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 14 回会合議事要旨

１．日時　平成２１年４月１６日（木）１０：００～１２：３０

２．場所　内閣府本府３階特別会議室

３．出席者

［委員長］
佐々木 良一（東京電機大学教授）
［委員］
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）
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
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係長）
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

（佐々木委員長）

○　本日は、技術戦略専門委員会報告書2008についてご議論いただきたい。

****

２．情報セキュリティ技術の将来に関する検討　について

****

○　「2.2.1（2）将来の社会ビジョンに係る主たる要素」の特に⑤について、柔軟性という言葉が良いのか適切性という言葉が良いのか、という議論があったが、事務局のご意見は如何か。

○事務局：　柔軟性の説明として、「必要かつ適切な情報セキュリティ水準が柔軟に確保できるように、」とあると何か弱々しい語感があることから、適切性を使ってはいかがという意見が出ている。

○　基本となる最低限のラインはクリアしながら更にどこまでやるかということについては、柔軟かつ適切でなければならない、ということか。

○事務局：　ベースラインとなる部分は当然化で確保されている。それを含めて、ということ。

○　おそらくここは、必要かつ十分といった意味だということで理解はした。この場合、技術としてというよりもアプリケーションの場で決まることなので、技術だけ取り出してもそれが「adequate」かどうかはわからない。同じものがどこで使われるかによって、適切なのか適切でないかが決まるという構造がある。もともと英語では「adequate」なんだろうと思うので、もしこの形で残すのであれば、「適切性」でいいと思う。

○　では、⑤については適切性ということにしておきたい。

○　「⑥最先端性」を肝に銘じておくのは難しく、意外ときつい目標が書かれている。技術が高いということだけでは⑥は達成できず、本当はインダストリアルな裏づけがあって初めて達成できることなので、我が国の IT の技術が実際に市場に応用されてなければ、最先端であったところで致し方ないというところがある。是非入れておいていただいた方がいいと思う。

○　「2.3 情報セキュリティ技術のグランドチャレンジ型研究分野の方向性」は、前回の記述が少し具体的すぎるという議論もあり、少し抽象的、包括的な書き方になっている。また、本委員会で、絞りきるのはある意味で難しい。むしろグランドチャレンジのさまざまな案を組み上げるような体制、仕組みを今後作っていくのが大事であると申し上げた。今年度以降、その辺の検討をこれからやっていこうかと考えるがいかがか。

○　「2.2.1（2）将来の社会ビジョンに係る主たる要素」の６つの要件と、こちらに書かれている要件と、対応している方がわかりやすいのではないか。１７、１８ページで書か

れていた 6 つの項目の内の、４つをとった、というのは何故なのか「⑥最先端性」は何故入ってないのか。

最先端性は 34 ページにおいては、最初、全体を網羅する形で書かれている、というご指摘がありましたが、もしそうであれば、そこも項目立てて、以上のすべての記述において最先端性を確保する、というような言い方にする方が素直ではないか。

○　①から⑥のうち、技術として考える話と、全般的な目標の二つがあり、例えば、ここでは技術に対応するものをとりあげました、ということはできるかもしれないが、確かに対応はつかないと落ち着かない。

○　②③④は要素技術であり、①⑤⑥は、ぞれを誰でもどこでも使えるようにしよう、最先端であるようにしよう、という在り方についてだろう。

○事務局：　修文については検討させていただきたい。

○　実際に最先端といった場合には、よその国が作った多少いい加減なものが入ってきたときでもちゃんと防げる、そういうことも必要なのだろうから、非常に重い課題ではあるが、実際に世の中では、必ずしも日本製品でない多くの製品において問題がある。

****

３．公的資金を用いた中長期的な研究開発の実施方法　に関して

****

○　現状では、例えば昨年終わったプロジェクトの評価が行われており、新しい評価制度を持ってきても、それが浸透するまでに若干時間がどうしてもかかってしまうという点については注意が必要である。既にご指摘があったように、さまざまな新しいことが行われていても、各担当の省庁、推進機関の方が良く理解してプロジェクトを遂行するということに関しては時間がかかるものかなと思っている。

○　今後、キュリティの研究結果の評価という点で、検討していただきたいことがある。情報セキュリティの研究において、脆弱性は見つかったが、対処方法が見つかってない場合に、その研究計画を評価しようとすると、その脆弱性を公表してしまうことになってしまう。アメリカの例を見ると、例えば本当に機微なものは例えば限られた上院議員の中からなる秘密の委員会がそれを評価して、予算について査定を行っている。ただし、何年か経って大丈夫だと思ったら公表する。日本にはこの構造がないように思える。情報セキュリティの研究の実施中、そのような問題に直面した場合、特にグランドチャレンジのような研究、あるいは途中のサイドエフェクトで出た場合には、困惑すると思う。

○　今の話はかなり具体的なことなので工夫の余地はあるのではないか。公的なところに、そこの人は受け取ったということだけ言えばよいという形にする。現在、報告書が必ずしも全部公開というわけではなく、明確に公開部分と非公開部分と分けて報告することが行われている部分もある。審査する人は守秘義務のサインをするプロセスかと思う。大変重要な点であり、方法はあるのではないか。

○　今も一般的な脆弱性についてはメーカー側でやるとか、あるいはメーカー側にやれない話については今 IPA さんなんかがそういう窓口になるというような制度がある。そのような、今、現実にある制度を利用することである程度対応できるのかと思う。

○　ICT 機器のセキュリティ脆弱性に関しては、研究開発者がメーカーの気付く前に見つけた場合、メーカーにこっそり知らせ、メーカーは他の人には一切知らせないまま修復する、というのが社会的には正しい。しかし、現状では、その研究開発者のアクティビティの評価のためには、研究開発費の運用の仕方を問われた場合、答えざるをえない。守秘義務を背負った方々が理由は述べずに評価できるなら良いが、何をしていたかさえ公開しないというのは結構難しいのではないか。特に、評価が行われる年度末に公開できる状態となっていなければ、評価ができなくなってしまう。そもそも情報セキュリティの場合は、問題が存在していたこと自体をあまり公表するのが適切ではないという場合があるかもしれない。

○　基本的には、メーカー側に脆弱性について伝え、メーカー側が対応するのが 3 ヶ月だと思っている。それ以上に遅れるようだったら一般にオープンにするというプレッシャーをかけながらやっていただくというのが基本的なかたちではないか。あまり、長い間秘密にしない方が良いだろうが、本当に短い期間で修復できないような問題点が発見された場合のために、道をつけるというのは確かに必要である。

○　リコール制度のように、ICT に係る重大なインシデントを見つけた場合は、メーカーと協議の上、3 ヶ月以上たっても公表できない場合に適切なアクションをとることがルール化されていれば、発見した研究者は適切にメーカーにプレッシャーをかけられる。

****

本年度の活動の進め方に関して

****

○　本年度の活動の進め方について御議論いただきたい。グランドチャレンジ型研究取り上げ方、進め方について検討していきたい。事務局はこの点について案をもっておられるか。

○事務局：　2 年間の検討の過程を通して、テーマ設定に関しては夢がないとダメだという話を最初していたが、夢だけでは実はそれは実現しないと考えている。とりあえず姿は作ったので今度は心を入れていこうということで、それを支えていくインフラストラクチャーとして、実際に働く人がいて、プロジェクトマネージメントのような感じで、来年度、ステークホルダーも含めて検討していこうかと思う。

○　例えば、公募型であれば公募をかける主体、既存のさまざまな組織との関連付け、総合科学技術会議等との関連性、各省庁の研究開発資金との関連、などの議論が必要であろう。どのようなスキームの中であれば動きやすいかという話については少しご検討いただきたい。

○　現在のところ、グランドチャレンジ検討ワーキンググループについてはこれからもお願いする方向であると考えてよろしいか。

○事務局：　ワーキンググループの再度形成も検討している。

○事務局：　グランドチャレンジ型研究開発を実現するに当たって、今度は具体的な手順を検討することになると思う。既存の各省庁の研究開発と、総合科学技術会議の政府全体の枠組みの整合性をとり、既存のものに乗っていくような仕組みを作らなければいけない。事務的な下ならしとして、まず関係省庁のベクトルと役割についてある程度コンセンサスを形成していくという仕事、次に、総合科学技術会議の研究開発のプロセスに乗るような仕組みを作っていかなくてはならない。全体的なコンセンサスとベクトルあわせを行い、具体的な予算にするのは次のプロセスと考えている。

○　セキュリティ分野は 1 年ごとに随分ターゲット、ニーズも変化する。一方、各省庁の施策はスパンが大変長く、最初に決定したことを最後までやらなければならないという形で動くと、始めた時にはすでに時代遅れになってしまうと困る。研究のプロジェクト管理、評価は適宜かつフェアな形で実施していただきたい。

○事務局：　経産省の新世代セキュリティの研究開発事業はスキームとしては大変柔軟で是非参考にしていきたいと思っている。

○　ご議論有難うございました。議論はこれで終了したい。本委員会の議論をふまえ、報告書につきましては事務局と相談して取りまとめしたいと思うので、御一任いただきたい。

以上