次世代ＩＰインフラ研究会
セキュリティＷＧ（第４回）議事要旨（案）

１　日　時：平成１７年3月１７日（木）１５：００～１７：００
２　場　所：三田共用会議所　第三特別会議室
３　出席者：
〔ＷＧ構成員〕
新井構成員、飯塚構成員（栗林代理）、歌代構成員、内田構成員、加藤幹之構成員、加藤佳実構成員、桑子構成員（大野代理）、笹木構成員、佐々木構成員（グループリーダー）、篠田構成員、武智構成員、手塚構成員、永瀬構成員、南浮構成員、藤谷構成員、星澤構成員、松島構成員、森構成員
〔ゲストスピーカー〕
水野執行役員（インテック）
辻田企画部長（電気通信事業者協会）
〔総務省〕
有冨総合通信基盤局長、江嵜電気通信事業部長、吉田情報セキュリティ対策室長、金谷電気通信技術システム課長
〔事務局〕
坂巻データ通信課長、秋本データ通信課調査官、山路データ通信課課長補佐

４　議　事

総務省から資料４－１（ＩＣＴ人材育成に向けた総務省の取組について）に沿って説明があった。主なやりとり以下のとおり。

○：マネージャー以上のクラスの者がセキュリティを分からないといけない。法律上の要求事項などをシステムやマネジメントにどう取り込むか、自分なりに考え、運用できる人でないとマネージャーは務まらない。技術的な要求仕様だけでなく、法律･経営的な素養、人的資源の評価等を含めた、社会全体の要求仕様を考慮した中級以上のセキュリティ人材育成に関する支援策の検討が必要。
○：中級以上の人材を小数でも作れれば、その人が新たにセキュリティ人材を育てることができる。初級教育だけでなく、中級以上の人材育成に力を入れることが必要。

南浮構成員から資料４－２（セキュリティ技術者の育成について）に沿って説明があった。主なやりとり以下のとおり。

○：教育（座学や実験）でできる範囲と、OJTでできる範囲があると思うが、その他にサークル（JPCERT、telecom-ISAC）などセキュリティをよく知る人との情報交換で伸びるという場合もある。
○：セキュリティ人材は、情報を苦労して使うことによって育つ。セキュリティ教育には、初級、仕込む（OJT）、情報交換等のフェーズがある。

続いて、ゲストスピーカーである㈱インテック水野氏から資料４－３（情報セキュリティ担当者の育成について）に沿って説明があった。主なやりとり以下のとおり。

○：情報通信業界では、発表の中で述べたスキルセットという考え方が定着してきている。社内でもスキルセットという考え方を使い、セキュリティ担当者が習得すべき項目を整理して、それぞれの項目を７段階のレベルに分けている。
○：担当者としては、共通して誰もが知らなければならない一般的な要求事項を理解しているだけでなく、相手のビジネスを把握し、納入システム（提供するサービス）に対する特別な要求を汲み取るスキルが必要。セキュリティ教育についても、そのような意識を持たせる教育が必要であり、それもスキルであるということを、教育のあらゆる場面で取り入れれば、現在の技術レベルでもはるかに良いものができるのではないか。

続いて、内田構成員から資料４－４（情報セキュリティ人材育成について）に沿って説明があった。主なやりとり以下のとおり。

○：情報セキュリティは総合科学であり、①技術、②管理・運用、③法制度など、技術の専門家としての教育の部分と、管理運用的な視点で、それをどのように使っていくかという視点がある。これまで、人材育成ということは技術中心の議論が多かったが、社会全体として、①～③をどのようにして組み合わせるかということを考えなければならない。
○：最近では、コンプライアンスの部門に、技術的なバックグラウンドを持った人間と法務のバックグラウンドを持った人間を集めて、個人情報保護、他社情報、知的財産の取扱い等に関する監査、ルール作り等を行い、セキュリティのコンプライアンスに関するＰＤＣＡサイクルを回している。セキュリティ部門では、技術的なことはカバーされているけれども、人が関わっている部分で事故が起こることが多く、技術、法務の二つの部門がどのようにうまくやっていくかは大きな課題。
○：システム提供者は、顧客に安全なシステムを提供のために内部資格等の勉強を通じてセキュリティに関する技術を修得するが、あくまでセキュリティはスキルの一部である。求められるセキュリティ人材のパターンが色々あり、社会全体として、どのようなタイプのセキュリティ人材、教育が必要かということを考える必要がある。
○：教育だけで新しい知識を習得することは無理であり、考え方をどのように身につけるかということが重要。カーネギーメロン大学が米国で開催する短期CISOコースでは、マネジメント系の色彩がかなり強い中に、技術を少し入れるという教育で、日本では多少無理があると感じる。日本に合ったセキュリティ教育体系を作る必要がある。また、海外のセキュリティセミナーや資格試験も、そのまま日本に持ってこられるかという点についても、内容を見て検討を行う必要がある。
○：セキュリティを生業にしていこうとする人は、徹底的に技術を知らなければならない。しかし、世の中の大半はユーザーであり、普通の国民にとって、セキュリティに関して必要な知識は何か、という点を考えなければ間違ってしまう危険性がある。
○：ＣＩＳＳＰ（Certification Information System Security Professional）など海外のセキュリテ

ィ資格を翻訳するには、英語の知識だけではなく、関係する法令等、たくさんの知識が必要。このような知識を全て備えた講師はいないことを前提で教育を進めて行かなくてはならない。法律に関しても、日本の教育ではＥＵの法律や英国の法律を勉強する人間が別々であり、そもそもこのような教育のあり方について考える必要がある。

○：全ての人にハイレベルなセキュリティ教育が必要とは考えていないが、レベルの高い人を育てることが重要。

○：レベルの高い人を育てれば、その人がねずみ算的にたくさんの技術者を育てることができる。米国では教育費用が高く、それだけ優秀な講師が実践的な教育を行っている。日本では入社まもない人間が新人教育を行っているというようなことでは、再生産という面で考えるとありえない話。

続いて、ゲストスピーカーである(社)電気通信事業者協会辻田氏から資料４－５（ＮＩＳＭについて）に沿って説明があった。主なやりとり以下のとおり。

○：シンガポールの制度のように、企業のような組織ではなく個人を対象として受講料を負担する政策支援の例は面白い。民間資格も助成対象に入っているが、実機を使い本当のオペレーションを勉強できる点で、実践的。特定企業に対し公的資金で援助してよいのかといった公平性の問題もあるが、日本でも出来るか。

○：厚生労働省が実施している英会話等の受講に対する教育訓練給付と考え方において似ている部分がある。

○：政策支援対象となる資格に関しては、一回認定したらそれで終わりというのではなく、毎年、定期的に見直しを行う必要がある。

○：国際的な取り組みを見ると、韓国などでは大学を中心に教育が進んでおり、大学院などでは千人単位で卒業生を出そうとしている。また、日本では“情報セキュリティ研究室”というように研究室単位となるのに対して、韓国では、“情報セキュリティ学部”というように大学の学部単位となっており、研究室は“サイバーテロ対応研究室”というように細分化されている。

以上