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８回会合議事要旨

１．日時　平成１９年６月６日（水）１０：００～１２：００

２．場所　内閣府別館９階大会議室

３．出席者

［委員長］
佐々木 良一 委員長（東京電機大学教授）
［委員］
田尾 陽一 委員（セコム株式会社顧問）
中西 晶　 委員（明治大学教授）
西尾 章治郎 委員（大阪大学大学院教授・文部科学省科学官）
宮川 晋　 委員（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）
米澤 明憲 委員（東京大学大学院教授）
（五十音順）
［政府］
内閣官房情報セキュリティセンター副センター長
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
内閣官房情報セキュリティセンター内閣参事官
内閣府政策統括官（科学技術政策担当）付参事官
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
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
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) 報告書案（技術戦略専門委員会報告書2006（案））について

○ 報告書案では社会システムデザインの部分でガバナンスの話が出ているが、ガバナンスに加えて、組織のコンプライアンスをシステムに入れていくことが重要であるということを追加してはどうか。

○ 確かに、コンプライアンスや内部統制、説明責任といった形の動きがあって、それに対応していくというのは非常に重要だと思う。そういったことを現状認識に加えていただきたい。

○ 循環モデルの図については、どういう組織が、どういうメカニズムでフィードバックや開発を行うのか不明。循環モデルとは何かということがこの図

だけでは分からない。

○ 具体的にどの主体が循環を加速化していくのか、役割をどう分担していくのかということに関しては、今回は強く踏み込んでいない。官民の役割分担の部分でフワッと書き、現場と技術開発の間を往復しながら行っていくということを分離して書いているという形になっている。この部分の重点化が必要ということであれば、このモデルのドライビングフォースに関しての検討、ドライビングフォースは何かという堀り下げが必要だという記述を書くまでではないかと思っている。

○ この報告書案では、セキュアＶＭの開発で循環モデルを使ったというように見えるが、そうではないのか。

○ セキュアＶＭは、循環モデルを見ていくときの、循環モデルを構築するときの問題点は何かということを抽出するための、あくまでも一つの試行であるという取扱いである。そういう形の記述で報告書案全体のトーンを揃えてある。

○ この報告書案では「情報セキュリティ技術の循環モデル」と、「公的研究成果の積極的還元」、「新たな研究領域の可能性」が並列的に記述されているが、後の２者は循環モデルを強化していく要素的なものではないか。循環モデルというものが実現することに、要素的なものとしてこの２者も有効に機能するという構造ではないかと思う。

○ 情報セキュリティ技術や、そもそものＩＴテクノジーはものすごいスピードで進化しており、新しい技術が開発されるたびにセキュリティの問題が付いている。新しい技術に対してクイックにレスポンスすることをストラテジとして推奨すると良いのではないか。また、この報告書案では英単語が多いことや書きぶりにカットアンドペーストの跡が見えるのが気になる。

○ 新しい技術や新しい問題が出て来たときの対応や改善という、今のご意見については、先ほどのご意見の「循環モデルの実現に対して有効に機能する要素」という扱いでまとめ直したい。

○ 循環モデルに「調達」は重要。特に政府調達は大きな話。政府が先に進み、セキュリティ問題がどこにあるかを示し、企業の競争原理や技術開発を促進してまた現場に吸収していくというメカニズムが重要。車でいえばエアバックや衝突防止用のシステムなどの基準を公開し、それに合わせてメーカーが最適な車を開発してそれを政府が公平に見て調達するということ。それによって社会が安全になり、開発に携わる人達の方向性も定まり、国際競争力も増す。循環モデルとはそういうものではないか。調達基準を情報セキュリティ分野で明確に打ち出し、開発者の意識を一定方向へガイドしていくのが政

府の役割ではないかと思う。

○ 今の政府統一基準は調達のところに影響を及ぼしてはいるが、最先端のものを要求している訳ではなく、ミニマムリクワイアメントを要求する構造がベースになっている。技術をリードしていくためには、コモデティの技術を高めていく取組みと、リーディングエッジを引っ張っていく取組みとがあるが、調達でリーディングエッジを引っ張って行くには何らかの別のメカニズムが必要になる。

○ セキュアＶＭの開発は、まさにそこを狙っているのではないか。

○ セキュアＶＭについては、あくまでも試行として進めている実験的なプロジェクトである。セキュアＶＭを使うと決めた訳ではなく、プロジェクト終了時に、これに比類する良いものが提供された場合には、それを使うこともオプションとして排除するものではない。

○ 民間企業ならば、セキュリティを守るために、これが世の中に足りないから開発するということで進められるが、政府がリードするということであれば、ある種の公平性を持った基準、ガイドラインを示し、この審査に通ったものは調達するといったものを出すべき。それが戦略ではないか。

○ その意味では、今、政府が持っているガイドラインは、情報セキュリティに関する政府基準として一定の役割をやっと果たし出したというところだと思う。ただ、リーディングエッジ側をどのようにしていくのかを考えるガイドラインは難しい。今の研究開発の投資の多くがリーディングエッジ側にいっており、フィールドに展開するものの研究開発は十分になされていない。この問題と調達がリンケージすることのミッシングリンクをどうやって、誰が探していくのかということを含めた調達のガイドライン、調達のメカニズムを考える必要がある。「政府は買います」と言うだけではいけない。

○ 循環モデルの表現について、何をフィードバックするのかを図に書いた方が良いのではないか。先ほどのご意見の、新しいことはカバーできないということも含めてフィードバックする、ということではないかと思う。

○ 先ほどのご意見の言葉で言うと、エアバックが無かったときには「エアバックが無いとダメだ」とは書けなくて、エアバックが無いときに政府がエアバックを開発しようとすると、公正競争上、どうやって行うかが難しいということだと思う。その意味では、今回の報告書案ぐらいにしか書けないということも理解した。ただし、それを問題点として認識したのであれば、どこかにそういう記述があっても良いのではないか。

○ 情報セキュリティ技術をとりまく関連技術を表す図については、この委員

会の最初の議論において出ていたものだと思うが、委員会での経過を経て変わっているところがあるのではないか。これまでの議論をふまえて見直していただきたい。また、研究開発・技術開発の俯瞰図が描かれているが、時系列的な変化が分かりくい。これには別に一表を作るか、解説を付けていただきたい。

○ 研究項目として、先ほどのコンプライアンスや内部統制に対応した研究課題が重要性を増しているということが、どこかに入った方が良いと思う。また、「ヒューマンリレーテッドＩＴリスク」という、リスクコミュニケーションやセキュリティ心理学といったものは、もう少し組織的に研究していく必要があると思っている。新たな学際領域の中に入っているのかも知れないが、スペシフィックに入れていただきたい。

○ ただ今のご意見に関して、ソーシャルエンジニアリングの話は非常にヒューマン系の話だと思う。単純な言い方をすると「人為的な」とか「人間的な」話だということ。

○ 先ほどの調達に関するご意見は、ポピュラーになった製品のガイドラインは示せるかも知れないが、先端を引っ張るものはそう簡単ではないということだったと思うが、「防衛」などでは何が起きるか分からなくてもミサイルシステムを作ることをずいぶん前から考えている人がいて、それはまさに先端の技術を行うということである。ＩＴ社会や電子社会、電子政府の全体を見て、どのように脅威が出て来るのか、どのようなやり方があるのかを考え、実証し、基準にしたものを調達するという、それ自体を研究開発の対象として行う必要があるのではないか。そんなに先のことを言っているのではなく、現実の脅威その他を分析しながら、全体としてこのような製品が足りないとか、こういう機能のものがあると良いというもの。そのイニシアチブを取るというのが結構重要ではないかと思う。

○ 「認証基盤のガバナンス」という言葉については、この委員会での共通理解があるものと受け止めて良いのか。

○ 私見であるが、政府機関ではＧＰＫＩや公的個人認証など色々あり、民間でも金融機関などでも種々の認証が行われている。これらの統一的な全体のデザイン、いわゆる大体の人が納得するこの程度のセキュアさの認証はこれでいくとか、政府の個人認証を使うとこの辺が保証されるとか、あるいはトラストポイントというものをどのように作っていくのかといった、そのような全体の構造のことを「ガバナンス」という意味で私は使った。その辺の全体の設計デザインが出来ていないのではないかと認識している。

○ 認証基盤というものは色々と出て来ているし、社会活動というものは色々とあって、それらを保証する制度は必要で、商制度、社会活動というものの

バランスある組合せと個々の理解というものをトータルに社会プロセスとして見ていくのがガバナンスであると。ただ今のご意見と、前回までにいただいている他の委員のご意見を合わせるとそういうことだと理解している。

○ 「ガバナンス」という言葉を直訳すると「統制」ということになると思うが、その意味では、認証基盤というのはそういう意志を持つものになるのか。

○ 認証基盤というのは、電子認証に基づく電子契約書の公的責任を考えたときの議論の中でもガバナンスの概念に触れてきているところがあるので、ガバナンス、統制の言葉の方が強くなってきているのではないかと思っている。また、認証基盤は単に本人確認の道具だけではなく、認証をもっと広く使うことにより今のリクワイアメントが広がり、そこに対して合理性のある要求が社会あるいは政府から出て来るであろうということは、過去にこの委員会でもご意見があったところ。

○ グランドチャレンジについてはこれまで色々と議論されてきたが、そろそろ具体的に検討する方が良いと思う。

○ グランドチャレンジ型の研究開発・技術開発の検討を行うこと自体がバリューを持つだろうという認識を持っている。もし、ワーキンググループでテーマが出て来るとするならば、総合科学技術会議側のフォローアップは毎年あるので、その中で精査が出来れば最善と考えている。グランドチャレンジの検討をしていくという段階でも副産物的に、問題の構造や新しい技術に対する認識などが出て来るので、これらを活用することもワーキンググループを作っていく中で併せて考えていきたい。

○ この委員会は情報セキュリティ政策会議にぶら下がる形であるが、この委員会にグランドチャレンジのワーキングを繋ぐには難しいところがあるので、形式的には切り離してワーキングを運営するということを考えている。

○ 何らかの形で、この委員会にワーキンググループでの検討の成果を出していただきたいと思う。

○ 認証基盤のところで初めて法制度の問題が出て来るが、法制度や著作権の問題は非常に大事なことだと思っている。また、産学官の役割のところに、標準化やいわゆる国際的な広がりということに関して産学官がどういうことをミッションとして持つのか、ということを書いてあると良いと思う。

○ 先ほどのご意見で、新しい技術が出現したときにクイックに対応する必要があるということだったが、循環モデルの図の中にどのように書くかが気になる。既に書いてある情報セキュリティ技術なのか、それともその裏にある、もう少しフォーマルな基礎の部分のレイヤをもう一枚加えて、そこに書き込

むのが良いのか。それとも、そこまでは行かないのか。

○ その意味では、コンポーネントが新しくなることもあるし、使い方が新しくなることもあるので、想定していないことが出て来るという意味では、このボックス全部ということになる。昔は個人情報保護法が無かったのでセキュリティリスクとは思っていなかったが、法律の整備によって企業にとってはリスクとして認識出来るようになるということも起きる。「新しい事態が常に出て来るということを認識しましょう」ということを言いたかったということ。

(2) 技術戦略専門委員会の今年度の進め方について

○ グランドチャレンジのワーキンググループは、その見直しを来年も再来年も行っていくのか。

○ グランドチャレンジと足り得るものが出て来た場合には、世に問わなければならない。その上で再考を求める意見が出て来るのであれば、さらに議論を進めていかなければならないものと考えている。見直しというよりは議論の仕方や視点を変えるというイメージではないか。ただし、情報セキュリティに関して、「これぞグランドチャレンジ」というものはなかなか出て来ないのではないかという予見も持っている。

(3) 決定事項

報告書案については、今後の修正を委員長に一任することが決定された。

以上