技術戦略専門委員会グランドチャレンジ検討 WG
第６回会合議事要旨

１．日時　平成２１年2月１７日（火）１７：００～１９：００

２．場所　内閣府本府５階特別会議室

３．出席者

［主　　査］
後藤 滋樹（早稲田大学教授）
［主査代理］
安達　　淳（国立情報学研究所教授）
［委　　員］
磯村 浩子（(社）日本消費生活アドバイザー・コンサルタント協会）
伊藤 光恭（ＮＴＴ情報流通プラットフォーム研究所）
加藤 雅彦（(株）アイアイジェイ　テクノロジー　IBPS 本部）
楠　　正憲（マイクロソフト（株））
西本 逸郎（(株）ラック　サイバーリスク総合研究所）
二木 真明（住商情報システム（株））
松並 勝　（ソニーデジタルネットワークアプリケーションズ（株））
三河尻 浩泰（(株）富士通ソフトウェアラボラトリ）
森山 浩幹（(株）エヌ・ティ・ティ・ドコモ）
山田 安秀（(独）情報処理推進機構）
（五十音順）

［政府］
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参事官付
警察庁情報通信局情報技術解析課
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
文部科学省大臣官房政策課情報化推進室
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
防衛省運用企画局情報通信・研究課情報保証室

４．議事概要

＊＊

議題　報告書（案）（４章：解決すべき課題と将来イメージ部分）について

＊＊

○　もう少し具体的な物の名前やテクノロジーを書き込むことは抑えた方が良いのではないか。例えば、ＩＴＳの部分でＩＣカードを差し込むと運転者が認証されるという書きぶりだが、これはＩＣカードでなくても良いので自動車が運転者を認証するという機能を書けば済む話だと思う。この辺りは精査し、必要のないところで個別具体的なテクノロジーの名前を書かないようにした方が良い。

○　いろいろなところにＩＴが使われるようになっているので、ＩＴを利用した計量システムを不正に改ざんする事案の発生なども報道されている。特に公共サービスにおける計量や課金などについては、システムや仕事が適正に行われているかを検証出来るような仕組みが必要だと思う。この種の議論はこれまでのWGで行ってこなかった視点だと思う。

○　長さや重さの適正さは国家が管理しているが、これの将来判のようなイメージだろう。

○　将来イメージ部分でキーワードという部分は浮かび上がっているが全体が見えていない。例えば、より機器と機器が複雑に結びつき、システムが相互作用してセキュリティの対処が難しくなる複雑性の部分や、人間社会が今以上にＩＴに依存することによって復旧したときに結構難しくなることなど、根幹となるセキュリティ上の課題をもっと打ち出すことが出来るのではないか。それの要素は既に書いてあると思う。見出しを書いてゆけば本当に大切な情報セキュリティ上の課題が浮かび上がってくると思うし、そうすると、４．１の少子高齢化、地球温暖化ともうまくつながってくると思う。

○　将来イメージには内容の重複があり読みにくいので整理するべき。（目覚まし時計が沢山出てくるなど）

○　利用者イメージの視点からは書きにくいかもしれないが、セキュリティに関する攻撃や脅威の観測技術というものは運用上重要だと思うので、そのような指摘が書き込まれると良い。

○　観測系の話はここには書きにくい、視点が家庭環境、通勤職場環境、娯楽…となっているので。

○　Ｐ３８の短期的・中長期的な研究開発の方向性のところに入れてはどうか。

○　検討する。

○　将来イメージのうち家庭環境のところには、いろいろな分野のことが書いてあるが、いわゆる防犯ということについては触れられていない。例えば、ホームネット管理会社というものがあって、それにはベンダー、通信事業者、警備会社などが参入すると

の記述もあるので、今のいわゆる家庭の防犯というものをどこかに盛り込むべきではないかと思う。

○　比較的低速なデータ通信線というものは、昔から警備会社などで夜間に無人になるような場所の監視には用いられており、相当数の需要があったと思う。

○　家庭の安全性を確保するという部分は、ご意見を踏まえたい。安全性を IT で行っているというアプリケーションイメージと、その安全系について情報セキュリティ上問題が起きては困るという、その２点について留意したい。

○　本論とは少し外れるが最近はグリーンやエコの流れがあるが、その視点から今回の報告書（案）を見ると、どんどん消費する電力が上がってゆくイメージがある。これはマイナスの印象を与えかねない。おそらく 2020 年頃になると各装置の電力消費量は劇的に下がっているのではないかという期待もあるので、将来イメージの前提には電力を多量に消費する様になるわけではないというコメントを頭に書いておいた方が良いと思う。

＊＊

議題　報告書（案）（５章：情報セキュリティ技術に関する戦略部分）について

＊＊

○　将来イメージの部分には先ほどから「生活」等のキーワードが出ていたが、見出しの中にそれを付けた方が内容は分かり易いと思う。

○　前回の WG で「構造的な製品開発の「知」の共有」と題して、製品（開発工程）のライフサイクルについて議論した。その中で流れの終わりが「運用」で止まっていたが、私は故障・寿命・廃棄まで含めて考える必要があると指摘した。これは、どこに反映されているか。

○　今回の報告書（案）では、このライフサイクルの議論をどこに位置づけるかという問題が解決されておらず、現段階では反映していない。もし、適当な位置について意見があれば伺いたい。

○　この話は、盛り込んだ方が良いと思う。

○　将来ビジョンと技術像のうち「サービス・ベンダ」の領域における記述に、体系的な運用やライフサイクル、フレームワークという言葉があるので、ここで書いてはどうかと思う。

○　報告書に記載されている「体系的」と「運用」という言葉を見ながら、どこに書き込むか検討する。または、新たにまとめて文章を起こすかもしれない。前回のＷＧで戦略性について議論した際に出た話なので、大きめに書いた方が良いかもしれない。

○　前回に委員が指摘したとおり、製造者の予想を遙かに超える古い物が使われ続けていて、そのようなものはセキュリティに関しても脆弱であるということがあり得る。また、現在も物を廃棄するときにどこまで対策をすれば良いかと言うことは明確になっておらず、CD や DVD をシュレッダーする人もいれば他のやり方をする人もいる。

捨てるときにどの程度までやれば良いかは、その物の仕組みをよく知っている人は対応できるが、知らない人は分からず困ってしまう。だんだん物の捨て方が難しくなって行く。

○　個々の機器にライフログ的な情報が沢山入った形になって、かつ、それをリセットする方法が分からないというケースが増えてくると思う。例えば、私が携帯ゲーム機の中古のソフトを買った時に、前の持ち主の点数がそのまま入っていたことがあったし、体重計に体重の推移が残っている程度の話であれば気持ち悪い位で済むだろうが、リース切れのパソコンを中古市場に出したところ、内部に残っていた個人情報が何万人分も漏洩するという事態が起こっている。デジカメなどに使われているフラッシュメモリーでは簡易フォーマットしただけでは、そこからデータを復元されて見て欲しくない写真がみられたりするなど、利用者のリテラシーが追いつかないまま、中古市場がこの不景気でますます広がってゆくと言うことはあるのではないかと思う。

○　５章はこのレポートのコアだと思う。前の方のグランドチャレンジの定義には「特定の大目標を設定」と「各要素技術全体の統合的開発を行う」グランドチャレンジ型の研究開発を設定することが注目されていると記載されている。これに対して５章で応える必要があると思うが、研究分野の方向性ということで挙げられている４つが今回のグランドチャレンジだといえるものなのだろうか。何かグランドチャレンジとしての答えが必要なのではないかと思えてならない。また、このグランドチャレンジを誰がやるのだというところは、政府がということでもなく、産業界が単独ということでもなく、日本全体としてやるということで良いのか。グランドチャレンジの牽引者として考えているのは、この報告書を見て、自分が当事者だと思う人が自ら牽引してゆくということを期待していると理解して良いか。この報告書は NISC が出すグランドチャレンジなので、政府が牽引者となることを一般の国民は期待すると思う。もし、そうではなく民間も大学の研究期間もそれぞれが当事者でありプレイヤーであるということであれば、その主体を書かなくてはならないと思う。細かいことは他にもあるが、５章は重要なところであるので角を押さえた展開になれば非常に良いと思う。

○　委員が言った４つの方向性は、私（事務局）からの提案である。これには各委員の意見を盛り込んだつもりであるが、これがグランドチャレンジのテーマになるかと言われると、まだ、そうではないと思う。１０年かけて行う仕事量はあると思うが、例えば、２番目の「利用シーンに応じて動的にセキュリティレベルを最適化するシステムの実現」では、ネットワークのアーキテクチャーから考えなくてはならないし、あるいは、マシンのアーキテクチャーも考えなくてはならない。バーチャライズドされたところで、何を根拠にして何がどこにあるとか、だれが管理・監視してゆく仕組みなども重要なテーマだろう。書き方はともかくとしてチャレンジングな内容だと思っている。ただ、これがグランドチャレンジかというと、まだ、世に言い放つ状況ではないと思う。それは、先ほど委員が言ったように、牽引する人が誰なのかが決まって

いないということがある。報告書の性質としては NISC の報告書として内閣官房がこれを基にコーディネーションしてゆく、実態としては、これを参考にして皆さんいろいろなことをするということで良いと思うが。この牽引者については、暗黙のうちに了解があるのか、または、明示的に書き込んでゆく必要があるのか。

○　主体については、もう少し書くようにしたい。ロードマップなので「将来予測」の部分はある程度の共通認識を持ってもらう材料として書いているものであり、全てを国が実施するわけではなく、国が行う部分もあり、民間がやる部分もある。その点はもう少し書くようにしたい。グランドチャレンジのテーマについては、テーマとしてではなく方向性と書いたのは、テーマを決めきるのは難しく例示的に方向性を書いた方が良いと思うためである。国が何をやるのかという点については、NISC はもちろん関係府省庁と調整をしてどこをどう担って貰うかを考えていく必要がある。

○　全体として、個別技術の積み上げと１０年以内に実現可能と思われるものを網羅的に書いているような印象があり、もう少し、例えば、危機感として今後５年１０年以内に今の技術では解決できない何らかの深刻な事態が起こるという問題意識など、グランドチャレンジと呼べるような大きなチャレンジが見えていると良いと思う。おそらく攻撃の種類としては、ビジネス目的の標的型攻撃が増えるとか、潜伏して顕在化しないものが増えているとか、ネットに対する国民の生活の依存度が高まっている状況に対して、サービス側の品質が担保されているかというと、先日も今１週間くらい止まっているブログのサービスがあるなど、技術的に可能か不可能かというのとは別の次元でサービスの信頼性が保たれない場合が増えていて、個人的にはこれをどう研究テーマに結びつけてゆくか非常に難しいが、これからの日本では技術的に出来ない問題よりも、技術的には可能なのに、なぜ、このようなものもやらないのだろうという問題が増えてくるような予感がある。

○　大手町の近くにはデータセンターが多い。田舎に持ってゆけないのかと言われるが、やはり、直ぐに駆けつけられるところになくてはならないのだろう。仮想化の部分やクラウドの部分は遅れているわけだが、仮想化の部分が進展すると日本から出て行ってしまうという問題と、仮想化においては捜査という観点からだけではなく、調査や分析という面からも何が起こったのかを把握する仕組みというものが級数的に難しくなっている。捜査について私はプロではないが、仮想化されたところから証拠の連鎖をどのように確保するのか、そのためのフォレンジックツールの開発とか、例えば、いつの間にか海外に移転していた自分のサーバーを調査するための仕掛けや仕組みを確立するなどのことは、課題でありチャレンジすべき事項なのだと思う。

もう一つは重要インフラの分野で基幹の業務とあまり関連のないサービスの運用において、今はまだ、何か問題が発生したら止めれば良いという発想で対応する事業者が多い。これが今後５年１０年と経つと依存度が高くなるので、これまでのように止めれば良いということではなく、サービスは継続し続けながら対応しなくてはならな

い。このような大きな転換期を近々迎えることになると思うが、この報告書に書くか否かは別として、それに備える仕組みを合意形成も含めて考えておく必要がある。いずれにしても仮想化の部分については１行触れておくべきである。

○　仮想化によって簡単になるのか難しくなるのかということでは、簡単になるところもある。ＯＳよりも下のレイヤーで動いているものでは、切り離してモニタリングする仕組みを作ることが出来るので、仮想化そのものはシステムを可視化する、ある状態を保つということにおいては非常に有効な部分はあると思う。一方でどこにあるかも含めて完全に仮想化されてしまった場合には、指摘のとおり捜査権が及ばなくなるなど、データについて主権を行使できない場面というのは今まで以上に起こってくるであろうし、その辺りのことを深く考えないで様々なシステムが日本国外のクラウドに行っている実態はあると思う。基本的に日本以外の国では、司法傍受だけではなく行政傍受も幅広く認められて、広く捉えて国益に叶う話となれば、産業スパイ的に中のデータを見ることがその国の法律的に触れなければ事業者としても従わざるを得ないような状況があり、いかに日本にとってクリティカルな情報が日本国内に留まった状況をつくってゆくかを真剣に考えてゆかなくてはならないと思う。ただ、一つ、大きなクラウドを運用している立場でいうと、まず、日本の電気代が高すぎる、しかも、土地の安い山間僻地の様なところでは、回線の競争が無いので高い回線を借りなくてはならず結局コストが高くなるので、どうしても日本に置かなくてはならないクラウド以外は置きにくいという実情がある。日本に寄せてゆくということと、海外にあるデータに対しても、いかにコントローラブルでマネージャブルにしてゆくかを考えることが重要だと思う。

○　トラステッドＯＳの話が出たので思い出したが、先ほどのプログラムの改編事件への対応について、あれは対システム改変技術なので内部犯行に備えた耐タンパー技術というコンテクストで読めると思う。

○　Ｐ２７の不正プログラムに強い計算機環境というところがある、ここでは不正プログラムについて書いてあるが、いわゆるハッキング的な攻撃の部分について書いたところがないので、これを束ねて、ここで言うプログラムの正当化保証、利用者、運用者が勝手に改ざんできないようにするなどのことを書いてはどうか。

○　ちょっと、直接書き込むのは難しいので、文言の書きぶりで対応したら良いと思う。もう一点、クラウドについては、どれだけ流行るかは分からないがこの動きは避けられないと思う。先ほど委員から指摘のあった、クラウドの関する注意点については、Ｐ３６の最後の３行くらいに関連した事項は書いてあって、利用シーンに応じて動的に変更して直接見せないようにしようとか、秘密分散して秘匿演算させるとか、その辺りのことも書いたつもりである。この辺りは、携帯電話でＷＥＢサービスがどんどん進んでマッシュアップで何でもできるとなったときに、このような技術をペアにして開発してゆかなくてはならないと思う。また、データセンターを国内に置くという

話もＰ３６の５行目あたりから、コストに見合うと判断されたら置く場所や使うコンピューティング要素なども考える必要がある、それらを全て合わせてアダプティブ、オプティマイズドということ。それから、フォレンジックスはＰ３７のところで気持ちとしては書いたつもりであるが、明示的に書いていない。また、Ｐ３７はいろいろなものがバーチャルになって、ＩＤＳとかを動かしプロテクションとディテクションをどうするかという話であり、フォレンジックスのことは明確に書いていないので、これは必要だと思う。何か起こっても後から何も分からないというのは情けないことだと思う。私事だが、以前に空港の自動販売機で航空傷害保険に入ったにもかかわらず、後日、契約が成立していなかったので保険料を返却するという連絡があった。私も素人ではないので、契約が成立したことを画面で確認していた筈だが、保険会社側はログを確認したところ契約が成立していない状況であったとのことだった。しかし、自分としては契約が成立した画面を見ているつもりである。よって、利用者と提供者のそれぞれで、そういった事実関係を事後検証が可能となるように、耐タンパー性があってごまかせない仕組みが必要だと思う。

○　先ほどの改ざんの話ではないですが、単純な間違えの他に、意図的に不正が行われる可能性もあるので気をつけなくてはならない。

○　大枠の話だが、社会ビジョンと言うところで、情報弱者、IT リテラシーの高くない人たちにどう安全にシステムを使って貰うかを議論してきたが、世代的には高齢の方はデジタルデバイドで、我々中間世代はデジタルイミグラントで今の若い人はデジタルネイティブだということを考えると、ここ５年から１０年くらいの戦いはデジタルイミグランドとデジタルネイティブとの戦いになるのではないかと思っている。今日、会場に来る際に乗った電車で隣に若者２人が座っていて、「おい、今降りた奴さ、マジコンもろに見えてたぜ」、「あれは、見せちゃいけないよね、せめてカバー付けておかなくちゃ。はら、俺のはこうなっているんだ」という話をしていた。こんな出来事から思ったが、そんな世代の人たちを、今システムを作っている我々もしくはわれわれよりも少し下の世代が指導していかなければならない。これはかなりタフな課題だ。彼らのほうが教える側より、システムを知っているということも多い。これは過渡期の課題だろう。やがて、彼らが指導的な立場に立つとまた別の問題が出てくるだろうが、これはまだ未知数。ただ、こうした困難さについての記述があっても良いかなと思った。

○　先ほどのデータセンターの話で、弊社もデータセンターを持っている立場から発言させて貰うと、仮想化の話とクラウドの話とは別のものだと思っている。仮想化はライセンスが安いものをしっかり使えば、コスト的にかなり抑えられる上に、実際にサーバーを立ててサービスをするよりリードタイムが非常に減るという利点があって、決して悪いものではないと思っている。ただ、聞いた話によると、非常に重要なデータをクラウドに載せている会社も中にはあるとのことで、万一、そのようなデータが

他国でシャットアウトされて使えなくなったらどうなるのかと。逆に、個人情報の管理やシステムの管理がしっかりしている日本が、このような重要なデータを扱う分野で強みを発揮するのではないかという話もある。逆に見るとコスト的な問題で、あまり SaaS 事業や ASP 事業が出来ていない日本というものがあって、そういったところを伸ばしてゆくためのセキュリティなどは、取り組んで行くべき分野だと私は認識している。世界に出て行ってしまうのが問題なのではなくて、日本に呼び込めないのが問題だ。ASP 事業や SaaS 事業はいずれ避けて通れない道になっていて、大きなところと、小さなベンチャーに２分されている。ここに問題があるという気がする。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

議題　報告書（案）（６章：公的資金を用いた中長期的な研究開発の実施方法部分）について

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

○　全体的に今回の報告書で取り上げられているテーマの多くは、かなり商用化に近いセキュリティ技術が多く、ここで、書かれている研究開発というのは国の資金を使って従前の枠組みの中でやる場合での目標設定などの話が主になっている。しかし、米国などの予算の蒔き方で見ると、研究開発フェーズのものだけではなく、その後のインキュベーション（起業支援）フェーズの中で良いものは高くても買うというような、購買を通じてベンチャーを育てるなど、もっと幅広いイノベーションパイプラインのなかで基礎研究を位置づけているように思い、その辺りの話がそっくり抜けていると感じた。もう一つは現実的な話として報告書で議論しているプロジェクトの予算は、この作業が何人月というような積み上げ型で金額を決めてゆく前提でやっていると思うが、果たして優秀なセキュアプログラマを１００万人月で雇えるのかという問題がある。セキュアプログラミングはかなり特殊な能力なので、民間であればそれなりの対価を支払わなければ受けられないサービスである。従来型の積み上げによって組んだ予算でプロジェクトマネージメントをいくらしっか管理しても、３年、５年というタームで素晴らしい結果を出すことはかなり難しいのではないかという印象を持っている。弊社でもルートキット対策とか、OS の基礎技術の部分でいろいろ苦しんでいるが、最後は良いものを造った会社を買うしかないという状況になっている。この報告書の議論は完全に国主導で２年とか３年で結果を出すというのを念頭に置いていると思うが、特にソフトウェアは開発した後のメンテナンスの方が費用かかるし、実社会に適用してゆくところ困難さというものがあって、例えばセキュア VM のように物は出来たが、これからどうして行くのか見通しが立っていないプロジェクトがあるように、プログラムマネージメントだけでは解決しない問題であるという気がする。

○　インキュベーションのところは、「技術戦略専門委員会報告書２００６」で、調達の中で買って行くべきであるとの提言はなされているが、ただし、実際に国が税金で物を各仕組みとしては難しいところがあって、なかなか実現していない。その問題を再

認識した。

○　正直に言って調達の改善はかなり難しい。国で買うものはある程度技術的に安定していて、かつ、安いものを買うべきであるというのが大方針で、新しくて不安定でどうか分からないものを良いと思われるので買うというマインドは全くない。同様の指摘は他の委員会でも議論になったことがあり、もともと価格の安い物を買うというのが大原則だった会計法の世界も、単なる競争入札だと品質や信頼性に問題が出てしまうので、価格だけではなく技術的な要素を加味するようになってきた。さらに技術の中身をベンチャー、中小企業、スモールビジネスについて優遇するというような話は以前から IT 戦略本部などでも出ているが、ようやく技術点が加味されるようになった段階だ。安定した品質で安い物を買うと言う考えは崩せていない。

○　USTR の介入などもある。国の研究開発で造ったから優先的に導入するというのは、現実門だとして難しいと思う。

○　多分 WTO の TBT などいろいろあるが、ただ、ナショナルセキュリティというと許される部分もあって、日本はちょっと字面どおり読み過ぎているところがあると思う。ここは、諸外国の例などを参考にしたら良いと思う。ここ何年かは非常にフレキシブルになってくると思う。

○　P41 のセキュリティだけの議論ではなく、一般論の議論ということはもっともだと思うが、一方でグランドチャレンジであればこその特別な要素がステートとして、マネージメントとしてあっても良いのではないか。グランドチャレンジで 10 年を見据えるということは、相手は人であり、自然科学と違ってどんどん状況が変化して行くことで、かつ、長い期間に渡る話ということであれば、変わって当たり前であろう。そういう特徴をもっと鮮明にテイストとして出すべき。

○　積極的にセキュリティ以外について議論をしたいという趣旨で書いたのではなく、出来るならばセキュリティに限った議論の方が望ましいのだが、現状の仕組みを前提とするとセキュリティだけ切り出して議論することが出来ないのでこういう形になっている。運用レベル、あるいは資金を運用する団体の内規、PO のガイドラインレベルなどの下位のレベルではセキュリティ分野に限ることは出来ると思うが、一般的な公募の世界とか、研究開発の指針、規則のレベルになると情報セキュリティだけ切り出して書くことは出来ないので、原則論として計画変更が可能であるべきと書く必要があるという問題提起となっている。なぜ今書いていないかということの理由もあるわけで、そこは今後とも関係機関と調整したいと思っている。おそらく指摘のあった、情報セキュリティで、かつ、グランドチャレンジだからよりダイナミックであるべきということは、そのとおりだと思うので、仮に、どこかの省庁で実際にそういった特化した資金配分機関などができれば、それに対して今の議論をすることになると思う。

○　第６章において、日本ではアメリカを中心に外の制度をいろいろ入れているのですが、それぞれ担当しているところは、しっかりとフォローをしているという風にまと

まっているが、パッチワーク的に今まで出てきているご意見をまとめても、自分自身の研究費を貰うという立場から言うと、Ｐ４６に書いてあるＰＯ、ＰＤというものの、裁量権を大きくすると言うということがポイントだと思う。つまり、このソフトウェア開発にどのくらいの予算を付けるのが妥当かどうかというのは、基本的には主観で決まる話なので、それについて、ある客観的な基準でといわれても難しい。それと、もう一つは、グランドチャレンジというものは、かなりはっきりとしたターゲットを示さないと出来ないが、過去の我が国においても、高度成長期には国がかなりはっきりとしたターゲットを示して産業全体を牽引してきたということがある。しかし、今はそういうことがなくなってきた。やはり、凡庸な人がＰＯなどになると、あまり、大したことはできないので、かなりのカリスマ性が要求されることになる。そういったところで、本当の意味でのグランドチャレンジが出せるというのをやってみるということも大切かなと思う。基礎研究の場合では、例えば遺伝子の研究だと何をやべきかは、かなりはっきりと言えるが、セキュリティだと制度設計で見落としたところを突かれるということがあるので非常に難しい。そこで、前の方の章でいろいろな問題点というか将来像が列挙されている中で、どこが肝なのかを選んで打ち出すと言うのが、こういったグランドチャレンジのＰＯに期待されることなのだろうと思う。

○　やはり、ＰＯ，ＰＤがいかにプロジェクトを評価しながら見ていけるかが重要。P46にも書いてあるが、ＰＯ、ＰＤを研究者のキャリアパスとして入れることが必要。

○　以前米国の NSF に調査に行ったときに、NSF は国防省のような非常に大きな権限を持った PO ではないが、PO にはどんな人がなるのかを見たら、第１級の研究者になれなかった人のキャリアパスにもなっており、プロジェクトを設計したり、予算を獲得したりするような仕事に従事する。そういった人が大学に行くと、大学の学部長とか学長になる。本当の研究者は研究をしてもらうのが一番良い訳で、お金を投資してやればよい。そのあたりで持ち味が違うのでそこを意識してやる必要がある。

○　せっかくグランドチャレンジと言っているので、例えば DARPA のアーバンチャレンジのように賞金を設定するなど、今の日本にはないプログラムマネージメントと違うスタイルというものがある。是非、違うやり方があって日本では法律上出来ないということをどこかに入れておくのは、それはそれとして、問題意識として整理されて良いのではないかと思う。

○　昨年度のグランドチャレンジの検討では、グランドチャレンジの実施方法にもいろいろ出て、その中で「ゴール FIX 型チャレンジ」として賞金を出すとか、一番良い物を買い取るという話があった。

○　我々のところでは規模は小さいが、コンペティション型の開発をやっている。この取組は、短期的でターゲットをしっかり設定して急激に技術レベルを上げるという課題に適していると思う。長いスパンで課題設定をする場合は難しいかもしれないが。

○　調べてみるといろいろな制度がある。３つ並列で同じ課題の研究開発を進めさせて

いて、ある時点で３つのうち一番良い物を選定して一つに絞り、落とした２つの予算を集めて３倍の予算を付ける方法などもある。良くできていると思ったが、私の印象では制度は良く設計されているものの、末端の運用はうまくいっていないように思う。

○　人材の流動性の問題も大きいと思う。結局そういった研究予算を付けたときに、どういう人を集められるか、そういう人たちがどういったキャリアパスを描いてゆけるかという環境が日米でかなり大きく異なる。米国で良いプロジェクトだからといって、ルールだけをそのまま持ってきても、日本でも優秀な人材が来るということにはならない。

○　途中段階での成果の活用の話がもう少しあった方が良いのではないか。P48 に改善の方向性ということで３点記述があるが、これは、途中段階で公表するというところまでに留まっていて、では公表したら直ぐ活用できるのかというと、インダストリー側が見たときには結構難しい気がする。アイデアを活用すること位は出来るかもしれないが、本当に成果を活用してもらおうというときには、もう少し後押しが必要ではないか。

○　今のことに関連して、国プロで動くプロトタイプを作るということと、客に買って使ってもらえる物を作るというところには、工数にかなりのギャップがあり、おそらく工数は１桁２桁増える。そこをどういうタイムスパンとスキームで考えて行くか、また、以前話したとおり米国であれば筋の良い技術だと思えば大学を飛び出して３年か５年ベンチャー企業の経営をし、もし成功しなければ大学に戻ったり、どこかに技術を売り払って利益を得たりいろいろなキャリアパスがあるが、日本では優秀な研究者ほどアカデミックのキャリアパスから外れることを好まず、アドバイザー的な形でしかリスクを取れないのでスピード感が取りにくいのかなと思う。

＊＊
議題　報告書（案）（全体）について
＊＊

○　全般的に今回の報告書の内容は応用研究というか、既にある技術の話であり、セキュリティに関する基礎研究的なテーマがどれだけあったかは気になっている。仮想化などは 40 年近い歴史の技術だが、基礎研究フェーズにあるセキュリティ技術というのは余り議論されていないような気がする。本日の問題提起で言えば先ほどの航空傷害保険の話のように、自分の目の前で起こったことの電子的な記録の一致をどうやって確認するのかなどは実は本質的な問題で、それを解決する見通しが全く立たないので電子投票の目処が立たないことがあり、これなどは基礎研究だと思う。

○　５章に戻るが、先ほどの航空傷害保険の話ではログが実態よりも本物になってしまうということであり、IT 化が進むとそうなっていってしまうかもしれず怖い話だと思う。そうなると犯罪者が IT の利活用を進めて行くのではないか。P38 を見ると短期的

な研究開発の方向性、その次のページもそうだが、どちらかというと守る技術や守る研究が多いが犯罪者がどのような犯罪を起こして行くのかという研究もあった方が良い。今は、フィッシングでお金を稼ぐような初歩的な犯罪だが、だんだん人を陥れるようなより恐ろしい犯罪が起こるようなことが予想されるので、そのあたりについての研究も必要だと思う。

○　私は今、非常に危機感を持っている。それはこの酷い景気の中でセキュリティに対する意識が顧客や運用者や組織のトップの中で劇的に下がっていることである。計画的にしっかりと取り組もうとしても、それどころではないとの一言で、どんどん軽んじられてゆく状況が急激に起こっている。高度な情報セキュリティ対策が求められるある企業が、セキュリティ監査において指摘された事項を改善するための作業を、トップの一言で凍結されてしまうという信じられない事態も起こっている。さほど高度なセキュリティを求められない一般の企業においてはなおさらで現場も困っている。３年、５年、10 年というスパンの中で考える前提として、このように景気が悪くなり、セキュリティにお金が回らないという状況があることを考えるべきである。また、加えて治安が悪くなるのでサイバー上の脅威も厳しくなり、これからリスクは上がってゆくということを、弱りかけているトップ等の意志決定者にエールを送る意味でも語りかけられないかと思っている。そこで、１００年に一度の危機というキーワードがあったので、むしろこの時期の方がセキュリティの重要度は上がると言うことを書いておいたらどうかと思う。

○　良く、ＣＩＡ(Confidentiality,Integrity,Availability:機密性、保全性、可用性)と言うが、本 WG の議論もほとんどがセキュリティというと情報の保護だという印象だが、事故前提ということを考えると大切なのは可用性であると思う。止めないと言うこと。経営者も保護しろと言われると動機が湧かない。儲からないしコストがかかる話でしかない。ところが、止めるなと言う方向からのアプローチは比較的経営者層も聞く耳がある。そこから入って次のステップに少しずつ進めて行くという方法は良い。アメリカではＡＩＣと言っているそうなので、上手いやり方だと思う。だから、１００年に一度という時期には「止めるな」だと思う。

○ Ｐ８の下の図で、最終的な社会への実装に当たるところに記述されているように、技術を中心に書かれているのは当然だが、他に意識の向上や教育という技術以外の面についても是非触れて貰いたい。

○　同感だ。使うのは人間でありその点は非常に重要である。また、悪事をはたらくのも人間であり、例えばプライバシーの技術が高まれば高まるほど匿名の人から脅迫されて警察でも捕まえることが出来ないというようなことが起こる。今は、いたずらをして捕まっている話も聞くが、初歩的な「かわいい」位の段階である。

○　関連して、先ほどの電車の話に出てきた若いデジタルネイティブ世代をしっかり教育してゆく必要があると思う。

○　技術以外の要素についての委員の指摘についてですが、７章に「まとめ」の章置いている。何か足りない感じがしていたが、最後は単なる議論のまとめだけではなく、この技術戦略でカバーできないけれども重要で必要なことを書き込むという視点が抜けていたと思うので是非書き込みたいと思う。

○　P38,39 に掛けて短期的・中長期的な研究開発の方向性の具体例とあるが、後半は箇条書きになっている。これについては、もう少しコメントを書き足すことは出来ないか。

○　関係者と相談して、前の部分とのリンケージとか、必要性についてもう少しクリアになるように書きたい。

以上