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２回会合議事要旨

１．日時　平成１７年9月２１日（水）１６：００～１８：００

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]
河田 惠昭 委員（京都大学防災研究所所長）
志方 俊之 委員（帝京大学教授）
篠田 陽一 委員（北陸先端科学技術大学院大学教授）
須藤 修 委員（東京大学大学院教授）
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）
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ー
2-1PT IPv6 グループリーダ兼経営企画部ビジネス開発担当課長）
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長
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) 情報セキュリティ技術戦略の骨子と方向性等について

○　事務局より説明

(2) 出席省庁による補足意見

○　先日行われた情報セキュリティ政策会議の中で、構成員から「重要インフラに対する攻撃には電磁波によるものもあり、現実にはむしろそちらの方が実施しやすく、また破壊力も大きい」との意見が挙げられている。参考までに、防衛庁においては、情報セキュリティ対策という位置付けではないが、電磁パルス対策に関わる研究も行っているところ。

このようなものを捉えれば、関連領域において「防衛」の領域が存在するとも考えられるが、「防衛」の領域については、事務局から「従来のセキュリティ領域」と「新たなセキュリティ領域」との区分が明確に示されていないため、今後、委員会での議論も踏まえて、年末に向けて整理していきたいと考えている。

また、今後、想定されている研究開発の評価の枠組みの中で部外評価を行うならば、保全上の観点から評価を受けられないものもあるという観点に配慮をいただきたい。

(3) 情報セキュリティ技術戦略の骨子と方向性についての討議

ア　情報セキュリティ技術を考える上での現状における主な問題点について

○　技術を作るのと使うのは２大要因で、事務局案のトーンは作る方に注力している。もっと使う方のストラテジについて踏み込んだ取組みがあっても良い。現場の概念が大事。オペレーションの現場が貧弱なのに、リサーチを太らせても仕方がない。もっとオペレーションの現場にフォーカスすべき。

日本はグランドチャレンジ型の実装をするんだ、ということ。シーズオリエントというよりも、あるべき姿のエクスペッテッドな姿を作って、実装するという強固な意志が先に示されるべき。

○　問題点の前に、まずどういう方向にすべきであるかを示し、それを受けてオブジェクトツリー的な展開のもとに問題点を整理すべき。その中にオペレーションの領域も入るのではないか。

○　情報セキュリティは政府なり、企業なり、そして国民生活なりの継続性を戦略目的にしている。継続性に責任を有する現場のオペレーションと一体化した研究開発、これを保証する組織のあり方、連携の仕方を産官学を含めてどうするかが課題。

情報セキュリティは基盤のオペレーション技術。その上に医療や防衛、警察といったサービス分野がある。情報セキュリティだけ切り出して研究開発するより、社会システムデザインと一体化して研究開発を行う必要があるのではないか。

○　情報セキュリティ技術領域への投資が少なく領域が狭いという問題について、領域を広げることには賛成。しかし、情報基盤技術を支えるためにもっと太く長く投資を続ける気構えを述べていただきたい。

○　この委員会で今後１０年ぐらいを見込んだグランドチャレンジについて議論しきれるかがポイント。確かに太く長く投資することは重要。しかし、何を目標にということをどう書くかが課題。中長期のターゲットポイントを明確に書くか、当面これは必要だとしておき、この先はちゃんと考えないといけないという書き方にするのかが分かれ道である。

○　長年同じ省庁に居ても、その省庁の中でＩＴ技術がどういう分野で使われているかの全体像は分かりにくい。ましてや他省庁の状況であればほとんど分からないのではないか。

グランドチャレンジはシードオリエンテッドなものだと思うが、まずニーズオリエンテッドであろう。今、これが起こったら困るということを積み上げていくと、こういうことがあったらなぁ、こういうことができたらなぁ、というシーズがあり得る。それがグランドチャレンジのサブジェクトになるのではないか。

イ　解決の方向性と具体的な方策について

○　研究開発実施体制の充実と改善よりも、先に運用実施体制の充実と改善があり、研究開発は本来、その後にやれば良い。人材育成についても研究開発というよりも、オペレーションの人材育成をやらなくてはならない。ただし、研究開発の人間とオペレーションの人間は極めてコンパチビリティが高い。

○　アプリケーション寄りのものを考えなければならないとの意見には賛成。そのほかにも電子署名とか認証などもあると思う。

○　長期間の研究の中で、先にあるべき姿を一つだけ決めてそれに向かおうとすると、１０

年間位やっているうちに現実から離れていって、つじつま合わせが始まってしまう。グランドチャレンジで理想論を一つだけ立ち上げるのは危険ではないか。

○　グランドチャレンジを一つに限定するつもりは無く、複数あって構わない。それは、いわゆる投資妥当性をどう見るかということ。

○　まずビジョンがないといけない。ビジョンがないと場当たり的になって、徒労に終わってしまう。ビジョンは当然、途中で見直して評価していくものだと思うが、ビジョンには数値目標があって、数値目標的なものがグランドチャレンジに相当する。

○　現場と技術開発との間でギャップが大きく、ここにリスクがある。技術水準が上がると安心してしまうが、思わぬところで穴が開いてしまうことがある。現場には見えない問題が、開発する方には見えている。開発するプロセスを共有することが大事。プロセスを共有することとは、プロジェクトに参画すること。そうしないと思わぬところで大きなミスにつながる。

○　ライフサイクルメカニズムについては、もっと強くするべきではないか。矜持的には開発側と供給側のループを上手くデザインすることが重要で、そこに組織科学とか行動科学を入れ込むこと。時系列的にはイノベーションの連鎖反応。一つの技術で構成されているように見えるが、現場のループが上手くとれているか、次に何が問題で、次に何をやらなくてはならないかということ。
　連鎖反応はある程度予期できるはずで、それにも対応できるように一つのアプローチでなく、複数のものを同時並行的に相互作用を起こさせるということ。
　案の中に既に書かれていると思うが、もう少し強く書いても良いのではないか。

○　現場と開発という話については、我々は、研究開発を狭義の情報セキュリティ領域において議論しているのではないかという印象がある。
　狭義の情報セキュリティ領域で、オペレーションがしっかりしている高信頼性組織というものを研究しているが、そういうものの研究も含めての研究あるいは開発というような発想で行けば、かなりこの案でもフォローできるのではないか。
　人材育成の議論については、高信頼性組織の研究の中で原子力のシステムを研究していたが、非常に先端的な技術者が育ってきたが、あるとき社会の評価が変わって非常に怖いものとされたときに、技術者の人達のモチベーションをいかに維持していくか、さらに開発者ばかりでなくオペレーションの現場の人達のモチベーションもどうやって維持していくかが、非常に大きな問題になるのではないかと思っている。

○　４つの解決の方向性と具体的な方策については、ここに分類できないものもあると思う。例えば、政府の予算は一つのキーワードに過剰に反応しているのではないか。集中的に投資が起きて予算が重複してしまい、その反面、他の分野については薄くなってしまう。こうした予算の問題はこの４つの中では分類できない。
　誰かが横断的に技術があるかどうかを把握して、表向きの皮にごまかされないような仕組みが必要なのではないか。

○　プログラムマネージャーの取り扱いをどうするかに係ると思われるが、今の意見では少し違っており、ポートフォリオ設計をきちんと見ろということが必要。あとは総合科学技術会議の範囲の議論もあるので、その辺をどうするか。イクジットを考えないといけない。

○　一つの問題について一つの解決方策があれば良いということを言いたいのではなくて、情報セキュリティ対策というのはこけてしまったら終わりなので、複数の施策を行

うことには意味がある。しかし、訳も分からずに行うのは無駄だということ。

○　セキュリティの問題については、どのレベルまで許容するのかが重要。２段階でやるのか多段階でやるのかという議論が必要ではないか。

○　レベルの問題については確率論が絡んでくるのではないか。発生する割合や被害の大きさも分かりにくい。また、対象によって様々なパターンが出てくる。

○　我が国の情報セキュリティ技術がどう使われ、どう貢献していくかをまず一番先に書くのではないか。そこでは、絶対に大丈夫な社会を作るというんではなくて、トラブルがあったときに、しなやかに対応するということを書く。
　そこには２つの道があり、セキュリティが持っている、どういうインパクトを与えるかというリスクに対する研究、それとそれに対する長期レンジの投資をどうするかということ。

○　未熟な分野であることを認めた時点では、コストや評価の話をするのは、それはやめておけということになる。スタートの時点でコストや評価の話を持ち出すことには反対。

○　私自身はセキュリティの問題は確率論として扱っており、ある部分はそれで可能だと思う。ある分野にどういう対策をとるのか、あるいはいくつかの代替案の中でどれをとるのか、どう組み合わせるのかということでも考えられるのではないか。

○　攻撃する側はいつも新しい手法をとってくる。これまでの確率に乗らない新たなものが出てきたときどう対処するのか。防災においてはカトリーナがそうだった。そういうときの被害は膨大なものになる。確率論でカバーできるのか。

○　確かにそういうこともあると思われる。定量ができないものとの比較もあるし、それを決めるのが誰かということもある。そういう人とのコミュニケーションをいかに図っていくかということもある。

○　まず、問題点が明確でない。これは問題点が分かった上で書かれているもの。問題点が分かった上でそれを解決するための問題点が書いてあるに過ぎない。問題点がどこにあるのかは各省庁でバラバラだと思う。

○　セキュリティに関連する分野においては共通の認識があるものもある。例えば、あるサイトへの不法アクセスというものにはどういう手法があって、どういう影響があるかとか。そうはいっても個別の問題が分からないということもある。
　では、問題が分からないから対策もできない、いろんな技術が開発できないかというと、そういうわけでもないということ。

○　議論の行方がよく分からないが、セキュリティレベルの設定が問題なのか、あるいは設定しないと議論が出来ないということなのか、それとも日本の技術レベルはいろんなものがあって、そういったものをもっと認識して議論しなくてはいけないということなのか。
　レポートの書き方としては個別の問題を最初に持って来るのは、これは今あってもこれからまた出てくるわけなので、それを書き並べてもレポートとしては良くない。むしろ、最初の問題点の前で理想的な社会の中でこういうことは起きないと現状を書いた上で、それを総括し、技術的にも科学的にも総合的にはこういう問題があると書かれた方が良い。もう少し戦略的な意識を持って世の中に発表した方が良いのではないか。

○　個別分野に関しては重要インフラ専門委員会が出来るそうなので、その委員会の中で問題点が挙がってくるのでないか。それを上から見るということもできるのではないか。
　セキュリティのレベルの議論については、あるレベルをこの委員会で決めるということではなくて、例えば予測可能な失敗というような感じで、これがこけると次はどこに落ちる、どこに落ちる、どこに落ちるといった感じで、そういう話ではないか。

○　全体としてこれ以上落としてはいけない、というレベルを設定するということ。ネットワークは、ある以上強くやられると全部やられるというリスクを持っている。

○　そういうことは技術的に解決できることではないか。現象的な問題意識ではない。個別の技術を見れば、どこをいじればどこを止められて、止められなかった場合にはその次どうするということがきちんと出来るのではないか。

○　それは技術に対する過信であって、そういうレベルではないから困っているということ。要素技術を集めてもトータルではバランスが取れるかというとそうではない。技術者がどれほど頑張ってもだめな部分はある。省庁も全部問題は分かっているわけではない。そこに大きなギャップがある。全部分かっているのであれば、それを出すか出さないかは別にして、解決はそれほど難しくはない。隠れたボトルネックは絶対にある。

○　今、ネットワークというと、基幹ネットワークしか考えていないが、いろんなネットがあるわけで、例えば個別のコンピュータを立ち上げている人にも影響はある。そういう意味では情報セキュリティを随分広い意味で考えなければならない。
　そこは技術として解決する話もあるし、どこまでで防ぐということも考えていくということもある。

○　まず脅威の分析から来る。それから脅威の見通し。その結果こうなる、将来こういった技術も出てきてこういった脅威もあり得ると。それが無いと共通の認識も無い。

○　個別の技術に関して、これは良くない、これは良くないというやり方では、この委員会の議論は収束しない。この委員会で議論すべきなのは、共通の認識について、こういう思想でやることを決めましょうということ。

○　そうであれば、ＤＡＲＰＡのような組織をどうやって作るかといった議題にすり替えた方が良い。

○　例えば、思想やその色を決めているものがあるとすると、レベルを決めるのか、あるいはあるシステムがこけたときにどこまでフォールバックするのか。一番下まで落ちてしまうのか、それともどこかにひっかかって、そのまま耐えてレジジエントに元の状態に戻れるようにするのか、そういうことをここで決めるのではないのか。

○　それはそのとおり。ただ、何が脅威かということを設定せずに、どうやってその脅威に対抗するかという検討はできない。

○　脅威設定を先に行うのは困難。例えば、グランドチャレンジは出来そうな感触はあるが、１０年先を見てグランドチャレンジを設定するときに、では我々は今ここにある脅威というのを１０年前に設定できていたかというと絶対にそんなことはない。したがって、脅威設定からやるというのは無理ではないか。

○　まず、我々がここで述べなくてはならないのは、一体この情報セキュリティというのは何のためにあるのかということ。その役割はこの委員会でコンセンサスを持ってここ

に書き下さないといけないだろうというのが１番目。
２番目には、脅威も含めてパーセクションの問題があり、これを吸い上げるということと、それからニーズとシーズという言い方もあるが、このパーセクションの合理性を戦略の中でどう担保していくかというのを考えないといけない。
３番目は、それから目標に向かって行くところの技術の役割というところが見えてくれば、それの実装というところを考えないといけない。それから脅威研究のインプットの研究と成果利用のアウトプットの研究とをどういった方向でやるかといった議論でまとめ込む。すると、皆さんの意見されている構造と今後が見えるのではないか。
それからもう一つは、先ほどのご意見の連鎖反応とループ。これをどう作るかということは、今、答えは無い。一つの技術領域であれば出来ると思うが、ただ、政策施策群を立てていくというプロセスを、ＤＡＲＰＡのメカニズムを持つことが良いのか、それとも今の総合科学技術会議が果たしていることをもっと頑張れということなのか、何なのかというところ。

○　一番最初に４つの問題が書かれているが、何をやろうとしてこの４つが問題意識となるのかあまりはっきりしない。それは、資料の最後の図で「新たな情報セキュリティ領域」と書いてあって、それは大賛成だが、その周りにはこの委員会に関係する省庁のことしか書いていない。これにもし厚生労働省とか、外務省のパスポートだとか、また教育分野とかを入れ込んだら、ＤＮＡは収集したらどう安全なのかとか、ネットワークアタックだけではない情報セキュリティが全部入った「新たな情報セキュリティ領域」ができあがる。
少し社会システム的なものも入れようとは見えるが、本格的にこれを入れようとしたときには、解決の具体的な方策として「場の設定」とが書いてあるところに突破口があるのではないかと思う。今のような問題点を解決するために、全体戦略としての「場」を設定するべきではないか。
ＩＴ社会になっているのに安全なＩＴデザインをやっているのはどこなのか。例えば、医療でも厚生労働省だけで出来ない。総務省とか、通信の問題も絡んでいるわけなので。さらに個人認証まで絡むと省庁横断で、技術横断で、学の横断になる。それらのイニシアチブをとる議論をこちらでするものと期待している。
非常に重たい課題なので、「場の設定」のところに、この後このような問題意識でこのようなことをやらないといけないと書いていただければ、かなり進んだのではないかと思う。

○　何をやったらいいか決定するとき、ストラテジを作るときには、これをやったら間違いないという健全性と、これをやったら完璧だという完全性と二つがある。何かをやろうとするときには、この健全性と完全性を考えることが必要。
健全で完全であれば完璧だが、健全だが完璧でない方法もある。それは全てを無にすること。それは健全ではあるが、完全では無い。
一般には完全なシステムを作ることは極めて困難で、人間の人智が及ぶ範囲内で健全なシステムを作ることだけが我々の大域的な考え方である。先ほどの意見をそのように理解すると、我々は一生懸命健全なシステムを作ろうとしているが、実は完全ではないので危険なことがあると客観的には思う。
また、現場のことをやろうとすると、すごく健全なストラテジがわかる。そこから帰納すると、グランドデザインができるはずだというのは、極めてまっとうな考え方だと思う。
そう考えると、場を設定すれば良いというのはそのとおりだと思う。何となく問題を先送りしたような感はあるが。必要があればボランティアをする用意はある。ＮＩＳＣの人とすると良いと思うが、ここは汗をかくという作業が必要。先ほど指摘のあった事例の収集は全部ではないが、いくつか収集する必要があると思う。試しにいくつか集めて、どういうストラテジに帰納するかを皆さんにお示しする必要がある。

我々のミッションは、上の会議にこういう技術戦略をとった方がいいですよということを提示することであると。そこで検証する必要があって、継続的に見ていく場が必要があるという意味で、最初のストラテジとそれに対するメタなストラテジの二つを提示することで我々のミッションを完了したい。

つまり、最初のストラテジはタクティクスかも知れないが、少なくともある領域については健全なものであるということを提示したい。そしてそれを完全なものに近づけるためのメタなストラテジとの二つセットで。ただし、そのためには素案が無いと困るので、ＮＩＳＣの皆さんと汗をかく人間が必要なんでしょうということ。

○　戦略というのは、最終的に一番下にはアクションプランというのがあるはず。例えば、津波の防災のためには現状の把握に１０項目くらいあって、その下に脆弱性の評価に１０項目くらいある。さらに対策についても１０項目くらいある。それらを全て行うのは無理なので、ある地域での津波の被害をゼロにするために、どのアクションプランを組合せるのかというのが戦略となる。

個別の問題を取り上げろというのではなくて、アクションプランの中から、日本に適した情報セキュリティのあり方を考えれば、そんなに沢山あるわけではない。なぜなら、全部は出来ないからである。どこかを重点的に持って行かないといけない。

個別具体的な問題というのは各省庁が抱えている問題ではなくて、情報セキュリティに内包する切り口。どういう組合せで攻めていくのかというアクションプランがここに示されていないから、これでは戦略とは言えない。これは長期計画である。日本ではどうするべきかというポリシーが必要。

○　戦術か戦略かという議論はあるが、まずどこを守る議論をしているかを明らかにする必要がある。我々にはどうしても基幹ネットワークというのが頭にあって、政府のネットワークと、それから企業のネットワークがあって、それからというのをある程度やっておかくてはならなくて、そのやった結果が、この４つの項目だと思う。

ただ、私も最初見たときに違和感があって、事務局にお願いしたのは、最終的にどのようにしたいかということがあって、どのようにしているのかということをオブジェクトツリーのように書かないといけないと。何となく分かるんだけど、不安なところがあるので是非書いていただきたい。今日、皆さんがおっしゃっているのも、言い方は違いますけれども似ているところがあるのかなと。

○　戦略ということですけれども、限定合理性の上で動いていると。これは時系列的にも矜持的にもいえる。戦略といっても今の戦略であって、時間がたてばほころびがいっぱい出てくる。また、これを書くときに、今までは政府は完全だという神話があったと思うが、そんなものは捨てた方がいい。限定合理性のもとで可能な限り英知を集結していると。それでいろいろ議論して戦略を出していくんだということを書いていただきたい。

また、１回戦略を打ち出すと、経路依存性というのがあってみんな引きずられる。逆に攻撃をかけて、反対に出るやつは穴がある、だから穴をカバーする必要があり、それへの対応はポートフォリオ設計が重要。ウェイトはここにかけるけれども、手薄になるところは絶対出てくる。そういう戦略性というものが、この委員会でも求められている。

ウ　今後３年間を見据えた重点領域の設定について

○　重点領域の設定については全体がペンディングとなっているが、意味的には、ここに具体的なアクションプランを書き込むのかなと考えている。したがって、ここが現時点でのポートフォリオなのか、あるいはそれを管理するマネジメントのことを書くのか、最終的にはその辺りになるのではないか。

また、基本戦略の素案の中に「今後３年間に取り組む重要政策」という項目があるが、そこに研究開発・技術開発の分野において書き込むものになるものということ。

○　領域の拡大に賛成。技術的な面、それから運用、そして法律といった面をシナジーというか、上手く取り込んだ研究開発、スキームを作るということが重要だと思う。
　それともう一つは非常に大局的であるが、いろんな段階でソフトウエアの問題となっているＯＳ。これは韓国、フランス、アメリカも取り組んでいるが、技術的にも防衛的にも、また民生にも使われるのでナショナルセキュリティ的なものになると思う。
　一つは広義の研究スキームの開発と、もう一つは根幹なソフトウエアであるセキュアなＯＳと、これは核として国が持っていないといけないと思うが、その二つのアクションプランが組まれると思うところ。

○　国産のＯＳに限らず、ソフトウエア以外にハードウエアでも可能性はある。持っていた方が良いと思うが、作ったからには王道をいく必要がある。作ったからには世界に出せるものをと。
　ただし､他と競争して勝てなくても技術部隊は戦略として残しておくこともあり得る。自分達で出来る技術を残しておくのは間違いなく重要。評価するためにも重要。先ほどの話と矛盾するが、なるべく使いたいが、ひょっとすると使わないかもしれないと思わないと危険。作ったから、絶対自分で使う。しかし、そこは日本という国がそこまでキープできるかどうか疑問｡技術をキープするためにはコストを度外視する必要があって、それを優先させるかどうかということ。不用意にやると、そこが逃げ込む場所になってしまう。

○　ＯＳについては、全てゼロから国産でとか、技術を守るために絶対にというのではなく、いろんなレベルや階層があり、各国が手を付けてもいる。民生品にも使おうとしている。マイクロソフトもかなり安全なＯＳを作っていて、それを製品として出すか出さないかは経営的な戦略を考えているというレベル。それとまともに対抗しようとするものではない。いろんな要素があるものを手短かに言ったので、もう少しきちんとした議論をする必要があると思う。

○　聞いた話では、トヨタという会社は本当は自分たちでタイヤも作れる技術を持っているが、ブリヂストンの方が優秀なのでそのタイヤを付けて出荷している。ただ、ブリヂストンが手を抜けば、いつでも自分たちでタイヤまで付けて出荷することはできる。本当の話かどうかは知らないが、先ほどの議論もそういう考え方と理解したが、それでよろしいか。

○　セキュアなＯＳには賛成。やり方はいろんな考え方があるが、やる以上は勝てる戦略で､勝てるシナリオに乗ったものでないといけない｡やりました､というだけではダメ。日本だから持っていないといかん、というものでもないと思う。

○　３年間を見据えた重点領域の設定については、先ほどの議論で「場の設定」について考えていただきたいと申し上げたが、現場、オペレーションとの一体化を図る上での研究開発を、そうした「場」の中で考えていただきたい。
　各省庁のアプリケーションの中には、情報セキュリティ技術を継続的に考えていくとの意見が出ていたが、継続的な脅威分析をやっていく場、社会システムデザインをやっていく場というものが横断的に必要である。継続的に脅威分析をしながら、研究開発テーマを絶えず更新して行く場を設定する。そういう提言を重点領域に入れていただきたい。予算は大してかかるわけではないので。

○　今日いただいた資料は、真ん中のあんこの部分だけという印象。最初のあるべき姿、まずどうあるべきかというのが形にならないと問題点というものが見つけられない。その指標があってどういうところが問題となるのか､そういう部分を書いていただきたい。それからアクションプランのことについて書く。前と後ろがどう繋がるかが、かなり難

しいところだと思う。

○　目的は何であって、それに対してどうやっていくのかというのは、是非骨子案に書いていただきたい。どういう形でまとめていくのかということについては、事務局にはもう少し早めに作業をして、早めに各委員に流していただきたい。それをメール等で議論していかないと、とても自信を持って報告書を出せない。

○　世の中に発信していく上でレポートとして非常に大事だと思うのは、グランドチャレンジの設定。例えばどのくらいの抽象度でやるのかということ。事務局でまとめ、次回かその次には出されるのが必要だと思うが、最終的には何がグランドチャレンジなのかアイデンティファイされるのが技術戦略的には重要。

○　グランドチャレンジは最終的には非常に大切だと思われるが、多少ばかばかしいものから始めてもかまわないのではないか。例えば、２０１５年にはウイルスに感染するＰＣは無くなるなど。妄想的でくだらないところから始めてもかまわないと思う。

○　まだグランドチャレンジについては同床異夢のような感じ。少なくともコンセンサスはとれるようにしないといけない。今のままだと議論が舞い上がったままになる可能性がある。今回の議論を事務局で整理して骨子案を作成し、次回はそれについて議論をまとめ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立ち上げたいとの旨、事務局から提案があり､それをベースに議論をしていきたいと考えているので宜しくお願いしたい。

(4) 今後の予定

○　事務局より説明。

以上