配布資料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
人材育成・資格制度体系化専門委員会
第３回会合議事要旨

１．日時　平成 18 年 10 月 13 日(金)　16：00～18：00

２．場所　内閣府別館会議室

３．出席者

[委員]

有賀 貞一 委員　(株式会社 CSK ホールディングス取締役)
大沢 彰 委員　(エヌ・ティ・ティ・コミュニケーションズ株式会社経営企画部 ビジネスモデル推進室セキュリティ担当部長)
筧 捷彦 委員　(早稲田大学教授)
木内 里美 委員　(大成建設株式会社社長室理事情報企画部長)
嶋崎 長三 委員　(財団法人日本データ通信協会専務理事)
知地 孚昌 委員　(岐阜県総合企画部次長(情報化推進担当))
西尾 章治郎 委員　(大阪大学大学院教授(文部科学省科学官))
藤本 正代 委員　(富士ゼロックス株式会社シニアマネジャー)
真瀬 宏司 委員　(株式会社パソナテック取締役会長)
松村 博史 委員　(独立行政法人情報処理推進機構理事)
満塩 尚史 委員　(環境省 CIO 補佐官)
和貝 享介 委員　(監査法人トーマツ)

(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
警察庁生活安全局情報技術犯罪対策課長
防衛庁運用企画局情報通信・研究課情報保証室長
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
文部科学省高等教育局専門教育課企画官
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

４．議事概要

(1)　先進的な情報セキュリティ技術・製品及び高度な管理手法の研究・開発者について

ア　トップエリート人材について

○　最近この分野では、国際競争力のある人材を作ろうという声が高いが、国際競争力のある人材を輩出していくような仕組みはあまりない。また、「国際競争力」と言った時に、海外に打って出て外貨を獲得するための高い技術か、国内産業全体を活性化するための高い技術かというところの定義づけが曖昧なまま議論されている。いずれにせよ、新しい創造性のある人材を輩出するには、長期間の教育プログラムが必要であるし、それほど多くの人が輩出されるわけではない。しかしながら、そういう非常に創造性の高いクリエイティブな人材が出てこないと、競争力があって海外でも売れる、あるいは、国内でも十分にベースとして活用できるようなものができてこないと思う。本当に秀でた人達を特別扱いして育成するというところが、日本の国民性にはあわないこともあるだろうが、社会の受け入れ方もなかなかトップエリートを作るような仕組みができていない。中国、韓国、ブラジルなど、エリート教育を続けているいくつかのモデルを見ると日本にもエリート教育は必要ではないかと感じる。従来の高等教育機関の枠組みを超えた何らかの育成方法を考えていくということも検討に値するのではないか。

○　エリート教育については、エリート人材が出ないかもしれないリスクを承知の上で育てると言われているところがあるが、研究者として進んでいった時に、素晴らしい研究者にはなれなかった人材をどうするのかということが課題としてあり、この部分を変える必要がある。具体的には、一部の研究者について、ビジネスでの活用ということを考える必要がある。研究者育成の過程で研究者にならなかった人達がビジネスで活用されることによって、ビジネスの世界がベースアップされると思うが、日本は海外に比べてそれが少ないと思う。

○　実は日本にはいい人材はいると思うが、ビジネスマインドがなさ過ぎるという問題がある。韓国、インド、中国などは、世界に商品を打って出ようという気持ちがあって、製品に出来る。日本には、凄くいいアイデアや卓越した技術を持った人材がたくさんいるが、製品になった験しがない。コンピュータサイエンスを学んだ上で、ＭＢＡも学ぶというようなコースを経ないと、本当の意味で国際競争力のある人材というのは出てこないと思う。逆に、ビジネスモデルを考えられる人材は技術力がなさ過ぎる。結局のところスーパー人材になってしまうが、トップエリートの育成のターゲットはそういうところだと思う。具体的には、世界的に有名なウイルス対策ソフトを打ち破ることができるような製品を作るということさえも考えることができる人材を作っていく必要があると思う。

○　トップエリートというのは研究者だけに限定されるのではなく、テクノロジーもマネジメントもきちっと理解しているトップエリートという意味だ。

○　国として新たなトップエリート養成機関のようなものを作るということまでは必要ないと思っている。なぜなら、最近は大学でも競争的資金による先導的人材育成があり、産学連携を色々やりながら、従来の枠からはみ出た形での申請を行わないと採択まで至らないということがある。このため、大学担当者は競争原理の中でエリート人材を育てる枠組みを作りかけており、今までの枠組みで、競争原理や先導的支援等に取り組むことによって、トップエリートの育成が可能ではないかと思っている。ビジネスモデルをきちんと持った学生の育成についても、今、大学ではインターシップをとても重要視しており、色々取組みを始めている。大学が問題に気づいて努力を始めている状況だと思うので、もう少しそれを伸ばす方向で目的が達成できるのではないか。

○　大学において今までと違う活動の兆しは確かにあるが、４、５年後に本当に望ましい人材が出てくるかということには少し疑問があると思う。一つには、教育側・教育者がどう変革されていくかということがよく見えないということがある。それからもう一つとして、大学の場合はカリキュラムが４年間の間に変えることができないという話を聞いたことがある。この分野については、毎年でも見直しながら必要な改訂をしていかない限り、本当にマッチングする人材育成ができないのではないか。そういった面がまだ色々残っている気がする。

○　大学のカリキュラムについてはもう少し柔軟にすることができると思う。
　トップエリート人材の問題というのは、情報セキュリティ分野のみに収まる問題ではなく、日本が科学技術の様々な分野でリードしていく上で議論しなければならない問題であり、様々な場で議論されている。この場は人材育成ということについて議論するところであるが、エリート校を作るべきだということに踏み込むよりも、今エリート教育が必要だという問題意識や、エリート教育に対する懸念や、アウトカムが社会にどう生きるのかということをきっちりした上での人材育成をしなければならないということを、しっかり議論したということを報告書に記載した上で、今後この問題に関する検討を様々な場でして欲しいという形で報告書に反映することとするということではどうか。

(2)　政府機関、企業等の組織に対して、情報セキュリティに関する製品・サービス・ソリューション等を提供する企業等における人材

ア　全般について

○　地方での拠点の整備や、地方公共団体での人材育成については、ソフト（人材育成のスキーム）とハード（地方での拠点の整備等）の連携をしないと、あまりアピール

のあるメッセージにはならないと思う。過去にもハードだけを整備して赤字になって苦しんでいるところもある。育成方策や資格制度の活用など総合的な取組みもしないと意味がないと思う。

○　セキュア・コーディングができない開発者がいて、欠陥のあるプログラムを作ってしまうという問題については、セキュア・プログラミングの教育を行うことも必要だが、システムの開発環境で欠陥のあるプログラムを作ることができないようにするなど、作ったもの自体がセキュアなものかどうかをチェックする仕組みが考えられる。開発者全員のレベルを高めてセキュアなことをやるようにというのは無理だと思うので、半ば強制的なそういう仕組みが必要だと思う。海外では既にそのような製品があるので、そういったものをきちんと使わせるという教育も必要だ。

○　ＩＴという切り口で都会と地方を見た時に、都会でしか市場や技術者やニーズがないということではなく、日本全体としてセキュアな社会を作っていくという観点で見れば都会も地方も同じであり、やはり地方においてもある一定の水準でスキルレベルを上げていくことが必要だ。日本全体としてセキュアな社会をつくっていくためには、地方に対しても投資するという役割を地方公共団体は負っていると思う。従来型の企業誘致という形ではなく、新たな産業振興の中の底上げという観点で、ＩＴや最近話題のセキュリティというものも一つの切り口で、取り組むべきことだと思う。

○　地方公共団体の人材育成の取組みについては、従来は、資格の取得件数や研修の数や研修の参加人数等がターゲットになっているが、本来の目的は、その結果としてその人が就業するということだと思う。結果として就業者が何人出たかという捉え方をしている取組みであれば、それは非常にいいと思うので、それについては報告書に記載するべきである。既にいくつかの地方公共団体で実績もある。

○　セキュリティに関する製品等を提供する人材等を各地域で確保する必要が本当にあるのか。利用者側にある程度の専門性を持った人材を育成することについては否定するつもりはないが、プロ側の人材を各地域が育成しなければならないのか。

○　日本全体としてセキュリティに取り組む際に、ＩＴに対して大きな投資を行っている都会の大手だけがセキュリティを守っていて、地方は守らなくてもいいという話ではないし、セキュリティに関する製品等を提供するのは都会のＳＩベンダだけで、地方にはそういう業者はいらないという話ではない。地方でも、地元のベンダを１０年以上かけて育てて上場企業を出すなどしている。そういう観点で、ＳＩベンダというのは別に都会のものだけではなく、地方公共団体の取組みについても報告書に盛り込むべきである。

○　地方公共団体の取組みは、ユーザ側に盛り込んでもいいのではないか。各地域の判断で情報セキュリティに関する製品等を提供する者を育てるのは構わないが、全ての地方で一般的に育成・確保する必要がある、ということまで提言するのか。過去にも、地方で暗号やセキュリティに関して相当有名な会社があったが、結局マーケットを掴みきれずに潰れたということがある。

○　逆に地方にしかできないと思っている。地方に住んでいる人間からすると、東京のベンダは全く信用できない。システムを構築するだけであとはいなくなる。セキュリティについては常時維持管理してもらう必要があり、そのためには、地元の企業にしっかり頑張ってもらわなければならない。

○　セキュリティを専門に扱うベンダと一般の SIer の話が少し混同しているのではないか。システムを構築している地方の一般の SIer にも是非セキュリティの知識を持ってもらいたいとは思う。他方、セキュリティ専門の SIer が地方に必要かということについては特段の考えはないが、いずれにしてもそれらを分けて記述するべきではないか。

○　都会対地方という話ではなくて、地域によって大きく差があり、その結果、どうしても動かない地方公共団体があるなど、なかなかうまくいかないという実態がある。そのため、地方公共団体の取り組みについては、過去にうまくいかなかったことの反省を踏まえて、ソフトと一体的に取り組むということをかかないと、説得力がないと思う。

○　科学技術振興調整費のプロジェクトの一環のプログラムを推進していた時に、産業界から色々な方々に講師として来ていただいて、一般の企業で本当にどういうことがセキュリティで問題になっているかということを学生自身が如実にする機会があり、その効果や影響は絶大であった。このような教育プランでこそ、そういった産学連携は重要だと思うので、教育プログラムの充実について産学連携という観点をもう少し強調して欲しいと思う。このことは、トップエリートの部分にも繋がると思う。

イ　管理系の製品等を提供する企業等における人材について

○　コンサルティング会社やセキュリティ監査を行う企業に従事する者については、基本的には技術系の製品等を売る者と同じような知識・経験を持つことが必要だが、それに加えて指導的あるいは批判的な視点が必要であるということで、別個に検討しなければならない。このような事業者における人材育成というのは、基本的に各事業者がそれぞれ行っており、指導的あるいは批判的な視点についても、一般のセキュリティ技術の部分に加えて、企業内ＯＪＴでやるような形になっているのが現状であると

思う。今後、例えば情報セキュリティ監査制度ができて、一定のレベルの能力・経験を持った人材が社会的あるいは公的に必要だということが明確になって、現状では各事業者任せになっているところについて、例えば制度を維持するのに不足があるということであれば、それについては事業者任せではなく、ある一定の育成プログラムや施策が必要になるのではないか。

○　今の日本の企業の中でこういう管理系のことをやっている人達というのは、まだまだ勉強しなければならないことがたくさんあり、どうしてもコンサルタントに頼ってしまうという現状があるため、コンサルタントや情報セキュリティ監査を行う人達の能力というのは非常に重要ではないか。しかしながら、どのようにして育成するのかということについては、この人達よりもスキルのある人達がいないと育成できないので難しく、支援等を行う必要があると思う。また、海外でより優れたものを知る機会を与えたり、同業の人達が集まって情報交換をして成長していくような場を与えたりするなど、様々な方策があると思う。

○　人材育成のモデルを考える時に、例えばエンジニアリング系であれば、研究開発・技術開発の現場があり、それと体系化された人材育成やスキルに関する空間が定義されており、教育機関や教育プログラムと現場の間でのすり合わせのモデルがうまくいっているところがあるだろう。米国型の場合、管理系のところにも同じような構造があり、研究機関等の周りにいる研究者達が活躍していて、それに対して業側が研究者達を入れた時のベネフィットがあるからということでうまくサイクルができている。日本の場合、このサイクルがうまくできておらず、ここのところの方向づけが一番難しいと思う。ＯＪＴというまだ完全には体系化されていない知見がある意味で体系化されて、パブリックに出て行くというメカニズムがない現状に対して、これを後押しするものは最終的にはどのようなモデルになるのだろうか。制度による後押し、あるいは海外の事例を持ってくるものもあるだろうが。研究・教育という今までの大学のようなところと企業のところの関係になるのか、それとも、監査等の制度側が運営するのがいいのか、それとも、完全にマーケットに任せるということでいいのか。そこのところを見えるようにしなければならない。

○　我々が、外部監査を受けた際には、東京のかなり技術力のあるコンサルタント会社にお願いした。そういったところまで地方でできるとは思っていない。会計を中心とした経営上の事業目的など狙いや目的がはっきりしているものに対するコンサルタント会社はあるが、セキュリティに関してのコンサルティングということを考えると、セキュリティを専門とした時に、コンサルタントのアウトプットが何かということが一般的にははっきりしていない。我々が専門会社にお願いしたのは、個人情報保護条例の話や社会的に騒がれてはいけないという話など、そこの部分だけをチェックしてもらったが、これが一つのコンサルタントのプロセスだと思う。例えば外部侵入とい

う技術的観点で見ると、最新技術を持っている専門的な会社でなければできないであろうという観点と、社会的な問題について日本でもアメリカでも様々な事例が出ており、その中で色々な経験を持っているところにお願いするのが一番いいだろうという観点で、それなりに目的は達成したと思う。セキュリティポリシーや内部監査の規定の有無等の管理系の項目だけでコンサルタントをやってもそれほどの目的は達せられないと思う。今述べた２つの観点は今日現在ニーズがあるところなので、そこからもう少し経営面まで発展していけば、ますます高度な技術が必要になってくるのではないか。

○　コンサルタントや監査というと、技術は関係ないという印象が日本では強く、だから良くない。コンサルタントや監査といえども、情報セキュリティ技術の最先端を理解している必要がある。アメリカあたりでは、コンサルティング会社においても先端の技術を理解している人達が相当おり、うまくいっている。しなしながら日本の企業はそういう最先端の技術がわからないので、規定類の有無を聞いたりしてごまかそうとするので良くないと思う。コンサルタントや監査については技術の最先端のところを逃さないような記載をすべきである。

○　技術を知らないコンサルタントというのは結構いる。もちろん管理系の話がメインであるということは間違いないが、技術系のところも知識としてはある程度知っておいて欲しい。セキュリティの管理に関しては、やはり最終的にはＩＴが関わってくるが、管理の部分は今までは業務系の話なのでＯＪＴでやってきたところが大きいが、それをもう少し経営工学的にというかシステマティックに整理したいと思っている。そこまで話が行ってしまうと、教育・人材というよりも、研究の話になってしまうかもしればいが、そういうところが進んで欲しいと思う。

○　このコンサルタントや監査の問題については、高度な情報分野の技術を持っている人でないといけないということであり、その他にこれまでの各委員の意見を整理して報告書に記載するべきであると思う。

○　コンサルタントや監査について、技術的な部分がいるというのはそのとおりだと思うが、情報セキュリティの性格上、重なり合っている領域が非常に広い部分であり、必ずしも技術というものが前面に出れば全て解決する問題ではなく、人事や労務管理など幅広いものが必要だということだと思う。一人でそれらを全部カバーするのも難しく、かなり人に依存する部分があると思う。

○　幅広いものが必要だということがベースになると思うが、必要な技術的なものをきっちりと持っている人でないとだめだということだと思う。

ウ　企業等における人材の育成を図るためにソフトウェア事業者について新たな規制の導入を求める意見について

○　ソフトウェア事業について、何らかの基準を満たさない事業者については事業を認めないというような新たな規制を設けることについては、基準を満たすかどうかの判断はユーザ企業が自らの責においてやるということと、規制を拡大することは世の中の流れに逆行するということから、反対だ。今、ベンダ・SIer も競争が非常に激化しており、仕事はたくさんあり、丸投げしているところも確かにあるようだが、そういう事業者は、ＳＯＸ法や派遣法や業務委託やコンプライアンスの問題等で、非常に急速に淘汰されると思うので、規制の導入ということは問題提起が少し違うと思う。逆に言えば、そういう問題は事業者が自分たちで考えるというものにすべきだと思う。

○　ごく最近、セキュリティを専門にするベンダが、大きなファイルをネット上に投げたため、ネットワーク障害を起こしたということがあり、実はこのベンダは昨年にもバグのあるファイルで大きな問題を起こした。結局、組織活動の問題が多く、この事例でも内部のマネジメントがきちっとてきでいないし、改善がされておらず、現実として同じことを繰り返している。こういった組織活動の問題が行き着くところが人材育成であろうといつも思っており、目に余る品質管理の問題に遭遇することがかなりある。建設業法や建築士法のようにある一定の水準にものを見ていかないと、品質管理一つをとってもはっきりしないのではないかということから、規制の導入を提案した。建設業は、登録業者でなければ建設業はできない。公共事業の場合は、経営事項審査があり、経営の状況や技術者の情報を含めてポイントがつけられてランキングされ、それによって入札資格が決められたりする。また、一定金額以上の工事を行う場合には、施行体制台帳という形で下請け体制も全部開示する必要がある。行った仕事の成果も点数で評価され、それが次の入札に影響する。そういう規制の中でも現実には品質管理の問題が起こったりするが、今のソフトウェア構築の状況を見ると、あまりにも自主管理機能がなく、品質管理の仕組みも良く出来ていない。品質管理のやり方のアイデアは色々ある。企業内でもやる方法はたくさんあるし、客観的に品質管理を専門的にやる人達の集団を置いて、きちっと見ていくというやり方もできるはずだが、実際にはやろうとしない。そういったものはプロ側任せになっており、非常に属人的な感じがするため、なかなか品質の担保ができないというようなことが起こる。こういった企業内のマネジメントの悪さは、自主的な改善に期待していては、良くならないと思う。日本の国内では淘汰は起こらないと思う。淘汰が起こらないので、日本の独特の商習慣と環境に守られて産業が育ってきており、改善機能がなかなかないため、何らかの形で規制のようのあものを導入しないとしっかりしてこないのではないか。

○　発注者側がセキュリティに対するレベルも含めて、明確にサービスレベルをどうい

うところまで期待しているのかということで、発注者側がセキュリティに対する考え方をもっと勉強して、発注者側が責任を持ってやるべきではないか。全て受注者側がやるということではなくて、発注者側、受注者側のそれぞれの考え方で解決すべきであると思う。

○　よく発注者側の問題として、要件定義がきちっとされていない等のことが挙げられる。実態としては、少なくとも要件をきちっと出さない限り、きちっとしたものが提供されないのは当たり前だ。しかしながら、細かな仕様まで求めるようなところがあり、それは提供側のエンジニアリング能力が不足しているからだと思う。つまり、提供する側が提案力を高めれば、細かな仕様まで出さないときちっとしたサービスを提供できないということはないとおもう。一般の人が住宅を建てる時に、要件定義はきちっと出すと思うが、詳細な仕様を出して住宅を発注することはないはずだ。ハウジングメーカーの場合は、きちっとした提案をし、最終的に合意形成に至っているはずなので、そういう意味での提案力やエンジニアリング能力を高めて欲しいと思う。現実的にはなかなかうまくいかないので、ユーザ企業としてはやるべきことをやるという面での力を付けて欲しいと願っている。

○　この委員会のミッションとしては、人材育成の観点であるので、規制について明確に出すことについては、非常に苦慮すべきことだと思うが。

○　規制の導入についてはこの委員会の報告書に盛り込んでも仕方がない気がするが、絶対に賛成だ。一見、情報処理サービス業会には厳しいことになるかもしれないと思うが、長い目で見ればそのようなことにはならない。事業をやること自体の許認可をするかどうかということは別の問題として、自分たちのやった仕事の品質や信頼性がきちっと担保できないような仕事は仕事だと思わない。２０～３０年前ならそれでも良かったと思うが、この業界もできてから４０年経っており、４０年も経った業界で、品質基準や信頼性基準やそれが計測可能かどうかわからないようなものは業だと思っていないので、システム関係に従事する者に対する規制について検討はすべきであると思う。しかしながら、ここでは規制の議論は盛り込まない方がいいかなという気はする。

○　この委員会の目的としては、どういう人材が必要なのか、あるいはその人材のスキルのベースをどのように図っていくのかという議論をしようという中で、ソフトウェア産業のあり方についてどうあるべきかということについては、大いに議論があるところだと思う。しかしながら、この委員会のミッションとして、ソフトウェア事業やそれに関わる産業に対して規制を設けるかどうかということを報告書に記載するのは少し筋が違うと思う。規制によってセキュリティ人材を育成しようという議論展開をするのであれば、規制議論だけしていればいい。しかしそうではない。製品をいくら

良くしても、やはり人材をどう育成していくのかということを考えなければならず、それをここで議論しようということだと思うので、議論の順番が違っており、規制の導入については報告書に記載すべきではない。

○　規制の導入について問題提起があったということは報告書に記載するが、規制そのものが人材育成のところを密接に関連していくような形での記述は控えるということでどうか。

○　規制の導入については、報告書に記載して欲しいということではなくて、人材の育成に係る資格のところで資格制度を一通り提案した上で、それとは別に情報分野に情報システム構築に携わることができる技術者の業務認定資格が、建設分野での建築士と同じような概念で、これによって業務の適正化や質の向上が図られるのではないかと思うが、文言で記載するというよりも、そういうことについてきっちりとご議論いただきたいということだ。

ウ　現在提供されている情報セキュリティに関する各種資格制度の評価について

○　この議論は、どの試験に対する議論なのか。一般のプログラマ向けの資格における情報セキュリティ要素の追加というのは、既に網羅的にセキュリティ関係の設問が追加されているものについて、さらに検討すべきということなのか。また、新たな資格制度の創設については、これから始まる国のＩＴ試験の制度改正に向けてのこの委員会としての提言ということになるのか。

○　現在提供されている各種資格制度への提言部分については、特定の制度・試験・資格制度に対して注文をつけるという趣旨ではなく、どちらかというと広く一般的にセキュリティに関しての要素を追加して欲しいということを見て欲しいという願いを書いているところである。

○　そうであれば、資格における情報セキュリティ要素の追加というのは、プログラマ向けの資格に限定しなくても良いのではないか。

(3)　情報セキュリティに係る人材の育成に向けた具体的な取組みについて

ア　資格制度等に関する取組みについて

○　官民の役割分担の観点で言えば、民間の資格制度や教育プログラムも数多く出てきているところであるので、民間でできるところは、今の時流から言えば、当然民間でやっていくんだろうなという感想を持つ。ただ残念なことに、海外からの受け売りの

輸入型のものが非常に多いので、もう少し日本の民間企業で頑張っていいものが作れないかなということを感じている。

○　例えば有名なベンダのデータベースの資格の試験に受かったからと言って、正規化されたデータベース設計ができる技術者というのはほとんどいない。同様に、例えばブラウザのセキュリティの設定はできても、セキュリティの一般論についてわかっている人はほとんどいない。そのため、ある意味で大学が本来はきちっとやるべきところを、この３０年ぐらい国家試験が担ってしまっているところがある。そういう意味で、一般的な知識・技術を汎用化・一般化して問うようなところに今の試験の意味はある。ハイレベルな資格を取っても、基礎の基礎の部分をわかっていない人が多いというところが、この業界や仕事をしている人達の問題だと思う。国家試験の意義の有無を言っている人がいるが、試験そのものを受けたこともなく実態を知らない人達が言っていることが多いということと、業界で同様のことを言っている人がいるが、過去数十年に渡って、ユーザ企業や学生よりも業界の合格率の方が低いのが現状であり、今すぐに国家試験の代替になるような手立てがないというのが現実だと思う。

○　今、大学の話が出たが、大学についても考える必要がある。情報処理学会でも専門教育学科の学生をどうするのかという議論はあるが、世の中は全部それで動いているわけではない。今は、大学卒の人が５０％を超えており、その人達が社会のある意味で基幹部分を担っているため、学部のいわゆる一般教育の部分が大事である。大学で理工学部を出ているのはわずか３割で、その中のわずか１割しか情報学科はいないので、専門学科の学生というのは３％しかいない。トップ向けにはそれでもいいのかもしれないが、学部の一般教育の部分がこれまで抜けていた。情報処理学会もやってこれず、大学側のテンポが遅い中で、ある意味で情報処理技術者試験が若干インセンティブになっていたりする。そういう意味で、その部分について何らかの言及をすべきだと思う。

○　組織の内部に情報セキュリティ担当者とあるが、内部監査についても考える必要がある。マネジメントのところで、外部監査や監査企業や監査人が出てくるが、実は、企業や政府の内部には、内部監査という組織があり、これは非常に重要だ。情報セキュリティ担当部門というのは、セキュリティの対策・施策を実施させる部門であるが、うまくいっているかどうかということは内部監査部門が実施し、その能力は外部監査と同様に、一般の技術的な知識の他に監査の視点が必要であるので、別枠で記載することが必要なのではないか。

○　資格制度の官民の役割については、必要・不必要について議論をするよりも、望ましいことや棲み分けなどについて書いていけばよいのではないか。

○　更新制や継続教育に関しては、更新制の方が望ましいと思うが。

○　国としてセキュリティ人材、広く言えばＩＴ人材というのを、どの分野でどのレベルでどれくらい必要かということを示す必要があるのか否かということを考えないと、官民の役割分担については結論が出てこないのではないか。最低限の知識を身に付ける資格制度の創設という意見があるが、その部分をカバーする資格制度がなくて国の施策として必要であれば、国の資格制度としてやるべきではないかということになるのではないか。この部分が民間でないということはコマーシャルベースに乗らないからではないかと思う。しかしながら、国の政策として必要だということであれば、この委員会として提言をするのが筋ではないか。

○　必要な人材を数として出すのは難しいのではないか。

○　一般論として国の試験の位置付けとは何であるかということだ。あるべき人材像を実現するための手段という位置付けだと思う。

○　国家試験の位置付けというものに対しての基本的な考え方を示していくということが一つだと思う。また、デマンドについては、マーケットサイズという問題が出てくればいいが、それは国家試験という考え方がそぐわないのであれば、そこに関しては制度上必要な点をどういうふうに変えるかということに言及するということではどうか。

○　国の戦略として人材を増やしたいということが目的であれば、資格制度を創設したら、それを活用するということも戦略の中に入っていないといけないと思う。

○　実は、産業構造審議会の答申を踏まえて、試験の継続性やあり方を含めて人材育成のワーキンググループが立ち上がる。そこで、要望・要求をまとめて、そういうところにぶつけていくのがいいのではないか。

○　ユーザ組織側の情報セキュリティ対策実施者の中に内部監査人が入ってくるのは良くないので、分けるべきだと思う。

○　民間部門においては、「職員」という言葉よりも、「社員」という言葉の方が適当だと思う。

○　保証型監査という言葉は外部監査という言葉にした方がいいと思う。

○　教育・資格制度の表を作る時に、細かいものをどこまで拾うかということについて

基準がある程度明確にならないと議論のしようがないと思う。

○　教育・資格制度の表を作る時にどこまで拾うかというところについては、クライテリアを設けるとそれについてのどこまで行くのかという議論が始まる。国や公的なものを入れるのは当然だとしても、民間のものについては線引きが非常に大変で難しい。

○　情報セキュリティ対策や人材育成の様々な資格について、今現在起きている社会的なセキュリティの事件が全部対策になっているのかという観点で見ると色々な観点がある。例えば、教育現場で生徒用のパソコンは全部与えても、先生に対して一人一台パソコンが与えられているということはなくて、先生たちが家に持ち帰って Winny で流出事故を起こしている。それに対してどうすればいいのかということや、ブロードバンド社会で、一般商店主がホームページを作ったり、子供が３歳からインターネットを触っていたりする時代において、「本当にセキュアな社会を作っていくためにはどうすればいいのか。」と言ったときに、資格以外の何かについても考える必要があるのではないか。

○　この委員会では、義務教育の部分についての議論は最初からしないということにしているはずだ。

○　最近 Web2.0 という言葉があるが、そういうソフトをカスタムメイドするとか、それぞれのところで個別に開発するという方向性には向かわない、若しくは向かってもどうしようもない時代になっていると思うので、リテラシーレベルを上げたり、教育方策で何とかしたりするというよりは、出来合いのセキュアな製品しか使わないといいような方向で考えていくしかないと思う。

○　スキル項目の分類については、何かを参考にして作るのであれば、その旨を示した方がいいと思う。

－以上－