資料１－４

平成 15 年 1 月 24 日

情報セキュリティの課題と方向性（議論の叩き台）

インターネットは、当初、科学者等の限られた利用者間の情報共有手段であったものが、その後、一般の利用者に開放されたことから、社会全体に急速に普及し、世界を結ぶ重要な社会基盤として発展している。誰でもネットワークに容易に接続でき、世界中の様々な情報に接することができる状況が出現したことは、情報流通の円滑化という面では革命的な進歩であるが、逆に世界のどこからでも不正なアクセス等が行われる機会も増大している。また、システムが複雑化・巨大化するにつれてソフトウェアのセキュリティホールも次々に発見される状況が続く一方で、インターネットからは、不正アクセス等を行うために簡単に利用可能なツールが入手可能となっている。

このような急激な状況変化に対応するため、世界的にも、制度や体制の整備、人材育成などが急務となっているが、情報セキュリティ対策が直接に利益や便益を生むものではないために、具体的な脅威が現実化するまでは一般にその重要性を認識されにくいという性格を有している。技術的側面においても、インターネットの基盤となっている技術（IPv4）は、部分的な改良は行われているものの、基本的に開発当時のものが継承されてきた。しかしながら、実用化が進みつつある次世代の IPv6 は、インターネットの基本的な機能の中に情報セキュリティ対策技術を標準的に装備した点で、大きな転換を示すものといえよう。

我が国においても、最近、不正アクセス（図 1）やウイルス被害の急増、ホームページの改ざんなどの被害発生が増大している。近年、ADSL などによるインターネットへの常時接続が急速に普及しているが、自らの端末への攻撃だけでなく、他のサイトを攻撃する際の踏み台としても使われてしまうおそれも増大しており、不正アクセス等への対策が一層必要になってきた。また、電子政府システム（参考 1）の本格稼動による行政サービスの充実、電子商取引をはじめとするネットワークビジネスの発展のためには、情報セキュリティを確保することが極めて重要である（注）。

（注）インターネットショッピング等は着実に浸透しつつあるものの、決済方法に不安を感じる等の理由から、インターネットショッピングの利用を敬遠する利用者もいる（図2）

図1　不正アクセス等の報告件数の推移（JPCERT／CCへの報告）

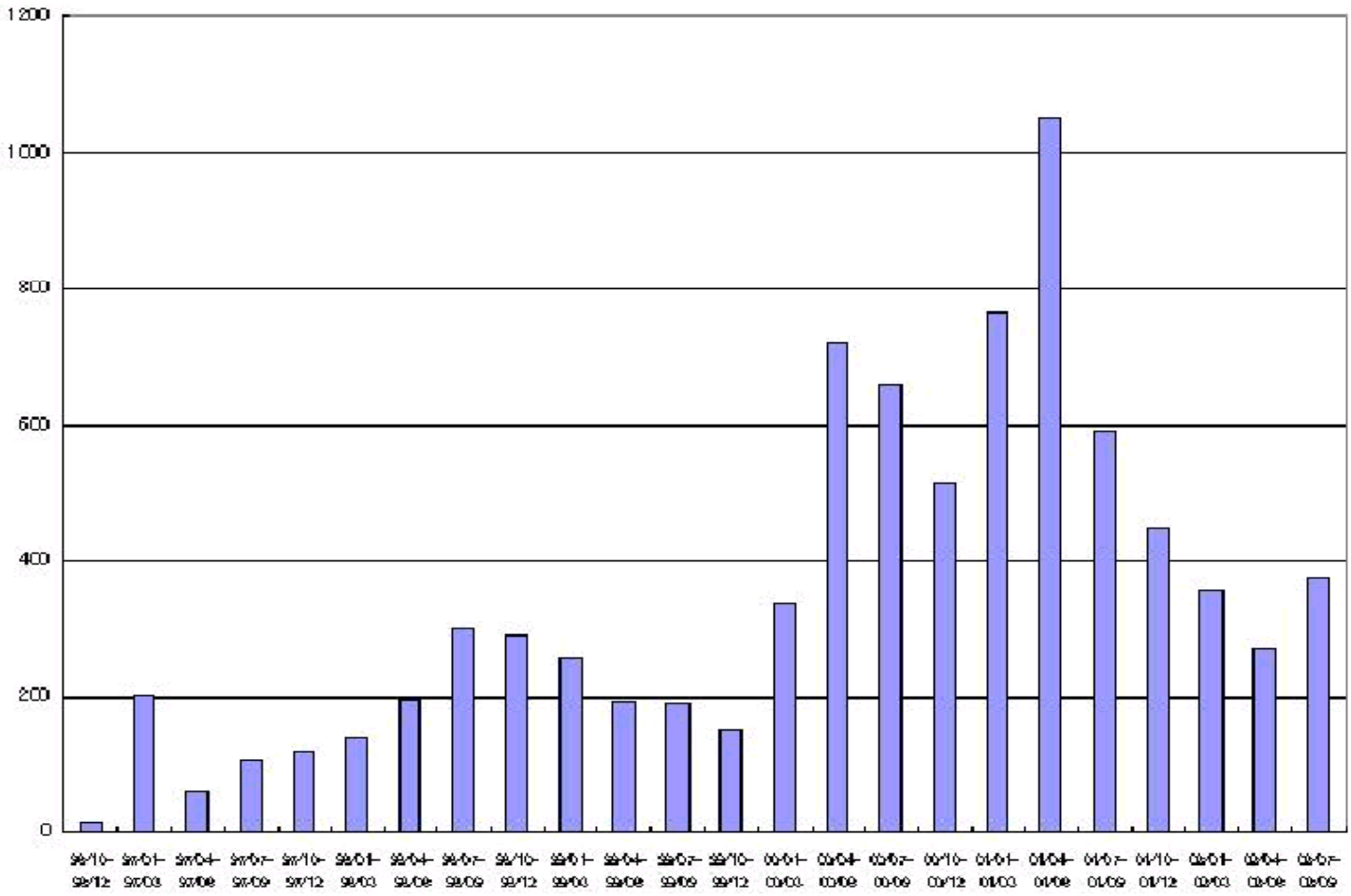
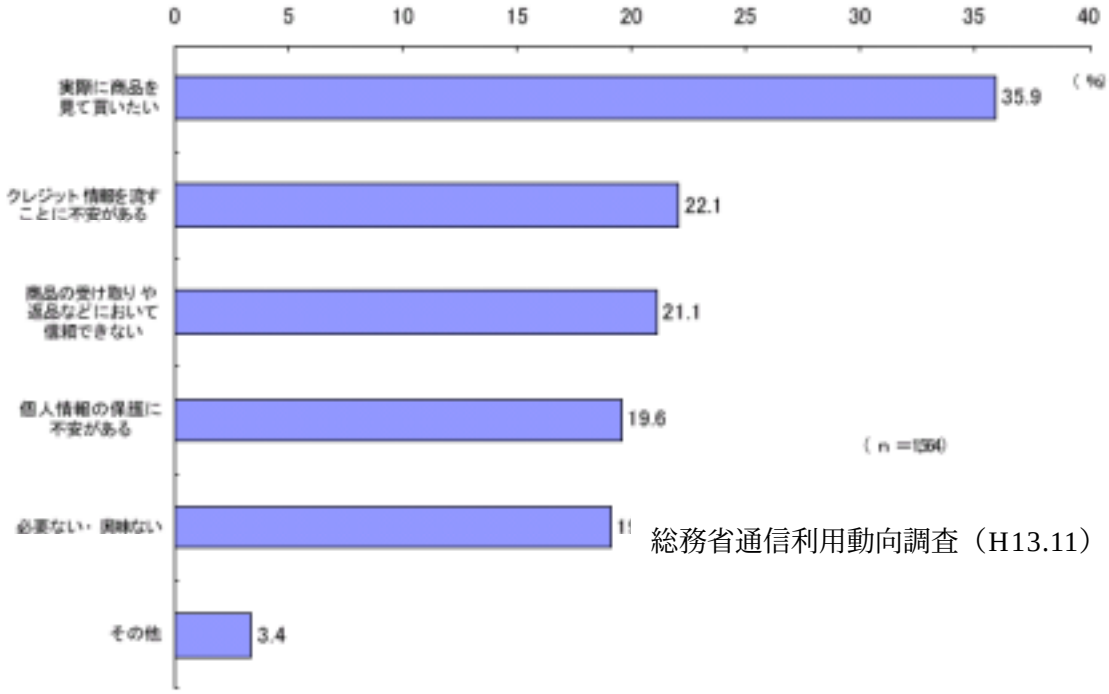


図２　オンラインショッピングを利用しない理由(インターネット 利用世帯主)



総務省通信利用動向調査（H13.11）より

１．情報セキュリティの現状

（１）我が国の意識と対策

これまで長い間、極めて安全性の高い社会であった我が国において、情報セキュリティに対する漠然とした不安は大きいものの（図 3、4）、

- 具体的な対策としては ID やパスワード、ファイヤーウォールのみの対応が大部分であり、暗号や認証、回線監視などを含め、本格的な対策を講じるまでには至っていない（企業の例：図 5）
- 前述したように情報セキュリティ産業の規模が非常に小さいこと
- 情報セキュリティの人材が極めて少なく育成体制も整備されていないこと

などにもみられるように、社会全体として、情報セキュリティ対策を具体的に講じるという意識が決して高いとは言えず、まずセキュリティ文化を高める教育の重要性が指摘されている。また、情報セキュリティのような総合的で体系的な対策が必要な分野は、我が国はあまり得意ではないといわれている。

図 3　インターネットの不安や不満

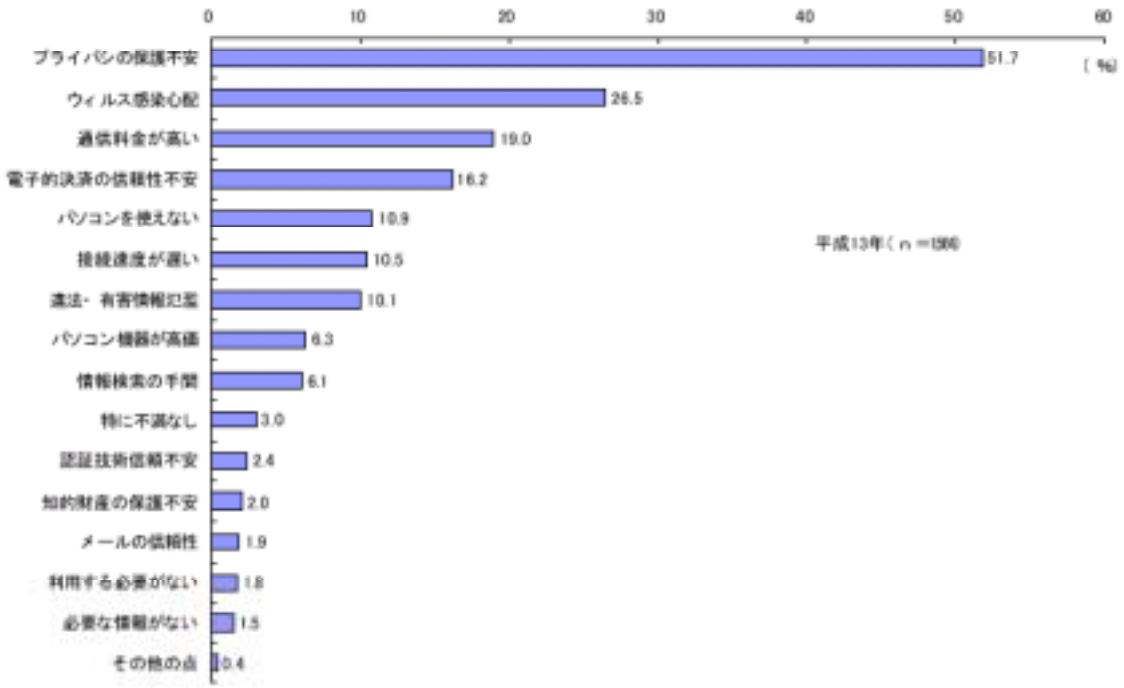
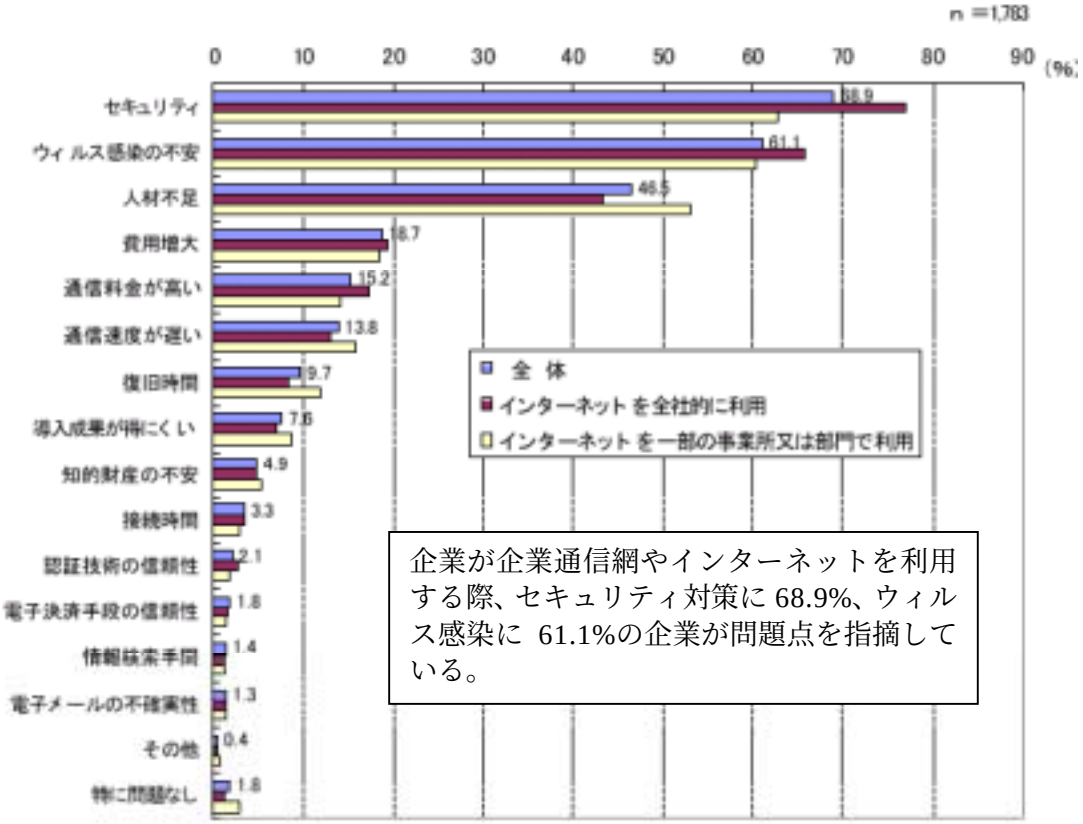


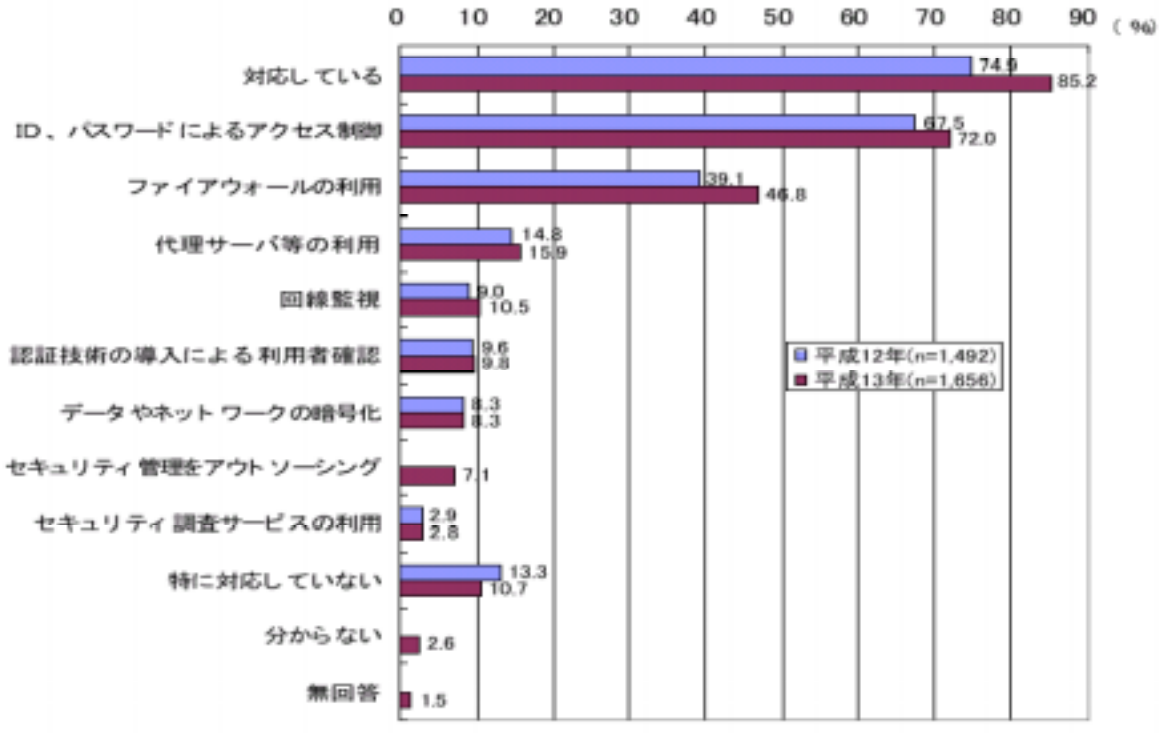
図４　　企業通信網やインターネットの利用上の問題点

総務省通信利用動向調査（H13.11）より



企業が企業通信網やインターネットを利用する際、セキュリティ対策に 68.9%、ウィルス感染に 61.1%の企業が問題点を指摘している。

図５　　通信ネットワークのデータセキュリティに関する対応（複数回答）



（２）情報セキュリティ対策の体制

①ガイドライン等

○政府の情報セキュリティ確保

・情報セキュリティポリシーに関するガイドライン（H12.7 策定、H14.11 一部改定）

・電子政府の情報セキュリティ確保のためのガイドライン（H13.10 策定）

○重要インフラ防護のためのサイバーテロ対策

・重要インフラのサイバーテロ対策に係る特別行動計画（H12.12 策定）

・サイバーテロ対策に係る官民連絡・連携体制について（H13.10 策定）

・ネットワークに関するセキュリティ・ガイドラインとしては、総務省の「情報通信ネットワーク安全・信頼性基準」が制定されており、さらに一定の安全・信頼性対策が実施されている情報通信ネットワークについて、登録・公表が行なわれている。

②システム評価、マネージメントの基準と評価機関

情報セキュリティを確保するための国際的な基準については、平成11年にＩＴ製品及びシステムのセキュリティを評価するための国際基準 ISO/IEC15408 が、また平成 12 年に情報セキュリティマネジメント（運用・管理）の国際基準 ISO/IEC17799 が制定されている。しかし、これらの基準もまだ完全なものではなく、また各国、各機関の対応状況も様々であるため、今後とも、これらへの対応を促進すると同時に、基準を改善する努力を継続する必要がある。

○ISO/IEC15408（注 1）に基づき、電子政府に利用する IT 製品、システムを評価するための認定されたセキュリティ評価機関としては、JEITA の IT セキュリティセンター、ECSEC（電子商取引安全技術研究組合）がある（注 2）が、要員の拡充が急務となっている。

○ISO/IEC17799 に基づき、情報セキュリティマネジメントの確立を評価する民間認証制度が運営されている。日本情報処理開発協会（JIPDEC）が、制度の運営、審査登録機関の認定を行なっている。

（注１）ISO/IEC15408 に基づく IT セキュリティ評価・認証制度に関し、その認証結果を相互に承認する国際相互承認スキーム CCRA（Common Criteria Recognition Arrangement については、現在、米、英、加、仏、独、豪、ニュージーランド、

オーストリアなど 16 か国が加盟しているが、我が国も、平成 15 年春～夏の参加を目指して準備中である。

（注２）これら 2 機関は、平成 14 年 12 月 20 日、(独)製品評価基盤機構より保証レベル 3 の認定を取得。この他に、セキュリティターゲット主任評価者を擁し、セキュリティターゲットの評価を行える企業もある。

各省庁の情報システム構築で、可能な限り ISO/IEC15408 に基づき評価・認証された製品等の利用を推進することとされている（行政情報化推進各省庁連絡会議了承、H.13.3.29）。

③インシデント対応組織

○2002年4月に内閣官房に設置された緊急対応支援チーム（NIRT）が、電子政府及び民間重要インフラ事業者を対象に、以下の活動を実施している。

・政府として緊急に執るべき措置に関する検討
・各省庁への助言、指導、調整等

○JPCERT/CC 及びIPA の2組織が、わが国におけるコンピュータ利用者全般を対象に情報収集・提供、インシデント対応支援活動を実施している。

・JPCERT/CC：不正アクセス行為への対応
・IPA ：コンピュータ・ウイルスへの対応、インシデント全体の届出受理

（注）米国のCERT/CCが、米国内のみならずインターネット全体を対象とするインシデント対応の中心として活動

○企業・業界レベルでのインシデント対応組織については、わが国は、英米と比較して極めて手薄であり、今後の充実が望まれる。

（注）米国では、業界団体や企業・機関レベルの組織が重層的に多数設置。民間の重要インフラ業界ごと（通信、情報、電力、金融など）に、インシデント情報を収集・分析し共有する情報共有分析センターISAC（Information Sharing and Analysis Center）を設置。

日本では、2002 年 7 月に、電気通信業界で Telecom - ISAC Japan が設立された。

○情報セキュリティ技術を研究開発するためにも、インシデント情報の分析が不可欠である。このため、例えばネットワークリスクマネジメント協会（NRA）が米国インターネット セキュリティ システムズ㈱（ISS）のX-Forceセキュリティ研究開発チームが世界中から

収集しているデータベースを日本語化して公開している。

④電子認証

現在、民間の PKI サービスのほかに、電子政府のインフラとして、国の行政機関（官職）の認証を行なう GPKI、地方自治体（官職）の認証を行なう LGPKI、住民の認証を行なう公的個人認証基盤 JPKI の整備が進んでいる。しかし、これらの制度も利用者の利便性の観点から、不断の見直しを行なう必要がある。また、情報セキュリティの共通基盤として、これら PKI やタイムスタンプなどの電子認証技術の信頼性向上等を図る必要がある。

（3）情報セキュリティ対策の特徴

情報セキュリティ対策においては、技術、体制、利用者の意識、システム評価、運用・監視等、全体としてバランスよく総合的に対応する必要がある。これら計画・実施・評価・監視の動的プロセスを常に回転させる必要があり、中でも情報通信システムの評価と運用、全体を管理するセキュリティマネジメントの体制、何か起きたときの危機管理体制を整備することが重要である。また技術的にも、弱い部分への攻撃を防ぐため、暗号技術等の基盤技術、ウィルス対策、不正アクセス対策など、様々な技術を適切なレベルで組合わせてシステムを構築する必要がある。詳細は後述するが、例えば、情報セキュリティのインシデントの大半は、組織内部の問題に起因すると言われており、その対策技術なども重要である。

なお、これらの対策が妥当なものであることを確認するためには、独立した者によって評価を受ける情報セキュリティ監査の実施が有効である。

さらに、いまや情報通信ネットワークが世界中に張り巡らされ膨大な情報が流通している現状では、ウィルスが非常に早い速度で世界中に蔓延すること、世界的に弱いところが狙われネットワーク全体が大きな被害を被るおそれがあること、などから、我が国の対策を考える上で国際的動向を十分に視野に入れるとともに、国際的な情報交換・連携を一層深めることにより、国際的に情報セキュリティを高めていく必要がある。

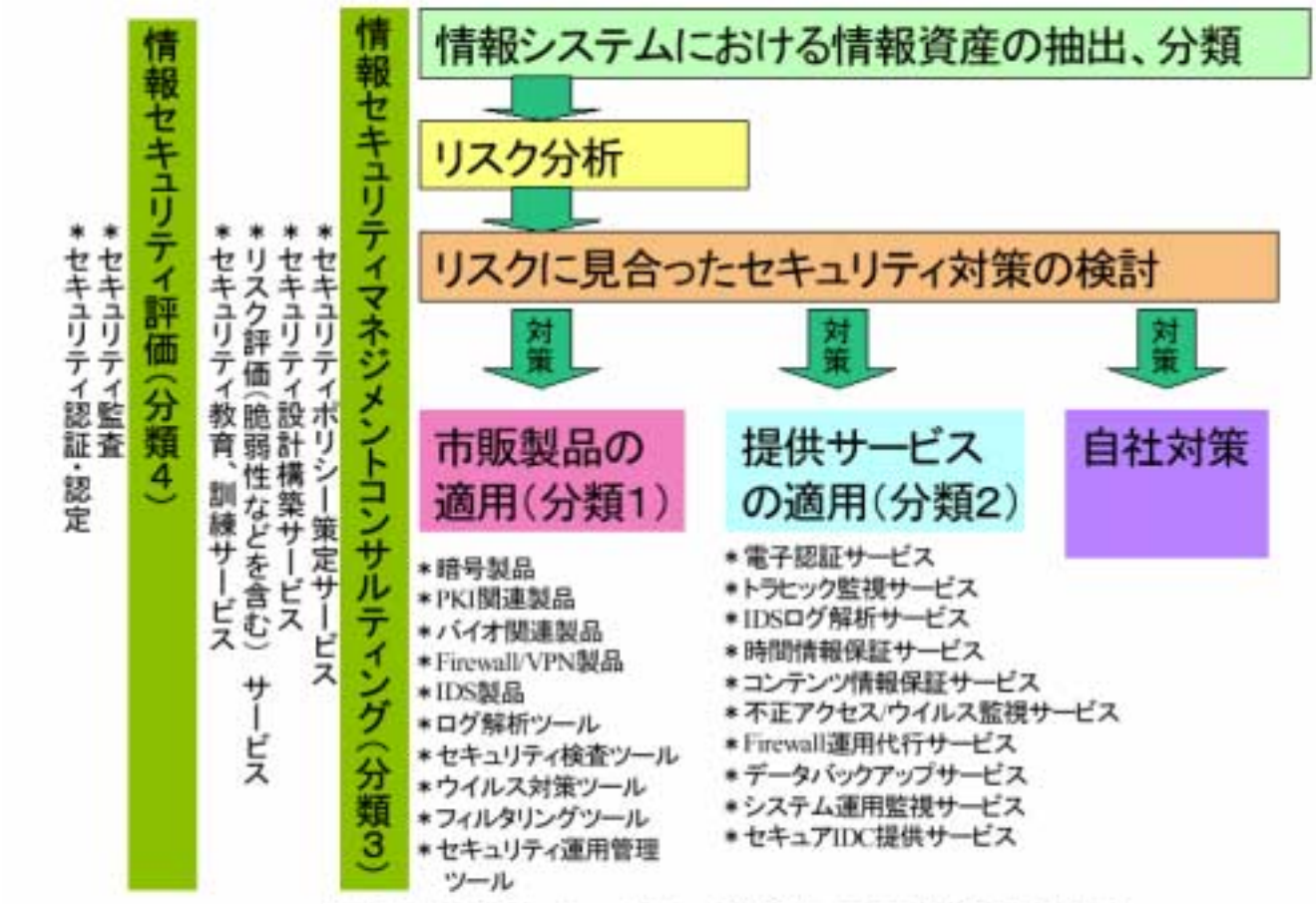
（4）セキュリティビジネスの市場規模

米国の情報セキュリティ市場規模は、7,351 百万ドル（約 8,500 億円、情報処理事業振興協会「情報セキュリティの現状 2001 年版」）と大きな産業に育っているが、日本はその約 10 分の 1 の約 867 億円と大きな格差がある。しかし逆にいえば、今後情報セキュリティ市場が我が国でも大きく

成長する可能性があるといえ、その意味からも本分野の研究開発及び人材育成が重要である。

なお、情報セキュリティに関するコンサルティングや診断サービスを提供している企業は、我が国でもメーカー系、キャリア系、コンサル会社系、独立系などがあり、これらの企業では、人材育成（研修）サービスも同時に実施しているが、欧米と同様にサービス分野はまだ発展段階にある。

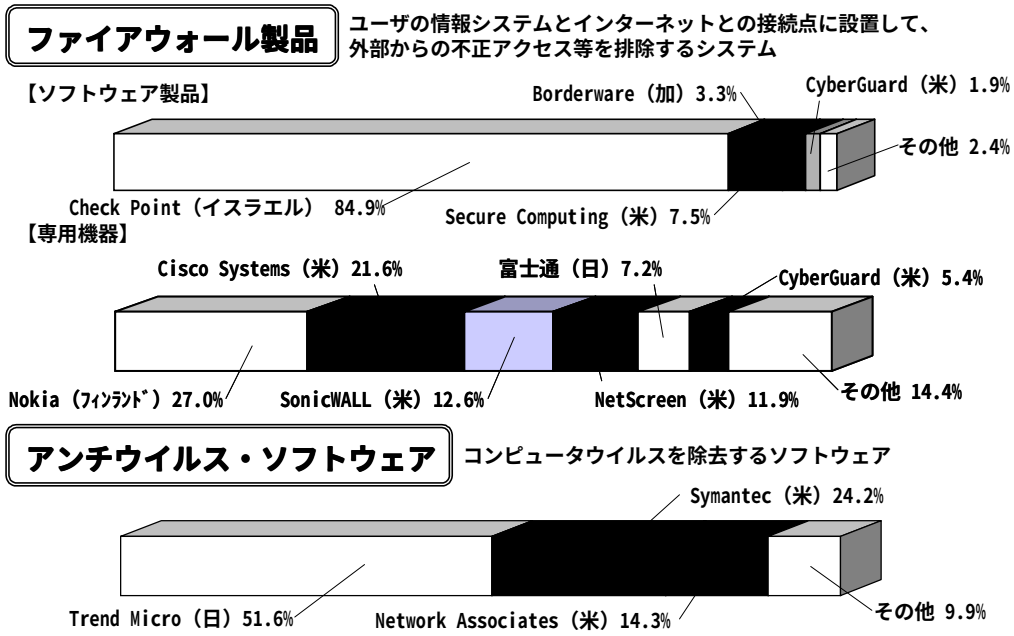
図 6　情報セキュリティビジネスの分類



情報セキュリティ・ビジネスの発展と官民連携のあり方に関する調査研究会 報告（総務省）より

セキュリティ製品の世界市場シェアの例を図 7 に示す。例えばファイアウォールのうち、ソフトウェアはイスラエル企業がほぼ独占状態にあり、ハードウェアについても欧米企業に席巻されている。一方で、ウィルス対策ソフトについては、日本に本社を置くトレンドマイクロ社が半分以上の市場シェアを有している。

図 7 セキュリティ・ソフトウェア（売上ベース）



出典：富士キメラ総研「２００２ネットワークセキュリティビジネス調査総覧」

３．研究開発の方向性

日本と海外における研究開発テーマの分布を比較するための一つの指標として、論文テーマの分類（参考4　表1）をみると、我が国においては、暗号技術の研究が47%、認証技術が33%に対し、ファイアウォール、侵入検知システムなどのアクセス管理技術はわずか6%であるのに対し、海外は暗号技術14%、認証技術29%、アクセス管理技術28%とアクセス管理技術の比重が大きい。一方、内外ともに、要素技術に比して、システム技術、社会技術関連の研究論文は少ない。ただ、最近は、この状況も多少改善されてきた模様である。

（注）要素技術：暗号技術、認証技術、アクセス管理、デジタル署名
システム技術：ウィルス対策技術、ネットワーク安全性技術、自動修復技術、脆弱性分析、リスク評価、相互依存性
社会技術：リスクコミュニケーション、ユーザインターフェース

（１）我が国における研究開発の現状と、強化すべき研究開発項目

我が国における研究開発の状況に関する資料しては、例えば参考4 表2がある。この資料もふまえつつ、今後強化すべき研究開発項目を、以下に示す。

①要素技術

要素技術、特に暗号関連技術については、産官学で基礎的な研究開発段階から製品開発レベルまで多様な研究が行われているが、以下の点については一層強化する必要がある。

- **暗号関連**
  より安全な暗号技術の開発を継続すると同時に、暗号強度の評価技術や暗号解読技術、暗号実装技術及び実装評価技術を強化する必要がある。
- **アクセス制御**
  ファイアウォール、侵入検知システムといったアクセス管理技術については、実用化段階の研究開発が行われているが、人工知能型の高度な侵入検知、誤報の確率を大幅に低減する確度の高い検知技術、内部からの脅威に対応する技術の開発が重要である。
- **真正性保持技術**
  電子透かしや電子署名などの真正性保持技術も、実用化が進んでいるが、利用者が安心感を持てるようなヒューマンインタフェースの開発が望まれる。また、現状では一定の期間がたつと電子署名の有効性の確認が困難となるため、長期間（数十年単位）に渡ってその真正性が確認されるような有効性確保技術の開発、関連の制度整備が必要である。
- **個人情報保護技術**
  個人方法の流れを制御する技術に加え、PKIなどのセキュリティ応用技術において個人情報が必要以上に他人に知られないための仕組みも重要である。

②システム的なセキュリティ技術

システム（ネットワークやソフトウエアなど）としての情報セキュリティ技術の研究開発は、要素技術に比べて相対的に遅れており、以下の研究開発が重要である。

- **新しい領域、統合的な対策**
  特に、モバイルやユビキタスネットワーク、グリッド・コンピューティングなどの新しい領域における情報セキュリティ技術の研究開発を早急に進める必要がある。
  例えば、ネットワークやシステムについて、高度なセキュリティ機能を有したネットワーク基盤実現のため、ネットワーク層認証を活用したセキュア・サービス・プラットホームの構築や、セキュアチ

ップを搭載した機器とICカードの連携によるセキュアなサービス利用のためのシステム開発などを推進する必要がある。
また、OS、ネットワーク、応用ソフトなど、異なる階層にまたがる統合的なセキュリティ対策として、個々のシステム構築時のノウハウを共有、体系化する取組が行われていない。
（注）以下の技術は、平成15年度予算で研究開発を開始する予定。
・ビジネスグリッドコンピューティングの安全性技術
また、以下の技術は平成 13 年度から研究開発が実施されているが、今後さらに充実を図る必要がある。
・ネットワークインフラのサイバー攻撃耐性・回復技術
・相互接続ネットワーク全体のセキュリティ制御統制技術

- ログ管理、ウィルス対策

不正アクセスを解析するためのログ管理において、現状では不正アクセスと同時にログが改ざんされるおそれがあるため、ログの安全な保管技術を開発する必要がある。また、ウィルス対策にも、免疫学的知見を応用する技術などの研究開発を推進する必要がある。

- 危機管理等

予防的な対策に比較すると、攻撃を受けた際の危機管理、攻撃後の情報復元やシステム再構築などの研究開発は一層少く、例えば、攻撃を防ぎきれない場合に重要なシステムをネットワークから切離すなど、攻撃の被害を最小化するシステム設計技術、システム障害の発生に備えて情報を隔離保存しておき迅速にシステムを復元する技術、暗号が破られた時にシステム再構築を容易にするための暗号実装技術などの研究開発が重要である。

- システム評価

システムセキュリティ評価があまり実施されていないため、それに必要なリスク評価、脆弱性分析などの研究開発を一層強化する必要がある。特に、完全に安全な情報セキュリティはあり得ないため、体系的なリスク評価を行い合理的な対策を選択すること、常にシステムを見直すことが重要である。

③社会技術的分野、管理・評価・運用等の支援

- 社会技術的分野

組織内部からの攻撃に対する対策技術については、ほとんど研究開発が行われていない。また、クラッカーの行動科学的分析やセキュリティ・ユーザインタフェースなど人間や社会を要素として考慮する社会技術的な分野においては、課題によって研究手法が確立して

いないものもあるが、情報セキュリティを確保するためには不可欠な分野であり、本格的に研究開発を開始する必要がある。また、漠然とした不安に対して安全性を納得させる方法、安全性の評価方法なども重要である。

- セキュリティ管理・評価、運用支援等

特に、電子政府や重要インフラのシステム改善、セキュリティ管理・評価、運用を支援するため、社会科学も包含した形でセキュリティ管理・評価ツール、運用支援ツール、体制・運用構築支援ツールの研究開発を推進する必要がある。
この際、組織内部からの攻撃、人間の行動とセキュリティとの関係も十分考慮し、また既存のツールも十分活用する必要がある。
ただ、欧米では情報通信システムのセキュリティを評価するためのツールが販売されているが、日本にはセキュリティの評価を行うためのデータ蓄積が不足しているため、ツールの開発が進んでいない。

- 非均一な環境でのセキュリティ支援技術

また、広域分散コンピューティングなど、複数のOS や不特定多数のユーザ、異なるネットワークで構成される非均一な環境下での、利用者の管理方針、新しいセキュリティポリシーの作成を支援する技術が重要である。

④この他、セキュリティ技術全体について、常に研究開発のレベル、スピードを再点検し、必要な加速・レベル向上を図る必要がある。

（２）推進体制

米国では、ホームランドセキュリティ法（2002 年 11 月）に基づき、国土安全先進研究庁（国土安全保障省）が設置され、また、サイバーセキュリティ研究開発法（2002 年 11 月）に基づき、米国立標準技術研究所（NIST）が産学官の研究開発を推進する体制に再編成される（参考 2）。

また韓国では、韓国科学技術院（KAIST）の情報セキュリティセンター（KISA）が民間の情報セキュリティを中心に、韓国電子通信研究所（ETRI）が国家セキュリティ技術研究所として政府機関の情報セキュリティを中心に、研究開発の拠点として活動している（参考 3）。

一方、我が国における情報セキュリティ技術の研究は、通信放送機構（TAO）、情報処理事業振興協会（IPA）、(独)通信総合研究所（CRL）、(独)産業技術総合研究所、大学などの一部で研究が行われている状況にあり、これらにおける研究開発の体制強化を図るとともに、相互の連携強化、人材交流等を推進していくことが必要である。

同時に、これらの機関の抜本的な強化あるいは新しい組織により、我が国における情報セキュリティの中核的な研究開発拠点を整備し、他の機関と連携しつつ研究開発を推進する体制を構築することについて検討する必要がある。

これらの機関は、相互に連携しつつ、以下のような活動について推進していくことが期待される。

- 実際のネットワークを用いて攻撃と防御を行いながら、実際に発生する問題点の洗い出し、改善策の検討などについて、フィールドにおける実証的経験に基づいた研究開発を行うこと
- 海外研究機関との研究成果交流・共同研究等を推進すること
- 最新の情報セキュリティ技術導入のためのテストベッドとしての機能
- 最新の知見に基づき、常に電子政府や重要インフラに関する技術的な問題点を洗い出し、内閣官房の活動を支援すること
- 情報系技術者と人文・社会学者との連携研究チームにより、セキュリティシステムのユーザーインターフェースやハッカー・クラッカーの行動科学的分析など社会技術的研究開発を推進すること

４．人材育成

○セキュリティ全般に関する社会的な関心の低さもあり、我が国の情報セキュリティ関連の人材は極めて層が薄く、量と質（経験、能力）とも大幅に不足しているといわれている。暗号技術については健闘しているものの、層は薄く、暗号以外の研究者の数は極めて少ない。特にセキュリティ監督体制が重要だが、専門的な能力を有する人材が極めて少ないといわれている。

○高度な技術者の育成には 7 年程度必要といわれており、早急に大幅な人材育成が必要である。

(1)人材育成の現状

①米国

○政府：日本より遥かに人材が豊富な米国でも、2 本柱の一つに人材育成（注）を据えた「サイバーセキュリティ研究開発法」により 2007 年までの 5 年間に総額 9 億ドル（約 1,100 億円）を投資（参考 2）。

（注）NSF を中心に専門家を育成するために大学や大学院

の教育プログラムに助成金を支給。

○資格：セキュリティ専門家認定については、公認情報システムセキュリティプロフェッショナル（CISSP：Certified Information Systems Security Professional）がある。

○大学：50 以上の大学で、大学院レベルを中心に情報セキュリティの教育コースを実施している。

○SANS 協会（System Administration Audit Network Security）：1989 年に設立された非営利の代表的ネットワーク・セキュリティー調査・教育組織。16 万 人のシステム・ネットワーク管理者、セキュリティ専門家が知識を共有し、直面する問題の解決策を模索する。また、ユーザを対象とする講習会（2001 年に 12,500 人が受講）、研究報告や各種情報提供を実施。
1999 年にセキュリティ技術認定プログラム GIAC（Global Information Assurance Certification）を開始。

②韓国（参考 3）

○韓国情報セキュリティセンター（KISA）や韓国電子情報通信研究所（ETRI）国家セキュリティ技術研究所から研究者・技術者を輩出

○大学に情報セキュリティの学科等が多数設置されている。

③日本

○大学：現在、大学の情報関係学科等の一部で情報セキュリティに関する講義も行なわれているが、情報セキュリティの学科はない。以下のような動きが始まっているが、更に充実させることが重要である。

・平成 13 年度の科学技術振興調整費で、早稲田大学及び大阪大学が講座を設置し人材育成を開始（参考 5）。

・中央大学が情報セキュリティの COE となり、その一環として副専攻コース（参考 6）を平成 15 年 4 月に設置する予定。

（注）この他、工学院大学は、ネットワークセキュリティ、知的財産、技術経営などのテーマについて、将来の専門職大学院、学部編成等を視野にいれて検討している。
また複数の自治体でも人材育成に関する検討の動きがある。

○民間：セキュリティ専門会社、コンサルティング会社、通信事業者、メーカー等が教育サービスを提供しているが、その内容やレベルは千差万別である。そこで、教育内容の作成や教育機関の資格認定等を行なう NPO として、2002 年 7 月、セキュリティ・エデュケーション・アライアンス（SEA/J）が設立され、本年 3 月より認定基礎コースが開校の予定。

（注）RSA セキュリティ、大塚商会、ソフトバンク・コマース、ディアイティ、トレンドマイクロ、日本ベリサイン、ヒューコム、マイクロソフトが中心

○政府：2004 年度までに、ISO/IEC15408 に基づく情報セキュリティ評価技術者及び情報セキュリティ設計技術者を育成するため、研修事業に対する助成を実施中。例えば、電子情報技術産業協会（JEITA）が、ISO/IEC15408 に基づくセキュリティ評価のための教育講座を実施しており、輸出企業を中心に 300 名程度が受講している。

○ネットワークリスクマネジメント協会（NRA）が、地方公共団体、政府機関等を対象にセミナーを行っている。

○資格：エンドユーザの国家資格として、中級レベルの「情報セキュリティアドミニストレータ試験」がある（受験者数は平成 13 年秋で約 2．4 万人、合格者数は 1．6 万人）

・情報通信サービスを提供する事業者の専門家の資格講習として、ネットワーク情報セキュリティマネージャ（NISM）が、NISM 推進協議会により平成 13 年に開始（約 300 名を認定。平成 14 年度から、基礎資格、専門資格が追加）。

・IT セキュリティ評価・認証のために、製品評価技術基盤機構（NITE）では、セキュリティターゲット主任評価者の資格付与試験を実施している。

○標準スキル：政府は 2004 年度までに、高度な情報セキュリティ技術者の育成・活用を推進するため、必要な技能の標準を策定し、人材育成プログラム作りを支援する。具体的には、情報処理振興事業協会（IPA）の委託を受けた日本ネットワークセキュリティ協会（JNSA）がスキルマップを作成中で、スキルスタンダードを検討している。

（2）今後の人材育成のあり方

○研究者、教員、高度技術者（注）、運用管理者と、目的やレベルに応じた人材育成を行なう必要がある。

・上級技術者の育成等：通常 7 年必要だが 3 年程度で早急に育成する必要がある。このために、教育プログラムの開発、一定の経験をもつシニア人材の活用も有効である。
なお、ISO/IEC15408 の評価者には、システム開発技術の実務経験が、また、ISO/IEC17799 の運用管理者には、セキュリティマネージメントの実務経験が必要である。

・ユーザ企業等の幹部、セキュリティ管理者、セキュリティ技術者：セキュリティ教育サービスを提供している企業を活用することが考えられるが、その教育内容やレベルの向上については、セキュリティ・エデュケーション・アライアンス（SEA/J）等の活動を促進する。

（注）電子自治体の実現に伴い、全国 3,200 の自治体に運用のための技術者が必要となる。

○国際的な対応等：教員として指導できる人材も乏しいため、企業、研究機関や海外などから幅広く専門家や実務者等を招聘するか、内外の企業や NPO 等と連携し、人材を育てるか、海外の大学や研究機関等への留学を推進する必要がある。海外の連携先としては、例えば米国 SANS 協会等が考えられる。

○教育内容：技術者・研究者の育成の目標を定めるために、スキルマップの開発・見直しを促進する必要がある。

大学等の教育内容については、実務的なウィルス対策、不正侵入対策、セキュリティマネージメントなどと同時に、基礎知識として暗号・電子透かし等とその応用（電子署名、暗号プロトコル等）が必要である。このうち、基礎知識については教科書も整備されてきているが、実務的な知識については、教科書の整備が課題となっている。また、企業と連携し、実習やケーススタディを重視する必要がある。

なお、セキュリティ技術を十分に理解するためには、ネットワーク技術やコンピュータ技術の知識が不可欠である。

○資格：今後、目的やレベルを考慮した国家資格の導入の検討が必要である。また、国際的に評価される SANS 協会の GAIC 認証との連携も図っていく必要がある。

○教育環境：実務的な知識については、攻撃側の行動を分析し適切な対応をとる実地の経験が重要であり、以下のような体制で人材を育成することが有効である。

・実際のシステムの運用監視機能と研究機能を併せ持つ体制
・模擬ネットワークで攻撃と防御をシミュレートできる体制

また、常に最新の教育内容で効率的に人材育成を行なうため、教育用ソフトを作成して、資格制度とリンクした教育を実施することも有効である。

○支援：研究開発振興調整費などを活用して、各地の大学、自治体等における人材育成や拠点整備の動き（参考 7 ）を積極的に活用・支援していく必要がある。また、情報セキュリティに関

する研究開発の中で、同時に人材育成に十分配慮していくことも有効と考えられる。

（３）当面の人材の確保

短期的には、研究能力を国際調達する必要がある。また、上級技術者、特にシステムの監査やセキュリティ評価レビューを行なえる人材が極めて少ないため、当面は海外から招くか海外に委託する必要がある。

（参考１）電子政府構築におけるセキュリティ確保の体制

（１）体制の現状

○各府省（CISO は官房長等）がシステム構築しセキュリティを確保するが、複数省庁のサービスを一元化するワンストップサービスの実施主体は以下のとおり。各省庁のシステムは基本的に独立しており、各省庁が各々セキュリティに関する責任を負う。

・総合行政サービスシステム：行政手続関係の情報へのリンクを提供（総務省）

・特定分野の申請手続き：複数省庁の申請手続きに関連する情報を一括的に処理する場合（関連省庁が共同して実施）

○内閣官房情報セキュリティ対策推進室は、関係省庁と協力し、

・政府の情報システムのセキュリティ確保

・重要インフラ防護のためのサイバーテロ対策

を推進。このうち電子政府については、「電子政府の情報セキュリティ確保のためのアクションプラン」に基づき、各府省のセキュリティポリシーの実施状況等について評価を行うとともに、その結果を踏まえて「情報セキュリティポリシーに関するガイドライン」の改定（H.14.11）などを実施。

○電子政府で調達される IT 製品、システムに対しては、認定されたセキュリティ評価機関により国際規格 ISO/IEC15408 に基づきセキュリティ評価されたものを利用することが推奨されている。

○産業技術総合研究所は、自発的に、汎用ソフトウェアや電子政府システムにおける技術上の問題点をチェックしている。

（２）電子政府の課題

○2003 年の電子政府実現に向けて、システム開発、体制整備、人材育成等の面で、セキュリティ対策の総合的な構築・推進を早急に進める必要がある。

○当面のシステム構築においては、

・現状の実績のある技術を用いて構築。

（注）総務省、経済省の共同事業として CRYPTREC(暗号技術検討会及び暗号技術評価委員会)により、10 年以上安心して利用できるという観点から一定の安全性をもち、電子政府で利用可能な暗号技術のリストアップを実施中。欧州（NESSIE プロジェクト）でも一定以上の安全性をもつ方式のリストアップを進めている。一方、米国では、DES、トリプル DES 等の標準暗号に加え、AES プロジェクトに

より次世代の“Rijndael”を選定し追加した。

・IT 製品・システムの調達にあたって、ISO/IEC15408 に基づくセキュリティ評価・認証制度の活用、CRYPTREC による電子政府推奨暗号の活用を積極的に行なうことが必要。また、情報セキュリティ監査の実施、ISO/IEC17799 に基づく情報セキュリティマネジメントシステム（ISMS）適合性評価制度の活用も必要である。

○セキュリティ管理・評価、監視・運用の体制の問題が大きい。特に自治体においては、これらをアウトソースすることと同時に、サービス企業のレベル向上が重要である。

（参考２）米国における情報セキュリティの最近の動き

１．2000 年　情報インフラ防護のための国家計画 Version1.0

○以下の組織の設立

・情報インフラ防護機関（IIIP）

・６箇所の情報共有分析センター（ISAC）

・国家インフラ保障会議（NIAC）

○研究開発計画の策定、人材育成、官民協力体制等

２．米国国土安全保障省 DHS の設立

ホームランドセキュリティ法（2002 年 11 月 25 日）に基づき、国土安全保障省を設置する。当該省における情報通信セキュリティ関係の体制は、以下のとおり。

○情報分析・インフラ防護担当次官

連邦コンピュータ関連レスポンスセンター（FedCIRC：Federal Computer Incident Response Center）から移管

○科学技術担当次官

国土安全科学技術諮問委員会の設置（次官への勧告等）

国土安全先進研究庁の設置(国土安全研究開発促進基金*の管理運営)

***　2003 年度は 5 億ドル**

○国土安全研究機構の設置（時限 3 年）

重要インフラの脆弱性分析、各種シミュレーション、テストベッドの提供等

３．研究開発

（１）ITR＆D 計画における情報セキュリティ技術の研究開発

・安全な通信のための高度な暗号化と認証技術

・高速無線、有線ネットワークにおいて安全確保、攻撃に対する抵抗力、及び自己回復力を実現する新たな方式

・偵察、自律兵器システムのための組み込み型ネットワークセンサー技術

・ミッションクリティカルなシステムのための高信頼度ソフトウェア設計

（２）サイバーセキュリティ研究開発法（2002 年 11 月 27 日成立）

2003 年以降の 5 年間に、総額約 9 億ドル（約 1,100 億円）の予算を割当てる（現在と比較すると、4 倍以上の増額）

・全米科学技術財団（NSF）が専門家の育成等を行なう
（大学に対し、人材育成への貢献等を条件としたCNSセンターの公募を行なうことを検討中）
・米国立標準技術研究所が研究開発の推進（産学官の共同研究への助成金等）

（３）研究開発の内容

表1　米国家予算による情報セキュリティにおける研究開発
（「情報セキュリティの研究開発」未来工研より）

研究開発項目	件数
①ソフトウエアなどの多様性確保	８
②侵入探知・対応やセキュリティマネージメント	２１
③攻撃に対する弾力性や強靭性のための、暗号・認証、ファイアウオール、フォルト許容システム、次世代言語やセキュアーOS・プロトコル等の次世代技術等	８３
④攻撃に対する迅速な復旧と再構築	３
⑤階層化・分散化・隔離などによる強度向上（モバイルを含む）	１７
⑥攻撃に対する新しい対応メカニズム（免疫性、自己組織化等）	１６

４．その他

情報セキュリティ専門ではないが、政府の情報システム技術者等の育成のため、学習コース検索システムを提供するとともに、高度な専門コースとしてプログラムマネージャ向けSTARプログラムやCIOユニバーシティー（注）等を提供している。

（注）既存の大学と協力し、CIOの持つべき能力の基準「クリンガー・コーエン・コア・コンピタンス」に従い必要な知識を教育

（参考３）韓国における情報セキュリティの現状

１．セキュリティ研究開発体制の経緯

1981 年　韓国電子通信研究所（ETRI）にセキュリティ技術研究所設置
1990 年　韓国情報通信セキュリティ学会設立
1996 年　韓国科学技術院（KAIST）に情報セキュリティセンター（KISA）設置。（ETRI 及び韓国電算院の情報セキュリティ専門家を糾合）
1999 年　ETRI に国家セキュリティ技術研究所設置
国家ネットワークのセキュリティに関する技術開発と政策支援
→KISA は民間の情報セキュリティ支援に移行
（情報セキュリティシステム評価・認証、ハッキング等相談支援）

２．法制度

情報通信基盤保護法
情報セキュリティ専門業者指定制度

３．ハッキング大会

2000 年　「第 1 回世界情報保護オリンピア」
KAIST 主催、ハッカースラブ（情報セキュリティ会社）運営
海外 21 ケ国 711 チームが参加したが、韓国チームが入賞独占
・第 1 段階通過の 128 チームのうち、外国チームは 14 のみ。
（米国は 297 チーム中 6、日本は 149 チーム中 2 など）
2001 年　「第 2 回世界情報保護オリンピア」開催（詳細不明）

４．韓国国内大学・大学院の情報セキュリティ関連学科学生数の現状

分類	大学名	学生数		備考	URL
		2001	2002		
学部課程（７）	ｷｮﾝｳｫﾝ大	ー	50		http://www.kyungwon.ac.kr/
	ﾓｸｳｫﾝ大	ー	40		http://www.mokwon.ac.kr/
	ﾓｯﾎﾟ大	ー	48		http://www.mokpo.ac.kr/
	ｽﾝﾁｮﾝﾋｬﾝ大	42	42		http://www.sch.ac.kr/
	ﾁｭﾝﾌﾞ大	30	40		http://www.joongbu.ac.kr/
	ﾎｿ大	ー	60	ｺﾝﾋﾟｭｰﾀ工学部：240 人	http://www.hoseo.ac.kr/
	ｾﾐｮﾝ大	ー	50	ｲﾝﾀｰﾈｯﾄ情報学部：150 人	http://www.semyung.ac.kr/
大学院課程（１８）	ｺﾝｸﾞｸ大	20	25		http://www.konkuk.ac.kr/2002/
	ｷｮﾝｷﾞ大	23	25	情報保護技術学科	http://www.kyonggi.ac.kr/
	ｷｮﾝﾌﾞｸ大	17	22	情報保護学科	http://www.kyungpook.ac.kr/
	ｸｧﾝｳﾝ大	11	3		http://www.kwangwoon.ac.kr/
	ｺﾘｮ大	45	75		http://www.korea.ac.kr/
	ﾀﾝｸﾞｸ大	11	7		http://www.dankook.ac.kr/index.jsp
	ﾄﾝｸﾞｸ大	45	50		http://www.dongguk.edu/default.asp
	ﾌﾟｷﾞｮﾝ大	ー	13		http://www.pknu.ac.kr/
	ﾖﾝｾ大	3	3		http://www.yonsei.ac.kr/yu/index.html
	ｲﾌｧ女子大	9	7		http://www.ewha.ac.kr/
	ﾁｮﾝﾅﾑ大	16	18		http://www.chonnam.ac.kr/
	ﾁｭﾝｱﾝ大	30	13		http://www.cau.ac.kr/
	ﾁｬﾝｳｫﾝ大	9	5		http://www.changwon.ac.kr/
	ﾎﾟﾊﾝ工大	12	5		http://www.postech.ac.kr/
	韓国航空大	ー	10		http://www.hangkong.ac.kr/main.asp
	ﾊﾝｾ大	6	6		http://www.hansei.ac.kr/
	KAIST（韓国科学技術院大）	10	10	学制専攻運営中	http://www.hansei.ac.kr/
	情報通信大学院大学校	12	25		http://www.icu.ac.kr/
大学院課程	ｿﾝｷﾞｭﾝｸｧﾝ大	1	1		http://www.skku.ac.kr/
特殊大学院		15	18	情報保護学科	
一般大学院	ｽﾝﾁｮﾝ航大	5	6		http://www.sch.ac.kr/
特殊大学院		15	4		
計		387	681		

出典　韓国国家情報院　「2002　国家情報保護白書」

（参考４）　情報セキュリティの研究開発動向（分析例）

表１　情報セキュリティ技術の研究開発動向の国際比較

「情報セキュリティ技術の研究開発課題」（未来工研）より

分　野	主な情報セキュリティ技術用語	国内論文		海外論文	
要素技術	認証 certification	(33%)	185	(29%)	1349
	アクセス管理 access control	(6%)	35	(28%)	1303
	暗号 encryption	(47%)	261	(14%)	644
	デジタル署名 digital signature	(2%)	10	(4%)	184
システム技術	ウィルス対策 virus	(1%)	5	(6%)	278
	セキュアネットワーク secure network	(0%)	0	(3%)	146
	修復 recovery	(4%)	23	(3%)	127
	脆弱性(分析)vulnerability	(0%)	0	(4%)	178
	リスクアセスメント risk assessment	(6%)	36	(3%)	163
	相互依存性 interdependency	(1%)	6	(1%)	65
社会技術	リスクコミュニケーション risk communication	(0%)	0	(3%)	123
	セキュリティユーザインタフェース security user interface	(0%)	0	(3%)	136

（注）国内論文：「電子情報通信学会」及び「情報処理学会」論文誌等での全文検索による単語出現件数（前者は 1994 年、後者は 1979 年以降。カッコ内は比率）

海外論文：「ＩＥＥＥ」および「ＡＣＭ」学会誌での全文検索による過去１０年の単語出現件数（カッコ内は比率）

いずれも、2000 年 4 月 25 日現

「情報セキュリティ技術の研究開発課題」（未来工研）より

表２　我が国における情報セキュリティ技術の研究開発概況（1/2）

技術分類				開発段階			研究開発の方向性の例
大項目	中項目	小項目	具体的内容例	理論	開発	実用	
要素技術	識別・認証技術	1）記憶による方法	ﾊﾟｽﾜｰﾄﾞ、暗証番号等			◎	＞マルチモーダル認証技術 ＞リアルタイム認証技術
		2）持ち物による方法	IDカード、ｽﾏｰﾄｶｰﾄﾞ等		○	◎	＞プライバシー保護への配慮 （プライバシー侵害を不可能にする技術）
		3）生体的特徴による方法 （バイオメトリクス）	指紋・虹彩・声紋・筆跡照合		◎	○	＞容貌による認証 ＞入手・複製困難なバイオメトリクス
	アクセス管理技術	1）アクセス制御技術	ファイアウォール		○	◎	＞インテリジェントファイアウォール ＞高速ファイアウォール ＞ファイアウォールの階層化・セグメンテーション化
		2）不正アクセス検知・追跡技術	侵入検知システム（IDS）		◎	○	＞リアルタイム追跡技術
			ログ管理・解析技術 安全なログ保管技術		○ ○	○	＞ソフトウェアエージェント
		3）コンテンツフィルタリング	フィルタリングソフトウェア		○	○	
	守秘技術	1）暗号技術	共通鍵暗号		○	◎	＞超高速暗号技術
			公開鍵暗号（RSA） 次世代公開鍵（AES）		○ ◎	◎	＞楕円曲線暗号 ＞情報論的に安全な方式(量子暗号等) ＞暗号と人のインターフェース ＞暗号モジュール化技術
		2）暗号安全性評価技術	差分解読・線形解読他		○	○	
		3）通信秘匿技術	暗号鍵回復技術	○	◎ ○	○	＞暗号ブレイク対応技術 ＞暗号解読技術 （暗号技術の悪用への対応） ＞暗号強度評価技術
	完全性保持技術	1）電子透かし技術	共通鍵的な電子透かし		◎		＞公開鍵的な電子透かし
		2）電子署名技術	デジタル署名・電子捺印		○	○	＞署名のヒューマンインターフェース

（略号）AES: Advanced Encription Standard

表2　我が国における情報セキュリティ技術の研究開発概況(2/2)

技術分類				開発段階			研究開発の方向性の例
大項目	中項目	小項目	具体的内容例	理論	開発	実用	
システム技術	耐力保持技術	1) ウィルス対策技術	ウィルスワクチン		○	◎	＞免疫学的知見の応用
			ウィルス情報自動配信システム		○	◎	＞ウィルス伝播防止技術
	セキュアネットワーク	1) バーチャルプライベートネットワーク(VPN)	セキュアなIPーVPN技術(IPSec, L2TP等)		◎	○	＞高速ＶＰＮ分離技術 ＞ポリシー自動学習アルゴリズム
		2) セキュアなワイヤレスネットワーク	WTLSなど		◎	○	＞Wireless LANs、Home Networks、Wearable Networksのセキュリティ保証
		3) セキュアなグリッド・コンピューティング	ワンステップ認証技術		○		
			最適資源配分		○	○	
	セキュアなソフトウェア	1) セキュアOS	セキュリティ・カーネル	○	○		＞次世代マイクロカーネル
		2) セキュアな言語					
		3) セキュアなアプリケーション					
		4) モバイルソフトウェアのセキュリティ					＞モバイルソフトウェアの信頼性保証技術
	相互接続性保証	1) システム・インタビリティ	PKI(公開鍵基盤)		○	○	
			複数認証機関の相互運用性の確保		○	○	
	リカバリ・システム	1) 被害予測システム	ウィルス流行警報システム		○		＞複数ＤＢからの情報共有・侵入警報・自動回避システム
			影響シミュレーションモデル	○	○		＞被害限定プログラム
		2) 修復システム	機能代替・切替システム		○		＞自動修復システム
			内部システムセグメント化		○		
			セキュリティホール自動検出		○		
	システムセキュリティ評価	1) システム評価技術	脆弱性・機能強度・対策分析		○	○	＞異分野システムの相互連関分析 ＞セキュアなソフトウエア・アーキテクチャ ＞組み合わせシステムの強度評価
		2) リスクアセスメント技術	コスト・ベネフィット分析	○	○		＞セキュリティ意志決定支援システム
社会技術	個人レベル	1) ハッカー・クラッカーの行動科学的分析	ハッカーの社会心理学的分析	○			＞クラッカーの行動パタン分析
		2) セキュリティユーザインタフェース	安心感の持てるセキュリティシステム		○		
	集団レベル	1) セキュリティとプライバシーの両立	パーソナル情報機器のプライバシー対策	○	○		＞次世代モバイル環境への対応 ＞情報倫理についてのコンセンサス形成手法
		2) 電子コミュニティでの信頼・リスク認知	ＥＣにおける信頼形成要因分析	○			
		3) 電子的コミュニケーションプロセス分析	「噂」の伝播メカニズム分析	○	○		＞チェーンメールのルート解析
		4) 新たな社会的格差の発生	新たな情報格差の発生	○			＞情報リテラシー対策(教育・研修)
	社会レベル～国際レベル	1) セキュリティ相互依存分析	複合システム連関分析	○	○		＞ネットワーク・カタストロフィモデル
			ヘテロなセキュリティシステム	○	○		＞冗長性のある社会システム構築
		2) 総合安全保障としての情報セキュリティ	セキュリティ技術の地政学的分析	○	○		＞総合安全保障における暗号技術の役割
		3) グローバルなＥＣ環境の展開	国際e-ビジネスのセキュリティ対策	○			

(略号) VPN: Virtual Private Network　IPSec: IP Security Protocol　L2TP: Layer2 Tunnelling Protocol　WTLS: Wireless Transport Layer Security

(注) Blue Tooth: PC, 携帯電話, PDAなどをワイヤレスLAN経由でネットワークに接続するためのハードウェア仕様。30～100フィート(9～30メートル)の見通し距離でデータの送受信が

（参考５）科学技術振興調整費【新興分野人材育成（基盤ソフトウェア）】のセキュリティ関係既存施策

（平成１３年度開始）

○「セキュリティ技術者養成センター」（早稲田大学　村岡洋一教授）

- 理工学部ネットワーク社会総合研究所に「ネットワーク技術者養成センター」を設立し、学内および産からの客員教授でセキュリティ技術者等を養成
- 学士／修士レベルを 60 人／年、博士レベルを 4,5 人／年、育成
- またインターネット等による遠隔授業を行う（数百人／年の学外利用を想定）

○「セキュア・ネットワーク人材育成」（大阪大学　西尾章治郎教授）

- 学内キャンパスネットワークを用いて、実運用ネットワークにおけるセキュリティ運用・不正アクセス対策でリーダーシップを取れる知識と経験を有する人材を育成
- 大学院生、学部生、社会人を含め、開始後３年までに 30 人、５年までに 50 人の人材を育成

（参考６）中央大学における情報セキュリティ人材育成

１．趣旨

従来、情報工学専攻、電気電子情報通信工学専攻、数学専攻などで行なわれてきた研究を統合し、情報セキュリティに関する総合的な技術的な知識を獲得し，実際にそれを実現し，安全性を確認する手段を得られるような高度な研究教育を行うため、4 月に情報セキュリティ副専攻を設置し、安全な電子社会の構築のための法的課題の知識も取得させる。修了者には、修了証書を授与する。なお、本件は COE の一環でもある。（なお、本件とは別に、独立研究科の設置も検討中。）

２．設置科目（７科目）

①電子社会と情報セキュリティ（2 単位、必修）
②暗号と電子認証（2 単位、必修）
③ネットワークセキュリティ（2 単位、必修）
④システム監査 I, II（各 2 単位、選択）
⑤情報セキュリティ法制 I，II（各 2 単位、選択）
（注）講義の他、「特別演習」におけるリサーチ・ペーパーを作成。

（参考７）自治体等の動きの例：秋葉原ＩＴセンター（仮称）

１．今後の予定

平成１５年５月着工、１７年２月一部開設、１８年２月全面開設

２．求められる最小限の機能

（１）集客等機能

ショールーム、コンベンションホール、多機能イベントホール等、デジタルワークショップ

（２）産学連携機能

産学の出会のプラットホーム。新産業の創出や人材育成の拠点とする

①サテライト連合大学院

複数の電子情報通信系関連の大学院研究室で構成される研究・教育機関の集合体。総学生数は、年間２５０名程度とし、先端技術分野での新産業創出拠点として、高度な専門分野における研究開発および人材育成を行う。

（研究分野）電子・通信、福祉・ロボット、国際メディア、環境情報等

②プロフェッショナル教育センター

企業の中核技術者等を対象に、情報通信技術の高度技術者の育成を行う、遠隔教育をベースとした専門教育機関。世界中の優良な教育コンテンツの収集等、海外の大学との連携や、インターネットを活用した遠隔教育を行い、サテライト連合大学院、起業センターと連携を図る。

（参考）対象科目：ネットワーク技術、電子回路設計技術、ソフトウェア開発技術等、総学生数：１万人/年（最終目標）

③起業センター（インキュベーションセンター）

施設の提供やマーケットリサーチ、特許等の知的所有権保護、資金面での相談等の支援を行い、サテライト連合大学院、プロフェッショナル教育センターと連携した技術開発サポート、経営支援人材のネットワーク形成を図る。

④総合情報センター

国内外の情報通信関係の電子図書館。

⑤プレゼンテーションセンター

⑥産学連携のプラットホーム

産業と大学の出会いや、交流の場（プラットホーム）の仕組みを構築

（３）情報ネットワーク機能

①秋葉原ＩＴ拠点情報センター

②学びと創造の場（ネットカフェや展示施設など）

③データセンター