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2回会合議事要旨

１．日時　平成 18 年 9 月 15 日(金)　13：00～16：00

２．場所　内閣府本府第３特別会議室

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)
内田 勝也 委員　(情報セキュリティ大学院大学助教授)
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)
田島 優子 委員　(弁護士)
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

４．議事概要

(1)　資格制度運営団体ヒアリング①

○　(ISC)^2 ジャパンより資料２に沿って説明。

(2)　資格制度運営団体ヒアリング②

○　ISACA 東京支部より資料３－１及び資料３－２に沿って説明。

(3)　地方自治体における情報セキュリティ人材の確保について

○　知地委員より資料４に沿って説明。

(4)　日本経団連アンケート結果報告

○　事務局より資料５－１及び資料５－２に沿って説明。

(5)　政府機関実態調査結果報告

○　事務局より資料６に沿って説明。

(6)　討議

ア　「情報セキュリティ人材」のカテゴリについて

○　「２００７年問題」で出てくる人達を有効活用するための方策を検討してもいいと思うが如何か。

○　システムプログラマーと呼ばれていた脆弱性テストを行うような人達はユーザ側にもいる必要があると思うが、そのような人達をどうするのかということを検討する必要がある。

○　ユーザサイドにおいてマネジメント系を中心に考えすぎていると思う。セキュリティ技術者とまでは言わないまでも、もう少し技術的な部分も入れた方がいいと思う。

○　昔はユーザ側にもシステムプログラマーは多くいて、ＯＳのバグフィックス等を行っていた。しかしながらＷｅｂ、クライアント・サーバの時代になって、そういう人達がいなくなったのは大きな疑問である。そういう発想をもう少しユーザサイドに植え付けていく必要がある。

○　「ＳＩｅｒ、ベンダ」の部分の人材の教育・研修やキャリアパスを考えるに当たっては、「ＳＩｅｒ、ベンダ」の部分についてもう少し具体的なフォーカスをした方がいいのではないか。セキュリティに関するコンサルテーションとかＳＥとか営業とかそういうことではないのか。

○　「セキュリティ・プロバイダ」の部分についてだが、製品を作って提供する人とそれを売る人では完全に技術レベルが違うので、その違いをはっきりさせないと、どういう人材像を意図しているかがわからなくなると思う。

○　セキュリティ専門のＳＥではない一般のＳＥでも知らなければならないセキュリティというのがあると思う。専門家がいる場合もあれば、一般のＳＥがユーザサイドにいる場合もあるので、そういう一般のＳＥの部分を分けて考えることも必要だと思う。それによって取得する資格制度も違ってくると思う。

イ　高度・先進的な技術の研究開発者について

○　国の力となり国の方向付けができるような、高度・先進的な人材の育成が、現状でできているのか疑問である。特に、従来の枠組みの教育システムの中では、そういう人達はなかなか出てこないと思う。さらに、そういう人達を受け入れる企業や研究所などの社会側の仕組みがうまくいっていないのではないか。このカテゴリの部分が国策として一番不足しているということを感じている。

○　この部分は長期的なオーダーで見る必要があるし、２０～３０人を育てても１人しか出てこない可能性があるかもしれないという認識を持つ必要がある。しかしながら、この部分について何もしないで済むということはないと思う。1 つとしては、ポストＣＯＥでセキュリティを少しやって欲しいということがあるが。

○　ポストＣＯＥについては、グローバルＣＯＥで分野を限らずということで公募でいいものを採択していくというスキームの他に、特に重要な部分については、ある程度分野を限って同様の手法をとるということも考えていきたい。

○　情報セキュリティに特化した高度なマネジメント技術のようなものが、この部分に入ってくるかどうかが見えにくい。

ウ　セキュリティ製品等の提供者について

○　セキュリティ・プロバイダではない一般のＳＩｅｒがある程度知っておくべき事項画あるという意味で、このカテゴリについても議論する必要があると思う。

○　このカテゴリに教育サービスというのが入ると思う。企業に対するアンケートの中で、民間の教育サービスへの期待が大きかったのは、そういうところにアウトソーシングすることによってコスト削減ができるところが多いのではないかと思う。

○　資格制度の体系化にあたっては、民間の試験制度と国の試験制度があるが、民間でやるべきことは何か、国でやるべきことは何かということについて真正面から議論をして欲しい。

○　国の試験制度については、民間のものと一律に議論するのではなく、量的拡大や全国網羅性やクラスごとの適正な実施等について、どこまで国がカバーするべきかという視点で議論するべきである。セキュリティ人材について、どういう分野のものをどういうふうに育てていくのか、その手段として国がやらなければいけない試験の仕組みはどういうものかということも議論して欲しい。

○　資格制度の体系化にあたっては、レベル感についても議論する必要がある。

○　「アプリケーションを開発するＳＥが」という部分があるが、プログラムの経験がないＳＥが増えているという実態との乖離感がある。これについては、企業内教育のあり方が極めて重要な問題であると思っているが、そういった問題がここでどう解決されるのかが見えにくい。資格試験はあくまで知識レベルの検証でしかなく、実際にどう対応できるかということとは別だと思うが、そことの位置付けがよく見えない。

○　情報産業の現状は品質担保の仕組みが何もない。建築士のような資格制度もある。必要な規制であれば、産業全体に規制をかけるべきだと思う。

○　ＯＪＴというのは何もやっていないということと同じではないのか。ＯＪＴを実施しているという企業や、ＯＪＴで十分だと言っている企業が多いが、ＯＪＴを実施するために必要な知識が不十分なのにできはるはずがないだろうと思う。企業内の教育の部分をもう少し明確に出す必要があるのではないか。

○　高等教育機関の中に、来年度で事業が終わる予定の大学が含まれている。また、既に事業が終わってしまったものの中にもいいものがあるので、その辺りの整理をしておいた方が良い。

○　監査には助言型と保証型がある。保証型の場合は、信頼性のために一定レベルの監査人であることを保証する必要があるので、規制になるかもしれないが、そういう方向が打ち出されると思う。そうすると、セキュリティ・プロバイダの中に監査人が入っていることについて少し違和感があり、外に置くべきと考える。

○　監査人が行う保証型の業務については独立性を守る必要があると思う。

○　地方の情報産業では、レベルを上げることによって実際に仕事を得ることができる

かどうかということを気にしているので、地方のレベルの上げ方を検討する際には、こういうモチベーションの問題を考えていく必要があると思う。

エ　セキュリティ対策の実施者について

○　高等学校からの教育というのは、長期的に考えれば、一般職員のみでなく幹部や高度・先進的な技術の研究開発者についても当てはまるということを考慮する必要がある。

○　トップを育てるためには、新規に参入してくる人達、つまり若い人達へのすそ野からの教育を行わなければならない。ただし、その内容は、今やっている情報リテラシー教育のレベルではだめで、「情報とは何か」ということをセキュリティも含めてしっかりと含める必要がある。

○　実際の業務内容から言うと、実施責任者は、セキュリティの技術は技術として、誰が専門知識を持っているかということだけわかっていればよく、その部分については外部委託するか内部で育成するかすれば良い。

○　危機管理の問題では、問題があった時に幹部が頭を下げることになるということを、具体的な事例を出しながら幹部に説明することが非常に効果的である。

○　行政機関においては、今まで紙で行っていた業務処理が、電子化されることによって、紙では許されていた管理の甘さが、電子によって少し意図的なものがあれば、必ず情報セキュリティの問題が発生するということを認識させることが一番である。また、外部の専門家を雇うことは短期的に効果があるが、ＣＩＳＯが変わっても定常的に回していけるのかということもある。そのためには、セキュリティ・プロバイダが把握しているような実践的な具体例を集約していく仕組みがあればと思う。

○　各主体が、２、３年後に情報セキュリティのレベルをどこまで持っていくのか、そのためにはどういう人がどれだけ足りないか、それを解消するためにはどういうツールを使うのか、といったことを明確にする必要があると思う。

○　幹部については、意識付けに留まらず最低限の知識を知っておいてもらわないと、行き過ぎた管理をしたり、無関心になってしまったりするといったように、濃淡が出る恐れがあるので、幹部が知るべき知識の標準をセットする必要がある。

○　一般のユーザ企業の情報システム部門にも濃淡があるので、それを考慮して欲しい。

○　「セキュリティ対策の実施者」の育成にあたっては、受益者の方を向いた教育をどのように行うのかということを議論して欲しい。

○　経団連のアンケートは、対象が経団連の中でも情報通信委員会の参加企業に対するものであり、意識が高いことは当然で、上澄みのところを対象として評価していることになるので、こういったデータをベースに考えると間違うのではないか。

○　企業の中でセキュリティに関する技術者は当然必要だが、ＰＤＣＡを仕組みとして回せるかということが非常に重要なので、それができる人材を作らないと効果が出ないと思う。

オ　資格制度の体系化・教育プログラムの在り方について

○　監査関係の資格の部分で「公認」という言葉が使われているが、政府が公表する文書で「公認」という言葉を使うと誤解を受けるおそれがあるので、十分に注意されたほうが良いと思う。

○　試験のみの資格でも、受験者・合格者に実務経験の長い人が多くを占めているなど、実質的に実務経験を問うている場合もあるということを考慮して欲しい。

○　資格制度のマッピングを作るというのは非常に難しい。民間試験は栄枯盛衰もあるので、公的機関としてどこまで公表するかを考えると悩ましい。とりあえず、この辺りは公表資料からは落としてはどうか。

○　資格制度についてはあまり参考になるものがなく、マッピングの図等を示すことについては意義があると思うが。

○　資格制度のマッピングについて、機能図にするのが１つのアイデア。

○　それぞれの求める人材が、どの資格を持っていればいいのか、どの教育を受ければいいのか、ということがわかるような図を作ればいいのではないか。

○　新しい資格試験を作るということや資格試験の中身について議論することは非常に難しいと思う。機能面や要素面をしっかりさせて、それを備えた人材を、ある一定の量・規格・レベルで育てるという方向で議論を進めた方が良いのではないか。

○　産構審で、ユーザ側のスキル標準とマッピングを含めて試験制度を見直すという動きが始まるので、そちらとの連携も検討するべきである。

○　公的認定資格の必要性の有無についてある程度議論をしておいた方がいいと思う。

○　政府機関における情報セキュリティ人材の育成を検討するに当たっては、定員削減が求められる中で、本当に公務員が情報セキュリティに関する業務をやらなければならないのかということを検討して欲しい。また、「監査法人」というと、公認会計士法上の監査法人というイメージがあるので、「監査企業」とした方が良い。

－以上－