資料10

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1回会合議事要旨

１．日時　平成 18 年８月 30 日(水)　14：30～16：30

２．場所　内閣府本府第５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)
関口 和一 委員　(日本経済新聞論説委員)
田島 優子 委員　(弁護士)
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)　委員長の選出

○　西尾委員を委員長に選出

(2)　西尾委員長挨拶

(3)　会議の公開等について

○　事務局より資料３について説明。資料３の案のとおり了承。

(4)　我が国政府の情報セキュリティ問題への取組みについて

○　事務局より資料４に沿って説明。

(5)　情報セキュリティ人材の育成に向けた検討

○　事務局より資料５－１、資料５－２、資料５－３に沿って説明。

(6)　情報セキュリティ人材育成・資格制度について

○　内田委員より資料６に沿って説明。

(7)　情報セキュリティ人材（高度 IT 人材）の現状と今後の課題

○　真瀬委員より資料７に沿って説明。

(8)　情報処理技術者試験制度について

○　松村委員より資料８に沿って説明。

(9)　自由討議

○　人材育成という言葉には広い意味がある。経営者への再教育・意識付けのようなものと、将来を担う若い人の育成のようなものとに分けて考える必要があるのではないか。

○　事務局の説明では、対象を政府機関とそれ以外に分けて検討を進めるということであったが、重要インフラについてはある程度政府の影響力が及ぶので、分けて考えるべきである。また、民間（特に中小企業）は情報セキュリティに対する意識や余裕がないところが多く、意識を高めることがポイントになってくるため、政府機関や重要インフラとは全く違ったアプローチをとる必要がある。以上のことを踏まえて、政府機関・重要インフラと大企業・中小企業に分けて検討を進めるべきである。

○　資料５－１の３ページの３つの分類は、研究開発者・プロバイダ・一般組織という考え方であると思うが、教育の問題としては、それぞれ、教育・訓練・周知という考

え方をしないといけない。

○　資料５－１の３ページの①のような人材を作っても、働き口がないのではないか。そういう面では、情報セキュリティ全体に関してブレイクスルーがないことが非常に大きな問題であり、それを踏まえて検討する必要がある。

○　資料５－１の９ページのＡタイプ・Ｂタイプについては、大企業と中小企業という位置付けをしないほうがいいと思う。小さな企業でも e-ビジネスを行っている企業などでは情報セキュリティが非常に重要であり、CISO に当たる人間を必ずおく必要がある。

○　アプリケーションプログラムを作る人材については、セキュア・プログラミング的な部分がこれから非常に重要になってくると思う。

○　情報セキュリティの確保にあたっては、各々の事象に対応するという考え方ではなく、全体的なコンセプトをまとめた上で対応しないと対応できない時代になった。このところについては、法律を作って規制するのが一番いいと思う。特に重要インフラについては、高度な検査や検証、さらには構築する人間の資格についてある程度規制しても良いのではないか。安全・安心を売りにしている日本の国家として、そういう方向性を踏まえながら議論をすべきである。

○　情報セキュリティ担当者には、マネジメントやコミュニケーションのスキルが非常に大事だ。

○　情報セキュリティの問題は、システム部門の問題と捉えられがちだが、実態は、全体のリスクコントロールの中の一部であり、経営の問題である。

○　情報セキュリティの問題は、テクニカル系の問題とマネジメント系の問題の両方があるが、両者が混乱し、バランスが悪くなりがちなので、そういった問題を認識した上で、整理・体系化するべきである。

○　情報セキュリティは、「情報の安全・安心」と考えた場合、営業やサポートなどＩＴ以外の業務も含めた全ての業務で確保される必要があり、そういった観点で検討を進めるべきである。その結果として、業務のクオリティが上がり、日本の国力の向上にも繋がる。

○　企業内での情報セキュリティ教育については、定期的に実施したり全社員に一斉に実施したりすることが難しい場合には、入社時や昇任時の研修や新年時など、様々な

機会を捉えて実施していくという考え方もありうる。

○　人材の国際的流動性の中で、セキュリティをどう確保するのか、あるいは期待するのかということを考えていくことも大事だ。

○　グローバルスタンダード的な観点からも、人材育成・資格制度について検討する必要がある。

○　大学に関連する部分については、先進的なセキュリティ技術の分野の人材についての議論と実務に使える人材についての議論の２つのパターンがあると思う。

○　幹部にはセキュリティを理解して貰う必要はなく、リスクを理解して貰おうとするべきではないか。そういう意味で、セキュリティとリスクを区別することについて議論する必要がある。

○　セキュリティ専門の SIer 等は問題ないが、通常のシステム構築を行う SIer に情報セキュリティを完全に身につけさせるのは難しいと思う。しかしながら、他の委員も指摘しているように、通常の SIer でもセキュア・プログラミングを理解する必要があり、それも含めて通常の SIer のセキュリティ技能を上げていく方策を検討することが重要である。

○　プロフェッショナルとスペシャリストを分けて議論すべき。プロフェッショナルというのは、マネジメントからテクニカルまで広く浅く理解して総合的なコンサルティングや実務を行う者、スペシャリストはそれぞれのカテゴリにおいて特殊技能・専門技能を持っている者になる。業界を見ていると、両者とも全般的に足りないと思う

○　人材育成に関しては、目指すべき社会構造を決め、そのために必要な人材の数を分析した上で、対策を検討するという考え方を取り入れる必要がある。

○　１００％セキュアというものは作ることができないという現実があるが、そうであっても、「こういう枠組みを作って運用すれば少なくとも現状よりは良くなる。」というようなアイデアを捻り出す必要がある。

○　情報セキュリティの分野では資格というのはあまり評価されないということであったが、情報処理技術者の受験者数は非常に多いので、こういうものは存続していくべきではないか。

○　行政機関においては、公務員として情報セキュリティ人材を採用する必要があるの

か。必要な部分について民間の人材をその都度活用していくという方向での検討も必要なのではないか。

(10) 今後のスケジュール

○　事務局より資料９に沿って説明。

－以上－