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 11 回会合議事要旨

１．日時　平成２０年９月２９日（月）１５：００～１７：００

２．場所　内閣府本府 5 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］
志方 俊之（帝京大学教授）
田尾 陽一（セコム株式会社顧問）
中西 晶　（明治大学教授）
[グランドチャレンジ検討ワーキンググループ主査]
後藤 滋樹（早稲田大学教授）
（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
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

○　前回の委員会で設置が決まった、グランドチャレンジ検討ワーキンググループの第 1 回会合が 8 月 28 日に開催されている。　グランドチャレンジ検討ワーキンググループにおいては、今までの委員会で指摘された内容を中心に、グランドチャレンジ型研究開発・技術開発のテーマ等についての検討を実施していく。

本日は、グランドチャレンジ検討ワーキンググループの主査である、後藤教授に出席いただいており、ワーキンググループでの検討状況の報告をいただく。また、本日の本委員会における議論をワーキンググループへのインプットとしていただく。

また、第２次情報セキュリティ基本計画についての検討を行っている、基本計画検

討委員会が１０月１４日に実施されるので、技術部分について本委員会での議論をインプットする予定である。

○　グランドチャレンジ検討ワーキンググループでの検討状況は、「資料３－２：グランドチャレンジ検討WGの議論の方向性について」に記載されている。

○　現在の予定では、グランドチャレンジ検討ワーキンググループは５回程度実施した後にとりまとめを行うとのことだが、とりまとめの段階においてグランドチャレンジのテーマはどの程度の具体性を持って、何個ぐらい出すかについての、現時点での案は存在するのか。

○　グランドチャレンジ検討ワーキンググループ第１回の会合においては、多岐にわたる議論を行ったため、何個テーマがまとまるかについては未検討である。会合が進むにしたがって、集約の方向性を明らかにしていく予定である。

また、具体性については、資料３－２の４ページ目に将来予測の対象期間についての記述があるが、対象期間によって異なってくると考えている。３年先を対象にするテーマについては、比較的具体的なものになるし、１０年先になると抽象的な表現にとどまる可能性がある。

○　了解した。そういった形で、検討を進めてもらえると望ましい。

○　具体的な例になるが、高齢者の情報を持っている、消防・救急等の高齢者のサポートを行うべき地域の組織が、個人情報保護法との関係で情報を共有できないという問題がある。こうした問題を解決する情報共有のやり方については短期、長期いずれに入るのか。

また、認証基盤については、電子政府の話と関連して、認証基盤を社会としてどう整備するか、政府としてどう整備するかが議論になっているが、これも短期、長期いずれに入るのか。この問題については、私は短期で決まっていくのではないかと考えているが、これについてもワーキンググループで検討することになるのか。

最後に、１０年後の将来予測については、高齢化が益々進行することが予想される。さらに団塊の世代がリタイアし、高齢者がITを使うことが増加すると考えられる。そういう高齢化社会でITの使用が増えるとなると、高い確率でセキュリティ上の問題が起こることが考えられるため、そういう問題をグランドチャレンジ検討ワーキンググループで取り上げていただきたい。

○　すべての問題を検討することは難しいが、上記の意見は政府と関係の深い分野であ

り、検討対象の枠内であると考える。

認証については、NII（国立情報学研究所）と国立大学法人７大学の間では、UPKIと言う電子学生証プロジェクトの取組が行われている例がある。但し、個人的には、公共団体における全国民の認証については必ずしもうまくいってこなかったと思っている。電子学生証等現在進行中のプロジェクトが存在するため、ご指摘のように、短期でやらねばならない問題があると認識している。

高齢者に関する情報共有については、ご指摘いただいたITを使用する高齢者が増える問題とともに、いわゆる情報家電と言う形で家電の中にコンピュータに近いものが入ってきているという問題も存在する。これらの問題については、詳しい委員がメンバーに入っているため、ご指摘を十分意識してグランドチャレンジ検討ワーキンググループにおいて検討を進める。

○　電子政府の件については、電子政府の利用が低迷していると言うことがあり、電子政府の使い勝手を向上させる検討会の開催が予定されている。その中で、認証については、今までは安心を前面に打ち出してPKIでセキュアに固めていたが、ユーザーあってのセキュリティなので、安心で使い勝手の良い電子政府に向けた検討を行っていく予定である。

○　電子政府利用促進に関して出ているキーワードとして、電子署名に変わるものとして、ID・パスワードに電子官印を合わせて使用するという話が出ていると聞いている。もしも、電子官印を用いることになった場合は、証跡が残らず、否認が防げないという問題がある。普及を促進するのも大切だが、技術的にもう少し整理する必要があると考えている。

○　電子政府の認証をどうしていくかはこれからの議論であり、利用促進のために新しいものを作るか、既存のものを使いやすくするかはこれから別の委員会で議論されることになる。

その点に関するグランドチャレンジとしては、使いやすさと安全性という二面性がある問題なので、単一の指標で決められない時代になってきている。リスク対リスクのバランスが重要なので、そういう視点からもグランドチャレンジを検討して欲しい。

○　短期、長期ともに、「安全」と言うときのレベルがどの程度なのかについて、整理するのは、まさにグランドチャレンジの研究開発テーマではないかと思う。

○　そういう意見もあるであろうと思う。

○　１点目は、ライフスタイル・社会的な問題からの視点をグランドチャレンジ検討に入れていただいたのは非常に重要であると思う。情報を集めるという意味では、社会学者やリサーチ会社も利用できるのではないか。但し、ニーズからの視点に偏ると将来予測をゆがめる恐れがあるので、その点は注意する必要がある。

２点目は、研究の進め方について、よく言われる１５％ルールのように、オフィシャルなプロジェクトに従事していても、１５％は自由に自分の研究やその時点での状況に対応した研究等を行う。そのような仕組みも考えられるのではないか。

３点目は、情報共有の仕組みについてだが、この仕組みは重要である。現在の脅威に対する情報共有については、重要インフラ各分野の情報共有の仕組みである、CEPTOR 等の仕組みがあるが、それとは異なり、プロジェクト毎の情報共有の仕組みとしてどういうものを組み立てるかは、政府全体の最適化を図る上で非常に重要であると考える。

最後、４点目は、個別の話になるが、グランドチャレンジ検討ワーキンググループで携帯電話・モバイル・RFID のセキュリティについての話題が出たなら押していていただきたい。

○　４点ご指摘いただいたことは、貴重な意見として、グランドチャレンジ検討ワーキンググループの検討に活かしたい。

その内で、具体例として携帯電話を挙げられたが、携帯電話の問題としては、セキュリティが破られると、多くの情報が入っているため、問題になるという理解でよいか。

○　その通りである。技術的には詳しくないので、その他の議論が有れば教えて欲しい。

○　第 1 回会合では携帯電話については特に言及されていなかった。但し、携帯電話は個々の機器の ID を取得できるため、注意が必要である。また、実際使用しているユーザーがあまりそういう認識を持っていないという問題もある。

○　ニーズ・シーズから将来を予測するというのは非常に難しい。どちらに偏ってもならず、両面から考えていく必要がある。また、ニーズ・シーズから将来を予測するに当たっては、例えば、社会基盤なら社会基盤だけという様に、目的を絞ら無いと発散して収拾がつかなくなる恐れもある。

２点目としては、グランドチャレンジと言うからには、現在の技術の延長よりも、将来のニーズを見ることが必要となると考える。例えば、できる機能を次々と機械に付加して必要とされない機能であふれても困る。自然科学者だけの視点ではなく社会科学者の視点も交えたバランスが必要である。

最後に、将来の技術予測に基づいて、例えば２０年後にすばらしいものができたとしても、それを使う人間が進歩しているかというと、必ずしもそうではない。また、将来の犯罪の例としてはゲノム技術を用いた犯罪も想定される。そうしたことから、弱い人を守れる災害対策や重要インフラ防護と言った国民の安全性を守るところから考えた方が良いと思う。すべてを対象にすると、あまりに話が大きくなりすぎるのではないか。

○　現在グランドチャレンジ検討ワーキンググループでは、１０月６日の第２回会合に向けて、意見の集約を行っている。第２回の会合では、今いただいたご意見を含めて、グランドチャレンジ検討ワーキンググループの中で検討させていただく。

○　なかなか難しい問題で、大変だと思うが、グランドチャレンジ検討ワーキンググループによる検討を進めて欲しい。

次に、今後のスケジュールについて事務局から説明をいただきたい。

○　資料３－１にスケジュールが書いてあるが、年度内にグランドチャレンジ検討ワーキンググループの案をとりまとめて、技術戦略専門委員会に報告する予定である。それを受けて、最終的には技術戦略専門委員会報告書という形で年度内３月までにとりまとめを行う。

また、関係の会議と調整して、政府のコンセンサスという形にしたいと考えている。例えば、総合科学技術会議やIT戦略本部への説明を考えている。

それと同時に、情報セキュリティ政策会議のセキュア・ジャパン２００９と言う年度計画にも具体積施策を盛り込む予定である。

○　説明は了解した。是非、グランドチャレンジの案を他の色々な部署と検討しながら、グランドチャレンジのスタートが切れるような形で動いて欲しいと願っている。

次に２つめの議題として、基本計画検討委員会第１次提言における技術戦略の検討課題と今後の方向性について、事務局から説明願います。

○　資料３－１の最後のページにあるように、第２次情報セキュリティ基本計画の策定に向けて、技術戦略専門委員会として、技術戦略をインプットする必要がある。そのために、本日の会合で議論し、１０月１４日の技術戦略専門委員会において佐々木委員長に報告をしていただきたいと考えている。

内容については大きく分けて３つの切り口がある。第１は第１次基本計画時の背景

がどの様に変化してきたか、第２は第 1 次基本計画で挙げられていた課題がどの様になったか及び第 2 次基本計画ではどの様にすべきか、第 3 は第 2 次基本計画に向けた基本計画検討委員会の第 1 次提言の中で取り上げられた技術戦略に関する部分についての検討である。

まず、背景となる状況の変化についてであるが、第 1 次基本計画において想定していた背景に大きな相違は存在しない。但し、第 1 次基本計画における想定は益々具体化して来ており、リスクの多様化、IT が使用される場面の増加と相まってリスクの全体量は増えてきていると考えられる。さらに、リスクが変化するスピードが速いため対応が遅れている面がある、無謬性を前提としているために対策が後手に回る、情報セキュリティにおける ROI（投資収益率）がはっきりと見えないためアピールが弱くなる、と言った問題も存在する。

これらの状況・想定の他に第２次基本計画が有効となる今後３年間で想定しておかねばならない要素があるかについてお聞きしたい。

次に、第１次基本計画で挙げられていた課題に対する検討課題と今後の方向性についてであるが、第１次基本計画には、①研究開発・技術開発の効率的な実施体制の構築、②情報セキュリティ技術開発の重点化と環境整備、③「グランドチャレンジ型」研究開発・技術開発の推進、の３つの柱が存在した。

①研究開発・技術開発の効率的な実施体制の構築、においては、技術開発の状況を継続的に見直し成果利用まで見据えた計画の策定や、政府が活用することを前提とした新たな技術開発の取組が求められていた。それらに対して、第１次基本計画下の活動として成功したのか、あるいはやる意味があったのか、そして、第２次基本計画でどの様に取り扱うべきかと言うことについて議論していただきたい。この議題はグランドチャレンジとも若干関係があるが、そのほかにも政府調達による技術開発成果の活用などとも合わせて議論したい。

②情報セキュリティ技術開発の重点化と環境整備、においては、その中にさらに３つのキーワードが存在する。「中長期的な目標に対する研究開発・技術開発の促進」については現在グランドチャレンジ検討ワーキンググループで検討しているが、そこでのアプローチにおける方法論として他のやり方の有無をお聞きしたい。次に、「情報セキュリティにおける投資効率の把握方法」は、旧態依然とした論文数・特許数等のやり方が使われているが、情報セキュリティにおける投資効率の把握方法・物差しとして適切なものが有ればご意見をお伺いしたい。最後に、「政府が取り組むべき研究開発」としてポートフォリオの作成以外に、研究開発・技術開発のテーマを把握し、効率的に投資をしていく方法があるかどうかをお聞きしたい。

③「グランドチャレンジ型」研究開発・技術開発の促進、においては、本日の第１

の議題で検討したが、グランドチャレンジ検討ワーキンググループで検討しているやり方の他に、どの様な体制が必要かをお聞きしたい。例えば、電子政府のシステム作成に当たっては、SBD(Security by design 又は Security based design)と言って企画段階からリスク及び必要な対策を検討してシステムを構築するというやり方をしようとしているが、それと似たような感じのビルトイン型の研究開発が有るかどうかのご意見をお聞きしたい。また、短期的な問題解決の進め方として、単に要素技術をインテグレーションする以外の方法があるかや、中長期の研究開発テーマとしてグランドチャレンジ型研究開発・技術開発以外に検討の方向性がないかどうかもお聞きしたい。

最後に、第２次基本計画に向けた第１次提言においては、技術開発の分野において、次のような論点が挙げられている。

情報セキュリティ対策を標準化すれば、低コストで誰でも容易に行えるようになるため、そういった取組を進めるべきでは無いかという論点。

技術面・運用面において、人為的なミスのような、人的側面をカバーした技術開発を検討するという論点。

国として重要な技術は、国策として推進すべきではないかという論点。この点については、国策として国産技術のみで情報システムを構築できるようにするべきだとの主張がある一方、政府調達においては国際標準を公平に採用するべきとの要求もあり、検討が必要である。

新しい情報技術の利活用が始まってから情報セキュリティ上の脅威が発生し、それに対する対策が取られるまでにタイムラグが発生してしまうが、そのタイムラグを短縮するにはどうすればよいかという論点。例えば、情報技術の発展と同時にビルトインの形で情報セキュリティの技術開発・研究開発を行うことで、後追いでセキュリティ研究開発・技術開発を行う間に問題が大きくなることを防止すると言ったやり方などが考えられる。

家電や自動車、オーディオ・ビジュアル機器に入っている所謂組込用ソフトウェアのセキュリティを守っていくための方策として何があるのかと言う論点。

以上のように、背景となる状況の変化、第１次基本計画で挙げられていた課題に対する検討課題と今後の方向性、第２次基本計画に向けた第 1 次提言において技術開発の分野で指摘された論点について議論していただきたい。

○　確認になるが、１０月１４日は情報セキュリティ政策会議になるのか。

○　１０月１４日は第２次基本計画を検討している、基本計画検討委員会である。

○　了解した。１０月１４日の段階では、先ほど事務局説明にあったすべての事項について答えが求められるのか。それとも、方向性を示した上で、今後それに従って検討するというレベルの回答でよいのか。

○　すべての事項に対して答えを出す必要はない。但し、PDCA サイクルでたとえると、第１次基本計画が Plan の段階だとすると、現在 Do の段階として実行しているわけだが、Check してそれに対して対応する段階も必要となる。そのため、第１次基本計画の評価と環境の変化を勘案した第２次基本計画に向けた技術戦略における方向性を出すことは必要となると考える。

○　それでは、順番に議論したい。まず、環境の想定に関して議論する。

環境の変化という点については、システムに対する社会依存度が益々上がってきている状況からは、安心・安全に対する要求も高まっていると考えられる。それに合わせて、私が IT リスクと呼んでいる、広い範囲の情報セキュリティに対するリスクも広がっているように見受けられる。

例えば、公開鍵証明書の期限切れによってシステムがダウンすると言った例があり、安全を目的として設置した対策が逆に安全性を下げてしまう結果になったことがあった。このように、セキュリティというか、安心・安全に対して考えるべき範囲は広がっており、情報セキュリティにおいてもより広い範囲で捉えるべき時代が来ているというのが一つの設定であると思われる。

○　一般論では、情報セキュリティの範囲は広がってきており、今までセキュリティの範囲とされていた枠を超えてきちんとカバーされる必要があると考える。但し、本技術戦略専門委員会の文脈において、そこまで広く考える必要は無いのではないか。

○　確かに、範囲がどこまでを対象とするかという話は難しいものがある。現実的には、情報セキュリティの範囲が広がっているという話が、多く出てきているとは思っているが。

○　既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランス及び低コストで対策を進める方策についての意見である。

この点について、現場で何が起こっているかと言うことを頭に描くと、具体例としては、営業がいかにして売り上げを上げるかと言うことで、そのために、お客様の情報を多く集めて PC に入れることになる。ところが、その PC を置き忘れたり、盗まれたりする例が多発しているので、それに対する対策をいかに取るかについて企業は苦

労している。他方で、省庁からは情報漏洩が発生した場合には直ちに報告すること及び、紛失・盗難にあったPCに情報が入っていた顧客すべてに対しての連絡や、記者会見が要求される。ここで、情報セキュリティ対策がされているPCだと、報告のみ良いとするガイドラインもあるのだが、分野において微妙にニュアンスが異なっていることに加え、要求が高くコストがかかるので企業に掛かる負担が大きくなっている。

このように、技術としての対策と、省庁等の考えが合致していないと、どこまで投資して良いか企業が悩み、投資効率も下がってしまう。顧客の情報保護とコストや実用性のバランスを考えなければならないと思う。

○　そういった技術を開発した方が良いと言うことか。

○　技術開発を企業に任せるのは基本だと思うが、マーケットがないと企業による技術開発は行われない。どこまでの認証を行うべきかという具体論をグランドチャレンジの中で行うという話が有っても良いのではないか。

○　事実関係で言うと、上記意見に対するニーズが高いことはよくわかっている。この点については、色々なリスクがある中で、プライオリティ付けをどうやっていくかが問題になっていると考えられる。

上記意見に対しては、リスクのプライオリティ付けに関するツールの開発・改良・研究が必要であるというのが一つの提案たり得るだろうし、そういったツールをベースにしたコンセンサスの形成も一つの提案たり得るであろう。

○　補足になるが、第１次提言における技術戦略に対する言及の中にも、技術対策レベルに関するコンセンサスの形成と言った言及がなされている。

○　セキュリティというのは守りの概念であるが、利便性を追求するあまりに守りがおろそかになっては困るので、全体としてみると守りが先となるのであろう。守りができないものが便利であると言えるはずはないのだから。

また、高齢化社会においては、高齢者でも使いやすい様に対策を実施する必要がある。一つの例ではあるが、ウェポン・システムの開発において、通信機は熱を出すので、敵に検知されないために外気温と同じ温度での運用が行われることがある。そういった機器はマイナス２０℃における運用も考えられるのだが、目盛りが細かいと手袋をした手で扱えないという問題が起こりうる。また、自動車においても１４０ものコンピュータが使われていると言うが、運転をする人間は、ブレーキ・アクセル・ハンドル等のみを考えているわけで、搭載されているコンピュータを意識する人はいない。このように、実際に使用する人間のことを考えて作成することが重要である。

セキュリティにおいても実際に使用する人間のことを考えることは重要で、高齢者に、複雑な操作や厳格な手順を求めることは難しい。これから高齢化していく中ではフェールセーフの考え方に基づいて、使う人のことを考えた対策が必要になるであろう。

○　おそらくウェポン・システムにおいては９９．９９９９％安全であると言った精度が求められることもあるだろうが、民生用のシステムでは、必ずしもそこまでの精度は要求されない。このように、第１次提言においても、システムの重要性によって適材適所でレベルを変えて良いと言う話になっているので、その点はご理解いただきたい。

また、先ほどの背景については高齢化社会への言及が無かったので、これについては考える様にしたい。フェールセーフのための技術開発や、ビギナーがいつまでたっても無くならないという問題、高齢化等の人的要素の変化を第２次基本計画に盛り込むことを検討したい。

○　重要な問題があると、それに対して議論して対象に応じて関与者がコンセンサスを取ることができるのが良い仕組みであろう。その際に、民間での研究については、市場が選択を行うのであろうが、採算を取るのは難しいが必要性の高い研究については、検討が必要である。

状況の変化の話をしてきたが、第１次基本計画で挙げられていた課題に対する検討課題と今後の方向性についても議論していただきたい。

○　現在グランドチャレンジ検討ワーキンググループで使用しているアプローチの他に、中長期的な研究開発・技術開発を行う方策についてご意見をいただきたい。

○　やり方は色々あると思う。今回のグランドチャレンジ検討ワーキンググループでは専門分野のカバレージを考慮して、各委員の意見を聞いているが、このやり方だと収まりは良いであろうが、極端な意見は出にくい。サイエンス・フィクションのように多少荒唐無稽でも良いので問題を設定して考えてみるという方法も考えられる。

例えば、日本では情報通信全体に対する大規模アタックを受けた経験はあまりないが、韓国のインターネットは SQL Slammer による攻撃の時は、長期間にわたって止まってしまったという事例もあるので、そのように最悪の事態を想定すると言うやり方も有るかもしれない。

○　検討中のグランドチャレンジでは、全体として対処すべき事項もあるし、個別に国

の一部や民間の一部で対処すべき事項もあるだろう。そういったものを含めてグランドチャレンジ検討ワーキンググループの報告が上がってくると、技術戦略専門委員会の報告書に反映のしようもあると思われる。

○　グランドチャレンジのテーマとして収まりの良いところも、悪いところも含めて俯瞰できるように報告を行いたいと考えている。

○　研究員の評価及び研究開発・技術開発の効果を計るのに良いアイデアはないか。今は、外形的にシステム開発予算の何%をセキュリティに使うという疑問とも思える考え方も出てきている。ロジカルに評価が定まるやり方が有れば、検討したい。

○　研究開発・技術開発の評価は大変難しいところがある。

○　システムを対象に考えた場合、システム自身が時代とともに移り変わっていく面があるが、他方で継続して運用するという要求も存在する。

例えば、暗号の危殆化を例にすると、一方では暗号の強度が落ちるため暗号方式を変えるという要求になり、他方では現行のシステムで運用しながらどの様に変えていくのかという問題が発生する。

このように、時間的な流れの中で考える課題は多く、そこに向けての研究開発・技術開発も必要になるのではないか。

また、セキュリティ技術をうまく使うことによって、日本としての競争力を高めると言うことも考えると良いのではないか。例えば、暗号対策によって、電子的な印鑑のようなものを実現し、社会生活を便利にすると言ったような。

○　後者の話は、先ほど、国策としてどこまでセキュリティを推進すべきかと言った話があったが、そこの話と関係するのではないか。

○　投資効果の把握という話があるが、グランドチャレンジなので、費用対効果にこだわりすぎるのは良くないのではないか。費用対効果にこだわりすぎると、チャレンジが小さくまとまりすぎてしまうように思われる。

○　費用対効果の話に関連して、プロジェクト管理手法についての検討も行われるのか。

○　プロジェクト・マネジメントについては、様々な場面に関連する知見を入れることができると良いと考えている。中長期的な研究開発・技術開発の促進や、投資効果の

話とも関連する。

インターネットの世界の標準において、１０年前ぐらい前はRFCによる技術仕様にセキュリティを考慮しないとかかれることが結構あった。このツケが今に回ってきているように感じられる。セキュリティのタイムラグについても、各ポイントにおいて、見直してチェックするという仕組みができれば良いとは思っている。

○　研究する立場から言うと、どの様になると情報セキュリティに関する研究がやりやすくなるのだろうか。

最近心配しているのは、一時期情報セキュリティに対する過剰投資があったが、今はそれが冷え込んで逆に減ってきている印象を受ける。

○　投資というものを考えたとき、研究開発・技術開発と製品化の間にはギャップがある。製品化を行っても論文を書けないので、大学の研究者に製品化をやらせるのは無理があるが、企業でやるにしても人・金・物・時間が掛かるので難しい面がある。

実用化については、片手間で考えるのではなく、実用化のテクノロジを研究開発する必要があるのではないか。

○　現状認識として、実用化・実装・運用に対する評価は、はっきり言って低い。セキュリティ技術の実装、実用化に対する重要性を認識してもらえるような仕組みは何らかの形で必要であろう。具体的にどうするかは難しい所がある。例としては、国による後押しを行うか、スキル標準等の話の中でオペレータのような実装・運用に関わる人を評価する仕組みを考えるか等の方法は考えられる。

ただし、この点をしっかり考慮しないと、せっかく良い技術を開発しても実用化されないために、高信頼性IT社会が実現できないという問題が起こりうる。

○　グランドチャレンジとは離れるが、一つの研究開発を企画から実用化まで行い、どの程度費用がかかるかを調査してみるというプロジェクトもおもしろいかもしれない。

○　他の議論が無ければ、本日の結論として、　議題１については、本日の議論を基にグランドチャレンジ検討ワーキンググループにて議論を深めていただく事とする。

議題２については、本日の議論及び後日各委員からいただく意見を基に、事務局と調整の上、１０月１４日の技術戦略専門委員会にて報告させていただく事とする。

以上