2012 年 5 月 31 日
民　主　党

情報セキュリティ政策の強化について

～　サイバー空間の安心・安全の確保にむけて　～

基本的考え方

情報通信技術（ICT）の発展・普及は目覚ましく、今や社会のあらゆる場面で ICT が利用されている。政府の文書は ICT によって作成・管理され、電力・ガス、航空・鉄道、金融といった社会インフラも ICT によって制御・運用がなされている。また、既に携帯端末の契約数は日本の人口を越えるなど、ほぼすべての国民が ICT に依存しながら日常生活を送っており、今後はこれがスマートフォンに取って替わるなど、社会の ICT への依存度は益々高まる一方である。

情報セキュリティは、このように「社会全体のインフラ」「インフラのインフラ」となった ICT を、安心して、かつ、安定的に利用するための不可欠な要素である。情報セキュリティが十分に確保されていなければ、国民が日常生活に不安を覚え、あるいは国家や社会経済全体が機能不全に陥る事態を招くことすらあり得ることとなった現在、情報セキュリティの確保は、国家の根幹にかかわる重要な課題である。

国際的にも、2007 年のエストニア政府機関等への DDoS 攻撃が発生して以降、サイバー攻撃に対する世界の関心は高まっている。

政府は、2010 年 5 月に「国民を守る情報セキュリティ戦略」を策定して様々な施策を推進しており、その結果、例えば、サイバー攻撃の原因となるボットと呼ばれるコンピュータウイルスについて、我が国国内のパソコンの感染率が世界でも有数の低いレベルに抑えられるなど、先進国として一定程度の水準の対策は実施されているところである。

しかしながら、昨年、標的型攻撃と呼ばれる新たな攻撃によって防衛関連企業や衆参両院の情報が窃取される、企業が保有する大量の個人情報がサイバー攻撃によって漏洩する、といった被害が次々と明らかになり、サイバー攻撃が大きな社会的問題となったことは記憶に新しい。この事実は、我が国の情報セキュリティ対策が十分な水準に達しておらず、まだまだ取り組むべき課題が多いことを表しており、その一因として、政府全体としての情報セキュリティ政策の重要性が確立されておらず、政治レベルでの専担の責任者が明確に定まっていないことが指摘されている。

このような状況を踏まえ、政府は、情報セキュリティ政策の優先度を一段格上げし、重点的な取組みを早急に実施することによって、国民が安心して ICT の利便を享受できる高度な情報セキュリティ環境を整備するとともに、世界に信頼される「情報セキュリティ先進国」としての地位を早期に確立し、将来にわたり維持していくべきである。

なお、政策の推進に当たっては、情報セキュリティの確保を追求するあまり、過度な規制によって企業や国民の社会経済活動を萎縮させることがないよう、十分な配慮が必要である。情報の自由な流通の確保を基本原則とし、ICT の利活用を促進するために如何に情報セキュリティを確保するかという視点に立って政策を推進することが必要である。

また、情報セキュリティの諸課題は日々進化・変化するため、情報セキュリティ政策については、常に更新していくことを前提とし、定期的・継続的に検証を行う仕組みを確立することが必要である。党としても、今後とも随時その時々の状況を検証し、必要な提言を行っていく。

1　体制の整備（司令塔機能の強化）

①　縦割りの排除と責任体制の明確化

政府は、政府全体の情報セキュリティ政策の司令塔として、2005 年より情報セキュリティ政策会議（議長：官房長官）及び内閣官房情報セキュリティセンター（NISC）を設置して情報セキュリティ政策を推進してきているが、依然として各省庁の縦割りが排除し切れておらず、政府全体として十分な連携・調整が図られているとは言いがたい状況である。

そこで当面は、総理に進言、意見具申ができる「総理補佐官（政務）」の職務として新たに情報セキュリティ政策を追加することにより、情報セキュリティの確保に関する責任を有する政務を補強し、重要度を一段格上げする。

また、この分野は、高度な専門的知識が不可欠であることから、米国のオバマ政権が政権発足後の 2009 年 12 月に、民間企業の CISO の経験もあるハワード・シュミット氏をサイバーセキュリティ調整官として指名したように、当該総理補佐官を専門的見地から補佐するための「内閣特別顧問（又は内閣官房参与）」を民間企業、学識経験者から任命することが必要である。

これらの総理補佐官、内閣特別顧問は、内閣官房情報セキュリティセンターを活用し、官房長官、担当官房副長官を補佐しつつ情報セキュリティ政策の強化を図っていくべきである。

今後、情報セキュリティの確保がさらに重要になってくることに鑑み、各府省庁横断的な司令塔機能を強化するため、官房長官の職務を助け、安全保障を含むサイバー空間の安全・安心の確保に責任を総合的に有する「官房副長官（政務）」を新設することも検討すべきである。

②　国際社会における日本のリーダーシップの発揮

国際社会においては、サイバー空間のルールに関する議論が活発化しており、情報セキュリティもその重要なテーマの一つとして国際的な議論が深められている。こうした中、諸外国は首脳や閣僚が戦略的に情報発信を行っており、我が国としても、総理や閣僚が、我が国の顔として、日本ならではのメッセージを国際社会に対して発信すべきである。

また、併せて、先述の総理補佐官、内閣特別顧問は、国際会議等に積極的に参加し、我が国の立場について効果的に発信するとともに、我が国の責任者として諸外国との調整を行うことが必要である。

２　重点政策分野

（１）新たな脅威への対応

③　官民連携による情報共有・高度解析機能の整備

昨今、標的型メール攻撃や新しいタイプの攻撃（APT: Advanced Persistent Threats）などサイバー攻撃が高度化している。こうした高度な攻撃の具体的な手法を明らかにするためには、官民関係者がそれぞれ把握できる情報を結集し、それらに対して高度な解析を加える必要がある。

政府において、昨年 10 月以降官民の情報共有ネットワークの構築などの取り組みが推進されているが、総務省・経済産業省が関係機関と連携して高度解析機能を充実させるなど本スキームの更なる充実に努めるとともに、官側における迅速・効率的な連携・情報共有がなされるなど実効性のあるシステムを構築すべきである。

また、民間側からの情報収集に重点が置かれる傾向にあるので、官民連携を実効あるものにするため、政府は官側からの積極的な情報提供に努めるべきである。

④　新たな防御モデルの確立

サイバー攻撃の高度化に伴い、従来の境界防御的発想では十分に信頼性が確保できなくなってきているため、③で述べた高度解析機能の整備によって得られた解析結果や、研究開発の成果なども活用しつつ、多層防御、出口対策、攻撃予知などを含む新たな発想に基づく、「新たな情報セキュリティ防御モデル」を早急に確立し（ニュー・ディペンダビリティの確保）、ガイドライン等を策定すべきである。

⑤　新手の攻撃に対する対処能力の向上や高度人材の育成・発掘

④で確立された防御モデルに基づき、情報システム・ネットワークの管理・運用に携わる ICT 人材がセキュリティの能力を身につけることができるよう、また、高度な情報セキュリティ技術を有する者を育成・発掘するため、政府として、例えば、実践方式での演習や、高度な技術を有する者の育成・発掘を目的とした「ハッカー・コンテスト」など、セキュリティ能力に関する育成支援策を検討すべきである。

また、既存の様々な ICT に関する資格制度について、新たな情報セキュリティ上の脅威や⑥に述べるような新たなサービスや技術に適応できるよう、随時見直しを行うべきである。

⑥　スマートフォン、マルチファンクションプリンターなど新たなサービスや技術に関する情報セキュリティ対策の確立

スマートフォンの急速な普及が進む一方で、スマートフォンを対象としたマルウェアの増加が報告されるなど、情報セキュリティ上の脅威が高まっている。また、現在、インターネットにおいて、新しい通信方式である IPv6 への対応が世界的に行われつつある。さらに、政府機関や企業等において、プリンターやコピー機をネットワークに接続して使用するマルチファンクションプリンター（MFP）の普及が進んでいる。スマートフォンやクラウドサービス、IPv6、MFP など新たに出現した情報通信サービスや技術について、情報セキュリティ上の課題や対応策を早急に検討すべきである。

⑦　災害時における情報セキュリティの確保

東日本大震災を踏まえ、物理的なバックアップシステム等の構築に加え、拠点の分散化等、災害時にも強靭な情報セキュリティシステムの構築に努めるべきである。

（２）ICT 産業における情報セキュリティ分野の重点化

⑧　情報セキュリティ分野に対する研究開発の重点化

政府の報告書によれば、2010 年度の情報セキュリティ研究開発費は、48.6 億円と 2006 年度(91.2 億円)に比べて約半分と大幅に減少している。一方、米国の研究開発費は、2007 年度から 2011 年度まで増加傾向にあり、5 年間で 91%程度増加し、2010 年度は 366 億円となっている。情報セキュリティ技術の重要性は、益々高まっているにもかかわらず、わが国の研究開発予算は大幅に減少しており、先進国の潮流に逆行している。政府は、情報セキュリティ研究開発予算の大幅増額を図るべきである。特に、能動的で信頼性の高い情報セキュリティの確保に資する研究開発に重点的に取り組む。その具体化のため、実践的な研究開発とそのための環境整備、及び研究開発成果の実用化に取り組むべきである。

総務省・経産省連携の下で推進した、ボットウィルス対策プロジェクトである「サイバークリーンセンター（CCC）」事業は、ボット感染率の大幅な低下を実現するとともに、世界的にも高い評価を得ている。本プロジェクトの継続的な推進を図るべきである。

情報セキュリティの研究開発分野では、（独）情報通信研究機構（NICT）は、インシデント分析センター（nicter）の開発など重要な役割を果たしている。現在、総務省、NICT が推進している国際連携によるサイバー攻撃予知・即応

技術の研究開発は、我が国におけるサイバー攻撃のリスクを軽減する取り組みであり、国際連携を一層促進するとともに、必要な予算の確保に努めるべきである。

⑨　政府調達における情報セキュリティ対策の実施

我が国の情報セキュリティレベルを向上させるためには、ICT 産業全体の活性化を通じ、その基盤となる情報セキュリティ分野の底上げを図ることが不可欠である。現状は、情報セキュリティに関連する企業は、外資系企業が多いのが実態であるが、我が国も世界を先導する情報セキュリティ技術などを有している。こうした技術を広く活かしていくためには、各主体が情報セキュリティ対策だけを目的とした個別対応に終始するのではなく、ICT を最大限に活用するという戦略を立て、それを安定的・確実に構築・実行するために必要な要素として情報セキュリティ対策を導入していくという考え方が重要である。

情報セキュリティ分野の重点化を図るためには、政府自身が率先して情報システムの調達において十分な情報セキュリティ対策を実施することが必要である。このため、政府の情報システムを再度検証するとともに、情報セキュリティ強化に資するシステムの増強を図るための予算等を計上し、政府統一基準を踏まえた調達を推進するべきである。

⑩　情報セキュリティ投資を促進するための税制

情報セキュリティ対策の重要性は認識していても、具体的な対策が進展しない大きな要因として、情報セキュリティ投資に関するコストの問題がある。とりわけ、情報セキュリティ投資に過重なコスト負担が難しい中小企業にとって深刻である。脆弱な情報システムが一部存在すれば、国全体の情報セキュリティを確保することが困難となるなどの観点も踏まえ、民間企業の情報セキュリティ対策を促進するため、中小企業の情報セキュリティ投資を促進する税制を維持すべきである。

（３）公的分野の対策強化

⑪　政府機関における情報セキュリティ対策の強化

政府は、情報セキュリティのための政府統一基準群、CISO 等連絡会議、情報セキュリティに係る年次報告書を策定するなど政府機関の情報セキュリティ対策に努めているが、情報セキュリティ上の脅威の高度化に十分対応できているとは言えない。民間企業ではなされている対策が政府ではなされていない

場合も多く見られるとの民間からの指摘なども踏まえ、政府は自ら率先して民間企業などよりも一層高度な情報セキュリティ対策を実施すべきである。そのためには、外部の専門家の知見等も活用し、⑨にも述べたとおり、政府の情報システムを再度検証するとともに、情報セキュリティ強化に資するシステムの増強を図るための予算等を計上し、政府統一基準を踏まえた調達を推進すべきである。

また、包括的なネットワーク監視やデータの収集・分析機能等の充実を図るとともに、それらを踏まえた対処マニュアルの作成、政府職員の教育訓練などについて所管を明確にした上で実施すべきである。また、各府省庁の CISO はその責務を再認識すべきである。

さらに、各府省庁の業務継続計画（BCP）において、代替施設等における情報セキュリティ対策が講じられていない場合も見受けられているところ、BCP においても情報セキュリティの観点を反映させるべきである。

また、政府における対応と同様に、衆議院、参議院の事務局は、情報セキュリティ対策の強化に努めるべきである。

⑫　安全保障面の情報セキュリティ政策の確立

2010 年 12 月に策定された「平成 23 年度以降に係る防衛計画の大綱」には、「サイバー攻撃への対応」などが謳われているが、昨今のサイバー攻撃事案や今後のサイバー攻撃の脅威の増大などを踏まえると、安全保障面から見た情報セキュリティ対策を強化すべきである。防衛省は、サイバー空間防衛隊（仮称）の整備等に取り組んでいるところであるが、最近の状況を踏まえ、サイバー攻撃に対処するための体制、対策の充実に努めるべきである。また、安全保障面の観点からソフトウェア、ハードウェアの在り方を検討すべきである。

また、サイバー攻撃等悪意のある活動の明確化に向け、カウンターインテリジェンスの観点から取り組みを行っている、インテリジェンス・コミュニティの知見の活用を含めた関係省庁との情報収集・分析、情報共有の在り方について検討を行うべきである。

更に、国際的に見ると、米国・国防総省がサイバー空間を空・陸・海・宇宙に次ぐ第５の作戦領域として位置づけ、集団的なサイバーセキュリティを強化するため同盟国や友好国との強固な協力関係を築くこと等を内容とした戦略を発表し、国連においても政府専門家会合を設置して情報セキュリティの領域における脅威や協力手段等について検討が行われるなど、安全保障面でのサイバーセキュリティを巡る国際的な議論が活発化している。我が国としても、我が国の安全保障・国益を確保するという視点に立って、こうした国際的な議論に積極的に参加・貢献することが求められる。

また、こうした国際的な議論の動向を踏まえつつ、悪意ある攻撃によって国

民の生命・財産が脅かされたり、国民の社会経済活動が重大な脅威にさらされたりするような有事を想定し、例えば、多段階の警戒レベルを設定し、それぞれのレベルにおいて必要な対応を行うなど、適切な対応の在り方について国内的な検討を進めるべきである。

⑬　重要インフラ分野等の情報セキュリティ対策の強化

情報通信、金融、電力や航空、鉄道、物流などの重要インフラ分野は、国民生活と密接に関係するため、情報セキュリティ対策の強化に努めるべきである。官民の情報共有体制として、平成 21 年以降セプターカウンシルなどの取り組みがなされているが、制御系システムに対する情報セキュリティ上の脅威が高まっていることなどもあり、再度、情報システムを検証するなど、技術進展等を踏まえた PDCA を促進すべきである。重要インフラ事業者間の連携を図るため、分野横断的なサイバー演習などを強化すべきである。また、東日本大震災の教訓を踏まえた事業継続計画（BCP）等の充実に取り組むべきである。さらに、これらの取組が着実に実施されるようガイドラインを策定する等、適切な枠組みを検討すべきである。

制御系システムの情報セキュリティについては、経済産業省において既に取り組んでいるが、一層の充実を図るべきである。

⑭　地方公共団体の情報セキュリティ対策の強化

中央省庁に比べて、地方公共団体の情報セキュリティ対策は十分とは言えない。地方公共団体は、情報システムの情報セキュリティ対策の強化に努めるべきである。その際、規模の小さな地方公共団体においては、自治体クラウドの活用なども検討すべきである。また、自治体業務の ICT 依存が高まる中、サイバー攻撃等への対応や災害時の業務継続について課題が見られることから、ICT 業務継続計画（ICT-BCP）ガイドラインの見直しを図るとともに、地方公共団体における ICT-BCP の策定を促進すべきである。

⑮　サイバー犯罪に対する体制の強化

サイバー攻撃の発生状況や手口に関する情報収集・分析及び違法行為に対する捜査のための体制を強化するとともに、必要な資機材の充実、外国治安情報機関との連携強化等を図るべきである。また、サイバー犯罪に関連した省庁間及び出先の法執行機関との連携を強化するべきである。

（４）社会全体への情報セキュリティ意識・対策の浸透

⑯　企業における情報セキュリティ対策の促進

企業経営者が情報セキュリティのリスクを理解・認識し、適切な対策を実施することを促すため、例えば、産官学全てに適用できるガイドラインの策定・活用、サイバー攻撃等を受けた際の調査・報告や公表、セキュリティ強度を可視化するための基準の策定など、具体的な方策について検討し、実施すべきである。

⑰　情報セキュリティに関する普及啓発の充実

政府は、2 月を「情報セキュリティ月間」と定め、情報セキュリティに関する普及啓発に取り組んでいるが、国民が情報通信技術を利用する際に最も不安に思う項目は、情報セキュリティと個人情報保護であることから、予算措置を含め、更なる普及啓発活動の充実に努めるべきである。その際、高齢者のインターネット利用が増加していることなどを踏まえ、高齢者の方々にも容易に理解して頂ける普及啓発活動の充実を図るべきである。

⑱　小中学校及び高等学校における情報セキュリティに関する教育の充実

高等学校の情報科教育において、情報セキュリティに関する教育を推進するべきである。また、小中学校においても、情報セキュリティを含む情報リテラシー教育を適切に実施すべきである。

さらに、教員等の学校職員自身の情報セキュリティに関する能力向上を図るべきである。

（５）国際連携・国際協力の強化

⑲　国際連携の推進

情報は、国境を越えて自由に流通することから、サイバー攻撃への対処に当たっては、国際連携を強化することが極めて重要である。二国間協議や多国間協議の場を通じて、具体的な国際連携方策を模索すべきである。

まずは、インターネットエコノミーに関する日米政策協力対話や日 EU インターネットセキュリティフォーラム、日 ASEAN 情報セキュリティ政策会合等において、情報の流通に関して基本的考え方を同じくする国々との連携を強化し、情報セキュリティに関する各国との情報共有・分析や具体的な国際共同プロジ

ェクトを進めるべきである。

また、⑫で述べたとおり、安全保障面での国際的な議論にも積極的に参加・貢献することが求められる。

⑳　新興国・発展途上国の情報セキュリティ対応体制の整備支援

新興国・発展途上国において、対外・対内調整を担う CSIRT（Computer Security Incident Response Team）の体制強化の支援及び連携強化等を図るべきである。

㉑　国際標準化の推進

スマートフォンやマルチファンクションプリンターなど新たな情報通信サービスに関する情報セキュリティ上の課題は、国、地域に関わりなく発生する共通の課題であることから、国際的な情報交換等を通じた国際連携の強化や、国際標準化の取組を推進すべきである。