

# 情報セキュリティ人材のキャリアデザインと人材育成

花田 経子†

†新島学園短期大学  
370-0068 群馬県高崎市昭和町 53  
k-hanada@mail.neesima.ac.jp

あらまし 企業経営において、情報セキュリティは大変重要であるものの、情報セキュリティ人材はまだ人数も少なくそれを養成することは難しいとされている。その主な理由は、彼らが一般のIT技術者と同じキャリアパスをたどることが難しく、人材育成体制も整備されていないためである。本研究では情報セキュリティ人材のキャリアデザインについて、さまざまな立場の経験者にヒアリングを実施し、彼らのキャリアパスとワークキャリアにおける内的キャリアを分析し、そこから彼らにとって必要なキャリアデザインと人材育成のありかたについて論じている。

## A study of information security staff's career design and human resource development.

Kyoko Hanada†

†NIHJIMA GAKUEN JUNIOR COLLEGE  
53 Syowa-machi, Takasaki City, Gunma 370-0068, JAPAN  
k-hanada@mail.neesima.ac.jp

**Abstract** In Enterprise Management, information security is very important. However, the number of information security staff is insufficient in a lot of enterprises. Because there is a problem in the information security staff's career design, it is very difficult to bring up the security staff. In this paper, I describe their career designs and human resource development.

### 1 はじめに

組織に属しそこで働く人々にとって、共通する課題としてキャリア(Career)の問題が取り上げられるようになって久しい。本稿で特に取り上げる情報セキュリティ人材を含めた広義でのIT人材はキャリアを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”とみなされることが多く、IT技術者自身も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。特に、2010年前後から日本国内では、情報セキュリティに関与する人材の不足が叫ばれるようになり、それらを増加させることが情報セキュリティ政策の一環であるという主張が多く見受けられるようになった。したがって、IT人材の中でも特に育成が遅れているとされている情報セキュリティ人材に関してはその人材育成だけではなく、

働いている人たちのキャリアデザインにも着目した上で望ましい人材育成のあり方を検討する必要がある。本稿では、一般的なキャリアデザインおよび IT 人材のキャリアデザインに関する概念を整理した上で、情報セキュリティ人材についてそのキャリアデザインの事例や人材育成について述べることにする。

## 2 IT 人材のキャリアデザイン

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、ワークキャリア (仕事を中心としたキャリア) とそれを下支えるライフキャリア (人生全般を示したキャリア) の双方を踏まえた中での “人生や仕事の意識化” として定義している。したがって、本稿では情報セキュリティに関与する人材 (これはそれらを専業とする人だけではなく、その業務に関与する人材を含めている) において、それらのキャリアデザインと人材育成の問題を検討している。これらの人材にとって、情報セキュリティという仕事がそれぞれの主としてワークキャリアにおいてどのような存在であるのか、それを自身の内外において意識化することが、本稿で論ずる “情報セキュリティ人材のキャリアデザイン” である。

また、キャリアデザインはその形式から下記の 4 つに分類することができる。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、この中で目標逆算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。

キャリアデザインの問題を論ずる際に、スキルとキャリアパスの関係を明示する必要がある。表 1 は、情報セキュリティ人材を含む広義の IT 人材に求められるスキルである。

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

表 1 IT 人材に求められるスキル

これらのスキルは、従来学校教育では定着が不十分であったこと、非 IT 技術者よりも多くの専門性を求められることから、表 1 における①や②に関しては採用後に社内における人材育成過程を通じてスキルの習得とレベル向上をめざすことが一般的であった。日本的雇用慣行とも整合性の合うこのような人材育成スタイルを伝統的育成モデルとして図 1 で示す。図 1 の伝統的育成モデルは、ウォータフォールモデルを用いた開発工程が主流の時代には、一般的な方法として広く定着し、現在でも多くの企業ではこの伝統的育成モデルを主として社内の人材育成を行なっている。ここでは、キャリアにおける職務の変遷とスキルレベル、業務経験年数が密接にリンクしており、そこから IT 技術者

特有の“キャリアアップを前提とした職務の変遷”が行われるようになった。企業側も、IT 技術者の側も双方が、この育成モデルを前提としてキャリア形成を行なっていくため、年齢を経っていくと IT 技術そのものよりもその枠組を形成していく設計部門や管理部門の方にキャリアパスをシフトしていく傾向が強くなり、それが前提となっている。筆者は、主にこれまで広義の IT 人材の中でシステム監査人のキャリアデザインについて調べてきたが、この人材育成伝統的モデルの中ではシステム監査人は上流工程を経験し、ほぼ技術系職務の経験をする必要性がなくなった人材が従事するキャリアとしてキャリアパスが形作られていた。システム監査人になった時点でおおむね 40 代後半～50 代であり、その後のキャリアパスを IT 技術者として経験するケースは非常に稀であった。一方で、セキュリティ人材に関しては、そもそも 1990 年代初頭まではセキュリティそのものの専門家は数少なく、システム監査人以上にそのキャリアパスの形成については検討されていない。

みを形成するなど、特に 2005 年以降 IT 技術者のキャリア形成に対して一定の見解を示している。このような ITSS 等の流れを受けて、現状での IT 技術者のキャリアパスを明示したものが図 2 である。この図 2 では、情報セキュリティ人材は専門職として、高いスキルレベルに位置づけられ、高度なスキルとネットワークやデータベースといった近年特に重要とされるようになったシステムの仕組みに精通している必要があるとされている。

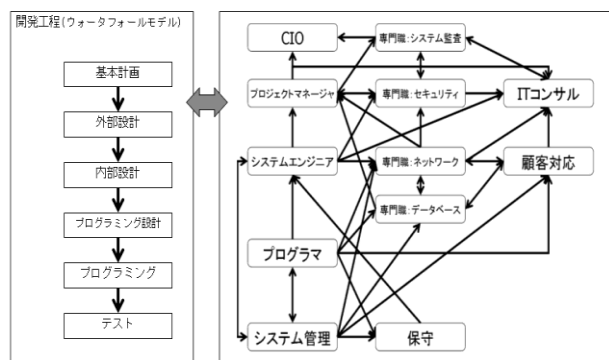


図 2 IT 技術者のキャリアパス現代的モデル

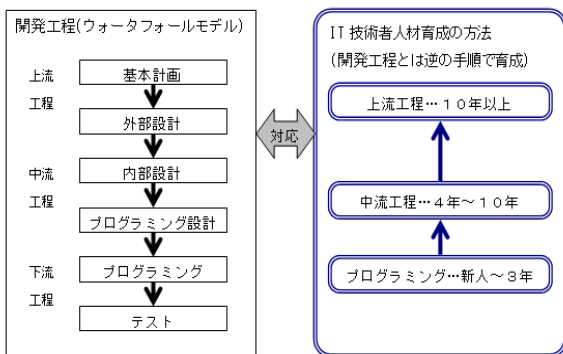


図 1 IT 技術者の人材育成伝統的モデル

しかし、近年のように開発工程でのウォーターフォールモデル等の採用が減り、IT 技術者の専門性も細分化され、加えてセキュリティ概念の高まりによって、図 1 の人材育成伝統的モデルの枠組みの中でキャリアパスを設定し、人材育成とあわせて実施していくことが難しくなった。そこで、経済産業省や IPA などが中心となってそれまでも存在していた情報処理技術者試験制度を再整備し、IT スキル標準(ITSS)の枠組

### 3 情報セキュリティ人材の世代と求められるスキル

特定の職業のキャリアデザインを研究する際に、そのキャリアパスに対するさまざまな影響を考慮しなければならない。特に重要なのが、世代・年代の考慮である。セキュリティは基礎研究として暗号理論などの研究は古くから行われ、またコンピュータウィルスの登場以降ウィルス対策などを中心としたセキュリティベンダーも登場しているが、そういう企業以外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。それ以前において、現在のセキュリティ概念で求められるような機密性や安全性、可用性、信頼性といった概念は、例えばシステム監査において当然のように重要視されており、またシステムの開発や運用といった現場においてもある程度組み込まれた形で検討されることは当然

のこととされた。特に、基幹系システムにおいては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。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のように区分する。

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)

表3 セキュリティ業務開始時期による年代区分

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、従事している人もおり、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76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。

このような中で、情報セキュリティ人材はどのようなスキルを求められているのかについては、IPAの調査報告書やNISCなどである程度明記されている。IPA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。IT技術力の中身は、本稿の表1とほぼ同様のものであるといえよう。一方で、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 事例から分析した情報セキュリティ人材のキャリアパス

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3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ーレベル/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。

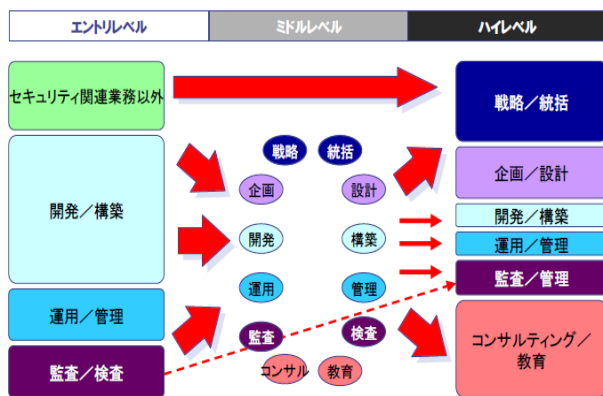


図3 IPA 報告書に基づく情報セキュリティ人材のキャリアパスモデル

実際に、このキャリアパスモデルを形成するには60人ほどの日本国内で活躍する著名な情報セキュリティ人材に調査をしており、これより個々の職務についてはさらに詳細なキャリアパスのモデルが示されている。このキャリアパスモデルは、とても詳細な調査の上で形成されたものであるため多くの情報セキュリティ人材に

受け入れられているようである。ただ、このキャリアパスモデルでは、情報セキュリティ人材としてのキャリアが上位レベルのキャリアであるというような誤った捉えられ方がなされるリスクも含まれている。これは、当該キャリアパスモデルの形成に際して、IT 人材のキャリアデザインに根強く残る“目標逆算型キャリアデザイン”を前提にしたキャリアパスモデルを作成しているからである。しかし、実際に各事例の人物を詳細に調べると、目標逆算型キャリアデザインによるキャリア形成をしている人物は非常に少ない。偶然活用型や節目重視型のキャリアデザインであることが多い。

筆者は、これまでシステム監査人について IPA 報告書が提示したキャリアの事例と同様な事例調査を独自に実施している。過去の事例研究では、現在システム監査を実施している人材および過去にシステム監査を実施した経験のある人材を中心に10数名の人物にキャリアの形成過程を外的ワークキャリアおよび内的ワークキャリアの両方の側面からヒアリングを実施した。その結果として、監査スキルとITスキルの2つの側面から関連人材についてのキャリアパスを示すと図4のように例示できる。

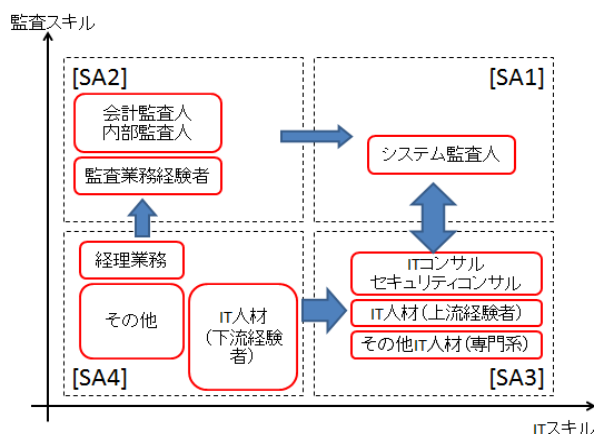


図4 監査スキル/ITスキルから見る関連人材のキャリアパス

キャリアのパスと事例の調査から、システム監査人の場合はその多くが“結果としてシステム監査人になった”人材であることがわかった。キャリアデザインの類型で示すならば、“偶然

活用型キャリアデザイン”や“節目重視型キャリアデザイン”が該当する。システム監査人になるためのキャリアパスとして選択できるパスの種類が非常に狭く、したがって“目標逆算型キャリアデザイン”によるキャリア形成が実現しづらい環境にあることがその主な要因といえる。加えて、求められるスキルが大変広範囲(IT人材に必要なスキルに加えてシステム監査を実現させるためのスキルが求められる)なため、それらを習得するための仕組みが必要であるが、整備されていない。したがって、人材育成としてはキャリアパスが選択しづらい上に、スキルを習得できないという状況下では、機能できないといえる。しかし、事例研究で多くの監査人や監査経験者がシステム監査スキルを“ITと経営の橋渡し”として重要視し、ITガバナンスに寄与することで職業人としての内的キャリアを充足させていることもわかった。そこで、彼らのこれまでのキャリアやヒアリングの結果から、システム監査において最も必要な“本質的なスキル”を整理したのが図5である。

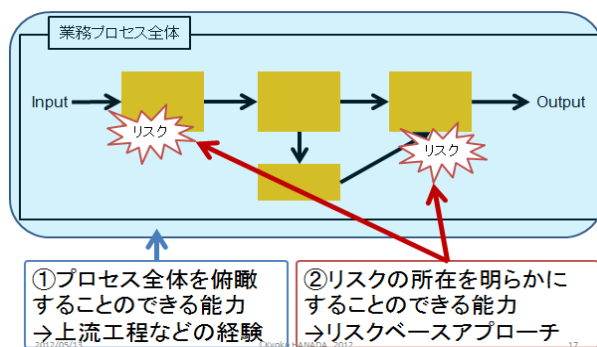


図5 本質的に求められているシステム監査人のスキル

システム監査人としては、プロセス全体を適切に俯瞰できる能力と、その中に含まれるリスクを見いだすことが最も重要である。そして、これはシステム監査人としてそのキャリアを維持していくためにはとても重要なスキルであると同時に、他のIT人材や非IT人材においてもこのスキルを保有することが経営において有益であるといえる。したがって、システム監査人その

ものの人材育成を考慮するよりは、まずはじめに図5で求められる根源的なスキルをまず醸成した上で、システム監査人としてのキャリアを選択した(あるいは配属された)人材について、システム監査の個々の細かいスキル(監査スキル)を習得していくほうが、経営にとっても、キャリアを形成していく人材本人にとっても現実的であろう。

これらのシステム監査人のキャリアに関する調査と同様に、情報セキュリティ人材についてもIPA調査報告書とは別途、著者独自に20名ほどの人物に対して、キャリアの形成過程を外的ワークキャリアおよび内的ワークキャリアの両方の側面からヒアリングを実施した。この中には、一部IPA調査報告書でとりあげられた60名の方と一致している人物も含まれている。IPA調査報告書および著者独自に実施したヒアリングの結果を元に、図4と同様の形態で情報セキュリティ人材のキャリアパスを示したものが図6である。

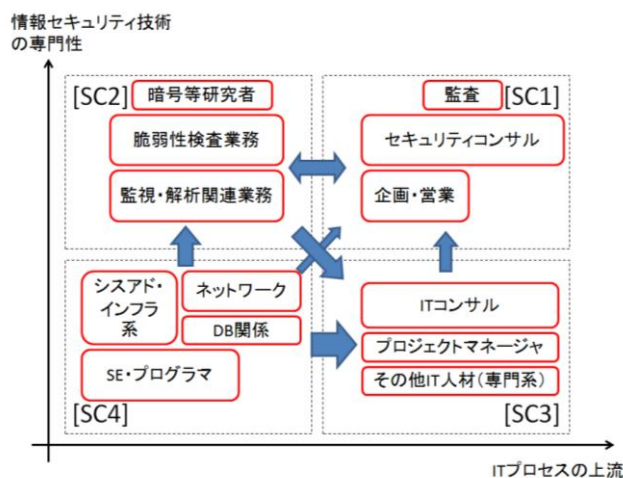


図6 情報セキュリティ技術の専門性/ITプロセスの工程から見る関連人材のキャリアパス

図4との比較を考慮すれば、図6の情報セキュリティ人材のほうがよりキャリアに至る選択肢が広いように見受けられる。しかしこれは、情報セキュリティ人材の職業としての分類が、システム監査人よりも幅広いためであり、選択肢が広いわけではないといえよう。

IPA報告書ではあまりとりあげられていない

が、著者のヒアリングからは SC4 から SC2 方向へのキャリアパスを選択した人物の多くが、組織内でのマネジメントを避ける傾向にある。日本の企業形態では、ある一定の年齢層や職階があがることで、所属グループの人的マネジメントを必然的に要求されることが多い。SC2 に属する人材の多くが、その人的マネジメントに従事していない。したがって、そこからコンサルや監査・企画や営業といったマネジメント能力を要求される職種にキャリアを転換するケースもあるものの、あまり内的キャリアが充足されていないことが多い。一方で、SC1 から SC2 にキャリアを転換する人材の多くは、人的マネジメントを避けて技術職として残りたいという要望が多い。SC2 のキャリアパスから他の転換が成功するためには、マネジメント能力が適切にあるかということが重要である。SC2 に属し、そこから別の象限へのキャリアパスを模索しない人材の多くは、マネジメント能力の有無にかかわらず、マネジメント能力を自身の職業遂行の上で重要視することを嫌う。そのため、SC2 にとどまる人が多い。SC2 を選択する人材の内的キャリアとして、情報セキュリティに直接関係しない人的マネジメントに自身のリソースを割くことは好まないということがその背景にあらう。こういった、内的キャリアも配慮したスキル形成・キャリアパスモデルの提示を実施して行くことも求められよう。

## 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、「米国におけるシステム監査の展開：1950 年代から 1970 年代までの文献をめぐって」、『名古屋文理短期大学紀要』第 20 号、名古屋文理短期大学、1995 年、1-9 頁。
- [3] 鳥居壮行稿、「システム監査研究の黎明期」、『文化情報学：駿河台大学文化情報学

部紀要』第 15 号 2、駿河台大学文化情報学部、2008 年、3-25 頁。

[4] 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。

[5] 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。

[6] 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。

[7] 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。

[8] 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>

[9] 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>

[10] 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](http://www.nisc.go.jp/conference/seisaku/training/common/pdf/training_report_final.pdf)