参考資料２

サイバーセキュリティ基本法等　関連資料

＜基本法関係＞

＜取組方針関係＞

別添1

サイバーセキュリティ基本法の概要

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒ 「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民1人1人の認識を深め、自発的な対応の促進等、強靱な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ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14条）

■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15条）

■多様な主体の連携等（第16条）

■犯罪の取締り及び被害の拡大の防止（第17条）

■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18条）

■産業の振興及び国際競争力の強化（第19条）

■研究開発の推進等（第20条）

■人材の確保等（第21条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第22条）

■国際協力の推進等（第23条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置等（第24条～第35条）

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■施行期日（第1条）

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■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（第2条）

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、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・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

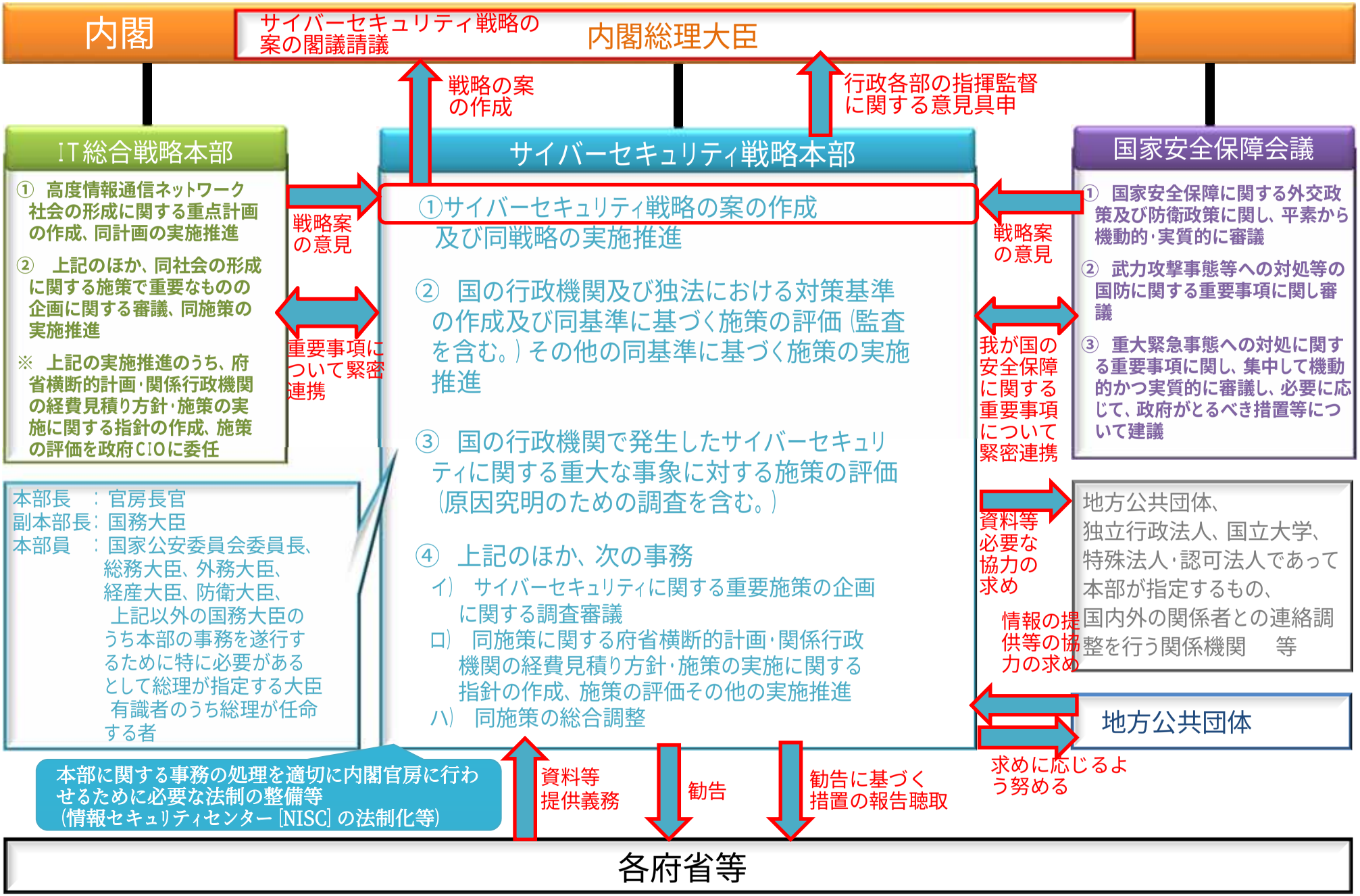
■検討（第３条）

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■IT基本法の一部改正（第４条）

⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

サイバーセキュリティ戦略本部の機能・権限



サイバーセキュリティ基本法

目次

第一章　総則

（目的）

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。

（定義）

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。

（基本理念）

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。

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。

三

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。

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。

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。

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。

（国の責務）

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。

（地方公共団体の責務）

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。

（重要社会基盤事業者の責務）

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。

（サイバー関連事業者その他の事業者の責務）

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、

五

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。

（教育研究機関の責務）

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。

（国民の努力）

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。

（法制上の措置等）

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。

（行政組織の整備等）

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。

第二章　サイバーセキュリティ戦略

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。

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　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

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。

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。

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。

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。

第三章　基本的施策

（国の行政機関等におけるサイバーセキュリティの確保）

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。

（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　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。

（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　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。

（多様な主体の連携等）

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。

（犯罪の取締り及び被害の拡大の防止）

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。

（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　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。

（産業の振興及び国際競争力の強化）

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。

（研究開発の推進等）

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。

（人材の確保等）

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。

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。

（教育及び学習の振興、普及啓発等）

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。

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。

（国際協力の推進等）

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。

第四章　サイバーセキュリティ戦略本部

（設置）

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。

（所掌事務等）

第二十五条　本部は、次に掲げる事務をつかさどる。

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　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。

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。

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。

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。

（組織）

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。

（サイバーセキュリティ戦略本部長）

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。

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。

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。

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。

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。

（サイバーセキュリティ戦略副本部長）

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。

2　副本部長は、本部長の職務を助ける。

（サイバーセキュリティ戦略本部員）

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。

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。

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　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

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

（資料提供等）

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。

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。

（資料の提出その他の協力）

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。

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。

（地方公共団体への協力）

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。

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。

（事務）

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。

（主任の大臣）

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。

（政令への委任）

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。

附　則

（施行期日）

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。

（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）

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。

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。

（検討）

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。

（高度情報通信ネットワーク社会形成基本法の一部改正）

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。

サイバーセキュリティの確保に関する件

政府は、サイバーセキュリティ基本法の施行に当たっては、次の諸点について法的措置も含めて検討を加え、その遺憾なきを期すべきである。

一　具体的な施策

1　サイバーセキュリティ戦略本部は、国家安全保障会議、高度情報通信ネットワーク社会推進戦略本部、内閣危機管理監等と緊密な連携を図ることとするほか、サイバーセキュリティに関する幅広い分野の有識者の意見を十分に取り入れ、施策に反映させるよう努めること。

2　サイバー攻撃関連情報の集約、予防策の構築並びにサイバー攻撃に対応するための演習及び訓練の企画及びその実施については、内閣官房情報セキュリティセンターを中心として総合的に実施すること。

3　内閣情報通信政策監と連携して、サイバーセキュリティに関する施策の評価を定期的に実施すること。

4　政府の各機関、重要社会基盤事業者及びサイバー関連事業者その他の事業者等における情報通信関連機器等の安全性に関する基準等については、未知の攻撃手法や

想定外の攻撃対象への攻撃にも柔軟に対応できるよう、防護対象の重要性の段階に応じたものとするなど、総合的かつ有機的な視点から策定すること。

5　大規模サイバー攻撃への対応要領を作成し、関係者の協力の下に行われる定期的な演習及び訓練を通じて実効性のある対応策の構築に努めること。

6　サイバーセキュリティ確保のため、サイバーセキュリティに関する技術の向上のための研究開発予算の充実等の取組を積極的に推進すること。

7　中小企業者その他の民間事業者におけるサイバーセキュリティの確保のための自発的な取組を積極的に促進すること。

8　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できるよう、必要な情報の提供及び助言その他の施策を積極的に推進すること。

9　地方公共団体が自主的な施策の策定及びその実施を推進できるよう、積極的な支援を行うこと。

10　内閣官房情報セキュリティセンターについては、サイバーセキュリティ対策を着実に実施するために必要かつ十分な人員、予算を継続的に確保し、サイバーセキュリティ戦略を積極的に実施すること。

11　サイバーセキュリティ戦略本部の事務のうち、監査、原因究明のための調査、府省横断的な計画及び関係行政機関の経費の見積り方針等の作成等について、迅速か

二

つ効果的に行う体制を整備すること。

二　人材の育成及び登用

1　サイバーセキュリティに関する高度かつ専門的な知識を有する人材の育成に早急に取り組むとともに、人材を関係行政機関及び民間企業等から幅広く登用するよう努め、官民の連携体制を整備すること。

2　国の行政機関等でサイバーセキュリティに係る事務に従事する者の関係府省庁及び民間企業等との積極的な人事交流を推進するとともに、過去の人事慣行にとらわれない人事評価の在り方を検討すること。

三　連携体制の整備

1　サイバー攻撃のもたらす被害の重大性に鑑み、国家安全保障会議等との連携の下、安全保障上の観点から迅速かつ実効性のある措置を講ずることを検討した上で、必要な措置を講ずること。その際には、平素から危機管理、安全保障までを連続的に対応できる体制を整備すること。

2　サイバーセキュリティに関する国際的な連携を推進するため、サイバーセキュリティに関する諸外国の政策や国内外における情勢等の分析、国際的な会議への対応等に関する十分な人員体制を確保し、迅速な情報共有と協力体制の構築を実現すること。

四　サイバー攻撃を組織的に行う集団等の動向を分析し、捜査機関等との情報の適切な共有を図ること。

五　二〇二〇年オリンピック・パラリンピック東京大会におけるサイバーセキュリティに関する事象に対処するための国内外の関係機関との連絡調整等を行う組織の在り方について、将来の推進体制を見据えて検討した上で、必要な措置を講ずること。

六　国民の基本的人権について十分に配慮しつつ、サイバーセキュリティの確保を図るため、インターネットその他の高度情報通信ネットワーク上の通信における実効ある帯域制御の在り方について検討すること。

七　立法機関及び司法機関におけるサイバーセキュリティの確保について、それらの機関からの要請に応じ、必要な協力を行うよう努めること。

右決議する。

平成二十六年十月二十三日
参議院内閣委員会

サイバーセキュリティ基本法案に対する附帯決議

政府は、本法の施行に当たり、次の諸点について適切な措置を講ずべきである。

一　サイバー攻撃関連情報の集約、予防策の構築並びにサイバー攻撃に対応するための演習及び訓練の企画及びその実施については、内閣官房情報セキュリティセンターを中心として総合的に実施すること。

二　サイバーセキュリティ戦略本部と内閣情報通信政策監との連携の下、サイバーセキュリティに関する施策の評価を定期的に実施すること。

三　政府の各機関、重要社会基盤事業者及びサイバー関連事業者その他の事業者等における情報通信関連機器等の安全性に関する基準等については、未知の攻撃手法や想定外の攻撃対象への攻撃にも柔軟に対応できるよう、防護対象の重要性の段階に応じたものとするなど、高度情報通信ネットワークの特性を踏まえた総合的な視点から策定すること。

四　サイバーセキュリティに関する高度かつ専門的な知識を有する人材の育成に早急に取り組むとともに、人材を関係行政機関及び民間企業等から幅広く登用するよう努め、官民の連携体制を整備すること。

五　サイバーセキュリティに関する国際的な連携を推進するため、サイバーセキュリティに関する諸外国の政策や国内外における情勢等の分析、国際的な会議への対応等に関する十分な人員体制を確保し、迅速な情報共有と協力体制の構築を実現すること。

六　サイバー攻撃を組織的に行う集団等の動向を分析し、捜査機関等との情報の適切な共有を図ること。

七　国民の基本的人権について十分に配慮しつつ、サイバーセキュリティの確保を図るため、インターネットその他の高度情報通信ネットワーク上の通信における実効ある帯域制御の在り方について検討すること。

八　立法機関及び司法機関におけるサイバーセキュリティの確保について、それらの機関からの要請に応じ、必要な協力を行うよう努めること。

右決議する。

別添5

「我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針」概要

1 機能強化の必要性

以下の観点から、我が国の「サイバーセキュリティ」強化のための推進体制の機能強化が不可欠

- あらゆる活動の**サイバー空間への依存の高まり**により、**リスクが深刻化**（甚大化・拡散・グローバル化）
- **「世界最高水準のIT利活用社会」の実現**が**成長戦略**の柱の1つ
- **国際的な連携の強化が必要な諸外国**においても、積極的な**体制強化**を実施
- **2020年東京オリンピック・パラリンピックに向けた対策の強化**が必要

2 サイバーセキュリティ基本法の制定

IT総合戦略本部

緊密連携

サイバーセキュリティ戦略本部
（本部長：内閣官房長官）

- サイバーセキュリティ戦略本部の所掌事務
  - ① サイバーセキュリティ戦略案の作成
  - ② 政府機関等の防御施策評価（監査を含む）
  - ③ 重大事象の施策評価（原因究明調査を含む）
  - ④ 各府省の施策の総合調整（経費見積り方針の作成等を含む）
- サイバーセキュリティ戦略本部に関する事務は、内閣官房副長官補が掌理

緊密連携

NSC（国家安全保障会議）

事務局

資料等提供義務

勧告

勧告に基づく措置の報告聴取

各府省等

3 我が国の推進体制の機能強化に向けた取組

(1) 情報セキュリティ政策会議の担ってきた機能は、サイバーセキュリティ戦略本部が担うこととなる。

(2) 内閣官房情報セキュリティセンター（NISC）を以下の組織に法制化（内閣官房組織令）する。

内閣サイバーセキュリティセンター（注）

- 内閣サイバーセキュリティセンターの所掌事務
  - ① GSOCに関する事務
  - ② 原因究明調査に関する事務
  - ③ 監査等に関する事務
  - ④ サイバーセキュリティに関する企画・立案、総合調整
- センター長には、内閣官房副長官補をもって充てる

(3) 今後、戦略本部の事務の稼働状況、オリンピック・パラリンピック東京大会開催に向けた準備、サイバー空間における脅威の増大等の諸情勢を踏まえつつ、法制の追加的な整備等について引き続き検討。

（注）英名称：National center of Incident readiness and Strategy for Cybersecurity

制度整備を踏まえた内閣サイバーセキュリティセンター（NISC）に関する主な検討事項

制度整備を踏まえ、内閣サイバーセキュリティセンター（NISC）に関して、2020年オリンピック・パラリンピック東京大会も見据えつつ、主に以下の項目について必要な措置の検討を行い、可及的速やかに結論を得る。

① GSOC機能の強化

- 新システム（2017年度～）の運用を見据えた体制、機材の整備　等

② 総合的分析機能の強化

- 諸外国の政策、サイバー攻撃の脅威情勢及び攻撃に使用された技術等の総合的な分析
- 高度な専門知識と深い知見を有する専門的人材の確保及び資質の向上

③ 国内外の情報集約機能の強化

インシデント情報の集約機能や助言機能等の強化に向けた、

- 官民連携のスキーム強化・構築
- NISC内の体制・システム整備及び能力向上

④ 国際連携の強化

- 緊急対応関連機関とのパートナーシップ構築等による国際的な窓口機能の強化

⑤ 人材の育成及び登用

- 各省庁からの出向等人材を通じ、NISC内の知見・経験を各省庁に還元
- 任期付任用や人事交流の推進等による技能を備えた人材の確保

平 成 26 年 11 月 25 日
情報セキュリティ政策会議決定

我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針

1　機能強化の必要性

情報システムや情報通信ネットワーク等により構成され、多種多量の情報が流通するインターネットその他の仮想的なグローバル空間であるサイバー空間が急速に拡大し、サイバー空間に対する社会経済活動等のあらゆる活動の依存度が更に高まりつつある。

その結果、サイバー空間を取り巻くリスクは次のように深刻化している。

・　政府機関、独立行政法人等の研究機関、重要インフラ事業者等[1]において、国の機密や技術情報の窃取などが目的とみられる標的型攻撃による脅威が顕在化する等、国家の安全保障・危機管理上の喫緊の課題として、サイバー空間を取り巻くリスクが甚大化している。

・　IoT (Internet of Things)と呼ばれる、あらゆるものがインターネットに接続される時代を迎えようとしており、スマートフォン、自動車、複合機などのモノや社会インフラにもリスクが拡散している。

・　サイバー空間には国境がなく、多種多様な主体による攻撃が世界中から我が国に対して行われており、海外において外国政府や軍の関与の可能性がある攻撃に使用された不正プログラム等が我が国でも同時期に確認されたこと等も明らかとなるなど、リスクがグローバル化している。

他方、我が国の成長戦略の柱の 1 つとなっている「世界最先端 IT 国家創造宣言」（平成 26 年 6 月 24 日閣議決定）は、「世界最高水準の IT 利活用社会」を実現することを目指している。

このような中、サイバー空間を取り巻くリスクの深刻化の現状、そして、サイバー空間の今後の更なる拡大・発展・変化を踏まえると、「世界最高水準の IT 利活用社会」の実現を通じた成長戦略及び国家の安全保障・危機管理を確固たるものとするためには、我が国において、サイバー空間を構成する情報システムや情報通信ネットワーク等において処理される情報及び実空間における重要インフラ等であって当該情報システムや情報通信ネ

[1] 「重要インフラの情報セキュリティ対策に係る第３次行動計画」（平成 26 年５月 19 日情報セキュリティ政策会議決定）において指定された事業者等及び当該事業者等から構成される団体をいう。

ットワーク等と一体化・融合しているものに関する機密性・完全性・可用性等が確保された状態である「サイバーセキュリティ」を強化するための推進体制の機能を強化することが不可欠となっている。

この点、政府方針としては、「サイバーセキュリティ戦略」（平成 25 年 6 月 10 日情報セキュリティ政策会議決定）において我が国の推進体制の強化を検討する旨を規定している。また、「「世界一安全な日本」創造戦略」（平成 25 年 12 月 10 日閣議決定）において、世界最高水準の安全なサイバー空間の構築に取り組む旨を規定しているほか、国際公共財（グローバルコモンズ）であるサイバー空間の防護が我が国の安全保障の観点からも不可欠となっていることから、「国家安全保障戦略」（平成 25 年 12 月 17 日閣議決定）においても、国全体としてサイバー防護・対応能力を一層強化するための組織の強化を推進する旨を規定している。更に、「「日本再興戦略」改訂 2014」（平成 26 年６月 24 日閣議決定）においては、情報の自由な流通の確保及びそのための IT の利用における安全性及び信頼性を確保し、成長戦略を確固たるものとするため、サイバーセキュリティに関する政府の機能について、国自らがリーダーシップを強く発揮できる推進体制への抜本的強化を図るため、法制度の在り方も含めて検討を深め、2015 年度までに法制上の措置など必要な措置を講ずる旨を規定している。

また、諸外国においても、近年、サイバーセキュリティを強化するため、その体制を積極的に強化してきている。例えば、我が国の同盟国である米国においては、2009 年 10 月に官民連携によるインシデント対応を強化するため、US-CERT 等から構成される国家サイバーセキュリティ・通信統合センター（NCCIC）を国土安全保障省に創設するとともに、同年 12 月に関連政策の統括・調整機能を強化するため、ホワイトハウスにサイバーセキュリティ調整官を設置した。米国とともに、我が国とサイバーセキュリティに関する基本的な価値観を共有する英国においても、2010 年 9 月に、政府横断的な統一性の確保及び戦略的なリーダーシップの強化のため、内閣府にサイバーセキュリティ・情報保証部を新設するとともに、2012 年夏のロンドンオリンピックにおける経験を踏まえ、2014 年 3 月に、ナショナル CSIRT として、内閣府の当該部に CERT-UK を設立した。また、仏国においても、首相府直属の国防・国家安全保障事務総局に置かれた国家情報システムセキュリティ庁の体制を 2015 年までに現在の 350 名から 500 名に拡充する計画を 2014 年 2 月に発表している。

さらに、2020 年開催予定のオリンピック・パラリンピック東京大会の開催時においては IT 利活用が飛躍的に進展していると考えられる中、これまでに経験したことのないサイバー攻撃が発生する可能性がある。2012 年夏に開催されたロンドンオリンピックでは、公式サイトに対し 2 億件以上のサイバー攻撃が発生したこと等に鑑みても、サイバーセキュリティに万全を期すための我が国の推進体制の機能強化が不可欠となっている。

2　サイバーセキュリティ基本法の制定

上記のようなサイバー空間をめぐる厳しい情勢の中、平成 26 年 11 月６日、第 187 回国会（臨時会）において、サイバーセキュリティの推進体制の強化等を内容とする「サイバーセキュリティ基本法」（以下「基本法」という。）が成立した。

今後、基本法に基づき、国家の安全保障・危機管理の観点を含め、サイバー空間の防護を図るためには、国の主導的役割（基本法第 13 条～第 23 条）を踏まえつつ、官民の関係者（国、地方公共団体を含む重要インフラ事業者等、企業、教育・研究機関及び一般利用者）がそれぞれに社会的立場に応じた役割を発揮しながら、国際連携や官民連携をはじめとして相互に連携し、共助することが必要である。なお、高度情報通信ネットワーク社会の形成を目的とし、民間が主導的役割を果たすこと等を基本理念とする高度情報ネットワーク社会形成基本法（平成 12 年法律第 144 号）の基本的な枠組みは今後とも堅持する。

国の主導的役割を果たすため、基本法により設置されるサイバーセキュリティ戦略本部（基本法第 24 条。以下「本部」という。）は、

① サイバーセキュリティの強化に係る施策に関する基本的な計画（サイバーセキュリティ戦略）の案を作成し、その実施を推進すること。

② 政府機関等におけるサイバーセキュリティに関する統一的な基準を作成し、当該基準に基づく各府省等の投資計画・実施計画及び施策の監査[2]等の評価その他の当該基準に基づく施策を推進すること。

③ 政府機関において発生したサイバーセキュリティに関する重大なインシデントに対する当該行政機関の施策について、その被害の原因究明調査等[3]の評価を行うこと。

④ 以上のほか、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、当該施策に関する府省横断的計画、関係行政機関の経費見積り方針及び施策の実施に関する指針の作成、当該施策の評価[4]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。

を所掌事務としている（基本法第 25 条第１項各号）。

また、その所掌事務の遂行に当たっては、

① サイバーセキュリティ戦略の案の策定に際し、本部は IT 総合戦略本部の意見をあらかじめ聴く仕組みとするとともに、サイバーセキュリティに関する重要事項について、IT 総合戦略本部と緊密な連携を図ること（基本法第 25 条第２項及び第３項）。

[2] 監査に当たっては、秘密の保持に配慮する。
[3] 原因究明調査に当たっては、秘密の保持や関係機関との連携・調整に配慮する。
[4] 施策の評価に当たっては、ＩＴ総合戦略本部と連携する。

② サイバーセキュリティ戦略の案の策定に際し、本部は国家安全保障会議（NSC）の意見をあらかじめ聴く仕組みとするとともに、国家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、NSC と緊密な連携を図ること（基本法第 25 条第２項及び第４項）。

③ 本部の司令塔機能を有効に発揮させるため、関係行政機関の長においては、本部に対し、サイバーセキュリティに関する資料等であって本部の審議に資するものを適時に提供するとともに、本部の求めに応じ、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提出等の必要な協力をしなければならないこと（基本法第 30 条第１項及び第２項）。

④ 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、独立行政法人、国立大学法人、大学共同利用機関法人、日本司法支援センター、特殊法人、認可法人、サイバーセキュリティ・インシデントが発生した場合における国内外の関係機関との連絡調整を行う機関等に対し、資料の提出等の必要な協力を求めることができること（基本法第 31 条第１項）。

⑤ 地方公共団体は、サイバーセキュリティに関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こと。また、本部は、この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こと（基本法第 32 条第１項及び第２項）。

⑥ 提出された資料等に基づき、本部長は、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、関係行政機関の長に対する勧告及び内閣総理大臣に対する指揮監督に関する意見具申等をすることができること（基本法第 27 条第３項及び第５項）。

が定められている。

3　我が国の推進体制の機能強化に向けた取組

上記２を踏まえ、以下のとおり、我が国のサイバーセキュリティに関する推進体制の機能強化を図る。

（1）情報セキュリティ政策会議

情報セキュリティ政策会議（以下「会議」という。）は、IT 総合戦略本部長決定により、2005 年 5 月、IT 総合戦略本部の下に設置された。会議は内閣官房長官を議長とし、議長代理である IT 政策担当大臣のほか、国家公安委員会委員長、総務大臣、外務大臣、経済産業大臣、防衛大臣及び IT 総合戦略本部長から委嘱された民間有識者から構成され、必要に応じ、構成員以外の大臣等も参加可能とされている。

会議は、３年程度を視座に据えた基本戦略を累次にわたり策定してきたところであり、現在、総理の指示により策定した「サイバーセキュリティ戦略」に基づき、会議の事務局である内閣官房情報セキュリティセンター（NISC）を通じ、様々な施策を展開している。

今般、サイバーセキュリティ基本法により本部が設置され、これまで会議が行ってきた官民における統一的・横断的な情報セキュリティ対策の推進という機能については、より強力な権限が付与された形で、法律上の根拠を持つ本部により担われることとなる。

（２）内閣官房情報セキュリティセンター（NISC）

本部が設置されることに伴い、現在、情報セキュリティ政策会議の事務局である NISC についても、サイバーセキュリティに関する政策及びインシデント対応の司令塔[5]として実質的かつ十分な権能を発揮し、本部に関する事務の処理を適切に行い（基本法附則第２条第１項）、かつ、政府全体のサイバーセキュリティの強化を総合的に推進できるよう、その制度の在り方について検討を行うことが必要である。

具体的には、サイバーセキュリティの強化に関する重要政策の基本方針の企画立案・総合調整等という特定の範囲・観点を持つ事務を一層効果的・効率的に遂行するため、それらを組織的・一体的に処理する専担の組織として「内閣サイバーセキュリティセンター（以下「センター」という。）」[6]を内閣官房に置くこととする。センターは、本部の事務局として本部の事務の迅速かつ効果的な遂行を図るために必要な措置を講じるとともに、

① 政府機関等における情報システムに対する情報通信ネットワーク等を通じた不正な活動の監視及び分析等を行う業務（GSOC[7]機能）

② 行政機関において発生したサイバーセキュリティに関する重大な事象の原因究明のための調査に関する事務

③ 行政機関におけるサイバーセキュリティの確保に関し必要な監査及び助言、情報の提供その他の援助に関する事務

④ その他のサイバーセキュリティの確保に関する企画及び立案並びに総合調整に関する事務

---

[5] 行政機関のみならず、立法機関及び司法機関におけるサイバーセキュリティの確保についても、当該機関からの要請に応じ、必要な協力を行うよう努める。

[6] 英語名は、「National center of Incident readiness and Strategy for Cybersecurity」とし、略称は NISC とする。

[7] Government Security Operation Coordination team（政府機関・情報セキュリティ横断監視・即応調整チーム）。外部からのサイバー攻撃等の情報セキュリティ問題に対して、政府機関の緊急対応能力強化を図るために整備され、2008 年４月より運用開始。

をつかさどることとし、現在の NISC の位置付け及びその担当する事務を法制（内閣官房組織令）上明確化する。

また、同センターの長である「内閣サイバーセキュリティセンター長」には、平素から事態対処・危機管理や安全保障までを連続的に対応できる体制を確保するため、事態対処・危機管理を担当し、かつ、国家安全保障局次長に充てられている内閣官房副長官補をもって充てることとする。

上記の制度整備を踏まえ、内閣サイバーセキュリティセンターに関し、2020 年オリンピック・パラリンピック東京大会も見据えつつ、主に以下の項目について必要な措置の検討を行い、可及的速やかに結論を得るものとする。[8]

① GSOC 機能の強化： 政府機関等における情報システムに対する情報通信ネットワーク等を通じた不正な活動の監視及び分析等を行う GSOC における、2017 年度からの新システムでの運用を見据えた体制強化の観点から必要な体制、機材及び施設の整備に関する具体的計画の策定・推進。

② 総合的分析機能の強化： 諸外国の政策、サイバー脅威に関する情勢、サイバー攻撃に使用された技術等の総合的な分析機能の強化並びに高度な専門知識と深い知見を有する専門家を活用する観点からの専門的人材の確保及び資質の向上。

③ 国内外の情報集約機能の強化： 政府機関、独立行政法人や重要インフラ事業者等におけるインシデント情報の集約機能や助言機能等の強化に向けた、官民連携のスキームの強化・構築や、NISC 内の体制・システム整備及び能力向上。

④ 国際連携の強化： 国際連携・国際協力担当グループの体制整備や、サイバーセキュリティに係る緊急時対応関係機関とのパートナーシップ構築等による国際的な窓口機能の強化。

⑤ 人材の育成及び登用： 各省庁からセンターへの積極的な人材出向等を通じたセンター内の知見・経験の各省庁への還元、任期付任用や人事交流の推進等による技能を備えた人材の確保。

（3）今後の取組

本方針に基づく体制整備については、順次、可及的速やかに実施する。

また、我が国におけるサイバーセキュリティを確保するための政府内の体制強化については、サイバーセキュリティ戦略本部による事務の実際の稼働状況、2020 年オリンピック・パラリンピック東京大会の開催に向けた準備、サイバー空間における脅威の増

[8] 本検討に当たっては、サイバー空間におけるカウンターインテリジェンス推進会議の取組との連携を引き続き図る。

大等時々刻々と変化する諸情勢を踏まえつつ、それらに柔軟かつ的確に対処する必要があることから、法制の追加的な整備等について引き続き検討する。

なお、本部設置後には、現行の「サイバーセキュリティ戦略」について、昨今の情勢変化を十分に勘案しつつ、必要な改定を加えた上で閣議決定を行い、今後の政府のサイバーセキュリティに係る取組姿勢等を内外に明確化することとする。