Vol.2012-CSEC-58 No.39
Vol.2012-SPT-4 No.39
2012/7/20

情報セキュリティ人材に求められるスキルと人材育成

花田　経子†

IPA から 2012 年 4 月 27 日に情報セキュリティ人材に関する基礎調査が発表され、情報セキュリティ人材は新規に 2.5 万人が不足しており、早急な人材育成の必要性が指摘されている。一方で、当該調査報告書では育成のために必要な情報セキュリティ人材そのもののスキルについては明確に規定されておらず、事例集も若い世代や現役の技術者の参考になりにくい構造となっている。これらを踏まえ、本稿では人材の事例調査を踏まえた人材のスキルについてとりまとめる。

Research on the skill and human-resources development of the information security staff.

KYOKO HANADA†

The report about the information security staff's human-resources development was released from IPA on April 27, 2012. In this report, since the 25,000 information security staff is insufficient, is indicated that it must hurry human-resources development. However, it turned out that the contents of this report have a mistake. Moreover, the information security staff's skill is also indefinite. In this paper, the information security staff's skill and human-resources development are described..

1. IT 技術者のキャリアデザインとスキル

IT 技術者の人材不足やキャリア形成の問題、人材育成の問題については、ここ 10 年ほど様々な形で論議され、スキルの標準化や人材育成手法の試みなどが情報処理推進機構（以下、IPA）を中心に行われている。キャリアデザインの分野においては、IT 技術者は“主体的かつ自発的なキャリア形成が進めやすい職種”として位置づけられており、多くの IT 技術者自身がそのようにとらえている。一方で、IT 技術者自身の雇用・労働問題や、人材不足問題などは常に問題視され、自発的なキャリア形成とのギャップが生じている。一般的にキャリアデザインとはキャリア開発(Career Development)やキャリアマネジメント(Career Management)よりも広く、Design を設計という本来的な枠組みではなく、“意味付けを行う”という意味で用いる事が多い。また、キャリアそのものも、ワークキャリア（仕事を中心としたキャリア）とそれを下支えするライフキャリア（人生全般を示したキャリア）の双方にまたがった形でとらえられている。本稿では、キャリアデザインをワークキャリアとライフキャリアを通じた“人生や仕事の意識化”として定義している。したがって、IT 技術者を中心とした人材のキャリアデザインとは、その職業が彼ら彼女ら自身のキャリア（主にワークキャリア）においてどのような存在であるのかを自身の内外において意識化することである。自分自身における意識化であるため、その内容は主観的な要素を多く含むものの、IT 技術者共通の要素も見受けられる。また、ワークキャリアにおける外的キャリアの経路を意味するキャリアパスは、IT 技術者に共通する部分も多い。キャリアパスをたどりつつワークキャリアを形成する過程で、IT 技術者はさまざまなスキルを身に着けていく。一般的に、IT 技術者に求められているスキルを表 1 に示す。

表 1 IT 技術者に求められるスキル

①IT 技術に関する専門的知識／能力	コンピュータ科学に対する基礎知識／能力、コンピュータシステムに対する知識／能力、システム開発・システム運用の知識／能力、ネットワーク・データベースの知識／能力、セキュリティ・標準化の知識／能力
②業務に対する知識	業務における特有の知識、情報化や経営に対する知識
③ビジネススキル	コミュニケーション・プレゼンテーション能力、マネジメント能力、文書作成・文書管理能力、問題発見・問題解決能力

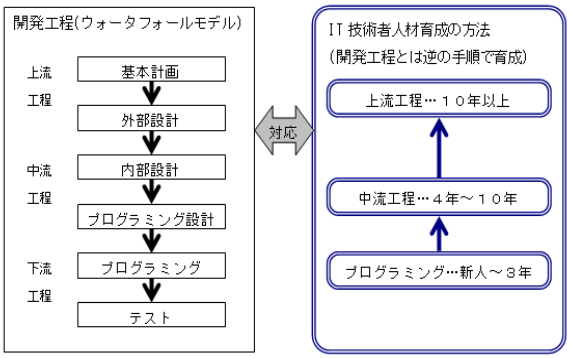

図 1　IT 技術者の人材育成伝統的モデル

表 1 のスキルはこれまで図 1 のような方法（伝統的育成モデル）において習得されてきた。基本的に IT 技術者の多くはこれまで表 1 の③に関するスキルを持った人材を新卒

Vol.2012-CSEC-58 No.39
Vol.2012-SPT-4 No.39
2012/7/20

採用し、①や②のスキルを社内で身に付けるという形で育成されていた。図 1 で示したとおり、WF モデルの下流工程から実務をさせつつ①および②のスキルと業務経験を経つつ上流工程へとステップアップする形で育成されている。したがって、IT 技術者におけるキャリアパスはより上流の工程へアップしていくことが一般的とされてきた。しかしながら、ネットワークなどの様々な技術の発達・システムそのものの細分化が進んだ結果、図 1 のような伝統的育成モデルでの人材育成やキャリアパスの形成は難しくなっている。そこで、現代型として取りまとめたものが図 2 である。図 2 であきらかなように、職務の細分化が進み専門性をより重要視される一方で、それまでは下流工程という扱いで一括りにされてきたシステム管理・保守に関する業務の重要性も増している。しかし、図 1 における伝統的育成モデルの影響は大変強く、これらの専門性を育成する仕組みが含まれていない。また、システム管理・保守業務はネットワークによる IT のインフラ化が進む中でより重要性を増している業務であるものの、キャリアパスの中であまり反映されていない。

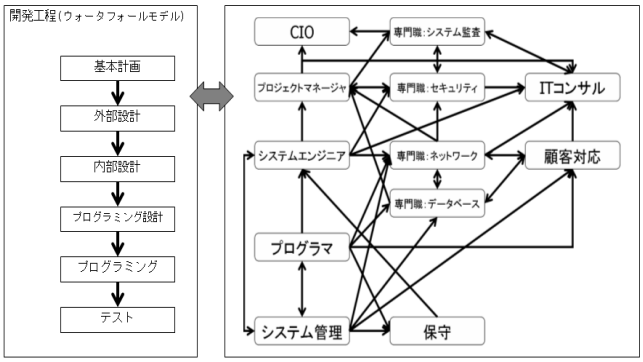

図 2　IT 技術者のキャリアパス現代型モデル

なお、一般的にキャリアデザインの類型として、下記の 4 つに分類できる。4 つのキャリアデザインはどれか一つのみを遂行するのではなく、複数選択して遂行されることが多い。

- 目標逆算型キャリアデザイン…人生を企業戦略同様に計画的に設計する
- 偶然活用型キャリアデザイン…予期していない偶然の出来事に積極的に対応する
- 節目重視型キャリアデザイン…節目はデザインし、他の時期はドリフトしながらキャリアを形成する
- 意味発見型キャリアデザイン…創造価値・体験価値・態度価値に意味を見いだすことでキャリアを意識化する

IT 技術者の多くは、この中で目標逆残型キャリアデザインを選択する傾向が強い。しかし、このキャリアデザインは自身の強い目的意識を持ち、キャリアにおける様々な葛藤を乗り越えて行かなければ実現できない。多くの人材がこのキャリアデザインを指向したとしてもそれによって自ら納得する形でキャリアを自発的に“設計”することが出来る人材は大変限られている。ここに、IT 技術者の多くがかかえるキャリア形成に絡む諸問題の要因がある。

2. システム監査人のキャリアデザインとスキル

筆者は、自身の専門的研究領域であるシステム監査において、そのキャリアデザインが図 1 や図 2 でしめされるようなキャリアパスに当てはまるかどうかを 3 年ほど検討してきた。システム監査は、EDP が業務に導入されるようになった 1950 年代頃から米国で進められるようになり、日本でも 1980 年代には EDP 導入がすすんだ大手民間企業で取り組みがなされるようになった。米国では、システム監査勃興期の 1970 年代に監査関連の専門家集団が IT に係る監査スキルを持った職業人としてキャリアが位置づけられている。一方で、日本においては経済産業省（当時は通商産業省）の情報化戦略の一環として、他の IT 技術者と同様に、情報化にかかわる人材育成が実施されてきた。国内でのシステム監査に関するスキルレベルを図ることのできる唯一の能力認定試験であるシステム監査技術者試験が情報処理技術者試験の一分野として実施されていることがその現れである。したがって、図 1 の伝統的モデルでは上流工程の経験人材がつく専門職として、最近の図 2 においても CIO と同じぐらいの上流工程・プロジェクトマネジメント経験者がその上位職としてつく専門職として扱われている。しかし、システム監査人を中心としたヒアリングを中心とした調査研究を進めた結果、他の IT 技術者に比べて求められるスキルやキャリアパスが大きく異なることがわかった。図 3 でそのスキルを、図 4 でそのキャリアパスを示す。

IT 技術者に求められるスキル	①IT 技術に関する専門的知識／能力
	②業務に対する知識
	③ビジネススキル
＋	
監査に関連したスキル	④システム監査の知識
	⑤システム監査の実施能力
	⑥監査実施にあたっての関連知識

図 3　システム監査人に求められるスキル

特定の職業においてキャリア形成を考慮する際には、その職業の発達段階を年代と相互比較した方が検討しやすい。国内におけるシステム監査人は、1970 年代の創世期の頃から実務を経験して現状の監査制度や人材育成制度を形成した第 1 世代、J-SOX の枠組み形成に深く関与している第 2 世代、現在の監査実務に直接関わっている第 3 世代および第 4 世代に分類することができる。システム監査人の多く

は、教育機関において形成されるというケースはほとんどなく、したがってほとんどが OJT 等で上から伝承される形で図 3 のスキルを習得し実務経験を積んでいる。監査スキルと IT スキルという 2 つのスキルのうちどちらかのスキルが成熟しないとシステム監査人のキャリアパスは開かれていないといえる。加えて、システム監査人は大企業において 1 社あたりの平均が 4 名前後であり、それほど多い存在ではない。そのため、スキルを積んだからといってシステム監査人になるというキャリアパスがすぐに開かれるわけではない。実態調査で明らかになったのは、ほとんどのケースにおいて現在のシステム監査人の大多数は“結果としてのシステム監査人”である。目標逆算型キャリアデザインのようなキャリア形成をおこなった人材はほとんど皆無であり、多くは偶然活用型あるいは節目重視型キャリアデザインの結果としてシステム監査人になっている。

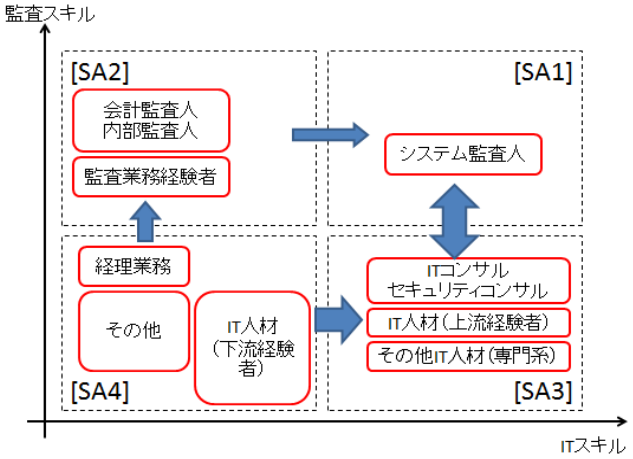

図 4　監査スキル／IT スキルからみる
システム監査人のキャリアパス

これらのシステム監査人は、第 1 世代・第 2 世代のころは 50 歳前後でシステム監査人になる事が多かったが、第 3 世代以降は 40 歳代と若返ってきているため、システム監査人になったあとのキャリアパスを形成することが大変難しく、人材育成の問題の一環として解決する必要性が生じている。若返りの傾向は大変強く、外部監査系システム監査人では、30 歳台の監査人・監査経験者が増加している。図 5 では、ヒアリングを中心としたシステム監査人自身に人に本質的に求められているスキルを示している。図 3 のスキルよりももっと本質的に職業人として必要なのは、図 5 の①および②である。特に、②は他の IT 技術者における職種では能力を開発することが難しい分野であり、一方で現在の情報システムの多くに求められる高信頼性および安全性を維持するのに欠かすことのできない能力である。したがって、このような能力を保持しているシステム監査人を監査業務のみに従事させるのではなく、一般的な IT 技術者として開発現場や運用現場に従事させることができるような人材配置・人材育成制度を構築することが出来れば、監査スキルを有効に活かすことができ、現在の IT が抱える諸問題を解決する緒となろう。

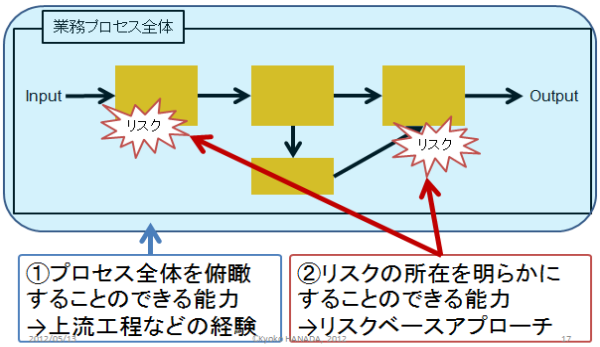

図 5　本質的に求められているシステム監査人のスキル

3. セキュリティ人材の世代とスキル

セキュリティ人材の育成が昨今大変盛んに議論されている。特に、数年前より内閣官房情報セキュリティセンター(NISC)において人材育成が国策の一環として議論され、多くの識者がそれについて論じるようになった。特に、2012 年 4 月 27 に IPA から発表された「情報セキュリティ人材の育成に関する基礎調査―調査報告書―」（以後、IPA 報告書）は、セキュリティ人材に関して詳細な調査を実施し、その上で現在の日本国内でのセキュリティ人材は大幅に不足しており、早急な人材育成が必要であると提唱している。

本稿では、システム監査人のキャリアデザイン研究の一環として、セキュリティ人材を比較する形で進めている。それは、現在のセキュリティ概念で求められているような機密性や安全性、可用性、信頼性といった概念は、システム開発や運用の現場では長年当たり前のように組み込まれており、別個のものとして扱っていなかったためでもある。当然、これらのシステムを監査するシステム監査では、これらへの対応は当たり前であり、リスク分析や脆弱性診断、BCP 等への対策などはシステム監査の中でごく普通に扱われていた。基幹系システムにおいて可用性は最も重要なことであり、それを達成するための高信頼性かつ安全性の高いシステムや、機密性を確保したシステムを設計し、運用することは当たり前であった。したがって、セキュリティ人材という枠組み自体も基幹システムが中心の時代には認識されることはなかった。もちろん、暗号技術などのセキュリティに係る理論研究や技術開発、コンピュータウィルス対策などを行う専門のベンダーは存在していたものの、一般的な企業において情報セキュリティが着目されるようになったのは近年、特に 1990 年代以降である。現在のように IT への依存度が低く、IT リスクの影響が大きくなかったことも要因であろう。そのような状況から、セキュリティ人材については IPA のセキュリティ人材基礎調査報告書を元に、表 2 のように年代を区分している。

表 2　セキュリティ業務開始時期による年代区分

SEC 第Ⅰ期	セキュリティ黎明期（1995 年以前）
SEC 第Ⅱ期	セキュリティ成長期(1996～2003 年)
SEC 第Ⅲ期	セキュリティ普及期(2004 年以降)

SEC 第Ⅰ期の世代は、現在セキュリティ業界で制度設計などの枠組みに関与したり、業界を代表する企業や団体などの代表になったりするなど、セキュリティに係る政策やビジネスモデルに対し大きな影響力を持つ世代である。この世代の多くは、技術職ではなくマネジメント職や営業職的な形でワークキャリアにおいては技術の第一線からは外れている。監査（システム監査等）経験のある人材も多い。情報セキュリティ人材の教育を第二のワークキャリアの目標として設定し従事している人もいるため、セキュリティ人材の育成に対する枠組み設計にも積極的に関与している世代であるといえよう。

ワークキャリアとして技術的にセキュリティ業界を牽引しているのは、SEC 第Ⅱ期の世代である。この世代の特徴に最も多いのは、いわゆる 7 6 世代（ナナロク）といわれる子どものころから PC に慣れ親しみ、プログラミングを子どもの頃から経験している年代が多く含まれていることである。この世代は、学生の頃にインターネット環境に接し、高等教育機関等で IT 教育を受けているケースも多い。そのため、図 1 の伝統的育成モデルにおけるプログラミングを長年経験することなく、すぐに中流工程に移ったり、開発ではなくネットワーク関係の管理業務など（主にインフラ関係）に従事したりしている。この世代のセキュリティに対するきっかけも第Ⅰ期とは異なり独特である。SEC 第Ⅱ期の人材は、人材育成の枠組みの中で形成されたものではなく、自発的に形成された人材であるといえる。SEC 第Ⅲ期の人材は、セキュリティが着目されるようになる中でセキュリティベンダーを中心として社内における人材育成制度の中で形成された人材と、第Ⅱ期と同じように自発的に形成された人材とが混在している。高等教育機関においてセキュリティを専門として研究し、その後セキュリティベンダーなどの企業にセキュリティ専門職として就職する人材も存在している。ただ、IT 人材としては図 1 の伝統的育成モデルが崩壊している状況下で形成されたこともあり、実際の開発現場や運用現場を知らないままセキュリティの専門教育を受けるケースなども多く、実務においての IT リスクへの対応などに問題があるケースも散見される。

IPA 報告書では、これらの人材に対するキャリアのヒアリングを実施している。おおよそ 60 名ほどの人材に対するヒアリングを元に、彼らのキャリアパスを示したものが図 6 である。このキャリアパスモデルではセキュリティのスキルをエントリレベル／ミドルレベル／ハイレベルの三層にレベル分けした上で、示している。

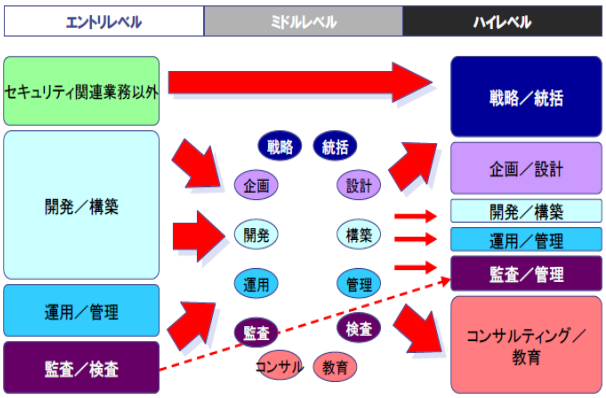

図 6　IPA 報告書に基づく情報セキュリティ人材のキャリアパスモデル

セキュリティ人材に求められるスキルは、IPA 報告書では IT 技術力（IT の基礎知識、プログラミング経験、システム開発経験、セキュリティの基礎知識、インフラの知識）に加えて、バランス力、マルチ視点、先見性、柔軟性、チャレンジ力、国際性、イマジネーション、経営の知識、洞察力、コミュニケーション力などが業務経験を経ていくうちに身につけるべきスキルであるとされている。また、内閣官房情報セキュリティセンター(NISC)で策定された「情報セキュリティ人材育成プログラム」においては、セキュリティ人材として“ハイブリッド型人材”と“問題発見・解決型人材”の二つが求められるとして、境界領域であるセキュリティに対応する人材のスキルが非常に高度なものであることを示している。NISC は、「人材育成・資格制度体系化専門委員会報告書―人は城、人は石垣、人は堀―」において以前より、“先進的な技術や高度な管理手法の研究開発者”、“セキュリティ製品等の提供者”、“セキュリティ対策に係る者”という 3 つのカテゴリに分けてそれらの人材カテゴリごとに必要となる人材育成対応策等を検討している。それぞれの人材カテゴリごとのスキルについてもふれられてはいるが、いずれにしても上述の通り大変高度かつ広範囲なスキルを求めており、現実に活躍している情報セキュリティ人材の実態にあまり即していないといえる。

4. IPA 報告書における問題点

IPA 報告書は、情報セキュリティ人材の実態調査としては今まで本格的に実施されていなかったこともあり、大変参考になるデータである一方で、大きな問題点を抱えている。その結果、“情報セキュリティ人材は不足しているという”情報だけが誤った形で発信されている現状にある。この点について、3 つの問題点を指摘したい。

第一の問題点は、情報セキュリティ人材の人数を推計する際の推計値の算出方法についてである。IPA 報告書では、現在の情報セキュリティに従事する専任人材の総数を、約

23 万人と推計している。そもそも、この 23 万人という推計には派遣社員や契約社員、公務員といった本来含めて算出すべきものが含まれていない。IPA 報告書も引用している NISC の定義では、セキュリティ人材とは、

- 先進的な技術や高度な管理手法の研究開発者
- セキュリティ製品等の提供者
- セキュリティ対策に係る者

の 3 つに分類される。この中で特にセキュリティ製品等の提供者とセキュリティ対策に係る者は、IT 技術者として一般的には含められている。周知の通り IT 技術者の雇用形態は正社員ばかりではなく、有能な技術者であっても契約社員や派遣社員といった形態をとっている場合も多い。また、公務員でも IT 技術者は当然存在している。したがって、統計上、専任人材の総数を正社員に限定しているのは大変不正確である。加えて、報告書では従業員規模 100 名以下の企業は対象外としている。IT 系企業の多くは 100 名以下であることも多い。実態調査してこれらのデータを除外した上で推計値を算出した根拠が不明である。不適切であるといわざるをえない。

もし仮に、第 1 の推計値算出の根拠が正しかったとしても、セキュリティ人材の専任総数が 23 万人であるというデータは実態に即しているとは言いがたい。このデータを、1 社あたり（ただし 100 名以上の企業に限定）の平均人数として仮に算出すると、セキュリティ人材の平均総数は 4〜5 名である。IT 技術者の総数を考えても、これは相当多い人数であるといえる。おそらくこの推計値はそもそもが誤っていると考えるのが妥当である。

第 2 の問題点は、セキュリティ人材のスキル不足度合いに関する点である。報告書では、仮に正しいとしたこの 23 万人のうち情報セキュリティ人材として十分なスキルを保有しているものは 9.3 万人であり、13.7 万人がスキル不足であるとしている。詳細を見ると、能力が足りていないという企業に対して、

A:業務が回らないほど危機的状況である・・・11%
B:多少無理すれば回る・・・39%
C:理想的ではない状況・・・50%

という状況であるとし、13.7 万人のうち A と B を足した約 50%の人材（つまり 6.9 万人）が早急に育成すべき人材であるしている。これを、一社あたりの平均値に換算すると 2〜3 人となる。もしこれが本当に正しいデータなのだとしたら、企業内のセキュリティ業務を専任している人材 5 名のうち、2〜3 名がスキル不足という状況は、企業にとってセキュリティ専任人材は大変無駄な人材であるということになる。システム監査同様にセキュリティも、企業において直接的な利益を生むことは殆ど無い。そのような部署に、役に立たない無能な人材を投入できるほど余裕のある組織はおそらくほとんどないであろう。普通の経営者であれば、IPA 報告書を読んだ段階で、セキュリティ人材を育成しなければならないとは結論付けることはないであろう。セキュリティ人材を専任で設置するぐらいなら、セキュリティベンダーと外部委託契約を結んだほうが費用対効果は高い。もし仮に、外部委託契約という話にならなかったとしても、報告書のようには判断せず、A の 11%のみの穴埋めをするのが普通であり、これに則せば、1.5 万人が早急にスキルを向上させるべき人材であるといえる。一社あたりの平均にすると 1〜2 名となる。しかし、いずれにしても一社あたりでスキルが不十分な専任人材が数名いるという企業にとっては大変な無駄な状況であることには変わらない。

さらに第 3 の問題として、これら専任人材のスキル不足を埋める方法に疑問がある。報告書では、この専任人材のスキル不足に加えて、現状では専任人材の人数そのものが足りてはおらず 2.2 万人不足していると推計している。離職率を踏まえれば新規に 2.5 万人を増やすべきだと指摘している。これが、報道されている人数である。第 1、第 2 の問題点で指摘したスキル不足人材の問題と合わせると、現状ではセキュリティ専任人材は 4〜5 名存在しているが、スキル不足が著しいので、今いる専任人材を 2 名ほど再教育して十分なスキルレベルになるよう配慮するか、もしくは新規に 1 名スペシャリストを雇用すべきであるということになる。このような提言にまともに答えようとする企業はほぼ皆無であろう。企業は、セキュリティのために経営されているわけではない。加えて、この報告書の最大の問題点はその新規の人材供給を学校教育での新規雇用を前提としていることである。これは大変に自己矛盾をはらんでいる。先のスキルに関する記述でも、「IT 技術力（IT の基礎知識、プログラミング経験、システム開発経験、セキュリティの基礎知識、インフラの知識）に加えて、バランス力、マルチ視点、先見性、柔軟性、チャレンジ力、国際性、イマジネーション、経営の知識、洞察力、コミュニケーション力などが業務経験を経ていくうちに身につけるべきスキルである」と指摘している。IT 技術力だけでも、ほとんどの学校教育では実現することはできない。報告書の提言通りにさまざまな点を実行したとしてもセキュリティ人材の育成も、十分なスキルレベルの確保も難しいといわざるを得ない。

上記の点から、IPA 報告書にはいくつかの問題点が存在しており、この点を踏まえた上で情報セキュリティ人材は単純に不足しているという扱いをするのは適切ではないといえよう。では、なぜ不足しているというような議論が発生するのかといえば、それは人材が不足しているのではなく、情報セキュリティのスキルを持った IT 技術者や IT ユーザが少ないからである。これらを混同することなく、先に示したシステム監査人のキャリアデザイン同様に、セキュリティに求められるコアなスキルを保持した IT 技術者を増やしていくことで、本来求められなければならないリスクの少ないシステム開発や運用、特に高信頼性かつ可用

Vol.2012-CSEC-58 No.39
Vol.2012-SPT-4 No.39
2012/7/20

性の高いシステムを開発したり、そのようなシステムの運用を実施することが可能である。学校教育も含めたセキュリティ人材の育成においては、“情報セキュリティしかできない人材”を育てるのではなく、“情報セキュリティのスキルも保有している IT 技術者”を育てることが最も必要であるといえよう。そのような人材育成プログラムが浸透すれば、IT 技術者のスキルも付加価値が増大し、またセキュリティ人材とよばれている人たちのキャリア形成においても有益であるといえる。

参考文献

1) 山口憲二編著、『キャリアデザインの多元的探究―職業観・勤労観の基礎から考えるキャリア教育論』、現代図書、2008 年。
2) 吉田洋稿、「第 7 章 IT 監査プロフェッションの育成」、(堀江正之編著、『日本監査研究学会リサーチ・シリーズⅦ IT のリスク・統制・監査』、同文館出版、2009 年)、163-187 頁
3) 拙稿、「内部監査を中心としたシステム監査人のキャリアデザインに関する事例研究」、『情報科学研究』第 30 号、専修大学情報科学研究所、2010 年、101-116 頁。
4) 拙稿、「システム監査人のキャリアパスと内的キャリアに関する事例研究」、『新島学園短期大学紀要』第 30 号、新島学園短期大学、2010 年 3 月、15-34 頁。
5) 拙稿、「システム監査人ではない人材におけるシステム監査スキルとキャリアデザインに関する考察」、『新島学園短期大学紀要』第 32 号、新島学園短期大学、2012 年 3 月、37-60 頁。
6) IPA、「情報セキュリティ人材の育成に関する基礎調査-調査報告書-」、
http://www.ipa.go.jp/security/fy23/reports/jinzai/documents/jinzai.pdf
7) NISC、「情報セキュリティ人材育成プログラム」、
http://www.nisc.go.jp/active/kihon/pdf/jinzai2011.pdf
8) NISC、「人材育成・資格制度体系化専門委員会報告書―人は城、人は石垣、人は堀―」、
http://www.nisc.go.jp/conference/seisaku/training/common/pdf/training_report_final.pdf