高度情報通信ネットワーク社会推進戦略本部　情報セキュリティ政策会議
第34回会合　議事要旨

１　日時

平成25年5月21日（火）　8：40～9：40

２　場所

総理大臣官邸２階小ホール

３　出席者（敬称略）

安倍	晋三	内閣総理大臣
菅	義偉	内閣官房長官
山本	一太	情報通信技術（ＩＴ）政策担当大臣
古屋	圭司	国家公安委員会委員長
岸田	文雄	外務大臣
小野寺	五典	防衛大臣
茂木	敏充	経済産業大臣
		（平　将明経済産業大臣政務官代理出席）
遠藤	信博	日本電気株式会社代表取締役執行役員社長
小野寺	正	KDDI株式会社代表取締役会長
土屋	大洋	慶應義塾大学大学院教授
野原	佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田	雅英	首都大学東京法科大学院教授
村井	純	慶應義塾大学教授

（その他出席者）

加藤	勝信	内閣官房副長官
世耕	弘成	内閣官房副長官
杉田	和博	内閣官房副長官
米村	敏朗	内閣危機管理監
櫻井	修一	内閣官房副長官補
古谷	一之	内閣官房副長官補
遠藤	紘一	政府ＣＩＯ
徳田	英幸	内閣官房情報セキュリティ補佐官
篠田	陽一	内閣官房情報セキュリティ補佐官

４　議事概要

(1)　総理大臣冒頭挨拶

私は、「世界最高水準のＩＴ国家」として、国民一人ひとりが、ＩＴの恩恵を実感できる社会の実現に取り組んでいる。そのような社会は、「力強く」、「活発」であるとともに、「安全」で「安心」できるものでなければならない。

昨今、「サイバー攻撃」が現実のものとなり、国家や重要インフラはもとより、広く国民がその脅威にさらされるようになった。今後、この脅威が一層深刻化すると見込まれる中にあって、「国家の安全保障」や「危機管理」の観点からは勿論、「国民生活の安定」と「経済の発展」のために、速やかに、かつ、強力に対応していく必要があると認識している。

私から皆様に、その取組方針の策定をお願いしていたところ。本日、「世界を率先する、強靭で活力あるサイバー空間を構築する」ための「サイバーセキュリティ戦略」を取りまとめいただくことに、厚く御礼申し上げたい。

今後、内閣が一丸となって、具体的な取組を進め、「世界最高水準のＩＴ国家」にふさわしい「安全なサイバー空間」の構築を目指してまいりたい。

(2)　討議

・　「サイバーセキュリティ戦略（案）」（パブリック・コメント案）について（決定）

・　「サイバーセキュリティ２０１３」の策定について

・　その他

上記について、事務局より資料に基づき説明が行われるとともに、構成員より意見が述べられた。

○　安全・安心な社会は、日本が世界に誇ることのできるものである。

現在、刑法犯認知件数は減少し、国民の安心感に関する各種の調査結果も改善するなど、治安情勢は一時期と比較して改善した。その理由の一つに、小泉政権下における犯罪対策があり、治安に対する政府の役割の大きさを示している。

改善したといえる治安情勢にあって、現在最も重要な課題はサイバー空間の安全・安心の確保である。今回の戦略は、今まさに政府が取り組むべき課題に応えたものであり、取りまとめに敬意を表する。

その中でも、特にサイバー空間におけるログの保存の検討は大変重要な課題であり、戦略に盛り込まれたことは画期的な意義がある。この課題を扱う上では、関係省庁が密接に連携し、急ぎすぎることなく、できる限りの検討を行わなければならない。

また、予算の確保についても目配りされている。この分野では、民間との技術力の共有等の協力が重要であり、我が国の強さの源でもあることから、是非進めてもらいたい。

なお、一見無関係に聞こえるかもしれないが、今後は女性の力によって日本を変えていく、という視点を持つことも重要になると考えられる。現在、女性の力の活用により、警察は良い方向へ大きく変化している。同様に、情報セキュリティの人材についても、女性の活用を進めてもらいたい。

○　今回の戦略では、これまでの「情報セキュリティ」という言葉を「サイバーセキュリティ」という言葉に改めた。

元来、サイバー空間という言葉は、現実空間と対比して、時間的・空間的な制約を受けない新たな別の空間を意味するために生まれた。しかし、この本質的にグローバルな空間であるサイバー空間と、ドメスティックな空間である現実空間とは、今や互いに融合し、一体となった。行政用語として「サイバー空間」を使い始めた意味は、サイバー空間は基本的にグローバルな空間であり、したがって、サイバー空間の安全を考える場合、ドメスティックな意味における我が国の安全に加え、グローバルな意味では、どこかから攻めてくることに対する安全ということもあるが、日本人が世界で活躍する際の安全に責任を持たなければならないということでもある。世界全体のグローバルな安全に対する我が国の貢献が必要である。そのため、サイバー空間に関する我が国の考えを世界に発信し、コミュニケーションをし、最高の見本になっていかなければならない。

特に、我が国はサイバー空間と現実空間の融合における先進国であり、インターネット普及率が 80%を超え、既に公共空間にセンサーネットワークが張り巡らされ、スマートフォンが広く一般に普及しているほか、農業、医療、教育、家庭、交通といった分野でもＩＴの浸透が進んでいる。加えて、我が国は、民間、行政、個人が互いに協力していくことができるという強みも持っている。したがって、マルチステークホルダーである関係者全てが、力を合わせて安全なサイバー空間を作り上げることで、我が国の安全を確保するとともに、世界の見本となることで、我が国が世界の安全に対して負うべき責任を果たしていかなければならない。

また、この場の各大臣におかれては、サイバーセキュリティを担う人材として、行政機関においてサイバーセキュリティを担う専門家のあり方について、検討して欲しい。現在は、現場の専門性が持続せず、国際的に調整している時にも２～３年も経過すれば担当者が異動し、代わる。我が国がサイバーセキュリティに関して、外交の場を通じて世界に発信していくに当たり、行政官の中にサイバーセキュリティに関する専門性と外に対する発信力を兼ね備えた持続的な人材が必要であり、それを育てるための体制が重要である。

○　先の国連報告にあるとおり、サイバー戦争を想定する国家が増加する情勢の下、「サイバーセキュリティ戦略（案）」を策定し、「サイバーセキュリティ立国」という我が国の方向性が明確になったことは意義深い。本戦略は、バランス良く、内容の濃いものであるが、今後３年間を目途に実行するものであり、これからが本番である。この後策定する年次計画では、本戦略と各省庁の取組との関係を明確化することで、国民に対し方向性を分かりやすく示して欲しい。その上で、本戦略の実行に際して３点の意見を述べる。

第一にＮＩＳＣの機能強化やサイバーセキュリティセンターへの改組について、国の中央機関が各省庁と連携するため、権限と実行能力の確保を進めてもらいたい。

第二に、サイバー攻撃対策における情報共有について、既に J-CSIP 等の枠組が稼働しているが、サイバー攻撃に対し各主体が先手を打って対応することを可能とするため、

官主導で国内の情報共有について更なる態勢の強化をしてもらいたい。また、最近の日米サイバー対話に見られるように、国家間の情報共有も重要であり、日米間で脅威情報の共有はもとより、サイバー攻撃対策技術の開発について、互いに分担することを検討してもらいたい。さらに、アジアにおける我が国の位置づけも重要であることから、技術や人材育成等の分野でリーダーシップを示し、太いパイプ作りに努めてもらいたい。

第三に、評価等について、３年後に更なる実力をつけるため、今回の戦略で打ち立てたKPIを活用し、我が国の方向性を示してもらいたい。

○　現在、サイバー空間では、日々新たな攻撃が発生し、しかも攻撃の手法が高度化している。この実態を国民に知らせるため、国民の注意を適切に喚起しなければならない。今回、これまでの「情報セキュリティ」という言葉を「サイバーセキュリティ」という言葉に改めたことで、適切に国民の耳目を引くことができる。

今回の戦略では、「情報の自由な流通の確保」を第一に掲げている。「情報の自由な流通」は、事業を国際展開する上での前提として不可欠であり、産業界にとって死活問題である。特に、電気通信業界においては、国際電気通信連合（ITU）等の場において、「情報セキュリティ」の名前の下で不合理な規制を行おうとする国家も見受けられており、これらの国々に対し、我が国が「情報の自由な流通の確保を前提とし、その上での情報セキュリティの確保が必要である。」という方針を示したことは、事業者の立場として力づけられる。その上で、サイバーセキュリティについても他の産業政策と同様、我が国の顔の見える外交が必要である。現在、サイバーセキュリティに関する各種の国際会議が開催される中、我が国政府からの高官出席は少ないことから、今後は政府が積極的に外交を進め、我が国のサイバーセキュリティのあり方を表明してもらいたい。

また、情報セキュリティ産業の活性化については、この分野においては主に海外企業が先端技術を保有することから、我が国はこれら海外企業保有の先端技術を使いこなすことが求められる。したがって、国内の情報セキュリティ産業を活性化するとともに、海外の企業とのつきあい方を検討することが重要である。

なお、我が国の大学等における現在の教育制度は、セキュリティに限らずソフトウェア全般について弱い。是非、我が国のソフトウェア教育全体を変えてもらいたい。

○　今回の「サイバーセキュリティ戦略（案）」は全般的に踏み込んだ内容となっており、取りまとめに敬意を表する。

第一に、サイバー空間の外交・防衛について、防衛については防衛省を中心に、外交については外務省を中心に検討し、踏み込んだ内容を示してもらった。現在、日米サイバー対話、１０月に開催されるサイバー空間に関するソウル会議等において、サイバー空間の問題を扱う上での「信頼醸成措置」がキーワードとなっている。今回の戦略により、我が国のサイバーセキュリティ戦略が示されたことで、会議の場において発信することができるようになったと評価できる。

第二に、人材の育成について、特に、突出した人材の発掘・育成に触れてあり、大学として高い目標が求められることに、身が引き締まる思いである。経済産業省、総務省と協力し、取り組んでいきたい。

第三に、ＮＩＳＣの強化に関して、秘密を守ることのできない国は、諸外国から信頼されないものであり、安全保障・外交の観点からも、政府の情報セキュリティの強化が必要とされている。現在、体制の強化方法として複数の案が提出されているが、顔の見える情報セキュリティの担い手が重要であることから、ＮＩＳＣを中心とした強化にしてもらいたい。

○　これまでとは次元の異なる取組が必要であるとの認識の下、「サイバーセキュリティ戦略」の名前を採用し、グローバルコミュニケーションと顔の見える外交、各々の組織がインシデント情報を共有する取組を盛り込んだこと等、良い戦略となった。

その上で、３点について意見を述べる。

第一に、「基本的な考え方」の部分に関して、「情報の自由な流通の確保」を掲げる上で、表現の自由の観点にとどまらず、「イノベーションの促進」、「オープン性の確保」、「相互運用性の確保」といった観点も是非盛り込んでもらいたい。これらは米国等に見られる論点であり、本戦略においても、サイバー空間の発展等が論点として含まれているものの、基本的な考え方において適切に位置づける必要があると考える。

第二に、一般利用者の役割に関して、現在の情報セキュリティの原則は、各インターネット利用者が自立的に情報セキュリティの確保に取り組む、というものである。この原則は重要であるが、「サイバー空間の衛生」にも触れられているとおり、一般のインターネット利用者による自助努力のみでは、今や対応が困難である。そこで、一般のインターネット利用者の取組を述べる箇所においても、同様に「自助努力のみでは困難」である旨に触れ、自助努力の上では関連事業者等が提供する情報やサービスを利用することが重要である、という結論とするべきである。

第三に、人材育成に関して、現在、戦略本文中には、16 万人の技術者において情報セキュリティスキルが不足しており、追加の教育・訓練を必要としていること、さらに８万人の潜在的な人材不足がある、という点が指摘されている。このように、現状において既に人材の不足は喫緊の課題である旨指摘しているにもかかわらず、戦略中に見える施策には即効性が不足していると感じる。そのため、現状の記述に加え、即効性のある人材育成施策を追加してもらいたい。

○　安倍総理よりの、「ＩＴ政策の立て直し」についての指示を踏まえ、3 月 28 日、第二次安倍政権発足後、初めての「ＩＴ総合戦略本部」が開催され、新たなＩＴ戦略の策定に向けた議論を開始した。

新たなＩＴ戦略の素案を議論・検討するため、「ＩＴ総合戦略本部」の下に「ＩＴ戦略起草委員会」を設置し、計４回開催し、検討を行っている。

情報セキュリティの強化については、ＩＴの利活用を支える不可欠な要素であるので、新たなＩＴ戦略にもその旨しっかり明記していきたい。

また、ＩＴ政策の司令塔機能を強化するために本国会に提出している政府ＣＩＯ法案については、先日５月９日に衆議院本会議において可決され、参議院に送付された。本法案で設置される内閣情報通信政策監は、ＮＩＳＣと連携し、政府情報システムを統合・集約化し、サイバー攻撃等に対するセキュリティ機能の強化を図るなど、より安全な政

府機関の情報システムの構築に向けた取組を進めることとなる。
　今後とも、この法案をできるだけ早期に国会で成立させ、政府ＣＩＯに政府の情報システムの統合・集約化を進めてもらい、ＮＩＳＣとの連携をとるよう努めてまいりたい。

○　本戦略の目的である「サイバーセキュリティ立国」の実現には、社会・経済活動の根幹をなすサイバー空間の安全・安心に対する国民の信頼を確保することが不可欠である。
　警察としては、人材育成等により捜査力及び解析力を強化するとともに、サイバー攻撃分析センター、サイバー攻撃特別捜査隊、不正プログラム解析センターの拡充等による体制整備を図り、サイバー犯罪等への対処能力の向上を図ることが喫緊の課題である。また、日本版ＮＣＦＴＡの創設やセキュリティ関連事業者等との情報共有を推進することにより、民間事業者等の持つ高度な知見を活用した取組を強化してまいりたい。
　併せて、有識者の御発言にもあったとおり、通信履歴の保存等による「匿名性の壁」を克服するための新たな取組等についても、関係省庁と密接な連携を図り、その理解を得ながら、実現に向けて着実に歩みを進めてまいりたい。

○　５月９及び１０日に開催された日米サイバー対話では、脅威認識の共有、重要インフラ防護をはじめとするサイバー領域での具体的対処の在り方及び国際的なルール作りなどの幅広い事項について議論し、二国間及び国際的なサイバー問題に関する幅広い協力を深化させることができた。日米同盟の抑止力を高めるため、引き続き政府一体となった協力を推進してまいりたい。
　国際的なルール作りに関しては、国連においてサイバー空間に関する政府専門家会合（国連サイバーＧＧＥ）に我が国は参加しており、６月に第３回会合が開催され、最終報告書がまとめられる。また、１０月に開催されるサイバー空間に関するソウル会議等のサイバー関連国際会議にも積極的に関与し、国際的な連携を推進してまいりたい。

○　本年２月、防衛副大臣を委員長とする「サイバー政策検討委員会」を設置し、今年度末に発足予定の「サイバー防衛隊（仮称）」の設立準備室を先週設置した。
　これから、安全保障の面で、国民の負託に応えるためのインフラ整備において対応することが重要である。
　現在、安全保障問題では、日米が密接に連携して対応している。その際、日本のサイバー対応がしっかりしていなければ、日米同盟、ひいては安全保障にも影響を与える。そのため、このレベルを上げることは、大変重要である。また、安全保障の問題においては、少なくとも我が国自体が人材育成、技術開発に、より貢献しなければならないとの危機感を持ち、今後とも積極的に貢献していきたい。

○　日本にとって「重要なインフラ」をサイバー攻撃から守る仕組みが、今回のとりまとめに盛り込まれていることは、大変重要である。
　経済産業省の独法のＩＰＡ（独立行政法人情報処理推進機構）は、企業・国民のセキュリティ対策を促進していく専門機関として、ノウハウを蓄積している。
　ＩＰＡでは、重工業・電力・ガス・石油・化学のインフラ５業界について、サイバー

攻撃を受けた情報を集約し、共有していく仕組みを構築した。１年間で２５０件の情報を集約し、共有している。これにより、新型ウイルスの攻撃が発覚した際、その日のうちに、他のインフラ企業にも情報共有したことで、複数企業に同種の攻撃を発見し、情報流出を未然に防ぐことができた事例もある。こうした取組も参考としつつ、重要インフラ事業者に対する対策を具体化するに際し、積極的に貢献してまいりたい。

また、本年４月、巧妙化する攻撃に備え、宮城県の多賀城市に、世界最先端のセキュリティ検証施設を構築した。同施設に、ＩＰＡ、産総研や我が国インフラメーカ等が集結し、模擬的なサイバー攻撃などによって、インフラ機器の弱点を検証し、克服する研究開発を開始した。こうした施設は日本と米国にしかない。今後、日米両国が連携して取組を進め、グローバルなセキュリティの評価機関確立を目指す。

(3)　自由討議

構成員から以下のような意見が述べられた。

○　これまで、ＩＴ政策は、情報産業・通信産業が主体だった。現在、ＩＴは医療、教育、家庭、交通といった分野に広がり、社会のインフラとしての意義が増している。関係する省庁も広がっており、そのため、いわゆる横串と呼ばれる政策が必要になっており、内閣が果たすべき役割が大きくなっている。サイバー空間は、全ての場所、全ての人、全ての産業において、新たなものを生み出す、我が国の基盤となった。したがって、今後の課題として、情報セキュリティについても、社会の全てのセグメントが参加できるようにしなければならない。

また、今後は世界中の国際会議において、サイバー空間に関する我が国の考え方が問われることとなる。そうした場では、必ず専門家が説明する必要があるが、まさに政府ＣＩＯがそうした役割を果たすべきであり今後は政府ＣＩＯが重要な会議に参加することのできる体制作りが必要である。

○　今回の戦略はこれでまとまったと思うが、将来更に検討を進める上での課題は、我が国の「情報」や「秘密」に関する考え方が旧態依然としていることである。インテリジェンスに関する問題やセキュリティクリアランスに関する問題に対し、我々はいずれ取り組む必要が出てくるであろう。

これまで、我が国においてはこれらの問題を検討する上で、半歩前に出ただけで強い批判にさらされる状況であった。しかし、現実空間とサイバー空間がつながった中で、「情報」や「秘密」を従来と同様の考え方の中で捉えることはできない。

是非将来の課題として、これら「情報」の考え方の問題に対して、政府として本格的に取り組んで欲しい。ただし、情報セキュリティ政策会議以外の場での検討となるのかもしれない。

○　現在、ＩＴ総合戦略本部において策定中の新たなＩＴ戦略については、従来、ＩＴ戦略はＩＴ戦略本部決定の形を採っていたが、今回は閣議決定の形を採り、ＩＴ立国を創造するための宣言となる予定である。これを打ち立てる上では、サイバーセキュリティ

は重要であり、今後有識者の知恵を借りてどのようにしていくかについて検討を進めたい。

また、ＩＴ総合戦略においては、国際戦略についても盛り込まれており、御指摘のとおり政府ＣＩＯが重要な国際会議に出席できるように強調することを検討したい。

さらに、国際的な信頼を守るためにも、秘密を守ることのできる国となるよう、ＩＴ総合戦略の観点からも検討を進めたい。

○　有識者の発言にあったとおり、ほとんどのインフラがサイバー空間と接続する時代となった。その結果、これまでのようなスタティックな対応とは異なり、リアルタイムのダイナミックな対応が必要となっている。その際、最も重要なのは情報の共有化と方向性の一元化であり、官民の間、官と官の間で情報の偏在・重複を避け、集約・共有した上で、ＮＩＳＣ等が中心となって方向性を示し、各省庁がそれに従うようにしなければならない。

○　本戦略では、ログの保存等の内容にも踏み込んだ。３・４年前とは環境が大きく変化しており、技術的にも大きな進歩があったことから、事業者への過大な負担も避けることができると考える。そのため、関係省庁が連携し、信頼関係を築いた上で、ログの保存に関する検討に取り組むことが重要である。

また、サイバーセキュリティを考える上では、いかにして民間の知見を活用していくかが重要である。民間の技術者を非警察官として任期制で雇用したり、手口分析について外部に嘱託したり、といったことは現在でも実施しているが、今後はもっと踏み込む必要があると考えている。

さらに、行政機関における情報セキュリティの専門性のレベルアップについては、有識者構成員御指摘のとおり非常に重要であると考える。そのためにも、日本版ＮＣＦＴＡを作るべきであり、協力を願いたい。

なお、日本版のデフコンであるSECCONについては、今年の２月に開催され、ハッキングの技術を持った学生等に対し、警察からもその技術力の活用を呼びかけたところである。今後も、突出した技術力を持つ者を積極的に活用していきたい。

○　通信の秘密について、現在、研究会等において議論を行っているが、御指摘のとおり状況は大きく変化している。従来、電話や電子メールの通信内容を第三者に知られてしまうという恐怖感が大きかった。しかし、近年は通信内容とは別に、ヘッダ等の送信者・受信者等の宛先情報を分離して確認することが可能になってきている例もある。このような新たな技術を用いた対応は、我が国の大きな武器ともなりうることから、検討してもらいたい。

○　従来、通信の秘密は、通信事業者に対して法律上の強い制約として働いてきた。しかし、現在の「通信の秘密」の概念は、電話の時代に構成されたものであり、インターネットの時代となった現在、そもそも何が秘密として保護され、何をオープンな情報として扱って良いかといった事項すら、不明確である。

したがって、通信の秘密に関し、不明確な部分を整理することで、事業者が対策を実施しやすくなると期待される。

○　サイバーセキュリティ戦略には、我が国の企業が国際的に展開する上での戦略の観点が盛り込まれている。そこで、ＩＴ総合戦略においても、是非我が国の企業が国際的に展開する際の外交や支援のあり方の観点を盛り込んで欲しい。

○　本日は、限られた時間にも関わらず、非常に有意義なご意見をいただいたことを、深く感謝申し上げる。

総理からの指示を受けて、検討を進めてきた「新たな戦略」について、本日、「サイバーセキュリティ戦略」のパブリック・コメント案として取りまとめることができた。この間、有識者の皆様には、何度もお集まりいただき、草案を作成いただくなど、大変お世話になったことを厚く御礼申し上げる。

今後、内閣官房を中心に、各府省庁連携の下、この「サイバーセキュリティ戦略」を着実に実行し、成果を上げられるよう取り組んでまいりたい。引き続きよろしくお願いしたい。

－　以上　－