平成 26 年 4 月 10 日

わが国のサイバーセキュリティ体制の強化に向けての提言

自　由　民　主　党
サイバーセキュリティ対策関係合同会議

わが国のサイバーセキュリティ体制の強化に向けて、以下のとおり提言する。

１　体制強化の必要性

サイバー空間は、インターネット等を介し、国内外における官民の多様な主体が相互に依存するグローバルな空間であり、わが国の国家安全保障、経済成長、国民生活の安心・安全にとって極めて重要な存在である。

しかしながら、サイバー空間においては、標的型メール攻撃などによる機微情報や技術情報の窃取や重要インフラ（金融、電力、鉄道など）への攻撃といったサイバー脅威の「甚大化」、スマートフォンの普及やＩｏＴ（Internet of Things）などによるサイバー脅威の「拡散」、国境を越えたサイバー攻撃などサイバー脅威の「グローバル化」が進んでいる。

安倍政権の成長戦略を確固たるものとしていくためには、世界最高水準の情報通信インフラの整備と、情報通信技術の利活用による行政、医療、教育分野をはじめ様々な分野の効率化やサービスの質の向上を目指す必要があるが、同時に、急速に高まるサイバー脅威に対処するため、サイバーセキュリティを含む情報セキュリティの強化に国を挙げて取り組むことが強く求められている。

このため、国自らがリーダーシップを従来以上に発揮できるよう、政府としてのサイバーセキュリティ体制の抜本的強化を早急に図るべきである。

２　体制強化に向けた基本的な考え方

情報通信政策の基本的枠組みを規定するＩＴ基本法（高度情報通信ネットワーク社会形成基本法）は平成１３年に制定され、「民間が主導的な役割を担うことを原則」（同法第７条）として、以降、ブロードバンド基盤の整備、インターネットや携帯端末の普及等が急速に進展し、「インターネット前提社会」が到来している。

こうした中、成長戦略を確固たるものとするためには、昨年６月に閣議決定された「世界最先端ＩＴ国家創造宣言」に基づき、あらゆる分野での情報通信技術の利活用を推進していくことが重要であり、民間の主導的な役割等を定めるＩＴ基本法の基本的枠組みは今後も堅持すべきである。

他方、ＩＴの利活用を支える情報セキュリティに関する取り組みにおいても産学官の連携が極めて重要であるが、特に政府機関等のサイバー脅威に対する防御体制の強化という国家の安全保障にも関わるサイバーセキュリティの観点からみた場合、国の主導的な役割の明確化が喫緊の課題となっている。

また、米国や英国等の諸外国においても、情報セキュリティを担う国の組織の機能強化や体制の拡充が相次ぎ図られており、わが国としても早急な対応が求められる。これは、サイバーセキュリティにおいて基本的な価値観を共有する国々における連携が不可欠な中、我が国の国益を守る上でも重要である。

さらに、国民の間では、サイバー空間が現実の生活やビジネス等の活動と切っても切り離せない存在となっていることの認識がまだまだ醸成されていない。国民一人一人が自らの問題として情報セキュリティを認識し、自らを守ることは、それに応える国内産業の活性化にもつながることが期待される。

このため、サイバーセキュリティの強化を含む情報セキュリティ政策の在り方について、基本理念、国や地方自治体等の関係者の責務、国による基本的施策、そして、これらの総合的かつ効果的な推進体制等を定めた、ＩＴ基本法の特別法ともいうべき「サイバーセキュリティ基本法」（仮称）が必要であり、スピード感を持ってこれを制定するためには、議員立法により提案することが焦眉の急である。

この基本法の制定により、政府が果たすべきサイバーセキュリティ強化に向けた姿勢を明確化するとともに、そのための体制強化を図ることが必要不可欠である。これは平成３２年開催予定の東京オリンピック・パラリンピックに向け、サイバーセキュリティ対策について万全を期す観点からも急務である。

３　サイバーセキュリティ基本法（仮称）の制定

基本法で定める基本理念、関係者の責務、国による基本的施策については、以下の内容を盛り込むことが必要である。

（１）基本理念

情報セキュリティ政策の基本理念として、以下の項目を掲げる。

① ＩＴ基本法の基本理念にのっとり、情報の自由な流通の確保及びそのための情報通信技術の利用における安全性及び信頼性の確保が、表現の自由、イノベーション、経済成長等の様々な恩恵をわが国にもたらすものであることを基本として、これらを阻むサイバー空間の脅威の深刻化に対し、官民の連携により能動的かつ積極的に対応する。

② 国民一人一人が情報セキュリティに関する認識を深め、自発的な活動が促進されるとともに、深刻化する脅威による被害を防ぎ、被害から円滑かつ迅速に復旧できる強靱な体制を構築することが重要であり、そのための取組を積極的に推進する。

③ 将来にわたり情報通信技術の恵沢を享受できるよう、その持続的な開発及び利用による創造的かつ活力ある経済社会を構築することが重要であり、そのための取組を積極的に推進する。

④ 人類共通の課題であり、わが国の経済社会の活力の向上等が国際的に密接な相互依存関係の中で営まれているため、サイバー空間における国際的な秩序の形成及び発展のための国際的協調、国際規範等の策定、信頼醸成措置の推進、開発途上国への能力構築支援の積極的な実施において、わが国は先導的な役割を担う。

（２）関係者の責務

上記（１）の基本理念を実現するためには関係者の連携が必要であり、各関係者の責務を以下のとおり掲げる。

① 国は、関係府省が最大限連携するとともに、その他の関係者と一体となって、サイバーセキュリティの強化を含む情報セキュリティに関する総合的な施策を策定・実施する。

② 地方公共団体は、サイバーセキュリティの強化を含む情報セキュリティに関する施策に関し、国との適切な役割分担を踏まえ、適切な情報セキュリティを確保するための自主的な施策を策定・実施するよう努める。

③ 重要インフラ事業者は、自らのサービスを持続的に提供するため、情報セキュリティの重要性に関する理解と関心を深め、情報セキュリティに努めるとともに、国又は地方公共団体が実施するサイバーセキュリティの強化を含む情報セキュリティに関する施策に協力するよう努める。

④　上記の他、その他の事業者及び教育研究機関等の責務について規定するとともに、国の関係機関間や関係者等との間の連携の強化に必要な施策を講ずること、サイバーセキュリティの強化を含む情報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ずること、行政組織の整備等を規定する。

（3）国による基本的施策

上記（2）の関係者の責務が十分に果たされるよう、国は以下の基本的施策を推進する。

①　行政機関及び独立行政法人等に関し、各行政機関における情報セキュリティに関する基準の整備、インターネットを通じた外部からの攻撃の監視及び分析、行政機関において発生する情報セキュリティに関するインシデント（事象）に関する演習又は訓練並びに国内外の関係者との連絡調整及び対処、行政機関等の間における情報の共有等を推進する。

②　重要インフラ事業者等に関し、重要インフラ事業者等における情報セキュリティに関する基準の整備・活用、重要インフラ事業者等の間における情報の共有、重要インフラ事業者等において発生する情報セキュリティに関するインシデントに関する演習又は訓練その他の自主的な取組等を促す。

③　企業及び教育研究機関が有する知的財産等に関する情報がわが国の国際競争力の強化にとって重要であることにかんがみ、企業及び教育研究機関が自発的に行う情報セキュリティに関する活動が促進されるよう、経営における情報セキュリティの重要性に関する理解と関心の増進、情報提供及び相談体制の整備、助言等を行う。

④　情報セキュリティを自立的に行う能力をわが国が有することの重要性を踏まえつつ、サイバー関連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、新たな事業の創出及び健全な発展並びに国際競争力の強化を図るため、情報セキュリティに関する先端的及び実用的な研究開発の推進、成果の普及、国際標準化及び評価・認証等を推進する。

⑤　大学、民間事業者等と緊密な連携協力を図りながら、情報セキュリティに係る多様な能力及び知識経験を持つ人材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、当該人材の確保、養成及び資質の向上のため、資格制度の活用及び若年技術者養成等を推進する。

⑥　国民が広く情報セキュリティに関する理解と関心を深めるよう、情報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等を行う。

⑦　情報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等を推進する。

⑧　サイバーセキュリティに関する事故等のインシデントのうちわ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のために必要な施策等を推進する。

⑨　国際的な情報セキュリティの向上を実現する観点から、我が国として積極的に国際貢献を果たすため、情報セキュリティに関する国際規範の策定及び国際標準化等に主体的に参画すること、信頼醸成措置の推進、開発途上国への能力構築支援の積極的な実施その他の国際的な連携確保のために必要な措置を講じるとともに、国際間における情報共有の推進その他の国際協力の推進等を行う。

（4）情報セキュリティ政策会議

現在、我が国のサイバーセキュリティを含む情報セキュリティ政策の重要事項は、内閣官房長官を議長とする情報セキュリティ政策会議で決定され、その事務局を内閣官房情報セキュリティセンター（ＮＩＳＣ）が担当している。

これらは平成１７年度に設置され、以降、情報セキュリティ関連の知見を蓄積してきたが法的な位置付けを持たない。各府省の情報セキュリティ対策は各々において推進することが基本であるため、ＮＩＳＣの知見を各府省において積極的に活用したり、各府省を横断する横串的機能の発揮は十分とは言えない。

このため、基本法において、現在ＩＴ総合戦略本部の下に設置され、司令塔として中核的な役割を担っている情報セキュリティ政策会議について、その機能・権限を明確化することが必要である。具体的には、情報セキュリティ政策会議は、ＩＴ総合戦略本部との連携の下、基本的な戦略の策定、各府省における情報セキュリティ対策に関する統一的な基準の作成、当該基準への準拠に関する監査、情報セキュリティ投資に関する経費見積もり方針等の策定及び重大インシデントが発生した場合の秘密の保持や関係機関との連携・調整に配意した原因究明等を担うこと等とする必要がある。

なお、これらの機能を有効に発揮させるためには、関係行政機関の長は必要な資料を政策会議に提出しなければならないこと等とするとともに、議長は、

必要がある場合には関係行政機関の長に対し勧告等を行えるようにすることなど、司令塔機能の強化を図ることが必要である。

4　組織体制の強化に向けて

上記の基本法の制定を踏まえ、政府においては、官民における情報セキュリティを一体的に推進する機能や政府機関を横断監視等する機能（ＧＳＯＣ等）を担うＮＩＳＣの法制化をはじめとする政府部内における組織体制の強化に可及的速やかに取組み、平成２７年度からの本格的な稼働を目指すことを求める。

以　　上