情報セキュリティ教育に関する
調査報告書

２００４年6月

情報セキュリティ教育研究会

はじめに

情報通信技術（IT）は急速に革新を繰り返しながら社会基盤として浸透しており、我々の社会生活・経済活動は IT 技術なくしては成り立たない状況であると言える。そうした現状において安全・安心な国民生活を成立させていくためにも情報セキュリティの確保が国家的な課題であり、国家 IT 戦略である e-Japan 戦略 II にも IT 社会基盤整備のための重要項目に挙げられている。この高度情報化社会を安全・安心なものとしていくためにはこのネットワーク社会に参画する個人・組織の全てが情報セキュリティの重要性を認識し、情報セキュリティ確保のための不断の努力を行っていく必要がある。

組織における情報セキュリティに関していえば、事業を行っていくにあたり情報システムを利用し、情報資産を活用していくわけであるが、継続的に事業を行い、サービスを提供すること、また保有する情報資産を安全に管理していく必要があるという意味でもその社会的責任は重く、情報セキュリティ対策の充実が求められている。

現状はというと情報システムが高度化・複雑化し、情報資産の社会的価値・影響度は高まるばかりであり、また IT 事件・事故も多く発生し社会問題になっているが、この現状に対応するため多くの情報システムユーザは情報セキュリティ確保のために相当の資源を割く必要に迫られている。とりわけ組織において情報セキュリティ対策の実施を担う立場にある責任者は、ネットワークやＯＳなどの基礎知識から、専門的な技術知識、それだけでなくマネジメントの観点から情報セキュリティポリシの策定・運用や組織のリスクアセスメント、関連法律の遵守など非常に幅広い知識やスキルが要求される。よってこうした人材を育成し、確保するためでなく、彼等を支える経営層の理解を得るため、また組織内エンドユーザのリテラシー向上のため、情報セキュリティに関する教育の充実の必要性が高まっている。

こうした状況において、経済産業省は「情報セキュリティ教育研究会」を設置した。研究会では、情報セキュリティ教育の専門家の参加を得て、民間の情報セキュリティ教育関係者やユーザ企業含めて情報セキュリティ対策の中核的役割を担う責任者に対する情報セキュリティの実践的な教育内容・方法を検討してきた。また併せて情報セキュリティ教育、人材育成に関して広く議論を行い、情報セキュリティ教育の充実・普及のために必要な検討事項をまとめ、提言としてとりまとめた。

政府は安全・安心なネットワーク環境を提供するため情報セキュリティ教育を更に充実・普及すべく必要な措置を講ずることを期待する。またこのネットワーク社会に参画する者の責務として、企業などの組織の責任者は、情報セキュリティ教育受講者、提供者ともに教育実施機会と内容の充実に尽力し、情報セキュリティの向上に努めていくことを強く期待したい。

平成１６年３月
情報セキュリティ教育研究会
佐々木　良一

情報セキュリティ教育研究会委員名簿

【座長】

佐々木　良一	東京電機大学　工学部　情報メディア学科　教授

【委員】

稲垣　隆一	稲垣隆一法律事務所　弁護士・ISMS 主任審査員 （日弁連 コンピュータ研究委員会 副委員長）
岩村　奉武	石川島播磨重工業株式会社　理事・情報システム部長 （社団法人日本経済団体連合会　情報通信委員会　情報化部会委員）
植田　　威	学校法人岩崎学園　理事　経営企画部　部長
内田　勝也	中央大学　研究開発機構　助教授
菊池　浩明	東海大学　電子情報学部　情報メディア学科　助教授
郡山　　信	財団法人金融情報システムセンター　監査安全部長
菅谷　光啓	SANS JAPAN Project 事務局
津田　　稔	東京商工会議所　IT 推進委員会　専門委員会　座長
中本　健司	SEA/J 事務局　コンテンツ部会長
原田　要之助	ISACA 東京支部 前支部長
伏見　　諭	株式会社情報数理研究所　専務取締役
舟本　　奨	ＩＴ人材育成事業者協議会　事務局長
丸山　満彦	ISACA 大阪支部長
吉田　　眞	東京大学大学院　工学研究科　教授　教育プロジェクト室担当

【オブザーバ】

独立行政法人 情報処理推進機構　（情報処理振興事業協会）
NPO 日本ネットワークセキュリティ協会
NPO ネットワークリスクマネジメント協会

【事務局】

経済産業省　商務情報政策局　情報セキュリティ政策室

目　次

１．検討の背景

企業や各種団体等の組織において情報セキュリティを維持するためには、そうした組織において利用される情報システムのセキュリティを維持する外部・内部の技術者の協力が不可欠である。特に、情報システムの最高責任者にあたる役員や理事等の経営層（以下、管理責任者という）を補佐する立場にあり、情報セキュリティ対策を実質的にリードする役割を担う人材（以下、実施責任者という）に求められる責任は極めて重い。

表１　参考分類イメージ

対象者分類	キーワード
管理責任者	CIO[1]、CISO[2]、（ISMS[3] でいうところの）情報セキュリティ委員会の長、等
実施責任者 （主たる教育対象の候補）	CIO 補佐、CIO 補佐官、（大学等における）メディアセンター長、（企業等における）情報システム関連部署の長、（ISMS でいうところの）情報セキュリティ委員会の推進事務局の長、情報システム運用管理者、等及び上記の補佐クラス
実施担当者	（大学等における）メディアセンターの職員、（企業等における）情報システム部員、（ISMS でいうところの）情報セキュリティ委員会の推進事務局担当者、情報システム運用担当者、等

２．本会の目的

組織の情報セキュリティを維持・向上させる責任と権限を実質的に負うべき実施責任者、すなわち「企業等における情報システム関連部署の長」、「大学等におけるメディアセンター長」、「ISMS でいうところの情報セキュリティ委員会の委員長や、CISO等を補佐する立場にある者」等を育成するための情報セキュリティ教育のあるべき姿を検討する。

[1] Chief Information Officer、情報システム担当役員
[2] Chief Information Security Officer、情報セキュリティ担当役員
[3] Information Security Management System、情報セキュリティマネジメントシステム

３．情報セキュリティ教育の現状

３．１　教育実施状況

（1）現在のスキル保有状況

現在、多くの企業や組織において、実施責任者たる情報システムの運用管理者は、情報セキュリティ関連部署に配置されていると推測される。こうした情報セキュリティ関連部署において、どのようなスキルを持つ人材が配置されているかの実態を次図に示す。

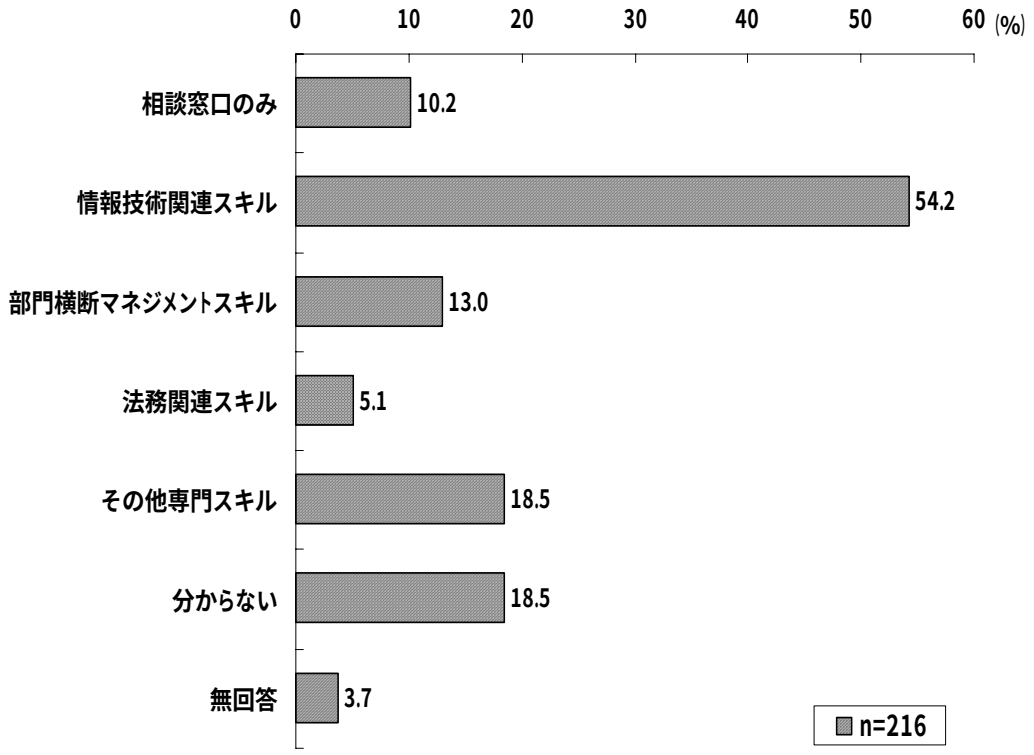

図１　情報セキュリティ管理部門の人材配置状況（出典：IPA/ISEC）

この図から明らかな通り、多くの組織においては、情報技術関連のスキルが中心となっている。しかしながら、実施責任者は、およそ役員層が就任するであろう管理責任者を実質的に補佐する立場（ＣＩＯ補佐官、ＣＩＳＯ補佐官）を担うべきであることから、単に情報技術関連のスキルだけでは不足であり、組織をマネジメントするスキルや法務関連のスキルを充実させることが重要と考えられる。

→ マネジメントや法務など、情報技術以外のスキルの充実

（2）情報セキュリティ管理者の設置状況

企業や組織において、どのような立場の人材が情報セキュリティ管理者を担当しているかを次図に示す。

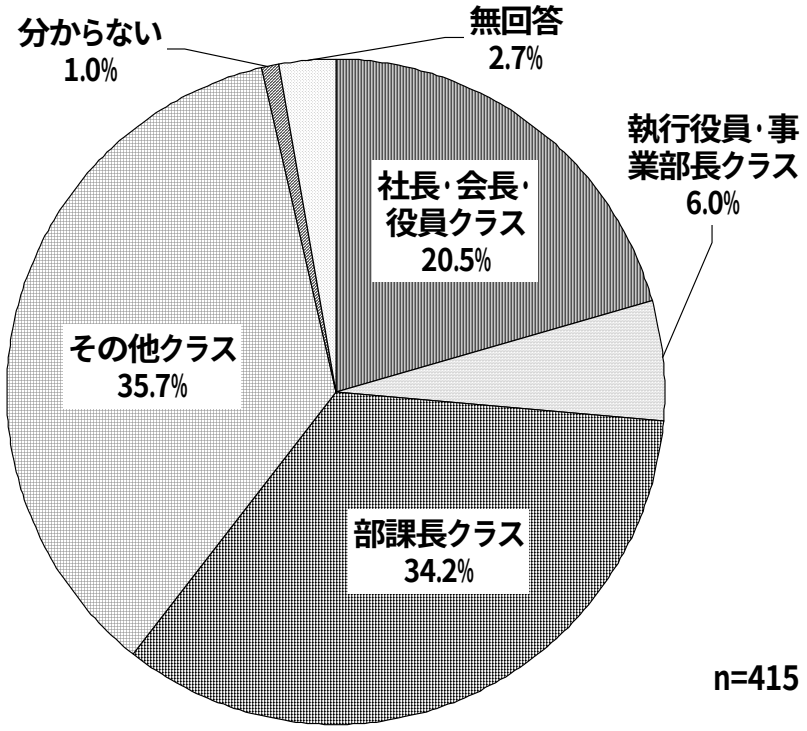

図２　情報セキュリティ管理者の役職（出典：IPA/ISEC）

本来、情報セキュリティは、組織全体をマネジメントする立場にある層が管理を担当すべきではあるが、実態としては、部課長クラス（あるいはそれ以下のクラス）が就任する場合が多い。そのため、少なくとも現状においては、そうした層を中心とする情報セキュリティ教育を推進することが、企業や組織全体の情報セキュリティの実現に寄与すると考えられる。

→　現実の担当者層への情報セキュリティ教育の充実

（3）情報セキュリティ教育の教育実施状況

情報セキュリティ管理者に対して、現在実施されている教育は、ほとんどがＯＪＴ中心となっており、求められるスキルを向上させるような教育は実施されていないのが実情である。

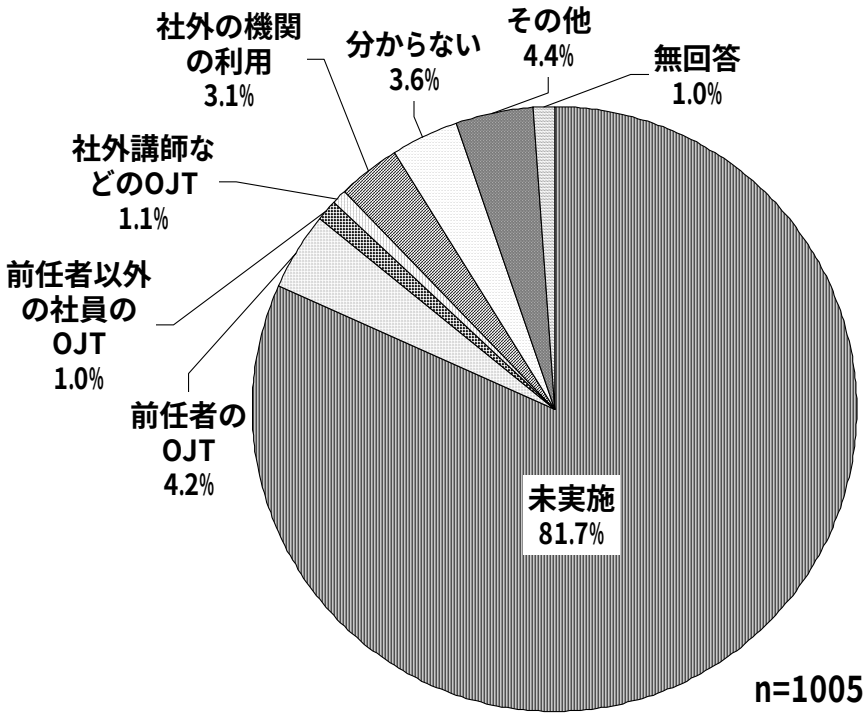

図３　情報セキュリティ管理者の育成及び教育体制（出典：IPA/ISEC）

まず、ほとんどの組織において実施されておらず、また実施されていたとしても、前任者あるいは他の社員からのＯＪＴが中心であり、専門的な教育は実施されていない。

→ ＯＪＴだけでなく、専門知識やスキルを付与するための教育を充実

（4）情報セキュリティ教育へのニーズ

現状では、あまり充実しているとは言えない情報セキュリティ教育ではあるが、必要性についてはそれなりに認知されている。

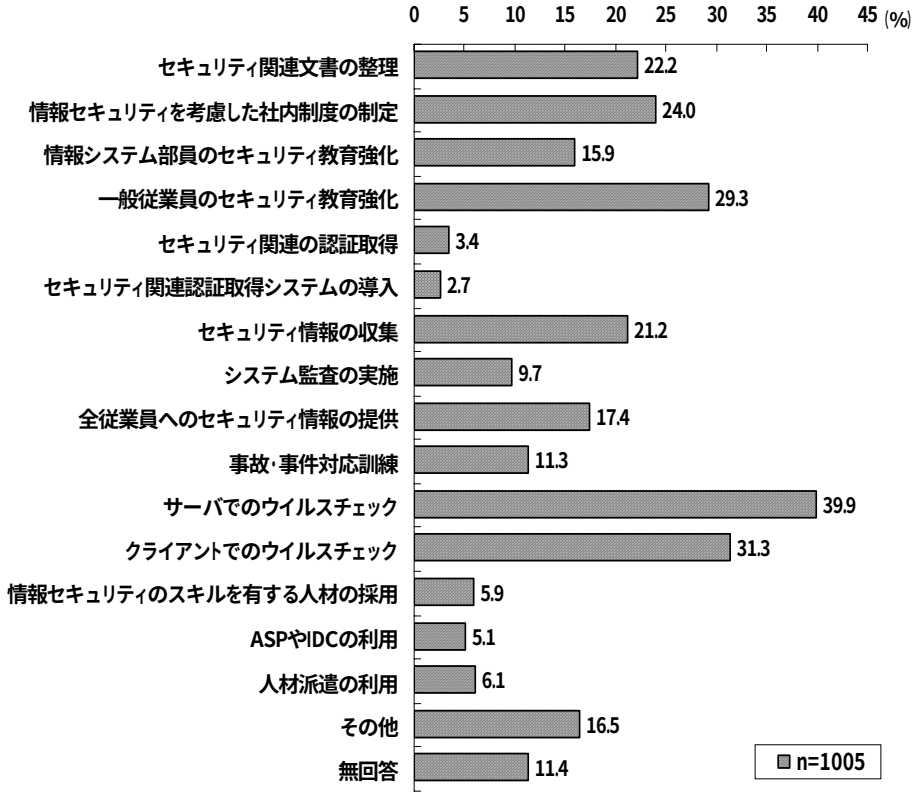

図４　今後実施していきたいセキュリティ対策（出典：IPA/ISEC）

一般従業員のセキュリティ教育強化、および情報システム部員のセキュリティ教育強化について、その必要性は認知されつつある。

→ 情報セキュリティ教育の普及や啓発、教育実施体制の整備など

（５）政府等への期待

情報セキュリティ対策を実現する上で、政府や公共団体等に期待されている役割は、次図の通りである。

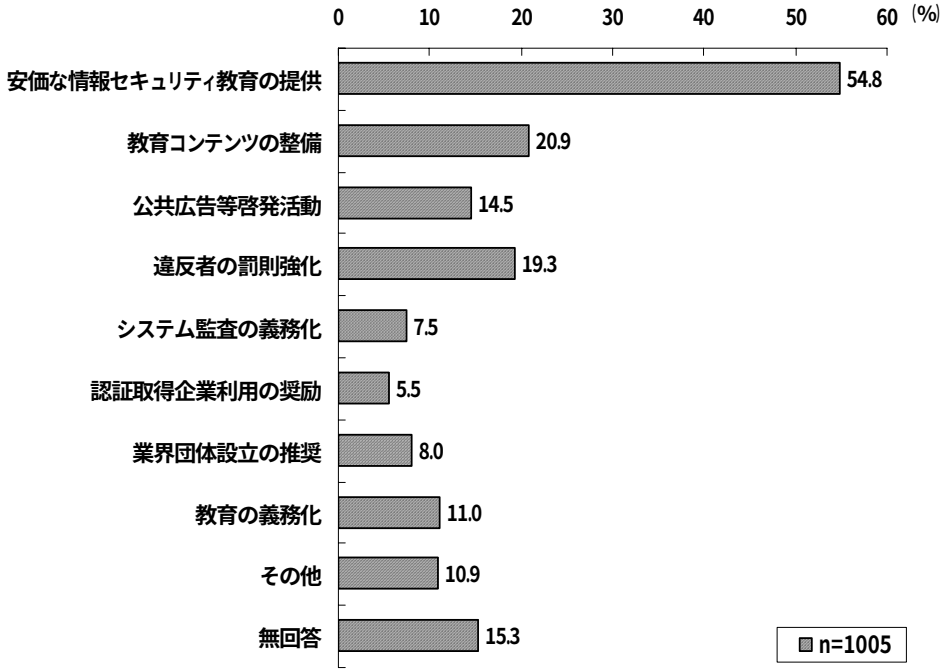

図５　政府及び公共団体に希望する情報セキュリティ対策（出典：IPA/ISEC）

企業や組織等が、政府や各種公共団体に対して期待している役割としては、低価格な情報セキュリティ教育の提供が突出している。その他に、教育コンテンツの整備や教育の義務化といった施策を求める声もある。

無償セミナー等の安易な実施は、確かに情報セキュリティ教育の普及を促進する効果が期待される一方で、情報セキュリティ教育を実施する主体（教育事業者等）による自由競争を阻害し、そうした産業の育成を阻害する可能性もあるため、慎重な対応が求められるところである。

→　低価格での情報セキュリティ教育の提供、教育用コンテンツの整備
　　（ただし、自由競争原理とのバランスへの配慮が必要）

３．２　情報セキュリティ教育制度および資格認定制度の現状

現在、国内において受講可能な、あるいは認知度のある情報セキュリティ教育制度および資格認定制度のうち、個々の製品や技術に特化した内容の制度を除き、実施責任者層に適していると思われる制度を以下に順次列挙する。

なお、これら制度のより詳細な情報の入手源を末尾の参考資料１）に、また、補足説明を末尾の参考資料２）に記した。

表２　現行の情報セキュリティ教育制度および資格認定制度

略称、通称	CISSP	Security+
正式名称	Certified Information System Security Professional	Security+
主催者	International Information Systems Security Certification Consortium, (ISC)2	The Computing Technology Industry Association, CompTIA
参照 URL	http://www.isc2.org/	http://www.comptia.jp/cont_certif_10.html
想定到達目標 受講対象者	■ 組織内でセキュリティをすべて仕切ることができる人 ■ セキュリティ実現のための計画を実現できる人 ■ セキュリティのコンサルティングをできる人 ■ セキュリティ面で責任を持って組織運営ができる人、あるいは補佐をできる人	■ 少なくとも２年間のネットワーク実務経験を有し、TCP/IP の正確な技術を持つ技術者を前提 ■ 下記に示す分野について、基礎的なレベルのスキルと知識を有する者を認定
スキル項目	■ Security Management Practices ■ Security Architecture and Models ■ Access Control Systems & Methodology ■ Application Development Security ■ Operations Security ■ Physical Security ■ Cryptography ■ Telecommunications, Network& Internet Security ■ Business Continuity Planning ■ Law, Investigations & Ethics	■ General Security Concepts ■ Communication Security ■ Infrastructure Security ■ Basics of Cryptography ■ Operational / Organizational Security
教育時間	８時間×５日　（CBK セミナー）	６日間　（SANS 教育コースの場合）

表２　現行の情報セキュリティ教育制度および資格認定制度（続き）

略称、通称	CISM	NISM
正式名称	Certified Information Security Manager 公認情報セキュリティマネージャー （2005 年より日本語による受験が可能）	Network Information Security Manager ネットワーク情報セキュリティマネージャ
主催者	Information Systems Audit and Control Association, ISACA （情報システムコントロール協会）	NISM 推進協議会　（情報通信ネットワーク産業協会、（社）テレコムサービス協会、（社）電気通信事業者協会、（社）電波産業会、（社）日本インターネットプロバイダ協会、（財）日本データ通信協会、ネットワークセキュリティ登録事業者協議会）
参照 URL	http://www.isaca.org/ （日本語：http://isaca.gr.jp/）	http://www.learningsite21.com/nism/top.html
想定到達目標 受講対象者	情報セキュリティ管理に責任を有する、経験豊富な情報セキュリティ管理者	（コースにより異なる） ※協議会の各加盟団体に加盟している事業者のみ受講可
スキル項目	■ Information Security Governance ■ Risk Management ■ Information Security Program(me) Management ■ Information Security Management ■ Response Management	（コースにより異なる。コースは以下の通り） ◇ ネットワークセキュリティ基礎（２日） ◇ ネットワークセキュリティ実践（３日） ◇ サーバセキュリティ実践（３日） ◇ セキュリティポリシ実践（２日） ◇ セキュリティ監視実践（３日）
教育時間	更新時に、年間 20CPE 時間以上、3 年間で 120CPE 時間以上が必要。（1CPE 時間は 50 分） 受験者向けに、CISM　Review　Course がある。	（各コース名の後ろに更新時の講習時間を記載）

表２　現行の情報セキュリティ教育制度および資格認定制度（続き）

略称、通称	CSBM、CSPM (Technical, Management)	GIAC
正式名称	Certified Security Basic Master Certified Security Professional Master	Global Information Assurance Certification
主催者	Security Education Alliance / Japan, SEA/J	SANS Institute
参照 URL	http://www.sea-j.net/course.html	http://www.giac.org/
想定到達目標 受講対象者	基礎コース：スキルマップのレベル１　（基礎知識）の習得 応用コース：高度なスキルが求められるセキュリティ関連業務従事者	（認定コースにより異なる）
スキル項目	■ 基礎コース ◇ ネットワークセキュリティ基礎 ◇ 攻撃手法 ◇ ファイアウォール ◇ 侵入検知システム ◇ 暗号・認証 ◇ PKI ◇ セキュリティプロトコル ◇ ウイルス ◇ クライアントセキュリティ ◇ 権限とデータ管理 ◇ 情報セキュリティポリシ ◇ 関連法規 ■ 応用コース（テクニカル編） ◇ 脅威とその対策、OS セキュリティ、サーバセキュリティ、ファイアウォール、IDS、VPN 導入設計、PKI の利用 ■ 応用コース（マネジメント編） ◇ 脅威と脆弱性、情報セキュリティマネジメント、リスクマネジメント、情報セキュリティポリシ、情報セキュリティ監査制度	（認定コースにより異なる。コースは下記の通り。） ◇ GIAC Security Essentials Certification (GSEC) ◇ GIAC Certified Firewall Analyst (GCFW) ◇ GIAC Certified Intrusion Analyst (GCIA) ◇ GIAC Certified Incident Handler (GCIH) ◇ GIAC Certified Windows Security Administrator (GCWN) ◇ GIAC Certified UNIX Security Administrator (GCUX) ◇ GIAC Information Security Officer (GISO) ◇ GIAC Systems and Network Auditor (GSNA) ◇ GIAC Certified Forensic Analyst (GCFA) ◇ GIAC IT Security Audit Essentials (GSAE) ◇ GIAC Security Consultant (GSCC) ◇ GIAC 17799 Security and Audit Framework (G7799) ◇ GIAC Security Expert (GSE)
教育時間	CSBM(２日間) CSPM テクニカル編(3 日間) CSPM マネジメント編(2 日間)	各６日間　（SANS の 教育コース） ※コース終了後、6 ヶ月間にわたるフォローアップあり

表２　現行の情報セキュリティ教育制度および資格認定制度（続き）

略称、通称	MSISTM	MSISPM
正式名称	Master of Science in Information Security Technology and Management	Master of Science in Information Security Policy and Management
主催者	Carnegie Mellon Univ.	Carnegie Mellon Univ.
参照 URL	http://www.ini.cmu.edu/academics/MSISTM/msistm_overview.htm	http://www.heinz.cmu.edu/msispm/
想定到達目標 受講対象者	■情報セキュリティの指導者育成	■情報セキュリティポリシ策定やセキュリティ業務管理の習得
スキル項目	■ Management **95-751**: Information Security Risk Management **45-750/45-775**: Managerial Economics and Business Management; ■ Technology (**18-345** or **18-756**) and (**15-410** or **18-842**): **18-345** Introduction to Telecommunication Networks or **18-756**: Packet Switching and Computer Networks AND **15-41**0: Operating System Design and Implementation or **18-842**: Distributed Systems ■ Security **18-730**: Introduction to Computer Security and two of: **18-731**: Network Security **18-732**: Secure Software Engineering **18-733**: Applied Cryptography、他	■ Required Courses (72 units) **91-857** Financial Modeling **95-751** Organizational Management and Information Security **95-752** Introduction to Information Security Management **95-754** Economics of Information Security **95-760** Decision Making in Uncertainty **95-796** Statistics for IT Managers **95-770** Security Policy Seminars: Healthcare, Finance, and/or Government **18-630** Introduction to Computer and Communications Security ■ Security Electives (Select 3 from below) (36 units) **95-750** Security Architecture and Analysis **95-753** Telecommunications Security **95-755** Advanced Topics in Information Security **95-756** Information Security Risk Management、他
履修期間	１６ヶ月	１６ヶ月

表２　現行の情報セキュリティ教育制度および資格認定制度（続き）

略称、通称	SS	スキルマップ
正式名称	情報セキュリティアドミニストレータ試験	（情報セキュリティプロフェッショナル育成について）
主催者	（財）日本情報処理開発協会　（～2003/12） （独）情報処理推進機構（2004/1～）	情報処理振興事業協会、 日本ネットワークセキュリティ協会
参照 URL	http://www.jitec.jp/	http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html
想定到達目標 想定対象者	情報セキュリティに関する基本的な知識を持ち、情報システムの情報セキュリティポリシの策定及びその実施、分析、見直しを行う者	（情報セキュリティプロフェッショナルの評価と教育を目的として、ある人が持つスキルや、企業や組織に求められる人材像を表現する。）
スキル項目	■ セキュリティ方針の策定 ■ セキュリティ基準の策定 ■ セキュリティシステムの設計 ■ セキュリティシステムの実装および検査 ■ セキュリティシステムの運用管理 ■ セキュリティの分析 ■ セキュリティポリシの見直し	■ 情報セキュリティポリシ ■ ネットワークインフラセキュリティ ■ サーバアプリケーションセキュリティ ■ OS セキュリティ ■ ファイアウォール ■ 侵入検知システム ■ ウイルス ■ セキュアプログラミング技法 ■ セキュリティ運用 ■ セキュリティプロトコル ■ 認証 ■ PKI ■ 暗号 ■ 署名 ■ 攻撃手法 ■ 法令・規格
教育時間	（特に定めなし）	（特に定めなし）

ここまでに紹介した情報セキュリティ教育制度および資格認定制度について、それぞれのポジショニングを検討する。横軸の左側をサプライヤ向け（主に）技術系の教育、左側をユーザ向け（主に）マネジメント系の教育とし、縦軸は上に向かうほど高度であるとして、各種の教育制度と資格認定制度をそれぞれの組み合わせごとにマッピングしたのが次図である。

この図から分かる通り、サプライヤ側については、
徐々に教育及び試験制度が整いつつあるのに比べ、
ユーザ側は教育制度が手薄となっている。

特に、ユーザ側において管理責任者、あるいは実施責任者の立場にある者に対する教育制度の立ち遅れが顕著であると言えよう。

さらに言えば、ユーザ側の入門者や初心者に対する制度的な措置は全くなされていないのが実情である。

OECD のセキュリティ原則では、すべてのネットワーク参加者に対して、その責任を果たすことを求めているが、現状を鑑みる限りにおいては、まだまだセキュリティ文化の普及は心許ない状況にあると言えよう。

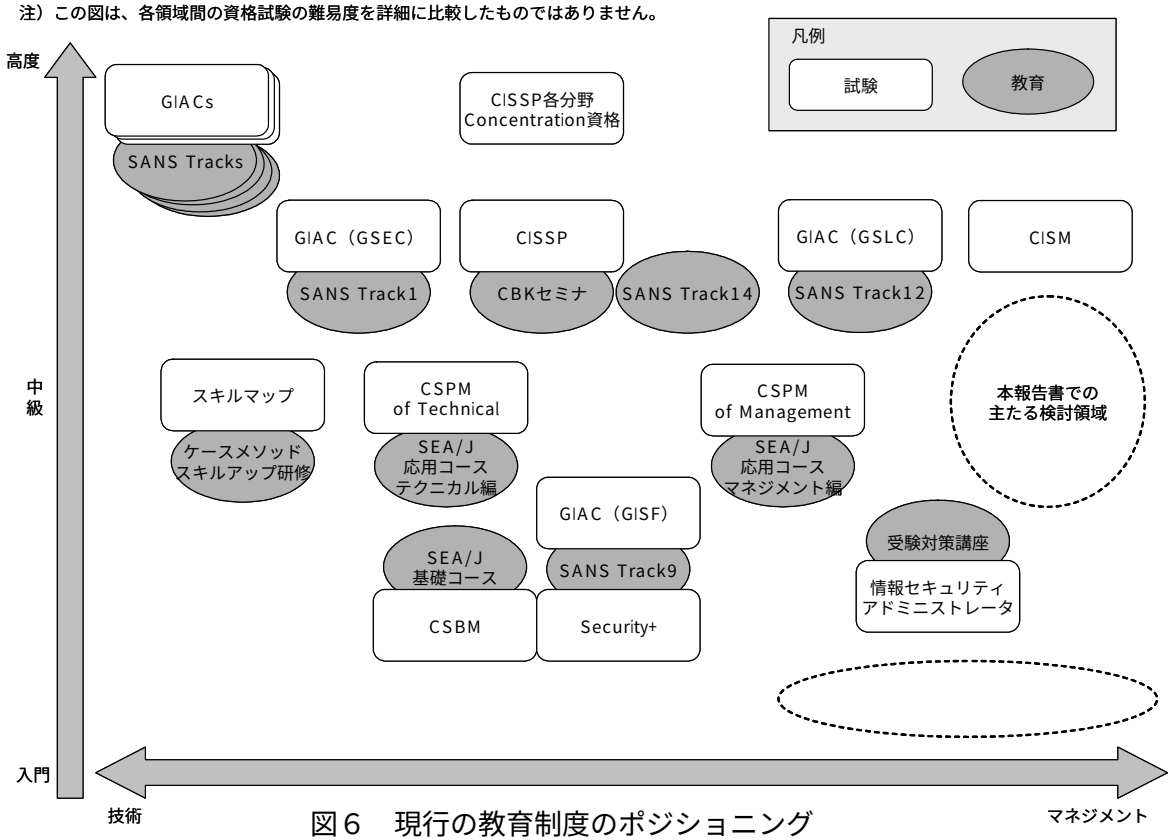

図６　現行の教育制度のポジショニング

４．情報セキュリティ教育カリキュラムの検討

４．１　検討の前提

前章で述べた情報セキュリティ教育制度および資格認定制度を参考にしつつ、実施責任者に最適な教育カリキュラムを検討するため、下表に記した通りの前提条件を定めた。

表３　情報セキュリティ教育カリキュラム検討時の前提条件

教育受講対象者	組織の情報セキュリティ管理者（第１章で実施責任者と呼ばれている立場）とする。マネジメントを行う立場であるが、技術的判断をも求められるという想定とする。組織の規模、業種は特定しない。
カリキュラムの想定レベル	「望ましくはここまでの知識を身に付けてもらいたい」という高度なレベルの教育を想定レベルとする。その後、コースの検討時に「知っておかなければならない最低限のレベル」としての教育項目をまとめる。
教育受講期間	二、三日、一週間、モジュール制など様々な形態が考えられるが、「あるべき論」を検討する。時間的制約については、コース検討時に検討する。
教育内容	（組織の構成を検討する、実施担当者を指揮する、セキュリティ施策を検討・判断するなど）通常時の対応、および緊急時の対応を行うために必要な知識。技術的知識、マネジメント的知識、法律知識などを含む。

以降の検討は、上記の前提条件に基づいて実施した結果である。

４．２　教育カリキュラムの体系

教育カリキュラムは、主に技術的側面からの情報セキュリティ対策について論じる「技術」系と、主に管理的側面からの情報セキュリティ対策について論じる「マネジメント」系で構成する。これら２つの系に加えて、全体を概観するために用意した共通系がある。

共通系は、すべての受講者が受講することを期待している。また、時間的な制約がある場合に、共通系だけの受講でも情報セキュリティの全体像を俯瞰できることを目指している。そのため、１科目（大項目）だけの構成とした。なお、検討に際して、大項目はおおよそ３時間程度を想定して設計している。

技術系は、（Ｔ１）セキュリティへの脅威～（Ｔ８）ＰＫＩ[4]までの大項目８科目で構成した。さらに、次章以降でコースを設計する際の指針とすべく、必修項目と選択項目に分類した。必修項目は、（Ｔ１）セキュリティへの脅威～（Ｔ５）認証・アクセス制御までの５科目である。（Ｔ６）ネットワーク技術～（Ｔ８）ＰＫＩの３科目については、選択項目としている。

マネジメント系は、（Ｍ１）情報セキュリティマネジメント～（Ｍ１０）監査までの大項目１０科目で構成した。必修項目は、（Ｍ１）情報セキュリティマネジメント～（Ｍ６）個人情報保護までの６科目である。（Ｍ７）システム開発管理～（Ｍ１０）監査までの４科目については、選択項目としている。

上記の情報セキュリティ教育カリキュラムの体系を次表にまとめて掲載する。

[4] Public Key Infrastructure、公開鍵暗号基盤

表４　情報セキュリティ教育のカリキュラム体系

分類	項番	大項目（１科目３時間程度と想定）	参考キーワード
共通系			
	０	**情報セキュリティ概論**	機密性･完全性･可用性、予防･発見･対処
技術系			
	Ｔ　１	**セキュリティへの脅威**	不正アクセス、サービス妨害、ウイルス、マルウェア、ソーシャルエンジニアリング
	Ｔ　２	**ネットワークセキュリティ**	ファイアウォール、侵入検知システム
	Ｔ　３	**OS セキュリティ**	
	Ｔ　４	**アプリケーションセキュリティ**	SSL (Secure Socket Layer)、S/MIME
	Ｔ　５	**認証・アクセス制御**	
	Ｔ　６	**ネットワーク技術**	ルーティング
	Ｔ　７	**暗号技術**	共通鍵、公開鍵、ハッシュ関数、電子認証
	Ｔ　８	**PKI**	認証局、登録局、発行局、電子公証
マネジメント系			
	Ｍ　１	**情報セキュリティマネジメント**	
	Ｍ　２	**情報セキュリティポリシ**	
	Ｍ　３	**リスクアセスメント**	
	Ｍ　４	**クライシスマネジメント（危機管理）と事前準備**	CERT、災害時復旧計画、事業継続計画
	Ｍ　５	**法令と標準化**	
	Ｍ　６	**個人情報保護**	
	Ｍ　７	**システム開発管理**	ソフトウェア開発ライフサイクル
	Ｍ　８	**情報管理**	著作権、ライセンス管理
	Ｍ　９	**教育・訓練**	モラル、モチベーション
	Ｍ　１０	**監査**	情報セキュリティ監査、システム監査

必修

※）上記の他に、「演習」系と、後述する「製品・サービス紹介」系を設ける。

前表に記した各科目においては、次の概要に示した教育を実施する。

表５　情報セキュリティ教育の各科目の概要

項番	科目名	科目の概要
0 必修	情報セキュリティ 概論	情報セキュリティの基本的な概念について学ぶ。また、以後の各科目を理解するために必要最低限の基礎知識を習得する。
T1 必修	セキュリティ への脅威	情報セキュリティを脅かす様々な脅威に関して、どのような種類があるのか、またどのような経路や手段などが用いられるのかを理解する。
T2 必修	ネットワーク セキュリティ	ネットワークを構築・運用する際に利用可能なセキュリティ技術について概観を与え、基礎的な知識を習得する。
T3 必修	OS セキュリティ	個々のコンピュータ、特にＯＳに関連して、コンピュータを守るために利用可能なセキュリティ技術について概観を与え、基礎的な知識を習得する。
T4 必修	アプリケーション セキュリティ	Web ブラウザ､電子メールソフト等を中心とするアプリケーションに関して、利用可能なセキュリティ技術について概観を与え、基礎的な知識を習得する。
T5 必修	認証・アクセス制御	情報セキュリティを維持するために重要な要素技術の一つである識別、認証、アクセス制御（３Ａ）について、基礎的な知識を習得する。
T6 選択	ネットワーク技術	ネットワークセキュリティを深く理解するために本来必要なネットワーク技術について、全体像を概観し、基礎的な知識を習得する。
T7 選択	暗号技術	共通鍵暗号、公開鍵暗号、ハッシュ関数、デジタル署名、鍵管理といった暗号技術の基礎的な知識を与え、主に暗号技術の利用方法について習得する。
T8 選択	PKI	暗号技術の重要な応用である PKI について、デジタル証明書の役割、認証局の役割や仕組み、電子公証や時刻認証などの新しい応用について習得する。
M1 必修	情報セキュリティ マネジメント	情報セキュリティをマネジメントするための基礎的なサイクル、及び物理的、人的セキュリティの側面について、基礎的な対策を習得する。
M2 必修	情報セキュリティ ポリシ	情報セキュリティポリシの必要性を認識し、構成について理解した上で、具体的な方針や規程類の策定方法を習得する。
M3 必修	リスク アセスメント	組織が保有する情報資産を適切に評価し、それら資産を取り巻く脅威、脆弱性に基づいてリスクを分析、評価するための基礎的な考え方を習得する。
M4 必修	クライシスマネジメント（危機管理）と事前準備	万が一クライシスが発生した際の基本的な対応方策を習得すると共に、そうした緊急時の対応を適切に実施するための普段からの準備事項を習得する。
M5 必修	法令と標準化	情報セキュリティを維持する上で有益な各種の規格・基準・指針・ガイドラインについて概観を得ると共に、遵守が必須となる法令について習得する。
M6 必修	個人情報保護	OECD８原則[5]、EU指令[6]等、個人情報保護の歴史的な背景を知ると共に、プライバシーポリシの策定やJISコンプライアンスプログラム等を習得する。
M7 選択	システム開発管理	自組織において情報システムを開発し、それを安全に運営するため必要となる、ライフサイクルに沿ったセキュリティの考え方を習得する。
M8 選択	情報管理	資産のインベントリ管理、著作物の知的財産権の管理、企業の営業機密等の管理について、基本的な考え方と実施すべき対策を習得する。
M9 選択	教育・訓練	管理する立場の者として必要な、利用者の啓発や教育訓練、また技術者の育成等に関する教育の方法・効果測定法などを習得する。
M10 選択	監査	管理する立場の者として必要な、情報セキュリティ監査、システム監査に関する基礎的な知識や手法を習得する。

[5] プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告

[6] 個人データ処理に係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC指令

４．３　教育カリキュラムの詳細説明

前節で述べた教育カリキュラムの体系に沿って、各大項目（科目）をさらに詳細化し、中項目として検討した。また、中項目の設定に際しては、当該中項目の内容について、教材等の開発者がイメージを掴みやすいように、参考となるキーワードを併せて設定した。ただし、このキーワードについては、技術の進歩等に伴って定期的な追加や更新を行う必要がある。

さらには、中項目についても、定期的な見直しを実施し、場合によっては追加や更新を行う必要性が考えられる。ただし、大項目については、できるだけ普遍的な内容となるよう配慮したため、当面の間は、変更の必要はないものと考えている。

以下、大項目の順に沿って、各大項目別の中項目とキーワードを掲載する。

表６　情報セキュリティ教育カリキュラムの詳細説明（共通系）

区分	必修/選択	番号	大項目（１科目３時間程度と仮定）	中項目	キーワード
共通	必修	0	情報セキュリティ概論		
				情報セキュリティの必要性	
					コンプライアンス経営概論、情報セキュリティと情報セキュリティ対策・情報セキュリティマネジメントの目的、費用対効果、説明責任
				情報資産	
					情報資産の分類、機密度の設定
				情報資産の重要性	
					機密性
					完全性
					可用性
				リスクの考え方	
					脆弱性
					脅威
				情報セキュリティ対策の側面	
					予防、検出、対処
					技術的対応と管理・運用的対応

表７　情報セキュリティ教育カリキュラムの詳細説明（技術系）

区分	必修/選択	番号	大項目	中項目	キーワード
技術	必修	Ｔ１	セキュリティへの脅威		
				ネットワークからの脅威	
					サービス妨害攻撃
					盗聴、改ざん、情報漏洩
					不正侵入
					踏み台
					メール爆弾
				組織内環境での脅威	
					媒体盗難、紛失
					論理爆弾
					メールの転送
					バックドア
					誤操作による情報漏えい
					ソーシャルエンジニアリング
				物理的脅威	
					災害
					破壊、妨害行為
				コンピュータウイルス、ワーム、マルウェアによる脅威	
					感染先による分類
					隠蔽手法による分類
					ウイルスが利用する技術による分類
					ウイルスの活動による分類
					デマウイルス
				電子商取引とコミュニケーション上での脅威	
					二重発注
					ユーザなりすまし
					否認
					名誉毀損
					サイバースクワッティング
					spam
				モバイル環境における脅威	

技術　必修　T２　ネットワークセキュリティ

- 基本的なネットワーク構成
  - ネットワーク構成
- ネットワークのリスク
- ゾーニング計画
  - AUP (Acceptable Use Policy)
- 境界防御
  - ネットワーク境界の考え方
  - DMZ (DeMilitarized Zone)
  - ネットワークアクセスコントロール
  - ファイアウォール
- ネットワークの管理
  - SNMP (Simple Network Management Protocol)
  - VLAN (Virtual LAN)
- NAT・NAPT
  - NAT（Network Address Translation、アドレス変換）
  - ダイナミック NAT
  - スタティック NAT
  - NAPT (Network Address Port Translation)
- ファイアウォール
  - アクセス制御
  - パケットフィルタリング
  - スタティックパケットフィルタリング
  - ダイナミックパケットフィルタリング
  - ステートフルインスペクション（Stateful Inspection）
  - アプリケーションゲートウェイ(Proxy)
  - ファイアウォールの運用管理
- IDS（不正侵入検知システム）
  - ファイアウォールと IDS
  - 不正アクセス検出の仕組み、プロミスキャスモード
  - NIDS（ネットワークベース IDS）と HIDS（ホストベース IDS）
  - （他機能との併用）
  - ルータ、ファイアウォールでの遮断
  - RST パケットによるセッションの遮断
  - IDS の弱点と対策
- 無線 LAN のセキュリティ
  - 無線 LAN の方式（IEEE802.11a、IEEE802.11b、EEE802.11g、Bluetooth、インフラストラクチャモード、アドホックモード)
  - 無線 LAN に関する脅威
  - 認証・暗号化方式（SSID（Service Set ID）、MAC アドレス認証、WEP（Wired Equivalent Privacy）、EAP（Extensible Authentication Protocol）、EAP-MD5、LEAP（Light EAP）、EAP-TLS、TKIP、WPA、IEEE802.1x、IEEE802.11i)

技術	必修	Ｔ３	ＯＳセキュリティ

- Windows セキュリティ
- Windows の脆弱性
  - Null セッション接続
  - rootkit、リモート操作
  - パスワードクラック
- UNIX セキュリティ
- UNIX の脆弱性
  - Linux、Solaris 等のセキュリティホール
  - sendmail、FTP、BIND、等
- セキュア OS
- セキュアアプリケーション
- セキュリティ手法
  - ログ管理
  - パッチ適用管理
  - サービスの管理
  - ファイルシステムの管理
  - アカウント管理
- 不正アクセス対策
- 侵入テスト
- ログ解析
- セキュアシステム構築
  - サーバセキュリティ
  - セキュアサーバ構築技法

技術	必修	Ｔ４	アプリケーションセキュリティ

- 電子メールのセキュリティ
  - 電子メールの仕組み
  - 電子メールによるウイルス感染
  - 電子メールでの認証情報漏洩
  - 電子メール操作ミスによる情報漏洩
- Web のセキュリティ
  - 代表的 Web ブラウザのセキュリティ設定
  - ベーシック認証、証明書を用いた認証
  - ログの取得
  - 不要ファイルの削除
- Web アプリケーションのセキュリティ
  - HTTP プロトコル（HyperText Transfer Protocol）
  - 動的コンテンツによる OS 操作
  - クロスサイトスクリプティング
  - HTTP サービスでの情報漏洩

技術　必修　Ｔ５　認証・アクセス制御

- 認証の単位
  - ユーザ
  - ノード
  - プロセス
  - メッセージ
- 認証方式
  - パスワード
  - Challenge & Response
  - RADIUS
  - ActiveDirectory
  - Kerberos
  - ハードウェアトークン
  - OTP (One Time Password)
  - 生体認証
  - SSO (Single Sign-On)
  - デジタル証明書
- サーバアクセスコントロール
- データベースアクセスコントロール
- 物理的アクセスコントロール
- 機密度に応じたアクセス管理

技術　選択　Ｔ６　ネットワーク技術

- ネットワークの形態
- OSI (Open Systems Interconnection) 参照モデル
- ネットワークプロトコル
  - Ethernet, TokenRing
  - IP、TCP、UDP、ICMP
- ネットワーク機器
  - ルータ、ハブ、スイッチ、ケーブル
  - サブネット
  - VLAN (Virtual LAN)
- ネットワークにおける通信の仕組み
  - DNS (Domain Name System)
  - ARP (Address Resolution Protocol)
  - ルーティング、フォワーディング
- 一般サービスで利用されるプロトコル
  - TELNET、メール（SMTP:Simple Mail Transfer Protocol、POP:Post Office Protocol、IMAP: Internet Message Access Protocol）、FTP:File Transfer Protocol、HTTP、SMB: Server Message Block
- インターネットドメイン階層
- 電子メールの仕組み
- Web ブラウジングの仕組み

技術　　選択　　Ｔ７　　暗号技術

- 暗号の基礎知識
  - 暗号の仕組み
  - 乱数
- 共通鍵暗号
  - ストリーム暗号
  - ブロック暗号
  - 鍵長と安全性
- 公開鍵暗号
  - RSA 暗号方式
  - 公開鍵と秘密鍵
  - 公開鍵暗号の長所と短所
- 暗号解読
- ハッシュ関数
- デジタル署名
- 鍵管理

技術　　選択　　Ｔ８　　ＰＫＩ

- デジタル証明書
  - PKI とは
  - PKCS
  - デジタル証明書の役割
  - 公開鍵暗号方式と証明書
  - X.509
- 認証局（CA)、登録局（RA)、発行局（IA)
  - 構築と運用
  - パブリック CA
  - プライベート CA
- リポケーション系
- トラストモデル
  - 階層型
  - メッシュ型
  - ブリッジ型
- 鍵管理
  - 秘密鍵の管理
  - 署名鍵と暗号鍵の分離
- PKI 関連法規
- PKI 関連サービス
  - 時刻認証
  - 電子公証

表８　情報セキュリティ教育カリキュラムの詳細説明（マネジメント系）

区分	必修/選択	番号	大項目	中項目	キーワード
マネジメント	必修	Ｍ１	情報セキュリティマネジメント		
				ISMS	
					成熟度モデル
					PDCA サイクル
					情報セキュリティポリシの概要
					リスクアセスメントの概要
					情報セキュリティ監査
					普及と啓発
					教育
					情報収集
				物理的セキュリティ	
					物理セキュリティに関する具体的な対策紹介
				人的・組織的セキュリティ	
					組織構造におけるセキュリティ上の役割　（加えて実施責任者の業務やプロフェッショナリティに言及、例えばリーダシップ、動機付け、ＲＯＩ[7]、危機管理など）
					関係するサードパーティ
					責任の明確化
					証拠収集と証拠保全
					倫理規定、プロフェッショナリティ
					プライバシーポリシ
				最小特権の原則	
				職務分離、ローテーション	

[7] Return on Investment

マネジメント	必修	M２	情報セキュリティポリシ

情報セキュリティポリシとは
- 位置づけと必要性

情報セキュリティ組織（委員会）
情報セキュリティポリシの構成
情報セキュリティポリシの構築
情報セキュリティルール
情報セキュリティ方針の策定
- 方針のテンプレート
- 方針の策定方法
- 方針の承認手続き
- 方針の定期的な見直しと改定

企業活動一般のセキュリティ規定の作成
- 雇用契約／職務規程
- 機密／文書／情報管理規程
- プライバシーポリシ
- セキュリティ教育の規定
- 罰則の規定
- 対外説明の規定
- 例外の規定
- 規則更新の規定
- 規定の承認手続き

情報システムの情報セキュリティ規定の作成
- インターネット・イントラネット利用規定
- インターネット向け公開サーバの設置および管理規定
- 社内サーバ・FW/IDS およびクライアントの設置および管理規定
- リモートアクセス規定
- アプリケーションインストール規定
- 情報管理の規定
- コンピュータウイルス対策運用規定
- クライシスマネジメント（危機管理）の規定
- 情報セキュリティ監査・システム監査の規定
- 情報システム管理者の規定
- ネットワーク管理者の規定
- システム開発の規定
- 規定の承認・変手続き

マネジメント	必修	M３	リスクマネジメント

- リスクマネジメント方針
  - 全社的なリスクマネジメント体制
  - 経営者の関心
  - 経営理念、情報セキュリティポリシとの整合性
- リスクアセスメント
  - 情報資産の分類
  - 情報資産の評価
  - 機密度の設定
  - 脅威の洗い出しと評価
  - 脆弱性の洗い出しと評価
  - 想定される被害の評価
  - ベースラインアプローチ、非形式的アプローチ、詳細リスク分析、組合せアプローチ
  - リスク評価
- リスク対応
  - リスク保有
  - リスク回避
  - リスク移転
  - リスク低減
- リスク受容
- リスクコミュニケーション

マネジメント	必修	M４	クライシスマネジメント（危機管理）と事前準備

- 情報収集
  - CERT/CC, JPCERT/CC, IPA セキュリティセンター
  - 関係組織・マスメディア・通信事業者とのコミュニケーション
- エスカレーションポリシ
  - 予防策
  - 検知と初期対応
  - 被害の局所化（拡大防止）
  - 被害の撲滅
  - 復旧
  - 事後分析
- インシデント対応マニュアル
  - インシデント予防策
  - インシデントの分析（ハードウェアとソフトウェア）
  - インシデント分析のリソースリスト
  - インシデント対応ツール（セキュリティパッチ、OS のバックアップ等）
- 証拠収集と証拠保全
- 組織内のインシデントレスポンスチーム
- 災害時復旧計画、事業継続計画
- 事後報告
  - CERT/CC, JPCERT/CC, IPA セキュリティセンターへの連絡と報告
  - 関係組織・マスメディア・通信事業者への連絡と報告

マネジメント	必修	M５	法令と標準化

基準・指針・ガイドライン等

- 法的判断の構造論
- 情報システム安全対策基準
- コンピュータウイルス対策基準
- コンピュータ不正アクセス対策基準
- システム監査基準
- 情報セキュリティ監査基準類
- ソフトウェア管理ガイドライン
- 情報通信ネットワーク安全・信頼性基準
- 情報システム安全対策指針
- 行政情報システムの安全対策指針
- 情報セキュリティポリシーに関するガイドライン

法令

- 電子署名及び認証業務に関する法律
- 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律
- 不正アクセス行為の禁止等に関する法律
- 電子商取引に関する準則

- 商法（特に会社法の機関の部分）
- 商法（いわゆるＩＴ化の部分）
- 個人情報保護関連法・個人情報保護条例
- 著作権法
- 商標法
- 不正競争防止法
- 労働法
- 労働安全衛生法
- 刑法（いわゆるコンピュータ犯罪の部分）
- 刑事訴訟法・国税徴収法・弁護士法
- 民法
- 消費者契約法
- その他特定の業界に関する法律

国際標準規格

- ISO/IEC 15408（JIS X5070）
- ISO/IEC 17799（JIS X5080）
- ISO/IEC TR13335
- その他 ISO/IEC セキュリティ関連項目
- RFC セキュリティ関連項目
- IEEE セキュリティ関連項目
- ITU-T

国際ガイドライン

- OECD「情報システム及びネットワークのセキュリティのためのガイドライン」
- OECD「プライバシー保護と個人データの国際流通についてのガイドライン」
- OECD「暗号政策に関するガイドライン」
- 欧州連合「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」

欧州評議会「サイバー犯罪条約」

マネジメント	必修	M６	個人情報保護

- OECD８原則
- EU 指令
- 個人情報の保護に関する法律
- 自治体条例
- プライバシーポリシ
- コンプライアンスプログラム
  - JIS Q 15001
- 認定制度
  - プライバシーマーク、個人情報保護マーク

マネジメント	選択	M７	システム開発管理

- 製品調達・導入
- セキュリティ計画
- 設計段階におけるセキュリティ
  - PP (Protection Profile)、ST (Security Target)
- 開発・要員計画
- テスト工程におけるセキュリティ
- 運用段階でのセキュリティ
  - バックアップなど
  - バージョンアップにおけるセキュリティ
  - パッチマネジメント（脆弱性管理）
- 外部委託管理

マネジメント	選択	M８	情報管理 ＩＴ資産管理 知的財産権管理 著作権、ソフトウェアライセンス管理 営業機密管理 コンテンツ管理 電子すかし、フィンガープリンティング 倫理規定

マネジメント	選択	M９	教育・訓練 利用者への啓発および教育訓練計画 啓発教育 技術教育 継続的教育の効果 利用者教育 啓発教育 基本教育 高度セキュリティ教育 セキュリティ技術者教育 トレーニング 外部教育サービス 教育方法 e-learning、OJT 教育効果の測定

マネジメント	選択	M１０	監査 監査の種類 外部監査・内部監査 任意監査・法定監査 助言型監査・保証型監査 監査手順 監査手法 ネットワークスキャナ 監査計画書 監査報告書 監査制度 情報セキュリティ監査 システム監査

５．教育コース

５．１　検討の前提

前章で述べた教育カリキュラムに沿って、実際に教育を実施する場合を想定して、教育コースを設計した。なお、ここで設計した教育コースは、ベストプラクティスとしての推奨案であり、必ずしもこのコース通りの教育実施を要請するものではない。

教育コースの設計に際しては、想定受講者を分類する軸あるいは切り口（組織の規模、顧客個人情報の取扱い有無、アウトソースの程度など）、教育実施の際の期間と日数（数日、一週間、一ヶ月など）、教育実施の際の形態（座学、e-learning、演習など）といった視点から検討を実施した。

５．２　検討結果

想定受講者を分類する軸（切り口）については、下記に示す様々な属性をもとに、比較検討を実施した。

- 業種別（中堅製造業／小売業／大規模金融業、重要インフラ企業／それ以外）
- 企業規模別（大企業／中企業／小企業）
- ネットワークインフラ管理形態別（社内運用管理中心／アウトソース中心）
- 自社システムの開発実施の有無
- 顧客などの個人情報の取扱い有無
- 業務のネットワーク依存度（電子商取引等の活用度高／低、売上比率）
- 業務のＩＴ活用度（パソコン等設置台数と従業員数との比率、機器の多用度）
- 扱っている情報のリスク（情報漏洩時やシステム停止時のリスク多寡）
- 従業員の電子メールアカウント所有比率、等々

その結果、次の考え方に沿って整理することとした。

- 「企業の規模」については、求められる情報セキュリティ対策のレベルは、規模に依存する訳ではないという意見から軸としない。
- 「業務の IT 依存度」等いくつかの軸については、リスク算出のためのパラメータの一つと考えられることから、「リスク」という軸に統合する。
- 複雑さを避けるため、上記に基づき「ネットワークインフラ管理形態（自社管理／外部委託）」、「業種（開発／ユーザ）」、「リスクの多寡（高／低）」の三軸に統合する。ただし、「リスク」は、個人情報の取扱い有無、業務のネットワーク依存度やＩＴ活用度、社会的な影響度等を勘案して決定する。

また、教育実施の際の期間と日数については、理想的な教育を実施するために必要と思われる期間から、例えば企業に勤める実施責任者が実際に職場を離れて教育を受講できる現実的な期間まで、広いレンジが考えられる。ここでは、１日からおおよそ２週間までをメドとしてコースを設計することとした。

５．３　コース案

（1）コース案１

前節で示した三軸（「ネットワークインフラ管理形態（自社管理／外部委託）」、「業種（開発／ユーザ）」、「リスクの多寡（高／低）」）を勘案することで、企業等が自ら最適なコースを選択できるように設計した結果が、ここに示すコース案１である。

表９　コース選択の基本的な考え方

軸（切り口）			共通	技術		マネジメント		演習	コース
ネット インフラ	業種	リスク	必修	必修	選択	必修	選択		
自社管理	開発	高い	○	○	○	○	○	○	A
		低い	○	○	○	○			B
	ユーザ	高い	○	○		○	○		C
		低い	○	○		○			D
外部委託	開発	高い	○	○	○	○	○	○	A
		低い	○	○	○	○			B
	ユーザ	高い	○			○	○		E
		低い	○			○			F

例えば、ネットワークインフラを自社で管理しているユーザ企業で、かつリスクが高いと想定される場合には、次ページ以降に示すコースＣを、またネットワークインフラを外部委託しているユーザ企業で、かつリスクが低いと想定される場合にはコースＦを選択することを推奨している。

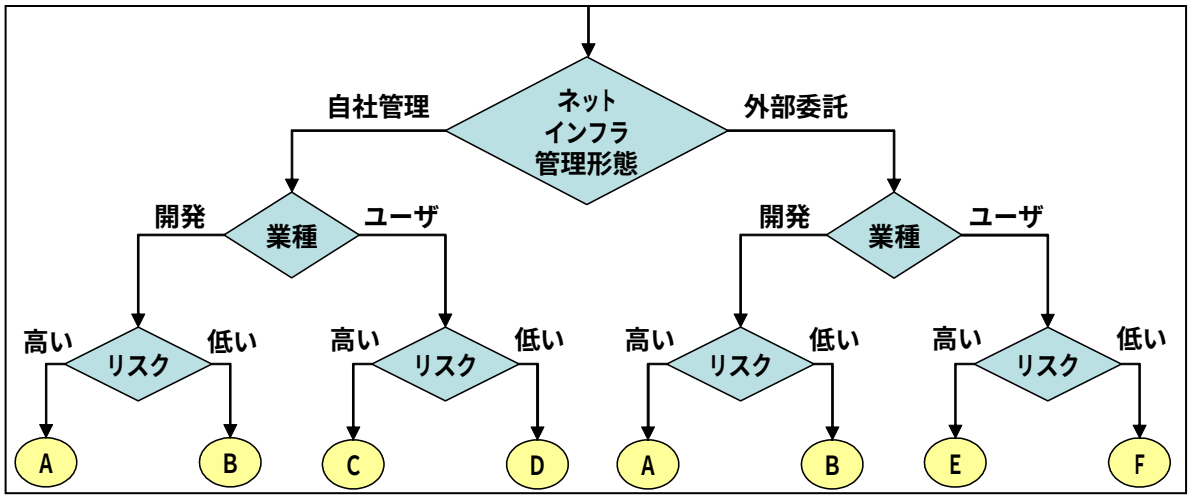

図７　コース選択のイメージ

例えば、コースＣを選択した場合には、共通系に加えて、技術系のＴ１～Ｔ５まで（必修の範囲）、マネジメント系のＭ１～Ｍ６（必修の範囲）までを受講することを推奨している。また、コースＦを選択した場合には、共通系に加えて、マネジメント系のＭ１～Ｍ６（必修の範囲）までを受講することを推奨している。コースＣの場合は約７日、コースＦの場合は約３日の期間を想定している。

表１０　コース案１における教育コースの詳細

	コースA	コースB	コースC	コースD	コースE	コースF
0.　情報セキュリティ概論	○	○	○	○	○	○
T1.セキュリティへの脅威	○	○	○	○		
T2.ネットワークセキュリティ	○	○	○	○		
T3.ＯＳセキュリティ	○	○	○	○		
T4.アプリケーションセキュリティ	○	○	○	○		
T5.認証・アクセス制御	○	○	○	○		
T6.ネットワーク技術	○	○				
T7.暗号技術	○	○				
T8.ＰＫＩ	○	○				
M1.情報セキュリティマネジメント	○	○	○	○	○	○
M2.情報セキュリティポリシ	○	○	○	○	○	○
M3.リスクアセスメント	○	○	○	○	○	○
M4.クライシスマネジメント（危機管理）と事前準備	○	○	○	○	○	○
M5.法令と標準化	○	○	○	○	○	○
M6.個人情報保護	○	○	○	○	○	○
M7.システム開発管理	○		○		○	
M8.情報管理	○		○		○	
M9.教育・訓練	○		○		○	
M10.監査	○		○		○	
演習	○					

←色付き枠は必修

(時間)

記号	１科目の時間	コースA	コースB	コースC	コースD	コースE	コースF
◎	5	0	0	0	0	0	0
○	3	20	15	16	12	11	7
△	1	0	0	0	0	0	0
×	0	0	0	0	0	0	0
合　計　時　間　数		60	45	48	36	33	21
		約８日	約６日	約７日	約５日	約５日	約３日

（２）コース案２

コース案２は、コース案１よりも、より現実的な設計を実施した結果である。即ち、受講期間を１０日、５日、３日、１日と予め設定し、その設定日数ごとに最適の組み合わせを検討するという設計方針のもとで検討した。下記において◎は５時間、○は３時間、△は１時間の教育時間を想定して設計されている。

表１１　コース案２における教育コースの詳細

	カテゴリーA	カテゴリーB	カテゴリーC	カテゴリーD
0.　情報セキュリティ概論	◎	◎	○	○
T1.セキュリティへの脅威	◎	○	○	△
T2.ネットワークセキュリティ	◎	○	○	△
T3.ＯＳセキュリティ	○	△	△	×
T4.アプリケーションセキュリティ	◎	○	△	×
T5.認証・アクセス制御	○	△	△	×
T6.ネットワーク技術	○	△	×	×
T7.暗号技術	○	×	×	×
T8.ＰＫＩ	○	×	×	×
M1.情報セキュリティマネジメント	◎	◎	○	○
M2.情報セキュリティポリシ	◎	○	△	×
M3.リスクアセスメント	◎	○	△	×
M4.クライシスマネジメント（危機管理）と事前準備	◎	○	△	×
M5.法令と標準化	○	△	△	×
M6.個人情報保護	○	△	△	×
M7.システム開発管理	○	△	×	×
M8.情報管理	○	△	×	×
M9.教育・訓練	○	△	×	×
M10.監査	○	△	△	×

(時間)

記号	１科目の時間	カテゴリーA	カテゴリーB	カテゴリーC	カテゴリーD
◎	5	8	2	0	0
○	3	11	6	4	2
△	1	0	9	9	2
×	0	0	2	6	15
合　計		73	37	21	8
		（約１０日）	（約５日）	（約３日）	（約１日）

（3）付加コース（製品・サービス紹介）

（1）（2）で紹介したコース案は、主に一般的、普遍的な知識や能力を付与することを目指したコースであるが、上記のコースに加えて、より実践的な知識や能力を付与するために、次に示すようなカテゴリーに属する具体的な製品やサービスを紹介する科目を加えることも効果的である。

■ 製品群
- ◇ ルータ
- ◇ ファイアウォール
- ◇ ウイルス対策ツール
- ◇ 脆弱性検査ツール（ホスト、ネットワーク、Web アプリケーション）
- ◇ 侵入検知（Intrusion Detection）システム（ホスト、ネットワーク）
- ◇ 侵入防止（Intrusion Prevention）システム
- ◇ コンテンツ・フィルタリング（メール、Web）
- ◇ SPAM フィルタ
- ◇ 認証システム（ＯＴＰ、ＩＣカード、バイオメトリクス、等）
- ◇ PKI 構築システム
- ◇ アイデンティティ・マネジメント
- ◇ ファイル、ディスク暗号化製品
- ◇ メール暗号化製品
- ◇ VPN（暗号通信）
- ◇ ログ解析ツール
- ◇ セキュリティ・アプライアンス製品
- ◇ 等

■ サービス群
- ◇ ペネトレーション・テスト、脆弱性検査サービス
- ◇ 情報セキュリティ監査サービス
- ◇ 情報セキュリティ教育サービス
- ◇ 運用監視サービス、マネージド・セキュリティ・サービス
- ◇ ＶＰＮサービス
- ◇ 脆弱性情報提供サービス
- ◇ 電子証明書発行サービス
- ◇ 電子公証サービス
- ◇ 保険
- ◇ 等

ただし、こうした具体的な商品やサービスの紹介は、極めて技術の流れが速く、陳腐化が激しいため、より定常的かつ頻繁なコース改訂が必要であることに留意されたい。

６．情報セキュリティ教育の新たな動向

情報セキュリティ教育に関連した新たな動きについて、次に紹介する。

（1）ＣＩＯ　Ｕｎｉｖｅｒｓｉｔｙ

概要

米国においては、米国連邦政府職員向けの IT 人材育成のために、CIO University という仮想の大学を開設している。主たる目的は、米国連邦政府の CIO 育成にあるが、民間にも門戸を開放し、学生の受け入れを行っている。

背景

米国の CIO カウンシルが資金を提供し、米国の ＧＳＡ（総務庁）が制度を運営している。実際には、既存の大学と協力して運営にあたっている。現在、制度に参加している大学は、カーネギーメロン大学、ジョージ・メイスン大学、ジョージ・ワシントン大学、メリーランド大学他の計７大学である。

教育内容

教育講座の内容は、1996 年に成立した Clinger Cohen Act に基づいて整備された、クリンガー・コーエン・コア・コンピタンスに準拠している。

同コンピタンスに基づいて、教育の内容を CIO Univ. Learning Objects として規定している。同 Learning Objects は、産学官からなる 100 名の専門家が策定した。このコースを終了すると、CIO カウンシルによる修了認定を受けることができる。

表１２　クリンガー・コーエン・コア・コンピタンスの構成

1.0	ポリシと組織
2.0	リーダーシップ／経営
3.0	プロセス／変更マネジメント
4.0	情報資源戦略と計画
5.0	パフォーマンス評価：モデルと手法
6.0	プロジェクト／プログラムマネジメント
7.0	資本計画と投資評価
8.0	調達
9.0	電子政府／e-ビジネス／電子商取引
10.0	ＩＴセキュリティ／情報保証
11.0	技術的事項
12.0	デスクトップ技術ツール

同コンピタンスでは、「１．０　ポリシと組織」および「１０．０　ＩＴセキュリティ／情報の保証」の２カ所において、セキュリティに関する教育内容を規定している。

教育コース

教育コースとしては、受講者の利便とニーズに合わせて、全コンピタンス・コース、一部のコンピタンス・コース、１週間の概略コース等が設定されている。

CMU[8]のプログラム概要

具体的な教育コースとして、CMU における教育コースを紹介する。

CMU には、CIO Certification Program（CIO Executive Certification）という教育プログラムがあり、その中のコース６ Information Assurance - Technical, Organizational, and Policy において、次の各項について教育を受けることができる。

- ◇ Federal Laws, Regulations, and Guidance
- ◇ Information Risk and Survivability for Executives
- ◇ Attack Methodologies and Predictive Analysis
- ◇ Hacking Exposed
- ◇ The Economic of Information Security
- ◇ Software, the Internet, and the Law

上記のコース６は、５日間かけて実施され、費用は米国政府職員ないし非営利団体の場合で 2500 米ドル、その他では 2950 米ドルである。

さらに CMU では、CIOI (Chief Information Officer Institute) という内部組織を設立し、SEI、CERT/CC、The H.J. Heinz School of Public Policy and Management などが協力体制を敷いている。

現在提供している CIO 向けプログラムとしては、情報セキュリティ以外にも下記のプログラムがある。

- ◇ Federal CIO Certificate Program
- ◇ Master ' s Certificate in IT Project Management
- ◇ Knowledge Management
- ◇ Responsible Information Management
- ◇ MSIT Executive Distance

CIOI の活動を紹介している Web ページは、次の通りである。

URL: http://cioi.web.cmu.edu/

[8] Carnegie Mellon University

（2）Global Council of CSOs

目的

Global Council of CSOs は、オンライン・セキュリティに関する問題の注意喚起に熱心な、有力企業、政府、学会のセキュリティ専門家グループで構成されたシンクタンクである。同カウンシルは、企業、国家のセキュリティ、将来の技術開発に対してCSO[9]が何をなすべきかという役割を明らかにすることに焦点をあてて設立された組織である。

設立メンバー（10 名）

下記の蒼々たるメンバーが名を連ねている。

- ◇ Howard A Schmidt (eBay)
- ◇ Bill Boni (Motorola)
- ◇ Vint Cerf (MCI)
- ◇ Scott Charney (Microsoft)
- ◇ Dave Cullinane (Washington Mutual)
- ◇ Mary Ann Davidson (Oracle)
- ◇ Whitfield Diffie (Sun Microsystems)
- ◇ Steve Katz (formerly of Citigroup)
- ◇ Rhonda MacLean (Bank of America)
- ◇ Will Pelgrin (New York State Office of Cyber Security and Critical Infrastructure)

活動概要

CMU が新たに設置した CyLab が、カウンシルの事務局を担当する。また、同カウンシルは、最初のステップとして、次の５つの目標についてリーダーシップを果たすことを目指している。

- ◇ 常に変わる環境の中で、技術的な問題ではなくビジネス上の問題に焦点をあてて、オンライン・セキュリティ問題に取り組むために CSO の力を糾合する。
- ◇ 企業組織内での CSO の適切な役割、背景などを定義する。
- ◇ 米国の国家戦略である "The National Strategy to Secure Cyberspace" を実現するための CSO の役割を定義する。
- ◇ サイバーセキュリティ問題について、CSO が政府と話し合う適切な時期と手段を定義する。
- ◇ セキュリティに関してどのようなビジネス上のニーズがあるかを定義したり、リスクを最小化するためにどのような技術を使用することができるかについて助言を得るために、技術ベンダーと率直かつ定期的な話し合いを実現する。

Global Council of CSOs の活動を紹介している Web ページは、次の通りである。

URL: http://www.csocouncil.org/

[9] Chief Security Officer、セキュリティ担当役員

（3）CISO Executive Membership

目的

企業の CISO とセキュリティ専門家のコネクションを提供することを目的として、NPO である ISSA が提供しているサービス（プログラム）である。

背景

米国NPOのISSA[10]内に設置されている。ISSAは、ITセキュリティ専門家の職能団体であり、CISSPに合格するとISSAに加入するという流れが典型的である。

活動概要

メンバーシップの参加者に対して、次のサービスを提供する。

- ◇ 個別に用意したオンライン情報へのアクセス
- ◇ オンラインフォーラムやイベントを通じた意見交換（メンバー限定）
- ◇ CISO Executive Membership conferences への参加
- ◇ 業界のトップ専門家による教育セミナーやオンライン相談
- ◇ 関連法令の理解と提言
- ◇ あらゆる業界のベンダーに対する統一的なメッセージ提供

スポンサー

同メンバーシップのスポンサーには、CISCO、fortinet、ISS、PGP、PriceWaterhouseCoopers、Symantec といった企業が名を連ねている。

CISO Executive の活動を紹介している Web ページは、次の通りである。

URL: http://ciso.issa.org/

[10] Information Systems Security Association

７．提言

７．１　骨子

2003 年 10 月、経済産業省から「情報セキュリティ総合戦略」が発表された。これは我が国の情報セキュリティ対策に関して、これまでの守りを主とした対処療法的な対策を見直し、我が国の強みを活かしながら世界最高水準の高信頼性社会を実現し、もって経済的競争力強化や総合的な安全保障の向上を目指すものである。この中で情報セキュリティ人材の育成については重要な項目として掲げられていると同時に、その取り組みは遅れているという指摘がなされている。

近年情報システムは、生活や事業活動基盤として必要不可欠な存在として浸透した。しかしながらこのネットワーク社会の大部分を占める利用者にとっては、急速な技術革新の結果、あまりにも多様かつ複雑なものになってしまった。企業などの組織体が事業を行うにあたり、情報システムを利用することは現在必要不可欠なわけであるが、全ての組織体の管理者・利用者が自らの情報システムの構造や安全な運用について理解し、対策を実施するのは困難な状況といえる。これまで原則として自己責任の下で費用対効果に見合ったセキュリティ対策を講じてきたが、情報セキュリティを巡るリスクが拡大・変質し、個々の企業や組織に生じる事件や事故が自身への影響だけでなく経済活動全体の停滞や国民全体の生命・財産に関わるリスクをもたらしかねない状況では、その対策のあり方を見直さなければならない。

とりわけ利用者側の対策で重要なのは、情報セキュリティ対策を講じるための知識・スキルの習得、セキュリティリテラシーの向上を目指す情報セキュリティ教育である。なぜならたとえ技術的に強固な情報システムを構築したとしても、その運用・管理の段階で人的要因により障害や事故が発生してしまうためである。新たなコンピュータウイルスや新たな手法のサイバー攻撃による事件も増加しているが、情報システム関連事故（IT 事故）は、こうした運用ミスや内部犯罪などの内部要因が多くの割合を占めており、それを未然に防ぐためにも情報セキュリティ教育の充実が喫緊の課題である。

情報セキュリティ教育をもって効率的に情報セキュリティレベルの向上を図るためには、実質的に情報セキュリティ対策の中心的役割を担う責任者（実施責任者）に明確な責任と権限を与え、情報システムの管理体制やリスクに応じた教育をすることが最も重要である。またこれにとどまることなく、その責任者を支える経営層や組織内エンドユーザのリテラシーを向上させていく必要がある。しかしながらリスクが変容し、拡大する今日、そうした人材の育成を個々の組織が組織内研修などによって行っていくには限界がある。有効な情報セキュリティ教育を実施するためには各方面が積極的に関与し、協調すべきであるが、まだ緒についたばかりで十分な取り組みがなされていない。

このため経済産業省によって設置された「情報セキュリティ教育研究会」では、民間の有識者とともに組織内の実質的な責任者を対象とした情報セキュリティ教育の内容、手法について検討してきた。研究会では組織の規模やリスクに応じた幾つかの教育コースを提案したが、これらが各方面で活用されることを期待している。情報システムのユーザ組織には必要な教育の導入を検討・実施する際に参照し、教育事業者にはカリキュラム構築や教材開発の際に参照さ

れることを期待している。そして政府や行政機関にはそうした取り組みを支援するため、業界団体やコミュニティと連携をとりつつ施策を講じていくことが求められる。経済産業省自身にも本カリキュラムに基づいた研修・セミナーの企画や、現行の試験制度の見直しを含めて、率先して情報セキュリティ教育の促進に貢献されたい。

　また研究会では利用者自身や教育事業者、政府、そして情報社会に参加する者全体に対して、それぞれに期待する役割や必要な方策について積極的な議論を行った。立場を越えた広い見地からの意見をいただいた結果、政府及びネットワークに参加する組織に対する５つの提言の骨子がまとめられた。先の情報セキュリティ教育カリキュラムの活用とともに、提言にある事項を踏まえて今後の情報セキュリティ教育に関する取り組みが実施されることが期待される。

（１）組織の責任者（経営層）への注意喚起
（２）情報セキュリティ教育の推進主体の設立
（３）情報セキュリティ教育の振興と研修の実施
（４）情報セキュリティ教育の普及・啓発の促進
（５）情報セキュリティに関連するスキル維持のあり方の検討

以下に提言骨子に係る詳細を記す。

７．２　各論

（１）　組織の責任者（経営層）への注意喚起

◆すべての組織の責任者は、情報セキュリティ教育の重要性を再認識し、
自ら主体的に情報セキュリティ実現のための行動を起こすこと。

研究会からすべてのネットワーク参加組織への提言

ネットワークに参加するすべての組織の責任者は、情報セキュリティの実現に果たす自らの役割を自覚すると共に、実現のために重要な要素の一つである情報セキュリティ教育の重要性を再認識し、自ら主体的に行動を起こすこと。左記、提言する。

上記実現のために、本研究会での検討結果（教育カリキュラム、教育コース等）を活用すること、あるいは本教育コースに準拠した教育コースへの参加を推奨する。

さらに、次項以降で述べる各提言について、自ら積極的に参加し、実現に向けて自らの役割を果たすことを推奨する。

（2）情報セキュリティ教育の推進主体の設立

◆情報セキュリティ関連技術等の進歩に合わせて、常に最適な教育のあり方を検討・整備するために必要な体制を整備すること。

また、ユーザ企業が自ら積極的に教育を推進するために、そうした主体的な行動を支援する枠組みを整備すること。

研究会から経済産業省への提言

経済産業省は、本研究会の活動成果である教育カリキュラム等を、情報セキュリティ関連技術の進歩に合わせ、陳腐化を避けるために、また常に最適な教育のあり方を検討・維持するために、必要な組織体制の整備を支援すること。左記、提言する。

併せて、ユーザ企業が自ら積極的に情報セキュリティ教育を推進するために、そうした行動を支援するための枠組みを検討し、上記の組織体制等を通じて支援すること。左記、提言する。

上記実現のために、例えば、ユーザ企業の経営層、有識者（例えば情報セキュリティ対策に積極的な経営層 10 名）等を主体としたコミュニティを３年以内に設立するなど、体制整備を推進することを推奨する。

研究会からユーザ企業等の組織の責任者、有識者への提言

上述した組織体制を通じて、自らが利用する教育カリキュラムや教育コースを改訂し、常に最新の状態に維持し、有用性を担保すること、さらに教材や指導要領の整備を推進することを推奨する。

加えて、そうした組織体制等を通じて、ユーザ企業の責任者自らが、情報セキュリティのさらなる向上に積極的に関与すること、ユーザ企業や有識者等から、サプライヤ・社会・政府等へ向けた積極的な提言や問題提起を実施すること、またカンファレンス等の場を通じて参加者同士が意識の共有と情報の交換を実現することを推奨する。

（3）情報セキュリティ教育の振興と研修の実施

◆情報セキュリティ教育の重要性を訴え、認識を広めるため、一般ユーザ企業を主たる対象とした普及・啓発活動を広範囲に実施すること。

研究会から経済産業省への提言

経済産業省は、情報セキュリティ教育の重要性をユーザ企業に直接訴え、その認識を広め、教育への投資を促し、またそれらを通じたリテラシーの向上と情報セキュリティ対策の向上を促進すること。左記、提言する。

上記のために、例えば地域のユーザ団体などと協力し、研修などの普及・啓発活動を行うこと。地域のユーザ団体と協力しながら、また受講者の負担を減らしながら、より多くの一般ユーザ組織担当者の受講が可能となるような工夫をする必要がある。

研修内容の検討に際しては、本研究会での検討結果である教育カリキュラムを参照すること。この場合、民間のセキュリティ教育事業者の提供する内容との重複は避け、役割分担を明確にするとともに、教育市場を活性化し、更には情報セキュリティ対策を促進していく工夫が必要である。

研究会からユーザ団体等への提言

団体に加盟している組織等に対して、情報セキュリティに関する普及・啓発活動への積極的な参加を促すこと、あるいは加盟組織による主体的な情報セキュリティ教育の実施を促すことを推奨する。

（4）情報セキュリティ教育の普及・啓発の促進

◆情報セキュリティ教育の普及を促進するために、情報セキュリティ教育事業の高度化や教育内容の充実を図るなど、普及促進策を実施すること。

研究会から経済産業省への提言

経済産業省は、情報セキュリティ教育の普及を促進するために、例えば情報セキュリティ教育事業のより一層の高度化や教育内容の充実を図るといった活動を通じた普及促進策を検討し、早急に実施すること。左記、提言する。

上記実現のため、情報セキュリティ教育に関するシンポジウムの定期開催（年１回以上）、各種教育コース紹介用のポータルサイトの１年以内の開設・運用等の活動を通じて、ユーザが教育コースを選択する際の利便を図ることを推奨する。

ポータルサイトの例：http://csrc.nist.gov/ATE/

これら活動は、前述した組織体制、あるいは NPO、あるいは大学等を中心に実施することとし、それら活動を支援する立場が望ましい。

また、本研究会における検討結果（教育カリキュラムや教育コース等）への準拠を教育実施者に推奨すること、あるいは教育コースの認定等の実施を検討することを推奨する。その実現のため、認定主体の設置を検討し、３年以内に認定を開始することを推奨する。

研究会から高等研究機関、教育事業者等への提言

高等教育機関、教育事業者等は、本研究会の検討結果に準拠した教育コースを開設すること、またユーザ企業等に向けた教育事業を積極的に展開することを推奨する。また、教育コース等の認定制度が創設された場合には、それらを積極的に活用することを推奨する。

（5）情報セキュリティに関連するスキル維持のあり方の検討

◆情報セキュリティに関連する各種の試験体系を見直し、必要に応じて情報処理技術者試験制度における試験の新設や改訂、また民間資格試験制度の活用等の方策を検討すること。

研究会から経済産業省への提言

経済産業省は、社会全体の情報セキュリティのリテラシーを高めるため、また担当者の評価を高めてこれを育成するために、情報セキュリティに関連する各種の試験体系の見直しに３年以内に着手すること。左記、提言する。

現在ある不特定事業者向けの情報セキュリティ関連公的試験は「情報セキュリティアドミニストレータ試験」のみであるが、唯一であるがために当該試験が想定する人材及びそれを目指す者以外にも多くが受験しており、評価が確立されていない。

試験の評価及び合格者の組織内での評価を高めるためにも、またそれを目指す者に対して参入を促し、その目標となり、スキルアップ、キャリアアップの指標となるためにも、我が国で不足している試験区分の新設及び改訂による対応を検討する必要がある。ただし民間の非営利団体などが試験を行う場合は、これらとの関係を整理し、場合によってはその振興によって対応することも検討すべきである。

また試験制度に求められる重要な論点として、知識及びスキルの水準維持、最新動向への適応を促すための方策の必要性が言われている。民間試験や非営利組織の試験制度の一部ではこのため更新試験が行われているものもあるが、技術的にも制度的にも急速に変化している情報セキュリティをとりまく環境を考えると、その必要性は高い。

付録）情報セキュリティ教育カリキュラムの設計試案

４．２　教育カリキュラムの体系で述べた教育カリキュラムの各項目に対して説明を加え、実際の教育コースやテキストを開発する際の参考になるような情報を付記した上で、この付録にまとめる。

区分	共通系
必修／選択	必修
番号	0
大項目（科目）名	情報セキュリティ概論
目標	情報セキュリティの基本的な概念について学ぶ。また、以後の各科目を理解するために必要最低限の基礎知識を習得する。
養うべき能力	企業や組織において情報セキュリティを実現するために必要最低限の知識と能力を習得する。
内容	情報セキュリティの必要性・重要性を理解させること。また、保護すべき対象としての情報資産の把握が必須であること、リスクを情報資産ごとに把握するための基本的な考え方、情報セキュリティ対策実現にはＩＴ技術だけではなく様々な側面が必要であること等を理解させること。
キーワード	コンプライアンス経営概論 情報セキュリティと情報セキュリティ対策 情報セキュリティマネジメントの目的、費用対効果、説明責任 情報資産の分類、機密度の設定 機密性、完全性、可用性 脆弱性、脅威 予防、検出、対処 技術的対応と管理・運用的対応
対応する中項目	情報セキュリティの必要性 情報資産 情報資産の重要性 リスクの考え方 情報セキュリティ対策の側面
教授法の例	講義、e-learning
教科書	【今後の要整備事項】
参考文献など	■土居範久監修、佐々木良一他編: 情報セキュリティ事典、共立出版、2003.7.10 ■セキュリティハンドブックⅠ 情報化とリスクマネジメント、日本セキュリティマネジメント学会編、日科技連、1998/3 ■セキュリティハンドブックⅡ 情報セキュリティとシステム監査、日本セキュリティマネジメント学会編、日科技連、1998/3 ■セキュリティハンドブックⅢ 情報資産の保護と情報倫理、日本セキュリティマネジメント学会編、日科技連、1998/3

区分	技術系
必修／選択	必修
番号	Ｔ１
大項目（科目）名	セキュリティへの脅威
目標	情報セキュリティを脅かす様々な脅威に関して、どのような種類があるのか、またどのような経路や手段などが用いられるのかを理解する。
養うべき能力	情報セキュリティにまつわる様々な脅威を把握することができる能力を養成する。具体的には、インターネット、社内ネットワーク、モバイル、物理的環境、ソーシャルエンジニアリング攻撃等のさまざまな側面における脅威を感じ取る能力を養成する。
内容	インターネット上で想定される脅威、社内ネットワーク上で想定される脅威、モバイル環境下における脅威、物理的環境に依存する脅威等について、攻撃手法の習得にならない範囲で、できるだけ具体的に脅威の内容を習得させる。
キーワード	サービス妨害攻撃 盗聴、改ざん、情報漏洩 不正侵入 踏み台 メール爆弾 媒体盗難、紛失 論理爆弾 メールの転送 バックドア 誤操作による情報漏えい ソーシャルエンジニアリング 災害 破壊、妨害行為 感染先による分類 隠蔽手法による分類 ウイルスが利用する技術による分類 ウイルスの活動による分類 デマウイルス 二重発注 ユーザなりすまし 否認 名誉毀損 サイバースクワッティング spam
対応する中項目	ネットワークからの脅威 組織内環境での脅威 物理的脅威 コンピュータウイルス、ワーム、マルウェアによる脅威 電子商取引とコミュニケーション上での脅威

	モバイル環境における脅威
教授法の例	講義、e-learning、実習（ネットワーク攻撃手法の再現など）
教科書	【今後の要整備事項】
参考文献など	■シムソン ガーフィンケル他：UNIX&インターネットセキュリティ、 オライリー・ジャパン、1998/12 ■Anonymous：クラッキング対策ファイナルガイド、翔泳社、1999

区分	技術系
必修／選択	必修
番号	Ｔ２
大項目（科目）名	ネットワークセキュリティ
目標	ネットワークを構築・運用する際に利用可能なセキュリティ技術について概観を与え、基礎的な知識を習得する。
養うべき能力	社内ネットワーク構築等において、セキュリティ対策上留意すべき事項を理解できること。自組織内のネットワークの設計や構築に際して、担当者やアウトソース先に対して、情報セキュリティの観点から必要となる事項を指示できること。
内容	ネットワークを構築・運用する際に想定されるリスクを理解させる。また、情報セキュリティに配慮したネットワークアーキテクチャの基本的な考え方を習得させると共に、個々のネットワーク接続機器類の基本的な動作を理解させ、設定に際して留意すべきポイントを習得する。
キーワード	ネットワーク構成 AUP (Acceptable Use Policy) ネットワーク境界の考え方 DMZ (DeMilitarized Zone) ネットワークアクセスコントロール ファイアウォール SNMP (Simple Network Management Protocol) VLAN (Virtual LAN) NAT（Network Address Translation、アドレス変換） ダイナミック NAT スタティック NAT NAPT (Network Address Port Translation) アクセス制御 パケットフィルタリング スタティックパケットフィルタリング ダイナミックパケットフィルタリング ステートフルインスペクション（Stateful Inspection） アプリケーションゲートウェイ(Proxy) ファイアウォールの運用管理 ファイアウォールと IDS 不正アクセス検出の仕組み、プロミスキャスモード NIDS（ネットワークベース IDS）と HIDS（ホストベース IDS） ルータ、ファイアウォールでの遮断 RST パケットによるセッションの遮断 IDS の弱点と対策 無線 LAN の方式 (IEEE802.11a、IEEE802.11b、EEE802.11g、Bluetooth、インフラストラクチャモード、アドホックモード) 無線 LAN に関する脅威 認証・暗号化方式 (SSID（Service Set ID)、MAC アドレス認証、WEP

	（Wired Equivalent Privacy）、EAP（Extensible Authentication Protocol）、EAP-MD5、LEAP（Light EAP）、EAP-TLS、TKIP、WPA、IEEE802.1x、IEEE802.11i）
対応する中項目	基本的なネットワーク構成 ネットワークのリスク ゾーニング計画 境界防御 ネットワークの管理 NAT・NAPT ファイアウォール IDS（不正侵入検知システム） 無線 LAN のセキュリティ
教授法の例	講義、e-learning、実習（ファイアウォール、侵入検知システム等の操作、ログの分析等）
教科書	【今後の要整備事項】
参考文献など	■クレイグ ハント他：TCP/IP ネットワーク管理、オライリージャパン、2003/06 ■エリザベス・D. ツビッキー他：ファイアウォール構築〈VOLUME1〉―理論と実践、オライリージャパン、2002/12 ■エリザベス・D. ツビッキー他：ファイアウォール構築〈VOLUME2〉―インターネットサービス、オライリージャパン、2003/01 ■マシュー・S. ガスト他：802.11 無線ネットワーク管理、オライリージャパン、2003/09 ■Bruce Potter 他：802.11 セキュリティ、オライリー・ジャパン、2003/05/26

区分	技術系
必修／選択	必修
番号	Ｔ３
大項目（科目）名	ＯＳセキュリティ
目標	個々のコンピュータ、特にＯＳに関連して、コンピュータを守るために利用可能なセキュリティ技術について概観を与え、基礎的な知識を習得する。
養うべき能力	代表的なオペレーティングシステムについて、固有の脆弱性について理解し、それら脆弱性からシステムを防御するための基本的な方策を実施できること。
内容	代表的なオペレーティングシステムに存在する固有の脆弱性を理解させる。その上で、それら脆弱性からシステムを防御するための手法、安全なシステムの構築方法（要塞化の手法）を習得させる。さらにより高度なセキュリティを実現するため、セキュアＯＳの仕組みを理解し、また侵入テストやログ解析の手法を理解する。
キーワード	Null セッション接続 rootkit、リモート操作 パスワードクラック Linux、Solaris 等のセキュリティホール sendmail、FTP、BIND、等 ログ管理 パッチ適用管理 サービスの管理 ファイルシステムの管理 アカウント管理 サーバセキュリティ セキュアサーバ構築技法
対応する中項目	Windows セキュリティ Windows の脆弱性 UNIX セキュリティ UNIX の脆弱性 セキュア OS セキュアアプリケーション セキュリティ手法 不正アクセス対策 侵入テスト ログ解析 セキュアシステム構築
教授法の例	講義、e-learning、実習（OS の各種設定、ログの分析等）
教科書	【今後の要整備事項】
参考文献など	■アイリーン フリッシュ他: UNIX システム管理〈VOLUME 1〉、 オライリージャパン、2003/07 ■アイリーン フリッシュ他: UNIX システム管理〈VOLUME 2〉、

	オライリージャパン、2003/08 ■マイケル・D. バウアー他: Linux サーバセキュリティ、、オライリージャパン、2003/10 ■ステファン ノーバーグ他：WindowsNT/2000 Server インターネットセキュリティ、オライリー・ジャパン、2001/06 ■SANS Institute: Securing Securing Linux Step by Step Ver1.0J NRI セキュアテクノロジーズ ■SANS Institute: Solaris Security Step by Step Ver2.0J NRI セキュアテクノロジーズ ■SANS Institute: Securing Windows 2000 Step by Step Ver1.5J NRI セキュアテクノロジーズ ■渡辺 勝弘･伊原 秀明:不正アクセス調査ガイド―rootkit の検出と TCT の使い方、オライリー・ジャパン、2002/04

区分	技術系
必修／選択	必修
番号	Ｔ４
大項目（科目）名	アプリケーションセキュリティ
目標	Web ブラウザ、電子メールソフト等を中心とするクライアントアプリケーションおよび Web サーバの動的コンテンツ等のサーバアプリケーション、ミドルウェアに関して、利用可能なセキュリティ技術について概観を与え、基礎的な知識を習得する。
養うべき能力	代表的なインターネットアプリケーションについて、それぞれに固有の脆弱性を理解した上で、それらを回避するための手段を実施できること。
内容	Web ブラウザ、電子メールを中心とするインターネットアプリケーション、Web サーバの動的コンテンツやミドルウェアについて、それらに存在する固有の脆弱性を理解させる。その上で、それら脆弱性を回避し、利用者の安全を確保するために必要な措置を習得する。 特に、無線ＬＡＮ利用時のセキュリティ対策については詳述する。
キーワード	電子メールのセキュリティ 　電子メールの仕組み 　電子メールによるウイルス感染 　電子メールでの認証情報漏洩 　電子メール操作ミスによる情報漏洩 　S/MIME、PGP WEB のセキュリティ 　受動的攻撃 　代表的 WEB ブラウザのセキュリティ設定 　ベーシック認証、証明書を用いた認証 　IP アドレスによるアクセス制限 　ディレクトリリスティング 　ログの取得 　不要ファイル（サンプルプログラム、旧バージョンの CGI プログラム等）の削除 　デフォルトバナーの削除 WEB アプリケーションのセキュリティ 　HTTP プロトコル（HyperText Transfer Protocol） 　クロスサイトスクリプティング脆弱性 　OS コマンドインジェクション、SQL インジェクション 　ユーザ入力値の検証（サニタイジング） 　GET メソッド、POST メソッドのセキュリティ 　Cookie とセキュアモード 　安全なセッション管理方式 　過度のメッセージ出力の抑制 　hidden フィールド、HTTP_REFERER
対応する中項	電子メールのセキュリティ

目	Web のセキュリティ Web アプリケーションのセキュリティ
教授法の例	講義、e-learning、実習（アプリケーションの各種設定、ログの分析等）
教科書	【今後の要整備事項】
参考文献など	■セキュアな Web サーバーの構築と運用、(独)情報処理推進機構、 http://www.ipa.go.jp/security/awareness/administrator/secure-web/ ■電子メールのセキュリティ、(独)情報処理推進機構、 http://www.ipa.go.jp/security/fy12/contents/smime/email_sec.html ■シムソン ガーフィンケル他：Web セキュリティ、プライバシー&コマース 上 ユーザー編、オライリージャパン、2002/12 ■シムソン ガーフィンケル他：Web セキュリティ、プライバシー&コマース 下 第 2 版 システム管理者・コンテンツ提供者編、オライリージャパン、2002/12

区分	技術系
必修／選択	必修
番号	Ｔ５
大項目（科目）名	認証・アクセス制御
目標	情報セキュリティを維持するために重要な要素技術の一つである識別、認証、アクセス制御（３Ａ）について、基礎的な知識を習得する。
養うべき能力	認証・アクセス制御の基礎的な知識を習得した上で、その考え方を様々な具体的場面において応用できること。
内容	認証・アクセス制御（特に３Ａ）に関連する基礎的な知識を習得させる。それらをネットワークアクセス、サーバアクセス、データベースアクセス、物理的アクセスといった場面において、具体的に活用するための手法について習得させる。
キーワード	認証の単位 　人、ノード、プロセス、メッセージ 認証方式 　パスワード 　　パスワードの長さと危険性 　　ブルートフォース攻撃 　　辞書攻撃 　　類推攻撃 　　ショルダーハッキング 　　安全なパスワード 　　shadow password 　　パスワードファイルのパーミッション設定 　Challenge&Response 　デジタル証明書 　ハードウェアトークン 　　ＩＣカード 　　ＵＳＢトークン 　ワンタイムパスワード 　生体認証 　　指紋、虹彩、静脈、顔面 　ＩＰアドレスによる認証 　ＩＰスプーフィング 　チェックサム 　ハッシュ 　デジタル署名 　認証サーバ、プロトコルＰＡＰ、ＣＨＡＰ 　RADIUS 　ActiveDirectory 　Kerberos 　シングルサインオン 　ディレクトリサービス、LDAP、Ｘ．５００

	サーバアクセスコントロール 　ログインプロセス 　TCPwrapper, xinetd データベースアクセスコントロール 　デフォルトアカウント、デフォルトパスワードの危険性 　パスワードファイルのパーミッション設定 物理的アクセスコントロール 　フロアゾーニング 　入退館、入退室管理 　マントラップドア、アンチパスバック 　監視カメラ
対応する中項目	認証の単位 認証方式 サーバアクセスコントロール データベースアクセスコントロール 物理的アクセスコントロール 機密度に応じたアクセス管理
教授法の例	講義、e-learning、実習（各種認証方式の実機操作等）
教科書	【今後の要整備事項】
参考文献など	■S. Garfinkel, G. Spafford: UNIX＆インターネットセキュリティ, 　オーム社 ■瀬戸洋一: サイバーセキュリティにおける生体認証技術、共立出版

区分	技術系
必修／選択	選択
番号	Ｔ６
大項目（科目）名	ネットワーク技術
目標	ネットワークセキュリティを深く理解するために本来必要なネットワーク技術について、全体像を概観し、基礎的な知識を習得する。
養うべき能力	特に自組織内でネットワークを構築し運用する際に、情報セキュリティ管理者として必要な知識を習得し、それに基づいてネットワーク設計者や運用管理者に対して、情報セキュリティ上の留意点等を指示できること。
内容	OSI のプロトコル７階層､IP のプロトコル 4 階層などの基礎的なネットワーク技術を習得する。それらの実際の応用としての、LAN、WAN、インターネットなどの仕組みを理解する。また、それらネットワーク上で動作するアプリケーションの仕組みについて理解する。
キーワード	ネットワークの形態 　インターネット、ＬＡＮ、WAN、無線ＬＡＮ、ダイアルアップ接続 　ベースバンド通信とブロードバンド通信 OSI 参照モデル ネットワークプロトコル 　Ethernet, IEEE802.3,TokenRing(IEEE802.5)、100Base-T 　Netware、NetBIOS、ＸＮＳ，AppleTalk、DECnet 　コネクション型プロトコル、コネクションレス型プロトコル 　IP、TCP、UDP、ICMP 　MAC アドレス、IP アドレス、ドメイン 　ポート番号、Well-known ポート ネットワーク機器 　ルータ、ＨＵＢ、スイッチ、ケーブル 　プロキシ 　サブネット 　VLAN 　認証 VLAN ネットワークにおける通信の仕組み 　ルーティング、フォワーディング 　ルーティングプロトコル（RIP, OSPF, BGP, EGP, IGP） 　ＡＲＰ、ＲＡＲＰ 　名前解決（ＤＮＳ） システム管理用プロトコル 　NTP、SNMP、SYSLOG、ICMP、DHCP 一般サービスで利用されるプロトコル 　TELNET、FTP、HTTP、SMB、NNTP セキュア・プロトコル 　IPv6 　SSH 　IPSec

	SSL／HTTTPS s-HTTP その他 SoftEther インターネットドメイン階層 電子メールの仕組み SMTP、POP、IMAP、APOP RFC８２１、RFC822 MTA（Sendmail 他），MUA、MDA オープンメールリレーの危険性 WEB ブラウジングの仕組み
対応する中項目	ネットワークの形態 OSI (Open Systems Interconnection) 参照モデル ネットワークプロトコル ネットワーク機器 ネットワークにおける通信の仕組み 一般サービスで利用されるプロトコル インターネットドメイン階層 電子メールの仕組み Web ブラウジングの仕組み
教授法の例	講義、e-learning、実習（ネットワーク設定操作と動作の理解）
教科書	【今後の要整備事項】
参考文献など	■Comer, Douglas E.; TCP/IP によるネットワーク構築（Vol.1）原理・プロトコル・アーキテクチャ、共立出版 ■小林浩・江崎浩: インターネット総論、共立出版

区分	技術系
必修／選択	選択
番号	Ｔ７
大項目（科目）名	暗号技術
目標	共通鍵暗号、公開鍵暗号、ハッシュ関数、デジタル署名、鍵管理といった暗号技術の基礎的な知識を与え、主に暗号技術の利用方法について習得する。
養うべき能力	暗号技術の基礎的な仕組みを理解でき、暗号技術を利用した各種のアプリケーション等を適切に利用できること。
内容	共通鍵暗号の仕組み、公開鍵暗号の仕組み、両者の違いを理解する。また、ハッシュ関数の役割とデジタル署名との関係について理解する。さらに鍵管理の重要性とその手法例について習得する。
キーワード	暗号の仕組み、乱数 ストリーム暗号、ブロック暗号、鍵長と安全性 RSA 暗号方式、公開鍵と秘密鍵、公開鍵暗号の長所と短所
対応する中項目	暗号の基礎知識 共通鍵暗号 公開鍵暗号 暗号解読 ハッシュ関数 デジタル署名 鍵管理
教授法の例	講義、e-learning、実習（暗号アプリケーションの設定と操作等）
教科書	【今後の要整備事項】
参考文献など	■ブルース・シュナイアー: 暗号技術大全、ソフトバンクパブリッシング、2003/05/31

区分	技術系
必修／選択	選択
番号	Ｔ８
大項目（科目）名	ＰＫＩ
目標	暗号技術の重要な応用である PKI について、デジタル証明書の役割、認証局の役割や仕組み、電子公証や時刻認証などの新しい応用について習得する。
養うべき能力	PKI の仕組み、役割等を理解した上で、それらを例えば自社業務に活用するための方策を検討できること。
内容	PKI の基礎的な仕組みを習得させ、デジタル証明書の役割や有用性について理解させる。また、CA 局、RA 局、IA 局の機能の差異や、リボケーションのさまざまな仕組み、今後発展が期待される時刻認証や公証制度について、利用のイメージを理解させる。
キーワード	PKI とは PKCS デジタル証明書の役割 公開鍵暗号方式と証明書 X.509 構築と運用 パブリック CA、プライベート CA 階層型、メッシュ型、ブリッジ型 秘密鍵の管理、署名鍵と暗号鍵の分離 時刻認証、電子公証
対応する中項目	デジタル証明書 認証局（CA), 登録局（RA), 発行局（IA） リボケーション系 トラストモデル 鍵管理 PKI 関連法規 PKI 関連サービス
教授法の例	講義、e-learning、実習（電子証明書の取得、設定、利用等）
教科書	【今後の要整備事項】
参考文献など	■カーライル・アダムズ: PKI―公開鍵インフラストラクチャの概念、標準、展開、ピアソンエデュケーション、2000/07

区分	マネジメント系
必修／選択	必修
番号	Ｍ１
大項目（科目）名	情報セキュリティマネジメント
目標	情報セキュリティをマネジメントするための基礎的なサイクル、及び物理的、人的セキュリティの側面について、基礎的な対策を習得する。
養うべき能力	企業や組織全体の情報セキュリティをマネジメントできること。
内容	情報セキュリティをマネジメントするために必要な PDCA サイクルを理解し、各ステップにおける実施事項（ポリシ策定、リスクアセスメント、普及、教育、監査）の概要を把握させる。また、技術系では触れていない、物理的セキュリティ、人的・組織的セキュリティについて理解させる。
キーワード	成熟度モデル PDCA サイクル 情報セキュリティポリシの概要、リスクアセスメントの概要、 情報セキュリティ監査、普及と啓発、教育、情報収集 物理セキュリティに関する具体的な対策紹介 組織構造におけるセキュリティ上の役割 （実施責任者の業務やプロフェッショナリティに言及、例えばリーダシップ、動機付け、ＲＯＩ、危機管理など） 関係するサードパーティ 責任の明確化 証拠収集と証拠保全 倫理規定、プロフェッショナリティ プライバシーポリシ
対応する中項目	ISMS 物理的セキュリティ 人的・組織的セキュリティ 最小特権の原則 職務分離、ローテーション
教授法の例	講義、e-learning
教科書	【今後の要整備事項】
参考文献など	■中尾・水本・平野・吉田: 情報セキュリティマネジメントガイド―JIS X 5080:2002(ISO/IEC 17799:2000)、日本規格協会 ■田渕 治樹: ISMS 構築のための情報セキュリティポリシーとリスク管理、オーム社 ■NPO 日本ネットワークセキュリティ協会(JNSA): 「情報セキュリティポリシーサンプル(0.91 版)」、http://www.jnsa.org/ ■トーマツ (編):セキュリティ・マネジメント戦略―ISMS によるリスク管理、日本経済新聞

区分	マネジメント系
必修／選択	必修
番号	Ｍ２
大項目（科目）名	情報セキュリティポリシ
目標	情報セキュリティポリシの必要性を認識し、構成、情報セキュリティを推進する体制（組織）について理解した上で、具体的な方針や規程類の策定方法を習得する。
養うべき能力	自社あるいは自組織の状況に鑑みて、適切な情報セキュリティポリシを策定できること。また、この情報セキュリティポリシを定期的に見直すことができること
内容	ポリシの構成、構築のステップを理解させる。またポリシを詳細化した各種のルール、規程類について、いかなる構成が適しており、どのような内容が必要であるかを検討するための知識と能力を習得させる。 ポリシを実行するための組織化（情報セキュリティ委員会）をどのように編成しポリシを具現化するか、さらには、経営者に説明しフォローすることが重要であることを理解させる。
キーワード	位置づけと必要性 方針のテンプレート、方針の策定方法、方針の承認手続き，方針の定期的な見直しと改定 雇用契約／職務規程、機密／文書／情報管理規程、 プライバシーポリシ セキュリティ教育の規定、罰則の規定、対外説明の規定、 例外の規定、規則更新の規定、規定の承認手続き 個人情報保護規定との関係 インターネット・イントラネット利用規定 インターネット向け公開サーバの設置および管理規定 社内サーバ・FW/IDS およびクライアントの設置および管理規定 リモートアクセスに関する規定 アプリケーションインストール規定、情報管理の規定 コンピュータウイルス対策運用規定、クライシスマネジメント（危機管理）の規定 情報セキュリティ監査・システム監査の規定、 情報システム管理者の規定 ネットワーク管理者の規定 システム開発の規定、規定の承認・変更手続き
対応する中項目	情報セキュリティポリシとは 情報セキュリティ組織（委員会） 情報セキュリティポリシの構成 情報セキュリティポリシの構築 情報セキュリティルール

	情報セキュリティ方針の策定 企業活動一般のセキュリティ規定の作成 情報システムの情報セキュリティ規定の作成
教授法の例	講義、e-learning、実習（セキュリティポリシや各種規程類の策定等）
教科書	【今後の要整備事項】
参考文献など	■中尾・水本・平野・吉田: 情報セキュリティマネジメントガイド―JIS X 5080:2002(ISO/IEC 17799:2000)、日本規格協会 ■田渕 治樹: ISMS 構築のための情報セキュリティポリシーとリスク管理、オーム社 ■NPO 日本ネットワークセキュリティ協会(JNSA): 「情報セキュリティポリシーサンプル(0.91 版)」、http://www.jnsa.org/ ■トーマツ (編):セキュリティ・マネジメント戦略―ISMS によるリスク管理、日本経済新聞

区分	マネジメント系
必修／選択	必修
番号	Ｍ３
大項目（科目）名	リスクマネジメント
目標	組織が保有する情報資産を適切に評価し、それら資産を取り巻く脅威、脆弱性に基づいてリスクを分析、評価し、組織のリスク方針と整合性のとれたリスク対策を実施し、マネジメントを適切に実施するための基礎的な考え方を習得する。
養うべき能力	自社あるいは自組織において、保有する情報資産を適切に評価し、またそれら資産に関連するリスクを把握できること。
内容	情報資産の分類の考え方、情報資産の価値評価、脅威と脆弱性の把握、リスクアセスメントの手法について理解させる。その上で、全社を対象にしたリスクポリシと整合する形で情報セキュリティに対するリスクリスク対応の考え方、合意形成の進め方等について習得させる。
キーワード	全社的なリスクマネジメント体制 経営者の関心、経営理念、情報セキュリティポリシとの整合性 情報資産の分類、情報資産の評価、機密度の設定 脅威の洗い出しと評価、脆弱性の洗い出しと評価、 想定される被害の評価 ベースラインアプローチ、非形式的アプローチ、詳細リスク分析、組合せアプローチ リスク評価 リスク保有、リスク回避、リスク移転、リスク低減
対応する中項目	リスクマネジメント方針 リスクアセスメント リスク対応 リスク受容 リスクコミュニケーション
教授法の例	講義、e-learning、実習（資産評価、リスクアセスメントの実施等）
教科書	【今後の要整備事項】
参考文献など	■NIST Risk Management Guide fir Information Technology Systems NIST800-30, 2001 ■ISO/IEC TR 13335 ■JIS Q 2001 ■JIPDEC リスクマネジメントシステム（JRMS），2004

区分	マネジメント系
必修／選択	必修
番号	Ｍ４
大項目（科目）名	クライシスマネジメント（危機管理）と事前準備
目標	万が一企業内における情報セキュリティに関するクライシスが発生した際の基本的な対応方策を習得すると共に、そうした緊急時の対応を適切に実施するための普段からの準備事項を習得する。
養うべき能力	クライシスが発生した場合に備えて実施すべき事前準備を把握できること。またそれらの準備を的確に実施し、万が一の場合には、その準備に従ってマネジメントを実施できること。
内容	事前準備としての情報収集の方法について習得する。またクライシス発生時のエスカレーションポリシ、インシデント対応マニュアル、災害時復旧計画や事業継続計画等の策定方法を理解する。さらに、法的対応に備えた証拠収集と証拠保全にあり方について習得する。
キーワード	CERT/CC、JPCERT/CC、IPA セキュリティセンター、 関係組織・マスメディア・通信事業者とのコミュニケーション 予防策、検知と初期対応、被害の局所化（拡大防止）、被害の撲滅、復旧、事後分析 インシデント予防策 インシデントの分析（ハードウェアとソフトウェア） インシデント分析のリソースリスト インシデント対応ツール（セキュリティパッチ、OS のバックアップ等） CERT/CC、JPCERT/CC、IPA セキュリティセンターへの連絡と報告 関係組織・マスメディア・通信事業者への連絡と報告
対応する中項目	情報収集 エスカレーションポリシ インシデント対応マニュアル 証拠収集と証拠保全 組織内のインシデントレスポンスチーム 災害時復旧計画、事業継続計画 事後報告
教授法の例	講義、e-learning、実習（情報収集方法、災害時復旧計画や事業継続計画作成等）
教科書	【今後の要整備事項】
参考文献など	■NIST Computer Security Incident Handling Guide, NIST800-61, 2004 ■SANS Institute: Computer Security Incident Handling Step by Step Ver2.2J, NRI セキュアテクノロジーズ

区分	マネジメント系
必修／選択	必修
番号	Ｍ５
大項目（科目）名	法令と標準化
目標	情報セキュリティを維持する上で有益な各種の規格・基準・指針・ガイドラインについて概観を得ると共に、遵守が必須となる法令について習得する。
養うべき能力	情報セキュリティに関連する各種の規格・基準・指針・ガイドラインについて概略を理解し、必要に応じてそれらを活用できること。
内容	下記、キーワードに列挙したような各種の規格・基準・指針・ガイドラインについて、その概略と最新情報の入手方法を習得させる。
キーワード	法的判断の構造論 情報システム安全対策基準 コンピュータウイルス対策基準 コンピュータ不正アクセス対策基準 システム監査基準 情報セキュリティ監査基準類 ソフトウェア管理ガイドライン 情報通信ネットワーク安全・信頼性基準 情報システム安全対策指針 行政情報システムの安全対策指針 情報セキュリティポリシーに関するガイドライン 電子署名及び認証業務に関する法律 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律 不正アクセス行為の禁止等に関する法律 電子商取引に関する準則 商法（特に会社法の機関の部分） 商法（いわゆるＩＴ化の部分） 個人情報保護関連法・個人情報保護条例 著作権法 商標法 不正競争防止法 労働法 労働安全衛生法 刑法（いわゆるコンピュータ犯罪の部分） 刑事訴訟法・国税徴収法・弁護士法 民法 消費者契約法 その他特定の業界に関する法律

	ISO/IEC 15408（JIS X 5070） ISO/IEC 17799（JIS X 5080） ISO/IEC TR 13335（JIS TR X 0036） ISO/IEC 9796 ISO/IEC 9797（JIS X 5055） ISO/IEC 9798（JIS X 5056） ISO/IEC 9979 ISO/IEC 10118（JIS X 5057） ISO/IEC 11770（JIS X 5058） ISO/IEC 13888（JIS X 5059） ISO/IEC TR 14516（JIS TR X 0081） ISO/IEC 14888 ISO/IEC TR 15443 (FRITSA) ISO/IEC 21827 (SSE-CMM) ISO/IEC 15026 (System and software Integrity levels) （JIS X 0134） （その他、JNSA 標準調査 WG 成果を参照） RFC セキュリティ関連項目 IEEE セキュリティ関連項目 ITU-T OECD「情報システム及びネットワークのセキュリティのためのガイドライン」 OECD「プライバシー保護と個人データの国際流通についてのガイドライン」 OECD「暗号政策に関するガイドライン」 欧州連合「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」 欧州評議会「サイバー犯罪条約」
対応する中項目	法令と標準化 基準・指針・ガイドライン等 法令 国際標準規格 国際ガイドライン
教授法の例	講義、e-learning
教科書	【今後の要整備事項】
参考文献など	■西村総合法律事務所: IT 法大全、日経 BP ■岡村久道編: 企業活動と情報セキュリティ、経済産業調査会、2002.11.18 ■別冊 NBL サイバー法判例解説、商事法務、2003/4/17 ■JIS ハンドブック 2004, 情報セキュリティ, 日本規格協会 ■JIS ハンドブック 2004, リスクマネジメント, 日本規格協会 ■JIS ハンドブック 2004, 適合性評価, 日本規格協会 ■JIS ハンドブック 2004, ソフトウェア, 日本規格協会

	■島田裕次他: 情報セキュリティ監査制度の解説と実務対応、日科技連、2003/10/26

区分	マネジメント系
必修／選択	必修
番号	Ｍ６
大項目（科目）名	個人情報保護
目標	OECD８原則、EU 指令等、個人情報保護の歴史的な背景を知ると共に、プライバシーポリシの策定や JIS コンプライアンスプログラム等を習得する。
養うべき能力	法令等を遵守しつつ、個人情報を適切に保護できること。自社あるいは自組織のプライバシポリシを策定し、あるいはコンプライアンスプログラムを策定できること。
内容	OECD8 原則、EU 指令等の歴史的な背景から、現行の個人情報保護法まで、関連する法令等を理解させる。また、プライバシーポリシの策定の考え方、コンプライアンスプログラムの策定のステップを習得させる。
キーワード	JIS Q 15001 プライバシーマーク、個人情報保護マーク
対応する中項目	OECD８原則 EU 指令 個人情報の保護に関する法律 自治体条例 プライバシーポリシ コンプライアンスプログラム 認定制度
教授法の例	講義、e-learning、実習（コンプライアンスプログラムの策定等）
教科書	【今後の要整備事項】
参考文献など	■三上・清水・新田: Q&A 個人情報保護法、有斐閣、2003/8/10 ■宇賀克也: 解説個人情報の保護に関する法律、第一法規、2003/7/7 ■藤原静雄: 逐条個人情報保護法、弘文堂、2003/8/15 ■三宅･小町谷: 個人情報保護法 逐条分析と展望､青林書院､2003/9/10 ■園部逸夫編: 個人情報保護法の解説、ぎょうせい、2003/9/20 ■三宅弘: Q&A 個人情報保護法 解説、三省堂、2003/7/20 ■牧野二郎著: 企業情報犯罪対策入門、インプレス、2004/2/11 ■島田裕次: 個人情報保護法への企業の実務対応、日科技連、2003/11/24 ■稲垣隆一: 個人情報保護法と企業対応、清文社、2003/10/10 ■岡村久道: 新法解説 個人情報保護法入門、商事法務、2003/6/27 ■北岡弘章著: 漏洩事件 Q&A に学ぶ 個人情報保護と対策、日経 BP 社、2003/6/16 ■奥田孝之: 先端技術の個人情報保護―生命科学・情報科学・技術倫理の考え方、地人書館, 2003.1.25 ■日本セキュリティマネジメント学会 個人情報保護研究会編: 経営戦略としての個人情報保護と対策、工業調査会、2002/8/30 ■個人情報保護実務研究会編: 個人情報保護 管理・運用の実務、新日本法規、2003/7/28

	■日本国際規格コンサルティング著: よくわかる JIS Q 15001、日本能率協会マネジメントセンター、2002.2.15

区分	マネジメント系
必修／選択	選択
番号	Ｍ７
大項目（科目）名	システム開発管理
目標	自組織において情報システムを開発し、それを安全に運営するため必要となる、ライフサイクルに沿ったセキュリティの考え方を習得する。
養うべき能力	自社あるいは自組織においてシステムを構築する際に、構築時点においてセキュリティ対策の作り込みができること。
内容	計画、設計、開発、テスト、運用、維持等のシステム構築の各ライフサイクルにおいて、情報セキュリティ実現のために実施すべき事項について習得させる。
キーワード	バックアップ PP、ST バージョンアップにおけるセキュリティ パッチマネジメント（脆弱性管理）
対応する中項目	製品調達・導入 セキュリティ計画 設計段階におけるセキュリティ 開発・要員計画 テスト工程におけるセキュリティ 運用段階でのセキュリティ 外部委託管理
教授法の例	講義、e-learning
教科書	【今後の要整備事項】
参考文献など	■SLCP-JCF98 委員会: 共通フレーム 98、通産資料調査会、1998 ■松尾明監訳、ISACA 東京翻訳: COBIT 3rd ed. マネジメントガイドライン、アイテック、2003 ■ソフトウェア開発モデル契約解説、日本電子工業振興協会 ■菅野孝雄: 実務者のための情報システム外注管理、コンピュータエージ社、1999

区分	マネジメント系
必修／選択	選択
番号	Ｍ８
大項目（科目）名	情報管理
目標	資産のインベントリ管理、著作物の知的財産権の管理、企業の営業機密等の管理について、基本的な考え方と実施すべき対策を習得する。
養うべき能力	企業や組織として、保有する情報の管理のあり方について、さまざまな側面から管理を実践できること。
内容	ＩＴ資産のインベントリ管理、知的財産権の管理、営業機密の管理、倫理規定のあり方等について習得させる。
キーワード	著作権、ソフトウェアライセンス管理 電子すかし、フィンガープリンティング
対応する中項目	ＩＴ資産管理 知的財産権管理 営業機密管理 コンテンツ管理 倫理規定
教授法の例	講義、e-learning、実習（倫理規定の策定等）
教科書	【今後の要整備事項】
参考文献など	■知的財産の取得・管理指針　（2003 年 3 月 14 日公表） http://www.meti.go.jp/policy/competition/downloadfiles/ip/030314guideline.pdf ■営業秘密管理指針　（2003 年 1 月 30 日公表） http://www.meti.go.jp/policy/competition/downloadfiles/ip/030130guideline.pdf ■技術流出防止指針～意図せざる技術流出の防止のために～（2003 年 3 月 14 日公表） http://www.meti.go.jp/policy/competition/downloadfiles/ip/030314guideline2.pdf ■斉藤 博：著作権法、有斐閣、2000 ■作花文雄：詳解　著作権法、ぎょうせい ■半田正夫：著作権法概説、一粒社、2003 ■半田正夫・紋谷暢男編：著作権のノウハウ、有斐閣、2002 ■加戸守行：著作権法逐条講義、著作権情報センター、2003 ■金井重彦・小倉秀夫編著：著作権法コンメンタール　上・下、東京布井出版、2000

区分	マネジメント系
必修／選択	選択
番号	Ｍ９
大項目（科目）名	教育・訓練
目標	管理する立場の者として必要な、利用者の啓発や教育訓練、また技術者の育成等に関する教育の方法・効果測定法などを習得する。
養うべき能力	自社や自組織内で教育を実施する立場として、計画、リソース確保、実施、効果測定等を実施できること。
内容	教育訓練計画の立案、教育方法の検討、利用者及びセキュリティ技術者の教育実施、教育結果の効果測定等について、具体的な進め方を習得させる。
キーワード	啓発教育、技術教育、継続的教育の効果 啓発教育、基本教育、高度セキュリティ教育 トレーニング、外部教育サービス e-learning、ＯＪＴ
対応する中項目	利用者への啓発および教育訓練計画 利用者教育 セキュリティ技術者教育 教育方法 教育効果の測定
教授法の例	講義、e-learning
教科書	【今後の要整備事項】
参考文献など	■IPA　情報セキュリティスキルマップ構築の調査研究 http://www.ipa.go.jp/security/fy15/reports/skillmap/index.html ■NIST SP 800-50 Building an Information Technology Security Awareness and Training Program, October 2003 ■NIST SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model April 1998

区分	マネジメント系
必修／選択	選択
番号	Ｍ１０
大項目（科目）名	監査
目標	情報セキュリティを管理する立場の者として必要な、情報セキュリティ監査、システム監査に関する基礎的な知識や手法を習得する。
養うべき能力	監査計画の立案、監査チームの養成、監査の実施、監査報告書の作成、フォローアップ等の一連のステップを実施できること。あるいは実施を指導できること。
内容	外部監査・内部監査の違いと意義、監査手法のバリエーション、監査計画書の立案方法、実際の監査の進め方、監査報告書の作成方法等について、具体的な進め方を習得する。
キーワード	外部監査・内部監査 任意監査・法定監査 助言型監査・保証型監査 ネットワークスキャナ 情報セキュリティ監査 システム監査
対応する中項目	監査の種類 監査手順 監査手法 監査計画書 監査報告書 監査制度
教授法の例	講義、e-learning、実習（監査計画の立案、監査チームによるロールプレイング等）
教科書	【今後の要整備事項】
参考文献など	■経済産業省　情報セキュリティ監査報告書 http://www.meti.go.jp/policy/netsecurity/audit.htm ■COBIT Ver.3 （Control Objectives, Management Guidelines, Audit Guidelines), ISACA（松尾明監訳、ISACA 東京翻訳: COBIT 3rd ed. マネジメントガイドラインのみ日本語版が出版されている） ■岡村久道編: 企業活動と情報セキュリティ、経済産業調査会、2002.11.18

参考資料１）情報セキュリティ教育関連の情報の入手源

国　内　制　度

■　ＩＴスキル標準関連

資料名	ＩＴスキル標準　―ＩＴｻｰﾋﾞｽ･ﾌﾟﾛﾌｪｯｼｮﾅﾙ育成の基盤構築に向けて　Ver.1.1 ＩＴｱｰｷﾃｸﾄ→専門分野：ｾｷｭﾘﾃｨ（概要、達成度指標、熟達度・知識項目） ＩＴｽﾍﾟｼｬﾘｽﾄ→専門分野：ｾｷｭﾘﾃｨ（概要、達成度指標、熟達度・知識項目）
発行者	経済産業省
発行年	2003.7
ＵＲＬ	http://www.meti.go.jp/policy/it_policy/jinzai/g030701aj.html

資料名	研修ロードマップ　Ver1.0 ＩＴｱｰｷﾃｸﾄ ＩＴｽﾍﾟｼｬﾘｽﾄ
発行者	経済産業省
発行年	2003.7
ＵＲＬ	http://www.meti.go.jp/policy/it_policy/jinzai/g030701rj.html

資料名	情報セキュリティプロフェッショナル育成に関する調査研究報告書 （いわゆるスキルマップ）
発行者	情報処理振興事業協会　セキュリティセンター
発行年	H15.3
ＵＲＬ	http://www.ipa.go.jp/security/fy14/reports/professional/ikusei-seika-press.html

■　情報処理技術者試験（情報セキュリティアドミニストレータ）関連

資料名	情報処理技術者試験　新制度の概要
発行者	（財）日本情報処理開発協会　情報処理技術者試験センター
発行年	平成 12 年 6 月
ＵＲＬ	http://www.jitec.jp/1_13download/gaiyo01.pdf

資料名	情報処理技術者試験　出題範囲
発行者	（財）日本情報処理開発協会　情報処理技術者試験センター
発行年	平成 14 年 11 月（改訂）
ＵＲＬ	http://www.jitec.jp/1_13download/hani01.pdf

資料名	情報処理技術者スキル標準　情報セキュリティアドミニストレータ
発行者	（財）日本情報処理開発協会　中央情報教育研究所
発行年	2001 年 9 月 28 日（最終更新日）
ＵＲＬ	http://www.jitec.jp/1_17skill/pdf0928/ss-09-0.pdf

資料名	情報処理技術者スキル標準　ＩＴ共通知識体系
発行者	（財）日本情報処理開発協会　中央情報教育研究所
発行年	2001 年 9 月 28 日（最新更新日）
ＵＲＬ	http://www.jitec.jp/1_17skill/pdf0928/ss-it-0.pdf

資料名	統計情報（応募者・受験者・合格者の推移など）
発行者	（財）日本情報処理開発協会　情報処理技術者試験センター
発行年	（随時更新）
ＵＲＬ	http://www.jitec.jp/1_07toukei/toukei_kydo.html

■　ＩＴコーディネータ関連

資料名	IT コーディネータ報告書
発行者	経営情報化推進協議会
発行年	2000 年１０月２日
ＵＲＬ	http://www.itc.or.jp/dlfiles/m_report.pdf

資料名	IT コーディネータカリキュラム作成ガイドライン　β版
発行者	IT コーディネータ検討グループ
発行年	2000 年 10 月 2 日
ＵＲＬ	http://www.itc.or.jp/dlfiles/m_C-guide.pdf

資料名	IT コーディネータプロセスガイドライン　β版
発行者	IT コーディネータ検討グループ
発行年	2000 年 10 月 2 日
ＵＲＬ	http://www.itc.or.jp/dlfiles/m_P-guide.pdf

資料名	IT コーディネータ資格ﾏﾙﾁｴﾝﾄﾘｰﾎﾟｲﾝﾄ制度運用ガイドライン［V1.4］
発行者	NPO IT コーディネータ協会
発行年	２００３年8月１日
ＵＲＬ	https://wws.itc.or.jp/point/dlfiles/pointv14_20030801.pdf

資料名	IT コーディネータ資格認定ガイドライン
発行者	NPO IT コーディネータ協会
発行年	２００１年2月１４日
ＵＲＬ	http://www.itc.or.jp/dlfiles/m_nintei_gaido.pdf

資料名	IT コーディネータ専門知識教材・研修コース認定ガイドライン［Ver1.4 仮改訂版］
発行者	NPO IT コーディネータ協会
発行年	２００２年１０月7日（訂正）
ＵＲＬ	http://www.itc.or.jp/dlfiles/m_guideline_Ver1.4.pdf

■ NISM (Network Information Security Manager) 関連

ＵＲＬ	http://www.learningsite21.com/nism/top.html

■ SEA/J (Security Education Alliance / Japan) 関連 （補足３）

資料名	認定コース内容
発行者	SEA/J
発行年	
ＵＲＬ	http://www.sea-j.net/course.html

■ システム監査学会関連（情報セキュリティ研究プロジェクト）

資料名	情報セキュリティ教育カリキュラム（モデル）作成にあたって
発行者	システム監査学会　情報セキュリティ研究プロジェクト
発行年	2002/11
ＵＲＬ	http://www.sysaudit.gr.jp/project/2002security/curmodel.pdf

資料名	情報セキュリティ教育カリキュラム（モデル）
発行者	システム監査学会　情報セキュリティ研究プロジェクト
発行年	2002/11
ＵＲＬ	http://www.sysaudit.gr.jp/project/2002security/curmodel.pdf

■ 情報処理学会関連

資料名	大学の情報系専門学科のための情報システム教育カリキュラム ・ISJ2001-（情報処理教育委員会 情報システム小委員会報告書）
発行者	（社）情報処理学会
発行年	2001/12
ＵＲＬ	http://www.ipsj.or.jp/katsudou/chosa/monbu.html（購入紹介ページ）

資料名	大学の理工系学部情報系学科のためのコンピュータサイエンス教育カリキュラム J97 (第 1.1 版)
発行者	（社）情報処理学会
発行年	1999.9
ＵＲＬ	http://www.ipsj.or.jp/katsudou/chosa/J97-v1.1.pdf

資料名	情報システム学の学部用プログラムのためのモデルカリキュラムと指針 IS ’97
発行者	（社）情報処理学会
発行年	1998.12
ＵＲＬ	http://www.wat.soft.iwate-pu.ac.jp/ipsj-is/is97j.pdf

■ JABEE (Japan Accreditation Board for Engineering Education) 関連

資料名	平成15年度 工学教育連合講演会 講演論文集「本格化した技術者教育認定制度」-JABEE 認定プログラムの事例紹介を中心として
発行者	日本工学教育協会
発行年	H15/6/14
ＵＲＬ	

■　基準類

資料名	ISMS 認証基準 Ver2.0
発行者	（財）日本情報処理開発協会
発行年	2003 年 4 月 21 日
ＵＲＬ	http://www.isms.jipdec.jp/doc/JIP-ISMS100-20.pdf

資料名	JIS X 5080:2002 情報技術 – 情報セキュリティマネジメントの実践のための規範
発行者	（財）日本規格協会
発行年	2002 年
ＵＲＬ	http://www.jsa.or.jp/　（購入案内ページ）

資料名	JIS Q 15001:1999 個人情報保護に関するコンプライアンス・プログラムの要求事項
発行者	（財）日本規格協会
発行年	1999 年
ＵＲＬ	http://privacymark.jp/ref/jisq15001.html

資料名	情報セキュリティ監査基準類
発行者	経済産業省
発行年	（随時更新）
ＵＲＬ	http://www.meti.go.jp/policy/netsecurity/audit.htm

■　論文、講演資料等

論文名	情報セキュリティ教育の現状と今後
著者	佐々木良一・杉立淳
掲載	電子情報通信学会、信学技報 TECHNICAL REPORT OF IEICE SITE2002-33(2003-2)

論文名	情報セキュリティ教育を俯瞰する
発行者	佐々木良一
掲載	Cyber Security Management Vol.3, No.30, Apl.2002

論文名	技術者・管理者向け情報セキュリティ教育試案
著者	内田勝也
掲載	JSSM 第 16 回全国大会 発表要旨
ＵＲＬ	http://www2.gol.com/users/uchidak/Seminar/JSSM200206.pdf

論文名	ソフトウェア・情報セキュリティ分野における人材育成
著者	内田勝也
掲載	シンポジウム電子社会の展望　（2003/4/12）
ＵＲＬ	http://www.21coe.chuo-u.ac.jp/security/kinen2003-04-12/uchida.pdf

資料名	米国大学院の情報セキュリティ教育を見る
著者	内田勝也
掲載	Cyber Security Management Vol.4, No.47, Sep.2003

■　調査報告書等

資料名	「情報セキュリティマネジメントの実態調査」報告書
発行者	情報処理振興事業協会　セキュリティセンター
発行年	2003/3
ＵＲＬ	http://www.ipa.go.jp/security/fy14/reports/current/2002-Sec-manage.pdf

資料名	情報セキュリティの実態調査 2001 調査報告書
発行者	情報処理振興事業協会　セキュリティセンター
発行年	H13 年度
ＵＲＬ	http://www.ipa.go.jp/security/fy13/report/security_survey/survey2001.pdf

資料名	OECD 情報セキュリティガイドライン見直しに関する調査
発行者	情報処理振興事業協会　セキュリティセンター
発行年	
ＵＲＬ	http://www.ipa.go.jp/security/fy14/reports/oecd/oecd-security.pdf

資料名	平成 13 年度情報セキュリティに関する調査の結果
発行者	（財）日本情報処理開発協会
発行年	H14/2
ＵＲＬ	http://www.jipdec.jp/security/01sec.html

資料名	不正アクセス行為対策の実態調査
発行者	警察庁
発行年	H14 年度
ＵＲＬ	http://www.npa.go.jp/hightech/cyberterror/nsresearch07/index.htm

資料名	情報セキュリティ対策の状況調査結果
発行者	総務省
発行年	2002/9
ＵＲＬ	http://www.soumu.go.jp/s-news/2002/020913_5.html

海 外 制 度

■ CISSP (Certified Information Systems Security Professional) 関連

資料名	CISSP Certification Common Body of Knowledge Study Guide
発行者	$(ISC)^2$
発行年	逐次更新
ＵＲＬ	https://www.isc2.org/cgi-bin/request_studyguide.cgi（入手案内ページ）

資料名	SSCP (Systems Security Certified Practitioner): Certification Common Body of Knowledge Study Guide
発行者	$(ISC)^2$
発行年	逐次更新（初版 2003 年）
ＵＲＬ	https://www.isc2.org/cgi-bin/request_studyguide.cgi（入手案内ページ）

書籍
➢ The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, Ronald L. Krutz, Russell Dean Vines (著) ➢ The CISSP Prep Guide: Gold Edition (All-In-One), Ronald L. Krutz, Russell Dean Vines (著) ➢ Advanced CISSP Prep Guide: Exam Q&A, Ronald L. Krutz, Russell Dean Vines (著) ➢ CISSP Certification: All in One Exam Guide (All-In-One (Series).), Shon Harris (著) ➢ Official $(Isc)^2$ Guide to the CISSP Exam, Susan Hansche (著) ➢ The CISSP All-In-One Exam Guide (All-In-One), Shon Harris (著), Gareth Hancock (編)

■ CISM (Certified Information Security Manager) 関連

資料名	CISM Brochure
発行者	ISACA
発行年	
ＵＲＬ	http://www.isaca.org/cismbrochure.pdf

資料名	CISM Exam Bulletin of Information
発行者	ISACA
発行年	
ＵＲＬ	http://www.isaca.org/cismboi.pdf 日本語は http://isaca.gr.jp/cism/images/2004CISM.pdf

書籍
➢ The CISM Prep Guide: Mastering the Five Domains of Information Security Management, Ronald L. Krutz, Russell Dean Vines (著) ➢ Certified Information Security Manager・ (CISM・) Review Manual 2004, Information Systems Audit and Control Association

■ GIAC (Global Information Assurance Certification) 関連 （補足６）

資料名	Program Details
発行者	SANS
発行年	
ＵＲＬ	http://www.giac.org/program.php

資料名	Objectives & Curriculum
発行者	SANS
発行年	
ＵＲＬ	http://www.giac.org/GIAC_Cert_Brief.pdf

資料名	SANS JAPAN ホームページ
発行者	NRI セキュアテクノロジーズ SANS JAPAN プロジェクト
発行年	
ＵＲＬ	http://sans-japan.jp/

■ CSI (Computer Security Institute) 関連

資料名	Course Brochure
発行者	CSI
発行年	
ＵＲＬ	http://www.gocsi.com/db_area/pdfs/infosec/seminars2003.pdf

■ Security+ 関連 （補足７）

資料名	CompTIA ホームページ
発行者	CompTIA
発行年	
ＵＲＬ	http://www.comptia.jp/

資料名	Security+ objective
発行者	CompTIA
発行年	
ＵＲＬ	http://www.comptia.org/certification/Security/security_plus_objectives_10-23.pdf

書籍
➢ Security+: Study Guide & Dvd Training System, Robert J. Shimonski (著) ➢ Security+ Certification All-In-One: Exam Guide (All-In-One), Gregory White (著) ➢ Security+ Prep Guide, Ronald L. Krutz (著), Russell Dean Vines (著)

■ Purdue 大学

資料名	Department of Computer Sciences, Course Information
発行者	Purdue 大学

発行年	（随時更新）
ＵＲＬ	http://www.cs.purdue.edu/courses/

■ Carnegie Mellon 大学

資料名	Master of Science in Information Security Technology and Management (MSISTM)
発行者	CMU
発行年	（随時更新）
ＵＲＬ	http://www.ini.cmu.edu/academics/MSISTM/msistm_overview.htm

資料名	Master of Science in Information Security Policy and Management (MSISPM)
発行者	CMU
発行年	（随時更新）
ＵＲＬ	http://www.heinz.cmu.edu/msispm/

■ NIST (National Institute of Standards and Technology)

資料名	SP 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model
発行者	NIST CSRC (Computer Security Resource Center)
発行年	April 1998
ＵＲＬ	http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf http://csrc.nist.gov/publications/nistpubs/800-16/AppendixA-D.pdf http://csrc.nist.gov/publications/nistpubs/800-16/Appendix_E.pdf

資料名	SP 800-50 Building an Information Technology Security Awareness and Training Program
発行者	NIST CSRC (Computer Security Resource Center)
発行年	October 2003
ＵＲＬ	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

参考資料２）情報セキュリティ教育関連制度に関する補足

１）　情報処理技術者試験の概要

名　称

情報処理技術者試験 情報セキュリティアドミニストレータ（通称 SS）
(Information Systems Security Administrator)

主　催

（独）情報処理推進機構　情報処理技術者試験センター（2004/1～）
（財）日本情報処理開発協会 情報処理技術者試験センター（～2003/12）

対象者像

情報セキュリティに関する基本的な知識をもち、情報システムの情報セキュリティポリシの策定及びその実施、分析、見直しを行う者

役割と業務

情報セキュリティ管理の現場責任者として、セキュリティに関する企画・実施・運用・分析のすべての段階で、物理的観点、人的観点及び技術的観点から情報セキュリティを保つための施策を計画・実施し、その結果に関する評価を行う業務に従事し、次の役割を果たす。

1）　情報資源の洗い出し、脅威分析、リスク分析を行い、組織体におけるセキュリティ管理のターゲットを示す情報セキュリティポリシを策定する。
2）　情報セキュリティポリシに則って、それを実現するための技術の選択と適用、運用に関するガイドラインの策定、一般利用者教育を行う。
3）　管理対象から出力される各種情報に従って、セキュリティ侵犯がないか常に監視し、侵犯発生時には対策を講じる。また、情報セキュリティポリシ策定時のレベルを維持できるよう適切な措置を講じる。
4）　セキュリティ侵犯事象の根本原因を追求し、改善策を策定する。

普及状況

（統計情報 http://www.jitec.jp/1_07toukei/suii_hyo.html より抜粋）

	合　計	平成 13 年度	平成 14 年度	平成 15 年度
応募者	58,130 名	23,778 名	34,352 名	42,417 名
受験者	38,223 名	15,988 名	22,235 名	27,913 名
合格者	4,899 名	2,111 名	2,788 名	3,149 名
合格率		13.2%	12.5%	11.3%

（統計情報 http://www.jitec.jp/1_07toukei/nenrei.html より抜粋）

平成１３年度			平成１４年度			平成１５年度		
応募者	受験者	合格者	応募者	受験者	合格者	応募者	受験者	合格者
33.0 歳	33.1 歳	32.8 歳	32.6 歳	32.7 歳	32.5 歳	32.9 歳	33.1 歳	33.7 歳

参考資料

試験の概要: http://www.jitec.jp/1_08gaiyou/gaiyou_kydo.html
情報処理技術者試験出題範囲: http://www.jitec.jp/1_13download/hani01.pdf
情報処理技術者スキル標準: http://www.jitec.jp/1_17skill/skill_00.html
統計情報: http://www.jitec.jp/1_07toukei/toukei_kydo.html

試験の概要

◇期待する技術水準

セキュリティ確保は各組織における基本的な責任であるとともに、社会的要請でもある。各組織においてセキュリティ確保・管理を遂行するために、次の知識・技能が要求される。

1）情報セキュリティポリシ、ガイドラインの策定ができる。
2）リスク分析、リスク管理ができる。
3）ＯＳ、ネットワーク、インターネットに関する技術、製品（ハードウェア、ソフトウェア、サービス）知識を有し、利用・活用できる。
4）防御技術に関する知識を有し、適用できる。
5）セキュリティ運用・管理に関する知識を有し、策定できる。
6）脆弱性に関する知識を有し、対処方法を検討・実施できる。
7）セキュリティ侵犯を発見し、対処できる。
8）セキュリティ、プライバシ関連法規の知識を有している。
9）セキュリティの監査、評価に関する知識を有し、対象を監査・評価できる。
１０）セキュリティの観点から人間及び社会に関する知見を有している。
１１）一般ユーザにおけるセキュリティ対策を策定できる。
１２）セキュリティに関する国際動向の知識を有し、適用できる。

◇出題範囲（午後）

１．情報セキュリティシステムの企画・設計・構築に関すること

情報戦略，情報システム（ネットワークを含む）の企画・設計・構築，開発管理，物理的セキュリティ対策，アプリケーションセキュリティ対策，データベースセキュリティ対策，ネットワークセキュリティ対策，システムセキュリティ対策など

２．情報セキュリティの運用・管理に関すること

情報セキュリティポリシの策定・評価・見直し，リスク分析，業務継続計画，セキュリティ運用・管理，脆弱性分析，不正アクセス検知・対策，ユーザセキュリティ管理，障害復旧計画，セキュリティ教育，契約管理，要員管理，システム監査（のセキュリティ側面） など

３．情報セキュリティの技術・関連法規に関すること

アクセス管理技術，ウイルス対策技術，暗号技術，認証技術，暗号応用システム，情報セキュリティ関連法規，国内・国際標準，ガイドライン，著作権法，プライバシ保護，情報倫理など

◇スキル標準

情報処理技術者スキル標準　情報セキュリティアドミニストレータ（別添）
〃　ＩＴ共通知識体系（別添）

2）　ＮＩＳＭの概要

名　称

NISM (Network Information Security Manager、ネットワーク情報セキュリティマネージャ)

主　催

NISM 推進協議会
（情報通信ネットワーク産業協会、(社）テレコムサービス協会、(社）電気通信事業者協会、(社）電波産業会、(社）日本インターネットプロバイダ協会、(財）日本データ通信協会、ネットワークセキュリティ登録事業者協議会）

対象者像

- ハッカーやサイバーテロの脅威に対処し、情報通信ネットワークの安全性・信頼性を確保するために、情報通信サービスを提供する事業者に配置する専門家

普及状況

（公表資料なし、不明）

補足事項

- 資格の種別と、対応する教育コース概要
  - ネットワークセキュリティ基礎
    - レベル：初級、日数：２日間、形態：講義
    - 前提知識：
      - インターネット技術の基礎知識を有すること
      - セキュリティ基礎知識を有すること
  - ネットワークセキュリティ実践
    - レベル：中級、日数：３日間、形態：講義・演習・実習
      （ネットワーク管理、セキュリティ管理などの業務に携わる方）
    - 前提知識：
      - 基礎コースを受講していること、または同等の知識を有すること。
  - サーバセキュリティ実践
    - レベル：専門、日数：３日間、形態：講義・演習
      （サーバ構築と運用の業務に携わる方）
    - 前提知識：
      - 基礎・ネットワークセキュリティ実践コースを受講していること、または同等の知識を有すること。
      - Windows NT／2000 および UNIX システムの基礎が習得されていること。
  - セキュリティポリシ実践
    - レベル：専門、日数：２日間、形態：講義・演習
      （セキュリティポリシ策定に携わる管理者および担当責任者）
    - 前提知識：
      - 基礎・ネットワークセキュリティ実践コース、または同等の知識を有す

ること。

- セキュリティ監視実践
  - レベル：上級・専門、日数：３日間、形態：講義・演習
    (ネットワーク管理、セキュリティ管理などの業務に携わっている方)
  - 前提知識：
    - 基礎・ネットワークセキュリティ実践コース、または同等の知識を有すること。

参考資料

- 公式資料 (Web より入手可)
  - http://www.learningsite21.com/nism/top.html

試験の概要（出題領域）

- （コースにより異なる）

３）　ＳＥＡ／Ｊの概要

名　称

基礎コース：CSBM (Certified Security Basic Master)
応用コース：CSPM (Certified Security Professional Master)
of Technical / Management

主　催

SEA/J (Security Education Alliance / Japan)

対象者像

- 基礎コース：技術者、企画、マーケティング、セールス、サポート等の業務の従事者
- 応用コース：高度なスキルが求められるセキュリティ関連の業務の従事者
  - テクニカル編：システム／セールスエンジニア、情報システム管理者、ＩＴコンサル
  - マネジメント編：情報システム管理者、情報セキュリティ監査員、法務担当

普及状況

（公表資料なし）

補足事項

- 基礎コース（２日間）
  - IPA スキルマップのレベル１（基礎知識）の習得を目標
  - 12 のスキル項目をベースに広く情報セキュリティ全般の基礎知識を習得
- 応用コース：テクニカル編（３日間）
  - 実機利用、演習あり
- 応用コース：マネジメント編（２日間）
  - 演習あり

参考資料

- 公式資料 (Web より入手可)
  - http://www.sea-j.net/course.html

試験の概要（出題領域）

- 基礎コース
  - ネットワークセキュリティ基礎
  - 攻撃手法
  - ファイアウォール
  - 侵入検知システム
  - 暗号・認証
  - PKI
  - ウイルス
  - クライアントセキュリティ
  - 権限とデータ管理

- 情報セキュリティポリシ
- 関連法規

■ 応用コース：テクニカル編
- セキュリティ対策の考え方
- 脅威とその対策
- OS の要塞化（Windows）
- OS の要塞化（UNIX）
- DNS サーバへのセキュリティ対策
- メールサーバへのセキュリティ対策
- Web サーバへのセキュリティ対策
- ファイアウォール導入設計
- IDS による侵入検知
- VPN 導入設計
- PKI の利用

■ 応用コース：マネジメント編
- 情報セキュリティとはなにか
- 情報セキュリティの構成要素
- 脅威と脆弱性
- 情報セキュリティマネジメント
- リスクの概念
- リスク分析の概要
- 詳細リスク分析
- リスクマネジメント
- 情報セキュリティポリシの概要
- 情報セキュリティポリシの策定
- 情報セキュリティ監査制度

補足４）　ＣＩＳＳＰの概要

名　称

CISSP (Certified Information Systems Security Professional)

主　催

(ISC)^2 (International Information Systems Security Certification Consortium)

対象者像

- 組織内でセキュリティをすべて仕切ることができる人
- セキュリティ実現のための計画を立案できる人
- セキュリティのコンサルティングができる人
- セキュリティ面で責任を持って組織運営ができる人、あるいは補佐をできる人

普及状況

- 全世界で 16,000 名（うち約 10,000 名が米国、911 もきっかけとなり急増）
- NSA (US) が任用する専門家向けの試験として採用の方向
- Scotland Yard (UK) のサイバー犯罪セクションの過半数が保有とされている
- NCS (シンガポール)が (ISC)^2 のパートナーとして、シンガポール、中国、マレーシア等で試験をホスティング
- USA 3000, Canada 300, UK 150, Russia 2 (特約店が出来たため今後増加)、Isreal 5, India 100, Korea 120+ (2002 年に 5～6 回実施、急増中), China 70 (急増中）, 香港 220, Japan 10 (2002 年時点で 20 数名) ←数字は 2001 年時点

補足事項

- 育成コース
  - CBK (Common Body of Knowledge) コース
  - 8 時間×5 日間、実務的な深いレベルの専門家ノウハウを提供
- CISSP の新規活動
  - Management Concentration（マネジメント層向け付加資格、NSA）
  - Architecture Concentration（技術者向け付加資格）
  - Government Concentration（政府機関向け付加資格）

参考資料

- 公式資料 (Web より入手可)
  - CISSP Certification Common Body of Knowledge Study Guide
  - SSCP (Systems Security Certified Practitioner): Certification Common Body of Knowledge Study Guide
- 書籍等
  - The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, Ronald L. Krutz (著), Russell Dean Vines (著)
  - The Cissp Prep Guide: Gold Edition (All-In-One), Ronald L. Krutz (著), Russell Dean Vines (著)
  - Advanced Cissp Prep Guide: Exam Q&A, Ronald L. Krutz (著), Russell Dean Vines (著)
  - Cissp Certification: All in One Exam Guide (All-In-One (Series).), Shon Harris (著)
  - Official Isc 2 Guide to the Cissp Exam, Susan Hansche (著)
  - The Cissp All-In-One Exam Guide (All-In-One), Shon Harris (著), Gareth Hancock (編集)

試験の概要（出題領域）

- Security Management Practices
- Security Architecture and Models
- Access Control Systems & Methodology
- Operations Security
- Physical Security
- Cryptgraphy
- Telecommunications, Network & Internet Security
- Business Continuity Planning
- Law, Investigations & Ethics

５）　ＣＩＳＭの概要

名　称

Certified Information Security Manager
公認情報セキュリティマネージャー

主　催

Information Systems Audit and Control Association
（情報システムコントロール協会）
（日本国内では、情報システムコントロール協会東京支部 CISM 担当）

対象者像

情報セキュリティ管理に責任を有する、経験豊富な情報セキュリティ管理者

コンセプト

CISM is business-oriented and focused on information risk management while addressing management, design and technical security issues at the conceptual level.

It is for the individual who must maintain a view of the "big picture" by managing, designing, overseeing and assessing an enterprise's information security.

CISM is designed to provide executive management with assurance that those earning the designation have the required knowledge and ability to provide effective security management and consulting.

It is business-oriented and focuses on information risk management while addressing management, design and technical security issues at a conceptual level.

While its central focus is security management, all those in the IS profession with security experience will certainly find value in CISM.

CISM は、企業・団体等の情報セキュリティプログラムに係る、マネージメント、設計、監督を行う、以下のプロフェッショナルの方をフォーカスしている。
セキュリティマネージャー（Security managers）
セキュリティ担当役員（Security directors）
セキュリティ担当役職者（Security officers）
セキュリティコンサルタント（Security consultants）

普及状況

なし（2003 年度より新設）

参考資料

- 公式資料（Web より入手可、日本語は http://isaca.gr.jp/cism/）
  - CISM Brochure (http://www.isaca.org/cismbrochure.pdf)
  - CISM Exam Bulletin of Information (http://www.isaca.org/cismboi.pdf)
    （日本語はhttp://isaca.gr.jp/cism/images/2004CISM.pdf）
- 書籍等
  - The CISM Prep Guide: Mastering the Five Domains of Information Security Management, Ronald L. Krutz (著), Russell Dean Vines (著)
  - Certified Information Security Manager･ (CISM･) Review Manual 2004, Information Systems Audit and Control Association

試験の概要（出題領域）

- Information Security Governance（情報セキュリティガバナンス）
  - Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations.
- Risk Management（リスク・マネジメント）
  - Identify and manage information security risks to achieve business objectives.
- Information Security Program(me) Management
  （情報セキュリティ・プログラム・マネジメント）
  - Design, develop and manage an information security program to implement the information security governance framework.
- Information Security Management（情報セキュリティ・マネージメント）
  - Oversee and direct information security activities to execute the information security program.
- Response Management（レスポンス・マネージメント）
  - Develop and manage a capability to respond to and recover from disruptive and destructive information security events.

※なお、2005 年より日本語による試験を実施予定

継続教育

CISM 資格を維持するためには、下記を条件とする定期的な更新認定が必要である。

- 毎年、最低２０時間の下記継続専門教育(CPE)の報告を行う。
- 指定された３年間に、最低１２０時間の下記継続専門教育(CPE)の報告を行う。
- 毎年、継続教育の維持費用を支払う。
- ISACA 職業倫理規則を守る。

補足）継続的な専門教育活動 50 分につき、1CPE 時間が与えられる（昼食や休憩の時間を除く）。CPE 時間は、1 時間単位で計上され、時間に満たない端数は切り捨てられる。 例えば、CISM が 8 時間のプレゼンテーション(480 分)に参加して､計 90 分の休憩をとった場合は、残りの 390 分を 50 分で割り（ ＝ 7.8)、小数点以下を切り捨てて、7CPE 時間となる。なお、詳細は、ISACA の Web 等を参照のこと。

６）　ＧＩＡＣの概要

名　称

Global Information Assurance Certification

主　催

SANS (SysAdmin, Audit, Network, Security) Institute

対象者像

- セキュリティプロフェッショナル（具体的には Certifications の内容による）
- セキュリティエンジニアやコンサルタントの高度なテクニカルスキルを客観的に証明する試験制度。それぞれの専門性に基づいて、SANS が提供するコース（研修）をいかに理解したかを問う。

普及状況

(ア) 2000 年 3 月にオンラインコース一つを開設し、最初の合格者を出す
(イ) 2003 年 2 月時点で７つのオンラインコースとなり、4300 名以上の合格者
(ウ) うち 2300 名以上が GSEC である
(エ) 2004 年中に GSEC が日本語でも受験可能となる予定

参考資料

Program Details: http://www.giac.org/program.php
Objectives & Curriculum http://www.giac.org/GIAC_Cert_Brief.pdf

試験の概要

- GIAC Certification の構成
  - Individual GIAC Certifications
    - GIAC Security Essentials Certification (GSEC)
      - SANS Security Essentials and the CISSP 10 Domains
    - GIAC Certified Firewall Analyst (GCFW)
      - Firewalls, Perimeter Protection and VPNs
    - GIAC Certified Intrusion Analyst (GCIA)
      - Intrusion Detection In-Depth
    - GIAC Certified Incident Handler (GCIH)
      - Hacker Techniques, Exploits and Incident Handling
    - GIAC Certified Windows Security Administrator (GCWN)
      - Securing Windows
    - GIAC Certified UNIX Security Administrator (GCUX)
      - Securing Unix
    - GIAC Information Security Officer (GISO)
      - Intro to Information Security
    - GIAC Systems and Network Auditor (GSNA)
      - Auditing Networks, Perimeters and Systems
    - GIAC Certified Forensic Analyst (GCFA)

        - System Forensics, Investigations, and Response
    - ✧ GIAC IT Security Audit Essentials (GSAE)
        - IT Security Audit Essentials
    - ✧ GIAC Security Consultant (GSCC)
        - Security Consultant
    - ✧ GIAC 17799 Security and Audit Framework (G7799)
        - SANS 17799 Security and Audit Framework
- ➢ GIAC Certification Tracks
    - ✧ GIAC Security Expert (GSE)
        - GCFW+ GCIA+ GCIH+ GCWN+ GCUX (+GSNA +GCFA)

Technical Level	Certification
Advanced	GIAC Security Expert (GSE)
Intermediate	GIAC Certified Firewall Analyst (GCFW) GIAC Certified Intrusion Analyst (GCIA) GIAC Certified Incident Handler (GCIH) GIAC Certified Windows Security Administrator (GCWN) GIAC Certified UNIX Security Administrator (GCUX) GIAC Systems and Network Auditor (GSNA) GIAC Certified Forensic Analyst (GCFA) GIAC Security Consultant (GSCC)
Foundational	GIAC Security Essentials Certification (GSEC) GIAC IT Security Audit Essentials (GSAE)
Basic	GIAC Information Security Officer (GISO) GIAC 17799 Security and Audit Framework (G7799)

- ■ GIAC Certificate の構成
    - ✧ GIAC Security Leadership Certificate (GSLC)
    - ✧ GIAC Gold Standard Certificate (GGSC-0100)

7） Security+ の概要

名 称

Security+

主 催

CompTIA (Computing Technology Industry Association, コンピュータ技術産業協会)

対象者像

- IT 実務能力を有する人材を基本とする
- 少なくとも２年間のネットワーク実務経験を有し、TCP/IP の正確な技術を持つ者を前提
- 出題領域に示す分野について、基礎的なレベルのスキルと知識を有する者を認定

普及状況

- CompTIA は世界に９拠点のグローバルな非営利 IT 業界組織
  - 米国、カナダ、英国、ドイツ、オランダ、南アフリカ、日本、オーストラリア
- 会員は 89 カ国 15,000 期間以上で、IT 企業、教育機関、各種団体等が参
- 活動の一つに認定資格の普及啓発活動がある

参考資料

- 公式資料 (Web より入手可)
  - Security+ objective（出題範囲）
- 書籍等
  - Security+: Study Guide & Dvd Training System, Robert J. Shimonski (著)
  - Security+ Certification All-In-One: Exam Guide (All-In-One), Gregory White (著)
  - Security+ Prep Guide, Ronald L. Krutz (著), Russell Dean Vines (著)

試験の概要（出題領域）

- General Security Concepts
- Communication Security
- Infrastructure Security
- Basics of Cryptography
- Operational / Organizational Security

おわりに

情報セキュリティに関しては、「人」の問題が大きい、とかねてより言われているところであるが、我が国においてその「人」は量的にも質的にも十分ではないという指摘がなされている。本研究会では主に企業や組織の情報セキュリティ対策の責任者の効果的、実践的な育成について検討し、かつ情報セキュリティ教育の関係者に対してそれぞれの役割を果たし、連携をとっていくよう提言を行った。しかし現状未だそうした動きは始動したばかりであり、課題は多い。

それぞれの組織においては、今後組織内で総合的に責任を持つ者が明確化されることが望まれる。組織はそうした人材を育成し、権限を与え、理解をもって従うことが重要である。今後CIO（Chief Information Officer）のみならず、CISO（Chief Information Security Officer）といった役職が、ＣＦＯ（Chief Financial Officer）などと同様に組織運営にとって重要な役割を果たし、広く認識されてその地位が確立されることが望まれる。

情報セキュリティ教育事業者、専門機関においては、専門人材育成の充実のみならず、事件・事故が発生した場合の対応など実践的な教育サービスの充実が望まれる。情報セキュリティを含むIT分野は革新スピードが速く、組織内での人材育成には限界があり、外部機関の役割は大きい。現在その情報セキュリティ教育市場は創成期であろうが、組織において情報セキュリティ教育に関する意欲は高いという調査結果も見られ、今後の充実・発展が望まれる。併せて認知度を高めるための普及啓発も重要な課題である。

リスクが拡大し、変質する「時代の節目」といえる現在、情報セキュリティ対策はこれまでのようにユーザの自己責任、努力だけでは十分に行えない。これは国家的課題であり、国として統一的な取り組みを行っていく必要がある。政府としては、関係府省庁が統一的な施策を講じ、民間部門と緊密に連携をとりながら社会全体としてのセキュリティレベルの向上を目指し、安心・安全な高信頼性社会の構築されることを期待したい。

（参考）検討の経緯

第１回：２００３年１０月１日
１．情報セキュリティ教育に関する論点と現状の整理
２．既存の教育コースのカリキュラムと資格認定制度のスキル要件
３．情報セキュリティ関連の施策について

第２回：２００３年１１月２０日
１．各委員からの情報セキュリティ教育に関するコメント
２．WG 検討結果の報告
３．今後の作業の方向性について

第３回：２００４年1月２１日
１．第二回研究会以後の委員コメント
２．WG 検討結果の報告
３．提言骨子の検討

第４回：２００４年2月２５日
１．報告書（案）について