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３回会合議事要旨

１．日時　平成１７年１０月１２日（水）１０：００～１２：００

２．場所　内閣府本府第３特別会議室

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]
篠田 陽一 委員（北陸先端科学技術大学院大学教授）
田尾 陽一 委員（セコム株式会社顧問）
中西 晶　委員（明治大学助教授）
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
警察庁情報通信局情報技術解析課長
防衛庁長官官房情報通信課情報保証室長
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：同室課長補佐)
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

４．議事概要

(1) 技術戦略専門委員会報告書骨子（案）について

○　事務局より説明

(2) 出席省庁による補足意見

○　本骨子案について、意見を３点申し上げたい。

まず、１点目は用語、つまり、言葉の問題について。これまでの議論として「防衛領域」をはじめ関連領域については未整理だと認識していたが、本骨子案では、似て非なる「安全保障的領域」や「軍事領域」などの用語が新たに出てきている。当方においても何が「防衛領域」なのか、また、該当する研究開発がどのようなものかもはっきりしていない。そのような中で、例えば事務局から説明を受けた「安全保障的領域」と「防衛領域」の違いについて、技術開発・研究開発の観点からどのような点が異なるのか理解が難しい状況である。従って、引き続き用語の整理をお願いしたい。

２点目は、複数領域利用を見越した研究開発について。事務局から「貴省庁の行政目的に『民間情報セキュリティ基盤の整備促進』が入らないことを前提」として、「貴省庁の技術開発が『民間情報セキュリティ基盤の整備促進』にも副次的に作用することを、貴省庁における投資判断の材料の一部とすべき」との提案である旨の説明を受けている。当方としても情報セキュリティの向上に貢献したいと考えており、研究開発の結果、民間技術の推進に寄与する研究成果については部外公表あるいは他機関との連携などが可

能と考えているが、行政目的に『民間情報セキュリティ基盤の整備促進』が入らないにも関わらず、それを目的化して投資判断の材料とした研究開発を行うのは難しいのではないかと考えているので、その点をご理解頂きたい。

３点目は、保全上の観点について。研究開発に関する登録、事前評価や事後評価などの記述や政府調達におけるガイドラインの記述があるが、前回の会議においても申し上げたが、保全上の観点から部外の評価を受けられないもの及び当庁の調達にそぐわないものもあると認識しているため、その点のご配慮をお願いしたい。

(3) 技術戦略専門委員会報告書骨子（案）についての討議

ア　情報セキュリティ技術を考える上での基本的な考え方

○　安心・安全に資する領域だけでなく、おそらく周辺領域には特有な言葉があって、そういう特有の言葉で議論されると、あたかも全然別個の問題が存在してしまうような気がしてしまう。おそらくきちっとした情報セキュリティの上位の概念で議論するようになれば、本来どのような問題があるのかを、より問題の根本に近いところで把握できるようになるのではないか。そういう意味で、情報セキュリティが抱える問題を、情報セキュリティの言葉で整理して記述していく必要があるのではないか。

これは書き方の問題ではない。周辺領域を付け加えることによって、技術開発のエフォートが分散してしまうような気がする。無制限に分散することを避け、情報セキュリティで扱わなくてはならない技術を内側の言葉で表現する。そこで、外側との関係を考えてみるということ。

○　安心と安全、というのは社会科学的にも定義が違う。安全というのは事実的に確保できるものだが、安心というのは、安全と認識していても安心と感じられるかというのは別問題であるという言い方をするので。安全・安心というか、あるいは高信頼性というのか、この委員会でどういうふうに定義するのかをはっきりさせておかないと、これから周辺領域の人間も入ってくるので、誤解を招く可能性があるのではないか。

それから、人工物であるものと災害などの自然発生的なものとの違い、ということを明確に謳い、じゃあＩＴにとってはどんな方法でといった形でまとめた方が、これもやはり誤解が少ないのではないか。最初に「違います」ということを宣言する。もちろん共通するところもあるけれども、明確に宣言しておいた方が確実な方向性が出せるのではないか。

○　安全・安心に関しては、安全というのはメジャラブルなインデックスが設定できる領域の考え方。安心というのはそのストレートマッピングではなくて、もう少しメジャラブルではないものもあると理解しており、当然、安全であっても安心ではないという状況があるものと解している。

それから人工物と自然発生的な災害のところの書き方については、報告書の体裁でさらに書いていくと、もう少し明確にできるのではないか。

○　情報セキュリティ技術の２大目標として、ＩＴが内包するリスクをゼロにすることと、ＩＴが適用された領域の持つ機能を守ったり改善を促進すること、の２つが挙げられているが、どちらも確立された領域の改善のことだと思われる。なぜここを二つに分けたのか。

○　情報通信技術そのものの中での情報セキュリティの取り扱いという領域があって、例えば「ＩＴで守る」という言葉が加速化パッケージで出たけれども、一例としては食のトレーサビリティを行ったときに、そのトレーサビリティのベースになるところでは当然、システムのセキュリティは考えなくてはいけない。そういう領域の応用領域での基盤化をどう考え、その中でセキュリティはどう役割を果たすのかというところをきちんとやらないとソーシャルリスクになるということを後者で書くということ。

したがって、適用領域でのリスクを下げるというところを情報セキュリティの役割として行きなさいというのが後者で、前者は技術開発の中で、今のコンピュータとネットワークの中でのセキュリティとしての考え方ではなくてそれを強化して行きなさいということ。書きぶりについてはもう少し検討したい。

○　今までの情報基盤を作る際には、システムを作る際のデザインのプリンシプルが、セキュリティというのはむしろ後付けで来ていたような感じがある。それが例えばパフォーマンスというのを重視していたので､いろんなプロトコルが設計されてたりしていた。今後は、そうした情報セキュリティ基盤はセキュリティを重視した設計にしなければならないと強く言っていただく方がいいのかなと思う。

○　知見を得て技術開発にフィードバックするという部分については、オペレーションにまでフィードバックしてほしい。基盤技術の多様性によってリスク低減を図るというところがあるが、実際のシステム的な事故の例を見ても、割と基本動作の確認といったものができていないということがある｡技術を開発すればリスクを応じきるというよりも、マンネリ化させないとか、トレーニングをちゃんとやるということの方が重要。新しい技術を入れるとそういうのが楽になるというのは劇的で、何も技術開発をするっていうことを「やめろ」というのではなくて、足していただきたいということ。オペレーションという概念をフロントの方に出していただきたい。

例えば「得られた知見は、ＩＴを対象とする情報セキュリティ技術の研究開発・技術開発（すなわち前者の目標に基づく活動）にもフィードバックされる。」とあるが、この部分を、その運用にまでフィードバックするとかそういう感じで。

だから、ひょっとすると２大目標と言っているけれども、これは本当にやろうとすると作る側だけじゃダメで、実践して下さいという言い方に限りなく近いのではないかと思う。

○　情報セキュリティ技術が理想的な役割を果たしていない例示については、特定の会社のことを出すのは問題があるとは思うが、Ｔ社のハードディスクが踏み台なってしまったという事例を指摘したい。まさにここの定義によると、安全ではなくてしかも利用者が安全であると感じられてなくて、最後は何となく出来たという感じなので、こうした事例を引くのが良いのではないかと思う。もちろん、特定の会社を非難するつもりは毛頭ないので、あくまでも例として。

イ　情報セキュリティ技術の研究開発・技術開発を推進する上での問題点

○　ブラックボックスを排除する努力が不十分との記述があるが、ここは私も非常に重要だと思う。ブラックボックスを極力排除することが需要になる、ということをさらに敷衍化すると、第１回目の議論でも出たように、例えばセキュアなＯＳを作っていくということを、この先の延長上ではそこまで言っていこうとしているということでよろしいか。

○　先ほどの意見とちょっとだぶっているが、成果利用までを見据えた研究開発・技術開発の不足については、「成果利用」を運用までを見据えたとはっきり言うことが必要だと思う。

前回も申し上げたように、情報セキュリティの研究開発を推進していくときに、構造的にはアプリケーションレベルすなわち社会的システムをどう作っていくかということが重要である。さらにそれらを支えているのはやはり運用の現場とか、運用の視点なのではないか。もう少し成果利用を運用にフィードバックする、あるいは上位の社会システムをどういうふうにしていくのか、というところを踏まえてやっていくという構造を強調していただきたい。

○　社会科学と情報セキュリティについては、文言的な問題ですが、他のところが何がどうだという表現になっているのに対して、ここはただ併記されているだけになっていて、じゃあどうすればいいのということになる。ここは関連性が不十分というふうに書いていただきたい。

内容については、情報システム運用に関わる部分だけに限定的に書かれていると思う。運用・開発と併記していただくか、情報システムに関わるものとしていただいた方が良いのではないかと思う。

それからヒューマンファクターという用語については、人間工学的にはヒューマンファクターという用語が良く使われるけれども、個人というか、一人一人のパーソナルな人間をイメージすることがあり、ここを日本語訳して「人間的要素」としていただくか、あるいはプラスアルファでマネジメントとか、組織的要因とか、一人の人間ではない、人間同士の相互作用の話であるということを何らかの形で表記していただきたい。

ウ　情報セキュリティ技術の研究開発・技術開発の新しい領域設定と推進構造

○　ブラックボックスというのは、例えば中のシステムがどうなっているのか分からない、それからもう一つは、分からないんだけれども使わなきゃならないというところがあって、それから中をよく見られるように、あるいはシステマティックに見られるようにという、そういう要望の対応が必要だという話だと理解している。

○　ブラックボックスの議論は私には良く分からなかった。ブラックボックスという言葉からすると、日本で使うときに外国製品のブラックボックスを排除するというのは分かるが、じゃあ、今度は我々が開発してきたものをオープンにするのか。おそらく商売としては、外国に輸出するときにブラックボックスではない形にするというのはあり得ない。インターナショナルな世界では、一体、どういった問題になるのか。ライセンスの問題、知的所有権の問題になる。ソースコードの問題は今後、ＩＴ社会、全世界を覆う問題だと思う。

今でも少し不十分ながら、国際標準に照らしてこれは安全であるというような仕組みはある。それを日本が積極的に推進していくことはできるのではないか。セキュリティ製品としては、ブラックボックスを全部オープンにするのはライセンス上も難しい。どうやって実現するか、誰がそれを保証するのかといった課題がある。

○　私の勘違いかも知れないが、私の理解では少なくともブラックボックスは残す。いくらブラックボックスのない製品を作ってもブラックボックスのある製品は残るので、完全に排除することはできないだろうと。ただし、私が一部書いていただいたのは、ブラックボックス性のない製品を使わなくてはならない領域というのは明確にあるということ。私自身、ブラックボックスが完全に無くなるということは考えられないわけで、何でもオープンにしていくということはできないだろうと。

○　一つは、ブラックボックスについてはどこかで安全性を担保するところがあれば、けっこういいなというところがある。例えば検査技術とか、コモンクライテリアとかそういうところが一つのイクジットであろうと。

もう一つは投資戦略の中で、もうこれは機能があるからとか、これは買ってくればいいからということで投資をやめてしまうと寡占化が起こる。そのときの投資判断として、ブラックボックスのところも投資しないといけないという判断をせざるを得ないというところがあると思う。その投資にストップをかけないということでここに書いている。

○　社会科学のところをどこまで広げていこうかと考えている。

一つはやはりオペレーターのマネジメント。どういうふうにケアするかということは、今後、考えなければいけない。モチベーションあるいは組織論的なところで、かなり固くやっていければ、セキュリティマネジメントシステムのところでの話とも繋がってい

くのではないかと思う。
　それから、広いところでは、今回はソーシャルエンジニアリングのところが書いていないが、あれはまさに心理学的な要因だが、ヒューマンファクターとして明記するべきではないかなと考えているところ。人間的な要因のところは、どちらに書くかということは難しいと思うけれども、人間側から見たヒューマンエラーとかヒューマンファクターというのは、この領域で検討すべき方策として挙げることができると思う。

○　我々がやっている社会工学的には、情報行動、インフォメーション・ビヘイビアという用語がある。そういうことが今のこの議論の中に入るのかどうか。

○　社会科学の部分を書いているときに、社会科学の先生からは、社会科学に括るなと怒られ、もう少しフルサイズに書かないと意味がわからないと言われている。そこで、社会科学をどう分割して何を書くかということに関しては､是非ともご指導いただきたい。
　先ほどの意見のように、情報ビヘイビアもあるし、最近、情報のダイナミックス、インフォメーション・ダイナミックスという話も出ていて、組織論の話とか、情報管理の話とか、そういうこともここに書くとき、エッセンスをどういうふうに入れるのかというのが困難なところ。そのあたり是非お願いしたい。

○　「社会科学と情報セキュリティ」のところで、業務特性とかヒューマンファクターという側面も大事だが、情報セキュリティ全体を含む社会システムデザインが何をしようとしているかが、研究・開発者や運用現場で分からない、というところがある。
　何かをしようとしたときに、戦略方針、制度、ガバナンスがどうなっているのかを、誰かが明確にしなければならない。企業の例を挙げよう。何か新しいビジネスモデルを作ったときに、投資の判断とか、これはやるべきでこれはやるべきでないとか。また、これはやるとお客さんに迷惑をかけるとか、やると儲かるかも知れないがやってはいけないとか。そういうことを、経営責任者がきちっと判断しなければならない。そこらへんを、制度とか、ガバナンスあるいはスキームとか色んな要素でカバーしている。これらのことを社会科学といわれると、私としてはそうだったんですかねという感じがしてしまう。

○　社会科学というと何でもありになってしまう。この言葉をそのまま残すかどうかも含めて、じゃあ、どのエリアまで含めるのか含めないのか、ターゲットをどこに置くのか、組織とかマネジメントの領域に置くのか、本当に社会システムとか政策科学のところまで広げるのか、逆にヒューマンファクターのところまで落とし込むのか、これは報告書を作る前に議論させていただければと思う。

○　役割分担で４分割されているが、ここで、この軸であまり明確にしすぎると、これは横断的なメカニズムを作ろうとしているんだろうと思うが、産学官の役割をあまりにも明確にすると逆にやりにくくなるんではないかと危惧する。
　ここは、こういう役割分担も見ながら、柔軟にやっていくんではないかなと思う。結局、予算取りのときに、これはお前のところでやる必要はないという取り合いのシード、種になってしまうのではないか。
　もう一点、人材育成のところについては、もうちょっと強く、セキュリティに限らずＩＴでご飯を食べていくことが楽しくて、僕らにとって重要であって、しかもやっている人にとってカネも儲かるっていうことを明示的に打ち出していただきたい。その理由は、学生の理科系離れが進んでいて、関係省庁も問題意識を持たれていろいろと対処されていると思うが、それ以上に深刻なのは、理科系の中でもＩＴ離れというのが学生の中で激しく進んでいて、かなり厳しいことになっている。
　どうして学生がＩＴから離れていくのかよく分からないが、多分、将来性とか仕事のキツさがあるのだと思う。他にもいろいろ要因はあると思うが、日本はこれからＩＴで

食べていくわけで、ちゃんとやるというスタイルを出していただきたい。

○　確かに、役割分担を明確にしろと書かれているのはやりすぎかなと思う。例えば弊社は、基礎研究から人材育成まで、それからオペレーションまで全部やっている。一方、企業というのは自分のビジネスをやるためには、必要な人材はどんな形であれ、追求するし、必要な基盤技術は先ほどご意見のあったように競争力の源泉として、他の人に公開しない形であえて作ったりするわけなので、これは役割の分担というよりは、短期的に成果が得られるものは産業界がやって、それ以外のものは政府がやりなさいということだと思う。

例えば、独自の暗号技術というのは保護されてしまっていて、貿易の際に非常に問題があり、アメリカではアメリカで作った暗号技術でしか暗号を解いてくれない。したがって、日本発の日本独自の暗号で閉じてアメリカに送っても意味が無い。でも、１０年間とかたつうちに、アメリカの決めている暗号技術もＣＰＵの処理速度や周辺環境の変化で陳腐化してきたときに、じゃあ、日本発の暗号技術を国際標準にしてもいいかというチャンスが出てくることも十分あるけれども、そこまで、例えば産業界に１０年後の戦略まで担保させるかというと、それは非常につらい。ですから長期的なストラテジのところこそ、国に持っていただきたいということ。

○　その辺りは確かにちょっと書きすぎの印象もあるが、一方では、何か言っておきたいという思いもあるのかなと思う。その辺は「はじめに」のところで書けば良いとの意見もある。また、私自身、戦略と産業の両立といったところは触れても良いのではないかと思っている。

○　このプラットフォームというのは技術を集積した結果のプラットフォームであったり、技術を集積するためのテストベットとしてのプラットフォームであると考えてよろしいか。

そのときに大学のキャンパスネットワークは、ある種の研究目的になる。セキュアネットでも人材育成ではそれは一つのテストベットとしながら教育もし、それをより強化するということもやっている。例えばこのプラットフォームというのをオールジャパンで「ばぁっと」作るのか、ある領域に限って限定して作るのか、具体的なイメージを教えていただきたい。

○　ここで考えていたのは二つあって、一つはＯＳというかシステムのようなもの、あるいはシステム環境といったものを考えていたのが一点。もう一つはネットワークがある環境。例えば、ＪＪ２みたいなものはテストベットになって、オープンになるようにされているけれども、ここにもっと技術というものの移転と、集積というものがあればテストベット化するはず。発展した形態でのプラットフォーム化というのは当然あると思う。

○　成果利用に関する政府調達プラス、やはり民間でも成果を使ってくれということも成果利用として挙げるべきだと思う。ここは丸をもう一つ作っても良いのかなと。あるいは政府調達だけでなく、何か書いていた方が良いのかなと。

それから、大学の役割で人材育成は研究者を育成するとはっきり書いているが、ＩＴ技術者イコールリサーチャーだという雰囲気、オペレーターというのは大学ではやらなくていいんだという雰囲気がある。大学の役割なのか、高等専門学校の役割なのかという議論はもちろんあると思うし、大学だけが教育機関だとは思わないが、研究及び運用の人間を輩出するというような書き方をしていただければと思う。

○　ここの書き方については、一般的な人材育成の話は一切書いて無い。先端領域での研究の領域を拡大していったり、あるいは研究を加速化していくときに、一つは、そこで

取り組む研究者がいるという前提だけれども、もう一つは研究活動を通じて、人材を作っていくということ、あるいは教育活動というものをそこに組み込むことによって、知見の体系化を相当に行うということの取り組み、そこを担うということの人材育成というのが相互に関係することによって、研究が加速化するというモデルが最近あって、そういうことを書いている。

したがって、ここではオペレーションの人材を育成するっていう考えは全く無くて書いていて、具体的方策の「先端領域での研究開発を実施するプロジェクトにおいて、研究者の育成を同時を行い知見の体系化を加速させる、新たな人材育成プロジェクトを実施する」というところに繋がっていくということ。

そういうことを意識して書いているというのが現時点。もし、人材育成についてジェネリックなことを書く必要があるのであれば、ここでなくてもっと別なところに立てないと、全体の論旨としてちょっとおかしくなってしまう。

○　運用を出すとした時点で、そこに直行軸が出てしまったような感じだと思う。全体のトーンとしてオペレーションを出していただけないか、足していただけないかというところについて、ここに入れるかどうかは別というのは結構。ただ、大学の役割という限定詞を付けた場合に､大学はオペレーターを作ってくれないのかということについては､我々は不満に思っていて、例えば、セキュリティの専門家を大学から採用しようとしても、セキュリティの論文を書いてくれる人が欲しいわけではなくて、本当は勉強してレクチャーしてトレーニングされた人が来ればいいという場合も多々ある。もちろんそこが相互的に連関しているのを否定するつもりは全く無くて、有効だということは認めている。ただ、それだけじゃないでしょう、ということ。

○　確かにそのご意見は分かるが、今後大学がやるべきなのは、実践的なというか、もう一段上の人を作るもので、ここではむしろ、産官学の実践的なレベルのものを踏まえた上で、そういう実践的な人の上に立って使いこなし、新たな研究領域を開発するような人を大学としては今後育てるべきだ、というところを逆に謳ってほしい。

○　役割分担のところは､「主たる役割」とすれば良いのではないか。今は、ここは非常にシャープに書いてあるので。ですから独立法人の主たる役割とか、もう少し薄めるというか、皆様ご意見があると思うので、もう少し柔らかくした方が良いのではないか。例えば大学では、高度なプロジェクトの高精度化とかいうんではなくて、例えば高度化とか、そういった形に。

○　産業界の役割において、国家プロジェクト等により創出された技術を、というところについては、ニュアンスとしてどういう意味なのか。もちろん国のお金が入ってビジネスが出来るようになるということは、それは非常に期待しているとは思うが、どういうものか分からないのにこれを使いなさい、ということがあるのかなということ。そういうことではないと思うが、もの次第ということなのか。

○　ここのところは使えとは言っておらず、生まれてきた技術のイクジットのところで産業界の手を経ないと使いものになりませんよということを書いているだけであって、要するに、国が研究した結果というのがあったときに、ここはあくまで産官学の連携のことを書いている。当然、そのもう一個のベースになっている、暗黙の了解のリサーチファンドみたいなものは国のカネが入るよねっていうところを前提に書いたときに、出口が社会であるならば、産業界の役割っていうのは、やっぱり社会に出て行くときのことを担うということがある、ぐらいのことしか書いてない。

逆にこれを読んで、これを使えと書いてあると言われると心外という感じですが、ここは表現の適正化を図るということでしょうか。

○　いろんなベンダーの方とお話をしていると、ある程度セキュリティを保持していないと政府からＪＩＳのようなマークが付かないとか、あるいはガソリンなどを流通させるのと同じことをやってくれないと、自分だけが飛び込んでコストが高くなるといったことでは困ると皆さんおっしゃっている。僕はそこのところは政府として大きな役割が取れるところだと信じていて、例えば政府の基準に合致していたらマークがもらえるだとか、行政指導みたいな厳しいものでなくても何でもいいんだけれども、何かそこをやることによって民間を入れてもらえないかということ。もちろん難しいことが多々あることは重々承知しているが。

○　例えば、文化専門委員会の方でも技術というものを、例えば情報セキュリティ部門のセキュリティのコンポーネントをどう導入促進するかという検討をしていて、その中で例えば経済産業省さんがやられている１５４０８というクライテリアみたいなものがあって、それを取得するとＣＣ取得マークというのが付いて、ＣＣ取得マークのＥＡＬ４のデジタルコピーが世の中にある。そうするとローカルにデータが残らないオプションが付く。彼がマーケット占有していく中でのセキュリティオプションの占有率は世界の中で十数%。この啓発の構造とか、社会の方の受け止め方、要するにパーセプションの問題、それからそれを受け入れていくのかという問題をこの技術戦略専門委員会の提言として受け止めていくのか、それともここでまとめたことをセキュリティ文化専門委員会の方にねじ込むのか、二つの道を考えたい。
　先ほどの人材育成もそう思っていて、書くことはやぶさかではないが、技術戦略として啓発も書くのか、技術戦略としてジェネラルな人材育成というのも書くのか、あるいは文化の方に突っ込むのかというあたりは、そろそろ最終的なイメージをご示唆いただきたい。

○　人材育成については、研究者の育成とは書いているが、技術者の育成とは一言も書いていない。研究者を作って研究の領域の活動を加速するべきだと書いているつもり。
　ここのロジックでは大学の役割はまず、研究をやってくれ。ところが、先端領域であるからこそ、研究者がいないのでは仕方ないから、まず研究者を作りつつ体系化するエンジンを回して下さいという書き方。だから、技術者を作れとはここでは全く書いてない。
　技術者を作れというのが技術戦略の中で必要だということであれば、別立てで問題指摘から新たにご提案してもらうのではないか。
　ここのところでは大学の研究を進めてくれということであって、研究者を作れということではない。研究者を作ることはジェネラルには言っておらず、この領域での研究を促進するために研究者を作ってくれと言っている。

○　ジェネラルな人材育成、情報セキュリティ関連の技術者も含めた人材育成の問題について、この報告書で指摘し、書くべきだと思う。オペレーションの現場への人も輩出しないと、せっかく作った技術が使われないということになる。
　もう一つ、確かに技術戦略の方から政府調達のところまで書くのはここの範囲ではないというのはそのとおりで、それは道理を越えていると言われればそのとおりかなと思う。単にボトムアップのやり方としては、そういうやり方もありますよ、という話であって、やるかやらないかの決定のところについては、どちらでもよいかなと思う。

○　そういう意味では表題のところを見ていただいて、「情報セキュリティ技術の研究開発・技術開発の新しい領域設定と推進構造」とあるわけなので、ある程度絞り込み型の方が私はよろしいのかなと思う。ただし、やはり人材の育成だとかそういうものは必要だと思うので、そういう問題との位置づけを「はじめに」とか最初の方で書いていただくのが現実的なまとめ方ではないか。

○　人材育成への取り組みについては、関係省庁の人材育成を担当している部門が、それぞれ独自のマークを作って、役に立たなくなってしまうということを懸念する。つぶしたはずの虫がわき出すのをおそれるということで、ここでは何かおさえの一言が必要なのではないかと思う。

○　３．１の表題と３．２の表題のあり方について見直されたい。３．１は「現在の投資領域のあり方」とあるが、ここは、上のフラグにもあるように「新しい領域設定」ではないか。

エ　今後３年間のアクションプラン

○　ここで一点だけ補足させていただきたい。グランドチャレンジ型のテーマ例については当然、限定されるものではなくて、あくまでも例として考え出したもの。

１番目は、ＣＲＡというロビー団体があるが、そこでのグランドチャレンジの議論の中で出てきたものの一つ。２番目は、事務局の思いつき。３番目は、ＣＲＡのグランドチャレンジの議論の中で最後に落ちたもの。

グランドチャレンジ型は、ビジョナリィゴールの言葉。何々の領域のことをやりなさいというのは、持続的取組促進型の方で吸収しようとしていて、もうちょっと言葉として分かるターゲットをやるということ。だから、例えばロケットを作れというふうに書くのではなくて、ロケット領域、ロケット技術と書くのでもなくて、「人を月に運ぶこと」と書くというのがグランドチャレンジ型。それで、持続的取組促進型の方を書くときには領域を書くということで、ここでは書け分きをしたつもり。

○　４．１のグランドチャレンジ型で３つの着手点の話があって、４．２の持続的取組促進型でいくつかのタスク化の話があるが、ここにあるのは、この３つのどれかにマッチするということなのか。

○　４．１のグランドチャレンジ型は、複合領域であるということと、もう一つはそれを達成するためのメカニズムが必要ということで、正確に言うとメカニズムによる領域を持った複合領域だということ。それに対して、４．２の持続的取組促進型の方はもっと地に足の付いた重点領域の話をしている。

○　どうして３年間なのかというと、情報セキュリティ政策会議の中で第一次の情報セキュリティ基本戦略を決めることとなっており、このタイムスパンが３年程度であるため。

実際には、４．１のグランドチャレンジ型の着地点的には、グランドチャレンジ型のアイデア出しをして、目標点を決めていくんだろうと。そして４．２の持続的取組促進型の方は３年間の重点投資領域であるというような考え方であると。

総合科学技術会議の方は５年間で、その点少し整合性が悪いが、セキュリティ分野の進化の早さなども見ていて、基本戦略の中でも３年間というのは妥当だろうと考えている。

○　実は私自身はこんなのが大事ではないかと、コメントとして３つぐらい出したが、ご自分が研究しているものばかりじゃないですかと言われて、若干反省しているところ。その中の一つで、長期的に環境が動いていく中でどうやってセキュリティを守り続けるかという技術はやはり重要かなと思っている。狭い範囲で言えば公開鍵暗号系とかハッシュ関数系とか。あるいは人間系も変わっていくんですね、若いときには適していたセキュリティ対策が年をとると動かなくなるっていうこともある。ぼけてしまうとか、死んでしまうとか、そのときにどうするのか。そこはまた大事かなと。

○　人を認証するのはいろんなレベルがあって、ネットワークではどうするかとか。そういったものをここで取り上げたらどうかと思うが、いかがか。

○　以前いただいたメモの中に認証の話があったが、そのマルチレベルの認証技術というのをここに書いてないというのは、別に入れたくないというんではなくて、グランドチャレンジ型で入れたらいいのか、持続的取組促進型で入れたらいいのかで悩んでいたということ。

例えば、セキュアＯＳは実はグランドチャレンジではないかと思ったりする。そこで、何かひも付けしておいた方が良いのかなと。あと、対タンパー・ハードウエアみたいなものは技術的には多分グランドチャレンジなんでしょうけれども、そのオーラルな説明を考えたときに、言葉で説明したときに、それは何かと考えたらやはり４．２の持続的取組促進型に行くのかなと。

ここの部分は何も排除したわけではなくて、どう置くかということに納得が付いたものだけを今のところ、理由付けられたものだけを書いているという立場。

４．１と４．２のどちらに置くかという峻別とどこに入れるべきかと悩んだ技術や、本当は入れるべきなんだけど悩んだ技術というのを、メモで資料の後ろに付けた方が良かったかも知れない。ここは気持ち的には全くクローズにはなっていなくて、まだオープンであるとご理解いただきたい。

○　これからのＩＴ社会で情報セキュリティというのは基盤技術としてどういう役割を果たしていくのか、やはり私が気になるのは社会システムである。どうやってデザインしていくのか、そのデザイン能力の中で情報セキュリティ能力をきちっと位置付けてやらないとだめだと思う。これがグランドチャレンジになるかどうかは分からないが。官庁でも、産業、学でも同じように社会デザインレベルでコラボレーションしていくことが重要だと思う。

もう一つ、アメリカが作ったルート認証をどうしてあまり意識せずにどんどん使っているのか。私は、ルート認証がコントロールできるようなＩＴ社会が必要なのではないかと思う。

○　社会システムのデザインと情報セキュリティというところが、もし一つの領域として立つなら、報告書の書き方も変わってくる。社会システムデザインと情報セキュリティデザインとの関係が取れていないのは、そこの役割が不明確であり、これはメカニズムの問題と領域の問題ではないという捉え方で今の報告書骨子では組んでいる。

ルートＣＡについては、一つの技術としては決着済みと考えていた。ただ、社会展開していく中でのオペレーションまで見ていくと決着はついていないのではないかなと思う。また、ＰＫＩの利用領域の拡大という意味では、決着がついていないことはまだ山のようにある。ＳＴＰについても、ＳＴＰ自身が本当に相互に運用可能なルートＣＡの開発は大きな問題で、そこで国の投資の役割は何なのかということもある。そうした国際標準でデプロイしたというのは世の中に沢山あり、国も投資していて、そうした点についてはどう考えるべきか、皆さんにお伺いしたかったところ。

○　私は社会システムのデザインと情報セキュリティの領域設定は入れるべしという意見。人材育成も含めて、そこに専門家というかプロデューサーがいないとまずいと思う。

ルート認証については決着済みといえば決着済みだが、それだけ取り出してビジネス側で何かやろうとしても、先行優位などでビジネスにならない。国の応援をいただきたい言っているわけではないが、ある意味ではブラウザ側が世界的に寡占化している現状があるので、トータルでは非常にやりにくいと思っている。なぜ、先行が強いかというと、ブラウザのバージョンが上がっていくところに入っているので、マイノリティは手が打てないという状況がある。携帯に関しても同じような認証の仕組みが入っているが、日本の政策は、先行有利という以外に、戦略性はないというのが現実。

○　グランドチャレンジ型の施策及び持続的取組促進型で加速すると思われる環境につい

ては、追加や削除の意見を委員並びに各省庁からメール等で事務局へご連絡いただきたい。

受け取った意見については、できるだけ反映するように致したいと思うが、これについては委員長と事務局の方で相談して対応させていただいて、次回どれを入れてどれを落とすかということについてもご了解いただくようにしたい。

○　最後の重点領域のところについては、言葉というか単語で「ＧＲＩＤ」とか「セキュアＯＳ」とかあるが、これで良いかどうか。セキュアＯＳと書いてあるが、今、セキュアＯＳをやっている人は狂喜乱舞する。そうではなくて、例えば「オペレーティングシステムを含むプログラムの実行環境の改善のための研究開発」とか、ちょっとぼかした言い方にしていただければと思う。

○　是非、良い言葉があったらいただきたい。これから報告書を文章として書き始めるが、そのときには骨子にあるような端的な書き方ではなくて、開いた書き方になってくる。そこで、より適正化が必要になってくるので、意見をいただきたい。

○　今回の議論を事務局で整理して報告書を作成していただいて、次回はそれについて議論をしていくということになろうかと思う。

委員各位と事務局を対象としたメーリングリストを既に立ち上げているので、今回の委員会で言い足りなかったことや、補足意見があれば是非メーリングリストでも発言頂きたい。

特に次回の委員会に都合により出席できない方がおられたら、メーリングリストでのご意見も参考にさせていただきたいので、是非よろしくお願いしたい。

(4) 今後の予定

○　事務局より説明。

以上