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 21 回会合議事要旨

１．日時　平成２４年6月２２日（木）１７：００～１９：００

２．場所　内閣府別館 大会議室

３．出席者

［委員長］
後藤 滋樹（早稲田大学理工学術院教授）
［委員］
阿草 清滋（京都大学客員教授）
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）
中島 秀之（公立はこだて未来大学学長）
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］
内閣官房情報セキュリティセンター長
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
（内閣府政策統括官付代理参事官付）

議事概要

（1） 後藤委員長　挨拶

（2） 情報セキュリティ研究開発ロードマップ（案）について

【事務局より資料２～４について説明】

○ 特段の意見がなかったため、情報セキュリティ研究開発ロードマップ（案）を本委員会の決定事項とする。

（3） 情報セキュリティ技術開発を活用した産業活性化検討ワーキンググループの検討状況について

【事務局より資料５．６、参考資料２、３について説明】

○ 事務局：　すべてのセキュリティ分野において産業活性化は困難であり、集中と選択が必要と考える。

○ 事務局：　情報セキュリティ研究開発戦略は 5 年をターゲットにしたものだが、昨今既に状況が変化していることも鑑み、見直しを行う点についてもご意見をいただきたい。

○ 委員：　関係者コミュニティの構築に関し、既存のコミュニティとはなにが違うのか。そのイメージを聞きたい。

○ 事務局：　コミュニティが存在ししっかりと動いている領域と、そうでない領域があると感じることがある。NISC では、セキュリティ領域について学会間等の連携を政府が関与することで、より密接な関係を築くための入り口を提供したいと考える。

○ 委員長：　政府の役割は、過度にガイドラインを入れたりすることなく民間の対応を見守って、問題があれば調整し、ファシリテートすることである。

○ 委員：　これまでに何度か発言したが、民間において積極的に問題に対処しているが、民間同士で意見交換したり、使用された技術情報がオープンになることはない。政府から必要な部分について情報提供を指示するくらいでないと、現状に留まることになる。また、重点化する製品ターゲットを定める上で、日本製のファイアウォールは非常に少ない等の現実がある。人口は少ないがイスラエル製の品質がよかったりする点は参考になる。

○ 補佐官：　2 点申し上げる。ひとつは産業活性化にあたり、細かな要素技術を研究して製品化する意義は薄い。例えば経済産業省が「世界一のファイアウォールを国産で開発する」旨を宣言して、予算をつけるくらいのことをすべきではないか。もうひとつは、日本のロードマップとアメリカのロードマップは、おそらく議論や作り方が異なるので比較できない。日本も○だけではなく、△や×の入った報告書を作成する必要がある。

○ 委員：　産学官という３つの母体をマージングすることは、それぞれが異質であるため困難である。米国では産学官の間を特定の人物が移動することが日本より容易であるから、それぞれの立場で得た秘密事項を他へ漏らさないよう厳密にルールを守って、それぞれの部局の仕事をこなす、いわゆる「人間のモビリティ」があるが、この考え方はセキュリティにおける推進母体の確保やコミュニティの構築などの突破口になるのではないか。

○ 委員：　日本学術会議におけるセキュリティの分科会において、研究者の視点からセキュリティ政策に関する問題点を指摘している。まだ NISC や総務省などとも連携を取ってい

ないと思われるので、コミュニケーションをとってもいいと考える。また、システム構成全体で考えた方が誤らないと思う。あと、日本企業のセキュリティに関する売上規模が小さいと言われるが、軍事を含めて海外ではかなり展開している等見えない部分を理解しておくべきである。

○ 委員長： 日本学術会議については確かにその通りで、総合科学技術会議のインプットとしても連携していく必要があると思う。モビリティについての発言についても同意する。コミュニティという前に、人間がそれぞれの持ち場でどのような役割を果たしていくかを異なった視点から見ることができることも重要である。産業界での人材育成において、アメリカでは社会からも人材を集めるが、日本の場合はひとつの会社から集めてくる。このあたりにも違いがある。

○ 委員： アメリカの DoD が国防の観点で研究を行っているが、日本ではその観点がない。セキュリティは国防であると思うので、政府が国を守る視点をもっと持つべきである。系統的なサイバーアタックを受ければ国が崩壊する可能性もある。また、システムを構築する人たちにも国家資格などが必要ではないか。

○ 委員長： ナショナルセキュリティについては、油断していると大変なことになるという思いがある。

○ 委員： 実運用において、攻撃元がミリタリーとしか思えないケースもある。問題は多々あるにせよ、我々のプラットフォームが外国製であり中身はブラックボックスである現実を踏まえる必要がある。また、ベンチマーク先について、アメリカやヨーロッパだけではなく、ロシア、中国、イスラエルなどにも参考事例があるのではないだろうか。

○ 委員： イスラエルは重要であると思う。国家と企業が協力に連携していると思われる。

○ 委員長： ヨーロッパはそれぞれの国が重点化・標準化する研究分野を絞り込んでいるが、日本は重点化することなく幅広く研究を行うことができた恵まれた国だったとも言える。重点化するには他の分野の切り捨てが必要で痛みとエネルギーを伴う。今の日本の立場は厳しいことを認識した上で、若い人たちが選択できるようなものを提示するのが我々の役割と考える。

○ 委員： ロードマップに出ている技術は、いずれも守る技術である。是非論はあるが、国防面から考えると、今後攻撃技術も教える必要があると感じる。産業活性化については、研究成果が産業界に何らかの形で還元される方法を考えないといけないと思う。

○ 委員： 拠点に対して先制攻撃をかける、アクティブ・セキュリティという考え方があり、そのような意志を持っている国家もある。

○ 委員長： 攻撃技術がわからないと何もできない。また、攻撃技術は商用利用にも応用可能である。研究成果の還元については、政府からの支援は税金で戻すという心構えが必要と思う。

○ 委員： 人材流動性は非常に重要である。産学官で人の動きがないことはよく指摘されている。人間の評価の仕組みが重要である。例えば基礎研究にウエイトがかかりすぎているため、基礎研究で優れた研究者は多くいるが、実用化につながる部分はあまり評価されない。評価されなければ優秀な人間が集まらない。あと、イスラエルがなぜ成功したかというと、官からベンチャーにどんどんお金が流れる SBIR のようなファンディングの細やか

な仕組みがあり非常に評価されている。日本の産業技術力が右下がりになる理由は、民間が主体的に特定の技術にコミットするのはリスクが大きいため、安全策で横並びになりがちなところにある。アメリカでは逆に新技術を使ったビジネスがしやすい環境があると思う。補足だが、日本では個人情報を生かしたビジネスがしにくい法制度などがあり、これらが研究開発のイノベーションのドライブフォースを妨げるようにも思う。あらゆる側面でのビジネスが盛んになれば、それにつれてセキュリティも盛んになる。

○ 委員：　ロードマップに関し、どのタイミングで、どういう判断で見直すのか、あるいは止めるのか、という中間目標が見えない。定期的な進捗管理についても技術戦略専門委員会では議論する必要があると考える。また、マーケットの在り方として、「技術が必要なので開発せよ。こういう製品があれば買う。」という引っ張り方が好ましいのではないか。

○ 委員：　産業化やマーケットに加え、特例措置のような調達の方法も重要である。テストベッドにおいて、国が何を準備できるかを検討する必要があると思う。攻撃技術については、例えばスーパーハッカーのような人材を政府として囲い込むことも必要かと考える。

○ 委員長：　日本は計画性が強すぎるところがあり、余裕がなくなって新しい技術が出にくい環境になってしまったかもしれない。

○ 委員：　この世界は今、日進月歩だと思う。サイバー犯罪と言うより国家間のサイバー・ウォーの時代であり、ハードでもソフトでも国家が最先端である必要がある。技術は国家がある程度リードしたら民間に任せ、国家は次の段階に進んでいるべきであり、国家がイニシアティブを取らないといけない。また、ロードマップの見直しについても、日進月歩の世界なので、5 年のものは 3 年で見直すなど、事務量との兼ね合いを見ながら適切に行っていく必要がある。攻撃と防御については、日本という風土ではこちらから攻撃をかけるのは困難であるが、攻撃を受けたら攻撃的に対応するアメリカのような対応も検討する時期に来ているのかもしれない。日本のような専守防衛の国としては、なんらかの対応をする必要がある。情報セキュリティセンターにもそれなりの機能を持たせてはどうか。

○ 事務局：　小さな一歩も大事と思い、事例を紹介する。国の重要な情報を扱う契約を扱う場合はセキュリティ条項を入れる旨を策定したが、その中に情報処理技術者試験資格と同等の資格を有すること、という条項を入れた。また、攻撃については難しいところがあるが、NISC での調達にあたってこれまでの条件に加えて、「CTF で優秀な成績を保持した職員がいること。」を項目にいれることも行っている。

○ 委員長：　攻撃技術も実用に役立つもの多く、広くカバーする必要があると感じる。しかし発言にあったように、研究開発はリスクが高い。リスクテイクする場合はサポートが必要である。産業界がばらばらに行っていることをコミュニティやコンソーシアムに求めることも必要と思う。

○ 補佐官：　産業活性化について、政府調達で国産品の優遇措置についてよく言われるが一向に実現されない。ならば、別の方法でインセンティブになるようなお金を投入すればいいと思う。たとえば、売れたら売れた分だけ、国産技術の分だけ割り戻すような施策はどうだろうか。

○ 事務局：　セキュリティ投資減税を実施するために、基準が必要ということで ISO15408 を条件としたが、対応する製品は外国製がほとんどだった。

○ 委員：　現状、現場では、日本の技術かシリコンバレーの技術かは気にされない。そもそも国産技術の定義が曖昧である。重要なのは日本を空洞化させないことである。

○ 委員長：　ルータやスイッチは分散システムを考えられているが、論理的には集中している。またバラバラの機種を導入したのでは実際の運用現場が持たない。また、セキュリティ技術が単独で存在するのではなく、何かのセキュリティであるところが重要である。

○ 委員：　メタな議論だが、他の政府の委員会に出てもいい意見が報告書から消えていることが多い。本日だされた有用な意見はきちんと残してもらいたい。

○ 委員長：　議事録についてはできるだけ具体的な意見を迫力があるように残しておき、次に議論する際にはこれをベースにして進めるものとする。我々自身も心がけて行くべき部分、ご意見、分担などについて指摘いただきたい。

○ 委員：　質問が１点ある。6 月 6 日に内閣官房が医療イノベーション 5 か年計画を発表したが、ここではネットワークはデータベースを相当重視している。しかしここにセキュリティがどう関わるかが明確ではなかった。横の連携が取れていないと感じたので、確認しあった方がよい。

○ 委員長：　個別の研究者の方には大変興味が高い部分であり、セキュリティ抜きにはできないと思われる。迫力のある実験を行うためにも、連携をお互いに取り、高めていくことは重要と考える。

○ 委員長：　本日の多岐にわたった議論につき、別途議事要旨を作成するので確認いただきたい。

（4）　閉会

以上