「情報セキュリティ人材育成の現状」

渡辺弘美@JETRO/IPA NY

1. 米国における情報セキュリティ資格制度と資格取得の現状

米国の情報・IT セキュリティ・プロフェッショナルにとって、関連分野の資格を取得することは、情報セキュリティ・システムの改善につながるだけではなく、情報・IT セキュリティ・プロフェッショナルとしてのキャリア構築に重要となっている。

そうした状況を背景として、後述する The International Information Systems Certification Consortium（ISC2）が制定している「Certified Information Systems Security Professional：CISSP」等や、SySAdmin, Audit, Network, Security（SANS）Institute が制定している資格である「Global Information Assurance Certification：GIAC」などの情報セキュリティ関連資格の取得者数が増加している。

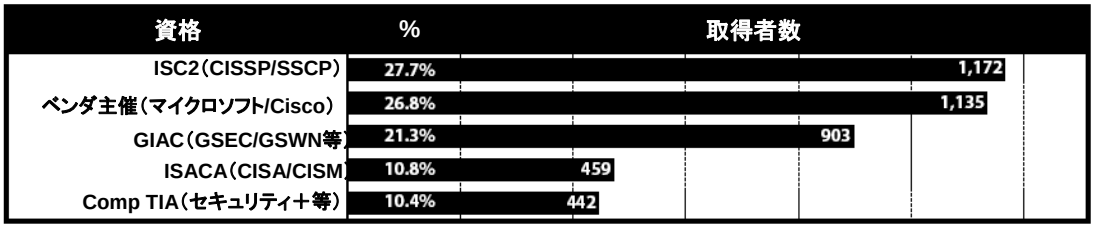
(1) 情報セキュリティ関連資格取得の意味

情報セキュリティ関連資格及び情報提供を行っている SANS（SySAdmin, Audit, Network, Security） Institute は、2005 年 10 月 20 日から 11 月 18 日にかけ、4,250 人以上の情報セキュリティ・プロフェッショナルを対象にした「2005 年情報セキュリティ給与と昇進についての調査（The SANS 2005 Information Security Salary & Career Advancement Survey）」を実施、その結果を発表した。同調査の結果は、経歴、雇用先、給与から、所有資格、仕事内容等に関する 30 にも及ぶ質問の結果から導き出されている。

同調査の回答者の大多数は、自身の職業に関連した資格を最低 1 種類を取得しており、中でも取得数が特に多かったのが、ISC2 によるもので、これに続き、マイクロソフト、Cisco などのベンダによる資格、SANS による GIAC（Global Information Assurance Certification）となっている。この他には、ISACA(Information Systems Audit and Control Association：情報システムコントロール協会、1967 年に設立され現在会員数は全世界に 50,000 以上)が行う CISA（公認情報システム監査人資格）や CISM（公認情報セキュリティマネージャーの資格）、CompTIA のセキュリティ＋資格がある。CompTIA の資格は、IT スキルの基礎レベルにおいて業界標準とされており、マイクロソフト社の「MCSA」や Novell 社の「CNE」とい

った上級レベルの資格の受験条件ともなっている。最も著名な資格は「+A」である。

資格別取得者数と割合

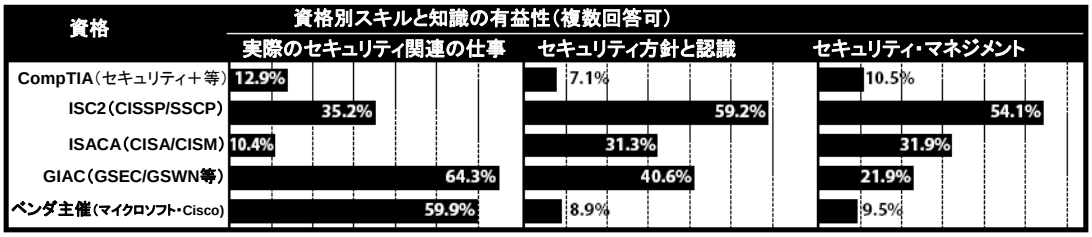


こうした回答者に、「資格取得は、キャリア構築などに意味があるか」という質問を行った。これに対して、「意味はなかった」とする意見が約 34%あった一方、何らかの「意味があった」とする意見がこれを上回り、「資格取得に伴う知識は、現場のセキュリティ向上に効果があった」とする声に並び、「新しい仕事に就けた（24.1%）」、「昇給につながった（19.6%）」、「昇進した（14.9%）」など、直接キャリア・パス構築に役立ったとする意見（約 58.6%）が多く聞かれ、資格取得とキャリアとの関連性が関係者の間で認識されていることを示す結果となった。

資格取得の意味

さらに、同調査では、資格の種類により、実際にどのように役に立つかという点についても質問しており、ISC2 は、セキュリティ・ポリシー作成、マネジメントなどといった仕事に非常に有益であると指摘される一方、GIAC は、セキュリティ対策のためのオペレーションなど、現場において役に立つスキルを要求される資格であるとの結果が出た。

資格とその有益性



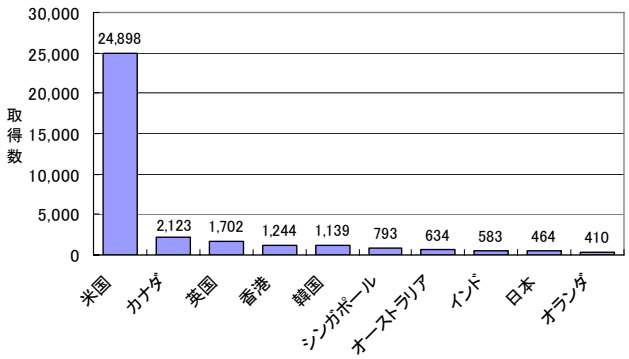
以下では、同調査で、中心的に取り上げられた ISC2 と SANS が提供するセキュリティ関連資格についてその概要をまとめる。

(2) The International Information Systems Certification Consortium（ISC2）

The International Information Systems Security Certification Consortium (ISC2)は、産業界が中心となり、情報セキュリティのプロフェッショナルを育成することを目的として 1989 年に設立された非営利団体である。ISC2 は、情報セキュリティのプロフェッショナル育成の「ゴールド・スタンダード」として、これまでに 100 以上の国で、40,000 人以上の情報セキュリティ・プロフェッショナルの認定を行ってきた。ISC2 は、CISSP のような資格試験を実施すると同時に、情報セキュリティ人材の質の底上げを狙い、セミナーを開催（2006 年 5 月 18 日の米国マサチューセッツ州ボストンや、韓国のソウルでの開催を筆頭に、欧州やアジア諸国でも予定）するなど積極的に活動を行っている。

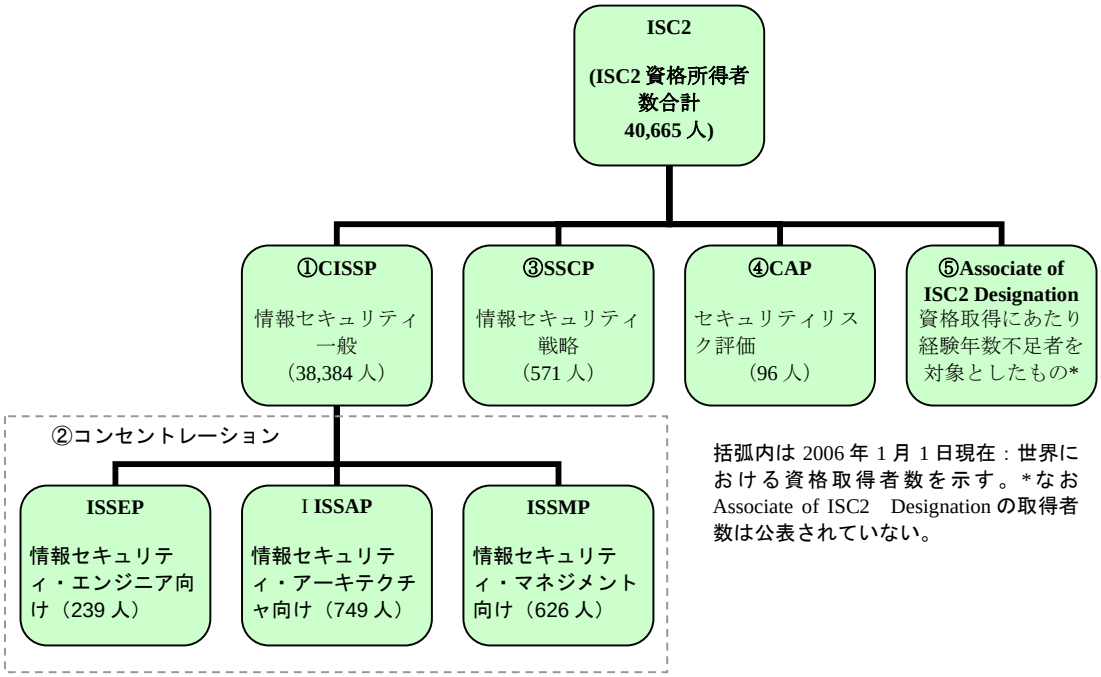
ISC2 が認定している情報セキュリティの資格の一つである「Certified Information Systems Security Professional：CISSP」の 2006 年 1 月 1 日現在の国別の取得者数を見ると、CISSP の資格取得者は、米国（24,898 人）を筆頭に、欧州、アジアから、南米、中東、アフリカと全世界に広がっている。

CISSP 国別取得数（2006 年 1 月 1 日現在）



ISC2 は、CISSP に加えて、以下の認定資格を提供している。

ISC2 が提供する情報セキュリティ関連認定資格



以下、各内容について、説明する。

① CISSP（Certified Information Systems Security Professional）

これは米国規格協会（American National Standard Institute：ANSI）より、ISO 国際標準化機構（International Organization for Standardization）/ 国際電気標準会議（International Electrotechnical Commission：IEC）スタンダード 17024 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であり、同分野における世界的標準となっている。

CISO（Chief Information Security Officer）、CSO（Chief Security Officer）または 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。受験資格は、ISC2 の Common Body of Knowledge（CBK）が定める以下の分野での職歴が 4 年以上、もしくは、当該分野での学士号を取得している者は、同分野での 3 年以上の職歴をもつことと定められている。ISC2 の CBK とは、世界中の情報セキュリティ・プロフェッショナルを対象にした、同分野における専門知識や原則に関する共通の枠組みを提供することを目的としたものであり、ISC では、情報セキュリティ実施における最重要事項の習得のレベルを計る基準として、CBK を用いている。ISC の CBK 委員会により CBK が、情報セキュリティの最先端の知識を反映するよう毎年見直し・修正が行われている。

ISC2 が CBK に指定している 10 分野：

- ✓ 情報セキュリティ・マネジメント
- ✓ エンタープライズ・セキュリティ・アーキテクチャ
- ✓ アクセス制御のシステムと方法論
- ✓ アプリケーション・セキュリティ
- ✓ 暗号学
- ✓ 通信・ネットワーク・インターネットのセキュリティ
- ✓ 物理セキュリティ
- ✓ 事業継続計画(Business Continuity Planning: BCP)
- ✓ 運用セキュリティ
- ✓ 法・捜査・倫理

ISC2 が提供している情報セキュリティ認定資格の中でも、特に CISSP については、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。

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	● 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	● 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。

② 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。また、コンセントレーションに含まれる資格試験を受験するために、CISSP 取得者であることに加え、ISC2 の「優良会員」であるという条件を満たすことが要求されている。ISC2 が定める「優良会員」とは、「ISC2 の定め

る倫理規定に則っている者」、「年会費を支払っている者」、「資格有効期限中、定められた「再教育（Continuing Professional Education: CPE）」プログラムにおいて一定の成績を収めている者」、と定義されている 。

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	➢ 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	➢ 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	➢ 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

特に ISSEP は、ISC2 と U.S. National Security Agency（NSA）の情報保証局（Information Assurance Directorate=NSA/IAD）との合意の下、2003 年 2 月に発表された特別プログラムで、NSA 職員として、あるいは外部コントラクタとして同省のために仕事をしたいと望む情報セキュリティ・プロフェッショナル向けの資格として設立された。NSA は、National Security Directive（NSD）45 及び Federal Technology Transfer Act of 1986 （15. U.S.C. Section 3710A）を基に、ISC2 と共に ISSEP に取り組むこととなった。ISC2 によれば、現在、ISSEP は、NSA だけではなく、米国連邦政府におけるセキュリティ関連職従事者及びコントラクタの必須資格として認定されている。

③　SSCP（Systems Security Certified Practitioner）

SSCP は、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であり、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。

- ✓ 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。

対象者は、これら 7 分野における 1 年以上の職歴があるシニア・ネットワーク・セキュリティ・エンジニア、シニア・セキュリティ・システム・アナリスト、及びシニア・セキュリティ・アドミニストレータとなっている。

④ CAP（Certification and Accreditation Professional）

ISC2 は、米国国務省（Department of State）の情報保証局（Office of Information Assurance）と協力し、CAP 資格を制定した。同資格は、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。

⑤ Associate of ISC2 Designation

上記の一連の資格と異なり、当資格は 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ものである。当資格を取得したものに対して、ISC2 は同分野でのキャリア構築に有益と思われる様々な支援を提供している。同資格の取得には、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ことになっている。

ISC2 アソシエート取得から CISSP・SSCP 取得まで

	アソシエート資格有効期間	資格取得に必要な経験年数	資格正式取得に必要なもの
CISSP	5 年	4 年	第三者からの推薦状
SSCP	2 年	1 年	

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

SANS は、世界で最も信頼されている情報セキュリティ・トレーニング提供及び資格認定団体の一つである。SANS が誇る膨大な情報セキュリティに関する資料・情報は、世界中の政府、大学、企業の研究成果から生まれたものであり、SANS は、これらを無料で公開している。同時に、インターネットの早期警告システムである「Internet Storm Center」も運営している。

① SANS が提供するセキュリティ関連プログラム

1989 年の創設以来、SANS は、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。これらの SANS が提供するプログラムは、一般的なシステム及びネットワーク・セキュリティ対策への活用は無論のこと、GIAC 資格取得に向けた学習にも効果的であるとされている。

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など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。

② GIAC (Global Information Assurance Certification)

SANS は、情報セキュリティのプロフェッショナルの技術を保証する手段として 1999 年に GIAC という資格制度を開始した。GIAC を取得しているということは、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。受験者は、自身のレベル（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）に応じたテストを受験することができる。

GIAC 資格取得者数は、2000 年 2 月に行われた GIAC の第 1 回資格試験では、1,000 人弱であったが、2002 年 3 月では、その数が 3,000 人以上に、そして 2005 年現在では GIAC 資格取得者数は 11,763 人となっている。

GIAC の受験者は、インフォメーション・セキュリティ・エンジニア、ネットワーク・オペレーション責任者、CEO、米国国防総省情報保証責任者（Department of Defense、Information Assurance Manager）と多岐に渡っている。

③ CISSP と GIAC の違い

ISC2 が実施する最大の資格試験である CISSP は、情報セキュリティ分野の概念的なものに対する資格証明書である一方で、GIAC は、CISSP で取り上げるような概念を、現場で活かす為の技術に対する資格証明と定義づけることができる。これは先の SANS による調査結果からも、この傾向は読み取れる。

また、CISSP の受験資格を得るには、最低 3 年間の実地経験が必要とされているが、GIAC は、誰でも受験することができるといった違いがある。

CISSP と GIAC の主な違い

資格	受験資格	資格内容	資格有効期間と その後の資格維持
CISSP	➢ 最低 3 年以上の実務経験	➢ 情報セキュリティの概念についての資格	➢ 3 年 ➢ ISC2 が定めるところの「優良会員」であること。
GIAC	➢ 特になし	➢ 情報セキュリティの概念を、現場で活かす為の技術に対する資格証明	➢ 4 年 ➢ 再受験

2. 大学における IT セキュリティ教育

情報セキュリティ分野でキャリアを目指す者にとって、資格取得と並び、同分野における学位の取得も重要となっている。SANS による既出の調査では、最終学歴と平均給与の比較も行われた。これによれば、最終学歴が学士号以下と、修士号以上の人材では年収（給与とボーナス合計）1 万ドル以上の格差があることが浮き彫りとなった。

セキュリティ・プロフェッショナルの最終学歴と平均給与

学位に関して、米国では、学士号を取得して、すぐに修士課程以上を目指す学生もいるが、職場の経験をベースに、さらなるキャリアアップの一環として、修士・博士課程に入りなおすケースも多いことがよく知られている。また、情報セキュリティをはじめとする IT 関連技術は、日々進歩が激しいため、プロフェッショナルとしてのキャリアを望む場合、以前学んだことでは追いつかず、常に新たな技術を習得する必要性にも迫られている。こうした状況を鑑み、米国では、自らの経験・ポジションにあわせ、新たなキャリア構築や次なるステップ・アップを支援する形で、資格に並び、大学が多様なプログラムを提供している。

例えば、ステップ・アップを目指す連邦政府 CIO 支援のために生まれたのが CIO 大学（CIO University）で、これは連邦政府の CIO カウンシル（Federal Chief Information Officers Council）と、連邦政府の一般調達局（General Services Administration：GSA）の後援を受けて、IT 教育の普及と充実を目指し、以下に見るカーネギーメロン大学を始めとする７つの大学が提携してスタートした教育プログラムである。CIO 大学のプログラムを通して、トップ・エグゼクティブのレベルの底上げを図り、政府の能力を向上させることを狙いとしている。現在は、CIO カウンシルより資金を受け、GSA により管理・運営が行われている。CIO 大学の学生の学費は、学生が所属する機関もしくは本人が支払うと定められている。

一方、CIO 大学参加校のような連邦政府との提携を行うことなく、独自の IT セキュリティ教育プログラムを積極的に展開している大学も多い。ここでは、独自の IT セキュリティ教育の例として、「ジョンズ・ホプキンス大学（Johns Hopkins University）」、「ジョージア工科大学（Georgia Institute of Technology）」、「南

カリフォルニア大学（University of Southern California）」そして、「コロンビア大学（Columbia University）」の IT セキュリティ関連プログラムを見ていく。

(1)　CIO 大学

「CIO 大学」は、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一連の大学の総称である。CIO 大学は、トップ・エグゼクティブを対象とした IT 教育の場であることから、CIO 大学提携校において IT 関連プログラムが実施されている。各大学は CIO 大学に参加する以前から、IT 関連のプログラムで定評のある大学が多く、既存プログラムと CIO 大学とを連携させて提供している。CIO レベルを対象としているため、プロジェクト・マネージメントや調達管理などが中心であるが、セキュリティ対策への重要性の高まりに併せ、関連したプログラムも提供されている。

①　CIO 大学設立の背景

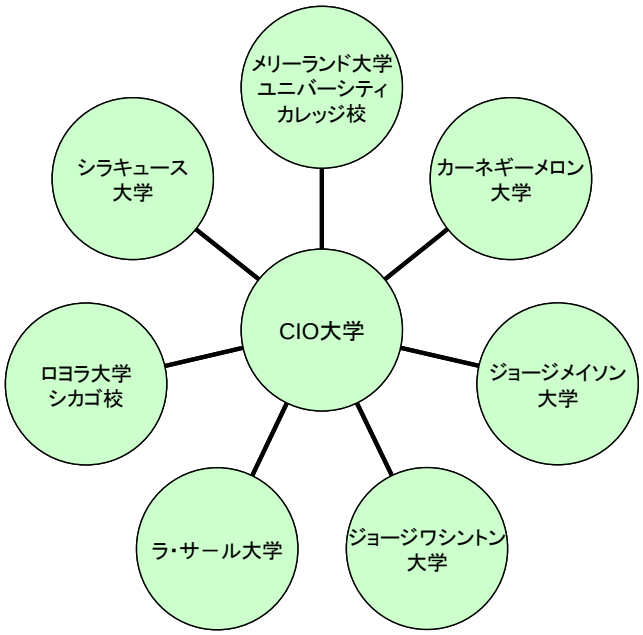
CIO 大学設立の大きな契機となったのは、1996 年に制定され、連邦政府の主要機関全てに CIO 職の設置を義務付けた「The Clinger Cohen Act」である。同法を受けて、CIO カウンシルと GSA は、トップ・エグゼクティブの IT 教育の充実を図る為、CIO 大学の設立に動き出した。

CIO カウンシルと GSA は、連邦政府の IT セクター及び、そのリーダー達のニーズに沿ったプログラムの設立が急務であるという認識の下、「Clinger-Cohen Act」に遵守した「コンピテンシー」を基盤にしたカリキュラム設定を目指した。「コンピテンシー」とは、CIO として、或いは、CIO 関連組織で働く人材として必要不可欠であると CIO カウンシルが見なした知識と技術を指している。カリキュラムを定めるにあたり、政府のみならず、民間にも利用してもらえるプログラムとするため、産・官・学の専門家がフォーカス・グループを結成、検討を重ね「学習目的」としてまとめた。現在、CIO 大学の提携大学として選ばれた大学は、それぞれの大学のコースやセミナー等に、CIO の「学習目的」を組み入れものを、CIO 大学のカリキュラムとして提供している。

②　設立の背景

CIO 大学は、現在 7 大学と提携しており、それぞれの大学が、「正規プログラム（単位取得を目指し、一般の大学院と同様に授業を受け、卒業資格を得ることを目指したもの）」、「モジュール・プログラム（IT の機能についての一般的理解を深めることを目的としたエグゼクティブを対象としたもの）」、「1 週間プログラム（個人の必要に応じて、IT 分野の再教育やアップデートを行うもの）」の 3 タイプのプログラムを提供している。これらプログラムを受講終了後、終了課程により、大学院卒業資格、大学院の単位、CIO 大学卒業の資格を得ることができる。

CIO 大学参加大学



③　　CIO 大学提携校の例：　カーネギーメロン大学

ここでは、上記 CIO 大学提携 7 大学の中でも、IT マネジメント人材育成に関する系統だったプログラムを提供している「カーネギーメロン大学」を取り上げる。

現在、同大学では、CIO 大学との提携プログラムとして、「IT プロジェクト・マネジメント（MS in IT Project Management：修士号）」、「連邦政府 CIO 資格認定プログラム（Federal CIO Certificate Program）」、そして「IT 遠隔教育（MS in Information Technology：MSIT、修士号）」の 3 プログラムを提供している。情報セキュリティについては、この３つの形態のうち、「IT 遠隔教育」で対応している。

同大学の CIO 大学向け「IT 遠隔教育」プログラムは、一般に遠隔地に住む学生などを対象としている。しかし、情報セキュリティのように、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、CIO 大学と提携しているカーネギーメロン大学の通常の修士課程では提供している場合、学生がこれを CIO 大学の単位として履修することを可能としている。

この IT 遠隔教育を通じて履修できる情報セキュリティ・プログラムとして、同大学の「H. John Heinz III School of Public Policy and Management」では、16 ヶ月に及ぶ修士課程プログラム、「情報セキュリティ政策と管理・運営（MS in Information Security Policy and Management: MSISPM）」を提供している。同プログラムでは、学生が情報セキュリティの重要な知識を習得することを目的としており、特に組織のトップやセキュリティ政策アナリスト等に必要と思われる以下の項目に重点を置いている。

- ✓ 組織が直面する情報セキュリティ・リスクについて
- ✓ 情報セキュリティにまつわる、技術的・人的課題についての理解
- ✓ 情報セキュリティを保護するための技術とプロトコールの評価；システムの脆弱性の改善及び、サービスの修復
- ✓ 安全な情報インフラの開発、取得、改善の管理・運営
- ✓ 情報セキュリティ政策、法的環境、市場発展のシステムと組織のゴール設定に対する影響力
- ✓ 特定業界に特殊な問題に対する情報セキュリティ政策についての対応と理解
- ✓ 情報セキュリティ分野における生涯教育と専門的発展

また、情報システム管理（MS in Information Systems Management）という修士課程プログラムも提供しており、以下 6 つのコースがセキュリティに関連した内容となっている。

- ✓情報セキュリティ・マネジメント入門
- ✓デジタル時代のプライバシー
- ✓ハッキングについて
- ✓情報セキュリティ・リスク
- ✓セキュリティ・アーキテクチャと分析
- ✓事故対策

(2)　CIO 大学提携以外の大学における IT セキュリティ・プログラム

以下では、CIO 大学とは提携を結んでいないが、IT 教育プログラムを幅広く行っている主な大学 4 校が実施している IT セキュリティ・プログラムについて見ていく。

①　ジョンズ・ホプキンス大学

同大学では、「JHU Information Security Institute」が IT 関連のプログラムを行っている。IT セキュリティに関しては、修士プログラムにおいて、以下を始めとする 30 以上のコースを提供している。

- ✓ 侵入検知の為の統計的手法
- ✓ セキュリティ情報基礎
- ✓ ネットワーク・セキュリティ
- ✓ 暗号学とネットワーク・セキュリティ
- ✓ インターネットとウェブセキュリティの為のプロトコルとシステム
- ✓ コンピュータ利用におけるセキュリティとプライバシー
- ✓ 情報アシュランス基礎
- ✓ 情報セキュリティの為のアルゴリズム
- ✓ コンピュータ・セキュリティ上級
- ✓ ソフトウェア・エンジニアリングの安全性
- ✓ ジャバ・セキュリティ
- ✓ 組み込みコンピュータ・システム
- ✓ IT セキュリティ・アシュランス
- ✓ 暗号学とコーディング

②　ジョージア工科大学

同大学では、コンピュータ学部が IT 関連のプログラムを行っており、IT セキュリティに関しては、情報セキュリティ・プログラム（MA in Information Security）で、修士号を取得することができる。

同プログラムでは、情報セキュリティ入門、暗号学応用、ネットワーク・セキュリティ、情報セキュリティ研究室など 7 コースが必修、そして専科として a. テクノロジー、b. 政策中心、の 2 プログラムが提供されている。

a. テクノロジー（以下含め合計 8 コース）
- ✓オペレーティング・システム応用
- ✓コンピュータ・ネットワーク
- ✓情報アシュランスの為のモデルと方法論
- ✓イン ターネットワーキング・アーキテクチャ＆プロトコル

b. 政策系（以下含め合計 6 コース）
- ✓科学、テクノロジーと公共政策
- ✓コスト・ベネフィット分析
- ✓情報システム管理、ビジネスプロセスの分析とデザイン
- ✓情報と情報システムのセキュリティとプライバシー

③　南カリフォルニア大学

同大学のコンピュータ・サイエンス学部が提供している「コンピュータ・セキュリティ」修士プログラムは、日々増していくコンピュータ・セキュリティへの脅威に対応する為、他の大学に先駆けて設立された、米国最先端のプログラムの一つである。同プログラムでは以下を含む 12 のコースが実施されている。

- ✓ セキュリティ・システム
- ✓ コンピュータ・コミュニケーション
- ✓ オペレーティング・システム上級
- ✓ ソフトウェア・エンジニアリング
- ✓ ソフトウェア・アーキテクチャ

また、「特別修士プログラム（Special Masters Degree Programs）」の一環として設立されたサイバーセキュリティ・プログラム（Graduate Cybersecurity Program）は、エンジニア大学院プログラムで全米 8 位にランクされるなど、全米トップ・レベルの優れたセキュリティ向け教育プログラムとして知られている。

④　コロンビア大学

同大学での IT 関連のプログラムは、「Computer Science at the School of Engineering」が提供しており、IT セキュリティに関しては、「コンピュータ・セキュリティ（Computer Security）」において修士号を取得することができる。同プログラムは、コンピュータ及びネットワーク・セキュリティ・テクノロジーに関する最先端の知識を学ぶことができる。ここで取り扱うセキュリティは、個々の利用者から、企業、軍隊、政府及び、国のインフラ・インフラ・システムとネッ

トワークに及んでいる。主なセキュリティ関連のコースは以下の通りとなっている。

- ✓ ネットワーク・セキュリティ
- ✓ 暗号学入門
- ✓ コンピュータ・セキュリティ入門
- ✓ セキュリティ上級
- ✓ 暗号学上級
- ✓ 侵入及び異常検知システム

3. 連邦政府主体で行われているＩＴセキュリティ教育

米国では先に述べた CIO 大学ばかりでなく、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。政府が発案者であるが、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。

主な連邦政府・省庁機関が行う IT セキュリティ教育

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

① 「Defense Security Service （DSS）Academy」

DSS は国防総省の管轄の組織で 1972 年に設立された。国防長官、国防総省関連組織等にセキュリティ関連のサービスを提供することを旨としており、その一環として国防総省の教育プログラムを実施している。DSS Academy は、DSS の 3 つのコア・ミッションの一つである「セキュリティ教育、トレーニング及びセキュリティ意識向上プログラム」の実施機関として位置づけられている。

同プログラムの提供対象は、同省のセキュリティ・プログラムの専門家、同省契約企業の社員、その他の政府機関職員、及び特定の外国政府職員となっており、このプログラムを通じて、受講者はセキュリティ分野における質の高い内容のプログラムやトレーニングを受けることができる。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。コースは、メリーランド州の当プログラム施設で行われる他、必要に応じて、米国内外へ出張授業を行う「モバイル」プログラム、や遠隔教育も行われている。

② 「Graduate School: USDA」

1921 年に米農務省長官により設立された「農務省（Department of Agriculture: USDA）大学院」は、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いる。同大学院は、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。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。

IT セキュリティ関連のコースでは、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 IT 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。同プログラムでは、情報セキュリティのデザインやマネジメント・スキルを含めた、論理的・実践的な知識を得ることができる。

③ 「Homeland Security Centers for Excellence」

国土安全保障省は、サイバー・セキュリティ R&D への支援の一環として、R&D 活動に資金提供を行う、いわば国の「サイバー・セキュリティ R&D センター」と

して、「Homeland Security Center for Excellence」と呼ばれるプログラムを 2003 年に設立した。同プログラムは、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。最近では、2005 年 1 月にはメリーランド大学、同大学の研究パートナーとしてカリフォルニア大学ロサンゼルス校（University of California at Los Angeles）、コロラド大学（University of Colorado）、ペンシルバニア大学（University of Pennsylvania）等が、3 年間で 1,200 万ドル、同年 10 月には、ミシガン州立大学が 5 年で 1,000 万ドル、12 月には、ジョンズ・ホプキンス大学が 3 年間で 1,500 万ドルのスカラシップを授与されている。

④　「Federal Cyber Service: Scholarship for Service」

National Science Foundation（NSF）が行っている同プログラムは、テクノロジー社会のニーズを満たすよう、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を図っている。同プログラムでは、以下のような資金支援を提供している。

- ✓ 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 年を通した学生や中小企業への資金援助

NSF の同スカラシップ授与に関して公開されている記録は、2001 年からとなっており、近年の例としては、ノースカロライナ大学シャーロット校（North Carolina at Charlotte）が 65 万ドル、ミシシッピー州立大学が 80 万ドル、空軍工科大学（Air Force Institute of Technology） が約 36 万ドルなどがある。

⑤　「National Centers of Academic Excellence in information Assurance Education（CAEIAE）」

CAEIAE は、NSA と国土安全保障省（Department of Homeland Security）が出資し、1998 年当時の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。また、認定校の学生は、国防総省の「情報アシュランス奨学金プログラム（Department of Defense Information Assurance Scholarship Program）」や「連邦政府のサイバー・サービス奨学金（Federal Cyber Service Scholarship for Service Program）」に申し込むことができる。2006 年は新たにメンフィス大学（University of Memphis）、ロチェスター工科大学（Rochester Institute of Technology）、オハイオ州立大学（Ohio State University）など 12 大学が CAEIAE の認定を受けた。

⑥　「ISC2 Authorized Academic Center Course Module」

2006 年 5 月、ISC2 は、米商務省から、情報セキュリティを扱う同省職員を対象にした、情報セキュリティ教育実施の委託を受け、商務省向け特別プログラムを発表した。ISC2 は以前から一般に提供してきた「Academic Center Course Module」と称する情報セキュリティ教育プログラムをベースに、この商務省向けプログラムを開発した。同プログラムの特徴としては、①受講者のレベルごとに「教室」を設け、オンサイト形式でコースを開催する、②全米の商務省職員に対し、商務省が 1 年分の授業のバウチャーを発行し職員は無料で受講できる、と言う 2 点が挙げられる。

主なコースは以下の通りとなっている：

a. アドミニストレーション：当コースでは、セキュリティ・アドミニストレーションのベストプラクティスを基に、以下を始めとしたセキュリティ・アドミニストレーションの実施において鍵となる事項について学ぶことができる。

- ✓ セキュリティ・アドミニストレーションの目的、原則と定義
- ✓ ライフサイクル・ディベロップメント
- ✓ セキュリティ・コントロール・アーキテクチャ
- ✓ データ分類
- ✓ 雇用対策とガイドライン
- ✓ 政策、基準とガイドライン

b. 悪質なコード：当コースでは、情報システムが提供するサービスを妨害するプログラムとして知られる「Malicious Code（悪質なコードあるいは悪意のあるコード）」に対して必要な対策を講じることができるよう、こうしたソフトウェアによってもたらされる危険性を理解・認識できるようになることを目指している。

⑦　「National Cyber Security Alliance（NCSA）」

NCSA は、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。NCSA では、オンラインの安全な利用の仕方に対する啓蒙活動を、個人ユーザ、中小企業、学校に対し、イベントやセッション等を通して行っている。中でも、サイバー・セキュリティの幼児教育に力を注いでおり、「K-12（幼稚園から高等学校レベルに相当）カリキュラム」と称したプログラムでは、生徒を始め教職員らに対して、「サイバー倫理プロジェクト」、「サイバー・スマート」を始めとする 6 つのコースを実施している。また、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。

（参考資料）

http://www.sans.org/salary2005/
http://www.isaca.org/Template.cfm?Section=Japanese
http://www.comptia.org/
https://www.isc2.org/cgi-bin/content.cgi?category=7
https://www.isc2.org/events/?displaycategory=1416
https://www.isc2.org/cgi-bin/constituent_count.cgi?displaycategory=1344
https://www.isc2.org/cgi-bin/content.cgi?page=818
https://www.isc2.org/cgi-bin/content.cgi?category=539
https://www.isc2.org/japan/about.html
https://www.isc2.org/cgi-bin/content.cgi?category=99
https://www.isc2.org/cgi-bin/content.cgi?page=813#cpes
http://www.nsa.gov/home.cfm
https://www.isc2.org/cgi-bin/content.cgi?page=242
http://www.fas.org/irp/offdocs/nsd/nsd_42.htm
http://www.usdoj.gov/olc/208.htm
http://www.acsac.org/2003/case/thu-c-1530-Oren.pdf#search='15%20U.S.C.Section%203710A'
https://www.isc2.org/cgi-bin/content.cgi?page=817
https://www.isc2.org/cgi-bin/content.cgi?category=1210
https://www.isc2.org/cgi-bin/content.cgi?page=820
https://www.isc2.org/cgi-bin/content.cgi?category=1334
http://www.sans.org/aboutsans.php
http://www.cisecurity.org
http://www.sans.org/faq.php
http://www.giac.org/overview/
http://www.giac.org/certifications/roadmap.php
http://www.sans.org/students.php
http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8199&channelPage=%252Fep%252Fchannel%252FgsaOverview.jsp&channelId=-13451
http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html ;
http://www.ed.gov/policy/gen/leg/cca.html
http://www.gsa.gov/Portal/gsa/ep/contentView.do?contentId=8820&programPage=%2Fep%2Fprogram%2FgsaBasic.jsp&channelId=-13451&ooid=12938&pageTypeId=8199&P=MEP&programId=9980&contentType=GSA_BASIC
http://www.jhuisi.jhu.edu/education/index.html
http://www.cc.gatech.edu/content/view/181/133/
http://viterbi.usc.edu/academics/programs/ms_computer_security.htm
http://www.cs.columbia.edu/education/ms
http://www.dss.mil/training/index.htm
http://grad.usda.gov/
http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0498.xml

http://www.nsa.gov/ia/academia/caeiae.cfm
http://www.iwar.org.uk/pipermail/infocon/2003-July/000400.html
http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5228
http://www.nsf.gov/about/glance.jsp
http://www.fas.org/irp/offdocs/pdd/pdd-63.htm
http://www.whitehouse.gov/pcipb/
http://www.nsa.gov/releases/relea00104.cfm
https://www.isc2.org/cgi-bin/content.cgi?page=892
http://biz.yahoo.com/prnews/060519/dcf014.html?.v=48
http://www.staysafeonline.org/

このレポートに対するご質問、ご意見、ご要望がありましたら、
hiroyoshi_watanabe@jetro.go.jp までお願いします。