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33回会合　議事要旨

１　日時

平成25年3月26日（金）　16：30～17：20

２　場所

総理大臣官邸２階小ホール

３　出席者（敬称略）

菅　　義偉	内閣官房長官
山本　一太	内閣府特命担当大臣（科学技術政策）
古屋　圭司	国家公安委員会委員長
新藤　義孝	総務大臣
	（柴山　昌彦　総務副大臣代理出席）
茂木　敏充	経済産業大臣
	（赤羽　一嘉　経済産業副大臣代理出席）
小野寺 五典	防衛大臣
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
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
佐々木 豊成	内閣官房副長官補
遠藤　紘一	政府CIO
佐々木 良一	内閣官房情報セキュリティ補佐官
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

⑴　討議

・　新たな情報セキュリティ戦略について

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

○　新たな情報セキュリティ戦略の方向性について、有識者構成員の間の議論について説明する。

まず、環境変化として、サイバー空間と実空間の融合・一体化について、この背景には、①インターネット普及率が８０％となるなど情報通信技術が普及し、あらゆる分野の基盤が完全なデジタル化を遂げ、その上で生活や産業等が成り立っていること、②ビッグデータ、IoT や M2M など次々と新しい技術が発展し変化が激しいこと、そして、③グローバルにも発展を遂げていることがある。サイバー空間は地球全体がインターネット等によりつながる空間であり、実空間は国土があって、生活や行政等がある空間である。この２つの空間が生活の中で、ＩＴ利用の普及により融合・一体化したことが一番大きな背景である。これが、経済・産業の牽引力となり、重要なＩＴ戦略の成果となっている。

一方で、サイバー空間においては、リスクが甚大化・深刻化しており、①国家・重要インフラ・医療等の情報化により、我々の命や健康に関わるような問題にも展開している、②基盤の発展によりリスクが拡散しており、広がる関係者による総力を挙げた対応が必要となっている、③サイバー空間のリスクは、サイバー空間には国境がないためグローバル化し、また、情報社会が縦割り社会を横に繋いでしまうことによりボーダレス化する。

○　環境変化を踏まえた対応として、４つの基本方針を掲げている。

一つ目として、セキュリティのために情報の流通を制限することなく、情報の自由な流通を「安全に」確保すること、二つ目として、縦割り社会の横をつなぐことにより、深刻化する新たなリスクへの対応が重要であるということ、三つ目として、これへの賢い対応として、リスクベースによる対応が重要であり、質の高い産官学の人材やその体制を有機的に利用した対応が必要ということ、四つ目として、サイバー空間はマルチステークホルダーであり、相互依存する官・公・学・産・民の全てが、他人事ではなく、自らの社会的責務を踏まえた行動するということが重要であり、そのための環境・体制整備をすることが基本的な方針である。

○　この４つの基本方針の下、官・公・学・産・民の各主体がそれぞれ異なる役割を有しながら、横につながって力をあわせる必要がある。このため、内閣において、この問題を議論し、環境を整備していくことがとても重要になる。

具体的には、

①　国としての役割として、グローバル空間における国際関係における外交メッセージの中で、サイバーセキュリティやサイバースペースのポリシーが議論されることがとても多くなっている。このため、各大臣又は各外交現場の中で、サイバー空間でのポリシーやサイバーセキュリティに関する取組についての統一的なメッセージを出すことが重要になる。また、国の役割である国を守ることとしてグローバル空間のサイバー

セキュリティが議論される視点を持つことが重要であり、実空間でのグローバル空間とナショナル空間を超えた所で、犯罪対策や防衛について考え、それらの体制を整備することが必要である。そして、これに対応した研究開発等の中長期的な施策も国の責任である。

② 重要インフラ事業者については、情報化の進展に伴い、ますますエネルギー政策等の様々な基盤が情報基盤と共に発展をしていく。例えば、電子行政やスマートグリッドに対するサイバー攻撃への対応を重要インフラ事業者等の役割として明確化することが必要である。

③ 企業や教育・研究機関のようないわば頭脳に当たるところが、きちんと利用されるところが国際競争力を高めるが、これらが情報を安全・安心して利用できる環境を整備するということが重要である。

④ あらゆるステークホルダーがそれぞれの力をもっており、我が国の情報の利用者は、クオリティが高いということを常々誇りとしているが、その中で、情報セキュリティに対する対応を若い時から伝えていくことが重要である。情報のシステムが１００％破壊、攻撃されない社会を作ることはできないが、これらが起こった時にどのような回復力を示すかが知恵の見せ所であり、優れた頭脳の人々が力を合わせる自律的な協調・自律的な役割が重要である。

⑤ 情報通信事業者に全てを任せるのは一番危険な考え方であり、全ての主体が自律的な責任を担い、それぞれの役割を果たすことが重要である。

○ 取組分野については、サイバー空間に対して、我が国の国土や生活の中にレジリエンスとしての回復力等が強化された安心・安全な世界をつくるための政府や起業における対策、サイバー空間の防衛や犯罪対策、そして、衛生が重要である。特に、サイバー空間の衛生については、社会にトラストをつくることであるが、特に認証制度は、きちんとしたエンドースとその運用があって初めてトラストが得られる。何かが起きた時に認証が取り消されるということが起こらなければトラストは得られない。こういった意味において、サイバー空間の衛生という仕組みや制度整備はとても重要である。

また、活力あるサイバー空間は、サイバー空間の発展に内外から貢献するということである。安心の技術を日本で作れば、世界中が安心な情報社会を作っていくことに貢献していくことになる。このことが産業、人材、リテラシーの向上においてとても重要な役割を果たす。非常にレベルの高い技術に支えられた社会をつくることが重要である。

さらに、外交、国際展開、国際連携において、それぞれの具体的な対象や場で、サイバー空間のセキュリティの問題が議論され、メッセージとなるような戦略をつくることが重要であり、我が国の共通のメッセージを作っていろんな場面で利用して頂く方向で戦略を考えること必要がある。

⑵ その他の構成員意見

その他の構成員から以下のような意見が述べられた。

○ グローバルなサイバー空間で、ボーダレスなセキュリティリスクがあるものの、国単

位の組織や制度で対応していることを踏まえるべきである。
　また、欧米や日本は国際的な会議等では情報の自由な流通を確保すべきとしている。これに対してサイバー空間を管理したいという国々もあり、しっかりと対応していかなければならない。そして、セキュリティ対策はＴＰＯに応じてしっかりと自由度を持たせる体制を作り、かつ、リスクベースは柔軟に適切に対応していく必要がある。

○　ボーダレスなセキュリティリスクに対応する中で、情報を適切に共有していく体制をしっかり構築する必要がある。また、縦割りの省庁等の組織の壁を取り払って全体的に情報共有体制を整理していく必要がある。

○　国際的に認証されている分野において、新たな認証制度を国が独自に作ってしまうのではなく、国内のベンダが日本国内においても認証を取りやすい環境を整備し、海外へ出て行けるようにすることが重要である。

○　環境の変化について、最近は国家機関が攻撃の主体となっている場合が多数有り、そのことが国民感情の不安感をあおっている。危機管理の観点からもフェーズが変わったといえる。それら環境の変化に対する基本的な方針を作成しなければならない。

○　資料１の１頁の基本的な方針について、特に②「リスクの深刻化への新たな対応」に記載のように、今までの取組と異なる新たな対応が必要と考える。国家がサイバー攻撃を仕掛けてくるという事態に対して、国は責任を持って国民を守らなければならない。また、③「リスクベースによる対応」について、あらゆることに対応するとコストが掛かりすぎるかもしれないが、他方、国民にとっては、問題が起こったときに対応してもらえるということが重要であり、想定外と言うことはできない。原因が解明されないことは何より困ることである。

○　各主体の役割の明確化について、今までは国には限界があるので民間企業に頑張ってもらい国はその手伝いをするという構造であったが、これからの方向性として国が主体になるよう変わらなければならない。

○　取組分野について、フォレンジックも大事であるが、サイバー空間の犯罪対策の観点から、証拠保全が非常に重要である。また、国土の強靭化が大事であり、これからはサイバーがその要となり、産業発展に繋がらなければならない。日本が世界一安全なサイバーの技術を持っていると言われることが、今後、外交の上でも非常に重要になってくる。

○　今後、我々がサイバー空間をいかに積極的に使っていくかということが成長戦略になる。一方で、ネットワークのブロードバンド化、コンピューティングパワーの増大がリアルタイム性を帯びたサービスを作り上げており、e-government、e-education 等の分野でもっと活用していかなければならない。また、システムの製造の観点からシステム

のパーツ、ユニット、システム全体の認証制度を作り上げるとともに、その標準化をグローバルに進めていく必要がある。そして、サイバーセキュリティ立国として日本の技術力を発揮し、グローバルでリーダシップを取れる能力を付けていくということが重要である。

○　新戦略を実現させるに当たっては、人材育成を中長期に考えなければならない。今後は、現在の有限な能力のある人材をいかに有効に使うか、情報をどうやって共有化させるかというシステムをしっかりと作り上げなければ新戦略も実行できない。また、民間を含む人材の連携をとって方向感を作り出すことが重要である。

　さらに、人材の育成では、大学や民間においての教育の中でシステムを構築しないと答えが出ないのではないか。人材は新戦略を実行する上で非常に重要なアイテムであるので、有効な在り方を示す必要がある。

○　従来は、ＤｏＳ攻撃やフィッシング詐欺のようなものが多かったが、今回の韓国の例に見られるように明らかに重要インフラや政府系の情報システムを狙った攻撃に変わってきており、我々が想定している以上に環境が大きく変化している。環境変化をしっかりと認識する必要がある。

○　重要インフラに対する攻撃が非常に重大な問題となりつつある。近い将来、韓国のような事案が我が国でも発生する可能性があるのではないかと認識している。重要インフラに対する攻撃をどれだけ未然に検出できるかという点が大きな要素である。残念ながら我が国では検出技術の開発があまり進んでいないが、早期に検出し、対応するという取組を進めていかなければならない。そういう意味で、重要インフラ防護のための方向性について明確に定めて行く必要がある。情報通信技術を利用している重要インフラ事業者の情報システムの防護方策については、電気通信事業者が政府と協力して提案していかなければならない。

○　資料１の２頁の⑤「情報通信関連事業者等による自浄的・自立的な役割」とのタイトルに違和感を覚える。情報通信関連事業者等は、サイバー空間の一部しか見ていないのに、国民は情報通信関連事業者等がサイバー空間を守ってくれると認識してしまうのではないか。

○　リスクベースの対応強化に当たり、サイバー空間においてどのような脅威があるのかを明確にしなければ、どのような対策を講じればよいのか理解できないように思う。

○　タリンマニュアルのルール１「主権」に「国家はその領域内においてサイバーインフラ及びその活動に関してコントロールを行使できる」と記載されている。サイバー空間において主権をどこまで行使できるのかという点が非常に重要な問題となってくると思う。

○　通信の秘密の過剰な保護はやめた方が良いと思う。現時点でもある程度のことはできるようだが、サイバー犯罪やサイバー攻撃の予防を目的として通信を傍受するのは、現行法制下では難しいように感じている。ほとんどの諸外国が既に行っていることなので、我が国においても検討すべきである。

○　セキュリティクリアランスの制度を確立することができれば、海外捜査機関との情報共有が一気に進む。我が国ではこれが不十分であるために友好国との情報共有もうまく行うことができていない。

○　産業競争力会議においても高度人材の育成が取り上げられているように、ＩＴの利活用を促進し、裾野を広げていかなければ、ＩＴ人材を育成することはできない。本日、サイバー攻撃に対応する人材の育成についても議論がなされたが、安倍政権のＩＴ戦略を総合戦略としてまとめていく中で活かしていきたい。また、政府ＣＩＯ法案を国会に提出しているところ、政府ＣＩＯとＮＩＳＣの関係をしっかりと整理していきたい。

○　遠隔操作ウイルス事案のような新手の犯罪にも適確に対処することが重要である。このために、「サイバー犯罪対処能力の強化等に向けた緊急プログラム」を発表した。同プログラムのポイントは、警察の捜査力及び解析力の強化と民間の知見の最大限の活用である。具体的には、一つには、手口等に関する技術的助言等を得るために民間事業者等を非常勤嘱託として積極的に雇用すること。二つには、米ＮＣＦＴＡへ捜査員を派遣して知識・技術を高めること。三つには、警察庁及び各都道府県警察においてサイバー犯罪捜査等に従事する専門捜査員の人員増を図ること。四つには、高度な専門知識を有するハッカー等の協力を確保し、捜査に有益な情報を得ること。

　省庁の壁を越え、緊密な連携を図りながら、新たな取組を着実に進めていく一つの方法として、以前、前田委員よりご指摘のあった、通信履歴（ログ）の保存は、「匿名性の壁」を克服するための有効な手段と考えている。

○　防衛省は、国家間の攻撃の中で直接攻撃を受ける可能性がある。現在部隊の運用については、クローズド系で運用しているが、今後、様々な脅威が想定されることから、参考２に記載のとおり、平成 25 年度予算においてサイバー攻撃対処のための経費を計上し、サイバー空間防衛隊を創設するとともに、その人材育成を進め、専門的な対処をしてまいりたい。

○　総務省では、参考１に記載のように、情報の自由な流通の確保と、それを阻害しない程度の過度な規制によらない信頼できるサイバー空間の構築を両立させていきたいと考えている。また、動的防御プロセス連携を確立し、ＰＤＣＡサイクルを待たずして、発生した問題に対して常に適時適切に意志決定をしていくことが必要である。さらに、事故前提社会という意識の下で、個人、中小企業に対しても自立的な対応を促すという仕組み作りを講じることも必要である。総務省としては、国際連携、官民の知恵の結集、省庁間の連携をキーワードとして取組を強化してまいりたい。

○　経済産業省では、これまでもＩＰＡをハブとして、重要インフラにおける情報共有体制を整備してきたところであるが、更に拡充・深化させていきたいと考えている。加えて、サイバー攻撃に対しても JPCERT/CC を通じ、国際的な連携を適確に実施する。こうした取組を引き続き推進するとともに、新戦略では産業振興という観点も重要であると考えている。具体的には、CSSC による制御システムのセキュリティ強化を推進していきたい。また、高度な知識・技術を持つ情報セキュリティ人材の育成が何よりも重要であると考えており、しっかりと対応していきたい。

○　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きましたことを、深く感謝申し上げる。有識者構成員の皆様方には、引き続き新たな情報セキュリティ戦略の起草に御尽力いただくようお願いしたい。

－　以上　－