第２章　ユビキタスネット社会における
セキュリティ確保

－情報家電のネットワーク接続に伴う課題－

２．１　ユビキタスネット社会におけるセキュリティ確保の必要性

第１章では、最近のネットワーク運用においてＩＳＰがどのようなインシデント事案に直面しているかについて、実情をレビューするとともに、今後の課題を整理した。

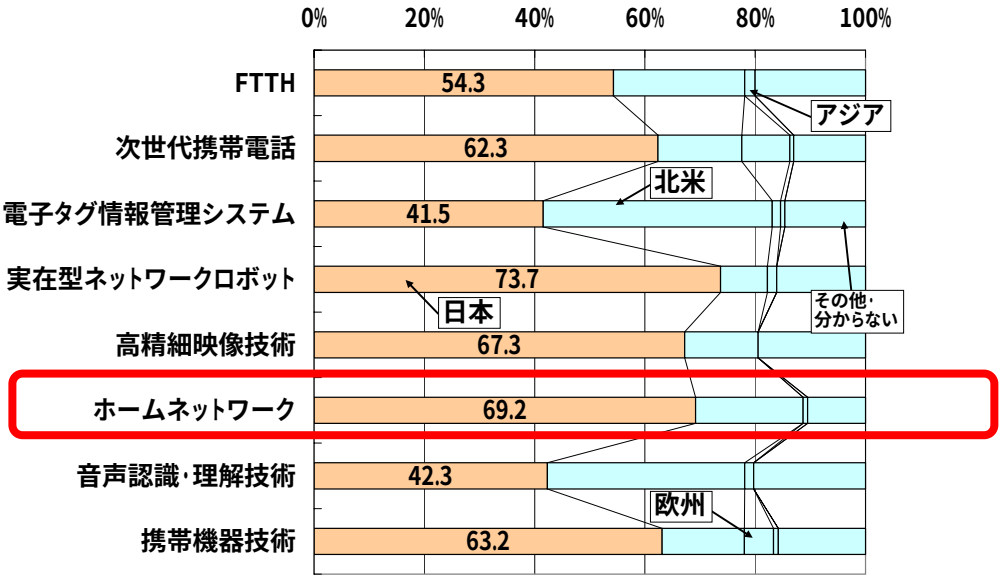
他方、我が国はブロードバンド通信の「安さ」と「速さ」において既に世界１の環境を実現し、２００４年１２月に総務省が取りまとめた「ｕ－Ｊａｐａｎ政策」では、２００１年1月のｅ－Ｊａｐａｎ戦略におけるキャッチアップ的な発想から脱却し、２０１０年には世界最先端（フロントランナー）のＩＣＴ国家として世界を先導することが目標とされている。

このｕ－Ｊａｐａｎ（ユビキタスネット・ジャパン）政策において、「いつでも、どこでも、何でも、誰でも」ネットワークに簡単につながる「ユビキタスネット社会」を実現することが必要不可欠な事項とされており、このユビキタスネット社会を支えるためにも、情報セキュリティの確保は重要な政策課題と言える。

すなわち、情報家電を含むあらゆる端末がネットワークにつながる「ユビキタスネット社会」を想定してセキュリティ確保に取り組んでいくことは、我が国がフロントランナーとして世界を先導していく上で不可欠であり、こうしたフロントランナーとしての取組みはセキュリティを含め、我が国のＩＣＴ産業の国際競争力を維持・強化する上でも重要と考えられる。

実際、情報家電を含むホームネットワークは、我が国が国際的に技術優位性を有すると考えられている分野であり、そのセキュリティ確保に向けた取組みは、ホームネットワークに関する我が国の国際競争力の維持強化に寄与するものである。

▽　情報通信技術の優位性に関する国際比較



※各技術の優位性について、情報通信技術者へのｱﾝｹｰﾄ調査）
（出典）ユビキタス社会の動向に関する調査

また、情報家電を始めネットワークにつながる端末が多種多様になることは、それによってサービスを提供するアプリケーション・サービス・プロバイダー（ＡＳＰ）、家電メーカ、ＩＳＰ等にとって新たなビジネス機会の創出につながるものと言える。

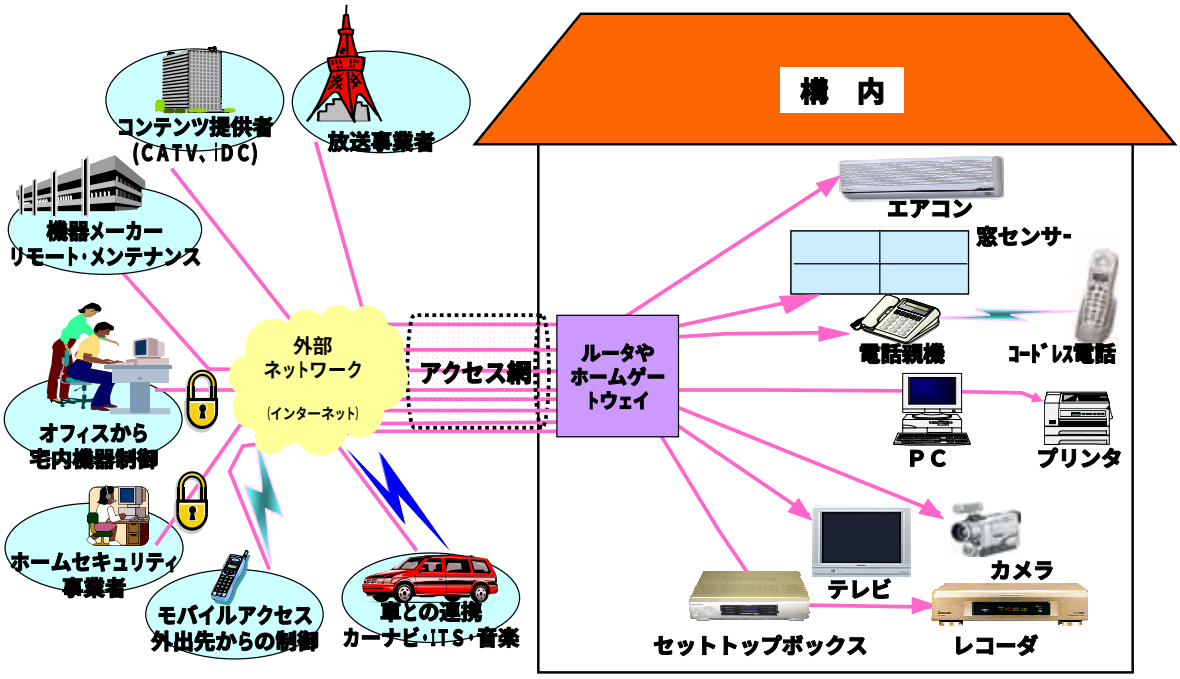
他方、家電業界やＩＳＰ業界の視点からではなく、消費者の視点からみると、家電がインターネットに接続され、通信機器として機能すると、情報セキュリティ上の問題も発生し得るということを認識していない消費者も多いと考えられるところであり、「誰でも、簡単かつ安全に」家電を利用できるようにするためのセキュリティ基盤を確立することが求められていると言える。

そこで、以下では、情報家電に焦点を当てて、そのネットワーク接続に伴うセキュリティ確保について検討する。

２．２　情報家電に対する期待と課題

「情報家電」とは、通信機能をもつ家電機器であり、ネットワークと接続することで、構内又は構外にある他の機器との通信を行い、構外からのサービスの利用や構内の機器の相互連携を可能にするものであり、「ユビキタスネット社会」の実現に寄与するものとして期待されている。

▽　情報家電の利用イメージ



▽　情報家電への期待

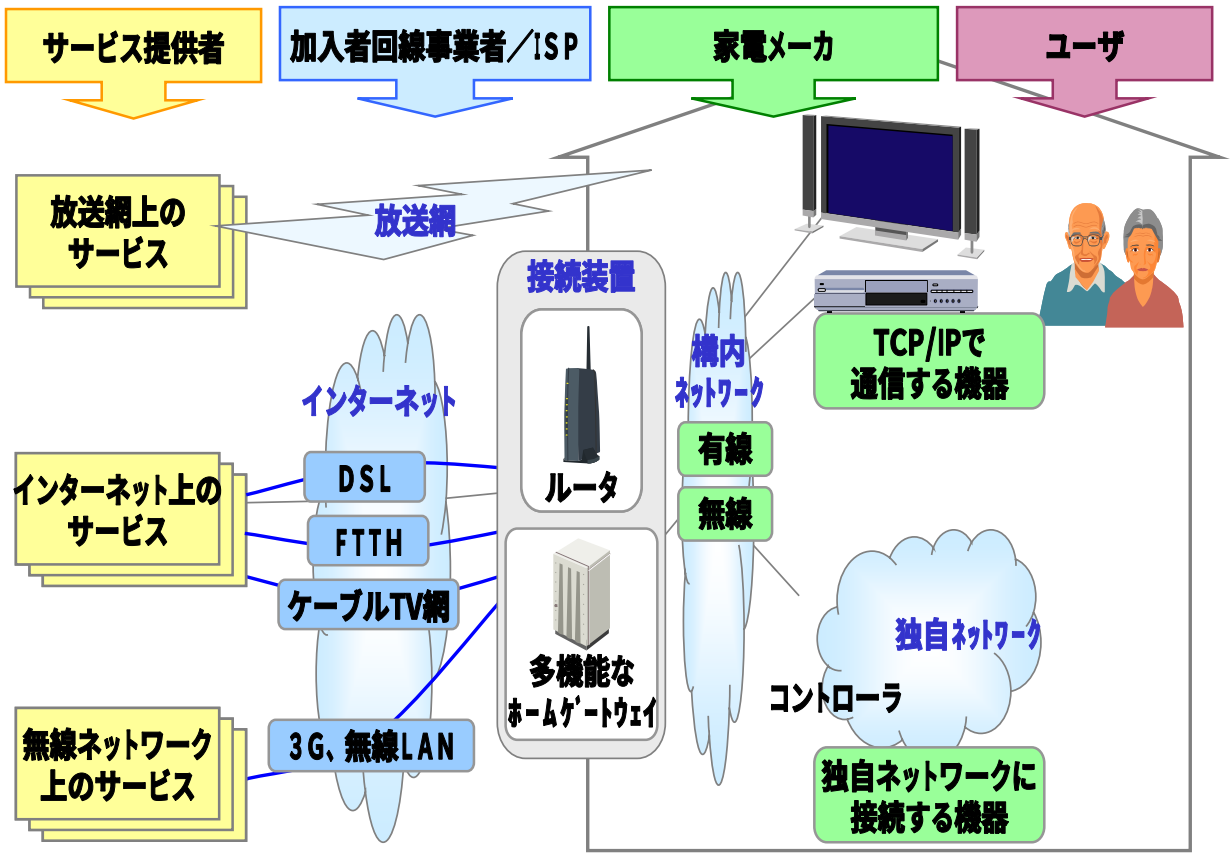
- 約1万人の調査→73%がネットワーク情報家電を使ってみたい
- 利用者の不安　①機器の価格②セキュリティ③サービス料金④使いこなせるか
- 機器価格は3千円～1万円アップ、サービス料金は300円/月ぐらいだと許容できる

機器の連携		宅外リモコン(機器連隔制御)	①エアコン ②VTR/DVD機器 ③風呂	69.9%	簡単・快適
		蓄積番組の視聴	好きなときに好きな番組が見られる(キーワード自動番組録画・リモート視聴)	54.6%	感動
		くらし安心	①ガス/火災 ②不審 ③部屋 ④照明 ⑤施錠	51.3%	安全・安心
サービス・機器の更新	TVによる情報提供	映像・情報配信	①BBサービス　②TV電話等	45.7%	感動
		地域情報や電子チラシの配信		39.7%	簡単・快適
		定点観測監視モニタ	①行楽地や道路/病院混雑状況 ②幼稚園	37.3%	安全・安心
		出かける前の情報確認	①天気 ②時刻表 ③乗換 ④地図等	34.8%	簡単・快適

2002年8月　松下電器調査

また、情報家電によるサービスには、家電メーカのほか、構内ルータ／ゲートウェイのメーカ、加入者回線（アクセス）網提供事業者、ＩＳＰと様々な事業者が関わるものであり、業種をまたがった連携や調整が、情報家電を定着させていく上で必要不可欠である。

▽　情報家電によるサービスに関わる様々な業種

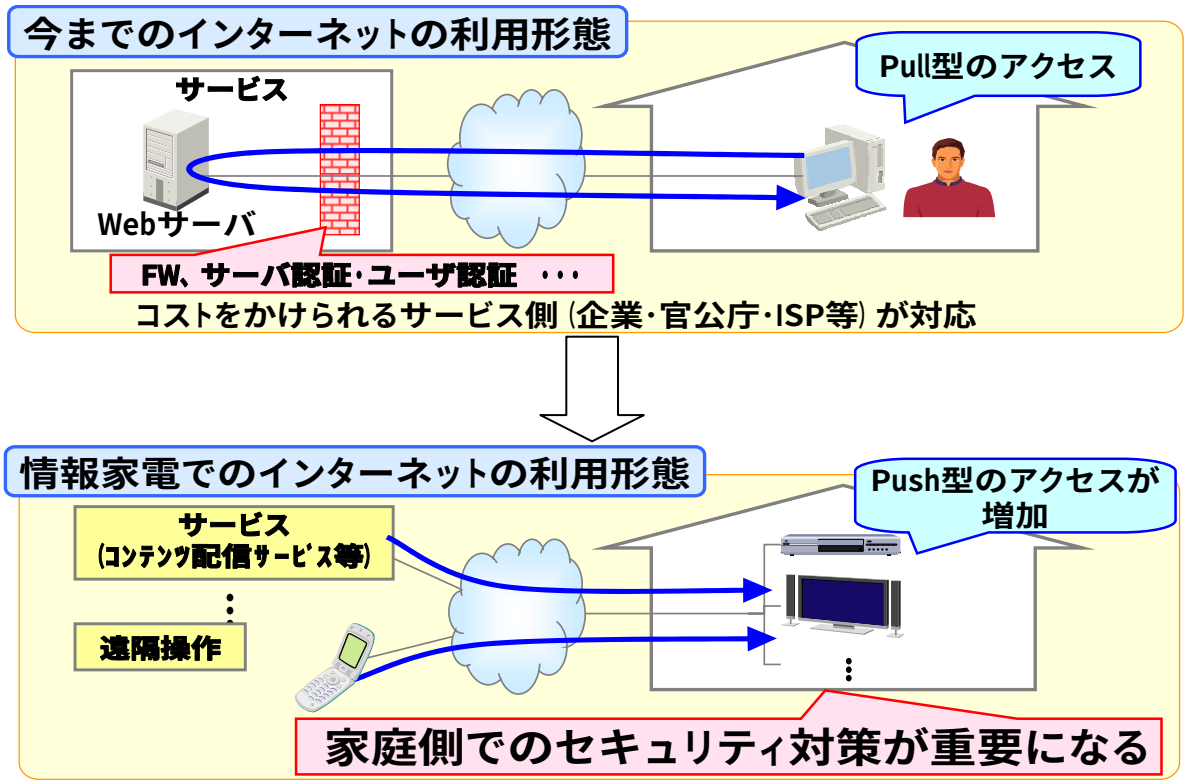


更に、情報家電によるインターネットの利用形態は、従来のインターネットの利用形態とは大きく異なる可能性がある点にも、留意しておくことが適当である。

すなわち、従来のクライアント・サーバ型のインターネットの利用形態においては、構内に居るユーザから構外のサーバにアクセスして情報を引き出してくる「Pull 型のアクセス」が主流であったが、情報家電によるインターネットの利用形態は、構外にいるユーザから構内の情報家電をコントロールしたり、サービス提供者が構内の情報家電に直接コンテンツを配信するなどの「Push 型のアクセス」が多くなると考えられるからである。

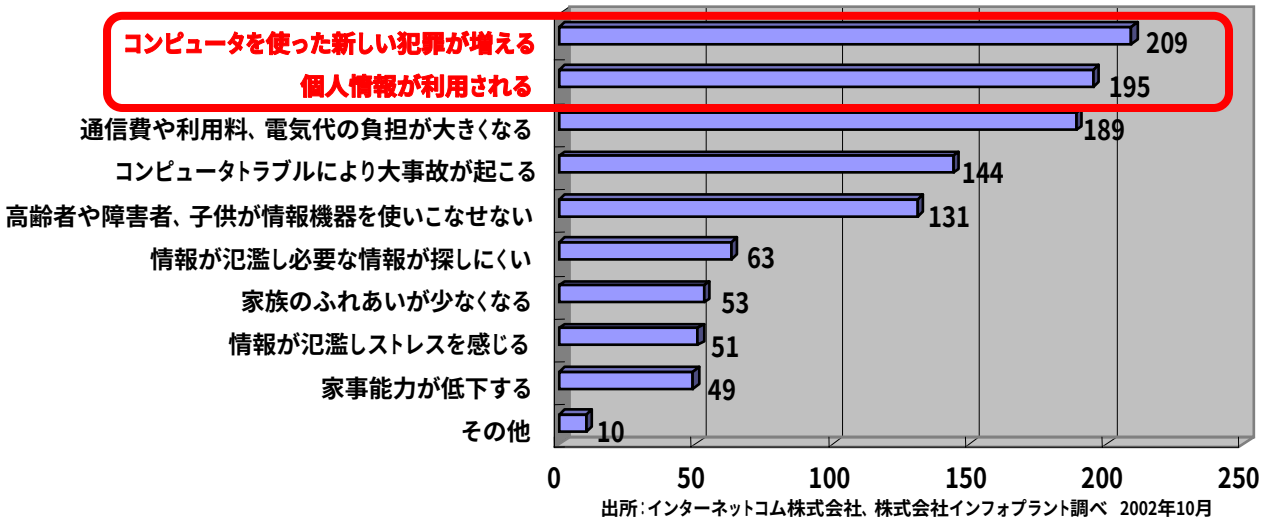
「Pull 型のアクセス」の場合、アクセスを受ける企業、官公庁、ＩＳＰ等において費用をかけてファイアウォールや認証機器を整備すれば良かったが、「Push 型」の場合にアクセスを受けるのは、構内にある情報家電であり、構内の情報家電側、すなわちユーザ側でセキュリティ対策を講じることが極めて重要になる。

▽　アクセス形態の変化とセキュリティ対策のリバランス



情報家電に関するユーザの意識を見てみても、セキュリティの確保が課題の上位に挙げられており、情報家電が普及する条件としてセキュリティ確保を図ることが重要となっている。

▽　情報家電とユーザの意識



実際、２００４年１０月には、

① 外部からユーザ名やパスワードの入力不要でアクセスできる設定になっていたＤＶＤレコーダが出荷され、外部からの不正アクセスにより、このＤＶＤレコーダを踏み台にして大量のスパム（無意味な電子データ）が送信されてしまう危険性が出荷メーカ自身から警告された事例や、

② 専用の接続装置でしか解除できない筈のケーブルテレビのスクランブル（視聴制限処理）を解除することのできる機器が出回った事例、

等、情報家電のセキュリティ事案が相次いで報道された。

そこで、次に情報家電のセキュリティ確保に関する課題を整理してみることとする。

２．３　情報家電のネットワーク接続に伴うセキュリティ上の課題

２．３．１　接続検証と規格化

そもそも、情報家電によるサービスの実現に当たっては、情報家電、構内ネットワーク、ゲートウェイ、加入者回線（アクセス）網、ＩＳＰ、アプリケーションサービス提供事業者（ＡＳＰ）というように、多段階にわたる接続検証を重ねる必要がある。

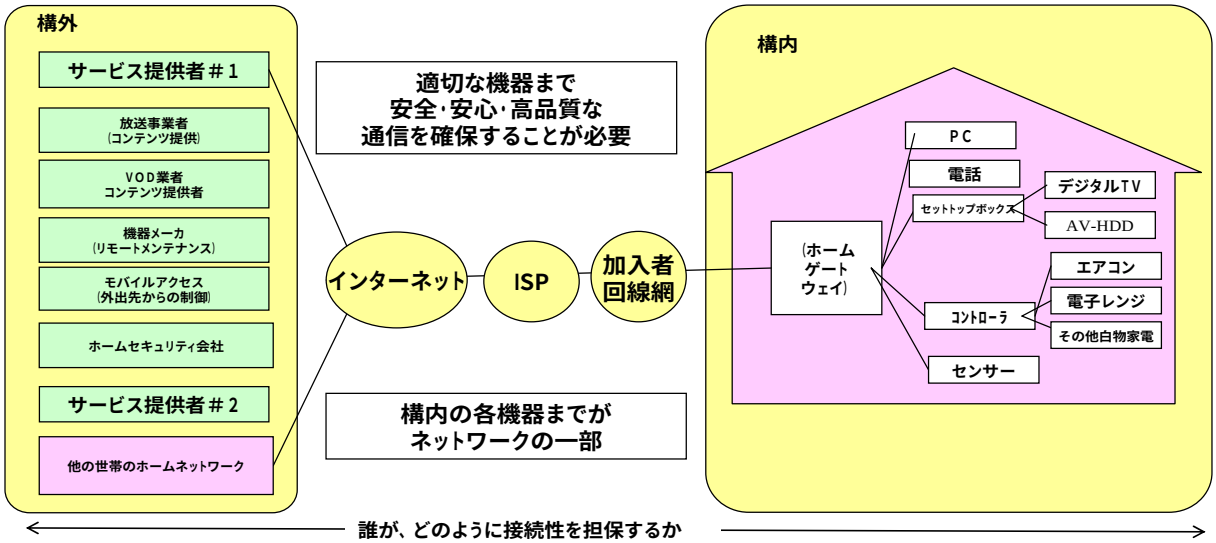
こうした接続検証を各社ごとに行うのでは、件数も無限大となり、非効率と考えられることから、業界の枠を超えて接続検証と相互利用可能な規格化を行うことが適当と考えられる。

その際、品質保証等の機能の提供方式のモデル化、接続に関する責任分界点の明確化、接続管理方式の策定等の作業も併せて行うことが望ましいと考えられる。

▽　接続検証

接続検証件数＝N × N × N × N × N × N × N ＝∞

(サービス提供者)　(ISP)　(加入者回線事業者)　(ｹﾞｰﾄｳｪｲ)　(宅内ﾈｯﾄ)　(IP情報家電)　(非IP情報家電)



２．３．２　情報家電がボット化した場合の対応

ＩＳＰからすれば、情報家電機器も、コンピュータと同様、ワームやボットプログラムに感染する可能性のある端末機器であり、情報家電機器がボット化した場合に、

①　当該情報家電機器との接続がＩＳＰの電気通信設備を損傷し又はその機能に障害を与えるとき、

②　当該情報家電機器との接続が他のユーザに迷惑を及ぼすとき、

等には、接続の停止やサービスの停止を行うことがあり得る旨を、予め約款又は契約で明確化し、ユーザに周知しておくことが必要である。

２．３．３　リモート・メンテナンスと機器認証

情報家電のセキュリティ確保を検討する際には、コンピュータについて講じられている以上のセキュリティ確保が情報家電には必要なのか否か、という観点から考察を加えてみることが有効である。

セキュリティ確保に関する課題について、コンピュータと情報家電の異同点を挙げてみると、下表のとおりである。

▽　セキュリティ確保におけるコンピュータと情報家電の異同

同じ点	違う点
①　コンピュータでは、Windows 等の汎用的なＯＳが多く利用されているが、情報家電においても機器固有のソフトウェアだけでなく Linux や TRON 等の汎用的なＯＳを利用するケースが増えつつある。そのため、ひとたび脅威が発生すると、全体が機能不全に陥る恐れがあり、情報家電についてもコンピュータと同様の脆弱性対策が必要である。 ②　接続環境が千差万別で、接続検証に手間がかかる。	①　表示画面が小さくキーボードがない等、ユーザインターフェースに難がある。 ②　バグの修正、仕様変更をユーザー側に適用することがしにくく、バグを内在した機器がコンピュータ以上に拡散してしまう可能性が大きい。 ③　プログラムの命令を実行する装置である CPU(Central Processing Unit;)の能力が低く、搭載メモリ容量が小さい。 ④　色々な情報家電製品が出荷され、それぞれのセキュリティ対策水準が異なると、結果としてセキュリティ対策の水準が低い製品に揃ってしまう可能性がある。

情報家電のＯＳやソフトウェアに脆弱性が発見された場合、コンピュータと同様、修正プログラムを適用する必要があるが、ほとんどの情報家電においてはコンピュータと異なり、表示画面が小さく、表示画面すら無い場合がある。

加えて、キーボードのような多機能な入力装置はなく、リモコンがあるものもあれば、制御用の入力装置すらないものまである。

更に、情報家電は、ＣＰＵ能力が低い、メモリが少ない等の特徴があることから、セキュリティ確保のために必要な作業を、端末側でこなすことは困難が伴う。

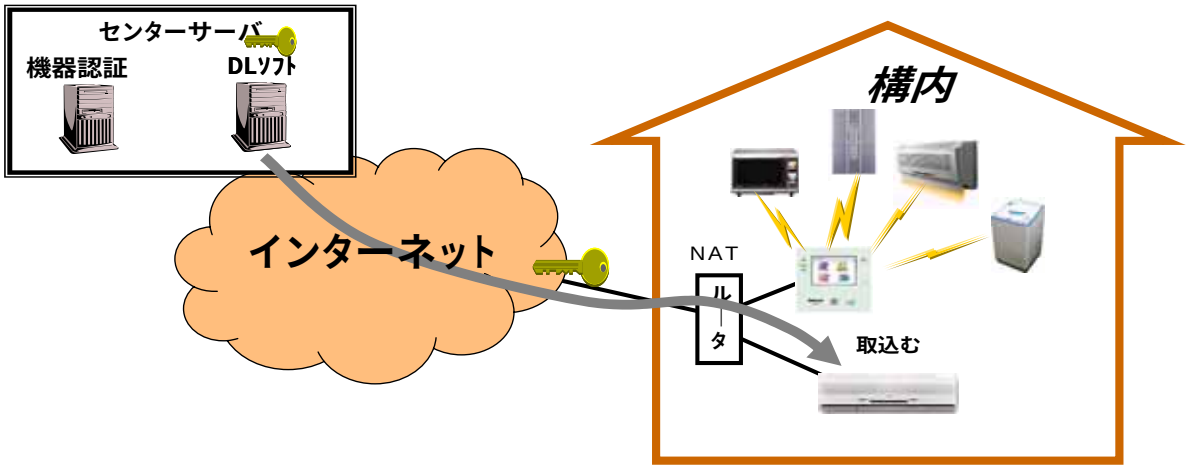
また、ユーザの多くは、自ら機器のメンテナンスができない層であると考えられる。

更に、情報家電は生活に密着しており、子供から高齢者まで様々な人々が利用すると想定されること、情報家電は通信機器でもあるという認識に欠ける消費者も多いと考えられること等から、情報家電のユーザに対し、コンピュータのユーザと同様に修正プログラムを適用してもらうよう期待するのは、現実的ではない。

以上から、構外の機器側から構内の情報家電に対して、能動的に修正プログラムを配信し、ユーザ側の操作を簡易にすることを検討する必要があると考えられる（いわゆる「リモート・メンテナンス」）。

しかし、こうしたリモート・メンテナンスに限らず、構内の情報家電に対して構外から接続するようなサービスを利用するに当たっては、構外から不正なアクセスが行われたり、不正なプログラムが適用されたりすることのないよう、構内の情報家電側から構外の機器やサービスを認証するとともに、逆に、構内にある情報家電が適切なものであるかどうかについて、構外の機器から構内の情報家電を認証することが求められる。

▽　リモート・メンテナンスのイメージ図



こうした機器認証の機能を

- 家電機器メーカが担うのか、ＩＳＰや携帯電話事業者が担うのか、それともサービス提供者が担うのか
- 各社ごとの認証で良いのか、業界を挙げた又は業界横断的な認証の仕組みが必要ではないのか、

という点については、関係各社のビジネスモデルとも絡む調整の難しい問題であるが、一定の規格化を図ることで、

① 家電機器メーカ、ＩＳＰや携帯電話事業者、セキュリティ・ベンダーのいずれにとっても、体制の構築、作業の統一等の面で費用削減を図ることができること、

② ユーザにとっても、家電機器メーカごとの独自の規格や操作方法等に対応する必要がなくなり、利便性の向上につながること、

から、どこまで規格化することが適当かについて関係業界で十分に検証し、調整することが必要であると考えられる。

２．３．４　情報家電を破棄・転売した場合の課題

（１）　サービス利用者と課金対象者が異なる可能性

情報家電を破棄・転売した場合において、元のユーザが当該情報家電を通じて利用するサービスの契約を解約しないと、当該情報家電を入手した別の人間がそのサービスを利用した場合、サービス料金を破棄・転売したユーザが支払ってしまう可能性がある。

クレジットカードによる支払いや月払い会費制等で支払額が僅少にとどまる場合は、破棄・転売後もサービス料金を支払っていることに気付かないことがあり得る。

このため、情報家電の破棄・転売時には、当該情報家電を利用して受けていたサービスの解約を行うようユーザに周知徹底を図るほか、サービスの利用履歴をユーザに対し適時通知する等の措置を検討することが必要である。

（２）　個人情報保護

また、破棄・転売した情報家電にサービスの利用に係る個人情報が残っていると、個人情報が漏洩し、悪用される恐れがあることから、破棄・転売の際には、サービス利用に係る個人情報を消去するようユーザを啓発することも求められる。

▽　情報家電に残っている可能性のあるサービス利用に係る個人情報

情報家電	残っている可能性のある個人情報
テレビ電話	**アドレス帳、通信料引落し口座等**
コンテンツ配信用レコーダ	**サービス契約情報、コンテンツ復号用秘密情報等**
エアコン、照明	**利用者の帰宅時間**
冷蔵庫	**冷蔵庫にあった食料品履歴**

２．４　家電業界とＩＳＰ業界との情報交換・情報共有の必要性

情報家電も、インターネットと同様、社会的に見て「有用」であるからこそ、その普及が期待されている訳であるが、これまでに見たように、セキュリティ・リスクを伴うものであることもまた事実であり、家電業界、ＩＳＰ業界、行政とが連携して、こうしたセキュリティ・リスクに迅速に対処していくための体制を構築していくことが求められている。

特に、情報家電のセキュリティ確保に関する課題の根底には、家電業界の技術者は、インターネットの技術を十分に知らず、逆に、インターネットの技術者は、家電側の要求をよく知らないという事情がある。

また、家電に関するユーザのセキュリティ意識は、コンピュータに関するユーザのセキュリティ意識に比べて低いという事情も、情報家電におけるセキュリティ確保をコンピュータにおけるセキュリティ確保以上に難しくしている。

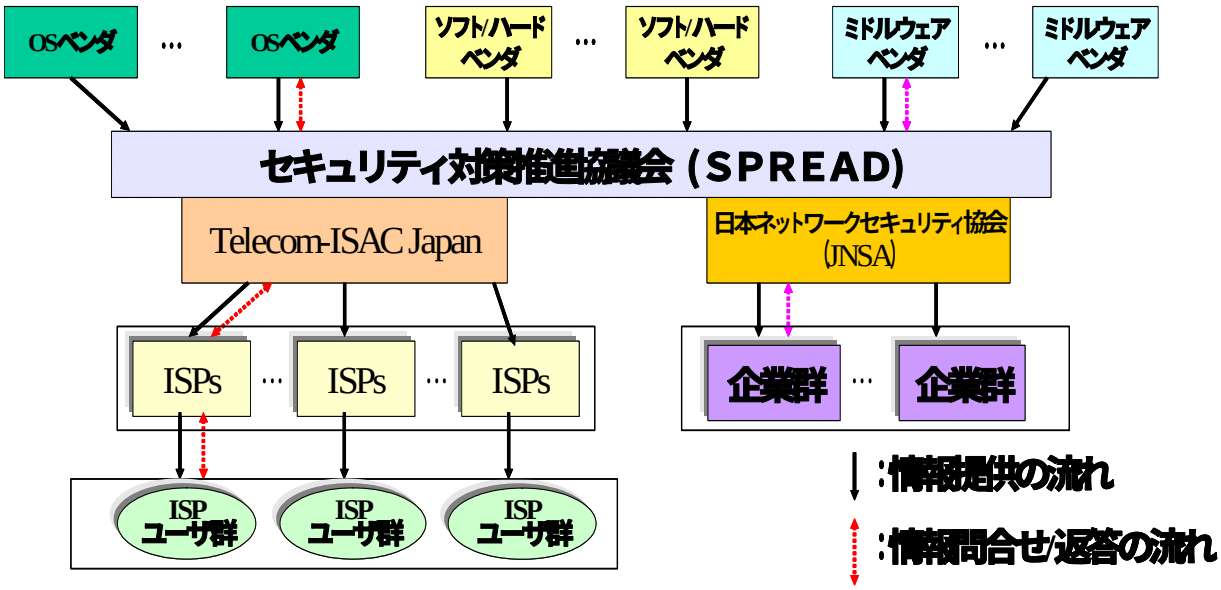
実際に、情報家電を攻撃対象とするインシデントや情報家電を踏み台とするインシデントが発生した場合に、家電メーカとＩＳＰとの間で、どの部署の誰を窓口として連絡を取り合えば良いのか、明確に決まっていない状況にある。

業界を越えた連携状況がこうした実態にある中では、ユーザは、どこに何を頼めば希望するサービスを利用することができるのか、情報家電を通じたサービスに苦情がある場合に、どこに申告すれば良いかも分からず、混乱するだけであろう。

こうした状況を克服し、情報家電の普及を促すためには、家電業界とＩＳＰ業界との間で業界横断的なセキュリティ情報の共有・分析・提供・公開、セキュリティに関するユーザの啓発に関する連携の枠組みを構築することが有効であると考えられる。

ＩＣＴ業界においては、既に 2004 **年** 6 **月に、メーカ等で構成される非営利組織である「日本ネットワークセキュリティ協会」（**JNSA**）と** Telecom-ISAC Japan **との間で、安全で快適なインターネット利用環境の普及とユーザ環境のセキュリティの確保・維持を推進することを目的として、「セキュリティ対策推進協議会**(SPREAD)**」が設立されている。**

▽　セキュリティ対策推進協議会（ＳＰＲＥＡＤ）



SPREAD：Security Promotion Realizing sEcurity meAsures Distribution

政府としては、こうした民間団体による取組みを支援していくことが望ましいと考えられる。

特に、

① 情報家電を攻撃対象とするインシデントは、情報家電の操作ができなくなるだけでなく、場合によっては人命に関わる事態（情報家電の操作により、風呂を沸騰させる、部屋を冷却する等）につながりかねないこと、

② 情報家電を踏み台としたインシデントは、情報家電の機器の総数が多いだけに、インターネット全体に過剰な負荷を与えかねないこと、

③ 情報家電は、これからサービスの本格的な多様化や利用の急拡大が見込まれており、現段階でセキュリティ対策を講じないまま、脆弱な機器が大量に市場に出回った場合は、回収等が困難なこと

等から、情報家電からの大容量のトラヒックがインターネット全体に与える負荷を軽減するとともに、人命に関わる事態につながらないよう情報家電の作動範囲を規定することが求められる。

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

ＩＳＰにおけるインシデント対応の現状と課題については第１章で、ユビキタスネット社会におけるセキュリティ確保策については情報家電に焦点を当てて第２章で、それぞれ検討を加えた。

ここでは、サービスの継続性とユーザ（法人ユーザ及び個人ユーザ）のデータ保護を確保する観点から、ＩＳＰを含む電気通信事業者において、経営陣が情報セキュリティマネジメントをどのように講じていくべきかについて、検討することとする。

情報そのものや情報システムは、その重要性の割には、我が国経営陣の評価が低いと言わざるを得ない。

金銭であれば、経営者や財務部門の一定のランク以上の従業員が管理するのに対し、情報や情報システムの管理については、社内の若いセキュリティ技術者や社外のセキュリティ・ベンダーに委託してしまう経営者が多いのが実情である。

しかしながら、情報システムが破られ、情報セキュリティが侵害された場合の被害は計り知れない。

このため、まず、情報セキュリティマネジメントやセキュリティ人材の重要性に関し、経営陣が、これまでの認識を改めるとともに、セキュリティポリシーを策定し、これに従って従業員教育やセキュリティ対策を実施していくことが必要不可欠である。

特に、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、セキュリティポリシーを策定し、セキュリティ対策を実施していくことが求められる。

この点に関しては、国際標準化機構（ＩＳＯ）と国際電気標準会議（ＩＥＣ）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。

また、国際電気通信連合（ＩＴＵ）では、我が国が中心となって検討を進め、電気通信分野を対象としたＩＳＭＳ（ＩＳＭＳ－Ｔ）を２００４年７月に勧告している。

一般の企業を対象とする汎用的なＩＳＭＳについては、現在、改訂作業が進められており、これを踏まえ、ＩＳＭＳ－Ｔについても、今後、改訂が必要となろう。

更に、ＩＳＭＳは国際規格であり、今後、ある国でＩＳＭＳに適合していると評価された組織が、他国においてもＩＳＭＳに適合しているものと評価されるよう、国際的な認証の仕組みを構築することも展望される。

このため、ＩＳＭＳ－Ｔの改訂作業に積極的に取り組むことにより、日本発の国際規格を提案していくことは、大きな意義を有するものと考えられる。

**　そこで以下では、ＩＳＭＳとＩＳＭＳ－Ｔの概要と今後をみた上で、我が国における今後の活動の方向性について検討することとする。**

３．２　ＩＳＭＳの概要と最近の改訂作業の動向

３．２．１　ＩＳＭＳの概要

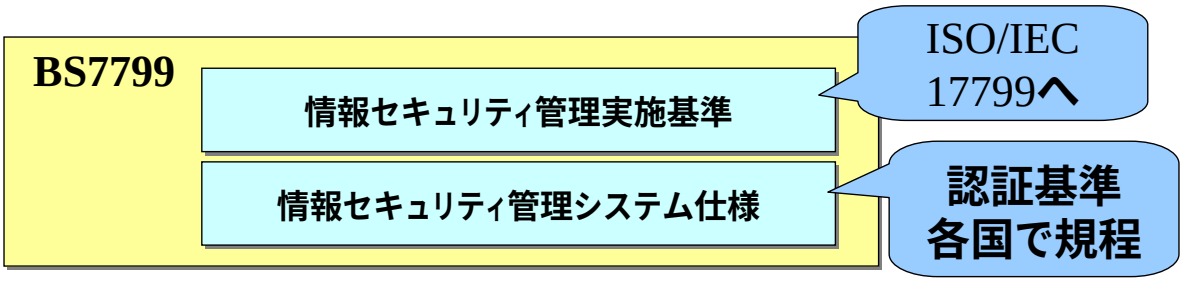
ＩＳＯとＩＥＣが２０００年１２月に国際規格として策定したＩＳＭＳであるＩＳＯ／ＩＥＣ１７７９９は、９５年に英国で国内規格として策定されたＢＳ７７９９を国際規格化したものであり、この国際規格では、情報セキュリティマネジメントに影響のある１２７の管理策（Control）を次の１０のマネジメント領域に分類している。

▽　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）

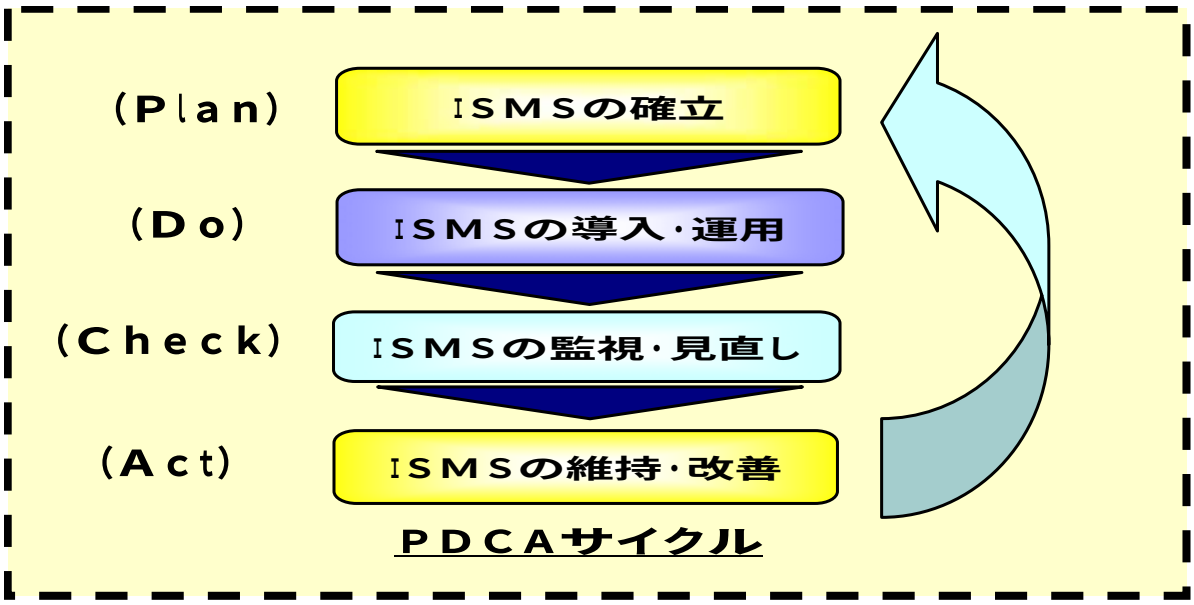
このＩＳＯ／ＩＥＣ１７７９９では、ＢＳ７７９９の「管理規格」のみが国際規格化され、ＩＳＭＳに適合しているか否かを評価する際の基準となる「認証規格」については、各国が実情に適した形で策定することとされている。

▽　ＢＳ７７９９とＩＳＯ／ＩＥＣ１７７９９



各国で実施されているＩＳＭＳ適合性評価は、評価を希望する組織が、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。

▽　ＰＤＣＡサイクル



３．２．２　ＩＳＭＳ適合性評価

実際のＩＳＭＳ適合性評価に当たっては、まずは組織自身の中で次の①から④のＰＤＣＡサイクルを実行し、当該組織の ISMS を確立することになる。

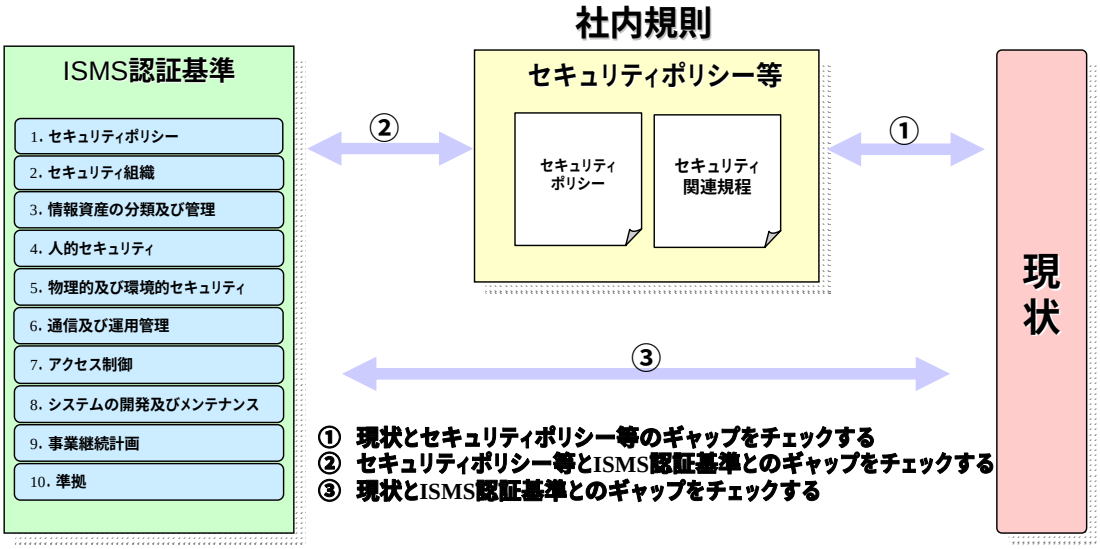
①　情報セキュリティ関連ルール（セキュリティポリシー及び実施手順）（以下、「セキュリティポリシー等」という。）を策定する。（Plan）

②　セキュリティポリシー等に沿った社員教育やセキュリティ対策等を実施・運用する。（Do）

▽　ＩＳＭＳ適合性評価ー第２段階（Do）

③　セキュリティポリシー等がＩＳＭＳ認証基準と整合しているか、また、セキュリティポリシー等に沿って社員教育やセキュリティ対策が実施されているか等を監査する。（Check）

▽　ＩＳＭＳ適合性評価－第３段階（Check）



④　監査等の結果を基に、セキュリティポリシー等や実施・運用を見直し、改善する。（Act）

次に、ある組織が自ら確立した ISMS に適合しているか否かを評価するに当たっては、審査の申請を受けた第三者（審査機関）において、

①　ISMS 認証基準と文書の整合性

②　セキュリティポリシー等と現状との整合性

について審査を行い、当該組織における ISMS が適切と判断できれば、認証を与えることになる。

ここでは、審査を希望する組織（事業所）、その組織におけるＩＳＭＳ認証基準とその適用範囲を確認の上、当該組織の責任者による承認が適正になされているか否か、という点のみを審査することになる。

換言すれば、第三者による審査においては、

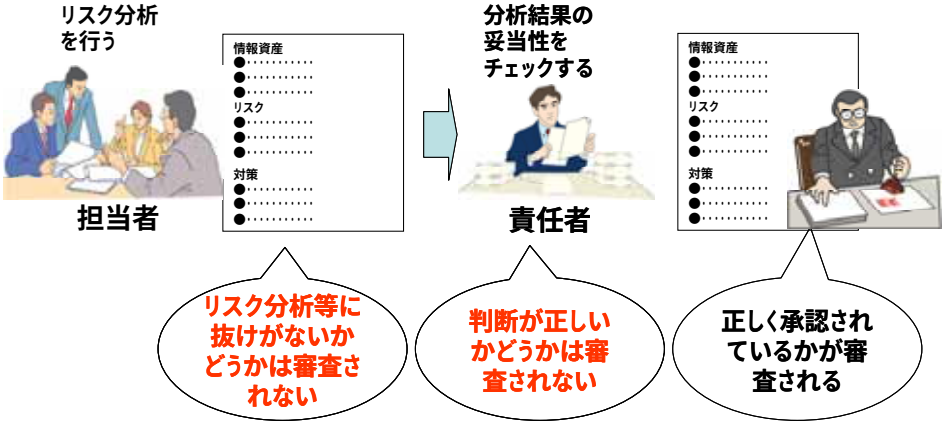
①　審査対象となる組織自身が実施するリスク分析等に抜けがないかどうか、

②　責任者による判断が正しいかどうか、

という点は、審査対象とならないものである。

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。

▽　ＩＳＭＳ適合性評価－第三者による審査



３．２．３　ＩＳＭＳの改訂作業の動向

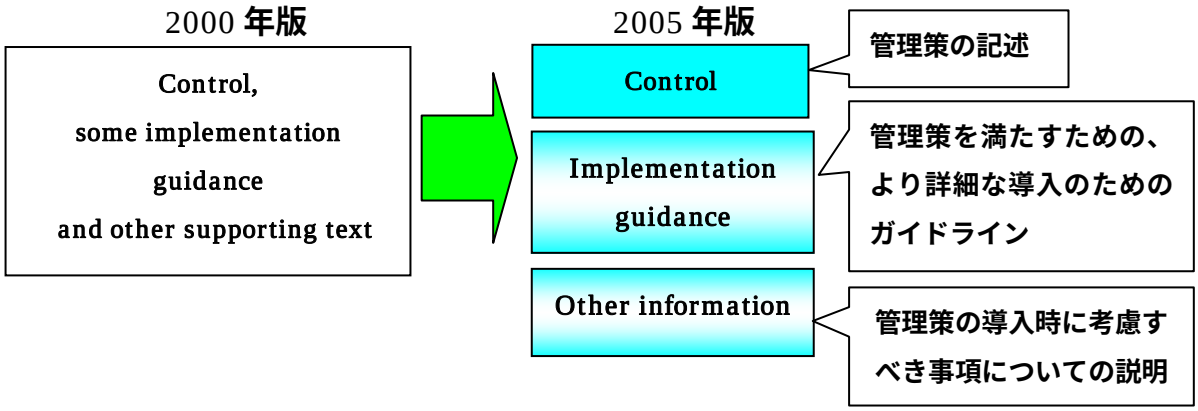
２０００年１２月に策定されたＩＳＯ／ＩＥＣ１７７９９（以下「２０００年版」という。）は、２００１年から改訂作業が開始され、２３カ国から２，５００以上の意見が提出された。

これを受けて改訂作業が進められたＩＳＭＳ（以下「２００５年版」という。）では、管理策（Control）が１２７から１３５に増え、新たなマネジメント領域として「情報セキュリティに係るインシデントのマネジメント」（Information security incident management）が追加されている。

また、２００５年版では、規定の仕方においても、管理策（Control）、導入のためのガイドライン（Implementation guidance）、関連情報（Other information）と３層に分けて規定されており、ＩＳＭＳを確立し、運用しようとする組織にとって導入しやすいものにする工夫が施されている。

▽　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



３．２．４　ＩＳＭＳの今後の課題

２００５年版は、２００５年４月のＩＳＯの会合において、編集上の意見を処理した後、投票が実施され、２００５年の後半には発行されるものと想定されているが、今後のＩＳＭＳの課題を整理してみると、次のとおりである。

（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が示され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。

ＩＳＭＳ－Ｔについては、３．３で検討する。

（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

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＞）を勧告した。

これは、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である。

一般の企業を対象とする汎用的なＩＳＭＳ（ＩＳＯ／ＩＥＣ１７７９９）と比べると、次の５つのマネジメント領域について、電気通信分野に固有の管理策（Control）を追加している。

▽　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）

また、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。

▽　電気通信分野における実装要件の例

ＩＳＭＳ－ＴとＩＳＭＳとで変更無し

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。
電気通信分野における実装要件（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。電気通信事業者に関係する資産には多くの種類があり、それには以下のものが含まれる。 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）　改訂ＩＳＭＳを参照する必要性

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であるが、上述したとおり、２００５年版が２００５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	

（２）　現行ＩＳＭＳ－Ｔへの追加項目の検討

現行のＩＳＭＳ－Ｔについては、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規定されていない。

２０００年版の「適合性」の領域には、「知的所有権」、「組織の記録の保護」、「データの保護及び個人情報の保護」、「情報処理施設の誤用の防止」、「暗号による管理策の規制」等が規定されているが、電気通信事業者に対しては、これ以外にも、次のような法令上の要求事項があることから、今後、ＩＳＭＳ－Ｔにこれらの要素を追加すべきか否かを検討する必要がある。

①　取扱中に係る通信の秘密は、侵してはならないこと。取扱中に係る通信に関して知り得た他人の秘密を守らなければならないこと。（電気通信事業法第４条）

②　電気通信役務の提供について、不当な差別的取扱いをしてはならないこと。（電気通信事業法第６条）

③　災害の予防若しくは救援、交通、通信若しくは電力の供給の確保又は秩序の維持のために必要な事項を内容とする通信等を優先的に取り扱わなければならないこと。（電気通信事業法第８条）

④　他の電気通信事業者から接続請求を受けたときは、原則として、これに応じなければならないこと。（電気通信事業法第３２条）

⑤　利用者又は電気通信事業者の接続する電気通信設備を損傷し、又はその機能に障害を与えないようにすること。他の電気通信事業者の接続する電気通信設備との責任の分界が明確であるようにすること。（電気通信事業法第４１条）

⑥　利用者の端末設備との接続によって、電気通信回線設備を損傷し、又はその機能に障害を与えないようにすること。電気通信設備を利用する他の利用者に迷惑を及ぼさないようにすること。利用者の端末設備との責任の分界が明確であるようにすること。（電気通信事業法第５２条）

⑦　個人情報保護法及び電気通信事業における個人情報保護に関するガイドライン（平成１６年８月３１日総務省告示第６９５号）を遵守すべきこと　等。

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、「資産の分類及び管理」、「物理的及び環境的セキュリティ」、「通信及び運用管理」、「アクセス管理」、「システム開発及び保守」、「インシデントのマネジメント」、ひいては「セキュリティ方針」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

３．４．１　ＩＳＭＳ－Ｔの国内における展開

前述したように、ＩＳＭＳ－Ｔは、ＩＴＵにおいて、我が国が中心になって検討を進め、我が国の提案が採用されて国際規格となったものであり、今後は、こうした国際規格を国内に展開していくことが適当であると考えられる。

その際には、２００５年版のＩＳＭＳの発行が近々想定されていることから、その内容を参照することを始め、電気通信分野に固有の法令上の要求事項を充たすことのできるよう、検討を加えていくことが必要である。

３．４．２　国内における普及促進

ＩＳＭＳ－Ｔを国内で普及促進させていくためには、これ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次の課題について、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適当である。

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　技術上の対策の適用方法

特に、中小規模の電気通信事業者や地方で事業を展開している電気通信事業者にとっては、派遣社員を含めた人的セキュリティの確保、アクセス制御の厳重化等において、大規模事業者や都市部の事業者に比べ困難を伴う面もあることから、政府においては、既存及び新規の施策を組み合わせ、これらの事業者に対し、より大きなインセンティブを付与することを検討するべきである。

３．４．３　国際規格化への貢献

ＩＳＭＳと同様、ＩＳＭＳ－Ｔは国際規格であり、今後、ある国でＩＳＭＳ－Ｔに適合していると評価された電気通信事業者（又はその中の一組織）が、他国においてもＩＳＭＳ―Ｔに適合しているものと評価されるよう、国際間の認証の仕組みを構築することが展望される。

このため、ＩＳＭＳ－Ｔについては、国内における普及促進を図るだけでなく、国際機関に積極的に提案を行い、日本発の国際規格化を進めることに、大きな意義があるものと考えられる。

換言すれば、国際的にも評価されるよう、ＩＳＭＳ－Ｔの国内における普及促進を図るとともに、国際機関への提案を準備することが求められるところであり、官民の知見を結集して、ＩＳＭＳ－Ｔの充実を図っていくことが重要であると考えられる。

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、我が国としても、ＩＴＵにおける検討に積極的に参画し、貢献していくことが期待される。

第４章　セキュリティ人材育成

４．１　我が国におけるセキュリティ人材の現状

あらゆるセキュリティ対策を講じる上で基盤となるのは、人材である。

２００３年のＩＴＵ調査によれば、ブロードバンド通信の「安さ」と「速さ」において、我が国は世界１との評価を受けているが、こうしたブロードバンドの進展状況に比べ、ブロードバンドを支えるセキュリティや、セキュリティ対策を講じる上で不可欠な人材が十分かどうかについては、疑問無しとしない。

そこで以下では、まず、我が国のセキュリティ人材の現状を見ておくこととする。

４．１．１　労働市場における情報処理技術者の「供給」面

電気通信業界に限定せず、我が国の労働市場全体で見ると、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代以下が約８割を占めているのが実態であり、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が指摘されている。

▽　就業人口の減少

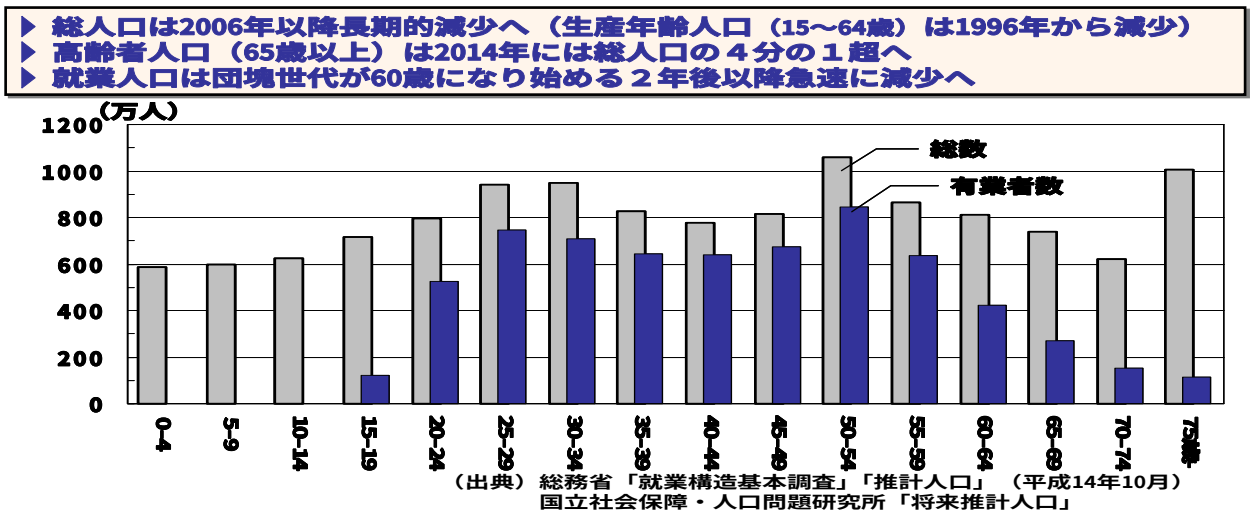
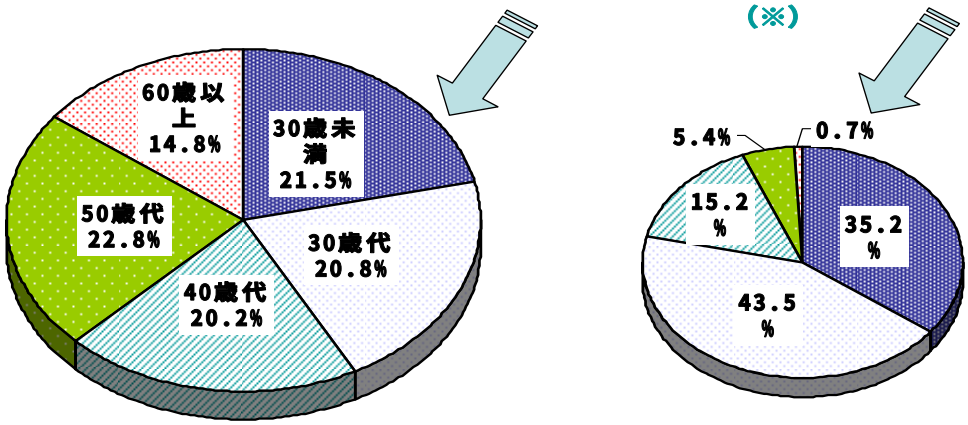


図　情報処理技術者の年齢構成

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

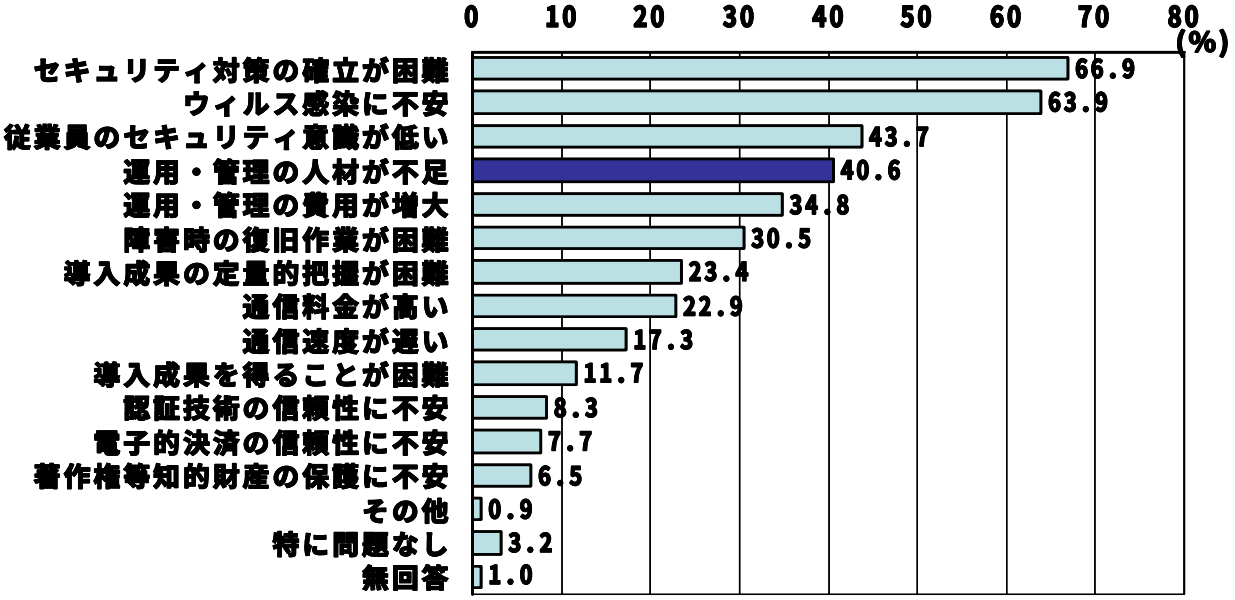


※　情報処理技術者：情報処理技術に関する高度の専門的知識・経験をもって，システムの分析，設計の仕事に従事するもの及びプログラムの設計，作成についての技術的な仕事に従事するもの
（出典）総務省「就業構造基本調査」及び「推計人口」より加工（平成14年10月）

４．１．２　労働市場における情報処理技術者の「需要」面

他方、ユーザ側から見ると、情報通信ネットワークの利用において、セキュリティ対策、ウイルス感染に続いて、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。

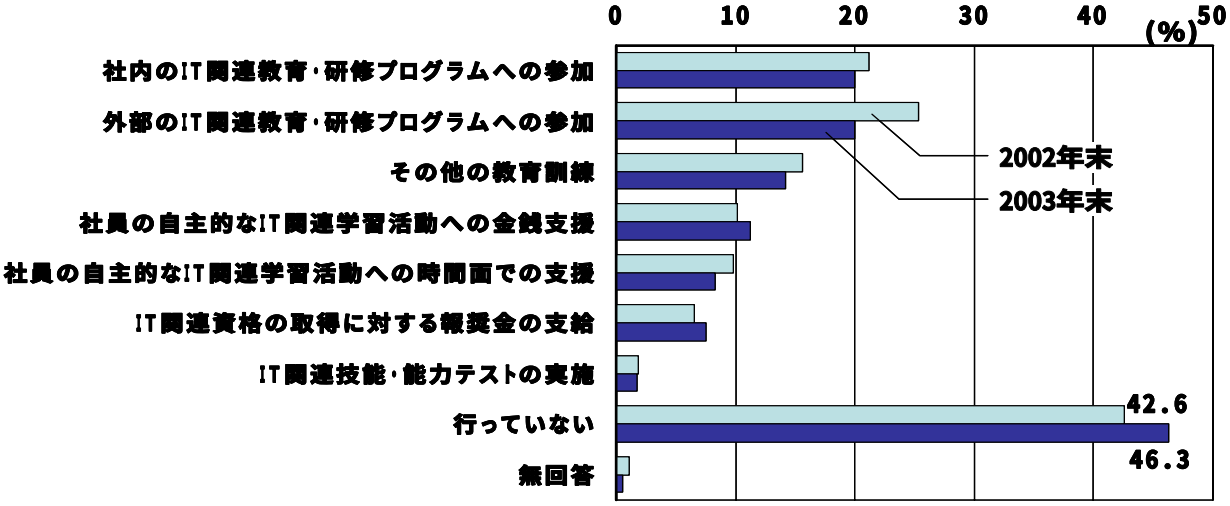
▽　ユーザ側の懸念事項



（出典）総務省「通信利用動向調査」（平成15年）

それにもかかわらず、企業における人材育成の状況をみると、人材育成を「行っていない」とする企業が４割以上を占めているのが実情である。

▽　企業における人材育成



（出典）総務省「通信利用動向調査」（平成15年）

２００３年に開催された総務省の「情報通信ソフト懇談会」では、企業における専門的ＩＣＴ人材は４２万人、そのうちセキュリティ人材は１２万人不足していると推計されている。

▽　企業における専門的ＩＣＴ人材の不足数

	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。

また、「日経ＩＴプロフェショナル」の２００４年６月調査によれば、２万人を超えるＩＴ技術者の４６％が、「人の助けを借りながら業務を遂行できる」水準との指摘もある。

４．１．３　我が国電気通信事業者におけるセキュリティ人材の現状

次に、我が国の電気通信事業者において、実際にセキュリティ人材が充足しているか否かについて見ておくこととする。

インターネットは、ＩＳＰ等のネットワークが相互に接続したネットワークであり、あるＩＳＰにおけるＩＣＴ障害が他のＩＳＰにも影響を及ぼす可能性があり、インターネットが社会経済活動を支えるインフラとなっている現状にかんがみると、ＩＳＰ等の電気通信事業者において、セキュリティ人材が十分に確保されているか否かは、国民の社会経済生活を支える上で非常に重要である。

そこで、総務省では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、セキュリティ人材（注１４）についてアンケートを行った。

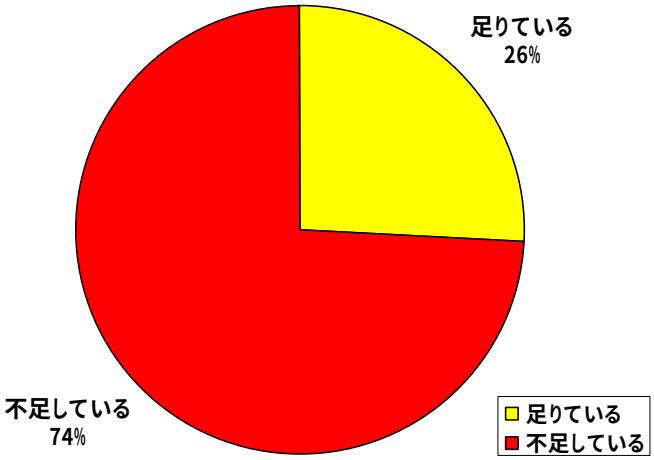
（注１４）このアンケートにおける「セキュリティ人材」としては、ウィルスチェック、コンテンツフィルタリング、不正アクセス監視、セキュリティ診断、リモートアクセス環境検査等のセキュリティサービスをユーザに対し提供できる従業員のほか、自社のネットワーク運用の障害予防、当該障害の監視・検出・制御、障害の再発防止等を講じることのできる従業員を想定している。

その結果は次のとおりである。

（1）セキュリティ人材の充足感

まず、セキュリティ人材の不足感についてアンケートをとったところ、約４分の３の事業者において、セキュリティ人材の不足している状況にある。

▽　セキュリティ人材の不足感　　**＜有効回答数197社＞**



また、有効回答を寄せた２０２社が現在雇用しているセキュリティ人材は４３０６人であり、今後追加したいセキュリティ人材の数は全体で１３２４人と、現在雇用しているセキュリティ人材を３１%増加させたいという結果になっている。

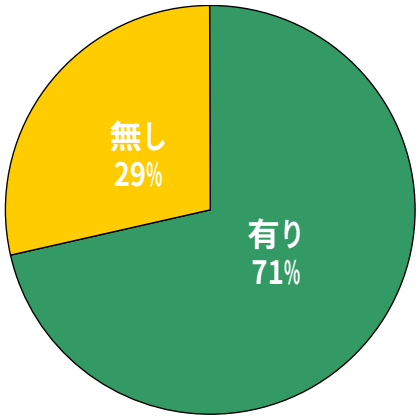
（2）セキュリティ人材育成の現状

次に、電気通信事業者において、セキュリティ人材をどのように育成しているかについてアンケートをとったところ、７割の事業者が社員のセキュリティ教育に取り組んでいる状況にある。

逆に言えば、３割にのぼる事業者は社員のセキュリティ教育を実施していない状況にあり、行政においては、セキュリティに係る人材育成の重要性について、事業者の意識を喚起すべきであると考えられる。

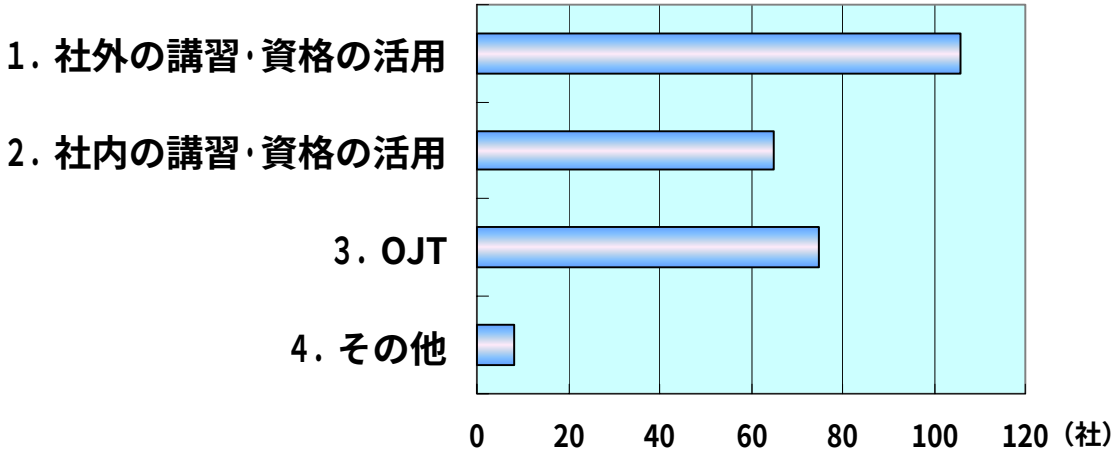
▽　電気通信事業者のセキュリティ教育の実施状況

＜有効回答数197社＞



セキュリティ教育を実施している事業者について、セキュリティ教育の実施方法を見ると、社外の講習・資格の活用やＯＪＴによる教育の割合が高くなっている。

▽　セキュリティ教育の実施方法　　＜有効回答数197社＞



電気通信事業者における人材育成の実態をより詳細に見ると、中核となるセキュリティ人材を社外の研修事業者による講習等に派遣して技能・知識を習得させ、その中核となる人材が、通常の業務運用の中で、他の従業員に対し、講習等で得られた技能・知識を伝えていく、といった形で人材育成を行っており、特に系統立てた育成システムを行っていない場合が多い。

特に、中小規模の電気通信事業者においては、セキュリティのためだけに専任者を配置するというよりも、通常のネットワーク運用業務やシステム構築の一環として、事業者内部のセキュリティ確保や、ユーザに対するセキュリティサービスの提供を行っている場合が多いのが実情である。

これは、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ず、結果として、セキュリティ人材の育成もできないという事情によるものである。

他方で、インターネットの分野は”dog year”あるいは”mouse year”と言われるほど技術革新が激しく、それに応じてセキュリティ事案も多様化しており、社外の講習等に人材を派遣してみても、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く、結局は、現実に追われる「いたちごっこ」ではないのか、という悩みを抱えている事業者も存在する。

現実の「後追い」ではなく、セキュリティ業務により積極的に取り組むためにセキュリティ人材を育成しようとする場合においても、セキュリティ人材は、以下のように技術から法令まで多くの技能・知識を習得することが必要であり、その育成には多くの時間と高額の費用を要するのが実情である。

▽　セキュリティ人材が修得すべき技術・知識の例

情報処理技術、ネットワーク技術、インシデント対応技術、監視技術、侵入検知システム（IDS）、ファイアウォール技術、トラヒック状況解析、ＩＳＭＳ、リスクマネージメント技術、国際規格、国内規格、国内法令、外国法令、等

実際、外部業者によるセキュリティ講習等は、期間が４～５日、費用が１回１人当たり４０～５０万円、高価なものでは８０～１００万円かかる場合がある。

このため、一定規模以上の電気通信事業者では、年間計画を組んだ上で、半強制的に従業員を社外の講習等に参加させることができているが、中小規模の電気通信事業者の中には、派遣期間及び費用の面で、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という事情も散見される。

加えて、地方においては、受講者が集まらないことから外部業者によるセキュリティ講習等がそもそも開催されず、地方で事業を展開している電気通信事業者にとっては、従業員を社外のセキュリティ講習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という側面もある。

また、そもそもインターネットの分野は、技術革新の進展が急激であることから、人材育成も継続的な取組みが必要である一方、社外の講習等に自社の従業員を派遣してみても、それによって得られるセキュリティ水準がどれ程かについての判定が難しく、結果として、電気通信事業者によるセキュリティ人材の育成を鈍らせる要因の１つとなっている。

このため、電気通信事業者の中には、特に地方において従業員にセキュリティ技術を習得させるための「場」を用意して欲しいとの要望があるほか、修得したセキュリティ技術の水準を評価できる仕組みを構築して欲しいとの要望もある。

このように、我が国電気通信事業者のセキュリティ人材の育成については、様々な課題を抱えているのが実情である。

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

上記において、我が国におけるセキュリティ人材の現状を見た訳であるが、これとの対比で米国の状況を見ておきたい。

この点については、１９９９年に米国商務省がＩＣＴ人材について公表した資料があり、次の点が伺われる。

①　ＩＣＴ人材は、１９９６年から２００６年までの１０年間で、１５０万人から２６０万人まで増加させることが必要であるとしていること。

②　他の業界への転職者数を差し引くと、１９９６年から２００６年までの１０年間で、１１０万人を超えるＩＣＴ人材の増加が必要であるとしていること。

③　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１０年間で、２５万人弱の** Computer Scientists **の増加が必要であるとしていること。**

▽　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

以上のように、米国では、既に１９９９年の時点で、１１０万人を超えるＩＣＴ人材の増加が必要とされていた点には、我が国としても注目する必要があると考えられる。

実際、米国では、１９９８年５月の大統領指令６３号（「ＰＤＤ６３」(注１５) という。）を受けて、国家インフラ防護センター（ＮＩＰＣ）(注１６) や情報共有分析センター（ＩＳＡＣ）(注１７) 等を創設したほか、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１８) においてＣＡＥＩＡＥ (注１９) と呼ばれる人材育成プログラムを実施している。

（注１５）ＰＤＤ６３： Presidential Decision Directive 63

（注１６）NIPC： National. Infrastructure Protection Center

（注１７）ISAC： Information Sharing and Analysis Center

（注１８）NSA: National Security Agency

（注１９）CAEIAE： The National Centers of Academic Excellence in Information Assurance Education

これらのプログラムには、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２０）やＳＦＳ（注２１）の奨学金制度への申請権が与えられている。

▽　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２０）　国防総省情報保証奨学金：　Department of Defense Information Assurance Scholarship Program

（注２１）　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

シンガポールにおいても、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２２））と呼ばれるＩＣＴ人材育成のプログラムを推進している。

（注２２）　CITREP：　Critical Infocomm Technology Resource Program

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である。

助成対象と助成上限額は次のとおりである。

▽　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	

４．３　我が国におけるセキュリティ人材育成

４．３．１　セキュリティ人材に関する我が国電気通信事業者の要望

上述のように、米国やシンガポールでは、セキュリティに関する講習を受講しようとする個人又はセキュリティ資格を取得しようとする個人に対し、一定額を助成する形で政府による人材育成が進められている。

これに関しては、我が国電気通信事業者に対するアンケートの回答をみても、セキュリティに関する講習や資格（以下「セキュリティ講習等」という。）について、費用面での助成や公的な位置付けを求めるものが多くなっている。

①　従業員のセキュリティ能力の向上を図る電気通信事業者に対する支援

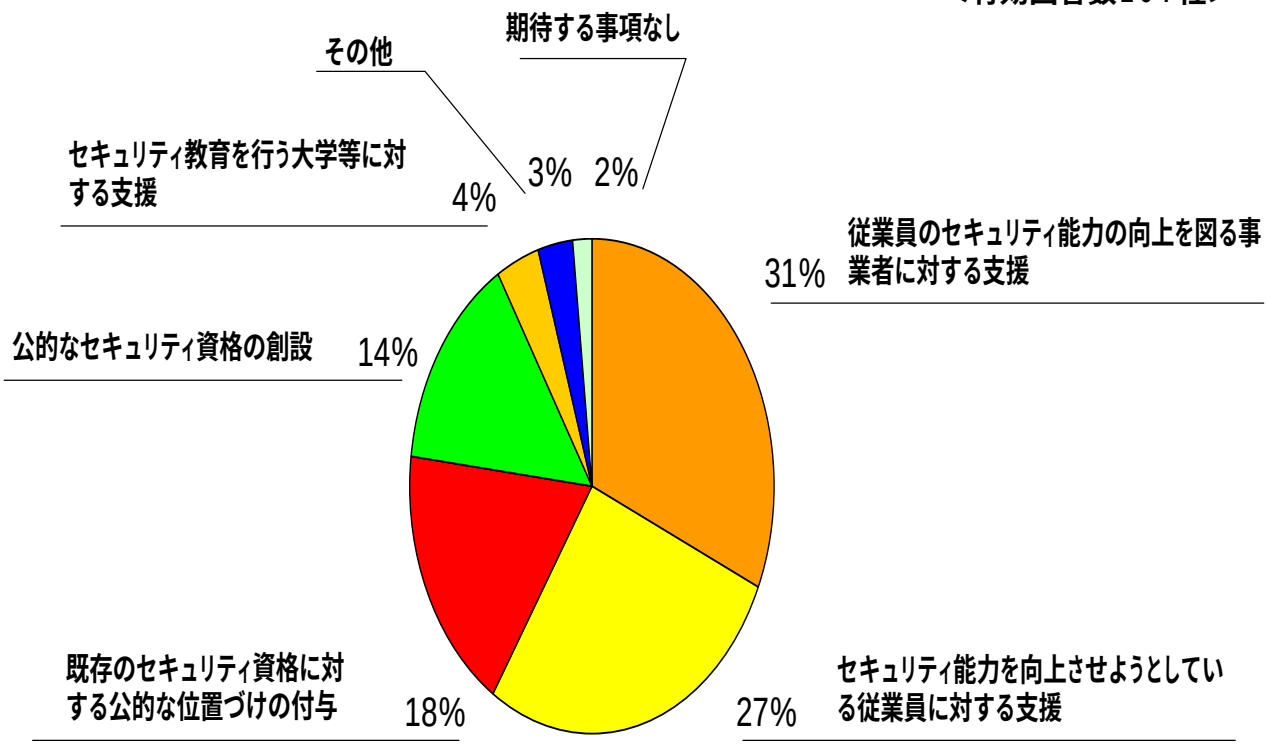
②　セキュリティ能力を向上させようとする社員に対する支援

③　既存のセキュリティ資格に対する公的な位置付けの付与

④　公的なセキュリティ資格の創設

▽　セキュリティ人材に関する電気通信事業者の要望

＜有効回答数１９７社＞



セキュリティ資格については、下表のとおり、民間企業によるものと公的なものとを問わず、既に多くのものが存在しており、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益と考えられる。

▽　セキュリティ資格の例

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

４．３．２　既存のセキュリティ講習等に対する評価の基準

（１）資格や認定の効果が有効期限付きのものか

まず、インターネットは、”dog year”**あるいは**”mouse year”**で技術革新を続けており、セキュリティ技術についても日々刻々変化していることから、有効期限付きのセキュリティ資格や認定であることが適当である。**

すなわち、セキュリティに関する資格や認定は、自動車免許のように有効期限付きのものであり、定期的に講習を受けること等が適当と考えられる。

有効期限付きのセキュリティ資格や認定は、更新を行うための組織が必要であること、新たな技術への対応ができること、教育体制が確立されている場合が多いこと等の特徴があり、これらの点からも望ましいと言える。

（２）実機を使った演習があるか

セキュリティ人材は、机上の知識だけでなく、実際の通信機器を用いて「生きた」技術・技能を修得することが不可欠であり、実機を使った演習があることも重要である。

（３）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重要である。

４．３．３　既存のセキュリティ講習等の例―ＮＩＳＭ

期限付きで、かつ実機を使った演習があり、技術だけでなく管理・運用、法制度についても講習等があるものとして、例えば「ネットワーク情報セキュリティマネージャー」（ＮＩＳＭ）がある。

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年に創設されたものであり、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の育成を目的として、ＮＩＳＭ推進協議会（注２３）によって実施されている人材育成プログラムである。

▽　ＮＩＳＭの概要

受講資格	**①　「ＮＩＳＭ推進協議会」を構成する団体に加盟する事業者に所属し当該事業者が推薦する者。** **②　加盟はしていないが、上司または管理する者が推薦する者であって、かつ「ＮＩＳＭ推進協議会」が承認した者。**
資格取得方法	**「講習の受講」＋「講習最終日に実施される認定試験に合格」**

（注２３）ＮＩＳＭ推進協議会は、（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から構成される。

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推進協議会より「認定」が与えられることとなっている。

また、ＮＩＳＭの特徴としては、次のような事項が挙げられる。

①　２年間の有効期限があり、更新試験により、資格を更新する。

②　実機を用いた実践的な演習がある。

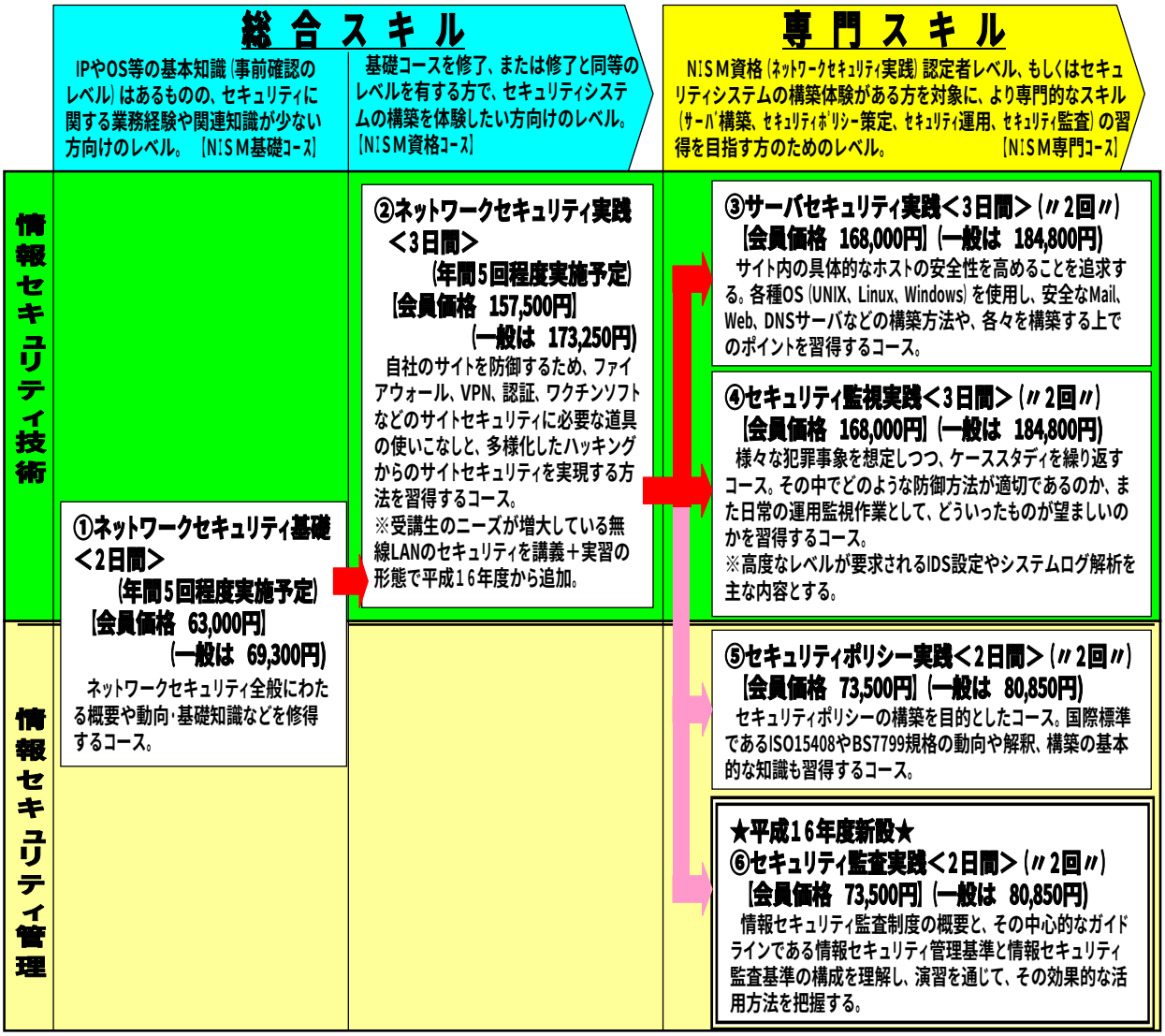
③　技術のみならず、管理・運用、法制度についても講習を実施する。

④　ベンダーフリーの講習・資格のため、特定のセキュリティ・ベンダーの技術に縛られることなく、最新の必要な技術について学ぶことができる。

⑤　ＩＳＭＳの取得時においても、「セキュリティに関する有スキル者（有資格者数）」として計上することができる。

⑥　入札資格の一例としている地方公共団体も存在する。

▽　ＮＩＳＭ資格体系



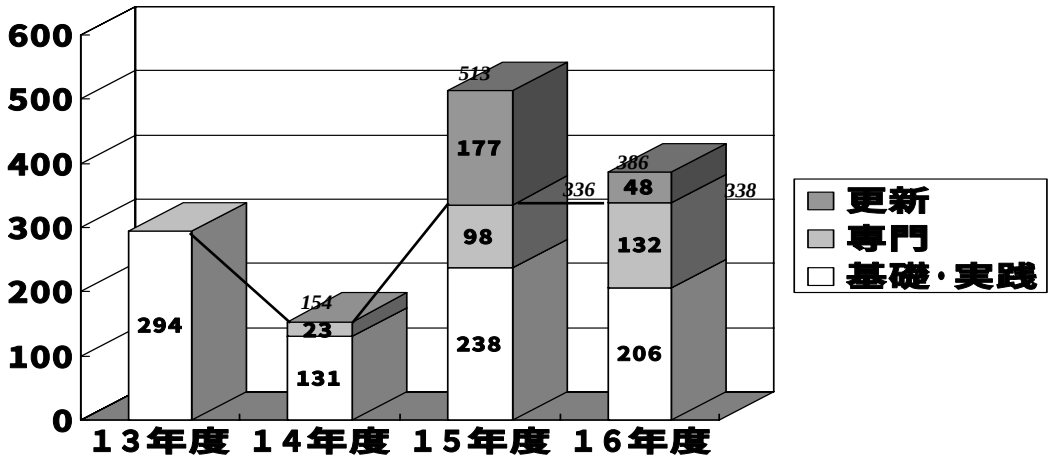
※　価格は税込。　　※　日程･講習会場等詳細はNISMﾎｰﾑﾍﾟｰｼﾞを参照。［URL］ http://www.nism.jp

ＮＩＳＭについては、２００１年の創設以来、１，３００名を超える認定取得者がいるが、電気通信業界におけるセキュリティ人材の需要の大きさからすると、依然として十分ではない。

今後とも、インターネットのセキュリティに関する技術革新の動向や電気通信事業者のニーズを踏まえ、講習をより良い内容にするとともに、電気通信事業者にとって広く利用されるよう、周知・啓発を図ることが適当と考えられる。

また、ＮＩＳＭに限らず、セキュリティ講習等に一般的に該当する傾向として、特に、従業員を参加させるに当たって負担の大きい中小規模の電気通信事業者や、地元で講習会が開催される機会の少ない地方の電気通信事業者にとって、利用しにくい側面があり、今後、中小又は地方の電気通信事業者への浸透を強化することが求められている。

▽　ＮＩＳＭの認定取得者数の推移



年度	受講者数 新規	受講者数 基礎・実践	受講者数 専門	受講者数 更新	受講者数 計	資格取得者数 新規	資格取得者数 基礎・実践	資格取得者数 専門	資格取得者数 更新	資格取得者数 計	年度末有効ID数(累積)
H13	295	295	－	－	295	294	294	－	－	294	294
H14	154	131	23	－	154	154	131	23	－	154	448
H15	339	240	99	177	516	336	238	98	177	513	667
H16	340	206	134	48	388	338	206	132	48	386	899
合計	1,128	872	256	225	1,353	1,122	869	253	225	1,347	－

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となっている。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**

電気通信事業者から大学等の教育機関に対しては、基礎的かつ系統だったセキュリティ教育を施して欲しいという意見もあるところであり、こうした産業界からの意見を踏まえ、教育機関が自らの教育カリキュラムを見直し、充実させるとともに、行政において教育機関の取組みに対する支援策を講じていくことが求められる。

４．４　事業者をまたがる総合的な演習の必要性

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。

また、近年、インシデントは広域にわたって同時に発生するケースがあり、ボットネットに代表されるような組織的攻撃も増加している。

このように、インシデント事案の広域化や組織的攻撃の増加という最近の傾向にかんがみると、電気通信事業者間及び電気通信事業者と行政との間で連携して、セキュリティ対策を講じることのできる人材が求められる。

ＩＴ戦略本部の情報セキュリティ基本問題委員会が２００５年４月に取りまとめた第２次提言においても、「演習・訓練及びセミナー等を通じて、重要インフラ（注２４）所管省庁及び重要インフラ事業者を中心に、高度なＩＴスキルを有する人材を育成」すべきこととされ、更に「想定脅威の拡がりに対応した具体的脅威シナリオの類型を元に毎年度ごとにテーマを設定し、各重要インフラ事業者、各重要インフラ分野内情報共有機構等の協力を得ながら、重要インフラ横断的な総合的演習を企画・実施」することとされている。

（注２４）上記第２次提言では、「重要インフラ」として、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）の７分野のほか、医療、水道、物流等を含める方向性が示されている。

更に、大規模なインシデント事案に際しては、「高度なＩＴスキルを有する人材」のほかに、これら「高度なＩＴスキルを有する人材」の協力体制を促進することのできる調整力のある人材を、プロジェクトリーダーとして育成し、専従的に確保することも必要であると考えられる。

実際、既に米国では、攻撃を想定した総合的な演習が、数次にわたり実施されている。

▽　米国における演習の事例

演習名称	実施時期	実施主体	演習の概要
The Day After	1996年3月（約半日）	国防総省（DARPA）	政府、大学、情報インフラ関係者による机上演習。攻撃の発生を想定して複数のシナリオを用意し、以下の演習プロセスを実施 The Day of　攻撃の発生 The Day After　対策 The Day Before　被害を最小化するための予防策の改善
Eligible Recover	1997年6月（2週間）	国家安全保障局（NSA）	NSAのスタッフが実際に攻撃を実施し、電力と電話のシステムを切断する方法等を模索、システムの脆弱性を検証
Digital Peral Harbor	2002年7月（3日間）	Gartner、米海軍大学	セキュリティ専門家が電力、通信インフラ、インターネット、金融サービスについて実行可能な攻撃方法と攻撃による損害を検証。
Livewire	2003年10月（5日間）	国土安全保障省（DHS）	通信、エネルギー、金融、地方自治の分野について、攻撃発生後の緊急対応体制が実際に機能するかを検証。

我が国においても、①セキュリティの専門家により実行可能な攻撃方法と攻撃による損害を検証するとともに、②攻撃発生後の緊急対応体制が実際に機能するか否か等について演習を通じて検証しておくことは、非常に重要なことと考えられる。

①については、ソーシャルエンジニアリングや、内部の従業員による意図的な経路の誤設定又はシステムへの脆弱性の埋込み等を視野に入れて検証することが有用である。

また、②についても、設備管理面やネットワーク運用面で各ISPの言葉遣いが統一されておらず、緊急時に意思疎通に齟齬を来すことが懸念されていることから、ネットワークの状況を定量的に伝えるための運用評価尺度に係る共通認識の醸成や言葉遣いの統一を、演習を通じて進めることが有益である。

更に、こうした演習には、セキュリティ講習等に参画できる機会が相対的に少ない中小又は地方のＩＳＰの参画を順次確保していくとともに、セキュリティに関する考え方や運用評価尺度が異なる場合のある情報家電機器メーカや大学等の学術ネットワークの参画を得ていくことが望ましいと考えられる。

加えて、電気通信事業におけるＩＣＴ障害が、金融、航空、鉄道、電力、ガス、政府・行政サービス、水道等の他の重要インフラに及ぼす影響についてもシミュレーションしておくことが有用であろう。

第５章　総括

以上、これまでの検討を総括すると、次のとおりである。

５．１　今後、集中的に取り組むべき３つの課題

ＩＰインフラにおいてセキュリティを確保していく上で、今後、集中的に取り組んでいく必要があるのは、次の３つの課題であると考えられる。

（１）ＩＣＴ障害の広域化への対応

ブラスターやソービッグＦ等のネットワーク感染型ワーム、Ａｎｔｉｎｎｙ等のＤｏＳ攻撃、さらにはボットネットの脅威というように、２００３年以降のＩＣＴ障害を特徴付けるのは、障害が広域に及ぶという点である。

経路障害の誤りによるＩＣＴ障害も、広域にわたって影響が及ぶ可能性があり、社会インフラとしてのインターネットを機能不全にする恐れがある。

そこで、まず、こうしたＩＣＴ障害の広域化に、どう対応していくかが今後の重要な課題であると言える。

（２）ユビキタスネット社会への対応（情報家電のネットワーク接続への対応）

次に、ユビキタスネット社会の到来に伴い、情報家電に代表される様々なモノがネットワークに接続され、ＩＰインフラ自体が多様化・高度化する中にあって、接続性の確保や機器認証、インターネット全体に与える負荷軽減、業界をまたがる障害対応の迅速化を確保していくことが課題となる。

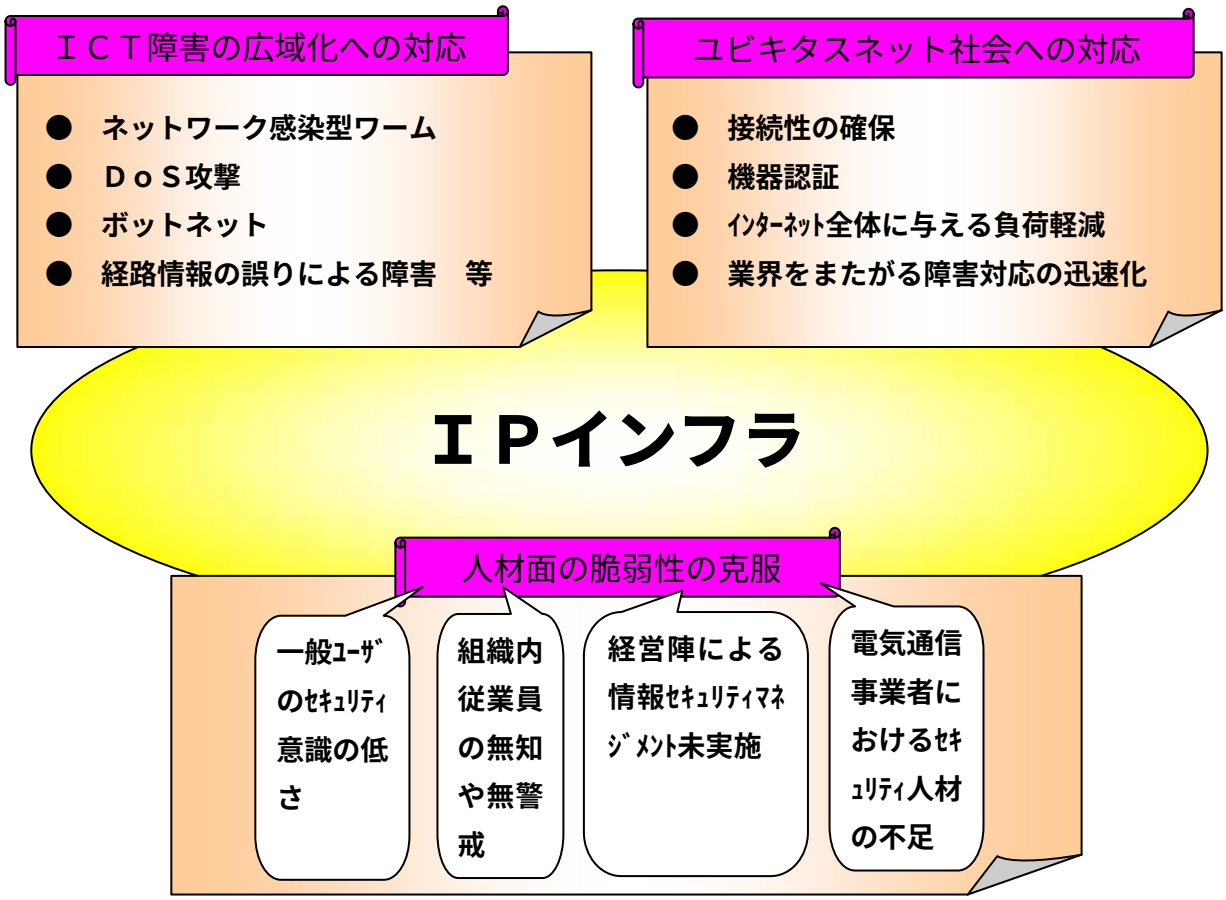
消費者の視点からみると、家電がインターネットに接続され、通信機器として機能すると、情報セキュリティ上の問題も発生し得るということを認識していない者も多いと考えられるところであり、「誰でも、簡単かつ安全に」家電を利用できるようにするためのセキュリティ基盤を確立することが求められていると言える。

（３）人材面の脆弱性の克服

あらゆるセキュリティ対策を講じる上で基盤となるのは人材であるが、情報セキュリティにおいて最も脆弱なのは人間である。

一般ユーザのセキュリティ意識の低さ、組織内従業員の無知・無警戒、経営陣による情報セキュリティマネジメントの未実施、ＩＳＰ等電気通信事業者におけるセキュリティ人材の不足など、人材面の脆弱性は多層にわたっており、これを克服する取組みを早急に実施していくことが求められる。

▽　今後、集中的に取り組むべき３つの課題



５．２　「情報セキュリティ政策２００５」

これら集中的に取り組むべき３つの課題に対し、誰が、何時から、どのように取り組むべきかについてまとめてみると次のとおりであり、行政においては、これらの取組みをパッケージ化し、「情報セキュリティ政策２００５」として包括的かつ精力的に推進していくことが望まれる。

（１）ＩＣＴ障害の広域化への対応

１）広域モニタリングシステムの構築・強化

まず、ＩＣＴ障害の広域化への対応については、ＩＳＰ１社のみの対応では限界があり、ＩＳＰ等が連携して、広域モニタリングシステムを構築すること等により、インシデント情報を共有し分析することが有効である。

この点に関し、Telecom-ISAC Japan **では、２００４年度から広域モニタリングシステムを構築しているが、**

①　ブロードバンド環境下で伝送される大容量データをどのようにすれば解析できるのか、

②　「通信の秘密」の保護や個人情報保護法に抵触しないようトラヒック情報やログ情報の把握をどの程度、またどのように仮装(masking)**し抽象化して把握すべきか、**

といった技術上・制度上の事項があることから、今後、Telecom-ISAC Japan **等の関係機関に政府もオブザーバとして参加する形で、事業者と行政とが協力して取り組んでいくことが適当である。**

２）ボットネット対策に関する研究開発

２００４年は、ボットネットの存在が認知され、その性質と対策の難しさが認識された年であり、効果的な対策はまだ見出されていない。

このため、ボットプログラムの感染防止と早期駆除、ボットネットによる攻撃の予防と防御について、セキュリティ・ベンダー、通信機器メーカ、ＩＳＰとが協力して早急に研究開発に着手すべきである。

行政においても、こうした研究開発に対し、２００６年度以降の支援策を検討するとともに、研究開発の推進に当たって必要となるトラヒック情報やログ情報の収集が「通信の秘密」や個人情報保護法に抵触しないよう適宜助言することが求められる。

３）経路情報の誤りによるＩＣＴ障害の検知・回復・予防に関する研究開発

経路情報の誤りによるＩＣＴ障害についても、障害の回復に相当の時間を要していることから、障害の広域にわたる検知、回復、予防を可能とする研究開発に、ＩＳＰが連携して早急に取り組むことが有効であり、行政としてもこうしたＩＳＰの取組みを支援していくことが求められる。

（２）ユビキタスネット社会への対応（情報家電のネットワーク接続への対応）

１）接続検証と規格化

そもそも、情報家電によるサービスの実現に当たっては、情報家電、構内ネットワーク、ゲートウェイ、加入者回線網、ＩＳＰ、ＡＳＰと多段階にわたる接続検証を重ねる必要があり、業界の枠を超えて接続検証と相互利用可能な規格化を行うことが適当である。

その際には、責任分界の明確化、接続管理方式の策定等の作業も併せて行うことが望ましい。

２）機器認証

構内の情報家電により構外からのサービスを利用するに当たっては、構内の情報家電側から構外の機器を認証することが必要であるとともに、構内にある情報家電が適切なものであるかどうかについて構外の機器から構内の情報家電を認証することも必要であることから、情報家電の普及を図っていくためには、機器認証が重要な課題となる。

この機器認証について一定の規格化を図ることで、提供側にとっては費用削減、ユーザ側にとっては利便性の向上につながることから、どこまで規格化することが適当かについて、関係業界で十分に検証し、調整することが必要である。

３）インターネット全体に与える負荷軽減（情報家電がボット化した場合の対応）

ＩＳＰからすれば、情報家電機器も、コンピュータと同様、ワームやボットプログラムに感染する可能性のある端末機器であり、例えば、情報家電機器がボット化し、ＩＳＰの電気通信設備の機能に障害を与える場合又は他のユーザに迷惑を及ぼす場合には、接続の停止又はサービスの停止を行うことがあり得る旨を、約款又は契約で予め明確化し、ユーザに周知しておくことが必要である。

４）業界をまたがる障害対応の迅速化

情報家電のセキュリティ確保に関する課題の根底には、家電業界の技術者は、インターネットの技術を十分に知らず、逆に、インターネットの技術者は、家電側の要求をよく知らないという事情があること等から、家電業界とＩＳＰ業界との間で業界横断的なセキュリティ情報の共有・分析を行うとともに、障害発生後の対応の迅速化に向けた取組みを推進していくべきであり、行政においても、こうした業界横断的な取組みを支援していくことが望まれる。

特に、①情報家電を攻撃対象とするインシデントは、例えば風呂を沸騰させ又は部屋を冷却すること等により、場合によっては人命に関わる事態につながりかねないこと、②情報家電を踏み台としたインシデントは、情報家電の総数が多いだけにインターネット全体に過剰な負荷を与えかねないこと、③現段階でセキュリティ対策を講じないまま脆弱な機器が出回ると回収が困難なこと等の事情があるとことから、インターネット全体に与える負荷を軽減するとともに、人命に関わる事態につながらないよう家電の作動範囲を規定することが求められる。

（３）人材面の脆弱性の克服

１）一般ユーザへの啓発

一般ユーザへの啓発は、今すぐに取り組まなければならない事項であり、セキュリティ・ベンダー、システム・インテグレータ、ＩＳＰ、通信機器メーカ、行政等が連携して、セキュリティに関する情報を分わかりやすく、迅速かつ確実に一般ユーザに提供することが重要である。

その際、ブロードバンドの普及により、トラヒックの受発信に関してユーザが大きなパワーを有している状況にかんがみると、インターネットにおいてセキュリティ対策を講ずるべき主体はＩＳＰのみではなく、ＩＳＰ、システム・インテグレータ、ユーザ等の関係者による取組みがどれ一つ欠けても十全なセキュリティ対策を講じることができない、という考え方を社会一般に醸成していくことも求められる。

特に、大量のデータ送信や他のユーザからの苦情申告等により、ユーザのコンピュータがボット化していることが判明した場合には、当該ユーザに対する個別の注意喚起や駆除の方法に係る情報提供を行う等、これまでよりも一層踏み込んだ形で啓発を行うことが必要である。

更に、ボット化したユーザのコンピュータが発生させるトラヒックがＩＳＰのサービスに支障を来たすような場合等においては、警告、利用の一時停止、更には契約解除といった措置をとることがあり得る旨を、約款又は契約で予め明確化しておくことも求められよう。

２）ソーシャルエンジニアリングの研究と対応策の提示

組織内従業員等の無知や無警戒、あるいは心理や行動様式につけ込んで組織のセキュリティを侵害する手法は、「ソーシャルエンジニアリング（social engineering）」と呼ばれ、米国等では既に研究が進んでいるところであり、我が国においても早急に研究を進め、攻撃を受ける側にとって有益な情報提供と対応策の提示を行っていくことが必要である。

３）ＩＳＭＳ－Ｔの国内における普及促進と国際規格化への貢献

情報セキュリティマネジメントについては、経営陣においてセキュリティポリシーを確立し、これに従って従業員教育やセキュリティ対策を実施していくこと等が極めて重要である。

この点に関しては、ＩＳＯ／ＩＥＣが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）についての国際規格を２０００年に策定しているほか、ＩＴＵが２００４年に電気通信事業分野を対象としたＩＳＭＳ（ＩＳＭＳ－Ｔ）を勧告しており、今後、こうした国際規格を国内で普及促進していくため、電気通信事業者と行政とが連携して、ＩＳＭＳ－Ｔの実施要件を２００５年中にも提示すべきである。

その際、一般の企業を対象とする汎用的なＩＳＭＳは、現在、改訂作業が進められており、この改訂版は２００５年後半にも発行されるものと想定されることから、ＩＳＭＳ－Ｔについても、この改訂版の内容を踏まえることが必要である。

また、現行のＩＳＭＳ－Ｔは、例えば「法適合性」（Compliance）について、通信の秘密の保護、重要通信の優先取扱い、接続、設備の責任分界等、電気通信分野に固有の内容は規定されていないことから、ＩＳＭＳ－Ｔの国内における普及促進を図るに当たっては、電気通信分野に固有の法令上の要求事項を踏まえることも求められる。

更に、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、その時までに国際的にも評価される提案を我が国として準備しておくことが期待される。

４）事業者をまたがる総合的な演習の必要性

あらゆるセキュリティ対策を講じる上で基盤となるのは人材であるが、当研究会が２００５年４月に実施した我が国の電気通信事業者に対するアンケート調査では、約４分の３の事業者においてセキュリティ人材が不足している状況にある。

電気通信事業者の現状をみると、社外の研修事業者によるセキュリティ講習等が活用されているが、従業員を参加させるに当たって負担の大きい中小規模の電気通信事

業者や、地元で講習会が開催される機会の少ない地方の電気通信事業者にとって利用しにくい面があり、今後、中小又は地方の電気通信事業者への浸透を強化することが求められている。

また、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く、インシデント事案の広域化やボットネット等による組織的攻撃の増加などの最近の傾向にかんがみると、電気通信事業者間及び電気通信事業者と行政との間で連携して、セキュリティ対策を講じることのできる人材が求められる。

特に、大規模なインシデント事案に際しては、「高度なＩＴスキルを有する人材」のほかに、これら「高度なＩＴスキルを有する人材」の協力体制を促進することのできる調整力のある人材を、プロジェクトリーダーとして育成し、専従的に確保することも必要であると考えられる。

米国でも攻撃を想定した総合的な演習が数次にわたり実施されていることから、我が国においても、①セキュリティの専門家により実行可能な攻撃方法と攻撃による損害を検証するとともに、②攻撃発生後の緊急対応体制が実際に機能するか否か等について演習を通じて検証するべきである。

また、こうした演習には、セキュリティ講習等に参画できる機会が相対的に少ない中小又は地方のＩＳＰや、セキュリティに関する考え方や言葉遣いが異なる場合のある情報家電機器メーカの参画を得ていくことが望ましい。

▽　「情報セキュリティ政策２００５」

課題	小分類	政策の内容	何時から	誰が				
				ISP	ﾒｰｶ	ｾｷｭﾘﾃｨ・ﾍﾞﾝﾀﾞｰ	行政	ﾕｰｻﾞ
ICT 障害の広域化	ﾈｯﾄﾜｰｸ感染型ﾜｰﾑ	広域ﾓﾆﾀﾘﾝｸﾞｼｽﾃﾑの構築･強化	04 年～	◎	◎	◎	○ (06 年以降の支援策検討)	
	ﾎﾞｯﾄﾈｯﾄ	ﾎﾞｯﾄﾈｯﾄ対策に関する研究開発	早急に	◎	◎	◎	○ (06 年以降の支援策検討)	
	経路情報の誤り	障害の検知･回復･予防に関する研究開発	早急に	◎			○ (06 年以降の支援策検討)	
ﾕﾋﾞｷﾀｽﾈｯﾄ社会におけるｾｷｭﾘﾃｨ確保	接続性の確保	業界横断的な接続検証と相互利用可能な規格化、責任分界の明確化	早急に	◎	◎		○ (06 年以降の支援策検討)	
	機器認証	規格化	早急に	◎	◎	◎	○ (06 年以降の支援策検討)	
	ｲﾝﾀｰﾈｯﾄに与える負荷軽減	ﾕｰｻﾞへの啓発 約款等の明確化	05 年～	◎	○		○	○
	業界をまたがる障害対応の迅速化	業界をまたがる情報交換･情報交流、 家電の作動範囲規定 総合的な演習	早急に	◎ ◎	◎ ◎ ◎	◎	○ ◎ (06 年以降の支援策検討)	
人材面の脆弱性	一般ﾕｰｻﾞ	啓発	今すぐ	◎	◎	◎	◎	○
	組織内従業員の無知、無警戒	ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞに関する研究と対応策の提示	早急に	◎	◎	◎	◎ (06 年以降の支援策検討)	○
	経営陣による情報ｾｷｭﾘﾃｨﾏﾈｼﾞﾒﾝﾄ	ISMS-T の普及促進（実施要件の提示）	05 年中	◎	◎	◎	◎	
		ISMS-T の充実に係る国際貢献	05 年～	◎	◎	◎	◎	
	ｾｷｭﾘﾃｨ人材の不足	演習を通じ、ｲﾝｼﾃﾞﾝﾄに円滑に対応できる人材の育成	早急に	◎	◎	◎	◎ (06 年以降の支援策検討)	

◎は主体的に取り組むべき主体、○は◎の支援者又は政策の対象者。