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 10 回会合議事要旨

１．日時　平成２０年7月２３日（水）１７：００～１９：００

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）
西尾　章治郎　（大阪大学理事・副学長）
宮川　晋　（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）
（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
（代理出席）
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

○　「資料 3：技術戦略専門委員会の活動方針（案）」に記載されている、短期的取組として 3 つ記載されているが、これは、「最適なセキュリティ水準を達成するソリューションの実現に必要な、技術開発・研究開発テーマについての検討」が一番大事なところを示したものということか。

○　その通りである。「最適なセキュリティ水準を達成するソリューションの実現に必要な、技術開発・研究開発テーマについての検討」が短期的な取組として提言していかなければならない例で、残りの「情報セキュリティのリスク及び対策の効果を可視化するための技術開発・研究開発の在り方についての検討」、「Technology Clearing house の実現に向けた検討」が出力を得るためのツールの例である。

○　コストと利便性のバランスをとりつつ、過不足のないセキュリティ対策を実施するための方法もツールの一つとして考える意味があると言う気がしている。

○　その通りである、「資料 3：技術戦略専門委員会の活動方針（案）」を作成した側はそのように考えていたが、表現が不足していた。

○　リスクの可視化は非常に大事なことだと思う。可視化することによって今まで気づかなかったようなセキュリティ上の新たな課題が見つかることも出てくるであろう。
ただ、可視化の良いツールを作ろうとすると、セキュリティの技術者だけではなく、アートの分野と技術の分野の橋渡し的人材と一緒にやらないと、可視化の本当に良いツールはできないと思う。
その点の進め方について、考えていることはあるのか。

○　例えば、ネットワークの運用・マネジメントの部分ではインターネットを把握するためにビジュアライズしようと、アート・クリエイターの人達を巻き込んで、色々な方法をやっていくという風に進んでいます。
他方、セキュリティに関しては、ACM（Association for Computing Machinery：教育および科学コンピューティング協会）か何かにセキュリティのためのビジュアライゼーションというミーティングがあったりもする。そういう他の動きも見ながら、異分野のツールを持っている人達を巻き込んでやっていきたいという風に考えている。

○　リスクの可視化ができたら良いというのは皆さんのおっしゃるとおりだが、本当に可視化できるかどうかは疑問に思っている。
可視化できていると言うことは、リスクとして織り込み済みと言うことだが、現実的には想定していなかったインシデントによる被害を受けて、それを専門家たちのチームによって解決してから、リスクが見えるものとして可視化されるのではないか。

ある程度可視化ができるツールが完成して、安心してしまうと、ツールで見ていないアタックが行われたときにはお手上げになってしまう。そのため、ツールだけでなくインシデント解析チームを国として作れるのだったら作っておいた方が良い。常にア

ップデートできていないツールというのは意味がない。

○　ツールをそろえただけではダメで、ツールをそろえて誰かに問題解決のために使ってもらうというのは資料 3 の 1 ページ目にある「Technology Clearing house の実現に向けた検討」の様な取組であろう。先ほどの意見は、それをデータマイニング的に使って新しい脅威をはっきりさせようという理解でよいか。

○　そのようにできたら、一番すばらしい。しかし、現実的には、新たな脅威が発生した場合は、ツールで検出するよりも先に被害が発生しており、短期的には被害を極小化する対応の方が問題になることが多く、専門家をすぐに問題の解決に当たらせることが重要になる。
一度被害を受けた後に、その対応をツールとして配布すると普通の企業は同じ被害から守ることができるというのが、イメージである。

○　ツールもプロ向けと、所謂セカンドレベル向けの両方あるように感じられる。しかも、プロ向けのツールであっても、ツールによって可視化することにより見えてくる世界もあるし、ツールでは対応できない攻撃もある。そのため、可視化ツールをすべての脅威に対して対応可能なものとして考えるのは危ないのはその通りだし、ツールを次々と変えていく部分を考えるのは必要だと思う。

○　大きな流れとしては、「資料 3：技術戦略専門委員会の活動方針（案)」に書いてある形で進めていただければと思う。

○　グランドチャレンジ型研究開発の検討方針については、3 月に聞いたときはうまくまとまっていないと思えたが、今見直してみると、結構色々考えられており悪くない。

○　報告書の原案と議事録を読み返してみると、グランドチャレンジのテーマを設定したら、テーマに即した技術開発が行われて、サブステンシャルなアウトプットが出なくてはならないという幻想にとらわれすぎていたように思える。
報告書 2006 でグランドチャレンジ型の研究開発に言及したときに、具体的な成果物は出てくる必要が無いことがきちんとかかれているので、もし、必ず具体的な成果物を出さなくてはいけないと言う認識があったのなら、もう一度考え直していただいて新たな視点で利用していただければと思う。

○　「資料 4：グランドチャレンジ型研究開発の検討方針（案)」の 4 ページにおいて、複合的で射程も長いものとして分類されているものが重要課題であると考えた方が良い

のか。

○　射程が長く、複合的なものが他と比べて特に重要であるというわけではない。

○　こういう形で報告書の中にいくつかの具体的な課題が出ており、良くまとまっているが、それらをグランドチャレンジという形でやるか、一般の研究という形でやるかは別途考える余地がある。
今回、第１次のグランドチャレンジ WG のレポートが出てきており、この委員会で大きな方向についての意見を出し､それを意識した上で第２次のグランドチャレンジ WG で検討すればよいと言う気がしている。

グランドチャレンジという形でやるのであれば、変化に対応できるセキュリティとか、ここまでやればこのレベルのセキュリティが実現できるのでこんなサービスが実現できるようになるのではないかというのを示してそこに対して色々なアプローチをしてもらうこととか、従来の所謂脅威の他にリライビリティ・アベイラビリティを含めたシナジーをねらったセキュリティとかがうまく出てきて、解が見え始めるとおもしろいのかなという気がしている。

○　グランドチャレンジの研究開発テーマの設定方法で、少し心配になっていることがある。当委員会でも２～３年前に申し上げたことがあるが、実のところ ICT に関する新しい技術を思いついたとき、相談する先が国内にない。例えば、インターネットのルーティング経路情報をセキュアにする研究において、研究を実用化する際に相談する相手はジュニファー社・シスコ社といった米国のベンダになってしまう。技術開発とかアイデアは全部うまく作れるが、最後のところでは英語で話さなければならない。
そのような現状を鑑みると、トロンプロジェクトみたいに全部自前で作ると言うグランドチャレンジがあっても良いと思っている。
商業的に見ると自前の資金ですべてをまかなうのは難しいのはわかっているが、国を支えるテクノロジとして、例えば、基盤技術はすべて自前で整備するというグランドチャレンジがあっても良いのではないか。要素技術が我が国から散逸してしまうのを防止するチャレンジである。
逆に言うと、そういうチャレンジが行われていると、交渉力になるので、そのようなチャレンジをやっていただけると非常に美しいと思う。

○　リスク変化対応型の R&D とか、アグレッシブな目標設定の仕方による R&D とかと同じレベルのものとして全部自前で開発すると言うものも考えられるのではないか。「資料４：グランドチャレンジ型研究開発の検討方針（案)」の４ページにおいては、粒度

と射程（期間）の二次元でまとめられているが、リスクの変化に対する対応や自前の技術による開発というのは別の要求を表す軸になると言う気がする。

○　グランドチャレンジを考えていく上で、グランドチャレンジは長期レンジで技術的な問題解決が大きいものに限るという様に、あまり狭く考えない方が良いというのが一つの意見であると思った。

○　商業的に見て短期的に採算がとれるものは、民間が黙っていてもやる。何もしなくとも民間によって達成されるものよりも、中長期的に我が国の ICT の底抜けを防ぐために交渉力としての自前技術が必要だと思う。
世界規模の R&D においては、交渉力不足を実感する。国として OS やルータの技術を持っていれば、もっと交渉力が付くので、そのような要素技術は国として涵養し、民間は短期的な利益を追求するという方向性を示していただけると非常に楽であると言うことを言いたい。
グランドチャレンジと言うからには、10 年ぐらいは評価されないが、歯を食いしばってがんばるというグランドチャレンジもあるのではないか。

○　ある期間で一旦止めて評価すると言う作業は必要だが、次のステップへどんどん PDCA を回して自己組織化していく技術開発のあり方も必要ではないか。脅威はどんどん変化していくのだから、リスクの変化に対応するセキュリティのあり方と言う表現の仕方をする必要もあるのではないか。

○　「資料 4：グランドチャレンジ型研究開発の検討方針（案)」には攻撃的な立場と防御のバランスをとるとあるが、グランドチャレンジにおいて、世界一安全な電子政府を実現するためには、日本に攻撃したら攻撃した方が損をする、日本が攻撃されたら 3 倍返しにして返すと言うのが、攻撃的な防御だと思う。そのような技術はあるのか。

○　仕返しの技術というのはあまり考えたことがない。

○　倫理からすれば政府をあげて攻撃するのは良くないが、やられたらやり返す、仕掛けられたら自動的に反撃するというのは良いのではないかと思う。

○　仕返しのシステムについては、B と言うところが A と言うところを詐称してアタックしてきたときに、誤認して A と言うシステムを叩いたときのリスクがすごく難しい。
仕返しをする前に、何らかのステップがないと、実施することはできないと思う。
どちらかというと、グローバルバックボーンにおける各国の入り口において日本向け

のアタックは止めるというのはやっても良いのではないかと思う。例えば、どういう事かというと、アジア方面から日本向けのアタックパケットが検出されたら、東京まで持ってきてから止めるのではなくて、グローバルバックボーンの入り口で止める。そうすることによって、日本からヨーロッパ等他の方面に向けたパケットは阻害されなくなる。

○　物理的なバトルにおいては、やられたらやり返すというのはあるが、サイバースペースでそれをやり始めると色々な抜け道あるので、物理的な紛争と同じ次元で仕返しを検討するとダメだと思う。
個人的にイメージする仕返しの技術開発は、直接反撃するのではなくて、例えば、グランドチャレンジの議論に出てきているように将来の脅威を見据えた技術開発をしておき、攻撃を受けたらそれをせせら笑うような対応が仕返しに相当するので無いかと思う。
直接反撃をやり始めると、際限なく応酬が始まり大変なことになる。

○　泥仕合になるよりは、無効化の技術をきわめて、何回攻撃を受けても何ともないような、相手に無力感を与えるやり方の方が平和的だと考える。

○　防御システムをチェックするために、仮想でも良いので、世界最高峰のアタックパワーがコントロールされた状態で我が国に存在すると言うことは重要である。ここで、重要なのは、単なるゲリラのようにならないためにコントロールされた状態で存在すると言うことである。グランドチャレンジの案の中にもあったので、これは良いと思った。
外に向かって使うことはないが、防御システムのチェックのために、公にアタックできる力を持っていると言う状態は良いと思う。

○　グランドチャレンジ型のアプローチと言うことで、第二次ワーキンググループで検討するために議論しているが、守ると言うことをあまり狭く考えずに、広く捉えてより効率的な方法を考えてもらう方が良いと思った。

○　「未成年や高齢者でも安全に使える端末環境の実現」とあるが、認知症の人や認知症でなくともIT社会から除かれている高齢者は、かなりの数が存在する。
そうした前提で、電子政府のみならず社会全体の安全と言うことを考えると、電子政府が広がっていく中で認知症の人やITになじみのない高齢者が、社会保障カードなど電子政府の機能を使うときに問題が生じうるし、そこを狙っている犯罪者たちも存在している。

そういう犯罪に対抗して安全性を保つための枠組みが、グランドチャレンジとしてのキーワードになると思う。ワーキンググループにおいても、そういうテーマが入ってくると良いと思う。

○　少し補足すると、「未成年や高齢者でも安全に使える端末環境の実現」というのは、1日に25万台ものゾンビPCが観測される現在の環境に、ITになじみのない人を晒しておくのが良いのかという問題があり、現状に即してきちんとプロテクトされた環境を作ってしまおうという意味である。
他方で、世界一安全な電子政府・電子社会というのは、第1次基本計画の時からずっと流れている理念であり、NISCとして常に持ち続けてきたものである。これを出すことで、電子政府を考える上で非常にわかりやすくなるので、資料に記載してある。
前述のご意見は、世界一安全な電子政府の実現と言うことか。

○　前回の委員会でも言ったが、セキュリティを考えるときに現実の社会の動きにぴったりとついて行く必要がある。スマートカード等の認証を例にしても、自分ではパスワードを覚えられないし、何を持たされているかもわからない人というのが、数百万人単位で存在し、かつ、それは減っていくわけではなくて確実に増えていく。
現実は明らかにその方向で進んでいるので、電子政府もそれについて行く必要がある。

○　技術というのは確実に動いており、例えば、暗号の危殆化というのはどこかで起こるであろう。それと同様に、利用者も時間とともに変化していくわけで、現在パスワードを8桁覚えていられる人が、ある日突然忘れるかもしれないと言った状況にどう対応していくかという課題は確かに存在する。
但し、それがグランドチャレンジかどうかというと、わからないと思う。

○　グランドチャレンジ研究テーマ案は、左上（複合的・短期）と右下（要素的・長期）には割とおもしろい案がいくつか出ているが、当然のことではあるが、右上（複合的・長期）は重要な問題ではあるがアプローチが見えないという状況になっていると思う。

○　右上（複合的・長期）のグランドチャレンジは、技術と言うよりもそれによって実現する社会の事を言っており、これをテーマにすると制度設計を含めて色々なことをしなければならないので、グランドチャレンジのテーマにはしづらいのではないか。
現在のグランドチャレンジ案は技術的なものと実現する社会のことが混在しているのが気になる。

○　逆に言うと、右上（複合的・長期）の技術課題をグランドチャレンジ案としてもう少

し出すと言う話はあるだろう。

○　右上（複合的・長期）だけだと、狭くなってしまうが、右下（要素的・短期）や左上（複合的・短期）は研究としてはおもしろそうだがグランドチャレンジと言うと狭かったり・近かったりしてしまうので、そのあたりが難しい。

○　グランドチャレンジというと、他国がやっていない事であるというイメージを持ってしまう。

○　海外ではセキュリティ、かつ、グランドチャレンジ型のアプローチというのは何か存在するのか。

○　ヨーロッパにおけるグランドチャレンジとしてはFP7（EUの第7次研究枠組み計画）でプライバシー・コンシャス・インフォメーション・プロセッシング等をやっている。他方、米国はセキュリティというか、CIIP（重要インフラ防護）のインフラ・プロテクション・プログラムとしてやっている。これは、クリティカル・インフォメーション・インフラストラクチャをどう守るかという大きなテーマの基に、領域と手法のマトリクスができていて、その中に全部落とし込まれている。

「資料4：グランドチャレンジ型研究開発の検討方針（案）」4ページのマトリクスと言えば、垂直方向の（要素的、複合的）という軸は成果管理の複雑さを、水平方向の（長期、短期）という軸はリファクタリングのやり方の頻度を示していると言える。現在の政府の予算構造においてはリファクタリングの仕組みは存在しないため、弊害が発生している。例えば、スーパーコンピュータの開発において、リファクタリングを行わないためアーキテクチャが動かせなくなってしまう。
そのため、長期的な課題になればなるほどリファクタリングをプロセスの中にきちんと最初から織り込んで、合理的なやり方をすることが必要である。FP7やCIIPにはリファクタリングの仕組みが存在し、リファクタリングチームが「このプロジェクトはやめろ」とか、「これをやらないと次にいけない」とかの指示を行っている。特にFP7のプライバシー・コンシャス・コンピューティングではドイツのBSIと言うグループがリファクタリングをリードしている。
このようなリファクタリングの仕組みがあれば、右上（複合的・長期）のグランドチャレンジの実施も考えられるのではないか。

○　技術戦略専門委員会としては右上（複合的・長期）のグランドチャレンジはターゲットとしなくても良いかもしれないが、日本政府としてはターゲットとするべき。

その際に、技術戦略を進めるにはリファクタリングのチームと一緒にやらないと、勝手な方向に進んで無駄が生じるので、技術戦略専門委員会としてはリファクタリングについて発信していくことが重要なのではないか。

○ 第一次報告書においても、プロジェクトマネジメントの方法とか、投資構造をドライブする社会システムをリファクタリング可能なように変えていかなければならないと言うことに言及されている。最終報告書でも大事なことであるので、盛り込んでいきたいと考えている。

○ 総合科学技術会議の情報通信 PT において、グランドチャレンジを残しているのは、セキュリティだと攻撃者がいるため、ムービングターゲットという内容を否定されにくい。そのため、リファクタリングをきちんとやれるプロジェクトマネジメントに挑戦できる良いチャンスだと思っているためである。
グランドチャレンジというと多額の出費があると思われているが、お金を使わずにリファクタリングをうまく実施できるプロジェクトとして、報告書に書き込み、11 月に行われる総合科学技術会議情報通信 PT にインプットするのが一番良いと思っている。

○ 左下（要素的・短期）の象限に「高齢者でも安心して使える端末・環境の実現」というのが挙げられているが、ここにある限りは実現しないだろうと思っている。例えば、先ほど認知症の話をしたが、知的活動が低下していく高齢者を考えると、預金・保険等自分が関わっているものを認識できなくなっている人をサポートするシステムなどがあった場合、個人情報保護法や後見人制度も関連してくる。このように考えると、「高齢者でも安心して使える端末・環境の実現」は左下（要素的・短期）では実現しないであろう。
直近で具体的な問題においても、技術的な戦略では解決できない問題がゴロゴロしていると思う。

○ 課題として短期的な話と、きちんと解決しようとすると長期的に時間がかかる話がある。環境変化と言う動的な面があるので、そこを考えてテーマ設定するのかと感じられた。

○ 日本は資源もない、食料もない、物理的な核という力もなく、あるのは知恵だけだと言う状況でありながら、巨大科学でも世界をリードできないのはムービングターゲットに合致したプロジェクト運営ができないためであると思う。
わからないものには投資しないため、肝心な部分における科学研究が行われていない。IT セキュリティはムービングターゲットに合致するので、これを切っ先に日本の非常

に保守的な投資概念を打ち砕けば、セキュリティのみならず日本のグランドチャレンジとして意味のあるものになる。そういう意気込みを持ってやっていただきたい。

○　総合科学技術会議の情報通信 PT にはリファクタリングの仕組みを備えたグランドチャレンジを持って行くともう少し良いのではないかと思う。

○　現状のように、プロジェクトは一回で終わってしまわなくてはならず、同じようなことをやりたい場合でも違ったテーマでやらなければいけないというのは、本当は違う。大事な問題や、難しい問題をやるとなると時間がかかると言うこともあり、ある程度進めてからさらに良くすると言う事が必要だという気がした。

○　最初にインシデントの被害を受けてから可視化すると言う話があったが、リスクをどの様に見て、不確定性をどの様に管理していくかについて、最近地震関係の人と話す機会があった。
彼らは、リスクと言うものは 378 種類あり、そこに入っていないものを不確定性であるという。378 種類というのはすごく考えられており、そのためのツール開発も行われていて、そういったノウハウが情報セキュリティの領域に来るとどうなるかについてチャレンジする人も出てきている。
このような、他の知見の活用方法もグランドチャレンジの中で考えておかなければならなくて、他人が持っている知見や別の領域の知見をうまく活用していくためのシステマティックな方法をどうするかというのをセキュリティでも考える必要があると思う。

以上