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１回会合議事要旨

１．日時　　平成１７年8月２２日（月）１７：００～１９：００

２．場所　　内閣府本府第３特別会議室

３．出席者

[委員]
河田 惠昭 委員（京都大学防災研究所所長）
佐々木 良一 委員（東京電機大学教授）
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）
西尾 章治郎 委員（大阪大学大学院教授・文部科学省科学官）
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セキュリティ対策室長（代理：同室課長補佐）
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
文部科学省研究振興局情報課長（代理：同課課長補佐）

４．議事概要

(1) 内閣官房情報セキュリティセンター長挨拶

(2) 委員長の選出

○　佐々木委員を委員長に選出

(3) 佐々木委員長挨拶

(4) 会議の公開等について

○　事務局より説明、原案のとおり了承

(5) 情報セキュリティ政策会議の概要

○　事務局より説明

(6) 我が国における情報セキュリティに係る技術戦略の推進についての問題意識（案）

○　事務局より説明

(7) 政府による情報セキュリティ関連研究開発・技術開発の現状

○　５省庁から説明

(8) 技術戦略に関する問題点の抽出と論点の整理についての討議

○　この委員会で、プライバシーと知財保護の点についても扱うべきではないか。

○　どの領域が入るか、どういうプライオリティ付けをするのかは、あれもこれもとなると大変なので、まずセキュリティ技術に関する俯瞰的なイメージを作るべきではないか。その中でプライオリティ付けができるのではないか。

○　我が国で閉じるとすると､開発した技術戦略を社会に展開することは難しいと思う。すごいいきおいでアイデアを作り、試作品を作り上げることは何度もやっているが、結果的に使っている製品は、全部ではないがアメリカ製になる。公平なプロキュアメントという意味では、普通の民間の会社というのは、世界にある技術を使えばいい。

○　アメリカ政府は割りと世界中から技術に関する情報を集めるという傾向があるようだ。しかしながら、今出ているビューポイントは、頑張って日本の中に閉じようと見えてしまう。その点違和感がある。

○　データを可視化して業務をこなすにはＧＩＳが適していると思うが、知的生産性が上がる反面、セキュリティを高めないとアタックがあり得る。システムが社会で作られてくることを踏まえてセキュリティを考えないと、要素技術だけのパッチワークで穴だらけにならないか。また、先進的なものだけでなく、同時に世の中で動いているものについてもやる必要がある。

○　マネジメント、あるいは組織論的なものをどこまでケアしていくのか。さらにはレイヤーを社会、ソーシャルな視点で見るのか、もっと個人、サイコロジカルな視点で研究するのか、ヒューマンインターフェースの話も出たが、あるいは組織という単位で見るのか。それらの優先順位をこれから付けて行かなければならない。

○　もう一方でセキュリティ文化専門委員会があるが、まさに文化は人間系の話で、そことの役割分担を我々はどうやっていくのか検討するべきではないか。

○　技術戦略専門委員会の議論は､広義の情報セキュリティに関する研究開発における、政府から見た投資の問題になる。そう考えると、こちらの場でクローズできるのではないか。社会が何をやるべきかというところまで行ってしまうと、セキュリティ文化専門委員会との関係が強く出てしまう。

○　防災、減災という問題と、サイバーテロや事件の予防・拡大阻止のプロセスは非常に良く似ている。情報セキュリティの問題も、結局は国としてあるいは組織としてどのレベルまで持ちこたえるのかということ。攻撃する側はこちらの弱点を狙って来るわけなので、被害をゼロにすることはできない。しかし、どのレベルで持ちこたえられるかはよく考えておかなければならない。

○　都市で起こる災害は複合災害という特徴がある。いわゆる外力は自然災害であって

も、出てくる被害の大きさ、あるいは被害の多様性は社会の仕組みとリンクしている状況にある。東京で地震があったということがリアルタイムで海外に伝えられたときに日本円や日本株が相当に処分されるということで、間接的な被害が、日本で起きる直接被害よりもはるかに大きくなる。

国にとっても災害時の情報のマネジメントをどうするのかというのが、実は被害とリンクしている、という点で重要。このときの情報のハンドリングをどうするということについては、日本が責任を持ってやっていかなければならないのではないか。

○　情報セキュリティをビジネス化する際に、いわゆるフィジカルなセキュリティとニーズが一体になっているところがあり、社会的コストとの兼ね合いが課題となっている。

○　第１次及び第２次の科学技術基本計画で、情報セキュリティ関係をあまり謳っていないということが、逆に奇異に思った。

○　今後３年間をベースにした提言を出すということだが、出口の部分において、この３年間で、何かのメジャーでこういうものをここまでやっていきますといったものをこの専門委員会で盛り込んでいくのか。そうではなくて、重要技術としてこういうものとこういうものがありますよ、といったところなのか。この委員会から出す提言には、それなりのインパクトが必要なのではないか。

○　数値化した評価体制に変えていかないといけないのは事実。単に重要だからというのではなく、投資した後の回収の部分を考えたときの、回収のインデックスを作っておかないといけない。そういった意味では、数値化というものについては構造の中で考えるべきではないか。

○　新しい技術を開発していく際に、いきなりコストの問題を数値目標として挙げるという考え方には反対。先行している分野では、投資に対して評価できる数値が出ているが、新しい技術では投資に対する効果が出しにくいので、同じ土俵で議論することはできないのではないか。

○　まず被害の実態を把握することが必要。全てに備えるということはできないので、これをやられたらだめ、というものと、これをやられてもある程度対応できるというものと、いくつかに分ける必要がある。そういうところから費用対効果は出てくる。

○　危機管理においては、オペレータそのものが一番危ない、というものがある。全体を知っている人はほとんどいないという体制を作らないと。誰かが全てを知ったら、その人がやられた場合におしまいになってしまう。

○　この委員会にはいろいろなサブジェクトがある。例えば企業や自治体など、どういった主体がベネフィットを受けるか。あるいは性質にも、純粋にテクニカルなものと、マネジメントなものもある。そういう切り口をどういうプライオリティを付けて進めていくかということがこれからの議論ではないか。

○　多少バイアスはあるかも知れないが、国産で信頼性の高い、あるいは安全性の高いオペレーティングシステム、いわゆるＩＴの根幹になる部分を我が国がどういうふうにしていくのか、というのは一度議論しておかなくてはいけないのではないか。それだけのＯＳが普及していくのかという課題もあるが、ある種のセキュアなＯＳを作っていくことが、いろいろな話がある中での核になるのではないか。

○　技術の最先端ということで、この先、集中型の話とＰｔｏＰ的な安全分散の話が技術の両極になっていくと思われる。特にＰｔｏＰというのは、そのシステムが進んでくるとネットワークの監視は難しくなってくる。また、全体のインフラの使用効率は上がるが、コンテンツのやりとりや共有などで、トラヒックが際限なく上がっていく可能性がある。実際にそういう兆候が見られており、そういうところも視野に入れておくべきではないか。

○　ＰｔｏＰ系ネットワークでアンストラクチュアルデータが相当増大しており、ストラクチャー化する動きがある。しかし、それとは離れた自由な空間というものがまた出て来る。その二つの大きなトレンドの中で、どうリスク分析するか、提案を出してみるべきではないか。

○　人材育成も含めて、こういう戦略は、技術要素をどう評価するかだけではなくて、いろんな技術要素をリンクさせた社会のシステムをどうするのかという、そこに大きな問題があるのではないか。

○　最終的にはビジネスも継続しなくてはならない。継続性確保のためにはあらゆる手段を使ってシステムを動かしていかなくてはならない。そうしたオペレーションを基点とした技術開発が重要。

○　オペレーションをちゃんと商品化する、社会のノウハウとするということ、それに対して日本側としてどうするかということ。また、全体の社会システムをどう維持するかという視点での分析と、産官学を挙げたチーム構成をどうするかということが非常に重要な問題ではないか。

○　問題意識としては、国家の情報力。サイエンスとしてだけでなく、国の施策としてちゃんと情報力というものを国の前面に押し出して、少なくとも総合科学技術会議が自分のサイエンスの立場で言うのではなく、もう少し大きなものを見て、その中で総合科学技術会議が取り扱えるところに行くようにインプットして行きたい。

○　各省庁の取組状況については、キーワードがオーバーラップしている部分がある。全体をちゃんと見て誰が何をやっているのかをきちんと把握しているところがあるのかどうか。非常に次元の高いデータベースのようなものを整備してスタテックに置いておくだけではなくて、いつもアップデートしておかなければならない。

○　まず脅威の分析から始めるべき。こういうことが起こったらこうなる。そのときの経済的な損失はいくらになる、あるいはお金には換算できない損害が発生する。どこにどのくらいの損害が起きるか分からないのでは、そもそも投資などはできない。それを国家的に行う必要があるのではないか。最低限、マニュアルによる代替が可能にするべきで、マニュアルにも切り替えられないシステムが各省庁にあるとすれば、そこはいくら投資してでも守らなければならない。

○　何が起きるか分からないのでは、どうしたら良いのか分からないのではないか。単にハッカーがやってくるだけではなくて、仮にどこかの国が我が国に対してやってくるのであればやり返すくらいの部隊を作らないといけない。何か商品を作って、スタンダードを作って、買いませんかという話ではない。

○　リスクアセスメント、脅威分析については、これまでの各省庁の取り組みにしても、内閣官房の情勢判断にしても、完璧ではないがいくつか着手しているところ。その意味ではいくつかの知見と、いくつかの調査結果は各省庁の中に残っているのではない

か。脅威分析を包括的に、かつ一発きりでなく定常的にやっていけという提言がされれば、これを基本計画の中に読み込んでいくことになるのではないか。

○　一般の人は被害の甚大さを知らない可能性がある。大きさも深刻さも知らない。被害の例を挙げていくだけでも、委員会としての提言にも深みというか、重みができてくるのではないか。

(9) 今後の予定

○　事務局より説明。

以上