

サイバーセキュリティ基本法案要綱

第一 総則

一 目的

(第一条関係)

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こと。

二 定義

(第二条関係)

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、磁気的方式その他の知覚によつては認識することができない方式（以下二において「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こと。

三 基本理念

(第三条関係)

1 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

であつて、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こと。

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止、かつ、被害から迅速に復旧できる強靱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こと。

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こと。

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こと。

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こと。

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こと。

四 国の責務

(第四条関係)

国は、三の基本理念（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こと。

五 地方公共団体の責務

(第五条関係)

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こと。

六 重要社会基盤事業者の責務

(第六条関係)

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。

七 サイバー関連事業者その他の事業者の責務

(第七条関係)

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。

八 教育研究機関の責務

(第八条関係)

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。

九 国民の努力

(第九条関係)

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。

十 法制上の措置等

(第十条関係)

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こと。

十一 行政組織の整備等

(第十一条関係)

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。

第二 サイバーセキュリティ戦略

(第十二条関係)

1 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。

ないこと。

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。

(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

(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

(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

(四) (一)から(三)まで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

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こと。

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こと。

5 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こと。

第三 基本的施策

(第十三条関係)

一 国の行政機関等におけるサイバーセキュリティの確保

国は、国の行政機関、独立行政法人及び特殊法人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。

二 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

(第十四条関係)

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。

三 民間事業者及び教育研究機関等の自発的な取組の促進

(第十五条関係)

1 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。

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。

四 多様な主体の連携等

(第十六条関係)

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

できるような必要な施策を講ずるものとする。

五 犯罪の取締り及び被害の拡大の防止

(第十七条関係)

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。

六 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

(第十八条関係)

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。

七 産業の振興及び国際競争力の強化

(第十九条関係)

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。

八 研究開発の推進等

(第二十条関係)

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。

九 人材の確保等

(第二十一条関係)

1 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。

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

キュリテイに係る人材の確保、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。

十 教育及び学習の振興、普及啓発等

(第二十二条関係)

1 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。

2 国は、1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。

十一 国際協力の推進等

(第二十三条関係)

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。

第四 サイバーセキュリティ戦略本部

一 設置

(第二十四条関係)

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。）を置くこと。

二 所掌事務等

(第二十五条関係)

1 本部は、次に掲げる事務をつかさどること。

(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。

(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。

(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。

(四) (一)から(三)まで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。

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こと。

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事。

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事。

三 組織

(第二十六条関係)

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こと。

四 サイバーセキュリティ戦略本部長

(第二十七条関係)

1 本部長は、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こと。

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こと。

3 本部長は、二の1の(二)から(四)までの評価又は七若しくは八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こと。

4 本部長は、3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こと。

5 本部長は、3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こと。

五 サイバーセキュリティ戦略副本部長

(第二十八条関係)

1 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、国务大臣をもつて充てること。

2 副本部長は、本部長の職務を助けること。

六 サイバーセキュリティ戦略本部員

(第二十九条関係)

1 本部に、サイバーセキュリティ戦略本部員(2において「本部員」という。)を置くこと。

2 本部員は、次に掲げる者(一)から(五)までに掲げる者にあつては、副本部長に充てられたものを除く。)をもつて充てること。

(一) 国家公安委員会委員長

(二) 総務大臣

(三) 外務大臣

(四) 経済産業大臣

(五) 防衛大臣

(六) (一)から(五)までに掲げる者のほか、本部長及び副本部長以外の国务大臣のうちから、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

(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

七 資料提供等

(第三十条関係)

- 1 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つて、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こと。
- 2 1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こと。

八 資料の提出その他の協力

(第三十一条関係)

- 1 本部は、その所掌事務を遂行するため必要があるときは、地方公共団体及び独立行政法人の長、国立大学法人の学長、大学共同利用機関法人の機構長、日本司法支援センターの理事長、特殊法人及び認可法人であつ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こと。

- 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きは、1の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こと。

九 地方公共団体への協力

(第三十二条関係)

1 地方公共団体は、第二の五の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こと。

2 本部は、1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。

第五 その他

一 施行期日

(附則第一条関係)

この法律は、公布の日から施行すること。ただし、第二及び第四は、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こと。

二 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 (附則第二条関係)

1 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。

2 政府は、1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。

三 検討

(附則第三条関係)

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つて、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。

四 その他

高度情報通信ネットワーク社会形成基本法の一部改正その他所要の規定を整備すること。