技術戦略専門委員会グランドチャレンジ検討 WG
第２回会合議事要旨

１．日時　平成２０年１０月６日（月）１５：００～１７：３０

２．場所　内閣府本府５階特別会議室

３．出席者

［主　　査］
後藤 滋樹（早稲田大学教授）
［主査代理］
安達 淳　（国立情報学研究所）
［委　　員］
磯村 浩子（(社) 日本消費生活アドバイザー・コンサルタント協会）
伊藤 光恭（ＮＴＴ情報流通プラットフォーム研究所）
加藤 雅彦（(株) アイアイジェイ　テクノロジー　IBPS 本部）
楠　 正憲（マイクロソフト（株））
西本 逸郎（(株) ラック　サイバーリスク総合研究所）
二木 真明（住商情報システム（株））
松並 勝　（ソニーデジタルネットワークアプリケーションズ（株））
三河尻　浩泰　（(株) 富士通大分ラボラトリ）
森山 浩幹（(株) エヌ・ティ・ティ・ドコモ）
山田 安秀（(独) 情報処理推進機構）

（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
内閣府政策統括官付参事官付
警察庁情報通信局情報技術解析課
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
文部科学省大臣官房政策課情報化推進室
文部科学省学術政策局政策課安全・安心科学技術企画室
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
防衛省運用企画局情報通信・研究課情報保証室

４．議事概要

○　前回に引き続き自己紹介を兼ねたコメントをお願いしたい。

○　　専門は家庭経営、生活経済学で消費者被害を家庭経済のリスクと捉えて、その対応にアプローチしている。消費者問題のテーマも大きく変わりつつあり、現在でも続いているが食品の安全問題、バブル後には契約の問題、現在では金融商品・サービスあるいは、情報通信サービスなどが重点になっている状況。最近では情報通信法というものが検討されているようだが、消費者保護規定が入れられるよう１１月中に２日間の相談電話を設置し、一般からの情報を集める活動なども予定している。情報通信サービス分野は、従来の食品や電機産業などの業界に比べて消費者対応、説明、表示など、まだ進んでいないところも多い分野ではないかと思い、ここでは利用者や消費者のサイドで原則的なことを申し上げたいと思っている。これからの議論の中で、先端を高くすることはもちろんだが、底辺を広く厚くすることにも技術を生かしていただきたいと思う。情報関連商品・サービス提供の分野では、法律や開発時の状況などの問題はさておき、ご意見はあろうかと思うが、内包する弱点などの責任は基本的には製造・製作した側にあるのではないかと考えており、たとえ利用者・消費者が一度は失敗しても安全にやり直せるようなフェイルセーフの考え方を是非、製品・サービスの分野に取り入れてもらいたいと思っている。

以下、資料に沿って事務局から説明

資料３（親委員会からの報告）

資料４～６（プロジェクト管理）

＊＊

プロジェクト管理について

＊＊

○　　企業でも、どのように投資をして、そのプロセスを評価するかということは結構問題となっており、また、先日会合で問題提起が合ったように随時方針は変えて行かなくてはならないし、そこには専門家の知見がいる。そういう専門家の知見が要らないようなプロジェクトは成功するはずもないということが１点。もう１点は、弊社のような企業はでは投資をどう考えるかというと、よく、ＩＴ関係の投資であるようにＩＰＯ（新規株式公開）により資金を集めて大きく出ると大抵は失敗してしまうが、それは良くも悪くもお金に紐がついていて、計画に対してどう責任を取って行くかというフレームというのが無いからだろう。一方で従来の利益の積み上げを取り崩す覚悟で投資を掛けているというものは比較的成功しているように見える。ただ、今のように非常にコンプライアンスが強くなって監査の目が厳しくなると、そこをどう上手く

やるのかが企業でも課題になっている。

私自身がセキュリティインシデントの現場によく行くが、結構大きなシステムでＳＩが入っていても、トラブルとなっていることがよく見受けられる。請負形式とか成果を決めて物事をやって行くと言うことには限界があり、決められた工程、施工技術、材料などを使って自動的に進められるものについては請負で良いが、研究開発などについては難しい部分がある。そこで資料に書いた改善案だが、研究開発は何らかの仮説を立てて計画をするわけだが、その仮説を常に評価してゆくような部分や、その評価に対して適切にプロジェクトが運営できているかということを検証するプロセス、別のスキームが要るだろう。

○　様々なプロジェクトを鳥観してみると、複数の組織がコンソーシアムを組んで実施しているものが多々あるが、実質的にはその個々のプロジェクトの主体が全体のことを考えず、もともと自分たちのやっていた研究テーマというものを継続的するためにやっているという側面が見られることが問題意識の発端。そういったものを改善して行くためには、プロジェクトの目的や内容、それを実施するためのリーダーが最初に必要で、そこからスタートするべき。改善案として示した「大統領的な権限を持ったプロジェクトマネージャー制度の導入」だが、前回の議論の中にあったＰＭＯ（プロジェクト・マネージメント・オフィス）制はそれとして、その組織の中に本当に強いリーダーがいなければ存続できないと思う。そのリーダーは個別要素の開発者とは違う中立性を持ち、できればビジネスに理解があって研究開発の出口の想定が出来る人が望ましい。また、世の中のニーズなり変化を反映するという責任を持つということは、先ほどの仮説を修正して行くことにもなる。それは、基盤的な技術であっても実用的な技術であっても同じで、最終的には出口に対して責任が持てる体制、それは、オフィスという組織ではなくて、人に任せなくてはいけない。ＩＰＡの中に未踏プロジェクトというものがあるが、このプロジェクトマネージャーは実際に最初に選ばれてプロジェクトの企画に加わり、プロジェクトの内容とリーダーがセットになって審査をし、公募を行う方式を採っている。そして、実際にこのプロジェクトでは、海外の有力企業にハイヤーされるくらいの天才プログラマーが産まれてきているので、そういうプロジェクトマネージャー形式というのは良いのではないかなと思う。

もう一つ改善案であるＮＩＳＣによる「継続費」の指定だが、これにより単年度主義弊害を排除するメカニズムを導入を図るもの。「継続費」は財政法で決められた複数年度に渡って予算の割付をする制度。小泉首相、竹中大臣のときの「骨太方針２００３」には、実際に「国庫債務負担行為」を利用した「モデル事業」として盛り込まれ、実際の国の事業に適用されたもの。その後「モデル事業」がどのようになったかは知らないが、それくらい強い権限なり、財政的な制度の裏付けの下に行わないと、前回

議論されたプロジェクト管理に関する様々な弊害というものは、ここでいろいろな議論をしても、財務予算プロセスの中で立ちゆかなくなってしまうので、これくらいの強い決意でやるべき。

○　それでは、プロジェクト管理について、意見を伺いたいと思います。

○　確かに、実際を見ていると研究を行う者と評価・推進する立場にいる者とが、うまく噛み合っているところは良いと思うが、研究を行う方が見て欲しいというところを、評価する方は少し違った観点で見ていることがある。また、冒頭に、民間企業や、独立行政法人においても、いろいろなルールもあり現状の改善するべき課題もあるとの指摘もあった。

○　山田委員のペーパーにもあるが、プロジェクトマネージャーの部分は、推進に責任を持つというサブジェクトだと思うが、プロジェクトの推進がうまく行っているかどうかということを評価する仕組みというものは必要だと思っている。研究の成果を推進する主体のあたかも成果であるように掲げてしまうといろいろな弊害が起こってしまう。推進の方法を改善しようとするというようなことが全くなくなってしまう。だから、これらは独立して、研究の成果とプロジェクトの推進のやり方は分離して評価する必要があるのではないか。

○　プロジェクトマネージャーはプロジェクトの推進をすることは当然として、その中で、世の中の環境変化なりに敏感で、やっていることの内容が将来は出口として、何かに利活用されるというところを意識した人でなくてはならない。従って、そのプロジェクトマネージャーには内在するものとして、成果の評価は日常的には含んでくる。もちろん、そのプロジェクトマネージャーに全て委ねて良いのかという問題もあるので、外部的な評価委員会なりを別途設ける必要はあると思うが、日常的にはプロジェクトマネージャーが常に管理をしていて、強い権限を持たせ、変えるべきだと思ったらば、その評価委員会を経るまでもなく改正する権限を持たせないと、多分、世の中の環境変化には追従できない。

○　プロジェクトの中身はもちろんだが、やり方について、特に上手く行っているとこ

ろについては意識的に記録に残すことが少ないので、当事者とは別に記録する人を置いて、やり方そのものを後に共有するとか、それを守るという方法で行うのが良いのではないかというご指摘だと思う。

未踏プロジェクトというのは、私が理解する限り IPA の中でも、比較的に新しく独特だと思う。ただしプロジェクトマネージャーが頼りになるべき存在となった現在でも、フルタイムで就いているわけではないでしょう。その点は何かありますか。

○　外から見た印象になってしまうが、やはりプロジェクトマネージャーは、社長とか、大学の先生でもかなり有名な、企業の社長であった方がリタイヤして大学の先生になった方が多く、かなり忙しい状況。従って、１年のうちどれくらいこのプロジェクトのマネージメントに時間を費やすことが出来るかというと、非常に限られている。その中で、プロジェクトを良くするために外部の環境も見た上で意見を反映させるというのは難しいと思う。もし、それをさせるためには高給を払い、見合う責任を果たしてもらうというようなメカニズムを組む必要があるだろう。普通に役所で決められている単価で行おうとすると、まず、プロジェクトマネージャーになろうという人は見つからないので、そういう面で工夫するという手が一つあると思う。

○　PM とか、PO という制度は、日本でもいろいろなところに出ている。私も、昔アメリカでそういう制度をやっているので参考にしたら良いと働きかけていた。アメリカの方ではフルタイムということだが、その米国でも人件費の使いすぎではないかと指摘されるとの話しも聞きく。日本という国はフルタイムでやる割合少ないかと個人的に思っている。関連でお尋ねるが、未踏プロジェクトは、いわゆる請負型というではないという理解で良いですか。

○　請負なのか委託なのかは、別途確認します。

○　弊社は小さな会社の割には、いろいろ研究にチャレンジしてきました。しかし、失敗も結構多くて成功率は３割も行かない。ただ、研究というのは、そういう失敗も想定をしなくてはならない訳で、その状況に対して仮説に則ってチャレンジをして、また、再チャレンジしてゆくということが適切に評価されていないといけない。一度沈んだら終わりというのは萎縮する理由となり、また、それに対応してアリバイ作りを

されても、本当に国のためにはならなくなる。客のニーズに合わせた開発というのは、基本的には研究にはならない。やはり、ニーズのないところにシーズから作って行く、読んで行くということが必要。お客のニーズより夢とか、そういった部分をつかんでゆくようなところが必要。ただ、それを具体化すると、ニーズに合っていないものをなぜ作るのかということを言われるので、なかなか辛い。

○　成功率については、それくらいあれば非常に研究開発では、むしろ高いのではないかと思う。シリコンバレー的なものでも、５％位といわれている。ある大企業の関係者からも、その会社を外から見ると成功しているように見えるが、社内のいろんなプロジェクトからいうと、やはり１割も行かないという話しを聞く。

研究開発は、リスクの高いものであって、どのように、そのリスクに向き合うかというのは、社会の知恵、組織の知恵ということかもしれない。

○　私も自社で研究に従事しており、先程の３割という話しは非常に同意するところ。やってみて、このやり方ではうまく行かないことが判明したという成果もある。ゴールに至るまでの途中の段階で、結構、失敗の繰り返しがある。それを、１年で切って、その時点で失敗であるため終了する、という形は、研究ということに向かないのではないのではないか。

○　国家プロジェクトの場合は全部成功したことになるので、そういう記録は残らない。ここで、失敗することは当たり前だと大きな声で言うべき。

○　失敗したという言い方が良くない、成果の途中の段階ということが明確に分かるとういうことが必要。会社でも、半年なり、１年なりで、こういうことをやってきたが、まだ、ここまでしか分かっていないというと、何だということになるが、だんだんゴールが見えてくると、ああ、そういう目的のためにやっていたのだなと、という理解は進んでくる。そのための説明というのは、非常に丁寧に細かくやって行く必要があると感じる。資料中の運営のところで、中間成果やノウハウが途中全然分からないというのは結構致命的だろう。

成果に対して、それを運用して行く発想も、もう少しあった方が良い。研究というのは最先端の話しで、これを最終的に社会のメリットとして還元して行かなければならないが、おおよその場合は成果が出たというところで終わってしまい、あとは自由

に使ってくださいという状況で放置されると、なかなか使いにくい。それをさらに社会の中に浸透させて行くということも含めての全体のプロジェクトだという発想で行かないと、今の発想で行くと閉塞感を感じる。

○　目標を立て研究成果を目指して研究をやって行く際に、結果として予定した成果に達しなかった場合に、それは失敗なのかというと、研究の過程で出てくるものも大きいと思う。特に中長期的で複合的な技術が必要となってくる課題となると、要素的にはいろいろなものが沢山出てくる。例えばアポロ計画などでも素材や制御技術、その他諸々の成果がその過程で出てきた。プロジェクトの進行では、当事者は最終的に予定された成果に向かって一直線に進んで行くので、その中間で何が出てきたか整理する余裕はない。よって、第三者的がプロジェクトを集中管理して研究の過程、中間段階で出てきたものをレビューしながら、別のものに使う検討をしてゆく組織があっても良いのではないかと思う。そうすると、環境が変わって最終的に当初予定した成果にたどり着けなかったとしても､その過程で､得られたものを社会に還元することで、それをプロジェクトの成果の一つに出来る。

○　ご指摘のとおり、企業などでは実際にやってみて、うまく行かなかったところというのは、貴重なノウハウになっているという場合がある。私も学生にポジティブなことだけ解説すると、いわゆるチュートリアルというのは、教科書を読んで受け入れをすれば出来るかもしれない。落とし穴があるとか、皆がこうやれば出来ると思っていても実は出来ない、ということを知っているが本当のプロであるということを言っている。そういったところがうまく共有されて行くことも、特に、今回話題になっている公的なもので推進する場合には、ある程度のところまでは共有したいと思う。もちろん、最終部分は企業の競争に委ねる活動であると思うが、実際にもシリコンバレーではサクセスストーリだけの人はあまり信用がなくて、七転び八起きをしてきた人がどのようにしてきたかを皆で研究しているようなところがある。日本でも日本が伸びて行く時代には、このあたりは何となく共有されてきたような気がするが、守りに入ってくると、それぞれがバラバラになっていると感じられるところがある。

○　私は以前の職場で全然成果が出ないと言われて続けていてことがありました｡ただ、そんなことをしている中で得たものというのは、今から考えるととても多い。最終的に形にならなくても、その過程で考えたことや部分的な要素が自分のノウハウとして残っていて今の自分を作っているということを考えると、当人は何十年か経ってやっ

と整理が出来た状態となったが、そうではなく、第三者的にそういうものを見ながら整理をしていって体系化を図るワークをする別の部隊があれば、それらをより早い段階でノウハウにして行けるのではないかと思う。

○　リスクをどう管理するかという話は難しい。スタンフォード大学の青木先生が、比較制度分析の本を書いていて、これは日本でもベストセラーの本ですが、そこで、いわゆるベンチャーキャピタリストとエンタープレイナーの共生モデルというのが書いてある。実は自由競争の様に見えるけれども小さい企業に資本を出す人がいると、その人は専門家ではないがその企業を注視しているので、小さい企業の自由競争の様に見えても、そのコミュニティ（業界）においては、あるところで情報はシェアされている。いくら NDA（秘密保持契約）があっても転んだところと同じところにお金を出すはずがないので、どうも社会的な仕組みとして、これは、日本だけではなくて、他の国でも、あるいは、アメリカの国内でも同じようなモデルは回っていないという指摘がある。世の中全般というのがどういう風に回っているのか、ということは専門家の方が研究はしているが、実際に研究するとか、研究の企画とか経営をされている方も含めて、すこし、世の中で共有されていった方が良いのかなと思うことがある。同じことが、公的なプロジェクトでも当てはまるという気がする。

○　評価の基準の方式の部分で量以外の評価軸があるかだが、研究の中間期にもいろいろなものが出てくる。それは、そのプロジェクトの直接の目的なり出口に対応していれば一番良いが、例えそのプロジェクトに直接関係なくても、実際に使われている、使えることが確実であるなど、他にどれだけ直接、間接に世の中に実際に利用され得るかということを、見る評価軸があるのではないかと思う。

○　その場合には、研究の当事者の方から主張するべきとなるのか。私も、あるところで評価する側の立場で仕事をしているが、評価される側の方に聞くと、研究が終わったばかりの段階では成果が直ぐに使われる訳がないと言われる。また、一部については数年後に追跡調査を行うが、その数年後に尋ねると、そんな昔のことをなぜ聞くのかと言われてしまう。評価の仕方の研究は、日本にも沢山専門家がいると思うが、個別プロジェクトについてしっかり具体的に見て行くというのは、まだまだ課題が大きいと感じている。

○　最初の計画に沿っているかどうかが現在の評価の中心だと思うが、最初の計画の時点なのか、後の評価のやりかたなのか分からないが、もう少し、評価軸を複数違った形で持ち、最初に紙に書いたことに対して評価をするだけでなく、複数の評価軸というのを考えるべきではないかと思う。

○　ある会の評価WGの評価軸は、それぞれのシステムに合わせてかなり多彩なものがある。ただ、メインの評価項目は所期の目的と比べて成果がどうなったかということがほとんどのプロジェクトで一番最初の評価項目にある。その後に、ものによっては、アウトリーチの活動が重視されているとか、対外的な発表、実用性、また、産学官みたいなプロジェクトもあるので企業側とのことなど、実は、相当な項目がある。そして、私も難しいと思っているのは、公的なものの評価は公平にやらなくてはという気持ちがどうしても働いてしまうことである。本当は個別プロジェクトで良いところは特記したいと思うし、評価の紙には文章で書くのだが、最後に集約して統計的に比較できるように評価結果を書く段階では、大文字の「A」「B」「C」という評価に分類されてしまう。すると、評価された方からは、特質をやはり見てくれていないということになり、先程の言った食い違いが起きている。

○　研究という大部分が失敗するもののリスク管理と言うことで唯一考えられるのは多様性しかない。アメリカでは大学にいる研究者から見た場合、国防総省、エネルギー省、NSF という３つがファンディングエージェンシーとしてあり、NSF で認められなくても国防総省のプログラムディレクターが面白いと言ってくれることもあり、その中で研究者は生きてゆく道を歩める。一般的に各省庁縦割りというのは悪い意味で使われる言葉だが、多様性から考えると違った観点で将来を見ている者がいるという方が安全だろうと思う。日本はお金がないので一丸となって総合科学技術会議が全部評価することにしてしまうとリスクが大きくなってしまうので、例えばセキュリティに関しては省庁毎の観点や軸を見据えて分野毎に予算を付け、セキュリティという観点でプロジェクトをどう採択するかを考えることが次善の策としてあると思う。ただ、我が国の方針を定め、それに限られた予算を投資して結果を求められるのは現実であり、余裕を持った研究開発を行うことは難しい。そういう中で、評価、評価と言われるのは、悪いものを悪いと評価するシステムが弱いのだと思う。いろいろなしがらみがある中で悪い評価を付けるには相当な覚悟が必要。ただ、悪い芽を潰すだけでなくて、伸びそうなところをどう確保するのかという点が重要になると思う。実際の評価は大変難しい。皮肉を含めて言うが、評価を受ける者に対しては評価基準を見せないというのが一番良い戦略だと思う。論文を書くことが評価軸だと知られたら研究者は

みんな頭が良いので論文を書く。数が勝負というなら数を出す。評価の軸に合わせてチューンして来る。特許を書けと言うことで、ずいぶん大学は特許を出すようになった。これが本当に、どれだけ役に立つ特許なのか私には分からないが、少なくとも評価基準と言うものを示したら、そのとおりやってくる。評価というものは主観評価でしかない訳だが、主観評価にどうやって客観性をもたせるかというと、例えば、評価する人数をある程度置くという話しになる。その辺を国の大きなプロジェクトでどう見るかということ。やはり国のお金を使って成功率が５％とかいうのは、基礎研究くらいしか言えず、ターゲットを設定した研究だともう少し成功率が高くなければ、それこそアカウンタビリティーの点で問題だと思う。特に心配なのが材料、バイオというときは基礎研究的なところに投資すると言うことが分かり易いが、ＩＴが絡むと基礎技術と言うと、制度設計の話となってしまうケースが多い。特に国が関わるものはそうだが、最近の日本の制度設計は例えば年金、法科大学院、裁判員制度など具合の悪いものが多い。しっかり考えても、あのような新しいシステムを作るというのは失敗するところが多いので、今後、ますますそれらが複雑になって行くときに、国があるレベルまで保障するかどうかというところが一番重要だと思う。

○　今、研究の多様性が非常に重要という話しがあったが、それと関連して目先のスコアカードが見えてしまうという理由の一つに、研究者のキャリアパスが必ずしも多様化していないという事があるのではないか。例えば本当に良い技術であればスピンオフして起業する位の気持ちを持っていれば、自分の人生にとっても良いものかどうかという視点が入ってくる。けれども、自分は研究者であり、社会にそれが使われるかどうかというのは所属する企業の責任であると考えると、逆に研究者としての自分がどう評価されるかというところに関心が行ってしまうということになる。必ずしも評価軸の多様性だけではなくて、様々な研究者のモチベーションがある中で、いかにガバナンスが働いて行くかと言うことを考えて行く必要もある。

また、長期の目標を建てにくい点に関してだが、決して予算規模が大きいと言えないなかで長期で評価することは難しい。その割には結構見ているフォーカスというのは民間企業の５年後１０年後に向けた投資に近いところがある様に思う。民間企業の場合は既存のデリバリーチャンネルがあると有利なので、それとは違うやり方を考えて行かないといけない。そのためには、どういったアプローチの違いがあるか、国のＲ＆Ｄの役割はどうか、どう見て行くかを考えなくてはいけない。個人的には発注者として一番品質に対して厳しくなるのは、自分が利用者になることだと思う。多くの先端技術が軍事研究から出てきたというのは、結局、報告書を受け取るだけではなくて、利用者として購入することがあり、それらが正しく動かないと人命に関わるなど、いろいろな不都合なことが起こるので、甘えの構造ではない厳しい評価が入っている

からだと思う。ソフトウェアの品質を巡る研究に関してもコストに対する考え方が違うところもあって、軍事の分野では１０年、１５年早く民間よりも導入されている技術がいろいろあると思う。よって、国が最初に使う、単に研究にファンドしているだけではない、というような切り口から出来ることがあるのではないか。

○　少なくとも今までの日本のやり方でうまく行くのであれば誰も苦労しない。お金がないといいつつ研究開発をしないと、これからの日本の道というのは大変限られてしまうし、非常に狭いところで生きて行かなくてはならないと思う。政府が大きいか小さいかというところではいろいろと議論があるが、やはり、公的なところが果たすべき役割は民間がいかに頑張ろうとあるだろうと思う。そして、民間が力を出しにくいと言うことであれば、ますます、政府の役割の分担するべきところは物量はともかくとして多いと思う。政府がファンディングだけではなくて発注者、利用者としての役割を果たすというものは、従来は強調されていなかったと思います。

○　成果をどう評価するかということは大きなテーマであり、進めてゆく上でいろいろと阻害要因があるのも理解できる。ただ、今後この WG で何回かディスカッションして行く中で、それら阻害要因となっている国の制度に対して提言をしてゆくことになるのか、それとも、それは仕方のないこととし、WG であるべき姿を出して、それと、既存の制度との間をつなぐ議論になるのか。

○　阻害要因を担当する役所に話しを持って行くことはやぶさかではないが、政府全体のコンセンサスになるようなものを考えないと現実的な解にはならない。いくら理想論を言っても、誰も見向きもしないようなものを作るつもりではない。

○　これからは日本の技術、情報セキュリティに関わらずＲ＆Ｄの在り方というのを作り上げて、それを持って行く、少なくとも情報セキュリティの技術開発はそれをモデルケースとして回したい。

○　補足すると、本ＷＧで得た結論は最終とはならない。結論を踏まえて、それを政府全体でのコンセンサスにするための努力が必要。それゆえ、各省にも出席を願っている。総合科学技術会議、財務省、会計検査院など、関係機関も納得するようなものに

しなくてはならない。全てこのWGで、最終的な答案を書くつもりでもない。そういう意味で、ここでは問題提起が出来るようなところまで持って行き、そして、他のところでも考えてもらうという形が理想的ではないかと思う。

○　そうして、全体のやりかたを　変えること自体もグランドチャレンジではないか。

○　いくら日本は計画性が強いと悪口を言ったところで、そう簡単に国の仕組み全体が急速に変わるものではない。ただ、その中でも、やり方はあると思う。１５年くらい前まで日本がうまくやってきた方法では、もう今後はうまく行かないのは明らかとなれば、工夫や提言というものがすぐには通らないとしても、いろいろ試してみて、観点を変えた方がいいのではないかという提案が必要になる。いくつか、具体的に出来ることも提案頂いている。これは、特に政府の中での話なので、誰かが文句を言っているよりは、こういうことを変えてゆこうという話しになるのが一番良いと思う。

○　研究と言うところを離れて実際にサービスを世の中に出している立場から言うと、サービスを出すにあたっても、研究と似たように目標とか、そういうものを建てさせられる。だいたいは収益を見るので、単年度黒字になる時期と累積損解消となる時期を見ることを絶えず意識して、最初に計画を建て進めることになる。ということは単純にいうと、非常に明確な目標基準があることであり、もし、それに至らなければ止めるしかない。あとは、そこで議論しながら進めてゆく、ということを繰り返している。先程からの議論を聞いていると、目標のようなものがもう少し明確になるべきかと思う。成果というのは多分企業の研究では、それが実用化するかどうかということが成功か失敗かの明確な基準だろうと思う。ただ、一方で多様性ということもある。これは他の企業とジョイントでサービスを始めるときに分かるが、自分の企業の基準と他の企業の基準は違っていて、あるメーカーと話しをすると、成功するまでずっとやるというところもあるし、それはそれで実績を上げているので分野ごとに目標の基準は違っても良いということは徹底させるべきだと思う。我々がサービスをやるときに、３年とか単年度黒字と累損解消の時期というのを見ながら、あとは、計画でこのくらいの需要数を見込んでいるということを基準に取るが、実際に経営企画とかそういう部門からは、何年後に目標に到達しなかったら撤退の審査をするという撤退基準というのも必ず出すようにと言われる。しっかりとした計画は必要だし、それを途中で変えるのも必要だが、我々のところでは計画を変えるときは非常に労力やお金が必要で、関係部門からも批判されながら行う。また、計画を行う方に課せられるものと

いうのも大きい。先程申し上げた撤退基準、ここまで行かなかったら、これは見極めるということも、逆に言うのも良いのではないかなと感じました。

○　弊社の場合は若干逆のこともあり、トップがやると言ったら１０年でも２０年でも諦めずに続けることもある。例えば、ペンコンピューティングなどは、かれこれ２０年くらい研究していますが相変らずものにならない。音声認識など、いくつかそういったものがあるが、経営に近いところで言うと３～５年と、５～１０年と、１０年以降というところをちょっと分けていまして、３～５年は製品のチームが扱って、ビジネスの基準で進めてゆく。５～１０年くらいのところが結構微妙なところでして、アドバンスドテクノロジー&ポリシーといって、もう少し柔らかい頭で考えたときに、社会制度のようなものが変わってくることも踏まえて、実現可能なところを考えてゆく。１０年より先のものというのは、良い論文を書きなさい、学会でプレゼンさせなさい、というところで、研究者にかなり自由にやるというようなことをしている。ただ、研究者のモチベーションも、グーグルの活躍を見て、より短期間で世の中のフィードバックを受けたいと言う気持ちが強まっており、これまでほとんどなかったが、研究所の技術を知的財産として他社に売る、研究所で作ったソフトに値段を付けて売るなどのことも始めている。それは、多分、実社会に成果を出すということを通じて、研究者に良い刺激になっているところもあるし、普通の製品とは少し違うポリシーで売ることによって、市場からのフィードバックを得られるというメリットもあるかと思っている。実は、研究所で良く動くものが出来ても、それを製品にしたときに見栄えのしないものになってしまうということが数年前の大きな課題としてあり、理由はいろいろあるが、プロトタイプを作ると言うこととそれを使ってもらえる製品に落とすというところでは、かなり発想が違っていて、そこの研究者の意識と製品開発者の意識のギャップをどうやって埋めてゆくかということが、数年前の非常に大きな課題でありました。そういう意味でここ数年行っているのは、開発者も研究的な新しい要素を提案出来るチャンスを増やしてゆき、反対に研究者も論文だけでなく動くソフトウェアを市場で提供して社会の評価を仰ぐなど、そのギャップを埋めということがある。結局最終的に研究がうまく行くということは、人をどうやって育てているかと、そのために何処にお金をかけるかというところにかかっている。そういう意味でいうと、ここ 20 年近く、なかなか政府による研究がうまく行っていないという話があったが、多分理由の一つとしてあると思うのは、市場での資金調達が非常に容易になったということであり、これまでであればトップノッチの、それぞれの企業の一番虎の子の技術者を国プロに出していた時代というのがあって、その時代はそれぞれの会社では資金調達が出来なかったから、競合他社とも一緒に組んで国の枠組みの中でやってゆくというところに一番いい人材が来た。けれども、市場で容易に資金を調達が出

来るのであれば、制約の多い国の資金でやる必要はないことになってくるので、それ以降は国でやっていてうまく行っていたかもしれないものが、民間の自主的な努力で出来るようになった部分があると思う。そうすると、これは、若干マーケティング寄りの発想になるかもしれませんが、やはり、人を育てるという意味で、資金が行き届いていないけれども、ポテンシャルがあるところにうまくチャンスを提供してゆくこと、そこで、しっかりと選抜されていて、高いポテンシャルがある人たちに対して、どういう風に機会を提供してゆくかという、非常に抽象的ですが育ちうるがチャンスが与えられていない人たちがいるか、あるいは、既にある領域では成果を出しているが、それをもう少し社会の役に立つような方向に頭を使うために、どういう風にマインドチェンジしてもらった方が良いかというところにお金を出す方法というのはないかなと思う。

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊
将来予測について
＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

○　資料７については、すべてを本日審議することは無理だろうと思うので、時間の許す限り行い、残りは次回のＷＧにて審議する。

早速ですが、高齢者、弱者への対応というところには２件、磯村委員、山田委員から、それぞれ、説明願います。

○　とにかく、情報弱者や高齢者などに対して、基本的な機能の範囲で使えるもの、例えば携帯電話などでは既にコマーシャルなどでもやっているものがありますが、同様に、情報セキュリティ対策でもそれらの方々が出来るような（やらなくても済むのであればその方が良いのですが。）ものがあれば良い。これは技術の問題ではなく、他の事情でまだ無いという状況だと思いますが、考え方を示しました。

○　ＩＴ弱者と言うか、社会的弱者、非健常者ですとか感覚の衰えた高齢者、高齢者でなくとも感覚の衰えた者、そういう方を全体として含めた、その層といいますか、そういう方々に対して手を施すということが必要なのではないかと思う。

資料にはすべて書き連ねたわけではなく、一つの例としてバイオメトリクスの認証を挙げた。この分野におきましては、高齢者ですとか非健常者についてのデータ・生体情報をどう評価するか、ということについて、実際には殆ど何もされていない状況の様だ。我々も別途調査中であるが、そういった認証方式とか、生体情報の劣化を想定した様な評価方式、データベース化といったものをやる必要があるだろう。この分

野でいうと、世界の全てを調べている訳ではないが、アジアでは韓国が比較的良くやっているようで、評価センターや技術開発センターを組織としても作って、国主体として進めているとのこと。アクセスシビリティにつきましても、視覚とか聴覚とかが衰えている方が、セキュリティソフトにパッチを当てると言っても、その作業がそういった方々に対して配慮されていないという部分がある。世界にどれくらい非健常者の方がいるか分かりませんが、日本でも数百万人いるはずで、そういった方々の中にも IT を使っている方が相当いるはずなので、そういった調査も含めてしっかりとした対応をする必要があるだろうと思う。これは、技術シーズというよりも、ビジョンという観点から必要。

○　今の件について、弊社でも問題意識を持っており、特に 2006 年くらいから高齢化社会に向けてあるべきパソコンの機能については日本に専任担当職員をおいて、世界的に連携をしながら研究をしている。大きく２点ほど取り上げると、１点目は、今は文字を大きくしようとすると画面が全部崩れてしまう技術的な制約がありますが、これを描画の座標の扱いとかを変えることによって、もっと高齢の方が見やすい画面にしても画面が崩れないための仕組みというものを整えようとしているところである。もう１点ですが、セキュリティ技術とアクセシビリティ技術とは非常に相性が悪いという問題がある。音声読み上げソフトというのは画面上の文字列をフックして読み上げることになるので、そこのＡＰＩを提供することは、すなわちマルウェアが何でも出来るような環境を用意すると言うことになる。一方でマルウェアを防ぎながらそういったスクリーンリーダー等のアクセシビリティ技術に対して適切なフックを用意する方法というのが見つかっておりませんので、このまま行くと、ＯＳのセキュリティ技術が向上することによって、ますます、デジタルデバイドが拡大してしまうということが起こりうる。そうならないために、社内でもいろいろ研究は取り組んでいるところですが、大きなトレードオフがあってセキュリティとの繋がりで非常に研究するべき要素が多くあると考えている。

○　情報セキュリティではないですが、一般のセキュリティの話しで問題なのは、振り込め詐欺です。あれも、携帯電話等の普及によって得た匿名性を利用して人を騙すという話しですが、それとマルウェアの話しは全く違うように思っていて、例えば、単一の機能を提供すればするほど、そういう犯罪のリスクにならないようしっかり考慮して、予め想定しておく必要があるのではないかと思います。

○　前にも指摘のあった、ソーシャルな面というのがありますので、技術的なところだけを見ているとなかなか難しいというお話しもあります。

○　他のところで議論をしていて困っていることに、「永遠のビギナー」というか、やる気がそもそも無い人々、特に若者を中心に例えばパソコンに winny を入れて人に迷惑を掛けても、自分は困らないから良いという人々をどうするべきかという課題があります。本人に自覚を持ってもらうことは無理だとしたときに、このようなことを技術的に押さえ込めるかどうか。一方で、技術的に勝手に押さえ込むことは個人の権利を侵害する部分があるとも思う。社会的弱者とは違う話しですが、この課題というのは技術的に対応するという発想自体がちょっと違うのか、そのあたりはどうか。

○　Ｐ１９です。「マルウェアフリーを実現するコンピューティング環境」と書いたのですが、今のパソコンや携帯電話でもスマートフォントなどでは同じだと思うのですが、実際の利用形態と言いますと、メールを、ＷＥＢ等々と使う機能は片手で数え終わる程度しかない。他にもいろいろなアプリケーションやフリーのソフトも使えるので、ＰＣを使うというのが普通だと思う。ただ、実際には永遠のビギナーを含む殆どのユーザーは、あるいは一般企業のサラリーマンも同様かと思いますが、これほどの自由度は必要なく、実際に決められたソフトウェアと決められたネットワークが使えれば問題ないのではないかと思う。「永遠のビギナー」対策としては、このような認証がなされていないプログラムを利用できないコンピューティング環境が良いと思っていまして、この環境を作ることによって、ソーシャルハッキング手法やマルウェアが動作できないような環境も実現できるのでは無いかと考えています。実現は簡単ではないと思うのですが、例えばＴＰM相当の技術を応用して、正規のソフトウェアを認証する機関を設置することなどが必要になってくると思います。これは、単に技術の問題ではなく、体制や制度も必要になるということですが、これを解くための課題とは、バッファーオーバーフローでデータがプログラムに化けることや脆弱性の問題については一過性のものだと思っていますが、こうした一過性のものがソフトウェアの認証機構を破綻させてしまうので、そういった脆弱性への対処を世の中どのようなスキームで対処して行くかということが、開発のプロセスで、脆弱性の発見、パッチマネージメントの戦略等の課題として出てくるのではないかと思います。

一方で、セキュリティの対策をすると常に出てくるのが、利便性が損なわれてしまうという問題で、そのバランスをどう取るかという点も、技術と裏腹な課題として出てくると思う。

○　サイバークリーンセンターというボット対策という事業があるが、ボットは感染したパソコンには殆ど影響を与えないが、第３者に対して迷惑を掛けるような影響があるので、「あなたのパソコンに入っているボットのプログラムを除去してください」という、駆除プログラムを配布している。この、駆除プログラムを実際にダウンロードして駆除している方々は、全体の感染者の３０％位で残りの７０％人たちは駆除しない。それは人ごとだから駆除しないのか、それとも別の理由なのか実は分からない状況なので、その心理分析をしようとしています。ただ、そのモチベーションを如何に高めるかという、これは技術的な対応ではなく、むしろ心理学ですとか行動科学に関係する部分ですが、技術と社会科学の両方合わせたようなアプローチをやってゆかないと、「永遠のビギナー」や意図的にこれをやらない人たち、これはＰ２Ｐもそうですが、モラルハザードを生じる人たちに対する対策というものは進まないかもしれない。よって、従来の対策と合わせ技でやってゆくのが良いのではないかと思い、そういう研究もトライをし始めている。

○　人間というのは一度自由度を得てしまうと、それを制限されることには非常に抵抗がある。今の winny などもそうだが、会社の中でもはセキュリティの強化が課題となっていて次々に禁止事項が設定されてゆくと、現場からかなり抵抗が出てくるが、最終的には自由と責任のバランスが落としどころだと思っている。あまり、責任を持ちたくない人には、限られたことしか出来ない環境を使うように、逆に、それ以上に自由度を得たいと思う人は、得る自由度の分だけ責任を負うという、そういうカルチャーを作ってゆく必要があると思う。

○　実は、技術的にはマルウェアフリーの環境は作れなくもない。実際、サーバー等の止まらないことが強く求められる世界では品質管理が非常に重要となっているので、ドライバーの認定のようなことはかなり進んでいて、本当に止まってはいけないところでは、ラベルの付いたドライバーだけを使ってもらうように電子署名を振るという仕組みが用意されている。また、特定のＯＳでは署名の付いていないドライバーは原則インストールできない仕組みにしていて、一部のディベロッパーからは、かなり困っているという話しも聞いているがトレードオフではないかと思う。パソコンにインストールされているソフトの本数は、１０年くらい前であれば、およそ７～８本であったが、最近は３～４本くらいまで減っているという話もあって、ワープロ、表計算、ブラウザ、その程度あれば事足りるという人が増えているのかなと思います。実際に

認証されたプログラムしか動かないという環境で一番身近なものは、アップル社が作っている携帯電話の iPhone に搭載されている音楽ソフトである iTunes で、アップルストアで買った音楽ファイルしか再生出来ない。これが、イメージに一番近いのではないかと思います。しかし、彼らもソフトウェアの検定認証作業を非常に手間取っているようで、そういった、どのプログラムを安全であると認定するのかというところについては、この WG で議論されているようなソースコードの検査技術ですとか、品質管理技術などが全般的に応用できるのではないかと思う。

○　永遠のビギナーの話は、自動車にたとえていうと、現在ではマニュアル車は１割に満たず殆どがオートマ車になっていて、大抵の人はアクセルを踏んでハンドルを回せば車は思うように走れる状況になっている。一方、コンピューターというのは、使用者がしなければならないことが非常に多く、その割にはソフトのインストールは自由に出来るものの、ネット上に漏れだした個人情報を消す手段は無いというように、思い通りに出来るところと､出来ないところの違和感は非常に大きい｡そういう意味で、先行している産業と比べてこの IT という産業自体が、まだ成熟していない、個人的には家内制手工業状態であって、大きな転換が必要だと考えている。

○　２点補足があり、基本的に、これは技術よりもコンセンサスの問題だと思う。最近のＯＳではパッチがあれば自動的に当たるのが標準となったが、これは、以前であればユーザーに無断でコンピューターが勝手に自分を書き換えることに否定的な意見が支配的だったのが、ブラスターの様な大規模インシデントがあって常識の方が変わったという事例です。今の漏れだしたファイルを消すことが出来ないという話しも、技術的には消すことが可能でして、例としては特定のマルウェアを２０万件ほど削除した実績があります。ただ、これは一歩間違えますと、それこそ、ＯＳベンダーの気に入らないファイルを全部消すことが出来ると言うことになってしまいますので、厳しくマルウェアの基準を決めて、特に社会的影響の大きい物だけ update のタイミングで消すようにしております。今後児童ポルノの流通をどうするかなど、いろいろな議論があるかと思いますが、どちらかというと社会的な合意形成がどうなってゆくかという問題の方が大きいと思います。恐らくコンマ何パーセントのアンコントローラブルなコンピューターは残るとしても、９割以上のコンピューターからあるファイルを削除することは既にインフラ的には可能な環境ができていると思います。

○　バイオメトリクスの件ですが、日本は一番高齢化が進んでいる。この状況を奇禍と

して、高齢者なり社会的弱者の認証技術、評価技術といったものを日本が先に備えることで、世界の他の国に対してアドバンテージを得る、そういう視点というのは戦略的に重要なのではないかと思う。ちなみに韓国では９年間の大プロジェクトにより、リサーチセンターとテストセンターの２つ作り、これは、日本でいえば 21 世紀 COE(Center Of Excellence)プログラムのような形でやっているのですが、そして、彼らが引っ張っているアジアのバイオメトリクスのフォーラム、コミュニティが出来ている。そこでは日本は出遅れた状態となっているが、日本は先に社会の高齢化が進んでいるので何か日本は貢献できるのではないか、また、して欲しいという暗黙のプレッシャーもある。そういう観点で一緒に考慮して、こういう分野を育ててゆくべきではないかと思う。

○　次の項目に移ります。開発支援、環境の標準化という観点で山田委員、松並委員、加藤委員コメントをお願いします。

○　NISC でも設計なり、製造の段階からセキュアなものを作ろうと、いろいろなプロジェクトが進んでいると思うが、実際に現場レベルで使えるものが無いのが現状だと思う。そこで、経営者の視点を加え現場の開発者の参画も願った上で、実証的な開発環境・手法定着のための技術を開発するべきではないかと考えたもの。

○　ソフトウェアの低価格化が進んでいる。品質劣化は現時点でも問題になっており、品質を技術により解決する必要がある。その一つの方法として形式手法というものがある。形式手法は数学的なアプローチで品質を確保するというソフトウェアの設計方法だが、今のところ、非常にコストがかかり、品質も高すぎてします問題がある。費用対効果を意識して、そこまでの品質は必要ないが、今よりも品質を上げたいという様なニーズに応える、コストを意識した形式手法があると良いと思う。

○　システムインテグレーションの話しだが、インターネット上でサービスを提供しようとすると、殆どウェブかメール辺りになるが、現状の技術を使って大規模なものを作ろうとすると相当複雑になってくる。この状況で、昔ながらのマンパワーに頼って仕事をしているのが、いわゆる SI 業界のよくある形ではないかと思う。ただ、そこは自動化とか、それもユーザーの要件からシステムを自動で起こすような、迅速で、オートメーションでシステムを組むということが出来るようにならないかと。そのために、データの部品化や自動化の技術などが必要ではないかと考える。

○　この、ソフトウェア工学的な事の重要性については良く理解しているつもりであるが、国が直面している困難な問題というのを掲げたときに、ソフトウェア工学的なところから始めましょうとなると、なかなか、役所には理解してもらえない。この議論は、個別の課題について議論をした後に、俯瞰図のような大きな絵を描き、その中で、この分野はソフトウェア人材育成も含めて大事であるという形で話しをまとめれば良いかと思う。または、本当にセキュリティの事を頑張らないとダメになって行きますよと言うところを強く言って、そういう議論に集中した方が良いと思う。

○　コメントしますと、私どもは新世代情報セキュリティ研究事業というものをやっておりまして、まさに、今年度、「形式手法によるセキュリティの向上」といったテーマで公募を掛け、既に採択したところです。主要な研究者の方を殆ど集めまして、形式手法、私どもとしては関数型言語もと言っておりますが、そういった基盤的なところからセキュリティを考えようと言う研究会を実施し、その中で人材育成を含めて、現場への応用に関するガイドラインというのを３年計画で作るということを行っております。ここに書かれている内容をほとんど網羅的にやりたいと思っていまして、コストとの兼ね合いという部分と、自然言語と形式記述言語への自動変換、こういった部分も範囲には入れて進めてゆく予定です。

○　形式手法と言うところを大本から言えば、ベリフィケーションといいますか、コレクトネス、ベリフィケーションというようなキーワードはあったかと思います。間違っていないプログラムを目指すという研究であったかと思いますが、最近では、間違っていないということよりも、セキュリティという観点で信頼性が上がるということだろうと思いますから、今、ご紹介頂いたように既に重要なものとなっているわけです。具体的な取り組みが行われていると言うことは非常に重要なことだろうと思います。

○　モデルベリフィケーションの一部に関しては、いま、チェックソフトを無償で提供してそれを実行してもらうことにより、ドライバーを検証するプロセスを取り入れている。関数型言語の話しが先程出ていたが、弊社でも、今年に入って、これまで研究所で持っていた関数型言語のチームを製品チームに移管し、数年以内に普通の法人向けなどで利用される環境で関数型言語も提供する方向になっている。ここ２－３年で

恐らく関数言語のコマーシャルソフトウェアの世界でのプレゼンスというものは、大幅に上がるのではないかと期待している。もう一点、委員からご指摘のあった、IT サービスシステムのオートメーション化は非常に重要なテーマだと思っており、これは、特に、他社が先行している部分だと思っていますが、いわゆるクラウドコンピューティングの技術というのはまさにここだと思われる。自動展開技術や自己復旧の技術によって、一人当たりの管理するサーバーは、弊社等では一人当たり千台近くになっており、例えばこれがメールサービス等では如実にコスト方向に影響を与えていて、今、多くの日本人の電子メール情報が、既にアメリカ国内にあると理解をしている。これが、今後例えば、エンタープライズのシステム等も含めてそうなって行くと、企業の情報も含めて海外に置かれたままの状態になり、日本法の保護の対象ではなくなってしまうということは、セキュリティ上もかなり真剣に考えなければいけない問題だと思う、少なくとも同等以上の運用の生産性を日本でも確保してゆく必要があるのではないかと思う。

○　企業だけではなくて、実は大学でも他の大学と話しをすると、既にそういうものを積極的に使っているところがあり、従来想定されていたような通信の秘密などが何処まで及ぶかということも含めて、関係者は相当議論しているところだと思う。なかなか話は複雑で、いろいろ法律的なところまで絡んで来ているようだ。

○　こういう枠組みを作ったら利用するべき。ただ、利用していることはだれも分からない、マークが付いているわけでもない。そういう、ソフトについては、素人が作ったようなプログラムでも、高度な技能を持つプロが設計したプログラムも、目的とする機能面で動いていれば評価は同じとなってしまう部分もあるので、ここは技術的な事だけではなく、強制的に適用するなどのことが必要だと思う。

○　次の分野、セキュリティ対策の要件、あるいは、リスクの評価可視化というくくりで、４件山田委員が２件、二木委員、三河尻委員コメントをお願いします。

○　資料の方ですが、「社会システムにおけるＩＣセキュリティの影響」ということで、IC カードだけではないのですが、主に IC カード、それも既に社会インフラ化してしまっている中で、なおかつ、昨年から今年に掛けて欧米で様々な問題、例えばオイスターカード（英国ロンドン市内で地下鉄等で用いられる交通用の IC カード）の問題

が起き、セキュリティブリーチ（抜け穴）の情報を公開するか否かという問題が起きた。そのような状況下において、IC カードのセキュリティが社会のシステム、社会インフラ化に対してどういう影響を及ぼしうるのか、連携している様々なサービスとの関係も評価をしなければならないのではないかと感じているところ。予測を実現するために必要とされる技術や課題は、資料に書いてあるとおりですが、統計や社会心理、行動科学といった、そういった技術なり知見なりを総動員しなくてはならない。⑥番にあるとおり、実際にブリーチが発生した場合に、どういう風に危機管理をするのかというマネージメント的な観点も整理する必要がある。また、備考にも書いたが欧米の地下鉄の例だと、司法当局がその情報が公表されることに対して差し止めをしたのだが、差し止めをしたところで実際にその情報は漏れていたわけで、仮にそれが日本で起きた場合にどうなるか、例えば政府は認知したが社会はまだ知らない状態のときに、同じように司法当局、あるいは政府自身がそういった差し止めをするのか。あるいは、その仕事をしている間に、国民が知ってしまった場合に、不安をかき立てられるとか、知っていたのに何もしなかったと批判をされる可能性もあるので、そういった情報の取り扱いの仕方も含めて、研究なり対策を講じてゆく作りをやってゆく必要があるだろうということです。

次の件ですが、「IT システムおけるプライバシー保護技術」です。先程委員の発言にもありましたが、企業の情報や個人情報が国境を越えて集約、収集されて分析されているという状況があり、その際にセキュリティの関係で言うと、プライバシーの暴露の技術を研究することによって、どうやって保護するのかを考える、その観点は情報セキュリティの世界においては、これから、ますます、重要になって来ると思います。

○　昨今、どこの会社でも BCP（業務継続計画）が流行になって、その検討の中で私もセキュリティの切り口から参加することがあるのですが、リスクといったときには、企業の中では他のリスクであったり、災害対策であったりいろいろな切り口がある。市場が変化をする中で経営層は即応して行かなくてはならないが、いろんなリスクを統一的な形で、システムの立場で言えば全部可視化出来るようなマネージメントが何か必要になってくるのではないかと思う。ともすれば、セキュリティの面からだけリスクを語りがちですが、経営層から言えば他にも、例えばお金に関するリスクは会社にとってある意味で致命的なものでありますから、そういう他の要素と上手く同じ土俵の上に載せて語れるような形にして行くことも重要。そういう観点から資料を書いた。お金の面については、いろいろな技法・手法が実際に用いられているし、確立されているように思う。セキュリティのリスクをどう、数値化して行くかを考えたときには、お金に換算するというのが一番安直かもしれないが、それ以外にどんなことが

あるのか、ということも真剣に考えて行かなくてはならない。

○　前回、情報セキュリティ対策について、個別の対策という、いわば分子はあるが、俯瞰的なマップという分母に当たるものがないという話しをしたが、その延長でまとめたもの。国内は悩みの連鎖とも言うべき状況で、そもそも情報セキュリティのガイドラインは私が知る限りでも５０種類以上ありバラバラである。実際には、次々に脅威が現れて、その都度対策を検討してきた経緯も考えると仕方がない状況でもあるが、それゆえ、なかなか分かり易い一覧性のものが出来なかった。それぞれの基準やガイドラインを作っている立場の方も必要性や思い入れがあり、自分たちの基準を守りたいという想いと、一方で統一したいという想いがあると聞いている。どうやって調整するかはなかなか難しい世界である。SSP、SIer、ベンダーなども都度局面毎に顧客に対応して行く中で一覧を持っているが、それぞれローカルなものとなっていて共通になっていない。私たちも、顧客にうまく提案し切れていないという悩みがある。顧客の方はどうかというと、トップはどこまでやれば良いかという投資判断の基準について悩んでおり、セキュリティの推進をしているセクションの方は複数の基準に非常に疲弊しており、かつ、推進部門が複数あることから、その調整に多くの労力を割き監査疲れが出ている。そして、運用部門の方は当然投入するリソース、投資が回っておらず、いつでも人、リソースが足りないということになっており、皆、悩みの連鎖に陥っている状況。今、現場では組織の疲弊と対策の形骸化が既に起こっていると考えている。その結果リスクが増大しているということが危機感の元であり、これを解決しようと考えたのが、「統一フレームワークによるセキュリティの推進」というアイデアである。

これは、ＤＢＳＣ（データベース・セキュリティ・コンソーシアム）において、「データベースセキュリティガイドライン」

(http://www.db-security.org/report/dbsc_guideline01_ver1.0.pdf)

としてゼロから半年くらいで作り上げたもの。分かり易いということで非常に評判が良いが、要は脅威を一覧として書き、何者が、どこから、何をして、どこに来るのかを整理して、それに対するセキュリティ対策等を箇条書きでザッと書いていったもの。そして、今は第２版を作っているが、データベースは他の基準とどう絡むのかということを分析していると、実は虫食い状態になっていることがわかった。一覧表を作ることによって、特に良く記載されている部分と記載されていない部分が分析できるようになった。我々はセキュリティ対策を語るわけだが、そもそも、何を恐れるが故にそれが必要かという分かり易い説明をなかなかし切れていない状況がある。アカウントを例として上げれば、「なりすましなどのアカウントの不正利用を防ぐため」という理由を入れたように、全てのアイテムに「.....」するためという理由をとにかく入れ

た。それで、対策が必要な理由が分かり易くなった。

ガイドラインを最初から検討するときに、例えば、あまり細かいところに落ちすぎていないか、構成上についても粒度を揃えるなどのポイントを考慮して作れば、一覧性のあるものは作れるということが実体験として分かった。そして、こういう一覧が出来ることで何が起こるかというと、もし、今これをＮＩＳＣの基準として公開する形となれば、いろいろな団体がこれを意識するでしょう。これは、もちろん、データベースだけではなく、他のネットワークやパソコンというレイヤーのものも同様に一覧にまとめてゆくと、結局それが一覧との関連性ということを、それぞれのガイドラインの外付けでまとめることが出来る。いきなり全部の基準を書き直すことは難しいと思うので、ガイドラインの後ろに付録として付けて、ガイドラインは俯瞰図の一覧の何番に該当すると位置づけて、それの逆引きが出来ればと思う。また、それぞれの団体における固有の要素は、what,why,how のところまで書き下す、そうすると、SSP とか SIer なども、それを顧客毎の状況に合った（対策の過不足等リスク分析など）具体的な実装方法というところの提案をしてゆくことによって、全体のフレームとそれぞれの基準を顧客に開示することによって、今、自分たちが対策の中のどこが出来ているのかを定量的に見ることが出来るようになると思う。いままでバラバラだったガイドラインの紐付けが出来ると、これにより全体が一気通貫で分かり易くなるのでないかということで、このアイデアを持ってきた次第である。

因みに、資料の予測内容の最後に書いたが、このフレームワークにより今から新しいテーマや新しい試みを分析できるようになる。有効なテクノロジーというのは沢山の脅威を解決できるものだと思う。今までは複数の対策が必要だったが、それが一個のデバイスで出来るようになると、効果、効率を含めて両方定量的に議論するような物差しになりうるのではないかと考えている。そういう意味でも、新しい脅威が出るたびに対策は増えて行くので、一度棚卸しというか定期的に見直してゆくことで、良いものになって行くのではないかと思う。

○　１点目は、委員の方から出された IC カード関係の話し。先日も NHK で ETC のキセルの話しをやっていたが、基本的には、やる方も守る方も費用対効果だと思う。この点は、恐らくクレジットカード会社が一番ノウハウを持っているのではないかなと思う。完全にパーフェクトなものを作ってゆくとよりも、それが統計学的にどうかということ。先のほどのキセルの話しも、恐らく、国民全員がキセルをするわけではないので、そのあたりを読んで考える必要がある。

２点目は、一見守られている単品の情報を集約して分かるようになるものについて。保護対象というのは、単品の個人情報だけではなくて、個別には守られている情報でも、集めて統合すると判明してしまうものもある。これについて今後どうしてゆくか。

この点についての対策は、日本は非常に遅れていると思う。

３点目は、二木委員の意見に対して。逆説的なのですが日本があまりリスク対策をしないのは、実は、それが本当のリスク管理ではないかと思う。先程、１０年１５年前は、研究開発も出ていないという話しだったが、その前は実は出ていたのではないか。最近の新しい仕組みに我々が適応できていないのではないかと思う。コンプライアンスであるとか、いわゆる欧米的な管理手法や分析手法などのリスク分析というのも、いわゆる欧米的なリスク分析であって、例えば、セキュリティ対策を今やることが経営上において良いかどうかは分からない。いざとなれば謝ってしまった方が早いかもしれない。極端な例え話だが、そのために非常に謝るのが上手な人を雇っておく方がリスク管理となるかもしれない。そこは、形式的な事だけで捉えてはいけないと思う。

最後の三河尻委員の意見について、政府の方で統一基準を作っていると思うが、それは政府の中でやっている部分で、これを如何に民間にも落としてゆくのかということだと思う。最近クレジットカード業界関係の方で、PCI DSS(Payment Card Industry Data Security Standard)という、いわゆるデータを保護するという観点で考えているものがあるが、非常にシンプルにやるべきことというのは纏まっている。そういう面でも先程の三河尻委員の言った、守る対象を具体的にしてゆくことはアプローチとして非常に有効だと思う。

○　指摘されているプライバシー保護技術の点ですが、まず、利用者のプライバシーという観点では、欧州では例えばイーコマース・ディレクティブなどで、いろいろ決まっている部分があるのですが、相当する制度というものが日本ではなくて、今後、どこをハーモナイズするのか、逆に、日本独自でやってゆくところはどこなのかという議論をしてゆかなくてはならないと思う。資料にグーグルストリートビューの話しが出ているが、被写体のプライバシーというのは、全く新しい問題として出てきて、これは例えば普通のデジカメにも GPS が載ってタグが付いてきたときに、ネット上の写真共有サービスには、正確な撮影時刻と位置が入る事になる、しかも、今は顔認識の技術が非常に進んでいますから、ネット上の写真を共有するサイトなどにアップされたあらゆる写真を顔で検索して、数年後イメージ検索をすると、特定の人を何時どこで何をしていたか、みんなが見られるということが現実的になってきている。監視カメラも自分でデータを持つよりは何処かにアウトソースして、問題が起こったときにはデータの補完だけでなく解決までアウトソースした方がきっと楽だろう。あるいは、車のバンパーに付いているカメラの映像というのを保存しておけば、交通事故の時にもっと周囲の車から見た映像によって、正確な判定が出来るというような議論が出てくるかもしれない。被写体のプライバシーというのは、今後１０年でどういう事

が可能になるかというところまで踏み込んで、制度上で検討が必要な点について議論が出来ると良いのではないかと思う。多分法律を守りながらビジネスをしたい人たちにとっても、何を守らなくてはならないか整理されていない段階にあると思います。

○　ストリートビューの話しが出たので便乗しますが、実は、20P のところに、情報のポータビリティーとかリロケータビリティのことを書いたのですが、裏側には、その情報の所有者が誰でオペレーションがどういう形で行われるのかということがあります。先ほど実際に被写体のというお話しがありましたが、本当にその部分というのは何の整理も出来ていないですし、制度もないし技術もないという状況になっているのではないかと思う。ただ、これを DRM の話しと絡めてしまうと整理がつかなくなるので新しいフレームが必要なのかと思う。

○　統一フレームワークの話しですが、これは、ちょっとアメリカとかのコンファレンスに行っても結構大きなテーマになっている部分がありました。いろいろなセキュリティに関するガイドラインが出ていまして、それぞれを満たしていることをどうやって確認しようかと言うことが大きなテーマになっている。例えば、ある人たちは IT を含んだ一番大きなフレームワークをベースにして、そこにマッピングしてみようとか、逆に、それぞれセキュリティ的に足りないものがあるから、一旦全部足してみて、それで、総和の表を作ってそこから逆マッピングしてやろうとか、いろんな事をしているようだ。結局、各基準が独立して生き残っている以上、最終的にそこに戻してやることが必要になるので、同じマップを作ったとしても要素が欠けてはいけないのでなかいかという気がする。例えば、会社の情報セキュリティ部門でそういった個々の基準をチェックすることを考えると、同じやり方が必要になると思う。

○　時間も無くなってきたようです。プロジェクト管理に関する部分については、時間は不足気味ではありましたが、いろいろご意見をいただきましたので、さらに、事務局の方で、洗練した形で、まとめてゆくという方向にします。

また、将来予測については、全ての項目を議論できませんでした。次回の会合でさらに議論頂きたいと思います。また、本日議論を踏まえて各委員さらにご意見がある場合や各員が発言を控えられたり、短めに切り上げられたりした部分については書面で意見を頂ければ、次回に紹介あるいは、整理してゆく段階で事務局の方で参考とさせて頂くということで、活用させて頂きます。詳しくは事務局の方からメールでご案内を差し上げます。

以上