

情報セキュリティに関する 人材育成活動の調査結果

2011 年 3 月

NTT データ経営研究所

- 目次 -

1	人材タイプⅠ「作る」	1
1.1	政府機関の取り組み	1
1.2	教育機関による取り組み	9
1.3	各種法人・団体による取り組み	10
2	人材タイプⅡ「使う」	13
2.1	政府機関の取り組み	13
3	人材タイプⅢ「教える」	14
3.1	政府機関の取り組み	14
4	海外における情報セキュリティに関する人材育成活動	15
4.1	米国における取り組み	15
4.2	英国における取り組み	23
4.3	欧州（EU）における取り組み	23
4.4	ドイツにおける取り組み	25
4.5	韓国における取り組み	25
4.6	中国における取り組み	27
4.7	インドにおける取り組み	28

1 人材タイプ I 「作る」

1.1 政府機関の取り組み

○経済産業省

・情報セキュリティ専門家および情報セキュリティ人材の育成

監査分野等における情報セキュリティ専門家の育成を行っているほか、文部科学省と連携して、情報セキュリティ人材を含めた高度 IT 人材の育成を行っている。産業界出身教員等を対象とした教育プログラムの実証や、実践的なインターンシップの実証等を推進するための産学連携体制を強化する。また、大学院において産学連携により高度セキュリティ人材育成プログラムを開発実施する。

・若年層からの高度セキュリティ人材の育成

若年層に対し、セキュリティ意識の向上と優れたセキュリティ人材の発掘と育成を図るため、産業界の第一線で活躍する技術者を講師とした実践的な講義等を合宿形式で実施する。

○文部科学省

・先導的 IT スペシャリスト育成推進プログラム

世界最高水準のソフトウェア技術者として求められる専門的スキルを有する企業等において先導的役割を担う人材を大学院において育成するための教育拠点の形成を支援する政策である。

大学名等	研究科名等	プロジェクト名称	概要
◎筑波大学	システム情報工学研究科	高度IT人材育成のための実践的ソフトウェア開発専修プログラム	世界最高水準の先導的ITスペシャリストを育成するために、実践的ソフトウェア開発技術の教育拠点を形成する。筑波大学大学院システム情報工学研究科コンピュータサイエンス専攻を核として、電気通信大学、東京理科大学、産業界との有機的連携により、組み込みソフト系及びエンタープライズ系人材の育成のための実践的ソフトウェア開発専修プログラムを設け、実習やプロジェクトワークに重点をおいた教育を実施する。
電気通信大学	電気通信工学研究科		
東京理科大学	理工学研究科		
◎東京大学	情報理工学系研究科	情報理工実践プログラム	「情報理工実践プログラム」では、社会を先導する独自のソフトウェアを開発することのできる技術創造人材を見出して開発実践に導くとともに、ソフトウェア開発の下流から上流までを俯瞰して開発過程を設計することのできる開発設計人材を養成する。基盤カリキュラムと先端的ツールを活用し、産学連携による実践工房において、技術創造と開発設計の相乗効果による先導的ITスペシャリスト育成を達成する。
東京工業大学	情報理工学研究科		
国立情報学研究所	アーキテクチャ科学研究系		
◎名古屋大学	情報科学研究科	OJLによる最先端技術適応能力を持つIT人材育成拠点の形成	計算科学及び情報通信の基礎の上にソフトウェア工学を系統的に修め、最先端ソフトウェア技術に柔軟に適用し、その応用及び技能への転化を可能にする人材の教育プロジェクトを提案する。ソフトウェア工学をメタ技術の観点から教授し、それを実際のソフトウェア開発へ適用するメタ技術展開力を、PBLとOJTの融合概念と位置付けるOJL(On the Job Learning)により涵蓋する教育カリキュラムである。
南山大学	数理情報研究科		
愛知県立大学	情報科学研究科		
静岡大学	情報学研究科		
◎大阪大学	情報科学研究科	高度なソフトウェア技術者育成と実プロジェクト・教材開発を実現する融合連携専攻の形成	情報通信技術、特にソフトウェアの高度な技術者育成を目標とし、ソフトウェア工学分野で教育・修得すべき内容をより豊富にかつ体系的・実践的に教育課程に取り込むため、関西圏の情報系7大学院に分散している該当分野の卓越した専門家群を結集し、融合連携型専攻を構築する。特に重要視する実践的教育については、参画企業と協働して、教科書的課題ではなく現実の開発プロジェクトそのものを教材として開発し、適用する。
京都大学	情報学研究科		
高知工科大学	工学研究科		
奈良先端科学技術大学院大学	情報科学研究科		
兵庫県立大学	応用情報科学研究科		
立命館大学	理工学研究科		
和歌山大学	システム工学研究科		
神戸大学	自然科学研究科		
大阪工業大学	情報科学研究科		
◎九州大学	システム情報科学府		
九州工業大学	情報工学研究科		
熊本大学	自然科学研究科		
宮崎大学	工学研究科		
◎慶應義塾大学	政策・メディア研究科	先端ITスペシャリスト育成プログラム	慶應義塾大学、早稲田大学、NTT、日本IBM、Mozilla Japanの産学NPO連携により、先端ネットワーク、大規模分散システムや新IT応用システムを構築でき、実践的ITスキルを備えたスペシャリストを養成する。特に、学生参加型の研究プロジェクトやインターンシップを通じて実践的な力を養い、合同プロジェクトレビューにより、幅広い視点でシステムを分析・評価・検証でき、先導的な役割を担える人材を育成する。
早稲田大学	理工学術院		
中央大学	理工学研究科		
情報セキュリティ大学院大学	情報セキュリティ研究科		

図 プログラム採択大学一覧¹

¹ http://www.mext.go.jp/b_menu/houdou/18/09/06092715/002.htm

・「研究と実務融合による高度情報セキュリティ人材育成プログラム」(ISS スクエア)²

情報セキュリティ大学院大学、中央大学、東京大学、国立情報学研究所他、企業・研究機関 11 社の産学連携による研究と実務を融合した人材育成プログラム。文部科学省の「平成 19 年度先導的 IT スペシャリスト育成推進プログラム」に採択され、平成 20 年度より開設した。

大学院修士課程の学生を対象に、先導的 IT スペシャリスト育成推進プログラムを実施している。修了者には、情報セキュリティ・スペシャリスト・サーティフィケート (ISSCertificate) が授与され、毎年、3 研究科で合計 30～40 名程度の高度情報セキュリティ人材育成を予定している。

<育成対象>

- ・ 高度情報セキュリティ実践リーダー・・・情報セキュリティ全般の確実な知識を持ち、企業活動や国の安心・安全を確保する観点から、実社会の正確な状況認識のもとに、CIO/CISO として組織の情報政策をリードできる人材
- ・ 高度情報セキュリティ研究・開発者・・・情報セキュリティ全般の知識を備え、優れた基礎能力を駆使して問題の本質を把握し、場当たりでない抜本的な情報セキュリティ対策や基盤技術を創出・先導できる人材

<科目>

- ・ 共通科目・・・情報セキュリティに関する総括的な考え方を身に付けるための科目群。情報セキュリティ各分野の諸課題について、学会・産業界の有識者・実務家がオムニバス形式で講義を実施
- ・ コア科目・・・6 分野について情報セキュリティの基盤となる中核知識を身に付けるための科目群。授業形式
- ・ フィールド科目・・・実務家としての不慣れ専門知識や研究のための知識・技術を身に付けるための科目群

² <http://iss.iisec.ac.jp/>



図 プログラム体系³

科目群	授業科目名
暗号・認証	暗号プロトコル(情) / 暗号と電子認証(中) / 情報セキュリティ(東) / 計算システム検証論(東)
ネットワーク	インターネットテクノロジー(情) / ネットワークセキュリティ(中) / インターネット工学(東)
システム	セキュアシステム構成論(情) / オペレーティングシステム特論第二(中) / 情報セキュリティ基盤論(東)
ソフトウェア	セキュアプログラミングとセキュアOS(情) / 高信頼プログラミング(中) / 計算機言語システム論(東) / セキュリティ要求分析(NII)
マネジメント	情報セキュリティマネジメントシステム(情) / セキュリティシステム監査(情) / 情報セキュリティ監査(中)
法制・倫理	セキュア法制と情報倫理(情) / 電子社会の法と経済(中)

※ (情)= 情報セキュリティ大学院大学、(中)= 中央大学、(東)= 東京大学、(NII)= 国立情報学研究所

図 コア科目⁴

³ <http://iss.iisec.ac.jp/>

⁴ <http://iss.iisec.ac.jp/>

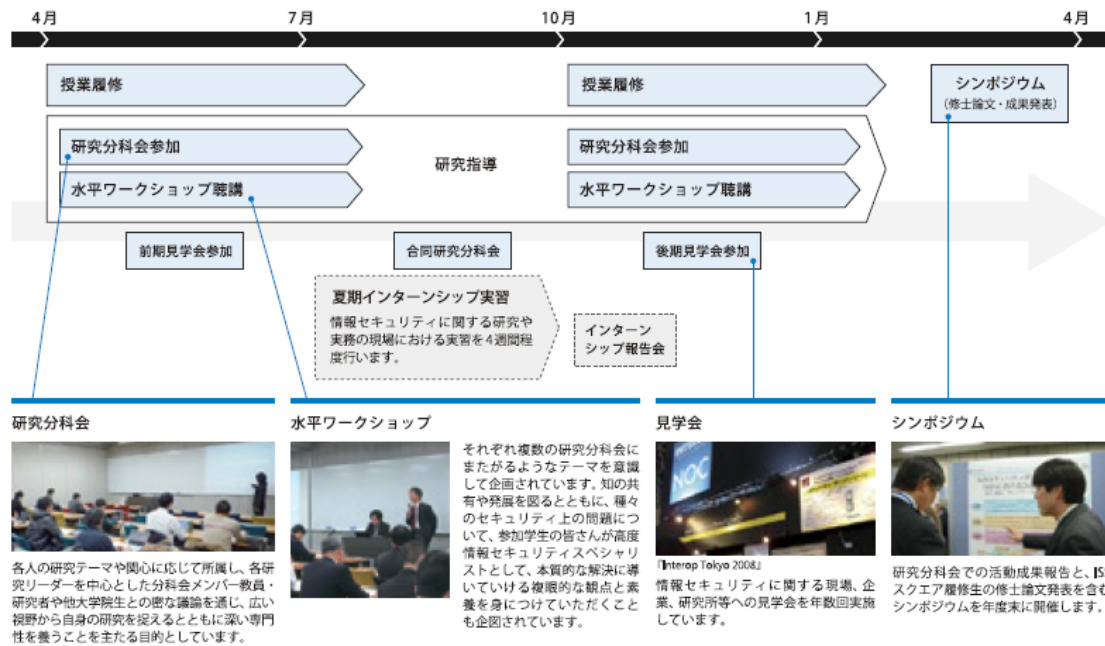


図 年間活動スケジュール⁵

⁵ <http://iss.iisec.ac.jp/>

・ IT Keys ((IT specialist program to promote Key Engineers as security Specialists))
プロジェクト

奈良先端科学技術大学院大学、京都大学、大阪大学、北陸先端科学技術大学院大学の情報系 4 大学院の教員と、情報通信研究機構、情報セキュリティ研究所、JPCERT コーディネーションセンター、NTT コミュニケーションズの 4 企業・団体の実務者の力を結集することにより、高度かつ実践的な情報セキュリティに係る人材の育成を可能とする産学連携型の教育プログラムである。文部科学省の「平成 19 年度先導的 IT スペシャリスト育成推進プログラム」の一つとして、平成 19 年 10 月に 3 年半の予定でスタートした。

教育コースでは、情報セキュリティ人材に求められるスキルマップの 16 のスキルを網羅的な実施のために、産学が連携してカリキュラムの実施を行っている。

<育成対象>

- ・ 最高情報セキュリティ責任者 (CISO: Chief Information Security Officer) ・ ・ 組織 (公的機関や企業等) において情報セキュリティ対策実施の責任者となる人材
- ・ 情報セキュリティ担当者 (CISO 補佐) ・ ・ ・ 組織 (公的機関や企業等) において実際に情報セキュリティ対策を立案しその実行を指示する人材

<科目>

- ・ 基礎科目 ・ ・ 大学院で指定するネットワーク関連及び情報セキュリティ関連の科目を各大学院にて受講する形式で、情報セキュリティに関する様々な仕組みを理解するために必要となる基礎的な情報科学や計算機工学・通信工学に関する知識を習得することを目的としている。
- ・ 先端科目 ・ ・ 情報セキュリティに関する最新の知識および法律面・倫理面・経営面など実務に必要な知識の習得を行うとともに、コンピュータネットワークの恒常的な革新に伴って現れる情報セキュリティの新たな問題にも対応できる能力を培うことを目的としている。
 - 情報セキュリティ運用リテラシー
 - 最新情報セキュリティ特論
- ・ 実践科目 ・ ・ 情報セキュリティ対策に関して豊富な知識・経験を有する情報通信研究機構、NPO 法人情報セキュリティ研究所、NTT コミュニケーションズ株式会社等の民間事業者および大阪大学が開催し、合宿形式 (不定期の集中講義) で行う。情報セキュリティに対する既知の脅威・攻撃に対して組織の規模や環境に応じた予防対策を行える能力、未知の脅威・攻撃に対して迅速かつ的確な対応を行い、永続的な対策を種々の観点から総合的に立案できる能力を培うことを目的としている。
 - 実践情報セキュリティ演習 (IT 危機管理演習、インシデント体験演習、

リスクマネジメント演習、無線 LAN セキュリティ演習、システム攻撃・
防御演習、・システム侵入解析演習など)

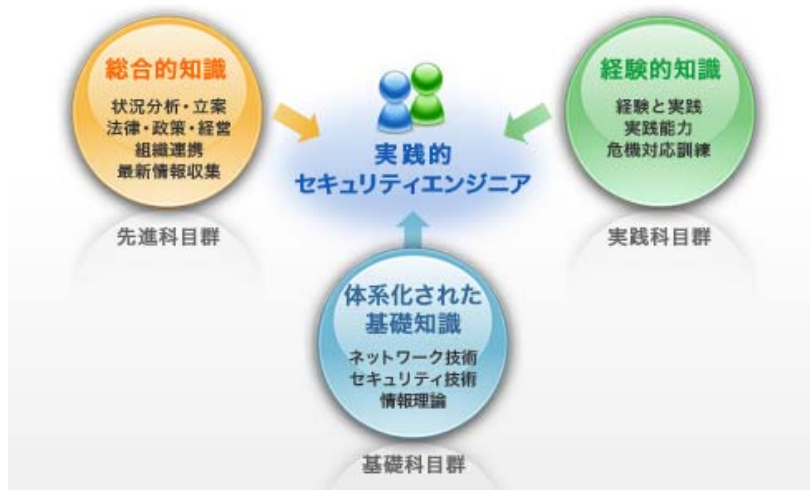


図 育成人材イメージと教育体系⁶

⁶ <http://it-keys.naist.jp/>

育成する人材に求められるスキルマップと各大学・団体・企業の担当分野

項 番	大分類	奈良先端科学 技術大学院大 学	大阪 大学	京都 大学	北陸先端科学 技術大学院大 学	情報 通信 研究 機構	情報セ キュリ ティ研 究所	JPC ERT /CC	NTTコ ミュニ ケーシ ョンズ
1	情報セキュリティマネジ メント						○	○	○
2	ネットワークインフラセキ ュリティ	○	○		○		○	○	○
3	アプリケーションセキユリ ティ			○					
4	OSセキュリティ			○	○			○	
5	ファイアーウォール	○		○	○				○
6	侵入検知			○	○			○	○
7	ウイルス				○				
8	セキュアプログラミング技 法	○							
9	セキュリティ運用	○	○	○			○		○
10	セキュリティプロトコル		○		○				
11	認証	○	○		○				
12	PKI		○		○				
13	暗号	○		○					
14	電子署名	○				○			
15	不正アクセス手法			○		○		○	
16	法令・規格			○		○	○	○	○
別 A	不正コピー防止と電子透か し		○						

(独立行政法人情報処理推進機構 情報セキュリティスキルマップをもとに作成)

図 育成する人材に求められるスキルマップと各大学・団体・企業の担当分野⁷

⁷ <http://it-keys.naist.jp/about/skill.html>

1.2 教育機関による取り組み

○情報セキュリティ大学院大学

情報科学、セキュリティ技術、管理運営、法制度・情報倫理の各分野の知識・スキルに関する科目を幅広く開設する。

科目区分	授業科目名	履修区分	単位数	修了所要単位数		
				博士前期課程	博士前期課程	博士後期課程
				2年制	1年制	
専攻	情報セキュリティ論講I	必修	2	24	42	-
	情報セキュリティ特別講義	必修	2			
	暗号・認証と社会制度	選択	2			
	暗号プロトコル	選択	2			
	アルゴリズム基礎	選択	2			
	数論基礎	選択	2			
	暗号理論	選択	2			
	計算代数	選択	2			
	個人識別とプライバシー保護	選択	2			
	インターネットテクノロジー	選択	2			
	不正アクセス技法	選択	2			
	ネットワークシステム設計・運用管理	選択	2			
	セキュアシステム構成論	選択	2			
	情報デバイス技術	選択	2			
	情報システム構成論	選択	2			
	オペレーティングシステム	選択	2			
	セキュアプログラミングとセキュアOS	選択	2			
	プログラミング	選択	2			
	ソフトウェア構成論	選択	2			
	セキュアシステム実習	選択	2			
	情報セキュリティマネジメントシステム	選択	2			
	セキュリティシステム監査	選択	2			
	セキュリティ管理と経営	選択	2			
	リスクマネジメント	選択	2			
	組織行動と情報セキュリティ	選択	2			
	統計的方法論	選択	2			
	セキュア法制と情報倫理	選択	2			
	法学基礎	選択	2			
	知的財産制度	選択	2			
	国際標準とガイドライン	選択	2			
	セキュリティの法律実務	選択	2			
	Presentations for Professionals	選択	2			
	統計的リスク管理	選択	2			
リスクの経済学	選択	2				
マスメディアとリスク管理	選択	2				
情報セキュリティ論講II	選択	2				
特設講義(ガバナンスとコンテンツジェンシー)	選択	2				
特設講義(セキュリティ監査)	選択	2				
特設講義(セキュアソフトウェア構成論)	選択	2				
特設講義(セキュリティ事故の対応と管理)	選択	2				
研究指導	研究指導	必修	6	6	-	-
	プロジェクト研究指導	必修	4	-	4	-
博士専門	情報セキュリティ特別研究	必修	6			
	情報セキュリティ博士演習	必修	2	-	-	8
	情報セキュリティ技術特論	選択	2			
	情報セキュリティ管理特論	選択	2			

図 開設科目一覧⁸

⁸ <http://www.iisec.ac.jp/education/curriculum.html>

○カーネギーメロン大学・兵庫県立大学

兵庫県立大学大学院応用情報科学研究科では、2011年4月から、新たに「高信頼情報科学コース」を設置し、同コース内で、カーネギーメロン大学と連携したダブルディグリー・プログラムを開始する(予定)。2005年よりアジアにおける情報セキュリティ教育研究拠点として、両大学が提携してカーネギーメロン大学日本校を運営していたが、2009年度末をもって終了し、その成果をダブルディグリー・プログラムという新たな形で情報セキュリティ人材の育成継続に繋げたものである。

このプログラムでは、兵庫県立大学在学中にカーネギーメロン大学の修士課程を履修し、合計2年間で両大学の学位を同時に取得できる。

1.3 各種法人・団体による取り組み

○JNSA

・「ISEPA」

日本と世界で、情報セキュリティに関する資格を認証する団体と、その資格のための教育を実践する団体を中心になって組織し、運営している団体。大学等の教育機関との連携、行政機関からのオブザーバ参加を得て活動を展開している。

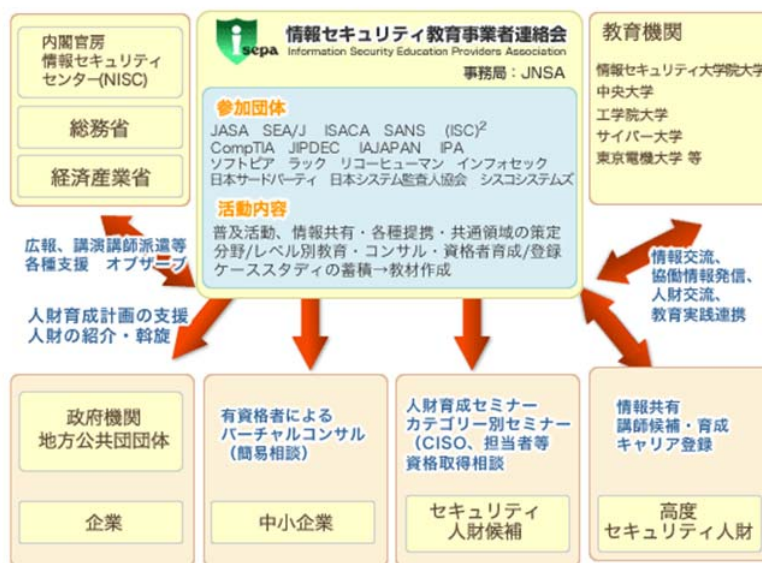


図 ISEPA の仕組み⁹

⁹ <http://www.jnsa.org/isepa/aboutus/outline.html>



図 制御システムセキュリティカンファレンス¹⁰

○情報処理推進機構（IPA）

・情報セキュリティスペシャリスト試験

情報処理技術者試験のうち、情報セキュリティに関する部分の試験である。本試験は高度 IT 人材として確立した専門分野をもち、情報システムの企画・要件定義・開発・運用・保守において、情報セキュリティポリシーに準拠してセキュリティ機能の実現を支援し、又は情報システム基盤を整備し、情報セキュリティ技術の専門家として情報セキュリティ管理を支援する者を対象とする。役割として、セキュリティ機能の企画・要件定義・開発・運用・保守を推進又は支援する業務、若しくはセキュアな情報システム基盤を整備する業務に従事し、次の役割を主導的に果たすとともに、下位者を指導する。

- (1) 情報システムの脅威・脆弱性を分析、評価し、これらを適切に回避、防止するセキュリティ機能の企画・要件定義・開発を推進又は支援する。
- (2) 情報システム又はセキュリティ機能の開発プロジェクトにおいて、情報システムへの脅威を分析し、プロジェクト管理を適切に支援する。
- (3) セキュリティ侵害への対処やセキュリティパッチの適用作業など情報システム運用プロセスにおけるセキュリティ管理作業を技術的な側面から支援する。
- (4) 情報セキュリティポリシーの作成、利用者教育などに関して、情報セキュリティ管理部門を支援する。

¹⁰ <http://www.jpCERT.or.jp/ics/conference2010.html>

○情報処理推進機構セキュリティーセンター（IPA/ISEC）

・「セキュリティ&プログラミングキャンプ」

22歳以下の学生・生徒を対象に4泊5日の合宿形式で行う、情報セキュリティおよびプログラミングの知識と技術を学ぶキャンプを行っている。キャンプにかかる費用、宿泊費、食事代（3食）、講義代、テキスト代、機器/施設使用料などはすべて主催者側で負担し、参加者は無料で参加することができる。プログラムの目的として、若年層のセキュリティ意識の向上と優秀なセキュリティ人材の早期発掘と育成、オープンソースやプログラミングの分野における優れた人材の早期発掘と育成を挙げている。



図 IPA の特設サイト¹¹

○JPCERT コーディネーションセンター（JPCERT/CC）

・「C/C++ セキュアコーディングセミナー」

プログラム開発者を対象に、セキュリティへの十分な配慮が必要なC/C++ 言語で脆弱性を含まない安全なプログラムをコーディングする具体的なテクニックとノウハウを提供している。

¹¹ <http://www.ipa.go.jp/jinzai/renkei/spcamp2010/outline/index.html>



図 C/C++ セキュアコーディングセミナー¹²

・「制御システムセキュリティカンファレンス」

制御システム関連製品を開発している企業の技術者、研究者および制御システムのユーザ企業（事業者）の技術者、研究者を対象とした、講演・パネルディスカッション等の内容のカンファレンスの開催している。

2 人材タイプII「使う」

2.1 政府機関の取り組み

○内閣官房、人事院、総務省

政府職員（一般職員、幹部職員及び情報セキュリティ対策担当職員）向けの統一的な教育プログラムの充実のための施策を行っているほか、政府職員に対する採用時の合同研修を実施している。また、地方公共団体職員に対しては、総務省が情報セキュリティ教育として、e-learningによる研修を実施している。

¹² <https://www.jpCERT.or.jp/event/securecoding-TKO-seminar.html>

3 人材タイプⅢ「教える」

3.1 政府機関の取り組み

○文部科学省

・高等学校学習指導要領 「情報」

2003 年より必修科目へ。セキュリティ対策の必要性についても指導することを求めている。



○総務省

・情報セキュリティ・サポーター

情報セキュリティ・サポーター（利用者の身の回りの詳しい人）を育成するための教材の作成や認定試験の開催等を支援している。

○警察庁

・情報セキュリティに関する講習の実施

教育機関関係者、地方公共団体職員、インターネット一般利用者等を対象の講演等を全国規模で開催する。

¹³ http://www.mext.go.jp/component/a_menu/education/micro_detail/__icsFiles/afieldfile/2010/01/29/1282000_11.pdf

4 海外における情報セキュリティに関する人材育成活動

4.1 米国における取り組み

米国では、政府機関及び大学等の教育機関が主導して情報セキュリティ人材の育成に取り組んでいる。

○The International Information Systems Certification Consortium (ISC2)

・CISSP (Certified Information Systems Security Professional)

米国規格協会 (ANSI) より、ISO 国際標準化機構/国際電気標準会議 (IEC) スタンダードの認証を受けた、情報セキュリティ・プロフェッショナル向けの資格。世界的標準にもなっている。

CISO (Chief Information Security Officer)、CSO (Chief Security Officer)、Senior Security Engineer、もしくは、これらを目指している人材を対象としている。

欧米政府及びその他機関・組織がその資格取得を促進・義務付けている。¹⁴

CISSP 取得を推奨・義務化している組織及び企業

国・地域	組織・企業名及び概要
米国	<ul style="list-style-type: none">● 退役軍人局：CISSP 資格取得者を認証し、取得費用についても負担。● NSA：CISSP 資格取得者の認証を実施。● Novell 及び Deloitte Touche Tohmatsu：CISSP 取得をセキュリティ業務従事者へ義務付け。
欧州	<ul style="list-style-type: none">● 英国スコットランドヤード (ロンドン市警) のコンピュータ犯罪局：半数以上の捜査が CISSP を取得。近年中に全員が取得予定。● 英国政府 (Infosec Training Paths and Competencies: ITPC)：情報セキュリティ業務従業者向けに英国政府が設立。同組織でのトレーニングにおいて、CISSP 資格保持者を、自動的に認証。● インターポール (国際警察機構)：欧州における情報テクノロジー犯罪専門局の捜査員、総勢 17 名が CISSP を取得。

15

・コンセントレーション

CISSP 資格取得者は、更に「コンセントレーション」と呼ばれる情報セキュリティに関する 3 種類の資格を得ることができる。これは、大学でいう「専門課程」に当たるもので、この取得には、CISSP の CBK 分野について、さらに深い知識を必要とされる。¹⁶

¹⁴ JETRO/IPA NY 「ニューヨークだより」 2006 年 (http://www.ipa.go.jp/about/NYreport/2006_06.pdf)

¹⁵ JETRO/IPA NY 「ニューヨークだより」 2006 年 (http://www.ipa.go.jp/about/NYreport/2006_06.pdf)

¹⁶ JETRO/IPA NY 「ニューヨークだより」 2006 年 (http://www.ipa.go.jp/about/NYreport/2006_06.pdf)

コンセントレーションの資格対象者及び対応分野

コンセントレーション	ISSEP	ISSAP	ISSMP
対象者	民間及び行政部門における情報セキュリティ・エンジニアリング専門家	情報セキュリティ・アーキテクチャ専門家	情報セキュリティ・マネジメント専門家
対応分野	<ul style="list-style-type: none"> ➢ システム・セキュリティ・エンジニアリング ➢ 認証及び認定 ➢ テクニカル・マネジメント ➢ 米国政府情報保証 	<ul style="list-style-type: none"> ➢ アクセスコントロール・システムと方法論 ➢ テレコミュニケーション及びネットワーク・セキュリティ ➢ 暗号学 ➢ 要求分析、セキュリティ・スタンダード、ガイドライン及び基準 ➢ BCP 及び障害修復計画 (Disaster Recovery Planning : DRP) に関連した技術 	<ul style="list-style-type: none"> ➢ 企業セキュリティ・マネジメント ➢ 全社的システム開発セキュリティ ➢ オペレーション・セキュリティ遵守監督 ➢ BCP、DRP、Continuity of Operations Planning (COOP : 管理計画の継続) の理解 ➢ 法、調査、科学捜査及び倫理

17

・SSCP (Systems Security Certified Practitioner)

情報セキュリティ部門の上級ポジションに就いている、もしくは今後就く予定の人材を対象とした資格。セキュリティ戦略策定に重要な以下 7 項目を対象としている。¹⁸

- ・ アクセス・コントロール
- ・ アドミニストレーション
- ・ 監査とモニター
- ・ 暗号学
- ・ データ・コミュニケーション
- ・ 悪質コード・破壊工作コード
- ・ 危険、対応と復旧

・CAP (Certification and Accreditation Professional)

リスク評価を行い、セキュリティに必要な環境を整備する立場にある者で、ISC2 の CBK が定める 5 分野 (①認証の理解、②システム許可プロセス、③認証、④認定、⑤継続的モニター) での職歴が 2 年以上の者を対象としている。¹⁹

06. pdf)

¹⁷ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

¹⁸ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

¹⁹ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

- Associate of ISC2 Designation

CISSP 及び SSCP 資格取得及び、情報セキュリティ分野でのキャリアを目指しているが、経験が十分でない者を対象とした資格。

資格の取得には、CISSP もしくは SSCP の試験に合格することが求められており、合格の後、アソシエートとして定められた期間内に必要な経験を積んだ後、第三者からの推薦状の提出をもって、正式に CISSP もしくは SSCP の資格を与えられる²⁰

○SANS (SySAdmin, Audit, Network, Security) Institute

- セキュリティ関連プログラム

セキュリティ・プロフェッショナル、ネットワーク・アドミニストレータ、CISO や CIO などを中心に、165,000 人にプログラムを提供してきた。SANS は、後述する GIAC (Global Information Assurance Certification) と呼ばれるセキュリティ資格の提供の他、トレーニング及び情報提供などの各種セキュリティ関連プログラムを実施している。これらのトレーニング・コースを受講 (1-2 日程度のプログラム) することにより、受講証明書 (Certificate) を得られる制度も提供されている。²¹

²⁰ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

²¹ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

SANS が提供するセキュリティ関連プログラム

プログラム		概要
資格	The GIAC Certification Program	システム保護担当者対象の技術資格。
トレーニング	Information Security Training	ネットワークやシステム・セキュリティに関するトレーニングを、世界 90 都市以上で毎日 400 コース以上を提供。
	The SANS Partnership Series	国防に関わる組織に属する情報セキュリティのプロフェッショナルを対象にしたトレーニング・プログラム。①国防に多大な影響を与えるポジションにある人材を擁する、②多数の情報セキュリティ人材を雇用している、③（しかし）予算上の理由から、必要十分なトレーニングを提供できない、といった組織を対象にしたもので、同トレーニングを受けている組織として、教育機関、州・地方警察、州・地方政府、米国の発展途上国及び、国際機関などが含まれている。
	Consensus Security Awareness Training	セキュリティ関連オンラインコース。
情報提供	SANS Weekly Bulletins and Alerts	「@RISK」と呼ばれる最新のセキュリティ・ニュースに関する電子メール・マガジン。週 2 日発行。
	Vendor Related Resources	セキュリティ関連商品の開発ベンダに関するニュース提供。
	Information Security Glossary	用語、頭辞語などの「辞典」 (http://www.sans.org/resources/glossary.php)
	Internet Storm Center	インターネットの早期警告システム
	SCORE	情報セキュリティの基本的なスタンダードとベストプラクティスに関するコンセンサスを構築する為のセキュリティ・プロフェッショナルのコミュニティ。インターネットに接続する、安全なシステムのコンフィギュレーションに関するスタンダードを構築している Center for Internet Security(CIS)による、世界共通のセキュリティ・ベンチマーク構築プロジェクトにインプットを提供している。
	SANS/FBI Annual Top Twenty Internet Security Vulnerability List	230 以上にも及ぶよく見られるセキュリティ問題のリスト提供。
	SANS Information Security Reading Room	セキュリティ分野に関連する 75 項目に関する 1,200 以上の研究文献を提供。
	SANS Step-by-Step Guides	人気のあるオペレーティング・システムやアプリケーションの保護方法をまとめたパンフレット。
	SANS Security Policy Project	セキュリティ・ポリシーのテンプレートの無料提供。
	Intrusion Detection FAQ	侵入検知に関する Q&A。
	SANS Press Room	SANS メンバーのインタビューの他、情報セキュリティに関するニュースなど、情報アシュアランス業界についてのメディア向け情報を提供。

22

・GIAC (Global Information Assurance Certification)

GIAC は、関連分野において仕事を遂行するために必要とされる、最低限の知識を持っていることを証明するものであり、その試験範囲は、論理・用語理解から、監査、セキュリティ、オペレーション、マネジメントに関する理解を問うものとなっている。レベル (Level 3-5) 及び必要分野 (セキュリティ・アドミニストレーション、管理、監査など) に応じた

²² JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

テストを受験することができる。²³

○CIO 大学

連邦政府のCIO評議会 (Federal Chief Information Officers Council) と、連邦政府の一般調達局 (GSA) の要請を受けて、連邦政府CIOのIT教育の普及と充実を目指し、カーネギーメロン大学を始めとする7大学がパートナーシップを組んでスタートした教育プログラム。

政府機関のみならず、民間組織においてトップ・マネジメントのポジションを目指すエグゼクティブ・クラスの人材を対象に、ITに関連した各種大学院レベル・カリキュラムを提供している。修了者には卒業大学からの修了証及び政府からのCIO大学修了証明書が付与される。学生の割合は、40%が政府から、60%が民間セクターからとなっている。

カーネギーメロン大学では、情報セキュリティに関してはオンサイトでのCIO大学カリキュラムに含まれていないが、「IT遠隔教育 (MS in Information Technology: MSIT、修士号)」のプログラムで対応している²⁴

- ・「H. John Heinz III School of Public Policy and Management」²⁵
- ・情報システム管理 (MS in Information Systems Management) 修士課程プログラム²⁶

○その他、大学における情報セキュリティ・プログラム

- ・ジョーンズ・ホプキンス大学の「JHU Information Security Institute」²⁷
- ・ジョージア工科大学の「MA in Information Security」²⁸
- ・南カリフォルニア大学のコンピュータ・セキュリティ修士プログラム²⁹
- ・コロンビア大学の「Computer Science at the School of Engineering」³⁰

²³ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

²⁴ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

²⁵ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

²⁶ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

²⁷ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

²⁸ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

²⁹ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

³⁰ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

○政府機関の取組み

連邦政府のリーダーシップの下、数多くの IT・情報セキュリティに関するプログラムが、連邦政府職員向けのみならず、一般人を対象に実施されている。提供の主体は政府自身の場合もあれば、民間委託や民間との協力で行うケースもある。さらに、政府自らが提供する場合でも、教育プログラムそのものを用意していることもあれば、民間の教育機関、中でも先端的セキュリティ R&D 活動を行う機関への資金提供を行う場合もあり、その形態は様々である。³¹政府機関の取組みは以下の通りである。

発案者	プログラム提供者	プログラム内容	プログラム名	プログラム提供対象
連邦政府	連邦政府	教育プログラム	①Defense Security Service Academy	国防総省職員を始めとする連邦政府職員、特定の外国政府職員、産業界など
			②Graduate School: USDA	18歳以上なら可(外国人留学生も受け入れ)
		資金提供	③Homeland Security Centers for Excellence	大学、大学院
			④Federal Cyber Service: Scholarship for Service	大学、学生、中小企業
			⑤National Centers of Academic Excellence in Information Assurance Education	4年生大学・大学院
連邦政府	民間	教育プログラム	⑥ISC Authorized Academic Center Course Module	米国国務省職員
連邦政府・民間	連邦政府・民間	教育プログラム	⑦National Cyber Security Alliance	個人ユーザ、中小企業、学校など

図 主な連邦政府・省庁機関が行う情報セキュリティ教育³²

・US サイバーチャレンジ

CSIS と SANS Institute は 2009 年 7 月、連邦政府と連携し、サイバーセキュリティの専門家を 1 万人育成すべく、US サイバーチャレンジを立ち上げた。高校生向けコンペを開催し、成績優秀者を表彰、奨学金や商品券を授与している。

・サイバーセキュリティ法案

2010 年 2 月、下院においてサイバーセキュリティ法案(Cyber security Enhancement Act)

³¹ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

³² JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

を可決した。各省庁が必要とするサイバーセキュリティ労働力の評価や、将来的に連邦政府で働くことを前提にした大学生、大学院生に対する奨学金等の項目を含んでいる。

○国防総省

- ・「Defense Security Service (DSS) Academy」³³

国防総省の教育プログラムを実施している。同省のセキュリティ・プログラムの専門家、同省契約業の社員、その他の政府機関職員、及び特定の外国政府職員が対象である。

提供しているコースは、対諜報活動、セキュリティ一般などの他に、情報セキュリティ、情報システム・セキュリティなど、合計7コースとなっている。

○農務省

- ・「Department of Agriculture:USDA 大学院」³⁴

教育・トレーニング等を通して政府の機能を高めると同時に、一般市民の生涯学習の場を提供することを目的としており、18歳以上なら誰でも入学することができ、留学生も受け入れている。

学位の授与は行っていないが、労働者に生涯教育とトレーニングの場を提供している。

ハッカー行為の検知や、ウィルス除去、ファイアーウォールの設定などといったスキルを学ぶことができる。また、技術の高い情報セキュリティ専門家に対する増加し続ける需要に応えるものとして、2週間の「情報セキュリティ・スペシャリスト認定プログラム (Information Security Specialist Certification Program)」も用意されている。

○国土安全保障省

- ・「Homeland Security Centers for Excellence」³⁵

国土防衛を念頭においたプログラムを提供している大学・大学院にフェローシップやスカラシップを付与している。

- ・「Federal Cyber Service: Scholarship for Service」³⁶

³³ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

³⁴ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

³⁵ JETRO/IPA NY 「ニューヨークだより」 2006年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

³⁶ <https://www.sfs.opm.gov/>

情報アシュランスやコンピュータ・セキュリティの分野に進む学生数の増加と、これらの分野の専門家をより多く輩出するため、高等教育のレベルの向上として、以下の資金支援などを実施している。

- ・ スカラシップ・トラック (Scholarship Track) : 情報アシュランスとコンピュータ・セキュリティの分野で活躍する学生に対するスカラシップ資金として、大学への資金援助
- ・ キャパシティ・ビルディング・トラック (Capacity Building Track) : 情報アシュランス及びコンピュータ・セキュリティの専門家による研究の質を向上させることを目指した、大学への資金援助
- ・ 1年を通じた学生や中小企業への資金援助

○NSA と国土安全保障省

- ・ 「National Centers of Academic Excellence in information Assurance Education (CAEIAE)」³⁷

クリントン政権によって発表された国家重要インフラ保護に関する「大統領指令 63」を基礎とし、その後 2002 年にブッシュ政権によってまとめられたサイバー・セキュリティに関する国家政策「President's National Strategy to Secure Cyberspace」を支援するプログラムとして開始された。

同プログラムは、情報アシュランス分野の教育水準を向上させ、同分野の専門家を多く育てることにより、国のインフラに見られる脆弱性を是正することを最大の目的としている。CAEIAE としての「認定」を受けた 4 年制大学、大学院が、当該分野の教育の場を提供する仕組みとなっている。

その他、国土安全保障省 (Department of Homeland Security: DHS) は、連邦政府に対するサイバー攻撃の増大に対応するため、サイバーセキュリティの専門家を大幅に採用すると発表している。今後 3 年間にわたり、最大 1,000 名を採用する予定であると発表している。

○米商務省/ ISC2

- ・ 「ISC2 Authorized Academic Center Course Module」³⁸

商務省からの委託を受け、ISC2 が自前の情報セキュリティ教育プログラム (「Academic Center Course Module」) をベースに、商務省職員向け特別プログラムを開発した。

³⁷ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

³⁸ JETRO/IPA NY 「ニューヨークだより」 2006 年 (<http://www.ipa.go.jp/about/NYreport/200606.pdf>)

○NCSA（官民共同組織）³⁹

国土安全保障省、連邦貿易委員会（Federal Trade Commission）や、AOL、E-Bay、マイクロソフトを始めとする多くの民間企業・組織からの資金援助を受けている官民共同組織である。

中小企業向けとして、「サイバー・セキュリティ入門」、「企業のサイバー対策」、「被害の復旧と報告」の3つのコースを実施している。これらプログラムを通して、サイバー・セキュリティの基本に対する理解から、実際にサイバー被害にあった際の報告手順などまで網羅し、中小企業を支援している。

4.2 英国における取り組み

英国では、優秀な人材の発掘型機会を提供する取り組みが行われている。

・サイバー・セキュリティ・チャレンジ

英国では、サイバーセキュリティ庁の主催で、セキュリティ分野における次世代の有能な人材を発掘するために、「サイバー・セキュリティ・チャレンジ」というコンクールを実施。官民合同でスポンサーになっている。このチャレンジイベントは複数のコンペで構成されているが、優勝者には、大学進学のパウチャーや特別なサイバートレーニングコースの受講、企業でのインターンシップの機会が賞として与えられる。

4.3 欧州（EU）における取り組み

○European Network and Information Security Agency（ENISA）⁴⁰

ENISA は、インシデント発生時に個別かつ具体的な支援を各国に行うことは無いが、普及啓発活動の一環として、2007年にCERTに関するワークショップを行っており、その中でインシデントの抑制活動（Mitigation、緩和等とも呼ぶ）のトレーニングを行った。これは、情報セキュリティに関するベストプラクティスの横展開の1つでもあり、同時に、CERT間の連携強化にもつながっている。

また、ENISAは適宜、他の調査機関、セキュリティサービス提供事業者、大学、その他の事業者等と協力して、調査研究活動を行っている。そのうちの例が、PISCE（Partnership for ICT Security Incident and Consumer Confidence Information Exchange）と呼ばれ

³⁹ JETRO/IPA NY「ニューヨークだより」2006年（<http://www.ipa.go.jp/about/NYreport/200606.pdf>）

⁴⁰ NTTデータ経営研究所「ヨーロッパの情報セキュリティ対策における協力・連携体制に関する調査研究」（平成22年3月）

るパートナーシップで、各国のセキュリティ機関、CERT、Eurostat 他の機関と連携している。

そのほか、ENISA では、24 時間 365 日の活動を行う CERT を支援するために、様々な、実践的なトレーニングを提供している。例えば 2008 年にはモルドバへ、サイバーアタックへの対応というテーマでトレーニングを提供したり、日本でも 2009 年に「感染コンピュータの調査」というテーマでハンズオンを実施したりしている。

○Institute for the Protection and Security of the Citizen (IPSC) ⁴¹

IPSC (Institute for the Protection and Security of the Citizen provides) では、EU の政策メンバ、加盟国、国連、その他国際機関に対して、数多くの科学技術面で調査プログラムの実施を支援している。IPSC は、EU の政策担当者及び関係機関に対し、研究開発面でのサポートを行なっている。

IPSC のプロジェクトの多くは、実施にあたり、EU 各国政府の調査機関、大学、シンクタンク等との連携が必要となる。例えば、IPSC では、スウェーデンの防衛省といくつかの関係機関、コンソーシアムと連携して、Changing Perceptions on Security and Interventions : CPSI) project という連携を進めている。また、別の例として、Europe's Evolving Security: Drivers, Trends, and Scenarios : FORESEC というプロジェクトもあり、IPSC が様々な EU の関係機関等 (戦略調査機関、危機管理イニシアティブ等) と連携している。

【研究開発のスキーム】

IPSC の研究テーマは多岐にわたるが、幅広く分野をカバーするという方針ではなく、分野を絞り込んで実施している。また、研究テーマの最適化も行っている。研究テーマは、ビジョンを元にトップダウンで決定するものとプロポーザルや環境変化のモニタリングから抽出されるボトムアップで決定するものの両方がある。トップダウンアプローチで利用するビジョンは、10 年のスパンで大きな研究目標を立てている。ビジョンに沿った研究テーマを研究者に割り振り、研究開発の取り組みとして、「グランドチャレンジかつテーマ性があるエリア」を設定した上で、それぞれの具体的な研究テーマが適用されていく。エリアが決定された後は、研究テーマのプレゼンテーションを研究者に行わせて、プロポーザル形式で研究テーマが決定されるだけでなく研究分野のテーマは 5 年おきに見直されている。

また、ローリング戦略として、研究テーマのレビューが毎年行われている。例えば、突発的に重要な問題として認識された問題は、技術投資案件に変更される。政策的な判断と比べて、IPSC では組織的に対応できる様な仕組みを持っている。

⁴¹ NTT データ経営研究所「ヨーロッパの情報セキュリティ対策における協力・連携体制に関する調査研究」(平成 22 年 3 月)

【研究開発の成果の活用】

基本的には公的な資金による研究成果は公表されるべきであると考えているため、公的な研究開発は公開される仕組みになっている。具体的は、Web サイトを通じて研究成果が誰でも自由に利用できるようになっている。また、この仕組みは、特に中小企業でも利用しやすいような配慮がなされている。さらに、JRC では、EU 各国で研究開発の成果を利用できるように、技術的な支援を他の EU 組織とともにやっている。

4.4 ドイツにおける取り組み

ドイツでは、政府の取組みとしては、BMI（内務省）配下の BSI（情報技術安全局）が、国民に対するセキュリティ教育を支援している⁴²。

また、BSI は、政府調達し、軍等で採用した製品に対してセキュリティレベルの認定を与え⁴³、民間に当該製品を普及させる取り組みを行っている。

4.5 韓国における取り組み

○新羅大学

資格取得等も視野に入れたコース。⁴⁴

企業等と提携した就職を意識した講座を提供している。

○イジスウォンセキュリティ教育センター

就職を意識した教育を中心に行っている。少数精鋭のコースを標榜している。⁴⁵

○シュンシン大学

就職、資格取得を目的としたコースである。募集人員に上限（20 名程度）を設けている。

46

⁴² https://www.bsi-fuer-buerger.de/cln_192/BSIFB/DE/Home/home_node.html

⁴³ The Highest Standards: SINA and BSI (http://www.secunet.com/fileadmin/user_upload/Download/Printmaterial/englisch/sn_SINA_GlobalIntranet_BR_E.pdf) Pp. 10

⁴⁴ http://ice.deu.ac.kr/xe/?mid=Community02&page=6&document_srl=856

⁴⁵ http://nice.mokwon.ac.kr/EMT/?ref=board/board.emt&bbs_table=m6_12&menu_table=m6_00&page=1&eb_idx=451

⁴⁶ http://www.sungshin.ac.kr/media/html/community/employment.html?bid=media_employment&sc_category=&sch=&sc_text=&page=1&idx=42062

○韓国大学

情報セキュリティの専門家の教育コースを提供している。就職を意識している。⁴⁷

○ソウル科学総合大学院

高度産業セキュリティ技術とマネジメント能力の両方を備えた、産業セキュリティ業界におけるマネジメントの専門家の育成する韓国国内初の MBA プログラム。国情院産業機密保護センターと協力して、2009年3月に国内初の産業セキュリティ MBA を開設したソウル科学総合大学院では、2009年9月、業界のセキュリティ専門家（ISP）のコースを開設して運営中している。12週間の短期コースを用意している。⁴⁸

○昌原大学校

就職を意識した情報セキュリティ専門家育成講座の提供を行っている。保証はしていないが、就職先として、A3、セキュリティ、SK インポセク、STG セキュリティー、ネトシキユオ、会計事務所、ハンレプ、アンレプココナッツ等が挙げられている。⁴⁹

企業と提携したコースの案内も行っている。⁵⁰

○慶熙大学

新羅大学と同様に、企業等と提携した就職を意識した講座を提供している。⁵¹また企業等と提携した就職を意識した講座を提供している。⁵²

○世明大学

企業等と提携した就職を意識した講座を提供している。

○韓国情報通信技能大学

企業等と提携した就職を意識した講座を提供している。⁵³

⁴⁷ http://eie.korea.ac.kr/public_html/board/board.php?bo_table=bo09_07&wr_id=153&page=5

⁴⁸ [http://www.assist.ac.kr/common/download.asp?filename=%BB%EA%BE%F7%BA%B8%BE%C8+%C0%FC%B9%AE%B0%A1+\(ISP\)+%B0%FA%C1%A4+%BA%EA%B7%CE%BC%C5.pdf&filepath=%2FUploadFile%2FAttach%2F07e5a59d-31ff-4231-92e9-daa1adba2ee1.pdf](http://www.assist.ac.kr/common/download.asp?filename=%BB%EA%BE%F7%BA%B8%BE%C8+%C0%FC%B9%AE%B0%A1+(ISP)+%B0%FA%C1%A4+%BA%EA%B7%CE%BC%C5.pdf&filepath=%2FUploadFile%2FAttach%2F07e5a59d-31ff-4231-92e9-daa1adba2ee1.pdf)

⁴⁹ http://electron.changwon.ac.kr/board/bbs/board.php?bo_table=free&wr_id=2216&page=236

⁵⁰ http://electron.changwon.ac.kr/board/bbs/board.php?bo_table=free&wr_id=2328&sf1=&stx=&sst=wr_datetime&sod=asc&sop=and&page=142

⁵¹ http://ce.khu.ac.kr/english/05_commu/commu_002_read.html?cpg=5&seq=7732

⁵² http://electron.changwon.ac.kr/board/bbs/board.php?bo_table=free&wr_id=2330&sf1=&stx=&sst=wr_datetime&sod=asc&sop=and&page=143

⁵³ <http://www.icpc.ac.kr/icpc/board-read6.do?boardId=bbs29&boardNo=12530954257866&command=READ&page=1&categoryId=-1&dept=mobiletelecom&idx=4>

○韓国政府における情報セキュリティ人材育成のための環境の整備

・サイバー保安官の要請

韓国政府は2012年までに、サイバー保安官を3,000人要請することを決定した。これに伴い、各大学に情報セキュリティ学科が新設され、関連する研究センターの設立も支援する予定である。

・ハッカーカンファレンス

韓国政府がスポンサーとなって2008年より開催されているハッカーカンファレンス「CodeGate」では、賞金付きのハッキングコンテストが実施されている。2010年の賞金総額は3500万ウォンであった。

4.6 中国における取り組み

○計算機科学与技术学院

コンピュータ学科のフォーラム内に「情報セキュリティカリキュラムユニット」というスレッドがあるため、情報セキュリティカリキュラムが設けられていると考えられる。⁵⁴ コンピュータウイルスの検出、除去方法と予防のメカニズムの理解を目的とした「アンチウイルス技術」という学科が設けられている。⁵⁵

○CCERT（中国教育和科研计算机网紧急响应组）

CCERT情報セキュリティ教育トレーニング機関がISC準拠のコースを提供している。CCERTの運営は、清華大学が行っている。⁵⁶

○北京大学

北京大学のコンピュータ情報セキュリティ研究センターは国からの資金提供を受けて、様々な情報セキュリティ技術の研究開発を行っている。

その他、セキュリティ学科を2002年に設立している。実務的な情報セキュリティの専門家から情報セキュリティの研究開発を行う人材まで幅広い人材の育成を目的としている。⁵⁷

⁵⁴ <http://www.cs.swust.edu.cn/modules/newbb/viewforum.php?forum=6>

⁵⁵ <http://www.ucourse.swust.edu.cn/courses/course/category.php?id=11>

⁵⁶ http://www.ccert.edu.cn/education/Course_Intro.php?handle=11

⁵⁷ http://www.ss.pku.edu.cn/index.php?option=com_content&task=category&id=228&Itemid=453

○蘇州大学

「ネットワークと情報セキュリティ」というタイトルの授業を有している。⁵⁸

○上海交通大学

情報セキュリティ工学研究グループのコンピュータセキュリティ部門を2007年に設立した。国家の安全保障のための様々な実証プロジェクトを遂行している。⁵⁹

○淮阴工学院计算机工程学院

e-learning で情報セキュリティの講座を提供している。200名以上の学生が受講している。⁶⁰

○浙江工商大学

e-learning で情報セキュリティのコースを提供している。⁶¹

○成都信息工程学院⁶²

情報セキュリティの4年制コースを設けている。

○重庆邮电大学计算机科学与技术学院⁶³

ネットワークセキュリティ技術コースを設けている。

4.7 インドにおける取り組み

○ハイダラバード工科大学 (Indian Institute of Technology Hyderabad) ⁶⁴

ハッカー養成コースを提供している。

○DOEACC Center Calicut

「Diploma in Information Security & System Administration」というタイトルで6カ

⁵⁸ http://kczxjy.suda.edu.cn/Able.ACC2.Web/Page_CourseDetail.aspx?ID=2783

⁵⁹ <http://www.sjtu.edu.cn/newsnet/cxzydisplay.php?id=27155>

⁶⁰ http://cis.hyit.edu.cn/hgis/netroom/netroom_down.aspx?downid=25

⁶¹ <http://e-learning.zjgsu.edu.cn/moodle/course/view.php?id=8>

⁶² <http://zjc.cuit.edu.cn/NewsCont.asp?type=574&id=10403>

⁶³ <http://cs.cqupt.edu.cn/MemberIndex.asp?MemberID=1668&MemberUID=>

⁶⁴ http://www.iith.ac.in/elan10/Hacking_Workshop_Curriculum.pdf

月のコースを提供している。⁶⁵

また、政府機関のCIO向けの情報セキュリティコースを提供している。このコースでは、政府機関のITセキュリティのマネジメントをできるようになることに加えて、政府機関の従業員への情報セキュリティの普及啓発を行えるようになることを目的としている。⁶⁶

○The Indraprastha Institute of Information Technology, Delhi⁶⁷

セキュリティ産業界で活躍できる人材の輩出を目指して、情報セキュリティ分野に特化したコンピュータサイエンス学科が設置されている。

○Indian Institute of Information Technology and Management-Kerala (IIITM-K)⁶⁸

IIITM-Kでは、Information Security Education and Awareness project (ISEA)という情報セキュリティ教育コースを提供している。

○Indian Institute of Information Technology Allahabad (IIIT-A)⁶⁹

「情報セキュリティと法」に関するコースを提供している。

○University of Pune⁷⁰

Pune大学では、Centre for Information and Network Securityという機関を設置して、6か月のフルタイムもしくは1年間の夜間通学での情報セキュリティ専門のコースを提供している。教育のほか、調査研究やセキュリティのコンサルティングサービスも行っている⁷¹。

○National Institute of Technology Karnataka⁷²

情報セキュリティレベルの引き上げと高度な情報セキュリティ人材育成のためのカリキュラム開発のための研究開発を行っている。⁷³

⁶⁵ <http://doeaccalicut.ac.in/html/course/SW500.html>

⁶⁶ <http://www.doeaccalicut.ac.in/html/infosec.html>

⁶⁷ <http://www.iiitd.ac.in/mtech2010.php>

⁶⁸ [http://www.iiitm.ac.in/wiki/index.php/Information_Security_Education_and_Awareness_project_\(ISEA\)](http://www.iiitm.ac.in/wiki/index.php/Information_Security_Education_and_Awareness_project_(ISEA))

⁶⁹ <http://ms.iiita.ac.in/Documents/msclis.pdf>

⁷⁰ http://www.unipune.ac.in/snc/CINS/cins_webfiles/academic.htm

⁷¹ <http://www.unipune.ac.in/snc/CINS/default.htm>

⁷² <http://isea.nitk.ac.in/isea/>

⁷³ <http://isea.nitk.ac.in/project/>

○Indian Institute of Technology Rookee⁷⁴

Indian Institute of Technology Rookee では、ISEA プロジェクトを行っている。

○University of Madras⁷⁵

情報セキュリティとフォレンジックに関するコースを提供している。

○Institute Of Management Technology⁷⁶

1年コースのサイバーセキュリティコースを提供している。

○Institute of Information Technology, DELHI⁷⁷

コンピューターサイエンスの知識がある学生を対象に、セキュアなソフトウェアやシステムを開発・構築・提供できるようになるためのコースを提供予定である。

○MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY (MANIT)

情報セキュリティ関連の1年の講座が提供されている。

⁷⁴ http://www.iitr.ac.in/ISEA/pages/About_Us.html

⁷⁵ http://www.unom.ac.in/academic/course_highlights2.html

⁷⁶ http://www.imtcdl.ac.in/opgdcfs_faq.htm

⁷⁷ <http://www.iiitd.ac.in/mtech2010-courses.php>