大学法人法（平成十五年法律第百十二号）第二条第一項に規定する国立大学法人をいう。）の学長又は理事長、大学共同利用機関法人（同条第三項に規定する大学共同利用機関法人をいう。）の機構長、日本司法支援センター（総合法律支援法（平成十六年法律第七十四号）第十三条に規定する日本司法支援センターをいう。）の理事長、特殊法人及び認可法人であって本部が指定するものの代表者並びにサイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関の代表者に対して、サイバーセキュリティに対する脅威による被害の拡大を防止し、及び当該被害からの迅速な復旧を図るために国と連携して行う措置その他のサイバーセキュリティに関する対策に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該求めを受けた者は、正当な理由がある場合を除き、その求めに応じなければならない。
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　本部は、その所掌事務を遂行するため必要があると認めるときは、重要社会基盤事業者及びその組織する団体の代表者に対して、前項の協力を求めることができる。この場合において、当該求めを受けた者は、その求めに応じるよう努めるものとする。

(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　本部は、その所掌事務を遂行するため特に必要があると認めるときは、前二項に規定する者以外の者に対しても、第一項の協力を依頼することができる。

(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.

（地方公共団体への協力）

(Cooperation for Local Governments)

第三十四条　地方公共団体は、第五条に規定する施策の策定又は実施のために必要があると認めるときは、本部に対し、情報の提供その他の協力を求めることができる。

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　本部は、前項の規定による協力を求められたときは、その求めに応じるよう努めるものとする。

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

（事務）

(Administrative Affairs)

第三十五条　本部に関する事務は、内閣官房において処理し、内閣サイバー官が掌理する。

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

（主任の大臣）

(Competent Minister)

第三十六条　本部に係る事項については、内閣法（昭和二十二年法律第五号）にいう主任の大臣は、内閣総理大臣とする。

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

（政令への委任）

(Delegation to Cabinet Orders)

第三十七条　この法律に定めるもののほか、本部に関し必要な事項は、政令で定める。

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

第五章　罰則
Chapter V Penal Provisions

第三十八条　第三十一条第二項の規定に違反した者は、一年以下の拘禁刑又は五十万円以下の罰金に処する。

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.

附　則
Supplementary Provisions

（施行期日）

(Effective Date)

第一条　この法律は、公布の日から施行する。ただし、第二章及び第四章の規定並びに附則第四条の規定は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。

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.

（検討）

(Review)

第二条　政府は、武力攻撃事態等及び存立危機事態における我が国の平和と独立並びに国及び国民の安全の確保に関する法律（平成十五年法律第七十九号）第二十一条第一項に規定する緊急事態に相当するサイバーセキュリティに関する事象その他の情報通信ネットワーク又は電磁的記録媒体を通じた電子計算機に対する不正な活動から、国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるもの等を防御する能力の一層の強化を図るための施策について、幅広い観点から検討するものとする。

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.

附　則　〔平成二十七年九月十一日法律第六十六号〕〔抄〕

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

（施行期日）

(Effective Date)

第一条　この法律は、平成二十八年四月一日から施行する。

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

附　則　〔平成二十七年九月三十日法律第七十六号〕〔抄〕

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

（施行期日）

(Effective Date)

第一条　この法律は、公布の日から起算して六月を超えない範囲内において政令で定める日から施行する。

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.

附　則　〔平成二十八年四月二十二日法律第三十一号〕〔抄〕

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

（施行期日）

(Effective Date)

第一条　この法律は、公布の日から起算して六月を超えない範囲内において政令で定める日から施行する。ただし、次条並びに附則第三条、第五条及び第六条の規定は、公布の日から施行する。

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.

（政令への委任）

(Delegation to Cabinet Order)

第六条　附則第二条から前条までに定めるもののほか、この法律の施行に関して必要な経過措置（罰則に関する経過措置を含む。）は、政令で定める。

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).

附　則　〔平成三十年十二月十二日法律第九十一号〕〔抄〕

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

（施行期日）

(Effective Date)

1　この法律は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。

(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.

附　則　〔令和元年五月二十四日法律第十一号〕〔抄〕

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

（施行期日）
(Effective Date)
第一条　この法律は、平成三十二年四月一日から施行する。
Article 1　This Act comes into effect on April 1, 2020.

附　則　〔令和三年五月十九日法律第三十五号〕〔抄〕
Supplementary Provisions [Act No. 35 of May 19, 2021] [Extract]

（施行期日）
(Effective Date)
第一条　この法律は、令和三年九月一日から施行する。
Article 1　This Act comes into effect on September 1, 2021.

附　則　〔令和三年五月十九日法律第三十六号〕〔抄〕
Supplementary Provisions [Act No. 36 of May 19, 2021] [Extract]

（施行期日）
(Effective Date)
第一条　この法律は、令和三年九月一日から施行する。ただし、附則第六十条の規定は、公布の日から施行する。
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.

（処分等に関する経過措置）
(Transitional Measures Concerning Dispositions)
第五十七条　この法律の施行前にこの法律による改正前のそれぞれの法律（これに基づく命令を含む。以下この条及び次条において「旧法令」という。）の規定により従前の国の機関がした認定等の処分その他の行為は、法令に別段の定めがあるもののほか、この法律の施行後は、この法律による改正後のそれぞれの法律（これに基づく命令を含む。以下この条及び次条において「新法令」という。）の相当規定により相当の国の機関がした認定等の処分その他の行為とみなす。
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　この法律の施行の際現に旧法令の規定により従前の国の機関に対してされている申請、届出その他の行為は、法令に別段の定めがあるもののほか、この法律の施行後は、新法令の相当規定により相当の国の機関に対してされた申請、届出その他の行為とみなす。

(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　この法律の施行前に旧法令の規定により従前の国の機関に対して申請、届出その他の手続をしなければならない事項で、この法律の施行の日前に従前の国の機関に対してその手続がされていないものについては、法令に別段の定めがあるもののほか、この法律の施行後は、これを、新法令の相当規定により相当の国の機関に対してその手続がされていないものとみなして、新法令の規定を適用する。

(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.

（命令の効力に関する経過措置）

(Transitional Measures Concerning Effect of Order)

第五十八条　旧法令の規定により発せられた内閣府設置法第七条第三項の内閣府令又は国家行政組織法第十二条第一項の省令は、法令に別段の定めがあるもののほか、この法律の施行後は、新法令の相当規定に基づいて発せられた相当の第七条第三項のデジタル庁令又は国家行政組織法第十二条第一項の省令としての効力を有するものとする。

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.

（罰則の適用に関する経過措置）
(Transitional Measures for Application of Penal Provisions)

第五十九条　この法律の施行前にした行為に対する罰則の適用については、なお従前の例による。

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.

（政令への委任）
(Delegation to Cabinet Orders)

第六十条　附則第十五条、第十六条、第五十一条及び前三条に定めるもののほか、この法律の施行に関し必要な経過措置（罰則に関する経過措置を含む。）は、政令で定める。

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.

附　則　〔令和四年六月十七日法律第六十八号〕〔抄〕
Supplementary Provisions [Act No. 68 of June 17, 2022] [Extract]

（施行期日）
(Effective Date)

1　この法律は、刑法等一部改正法施行日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

(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:

一　第五百九条の規定　公布の日
(i) the provisions of Article 509: the date of promulgation

附　則　〔令和七年五月二十三日法律第四十三号〕〔抄〕
Supplementary Provisions [Act No. 43 of May 23, 2025] [Extract]

（施行期日）

(Effective Date)

第一条　この法律は、重要電子計算機に対する不正な行為による被害の防止に関する法律（令和七年法律第四二号）の施行の日から施行する。ただし、次の各号に掲げる規定は、当該各号に定める日から施行する。

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:

一　附則第四条の規定　公布の日

(i) the provisions of Article 4 of the Supplementary Provisions: the date of promulgation;

二　第一条の規定、第三条中特別職の職員の給与に関する法律第一条第八号の改正規定及び同法別表第一の改正規定（「及び内閣情報官」を「、内閣情報官及び内閣サイバー官」に改める部分に限る。）、第五条、第七条、第十二条及び第十五条の規定並びに第十七条中内閣府設置法第四条第一項に一号を加える改正規定及び同条第三項第二十七号の六の次に一号を加える改正規定　重要電子計算機に対する不正な行為による被害の防止に関する法律附則第一条第二号に掲げる規定の施行の日

(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.

（サイバーセキュリティ基本法の一部改正に伴う経過措置）

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

第二条　この法律の施行の日（以下この条及び次条において「施行日」という。）前に第十三条の規定による改正前のサイバーセキュリティ基本法第十七条第一項のサイバーセキュリティ協議会の事務に従事していた者に係る当該事務に関して知り得た秘密を漏らし、又は盗用してはならない義務及び施行日前に同法第三十一条第一項第三号に掲げる事務の委託を受けた法人の役員又は職員であった者に係る当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用してはならない義務については、施行日以後も、なお従前の例による。

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.

（罰則の適用に関する経過措置）
(Transitional Measures for Application of Penal Provisions)

第三条　施行日前にした行為及び前条の規定によりなお従前の例によることとされる場合における施行日以後にした行為に対する罰則の適用については、なお従前の例による。

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.

（政令への委任）
(Delegation to Cabinet Orders)

第四条　前二条に定めるもののほか、この法律の施行に関し必要な経過措置（罰則に関する経過措置を含む。）は、政令で定める。

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.