サイバーセキュリティ基本法
The Basic Act on Cybersecurity

（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情報通信技術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、高度情報通信ネットワーク社会形成基本法（平成十二年法律第百四十四号）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　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.

（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　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.

（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) 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　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 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　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 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　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) 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　サイバーセキュリティに関する施策の推進は、高度情報通信ネットワーク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 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　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 promotion of the Cybersecurity policy is required to be carried out with due consideration not to wrongfully impinge upon the peoples' rights.

（国の責務）

(Responsibility of the 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 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.

（地方公共団体の責務）

(Responsibility 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 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.

（重要社会基盤事業者の責務）

(Responsibility of CII Operators)

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 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.

（サイバー関連事業者その他の事業者の責務）

(Responsibility of Cyberspace-Related Business Entities 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 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.

（教育研究機関の責務）

(Responsibility 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 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.

（国民の努力）

(The 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 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.

（法制上の措置等）

(Legislative and Other 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 necessary measures for the implementation of Cybersecurity policies including legislative, financial, or taxation measures.

（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 providing Cybersecurity policies, the national government is to make an effort 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 The 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 (hereinafter referred to as the "Cybersecurity Strategy") with the aim of the comprehensive and effective promotion of 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 addresses the following:

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 objectives of Cybersecurity policies;

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) matters regarding 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の促進に関する事項

(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

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 the matters listed in the preceding three items, other matters required for the comprehensive and effective promotion of 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 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　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 prescribed under the preceding two paragraphs apply 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) 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.

第三章　基本的施策
Chapter III Basic Policy

（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 of 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）第四条第十五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、国の行政機関及び独立行政法人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　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.

（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促進）

(Ensuring of Cybersecurity at CII Operators 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、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　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.

（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, Research, 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) 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　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) 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.

（多様な主体の連携等）
(Coordination with Multiple Stakeholders)

第十六条　国は、関係府省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 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.

（犯罪の取締り及び被害の拡大の防止）
(Crackdown on Cybercrime and Prevention 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 provide necessary measures to crackdown on cybercrime and prevent the spread of damage.

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

（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 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.

（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 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.

（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, 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　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, 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.

（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) 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　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) 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.

（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 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.

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 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.

（所掌事務等）
(Functions 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 will carry out the following functions:

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 the Cybersecurity Strategy and promoting its implementation.

二　国の行政機関及び独立行政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 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.

三　国の行政機関で発生した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。）に関すること。

(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).

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。

(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　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、高度情報通信ネットワーク社会推進戦略本部及び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 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　本部は、サイバーセキュリティに関する重要事項について、高度情報通信ネットワーク社会推進戦略本部との緊密な連携を図るものとする。

(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　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 are to work in close coordination with the National Security Council with regard to 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 are to consist of the Chief of Cybersecurity Strategy, the Deputy Chief of Cybersecurity Strategy, and the members of the Headquarters of Cybersecurity Strategy.

（サイバーセキュリティ戦略本部長）

(The 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、内閣官房長官をもって充てる。

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

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 is to engage in the overall management of the Headquarters' functions and the oversight of personnel at the Headquarters.

３　本部長は、第二十五条第一項第二号から第四号までに規定する評価又は第三十条若しくは第三十一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) 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　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 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　本部長は、第三項の規定により勧告した事項に関し特に必要があると認めるときは、内閣総理大臣に対し、当該事項について内閣法（昭和二十二年法律第五号）第六条の規定による措置がとられるよう意見を具申することができる。

(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).

（サイバーセキュリティ戦略副本部長）

(The 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) 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　副本部長は、本部長の職務を助ける。

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

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

２　本部員は、次に掲げる者（第一号から第五号までに掲げる者にあっては、副本部長に充てられたものを除く。）をもって充てる。

(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).

一　国家公安委員会委員長

(i) The Chairperson of the National Public Safety Commission;
二　総務大臣
(ii) The Minister for Internal Affairs and Communications;
三　外務大臣
(iii) The Minister for Foreign Affairs;
四　経済産業大臣
(iv) The Minister of Economy, Trade and Industry;
五　防衛大臣
(v) The Minister of Defense;
六　前各号に掲げる者のほか、本部長及び副本部長以外の国務大臣のうちから、本部の所掌事務を遂行するために特に必要があると認める者として内閣総理大臣が指定する者
(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
七　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者
(vii) Among experts with exceptional knowledge and experiences on Cybersecurity, those designated by the Prime Minister.

（資料提供等）
(Submission of Materials)
第三十条　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 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　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 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.

（資料の提出その他の協力）
(Submission of Materials and Other Cooperation)
第三十一条　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、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（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。）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、資料の提出、意見の開陳、説明その他必要な協力を求めることができる。

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　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、前項に規定する者以外の者に対しても、必要な協力を依頼することができる。

(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.

（地方公共団体への協力）

(Cooperation for Local Governments)

第三十二条　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 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　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) When cooperation is requested pursuant to the preceding paragraph, the Headquarters are to make an effort to meet the request.

（事務）
(Functions)
第三十三条　本部に関する事務は、内閣官房において処理し、命を受けて内閣官房副長官補が掌理する。
Article 33 The functions of the Headquarters are to be performed by the Cabinet Secretariat and managed by a designated Assistant Chief Cabinet Secretary.

（主任の大臣）
(Chief Minister)
第三十四条　本部に係る事項については、内閣法にいう主任の大臣は、内閣総理大臣とする。
Article 34 For matters pertaining to the Headquarters, the Prime Minister is to be the chief minister as prescribed in the Cabinet Act.

（政令への委任）
(Delegation to Cabinet Orders)
第三十五条　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 35 Beyond the provisions of this Act, necessary matters pertaining to the Headquarters are to be prescribed by Cabinet Order.

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 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.

（本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等）
(Updating of the Legal System Necessary to Enable the Cabinet Secretariat to Appropriately Perform the Headquarters-Related Functions)
第二条　政府は、本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備（内閣総理大臣の決定により内閣官房に置かれる情報セキュリティセンター

の法制化を含む。）その他の措置を講ずるものとする。

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　政府は、前項の措置を講ずるに当たっては、専門的知識を有する者を内閣官房において任期を定めて職員又は研究員として任用すること、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の情報システムに対する不正な活動の監視及び分析並びにサイバーセキュリティに関する事象に関する国内外の関係機関との連絡調整に必要な機材及び人的体制の整備等のために必要な法制上及び財政上の措置等について検討を加え、その結果に基づいて必要な措置を講ずるものとする。

(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.

（検討）

(Examination)

第三条　政府は、武力攻撃事態等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）第二十四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 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.

（高度情報通信ネットワーク社会形成基本法の一部改正）

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

第四条　高度情報通信ネットワーク社会形成基本法の一部を次のように改正する。第二十六条第一項中「事務」の下に「（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二十五条第一項に掲げる事務のうちサイバーセキュリティに関する施策で重要なものの実施の推進に関するものを除く。）」を加える。

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))"