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
技術戦略専門委員会
第 16 回会合議事要旨

１．日時　平成２２年１１月２５日（木）１３：００～１５：００

２．場所　中央合同庁舎第４号館第４特別会議室

３．出席者

［委員長］
後藤 滋樹（早稲田大学教授）
［委員］
阿草 清滋（名古屋大学大学院教授）
岡田 羊祐（一橋大学大学院教授）
小柳 和子（情報セキュリティ大学院大学教授）
志方 俊之（帝京大学教授）
須藤 修（東京大学大学院教授）
田尾 陽一（セコム株式会社顧問）
中西 晶（明治大学教授）
宮川 晋（NTT コミュニケーションズ株式会社　先端 IP アーキテクチャセンタ・経営企画部（兼務）担当部長）

（五十音順）

［政府］
和田隆志 内閣府大臣政務官
内閣官房情報セキュリティセンター内閣審議官
内閣官房情報セキュリティセンター内閣参事官
内閣官房情報セキュリティセンター情報セキュリティ補佐官

議事概要

（１）後藤委員長　着任挨拶

（２）内閣官房情報セキュリティセンター副センター長 阪本審議官　挨拶

（３）今回の技術戦略の検討課題【事務局より資料に沿って説明】

○　今までコンピューターセキュリティは守りの発想だったが、今後は攻めの発想も必要。また、大規模サイバー攻撃が実際に発生しており、ミティゲーション（攻撃を軽減してフィルトアウトする）技術の必要性は高まっていくと考えているが、この技術や製品は海外メーカーに頼っており、国産の技術を作った方がよい

（４）政務官挨拶

【政務官入室】

○政務官：　情報セキュリティについて、今ほど国民の皆様方の関心が高まっている時はないと思っている。そのようなときに時宜を得てご議論いただくことは、本当に我々としてありがたい。「いたちごっこ」のこの世界の中で、技術的にどのようなことが可能か、いろいろ教えていただき、全力で取り組んで参りたい。

（５）委員・補佐官コメント

○委員長：　委員の方々から研究開発戦略の策定という観点から一言お願いしたい。

○　書き換え可能な性質が、ソフトウェアの大きなメリットであるが、その性質が情報セキュリティ上で問題となっている。ソフトウェアを作るプロセスをきっちりとすることが重要であり、人海戦術に頼った方法では情報セキュリティ上の穴が開くのではないか。

○　情報セキュリティのような汎用性のある基盤技術の開発には、国研などの公的機関がイニシアチブをもって開発を主導あるいは支援することが必要と考えるが、そのための研究費は大幅に減少する傾向にある。また一方で、民間部門の投資インセンティブをいかに高めていくかという産業政策的な視点が挙げられているが、公的な研究開発支援と相反しないように、公的部門と民間部門とが補完的となるように研究開発の仕組みを創っていくことが大切であり、官民連携の具体的な取組みを如何に進めるかが課題である。

○　情報漏えいに関して大学で論じる場合、大部分が企業の情報や個人の情報を対象としており、国家の情報の漏えい対策については扱えていないことから、この部分は国が率先して検討するべき。また、従来は些事な情報だと思っていたことが、クラウドによって大量に集められると、プライバシー上の大変難しい問題を引き起こすことになると考えられる。法律的な問題にも係わるため、クラウドのセキュリティについては、国が率先して検討したほうがよいと考える。

○　情報セキュリティの研究開発に関する予算が国全体で40数億円しかないという状況は、大きな問題。情報セキュリティは国家存立の基盤の保持に係わることであるので、しっかり対処する必要がある。また、一般企業でもかなりサイバー攻撃の被害を受けているが、企業の信用に関わると考え、大きい企業ほど隠したがる。官民の情報連携を進めるためには、情報を守るというガバナンス的な要素を、官民の情報共有の運用のあり方の中に取り入れる必要がある。

○　クラウドベースのネットワークをフルに使って社会で活用するというフェーズであり、ネットワークセキュリティについて相当の研究開発費用を投入する必要があるにも関わらず、情報

セキュリティの研究開発費の大幅な減少は、常識では考えられない状況。リアルとサイバーが融合した社会では、先読みの情報セキュリティ、高度なセキュリティ技術が要請されるので、かなりの予算が必要。将来を見据えた体系的な研究開発が必要。

○　尖閣問題については、情報の漏えいが起こる可能性があるという事故前提の考え方に基づいて、組織のマネジメントをちゃんとやってきたのかが問題の本質。

研究開発戦略については、ボトムアップ的にではなく、研究開発全体をどうするかという戦略の下で推進しなければならない。社会の将来像を描き、想定するダメージやリスクを計算し、リスクを可視化することにより、国民にとって取り組む必要があるもの等を明確にすることが必要。

○　攻撃者もセキュリティ技術を扱うのも人間。人の心理や組織での感情を含めて、国のセキュリティ政策を考える必要がある。

○補佐官：　Ｒ＆Ｄの中長期的な視点で、よりディペンダブルな情報システムを先回りして構築する「攻め」の発想の情報セキュリティ技術研究開発が必要。今、欧米で動き出しているIPv4,IPv6の次のフューチャーインターネットのプロジェクトにおけるＲ＆Ｄの方向性は、中長期的に元々セキュアなシステムを指向してつくっている。設計時からセキュリティがきちんと配慮されたシステムを考えていかなければならない。システムのつくり方に立ち返って、安全安心な社会に向けた新しい価値やサービスを創出できる情報システムをつくっていけるようなテーマが出てくれば、より明るい研究開発戦略になるのではないか。

○補佐官：　研究開発、実用化、普及というサイクル各段階におけるインセンティブや触媒のような視点で仕掛けていく、研究開発サイクルを起爆するのがコストパフォーマンスが良い方法ではないか。日本に世界一セキュアなICT環境をつくるといった、わかりやすい目標に向かって投資をすることは、税金の使い道として説得力がある。

○委員長：　サイバーの世界では既に非戦闘員である民間レベルでも相当の被害がある。何も対処せずに守るだけというのは通用しないと感じる。サイバー世界のならず者を追いつめるには国際的な連携も必要。

ネットワークの規制については、民間が自主規制する場合もあるが、やはり公的機関が見守る必要があると思う。役割分担に抜けが発生しないよう、多少オーバーラップをするつもりで対処する必要がある。

（６）政務官挨拶

○政務官：　最近の情勢は本当に危機的な状況であると感じる。他国でも情報漏えいの発生はあるが、日本のように自国の国益を害するような情報漏えいは起こっていない。国の研究開発予算が落ちていることについては、認識を新たにしたが、むしろ決意をもって取り組むという意思を示す意味で今回は良い契機ではないか。

一方で、今回の尖閣の件につき、万一の事態が起きたときの技術的な対処方法が日本にはないことが露呈した。他国では情報遮断のルートがあり、最小限の被害に食い止める努力がされていると聞く。誰かがモラルに反する行為をとったときに、国家としての対処を考える上で、ご専門の皆様方の英知を集める必要がある。

この機会に、日本全体として情報セキュリティを大事にしなければ、国全体が沈没する危険

性があることを国民に相当強力に発信するべき時期に差し掛かっているのではないか。
【政務官退室】

（７）自由討議

○補佐官：　原子力発電所の遠心分離器の回転速度を変えるマルウェアが出てきたなど、情報インフラに対する脅威にリアリティが出てきている。今後は、こういった重要インフラを取り巻く動きに注目していく必要がある。

攻撃者への対応においては、米国のMoving Target Defenseなど、相手の動きを知った上で対応するという手法の研究がトレンドとなっている。また、セキュリティ対策と個人情報保護対策のように、あるリスク対策が別のリスクを生み出すような問題もあるので、相反する意見を調整する仕組みの研究も重要。

○　利便性はきちんと確保された上で、効果が見えることが大切。例えば、ディペンダブルなソフトの作り方やテスト方法について国が責任分界の基準を定めないと、事業者は過剰な対応を取るようになってしまう。また、リナックスのようなオープンソースについても、市販製品に使うレベルと国の重要システムで使うレベルとの境界を国が設定し、目的に合わせてセキュリティレベルをコントロールすることが重要。

○　サイバーにおける戦いには、ルールはない。米国におけるサイバーウォーの研究も、やられそうなところを発見するという意味でアタック技術の研究からスタートした。故意に弱点を見せてトレースバックをし易くし、相手がそれに引っかかったら撃ち返すくらいの研究が必要。

人材開発の観点では、この分野は学位取得が遅くなる傾向があり、良い人材が集まり難い。ＩＴを担当している人が、やっていて良かったと感じるようにしなければならない。

○　「攻め」の発想に関し、プライバシー情報はもっと適切に使えば、もっと新しい何かができるのではないか。

○補佐官：　SUICA等のシステムでは、何百万人というトラフィックがリアルタイムにセンシングされている。個人と紐付いた情報を匿名化し、無名性を保証する技術をきちんと作ることが重要。また、医療分野では、癌や認知症の治験データを共有する仕組みが求められており、共有できれば製薬のプロセスも早まると考えられる。治験データはセンシティブな情報であり、病院から出すべきでないという発想になると、世界からどんどん遅れてしまうと危惧している。

○　ＩＴ戦略本部において、名寄せが可能な国民ＩＤを使って、高度な医療・行政サービスの実施が検討されている。名寄せに対する日弁連の意見は、かつて否定的だったが、今年10月にはようやく追認されるようになった。ただし、個人情報保護等などを制度的に担保するため、第三者機関による監査等ができる仕組みを早期に作るべきと言われている。このように世論が変化してきており、これに合致したセキュリティの社会科学的、工学的対応を打ち出す必要がある。

○補佐官：　新しい施策を進める上でこのような対応は必要であるが、どの範囲でやれば良いかについては国民的な合意形成が重要。システムの移行や故障時の運用を詰めていくと、プラスの部分が明確になってくると思う。

○委員長：　社保庁の問題などもあり、国が扱うプライバシー情報に対して国民のスタンスが定まっていないように感じる。個人情報保護法は、ここまで守れば流通しても問題ないという基

準を示すために作ったはずだが、過剰反応が起こって、大変不便なことになってしまった。説明の仕方によって国民側の理解も変わってくるので、状況がより合理的に進むようにご提言頂くのが良いと考える。

情報セキュリティに係わる提起は、皆がやりがいや手ごたえを感じるという方向に進んでいければよいと考える。昔の現場のほうが、やりがいがあったと感じることもあり、現在の状況に非常に危機感を持っている。

○　日本の社会は責任の取り方が明確でないように感じられる。上位の責任者が責任をシェアするようにしないと、現場が萎縮してしまう。組織や政府のトップが持つべき責任を明確にすればよい。

○　情報セキュリティは目に見えないものなので、それを支えている人たちのモチベーションを上げていく方法を議論する必要がある。

○　日本の通信会社は守秘義務から、客のシステムが攻撃されているという情報を認知すること自体ができないルールとなっている。日本においては、国民の意識を変えていかないと、技術を取り入れることができないということが問題。

○委員長：　通信の秘密は別途検討されているが、ある国だけで決められるものではなく、世界的な相場感のようなものをどこまで納得するかということだと思う。

○　国家存続に係る重要なコンピューターシステムのランニングが下がっていたとしても、クライアントから対応要請がないと、現象の解析も攻撃を止めることもできない。このような場合にどうするかというのは大きな問題。

○委員長：　国民の感覚で言うと、通信の秘密は順守すべきルールであるが、一方ではネットワークの状況を見守って欲しいというニーズが、個人にも企業にもあるのだと思われる。基本的な考え方が変化しつつあると理解した。

○　国民にサイバーウォーについても理解を深めて欲しい。国家が国家に対してサイバーウォーを仕掛けたらどういうことが起こり得るのか、海外で起こっている事例を加えて、白書のようなものを公表して欲しい。国家間のサイバーウォーが仕掛けられたら、生命が奪われる可能性がある事態なので内閣が自ら対応する必要がある。

○委員長：　日本に海外のような通信機器ベンダーがないことについては、産業政策においてそれが適切かどうかという問題がある。別の観点として、世界中が同じ製品を使うことが果たして安全と言えるかという問題もある。通信は典型的な重要インフラであり、通信事業者に求められる品質についての国民的な理解が必要。

（8）まとめ

○補佐官：　技術戦略のまとめ方については、学会、業界、国等どこかに向けての提言のようなものを作らなければ、単なるレポートで終わってしまう可能性がある。

○委員長：　誰に向けてのメッセージなのかを明確にすることが重要。本日の議論の中でも、様々な説明方法、表現方法が提案されたが、小説や映画等で発信するということも考えられる。国民の意識を変えるためには、事実を事実として説明する手法だけではうまくいかない。色々な方の協力が必要。

（7）資料の取り扱い、今後のスケジュール等

〇事務局：　次回の会議は２月初旬を予定している。

〇委員長：　本日は大変貴重な情報、指摘を有難うございました。議論はこれで終了したい。

以上