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40回会合　議事要旨

１　日時

平成26年7月10日（木）　13：15～14：00

２　場所

総理大臣官邸４階大会議室

３　出席者（敬称略）

菅　　義偉	内閣官房長官
古屋　圭司	国家公安委員会委員長
上川　陽子	総務副大臣
岸　　信夫	外務副大臣
武田　良太	防衛副大臣
亀岡　偉民	内閣府大臣政務官
田中　良生	経済産業大臣政務官
小野寺　正	KDDI株式会社代表取締役会長
中谷　和弘	東京大学大学院法学政治学研究科教授
林　紘一郎	情報セキュリティ大学院大学教授
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）

世耕　弘成	内閣官房副長官
杉田　和博	内閣官房副長官
西村　泰彦	内閣危機管理監
遠藤　紘一	内閣情報通信政策監
髙見澤 將林	内閣官房副長官補
古谷　一之	内閣官房副長官補

４　議事概要

(1)　議長冒頭発言

大変お忙しい中御出席いただき、感謝申し上げる。

サイバー空間を取り巻く情勢は、ますます厳しくなっている。平成25年度における政府機関への脅威の検知件数は、前年度比５倍の約508万件に急増しており、サイバーセキュリティ対処能力の強化が喫緊の課題となっている。

このような情勢を踏まえ、国会においては、サイバーセキュリティ基本法案を御審議いただいているところ、政府としては、同法案の早期成立を強く期待するとともに、盤石の態勢を構築するため、サイバーセキュリティ推進体制の充実強化を進めていく必要がある。

各構成員の皆様におかれては、このような観点から、活発な御議論をお願いする。

(2)　討議

【討議事項】

・　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(案)

【決定事項】

・　情報セキュリティ研究開発戦略(改定版)(案)
・　新・情報セキュリティ普及啓発プログラム(案)
・　サイバーセキュリティ政策に係る年次報告(2013年度)(案)
・　サイバーセキュリティ2014(案)

【報告事項】

・　高度サイバー攻撃対処のための取組等

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。

○　５点申し上げる。

第一に、サイバーセキュリティ基本法が次の国会で無事成立すれば、世界に誇れるサイバーセキュリティ法、新しいサイバーセキュリティの国際標準になるといっても過言ではない。今後、途上国や新興国のサイバーセキュリティ政策について、日本がキャパシティビルディング、能力構築に一層貢献することが求められるが、基本法はその際の基軸となるものである。

第二に、サイバーセキュリティ基本法のもとでサイバーセキュリティ戦略本部にはサイバーに関するハブ機能として、ＮＳＣ及びＩＴ戦略本部との緊密な連携が求められることになる。緊密な連携が真の意味で成功するためには、さまざまな配慮や工夫がなされる必要があり、例えばサイバーセキュリティ戦略本部とＮＳＣの関連会議との合同開催等も視野に入れて欲しい。

第三に、サイバーセキュリティ基本法では、独立行政法人等に対しても資料等必要な協力が求めることができるところ、日ごろからサイバーセキュリティ対策への十分な理解を促し、いざというときに円滑な協力が得られるよう、一層丁寧な説明を心がけられたい。

第四に、新聞では大手電力事業者がWindowsＸＰのパソコン約４万8,000台を使用し

て、今後も５年間使用を続けるという報道があった。来年９月までに新しいＯＳに更新する旨の追加報道もあり、少しは安心したものの、電力システムのサイバー攻撃による大規模停電等の甚大なリスクがある懸念される。

国際空港でＸＰを使っているという報道もあり、重要インフラ事業者でこのようなことがないかどうか、改めて点検と適切な対応をお願いしたい。ネットにつながなければいいという考え方は安易で危険である。また、Windows Server 2003 のサポートも来年７月に終了するため、企業の更新が遅延することのないよう、今から注意喚起を強化していただきたい。

第五に、官職の名称について、事務局からは「サイバーセキュリティ官（仮称）」を示されているところ。「サイバーセキュリティ戦略官」や「サイバーセキュリティ審議官」といった名称の方が、役職の名称であることが理解しやすいと思われる。いずれにせよ、「サイバーセキュリティ」という名称を広めていくためにも、官職名の中に含ませるべきである。

○　３点申し上げる。

第一に、本日の討議事項である「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(案)」は、早急に決定する必要がある。そのためにも、できるだけ早期にサイバーセキュリティ基本法案が成立することを期待する。

第二に、マイナンバーのシステム整備におけるセキュリティ対策について。マイナンバーのシステム整備が進められており、自治体においてもシステムの調達が始まっている。

このシステム整備に際しては、Security By Design の考え方が不可欠である。現在、各自治体の情報システムについては、あくまで各自治体に閉じたシステムを前提にした情報セキュリティガイドラインが整備されている状態であるが、マイナンバーのシステム整備に際しては、外部との情報連携が行われることを前提とする必要がある。このため、責任分解点や連携の際のセキュリティ確保のあり方について、早急にガイドラインを策定することが必要であり、それに沿ってシステム構築が行われるようにされたい。

第三に、普及啓発プログラムについて。まず、一般の成人をターゲットとする取組は、国が直接施策を実施するということを中心にするよりは、民間等に主体になってもらう体制をどうつくるかという方向とし、国はそれら民間等の活動、体制構築支援に徹するべきである。

次に、これまでのセキュリティ対策はＰＣを中心に普及してきているが、スマホ、タブレットに加え、今後カーナビ、スマートカー、スマートテレビ、センサー、Ｍ２Ｍなど、様々な新しい機器、サービスが出現する。その際、機器の利用者である個人の普及啓発よりも、まずは機器の製造やサービスを提供する事業者が連携して、適切な利用環境を構築することが重要である。グローバルな市場環境の変化を踏まえ、事業者間あるいは業界間の連携をしっかりと取り、適切な利用環境の整備をお願いしたい。

○　３点述べる。

第一に、サイバーセキュリティ基本法案の早期成立を期待する。また、法律の成立後

は直ちに対応策を打ち出していただきたい。情報セキュリティ会議の役割もさらに重視されることになり、身の引き締まる思がする。

第二に、「新・情報セキュリティ普及啓発プログラム」の中で、協議会形式の場の設定と地域における取り組みの促進を掲げている点に注目している。残念ながら、サイバー分野では攻撃者と防御者の非対称性があり、防御側が協力体制を整備をしないと守ることができないという状況にある。しかし、官民協力あるいは産学官連携は、言うは易く行うは難い例の１つである。そのような中で、協議会形式の場というものを打ち出したことは、小さいかもしれないが一歩前進であり、それと同時に地域における取り組みの促進を強調している点ももう一つの前進である。

情報セキュリティ政策会議は東京に所在し、中央官庁とのつき合いが多いことから、どうしても東京あるいは首都の発想に偏りがちである。しかし、地方には地方のやり方があり、時間がよりゆったり流れていて雑音も少なく、全体の所帯が小さいことから、協力しやすいといういい面もある。そこで、地域における取り組みの促進をほどよい競争の中で推進すれば、「○○モデル」といった新しいアイデアが生まれてくる可能性もあることから、ぜひ推進して欲しい。

第三に、研究開発の効果・成果を高めるための方策等として、情報セキュリティ技術と社会科学など他分野との融合が掲げられている。全面的に賛成するものである。これまで、情報セキュリティを主体とした大学院をつくる際、理系が７で文系が３ぐらいの比率でやろう企画し、実践してきた。その経験を通じて、理系の方からは文系、とりわけ法学に対する期待が非常に高いと感じている。個人的にも法学分野の教育者であることから、セキュリティ技術を支えるため、法学的な面でもう少し努力してみたい。

○　刑事法の観点から、犯罪を中心に述べる。

現在、営業秘密として保管されてきた個人情報が内部犯行により流出するなど、情報流出の問題が世間を賑わせているところであるが、マイナンバー制度の開始もあり、今後の課題となるおそれがある。この点、情報セキュリティ政策会議発足間もないころ、有識者構成員の一人から、情報セキュリティの一番のポイントは「人」であるという考え方が示された。秘密は「人」から漏れるという考え方であり、「人」をどうするかということが最大の課題である、という認識であった。

この「人」の問題は、特定秘密の保護に関する法制度を含め、安全保障に関わる機微な情報の取扱の分野に関連してくると考えられることから、今後、政府機関のサイバーセキュリティ対策に関わる者については、能力的に高いということと、秘密の保全に関しての両方のレベルの高さを求めていくべきである。公務員だけで全ての面倒を見ることは、かなり苦しい面があるが、厳格に範囲を絞るなど保秘のやり方を様々に工夫する必要があり、サイバーと秘密保護は表裏一体の関係だと考えられる。

また、前回の会合は５月 19 日であったが、同日、米国司法省が他国の軍人５名をサイバー攻撃の容疑で起訴したと報道があった。我が国でも、６月５日の記者会見において、国家公安委員会委員長から警視庁による重要基幹産業に対するサイバー攻撃の実態解明の状況について発言があったところ。

このような脅威の情勢を踏まえれば、情報セキュリティ政策会議やＮＩＳＣの機能強

化は待ったなしという情勢である。政府機関、重要インフラ等を対象とした重大インシデントの原因究明に関するＮＩＳＣの機能強化は非常に重要であるとともに、防衛省や警察庁を含めた事態対処官庁との連携も非常に重要であり、サイバー攻撃を敢行した者を捕まえることの必要性はますます高まっている。

そして、原因究明のために重要なのは事後追跡可能性の確保であり、通信履歴（ログ）をきちんと保存しておくということが非常に重要な課題になっている。現在、国際的な安全保障の枠組みにおいてサイバー空間が注目されている中にあって、我が国だけがログを保存しておらずブラックボックスとなった場合、申し開きが立たないことになるであろう。

○　シンガポールでＩＴＳの研究をしており、ＧＰＳの位置情報を利用して車両の位置を追跡し、都市内に入ると、距離や滞在時間に応じた課金を行うためのシステムを開発している。この技術は我が国のものであるが、シンガポールでどのように発展するかはこれからのことである。ＩＴＳは国交省の管轄である。一方で、農業でも農業機械が発展しており、これからＩＴが利用されることで様々な新しい農業の未来をつくっていくであろう。これは当然農水省の管轄であろう。それぞれの分野で研究開発がバラバラに進められているが、セキュリティという観点で共通に見られるような枠組みやアプローチというのはどこでできるのかということを考えなければいけない。これはＮＩＳＣの情報セキュリティに関する研究開発というテーマの大きな意義になる。全ての産業と全ての国民が依存しているＩＴのインフラストラクチャーが構築されて利用されていくことを前提に、セキュリティを考えるに当たっては、ばらばらに考えているだけではなく、全体を考える仕組みと責任をＮＩＳＣからつくることが大事である。

また、ＩＴ関係一般、特にセキュリティは、情勢が急激に変化する。このため、人材育成において、常に新しい能力を構築する必要があり、難しい点となっている。この種の常に新たな課題へ対抗する人材を育成する際に一番参考になるのは、米軍が採用している「シリアスゲーム」というシミュレーションを用いた人材育成手法である。前日の戦場で発生した事象をゲームの中でシミュレートして、翌日にはゲームを通じてトレーニングできるという手法である。新しい事象をゲームの中に随時取り入れてトレーニングすることで、多くの人が対応できるという体制を構築するものである。セキュリティも、多くの人が新しい防御手法を憶えていくことでスケールのある人材育成を進めることができると考える。なお、この訓練手法は「ゲーミファイ」と呼ばれることもある。

付言してもう一つ、オリンピック・パラリンピック東京大会開催に際してのサイバーセキュリティに確保について。我が国でワールドカップを開催した際は、決勝戦の試合でサイバーテロが発生した場合を想定したシミュレーションを行い、専門家が知恵を集めて各組織がどういう役割をどこで果たすかということを検討した。

ロンドン大会の教訓を聴くと、たくさんのことが起こると考えられる。「オリンピックの最中にこういうことが起こる」という具体的なシナリオを作って皆で議論し、対応する体制を幾つか動かすことが重要である。

○　３点申し上げる。

第一に、我が国のサイバーセキュリティ推進体制の機能強化は、事務局資料の方向性でどんどん進めるべきである。その今後の課題として、例えばサイバーセキュリティ戦略本部の機能となる国家にかかわる重大なセキュリティ事案の評価や原因究明のため、高度なセキュリティの技術を持った人材の配置が必要となる点が挙げられる。それらの専門性の高い優秀な人材を国としてどのように育成し、配置していくのか。従前から様々に検討してきたが、まさしく「人」にかかわる問題であり、今後さらに検討されたい。

第二に、情報セキュリティの研究戦略をきちんと策定していくことは非常に有効である。その推進上の課題として、例えば今回は５分野を掲げた重点分野に対し、どうやって資金を投入し、その結果を効率的にフィードバックしていくかである。現在、国の独立行政法人等の研究機関に、セキュリティという名下で資金配分されているが、それを最終的に評価するところがない。研究開発の評価は必要であることから、是非ＮＩＳＣでセキュリティの研究について情報を集め、評価を行い、不足する箇所と、次に取り組むべき課題を示してＰＤＣＡサイクルを回して欲しい。

第三に、サイバーセキュリティ政策に係る年次報告書の取組は、一元的に行ったことが大変評価される。ただし、何分大部であるため、全体を見る人はほとんどいないところ、報道関係者等がメインで見る事になる概要資料中政府機関への脅威として 508 万件、６秒に１回といった数値が挙げられており、国民の視点からは危機感をあおっているように思える。例えば、「政府機関であればこういう対策をとっているので、これだけ脅威はあるけれども、かなりの部分は守ることができている。」あるいは、一般国民に対しては「この脅威はあくまでも政府に対するものであり、個人のＰＣに対する脅威もあるが、例えばＯＳのバージョンアップを適切に行い、セキュリティソフトをインストールするなどの対策を行えば、かなりの部分は安心・安全で使うことができる。」ということも普及・啓発することで、一方的に「怖い」という反応を引き起こさないように配意する必要がある。マイナンバー制度の開始の際にも、国民的に見ると「怖い」という反応が必ず出てくるだろう。「脅威がある。」という事実と、「的確に対応すればそれなりにきちんと守れる。」という観点を盛り込んで欲しい。一方で、重要インフラのほうは、重要インフラに対する攻撃リスクが増えてきているのは事実である上、重要インフラが攻撃された場合の社会的影響ははかり知れないことから、脅威が増えているという事実を述べたほうが全体としての整合がとれると思われる。

○　いずれも重要な議論であるところ、１点申し上げる。

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り組み方針について、サイバー空間における脅威は深刻化しており、サイバーセキュリティ推進体制の機能強化は重要な課題である。中でも、重大インシデントの原因究明は、警察による捜査と調和して政府全体として被害拡大の防止が迅速に図られるようにする必要がある。

さまざまな事案対応等を通じて、警察が培ってきた実践的対応能力と知見を生かして、引き続きサイバーセキュリティ推進体制の機能強化に貢献するよう、警察を指示してまいりたい。

もう一点、原因の究明にはログの保存というものが極めて重要である。これらはいわばサイバー犯罪の事後追跡という視点だけではなく、我が国の安全保障上の観点からも

極めて重要なものであると考える。サイバーセキュリティ戦略等に基づいて関係省庁と議論しながら、ログの保存のあり方について、速やかな対応を進めるよう警察庁を督励してまいる。

○　巧妙化するサイバー攻撃は、我が国の経済活動の阻害要因や国家の安全保障への脅威となっており、2020年の東京五輪を見据え、今のタイミングで政府のサイバーセキュリティ推進体制を強化していくということが大変重要。

東京五輪は、多くの外国人に日本に来ていただく大変大事な機会でもあり、ＩＣＴは訪日外国人と日本の魅力の架橋。先日、私は、訪日外国人が「選べて(Selectable)」「使いやすく(Accessible)」「高品質な(Quality)」ＩＣＴを利用することができる環境、世界最高水準のＩＣＴおもてなし環境を実現するための取組として「SAQ^2(サクサク)JAPAN Project」を公表した。こうしたプロジェクトが実際に効果を発揮するためには、その大前提として、情報セキュリティを確保することが必要不可欠。訪日外国人のＩＣＴ利用のシーンをしっかりと見据えて、あらゆる分野の関係者の知識を結集して検討するということが重要。

また、2020年において、いわゆるIoTの広がりなど、ＩＣＴ利用環境が大きく変わることが予想される。インターネットにつながるモノの膨大な増加と、新サービス・新商品の登場が相まって、サイバーセキュリティ対策は指数関数的に困難な局面を迎えていくことから、将来を見据えた先端的、実用的な研究開発を一層強化していくということが必要不可欠。

総務省では、これまでも、国際連携によるサイバー攻撃の発生の予知検知・即応技術を確立する研究開発プロジェクトとして「PRACTICE」、あるいは独立行政法人情報通信研究機構におきまして、サイバー攻撃の状況をリアルタイムで把握分析するシステムとして「nicter」の構築等に取り組んできたところ。

特に、サイバー攻撃のボーダーレス化を考慮すると、東京五輪は世界から日本の信頼性が問われる機会になるとともに、政治的な背景に基づく動向とも合わさって、予知も働きにくくなる。このため、世界で何が起こっているのかというグローバルな視点を持ちつつ、国際連携と並行して必要な対策を講じていくことが肝要。

今後とも、本日決定する「情報セキュリティ研究開発戦略」等にも基づき、情報通信研究機構等、関係機関と連携しながら、機器間の通信における情報セキュリティ対策技術の開発の推進等、我が国のサイバー攻撃に対する防御能力の向上に寄与してまいりたい。

○　本日、議論された「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（案)」は、サイバー空間を取り巻くリスクがますます深刻化している現在、時宜を得たものと考える。中でも、ＮＩＳＣの機能強化は、政府が一体となってサイバー対策に取り組む上で必要な施策である。参議院で継続審査となった「サイバーセキュリティ基本法」の早期成立と合あわせ、本取組方針案についても、早期に決定され、実行に移されていくよう、期待する。

外務省としては、サイバー犯罪やサイバー攻撃への対応は、一国のみで対応できるも

のではないことを踏まえ、取組方針案の中にも示されている「国際的な規範形成への積極的な参画」を始め、外交面で引き続き積極的に参画してまいる。

具体的には、今月下旬から実施される「国連サイバー政府専門家会合（ＧＧＥ）」にサイバー政策担当大使を参加させ、サイバー空間の安定的な利用確保のため、従来の国際法のサイバー空間への具体的な適用のあり方につき、明確な形で国際社会の合意形成を図ってまいる。

また、途上国のセキュリティホールをなくすための、能力構築支援も大変重要。５月下旬には日・ＡＳＥＡＮサイバー犯罪対策対話も開催し、ＡＳＥＡＮ諸国とのサイバー犯罪に関する情報共有や能力構築支援について議論を行った。現在、関係省庁と連携し、ベトナムへの政府調査団の派遣を検討しており、ベトナムをサイバー分野の能力構築支援におけるモデルケースとしたいと考えている。

○　サイバー攻撃への対処は我が国の安全保障・危機管理上重要な課題。防衛省としても、平素から自衛隊の効率的な活動を妨げる行為を未然に防止するためのサイバー空間における常続監視体制を構築するとともに、事態発表時には、被害の極限等を迅速に行うことが必要と認識。

また、防衛省では昨年２月、防衛副大臣を委員長とした「サイバー政策検討委員会」を設置。サイバー攻撃対処のための「体制の整備」、「事業・運用」、「人材の育成・確保」、「防衛産業との協力」といった課題についての検討を継続的に実施しており、私自身も問題意識を持って現在取り組んでいる。

さらに、今年３月に設置したサイバー防衛隊は、迅速かつ効果的なサイバー攻撃対処の中核部隊として、防衛省・自衛隊のネットワークの監視及び事案発生時の対処を 24 時間体制で実施。

また、本日の議題である「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（案）」はまさに喫緊の課題であり、国家の安全保障・危機管理の観点からも早期実現が不可欠と認識。防衛省としても最大限の協力をいたすとともに、情報分析機能等の強化等、更なる体制の充実を図ってまいりたい。

○　先日、高度情報通信ネットワーク社会戦略本部において改定された「世界最先端ＩＴ国家創造宣言」においては、基本理念として、サイバーセキュリティに関する対策の拡充とサイバー攻撃への対処能力の向上、これらを推進するための取り組み体制の強化等を図り「サイバーセキュリティ立国」を実現することが急務であるという旨追記されたところ。

また、同宣言において、国家の安全保障・危機管理のみならず、ＩＴ・データ利活用の促進等を通じた我が国の産業競争力強化のためにも不可欠なものとして「サイバーセキュリティの強化」について、引き続き明記されたところ。

それらの点を踏まえ、引き続き、情報セキュリティを確保したＩＴの利活用を積極的に推進してまいりたい。

○　我が国に対するサイバー攻撃において、最先端の技術情報を持つ企業やインフラ関連

企業は、極めて狙われやすい標的。

技術情報などを狙う標的型のサイバー攻撃では、まず初めに、独法等の政府機関、業界団体、取引先企業等を狙い、そこで得られた情報を使って目的の企業を狙うといった連鎖の傾向がある。

このため、今月16日にＩＰＡ（(独) 行政法人情報処理推進機構）において「サイバーレスキュー隊」を正式に発足させる。この取り組みは被害に遭った独法や民間企業等の現場に駆けつけて、情報の流出を食いとめ、再発防止策の実施を支援するというもの。

こうした取り組みを着実に進め、産業界におけるサイバーセキュリティ体制を強化してまいりたい。

(3) 議長締め括り挨拶

本日、活発に御議論いただき、まことに感謝申し上げる。

冒頭にも述べたとおり、深刻さを増すサイバーセキュリティ情勢への対応は、まさに待ったなしの状況である。政府としては、サイバーセキュリティ推進体制の機能強化について、高いプライオリティを持って推進すべきであると考えている。

また、こうした取り組みによるサイバーセキュリティが確保されることは、国家の安全保障・危機管理上不可欠である。加えて安倍政権が掲げる成長戦略をより確固たるものにし、2020年オリンピック・パラリンピック東京大会の成功を期す上でも、極めて重要であると認識している。

今後とも、我が国のサイバーセキュリティの確保に努めてまることから、各構成員の皆さんにはさらなる御協力を賜りますよう、お願いを申し上げる。

－　以上　－