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32回会合　議事要旨

１　日時

平成25年2月22日（金）　17：00～17：30

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
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
	（橘　慶一郎　総務大臣政務官代理出席）
茂木　敏充	経済産業大臣
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
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）

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

４　議事概要

(1)　議長冒頭発言

近年、サイバー攻撃の態様が一層複雑・巧妙化するなど、サイバー空間におけるリスクが深刻化している。これを踏まえ、総理から、本政策会議において、「新たな情報セキュリティ戦略」を本年夏までに、策定するよう指示があった。本日は忌憚のないご意見を伺いたいと思う。

また、残念ながら政府機関等において、情報流出事案が発生しており、大臣自らが情報セキュリティ対策の重要性を深く認識し、危機感を持って、各府省庁における態勢が万全なものとなるようお願いする。

(2)　討議事項

・　新たな情報セキュリティ戦略について
・　政府におけるサイバー攻撃等への対処態勢の強化等について
・　情報セキュリティ月間の実施状況について
・　重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第３版）の改定について
・　その他

上記について、事務局より資料を配布し、事務局より説明が行われた。

(3)　構成員意見交換

構成員から以下のような意見が述べられた。

○　国際政治の観点から言えば、この３年間、サイバー攻撃やサイバーセキュリティは非常に重要な問題になっている。先般、中国からアメリカ政府に対して執拗な攻撃が行われているという報道がされていたが、それに先だって、オバマ大統領はサイバーセキュリティ強化に関する大統領命令に署名している。我が国としても、このような状況において、サイバースペースにおける法的課題を考える必要がある。

○　法的課題として、例えば、領空侵犯や領海侵犯のルールのアナロジーをサイバースペースに適用して、国際的なルールを作ることはできないかを考える必要がある。これらのルールをサイバースペースに適用することができれば、日本主権下にあるサーバ、回線、端末に対して危害が加えられたときに、我々は止めることができる権利を主張することができると考える。

○　サイバー攻撃を疑う通信があった場合、その通信を傍受し、内容を精査し、攻撃を受けているかを判断できるようにしてもよいのではないかと思う。この場合、憲法上の通信の秘密に抵触する可能性はあるが、国家安全保障上の利益とバランスを取った上で、海外からの通信に限定したり、ヘッダ情報に限定したりすることによって、通信の秘密を緩和できないか考える必要がある。

○　サイバー攻撃は、政府機関だけでなく民間企業も攻撃を受ける可能性があることから、政府機関と民間企業との間の情報共有も重要である。この情報共有を進めるためには、法令によって義務づけることを検討してもよいのではないかと思う。そして、情報共有を進めていくことが、情報セキュリティ産業の育成や人材育成につながっていくと考える。

○　これまでの基本計画策定時に比べ、サイバー攻撃のリスクが深刻になっているなど、サイバーセキュリティを取り巻く問題は質的に変化している。具体的には、実際の生活に直結する社会インフラへのサイバー攻撃により、リアルな被害に直結する可能性や、日本をターゲットにしたゼロディ攻撃の被害に遭う可能性がある。このように、サイバーセキュリティを取り巻く問題が質的に変化しているということを十分に踏まえた戦略作りや体制の整備の必要がある。

○　サイバーセキュリティに関して、トップは２つの方向に注力することが重要である。１つ目として、最新のサイバーセキュリティ関連情報を的確に共有できる体制を整備すること、2 つ目として、各組織が対策を実施するモチベーションを高める環境を整備することである。組織の枠を超えた情報共有体制を作るためには、重要インフラ産業や一般企業でも情報を共有できる体制作りを支援すること、通信の秘密について緩和してゼロディ攻撃への情報共有をしやすくすることが重要であると考える。また、モチベーションを高める環境整備については、経営層に向けて被害事例の紹介等を通じて啓蒙をしていくこと、コーポレートガバナンスの重要な事項とする仕組みにすることが重要である。

○　人材育成に関して、サイバーセキュリティの専門的な人材が不足している。大学での人材育成だけではなく、産業構造の変化に応じてスキルチェンジを求められる年代層を含む各年代層がセキュリティ人材に移行できるよう人材育成サービスを支援すること、ハッキングコンテストを活性化することも重要である。

○　遠隔操作の事件において、警察のサイバー犯罪捜査は完全でないと言われている。警察は、国民の期待に応えなければならないが、ログによる追跡が出来なければ、捜査が不可能となってしまう。ログの保存については、これまで長いこと議論されてきたが、具体的な政策として一歩前に出る段階に来ていると思う。安全の基盤が欠けていれば、サイバー空間の発展はないと思う。例えば、ネット選挙やマイナンバーにおけるなりすましをどのように防いでいくかを考えていく上でも、事後追跡可能性が必要である。このような状況において、通信の秘密に関する考え方を実利の側から動かさないと危機に対応できないと思う。今回の新たな情報セキュリティ戦略では、柱としてログの保存について一歩前の政策を出していただきたい。

○　IT は様々な面で利用されており社会の基盤になっているため、サイバー攻撃から守るということは重要であるが、情報システムに対する攻撃や事故は必ず発生するものであ

る。攻撃や事故があったとき、情報システムを回復できる力が必要となる。東日本大震災におけるITインフラの回復力については、世界中から評価されている。今後、安心安全な社会を作るために、情報システムの回復力を持つことを進めていく必要がある。

○　日本は、スマートテレビの環境や高速のネットワークなどの環境の整備が、他国に比べて圧倒的に進んでいる。このような中、日本がどのように世界に貢献するか考える必要がある。

これまでインターネットは、アメリカ、日本、ヨーロッパ、オーストラリアのマーケットが主導してルールを決めていたが、今はアジア・アフリカにおけるマーケットも大きくなっている。今後は、グローバルなサイバー空間をいかに安心・安全にしてくのかという戦略について、日本がリーダーシップを発揮して考える必要がある。そのためには、日本として、グローバルなサイバー空間と日本のサイバー空間の両方を守備範囲として守っていかなければならない。

○　クラウドの基本的な基盤となっているネットワークのブロードバンド化とコンピューティングパワーは、この２０年間で大きく発展した。このことは、多くのシステムやプロダクト、インフラがソフトウェアディファインドの方向に向かっていることを示している。今後、ソフトウェアディファインドが進み、リアルタイム性を持ったサービスが増えていった場合、ソフトウェアのセキュリティが一層求められる。これまでは、標的型攻撃に対する対策だけ議論してきたが、今後は、ソフトウェア自体が攻撃される可能性を考える必要がある。

○　情報セキュリティの領域において、日本がアジアにおけるリーダーシップを発揮するためには、日本の国家像をミッドターム、ロングタームで考える必要がある。特に、日本のセキュリティの認証機関で、日本や海外のシステムやプロダクトを認証することにより、リソースの少ない日本が技術立国として、アジアでリーダーシップを取ることができると思う。日本としては、レベルの高い認証機関を作るための方策について考える必要がある。

○　先日開催された第３回日本経済再生本部において、総理から、世界最高水準のIT社会を実現するべく、IT政策を立て直すよう指示を受けた。今後、早期にIT戦略本部を開催し、安倍総理の下の安倍ビジョンというものをIT戦略本部でしっかりと打ち出していきたい。

情報セキュリティについては、IT政策を推進していく上で、不可欠なものであることから、IT政策担当大臣として、情報セキュリティを確保した情報通信技術の利活用を推進してまいりたい。

また、法律に基づく政府CIOを設置するため、関連法案を通常国会に提出する準備をしており、政府CIOの下で、情報セキュリティを確保した、より安全な政府機関の情報システムを構築してまいりたい。

○　基本的な論点を整理していただいた方が良い。例えば、情報を盗まれるのか、情報システムを機能しなくするのかによって、その性格は異なる。また、政府機関や企業を対象にするかによっても異なるし、リスクの大きさ、リスクの種類、攻撃側の性格によっても異なる。さらに、防御についても、予防、攻撃を受けたときの対応、ログを残して犯人を捜すのかによって異なるので、そのような観点から一度、整理をしていただいた上で、対策を出した方がよい。

　また、インテリジェンスを取り扱う機関とそれ以外の機関の情報システムの共有をどこまで行うのかについて、つめていくことも重要である。

○　本日は、大変限られた時間にもかかわらず、ご出席いただいたことを深く感謝申し上げる。議長としては、もう少し時間をとって会議が充実するように責任を持って会議を行っていきたい。政府CIOが機能するように山本大臣を中心に取り組んでいきたい。

　有識者構成員の皆様は、大変御多忙とは思うが、本政策会議で策定される新たな戦略は、我が国の経済成長、危機管理の礎となるよう、ご協力をいただきたい。

－　以　上　－