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。