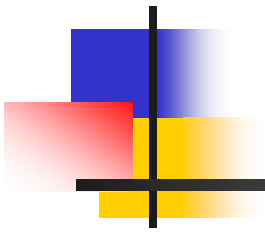


第３章　電気通信事業における
情報セキュリティマネジメント

３．１　電気通信事業における情報セキュリティマネジメントの必要性

情報セキュリティマネジメント

国際標準化機構（ＩＳＯ）と国際電気標準会議（ＩＥＣ）とが共同で設立している技術委員会（ＪＴＣ１）が、２０００年１２月に策定した国際規格（ＩＳＯ／ＩＥＣ１７７９９）があり、これを基に、一般の企業を対象とした汎用的な情報セキュリティマネジメントシステム（ＩＳＭＳ）とその適合性評価制度の整備･展開が、各国で進んでいる。

テレコム分野では

自らの電気通信設備をユーザの通信の用に供する電気通信事業者は、「通信の秘密」に属する情報を始めとして多くのユーザ情報を取り扱うものであり、情報資産をより適切に管理することが求められること等から、関係法令をも踏まえた電気通信事業に固有のＩＳＭＳが必要。

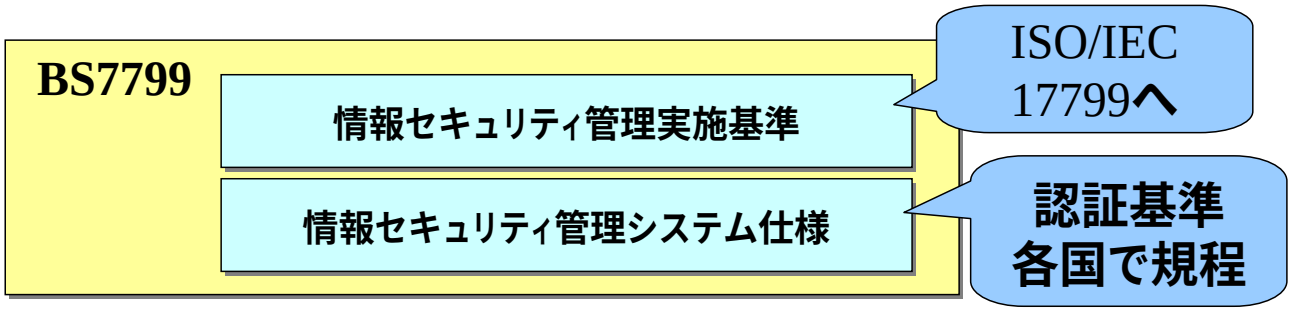
ITUで策定されたISMS-T（X.1051）の国内規格化が必要

３．２　　ＩＳＭＳの概要と最近の改訂作業の動向
３．２．１　ＩＳＭＳの概要

○ ISO/IEC17799では、情報セキュリティマネジメントに影響のある127の管理策（Control）を、次の10のマネジメント領域に分類している。

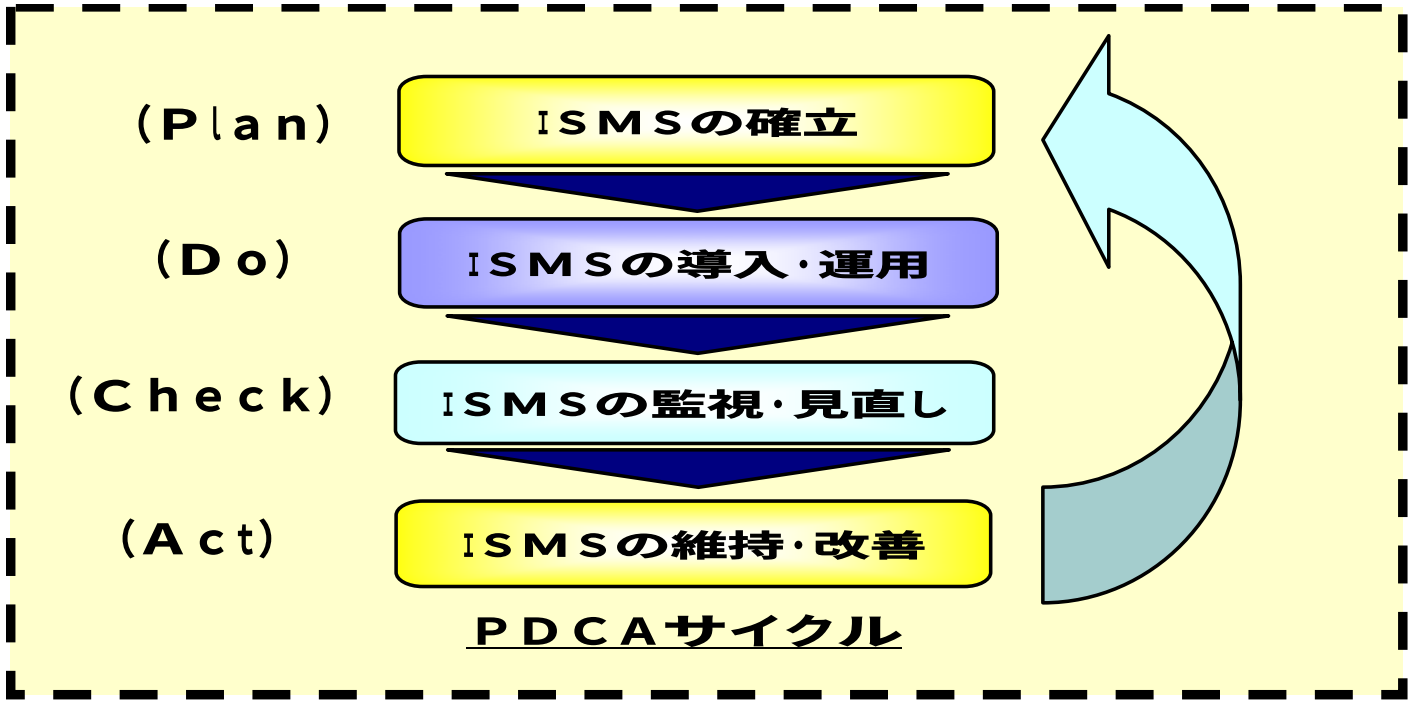
▽　ＩＳＭＳ（ＩＳＯ／ＩＥＣ１７７９９）のマネジメント領域

１．セキュリティ方針（Security policy）
２．セキュリティ組織（Security organization）
３．資産の分類及び管理（Asset classification and control）
４．人的セキュリティ（Personnel security）
５．物理的及び環境的セキュリティ（Physical and environmental security）
６．通信及び運用管理（Communications and operations management）
７．アクセス制御（Access control）
８．システムの開発及び保守（Systems development and maintenance）
９．事業継続管理（Business continuity management）
10．適合性（Compliance）



３．２．２　ＩＳＭＳ適合性評価

各国で実施されているＩＳＭＳ適合性評価は、評価対象となる組織が、ＩＳＭＳを確立し（Plan）、導入・運用し（Do）、監視・見直しを行い（Check）、維持・改善を行う（Act）というＰ－Ｄ－Ｃ－Ａサイクルを実施していることを、第三者（審査機関）が評価する、という形で実施されており、評価は企業単位ではなく、組織（事業所）単位で行われている。



すなわち、第三者の審査は、組織の中でＰ－Ｄ－Ｃ－Ａサイクルが適正に実施されているか否かを評価するものであり、組織内において一定水準以上のセキュリティ対策が実施されていることを保証しているものではない点に、留意する必要がある。

３．２．３　ＩＳＭＳの改訂作業の動向（１）

２０００年１２月に策定されたＩＳＯ／ＩＥＣ１７７９９（以下「２０００年版」）は、２００１年から改訂作業が開始され、１３５の管理策と１１のマネジメント領域から成る改訂ISMS（以下「２００５年版」）が、２００５年の後半には発行されるものと想定されている。

▽　２０００年版と２００５年版の規定の比較

２０００年版	２００５年版
セキュリティ方針	Security policy
セキュリティ組織	Organising information security
資産の分類及び管理	Asset management
人的セキュリティ	Human resources security
物理的及び環境的セキュリティ	Physical & environmental security
通信及び運用管理	Communications & operations management
アクセス制御	Access control
システムの開発及び保守	Information systems acquisition, development and maintenance
	Information security incident management
事業継続管理	Business continuity management
適合性	Compliance

マネジメント領域の追加

３．２．４　ＩＳＭＳの今後の課題

	概要
(1) 産業分野別の ＩＳＭＳの策定	守るべき情報やマネジメントの対象となる資産は、産業分野ごとに異なるものであり、各業界の特性によっては、その業界に固有のISMSを策定することが望ましいと考えられる。実際、医療分野についてはISO／IEC27799が、金融分野についてはISO／TC68が、**電気通信分野についてはITUにおいてISMS－T**が、それぞれ策定されている。
(2) ISMSの確立・ 運用に対する 支援	ISMSを確立し、運用しようとする組織が直面しがちな次の課題について、情報を共有し、課題解決に向けたガイドライン作り等の支援活動を行っていくことも必要になるものと考えられる。 ① 組織内の情報セキュリティのための体制 ② 社員の教育訓練 ③ 内部監査 ④ 個人情報保護等、法制上の要請への対応 ⑤ 技術上の対策との連携や技術上の対策の適用方法 こうした支援活動も、業界の特性に応じて、業界別に行うことが適当であろう。
(3) 国際的なクロス ボーダー認証の 実現	ISMSは国際規格であることから、ある国でISMSに適合していると評価された組織は、本来、他国においても同様に評価されるべきものであり、こうした国際間の認証の仕組みを構築することも、今後の課題になるものと考えられる。

３．３　　ＩＳＭＳ－Ｔの概要と今後の改訂の方向性
３．３．１　ＩＳＭＳ－Ｔの概要（１）

○ITUでは、２００１年以来、我が国が中心となって検討を進め、２００４年7月に電気通信分野を対象としたISMS（ISMS－T＜X．１０５１＞）を勧告。

○このＩＳＭＳ－Tは、電気通信システム及び電気通信サービスを対象としてＩＳＭＳを実装していくに当たっての要求条件を規定しているもの。

▽　ＩＳＭＳ－Ｔで管理策が追加されているマネジメント領域

３．資産の分類及び管理（Asset classification and control）
５．物理的及び環境的セキュリティ（Physical and environmental security）
６．通信及び運用管理（Communications and operations management）
７．アクセス制御（Access control）
８．システムの開発及び保守（Systems development and maintenance）

３．３．１　ＩＳＭＳ－Ｔの概要（２）

○汎用的なISMSと比べると、変更を加えていない管理策 (Control) についても、電気通信分野に固有の実装要件をImplementation Requirementsとして定めている。

資産の分類及び管理（Asset classification and control）

管理策（Control）

それぞれの資産を明確に識別しなければならない。また、全ての重要な資産について目録を作成し、維持しなければならない。

ＩＳＭＳ－ＴとＩＳＭＳとで変更無し

電気通信分野に於ける実装要件（Implementation requirements for Telecom）

各電気通信事業者に関係する重要な資産について目録を作成し、維持すること。以下の者が含まれる。

ａ）交換設備資産
ｂ）伝送設備資産
ｃ）運用設備資産
ｄ）電気通信サービス資産
ｅ）人々とその資格と能力
ｆ）組織の評判やイメージといった無形資産

電気通信分野に固有

３．３．２　ＩＳＭＳ－Ｔの今後の改訂の方向性　（１）

○現行のISMS－Tは、2000年版のISMSを踏まえてITUで勧告化されたもの
○2005年版が今年後半にも発行されると想定されていることから、今後、ISMS-Tの充実を図っていく際には、2005年版を参照しつつ、抜け落ちている点や修正等すべき点がないかどうかを精査すべきであると考えられる。

ISMS（2000年版・2005年版）とISMS－Tの管理策の比較

２０００年版 ＩＳＭＳ	２００５年版 ＩＳＭＳ	ＩＳＭＳ－Ｔ
セキュリティ方針	Security Policy	
セキュリティの組織	Organizing information security	Organizing Information security
資産の分類及び管理	Asset management	Asset management
人的セキュリティ	Human resources security	Human resources security
物理的及び環境的セキュリティ	Physical & environmental security	Physical & environmental security
通信及び運用管理	Communications & operations management	Communications & operations management
アクセス管理	Access control	Access control
システム開発及び保守	Information systems acquisition, development and maintenance	Information systems acquisition, development and maintenance
	Information security incident management	
事業継続計画	Business continuity management	
適合性	Compliance	

３．３．２　ＩＳＭＳ－Ｔの今後の改訂の方向性（２）

現行ISMS－Tへの追加項目の検討

現行のＩＳＭＳ－Ｔについても、例えば、「適合性」(Compliance) について、電気通信分野に固有の管理策は盛り込まれていない。

２０００年版のISMSや現行のISMS-Tには、規定されていないが、電気通信事業者には次のような法令上の要求事項があることから、今後、これらの要素を追加すべきか否かについて検討する必要がある。

① 通信の秘密の保護 (電気通信事業法第４条)

② 不当な差別的取扱いの禁止 (電気通信事業法第６条)

③ 重要通信の優先取扱 (電気通信事業法第８条)

④ 接続義務 (電気通信事業法第３２条)

⑤ 責任分解の明確化 (電気通信事業法第４１条及び５２条)

⑥ 個人情報保護法

以上のような法令上の要求事項は、「適合性」の領域だけでなく、その他の領域にまで影響を及ぼす可能性があることから、現行のＩＳＭＳ－Ｔをこうした観点から見直し、充実させていくことが求められる。

３．４　我が国における今後の活動の方向性

1．　ＩＳＭＳ－Ｔの国内規格化

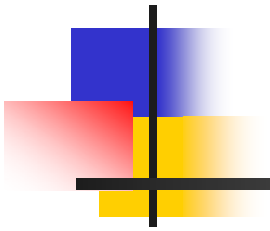
2．　国内規格の普及促進

○　国内規格を整備した後は、その国内規格に従って情報セキュリティマネジメントを行おうとする電気通信事業者が直面しがちな点について、情報の共有や課題解決に向けたガイドライン作り等の支援活動を行っていくことが求められる。

3．　国内規格の国際展開

○　今後、国際機関に積極的に提案を行い、日本発の国際規格化を図ることは、大きな意義を有するものである。そのために、国際的に評価される国内規格を策定することが必要であり、官民の知見を結集して、国内規格の策定に早急に取り組むべきである。

２００５年秋のＩＴＵの会合では、ＩＳＭＳ－Ｔの修正勧告の検討が開始される可能性があり、その時までに我が国で何らかの検討成果が取りまとめられることが期待される。

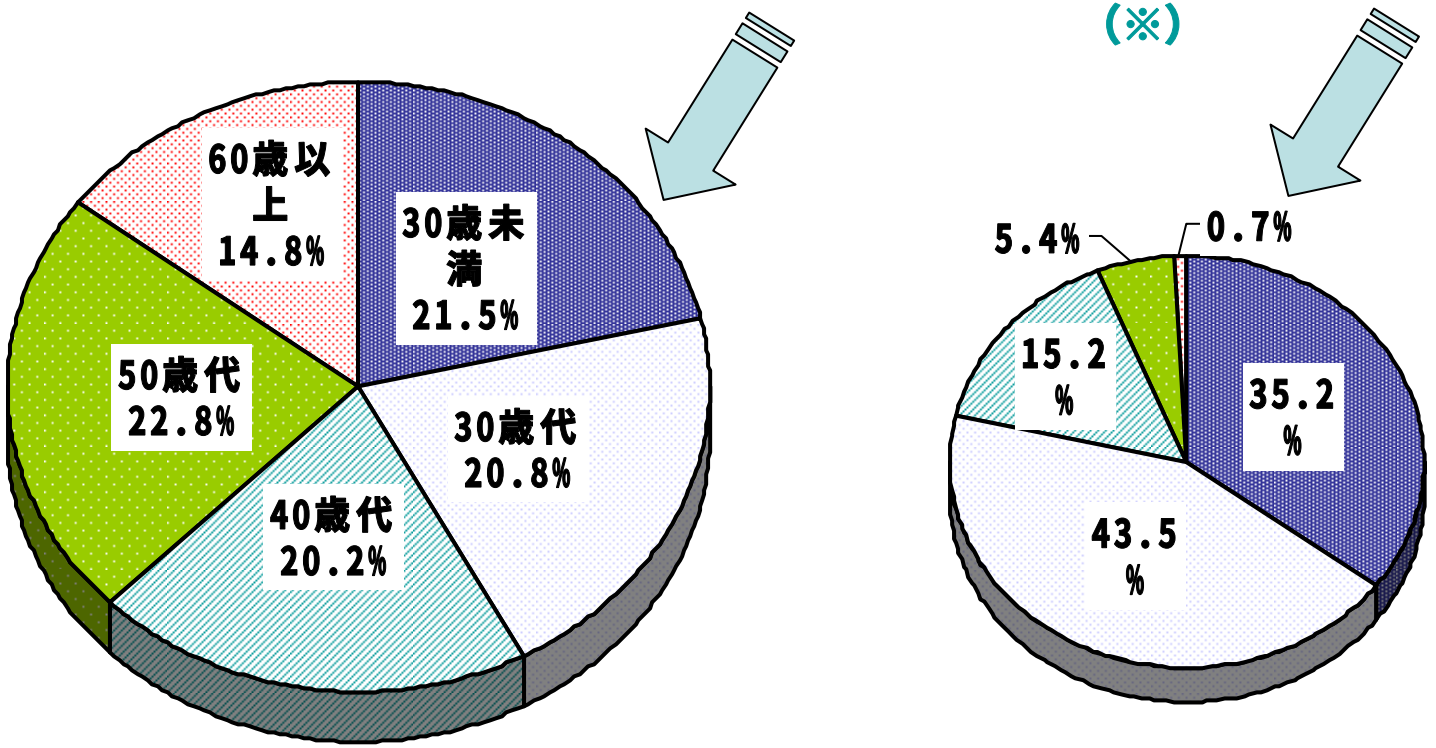


第４章　セキュリティ人材育成

４．１　　わが国におけるセキュリティ人材の現状
４．１．１　労働市場における情報処理技術者の「供給」面

- **就業人口が高齢化し、かつ減少する中で情報処理技術者については30歳代以下が約８割を占めているのが実態。**
- **若年就業者の減少が，情報処理技術者の絶対的な不足をもたらす恐れ。**

総人口　12,744万人　＞　有業者　6,501万人　＞　情報処理技術者　92万人（※）

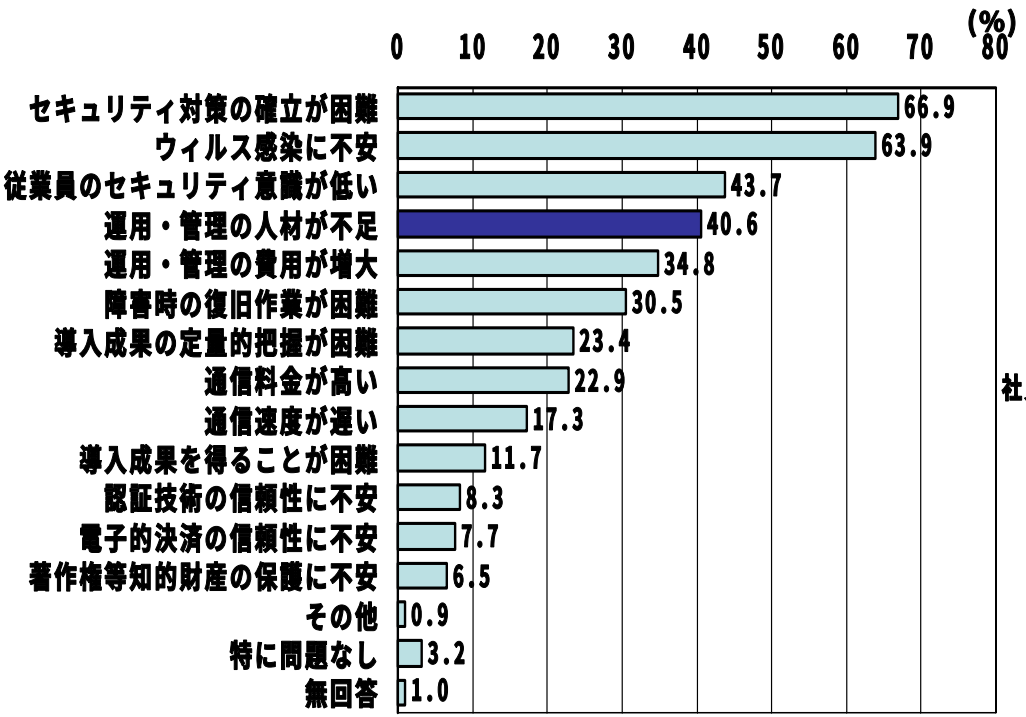


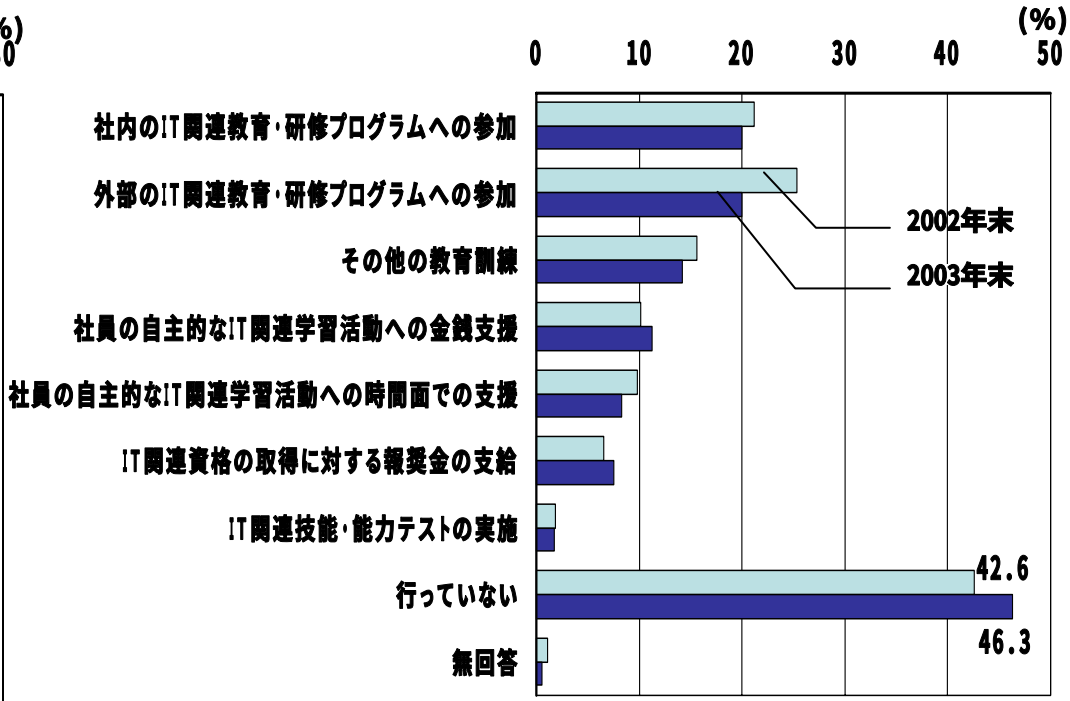
※　情報処理技術者：情報処理技術に関する高度の専門的知識・経験をもって，システムの分析，設計の仕事に従事するもの及びプログラムの設計，作成についての技術的な仕事に従事するもの

（出典）総務省「就業構造基本調査」及び「推計人口」より加工（平成14年10月）

４．１．２　労働市場における情報処理技術者の「需要」面（１）

▶ 企業ユーザに対するアンケートでは、従業員のセキュリティ意識の低さや人材不足が懸念事項として挙げられているが、それにもかかわらず社員に対するセキュリティ教育を行っていない企業が４割を超えている。





（出典）総務省「通信利用動向調査」（平成15年）

４．１．２　労働市場における情報処理技術者の「需要」面（２）

▶ ２００３年時点で、セキュリティに従事することのできる上級・中級のICT人材は、１２万人不足

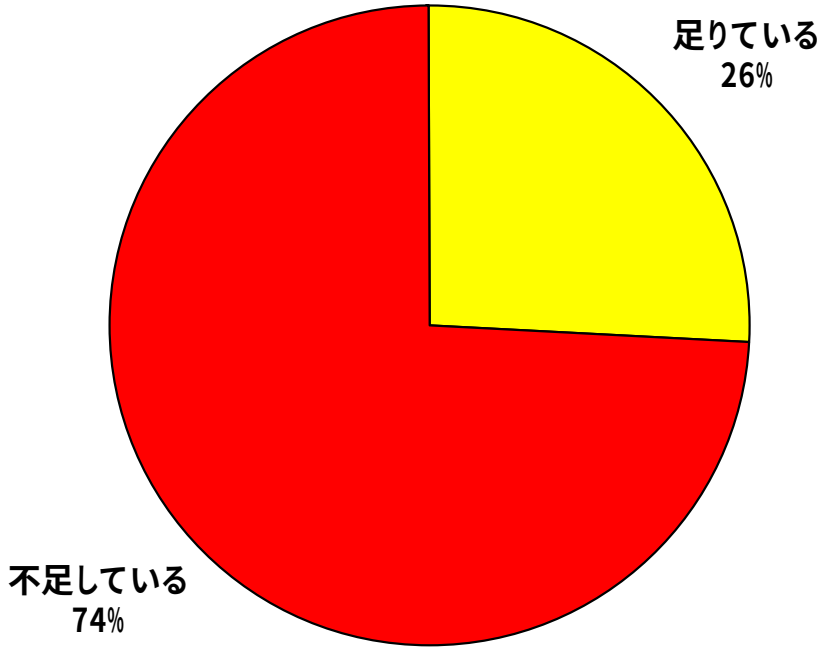
	所要数	現存数	不足数
上級人材	36万人	10万人	26万人
中級人材	92万人	76万人	16万人
セキュリティ人材 （上級・中級の中に含まれる）	25万人	13万人	12万人
プロジェクトマネージャー・ITアーキテクト・CIO （上級の中に含まれる）	10万人	1万人	9万人

※　ＩＣＴ人材（上級人材、中級人材、セキュリティ人材）の現状について、平成15年に総務省で開催された「情報通信ソフト懇談会」の人材育成ＷＧにおいて推計。また、プロジェクトマネージャー、ＩＴアーキテクト、ＣＩＯの３類型の人材の現状についても同ＷＧの主要メンバーの意見を踏まえ、同様の手法により推計。

※　上級人材：専門的な知識、技能を一通り備える。複雑なシステム等の設計及び運用が可能。
　　中級人材：特定分野の基本的な知識、技能を備える。比較的容易なシステム等の設計及び運用が可能。

４．１．３　電気通信事業者におけるセキュリティ人材の現状（１）

電気通信事業者に対するアンケート結果(注1)によれば、<u>７４％の事業者</u>において、セキュリティ人材(注2)が不足



＜有効回答１９７社＞

(注1)　総務省が２００５年4月に、(社)電気通信事業者協会、(社)テレコムサービス協会、(社)日本インターネットプロバイダー協会、及び(社)日本ケーブルテレビ連盟の加盟事業者に対して実施したアンケート

(注2)　ウィルスチェック、コンテンツフィルタリング、不正アクセス監視、セキュリティ診断、リモートアクセス環境検査等のセキュリティサービスをユーザに対し提供できる従業員のほか、自社のネットワーク運用の障害予防、当該障害の監視･検出･制御、障害の再発防止等を講じることのできる従業員を想定

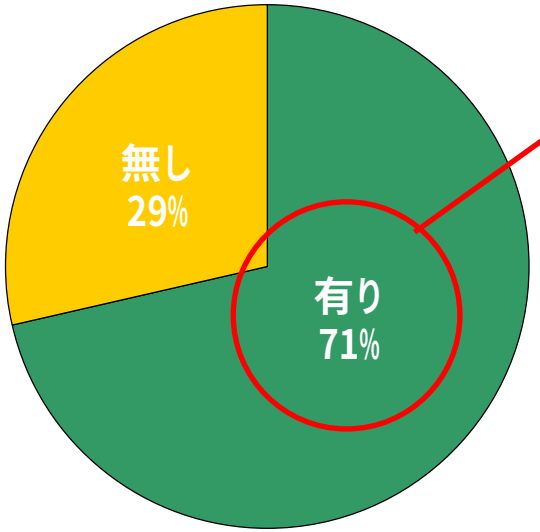
４．１．３　電気通信事業者におけるセキュリティ人材の現状（２）

○　3割の事業者は、社員のセキュリティ教育を実施していない

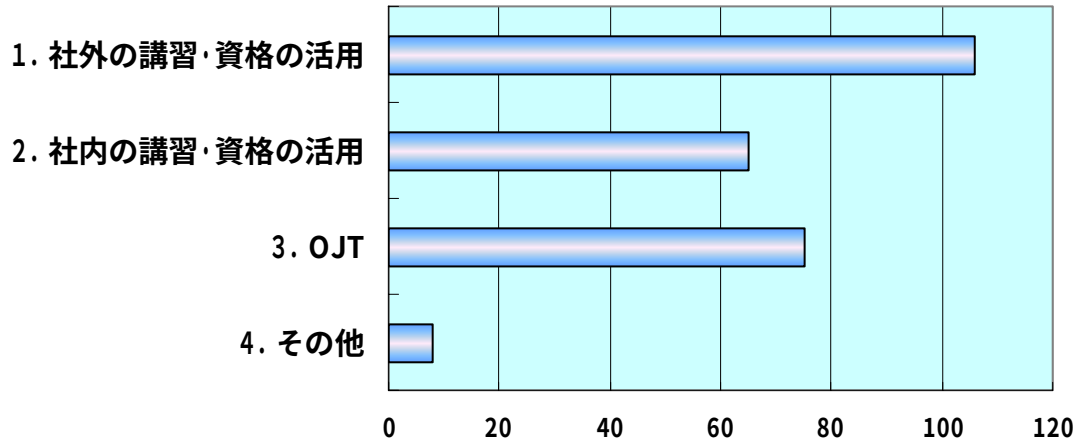
○　社員に対するセキュリティ教育を実施している事業者では、**社外の講習・資格の活用**やOJTの割合が大きい

【電気通信事業者のセキュリティ教育の実施状況】

＜有効回答197＞



【電気通信事業者のセキュリティ教育の実施状況】



４．１．３　電気通信事業者におけるセキュリティ人材育成の課題

セキュリティ技術･知識面の課題

① **実際のネットワーク運用やシステム構築に従事していないと、「生きた」技術の修得が見込めない**

② **インターネットの分野は技術革新が激しく**、それに応じて対応を要するセキュリティ事案も多様化しており、**社外の講習等で修得した技術だけでは対応できないインシデントが発生する場合が多い**

③ セキュリティ人材は、**技術から法令まで多くの技能･知識の習得が必要であり、その育成には多くの時間と高額の費用を要する**

ネットワーク運用･費用面の問題

① 自社のネットワーク運用において**中核を担う従業員を、社外の講習等にはとても参加させられない**

② **地方においてはセキュリティ講習が開催されていないことから**、地方で事業を展開している電気通信事業者にとっては、従業員を社外の講習会等に参加させようと思えば、**東京か大阪まで従業員を出張させなければならないことから、余計に費用がかかる**

セキュリティ技術･知識の評価に係る問題

○ **社外の講習等に自社の従業員を受講させたとしても、それによって得られるセキュリティ水準がどの程度か判定が難しい**。

４．２　　他のICT先進国におけるセキュリティ人材の現状と育成策
４．２．１　米国におけるICT人材数

米国商務省は、１９９９年に次の通り発表している。

① ＩＣＴ人材は、１９９６年から２００６年までの１０年間で、<u>１５０万人から２６０万人まで増加させることが必要</u>

② ＩＣＴ人材のうち、セキュリティ人材はComputer Scientistsに分類されており、１９９６年から２００６年までの<u>１０年間で、２５万人弱のComputer Scientistsの増加が必要</u>

表　米国のICT人材数

米国商務省発表資料（１９９９年）

単位：千人

	1996年	2006年	Change, 1996-2006		
			Net Replacements	New Jobs	Total Growth
Computer Scientists	212	461	19	249	268
Computer Engineers	216	451	15	235	250
Systems Analysts	506	1,025	34	520	554
Computer Programmers	568	697	177	129	306
Total	**1,501**	**2,634**	**244**	**1,134**	**1,378**

http://www.technology.gov/Reports/TechPolicy/digital.pdf

４．２．２　米国におけるセキュリティ人材の育成策

○ **国家の情報インフラの脆弱性を低減するためのセキュリティ人材育成策として**、国家安全保障局（ＮＳＡ）(注1)において**ＣＡＥＩＡＥ**(注2)**と呼ばれる人材育成プログラムを実施**

○ このプログラムには、４年生の大学生と大学院生が応募することができ、**国防総省の情報保証奨学金**(注3)**やＳＦＳ**(注4)**の奨学金制度への申請権が与えられる**。

ＣＡＥＩＡＥプログラム（ＳＦＳの奨学金を受けた場合）

対象	**４年生の大学生と大学院生**
対象期間	最大２年間
奨学金	**必要な全ての経費、書籍、授業料、部屋代など**
給付金	**大学生：年間最大**8,000**ドル** **大学院生：年間最大**12,000**ドル**
条件	奨学金受給期間又は１年のいずれか長い期間、**連邦機関に勤務**

（注1） NSA: National Security Agency
（注2） CAEIAE: The National Centers of Academic Excellence in Information Assurance Education
（注3）国防総省情報保証奨学金: Department of Defense Information Assurance Scholarship Program
（注4）SFS: Federal Cyber Service Scholarship for Service Program

４．２．３　シンガポールにおけるセキュリティ人材の育成策

○ シンガポール情報通信開発庁（IDA）において、**「重要な情報通信技術資産プログラム」（CITREP（注1））と呼ばれるICT人材育成のプログラムを推進**

○ このプログラムは、電気通信事業者や情報通信ネットワークを活用する組織が必要とする**情報システム（情報セキュリティを含む）に関する教育訓練又は資格取得の費用について、一定の助成を行うもの**

（注1）CITREP：Critical Infocomm Technology Resource Program

ＣＩＴＲＥＰの助成対象と助成上限額

助成対象	教育訓練を受け、又は資格を取得しようとする**個人等**
助成上限額	**教育訓練に係る費用の最大７０％（Ｓ＄3,500：約23万円）まで** **資格試験に係る費用の最大７０％（Ｓ＄1,000：約6.5万円）まで**

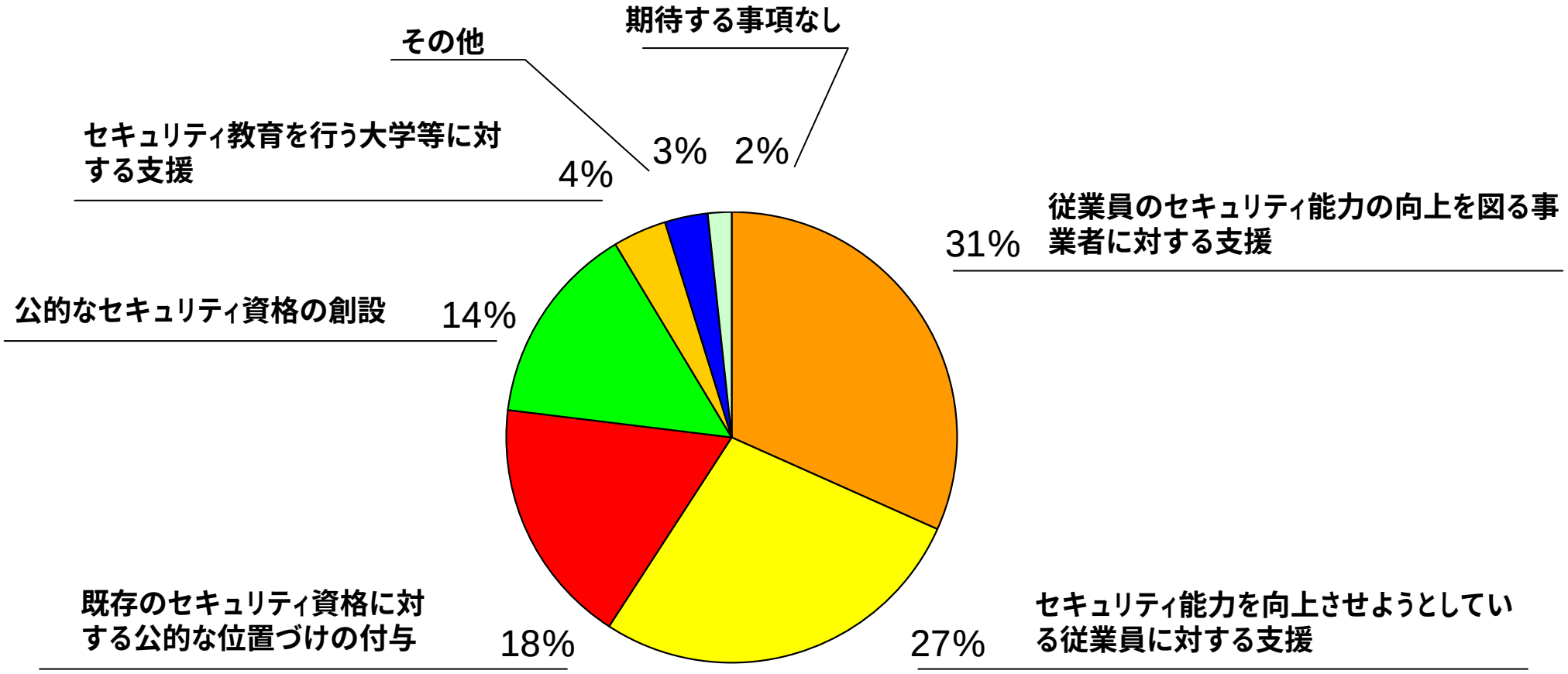
ＣＩＴＲＥＰの対象資格試験例（情報セキュリティ関係：一部分）

CISSP CBK Review Seminar	Security Certified Network Professional (SCNP)
Check Point Certified Security Administrator & Certified Nokia Security Administrator - ECS (VPN-04)	Security Technology and Management Course (eSTEEM)
Computer Hacking Forensic Investigator	Sun Certified Security Systems Administrator - IM
CSPFA CISCO Secure PIX Firewall Advanced	Sun Certified Security Administrator for the Solaris Operating Environment - ECS (SC-300)
Developing Secure Internet Applications	Sun Network Intrusion & Detection - ECS (SC-345)
eXtreme Hacking	Ultimate Hacking
Linux Network Administration and Security	Web Application Security Training
Securing Cisco IOS Networks	

○ アンケート結果によれば、セキュリティ人材育成に係る政府の支援策として、セキュリティに関する講習や資格に関して、費用面での助成や公的な位置づけを求めるものが多い。

【セキュリティ人材育成に係る政府支援策の期待】

＜有効回答１９７社＞



４．３．２　既存のセキュリティ講習等に対する評価

セキュリティ講習等については、民間企業によるものと公的なものとを問わず、すでに多くのものが存在。

これらのうち、インターネットの分野においては、どれが有用かを評価する際の基準を示すことの方が有効と考えられる

○　資格や認定の効果が有効期限付きのもの

○　実機を使った演習があるか

○　技術だけでなく、管理・運用、法制度についても講習があるか

セキュリティ人材の育成に当たっては、「技術」のみならず、「管理・運用」や「法制度」についても“三位一体”で知識を習得させることが必要

セキュリティ講習等の例

略称、通称	正式名称	主催者	発足	期限	取得形態、教育時間	取得費用
NISM	Network Information Security Manager ネットワーク情報セキュリティマネージャー	NISM推進協議会 （CIAJ、ﾃﾚｻ協、TCA、ARIB、JAIPA、ﾃﾞ協、NS協、TTCで構成）	2001	2年	「講習+認定試験」のみ （講習は2日間と3日間（コースによる））	■ ネットワークセキュリティ基礎（69,300円／63,000円） ■ ネットワークセキュリティ実践（173,250円／157,500円） ■ サーバセキュリティ実践（184,800円／168,000円） ■ セキュリティ監視実践（184,800円／168,000円） ■ セキュリティポリシー実践（80,850円／73,500円） ■ セキュリティ監査実践（80,850円／73,500円） ※　金額は一般価格／会員価格
SS	情報セキュリティアドミニストレータ試験	（財）日本情報処理開発協会（～2003/12） （独）情報処理推進機構（2004/1～）	2001	なし	「認定試験」のみ	5,100円（受験料）
CISSP	Certified Information System Security Professional	International Information Systems Security Certification Consortium, (ISC)2	1989	約120時間／3年間の教育単位取得が必要	「講習+認定試験」「認定試験」のいずれも可。 講習は8時間×5日	630,000円（受講料（受験費用込み）） 68,500円（試験のみの場合）
Security+	Security+	The Computing Technology Industry Association, CompTIA	2003	なし （試験内容は2年で改訂）	「講習+認定試験」のみ 講習は6日間	504,000円（受講料（受験費用込み）） 28,665円（試験のみの場合）
CISM	Certified Information Security Manager 公認情報セキュリティマネージャー	Information Systems Audit and ControlAssociation, ISACA（情報システムコントロール協会）	2002	5年	「認定試験」のみ　ただし、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）	505ドル
CSBM、CSPM (Technical, Management)	Certified Security Basic Master（情報セキュリティ技術認定［基礎コース］） Certified Security Professional Master（情報セキュリティ技術認定［応用コース･テクニカル編／マネジメント編］）	Security Education Alliance / Japan, SEA/J	2000	なし	「講習＋認定試験」「認定試験」のいずれも可。	■ 基礎コース（受講＋受験料99,750円／受験のみ15,750円） ■ 応用コース･テクニカル編（受講＋受験料204,750円／受験のみ15,750円） ■ 応用コース･マネジメント編（受講＋受験料141,750円／受験のみ15,750円）
GIAC	Global Information Assurance Certification	SANS Institute	2002	2～4年（受講分野による）	「講習＋認定試験」「認定試験」のいずれも可。 講習は各6日間	受験費用63,000円 （トレーニングとの同時申込みの場合は、受験費用は31,500円。別途受講料が必要。）

※HP等を参考に作成

４．３．３　既存のセキュリティ講習等の例　～ＮＩＳＭ～

NISM創設の背景

NISMは、2000年に郵政省で開催された「電気通信事業におけるサイバーテロ対策検討会」の報告書を受けて、2001年に創設された人材育成プログラム。

NISMの目的

ハッカーや不正アクセス、コンピュータウィルスなどから、情報通信ネットワークとそのユーザを防御するための専門知識を持つ技術者を育成。

認定の付与

このNISMでは、講習を受講して、講習最終日に実施される試験に合格した者に、NISM推進協議会(注)より「認定」が与えられる。

(注) NISM推進協議会構成団体：(社) 電気通信事業者協会、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) 電波産業会、(社) 日本インターネットプロバイダー協会、(財) 日本データ通信協会、(社) 情報通信技術委員会

NISMの特徴

① 2年間の有効期限があり、更新試験により、資格を更新。

② 実機を用いた実践的な演習。

③ 技術のみならず、管理･運用、法制度についても講習を実施。

ＮＩＳＭ資格体系

MIC
Ministry of Internal Affairs and Communications

総 合 ス キ ル

IPやOS等の基本知識（事前確認のレベル）はあるものの、セキュリティに関する業務経験や関連知識が少ない方向けのレベル。【NISM基礎ｺｰｽ】

基礎コースを修了、または修了と同等のレベルを有する方で、セキュリティシステムの構築を体験したい方向けのレベル。【NISM資格ｺｰｽ】

専 門 ス キ ル

NISM資格（ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ実践）認定者レベル、もしくはセキュリティシステムの構築体験がある方を対象に、より専門的なスキル（ｻｰﾊﾞ構築、ｾｷｭﾘﾃｨﾎﾟﾘｼｰ策定、ｾｷｭﾘﾃｨ運用、ｾｷｭﾘﾃｨ監査）の習得を目指す方のためのレベル。【NISM専門ｺｰｽ】

情報セキュリティ技術

①ネットワークセキュリティ基礎＜2日間＞
（年間5回程度実施予定）
【会員価格　63,000円】（一般は　69,300円）
ネットワークセキュリティ全般にわたる概要や動向・基礎知識などを修得するコース。

②ネットワークセキュリティ実践＜3日間＞
（年間5回程度実施予定）
【会員価格　157,500円】（一般は　173,250円）
自社のサイトを防御するため、ファイアウォール、VPN、認証、ワクチンソフトなどのサイトセキュリティに必要な道具の使いこなしと、多様化したハッキングからのサイトセキュリティを実現する方法を習得するコース。
※受講生のニーズが増大している無線LANのセキュリティを講義＋実習の形態で平成16年度から追加。

③サーバセキュリティ実践＜3日間＞（〃2回〃）
【会員価格　168,000円】（一般は　184,800円）
サイト内の具体的なホストの安全性を高めることを追求する。各種OS（UNIX、Linux、Windows）を使用し、安全なMail、Web、DNSサーバなどの構築方法や、各々を構築する上でのポイントを習得するコース。

④セキュリティ監視実践＜3日間＞（〃2回〃）
【会員価格　168,000円】（一般は　184,800円）
様々な犯罪事象を想定しつつ、ケーススタディを繰り返すコース。その中でどのような防御方法が適切であるのか、また日常の運用監視作業として、どういったものが望ましいのかを習得するコース。
※高度なレベルが要求されるIDS設定やシステムログ解析を主な内容とする。

情報セキュリティ管理

⑤セキュリティポリシー実践＜2日間＞（〃2回〃）
【会員価格　73,500円】（一般は　80,850円）
セキュリティポリシーの構築を目的としたコース。国際標準であるISO15408やBS7799規格の動向や解釈、構築の基本的な知識も習得するコース。

★平成16年度新設★
⑥セキュリティ監査実践＜2日間＞（〃2回〃）
【会員価格　73,500円】（一般は　80,850円）
情報セキュリティ監査制度の概要と、その中心的なガイドラインである情報セキュリティ管理基準と情報セキュリティ監査基準の構成を理解し、演習を通じて、その効果的な活用方法を把握する。

※　価格は税込。　※　日程・講習会場等詳細はＮＩＳＭﾎｰﾑﾍﾟｰｼﾞを参照。【URL】 http://www.nism.jp

４．３．４　大学におけるセキュリティ人材育成

○ e-Japan戦略等の国家戦略においても、セキュリティ人材の育成は喫緊の課題

○ セキュリティ人材育成のため、一部の大学での取り組みが始まっている。

表　大学におけるセキュリティ人材教育

大阪大学	セキュア・ネットワーク構築のための人材育成
早稲田大学	セキュリティ技術者養成センター
中央大学	２１世紀ＣＯＥ　電子社会の. 信頼性向上と情報セキュリティ 情報セキュリティ・情報保証 人材育成拠点
工学院大学	セキュアシステム設計技術者の育成
情報セキュリティ大学院大学	修士課程　2004年4月開校
カーネギーメロン大学情報大学院	修士課程　2005年9月開校

○ 電気通信事業者が大学等の教育機関に期待する役割として、学生が卒業した後、すぐに電気通信事業の業務ができるように、基礎的かつ系統だったセキュリティ教育を施すことが求められている。

４．４　政府による支援策

○　セキュリティ人材の育成は、個々の電気通信事業者で対応すれば済むものではない。

○　サイバーテロなど、過去に経験したことのないようなＩＣＴ障害に際しては、個々の電気通信事業者と行政とが連携して万全の対策を講じることが求められる。

○　このため、例えば、インターネットの実網に近い環境のもとで、我が国を代表するセキュリティ専門家が最新の技術に基づく攻撃を実施し、これに対し、予防、制御、復旧の各側面に関するサイバーテロ演習等を、中小、地方のＩＳＰや情報家電機器のメーカをも巻き込む形で実施することも一案と考えられる。

○　こうした演習を通じて、演習に参加した事業者間でノウハウの蓄積と人材育成を行うとともに、電気通信事業者、情報家電機器ベンダー及び行政という業界の枠や官民の枠を超えて高度な技能を有する人材を育成することは、非常に有意義なことと考えられる。