

# 情報セキュリティ教育の現状と人材育成

花田 経子†

岡崎女子大学 子ども教育学部†

## 1. はじめに

2016年2月1日よりサイバーセキュリティ月間  
 が開始され、2月2日には、新たな枠組みを制定  
 するための改正法案（サイバーセキュリティ基  
 本法及び情報処理の促進に関する法律の一部を  
 改正する法律案）が閣議決定された。この中で  
 特に取り上げられているのが、情報セキュリ  
 ティに関与する人材の確保と育成についてである。  
 情報処理の促進に関する法律の改正案の一部に  
 は、新たな資格制度の創設が盛り込まれ、『情  
 報処理安全確保支援士(仮称)』というような新  
 たな士業についても検討がなされている。また、  
 企業経営サイドにおいても情報セキュリティの  
 確保を事実上義務付けていく方向性には変わり  
 なく、そのためにもこのような状況に対応でき  
 るような人材育成が官民挙げて求められてい  
 るといえよう。IT化の進展によって、一般的  
 な産業だけではなく、すべての人の生活にお  
 ける安全の確保や財産の保持、サービスの享  
 受等を脅かす恐れのあるITリスクへの対応は  
 必須である。現状では諸説あるものの、日  
 本国内における情報セキュリティに関与する  
 人材は量・質ともに不足しているとされてお  
 り、これらの確保と人材育成については、学  
 校教育機関を含めすべてのサイドで連携し  
 て実施していく必要がある。本稿では、こ  
 れらの情報セキュリティに関与する人材に  
 対する育成の状況と教育における課題に  
 ついて、特に検討を行っている。

## 2. 情報セキュリティ人材の人材育成にお ける方向性～NISCの戦略より

情報セキュリティに関与する人材(以後、情報  
 セキュリティ人材)に関する調査データとして用  
 いられているものとしては、情報処理推進機  
 構(IPA)が2012年4月に『情報セキュリティ人材の  
 育成に関する基礎調査』がある。当該報告書は、  
 主にWebアンケートを通じて国内企業の情報セ  
 キュリティ専任人材がおおむね何人であるかを推  
 計値として算出し、公表している。その結果に  
 寄れば、国内企業の情報セキュリティ専任人材  
 は約23万人と推計し、そのうちの13.7万人がス

キル不足であると発表されている。加えて、そ  
 れらのスキルを充足していく必要性に加えて、  
 今後の情報セキュリティに関するマーケットの  
 拡大を見込んで新たに新規(新卒)で2.2万人の  
 人材を高等教育機関は輩出していく必要性があ  
 るとも述べている。

段階	手法	目指す人物像
高等教育・職業能力開発	基礎理論と実践演習の双方を実施、職業訓練としてのリカレント教育もあり	①ハイブリッド型人材の育成(経営と実務の橋渡し)
初等中等教育	情報活用の実践力、情報科学の基礎的理解、教員向けの指導力向上など	②すべての人にとって必要
突出した専門家の育成	専門的な研究機関(大学院等)での研究、専門的な競技、人的ネットワークの形成	③突出した能力を有しグローバルに活躍できる人材
各キャリアのロールモデル	それぞれにおけるロールモデルとなる人物の形成、キャリアパスの形成に必要なスキルセットの提示	④キャリアパスの俯瞰化ができスキルセットを明示できる人材
組織力強化	組織の壁を越えたコミュニティ形成	⑤人的ネットワークの形成

表1 サイバーセキュリティ戦略にて取り上げられている人材育成の方向性  
 (当該資料を基に筆者が作成)

この調査データが国内の情報セキュリティに  
 関係する部署・企業等に与えた影響は大きく、  
 NISC や経済産業省等のサイバーセキュリティ政  
 策の在り方にも大きな影響を与えた。たとえ  
 ば、2015年9月に閣議決定された『サイバーセ  
 キュリティ戦略』では、情報セキュリティ人材  
 の育成に関して、表1の方針を定めている。

情報セキュリティ人材の育成の中で、まずは

②のように初等中等教育での人材育成を基本としながら、①や③の人材を高等教育機関で育成していくべきだという方針が示されている。②で求める初等中等教育での人材育成については、2002年からの高等学校における教科情報の必修化、2012年以後に適用された最新の学習指導要領により、情報モラル教育が進められてきている。しかし、特に高等学校における教科情報については、様々な課題が指摘され改善が進んでいないこともあり、まずは教員養成についての課題を解決する必要がある<sup>1</sup>。したがって、②の教員養成も高等教育機関は担わねばならない。④および⑤については、一般的には産業界での人材育成を前提としているものの、人材育成においてはキャリアパスを考慮した形でカリキュラムを編成しなければならないため、結果的にこれらの要素も高等教育機関で対応すべき事項となりうる。しかし、これらの高等教育機関に求められる事項がすべて可能であるのかについては、十分な検討が必要である。

ある特定の職能に関する人材の育成については、一般的には初等中等教育では全般的かつ総合的な知識・技能を習得させるにとどめ、より具体的かつ専門的な技能に関しては高等教育機関における教育課程か、職業者として従事した企業・団体等での人材育成の枠組みの中で実施されることが多い。特に、情報セキュリティ人材を含むIT技術者の人材育成は、図1のパターンが一般的であり、高等教育機関における情報教育の枠組みが十分に発揮されていなかった。

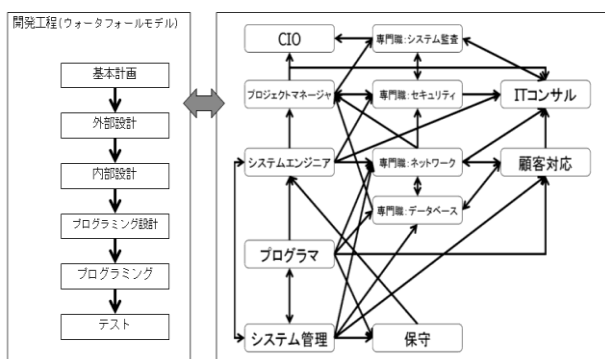


図1 IT技術者のキャリアパス現代的モデル

したがって、今現在情報セキュリティ業務に従事している要員の大半は高等教育機関におい

て情報セキュリティ人材として育成されてきたわけではなく、大多数が基本的な情報処理に係る技能・知識を高等教育機関あるいは企業内の研修において身に着けたうえで、業務上の必要性から社内研修・社外研修・独学等によってスキルを習得している。NISCが表1の方向性で人材を確保していくのであれば、高等教育機関において抜本的な教育課程の見直しが行われなければならない。

### 3. 高等教育機関における情報セキュリティ教育の現状

高等教育機関のうち、大学院教育では情報セキュリティに関連する科目設置・学科の設置は2012年のIPAによる報告書以降、増加傾向にある<sup>2</sup>。情報セキュリティ大学院大学のように情報セキュリティに特化した大学院をはじめ、社会人のリカレント教育を主とした東京電機大学の国際化サイバーセキュリティ学特別コースなど、特色あるカリキュラムを構成した大学院が多い。これは、大学院教育では表1の①や③の人材を輩出し、これらの人材にとってのコミュニティの一環としての位置づけを担うよう求められているためでもある。2012年から文部科学省が3年度分の予算を立てて実施した『情報技術人材育成のための実践教育ネットワーク形成事業—分野・地域を越えた実践的情報教育協働ネットワーク』(通称、enPiT)にも、セキュリティ分野の『SecCap』がある。SecCapでは、5つの連携大学(情報セキュリティ大学院大学、奈良先端科学技術大学院大学、北陸先端科学技術大学院大学、東北大学、慶應義塾大学)が中心となって多彩な講義科目と演習科目を用意している。特に、演習科目は脆弱性診断業務演習やデジタルフォレンジック演習、ハードウェアセキュリティ演習、インシデントレスポンス演習、BCP演習等のこれまでの大学院での通常講義では実施されてこなかった演習が多い。これまでより実践的な形で突出するセキュリティ人材を育成してきた『セキュリティ・キャンプ』

(経済産業省主催)の修了生なども、当該SecCapのコースを受講する事例が増えている。

文部科学省は、これらの状況を踏まえ、また次のオリンピック(東京オリンピック)等の諸問

<sup>1</sup> 例えば、情報科の免許を保持した教員の採用や更新講習の実態に関しては、中野[2014]などで論じられている。

<sup>2</sup> 2011年11月1日に東京電機大学にて開催された日本セキュリティ・マネジメント学会第24回学術

講演会にて、吉浦裕氏(電気通信大学)により情報セキュリティに特化した科目の設置が、東京近郊では3大学の大学院に限定されているという発言があった(筆者講演メモより)。現状ではこれよりも増加している。

題への対応も含めて、教育課程において情報セキュリティ教育への対応を少しは進めている。先般2月2日の閣議決定に含められる案件の一つとして、文科省はSecCapの学部教育での実施と、高専（高等専門学校）におけるサイバーセキュリティに関する教育課程の推進を検討しており、特に高専ではサイバーレジ演習などの実施などより具体的な技術者育成のための施策をいくつか検討している。このような点は、先の表1における①の人材や③の人材の育成には寄与できる可能性はある。

一方で、これらに該当しない一般的な学部教育では情報セキュリティ教育はまだ進展していない。突出した人材の多くが関係している『セキュリティ・キャンプ』では、2013年以降大学生(学部生)の在籍比率が増えておりほぼ6割近くになっている。これらの出身大学をさらに詳細に検討すると、私立大学と首都圏近郊の大学出身者が過半数を超える。情報セキュリティに関する学部教育では地方の国立大学では十分な教育が実施されていない可能性がある。しかしながら、地方の国立大学出身者の多くは、地元自治体職員や地元ユーザ企業で意思決定を担う人材となっていくケースが多い。それゆえ、彼らの情報セキュリティに関する教育が適切に実施されていなければ、地方の自治体やユーザ企業の情報セキュリティレベルは低いままとなかなかねないリスクをはらむ可能性がある。また、同様に地方の国立大学出身者が、教職課程を経て、教員として初等中等教育に従事することもふまえ、前述した表1の②の人材を底上げするための教員の養成も重要課題となりうる。

そこで、予備調査としてまず地方の国立大学(国立大学法人)のカリキュラムに情報セキュリティに関する内容がどの程度含まれているのかを、2015年度版の各大学が公開するシラバスから調査しとりまとめたものが表2である。

科目内容(分野別)	科目数
セキュリティマネジメント	5
セキュリティ基礎	1
ネットワーク	8
暗号	5
医療情報	6
情報法	1
情報倫理	26
図書館情報	1
総計	53

表2 情報セキュリティに関する科目数(北海道・青森県・岩手県)

表2で取り上げた北海道と青森県、岩手県に

ついては、『セキュリティ・キャンプ』の大学生による応募が比較的少ない都道府県ということで上げている。また、これらの掲載した科目のシラバスにおいて、15回の構成からおおむね情報セキュリティの内容がどの程度取り上げられているかを表したものが表3である。

科目にしめるセキュリティ分野の割合	科目数
10%	14
20%	18
30%	14
50%	3
80%	1
100%	3
総計	53

表3 科目内にしめる情報セキュリティ分野の割合

特に地方の国公立大学における情報関連科目の取り扱い方が、表2および表3に現れている。本稿ではカウントしていないが、ほとんどは全学共通科目として情報センターにおいて基礎科目として情報関連科目が位置付けられており、その中では、情報モラルを中心とした情報倫理教育の一部にとどめられているのが現状である。一部工学部等の情報学科は別だが、その他の学部ではそれ以上の科目が設置されていることはまれである。表1の①、②、③、④、⑤のそれぞれの人材育成を高等教育機関において担うというのは現状では難しく、したがって、それを補うためには企業内における人材育成の枠組みを用いるしかないともいえよう。

## 参考文献

- [1] 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>、2012.4.27アクセス
- [2] NISC、「サイバーセキュリティ戦略」、<http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf>、2015.11.5アクセス
- [3] 中野由章・中山泰一稿、「高等学校情報科教員の現状－その問題点と我々にできること－」、『情報処理』Vol.55、No.8、情報処理学会、2014年、872-875頁。
- [4] 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。
- [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] SecCap、「SecCapについて」、  
<<http://www.seccap.jp/about/>>、2015年11月6日アクセス。