

平成 23 年度 第 1 回情報セキュリティ人材育成検討委員会 議事概要

日時：平成 23 年 9 月 15 日(木) 10:00～12:00

場所：IPA 13 階 会議室 A, B

出席委員：今井委員長、田口委員、名和委員、浜田委員、平木委員、三輪委員、安尾委員、
与儀委員、樂満委員

オブザーバ：内閣官房セキュリティセンター、総務省、文部科学省、経済産業省ほか

IPA：笹岡参与、巽参事、平林 GL

概要：

- (1) 笹岡参与による開会挨拶
- (2) 委員及びオブザーバによる自己紹介
- (3) 委員会の趣旨及びスケジュール概要について説明（資料 2）
- (4) 与儀委員による「情報セキュリティ人材アーキテクチャガイドブック（以下「ガイドブック」という。）」及び安尾委員による「情報セキュリティ人材育成検討委員会用資料」に関する説明

今井委員長 ガイドブックは、どのように利用しているか？

与儀委員 情報セキュリティ教育事業者連絡会と連携し、関連のイベントで配布するなどの活動を実施。ただし2009年以降更新できていない。また本ガイドブックと関連して、ISEPA（情報セキュリティ教育事業者連絡会）のサイトでは、3カ月毎の情報セキュリティの民間資格取得者の推移を公開している。

今井委員長 キャリアパスを作っているが、これはラックの実例に基づくものか？
また、CSOや社長に行くパスはないのか？

与儀委員 ラックもそうだが、他の企業にもワーキンググループに入ってもらい、それらの代表的な例として掲示している。また、CSOや社長に行くパスも皆無ではない。

なお、米国などは経営陣にはいるのであれば、MBAぐらいは持っているが、セキュリティに関してもコンサルタントには、この資格は必要と言うことが明確になっている。

今井委員長 安尾委員の資料にある情報セキュリティ委員会の委員は何人ぐらいいるのか？また、どのような経歴の人か？

安尾委員 専門にしているのは10名弱で、基本的には中途採用。即戦力を重視する。
樂満委員 ガイドブックでは様々な職種が定義されているが、職種ごとに専任者を置くべきか？

大企業では役割分担が可能だと思うが、小規模な企業では一人で複数の役割を担うことになる。複数の役割を担う人に、様々なスキルを求めることは難しいと思う。

与儀委員 専任者を置くかどうかは、組織モデルの問題。大企業は、すべての機能を

自社で完結することも可能だが、現実的には、国内の企業では、1人が複数の職務を兼務している場合が多い。どの程度セキュリティを担う人材を置くかは難しい問題で、セキュリティ担当の適正数は（資本金や従業員数のような）企業規模によって割り出すのか、保有サーバー数で割り出すのか、我々も検討しきれていなかった問題である。

今井委員長 それでは、情報セキュリティ人材をどのように定義するか、ご議論いただきたいと思う。需給ギャップを考えると、どのように定義したらよいか？

浜田委員 各企業のセキュリティ委員会の構成は、総務系とIT系に分かれ、人材的に見ると全く異なる人材。これを一緒にすると大変なので、IT系に限って検討フォーカスすべきではないか？

人材育成で難しいのは、各企業が体制をどう組織し、個人の能力向上をどう図るのかということ。様々なコンビネーションがあり得る。また、どのレイヤーで実施していくのか、つまり、ポリシーで実施するのか、より現場のレベルで実施するのかなどでも方法が大きく異なってくる。

通常の事業会社は、情報セキュリティについて、基本的にはアウトソーシングやIT系子会社に任せており、自社で情報セキュリティ人材の育成を考えるのは難しい。

仕事のエレメントだけでなく、ユーザサイドとしては、実際の組織形態がどうであり、どのような問題があるのかフォーカスすることが必要だと思う。

三輪委員 浜田さんに賛成で、総務系とIT系ではやることは全く違う。

私が今、コンサルタントとしてみているところは、全国で6,000箇所の拠点があり、毎日1億件のカードの処理を行っているが、その中では、何をどう守るかという、セキュリティアーキテクトの問題となっている。標的型攻撃に対する先進的な対応などという（技術的に高いレベルの）問題ではなく、そこにカードを使用したきった紙が放置されているのをどうするかというような問題になってくる。どこにフォーカスを置くか決めないと発散してしまう。

大企業では法務部門があっても、社員の人材育成として弁護士を育てることが会社の行うべきことではない。法務部門があっても専門的なところは、法律事務所を使えばよく、その判断を行う人材を育てることが重要である。今回の委員会では、ユーザ部門における専門家を使う人材を育てるのか、それともその発注を受ける側の専門家を育てるのか明確にすべきである。また、セキュリティ人材の定義ギャップがある。育てたい人材と企業のほしい人材は差がある。調査を実施して、情報セキュリティ人材が足りているかと質問すると皆、不足していると答えるかも知れないが、では能力のあるセキュリティ1,000人そろえたら雇用してくれるかと聞いたら、誰も要らないと回答すると思う。必要とは言いが雇用はしない、その点では別の意味での人材需給のギャップが存在する。

- 今井委員長 今日ではスコープに関する結論を出す議論の段階ではなく、各委員の考えを共有できればと思う。
- 樂満委員 情報セキュリティ人材という言葉の定義は難しい。セキュリティは網羅的に行う必要があり、USBメモリの紛失対策から、Webサーバーへの攻撃対応、個人情報の漏えい対策まで全てカバーする必要があり、物理的セキュリティも含まれる。
- したがって、具体的に何のセキュリティ人材が不足しているか分析を進めないと、どのような人材が必要かがわからない。Webサーバーへの攻撃が困るならば、SQLインジェクションに対する脆弱性がないようなシステムを作れる人材が必要となるが、実はそのような人材は既にいるが、それをWebサーバーにも適用するよう、組織的に指示を出す人材がいなくてもいい。どういう人材が必要なのかを分析する必要がある
- また、網羅的に全ての知識を高められるかという一人では無理で、そのような万能な人材はいない。その場合、いかに補っていくかという人材のマップの仕方で抜けのないようにすることだと思う。
- セキュリティはDBやネットワークなどの全ての分野の頂点のスキルがあるので、その育成をどうするのが難しい。
- 三輪委員 今回の定義について事務局に出口を聞きたい。対象者は学生で、新卒のレベルを上げようとするのか、社会人の中から育てようとするのかどちらか？
- 平林G L 今、企業の中で情報セキュリティ人材が足りていないと言われていて、それをどうすれば解決できるかを考えたいと思っており、新卒か社会人かは決めていない。
- 三輪委員 しかし、IPAがこの委員会の議論を踏まえて何をしたいのかということがあるはずで、その点を率直に聞きたい。
- 平林G L 個人的な見解だが、人材育成を考える場合、能力の育成、能力の測定、能力の発揮の3つがうまく連動しないとうまく行かないと考えている。IPAは、これまで直接育成を行う事業はほとんど行っておらず、情報処理技術者試験やスキル標準など、能力を測るモノサシを提供してきた。例えば、情報処理技術者試験では、実際の育成は各種の学校や民間の教育会社などにお任せしているし、能力の発揮は合格者に人事や給与面でのインセンティブを与える企業が多く、このエコシステムの中で人材育成が回っている。今回の議論の結果、IPAの既存の人材育成ツールを活用していくのか、新たな事業を立てるべきかも検討することになると思うが、人材育成のエコシステムまで考えて実施したい。IPAの既存のツールで考えるなら、試験やスキル標準でもう少しセキュリティを前に出すこともあるかもしれないし、民間の資格もあるのでそちらとの連携と言うのもあるかもしれない。また、企業が持っているセキュリティ人材育成のノウハウを大学の教育に活かすことをIPAがサポートすることも考えられる。
- 三輪委員 そういう意味では需給ギャップをはっきりさせればよい。大学や専門学校

の情報系の学生を供給とみて、どれだけ需要があるかと言えば、供給過多だと思う。さらに、供給したものと企業のほしいものとはスキルにギャップがある。また、情報セキュリティの職種について、日本には求人がない。米国やヨーロッパではセキュリティアーキテクトやセキュリティマネージャーなどを募集している。日本企業ではゼロ。それでは日本ではセキュリティが十分行われているかと言うと、それも違う。標的型攻撃が来たら日本は危ない。セキュリティ対策とレベルには大きなギャップがある。この問題では、シーズである人を育てることよりもニーズを作り出す人を育てる必要がある。そもそも情報セキュリティが必要だと言う人がいない。

名和委員 経験則だが、企画、設計の段階は事業の内容とセキュリティの両方がわかっていないとできない。発注とか開発はセキュリティのわかるプログラマーが必要であるとか、それを発注できる人材が必要である。それから、実装、運用についてもセキュリティ人材の定義もニーズも変わってくる。セキュリティの事故は起こらないように作っているはずだが、最近は想定外のことが発生している。

三輪委員ご指摘のとおり、我が国では情報セキュリティ人材の求人広告は出ていないが、このような人材はヘッドハンティングの領域ではないか。ただ、ヘッドハンティングの仲介を行っているのは日本の会社でなく、英、米などの海外の会社である。

人材育成では、旧来の事業活動のセキュリティ対策に向けたものと想定外の事象におけるインシデントレスポンスに向けたものの2つの軸があると思う。

田口委員 ユーザ企業にアンケートを取るとセキュリティの高度な人材が不足していると間違いなくでてくる。ただ、高度でない人材は余っているので、新たに採用することは難しくなっている。そう考えるとまずは、IT系のベンダーサイドのエンジニアについて、ユーザサイドの必要に応じて、このレベルや職種について定義し、その需給ギャップを見て行くのが妥当だと思う。ベンダーサイドの高度な人材を定義して、その需給ギャップをみるのがよいと思う。ITエンジニアは100万人いても、セキュリティ人材は1,000人もいないレベルで、増やす必要がある。IPAの施策としても、セキュリティのアーキテクトもいれば、危機管理対応のコンサルタントもいると定義して、世の中に広めるべきではないか。

安尾委員 極論だが、情報流出事故などが発生したときの保険のために情報セキュリティ対策を行っている企業もある。また、何としても情報を守りたいという企業もある。

両者では求める人材やスキルが異なり、前者は、総務的、管理的な仕事为中心で、後者は、情報でセキュリティの技術を追求することになると思う。

人材育成を考える場合、どちらかを対象にするのか、両方を対象にするのか決めるのは難しいと思う。

(5) 「情報セキュリティ人材の育成に関する調査事業」について、説明。(資料3)

- 与儀委員 著名な大学で情報工学を学んだ人が、情報システム部門に配属されるかと言えば、配属されない。優秀な人材は、まず研究部門や事業部門に配属され、そこから漏れた人が情報システム部門に回されるという傾向がある。
- 樂満委員 与儀委員の意見は、情報セキュリティ人材の募集がないのとリンクしていると思う。募集がないのは、いないのではなく、どのような人材がいるのかわからないからではないか。どのような能力をもった人材がいるのかを明確にする必要がある。
- 三輪委員 資料3 ページに学科の定員数があるが、例えば、今井先生の研究室とか、学科では見当たらないが専門学校で情報セキュリティ学科があるところもある。大学の場合、学科単位ではなく、研究室単位で洗い出したほうがよい。
- 平林G L 研究室単位で供給能力を見る場合、自他共に認める情報セキュリティの研究を行っている研究室もあるが、自称で研究をしていると言っているところがある可能性も有り、それを客観的な基準で排除するのは難しいと言う懸念がある。
- 三輪委員 それこそ需給ギャップであって、企業にしてみれば、自称でセキュリティの研究をしてきたというような学生は全くいない。
- 樂満委員 学生に関しては、IT スキルを教えることはできるが、ISMS のように組織をどう回していくところの人は難しい。そういう部分は社会の経験が必要だと思う。
- 今井委員長 ハイブリッド人材、いろいろな分野にミートする人がセキュリティを見ているのが現状だと思う。学生の段階で育成するのが必要だと思う。
- 安尾委員 キャリアパスは必要だと思う。例えば、OS とか DB とか、それを専門にするプロも必要だが、それを正しく評価するしくみがない。それを作ってあげると、それが、ひとつのパスになると思う。
- 浜田委員 情報セキュリティ人材というとピンとこないと思う。各社情報セキュリティ対策は適切に実施しているが、IT インフラの担当者が情報セキュリティ対策も実施している。従って、情報セキュリティ人材はいるかと聞くと、いないと答える。
- 情報セキュリティの現場では、インフラ、DB、ネットワークの全てを知らないといけない。今はそういう人がいるから良いが、今後アウトソースや外注化で実業務が減ってくるとどこまですればよいか判断できる人がいなくなる。各社のCIO、部門長はそのことを危惧している。
- 今井委員長 本来は、情報セキュリティ人材という言葉で定着させていく必要がある。
- 田口委員 キャリアパスモデルはこれまで育ってきた人を分析して、こういうパスになりますと示すことになると思うが、情報セキュリティでは、今のところ

そういう育ち方をした人がいないので、これからこういう人材が必要で価値があり、CIO が認めて社員として採用するのか、プロジェクトとして採用するのかは別にして、世の中にこういう人がいますとアピールしていくようなモデルのほうが、より実践的で定着しやすいと思う。大学の方は、少し期待薄の感じがするが、社会人になってから、IT エンジニアが、セキュリティを体系的に学ぶ場所が必ずしもない。また、卒業したところで、社会的な資格が得られるかということ必ずしもそうでない。そういうところが問題だと思う。

- (6) 今後のスケジュールについて説明し、次回は各委員の人材育成の取組みについてご紹介いただくこととし、メールで日程調整することになった。
- (7) 異参事による閉会挨拶

以上