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 15 回会合議事要旨

**１．日時**　平成２１年８月２８日（金）１５：００～１７：００

**２．場所**　内閣府別館大会議室

**３．出席者**

［委員長］
佐々木 良一（東京電機大学教授）
［委員］
岡田 羊祐（一橋大学教授）
小柳 和子（情報セキュリティ大学院大学教授）
後藤 滋樹（早稲田大学教授）
田尾 陽一　（セコム株式会社顧問）
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内閣官房審議官
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）
警察庁情報通信局情報技術解析課長
（総務省情報通信政策局情報通信政策課情報セキュリティ対策室長代理課長補佐）
文部科学省大臣官房政策課情報化推進室長
（経済産業省商務情報政策局情報経済課情報セキュリティ政策室長代理課長補佐）
防衛省運用企画局情報通信・研究課情報保証室長

## ４．議事概要

（１）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

（２）岡田委員着任挨拶

（３）本年度の技術戦略の検討課題について

ア　第２次基本計画における技術戦略

【事務局より資料に沿って説明】

○　１０頁の記載で、「民間による技術開発のインセンティブが弱い」というクライテリアがあったが、民間は自ずと自分の会社が儲かることを基準にインセンティブに設定してしまう。「社会全体の全体最適のためにインセンティブは働かせるべきだが、一民間企業の営利活動の中ではインセンティブを設定するのは難しい研究開発を、政府として実施すべきだ」というぐらいの説明をしてもいいのでは。実際セキュリティ分野の中では、そのような研究は多数ある。商売のネタにするべき技術ではないとなった際に公的資金を投入することには合理的な目的があるというロジックとなると思う。

次に、「安全・安心なIT基盤の実現に直結するもの」というクライテリアは、効果が高いといった場合に何を目的とした効果なのかが微妙であり、難しい。企業活動においては利益率が高い等の分かりやすい基準が設定できると思う。政府のお金の使い方としても同様の視点を排除するわけではないが。

最後に「利用が進んでいないもの」というクライテリアについて、利用が進まない理由が、果たして政府が関与することによって解けるものなのか。そもそも、元々無理があったものを無理矢理もってくるようにも読める。いずれにせよ、この３つのクライテリアに関してはもう少し明確に記述する方が納得性の高いものとなると思う。

○事務局：　自社の直接的な利益にならず個々の企業として開発のインセンティブの弱いものの例として、例えば、DNSのサイニングがある。儲かるという話だけでは、インセンティブが足りないというのは、おっしゃるとおり。クライテリアについては、もう少し詳しく説明した方がいいかもしれない。

また、技術はできてきているが利用は進んでない例として、TPM（Trusted Platform Module）などがある。有効に使えば大きな効果があるはずだが、不適切な使い方していることから、みんな誰も信用しなくなってきている。TPMのモジュールを著作権の保護に使うといったような間違った使い方するとおかしなことになってくる。いずれにせよ、この目的マップの中のどこかにカテゴライズされるのではないかと思うが、ほかに足りないものがあるかどうか、というのが気になるところ。

○　今の話の中でもインセンティブの話があったが、研究開発投資を行うことで得られる、社会が享受できる利益（社会的な収益率）と私的な利益として確保できる利益との乖離が大きいものは、政府がサポートする必要があると考えられている。また、社会全体で投入されている研究開発投資や科学技術の予算は、生み出されるリターンと比較して過

少であろうという考え方が多数の経済学者にあり、何らかの公的な支援が必要であろうとも考えられている。ただ使い方にいろいろな無駄があったり、効果が薄かったり、ということがあり得るので、制度設計には相当注意が必要である。

具体的にどういうものが効果が高いのかというと、全員が予防接種をしないと効果を期待できない感染症対策のような、マーケットを経由しないでさまざまな効果が及ぶ、外部性あるいは外部効果が高い領域がある。市場では適切な開発投資は行われないので、公的なサポートが必要であると言われている。また、研究開発の側面でいうと、例えば、知識が広くリユースされるような領域、すなわちプラスの外部効果がある領域においても、合理的な公的投資が行うことができる。したがって、生み出される知識の公共財的な性格がどの程度強いのかによって、公的支援の強度が変わってくる。ところが商用化が見えてきた段階だと微妙であり、どこまで公的支援が必要か、というのは程度問題であるので、その見極めはなかなか難しい。

科学政策と技術政策で、担い手のモチベーションの違いがあり、市場に投げていて最適な効果を期待してよい技術政策と、公的資金を使いながら多様性を維持しつつ、基礎研究を行うこととがよい科学政策とがある。これはだいぶ話が違ってくるので、科学政策と技術政策とは分けて考えるべき。

民間企業が商用化していくプロセスにおいても、市場競争の過程の中で、良い技術が商用化されないというのはあり得る話。そういう場合にはなんらかの介入的な措置を正当化できる余地がある。ただし、あまり政府がある特定のプロジェクトに介入しすぎると、不確実な技術領域ではかえって劣った技術になってしまい、さじ加減が難しい。

○　全体の考え方で二点、質問がある。

一点目に、情報セキュリティ技術戦略を考えるときには、アジアのIT環境全体をにらみセキュアなIT環境をリードしていくか、日本国内だけを考えるか、どちらがよいのか。

二点目に、この目的マップはすべて情報の話であるが、経験上、ハードウェア、建物等の周辺環境全体や組織を管理しなければ、全体の安全・安心というのは守れない。システムダウンとかバグ、改ざん等のみに集中して議論するべきなのだろうか。

○事務局：　一点目の国内だけ見ていればよいか、あるいはグローバルな視点でものを言うべきか、という話については、立場を明確にすれば場合にはよってはどちらもあり得ると考える。例えば関税によって国内を優遇するというのはツールもありうるし、情報セキュリティ分野でイニシアティブを発揮するために、アジア戦略を検討するというアプローチもある。

○事務局：　マーケットの開放性というところでわが国は成り立っているので、基本的には技術が社会に出ていくプロセスはグローバルマーケットを前提に考えるという流れであると思っている。

○事務局：　二点目については、建物の鍵のシステムやナショナルセキュリティ等の周辺

環境についての議論も確かにあってもよいと思うが、どこまで広げて考えるか、本委員会において投資戦略を決定する場で検討すべき内容かどうか、ということについては注意が必要である。

○　目的マップのような形で整理することは重要。ただ、丸くなって当たり前の対策だけが残るということについて懸念がある。例えば、機密性・完全性・可用性に加えて「その他」というカテゴリーもあるとよいと思う。平面の上に全体を統合するような方針を考える必要があるのかとも考える。機密性については、第３者にとっての機密性であるが、最近は情報を取り扱う人にとっての機密性も出てきている。例えば、疫学調査をさまざまな機関が行っているが、個人情報を出せないということでデータのマッチングができなくて困っている。情報処理マッチングを行ったとしても、その人が最終結果を見られないような、例えばスマートカードの大型版を作る等の仕組みをどう作っていくか。そのような見方も必要。

○　目的マップ、よくまとまっていると思う。ただし綺麗にまとまっているものは概して、やや表現が抽象的になっていると思う。抜けがないか等について実務を行っている方から緊急性、プライオリティ等の観点からご意見を頂くのがよいだろう。昨年度のグランドチャレンジ検討ＷＧにおいても、最終的に報告書に盛り込まれた内容はかなり精選されたもののみであるが、途中の議論はさまざまな観点からの検討があり、それは報告書にも生かされている。

○　目的マップについては、重要なものが落ちてはいないかという懸念がある。例えば、縦軸がすべて「～防止」である。”Protect”というのはネガティブな表現なので、ポジティブにセキュリティを考えるなど、ダイナミックにセキュリティをとらえることで何かが見えてくるのでは。

○　昨年度もグランドチャレンジＷＧにおける検討の際にも、外からの攻撃を防ぐだけでは効率が悪い、本当は元のところを断たなければ本当の対策にならないというご指摘もあったが、連携が非常に難しいところ。先生方もご承知のとおり、IETF(The Internet Engineering Task Force)においてもトレースバック技術の標準化の話は非常にブレーキがかかってしまう。ただ問題意識というのは忘れないように書いておかなければならないと思う。

○　ボットの問題においても、ＩＰトレースバックしてボットＰＣを捕まえるだけだと効率が悪く、なんとかしてボットをコントロールしているハーダー（攻撃者）のコンピュータまでたどり着かなければならないという話はある。ただ難しいところもあるので、大きな目的を設定しつつ、どういう順番で進めていくか、という問題はある。

○　この目的マップというのは過去議論してきた内容が反映されているのか。

○事務局：　おおむねその通り。事後対策については、現象を断つのか原因を断つのか、という問題は以前からあった。

○事務局：　情報セキュリティはそれ自体では成り立たない学問・技術分野である。他の

行いたいことに付随して起こる何かを解決するものである。しかも、現在、ＩＴ分野全域をカバーしなければならなくなっており、何か投資を行ったとしても不完全な解しか出来上がってこないという問題がある。そのような技術分野の例を他にご存知であれば、委員に教えていただきたい。

○　技術の連関を考える際に、moduleがどういう関係性をもっているかということにはいろんなパターンがあり得る。暗号等の非常にジェネリックなものは大学で研究する必要がある。また、補完的に利用されるものは、必ずしも公的に開発する必要はないかもしれないが、相互利用可能である必要がある。

技術開発の担い手が誰かということにもより、産学官に渡るものであれば知見のコーディネートが必要となる。

○　先ほど委員がおっしゃった、目的マップの中で縦軸がすべて「～防止」でありダイナミック性に欠けるという話であるが、これはITセキュリティとは何か、ということにも繋がる。安全に契約を行う上でのidentificationが安全に設計されるIT環境をつくっていくという話であれば、ダイナミックなものになるのではないか。攻撃があって防止するだけではなく、基盤をつくるべきという話は情報セキュリティについてはよく言われるところである。その話が目的マップにうまく入っていると面白いと思う。2000年くらいにアジアPKIフォーラム等でアジア全体をidentifyして、迅速に企業間契約を行える環境をつくるためのイニシアティブをとるという話があった。現在、再びその検討を行う必要があるのではないか。

○　確かに公開鍵暗号で新しい価値をつくっていくという話は過去あったが、最近は新しい価値をつくっていくというのは、少し見えなくなっているという感じはする。セキュアＬＳＩ、セキュア組み込みチップにある種の基準を十分クリアできるような製品をつくっておき、それをベースにさまざまな製品をつくり、日本の競争力を増していくということができれば、非常によいことだと思う。ただゼロリスクにはならないという問題に対応するのは非常に難しい。常に守りだけを積み重ねていくというのは非常に難しいと思う。

○　研究投資を行ったものの商品価値があるかどうか分からないものでも、例えばシステム攻撃の発生などの偶発的な要素によって突然システムのプロテクションの需要が増す、というような偶発的に商品価値が増すという場合もある。PKI（Public Key Infrastructure）もEGP（Exterior Gateway Protocol）の経路を守るために使おうかという話がインターネットのオペレータの間で粛々と進んでいる。テクノロジーとして習熟して放り出しておくと、開発された技術が３～４年たってから当初の想定と別のところで価値が見出されて利用されるということがよくある。逆に昔の方がそういう技術開発をやっていてくださらないと、現実的な問題を一から片付けなくてはならない上に、間に合わなかったり、十分な検討がそのときの担当だけでできない場合があるので、必ずしも投資したのがそのときに何か見えてないといけないというわけではないと思う。

例えば、５年前は回線費用にセキュリティの追加料金を払うという意識はなかったが、去年あたりから払うという人が増えてきた。社会的な常識の転換が行われるとビジネスモデルが大きく変化する。想定された範囲内での効果の測定しかできないというのであれば見誤るだろう。

また、ゼロリスクということに関して、我々はよく、セキュリティ上のリスクはClearance（除去）できるものではなく、mitigate(軽減)するものであると言っている。Protection Device とは言わず、Mitigation Deviceと言う。目的マップに書いてあるのは０か１の話であり、本当は、ここに全て「なるべく」というのがくっつくはず。0～100%のどの程度これができるのか、という軸があればより分かりやすいと思う。

防止と逆の観点から、攻撃の話であるが、攻撃手法の研究にはなかなか踏み込めない。攻撃手法について考えてみることは防御にとって最重要であるが、犯罪を構成してしまうことが多く、ある特定の環境で権威のある人たちが積極的な攻撃手法を研究する際の方法について検討することは、技術戦略にとって非常に重要だと思う。

○　米国では攻撃させるツールがあって、それを用いて防御を学ぶということが行われ始めており、それは今後やはり日本でも行っていかねばならないと思う。どんどんレベルが高くなっていき、頭の中だけで考えてもそれを防げない。

また、開発した技術が使われないという問題については、将来を考えて必要になるであろう技術というものは、時間差はあっても、どこかで使われるはずである。その意味ではいろいろと方法はあり、あきらめない方がよい。ただ、企業としては、評価に繋がるかどうかは不明である。つまり、時間が経ち、当たり前の技術になってくるとお金は支払わない、ということになり、投資が回収できるかというのは企業としては難しい。

イ　高セキュリティ機能を実現する次世代OS環境の評価

【事務局より資料２に沿って説明】

○　BitVisorの特徴などの概略をご説明いただきたい。

○事務局：　ただ単にVM（Virtual Machine）というと物理ハードウェアをスライスしてソフトウェアからはハードウェアのように見えるような環境を多重に作り出すもの。これで、例えば一台のノートパソコンの上で複数のOSを同時に稼動したり、クライアントとサーバを同士に稼動したりといったことができる。その考え方を拡張し、セキュアな環境を提供するためにVMを使う、という考え方でセキュアVMは作られている。OSをセキュアにするのは非常に難しく、いくら対策をとっても穴がでてきてしまう。あるいはユーザの簡単な操作によって外部からなにかを呼び込んでしまう。OS自体を改善するのではなく、その周辺で起きることを監視してあげて、不正なネットワークの監視、USBメモリからの書き込みが起きそうになったら検査又は停止する、そもそもそれを許可しないだとか、ということができるようにする、といった方法でVMを使ってセキュアな環境を実現するものだった。BitVisorはさらにその考え方を一段進めて、ネットワーク上で

業務システムが走っている場合、普通はサーバとクライアントの間で通信を行って業務をこなしているが、業務が走っている仮想的な面全体をプロテクトした空間を作ってあげようというもの。

○　面白そうな話なので、ぜひそれが広がっていくといいと思う。

○　資料２の12頁、経緯及び今後の予定に関して主語を確認したい。科学技術振興調整費の実施主体は筑波大学になっているのではないかと思うのだが、内閣官房はどのように関わっているのか。

○事務局：　科学技術振興調整費の実施主体は筑波大学で、昨年度で開発は完了している。内閣官房は実運用環境において想定される利用者、想定される利用環境を有している組織ということで関わっている。仕様要求の提出、研究運委員会の一員として進捗状況管理などを行ってきた。「今年度は、政府機関でのセキュアVMの導入・運用に向けた課題整理を行う予定」との記述に関しては、主語は内閣官房である。

○事務局：　重要課題解決型研究というカテゴリーは、政策課題とそれを実際に解決できうる研究グループが一体になり、全体の設計を行いプロジェクトを推進するもの。実施者は研究者側であるが、運営委員会側は科学技術振興機構のプログラム運営者、内閣官房、総務省、経済産業省等の政策担当、委員長が実施担当の代表者になるという構造で動いている。技術開発の政府内での利用については、内角官房が行っていこうとしていたもの。

ウ　研究開発プロジェクトの管理・評価体制の改善

【事務局より資料２に沿って説明】

○　この施策の出口はどのような方向か。

○事務局：　まだ決まっていないが、国のプロジェクトにおいて該当する手続きが見つからないだとか、予算の目的・性質に合わせてベストな変更の方法について合意したものが共有できればよいと思っている。

○　研究変更の柔軟化ということだが、報告書２００８にあるように年度間の流用性が自由であればそもそも問題は生じないのかなと思うし、あとはいつの時点で審査を行うかということも関係する。審査した上で３～４年なりの間は自由に研究してもらう、というスタンスもありうると思う。その場合も一年ごとになんらかの評価を行うということになると思うが、評価に向けられる全体のリソースの配分方法も関係すると思う。外国の例も参考にすると良いと思う。わが国では最初の段階でのセレクションにリソースをあまり割いていない。方向としては賛成であるが、どこまでやるかということも含めて議論していきたいところである。

○　中間成果の活用の事例が見つからないというのは、成果が活用されていないということなのか。

○事務局：　中間成果の活用がされていることはあるかと思う。ただし国の施策としてプロジェクトを実施する上で、最終成果がでるのを待ってから利活用するのではなく、途中成果を活用することをポジティブに推進する仕組みを調べたときに見当たらなかった。

○事務局：　全体として計画経済的な運営になっていて、3年間で研究、2年間で成果活用の促進などときっちり決まっている。利用可能なサイドエフェクトが出た場合、あるいは、海外で技術の標準化が行われ、自分の実施していた研究が無意味になってしまった場合においても最後まで研究を実施して結果を出すことを求められる。さまざまな状況の変化の中で研究計画を切り替えていくときに制度の面などからどう吸収するかということを考えていかなければならないというのが根本的な問題意識である。

（5）資料の公開と今後のスケジュールについて

○　事務局：　次回委員会の日程はまた別途調整させていただきたい。

（6）その他

○　研究開発プロジェクトの管理・評価体制の改善については昨年から他のところでもいろいろと議論があった。プログラムオフィサー（PO）にヒアリングした結果、自分にどれだけの権限が与えられているのか不明確であるということであった。まだまだいろいろな努力をしなければならないが、改善の方向に向かって進んでいるんだろうと思う。

○事務局：　POは自分で何も決められないというところがある。

○委員長：　ご議論有難うございました。議論はこれで終了したい。