重点分野推進戦略専門調査会 情報通信研究開発推進プロジェクト 第１回会合
議事録（案）

日時：　平成１５年1月２４日（金）１７：００～１９：００
場所：　中央合同庁舎第４号館　４階 共用第４特別会議室
出席者：細田 科学技術政策担当大臣、大山 総合科学技術会議議員、
池上、佐々木 元 各重点分野推進戦略専門調査会専門委員、
飯塚、大木、大野、岡本、佐々木 良一、土居 各招聘者、
事務局（大熊政策統括官、和田審議官、杉山参事官）
（敬称略）

議事：
１．　細田 科学技術政策担当大臣挨拶
IT 担当大臣を私がやることになり、科学技術政策と一緒にやれるのは良いこと。
総合科学技術会議では ＩＴが大きな分野のひとつである。総理官邸でも、e-Japan 戦略で電子政府や教育の IT 化など、様々な取り組みを行っている。国民の目から見て分かりやすいところを戦略にしている。一方、専門的に見て、これからさらにやらないといけないことも多い。セキュリティは IT 戦略で触れてはいるが、さらに深堀が必要。ソフトウェアや教育体制もそうである。研究開発ではより長期に渡る分野もある。
政府としては、IT 戦略本部の出井調査会もあり、アマチュア向きとプロ向きの両方をミックスしたような良い報告を出していきたい。先生方には、プロ向きの、我が国の IT 戦略において外してはいけない点を押さえて、あるべき体制、予算のご検討をお願いしたい。これが主たる目的だと理解している。是非とも多角的なご議論をお願いしたい。
[池上]
平成 13 年度９月に情報通信分野の推進戦略を決定している。より具体的に、正確に方向付けを検討していきたい。5 月を目途にとりまとめて平成 16 年度の予算に向けて反映していきたい。

２．　出席メンバの紹介
[事務局]
本日出席された大臣、議員、専門委員２名、招聘者６名、事務局３名を紹介。

３．　配布資料の確認
[事務局]
資料１から資料７まである。また、本会合の運営要領案（資料１－３）が了承された。

４．　一般傍聴者の入場
運営要領に基づき、一般傍聴者が入場。

５．配布資料の説明
[事務局]
情報セキュリティの課題と方向性（議論の叩き台）（資料１－４）を説明。
[池上]
誤り等、バージョンアップの必要がありましたら事務局か私の方へご指摘いただきたい。
[飯塚]
NTT コミュニケーションズにおけるセキュリティマネジメント体制とセキュリティ人材育成のあり方（資料 2）を説明。高度な専門性を持った人材育成と、お客様に提供するサービスを生成する過程がセキュリティと不離不可分であるという考えにたった、底上げを含めた人材育成の二種類がある。一社ではできないことがあり、競争条理を超えた業界としての協力体制が必要。
官民連携の余地もあり、人材育成のための大学等との連携や、技術戦略、国策としての更なる措置も必要である。

[大木]
情報セキュリティ人材育成の現状（資料３）を説明。セキュリティに関しては、セキュリティを専門とする人、ＩＴプロフェッショナルでセキュリティの専門家ではないがそれも分かるという人と、一般社員の大きく三階層に分かれている。アーキテクチャとして、どういう機能が必要か判断する人間が必要である。

国際標準に則ることは必要であるが、日本独特の方法論について研究の余地がある。

国への期待は、技術開発の重点をハード中心からソフト・サービスへ移すことにある。マクロ的にこの分野でどの程度人が必要なのかを示すことが、今後の育って来る人のモチベーションにもなる。上級技術者の処遇や社会での位置付けをはっきり示す必要がある。また、技術認証のサーティフィケーションによって技術の変化のスピードが妨げられないようにするということが必要。

[大野]
高度情報通信危機管理研究の現状とその発展へ向けての提案（資料７）を説明。ＣＲＬのグループでは実験やデータベースの開発や、最近では電磁波セキュリティの研究等を行っている。IETF や ITU-T といった機関で標準化活動をしている。国際標準になることで大きなアドバンテージがある。例えば ITU-T では非常時通信のＳＧ１６ができた。どうやって次世代の非常時通信システムを作成するかといった話がすぐ始まる。次に問題になるのは機器から漏れ出す電磁波ではないかと思われるので、電磁波セキュリティの研究を開始している。

内閣官房では、電子政府の安全確保を意図したチームとして NIRT を立ち上げ、昨年度より十数名のメンバーで活動している。

[岡本]
筑波大学での情報セキュリティ人材育成の現状と計画（資料４）を説明。筑波大学ではシステム情報研究科でリスク工学専攻を置いている。ソフトコンピューティングとサイバーリスク、巨大システムリスクの３つの分野がある。サイバーリスクの中に、セキュリティの人材育成を行っているが未だ十分ではない。先端学際領域センター TARA で情報セキュリティ管理の研究を行っている。他大学、研究機関、企業とも連携して人材育成に取り組んでいる。国に提言したいのは、大規模システムのセキュリティ対策技術、不正侵入対策、限られた資源を有効に活用するためのリスク評価を強化すべきという点。その他にも内部犯罪対策や安心して利用できる情報セキュリティシステムが必要。また、やる気の有るところは１箇所だけでなく、同じところに補助が集中しないようにしていただきたい。

[佐々木（良）]
東京電機大学における人材育成の現状と計画－セキュリティ技術関連－（資料５－１）を説明。大学と企業が協力して教育を進めていかなくてはならないだろうと思っている。東京電機大学大学院の講義は、従来は暗号とセキュリティプロトコルが中心だったが、これから暗号、ネットワークセキュリティ、不正侵入対策の３つについて、来年度あるいは再来年度から開始したいと思っている。講師について、大学で難しいところは企業の方にも協力してもらう予定。国に対しては、企業と大学が協力する場のサポートをお願いしたい。

今後研究を強化すべき項目（資料５－２）を説明。大事なのは、公開鍵暗号の危殆化対応技術であり、これがだめになると信頼の基盤である PKI や CA がガタガタになってしまうので、早めに手を打つ必要がある。

[土居]
ISMS の運営委員長を仰せつかっている。認証については、現在 60 社弱、日本を除いた世界では 150 社程度。更に多くの国内企業が取得に向けて動いている。これは、ＩＳＯ９０００，ＩＳＯ１４０００と、それと対になるＩＳＯ１７７９９の認証制度で、組織の総体を認証するものである。電子政府がらみ、あるいは中小企業などで、ある特定の部分だけを認証して欲しいというものに応えるのは難しい。そこで、経済産業省で情報セキュリティ監査制度を 4 月に立ち上げようとしている。ここで問題になっているのは、人がセキュリティホールであること。OECD で「セキュリティ文化」を世界中の個人個人が身につけようと提言されている。これを踏まえ内部監査、外部監査ができるような監査制度を立ち上げようと努力しているところ。インシデント対応体制の整備も必要。

日本の JPCERT では、体制不十分ということもあり、実際の不正アクセス対策を施すのに必要な脆弱性情報／対策情報がまとまっていない。国内のオープンソフトウェアなどの送付とウェアや装置を対象とした対策情報データベースもない。そこで、私の研究所と JPCERT と連携して国内の企業に活用していただくようなデータベースを構築しようとしている。米国で CERT Advisory と CERT/CC Vulnerability Notes があるが、Vulnerability Notes については残念ながら日本のものがない。各社のものがあるが、統一がとれていない。これらの対策情報を取り込んで、データベース化をしようとしている。インシデントが起こった際はこちらを見ていただければ対応策が取れることになる。業界のみなさんの協力をお願いしている。あるところから先は、やはり国としての体制が必要となる。

６．フリーディスカッション

[池上]

日本が弱いと言われている人材育成についてプレゼンテーションを頂いた。昔のネットワークの時は、盗聴のみ気にすれば良くて、インターネットが出来てから良く分からなくなった。

[大山]

各位から、示唆に富むご意見、ご提言をいただいた。今回初めて参加するが、私の基本的な認識と当面の関心事について述べる。ネット社会は技術革新を背景に、社会の隅々に急激に波及するものであり、情報セキュリティのリスクが急激に高まっている。この対策はプライオリティの高い緊急課題であると認識している。また、セキュリティに関してはコスト対効果の観点において、企業等でその効果が見えにくいこともあって、トラブルが発生して初めて問題として顕在化する。先手必勝型の方法が、なかなか出来ていない。これを契機に課題を積極的に顕在化して、我が国独自の情報セキュリティの構築に必要な基盤技術の強化をみなさんと進めていきたい。最大の関心事は「プロフェッショナル」な人材の育成。大学と企業が協力して、より実践的なカリキュラムを作成して、よりレベルの高いプロフェッショナルナな人材を緊急に育成する必要がある。もう一つは関連ソフトウェア技術の強化も重要。

[佐々木(元)]

セキュリティという、情報化社会を支える非常に重要な問題について、多面的な立場からご意見をいただいた。3 点感想を申し上げる。(1)日本はセキュリティに対する考え方について、国際社会の中において果たしてそれだけの認識を持った取り組み方がなされているかどうか。こういった情報システムに限らず、日本のシステムは使い易く作られているが、人間の性善説に基づく考え方で運営されているのではないか。やはりセキュリティに関して相当幅広く、多面的に捉える必要がある。教育が必要になってくるだろう。一般国民も PC とインターネットでやり取りする時代だから、そこを啓蒙する事が必要なのではないか。(2) セキュリティ製品、またモジュールやパーツの研究開発でレベルの高い物を作り上げていくということと、それをシステムの中にビルトインしてどう事業化するかということの 2 つの側面から捉えていく事が重要。特に事業化は、グローバルなデファクトとどう整合性を取るか、或いはどういう関係になるのかが重要。特に OS に支配される様な部分をどう取り上げていくか。こうなると、国としての政策も必要となるのではないか。(3) インターネットの危機管理の中で、通信ネットワークが IP 化によって脆弱化されているのではないか。また、通信サービスの民営化で、かつての様に NTT が日本全体のネットワーク管理をしていた状況と今は違っている。危機管理の面から見て、通信ネットワークをどう考えていくべきかというのも、一つポイントとしてあるのではないかと感じた。

[大臣]

セキュリティについて政府が何をしなければならないのか。特に大野さんが内閣官房でチームリーダで研究されている訳だが、実際やっておられると色々足らざる部分等が、人間の面でも予算の面でも、あるいは考え方の面でも沢山あると思う。これから IT 戦略本部でも方向を出す時に、分かり易い形で出すのも使命だ。一般向けの他にプロ向けの専門的なことも必要。標語として、「元気」「安心」「便利」といったものを標榜しているが、「安心」というのはセキュリティの問題で、大きな柱として取り組んでいく。さらに具体的に、産業や大学を含め、研究者の間でやるべき事をまとめて行かないといけない。今後また、もう 1 回集まって頂くのも一つの考えだ。また、ご意見を具体的に賜る事が出来たら、政府として方針の中にこれを盛り込めという事があ

ったら、別途お話頂ければ大変有り難い。もちろん、教育の話も含め、幅広く対応する必要があり、宜しくお願い申し上げる。
[池上]
大臣の仰る通り、一般向けとプロ向けがあり、ここで議論されるのはプロ向けの方だ。プロ向けとして「国として是非これを」というのを詰めて頂きたい。大木さんから「日本独自の方法があるのではないか」との不思議なご発言があったが、これは一体どういうものか。
[大木]
私はコンサルタントをやっているが、ベースは国際標準使うのだが、欧米のセキュリティの常識と日本の常識は少し違う。しかし技術的にはインターネットで繋がっており、同様に脅威に対抗しなければならないので、達成するものは同じでもアプローチは違う事が有り得るのではないか。アプローチ、メソドロジも技術だと思っており、日本の文化や組織の運営に基づいたやり方で日本独自のものもあり得るのではないか。韓国では儒教思想のベースがある様に、日本でも同様のものがあると思う。そういうアプローチも研究の価値があるのではないか。
[池上]
セキュリティマネジメントの中で、社内の人間が一番問題だというお話があったが、そこの部分か。
[大木]
責任の分担とか組織の運営に関しては、例えば、日本の企業と欧米の企業の意思決定の仕方は違うし、組織と個人の関係もかなり違う。その中で、国際的な標準と同じ管理を組織の中に作っていくためには、やはり日本独自のアプローチが必要だ。これはまだ先の話だと思うが、日本の国全体で考えるべき色々なセキュリティの機能の配置についても日本独自の方法論があるのではないか。
[大臣]
今度の国会で個人情報保護法を出しなおす。考え方の基本は、例えば 5,000 以上の個人情報を扱うような情報処理の企業において、情報を漏らしたり、売り飛ばしたりする者にソフトに「駄目だよ」と勧告をして、聞かないものは処罰するという程度のもの。いろいろ配慮しても、難しい面がある。そういう日本人の感覚がある。また逆に、卑近な例では、クレジットカードや通販に対して警戒心が多く、社会的に「これは便利だからどんどんやろう」とはいかない風土がある。しかし、欧米がどんどん進んでいくと、セキュリティの面でももちろん深堀りするし、同時に流通形態等色々の面で社会的な革新のスピードが大きく、日本では需要や社会的要請が小さいために遅れてしまう心配がある。日本的風土に安心している面と、逆にそうしたものに近寄らないという面もあり、そのどちらも大きな問題だと思う。ブレークスルーがきちっとあって、個人認証や住基ネットの問題もあるが、しかしきちっとした説明をしないといけない部分と、セキュリティの問題についての国民的確信を得ないといけない部分がたくさんある。
[池上]
倫理的な部分では日本人のやり方というのはあるかも知れない。技術的には、プライバシーを捨てて入るのがインターネットだった。入った途端に「プライバシーだ」と言われても、技術的には非常に困る。100%安全かと言われたら、技術的には無理。そこを如何に技術面から取り組むか。
[大臣]
どう法規制するか等の議論が早々におこなわなければならない。
[池上]
本件、結果については大臣にご報告いたします。
[土居]
セキュリティに絞った話も重要だが、システムを、法的な面も含め、どう運用するかも考える必要がある。使われているデバイスを考える時は、ソフトを全体として考えないといけない。というのも、携帯電話でも、松下やソニーが回収といった問題があったが、これらはセキュリティに関するトラブルによるものだった。これらはソフトウェアの作り方、つまりソフトの「信頼性」、そして、さらに如何に「生産性」を上げるかという課題が根底にある。東芝のラップトップ PC もせっかく世界で 1 位になって稼いでいたのに、何の事故も無かったにも関わらず訴えられて、

これまでの利益を吐き出させられた。要はものづくりがどこまで行っているかという事に関わってくる。今のマイクロソフトは Windows で週に 1 回、時には 2 回位、「穴ぼこ」を塞げと言ってくるが、それで、穴を塞いだのか、穴が広がっているのか、穴の数が増えているのか、誰も分からない。しかし、マイクロソフトの戦術とすると、何かが起こった時の Excuse になる訳だ。日本の得意な情報家電、ユビキタスコンピューティングとなってくると、作った物が世界中に拡がる。その時にマイクロソフト流の事が出来るかどうか。私の気に入っている言葉に「Sustainable Computing」というのがあり、これはソフトウェアの Dependability、Quality、及び Security に関わるもの。そういったものを総体として物事を進めていかないといけない訳で、我が国としては、総合科学技術会議でもソフトの生産性と信頼性の議論を、セキュリティと密接な関係で進めていく必要がある。

[池上]

Linux ならどうにかなるというのもあるが、その辺りはどの様にお考えか。

[土居]

多くのユーザが使っている製品だと、色々な事が分かっているので、ウィルス被害が多く、ネットスケープ等のユーザが少ない製品は被害が少ないという事もある。例えば中国は、政府がマイクロソフトに対してソースコードを出せと言う事をやった。我が国は数ヶ月前にやっと副大臣、あるいは自民党の方がものを申されたが、かなり遅い。ソフトが全部出されたら全て大丈夫かというと、今度はそれなりの体制を作らないといけない。Linux が読めるかと言ったら、読める限界を超えて育ってしまっている。ただ、何かがあった時には、ソースコードがオープンになっていると、例えば「穴ぼこ」を塞いでいる、あるいは、「穴ぼこ」を広げているのかどうかは分かるという意味で、オープンソースは良い。ただ、新しいものをいわゆるオープンソースで進める時は、余程腹を括らなければならない。例えば Linux だとリーナス・トーバルズが「教祖」として、やっている。新しいものは必ずしも「教祖」を必要とするとは思わないが、要するにその様な体制で、オープンにしたものが方言だらけになってしまうと、オープンにした意義が、ある意味無くなる。支援体制というか、政府がやるかどこがやるのかと考えると、恐らく、民間企業が学と一緒になってやる必要があると思う。

[飯塚]

一つの問題は、日本独自でないソフトに起因する問題、あるいは日本の技術がデファクトとして世界的に通用しないといけないという問題。そのためには、色々な標準化活動等、いい意味で国策として軌を一にしてやらない太刀打ち出来ない。NTT グループは言うまでも無く、各省庁、そしてメーカ含め、それが欠けている気がする。ハイパーコンペティションの中では、国が国策として取り組まないといけない。

[大野]

オープンソースの問題は、行政がどういうシステムを使うかという議論をする時と、大学等がどういうシステムを研究していくかという時では、全然話が違ってくる。今の問題は、オープンソースの問題というより、単一生態系になってしまったので脆弱になっているという事。もし、マイクロソフトの様にソース公開しなくても、コンペティティブな会社が 4、5 社あって、競争していれば、こんなに脆弱にならなかった。単一生態系にならない方策があれば、それが情報システムを安定させる力になる。そのための一つのアプローチとしてオープンソースが脚光を浴びている訳だ。どういうシステムを電子政府に導入したらハッピーになれるかを考えた時、オープンソフトは一つのアプローチに過ぎない。しかし、大学や研究所で若い力を育てて、パワフルな人材を育てなければならないという時は、オープンソースの様なモデルがないと、人が育たないので、重要なアプローチとなる。そこの所がしばしば混同されて議論されている。政府として安全なシステムを作りたいのであれば、単一生態系こそ危惧すべきで、Linux がシェア 100%となったら、またその時に別の問題が起こるはず。その点は意識して考えるのが良い。

[池上]

オープンソースに資金を投入しようとしても、受け皿が少ない。日本では、オープンソースをやっている者がいない訳ではないが、通常の大学の教育だと、うまくいかないかもしれない。どのようにしていけばいいのか。

[土居]

ものによる。敵対するものを作ろうとしても、今の我が国の大きい所は、要するにそれを使わないと上に載っているのものが売れないという状況に立ち至っている。我が国のかつてのメインフレーマーと呼ばれていた人達は、国内 OS を使っていた。今現在、メインフレーマー、またその他の所もそうだが OS（おお S）も「中 S」も「小 S」もやってない。「小 S」で TRON 位がまだやっている。コンパイラも富士通、日立、NEC がベクタ型のスパコンで世界制覇していたから少しはコンパイラの人材がいるが、教える人間がいない。コンパイラ屋も OS 屋も 10 本の指で足りる位だ。欧米の大学では、有り得ない事。我が国の業界はソフトハウス含め、ゼネコンのように下請け構造があり、知識集約型産業であるべきものが、労働集約型産業となっている。学部・学科で優秀な者はこの業界に行かないという事になっているという困った状況であり、もっとフラットにして頂きたいと言っている。セキュリティにも関係があり、下請けの段階でどういう団体が入ってくるか分からなくて、色々と問題が起こっている。産業界も大学もそれぞれが努力して構造改革をしないといけない事だけは確か。

[池上]

アメリカだと、Linux を使って OS の教育をやっていたが、日本ではその様な取り組みは行われていない。

[大野]

オープンソースをやって良いのは、コードを見て安心できるから。しかし、コンパイラが嘘つきだと駄目になる。設計図通りに動く機械語コードを作れる事が重要で、悪意のあるコンパイラがあるとバックドアが入る。コンパイラのセキュリティチームが必要。先生の仰る通り、コンパイラのエキスパートは日本では大量に育つ目途はない。それが心配だ。

[池上]

企業サイドからみるといかがか。

[佐々木（良）]

企業がまたは専門機関が教育するという 2 つの方法がある。専門に教育を行う所の人達はかなり力を付けてきている。そこで、一般の人を教育する事は出来る。しかし、プロの拡大再生産が出来ているかというと、なかなか難しい。対症療法的なのは、専門企業で出来るが、大学で法律や OS 等の知識を学んだ人でなければ教育出来ないとも言われており、大学でもセキュリティ教育として、こうしたベースの知識も教えないといけない。セキュリティ教育もビジネスにしようという動きがあって、最近になって中規模のセキュリティ教育をやっている企業 8 社がコンソーシアムを作り、コンテンツを良いものにしたり、教育の内容を認定する等している。また米国の SANS が日本に入ってきて、一緒にやろうと言う等の動きもある。しかし、いずれもニーズに比べて動きが遅く、小さい。

[池上]

もし国としてという言い方をすると、コンピュータエシックの話や、セキュリティの話をもう少し力を入れるという様な事か。

[佐々木（良）]

必要だと思う。大学と企業が協力する場を作る必要がある。大学は、従来企業がやっていた部分をもう少し丁寧にやらなければならない。企業は、又相互に入りこまないといけない。互いが重なり合う場がまだ足らないと思う。

[大木]

企業から言うと、事業環境は厳しく、育成するというよりも新たな技術を身に付けるのは本人任せになっている部分が多い。IBM にはメンター制度というものがあって、一人の先輩について同じ興味ある分野の指導を受けたり、テクニカルコミュニティを形成してその中で同じテーマでディスカッションする場があるが、実務に追われて時間を割けないのが現状だ。特に最近だと事業環境が厳しく、もっと実務をやれとのプレッシャーもある。セキュリティの様に変化が激しい分野だと、必ずしも適格なメンターが目の前にいないという事もある。また、セキュリティに関して企業をまたいで技術者が同じコミュニティで議論する事は、知的所有権や機微にわたる情報もあり、企業としてはなかなか難しい。国としての枠組みがあっても良いのではないか。学会の様なものがあって、企業の社員も入って行き易いような環境作りが一つのソリューションではないか。

[池上]
インターネットだと WIDE があるが、あれと同じようなものをセキュリティに関して作るのはいかがか。
[大野]
私は WIDE プロジェクトのボードメンバだが、WIDE プロジェクトに 600 人、700 人参加して、ある程度の足跡を残せたのは、面白かったから。何もない所から自分達で解決するというのが凄くエキサイティングだった。面白いものが無いと、学生も食いついて来ない。感動がないと、カリキュラムを作っても人が別の面白いものに行ってしまうのではないか。ちょっとしたファイアウォールを作って、繋いでお互いにせめぎあっている様な経験があれば凄く活きて来る気がする。
[飯塚]
先程土居先生が、こうしたセキュリティやソフトは知識集約産業であるべきなのに、労働集約産業と間違えられているとご指摘された事は、産業界側が反省しなければならない問題。同時に大学においても、先程来論議になっている OS、CPU、暗号、またその延長線上でなければ解決できないセキュリティ等が、本当にキーテクノロジとして、学生も認識出来ているか、あるいは大学でも充実しているかというとそうでない面もある。解決策はよく言われる通り、産学協同等で当面は解決するしかないが、大野さんが仰った様に学生自身も面白いと思ってチャレンジしてくれないと、人材が育たない。そのための盛り上げのアクションも非常に大事。
[池上]
バーチャルなものを作って皆でアタックさせるというのもあるのではないか。ソフトウェアの場合実証は難しく、何か国で何かやってもらえないかという意見がある。私はソフトウェアは芸術大学方式にやらないと人が育たないのではないか、要するに技術を磨いて、常にコンテストをしながら力を付けるという分野ではないかと思っている。その辺はお知恵を拝借していきたい。
[土居]
人材育成について IT 戦略本部が出しているもので e-Japan2002 があるが、人材育成は 3 つしか書いてない。その内の 1 つとして大学院の学生を増やそうという事がある。それは、フィージブルでない。要するに、国立大学が対象だが、教官ポストを増やすという事は一切書いていないが、情報だけに学生を増やすというのは学内で無理な制度。教師に関しては、ソフトウェアだけを取ると、国公私立大でかなり広くソフトウェアを取っても 130 人しかいない。これでは深掘り出来ないし、しつこくやりたくても出来ない。一番根幹の OS、コンパイラ等の人材はいなくなる。従って IT 戦略本部の作戦もそういう事を踏まえた上で、実際に我が国の人材育成が出来るような具体的なものを考えて頂きたい。
[池上]
事務局から言われた様に、個別技術について、例えば暗号について論文を書くのは良いが、セキュリティやシステムとなると弱いという事だが、ご意見はないか。
[岡本]
暗号というものは、元々最初符号から来ており、割とそちらの分野の人が入って来て始まったもの。定式化していてやり易い。全体的に捉えるとなると、大学だけではなかなか難しい。大学でセキュリティを教えていると、基礎的な事を重点的に教えているが、もっとアドバンストな所も教えないといけないと思う事もある。今度の人材育成はそちらを目指しており少し変わってきているが、どちらかと言えば、基礎に力が入っている。システム的な所は、企業とタイアップすべきところもあるが、足りなかった。
[池上]
企業というのは日本の企業か、それともグローバルな意味での企業か。
[岡本]
日本の企業。最近は大分システムのところもキャッチアップしてきたと思う。暗号で言えば、システムとして組んだ時に、個々は強いのだが全体としては弱いということもある。全体として破られない証明可能な仕組みについてどうやるか等が課題になっている。
[大木]
セキュリティについて、色々なプロジェクトに参加して一番重要になるのは全体のアーキテクチャを作る所。残念ながら日本では、このアーキテクトになる人材は非常に少ない。ファイアウ

ォール等の個別の分野では結構人材がいるが、全体を押さえる人材は非常に少ない。恐らくシステムセキュリティとはそういう事を仰っていると思うので、そういうものの見方が出来る人材を育てるのが急務。逆に若い人にとってプロフェッショナルになる分野の奥行きや面白さもそこにかなりある。そういった意味で、若い人にそういった夢を見て頂くという事も含め、そういう人材に向けての誘導が効果的かと思う。
[佐々木（良）]
　セキュリティシステムが弱いという事について、システムに関する論文が少ないか言うと、ここ 2、3 年で随分変わってきた。ただ、セキュリティシステムをきちんと設計出来る人は多くはない。色々な社会の仕組みにも問題がある。チーフデザイナーをきちんと決めて、その下でトップダウンで何かを決めるというのは、社会としてもそうなっていないし、そのための教育もなされていない。チーフデザイナーの育成が実際なされていない。社会全体の問題で、教育も考えないといけない。
[池上]
　残念だが時間になったので、色々ご意見はあるかと思うが、後は事務局で整理してご意見をまとめたい。足らない言葉が多々あると思うし、あるいはお気づきになった点があれば事務局にご連絡頂きたい。
[佐々木(元)]
　セキュリティという見地に立って、日本としてどういう要素技術は確保すべきか、そしてそのためにはどういう方策を取って行くのが適切であるかのご議論も大事だと思った。
[池上]
　それはまた個別に伺うので、宜しくお願い申し上げる。
[大山]
　具体的な方策に繋がる提言が一番重要な事だと思うので、今後とも具体的な提言を頂きたい。
[事務局]
　色々、またご提言をお願いするが、人材育成について、先程システムデザイナー、アーキテクトという話があったが、どういう領域の人材をどの程度増やさないといけないかというのを作成する参考のために、皆さんに、どの様なマトリックスを作成すべきか、またそれについてどの様な人材が必要なのかという案を頂きたい。また、企業の方に、現在セキュリティの人材はどういう人達がいて、足りてるのか足りてないのか、どういう所が不足しているのかという所を、お聞かせ頂ければと思っている。

以上