資料２

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９回会合議事要旨

１．日時　平成２０年3月２１日（金）１６：００～１８：３０

２．場所　内閣府別館９階大会議室

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］
志方 俊之 委員（帝京大学教授）
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（科学技術政策担当）付参事官
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

○　ポートフォリオとして評価しろと言われても、この荒さの段階だと、今日どうこうしろと言う話ではない。これからのまとめ方の話として、研究開発・技術開発のタイトルと内容が乖離しているケースが多々あるので、出来ればもう一段ブレイクダウンした形で、実際に何が開発されたのか、例えば、アウトプットが論文で出たとすれば、分類用のキーワードがあると思うので、そのレベルで補足して行く必要がある。

○ この資料は、例えば、プライバシー保護についての研究数は昨年度同様少ない状況であるとか、こういったことは少なくとも言えると。ただ、この資料は正しいけれども、その先踏み込んではいないので、各委員も議論は難しいだろう。

○　全体の話だが、これは一つのナレッジマネージメントの仕組みのようなも

のだろう。ただ、このレベルでは資料を集めた程度のものでしかないので、なかなか議論はしづらい。積極的な調査を対象に打つか、このように様々な公表資料の中から吸い上げるという形にするのかいろいろ方法はあるが、実際にデータベースとして、各テーマについて具体的に何が成果として上がっているのかというところまで、定常的に集められるような仕組みを作ると言うことも必要なのではないか。

○　脅威が分かれば問題は半分解決したようなものなので、今日の状況についての把握や認識というものは、グランドチャレンジにはそぐわない話である。全く考えてもいなかったようなことが脅威になるからこそ、グランドチャレンジをする必要性がある。全体を俯瞰しようとしても、表立って行っていない研究開発・技術開発を充分把握できる筈はない。また、把握した研究も表題と実際に行っている研究内容とは必ずしも一致しているとは限らず、かなりの人数を掛けて精査しないと正確な俯瞰や実施状況の把握は困難。ここでは公募型の研究は出てこないが、公募型の研究も意外なものがあるので把握する必要がある。

○　グランドチャレンジ WG の検討結果で気になったが、「脅威はそれほど大きくないとする立場」というのは、どういうことか。このようなことは、かなりの情報を集めていて、かつ、それを評価するやり方なり評価できる立場にないと言えないと思うが。

○　WG では、予め方向を決めて掛かった訳ではなく網羅的に検討したので、この立場が出てきた。例えばサイバークリーンセンター等の活動を通して、日本国内からのスパムの発信、あるいは、ボット感染の台数というのは把握している限り下がってきているという話がある。もし、そうなのであればグランドチャレンジではなく、そういった個々の活動に力を入れれば良いのではないかと考える立場である。

○　ネットワーク社会で脅威があるかどうかは、何かに挑戦している、あるいは何かを実現しようとする強固な意志がなくては出てこない。例えば、ネットワークを使って何か競争力のある新しいサービスを開拓しようとするなど、強固な意志があった時に初めて、脅威を潰すために開発したい技術とか、いろいろなものに挑戦する意欲が湧く。このように、アクティブな積極性を中心的な戦略として打ち出すところに初めて、セキュリティに関する研究投資だとか、グランドチャレンジが出てくるのではないか。そういう意志がない受け身の対応を考えるのであれば、今ある状態を何とか保護しようと適当な防護システムを買ってお茶を濁すというのが大体のところになるし、そもそも、こういった研究開発テーマはそれほど考えなくても良いのではないか。

○　脅威を見る場合には、相手に意志がある場合と地震のように相手に意志がない場合とでは、同じ BCP（業務継続計画）でも違ってくる。特に IT セキュ

リティの問題は両方取り組む必要がある。
　ポートフォリオは、短期的なものと中長期的なものとで異なるはず。短期的な課題に対しては企業、官庁にも問題意識があり自主的な取組も期待できるが、中長期的なものについては、国がしっかりとしたインセンティブを与えて、すこし大らかにやってゆかなくては、誰も取り組まないだろう。

○　脅威というものはいろいろあるし、これからも、どんどん新しいものが出てくるのだろうと思う。統計だけ見れば、アメリカにおけるセキュリティ被害額というものは２００１年がピークとなって以降だんだん下がっているが、それは意識が高く、しっかりした団体ほど回答に応じるというような調査統計上の問題もあると思われるため、本当に全体を代表したものとは言い切れない。
　おそらく統計の対象となっていない一般の家庭や、ゲームや、携帯の状況を考えると決して脅威は減っておらず、これから増えゆくと思う。だから、グランドチャレンジ型の研究が不要である話は違う。

○　セキュリティに関する課題は目的ＦＩＸ型で実行しやすいかというと、これは難しい。セキュリティの問題というのはいろんな形で外部環境が変化し、特に攻撃する側が高度化してゆく中で取り組む必要がある。だから、現実的にはゼロに出来ず常にリスクはある。

○　この問題はバイオテロ等との対抗策とも近いと思う。今は守る側として議論をしているが、脅威になる側、悪意を持った人間の視点から考えると、どのようなことが仕掛けられるか。それを想定した後に対抗策を考えるというのが一つのやり方ではないか。

○　当委員会が以前提示した重点的研究開発項目に取り上げられたテーマにおいては、重要性がさらに認識されて現実にいろんな動きが出てきている分野もある。例えば、心理学的なアプローチや社会的なアプローチが必要だとして、情報処理学会の中にセキュリティ心理学とトラスト研究グループが出来た。私はセキュリティを超えてIT リスク学のようなものが必要になってくると思うが、これはセキュリティ・マネジメント学会の中で研究会を立ち上げてやってゆくことになっている。IT リスクマネージメントとアセスメントとコミュニケーション３つを統合的に扱ってゆく必要があり、リスクの問題に対する一般の人たちのリレラシーのようなものが次にくると思う。それはどう教育してゆくのか、うまく行かなかった場合の危機管理をどうするのか、そういったことはIT の分野でも重要になってくるだろう。従来よりも広い分野での研究を始めているが、そういう意味では研究テーマの項目として出していたようなものが、少しずつ動き始めているといえる。ただ、それとグランドチャレンジは同じ物ではないだろうが。

○　攻める方の立場として技術開発をしないといけない。ただ、日本では攻撃する側立場からのアプローチ、表立って攻める方法を議論するということは抑

制される方向にある。もし、この委員会がグランドチャレンジへの方向付けとして、攻める方と守る方のバランスを取るべきと表明することは重要なのではないか。確かに守る立場から言えば、一度相手が何をやってくるだろうかと想像してからの対処となり一段間接的な対応となるので、何が何でも攻めようとするものに対応する技術というのは出来にくいのではないか。

○　IT セキュリティの初期に、ペンタゴンで攻撃側のチームと防御側のチームを作り、２万くらいのセキュリティホール全部に攻撃を仕掛けるという試みがあった。そのときにどれだけ侵入に成功して、どれだけが妨害できて、どれだけが検知されたかということが明らかとなったが、その時の攻撃側のスタッフは、ほとんど監獄の中から採ってきたと言われるくらいの人たちで、悪意というかイーブルなセンスがあった。われわれは自然とか科学の発達による偶発的な脅威に対するＢＣＰと、増幅した悪意に対するＢＣＰと両方やらないといけない。これをしないと負けると思う。そして、対象のレンジが広ければ、かなり国がインセンティブを与えないと、民間ベースでは動かない。

○　ポートフォリオについてみると、金額ベースはともかく、例えば暗号や機器セキュリティに付いては、かなり急激にテーマの数というのが縮小してきている。これを見ても、いろいろな意味でグランドチャレンジ的なドライビングフォースが必要だと思う。例えばサイバークリーンセンターの話もあるし、アメリカのリスク分析会社の報告でアンチウィルスの戦いは守る側が勝ったというような報告もある、そんなことで、目の前の脅威は押さえられるような気がしてきたが、私は、これは危ないと感じている。

○　脅威は上位層に移って行っている傾向が一般的にはあると思う。単純にデータを壊すという時代から、情報を盗み出す様な時代、そして、それを旨く使って騙すという時代となってきている。これからますます、いわゆるハッカーといわれる人たちと、犯罪者とのコラボレーションというのが強まってゆくだろうし、より、巧妙になってゆくのだろうと思う。
　グランドチャレンジは別として、脅威そのものは大きくなっているという立場で考えてゆくべきだろうというのが、この委員会での一つの大きな方向だと思う。

○　WG で具体的に出されたグランドチャレンジのテーマは、レベル感というか粒度が全然そろっていない。非常に細かい技術開発項目が載っているかと思えば、何かが「ゼロ」とか非常に漠然としたような目標まである。この委員会の考え方として、どのくらいの粒度のものを期待しているかを議論しておかなければならないと思う。それを検討ＷＧの方にインプットしないと、いつまで経っても粒度がそろわない議論が続くことになる。例えば、ウィルスに感染した PC を 10 年後はゼロにするとか、感染しても５分で直るとか。あまり細かい技術開発項目を並べてもいけないが、そこに至るまでの間で、粒度を指示しなくてはならない。

○　粒度について目標 FIX 型ということでは、被害ゼロという例えは分かり易い。しかし、セキュリティというリスク問題の特徴からいうと、ゼロリスクというのはあり得ない。形容矛盾になり、かつ、実施にあたっては、いつまで経っても安心できないということになる。省エネなどはこの考えでやってゆけると思うが。私としては従来議論されていなかったような部分を旨く切り出して、また、目標の設定を長く作り、それをベースにしてさらに掘り下げてゆくというようなことができると良いと感じるが。

○　電子政府評価委員会の議論を踏まえると、電子政府というのは国の戦略だと思う。政府を電子化するということを徹底的に実行するとなれば、脅威やいろいろな問題を全部洗い出して、完全に安全で電子化した政府を実現するという目標があると思う。
　まつわるテーマというのは、おそらく猛烈にある。全体として完全に安全で、プライバシーも保護した上で、電子申請を基本とするような電子政府を実現しようとしたら、相当な労力といろいろな知恵で問題を洗い出して実際の最適を作らなければならない。そういうＩＴ側の責務もあると思う。これは本当にエネルギーが必要な話であるが、この安全性がある政府機能を作れたら、世界の中で競争力のある国造であるのかなと思う。

○　確かに、何かを実行するということをベースにして、それの補完としてのセキュリティあるいはディペンダビリティーを含めた広い概念を検討してゆくというのは、グランドチャレンジ型に向いているかもしれない。グランドチャレンジ型で考える場合は、先程話があったように現在の脅威ではなくて、将来の脅威を見据えてスタートすべきというアプローチが一つと、もう一つはテーマとして電子政府が良いのかどうかは別として、何か国にとって、国民にとって必要なものを大きく展開する際における、セキュリティ上の問題を洗い出してゆくアプローチ、これもあると思う。とりあえず、この２つをベースにブレイクダウンしてゆく考え方はあると思う。

○　先程他の委員の話で、攻撃型に興味があるとうお話しがあったが、私が言った攻撃というのは、例えば電子政府を実現するということが攻撃型だということであって、破壊するという意味の攻撃ではない。ただ、同じ言葉を使って、破壊するという意味の話をすると、最もセキュリティの高い電子政府を作ると宣言すると、攻撃側の人間は、いかに日本政府が安全なものを開発していると言っても、どこかにセキュリティホールがあるだろうと絶えず見張っているだろう。私が言ったのは、それを防ぐことが攻撃である。電子政府を作るということは一種のアグレッシブな設定であり、攻撃したい人間がどちら側に属していようと、どこかで相まみえることになる。

○　一つの動きとして私が心配しているのは、電子政府の中で暗号の危殆化の問題が出てきていること。それに対応しての動きが遅いのではないか。グラン

ドチャレンジとは別に大きな課題だと思う。既に存在するデジタル署名付きの文書の暗号が危殆化するということが分かった時にどうするのか、これは、今から取り組んでおかないと大変なことになるだろう。将来に対応した新しい暗号に換えるにしても、例えば、何千万枚も発行されて出回っている IC カードの暗号が危ないとなったときに、これを一度に速やかに新しい暗号に更新するのは簡単ではない。また、換えるという行為にともなって発生する、新たな脆弱性の作り込みという問題がある。しかも、運用はずっと続けなくてはならない。また、製品というのは日本の中だけで作っている話でもない。こういう問題を考え整理をして、やるべき事を明確にしてゆくことは非常に重要なことだと思うし、ＮＩＳＣの方で取り組んでもらわなければならないテーマだろうと思う。

○　電子政府の取組が着実に進んでいれば、それに追従して将来に渡って安全安心にするような、ミニマムリスクで運用してゆくための方法などに取り組んでも良いのかもしれないが、今の状況だと電子政府の方が倒れるとセキュリティの方も倒れる危険がある。
　暗号の危殆化は来月の政策会議で決定をするが、今の仕組みの中で政府が実現出来ることとなるので、政府全体で合意したやり方にならざるを得なかったが、一応今回の問題はクリアできる。ただ、これから先にどんなことが出てくるか。今は GPKI だけにしか議論していないので、あとは普通の PKI とか、JPKI とかどういう風にパーンしてゆくのか、リサイニングはどうするのかいう話はこれからずっと話して行かなくてはならない。

○　暗号の危殆化に関しては、ガイドラインのパブリックコメントが丁度終わり、４月の末の政策会議で決定する予定です。アメリカの様にデットエンド型ではなく、つまり、期限を定めてそれまでに全部換えるというのではなく、一応２０１２年までに平行運用して、その後、もし、危なくなればすぐにクライシスマネージメントというか、いろいろな対応を打つということを担保しながら、平行運用し、次第に換えてゆくというような方向で案を考えている。それとは別に、もちろん強い暗号を造る、バグのないというような別の面での研究開発も必要かもしれないが、現在のところはこのような形になっています。

○　今回決めるガイドラインは、インフラストラクチャーの中に組み込まれ、広く使われている暗号が危殆化して、それを取り換えなくてはならない最初の経験となる。この後、政府だけでなく民間の認証局、個人の PC の中には証明書の更新などもあり、これらをどういう風にリボルブしてゆくか考えてゆかなければならない。今回の対応が第１回目だが、これからプロセスも改善して行かなくてはならないし、2012 年までの間にシュミレーションなどを行わなければならない。そのための技術開発や予算のあり方を考える必要がある。

○　電子政府だけでは済まない世界分野もある、民間の方の話はどうするのかとかという話もよろしく。

○　IT 社会を造ることによって、日本の安全な社会、世界の中でも競争力のある社会にする、そういうことを全部含めて IT 化を選んで、IT 社会を造るために先導的な役割として電子政府を造るんだと宣言したものと私は思っており、社会のいろんな仕組みが IT 社会あるいは、２１世紀にフィットしたもので造られること、そのデザインを社会システムデザインと私は呼びますが、その社会システムデザインをやるという意志がないと電子政府も出来ない。
○　イーガバメントにおいて政府という印象は、電子政府の窓口のところで決まる。その辺がどうデザインされるかというところが一番大事で、国民が自由に、いろいろな情報を得られ申請ができるという話になれば、かなりセキュリティの脅威が出ると思う。また、IC カードが全て安全だと言うわけでもない。そのあたりのレジストレーションを誰がどうやるかということもある。

○　「電子私書箱」という概念がずいぶん言われているが、聞くところによると、その主体となるのは、ある基準を満たす民間団体となるとのこと。結構なお話しなのかもしれないが、扱う内容はプライベートな情報の塊ですから、それはどうやって守るのか、各企業に任せるという話ではないと思うが、標準的な基準というのはどうするのか。利活用のアイデアはどんどん進んでいるのかもしれませんが、網羅的に電子政府を一つの核とするような IT 社会のデザインを社会デザインと呼ぶとしたら、それとぴったり裏腹な関係で情報セキュリティ戦略が打たれないと、どうにもならないというのが私の考え。

○　情報セキュリティを、何時までにこのレベルまで実現しますと早めにアピールすることによって、電子政府システム、情報家電システム、製品の強化、日本の国の活性化に繋がってゆくとか、そういうアプローチが必要なのではないかという気がする。セキュリティというのは難しいが、尺度と基準のような議論を固めておいて、セキュリティとアプリケーションをリンクしてその活性化などを考えてゆくのも、グランドチャレンジになりうる。そこをやらないと、セキュリティの話は受け身になる。今の事もグランドチャレンジの３つ目の候補として御議論頂ければと思う。何かの他の製品なりシステムなりを実現するために必要なセキュリティ機能を先に決めて、それを実現してゆくプロジェクト的なものがあっても良い。

○　先程時間軸の議論があって、今、社会システムデザインという話があった。本日の資料や話しでは全体像が見えにくいと思う。電子政府の話、情報家電の話、組織的な対応の話、このようなものを一枚の絵に出来ないか。それぞれの具体的なイメージとしては、私たちが６０年代、７０年代に未来の世界って、エアカーがあったり、リニアがあったりして、それぞれの場面でどういう風なセキュリティ技術が必要なのかっていうことをそこから深堀してゆく。今は、非常にロジカルに技術的対応についてはこれ、社会的対応についてはこれと、一対一対応でブレイクダウンしているが、実際にセキュリティが働く場面は様々なところがあり、例えば情報家電だったら、携帯電話だったらと絵が描けるのではないか。実際企業のなかでは、開発としては何をやってゆくか、電子

基盤はどう造っていったらいいかというところが、まず見える。その絵に対して全体の中でグランドチャレンジの目標たるところはどこかとう議論が別の視点からできるのではないか。これは文字で書いてということと、多分違うのではないか。その違うモデル、違うターゲットについて語っているところを、一端全体像を描いてみるという作業も必要なのではないか。

　方法は、いろいろなやり方があると思う。一つは最終的な利活用の場面を出して、その裏にある技術というのはどういう形にするかという話も出来るし、逆に開発の場面、研究の場面の方をメインにして、じゃあ、どういうところが必要かをみることもできる。ただ、私が最初に抱いたのは利活用の場面から逆にサーチしてゆくというようなイメージ。

○　あるべき世界を描いて、そこから逆算してゆくというという話だと思うが、検討ＷＧでそういう議論をしなかった訳ではない。未成年や高齢者などの情報弱者向けにいわゆる The internet から隔離され、安全なネット環境を実現する技術もしくは社会的な仕組み、それを The internet ではなくて、A internet という言い方をした人がいた。要するに自由奔放に振る舞って、どんなことでも出来る internet が必要なのは、ごく一部の人だけであり普通の人は例えば電子政府に対応したネットワークがあれば良いのではないかと。電子政府に対応した A internet の安全性を強力に推進し、A internet を使っている人は The internet へは行けませんよということにしてしまえば、それはそれでグランドチャレンジかなという言い方をする人もいました。

○　事務局としては、ビジョナリーゴールとテクニカルコンポーネントも全てグランドチャレンジになりうるという風に考えて資料を作成しているのですか。

○　これは、説明が足りなかったかもしれませんが、テーマの分野、技術的対応、社会的対応、組織的対応、脅威を把握する技術、それぞれに対して、プロジェクトの型が適用できるという意識で作っている。ただ、今までうまく行かなかった事、例えばプロジェクト管理、評価の仕組み、導入するかどうかどうか。今、プロジェクトマネージャーをいろいろなプロジェクトで使っていますが、今ひとつ権限が低かったり、任期が２年で短かったりしてうまく行っていない。それは良くないので、もう少しプロジェクトマネージャーの権限あるいは責任というのを拡大するということを、改善点として入れています。

○　そうすると、グランドチャレンジとそうでないものの違いは、規模の大きさだけというイメージか。

○　規模というか、先程から言っている粒度というか、今までの施策に基づく資源の投入方法は比較的技術開発課題に近いところ、あるいは技術開発そのものを対象としていたわけですが、私の個人的なグランドチャレンジに対するイメージというのは、もう一段高いレベルで、例えば電子政府の例で言うと、電

子政府になったらどういう課題が出てくるのかと、それを解決するための技術的な課題から考えるという、それくらいの粒度。ただ、それをすると、今まで予算と一体化して技術開発課題を出していたので、各研究者が取り組んでいたものが、その裏付けが明確でない状態で、取り組む者が現れるかという問題があり、それとトレードオフの関係にある。私のレベル感としてはそれくらいのところ。

○　少なくとも、グランドチャレンジというのは、広めに考えようということは一致している。私は、ゴールフィックス型をグランドチャレンジというのかと思っていたが、将来出てくる脅威に対するものを、今から取り組んで行くこととか、製品との関係で必要となるセキュリティがどのような者かを明確にした上で、そこから生まれてくる製品をどんどん作ってゆくものなども、グランドチャレンジテーマとして考えてもらえればと思う。

○　先程、個人的な懸念として指摘したが、ポートフォリオに関して、情報セキュリティ関係の研究開発・技術開発は、テーマの件数ベースで急激な減少傾向にあり、早急に 21 年度には盛り返す投資を行う必要があると思う。それにむけてグランドチャレンジ WG のアウトプットを使ってゆきたいと考えている。

以上